#### 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

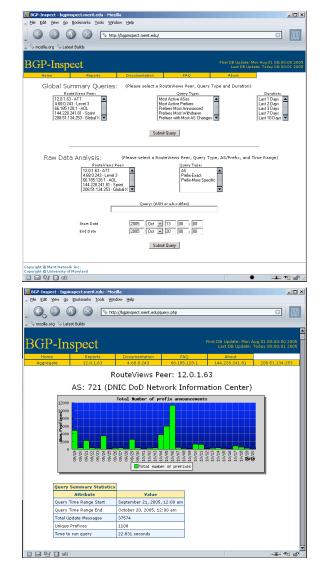
- Removing redundancy from BGP datasets
  - ASPATH, COMMUNITY, UPDATE Msgs are repeated over and over, only time changes
- Compressed-Chunked Files
  - Compromise between size and usability
- B+ Tree indices
  - Indexing based on time, this enables fast time-range queries
- Caching while processing input 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-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

	erit.edu - Mozilla							
Ele Edit Yew Go Bookmark		elp						
6.66	http://bgpi	spect.m	erit.edu/quer	/.php				m
♀ mozilla.org ♀ Latest Builds								
<b>3GP-Inspe</b>	ct					DB Update: Mo	in Aug 01 00:00 te: Today 00:00	00 2005
JOI -mspc						Last DB Updat	te: Today 00:00	:01 2005
Aggregate R	eports Do .0.1.63 4	.68.0.2	ation 43	FAQ 66.185.128.1	. 1	About 44.228.241.81	208.51.10	34.253
	Route	م <i>ا</i> /ام	NC PAA	r: Aggre	aste			
	Pre			13.0.0/1	16			
16 14		P	refix Act	ivity				
Mun Messages 0.1 h 0.3 1 1 0.70	0.1.63 □4.68.0.2	43 06	8/01 6.185.128.1		95/05 95/05 41.81	41/01 208.51.134.253	w/w	
Query St	ummary Statistics		1					
	Attribute			Value				
Query Time Ran				r 30, 2005, 12				
Query Time Ran	ge End ssages(All Peers)		October 2 123	0, 2005, 12:00	lam			
	Messages(All Peers)	1	115					
Total Withdraw M	1essages(All Peers)		8					
	ssages - 12.0.1.63		21					
Total Announce I	Messages - 12.0.1.6	3	20				-10-	- 1
$\Theta, \Theta, \Theta, \Theta$	Shttp://bgpins	pect.mer	it.edu/query	php				M
mozila.org 🛇 Latest Builds		-	-		-			F
mozila.org ∿Latest Builds GP-Inspec	t				First C	)B Update: Mo Last DB Updat	n Aug 01.00:00: e: Today 00:00:	00 2005 01 2005
		umenta	tion	FAQ	First C	DB Update: Mo Last DB Updat About	n Aug 01 00:00; e: Today 00:00;	00 2005 01 2005
	oorts Doo			FAQ 12.0.1			n Aug 01 00:00; e: Today 00:00;	00 2005 01 2005
GP-Inspec	Route	View	/s Peei		1.63	About	n Aug 01 00:00 e: Today 00:00:	00 2005 01 2005
GP-Inspec	oorts Doo	View	/s Peei		1.63	About	n Aug 01.00:00 e: Today 00:00:	00 2005 01 2005
GP-Inspec Home Ref Construction Top 20 Prefixes	Route Route	View : Act	ive Pre	efixes, L	1.63 ast 7	About Days	n Aug 01 00:00; e: Today 00:00;	00 2005 01 2005
GP-Inspec	Route	View	/s Peei	efixes, L	1.63 ast 7	About	n Aug 01 00:00: e: Today 00:00:	00 2005 01 2005
GP-Inspector Home Rep O Top 20 Prefixes Rank 1 2	Doc           Route           verall Most           Prefix           81.213.47.0/24           199.191.128.0/22	View Act 10685 10316	Announc 6202 10316	efixes, L Withdrawn 4483	L.63 ast 7 0	About Days	n Aug 01.00:00; e: Today 00:00;	00 2005 01 2005
GP-Inspector tone Rep O Top 20 Prefixes Rank 1 2 3	Prefix           81.213.47.0/24           199.191.160.0/24	View Act 10685 10316	x Peer ive Pre 6202 10316 10316	efixes, Lo Withdrawn 4483 0 0	L.63 ast 7 0rigin 0 0	About Days	n Aug 01 00:00; e: Today 00:00;	00 2005 01 2005
GP-Inspec Norre Reg C Top 20 Prefixes Rank 2 3 3 4	Prefix           81.213.47.0/24           199.191.128.0/22           199.191.192.0/24	View Act 10685 10316 10316	Announc 6202 10316 10316 10316	efixes, L withdrawn 4483 0 0 0 0	0 <b>Origin</b> 0 <b>Origin</b> 0 0 0 0	About Days	n Aug 01 00:00 e: Today 00:00	00 2005 01 2005
GP-Inspector Home Reg CONT Top 20 Prefixes Rank 1 2 3 4 4 5	Deed           Route           verall Most           Prefix           81.213.47.0/24           199.191.128.0/24           199.191.20.0/24           199.191.20.0/24	View Act 10685 10316 10316 10316	Announc 6202 10316 10316 10316 10316	efixes, L Withdrawn 4483 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	About Days	n Aug (1. 00-06) e: Today (0:00)	00 2005 01 2005
GP-Inspec Norre Reg C Top 20 Prefixes Rank 2 3 3 4	Prefix           81.213.47.0/24           199.191.128.0/22           199.191.192.0/24	View Act 10685 10316 10316	Announc 6202 10316 10316 10316	efixes, L withdrawn 4483 0 0 0 0	0 <b>Origin</b> 0 <b>Origin</b> 0 0 0 0	About Days	n Aug 01 00:00 e: Today 00:00	00 2005 01 2005
GP-Inspector None Real Contemportant Top 20 Prefixer Rank 1 2 3 4 5 5 6 7 7 8	Prefix         Dec           Prefix         81.213.47.0/24           199.191.126.0/24         199.191.126.0/24           199.191.126.0/24         199.191.126.0/24           199.191.126.0/24         199.191.200.0/24           199.191.208.0/24         192.35.39.0/24           81.212.149.0/24         81.212.149.0/24	View Act 10685 10316 10316 10316 10316 10316 9463 4446	/s Peer ive Pre 6202 10316 10316 10316 10316 10316 10316 8967 3373	Withdrawn           4483           0 <t< td=""><td>Crigin 0 0 0 0 0 0 0 0 0 0 0 0 0</td><td>About Days</td><td>n Aug 01 00:00</td><td>00 2005 01 2005</td></t<>	Crigin 0 0 0 0 0 0 0 0 0 0 0 0 0	About Days	n Aug 01 00:00	00 2005 01 2005
GP-Inspec torre Rep CO Top 20 Prefixes Rank 1 2 3 4 5 5 6 7 8 8 9	Perfix         Date           Prefix         121.47.0/24           199.191.126.0/22         199.191.126.0/24           199.191.126.0/24         199.191.20.0/24           199.191.20.0/24         199.191.20.0/24           199.191.20.0/24         199.191.20.0/24           193.191.20.0/24         199.191.20.0/24           193.192.0/24         193.192.0/24	View Act 10685 10316 10316 10316 10316 10316 4446 4103	/s Peer ive Pre 6202 10316 10316 10316 10316 10316 3967 3373 3107	efixes, L 4483 0 4483 0 0 0 0 0 0 0 496 1073 996	L.63 ast 7 0 0 0 0 0 0 0 0 0 0 4022 0 0	About Days	n Aug 01 00:00 e. Today 00:00	.00 2005 01 2005
GP-Inspector Hores Reg C Top 20 Prefixes Rank 1 2 3 4 5 6 7 7 9 9 10	Prefix Prefix 81.213.47.0/24 199.191.128.0/24 199.191.108.0/24 199.191.208.0/24 199.192.108.0/24 199.25.39.0/24 81.212.149.0/24 69.26.199.0/24	View Act 10685 10316	/s Peer ive Pre 6202 10316 10316 10316 10316 10316 8967 3373 3107 3312	<ul> <li>Withdrawn</li> <li>4483</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>1073</li> <li>996</li> <li>499</li> </ul>	L.63 ast 7 0 0 0 0 0 0 0 0 0 4022 0 0 0 0 0 0 0 0	About Days	n Aug (1. 20:00 e : Taday Go (00.	00 2005 01 2005
GP-Inspec torre rep C Top 20 Prefixes Rank 2 3 4 5 5 6 7 7 6 9 9 10 11	Prefix         Date           Prefix         81/213-47.0/24           19/191.128.0/22         199.191.100.0/24           199.191.100.0/24         199.191.200.0/24           199.191.208.0/24         199.191.208.0/24           199.191.208.0/24         199.191.208.0/24           199.191.208.0/24         199.191.208.0/24           199.191.208.0/24         199.191.208.0/24           199.191.208.0/24         199.191.208.0/24           192.353.9.0/24         209.140.24.0/24           209.140.24.0/24         209.140.74.70/24	View Act 10685 10316 10316 10316 10316 10316 4446 4103	/s Peer ive Pre 6202 10316 10316 10316 10316 10316 3967 3373 3107 3312 2800	efixes, L Withdrawn 4483 0 0 0 0 0 496 499 996 499 979	0 Crigin 0 Crigin 0 0 0 0 0 0 0 0 0 0 0 0 0	About Days	n Aug (H. Golder et Todsy Golder	00 2005 01 2005
GP-Inspector Hores Reg C Top 20 Prefixes Rank 1 2 3 4 5 6 7 7 9 9 10	Prefix Prefix 81.213.47.0/24 199.191.128.0/24 199.191.108.0/24 199.191.208.0/24 199.192.108.0/24 199.25.39.0/24 81.212.149.0/24 69.26.199.0/24	View Act 10685 10316 10316 10316 10316 9463 4446 4103 3811 3779	/s Peer ive Pre 6202 10316 10316 10316 10316 10316 8967 3373 3107 3312	<ul> <li>Withdrawn</li> <li>4483</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>0</li> <li>1073</li> <li>996</li> <li>499</li> </ul>	L.63 ast 7 0 0 0 0 0 0 0 0 0 4022 0 0 0 0 0 0 0 0	About Days	n Aug (1. 00/06) e: Today 00/00	00 2005
GP-Inspect torrs rep CO Top 20 Prefuess Rank 1 2 3 4 5 6 6 7 7 8 9 9 10 11 12 13 14	Prefix Prefix 81.213.47.0/24 1991.91.128.0/22 1991.91.128.0/22 1991.91.128.0/24 1991.91.128.0/24 1991.91.128.0/24 1991.91.128.0/24 1991.91.128.0/24 1991.91.128.0/24 191.91.91.08.0/24 2091.04.20.76 21.21.347.0/24 21.31.347.30/24 21.31.347.30/24	View : Act 10685 10316 10316 10316 9463 4446 4103 3811 3779 3553	Announc 6202 10316 10316 10316 10316 10316 10316 3373 3317 2800 1792 1455 2235	Withdrawn           4483           0           1761           1455           490	Content of the second s	About Days	n Aug 01 00:00 e: Today 00:00	00 2005
GP-Inspector Top 20 Prefixed Rank 1 2 3 4 5 6 7 7 6 9 10 11 12 13 14 15	Image         Descure           Route         verall Most           uerall Most         1919.128.0/21           1919.128.0/21         1919.128.0/21           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.139.0/24         1919.148.0/24           1919.144.025.0/24         1919.148.0/24           1919.144.0/24         1919.148.0/24	View - Act Total 10685 10316 10327 10377 10377 10377 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 10377777 10377777 103777777777777777777777777777777777777	Announc 6202 10316 10316 10316 10316 10316 10316 10317 3373 3107 3312 2800 1792 1455 2235 2389	Withdrawn           4483           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           1073           996           499           979           1761           1455           490           \$7	L.63     ast 7     vrigin     0	About Days	n Aug 01 00:00 e: Today 00:00	00 2005 01 2005
GP-Inspec torre term C C C C C C C C C C C C C C C C C C C	Prefix Prefix 01.213.47.0/24 199.19.128.0/22 199.19.12.00.0/24 199.19.12.00.0/24 199.19.12.00.0/24 199.19.12.00.0/24 192.23.97.0/24 027.168.184.0/24 027.168.184.0/24 025.045.85.80.0/24	View - Act Total 10855 10316 10317 10352 10372 10375 103	Announc 6202 10316 10316 10316 10316 10316 10316 3967 3373 3107 3312 2800 1792 1455 2235 2235 22389 2076	Withdrawn           4483           4483           0           1073           996           499           979           1761           1455           490           57           59	L.63 ast 7 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	About Days	n Aug 01 (0:00 e: Today (0:00	00 2005
GP-Inspector Top 20 Prefixed Rank 1 2 3 4 5 6 7 7 6 9 10 11 12 13 14 15	Image         Desc           Route         Verall Most           uerall Most         1919.128.0/21           1919.128.0/21         1919.128.0/21           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.128.0/24         1919.128.0/24           1919.144.205.0/24         1919.148.0/24           1919.144.0/24         1919.148.0/24	View - Act Total 10685 10316 10327 10377 10377 10377 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 103777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 1037777 10377777 10377777 103777777777777777777777777777777777777	Announc 6202 10316 10316 10316 10316 10316 10316 10317 3373 3107 3312 2800 1792 1455 2235 2389	Withdrawn           4483           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0           1073           996           499           979           1761           1455           490           \$7	L.63     ast 7     vrigin     0	About Days	n Aug 01 00:00	00 2005

### 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.

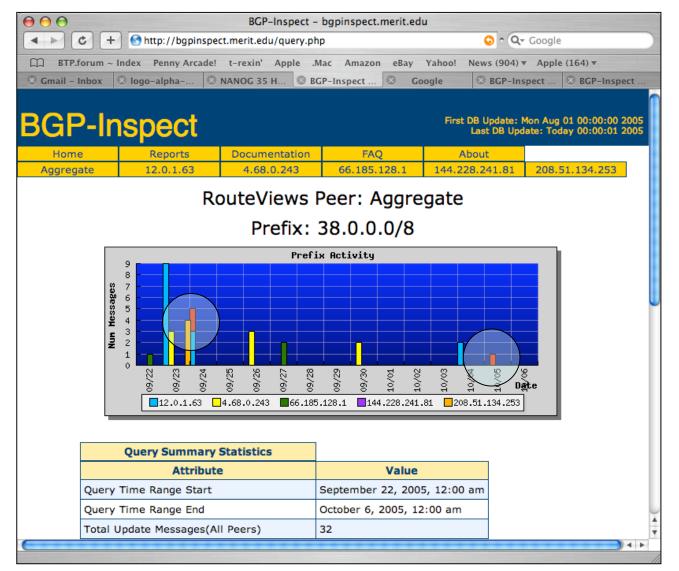
## Newly Added Features (3)

- 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

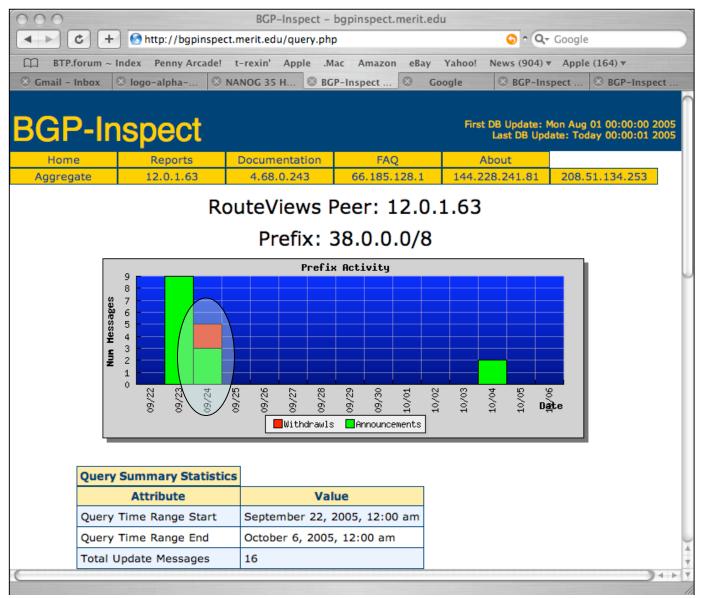
#### Case Study: Cogent de-peering

 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 38.0.0/8 (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



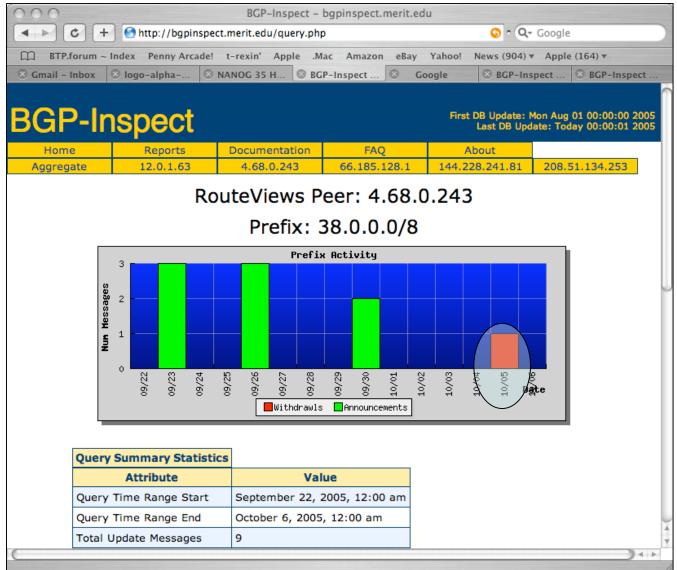
# Case Study (cont.) - AT&T



# Case Study (cont.) - AT&T

	E + Shttp://bgpinspect.merit		spect – bgpinspect.merit.edu	<b>0</b> • 0	- Google	
	orum ~ Index Penny Arcade! t-rex					
S Gmail - I			BGP-Inspect S Google		▼ Apple (164) ▼ spect SBGP-Inspect	ct
© Ginan - n		33 n	w bur-inspect w doogn	© Bur-III	spect   @ bur-inspec	P
[	Prefix Announcements:					- 1
	Time		AS Path	Communities		- 1
	September 23, 2005, 4:12 am	а	7018 174	7018:5000		
	September 23, 2005, 4:12 am	а	7018 174	7018:5000		
	September 23, 2005, 4:18 am	а	7018 174	7018:5000		
	September 23, 2005, 4:44 am	a	7018 174	7018:5000		
	September 23, 2005, 4:45 am	а	7018 174	7018:5000		
	September 23, 2005, 4:46 am		7018 174	7018:5000		
	September 23, 2005, 4:47 am	а	7018 174	7018:5000		
	September 23, 2005, 4:50 am	a	7018 174	7018:5000		
	September 23, 2005, 4:50 am	а	7018 174	7018:5000		
5	September 24, 2005, 11:56 am	w	-	-		
	September 24, 2005, 11:56 am	а	7018 174	7018:5000		
	September 24, 2005, 11:59 am	w	-	-		
	September 24, 2005, 12:00 pm	а	7018 65000 65001 7018 174	7018:5000		
	September 24, 2005, 12:00 pm	а	7018 174	7018:5000		
	October 4, 2005, 12:01 am	а	7018 65000 65001 7018 174	7018:5000		
	October 4, 2005, 12:12 am	a	7018 174	7018:5000		
	ferit Network Inc. Iniversity of Maryland					_
spyright © 0	any croicy of Platyland					4 1

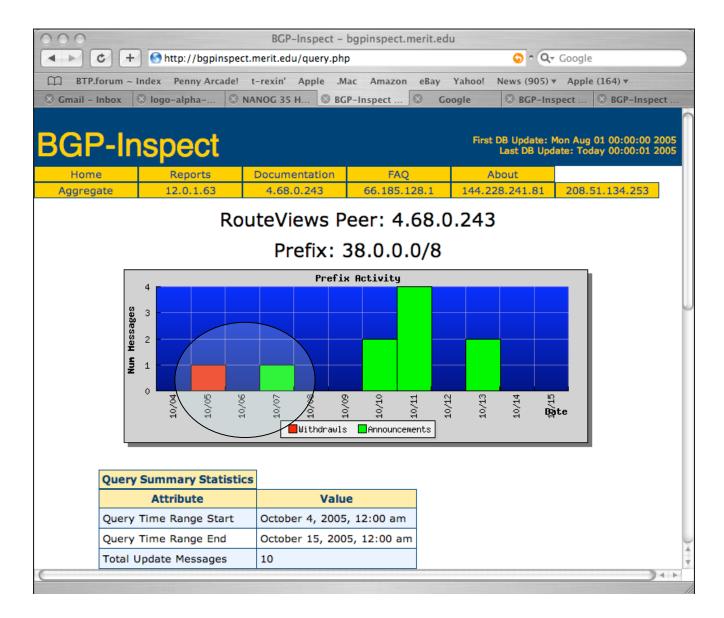
### Case Study (cont.) - Level 3



## Case Study (cont.) - Level 3

000	BGP-I	Inspect – bg	pinspect.merit.	edu		
A P C + Shttp://bgpinspect.r	merit.edu,	/query.php			😋 ^ 🔍 Google	e )
BTP.forum ~ Index Penny Arcade! t	-rexin'	Apple .Mac	Amazon eBa	y Yahoo!	News (904)  Appl	e (164) 🔻
🛇 Gmail - Inbox 🛛 logo-alpha 🛇 NA	NOG 35 H	I 🛞 BGP-	Inspect 🛞	Google	BGP-Inspect	⊗ BGP-Inspect
Maximum AS Path Length	2					0
Minimum AS Path Length	2					
Average AS Path Length	2.00000	00				
Origin AS Changes	0					
Number of Unique ASes	1					
Origin ASes List	174					
Time to run query	3.226 s	econds				
Prefix Announcements:				_		
Time			Communities	5		
September 23, 2005, 4:15 a		3356 174		_		-
September 23, 2005, 4:15 a	m a	3356 174	-	_		
September 23, 2005, 4:22 a	m a	3356 174	-	_		
September 26, 2005, 2:38 p		3356 174	-	_		
September 26, 2005, 2:38 p	m a	3356 174	-			
September 26, 2005, 3:37 p	m a	3356 174	-	_		
September 30, 2005, 1:00 a	m a	3356 174				
September 30, 2005, 1:23 a	m 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 <u>http://bgpinspect.merit.edu</u> 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