Leveraging Routing Analytics to Enable Intent-based Automation
Today’s Presenters

John Malzahn
Senior Manager,
Service Provider
Solutions Marketing
Cisco

Martin Thygesen
Product Manager,
Service Provider
Network Automation
and Analytics
Cisco
Crosswork Network Insights
Cisco Knowledge Network

Martin Thygesen
Product Manager
2020-01-28
Agenda list

1. Network Insights Refresh
2. What’s Changed
3. What’s Coming
4. Find out more
Crosswork
Network Insights
Refresh

https://crosswork.cisco.com
BGP on the Internet

Problem Statement

• On the public Internet, route distribution occurs by learning routes from a neighbor and advertising to other neighbors. Routes beyond the first hop are learned by trusting advertisements of neighbors.
BGP on the Internet

• Historically it has been trust based – we advertise our prefixes and expect everyone to do same.

• If we catch some one advertising wrong prefixes, we tell them not to.
  • If it was a mistake they would comply.

• If they do not stop advertising wrong prefixes, we call their upstream providers and tell them to not accept/filter out.
Problem: Routing Infrastructure is vulnerable to hijacks and errors

Google outage November 13, 2018

"FOR TWO HOURS Monday, internet traffic that was supposed to route through Google's Cloud Platform instead found itself in quite unexpected places, including Russia and China...

Indeed, on Tuesday morning Main One said in a statement that, "This was an error during a planned network upgrade due to a misconfiguration on our BGP filters. The error was corrected within 74mins."  
https://www.wired.com/story/google-internet-traffic-china-russia-rerouted/

Nationwide Comcast Outage: Nov. 6, 2017

"The culprit was a configuration issue from Level 3, a telecommunications and internet service provider owned by CenturyLink. In a statement to CNN Tech, CenturyLink said a "configuration error" disrupted service and technicians restored service in 90 minutes."

*Source: CNN

Google causes outage in Japan: Aug. 26, 2017

"Yesterday some Internet users would have seen issues with their Internet connectivity, experiencing slowness or parts of the Internet as unreachable. This incident hit users in Japan particularly hard and it caused the Internal Affairs and Communications Ministry of Japan to start an investigation into what caused the large-scale internet disruption that slowed or blocked access to websites and online services for dozens of Japanese companies."

*Source: BGPMON Blog

Amazon Route 53 Outage: April. 24, 2018

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

*Source: Ars Technica
Is this important?

Arbor Networks
2013 Customer Survey

What are your most concerning threats?

“BGP Route Leaks and Hijacks”

#3

Over and above DDoS!

Figure 4: Most Concerning Threats
Source: Arbor Networks, Inc.
Our Goal: Minimizing & Preventing Downtime
Real Time Visibility - Automated Remediation - Automated Validation

Mean-Time-To-Repair (MTTR) – Key KPI impacting customer experience

Crosswork Network Insight’s Focus
What’s happening to BGPmon?

Previously Published
EOL March 1 2020

Complete Rebuild from
Ground up ++ Much More!

Cisco Crosswork Network Insights

FCS February 1 2019

How do we link Route Awareness to Network Automation?
Crosswork Network Automation

**Situation Manager**
connect events from multiple sources together and provide root cause analysis, collaborate on events for resolution.

**Health Insights**
learn and measure health of network elements.

**Change Automation**
safely execute operational tasks with structured workflows.

**SON**
intent based automation for RAN

**Optimization Engine**
optimize network paths to improve utilization & efficiency (SR-PCE)

**Data Gateway (Collection)**
On-premise single point data collection
Reduce Strain and Improve Scale

**Network Services Orchestrator**
mass scale intent-based configuration across multi-vendor

**Trust Insights**
track integrity of infrastructure

**new**
analyze and identify the source of routing anomalies

**collection of data from Data Gateway**

**Converged SDN Transport**

**Converged SDN Transport**

**Health Insights**
learn and measure health of network elements.

**Network Services Orchestrator**
mass scale intent-based configuration across multi-vendor

**Change Automation**
safely execute operational tasks with structured workflows.

**SON**
intent based automation for RAN

**Optimization Engine**
optimize network paths to improve utilization & efficiency (SR-PCE)

**Data Gateway (Collection)**
On-premise single point data collection
Reduce Strain and Improve Scale

**Network Services Orchestrator**
mass scale intent-based configuration across multi-vendor

**Trust Insights**
track integrity of infrastructure

**new**
analyze and identify the source of routing anomalies

**collection of data from Data Gateway**

**Converged SDN Transport**

**Health Insights**
learn and measure health of network elements.

**Network Services Orchestrator**
mass scale intent-based configuration across multi-vendor

**Change Automation**
safely execute operational tasks with structured workflows.

**SON**
intent based automation for RAN

**Optimization Engine**
optimize network paths to improve utilization & efficiency (SR-PCE)

**Data Gateway (Collection)**
On-premise single point data collection
Reduce Strain and Improve Scale

**Network Services Orchestrator**
mass scale intent-based configuration across multi-vendor

**Trust Insights**
track integrity of infrastructure

**new**
analyze and identify the source of routing anomalies

**collection of data from Data Gateway**

**Converged SDN Transport**
Crosswork Network Insights
Why and Who is this important to?

<table>
<thead>
<tr>
<th>Why?</th>
<th>BGPmon -&gt; Crosswork Network Insights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Subscribers Migrating</td>
<td>16000</td>
</tr>
<tr>
<td>Paid Subscribers</td>
<td>240+</td>
</tr>
</tbody>
</table>

**Scale**

<table>
<thead>
<tr>
<th>Route Updates</th>
<th>+350 million BGP updates per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Routing Sources</td>
<td>~600 Active Route Tables</td>
</tr>
<tr>
<td>Community Contributions</td>
<td>Bgpstream, BGPevents Twitter</td>
</tr>
</tbody>
</table>
Crosswork Network Insights Offers
Proof of Value Model

• What is it?
   It monitors BGP Events

• Who is it for?
   Anyone who manages BGP Peering

• How do I use it?
   SaaS, external notification service

• What are the variables?
   Price per Prefix Monitored

• How to show value?
   Use the POV spreadsheet CCNI POV

Proof of Value

<table>
<thead>
<tr>
<th>Service Provider Annual Return on Investment</th>
<th>Company X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ofcom subscriber refund per day for loss of service*</td>
<td>£ 8.00</td>
</tr>
<tr>
<td>GBP/USD exchange rate</td>
<td>1.28</td>
</tr>
<tr>
<td>USD subscriber refund per day for loss of service</td>
<td>$ 10.24</td>
</tr>
<tr>
<td>Subscriber refund cost per minute of internet outage</td>
<td>$ 0.0071</td>
</tr>
<tr>
<td>Total subscribers</td>
<td>155,700,000</td>
</tr>
<tr>
<td>Autonomous system numbers (&quot;ASNs&quot;) owned by account</td>
<td>3</td>
</tr>
<tr>
<td>Probability of internet peering outage**</td>
<td>6.575%</td>
</tr>
<tr>
<td>Expected customers impacted</td>
<td>10,237,808</td>
</tr>
<tr>
<td>Customer care call rate</td>
<td>10%</td>
</tr>
<tr>
<td>Expected customer care calls</td>
<td>1,023,781</td>
</tr>
<tr>
<td>Average cost per customer care call</td>
<td>$ 15.00</td>
</tr>
<tr>
<td>Expected annual care call cost</td>
<td>$ 15,356,712</td>
</tr>
<tr>
<td>Average internet outage duration (minutes)**</td>
<td>2,218</td>
</tr>
<tr>
<td>Bill credit rate</td>
<td>80%</td>
</tr>
<tr>
<td>Expected annual bill credit cost</td>
<td>$ 12,918,021</td>
</tr>
<tr>
<td>Total expected outage cost</td>
<td>$ 28,274,733</td>
</tr>
<tr>
<td>Automated improvement to resolve internet outage</td>
<td>50%</td>
</tr>
<tr>
<td>Expected financial benefit</td>
<td>$ 14,137,367</td>
</tr>
<tr>
<td>Crosswork Network Insights Essentials list price per prefix</td>
<td>$ 135.00</td>
</tr>
<tr>
<td>Prefixes</td>
<td>5,001</td>
</tr>
<tr>
<td>Crosswork Network Insights Essentials total price</td>
<td>$ 675,135</td>
</tr>
<tr>
<td>Crosswork Health Insights price</td>
<td></td>
</tr>
<tr>
<td>Crosswork Situation Manager price</td>
<td>$ 750,000</td>
</tr>
<tr>
<td>Crosswork Change Automation price</td>
<td>$ 350,000</td>
</tr>
<tr>
<td>Total Intelligent Peering solution price</td>
<td>$ 1,775,135</td>
</tr>
</tbody>
</table>

Return on Investment | 696%
Which Routes do I need to monitor?

Problem
Routing Events impact how traffic comes to my network but also how traffic leaves my network, how do I quickly identify when my critical routing services are not available?

Resolution
Monitor critical internal and external routes that are key to your business success.

- DNS & CA Root Servers
- Cloud Services
  - Azure, GCP, AWS
- Message Services
- Financial Services
- B2B Services
- My Routes
- My Routers
- Applications & Systems that are key to Operational Continuity
What are some of the Routing Analytics use cases?

**Automation Focus**
- Route Node Redundancy
- Route Pre/Post Change Check
- Route Multi-Path Redundancy

**Security Focus**
- Route Leak Detection
- Route Hijack Detection
- Route Attribute Compliance

**Forensic Historical Analysis**

**Global Looking Glass**

**Less Secondary Review**

**More Secondary Review**
# Crosswork Network Insights

## What are our External Route Use Cases?

<table>
<thead>
<tr>
<th>External Route Analysis Use Cases (Internet Features)</th>
<th>Description</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic Time Series Route Analysis</td>
<td>3 month review of full BGP attributes for fault analysis</td>
<td>Shipping</td>
</tr>
<tr>
<td>Route Looking Glass</td>
<td>Query a Route’s BGP state on all collectors in a single interface</td>
<td>Shipping</td>
</tr>
<tr>
<td>Route Hi-Jack</td>
<td>Customisable Route Hi-Jack Alerting</td>
<td>Shipping</td>
</tr>
<tr>
<td>ASN Hi-Jack</td>
<td>Customisable ASN Hi-Jack Alerting</td>
<td>Shipping</td>
</tr>
<tr>
<td>Route Leak – Malicious, External</td>
<td>Customisable Route Leak Alerting from others</td>
<td>Shipping</td>
</tr>
<tr>
<td>Route Leak – Accidental, Self</td>
<td>Customisable Route Leak Alerting from self</td>
<td>Shipping</td>
</tr>
<tr>
<td>Automation API’s</td>
<td>Configure, Get Alarms and State or all Monitored Routes</td>
<td>Shipping</td>
</tr>
<tr>
<td>Path Hi-Jack Detection</td>
<td>Consensus BGP ASN neighbour checking and Alerting</td>
<td>Shipping</td>
</tr>
<tr>
<td>Peering Device Visibility</td>
<td>Monitor Specific Internet Peering Router Operation</td>
<td>ETA CYQ2 2020</td>
</tr>
<tr>
<td>Peering Device Specific Alarms</td>
<td>Customisable Route Alerting specific to my edge routers</td>
<td>ETA CYQ2 2020</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 CYQ2 2020</td>
</tr>
<tr>
<td>DDoS Tools Integration</td>
<td>Integration with Radware DDoS and Stealthwatch bundle</td>
<td>Roadmapped</td>
</tr>
</tbody>
</table>

Timelines are not committed and subject to change.
Why Crosswork Network Insights?

Why is a BGP Routing SaaS Service important?
Questions to consider:
• Is the Service Independent from my infrastructure?
• Is it Remote, can it tell me if my infrastructure is down?
• What happens when my onsite Routers fail?
• Is the Route Data commercially reusable outside of research usage?
• Can you monitor the Route Data source is operational?
• Do you understand the TCO of a Route Data Service?
## Supported Alarm Types – Jan 2020

<table>
<thead>
<tr>
<th>Alarm Type</th>
<th>Supported</th>
<th>Configured Prefixes</th>
<th>Unconfigured Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Origin Violation</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SubPrefix Advertisement</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Prefix Withdrawal (normally advertised)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ROA Failure</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Upstream AS Change</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Parent Aggregate Change</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Unexpected AS Prefix</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>AS Path Length Violation</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Prefix Advertisement (normally not advertised)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Valid AS Path Violation (AS path REGEX)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>New Global Peer Edge (replaces Man in the Middle)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Supported Notification Endpoints

- Email
- SMS
- Syslog NG via Amazon S3
- Slack
- WebEx Teams
Example: Email & WebEx Teams Notification

You are subscribed to crosswork.cisco.com
Alarm count is 1 starting at 2019-08-14 10:53:44.846100335 +0000 UTC for Cisco Sales organization. Please see each alarm details below:

Express_4657_1
Alert Details: https://crosswork.cisco.com/#/alarm/ad248f4c-6558-4762-ba6f-733b828926
Prefix Withdrawal for PREFIX 263.116.0.8/16
Priority: High Condition: Active State: ACTIVE
Last Activated: 2019-08-14 10:53:44.841109856 +0000 UTC
Last Deactivated: 
Activate Peer Threshold Reporting Peers Co

notificationEndpoints for CCNI-TestingOnly-

Today

notificationEndpointsTesting 04:20
You are subscribed to crosswork.cisco.com.
Alarm count is 1 starting at 2019-08-20 20:15:16.745578544 +0000 UTC for Delos incorporated organization. Please see each alarm details below:


To change your notification settings, please login to https://crosswork.cisco.com.
REST API Access

• Automate monitored prefixes and ASNs using REST API
  • Enables onboarding of prefixes/ASNs – for ex bring your own IP

• Automate and integrate alarms info with other tools
  • Enables single plane of glass applications to get visibility
  • Enables Auto Remediation tools to be run when routing incidents are detected by Network Insights.

• Automate administrative items – add/delete users and policy configurations, end points etc.

https://crosswork.cisco.com/apiDoc/CiscoCrossworkCloudAPI
Support & Feedback
Menu > Help & Support > Submit Product Feedback

Submit Feedback and support issues directly from the Application

- Feature Requests
- Sales Support (Trials & Free)
- Other Issues (How To / How Come?)

Submit Product Feedback
We'd like to hear what you think. Please complete the form below and we'll get back to you as quickly as possible.

- Feature Request
- Sales Support
- Other Issue

Description

[Submit] [Cancel]
What’s Changed?
Crosswork Network Insights

Feature Changes – We are a little different, as a SaaS tool we ship updates weekly.

<table>
<thead>
<tr>
<th>Type</th>
<th>Unique Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Features</td>
<td>CCNI-1415</td>
<td>Enhancements to display all relevant alarm detail information on the Alarm Details pages.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1855</td>
<td>History timeline was extended to allow users to select a time period up to 3 months in the past.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1746</td>
<td>Added ability to search tables and table columns. You can also filter on Origin ASN (for prefixes) and filter on Prefixes (for ASNs).</td>
</tr>
<tr>
<td></td>
<td>CCNI-1763</td>
<td>Added snapshot views of ASNs when you click on an ASN, then click the History tab.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1161</td>
<td>Moved BGP Updates from the sidebar to a new tab in the ASN and Prefix details page.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1163</td>
<td>Added Quick Search functionality for Prefixes and ASNs.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1208</td>
<td>Added Slack as a notification endpoint option.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1209</td>
<td>Added Webex Teams as a notification endpoint option.</td>
</tr>
<tr>
<td>Bug Fix</td>
<td>CCNI-1855</td>
<td>Fix to ensure only active alarms can be in Acknowledged state.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1562</td>
<td>Replaced CCNI with Crosswork Network Insights.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1570</td>
<td>Resolved an issue with clear notifications being sent to s3 notification receivers.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1600</td>
<td>Fix to send notifications when an alarm goes from active to cleared.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1677</td>
<td>Fix to prevent users from accessing alarms in other organizations.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1683</td>
<td>Resolved a page loading issue with the Alarm History page.</td>
</tr>
<tr>
<td></td>
<td>CCNI-1693</td>
<td>Fix to make user names case insensitive.</td>
</tr>
</tbody>
</table>
Crosswork Network Insights Offers
New Feature Limitations based on subscription Tiers

**BASIC**
L-SPAUTO-NI-B
Price and Feature Parity with BGPmon Today

**ESSENTIALS**
L-SPAUTO-NI-E
Basic+
Enhanced Alarms
7 Days Data Analysis
Collaboration Tool Integration

**STANDARD**
L-SPAUTO-NI-S
Essentials+
Latest Alarms and Features
90 Days Data Analysis
Crosswork Integration

New
Existing - Changed
Existing
## Crosswork Network Insights Feature Comparisons

### External Route Analysis

<table>
<thead>
<tr>
<th>Feature</th>
<th>BGPmon Premium</th>
<th>CCNI Free</th>
<th>CCNI Basic</th>
<th>CCNI Essentials</th>
<th>CCNI Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix Limits</td>
<td>User Pays</td>
<td>Limited Free</td>
<td>User Pays</td>
<td>User Pays</td>
<td>User Pays</td>
</tr>
<tr>
<td>8 BGPmon Alarms</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>4 New Alarms (all new alarms)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Customizable Intent based Policies</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Alarm History</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Email / SMS notifications</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Syslog &amp; Collaboration Tools notifications</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Months Forensic Data</td>
<td>✗</td>
<td>✗</td>
<td>1 Day</td>
<td>7 Days</td>
<td>3 Months</td>
</tr>
<tr>
<td>Time Series Graphing</td>
<td>✗</td>
<td>✗</td>
<td>1 Day</td>
<td>7 Days</td>
<td>3 Months</td>
</tr>
</tbody>
</table>

**ETA CYQ2**

2020
Crosswork Network Insights Feature Comparisons
External Route Analysis

<table>
<thead>
<tr>
<th>Feature</th>
<th>BGPMon Premium</th>
<th>CCNI Free</th>
<th>CCNI Basic</th>
<th>CCNI Essentials</th>
<th>CCNI Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Peermon Connections</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>New Peermon Connections</td>
<td>✔</td>
<td>Subject to Approval</td>
<td>Subject to Approval</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>BYO SSO Oath/SAML</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>Topology</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>API Support</td>
<td>✔</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Crosswork Portfolio Integration</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
<tr>
<td>New Features Post BGPMon EOL</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✔</td>
</tr>
</tbody>
</table>

ETA CYQ2
2020
What’s Coming?
Understanding Peermon
Changes Coming

All Peers
Good for Visibility, Difficult for Automation use cases

Current Alarm Scope

My Peers
Good for events from Self
Good for Automation use cases

New Alarm Scope

Use cases
BYO-IP > Web OTT
ROA Automation > Transit SP
SP Provisioning Automated Checking > SP
ASN to ASN Compliance Checking
## Crosswork Network Insights Roadmap

### Platform
- **Q1 CY 2020**
  - Peer Geolocation Data
  - More UX updates

- **Q2 CY 2020**
  - Peermon
  - Read Only
  - Peermon Read/Write for existing users
  - CDG Tethering
  - RPSL Reports
  - RPSK Alarms

- **Q3 CY 2020**
  - Data Collection from On-Prem Sources with 12 months data retention
  - Interface and BGP-LS data collection and retention
  - File based import on-prem

- **Radar**
  - Data Sovereignty Assurance
  - External Crosswork Integration
    - Flow Data Export
    - Telemetry Data Import
    - Event Correlation
    - Peer Config Automation

### Routing Analytics
- **Q1 CY 2020**
  - ROA ASN and Prefix Reports
  - New ROA Alarms
  - Topology Views
    - eBGP ASN adjacency 2 hops max
    - BGPMon Alarm Parity
    - ROA Changes
  - Topology Views
    - eBGP ASN to ASN path
    - ASN Historical View

- **Q2 CY 2020**
  - ASN Health Assessment
  - Prefix Health Assessment
  - Peermon
    - Device Status Alarms
    - Looking glass
    - Source Specific filters for All Alarms
  - Alarm Features
    - Peer Based filters
    - Peermon DNS Root Servers

- **Q3 CY 2020**
  - Alarm Features
    - Advanced Configuration
  - iBGP Analytics EFT & FCS
    - Topology for iBGP Beta
    - Looking Glass
    - BGP Updates
    - Alarms

- **Radar**
  - Troubleshooting Assistance
    - Suggest remediation actions for known problems
  - xBGP Peer Profile Checking
  - BGP Protocol Health
  - BGP Optimization
  - Predict Network Posture

### Traffic Analytics
- **Q2 CY 2020**
  - EFT Traffic Analysis Candidates
  - GA Traffic Analysis

- **Q3 CY 2020**
  - eBGP Traffic Ingress Peering Engineering Recommendation
  - Traffic SLA based utilization tracking and Alerting per Prefix Source/Dest.

- **Radar**
  - Bundle Package Solution with other Crosswork Systems including WAE, Optima, Bandwidth and Automation (BAM)

---

© 2019 Cisco and/or its affiliates. All rights reserved.
What is Traffic Analysis?

Crosswork Network Insights – Traffic Analysis

A cloud-based SaaS offer that provides traffic analysis and recommendation for network boundary devices

Customer Challenges:

Who should I peer with?

Can I re-direct my device flow data to more than one place?

What changes do I need to make to achieve a Peering Traffic load balance?

Who should I be peering with and who are my top talkers?

When?

FCS expected CY2020 Q2
Where is Traffic Analysis Needed?

Traffic Analytics and Peering Engineering Recommendations apply to all IGP boundaries. Initial policies are designed to load balance traffic on groups of interfaces. This helps customers drive up infrastructure utilization and return on investment.

<table>
<thead>
<tr>
<th>Section</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>eBGP / BGP-LU Boundary</td>
<td>Focus</td>
</tr>
<tr>
<td>Peering &amp; Transit</td>
<td>EPE &amp; IPE</td>
</tr>
<tr>
<td>Internet Edge</td>
<td>EPE &amp; IPE</td>
</tr>
<tr>
<td>Mobile Rings</td>
<td>EPE</td>
</tr>
<tr>
<td>BGP-LU</td>
<td>EPE</td>
</tr>
<tr>
<td>Res. &amp; Bus. WAN Rings BGP-LU</td>
<td>EPE</td>
</tr>
<tr>
<td>DC Edge BGP TOR</td>
<td>IPE</td>
</tr>
</tbody>
</table>

A Preview of Traffic Analysis
Use Cases?
Routing Events impact the operation of the Networks, Time to Identification and Resolution is very poor. Event information is useful to Automation and Operations.

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).
Use Case 1: Forensic Route Analysis

Network Insight collect and store 2 months of forensic BGP data records.

This is particularly useful to:
- Security Operations
- Network Operations
- Commercial Disputes
- Evaluating Peering Candidates for stability/coverage
Use Case 2: Route Hijack Detection

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

Alarm Conditions test for any of the following:
- ASN Origin Violation
- Unexpected Longer Prefix Match
- ROA/RPKI Failure/Miss-match
- AS Path Length Violation
- New Global Peer Edge Detection
Use Case 3: New Global Peer Edge

Network Insights detects abnormal ASN relationships through various source data to advise when possible New Global Peer Edge conditions exist.

Man in the Middle Attacks have no absolute signature since AS Mid Path relationships are not signed or published securely in a single source of truth and ROA only protects first hop Peering (BGPSec was not ratified)

Conditions used to detect path Attack symptoms:
- Abnormal AS path length changes (Unique Edges)
- ASN Neighbor white list checking (third party)
- Common origin Prefix Path variations
- Low frequency ASNs in paths
- RPSL Import/Export hints
- Our Secret Sauce

Reasons can be for an attack but also for business reasons to impact traffic settlement and inspection
Use Case 4: Route Leak Detection

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

Polices can be enabled/disabled as part of a planned change workflow to reduce noise.

Alarm Conditions test for any of the following possible Route Leak symptoms:
- 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)
Why Cisco

1. Networking market leadership
2. Global multivendor network deployments
3. Commitment to open standards
4. Most comprehensive network automation portfolio
5. Most comprehensive security portfolio
Attending Cisco Live Barcelona or MWC?
Come See Us

Cisco Live Barcelona
• January 27 – January 31
• World of Solutions, Cisco Service Provider Booth, Fira Gran Via

Mobile World Congress
• Barcelona, February 25 – 28
• Cisco Booth Located in Hall 3 Booth #3E30
Find out more and Request a Trial

cisco.com/go/crosswork

Contact us ask-cni@cisco.com

Crosswork Network Insights Trials
http://crosswork.cisco.com/
Questions?
Backup Slides
Showcasing the new User Interface
New easy to use interface

2 themes Dark & Traditional

1. Whois Data
2. Geo Peer Data
3. Observed Data
Policies are now specific to the input source

1. ASN Policies
2. Prefix Policies
3. Peer Policies (coming, CYQ2)
4. Traffic Policies (coming, CYQ2)
New Policy and Rule Configuration

1. Origin ASN
2. Upstream ASN easy to input
3. Add Rules with clear requirements
AS Path Expression and Upstream AS now ready

1. Create a Path Expression
2. Input a test path to validate the Expression
3. Test the Expression

Path Expressions are useful when defined as known failure outcomes.

An example would be if a failover AS path is not normally observed.
Questions and feedback in the user interface

1. Direct access to support case open
2. Submit feedback and requests
3. Link to Cisco Communities
4. Link to API Documentation

Submit Product Feedback

We'd like to hear what you think. Please complete the form below and we'll get back to you as quickly as possible.

- Feature Request
- Sales Support
- Other Issue

Description
I would like to be able to get alerts when my Peer Device is down

Press the Submit button to send your feedback.
User Preference and API Keys

1. User Interface Settings
2. API Keys List
3. API Key Creation
A Preview of Traffic Analysis
What is Traffic Analysis?

Crosswork Network Insights – Traffic Analysis

A cloud-based SaaS offer that provides traffic analysis and recommendation for network boundary devices

Customer Challenges:

Who should I peer with?

Can I re-direct my device flow data to more than one place?

What changes do I need to make to achieve a Peering Traffic load balance?

Who should I be peering with and who are my top talkers?

When?

FCS expected CY2020 Q2
Where is Traffic Analysis Needed?

Traffic Analytics and Peering Engineering Recommendations apply to all IGP boundaries. Initial policies are designed to load balance traffic on groups of interfaces. This helps customers drive up infrastructure utilization and return on investment.
**Use Case:**
Peering Engineering Recommendation

**Egress for FCS Ingress Post FCS**

Provide Analysis of what prefixes preferences should be changed to achieve Peering Traffic Engineering objectives.
Where does this get us?

- **FCS FY Q3 2020**
- **Today**
- **BGP**
- **BGP+ Flow**
- **BGP+ Flow+ Topology**
- **BGP+ Flow+ Topology Telemetry**
- **BGP+ Flow+ Topology TCP Probing**
- **BGP+ Flow+ Topology TCP Probing Traffic Sniffing**
- **BGP+ Flow+ Topology SID Mapping**
- **BGP+ Flow+ Topology Telemetry Multi-domain**
- **BGP+ Flow+ Topology Telemetry + Telemetry**
- **EPE / IPE Automation + Optima + Change Automation + SR-PCE + XR vRR**
- **Planning + WAE External Demand Matrix**
- **Analysis SLA Management + Health Insights + Netrounds**
- **Detection, DDoS + Radware + Stealthwatch + AMP + Netrounds**

© 2019 Cisco and/or its affiliates. All rights reserved.