MULTINATIONAL BANKING CORPORATION INVESTS IN ROUTE ANALYTICS TO AVOID OUTAGES

CASE STUDY

PACKET DESIGN™

Table of Contents

This case study discusses the cause of a network outage at a multinational banking and financial services corporation and how Packet Design's Route Explorer was implemented for its analytics, modeling and planning capabilities to avoid a recurrence.

Organization Background and Network Summary

A global banking organization delivers various financial services to its customers, including web and mobile e-commerce and online banking, global credit and debit card services, and asset and investment management. The company has nearly 5,000 banking centers, more than 15,000 automatic teller machines (ATM), five data centers and several customer assistance contact centers. Given the critical need for security, high availability, compliance and rapid response to requests and incidents, the bank, like many others, largely operates and manages its own IP/MPLS network, with some network operations being outsourced.

The branches, ATMs and data centers form a large interconnected network referred to as the "bank network." Major branches serve as concentration points to combine different types of traffic from smaller branches before being sent to the backbone network. Internal transactions related to banking operations stay within the bank network whereas customer-facing services, such as e-commerce, online banking, wealth management and customer relationship management (CRM), traverse the Internet and are run from DMZs located in the data centers. The network is comprised of HP and Cisco devices, with Cisco ASR and Cisco 7600 series routers used at the edge in the data centers and concentration points.

Outage Precursor and Impact

The network team had scheduled a weekend maintenance window to perform close to 5,000 changes across the bank network. Among these changes were updates to the BGP routing table at six locations -- four data centers and two of the large branch concentration points. As part of the change, new route numbers were to be added to routing tables in the Cisco ASR and Cisco 7600 series routers, along with updated route-maps.[1]

During the maintenance window, the bank began to receive complaints from customers and the customer support teams that the bank's website and online banking facilities were inaccessible. Customers were getting a "page cannot be displayed" error on the website and the mobile banking applications displayed "connection error." Customers and support associates who were already in website and online banking sessions were disconnected and unable to log back in again. At the same time, customers using the bank's debit cards were unable to complete their transactions and support

1 A route-map can be defined as a series of statements that ensures that routes (route numbers or prefixes) in the routing table match policies defined to permit or deny the route advertisement to the rest of the network. A route-map can also include optional attributes about the routes.

associates were unable to access various customer support applications, including the CRM system. The network team received alerts from web monitoring tools about dropped sessions and the bank's traffic analyzer reported a drop in the volume of traffic to the data centers.

After about 40 minutes of downtime, the issue resolved automatically, and the website and banking services were back online and accessible to the customers and support associates. The bank's post mortem analysis reported more than 200,000 failed interactions.

Outage Analysis

Within a few minutes of the issue being first reported and alerts generated by their monitoring tools, the network team began analyzing the problem by checking error logs and change logs for the bank network's DNS servers, proxy servers and all network devices. Escalations were triggered and conference calls were set up to analyze and troubleshoot the issue. While this analysis was being performed, the monitoring tools reported that traffic to the data center had returned to baseline and banking applications and customer services were once again accessible.

Troubleshooting is extremely hard and sometimes impossible when the issue is already resolved and there is no 'smoking gun.' The bank's network team faced such a scenario and their existing network and traffic monitoring systems could not pinpoint the root cause. It was only after hours of manual analysis of the events that led up to the outage that the network team realized it was the BGP routing table changes on the edge routers that caused the problem. They determined it was related to the sequence in which the commands were issued to the routers.

The sequence of adding new route numbers on the routers involved first specifying the new route numbers and then the route-map. The process had been tested in the lab using a Cisco 7600 series router, like the bank's edge routers. The same sequence was then followed during the maintenance window on the live network -- on the four Cisco 7600 series routers and then on the two Cisco ASR routers. However, the IOS for each of these router models handles BGP updates differently. The Cisco 7600 waits for a soft reset command to apply the new routes and advertise the new route numbers based on policies defined in the route-map. The Cisco ASR has a feature that saves route updates automatically as each command is applied. This difference resulted in the new route numbers from the ASR being advertised to the DMZ routers, causing traffic destined for the Internet to be redirected to the bank network and blocking user access to the banking applications hosted from the DMZ.

As the change team completed the scheduled changes, unaware of the outage, the new routes were advertised as per policy and the issue ultimately resolved itself. The post mortem analysis later determined through testing that the new routes had been advertised and propagated through the entire bank network within 30 seconds of the commands being entered on the Cisco ASRs.

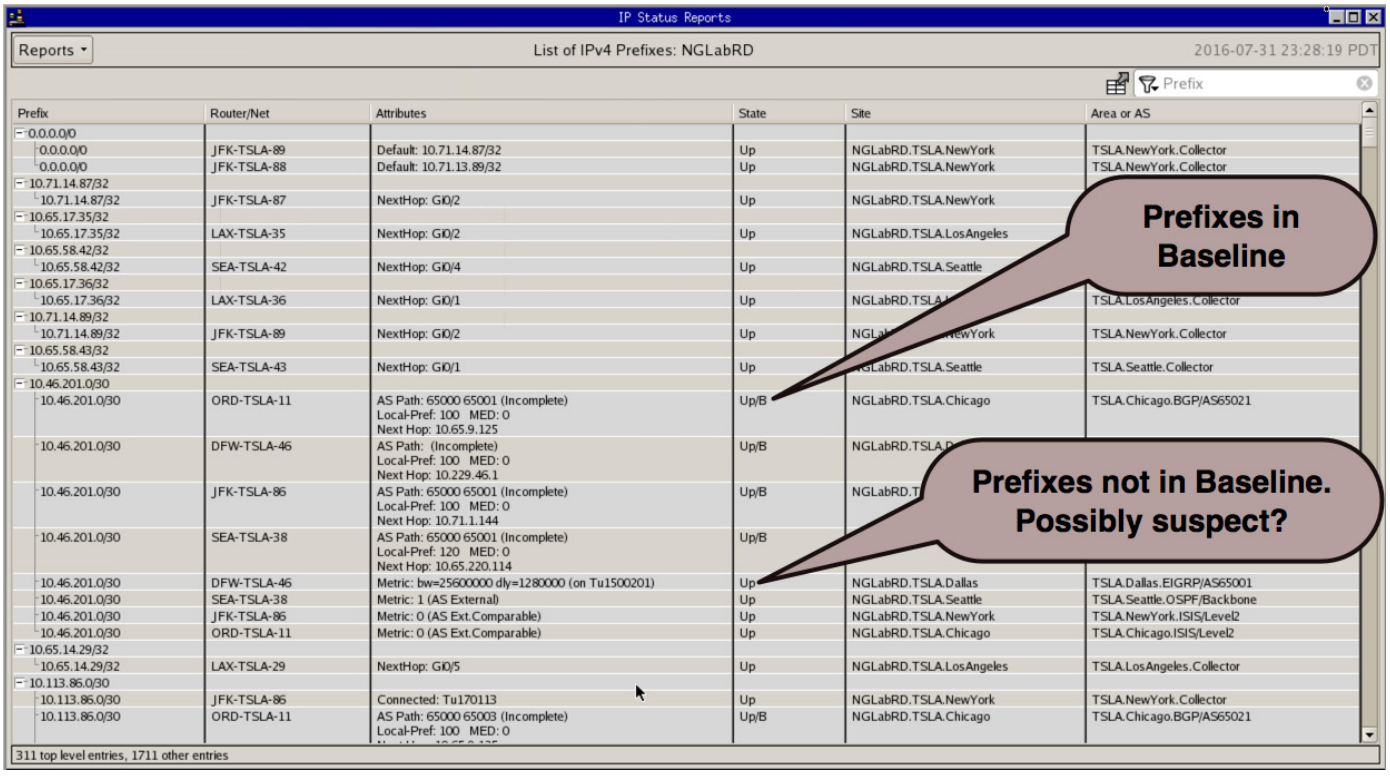
Corrective Actions

The bank identified several action plans to mitigate the risk of a recurrence and enable faster detection and resolution should there be one. The requirements included the following:

- Monitor and alert on changes in routes and route advertisements. This would prevent inadvertent advertisement of routes or route leakage that could lead to similar outages. The monitoring and alerting must be done in real time considering that the new route numbers were advertised and propagated in the network within 30 seconds. Using SNMP or other periodic data collection could result in a similar condition being missed.
- A method to capture and analyze route path change history. This would help the network engineers performing root cause analysis to troubleshoot conditions that were no longer present.

Based on these requirements, Packet Design's Route Explorer was selected for an extensive evaluation and ultimately acquired by the bank.

Route Explorer is the base component of the Packet Design Explorer Suite which combines route, traffic and performance analytics. Route Explorer is used worldwide by network engineers, architects,



Prefix	Router/Net	Attributes	State	Site	Area or AS
0.0.0.0/0					
0.0.0.0/0	JFK-TSLA-89	Default: 10.71.14.87/32	Up	NGLabRD.TSLA.NewYork	TSLA.NewYork.Collector
0.0.0.0/0	JFK-TSLA-88	Default: 10.71.13.89/32	Up	NGLabRD.TSLA.NewYork	TSLA.NewYork.Collector
10.71.14.87/32					
10.71.14.87/32	JFK-TSLA-87	NextHop: Gi0/2	Up	NGLabRD.TSLA.NewYork	
10.65.17.35/32					
10.65.17.35/32	LAX-TSLA-35	NextHop: Gi0/2	Up	NGLabRD.TSLA.LosAngeles	
10.65.58.42/32					
10.65.58.42/32	SEA-TSLA-42	NextHop: Gi0/4	Up	NGLabRD.TSLA.Seattle	
10.65.17.36/32					
10.65.17.36/32	LAX-TSLA-36	NextHop: Gi0/1	Up	NGLabRD.TSLA	TSLA.LosAngeles.Collector
10.71.14.89/32					
10.71.14.89/32	JFK-TSLA-89	NextHop: Gi0/2	Up	NGLab NewYork	TSLA.NewYork.Collector
10.65.58.43/32					
10.65.58.43/32	SEA-TSLA-43	NextHop: Gi0/1	Up	GLabRD.TSLA.Seattle	TSLA.Seattle.Collector
10.46.201.0/30					
10.46.201.0/30	ORD-TSLA-11	AS Path: 65000 65001 (Incomplete) Local-Pref: 100 MED: 0 Next Hop: 10.65.9.125	Up/B	NGLabRD.TSLA.Chicago	TSLA.Chicago.BGP/AS65021
10.46.201.0/30	DFW-TSLA-46	AS Path: (Incomplete) Local-Pref: 100 MED: 0 Next Hop: 10.229.46.1	Up/B	NGLabRD.TSLA.D	
10.46.201.0/30	JFK-TSLA-86	AS Path: 65000 65001 (Incomplete) Local-Pref: 100 MED: 0 Next Hop: 10.71.1.144	Up/B	NGLabRD.T	
10.46.201.0/30	SEA-TSLA-38	AS Path: 65000 65001 (Incomplete) Local-Pref: 120 MED: 0 Next Hop: 10.65.220.114	Up/B		
10.46.201.0/30	DFW-TSLA-46	Metric: bw=25600000 dly=1280000 (on Tu1500201)	Up	NGLabRD.TSLA.Dallas	TSLA.Dallas.EIGRP/AS65001
10.46.201.0/30	SEA-TSLA-38	Metric: 1 (AS External)	Up	NGLabRD.TSLA.Seattle	TSLA.Seattle.OSPF/Backbone
10.46.201.0/30	JFK-TSLA-86	Metric: 0 (AS Ext.Comparable)	Up	NGLabRD.TSLA.NewYork	TSLA.NewYork.ISIS/Level2
10.46.201.0/30	ORD-TSLA-11	Metric: 0 (AS Ext.Comparable)	Up	NGLabRD.TSLA.Chicago	TSLA.Chicago.ISIS/Level2
10.65.14.29/32					
10.65.14.29/32	LAX-TSLA-29	NextHop: Gi0/5	Up	NGLabRD.TSLA.LosAngeles	TSLA.LosAngeles.Collector
10.113.86.0/30					
10.113.86.0/30	JFK-TSLA-86	Connected: Tu170113	Up	NGLabRD.TSLA.NewYork	TSLA.NewYork.Collector
10.113.86.0/30	ORD-TSLA-11	AS Path: 65000 65003 (Incomplete) Local-Pref: 100 MED: 0	Up/B	NGLabRD.TSLA.Chicago	TSLA.Chicago.BGP/AS65021

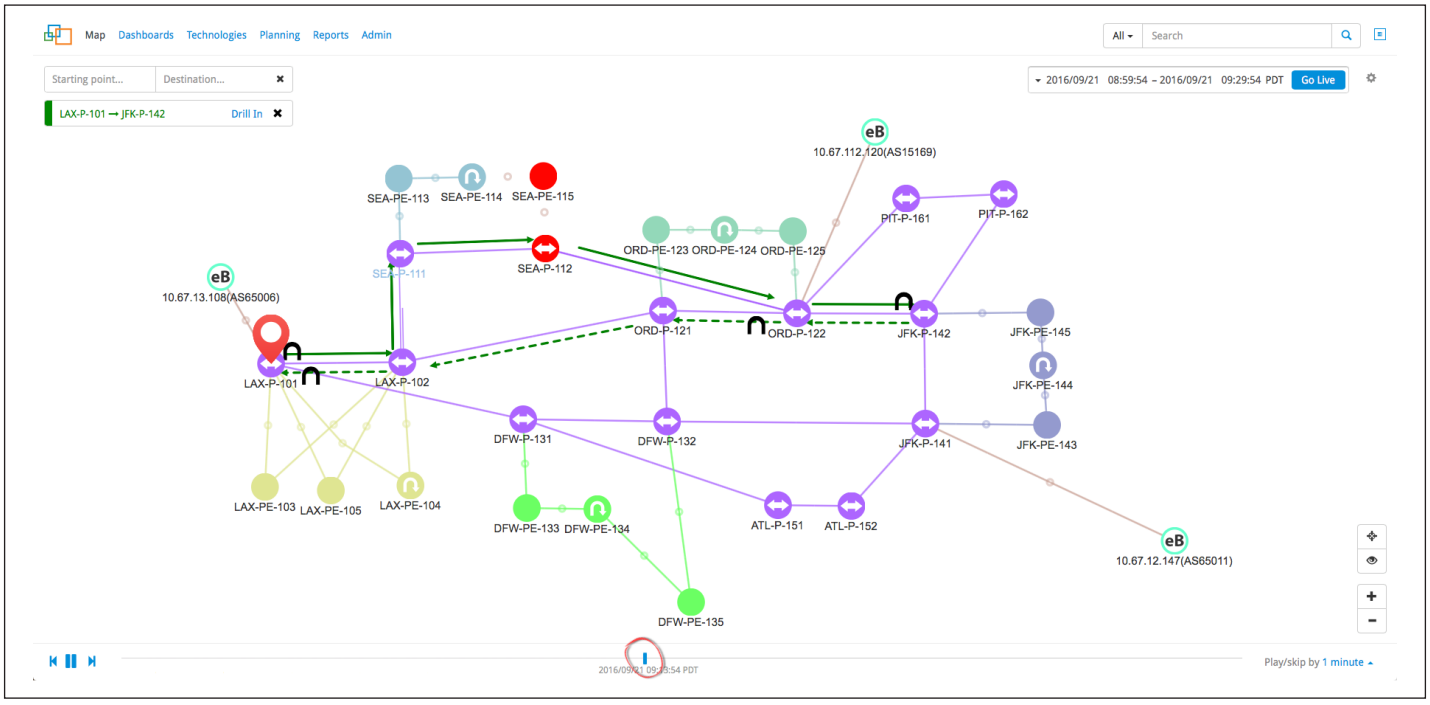
Detecting BGP Prefixes not in Baseline

planners and operations teams responsible for today's complex, mission-critical enterprise and service provider networks. It provides management visibility into routing behavior for IGP and BGP protocols, multicast, MPLS VPNs and traffic engineering tunnels, with real-time monitoring, historical reporting and interactive modeling capabilities.

Route Explorer is deployed as a passive routing device so it receives (and records) the BGP and IGP exchanges between the routers in a network. The data is used to build and maintain real-time and historical topology models of the IP/MPLS network and overlay services which are used for real-time monitoring and alerting of route, path and topology changes, providing back-in-time forensic analysis, and what-if modeling capabilities to mitigate the risk of unexpected results from maintenance changes.

Route Explorer collects route number data and establishes a baseline. When new routes not in baseline are detected, Route Explorer issues an alert. This ensures the bank knows immediately if new routes are advertised to the DMZ or to the bank network, so the team can take steps to avoid another outage.

To address the bank's second requirement, Route Explorer's recorded routing data and topology models can be viewed to analyze past events. A DVR-like playback feature allows the network team to "rewind and replay" the network's routing behavior to understand how routing path changes, even those that lasted only for a few seconds or minutes, impacted services.



Routing Path History via Playback Feature

In addition to the documented requirements, the bank discovered that Route Explorer strengthens the change management process. By analyzing what-if scenarios, engineers can predict the impact of planned changes. For example, the engineers can simulate adding or removing routers, interfaces, routes, prefixes and peers to see how the network converges and observe unexpected results.

After a six-month evaluation, the bank determined that Route Explorer met the requirements and deployed the product in the live network, providing an additional layer of assurance for its critical online services.

To learn more about Packet Design and the Explorer Suite, please visit www.packetdesign.com.