

# The BGP-Inspect Project

Manish Karir, Jon Oberheide (Merit)  
Dionysus Blazakis, John Baras (UMd)

# 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
  - Goal is to attempt to make it easier to use raw data from archives such as Route Views, by pre-processing, reformatting and indexing the data

# Outline

- BGP-Inspect and BGPdb
  - Overview and new features
- BGP-Inspect in Action!
  - Case studies
- Conclusions, Future Work and Discussion

# 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

- 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

# BGP-Inspect: Current State

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

Dataset: August 1 - Present  
Current BGPdb size: 102GB  
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-Inspect - bgpinspect.merit.edu - Mozilla  
http://bgpinspect.merit.edu  
First DB Update: Mon Aug 01 00:00:00 2005  
Last DB Update: Today 00:00:01 2005

Home Reports Documentation FAQ About

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

RouteViews Peer: 12.0.1.63-ATT, 4.68.0.243-Level 3, 66.185.123.1-AOL, 144.228.241.81-Sprint, 208.51.134.253-GlobalX

Query Type: AS, Prefix Exact, Prefix More Specific

Durations: Last 1 Days, Last 2 Days, Last 3 Days, Last 7 Days, Last 10 Days

Submit Query

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

RouteViews Peer: 12.0.1.63-ATT, 4.68.0.243-Level 3, 66.185.123.1-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/nn)

Start Date: 2005 Oct 13 00:00  
End Date: 2005 Oct 20 00:00

Submit Query

Copyright © Merit Network, Inc.  
Copyright © University of Maryland

BGP-Inspect - bgpinspect.merit.edu - Mozilla  
http://bgpinspect.merit.edu/query.php

Home Reports Documentation FAQ About

Aggregate 12.0.1.63 4.68.0.243 66.185.123.1 144.228.241.81 208.51.134.253

RouteViews Peer: 12.0.1.63  
AS: 721 (DNIC DoD Network Information Center)

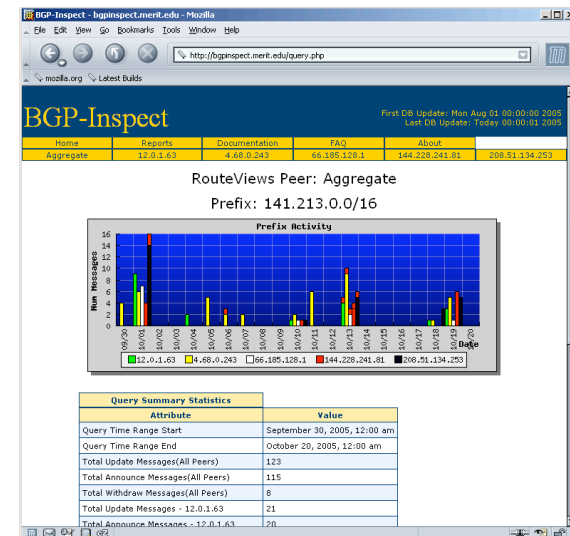
Total Number of prefix announcements

Query Summary Statistics

Attribute	Value
Query Time Range Start	September 21, 2005, 12:00 am
Query Time Range End	October 20, 2005, 12:00 am
Total Update Messages	37574
Unique Prefixes	1109
Time to run query	22.831 seconds

# 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



RouteViews Peer: 12.0.1.63  
Overall Most Active Prefixes, Last 7 Days

Rank	Prefix	Total	Announce	Withdrawn	Origin AS Changes
1	81.213.47.0/24	10685	6202	4483	0
2	199.191.128.0/22	10316	10316	0	0
3	199.191.160.0/24	10316	10316	0	0
4	199.191.192.0/24	10316	10316	0	0
5	199.191.200.0/24	10316	10316	0	0
6	199.191.208.0/24	10316	10316	0	0
7	192.35.39.0/24	9463	8967	496	4022
8	81.212.149.0/24	4444	3373	1073	0
9	69.26.199.0/24	4103	3107	996	0
10	209.140.24.0/24	3811	3312	499	0
11	81.212.197.0/24	3779	2800	979	0
12	213.184.73.0/24	3553	1792	1761	0
13	209.144.205.0/24	2910	1455	1455	0
14	207.168.184.0/24	2725	2235	490	0
15	66.150.140.0/23	2446	2389	57	0
16	216.85.83.0/24	2135	2076	59	0
17	63.144.114.0/24	1865	1795	70	0
18	203.135.6.0/24	1815	1735	80	0



# Newly Added Features

- Daily auto-load script
  - Cron job
  - Fetch the previous days Route Views data from the public server
  - Insert everything into BGPdb
    - Both for raw queries...
    - ...and for the summary statistics.
  - “Productionized” - everything hardened for public use

# Newly Added Features (2)

- Multi-peer queries
  - As requested from last session, a response from multiple peers can be requested from a single query.
  - Tabbed Interface
    - One aggregated tab giving summary info and a multi-bar graph...
    - ...and a tab with detailed results for each peer.

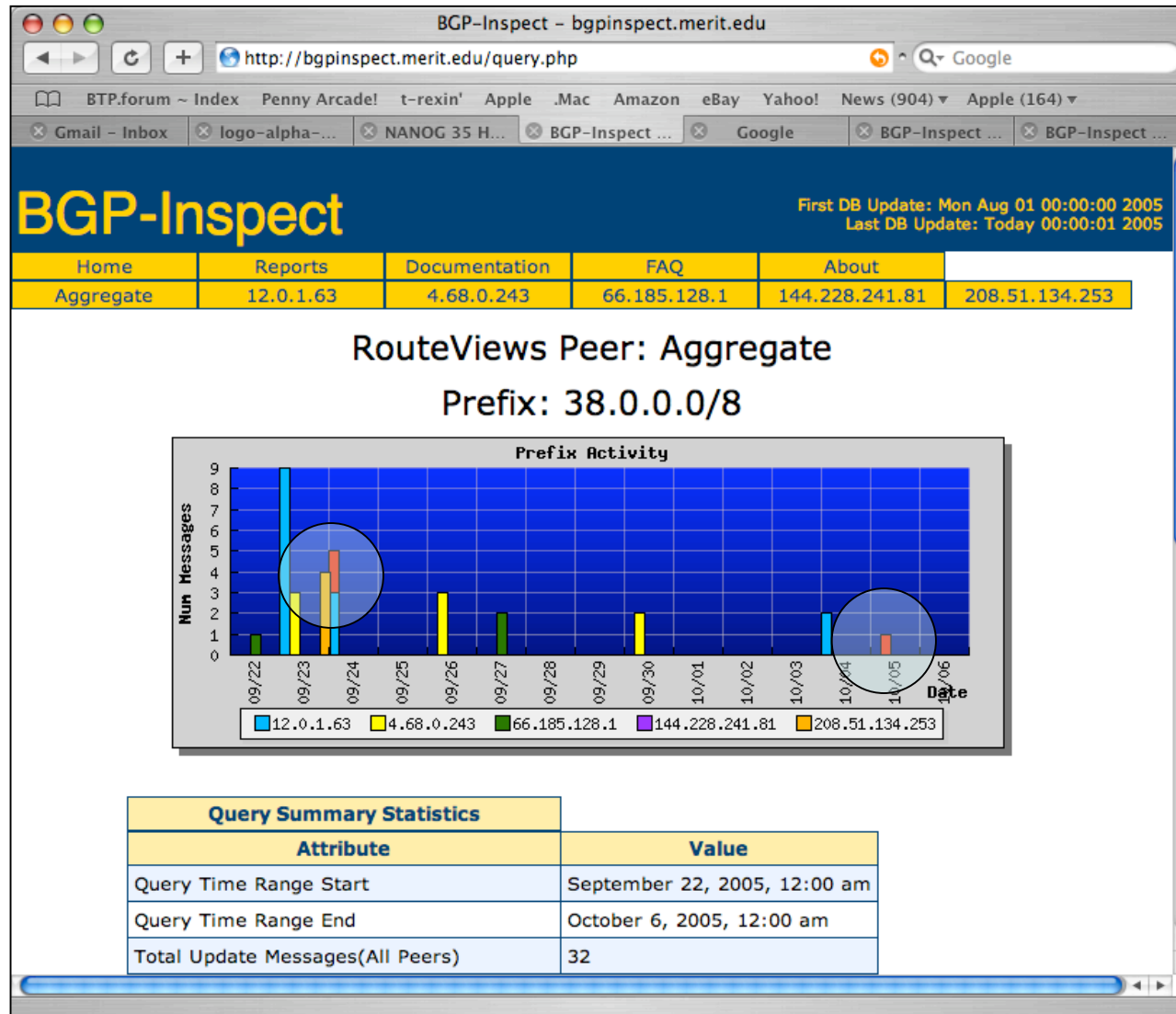
# Newly Added Features (3)

- Internal fixes and clean-ups
  - Redesigned web infrastructure
    - Cleaner, more structured PHP as opposed to a C CGI implementation
    - UI enhancements (more to come?)
  - New build system to facilitate a source release in the future

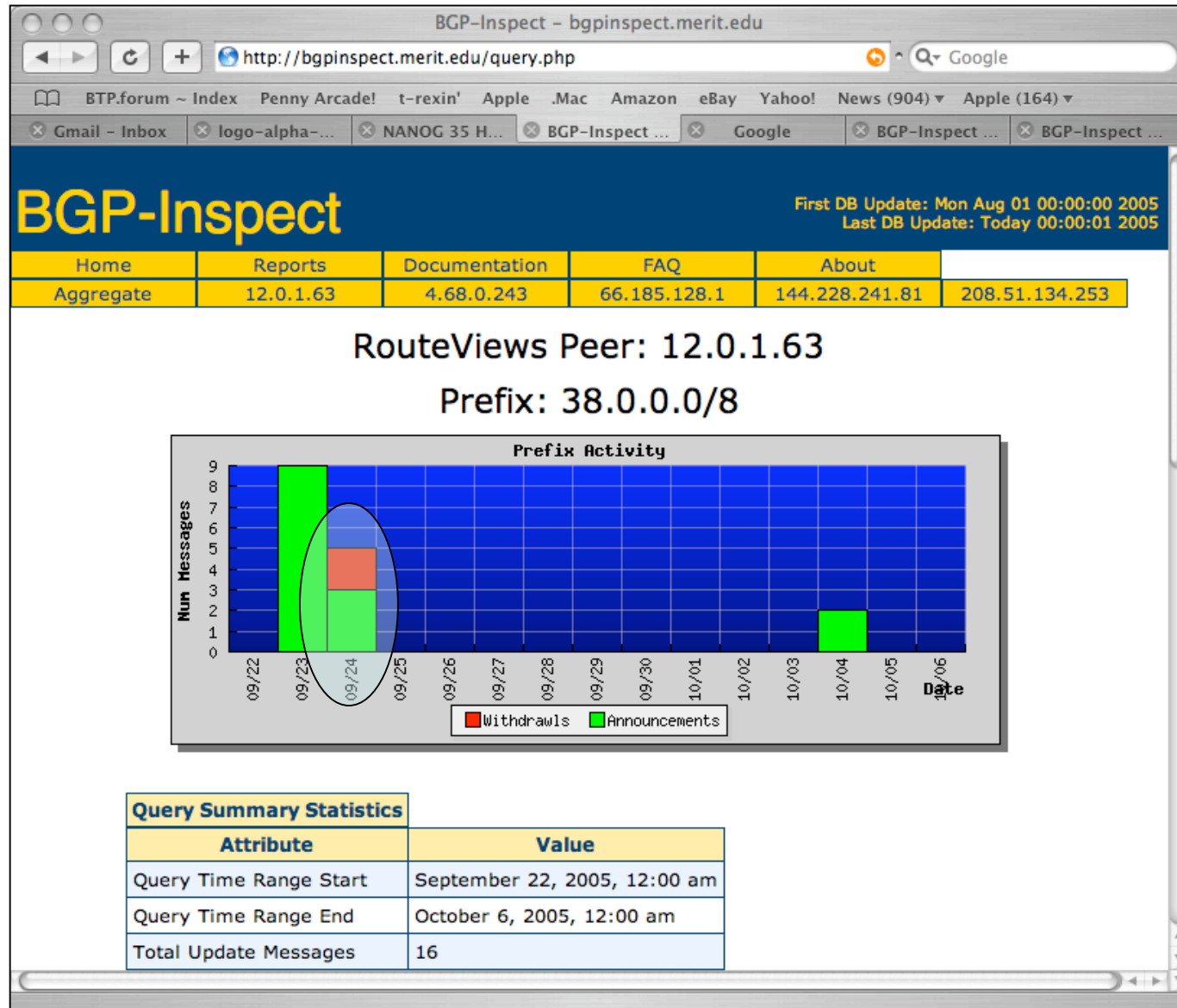
# Case Study: Cogent de-peering

- **On Oct 5th 2005, Level 3 and Cogent stopped peering directly with each other.** In order to examine the impact of this event we ran a raw data analysis query for 38.0.0.0/8 (Cogent) for the various Route View peers (that we currently index). This determines the reach-ability impact of this event on 38/8 from the 5 peers in our data. Our initial analysis ranges from September 22nd through October 6th.

# Case Study (cont.) - Aggregate



# Case Study (cont.) - AT&T



# Case Study (cont.) - AT&T

BGP-Inspect - bgpinspect.merit.edu

http://bgpinspect.merit.edu/query.php

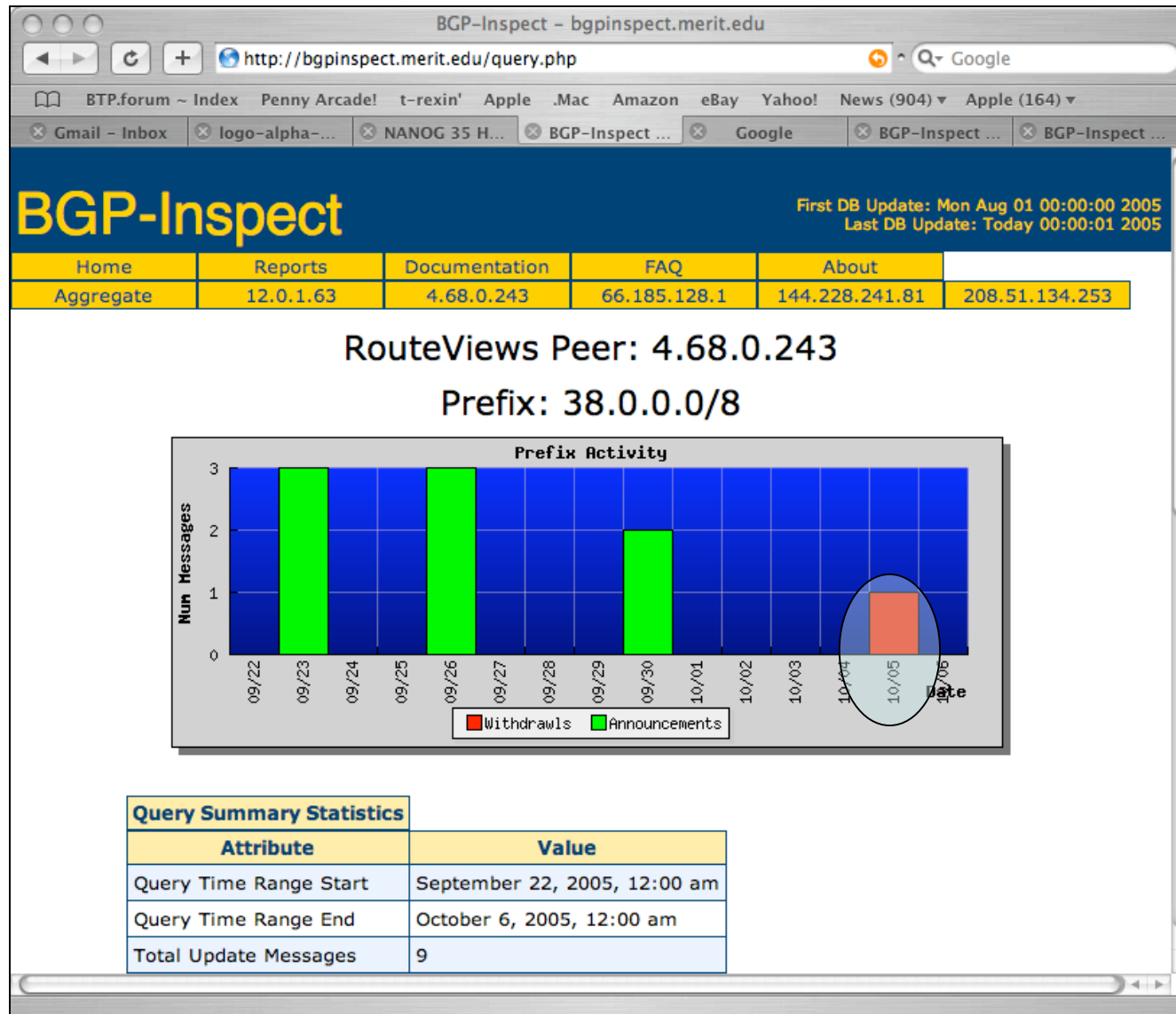
BTP.forum ~ Index Penny Arcade! t-rexin' Apple .Mac Amazon eBay Yahoo! News (904) Apple (164)

Gmail - Inbox logo-alpha-... NANOG 35 H... BGP-Inspect ... Google BGP-Inspect ... BGP-Inspect ...

Prefix Announcements:			
Time	Type	AS Path	Communities
September 23, 2005, 4:12 am	a	7018 174	7018:5000
September 23, 2005, 4:12 am	a	7018 174	7018:5000
September 23, 2005, 4:18 am	a	7018 174	7018:5000
September 23, 2005, 4:44 am	a	7018 174	7018:5000
September 23, 2005, 4:45 am	a	7018 174	7018:5000
September 23, 2005, 4:46 am	a	7018 174	7018:5000
September 23, 2005, 4:47 am	a	7018 174	7018:5000
September 23, 2005, 4:50 am	a	7018 174	7018:5000
September 23, 2005, 4:50 am	a	7018 174	7018:5000
September 24, 2005, 11:56 am	w	-	-
September 24, 2005, 11:56 am	a	7018 174	7018:5000
September 24, 2005, 11:59 am	w	-	-
September 24, 2005, 12:00 pm	a	7018 65000 65001 7018 174	7018:5000
September 24, 2005, 12:00 pm	a	7018 174	7018:5000
October 4, 2005, 12:01 am	a	7018 65000 65001 7018 174	7018:5000
October 4, 2005, 12:12 am	a	7018 174	7018:5000

Copyright © Merit Network Inc.  
Copyright © University of Maryland

# Case Study (cont.) - Level 3





# Case Study (cont.) - Level 3

BGP-Inspect - bgpinspect.merit.edu

http://bgpinspect.merit.edu/query.php

BTP.forum ~ Index Penny Arcade! t-rexin' Apple .Mac Amazon eBay Yahoo! News (904) Apple (164)

Gmail - Inbox logo-alpha-... NANOG 35 H... BGP-Inspect ... Google BGP-Inspect ... BGP-Inspect ...

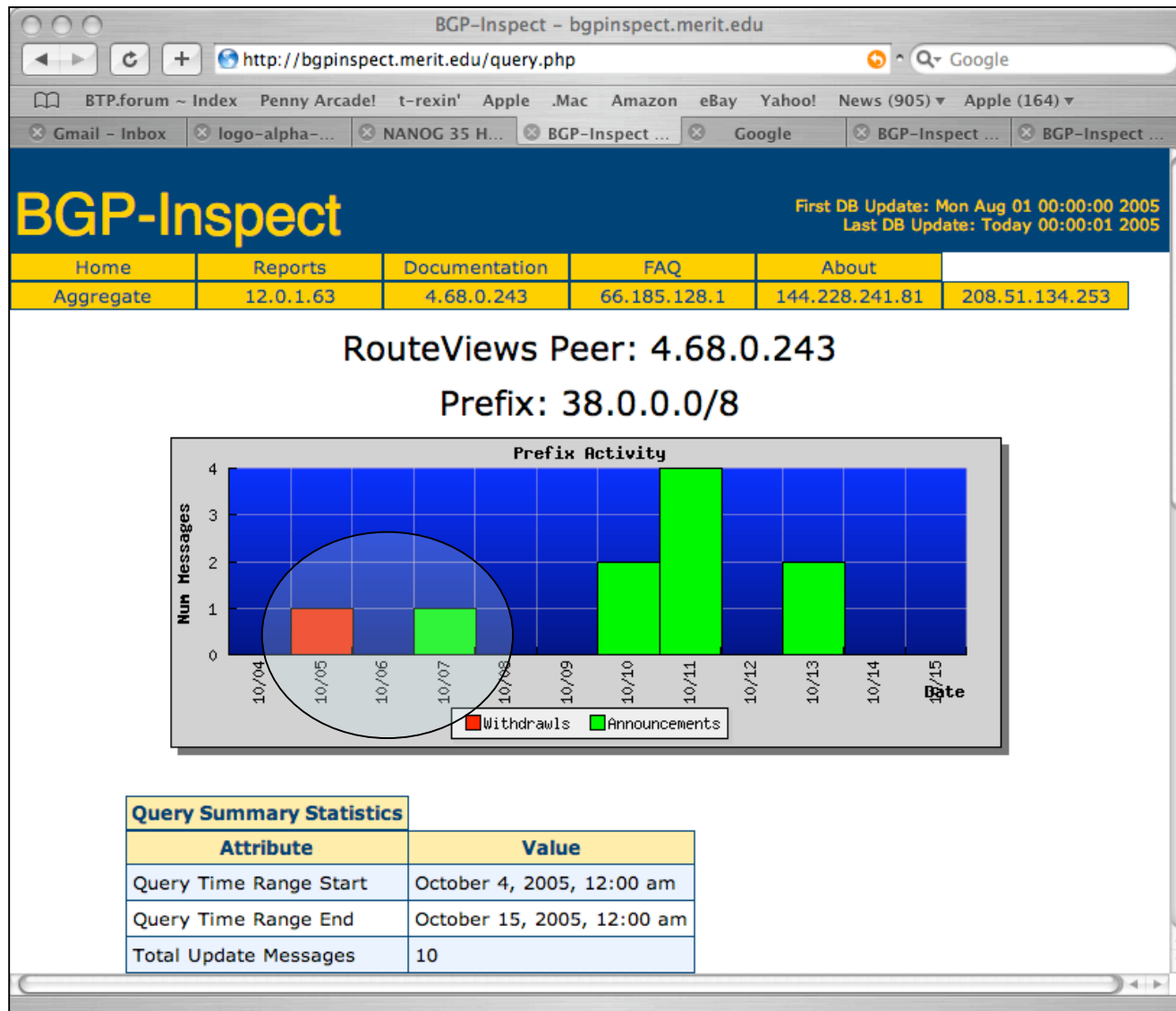
Maximum AS Path Length	2
Minimum AS Path Length	2
Average AS Path Length	2.000000
Origin AS Changes	0
Number of Unique ASes	1
Origin ASes List	174
Time to run query	3.226 seconds

**Prefix Announcements:**

Time	Type	AS Path	Communities
September 23, 2005, 4:15 am	a	3356 174	-
September 23, 2005, 4:15 am	a	3356 174	-
September 23, 2005, 4:22 am	a	3356 174	-
September 26, 2005, 2:38 pm	a	3356 174	-
September 26, 2005, 2:38 pm	a	3356 174	-
September 26, 2005, 3:37 pm	a	3356 174	-
September 30, 2005, 1:00 am	a	3356 174	-
September 30, 2005, 1:23 am	a	3356 174	-
October 5, 2005, 4:49 am	w	-	-

Copyright © Merit Network Inc.

# Case Study (cont.) - Level 3



# Conclusions and Future Work

- Efficient tools for BGP analysis are needed and we've created some.
- 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
  - Automated anomaly detection using these tools