Extracting Information from Network Data

Manish Karir, Jon Oberheide
Merit Network, Inc.

Dionysus Blazakis
University of Maryland
Outline

• The Problem
• BGP/Routing Information
  – BGP-Inspect – Information Extraction from BGP Update messages
  – VAST – Internet AS topology Visualization
• Netflow/Traffic Information
  – Flamingo – Internet Traffic Exploration
• Conclusions
The Problem

• Large amounts of data are now, or soon will be available:
  – Route Views, RIPE Archives, PREDICT, etc

• The problem is no longer access to raw data but how to extract useful information from the raw data

• Need tools that can:
  – Scale to large input datasets
  – Provide useful data summarizations
  – Are easy to use
  – Provide useful information

• BGP-Inspect, VAST, Flamingo are tools that we have implemented that attempt to address this problem
BGP-Inspect: Why and What

• Analyzing MRT Data:
  – Large volumes of data ~RV-66G compressed
  – Extracting useful information requires writing custom parsers even for basic information
  – Lots and lots of redundancy

• Approach:
  – Preprocess Route Views data
  – Remove redundancy as much as possible
  – Use data compression to the extent possible
  – Build efficient indices to help queries
  – Pre-compute and store commonly used statistics at data load time not at query time
  – Build easy to use interface
BGPdb vs. BGP-Inspect

- BGPdb is the core of the BGP-Inspect system
- BGPdb represents the pre-processed database, which is queried by the BGP-Inspect interface
BGPdb – Techniques and Algorithms

- Removing redundancy from BGP datasets
  - ASPATH, COMMUNITY, UPDATE msgs are repeated over and over, only time changes

- Compressed-Chunked Files
  - Compromise between size and usability

- B+ Tree indices
  - Indexing based on time, this enables fast time-range queries

- Caching while processing input datasets
  - Messages are repetitive, so keep cache of previous processing for speedup
BGPdb – System Architecture
BGP-Inspect Interface
Global Queries – Most Active ASes
Raw Data Analysis – AS Query

BGP-Inspect-Routeviews

Global Summary Queries: (Please select a peer, query type and duration)

Peer:
- [P1: 5.5.5.1 - AT&T]
- [P2: 6.6.6.2 - Level 3]
- [P3: 7.7.7.3 - AT&T]
- [P4: 8.8.8.4 - Telstra]
- [P5: 9.9.9.9 - BT]

Duration:
- Last 1 Day
- Last 7 Days
- Last 30 Days
- Last 90 Days
- Last 365 Days

Submit Query

Raw Data Analysis: (Please select a peer, query type, AS, prefix, and time range)

Query Type:
- [P1: IPv4 prefix]
- [P2: IPv6 prefix]

Start Date:
- [P1: 0000-01-01]
- [P2: 2020-01-01]
- [P3: 0000-01-01]
- [P4: 2020-01-01]

End Date:
- [P1: 0000-12-31]
- [P2: 2020-12-31]
- [P3: 0000-12-31]
- [P4: 2020-12-31]

Submit Query

BGP-Inspect-Routeviews

Peer: Aggregate

AS: 145 (MCC-194 MCI Communications Corporation)

Total Number of prefix announcements

Query Summary Statistics

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Time Range Start</td>
<td>June 8, 2006, 12:00 am +0000</td>
</tr>
<tr>
<td>Query Time Range End</td>
<td>June 8, 2006, 12:00 am +0000</td>
</tr>
<tr>
<td>Total Number of Prefixes (All Peers)</td>
<td>16119</td>
</tr>
<tr>
<td>Total Prefixes - 12.0.1.63</td>
<td>4786</td>
</tr>
<tr>
<td>Total Prefixes - 4.68.0.243</td>
<td>6</td>
</tr>
<tr>
<td>Total Prefixes - 64.895.122.1</td>
<td>0</td>
</tr>
</tbody>
</table>

Copyright © Merit Network Inc.
Copyright © University of Maryland
Raw Data Analysis – AS Query

BGP-Inspect-Routeviews

Peer: 144.228.241.81
AS: 145 (MCC-194 MCI Communications Corporation)

Query Summary Statistics
- Query Time Range Start: June 8, 2006, 12:00 am +0000
- Query Time Range End: June 20, 2006, 12:00 am +0000
- Total Prefixes: 144
- Time to run query: 12.273 seconds

Prefixes Announced

<table>
<thead>
<tr>
<th>Time</th>
<th>Prefix</th>
<th>AS Path</th>
<th>Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 8, 2006, 11:01 am +0000</td>
<td>140.219.134.0/24</td>
<td>3549/1239</td>
<td>5949:1011 5949:16840</td>
</tr>
<tr>
<td>June 9, 2006, 11:02 am +0000</td>
<td>140.219.134.0/24</td>
<td>3549/1239</td>
<td>5949:16840</td>
</tr>
<tr>
<td>June 8, 2006, 11:02 am +0000</td>
<td>140.219.134.0/24</td>
<td>3549/1239</td>
<td>5949:16840</td>
</tr>
<tr>
<td>June 8, 2006, 12:06 am +0000</td>
<td>140.219.134.0/24</td>
<td>3549/1239</td>
<td>5949:16840</td>
</tr>
</tbody>
</table>
Raw Data Analysis – Prefix query
Raw Data Analysis – Prefix query

Peer: 66.185.128.1
Prefix: 140.219.134.0/24

Query Summary Statistics
- Value
  - Query Time Range Start: June 6, 2006, 12:01 am +0000
  - Query Time Range End: June 6, 2006, 12:36 am +0000
  - Total Update Messages: 195
  - Total Advertisement Messages: 44
  - Maximum AS Path Length: 6
  - Average AS Path Length: 2.83
  - Origin AS Changes: 6
  - Number of Unique ASes: 1
  - Origin AS List: 145
  - Time to run query: 9,012 seconds

Prefix Announcements:
- Time
- Type
- AS Path
- Communities

<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>AS Path</th>
<th>Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
<tr>
<td>June 6, 2006</td>
<td>a</td>
<td>13549 1239 22204</td>
<td>3549:2193 3549:30846</td>
</tr>
</tbody>
</table>
BGP-Inspect: Current State

BGP-Inspect – Beta v0.5
http://bgpinspect.merit.edu

Dataset: August 1, 2005 - Present
Current BGPdb size: 170GB
Currently indexing data for 5 peers (AT&T, Level 3, AOL, Sprint, Global X)

- Example queries (per peer, 1,7,10 days):
  - Most active AS’s
  - Most active prefixes
  - Prefixes with most OriginAS changes

- Raw Data Analysis (per peer)
  - Prefix/AS, Time Range
  - Uniques prefixes by AS
  - OriginAS changes for a prefix
  - Time to run query
  - More specific prefixes announced
BGP-Inpsect: Current State (2)

- Equipment
  - Dell 2650 - Web and DB server
  - Dell 2850, dual Xeon with NFS mounted 500GB SATA

- Traffic?
  - ~30+ unique IPs per day
BGP-Inspect Next Steps

• BGP-Inspect is available at http://bgpinspect.merit.edu and your feedback is very much appreciated.

• Future…
  – More interesting things with the multiple peer response UI (different ways of highlighting the differences between peers)
  – pyBGPdb - a python interface to the BGPdb database providing fast raw queries
Outline

• The Problem
• BGP/Routing Information
  – BGP-Inspect – Information Extraction from BGP Update messages
  – VAST – Internet AS topology Visualization
• Netflow/Traffic Information
  – Flamingo – Internet Traffic Exploration
• Conclusions
VAST – Visualizing AS Topology

- VAST allows users to easily navigate, and explore various topological properties and features extracted from raw BGP update messages.
- VAST uses both a quad-tree based algorithm as well as an octo-tree based method to build various visualization.
- The ability to navigate the three dimensional space to fully explore the dataset make VAST a unique tool.
The Basic Quad-Tree

00

01

10

11

First Bit

Second Bit

0

1
Octo-Tree Algorithm

![Octo-Tree Algorithm Diagram](image-url)
VAST - Visualization Methods

- Out-degree per AS
- Per AS unique prefix originations
- AS topology with line scaling:
  - Peer out-degree
  - Frequency with which AS pair is seen
  - Unique prefixes with certain AS pair
  - Total address space over an AS pair
VAST – Techniques

- Position of a node determined by quad/octo-tree
- Size determined by out-degree of node, larger out-degree -> larger size
- Color determined by out-degree of node, larger out-degree -> more yellow
- Line thickness depends on various factors(selectable), out-degree of neighbor, number of prefixes, address space size, or frequency of messages
- 3D navigation of visualization, slider bar controls, selectable listing of displayed information to control/filter what is being displayed
VAST – ASN Distribution

AS 1239
AS 701
AS 7018
VAST - AS CORE
VAST – AS CORE
VAST – AS CORE
VAST – AS CORE
VAST – AS CORE
VAST – AS CORE (500 Club)
VAST – AS9121 connectivity
VAST – AS9121 connectivity
VAST – AS9121 connectivity
VAST – AS9121 connectivity
VAST – AS9121 Route Leakage
VAST – AS9121 Route Leakage
VAST – AS Out-degree
VAST – Unique Prefix
Outline

• The Problem
• BGP/Routing Information
  – BGP-Inspect – Information Extraction from BGP Update messages
  – VAST – Internet AS topology Visualization
• Netflow/Traffic Information
  – Flamingo – Internet Traffic Exploration
• Conclusions
Flamingo – Visualizing Internet Traffic Data

• Introduction: What is Flamingo
• Visualizations
• The Flamingo Tool
  – Combining visualization with controls
• Case Studies
  – Traffic Anomaly
  – Network Scans
  – Worm traffic
  – P2P traffic
  – The Slashdot effect!
Flamingo - Introduction

• Flamingo is a unique software tool that enables 3D Internet traffic data exploration in real-time
• Provides a series of different visualization methods to illustrate different aspects of the data
• Based on information extracted from netflow records
• Includes additional tools/filters to allow people to easily extract “information” from raw netflow data
Introduction: Flamingo Architecture

- **Client/Server Architecture**
- A single server can support multiple clients
- A single server can act as collector for multiple netflow feeds
- Supports both aggregation as well as non-aggregation mode
Flamingo - Visualization Methods

- Based on Extended Quad-Tree Implementation
- Traffic Volume by src/dst IP prefix
- Traffic Volume by src/dst AS
- Traffic distribution across src/dst ports
- Traffic flows between src/dst IP prefixes
- Traffic flows between src/dst IP/ports
The Basic Quad-Tree
Traffic Volume by Src/Dst IP

• The 2D quad-tree map is used as the base of a visualization cube
• We plot prefixes from a BGP routing table onto the base of the cube, size of prefix determines size of representation on 2D base
• Longest prefix match is used to map netflow IP addresses onto BGP prefixes
• The z-axis/height is used to represent the volume of traffic
• Different color is used for each prefix
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>…/8</td>
<td></td>
</tr>
<tr>
<td>…/16</td>
<td></td>
</tr>
</tbody>
</table>
Traffic Flows by Aggregated Src/Dst IP

• Flows contain source and destination information, which might map to 2 different prefixes, so far we only have the ability to represent a single flow
• Solution: Use 2 inside surfaces of a cube, one for source, one for destination, represent a flow by a line between them
• Thickness of line represents relative traffic volume
Traffic Flows by Src/Dst IP and Port

• Flows contain source/destination port number information as well

• Solution:
  – Use base of cube to represent prefixes, both source and destination are on the same base
  – The z-axis is used to represent port numbers, source and destination
  – (srcIP, srcPort) >>>>>>>>>> ((x1,y1), z1)
  – (dstIP, dstPort) >>>>>>>>>> ((x2,y2), z2)
  – Line between these 2 points in 3D space represents a flow from (srcIP, srcPort) to (dstIP, dstPort)
  – Line thickness represents relative volume of traffic
  – Same color used for all flows with same source IP
Flamingo Visualization Tool
Flamingo Controls

Text Representation of Visualized Information

![Image of Flamingo Controls]

Slider Bar Controls

Address Range Configuration
Case Study: Traffic Anomaly Sunday- Oct 16, 2005

- Large burst of traffic visible outgoing from 141.213.x.x(x.x.umich.edu)
- Start time roughly – 12PM - End time roughly – 6PM
- Single srcIP/port – few(4) targetIP’s/multiple ports
- UDP flows
- Traffic pattern visible in the normal clutter
- We then proceed to examine the src (141.213.x.0/24) and target prefixes (216.74.128.0/18, 217.199.32.0/19) in more detail in the following sequence of images
Overall Traffic Pattern at Primary Router Sunday, Oct16 2005

Anomaly
Traffic Volume sourced from /24 subnet by individual hosts

Src IP Addresses
141.213.x.0/24

5 million flows

141.213.x.x/32
Distribution of Target IP Addresses

<table>
<thead>
<tr>
<th>Src IP Addresses</th>
<th>Dst IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>141.213.x.0/24</td>
<td>217.74.x.248.0</td>
</tr>
<tr>
<td>217.74.x.249.32</td>
<td>217.74.x.250.32</td>
</tr>
<tr>
<td>217.74.x.251.32</td>
<td>217.74.x.252.32</td>
</tr>
<tr>
<td>217.74.x.253.32</td>
<td>217.74.x.254.32</td>
</tr>
</tbody>
</table>

Few (4) Specific Target IP’s

Source IP Addresses: 141.213.x.0/24
Distribution of flows in terms of src/dst ports/protocol

One or two Src Ports

Dst ports Vary 0-65K
Case Study: Worm Traffic/Port 42 Scans

Scan:
Dst: 35/8 Port:42
Src: 219.188.209/24 Port: various
Case Study: /24 Network Scan
ssh scans
ssh scan
Case Study: Slashdot Event Oct 31, 2004

Traffic Volume

Flow Volume
Zotob Worm Infection
P2P Traffic
Dark-space Traffic Visualization
Conclusion

• Obtaining raw data from networks is becoming easier, however using it effectively continues to be challenging

• Tools are the key in making raw data useful

• Operators often know what they are looking for, we should just make it easier for them to quickly get the information they need; there is some incident that is brought to their attention etc.

• Visualization can help to understand complex multi-dimensional data, instead of a database based query-response system which does not allow you to easily “explore” your data