

Tools and Techniques for the Analysis of Large Scale BGP Datasets

Manish Karir, Larry Blunk (Merit)

Dion Blazakis, John Baras (UMd)

The Problem

- Large amounts of data are now, or soon will be available:
 - RouteViews, 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
 - Goal is to attempt to make it easier to use raw data from archives such as RouteViews, by pre-processing, reformatting and indexing the data

Outline

- BGP::Inspect and BGPdb
 - Architecture, Techniques, Algorithms
- BGP::Inspect Interface
 - Basic queries, Global Summarizations
 - Detailed specific queries, AS/Prefix
- Case Study 1 – The AS9121 Incident
- Case Study 2 – Prefix Hijacking Example
- Conclusions, Future Work and Discussion

BGP::Inspect

- 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 RouteViews 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

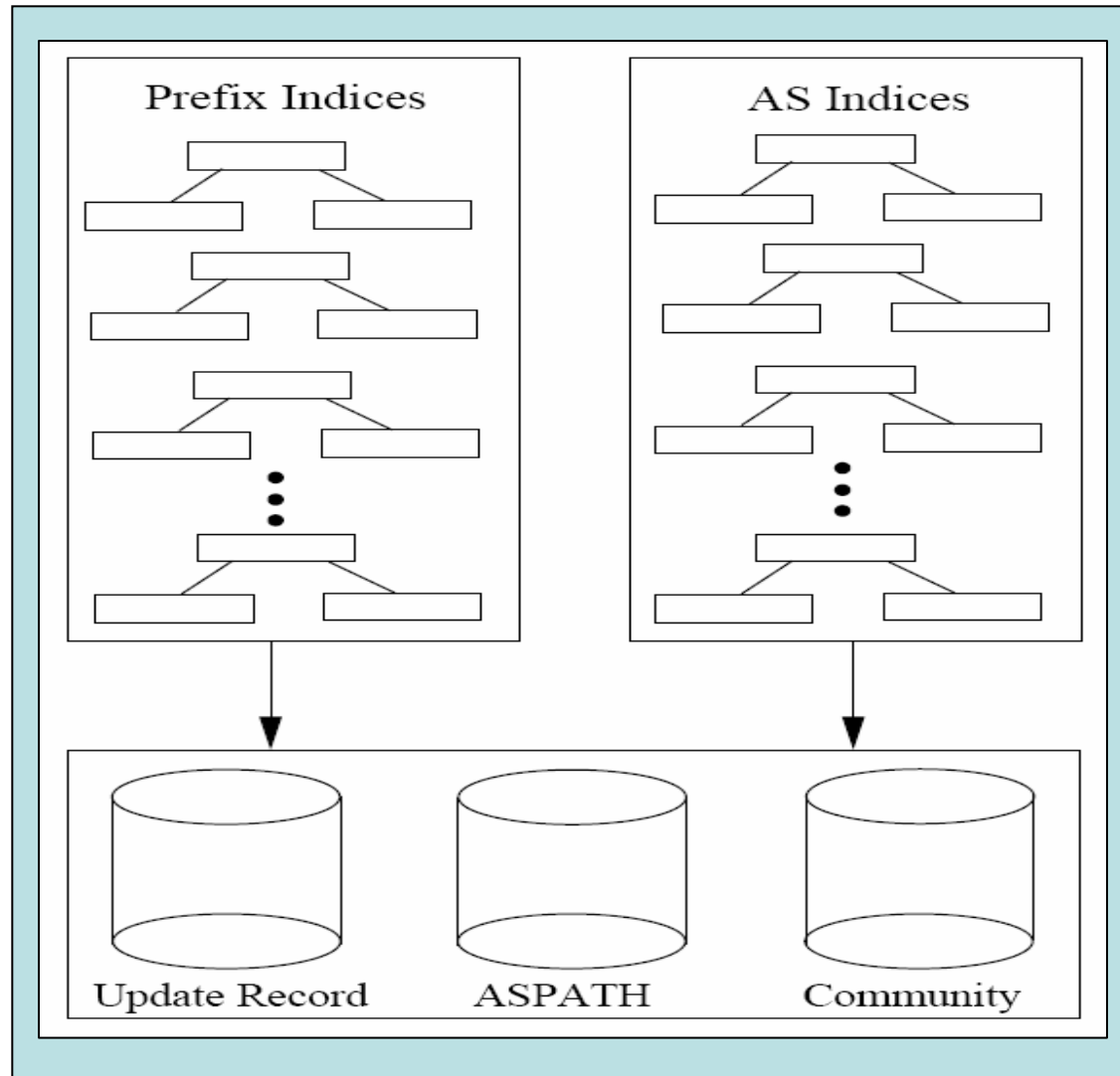
BGPdb

- BGPdb is the core of the BGP::Inspect system
- BGPdb represents the pre-processed database, which is queried by the BGP::Inspect interface
- Provides some useful techniques that maybe applied to processing other large datasets not just BGP datasets

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



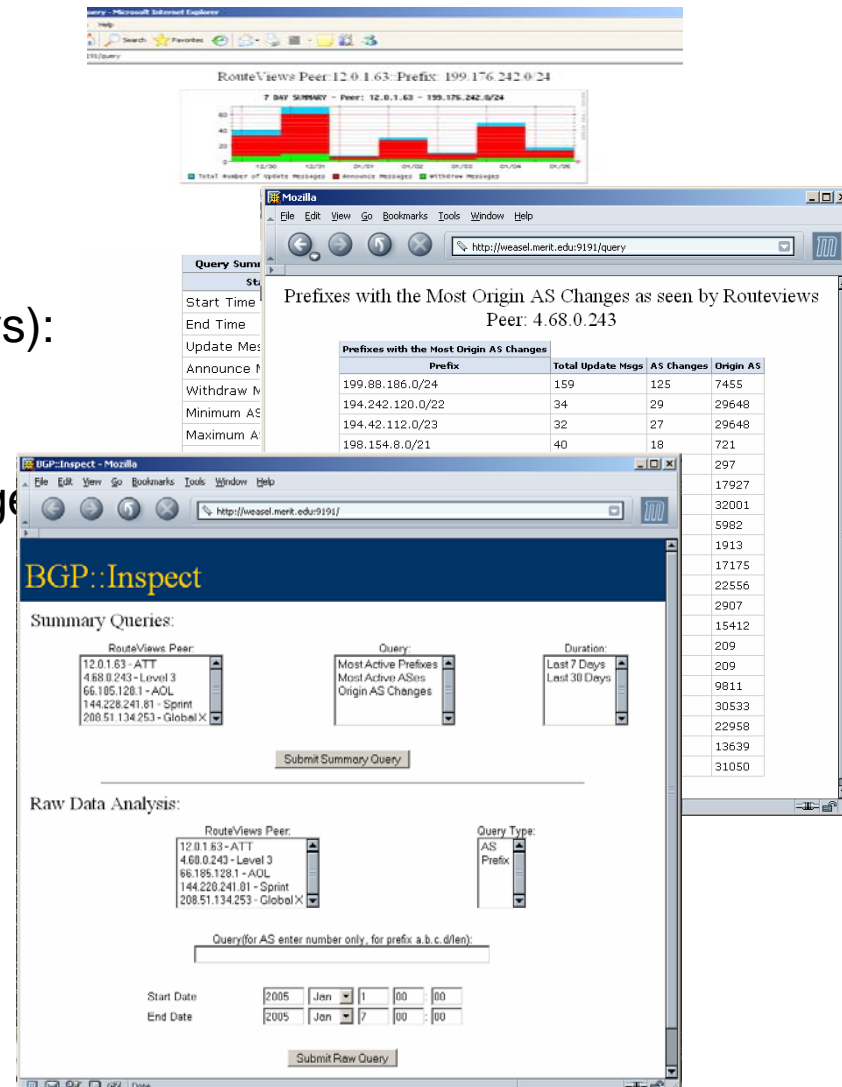
BGP::Inspect

BGP::Inspect – Beta v0.2

<http://weasel.merit.edu:8080>

Dataset: Jan1- March31 2005

- Example queries (per peer, 1,7,30 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::Inspect Interface

The screenshot shows a Mozilla browser window titled "BGP::Inspect - Mozilla" with the address bar containing "http://weasel.merit.edu:8080/". The page header features the "BGP::Inspect" logo and database update information: "First DB Update: Sun Jan 1 00:00:00 2005" and "Last DB Update: Fri Apr 1 00:01:59 2005".

The interface is divided into two main sections:

- Global Summary Queries:** (Please select a RouteViews Peer, Query Type and Time Interval)
 - RouteViews Peer:** A dropdown menu with options: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - AOL, 144.228.241.81 - Sprint, and 208.51.134.253 - GlobalX.
 - Query Type:** A dropdown menu with options: Most Active ASes, Most Active Prefixes, Prefixes Most Announced, Prefixes Most Withdrawn, and Prefixes with Most AS Changes.
 - Duration:** A dropdown menu with options: Last 1 Days, Last 7 Days, and Last 30 Days.
 - A "Submit Query" button is located below the dropdowns.
- Raw Data Analysis:** (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)
 - RouteViews Peer:** A dropdown menu with the same options as the Global Summary Queries section.
 - Query Type:** A dropdown menu with options: AS, Prefix-Exact, and Prefix-More Specific.
 - Query:** A text input field with the placeholder "(ASN or a.b.c.d/en)".
 - Start Date:** A date selector showing 2005, Jan, 1, 00:00.
 - End Date:** A date selector showing 2005, Jan, 7, 00:00.
 - A "Submit Query" button is located below the date selectors.

At the bottom of the page, the following copyright information is displayed: "Copyright(c) Merit Network Inc." and "Copyright(c) University of Maryland". The browser's status bar at the bottom shows "Done" and various system icons.

Global Queries – Most Active ASes

BGP::Inspect First DB Update: Sun Jan 1 00:00:00 2005
Last DB Update: Fri Apr 1 00:01:59 2005

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT
 4.68.0.243 - Level 3
 66.185.128.1 - AOL
 144.228.241.81 - Sprint
 208.51.134.253 - GlobalX

Query Type: Most Active ASes
 Most Active Prefixes
 Prefixes Most Announced
 Prefixes Most Withdrawn
 Prefixes with Most AS Changes

Duration: Last 1 Days
 Last 7 Days
 Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.0.1.63 - ATT
 4.68.0.243 - Level 3
 66.185.128.1 - AOL
 144.228.241.81 - Sprint
 208.51.134.253 - GlobalX

Query Type: AS
 Prefix-Exact
 Prefix-More Specific

Query: (ASN or a.b.c.d/men)

Start Date: 2005 Jan 1 00:00
 End Date: 2005 Jan 7 00:00

Submit Query

Copyright (c) Merit Network Inc.
 Copyright (c) University of Maryland

RouteViews Peer: 12.0.1.63

Most Active ASes, Last 7 Days

Top 20 Most Active ASes:			
Rank	AS Number	AS Name	Number of Announcements
1	14846	NBCINT-3 NBC Internet	929972
2	3921	GENERA General Electric Company	865959
3	1295	GENERA-2 General Electric Company	830059
4	19981	HELLER-23 Heller Financial Inc.	189783
5	21617	NARA National Archives and Records Administration	145706
6	23155	HARRIS-61 Harrisonville Telephone Company	136222
7	7018	ATTW AT&T WorldNet Services	51673
8	16581	THETIT-3 The Titan Corporation	42252
9	10968	CARGIL-9 Cargill Incorporated	32871
10	2386	ADCS-1 AT&T Data Communications Services	30912
11	6318	CHECKF CheckFree Corporation	28170
12	14060	NNC-16 National Network Corporation	26950
13	12062	DECISI-34 Decision One	23737
14	80	GENERA-2 General Electric Company	21255
15	24219	NFI-AS-AP No Fuss Internet	19166
16	9829	BSNL-NIB National Internet Backbone	15717
17	14689	AES-2 A.G. Edwards & Sons, Inc.	14085
18	306	DNIC DoD Network Information Center	13628
19	27343	MONSA Monsanto	10252
20	3464	ASC Alabama Supercomputer Network	9544

Global Queries: Most OriginAS Changes

BGP::Inspect - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/

BGP::Inspect

First DB Update: Sun Jan 1 00:00:00 2005
Last DB Update: Fri Apr 1 00:01:59 2005

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.01.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - AOL
144.228.241.81 - Sprint
208.51.134.253 - Global X

Query Type: Most Active ASes
Most Active Prefixes
Prefixes Most Announced
Prefixes Most Withdrawn
Prefixes with Most AS Changes

Duration: Last 1 Days
Last 7 Days
Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.01.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - AOL
144.228.241.81 - Sprint
208.51.134.253 - Global X

Query Type: AS
Prefix-Exact
Prefix-More Specific

Query: (ASN or a.b.c.d/men)

Start Date: 2005 Jan 1 00:00
End Date: 2005 Jan 7 00:00

Submit Query

Copyright(c) Merit Network Inc.
Copyright(c) University of Maryland

Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

RouteViews Peer: 66.185.128.1

Prefixes with Most OriginAS Changes, Last 7 Days

Top 20 Prefixes:					
Rank	Prefix	Total	Announce	Withdrawn	Origin AS Changes
1	69.26.163.0/24	738	738	0	514
2	217.52.44.0/24	538	536	2	215
3	133.18.0.0/16	234	219	15	115
4	196.4.55.0/24	113	111	2	60
5	196.201.255.0/24	82	82	0	41
6	217.173.80.0/20	72	72	0	28
7	66.156.0.0/16	34	34	0	27
8	195.155.161.0/24	106	106	0	27
9	84.44.65.0/24	69	68	1	23
10	198.154.8.0/21	63	57	6	23
11	203.20.53.0/24	55	53	2	22
12	65.83.0.0/16	26	26	0	21
13	68.17.0.0/16	26	26	0	21
14	83.210.99.0/24	45	45	0	21
15	192.84.122.0/23	68	57	11	21
16	203.145.145.0/24	25	25	0	21
17	192.222.96.0/22	50	45	5	19
18	204.107.76.0/24	41	40	1	18
19	83.210.34.0/24	39	39	0	16
20	83.210.98.0/24	31	31	0	16

Raw Data Analysis – AS Query

BGP::Inspect - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/

BGP::Inspect

First DB
Last DB

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - ADL, 144.228.241.81 - Sprint, 208.51.134.253 - Global X

Query Type: Most Active ASes, Most Active Prefixes, Prefixes Most Announced, Prefixes Most Withdrawn, Prefixes with Most AS Changes

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - ADL, 144.228.241.81 - Sprint, 208.51.134.253 - Global X

Query Type: AS, Prefix-Exact, Prefix-More Specific

Query: (ASN or a.b.c.d.mn) 3921

Start Date: 2005 Mar 25 00:00

End Date: 2005 Jan 31 00:00

Submit Query

Copyright(c) Merit Network Inc.
Copyright(c) University of Maryland

Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

RouteViews Peer: 12.0.1.63::Autonomous System:03921

GENERA General Electric Company

AS SUMMARY - Peer: 12.0.1.63 - AS03921

Attribute	Value
Query Time Range Start	Fri Mar 25 00:00:00 2005
Query Time Range End	Thu Mar 31 00:00:00 2005
Total Announcements	865959
Unique Prefixes	41
Time to run query	101.700989

Time	Prefix	AS Path	Communitie
Fri Mar 25 00:00:06 2005	165.156.0.0/16	7018 80 3921	7018:2000
	192.104.171.0/24		
	192.131.156.0/24		
	192.131.157.0/24		
	192.131.158.0/24		
	192.131.159.0/24		
	192.131.160.0/24		
	192.131.165.0/24		
	192.131.167.0/24		
	192.131.168.0/24		
	192.131.171.0/24		
	192.131.172.0/24		
	192.131.174.0/24		
	192.131.175.0/24		
	192.131.177.0/24		
	192.131.179.0/24		
192.131.180.0/24			
192.131.182.0/24			
192.131.183.0/24			
192.131.184.0/24			
192.131.185.0/24			
192.131.186.0/24			
192.131.188.0/24			
192.131.189.0/24			
192.131.190.0/24			
192.131.191.0/24			
192.131.192.0/24			
192.131.193.0/24			
192.131.194.0/24			
192.131.196.0/24			
192.131.197.0/24			
192.131.198.0/24			
192.131.199.0/24			
192.131.200.0/24			
192.131.201.0/24			
192.131.203.0/24			
192.131.205.0/24			
192.131.206.0/24			
192.131.208.0/24			
192.131.209.0/24			

Link not found: ""

Raw Data Analysis – Prefix query

BGP::Inspect - Mozilla

http://weasel.merit.edu:8080/

BGP::Inspect First DB Update: Sun Jan 1 00:00:00 2005
Last DB Update: Fri Apr 1 00:01:59 2005

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - AOL, 144.228.241.81 - Sprint, 208.51.134.253 - GlobalX

Query Type: Most Active ASes, Most Active Prefixes, Prefixes Most Announced, Prefixes Most Withdrawn, Prefixes with Most AS Changes

Duration: Last 1 Days, Last 7 Days, Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - AOL, 144.228.241.81 - Sprint, 208.51.134.253 - GlobalX

Query Type: AS, PrefixExact, PrefixMore Specific

Query: (ASN or a.b.c.d/en) 83.210.99.0/24

Start Date: 2005 Mar 25 00:00

End Date: 2005 Mar 31 00:00

Submit Query

Copyright(c) Merit Network Inc.
Copyright(c) University of Maryland

Mozilla

http://weasel.merit.edu:8080/cgi-bin/query.cgi

RouteViews Peer: 144.228.241.81::Prefix:83.210.99.0/24

PREFIX SUMMARY - Peer: 144.228.241.81 - 83.210.99.0/24

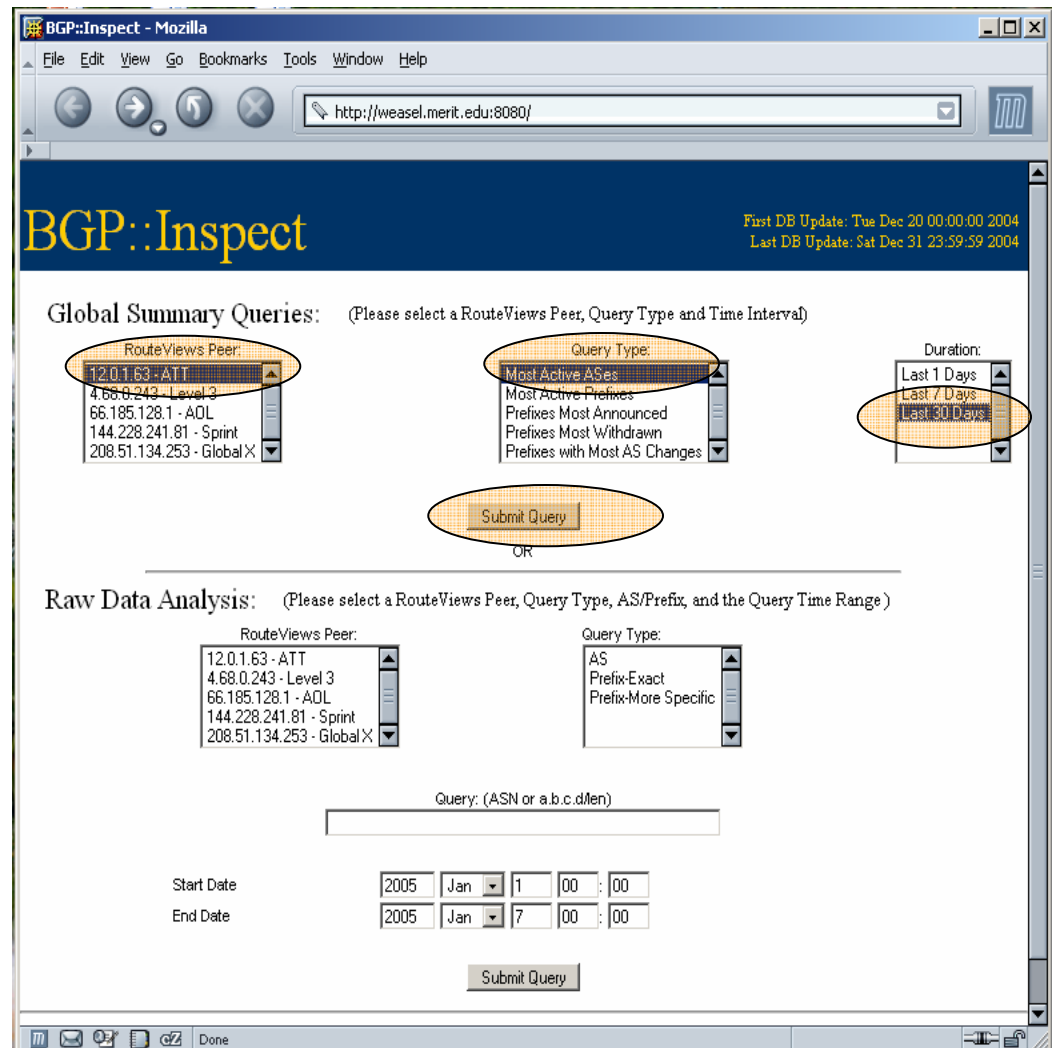
Attribute	Value
Query Time Range Start	Fri Mar 25 00:00:00 2005
Query Time Range End	Thu Mar 31 00:00:00 2005
Total Update Messages	33
Total Announce Messages	33
Total Withdraw Messages	0
Maximum AS Path Length	5
Minimum AS Path Length	2
Average AS Path Length	3.848485
Origin AS Changes	23
Number of Unique ASes	4
Origin ASes List	23918 31050 29257 30593
Time to run query	0.704946

Prefix Announcements:

Time	Type	AS Path	Communities
Fri Mar 25 03:57:31 2005	a	1239 2914 17675 23918	1239:321 1239:1000 1239:1006
Fri Mar 25 03:57:58 2005	a	1239 3356 4716 23918	1239:321 1239:1000 1239:1011
Fri Mar 25 03:58:24 2005	a	1239 2516 17675 17675 23918	1239:123 1239:1000 1239:1011
Fri Mar 25 09:02:33 2005	a	1239 286 286 286 31050	1239:123 1239:5000 1239:5080
Fri Mar 25 16:10:29 2005	a	1239 29257	1239:123 1239:5000 1239:5140
Fri Mar 25 22:01:43 2005	a	1239 1299 31050	1239:321 1239:5000 1239:5070
Fri Mar 25 22:02:12 2005	a	1239 286 286 286 31050	1239:123 1239:5000 1239:5080
Sat Mar 26 15:27:57 2005	a	1239 29257	1239:123 1239:5000 1239:5140
Sun Mar 27 02:09:52 2005	a	1239 2914 17675 23918	1239:321 1239:1000 1239:1011
Sun Mar 27 02:10:20 2005	a	1239 2516 17675 17675 23918	1239:123 1239:1000 1239:1011
Sun Mar 27 23:34:39 2005	a	1239 29257	1239:123 1239:5000 1239:5140
Mon Mar 28 01:25:45 2005	a	1239 286 286 286 31050	1239:123 1239:5000 1239:5080
Mon Mar 28 04:03:32 2005	a	1239 29257	1239:123 1239:5000 1239:5140
Mon Mar 28 13:05:17 2005	a	1239 286 286 286 31050	1239:123 1239:5000 1239:5080
Mon Mar 28 19:29:03 2005	a	1239 2516 17675 17675 23918	1239:123 1239:1000 1239:1011
Tue Mar 29 02:29:48 2005	a	1239 286 286 286 31050	1239:123 1239:5000 1239:5080

Case Study 1 – AS9121 Incident

- At ~09:19 UTC on Dec 24, 2004, AS9121 began re-originating a large number of globally routed prefixes
- Forensics:
 - What happened?
 - Who did it?
 - Could there have been some early detection?
 - How widespread was it?



Step 1: What...

RouteViews Peer: 12.0.1.63
Most Active ASes, Last 30 Days

Rank	AS Number	AS Name	Number of Announcements
1	21617	NARA National Archives and Records Administration	537806
2	23155	HARRIS-61 Harrisonville Telephone Company	265852
3	7018	ATTW AT&T WorldNet Services	89131
4	16581	THETIT-3 The Titan Corporation	64469
5	10968	CARGIL-9 Cargill Incorporated	56425
6	2386	ADCS-1 AT&T Data Communications Services	55540
7	12062	DECISI-34 Decision One	40787
8	5416	BATELCO-BH	30638
9	14689	AES-2 A.G. Edwards & Sons, Inc.	24173
10	721	DNIC DoD Network Information Center	22463
11	9121	TTNET Ttnet Autonomous System	21599
12	16988	INTERN International Paper	17348
13	27455	GBRI Great Barrier Reef, Inc.	16327
14	26170	FRIS Flat Rock Internet Service	16128
15	27343	MONSA Monsanto	16118
16	25780	NFA National Futures Association	16112
17	4134	CHINANET-BACKBONE No.31,Jin-rong Street	14518
18	306	DNIC DoD Network Information Center	14498
19	18566	CVAD Covad Communications	12475
20	702	AS702 MCI EMEA - Commercial IP service provider in Europe	11195

BGP::Inspect

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - ADL
144.228.241.81 - Sprint
208.51.134.253 - GlobalX

Query Type: Most Active ASes
Most Active Prefixes
Prefixes Most Announced
Prefixes Most Withdrawn
Prefixes with Most AS Changes

Duration: Last 1 Days
Last 7 Days
Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

1 RouteViews Peer: 12.0.1.63 - ATT

2 Query Type: AS
Prefix-Exact
Prefix-More Specific

3 Query (ASN or a.b.c.d/m): 9121

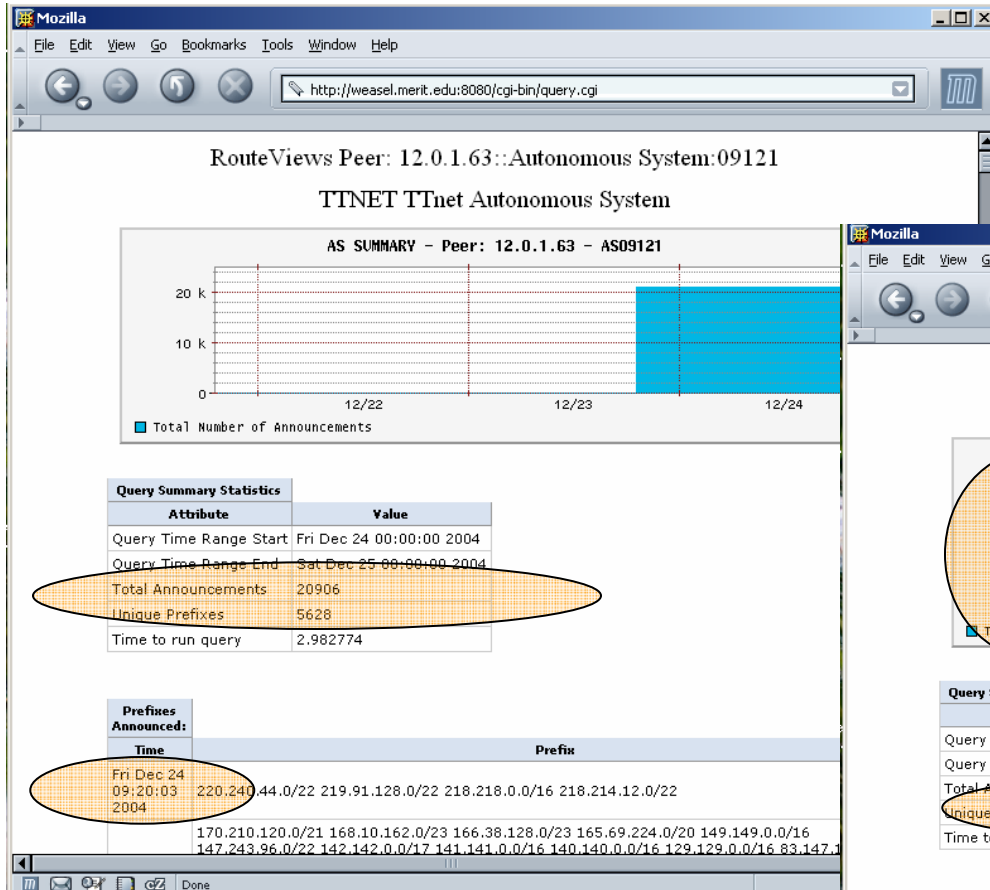
Start Date: 2004 Dec 23 00:00

End Date: 2004 Dec 25 00:00

4

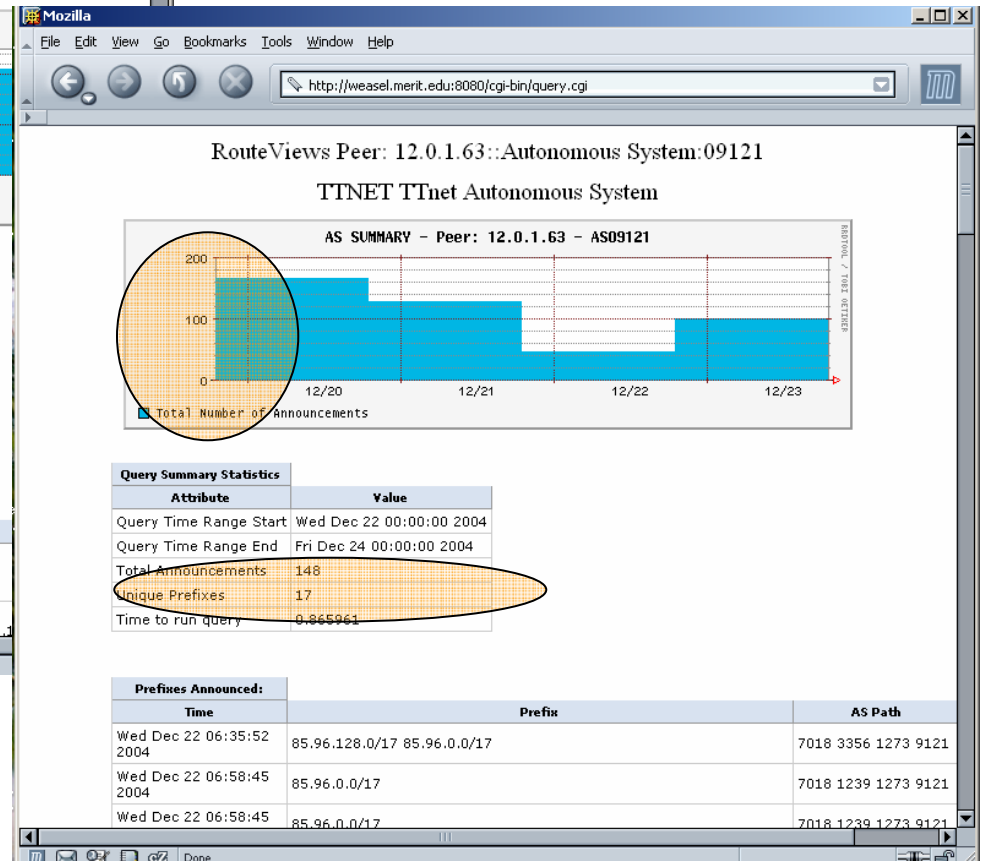
5 Submit Query

Step 1.5: Hmm...interesting...



Dec 24

Dec 22, 23



Step 2: Was I affected?/Should I care?

BGP::Inspect - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/

BGP::Inspect

First DB Update: Tue Dec 20 00:00:00 2004
Last DB Update: Sat Dec 31 23:59:59 2004

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - ADL, 144.228.241.81 - Sprint, 208.51.134.253 - GlobalX

Query Type: Most Active ASes, Most Active Prefixes, Prefixes Most Announced, Prefixes Most Withdrawn, Prefixes with Most AS Changes

Duration: Last 1 Days, Last 7 Days, Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.0.1.63 - ATT, 4.68.0.243 - Level 3, 66.185.128.1 - ADL, 144.228.241.81 - Sprint, 208.51.134.253 - GlobalX

Query Type: AS, Prefix-Exact, Prefix-More Specific

Query: (ASN or a.b.c.d/mn) 35.0.0.0/8

Start Date: 2004 Dec 24 00:00

End Date: 2004 Dec 25 00:00

Submit Query

Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

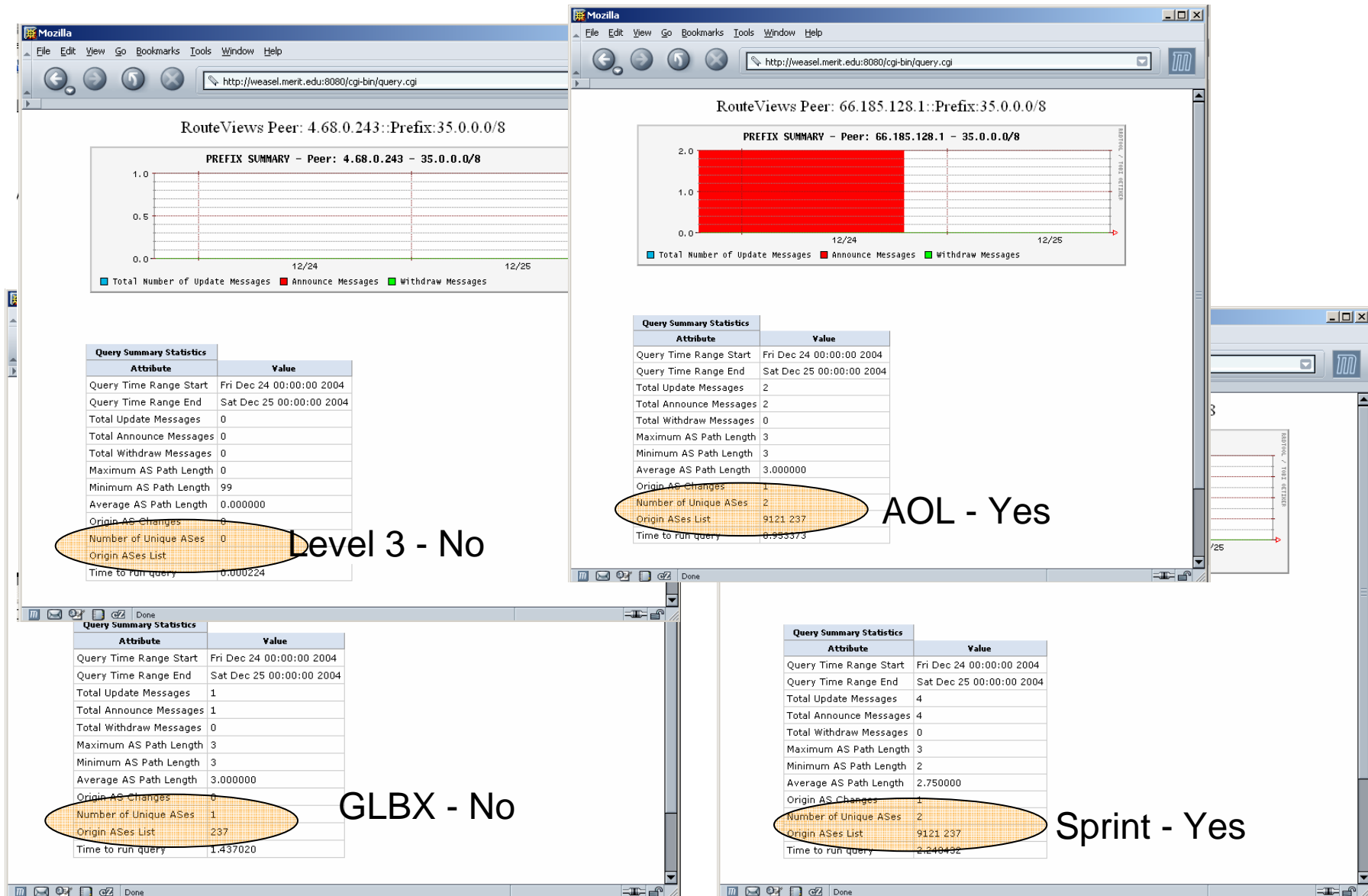
RouteViews Peer: 12.0.1.63::Prefix:35.0.0.0/8

PREFIX SUMMARY - Peer: 12.0.1.63 - 35.0.0.0/8

Total Number of Update Messages, Announce Messages, Withdraw Messages

Query Summary Statistics	
Attribute	Value
Query Time Range Start	Fri Dec 24 00:00:00 2004
Query Time Range End	Sat Dec 25 00:00:00 2004
Total Update Messages	2
Total Announce Messages	2
Total Withdraw Messages	0
Maximum AS Path Length	3
Minimum AS Path Length	3
Average AS Path Length	3.000000
Origin AS Changes	1
Number of Unique ASes	2
Origin ASes List	9121 237
Time to run query	0.011499

Step 3: Where...



Step 4: How widespread...

RouteViews Peer: 4.68.0.243::Autonomous System:09121

TTNET TTnet Autonomous System

AS SUMMARY - Peer: 4.68.0.243 - AS09121

Query Summary Statistics

Attribute	Value
Query Time Range Start	Fri Dec 24 00:00:00 2004
Query Time Range End	Sat Dec 25 00:00:00 2004
Total Announcements	10645
Unique Prefixes	3707
Time to run query	2.644814

Level 3

RouteViews Peer: 66.185.128.1::Autonomous System:09121

TTNET TTnet Autonomous System

AS SUMMARY - Peer: 66.185.128.1 - AS09121

Query Summary Statistics

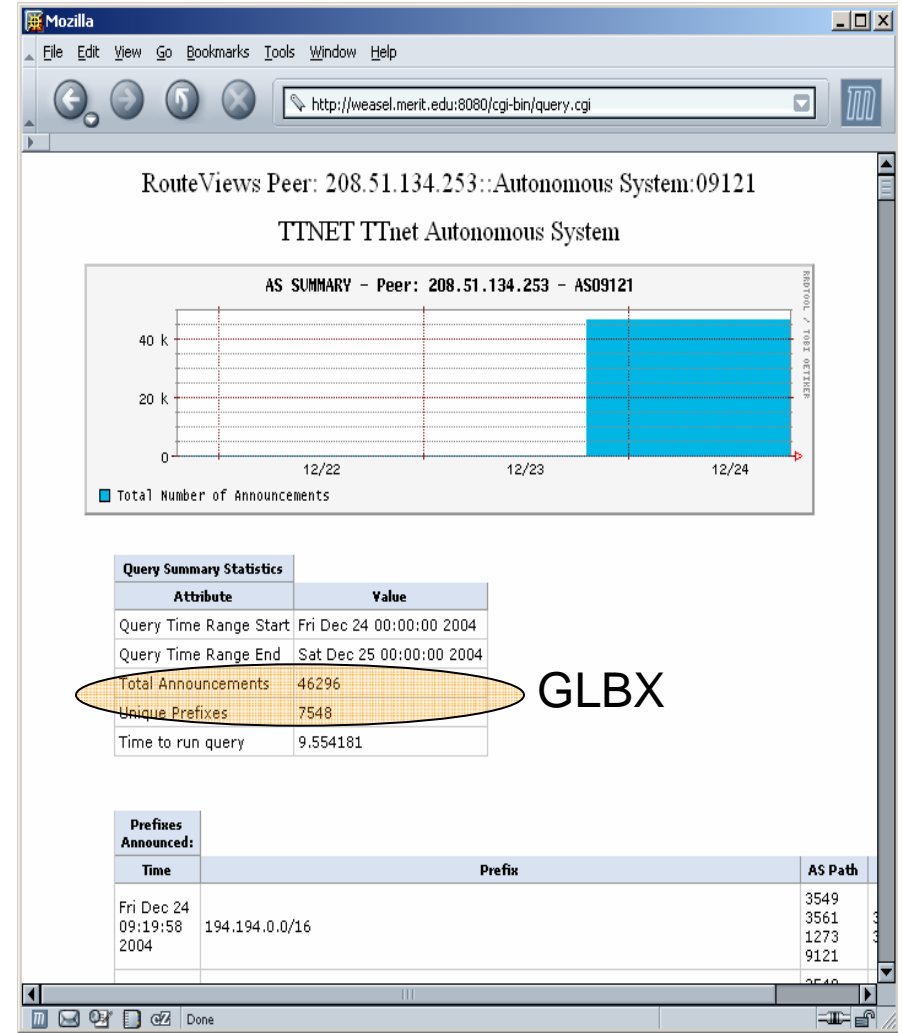
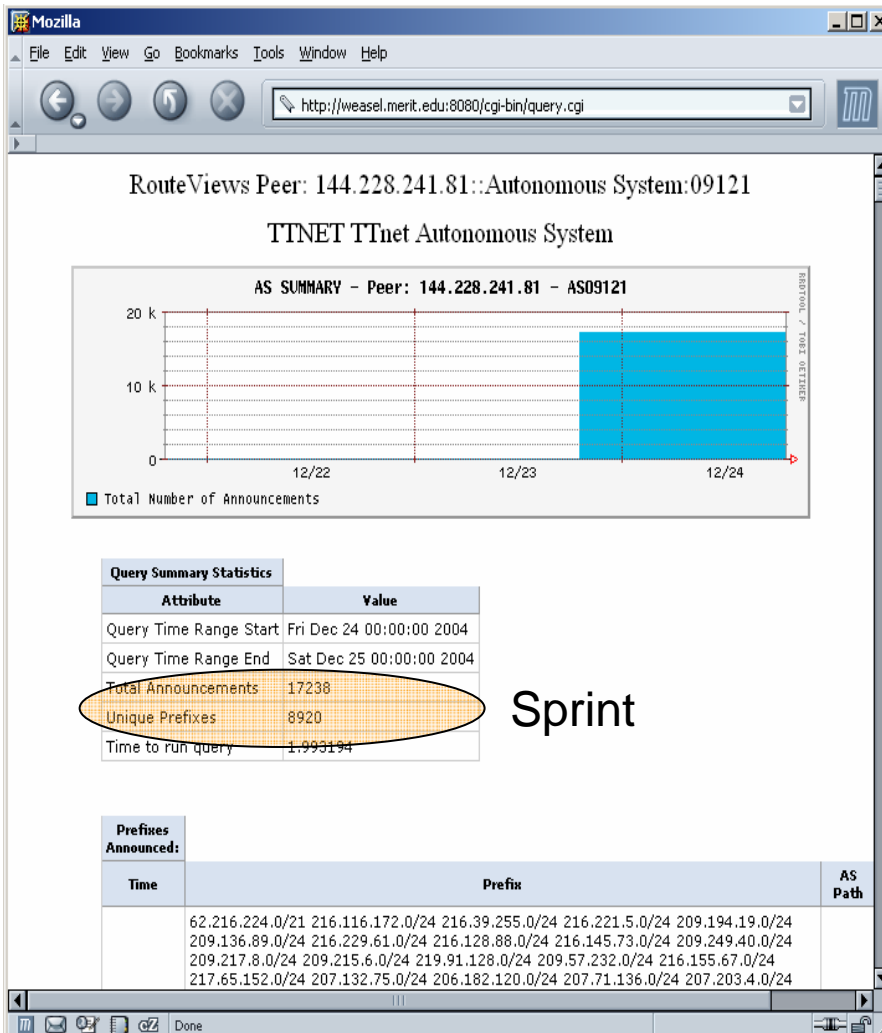
Attribute	Value
Query Time Range Start	Fri Dec 24 00:00:00 2004
Query Time Range End	Sat Dec 25 00:00:00 2004
Total Announcements	28413
Unique Prefixes	12109
Time to run query	3.945105

AOL

Prefixes Announced:

Time	Prefix	AS Path
Fri Dec 24 09:20:03 2004	203.155.80.0/20 203.202.1.0/24 203.203.0.0/16 203.238.37.0/24	1668 1299 9121
	203.254.53.0/24 204.116.184.0/23 204.157.81.0/24 205.109.160.0/19	
	206.78.128.0/19 206.206.0.0/20 207.111.160.0/20 208.14.222.0/23	
	209.177.96.0/23 210.18.192.0/22 210.50.224.0/19 211.19.192.0/20	
	211.27.200.0/21 212.20.192.0/19 212.52.224.0/19 212.68.144.0/20	
	216.150.78.0/24 216.229.61.0/24 216.238.54.0/23 216.239.55.0/24	
	217.65.152.0/24 217.73.144.0/20 217.167.126.0/24 217.201.16.0/20	
	218.159.69.0/24 218.214.12.0/22 218.250.32.0/19 219.90.128.0/17	
	219.91.128.0/24 220.220.0.0/15 220.240.44.0/22	
	222.222.222.0/24 222.222.222.0/24 222.222.222.0/24 222.222.222.0/24	

Step 4: How widespread...



Step 5: How long...

BGP::Inspect First DB Update: Tue Dec 20 00:00:00 2004
Last DB Update: Sat Dec 31 23:59:59 2004

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT
 4.68.0.243 - Level 3
 66.185.128.1 - ADL
 144.228.241.81 - Sprint
 208.51.134.253 - Global X

Query Type: Most Active ASes
 Most Active Prefixes
 Prefixes Most Announced
 Prefixes Most Withdrawn
 Prefixes with Most AS Changes

Duration: Last 1 Days
 Last 7 Days
 Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

RouteViews Peer: 12.0.1.63 - ATT
 4.68.0.243 - Level 3
 66.185.128.1 - ADL
 144.228.241.81 - Sprint
 208.51.134.253 - Global X

Query Type: AS
 Prefix-Exact
 Prefix-More Specific

Query: (ASN or a.b.c.d/men)
 9121

Start Date: 2004 Dec 19 00
 End Date: 2004 Dec 20 00

Submit Query

Time	Unique Prefixes Announced by 9121 as seen by Sprint
07-08	0
08-09	0
09-10	4604
10-11	56
11-12	804
12-13	56
13-14	196
14-15	159
15-16	34
16-17	92
17-18	54
18-19	172
19-20	4496
20-21	229
21-22	15
22-23	0

Primary Event

Secondary Event

Case Study 2 – Prefix Hijack Incident

- Incident: On Feb 10th, AS2586, announces 207.75.135.0/24, which is part of Merit's CIDR block 207.72.0.0/14
- Trouble ticket filed, bogus announcement withdrawn by AS2586 by Feb 10th, 19:22hrs
- How do we find out what happened?
- Could there have been automated detection?
- What was the impact, how widespread was it?

The screenshot shows the BGP::Inspect web application interface in a Mozilla browser window. The browser's address bar shows the URL `http://weasel.merit.edu:8080/`. The application header includes the title "BGP::Inspect" and database update information: "First DB Update: Sun Jan 1 00:00:00 2005" and "Last DB Update: Fri Apr 1 00:01:59 2005".

The main content area is divided into two sections:

- Global Summary Queries:** This section prompts the user to "Please select a RouteViews Peer, Query Type and Time Interval". It features three dropdown menus: "RouteViews Peer" (with options like 12.0.1.63 - ATT, 4.68.0.243 - Level 3, etc.), "Query Type" (with options like Most Active ASes, Most Active Prefixes, etc.), and "Duration" (with options like Last 1 Days, Last 7 Days, Last 30 Days). A "Submit Query" button is located below these menus.
- Raw Data Analysis:** This section prompts the user to "Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range". It includes:
 - A "RouteViews Peer" dropdown menu (annotated with a circled 1) with "12.0.1.63 - ATT" selected.
 - A "Query Type" dropdown menu (annotated with a circled 2) with "Prefix-More Specific" selected.
 - A "Query: (ASN or a.b.c.d/men)" text input field (annotated with a circled 3) containing "207.72.0.0/14".
 - Start and End Date pickers (annotated with a circled 4) showing a range from 2005 Feb 9 00:00 to 2005 Feb 12 00:00.
 - A "Submit Query" button (annotated with a circled 5) at the bottom.

At the bottom of the page, there is copyright information: "Copyright(c) Merit Network Inc." and "Copyright(c) University of Maryland". The browser's status bar at the very bottom shows "Done".

Step 1 – Finding out what happened...

RouteViews Peer: 12.0.1.63::Prefix:207.72.0.0/14

Query Summary Statistics	
Attribute	Value
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	2
More Specific Prefixes	207.72.0.0/14 207.75.135.0/24
Total Update Messages	10
Total Announce Messages	9
Total Withdraw Messages	1
Maximum AS Path Length	6
Minimum AS Path Length	3
Average AS Path Length	4.222223
Number of Unique ASes	2
Origin ASes List	237 2586
Time to run query	165.154068

More Specific Prefix Announcements:				
Time	Prefix	Type	AS Path	Communities
Thu Feb 10 10:54:18 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 10:54:22 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 11:05:50 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:05:58 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:48:12 2005	193.40.48.0/24 193.40.149.0/24 193.229.1.0/24 194.204.2.0/24 194.204.8.0/24 194.204.9.0/24 194.204.12.0/24 194.204.16.0/24 194.204.30.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.52.0/24 194.204.58.0/24 194.204.61.0/24 207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:20 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:38 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:02 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:07 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:14 2005	202.63.102.0/24 202.63.103.0/24 202.63.109.0/24 202.63.110.0/24 202.63.111.0/24 207.75.135.0/24 208.216.139.0/24	w	- - - - -	-

Average AS Path Length	4.222223
Number of Unique ASes	2
Origin ASes List	237 2586
Time to run query	165.154068

More Specific Prefix Announcements:				
Time	Prefix	Type	AS Path	Communities
Thu Feb 10 10:54:18 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 10:54:22 2005	141.213.0.0/16 141.211.0.0/16 198.49.118.0/24 198.49.116.0/23 192.245.254.0/24 192.245.252.0/24 192.153.193.0/24 192.138.137.0/24 192.108.191.0/24 164.76.0.0/16 161.57.0.0/16 148.61.0.0/16 147.124.0.0/16 141.218.0.0/16 141.216.0.0/16 141.215.0.0/16 141.210.0.0/16 207.72.0.0/14 198.108.0.0/14	a	7018 209 237 237 237 237	7018:5000
Thu Feb 10 11:05:50 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:05:58 2005	198.108.0.0/14 204.38.0.0/15 207.72.0.0/14	a	7018 174 237	7018:5000
Thu Feb 10 11:48:12 2005	193.40.48.0/24 193.40.149.0/24 193.229.1.0/24 194.204.2.0/24 194.204.8.0/24 194.204.9.0/24 194.204.12.0/24 194.204.16.0/24 194.204.30.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.52.0/24 194.204.58.0/24 194.204.61.0/24 207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:20 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 11:48:38 2005	194.204.16.0/24 193.40.48.0/24 193.229.1.0/24 194.204.52.0/24 193.40.149.0/24 194.204.30.0/24 194.204.8.0/24 194.204.58.0/24 194.204.61.0/24 194.204.32.0/24 194.204.33.0/24 194.204.34.0/24 194.204.12.0/24 194.204.9.0/24 207.75.135.0/24 194.204.2.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:02 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:07 2005	207.75.135.0/24	a	7018 1239 3336 2586	7018:5000
Thu Feb 10 19:22:14 2005	202.63.102.0/24 202.63.103.0/24 202.63.109.0/24 202.63.110.0/24 202.63.111.0/24 207.75.135.0/24 208.216.139.0/24	w	- - - - -	-

Step 2 – Who, why...

BGP::Inspect - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/

BGP::Inspect

First DB Update: Sun Jan 1 00:00:00 2005
Last DB Update: Fri Apr 1 00:01:59 2005

Global Summary Queries: (Please select a RouteViews Peer, Query Type and Time Interval)

RouteViews Peer: 12.0.1.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - ADL
144.228.241.81 - Sprint
208.51.134.253 - GlobalX

Query Type: Most Active ASes
Most Active Prefixes
Prefixes Most Announced
Prefixes Most Withdrawn
Prefixes with Most AS Changes

Duration: Last 1 Days
Last 7 Days
Last 30 Days

Submit Query

OR

Raw Data Analysis: (Please select a RouteViews Peer, Query Type, AS/Prefix, and the Query Time Range)

1 RouteViews Peer: 12.0.1.63 - ATT
4.68.0.243 - Level 3
66.185.128.1 - ADL
144.228.241.81 - Sprint
208.51.134.253 - GlobalX

2 Query Type: AS
Prefix-Exact
Prefix-More Specific

3 Query: (ASN or a.b.c.d/en) 2586

4 Start Date: 2005 Feb 7 00:00:00
End Date: 2005 Feb 13 00:00:00

5 Submit Query

Copyright(c) Merit Network Inc.
Copyright(c) University of Maryland

Mozilla

File Edit View Go Bookmarks Tools Window Help

http://weasel.merit.edu:8080/cgi-bin/query.cgi

RouteViews Peer: 12.0.1.63::Autonomous System:02586

UNINET-AS AS Uninet

AS SUMMARY - Peer: 12.0.1.63 - AS02586

Total Number of Announcements

Attribute	Value
Query Time Range Start	Mon Feb 7 00:00:00 2005
Query Time Range End	Sun Feb 13 00:00:00 2005
Total Announcements	77
Unique Prefixes	18
Time to run query	0.104736

Time	Prefix	AS Path	Com
Wed Feb 9 01:29:33 2005	194.204.0.0/19	194.204.0.0/18	701
Wed Feb 9 01:29:37 2005	194.204.0.0/19	1273 3336 2586	701
Wed Feb 9 01:30:03 2005	194.204.0.0/19	7018 1239 3336 3336 2586	701
Wed Feb 9 01:33:23	194.204.0.0/19	7018 3356 1273 3336	701

Step 3 – where...

The image displays four screenshots of a Mozilla browser window, each showing a route view query result for a different provider. The browser address bar in all screenshots is `http://weasel.merit.edu:8080/cgi-bin/query.cgi`.

Sprint

RouteViews Peer: 144.228.241.81::Prefix:207.72.0.0/14

Attribute	Value
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	3
More Specific Prefixes	207.75.204.0/23 207.72.0.0/14 207.75.135.0/24
Total Update Messages	6
Total Announce Messages	5
Total Withdraw Messages	1
Maximum AS Path Length	6
Minimum AS Path Length	3
Average AS Path Length	4.200000
Number of Unique ASes	3
Origin ASes List	14716 237 2586
Time to run query	78.842575

Level 3

RouteViews Peer: 4.68.0.243::Prefix:207.72.0.0/14

Attribute	Value
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	2
More Specific Prefixes	207.72.0.0/14 207.75.135.0/24
Total Update Messages	6
Total Announce Messages	5
Total Withdraw Messages	1
Maximum AS Path Length	6
Minimum AS Path Length	3
Average AS Path Length	4.000000
Number of Unique ASes	2
Origin ASes List	237 2586
Time to run query	70.439163

Global X

RouteViews Peer: 208.51.134.253::Prefix:207.72.0.0/14

Attribute	Value
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	3
More Specific Prefixes	207.75.224.0/24 207.72.0.0/14 207.75.135.0/24
Total Update Messages	15
Total Announce Messages	14
Total Withdraw Messages	1
Maximum AS Path Length	6
Minimum AS Path Length	3
Average AS Path Length	4.000000
Number of Unique ASes	3
Origin ASes List	17132 237 2586
Time to run query	88.714783

AOL

RouteViews Peer: 66.185.128.1::Prefix:207.72.0.0/14

Attribute	Value
Query Time Range Start	Wed Feb 9 00:00:00 2005
Query Time Range End	Fri Feb 11 00:00:00 2005
Number of More Specific Prefixes	12
More Specific Prefixes	207.72.0.0/14 207.72.44.0/24 207.72.45.0/24 207.73.116.0/22 207.73.120.0/21 207.74.92.0/24 207.75.44.0/23 207.75.122.0/24 207.75.135.0/24 207.75.204.0/23 207.75.224.0/24
Total Update Messages	58
Total Announce Messages	57
Total Withdraw Messages	1
Maximum AS Path Length	8
Minimum AS Path Length	3
Average AS Path Length	4.421052
Number of Unique ASes	8
Origin ASes List	237 25773 33272 26932 10789 2586 14716 17132
Time to run query	45.647362

Conclusions and Future Work

- There is a need to build efficient tools that help extract useful information from large BGP datasets
- BGP::Inspect is currently available to the network operator and research communities and feedback is appreciated
- Aside from BGP::Inspect we have presented some basic techniques such as chunked-compressed files, B+ Tree indexing, data redundancy elimination, and caching that can be applied by other data mining tools to help analyze other large datasets as well.
- The goal is not just to provide access to the data, but to try to provide useful data summaries as well, that can help researchers and network operators quickly identify potentially “interesting” events. Top20 lists are a good way to bring potentially interesting things to the attention of people.
- Tools need to be useful before they can be used, and in order to be useful, feedback from potential users is critical.
- BGP data analysis need not be hard/painful/tedious, that’s what tools are for!
- Where do we go from here, so we have basic capabilities what about:
 - Automated anomaly detection, notification, same tool?, different tool?
 - More scalability,? What are the limits?
 - What are more useful queries? What book-keeping do we need to track those?