Finding and Diagnosing BGP Route Leaks

Posted by Nick Kephart (https://blog.thousandeyes.com/author/nick/) on April 1, 2015

There have been a number of high profile routing leaks in the past few weeks. So today we're going to review several of these leaks in detail to understand how they work, how you can detect them and how you can determine their severity. Our examples cover the Google / Hathway route leak and the Enzu route leak, both in March 2015.

What is a Route Leak?

Route leaks involve the illegitimate advertisement of prefixes, blocks of IP addresses, which propagate across networks and lead to incorrect or suboptimal routing. Route leaks are similar in structure and effect to route hijacks, BGP hijacks (https://blog.thousandeyes.com/4-real-bgp-troubleshooting-scenarios/) and BGP man-in-the-middle attacks. However, while hijacks typically connote malicious attacks, route leaks instead are usually inadvertent and due to filter misconfigurations.

To understand a route leak, we first need to understand how routes are propagated across the Internet. Routes are defined between networks with common routing policies, known as Autonomous Systems (ASes). An AS originates prefixes for IP address ranges that it owns and communicates the AS Path, or sequence of ASes to reach the origin, to other ASes using Border Gateway Protocol (BGP). An AS also advertises prefixes for traffic that can be delivered by that AS. As in Figure 1, AS100 will announce its own prefixes to its downstreams, upstream and peers. AS100 will also announce certain prefixes that it learns and will prepend its AS number to the path, so AS100 will announce [100 300] to its peers.

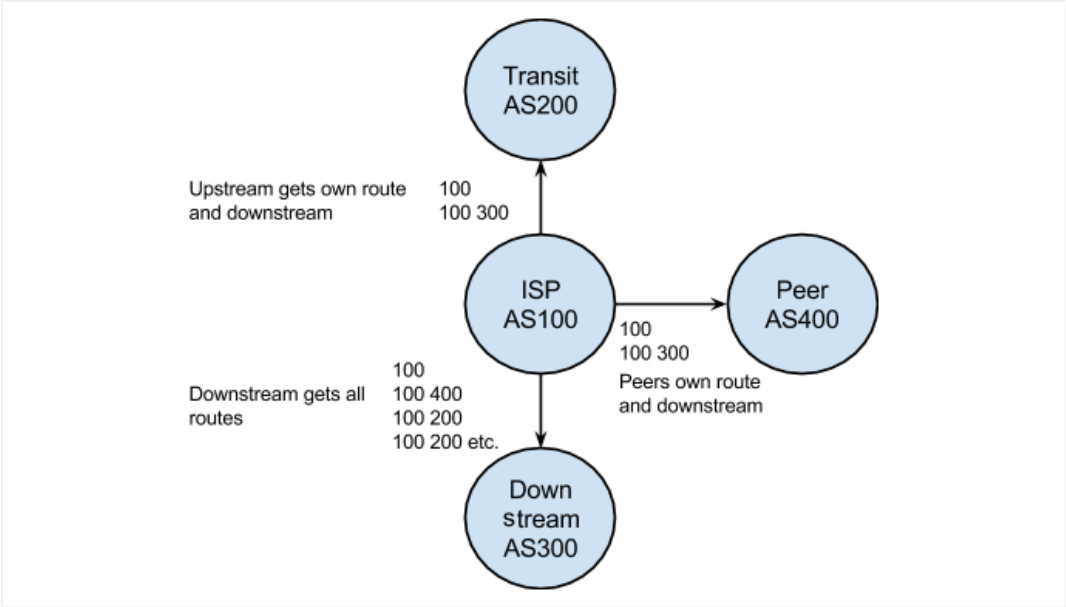


Figure 1: Typical routing advertisements for example AS100.

Route leaks can happen from an AS originating a prefix that it does not actually own or an AS announcing that it can deliver traffic through a route that should not exist. Route leaks are particularly prone to propagation when a more specific prefix is advertised (as BGP prefers the most specific block of addresses) or when a path is advertised that is shorter than the currently available paths (as BGP prefers the shortest AS Path). Practically, route leaks occur when BGP advertisements are not properly filtered using the no-export community. ASes typically advertise routes to providers and peers, filtering which routes are sent to which ASes. In Figure 2, AS100 improperly announces the path of its peer AS400 to its upstream transit provider.

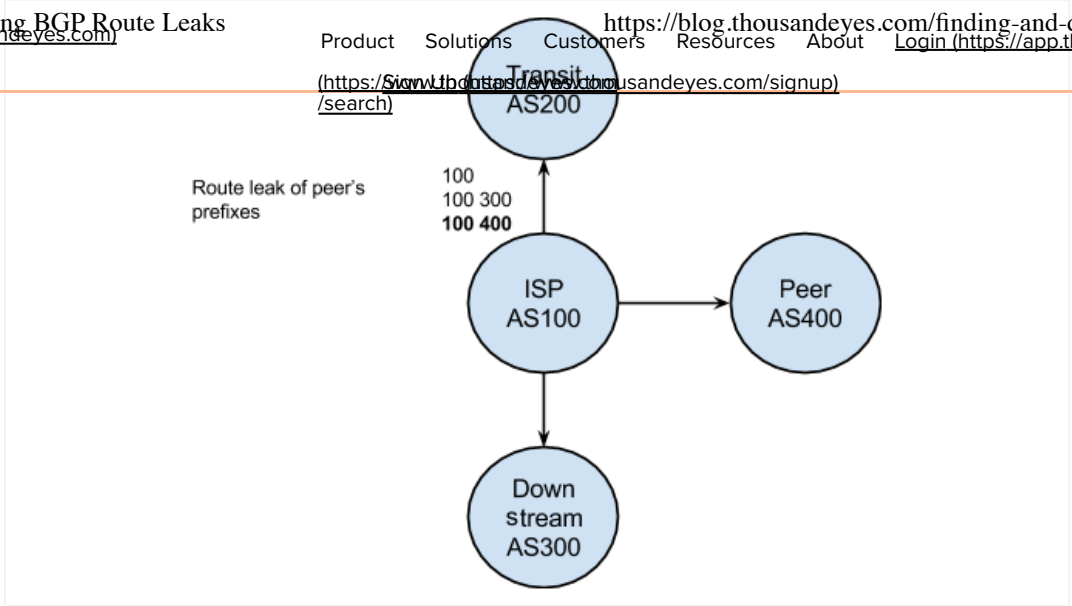


Figure 2: Example of a route leak where AS100 incorrectly announces routes for its peer to its transit provider. Similar to the Google example below.

Spotify Example

Our first example occurred in March 2015, when hosting provider Enzu leaked routes to dozens of prefixes. Spotify's prefixes were among those leaked. In Figure 3, the normal routes to Spotify (AS43650) go through upstream AS Carpathia Hosting (AS29748) and Tier 1 ISPs such as Level 3 (AS3356) and Tata (AS6453). See the interactive data here (https://ejqoke.share.thousandeyes.com).

Figure 3: Routes to Spotify GSLB Streaming (193.182.8.0/21) under normal conditions with upstream Carpathia Hosting (AS29748).

On March 26th, in addition to the 10 /21, /22 and /24 prefixes that Spotify normally originates, two additional /23 prefixes showed up. In Figure 4, prefix 194.68.30.0/23 appears, is visible from only a subset of BGP monitors and has a peculiar AS path that includes Los Angeles Internet Exchange (AS40633) and Enzu (AS18978). In this case, Enzu originated the prefix and leaked the routes to LAIX.

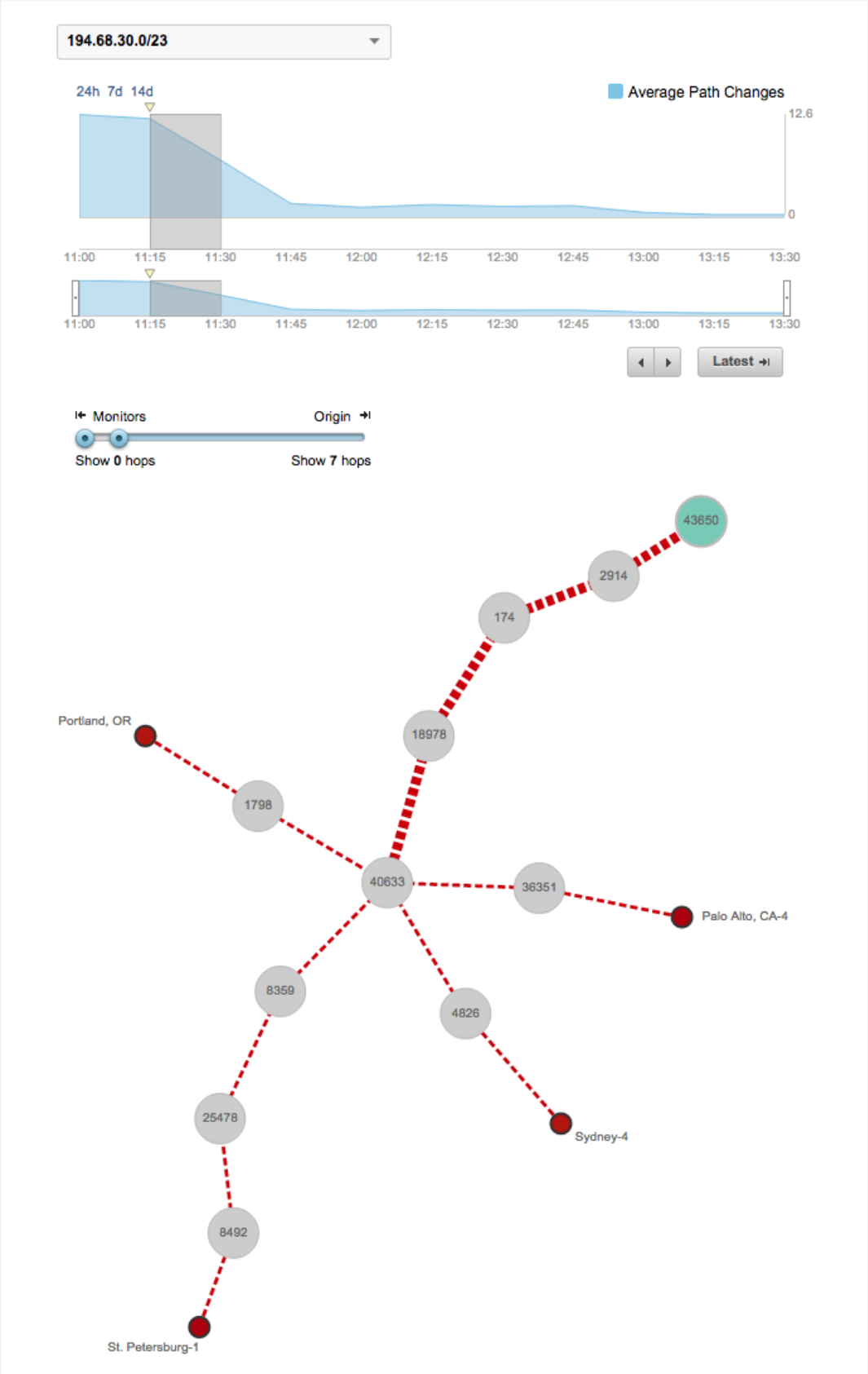


Figure 4: Spotify route leak with a newly advertised /23 prefix and AS18978 included in the AS path.

Also affected were Amazon prefixes, including services hosted in AWS such as Tinder and Clash of Clans. A

variety of more specific prefixes were originated, such as /20s and /23s. More specific prefixes originating from a incorrect AS is often the result of improper filtering of a BGP Optimizer which takes prefixes and breaks them into smaller prefixes to more finely ... .org/pipermail/nanog/2015-March/074341.html) that "a Tier 2 ISP that connects to [the Enzu] network made an error in their router configuration... stopped advertising the no-export community string... causing the route leakage."

Google Example

In March, Google was also the victim of a routing leak (http://arstechnica.com/information-technology/2015/03/indian-isps-routing-hiccup-briefly-takes-google-down-worldwide/). In this case Google's prefixes were leaked by Hathway, an Indian ISP, and accepted by their peer Bharti Airtel. Bharti then advertised routes to dozens of major ASes around the globe. In Figure 5, we can see the leak of an existing prefix 74.125.200/24 from Hathway, with traffic from Bharti (AS9498) transiting via Hathway (AS17488) to Google. This leak lasted for nearly a day, from 10:30 UTC on March 11th to 9:15 UTC on March 12th.

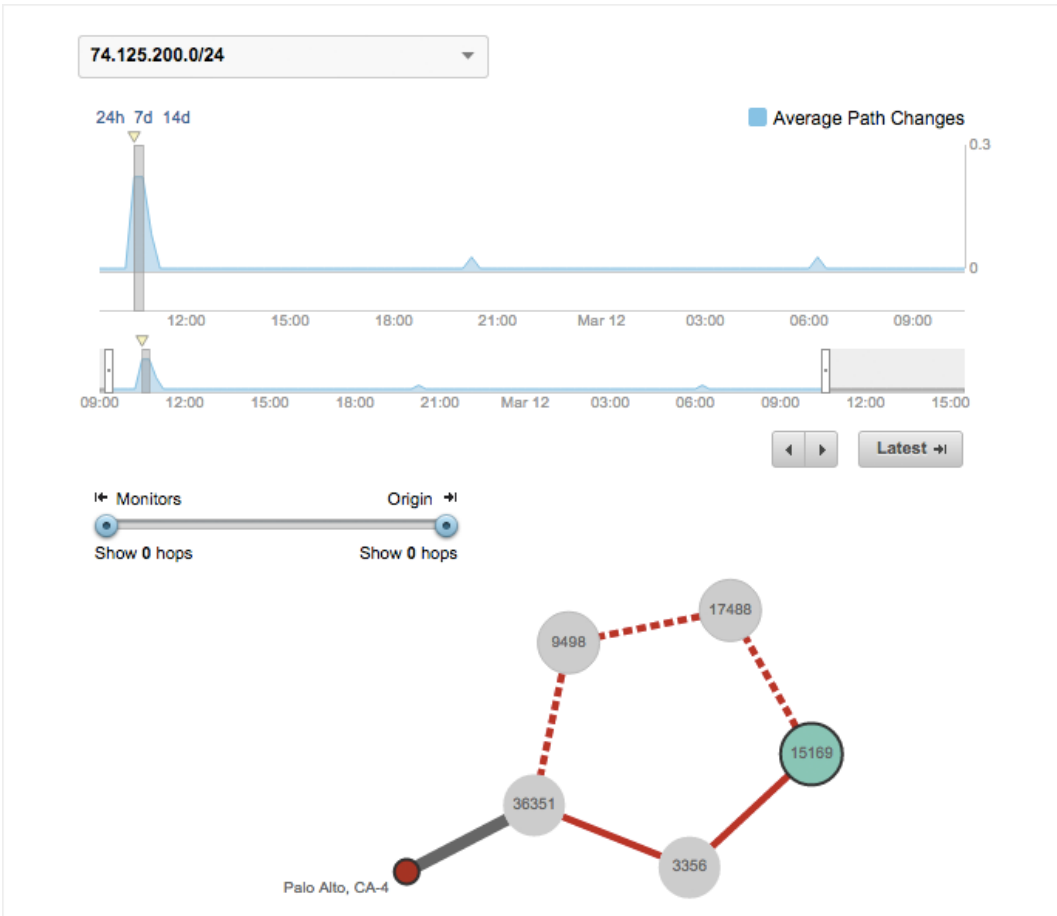
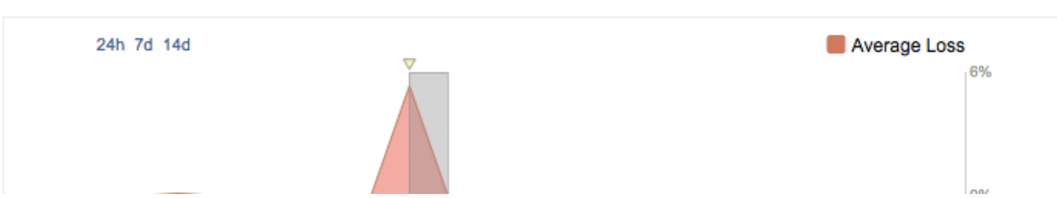


Figure 5: Route leak to Google via Hathway AS17488 that affects Bharti Airtel AS9498.

How to See if Users Are Affected

Route leaks are important to triage, but what a network operator really cares about is if the route leak has a widespread impact that affects actual traffic paths. That's possible to do with synthetic probing and path tracing.

Let's return to our Google example. Hathway has leaked routes to its provider Bharti Airtel. In Figure 6, our probe in New Delhi was affected by the routing change with traffic transiting Bharti rather than Tata, the normal upstream provider. Traffic entering the Bharti network was dropped at the edge, as Bharti likely filtered out packets destined to Google via Hathway.



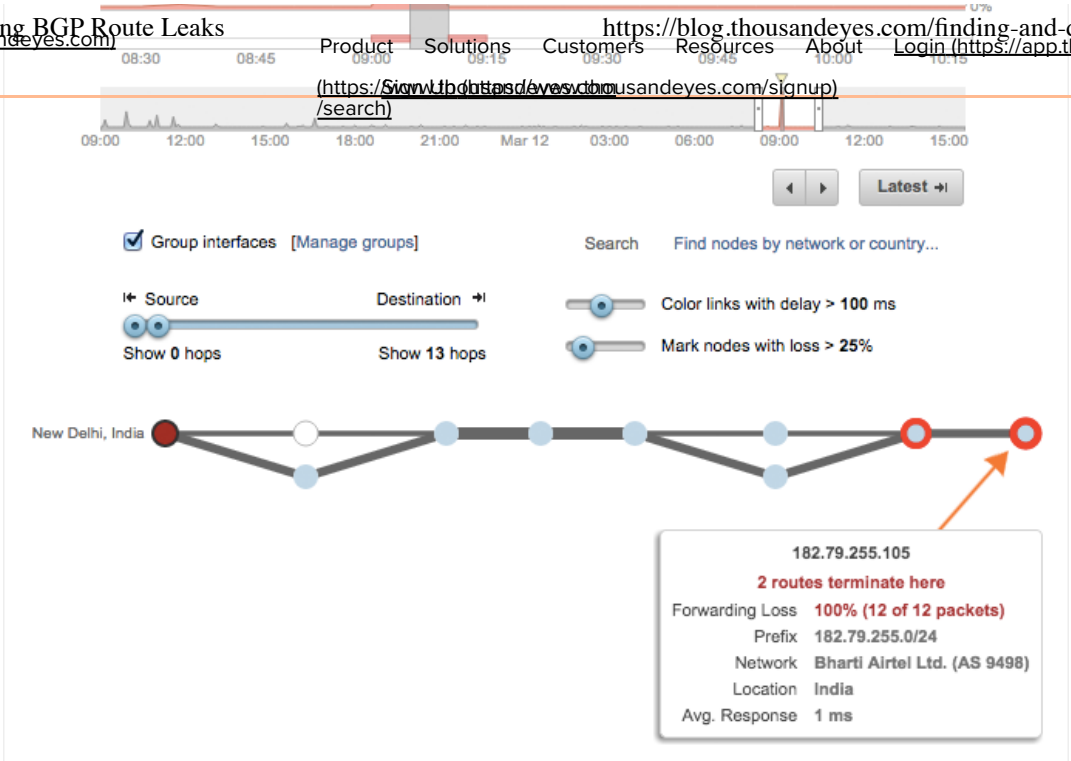


Figure 6: Routes affected to Google from New Delhi that terminate in the Bharti Airtel network.

So why was actual traffic affected in the Google route leak and not in the Enzu leak? First, in the Google leak Hathway directly peered with Google, meaning that the AS path it advertised was short (length of 3) and more likely to be preferred by other networks. Second, some of these other networks, such as Bharti, accepted these routes.

In the case of the Enzu leak, affecting Spotify and Amazon-based services, we did not see any path changes for our several dozen monitors. This is likely because of the relatively long path (length of 5+), from LAIX > Enzu > Cogent > NTT > Spotify.

Therefore, which AS leaks a route is important: in terms of with whom they peer, how their peers trust their advertisements and how far they are from the hijacked AS (AS path length).

Testing and Alerting for Route Leaks Up

Finding route leaks can seem daunting since it can be hard to verify which routing changes are legitimate. But you can use several heuristics that you can see in the BGP Route Visualization:

- Newly announced, more specific prefixes (see covered prefixes)
- Path changes that include unexpected (non-tier 1) networks (see path change timeline)

To start monitoring for route leaks, setup a test with BGP route visualization enabled. This can be a Page Load or HTTP for a web service, a Network test for a non-HTTP service or a BGP test if you're only interested in routing.

There are several types of alerts which can be useful to set up:

- **Origin ASN:** Set to your own, or hosting provider's, ASN to be alerted if any other origin is detected.
- **Next Hop ASN:** Set to your upstream ISPs to be alerted if any other routes are advertised.
- **Covered Prefix:** Set to 'exists' to alert on any sub-prefixes or to 'not in' to alert on any sub-prefixes not in your expected list.

For more info on detecting BGP leaks, check out the blog post on BGP Alerting (https://blog.thousandeyes.com/proactive-bgp-alerting/). You can setup these tests and alerts by creating a free ThousandEyes Lite (https://www.thousandeyes.com/lite?utm_source=blog&utm_campaign=lite&utm_medium=cta) account.

Categories: Product (https://blog.thousandeyes.com/category/product/)

Tags: BGP (https://blog.thousandeyes.com/tag/bgp/), BGP Hijack (https://blog.thousandeyes.com/tag/bgp-hijack/), Network Outage (https://blog.thousandeyes.com/tag/network-outage/), Peering (https://blog.thousandeyes.com/tag/peering/), Route Leak (https://blog.thousandeyes.com/tag/route-leak/)

Subscribe to the Blog

Stay connected with blog updates and outage reports delivered while they're still fresh.

Email Address Subscribe

« Previous Post (https://blog.thousandeyes.com/monitor-dynamics-crm-performance/)

Next Post » (https://blog.thousandeyes.com/5-must-track-web-performance-metrics/)

Recommend Share Sort by Best

Join the discussion…

avinash • 2 years ago

In the google case, google would have already advertised the prefix to hathway right? so as per bgp process ebgp routes recieved by hathway will be send to airtel rite from hathway ? so how do we say that has route leak? only if google would have advertised that as community no-export then it makes sense for hathway not to advertise..?

• Reply • Share ›

Nick Kephart Mod ➚ avinash • 2 years ago

Avinash,

Hathway does peer with Google, but through a private connection that is not normally advertised as a route to any other non-customer peers. So it was a leak in that it was inadvertent on Hathway's part. Because of the specificity of the prefixes advertised, and the fact that it was not no-export, it was picked up by Bharti one would expect from a major peer.

• Reply • Share ›

avinash ➚ Nick Kephart • 8 months ago

Thank you nick for the explanation...apologize for the delay in reply...

• Reply • Share ›

ALSO ON THOUSANDEYES

Monitor Global Performance of Microsoft Dynamics CRM

2 comments • 2 years ago•

Nick Kephart — ThousandEyes does elements of app monitoring along with network monitoring. Our Enterprise Agents can run scheduled, scripted …

Internet Censorship Around the World

1 comment • a year ago•

Vincent Olisah — Great anallayses!!

Troubleshooting Path MTU and TCP MSS Problems

1 comment • 2 years ago•

skalwani — Very useful!

Comparing Latency of the Top Public DNS Providers

1 comment • 2 years ago•

Chris R — Very interesting! Would also be very interesting to see a more recent update on the performance.

Subscribe Add Disqus to your siteAdd DisqusAdd Privacy

Subscribe to the Blog

Stay connected with blog updates and outage reports delivered while they're still fresh.

Email Address Subscribe