A Demonstration of Crosswork Network Insights

A Cloud Based Subscription Service for Network Routing Analytics

Martin Thygesen
Product Manager
Jan 2019
Cloud Based Network Route Analytics

**Operator Constraints**

- Too Many Routers, Peering Locations
- Fragmented View of the Internet
- Lack of Central Visibility for Troubleshooting
- Peering Data Lacks Real-Time Agility

**What's Needed**

- A Global Shared Information Service
- Unified View for Route Analysis
- Route Event Visibility Past, Present, and Trending
- Real Time Data Collection at Internet Scale

Network Providers adopting new approaches
Mean-Time-To-Repair is one of the main KPIs impacting customer experience

Our Goal: Minimizing & Prevent Downtime
Real Time Visibility - Automated Remediation - Automated Validation

Automated Remediation
+ Real-time Analytics
+ Streaming Telemetry

MTTR After

Cisco Network Insight’s Focus
What is Network Route Analytics as a Service?

A Cloud Service platform provides network operators insightful real-time and historical BGP routing data analytics to significantly reduce the mean time to repair.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Problem
Routing Errors are impacting the operation of the Networks, Time to Identification and Resolution is very poor

The Resolution
Aggregate Global & Local Routing Prefix information in a cloud service to quickly identify the source of anomalies based on a consensus view of the Routing Databases (internal & external)

Cisco Network Insights Architecture

Collection Interfaces

- Public Data Collector
  - Public (RouteViews, RIPE, APNIC)
  - Internet Exchange Route Servers
  - Cisco Public Peering
  - Map & Geo Data Lookup Services

- Traditional BGP/BMP Connections
  - BGP or BMP Direct from your network to Network Insights service

- Data Connector Node
  - OpenBMP Collector
  - BGP/BMP Feeds
  - Telemetry & Flow future

Services Bus Interface

- Web
- Mobile
- Social
- API
- Third Party

Cisco Network Insights

- Route Data Stores
- Analytics
- Alarms
- Event Monitoring
- Security & Identity

© 2018 Cisco and/or its affiliates. All rights reserved to Cisco Partner Confidential
Cisco Network Insights
A Cloud Network Routing Analytics Platform

Why Cloud?
Why can’t I run this myself?

Route Data Stores
350+ Million Entities

BMP
BGP

BMP
BGP
BGP-LS

500+
Internet Route
Feeds & Growing

On Premise
Peer Feeds

SPEED
SCALE
COST

© 2018 Cisco and/or its affiliates. All rights reserved to Cisco Partner Confidential
## Cisco Network Insights

*A Cloud Network Routing Analytics Platform*

<table>
<thead>
<tr>
<th>Capability</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intellectual Property</strong></td>
<td>We have the in house knowledge and experience to maintain and drive change in the industry in both Hardware and Software areas. We build and maintain BGP stacks for routers, every day.</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Traditional BGP collection tools do not report events for up to 5-15 minutes in most cases. We collect and alert on Routing events within seconds. We leverage our own dedicated Collection Notes for near real time Route Update detection.</td>
</tr>
<tr>
<td><strong>Scale</strong></td>
<td>Our platform aggregates 2 months of routing event data from Internal and External route sources. We can Alert and Report on this in seconds. We are currently store and process 350+ million unique IP entities and their history. We have plans to increase this significantly.</td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td>We work with other multivendor Cisco Product teams to enable simple integration and API features that reduce the cost of implementing smart automation. Cisco Crossworks integrations can provide a complete automation solution.</td>
</tr>
<tr>
<td><strong>Knowledge and Experience</strong></td>
<td>Unlike other software vendors our multidisciplinary team works towards ensuring our product is easy to adopt and use regardless of your network hardware and software architecture.</td>
</tr>
</tbody>
</table>
## Crosswork Network Insights

### What are our External Route Use Cases?

<table>
<thead>
<tr>
<th>External Route Use Cases (Internet Features)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Hi-Jack</td>
<td>Customisable Route Hi-Jack Alerting</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>ASN Hi-Jack</td>
<td>Customisable ASN Hi-Jack Alerting</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Route Leak – Malicious, External</td>
<td>Customisable Route Leak Alerting from others</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Route Leak – Accidental, Self</td>
<td>Customisable Route Leak Alerting from self</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Forensic Time Series Route Analysis</td>
<td>2 month review of full BGP attributes for fault analysis</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Peering Device Visibility</td>
<td>Monitor Specific Internet Peering Router Operation</td>
<td>ETA Q2 2019</td>
</tr>
<tr>
<td>Man in the Middle Path Hi-Jack</td>
<td>Consensus BGP ASN neighbour checking and Alerting</td>
<td>ETA Q2 2019</td>
</tr>
<tr>
<td>Route Looking Glass</td>
<td>Query a Route on any collector device</td>
<td>ETA Q2 2019</td>
</tr>
<tr>
<td>Route Presence &amp; Absence Check</td>
<td>Query all my Peering Routers for a Prefix Presence or Absence</td>
<td>ETA Q2 2019</td>
</tr>
<tr>
<td><strong>Roadmap: Peering Prospect Analysis</strong></td>
<td>Recommend new direct Peers</td>
<td>ETA Q4 2019</td>
</tr>
<tr>
<td><strong>Roadmap: Internet Peering Automation</strong></td>
<td>Recommend Ingress/Egress Route changes based on policy</td>
<td>ETA Q4 2019</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved to Cisco Partner Confidential
Crosswork Network Insights

What are Policies and Alarms and how they relate to our BGP Use cases?

Prefixes

A.B.D.C/24
A.B.D.E/24
A.B.D.F/24
A.B.D.G/24
A.B.D.H/24

Policy Container

Alarm 1
Alarm 2
Alarm 3

Input Tag Matching

Output Tag Matching

Notifications End Points

SMS
Email
Syslog via S3
Situation Manager
Streaming API

Customised Event Detection Workflow Reduces Noise
Use Case Example:

Route Hijacks can be performed in many ways. Some are malicious, some are accidental.

Our layered BGP Policy Alarm Architecture lets you customize monitoring criteria to match your peering Architecture.

Our Alarm Conditions test for any of the following conditions:

- ASN Origin Violation
- Unexpected Longer Prefix Match
- ROA/RPKI Failure/Miss-match
- AS Path Length Violation
- Man in the Middle Detection
Recent BGP Hijack examples of interest


https://www.theregister.co.uk/2018/11/13/google_russia_routing/


https://scholarcommons.usf.edu/mca/vol3/iss1/7/
Use Case Example:

Route Leaks can be performed in many ways. Some are accidental, some are complex logical issues.

Layered BGP Policy Alarm Architecture lets you customize monitoring criteria to match your peering architecture intent.

Policies can be enabled and disabled as part of a planned change workflow to reduce event noise.

Our Alarm Conditions test for any of the following conditions that can be symptoms of a Route Leak:

- Upstream AS Change (whitelist / blacklist)
- ASN Origin Violation
- Prefix Aggregate Change
- Unexpected Longer Prefix Match
- AS Path Length Violation (too short / too long)
- Peer Router Prefix Violation (whitelist / blacklist)

© 2018 Cisco and/or its affiliates. All rights reserved to Cisco Partner Confidential
Recent BGP Hijack examples of interest


https://dyn.com/blog/widespread-impact-caused-by-level-3-bgp-route-leak/


https://arstechnica.com/information-technology/2015/03/indian-isps-routing-hiccup-briefly-takes-google-down-worldwide/
Use Case Example:
Is my Google CDN Route 100% Redundant before I upgrade routers on my Peering edge nodes?

**Option 1**
**Query x 100 edge routers with show commands**
```
Router# show ip bgp 8.8.8.0/24.
BGP routing table entry for 8.8.8.0/24, version 19
Paths:(5 available, best #5)
  Multipath:eBGP
Advertised to non peer-group peers:
  10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
  22
  10.0.0.2 (metric 20) from 10.0.0.4 (10.0.0.4)
  Origin IGP, metric 0, localpref 100, valid, internal, multipath
  Extended Community:0x0:0:0 RT:100:1 0x0:0:0
  Originator:10.0.0.2, Cluster list:10.0.0.4
  22
  10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
  Origin IGP, metric 0, localpref 100, valid, internal, multipath
  Extended Community:0x0:0:0 RT:100:1 0x0:0:0
  Originator:10.0.0.2, Cluster list:10.0.0.5
```

**Option 2**
**API Query**
```
<get GLOBAL-RIB-CHECK 8.8.8.0/24>
Response
<ANSWER 100%>
  OK GO, RUN CHANGE

<ANSWER 95%, but check R1, R3, R4>
  MAYBE, but run 3 show commands

<ANSWER 90%, check R20-40>
  STOP! change
```

**NUMEROUS BENEFITS**
- HIGHER CPU ON ROUTERS
- COMPLEX TO QUERY MULTIPLE ROUTES
- TOTAL DURATION LONG ~ 10 min
- LATENCY LONG ~ 1 min per router
- DATA IS NOT REUSABLE
Cisco Network Insights
A Cloud Network Routing Analytics Platform

Timelines

2018

Q4 CY2018 (Completed)
• Service Operational in Cloud
• External Routing and Peering Analytics
• Purchasing via Cisco Commerce Workspace
• Start Customer Trials ‘Dec 20’

2019

Q1CY19 (Underway)
• SAML/OATH Federated ID
• Alarm Feature Parity
• Historical Data Query
• Integration with Situation Manager
• User Interface Enhancements
• General Availability ‘Jan 30’

Q3CY19 (Working Towards)
• New features and Roadmap Development
Contact Us!
cni-plm@cisco.com
A word on BGPMon to Cisco Network Insights

- There is no reuse of the BGPMon Application
- This is a complete re-write from the ground up
- There is no reuse of existing contributions for OBMP or SNAS.io
- A basic prefix migration feature will be provided for paying BGPMon customers, however basic ASN prefix import and learning may be a quicker path.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Home Dashboard

Our landing page is designed to give network operators a high level view of the health of their IP Prefix Assets
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Prefixes Dashboard

Our Prefixes Dashboard provides the operator with the ability to sort and locate IP Prefixes that are monitored. From here an user can quickly see trends affecting one or more prefixes.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Prefix Details Page

Our Prefix Details page provides the operator with a view of the Prefix and its history. The user can quickly see the state of the alarms observed. They can adjust the time window to focus on proximity events and visualize impacted locations.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Alarm Summary Page

Our Alarm Summary page provides clearly displays the various Alarm types and their state. The operator can sort and order Alarm types based on various criteria and time series. Once an alarm of interest has been located it can be investigated in more detail.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The Alarm Details Page

Our Alarm Details page provides the operator with a view of the impact and origin of the alarm type. The user can quickly see the locations where the alarm was observed as well as the origin details of the Prefix in Alarm.
Cisco Network Insights
A Cloud Network Routing Analytics Platform

The ASN Summary Page

Our ASN Summary page clearly displays the various ASN the operator is subscribed to. The user can sort and order the ASN list based on various criteria.
The ASN Details Page

Our ASN Details Page provides a clear understanding of an ASN and its IP Prefixes. A user can quickly see the ASN and its globally observed neighbor relationships.