G-RCA:
A Generic Root Cause Analysis Platform for Service Quality Management in Large IP Networks

He Yan, Lee Breslau, Zihui Ge,
Dan Massey, Dan Pei, Jennifer Yates

Colorado State University and AT&T Labs-Research

Outline

- Motivation
- Challenges
- G-RCA Design
- Case Examples and Operational Experience
- Conclusion

Motivation

- New applications demand high reliability and performance
  - online banking, 911 over VoIP, IPTV, Gaming, …
  - Best-effort service is no longer acceptable

- This change has transformed the way that ISPs conduct service quality management (SQM)
  - individual network element -> end-to-end service quality
    - Router, Link, Line-card -> User perceived performance in a CDN or VPN service
  - hard failure -> transient problem
    - Fiber cut, router failure -> line flap, protocol flap

- The traditional root cause analysis (RCA) systems are reaching their limits.

Challenges in RCA for SQM

- Complex service dependency model

  the quality of a VOIP call across the ISP network depends on the status (congestion level, bit error rate, etc.) of the routers and links along the network path carrying the traffic, which is dynamically determined based on the link weights

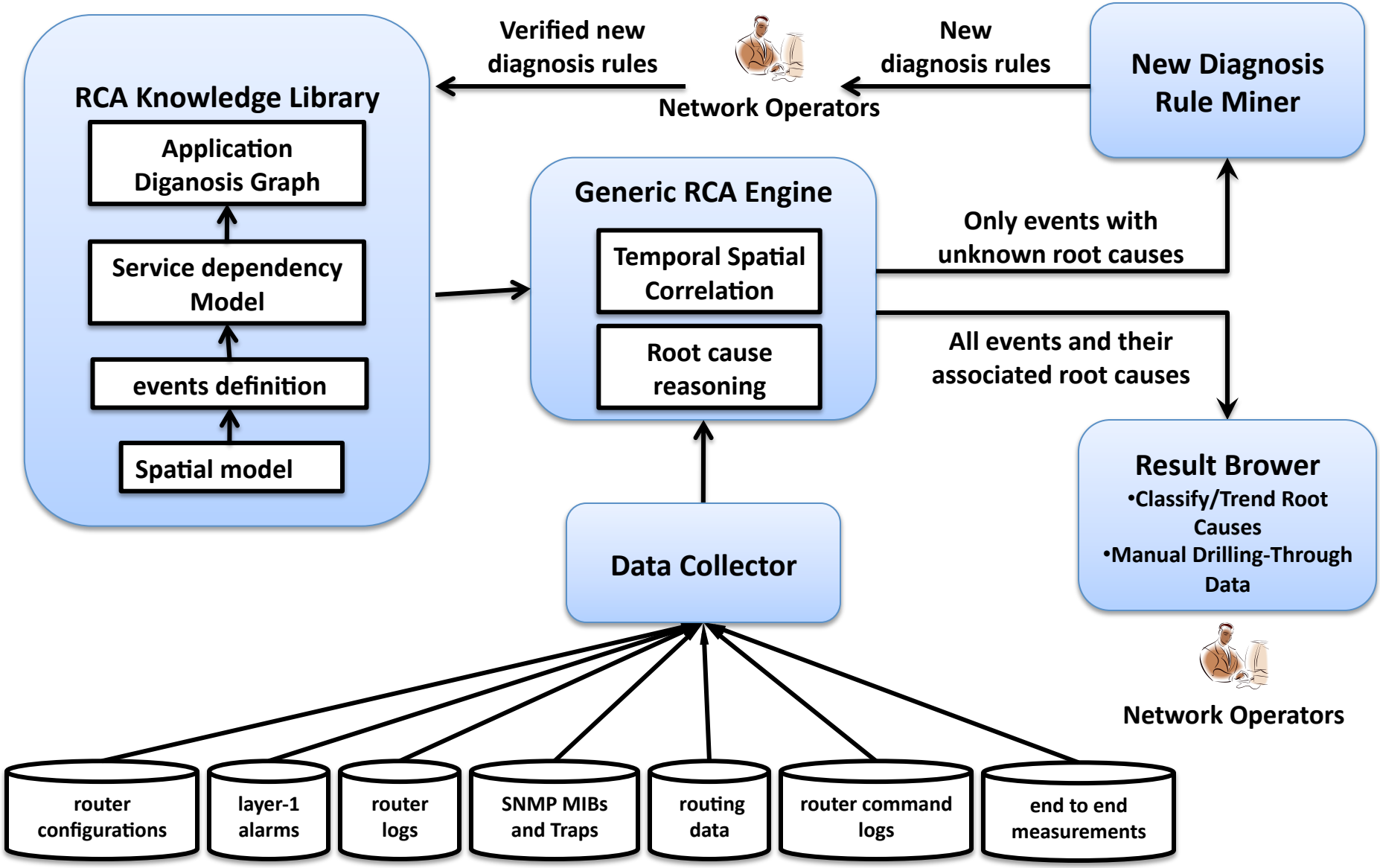
- Ever-changing environment

  new services (e.g., multicast VPN), new technologies (e.g., MPLS TE), new devices (e.g., OC768 line cards) are introduced into ISP networks at a fast rate
  - It requires RCA to deal with imperfect domain Knowledge
  - It needs RCA tools for new services

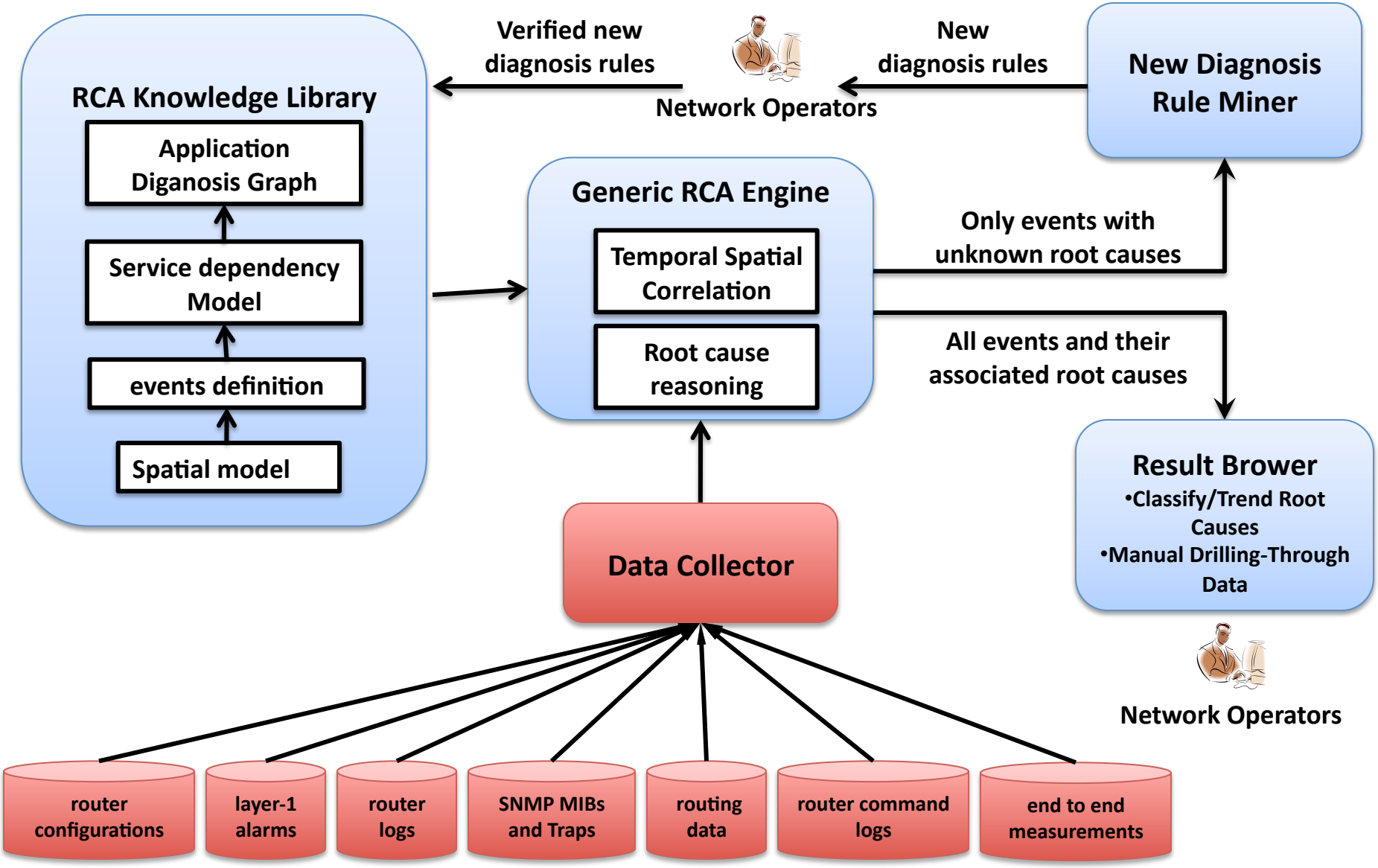
- Data Collection
  - proactively collect data (alarms, logs and performance measurements) to enable the analysis of transient service disruptions

- Scalability
  - Analyze a large number of transient service disruptions over extended period to determine the primary root causes

G-RCA Design


RCA Knowledge Library
Application Diganosis Graph
Service dependency Model
events definition
Spatial model
Verified new diagnosis rules
Network Operators
New diagnosis rules
New Diagnosis Rule Miner
Generic RCA Engine
Temporal Spatial Correlation
Root cause reasoning
Only events with unknown root causes
All events and their associated root causes
Result Brower
•Classify/Trend Root Causes
•Manual Drilling-Through Data
Network Operators
Data Collector
router configurations
layer-1 alarms
router logs
SNMP MIBs and Traps
routing data
router command logs
end to end measurements

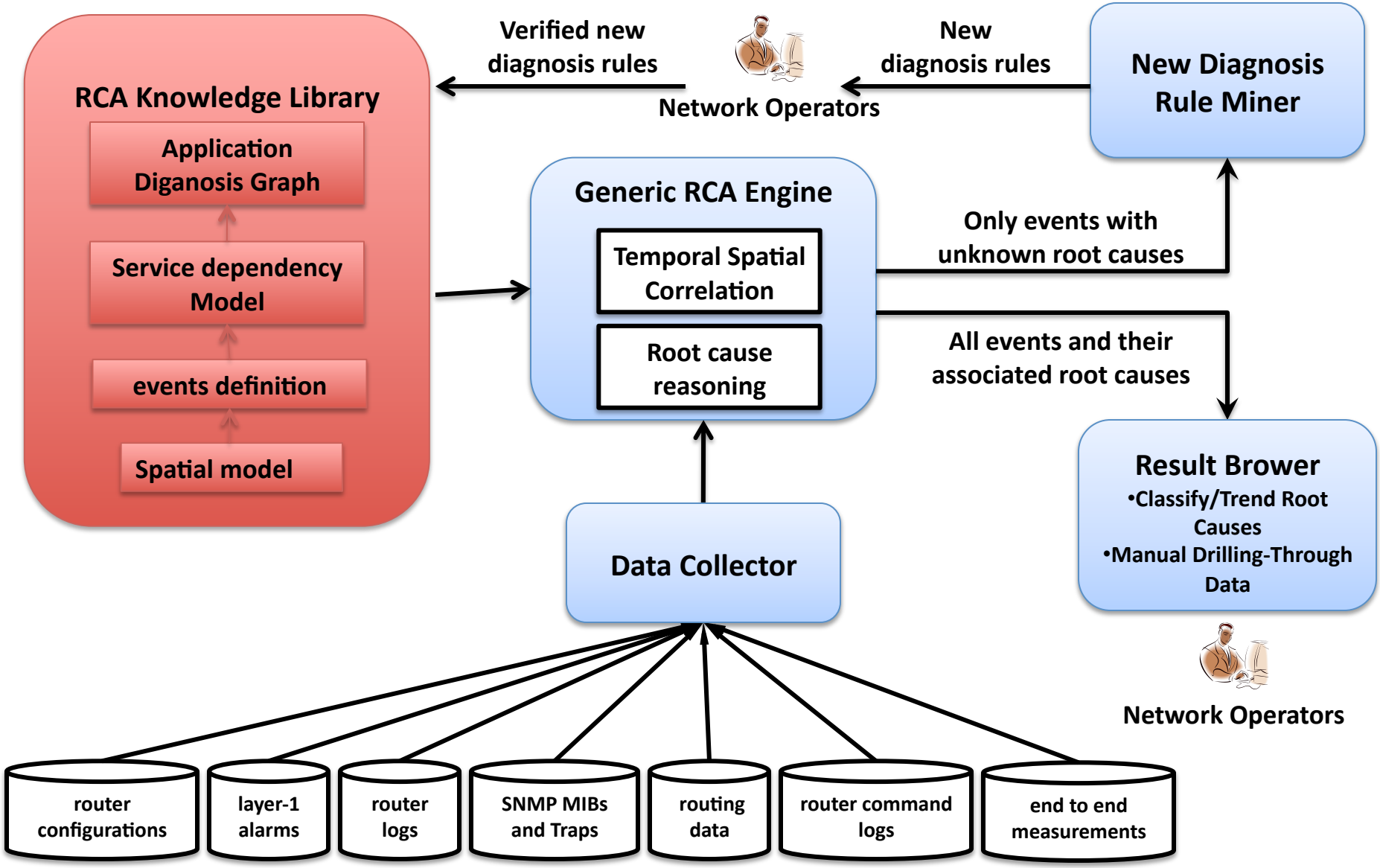
G-RCA Design


Verified new diagnosis rules
New diagnosis rules
Network Operators
New Diagnosis Rule Miner
RCA Knowledge Library
Application Diganosis Graph
Service dependency Model
events definition
Spatial model
Generic RCA Engine
Temporal Spatial Correlation
Root cause reasoning
Only events with unknown root causes
All events and their associated root causes
Result Brower
•Classify/Trend Root Causes
•Manual Drilling-Through Data
Network Operators
Data Collector
router configurations
layer-1 alarms
router logs
SNMP MIBs and Traps
routing data
router command logs
end to end measurements

Data Collector

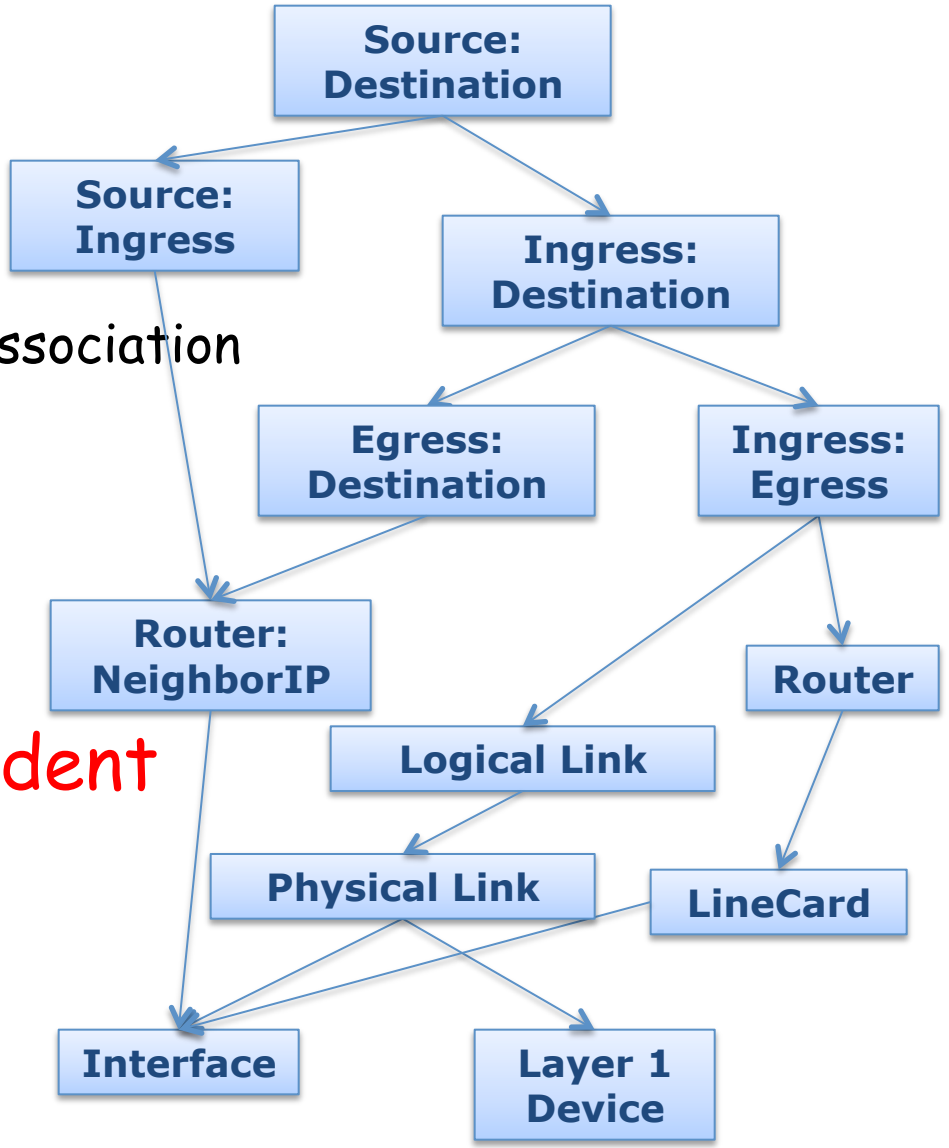
- Proactively collects information from various network devices and systems
  - router configurations, layer-1 alarms, router logs, SNMP MIBs and Traps, inter/intra-domain routing data, router command logs and end-to-end performance measurements
- Normalizes them to facilitate analysis across data sources
  - Different data sources may use different device naming conventions and time zones
  - Normalization hides data complexity for other G-RCA components
- Stores them in database tables in real-time

G-RCA Design


RCA Knowledge Library
Application Diganosis Graph
Service dependency Model
events definition
Spatial model
Verified new diagnosis rules
New diagnosis rules
Network Operators
New Diagnosis Rule Miner
Generic RCA Engine
Temporal Spatial Correlation
Root cause reasoning
Only events with unknown root causes
All events and their associated root causes
Result Brower
•Classify/Trend Root Causes
•Manual Drilling-Through Data
Network Operators
Data Collector
router configurations
layer-1 alarms
router logs
SNMP MIBs and Traps
routing data
router command logs
end to end measurements

RCA Knowledge Library

- Spatial Model
  - topological information
  - cross-layer dependency
  - logical and physical device association
  - dynamic routing
- Mapping is time-dependent



RCA Knowledge Library

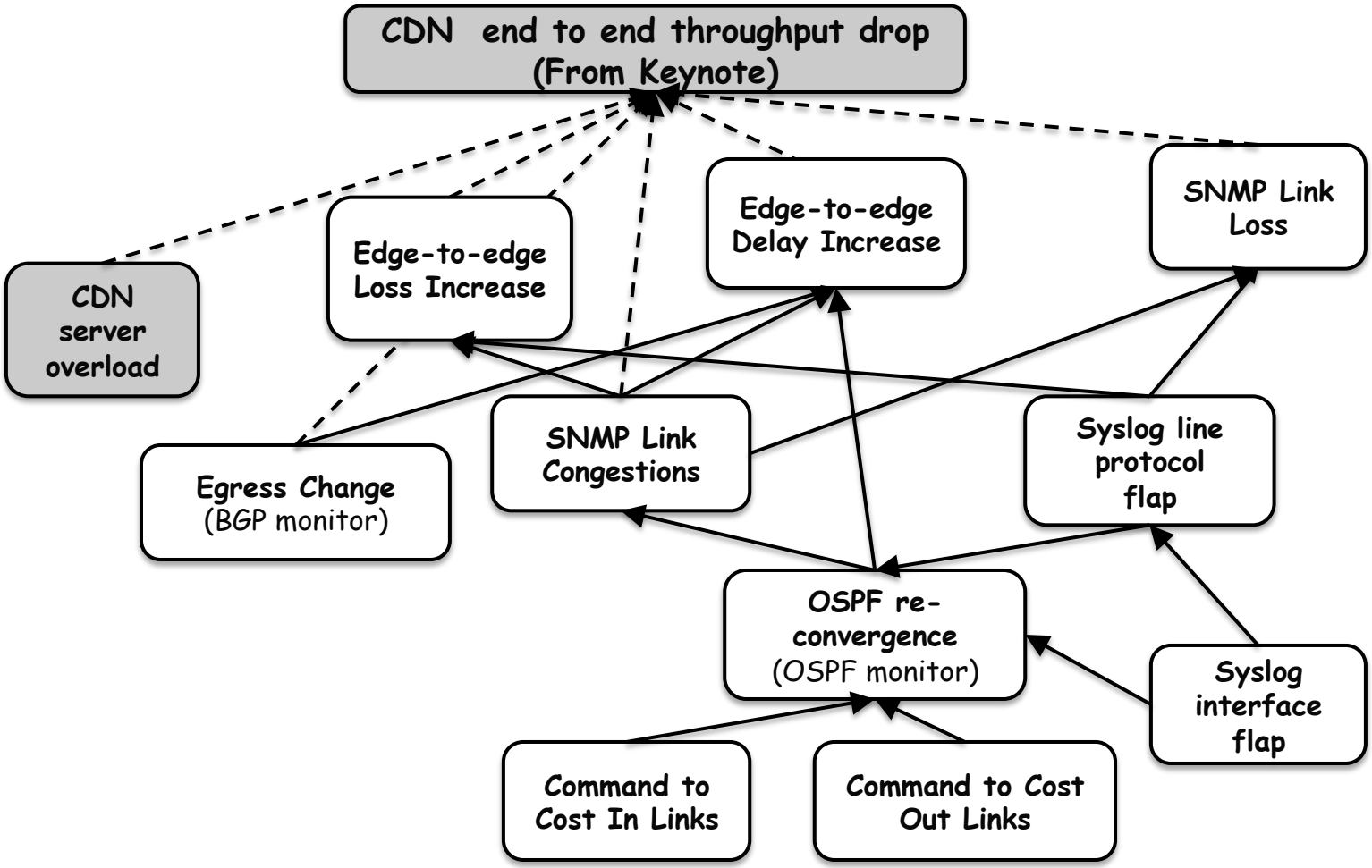
- Event
  - a signature that captures a particular type of network condition.
    - e.g.: Interface flap or router reboot
  - event definition consists of event name, location type and retrieval process
    - e.g.: (link-congestion, interface, my query)
  - event instance consists of event-name, event start-time, event end-time and event location
    - e.g.: link-congestion, 2010-01-01 12:30:00, 2010-01-01 12:35:00, newyork-router1:serial-interface0
  - G-RCA pre-defines and implements a wide range of commonly used events.
    - Help network operators quickly instantiate new RCA application for new service,

RCA Knowledge Library

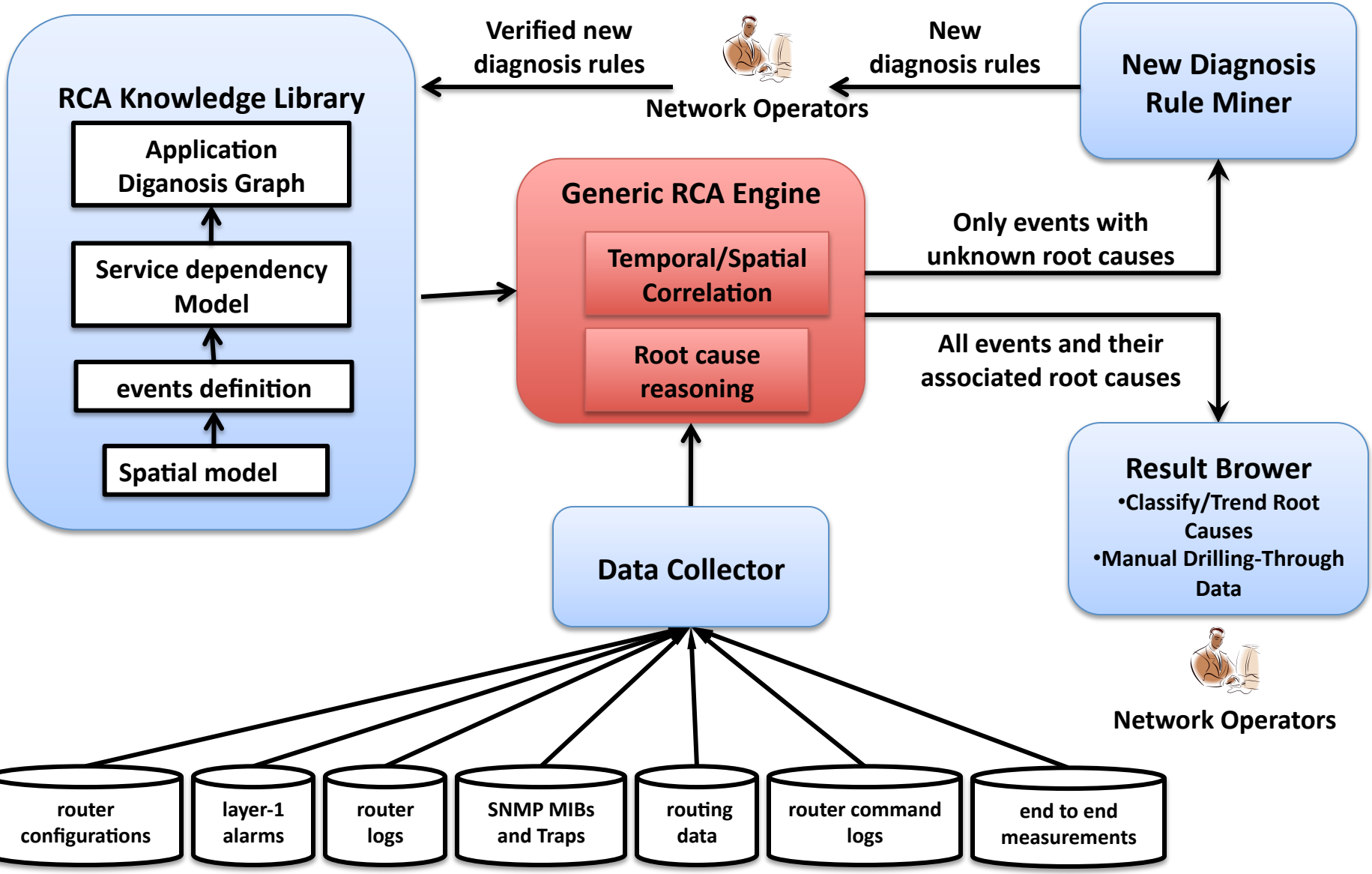
- Service Dependency Model
  - Built on top of event definitions and spatial model
  - Consists of diagnosis rules
    - Symptom and diagnostic events are picked from event definitions
    - e.g.: interface flap -> line protocol flap
  - G-RCA pre-defines the common used diagnosis rules.
  - Application specific rules can be added

RCA Knowledge Library

- Application Diagnosis Graph



G-RCA Design

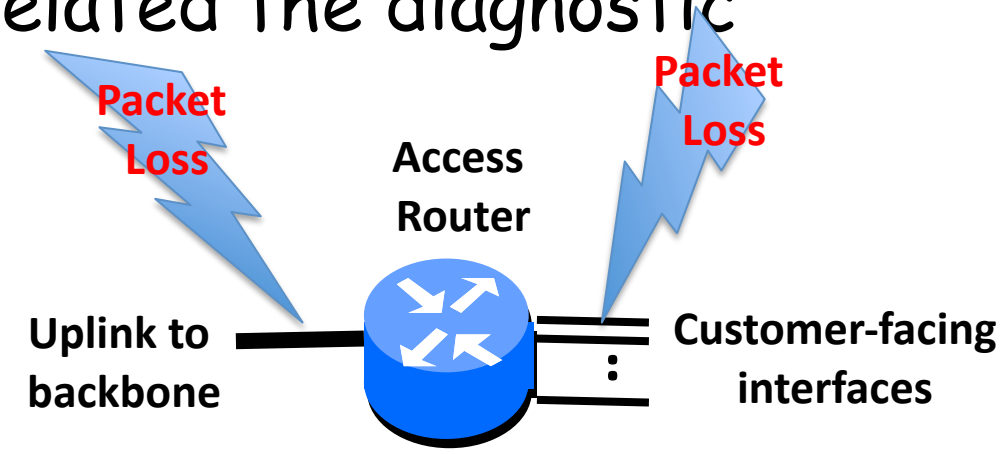

RCA Knowledge Library
Application Diganosis Graph
Service dependency Model
events definition
Spatial model
Verified new diagnosis rules
Network Operators
New diagnosis rules
New Diagnosis Rule Miner
Generic RCA Engine
Temporal/Spatial Correlation
Root cause reasoning
Only events with unknown root causes
All events and their associated root causes
Result Brower
•Classify/Trend Root Causes
•Manual Drilling-Through Data
Network Operators
Data Collector
router configurations
layer-1 alarms
router logs
SNMP MIBs and Traps
routing data
router command logs
end to end measurements

Generic RCA Engine

- Temporal Correlation Module
  - Given a symptom event instance, find out the temporally correlated the diagnostic event instances
  - Imperfect timing information
    - cause and effect rarely follows each other (protocol timers)
    - inaccuracy/uncertainty in the timing of network measurements.
  - Padding time-margins to both symptom and diagnostic event instances.

Generic RCA Engine

- Spatial Correlation Module
  - Given a symptom event instance, find out the spatially correlated the diagnostic event instances
  - Indirect mapping

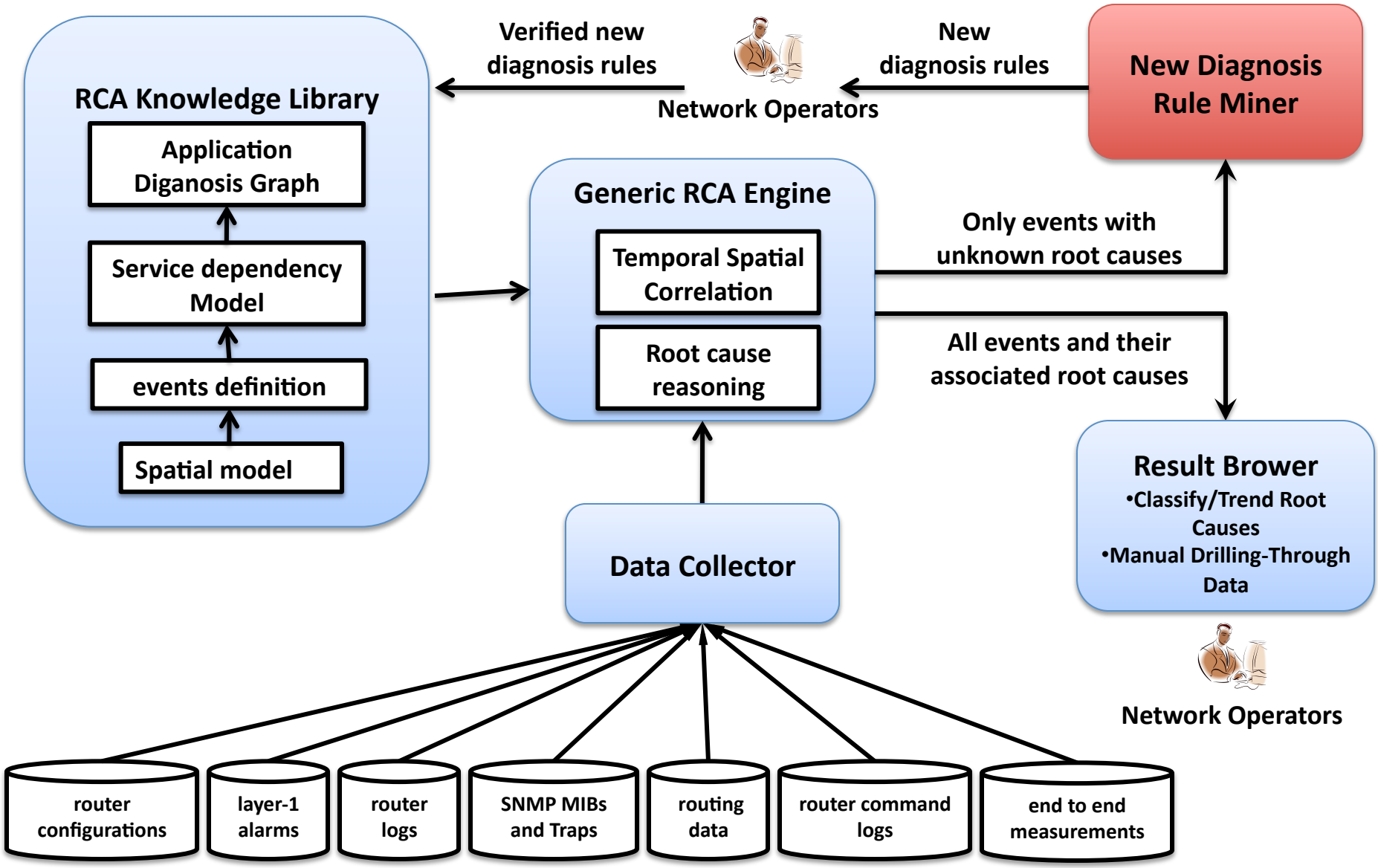


  - Joining location type.
    - In the example, "Router" is the joining location typ.

Generic RCA Engine

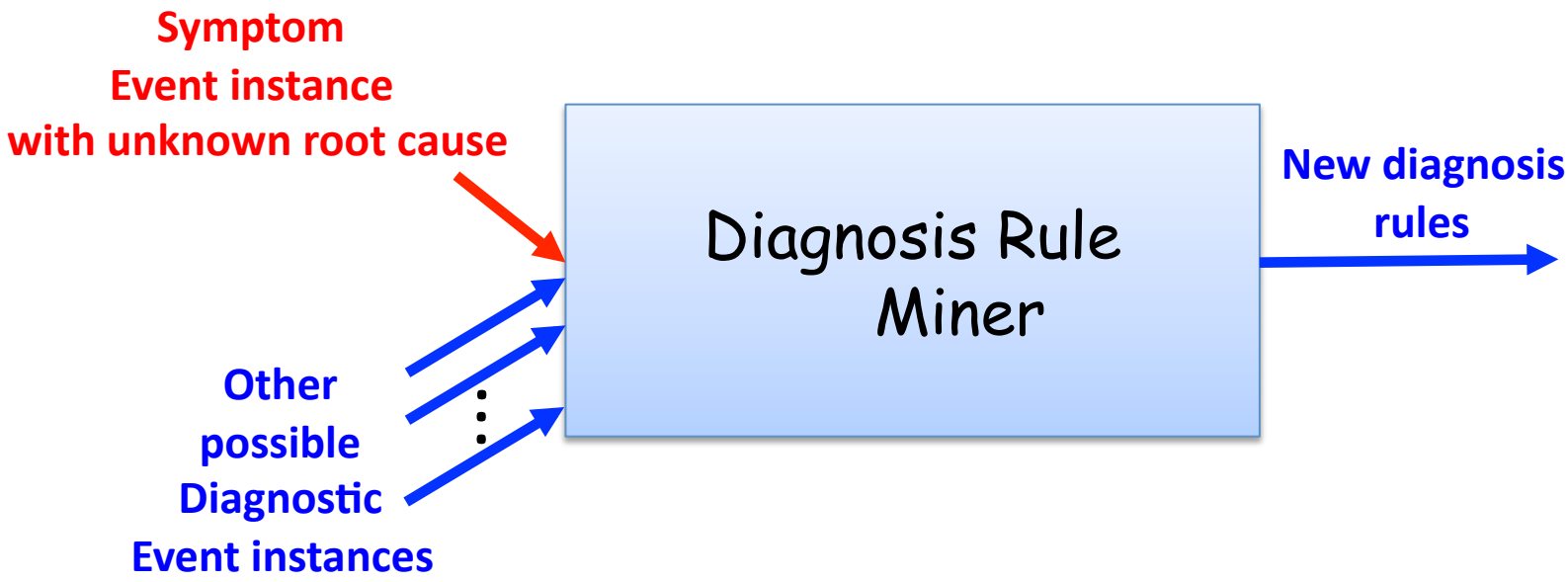
- Root Cause Reasoning Module
  - determine the root cause of a symptom event instance based on temporally and spatially correlated diagnostic event instances.
  - rule-based decision-tree-like reasoning
    - associate a priority value for each edge in the diagnosis graph
    - The higher the priority value, the more likely the diagnostic event to be the real root cause

G-RCA Design


Verified new diagnosis rules
New diagnosis rules
New Diagnosis Rule Miner
Network Operators
RCA Knowledge Library
Application Diganosis Graph
Service dependency Model
events definition
Spatial model
Generic RCA Engine
Temporal Spatial Correlation
Root cause reasoning
Only events with unknown root causes
All events and their associated root causes
Result Brower
•Classify/Trend Root Causes
•Manual Drilling-Through Data
Data Collector
Network Operators
router configurations
layer-1 alarms
router logs
SNMP MIBs and Traps
routing data
router command logs
end to end measurements

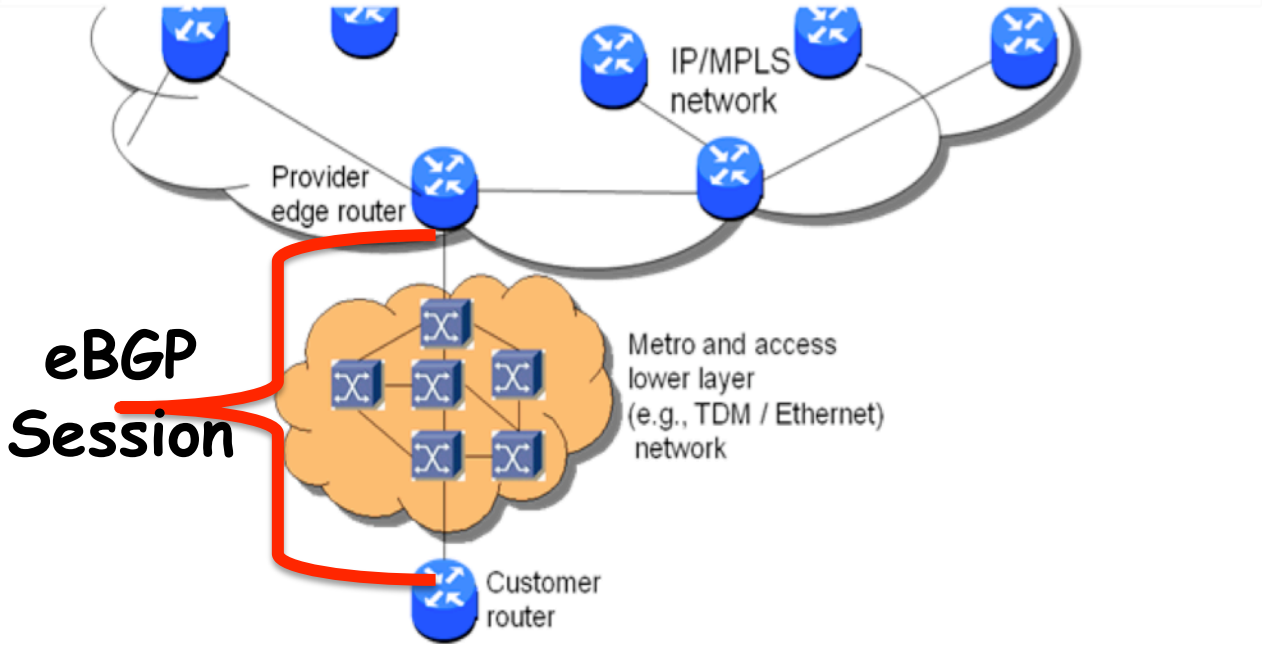
New Diagnosis Rule Miner

- Pair-wise statistical Correlation test[19]
  - Symptom event instances with unknown root cause
  - Other possible diagnostic event instances



Case Example 1
BGP flaps root cause analysis

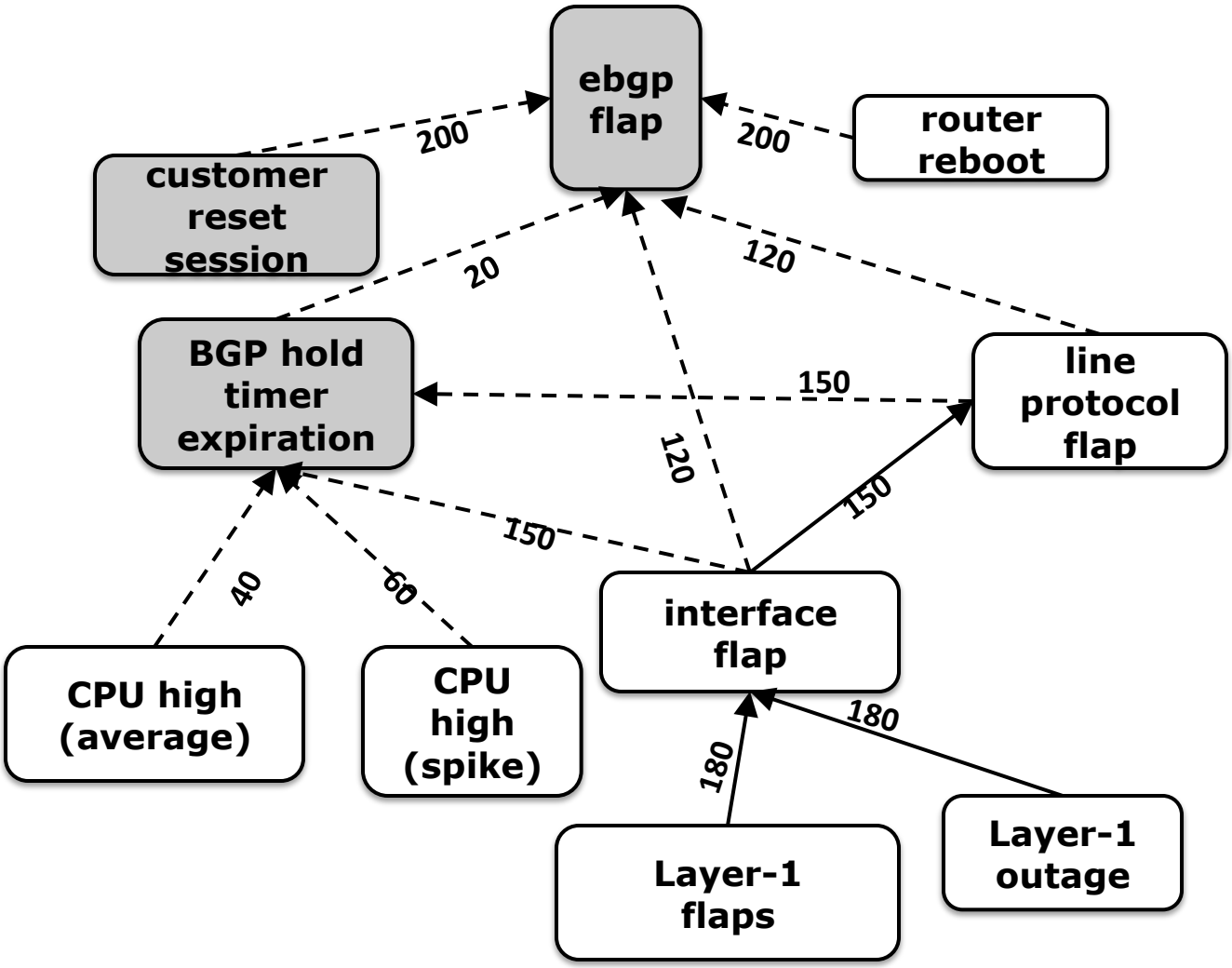
- minimize the number of eBGP session flaps
- a challenging problem across the trust domain



Case Example 1

BGP flaps root cause analysis

- Application Diagnosis Graph



Case Example 1
BGP flaps root cause analysis

- Operational Experience
  - 5 provider edge routers in different locations
  - each has several hundred eBGP sessions established with customer routers

Root Cause	Percentage (%)
router reboot	0.047
customer reset session	0.088
CPU high	0.886
CPU rising (high)	15.32
CPU rising (medium)	4.318
interface flap	29.004
line protocol flap	15.72
eBGP HTE(due to unknow reasons)	18.381
Short Layer-1 Flaps	0.205
Longer Layer-1 Outage	0.428
unknown	15.603

Case Example 2
PIM Adjacency Change in Multicast VPN

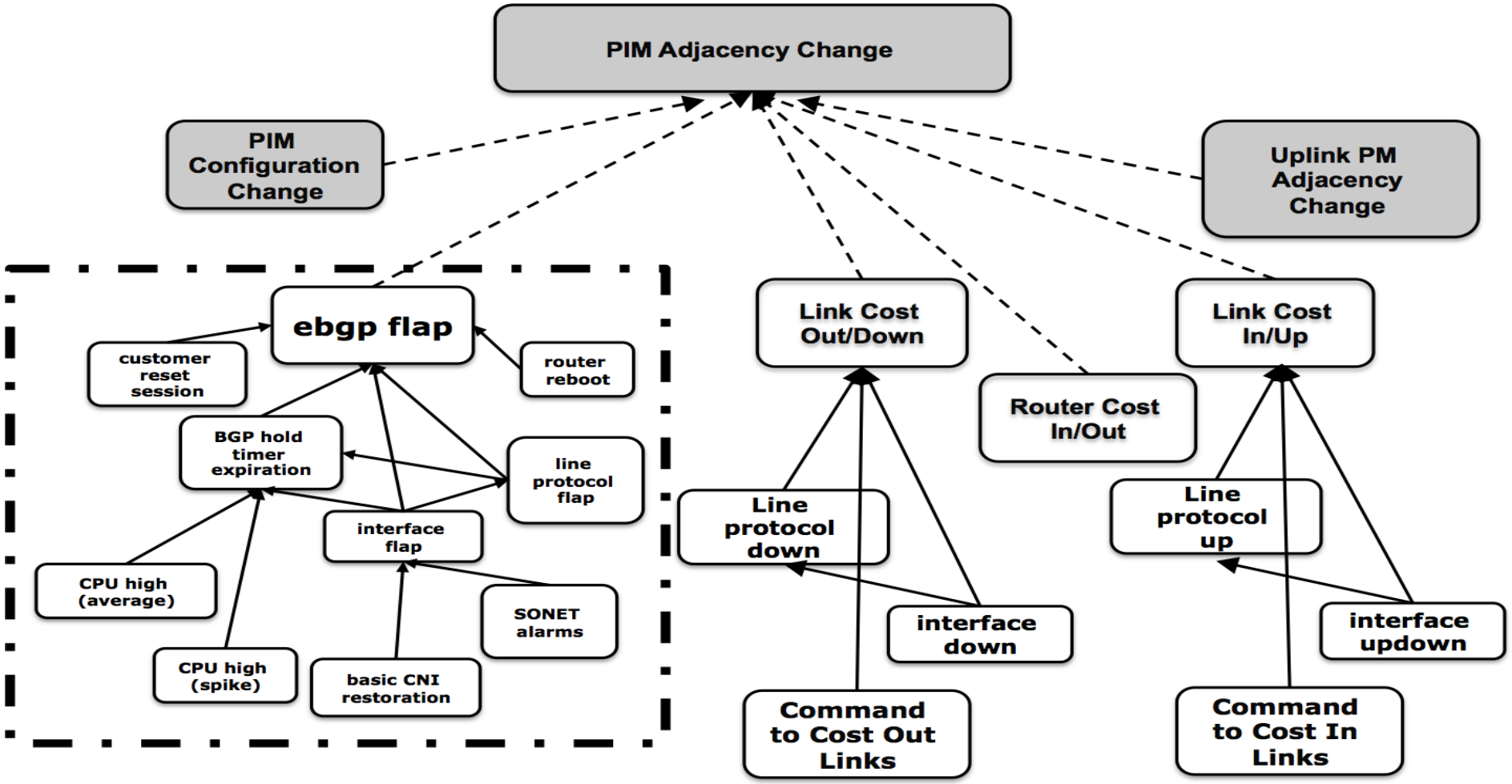
- For each MVPN customer, all PERs at which the customer attaches to the provider network maintain PIM Neighbor adjacencies with each other

- The loss of PIM neighbor adjacencies
  - a good indicator of service related problems.
  - reported via syslog
  - thousands per day

Case Example 2

PIM Adjacency Change in Multicast VPN

- Application Diagnosis Graph



Case Example 2
PIM Adjacency Change in Multicast VPN

- Operational Experience
  - Running the G-RCA PIM application daily
    - Takes about 1-2 hours.
    - For each day, the root causes for between 60% and 95% PIM adj-changes are identified.
  - Help operators filter out the events that has no service impact
    - Caused by link flaps between the customer and provider routers
    - Caused by customer disconnects on the PE router
  - Found an unexpected root-cause
    - OSPF routing changes
    - software bugs in router

Conclusion

- Root cause analysis is critical for service quality management in large IP networks
- G-RCA: First generic, automated and scalable root cause analysis platform for SQM in large IP networks
- Operational experience is very positive
  - Becoming a powerful tool inside AT&T
- Future Work
  - simplify its configuration to further improve its usability.
  - extend the G-RCA platform into other networks and services such as cellular data network and IPTV network.

Thank You !