

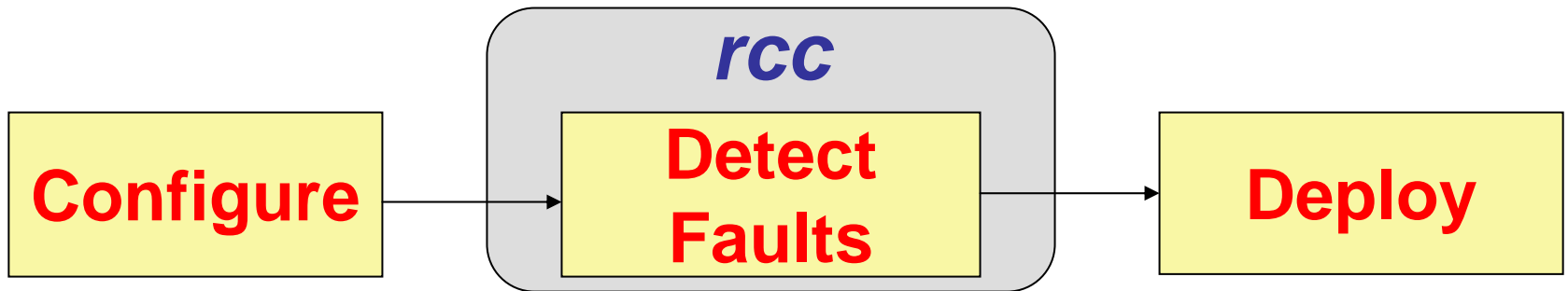
# Network Troubleshooting: *rcc* and Beyond

**Nick Feamster**  
Georgia Tech

(joint with Russ Clark, Yiyi Huang, Anukool Lakhina)

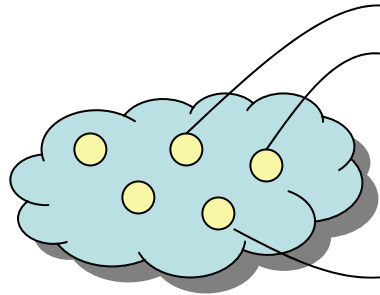
# rcc: Router Configuration Checker

- **Proactive** routing configuration analysis
- **Idea:** Analyze configuration *before* deployment



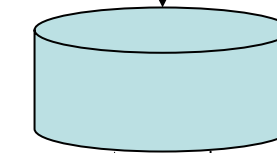
Many faults can be detected with static analysis.

# rcc Implementation



**Distributed router configurations**  
(Cisco, Avici, Juniper, Procket, etc.)

<http://nms.csail.mit.edu/rcc/>



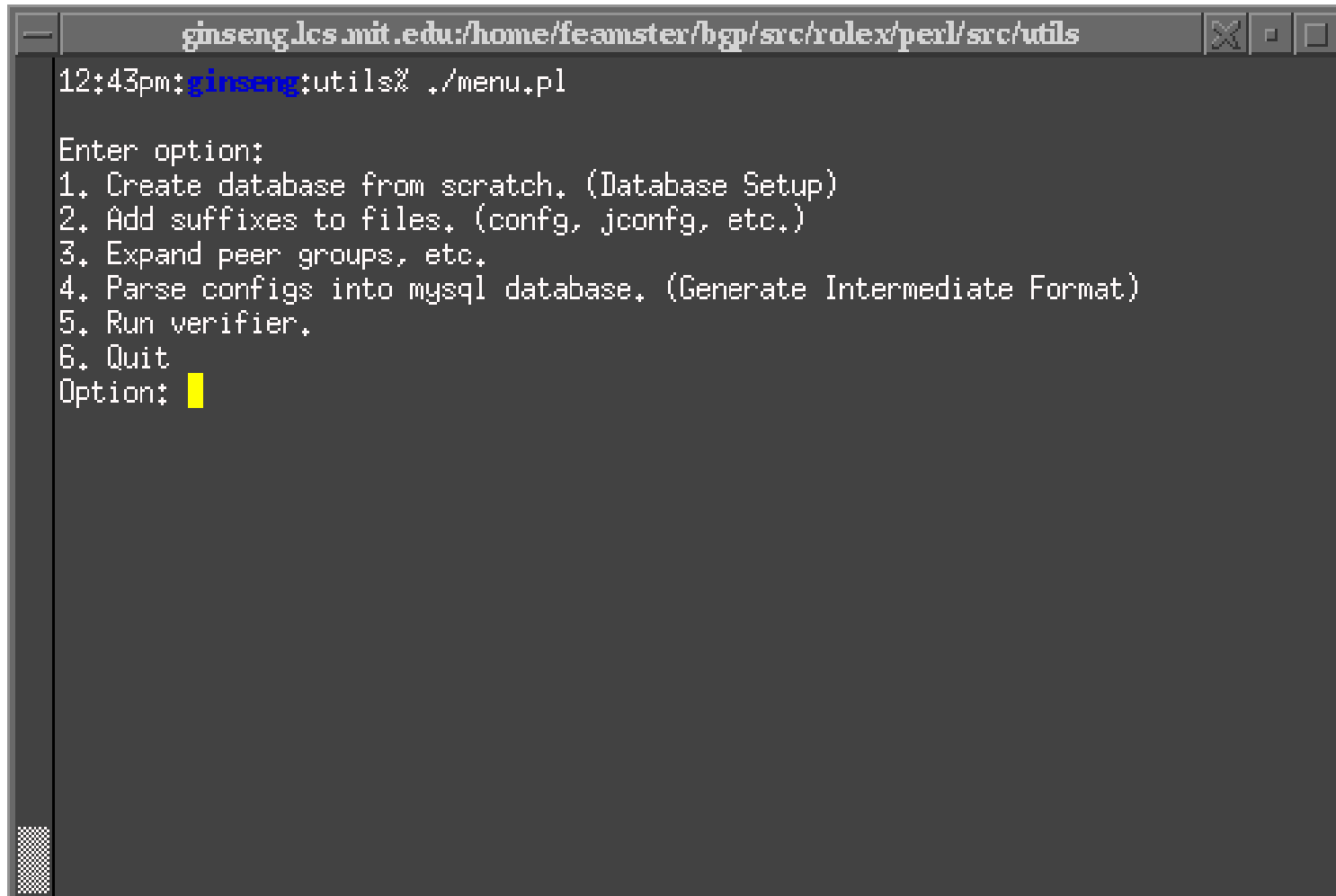
**Relational Database (mySQL)**



***Faults***

Constraints

# rcc Interface

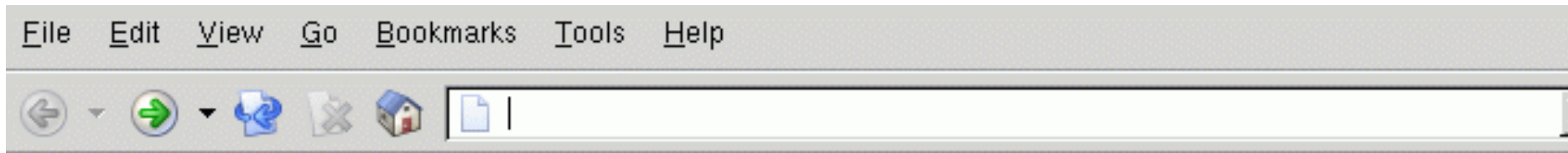


```
ginseng.lcs.mit.edu:/home/feamster/bgp/src/rolex/perl/src/utls
12:43pm:ginseng:utls% ./menu.pl
Enter option:
1. Create database from scratch. (Database Setup)
2. Add suffixes to files. (config, jconfig, etc.)
3. Expand peer groups, etc.
4. Parse configs into mysql database. (Generate Intermediate Format)
5. Run verifier.
6. Quit
Option: █
```

# Parsing Configuration

```
Enter option:
1. Create database from scratch. (Database Setup)
2. Add suffixes to files. (config, jconfig, etc.)
3. Expand peer groups, etc.
4. Parse configs into mysql database. (Generate Intermediate Format)
5. Run verifier.
6. Quit
Option: 4
Enter config directory [/home/feamster/rcc-demo/trans/]:
Config dir is: /home/feamster/rcc-demo/trans/
/home/feamster/rcc-demo/trans//rtr-a-config
ERROR: undefined prefix-list/distribute list BLOCK-F00 (rtr-a, 172.114.63.145)
/home/feamster/rcc-demo/trans//rtr-b-config
ERROR: undefined prefix-list/distribute list 45 (rtr-b, 86.22.187.24)
/home/feamster/rcc-demo/trans//rtr-c-config
Config dir is: /home/feamster/rcc-demo/trans/
Inserting into DB...done.
Inserting ACLs...done.
Inserting into DB...done.
Inserting ACLs...done.
```

# List of Faults



## rcc Error Summary

[Network Advertisement](#)

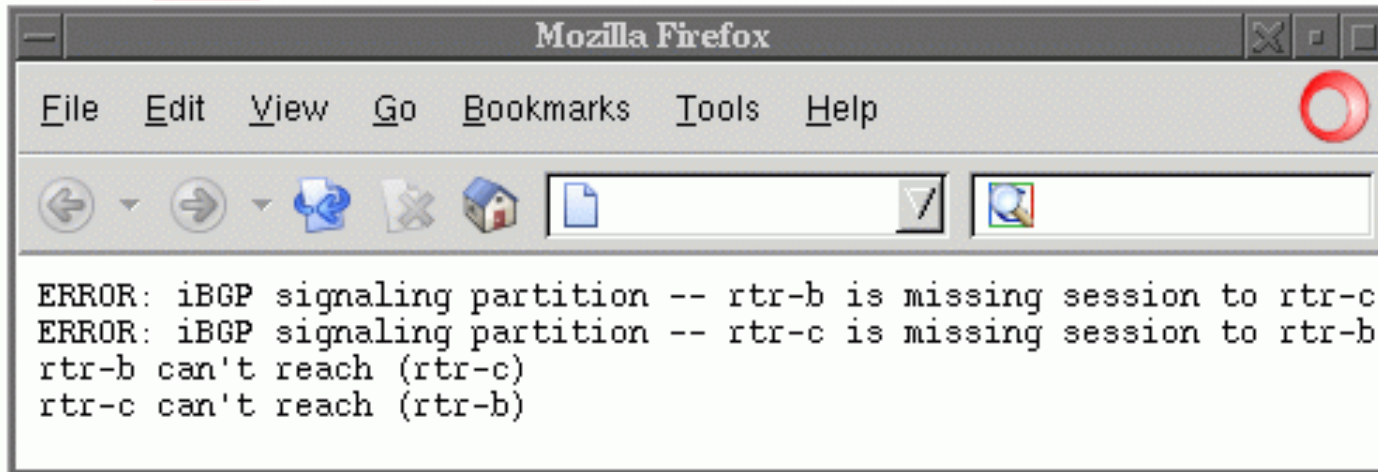
network statements without routes

[Determinism](#)

deterministic-med, router ID tiebreak

[iBGP Signaling](#)

Possible iBGP partitions



ASes  
lists, etc.  
sessions

# Yes, but Surprises Happen!

- Link failures
- Node failures
- Traffic volumes shift
- Network devices “wedged”
- ...
  
- **Two problems**
  - Detection
  - Localization

# A Closer Look

- **Proactive** analysis
  - Fault avoidance
  - Policy conformance
- **Reactive** diagnosis
  - Correcting network faults
    - Detection
    - Localization
  - Active and passive measurements
  - Need user's perspective

**Idea:** These analyses should inform each other

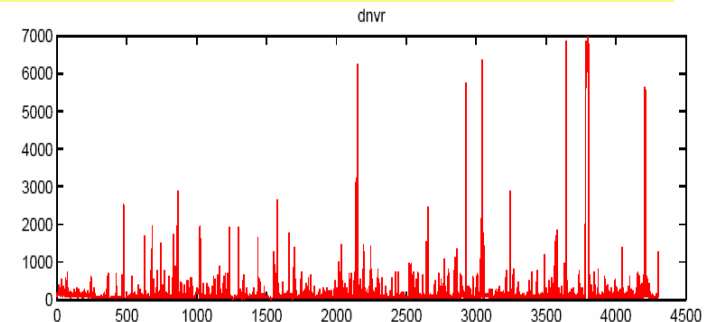
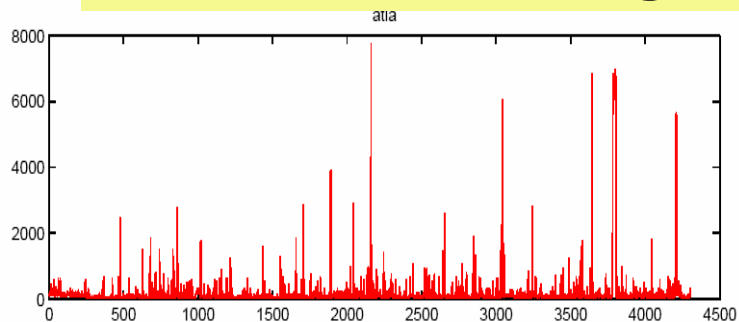


# Detection: Analyze Routing Dynamics

- **Idea:** Routers exhibit **correlated behavior**



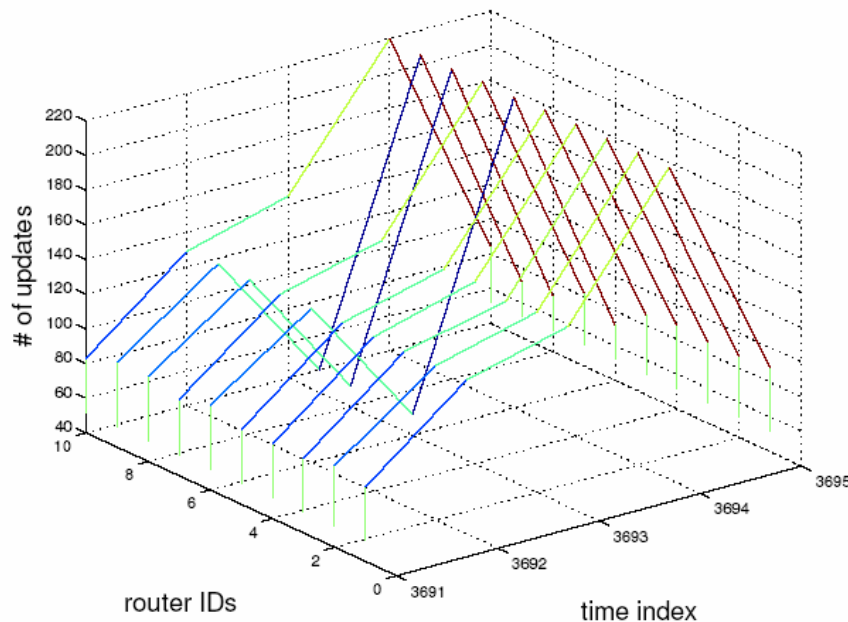
**Blips across signals may be more operationally interesting than any spike in one.**



# Detection Three Types of Events

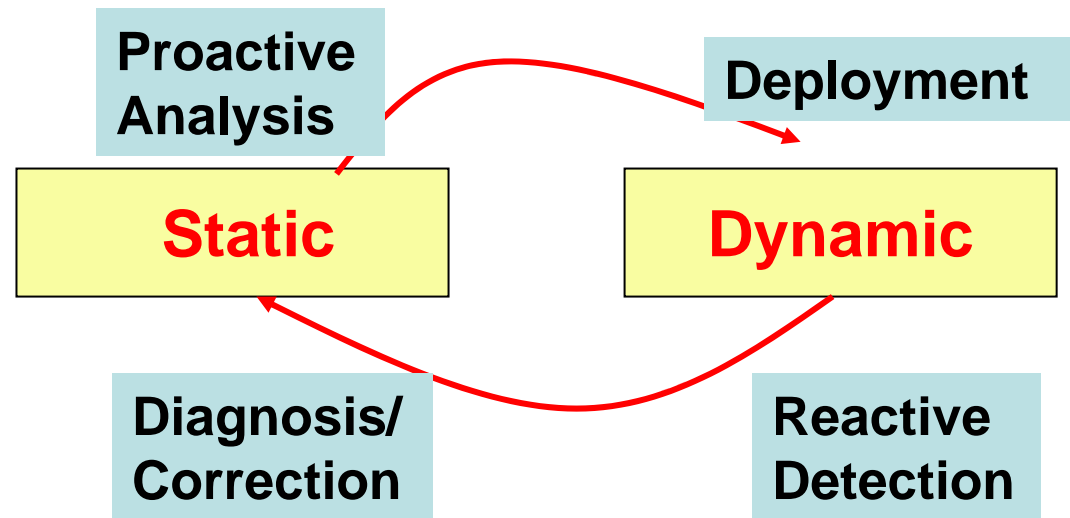
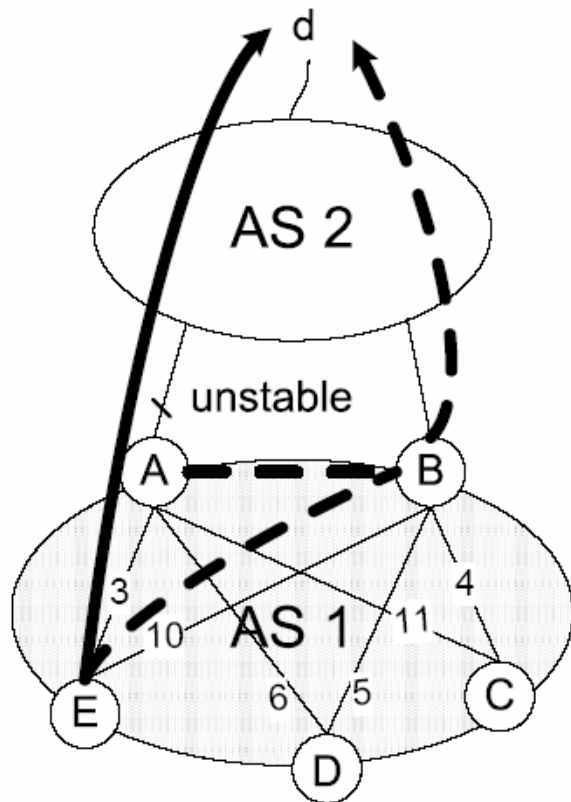
- Single-router bursts
- Correlated bursts
- Multi-router bursts

- **Common**
- ***Commonly missed using thresholds***



# Localization: Joint Dynamic/Static

- Which routers are “border routers” for that burst
- Topological properties of routers in the burst



# Configuration Analysis: Next Steps

- **BGP/MPLS Layer 3 VPNs**
  - Need access to these configurations to do this!
  - **Help needed!**
- **Firewall and switch configurations**
  - Take high-level operator policy as input
  - Analyze static configuration to see whether configuration matches policy
  - Perform active probing experiments to check

# Firewall configuration: Case Study

- **Georgia Tech Campus Network**
  - Research and Administrative Network
  - 180 buildings
  - 130+ firewalls
  - 1700+ switches
  - 55000+ ports
- **Problem:** Availability/Reachability
  - Flux in firewall, router, switch configurations
  - No common authority over changes made

# Specific Focus: Firewall Configuration

- Difficult to understand and audit configs
- Subject to continual modifications
  - Roughly 1-2 touches per day
- Federated policy, distributed dependencies
  - Each department has independent policies
  - Local changes may affect global behavior

# Firewall Configurations

- **Georgia Tech Campus Network**
  - Research and Administrative Network
  - 180 buildings
  - 130+ firewalls
  - 1700+ switches
  - 55000+ ports
- **Problem:** Availability/Reachability
  - Flux in firewall, router, switch configurations
  - No common authority over changes made

# Specific Focus: Firewall Configuration

- Difficult to understand and audit configs
- Subject to continual modifications
  - Roughly 1-2 touches per day
- Federated policy, distributed dependencies
  - Each department has independent policies
  - Local changes may affect global behavior