Cyber DEfense Technology Experimental Research (DETER) Network
Evaluation Methods for Internet Security Technology (EMIST)
USC Information Sciences Institute • University of California, Berkeley • University of California, Davis • Penn State University
Purdue University • International Computer Science Institute • Stanford Research Institute (SRI) • Network Associates • SPARTA

Routing Data

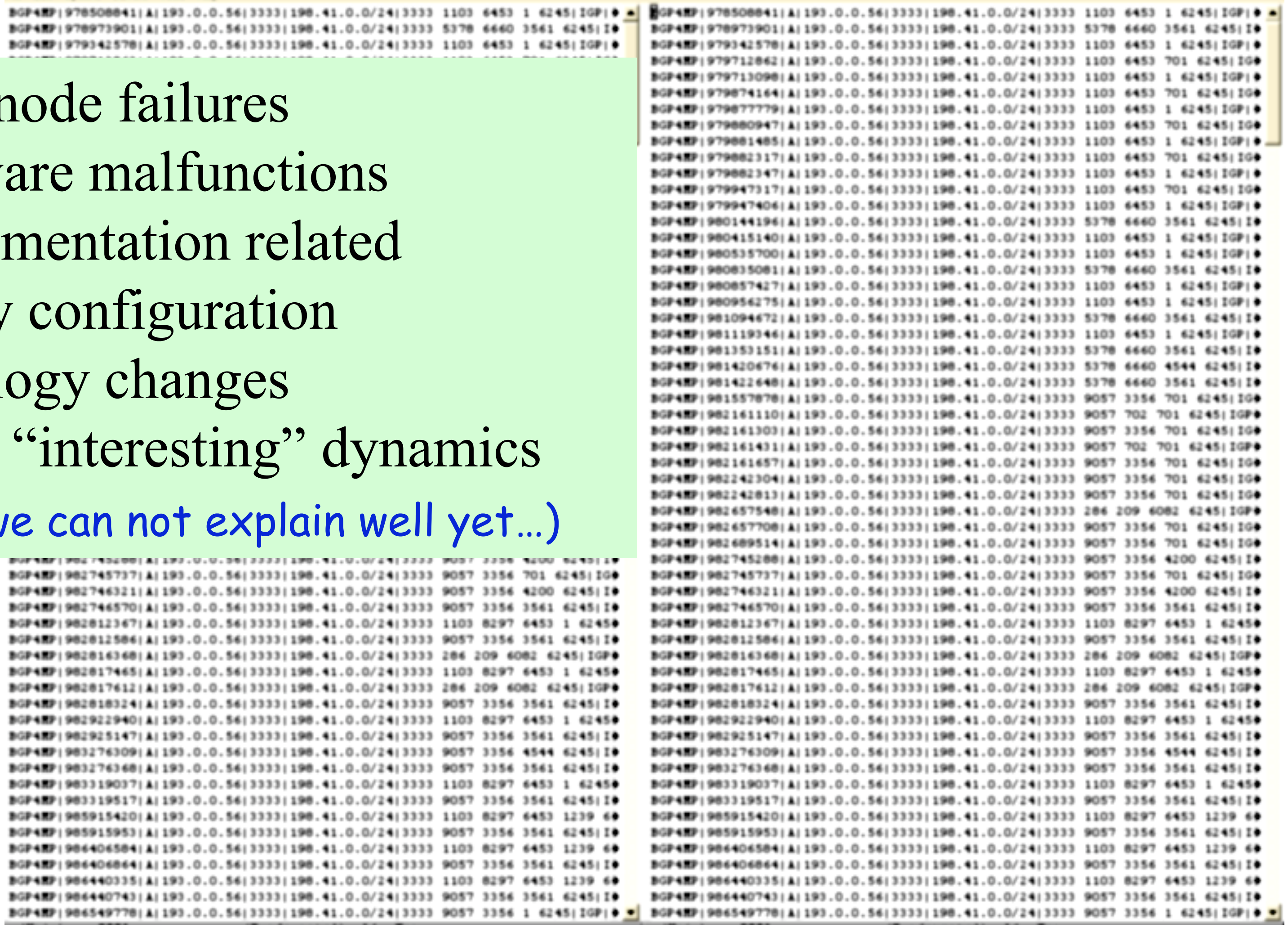
the PREDICT Anonymization Panel

S. Felix Wu
Computer Science Department
University of California, Davis
wu@cs.ucdavis.edu
http://www.cs.ucdavis.edu/~wu/

Route View Data

- ➢Link/node failures
- ➢Software malfunctions
- ➢Implementation related
- ➢Policy configuration
- ➢Topology changes
- ➢Other “interesting” dynamics

(that we can not explain well yet…)



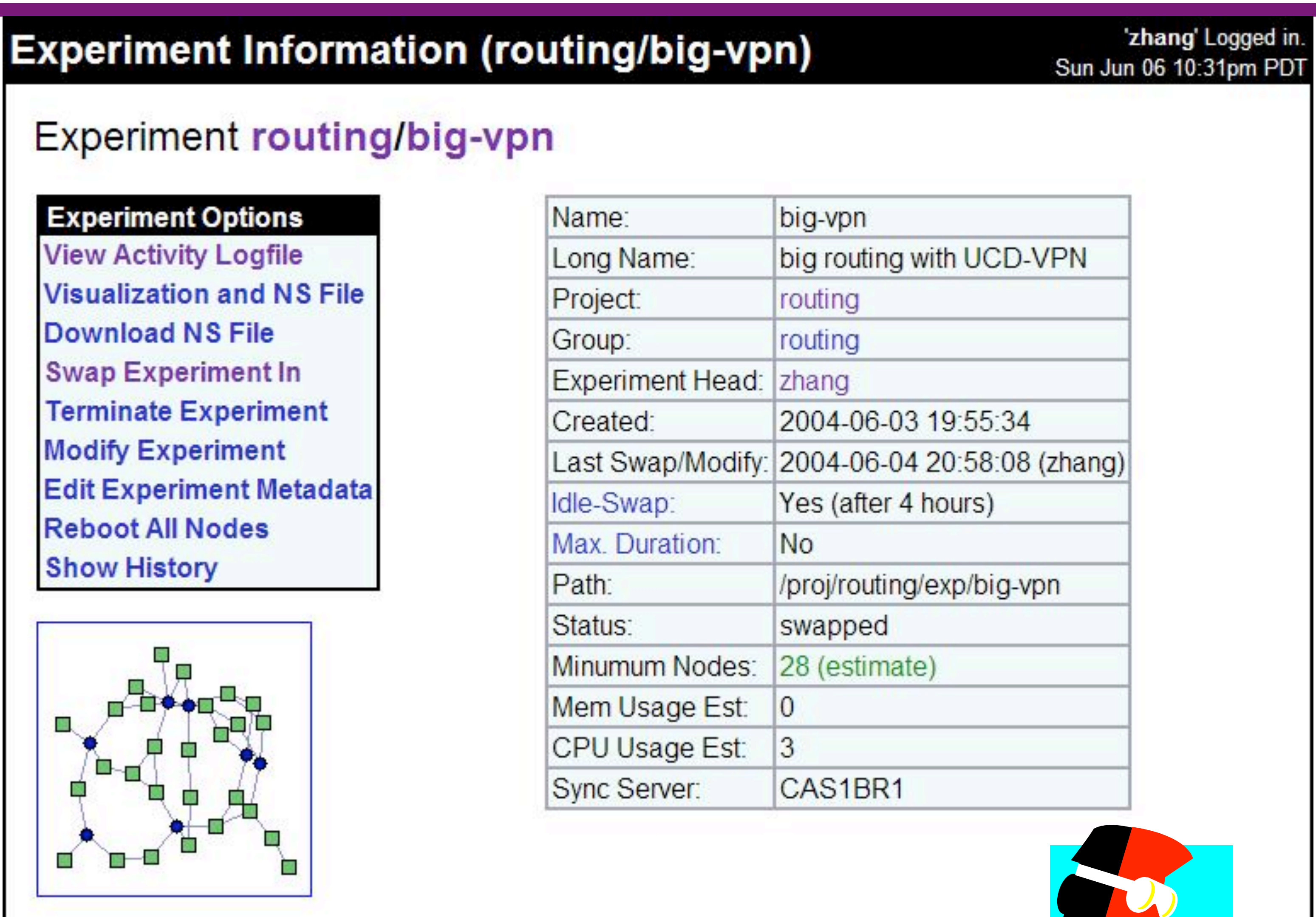
```
BGP4MP|978508841|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|978973901|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|979342578|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979712862|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979713098|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979874164|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979877779|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979880947|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979881485|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979882317|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979882347|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|979947317|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 701 6245|IG●
BGP4MP|979947406|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980144196|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|980415140|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980535700|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980835081|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|980857427|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|980956275|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|981094672|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981119346|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|981353151|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981420676|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 4544 6245|I●
BGP4MP|981422648|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|981557878|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982161110|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 702 701 6245|IGP●
BGP4MP|982161303|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982161431|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 702 701 6245|IGP●
BGP4MP|982161657|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982242304|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982242813|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982657548|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982657708|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982689514|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982745288|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4200 6245|I●
BGP4MP|982745737|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982746321|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4200 6245|I●
BGP4MP|982746570|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982812367|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982812586|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982816368|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982817465|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982817612|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982818324|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982922940|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982925147|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983276309|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4544 6245|I●
BGP4MP|983276368|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983319037|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|983319517|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|985915420|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|985915953|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986406584|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986406864|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986440335|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986440743|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986549778|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 1 6245|IGP|●
```

```
BGP4MP|978508841|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|978973901|A|193.0.0.56|3333|198.41.0.0/24|3333 5378 6660 3561 6245|I●
BGP4MP|979342578|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 6453 1 6245|IGP|●
BGP4MP|982745737|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 701 6245|IG●
BGP4MP|982746321|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4200 6245|I●
BGP4MP|982746570|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982812367|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982812586|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982816368|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982817465|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982817612|A|193.0.0.56|3333|198.41.0.0/24|3333 286 209 6082 6245|IGP●
BGP4MP|982818324|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|982922940|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|982925147|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983276309|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 4544 6245|I●
BGP4MP|983276368|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|983319037|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1 6245●
BGP4MP|983319517|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|985915420|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|985915953|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986406584|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986406864|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986440335|A|193.0.0.56|3333|198.41.0.0/24|3333 1103 8297 6453 1239 6●
BGP4MP|986440743|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 3561 6245|I●
BGP4MP|986549778|A|193.0.0.56|3333|198.41.0.0/24|3333 9057 3356 1 6245|IGP|●
```

What data?

- Replay and “Interactive” Replay

DETER/EMIST Routing Experiments



Experiment Information (routing/big-vpn)

'zhang' Logged in.
Sun Jun 06 10:31pm PDT

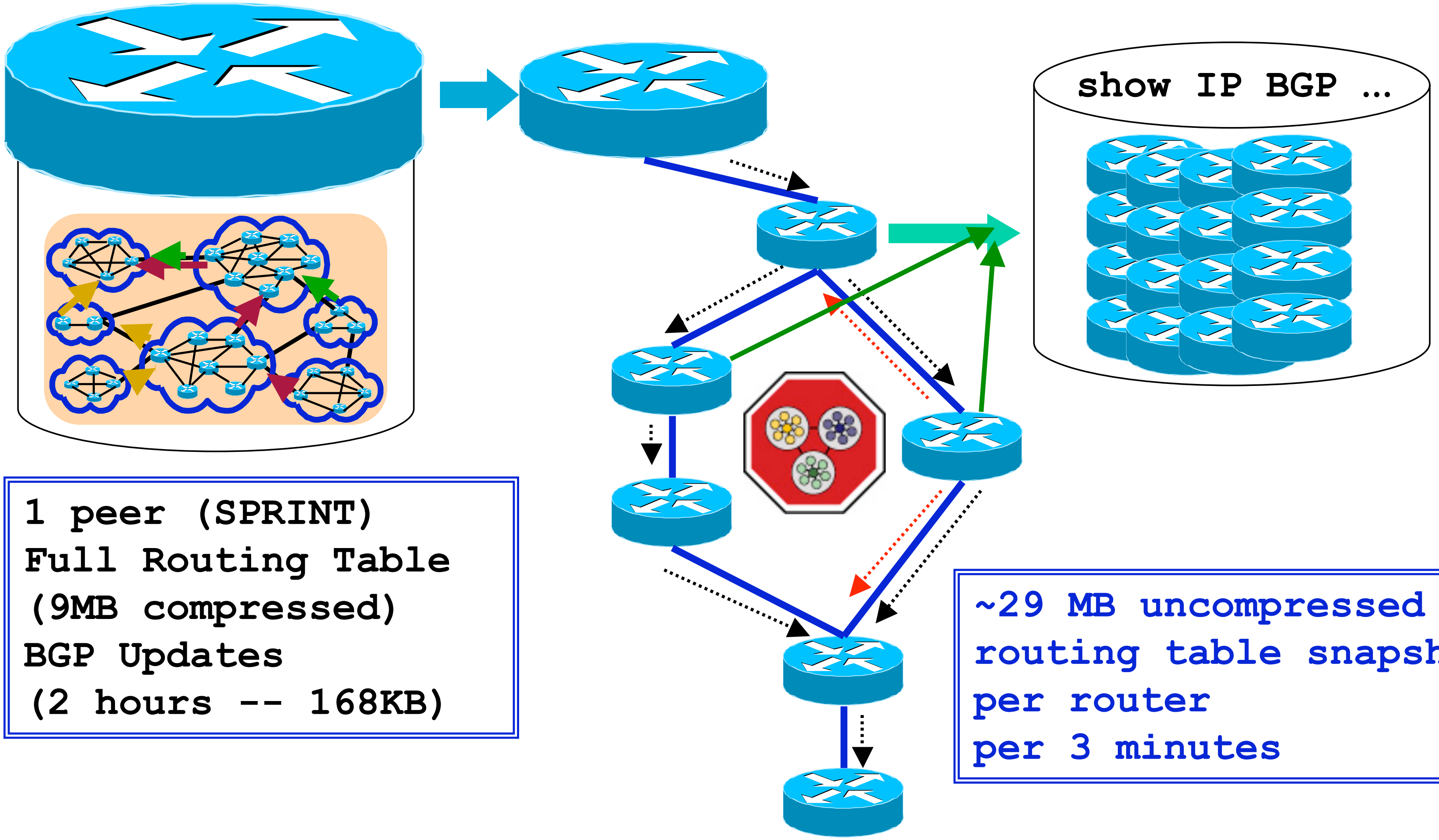
Experiment routing/big-vpn

Experiment Options

- View Activity Logfile
- Visualization and NS File
- Download NS File
- Swap Experiment In
- Terminate Experiment
- Modify Experiment
- Edit Experiment Metadata
- Reboot All Nodes
- Show History

Name:	big-vpn
Long Name:	big routing with UCD-VPN
Project:	routing
Group:	routing
Experiment Head:	zhang
Created:	2004-06-03 19:55:34
Last Swap/Modify:	2004-06-04 20:58:08 (zhang)
Idle-Swap:	Yes (after 4 hours)
Max. Duration:	No
Path:	/proj/routing/exp/big-vpn
Status:	swapped
Minumum Nodes:	28 (estimate)
Mem Usage Est:	0
CPU Usage Est:	3
Sync Server:	CAS1BR1

Routing Experimentation



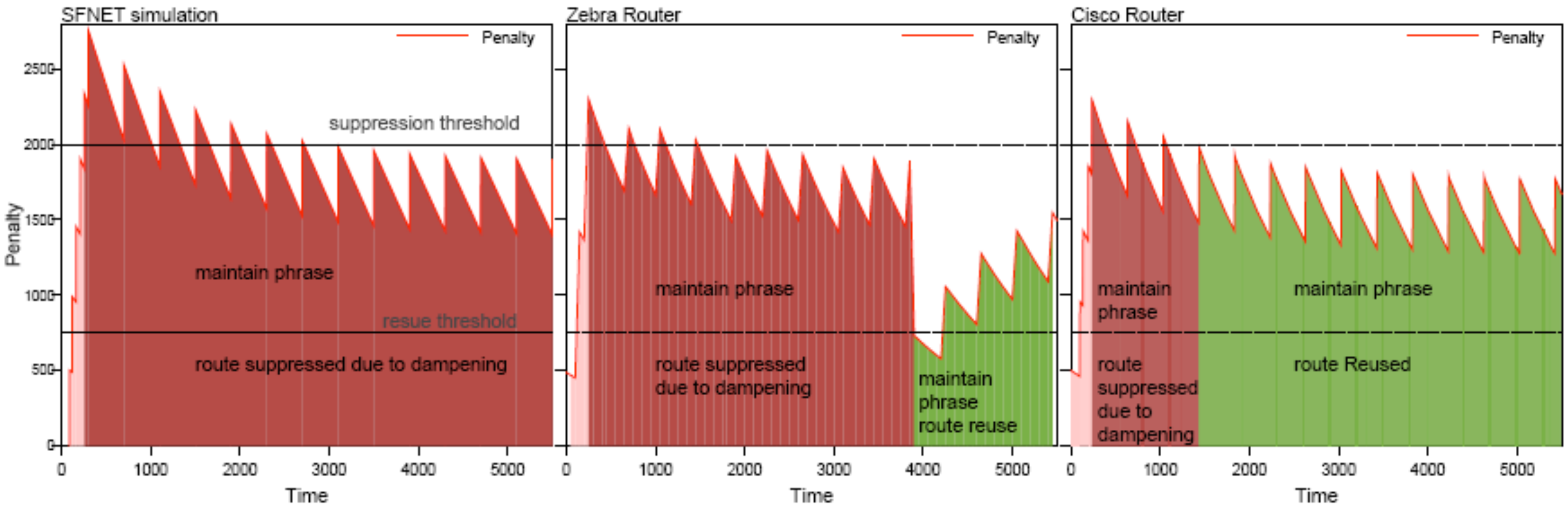
1 peer (SPRINT)
Full Routing Table
(9MB compressed)
BGP Updates
(2 hours -- 168KB)

~29 MB uncompressed
routing table snapshot
per router
per 3 minutes

What data?

- Replay and “Interactive” Replay
- A Sample of Examples:
  - Intra-AS topology and policy configuration
  - Router specific information
    - Dampening implementation
    - MRAI timer

Different Dampening Implementations



SSFNet **Zebra** **Cisco**

Data Anonymization

- Property-Oriented Transformation
  - Interesting/hidden properties
  - Consistent transformation

- The Issue:
  - Correct Transformation → Well-known Properties
  - Unknown properties are our main interest

Why Anonymize Routing Data?

- “cover-up” for operational mistakes or something along the line …

Why Anonymize Routing Data?

- “cover-up” for operational mistakes or something along the line …

- “valuable” information for critical infrastructure attackers

Why Anonymize Routing Data?

- "cover-up" for operational mistakes or something along the line …
- "valuable" information for critical infrastructure attackers

- The public routing data (e.g., route view) might be sufficient for the attackers already, but is still insufficient for clearly understanding the Internet routing behavior.