Cyclops: The AS-level Connectivity Observatory

Ricardo Oliveira,Ying-Ju Chi,Mohit Lad, Lixia Zhang

University of California, Los Angeles

Speaker: Ricardo Oliveira
rveloso@cs.ucla.edu

“Did AS9318 leak routes from Yahoo?”
@Nanog mailing list, July 8th 2007

“Did Cogent depeer Limelight, WV Fiber and nLayer?”
@Nanog mailing list, Sept 28th 2007

“Can anyone confirm a partition between Telia 1299 and Cogent 174?”
@Nanog mailing list, March 14th 2008

Need #1: AS connectivity

- Even though AS connectivity can be inferred from BGP updates collected from hundreds of vantage points - the **public view (PV) …**

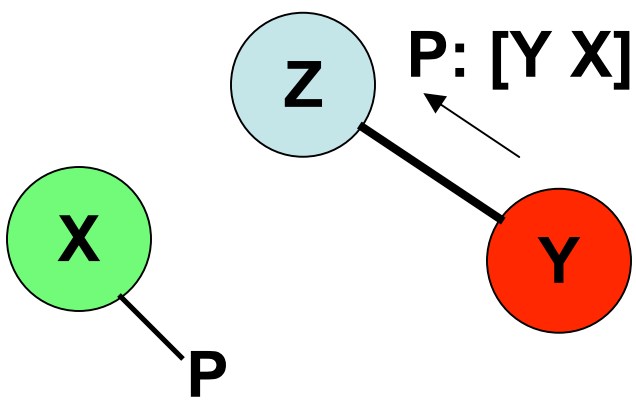
- … there's no tool to gather this info to infer **the AS connectivity and changes**

Need #2: fault detection

- Each ISP knows who its neighbors are: **the ground truth**

- Public view captures part of the ground truth and **more**…

- **False link prefix hijack and misconfigurations**

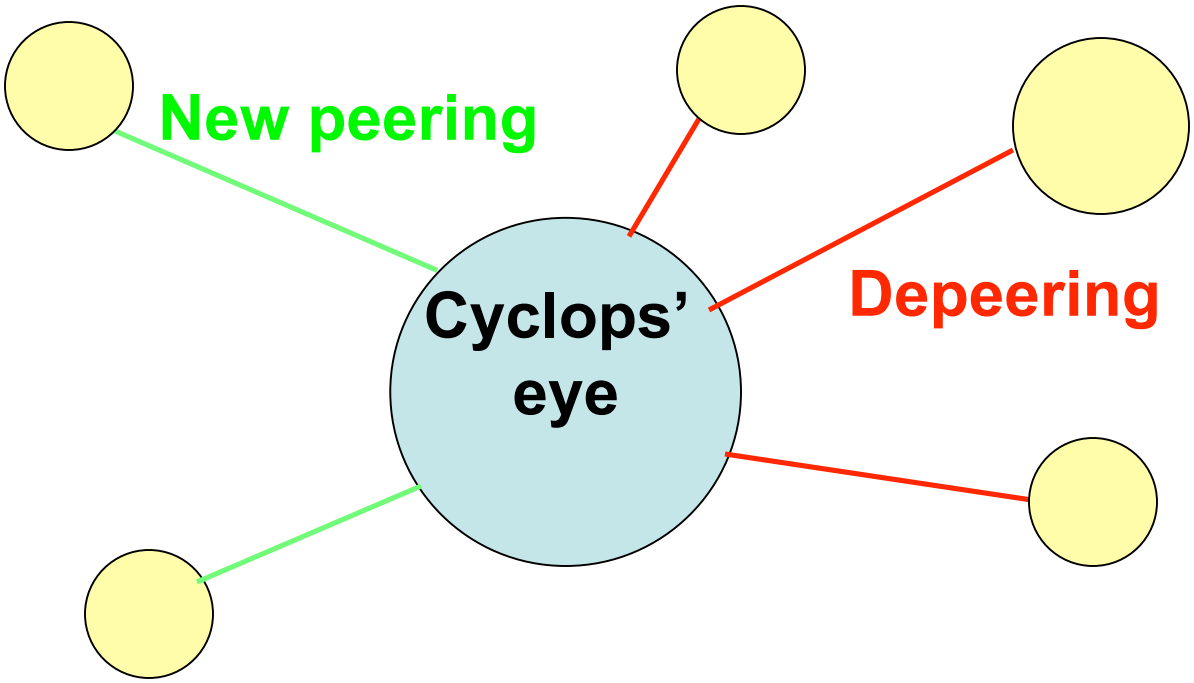


- Y starts announcing a false link to Z w/ X's prefix P

- In this case the link X-Y will appear in the PV

Cyclops concept

- Show 1-hop connectivity of specific AS at a time: **eye of the cyclops**



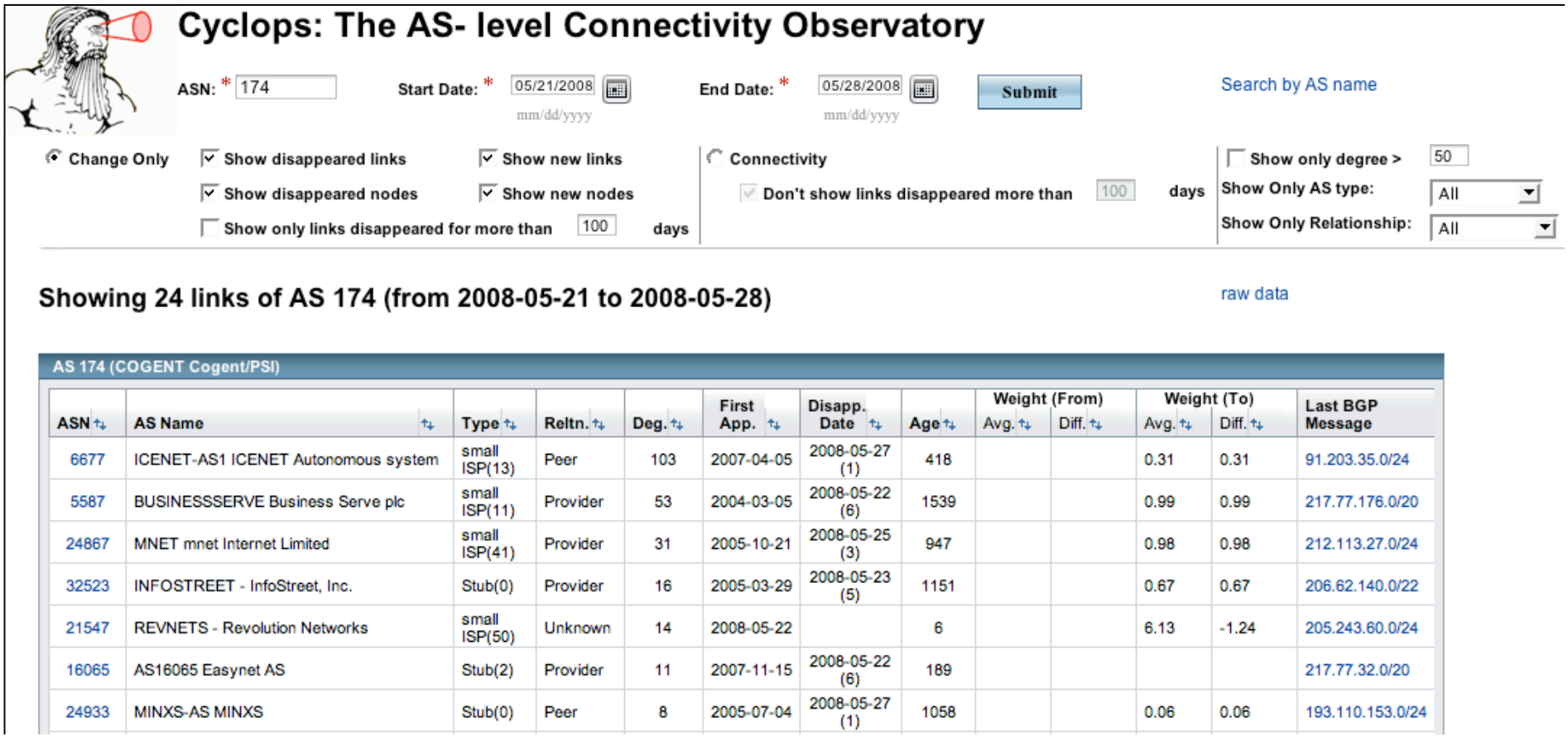
The 3 flavors of Cyclops

Raw data: raw connectivity data to be processed at ISP side

- 2153@CSUNET-NE - California State University Network@Transit-Unknow@Provider@42@2003-12-31@2008-03-13@1532@TABLE_DUMP|1205284560|B|134.55.200.1|293|128.97.0.0/16|293 2153 52|IGP|||||||

The 3 flavors of Cyclops

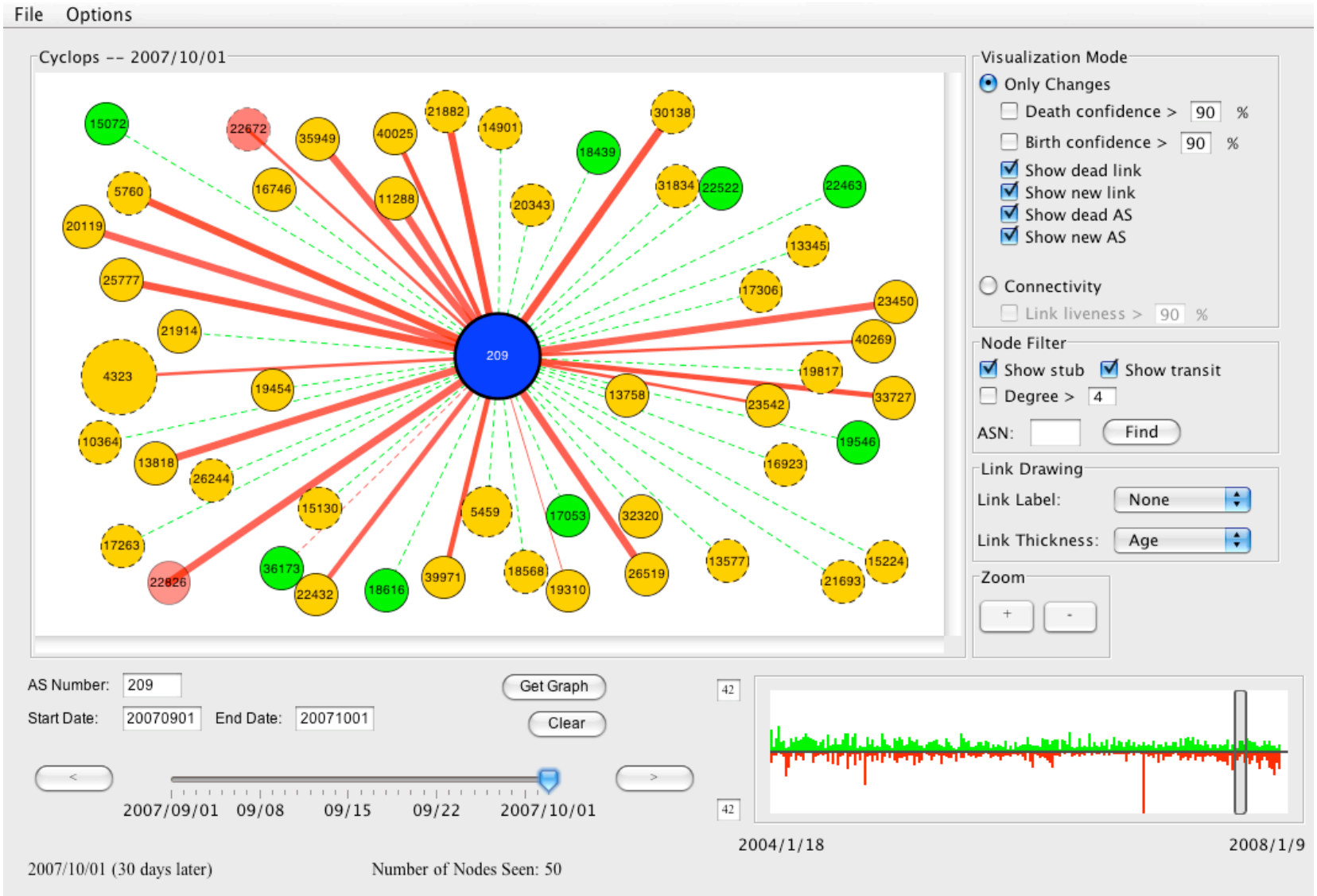
Web interface: quick way of getting list of neighbors and changes for a specific network



ASN	AS Name	Type	Reltn.	Deg.	First App.	Disapp. Date	Age	Weight (From) Avg.	Weight (From) Diff.	Weight (To) Avg.	Weight (To) Diff.	Last BGP Message
6677	ICENET-AS1 ICENET Autonomous system	small ISP(13)	Peer	103	2007-04-05	2008-05-27 (1)	418			0.31	0.31	91.203.35.0/24
5587	BUSINESSSERVE Business Serve plc	small ISP(11)	Provider	53	2004-03-05	2008-05-22 (6)	1539			0.99	0.99	217.77.176.0/20
24867	MNET mnet Internet Limited	small ISP(41)	Provider	31	2005-10-21	2008-05-25 (3)	947			0.98	0.98	212.113.27.0/24
32523	INFOSTREET - InfoStreet, Inc.	Stub(0)	Provider	16	2005-03-29	2008-05-23 (5)	1151			0.67	0.67	206.62.140.0/22
21547	REVNETS - Revolution Networks	small ISP(50)	Unknown	14	2008-05-22		6			6.13	-1.24	205.243.60.0/24
16065	AS16065 Easynet AS	Stub(2)	Provider	11	2007-11-15	2008-05-22 (6)	189					217.77.32.0/20
24933	MINXS-AS MINXS	Stub(0)	Peer	8	2005-07-04	2008-05-27 (1)	1058			0.06	0.06	193.110.153.0/24

The 3 flavors of Cyclops

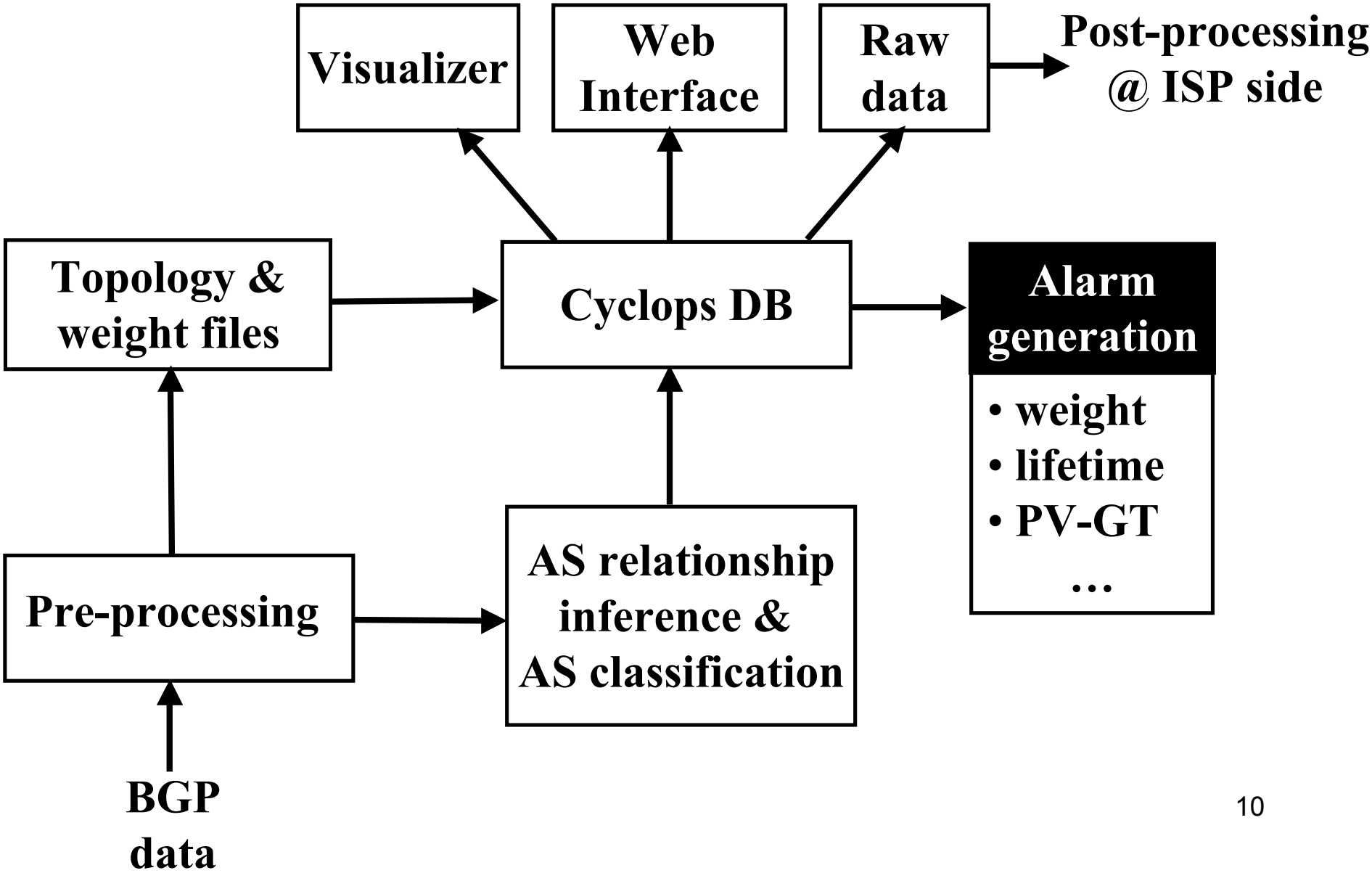
Visualizer: enables visual correlation of changes



Cyclops in a nutshell

- **Fault detection**: BGP misconfigurations, false link attacks, route leakages
- Provide AS **topology snapshot** and changes-only view
- Detection of **anomalous** (de)peering events
- **Event correlation** and root-cause inference

Cyclops architecture



Updating Cyclops DB

- Currently done in a **daily basis**; creates some delay in detection and reaction time

-Plan to move it to **real time** using BGPmon tool from CSU:
http://bgpmon.netsec.colostate.edu/

Cyclops raw data

- Available at **http://cyclops.cs.ucla.edu/rawdata**

- Last digit of ASN is the directory to look at, e.g. UCLA AS-52 is at **http://cyclops.cs.ucla.edu/rawdata/2/52**

- `2153@CSUNET-NE - California State University Network@Large ISP@Provider@42@2003-12-31@2008-03-13@1532@TABLE_DUMP|1205284560|B|134.55.200.1|293|128.97.0.0/16|293 2153 52|IGP|||||||`

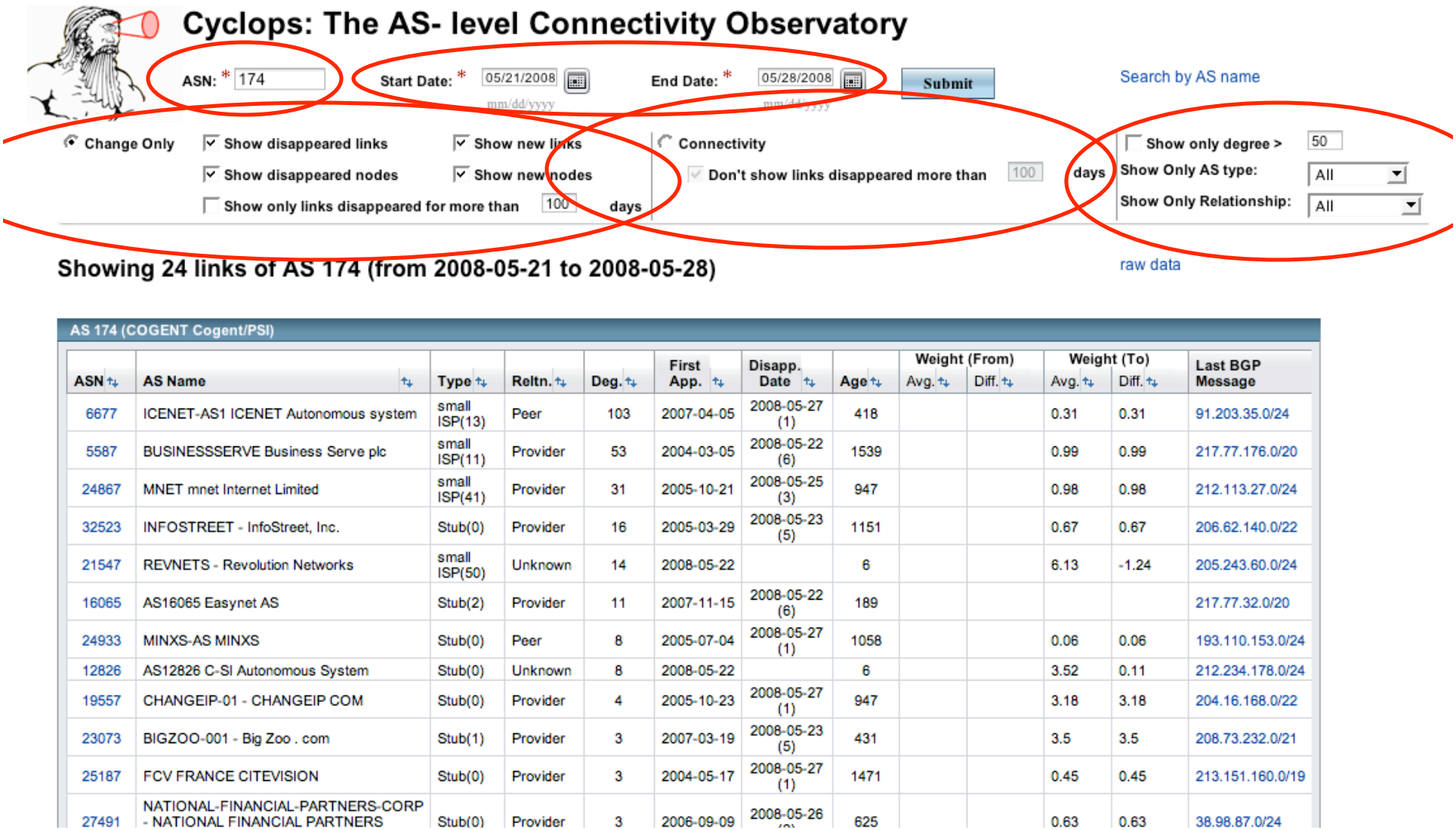
- Known valid UCLA neighbors: AS2153 an AS2152
  - Everything else that appears connected to UCLA should trigger an alarm

- Easy to setup a script to periodically download these files and process them using filters to produce **an alarm list**

Web interface

- Allow users to have a quick view of the snapshot+connectivity
- Two modes:
  - **“Change only”**
  - **“Connectivity”**
- Allow filtering and sorting by relevant parameters

Web Interface



ASN	AS Name	Type	Reltn.	Deg.	First App.	Disapp. Date	Age	Weight (From) Avg.	Weight (From) Diff.	Weight (To) Avg.	Weight (To) Diff.	Last BGP Message
6677	ICENET-AS1 ICENET Autonomous system	small ISP(13)	Peer	103	2007-04-05	2008-05-27 (1)	418			0.31	0.31	91.203.35.0/24
5587	BUSINESSSERVE Business Serve plc	small ISP(11)	Provider	53	2004-03-05	2008-05-22 (6)	1539			0.99	0.99	217.77.176.0/20
24867	MNET mnet Internet Limited	small ISP(41)	Provider	31	2005-10-21	2008-05-25 (3)	947			0.98	0.98	212.113.27.0/24
32523	INFOSTREET - InfoStreet, Inc.	Stub(0)	Provider	16	2005-03-29	2008-05-23 (5)	1151			0.67	0.67	206.62.140.0/22
21547	REVNETS - Revolution Networks	small ISP(50)	Unknown	14	2008-05-22		6			6.13	-1.24	205.243.60.0/24
16065	AS16065 Easynet AS	Stub(2)	Provider	11	2007-11-15	2008-05-22 (6)	189					217.77.32.0/20
24933	MINXS-AS MINXS	Stub(0)	Peer	8	2005-07-04	2008-05-27 (1)	1058			0.06	0.06	193.110.153.0/24
12826	AS12826 C-SI Autonomous System	Stub(0)	Unknown	8	2008-05-22		6			3.52	0.11	212.234.178.0/24
19557	CHANGEIP-01 - CHANGEIP COM	Stub(0)	Provider	4	2005-10-23	2008-05-27 (1)	947			3.18	3.18	204.16.168.0/22
23073	BIGZOO-001 - Big Zoo . com	Stub(1)	Provider	3	2007-03-19	2008-05-23 (5)	431			3.5	3.5	208.73.232.0/21
25187	FCV FRANCE CITEVISION	Stub(0)	Provider	3	2004-05-17	2008-05-27 (1)	1471			0.45	0.45	213.151.160.0/19
27491	NATIONAL-FINANCIAL-PARTNERS-CORP - NATIONAL FINANCIAL PARTNERS	Stub(0)	Provider	3	2006-09-09	2008-05-26	625			0.63	0.63	38.98.87.0/24

Detecting anomalies

AS 174 (COGENT Cogent/PSI)

ASN	AS Name	Type	Relationship	Degree	Appearance Date	Disappearance Date	Lifetime	Weight	Last BGP Message
1668	AOL-ATDN - AOL Transit Data Network	Transit-Tier1	Unknown	108	2008-01-29 (0)	2008-01-29 (43)	0		64.236.38.0/24
35456	FUBRA-AS Fubra Limited	Stub-Unknown	Unknown	37	2008-03-11 (0)	2008-03-11 (1)	0		87.124.0.0/17
3595	GNAXNET-AS - Global Net Access, LLC	Transit-Unknown	Unknown	19	2008-01-29 (0)	2008-01-29 (43)	0		63.247.71.0/24
10994	TAMPA2-TWC-5 - Road Runner HoldCo LLC	Transit-Unknown	Unknown	10	2008-03-05 (0)	2008-03-05 (7)	0		71.40.128.0/18
3360	CSC-ASN - Computer Sciences Corporation	Transit-Unknown	Unknown	5	2008-01-29 (0)	2008-01-29 (43)	0		62.248.116.0/24
23664	WIPRO-TECH-AS-AP Wipro Technologies,	Stub-Unknown	Unknown	2	2008-01-10 (0)	2008-01-10 (62)	0		203.91.192.0/22
39122	BLACKNIGHT-AS Blacknight Internet Solutions Ltd	Stub-Unknown	Unknown	10	2008-02-25 (1)	2008-02-26 (15)	1		78.153.192.0/19
41695	VOSTRON-AS Vostron Ltd	Stub-Unknown	Unknown	3	2008-03-10 (1)	2008-03-11 (1)	1		89.21.224.0/19
43889		Unknown	Unknown	1	2008-03-04 (1)	2008-03-05 (7)	1		79.170.216.0/21
11160	COSTAR-SANDIEGO - COSTAR GROUP	Stub-Unknown	Unknown	3	2008-03-09 (2)	2008-03-11 (1)	2		204.253.48.0/24
40695		Unknown	Unknown	1	2008-03-07 (4)	2008-03-11 (1)	4		38.103.1.0/24
19332	Marcatel	Transit-Unknown	Unknown	10	2008-03-06 (5)	2008-03-11 (1)	5		148.243.52.0/24

Suspicious ephemeral routes, most likely misconfigurations or malicious attacks

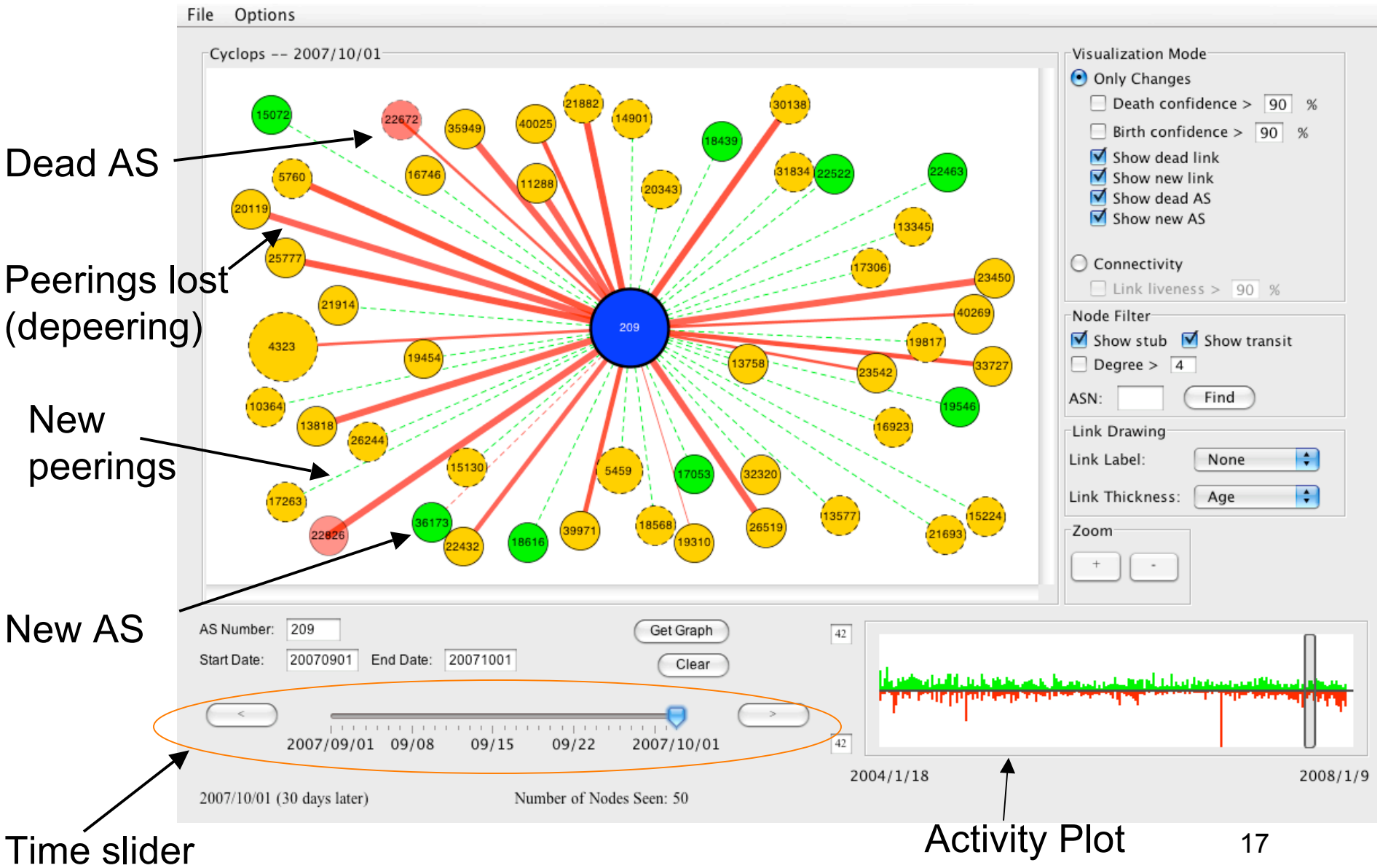
Detecting anomalies

AS 174 (COGENT Cogent/PSI)

ASN	AS Name	Type	Reltn.	Deg.	First App.	Disapp. Date	Age	Weight (To) Avg.	Weight (To) Diff.
30912	DCSNET-GLOBAL-TRANSIT-AS DCS.net	small ISP(17)	Provider	8	2007-02-26		455	1182.63	1182.63
16559	REALCONNECT-01 - RealConnect, Inc	Stub(1)	Provider	72	2005-03-23		1160	2037.92	466.72
3267	RUNNET-AS RUNNet	large ISP(252)	Provider	238	2007-11-15		193	1322.39	419.74
6730	SUNRISE sunrise (TDC Switzerland AG)	large ISP(111)	Provider	659	2004-02-17		1560	255.77	255.77
20485	TRANSTELECOM JSC Company TransTeleCom	large ISP(1746)	Provider	572	2005-08-11		1019	165.78	165.78
5462	CABLEINET Telewest Broadband	large ISP(52)	Provider	408	2004-03-03		1545	158.07	158.07
2914	NTT-COMMUNICATIONS-2914 - NTT America, Inc.	Tier-1(10603)	Provider	757	2003-12-31		1608	617.41	147.97
812	ROGERS-CABLE - Rogers Cable Communications Inc.	large ISP(88)	Provider	110	2003-12-31		1608	440.97	142.66

Cyclops also keep tracking of number of routes in each link; possible to sort links by weight variation

Cyclops Visualizer



Visualizer Components

- **Main layout**

Disappeared link/node

New link/node

Existing link/node

Cyclops' eye

Expanded node

stub

transit

tier-1

- Link thickness represents link weight (#prefixes, age)

- Transparency represents change confidence

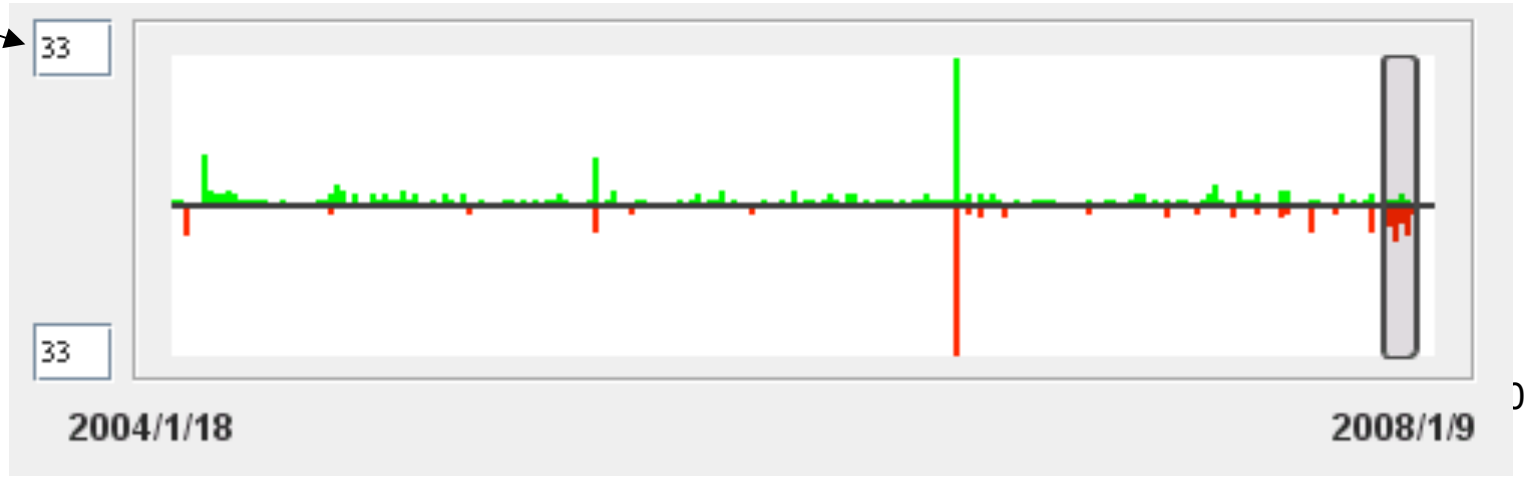
Cyclops Visualizer

- **Event correlation:** enables visual correlation of events happening in different ASes
- **Activity plot:** help identify periods of "anomalous" number of AS connectivity changes
- **Time slider:** finer control over time window

Visualizer components

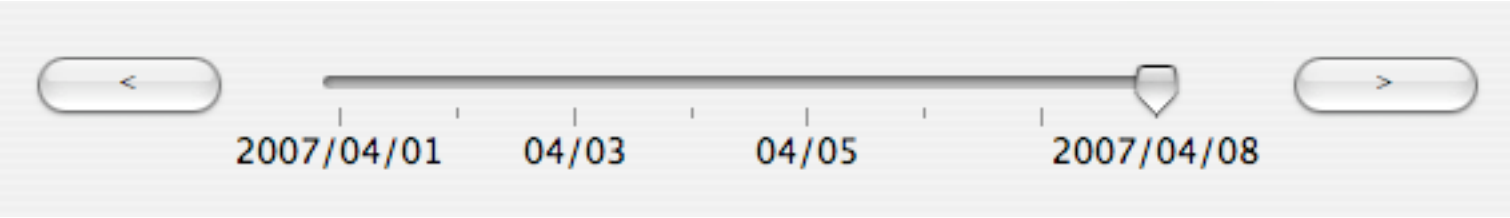
- **Activity graph:** makes it easier to spot abnormal events, e.g. massive depeerings
  - each bar represents changes aggregated over 1 week
  - top green bars represent new peerings; bottom red bars represent depeerings
  - Vertical scale can be set by the user
  - Grey slider allows to focus on period of interest

No. of changes

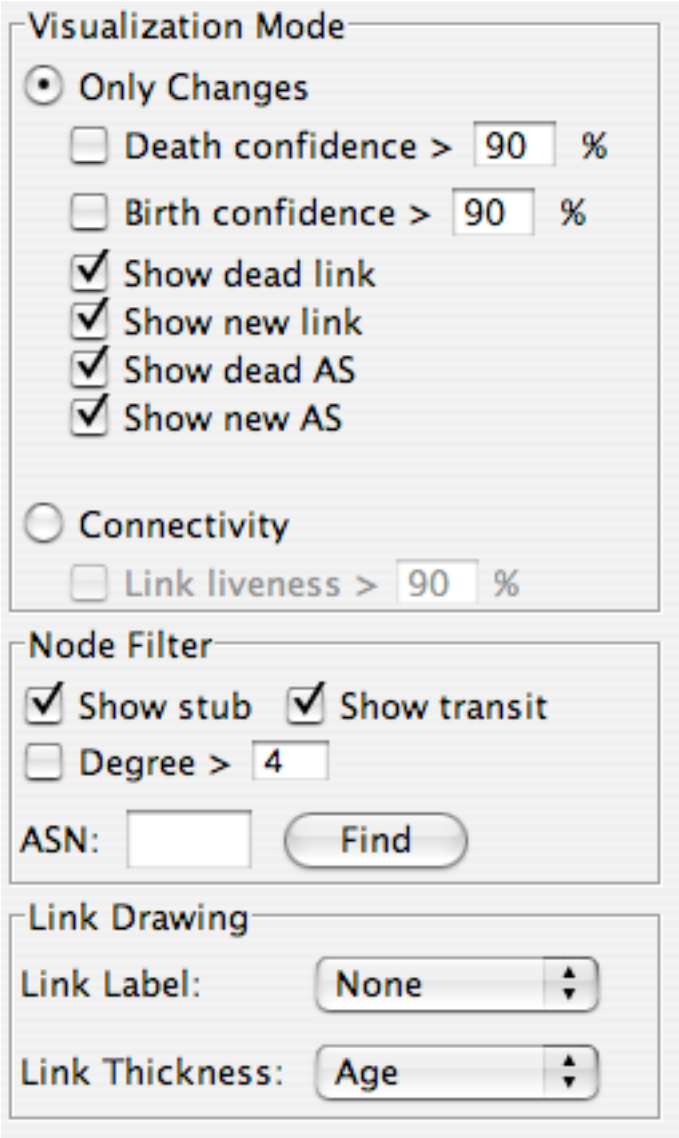


Visualizer Components

- **Time slider**: fine gain control of the observation time we're interested; allows to move to next/previous change



Visualizer components



- **Visualization modes:**

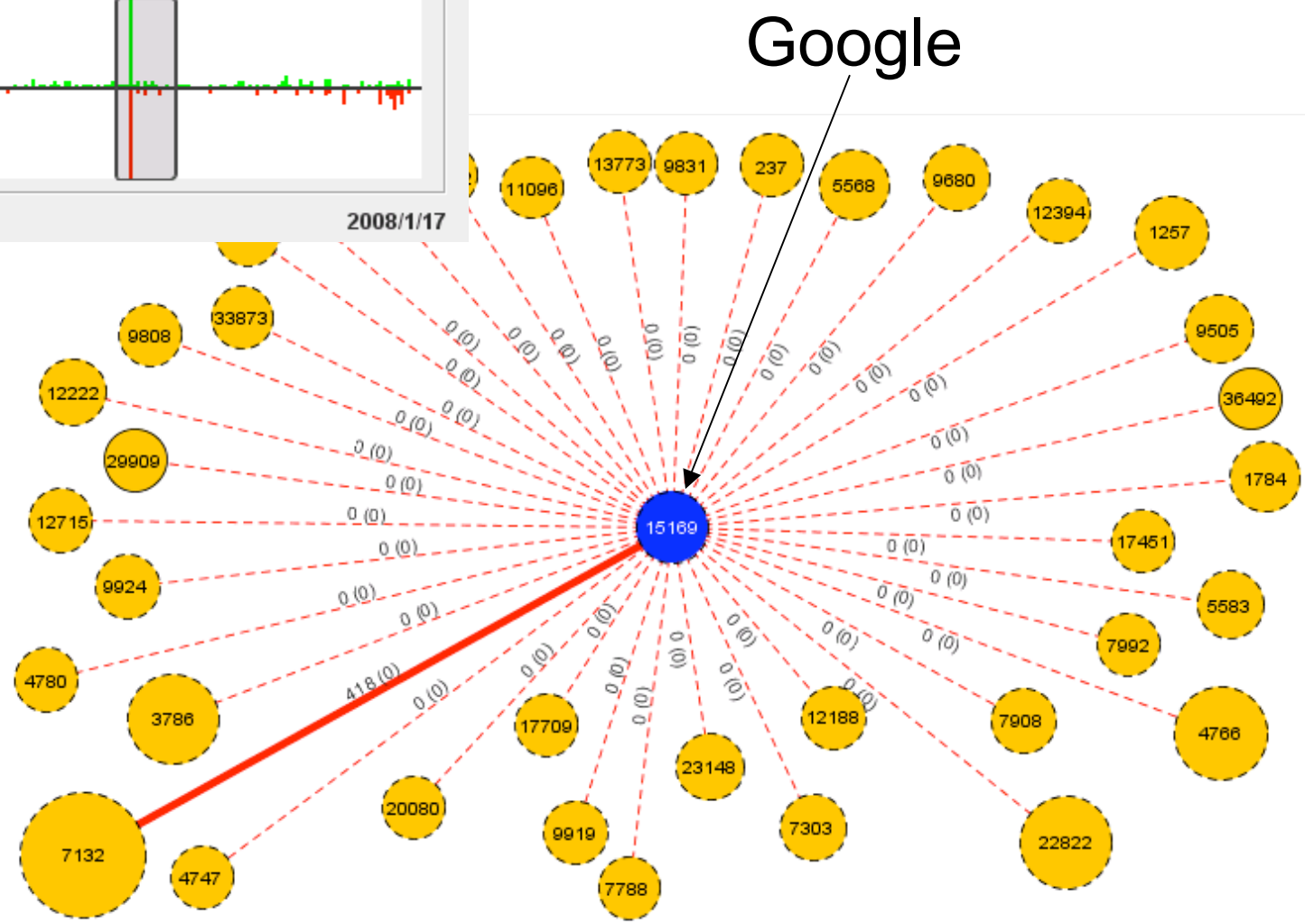
- "*Only changes*" display only the changes in the relevant time period; changes can be filtered by confidence [sigcomm'07]

-"*Connectivity*" displays the topology snapshot at a given time

- **Other options:**

- filters by type of AS and degree
- configure link labels and thickness, e.g. #routes, age

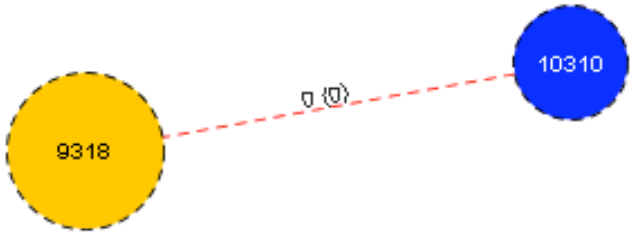
Case study #1: Google's route leakage



July 19, 2006

Activity plot helps spot anomalous changes

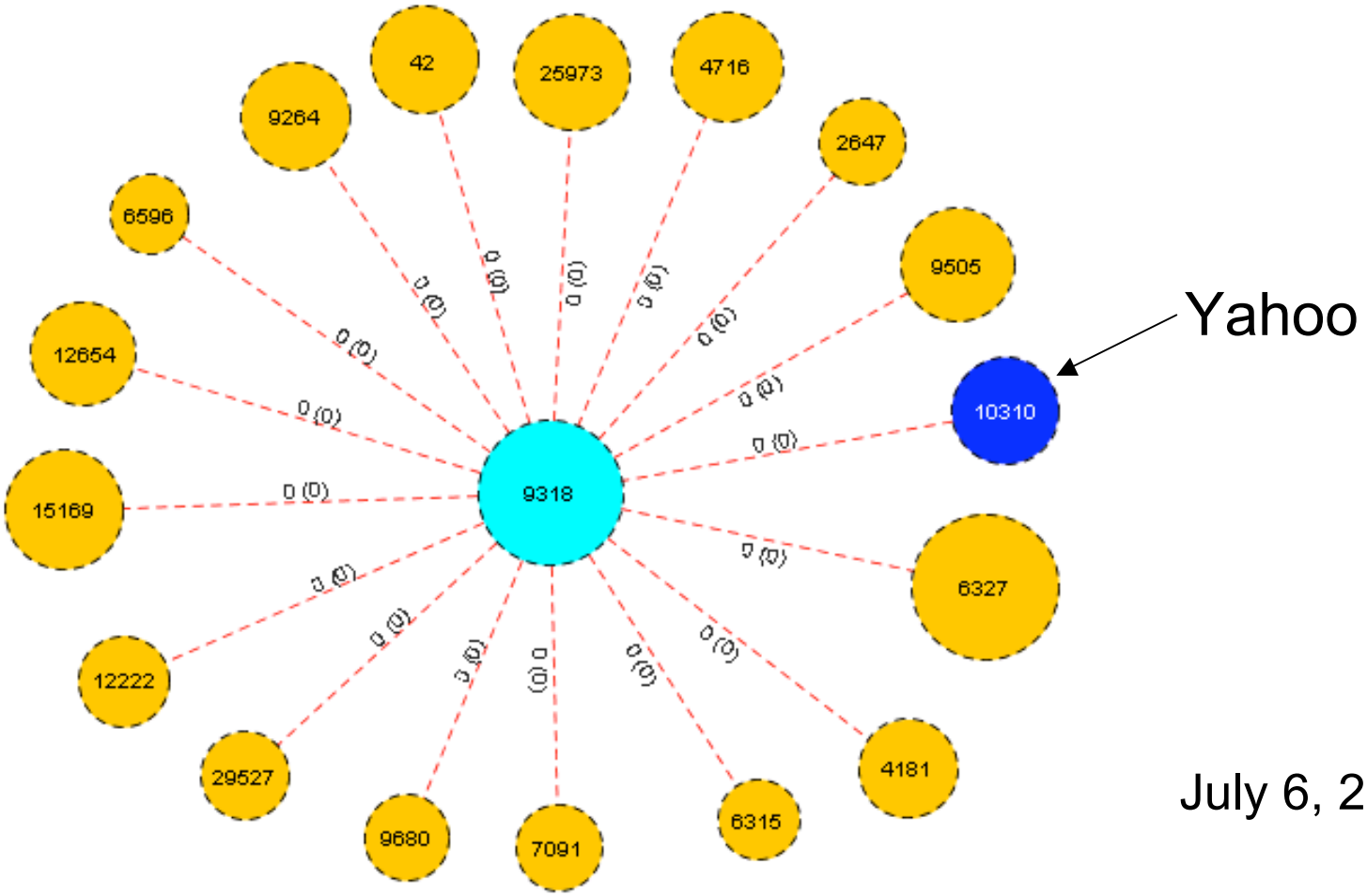
Case #2: Yahoo's outage



July 6, 2007

After studying Yahoo's connectivity, we noticed a transient peering with AS9318

Case #2: Yahoo's outage



July 6, 2007

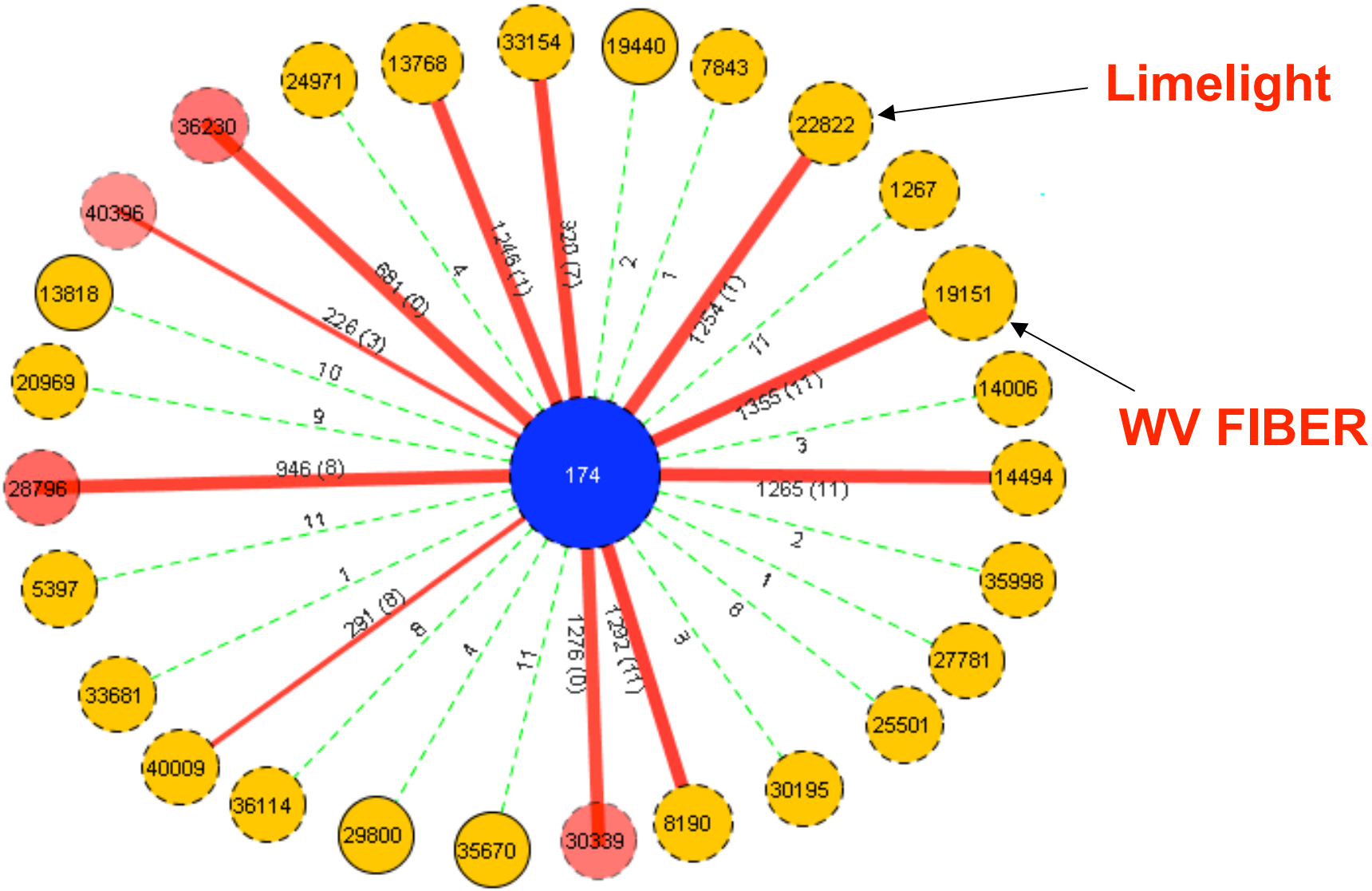
AS 9318's route leakage caused Yahoo's outage

http://isc.sans.org/diary.html?storyid=3112

Case#3 Cogent depeerings (9/15 – 29)

“Did Cogent depeer Limelight, WV FIBER, and nLayer?”
@Nanog mailing list, Sept 28th 2007

Case#3 Cogent depeerings (9/15 – 29)



Apparently nLayer not depeered…

Future work: Cyclops' alarms

- Idea is to allow ISPs to register for alarms; examples of alarms are:
  - Large shifts in number of routes/link
  - Links with very short lifetime
  - Differences between PV-GT (ground truth)

- Feature under development, would like to hear ISP ideas about this; who would like to sign up for these alarms?

Req Feedback

- We encourage everybody to try it out (the server can be down if all try at same time;))

  http://cyclops.cs.ucla.edu

- What would you like to change in Cyclops?
- What new functionality you would like to see?
- Did it help diagnosing some problem in your network? Let us know!
- And please report any data inconsistency

More resources

- AS-level connectivity raw data
  http://cyclops.cs.ucla.edu/rawdata

- Cyclops mailing list:
  http://www.cs.ucla.edu/mailman/listinfo/cyclops

- IRL topology page
  http://irl.cs.ucla.edu/topology

Send all questions and comments to **cyclops@lists.cs.ucla.edu** Thanks!