



Direct Internet Access (DIA): Rethinking WAN for the Cloud Era

Even CIOs and IT managers who only a few years ago had no intention of upending their traditional, MPLS-based network architectures are being forced to consider changes. As options for cloud networking have grown alongside booming SaaS adoption, enterprise IT has no choice but to explore more agile network models that deliver business apps at the speeds end users now expect.

As a result, IT teams have been ripping up networks based exclusively around MPLS and centralized data centers en masse, hitching their wagons not just to the promise of improved speed and performance, but also significant cost and labor savings as legacy hardware — and associated management — gets retired.

Due to the increase in security, reliability, and connection speed, one of the most compelling MPLS alternatives is simply Direct Internet Access (DIA) for app delivery that retires the centralized-data center model of legacy network architectures in favor of a distributed network organization—and for good reason. Many companies will use DIA as part of a larger solution because it pairs nicely with SD-WAN deployments or redundant setups.

For starters, the internet is ubiquitous, as almost every branch office already partners with an ISP who can facilitate delivery paths for apps over the internet, making DIA extremely easy for IT to deploy along with a VPN service. The cost-to-bandwidth ratio is also simply much lower when teams don't have to purchase dedicated MPLS.

Because users are accustomed to experiencing sub-2 second speeds on their personal apps when they aren't on the enterprise network (instead leveraging LTE or using their own cellular data/WiFi), anything less can feel like a lag that hinders user satisfaction.



SAVE
20 to
30%

Reports indicate that enterprises that retire MPLS-only architectures can save between 20-30% of their IT budgets.

BUT AS WITH ANY MAJOR OPERATIONAL OVERHAUL, THERE ARE PIVOTAL CONSIDERATIONS THAT COME INTO PLAY BEFORE TEAMS TO GO ALL-IN ON DIA. THESE INCLUDE:

- What are the trade-offs when sending traffic directly over internet pathways that IT teams don't own or control?
- What additional security features will need to be introduced to supplement secure business-critical apps traveling over public internet?
- Will IT lose the visibility they need into app delivery paths they need to diagnose or prevent performance issues?

Teams also need to consider the benefits of networking technologies — specifically software-defined networking (SD-WAN) configurations — that combine multiple avenues for connectivity.

For instance, SD-WAN enables access choices between DIA, MPLS and LTE, as well as “soft benefits” related to centralized management, security, and operational agility. But once deployed, will these tools actually deliver the cost and labor savings that CIOs crave, or simply replace old IT headaches with new ones? And will the network actually perform better with new network architectures than they did before implementation?

Getting a full picture of what DIA entails — whether or not teams balance this networking option alongside legacy solutions with SD-WAN — will help teams understand whether or not this option is best for their organization's needs.

Setting the right expectations — and trusting the internet

Turning to public internet for transport of enterprise-grade traffic involves setting and managing the performance expectations from the perspective of the application user. That's why it's important that teams take their time in choosing an upstream ISP they can trust and optimizing their BGP routing across multiple internet circuits from the start. Large enterprises should always negotiate SLAs with their ISP around performance and outages. This helps set the foundation for success by ensuring the pathways that apps will commute are primed to deliver an acceptable baseline of performance expectations.

The end-user's perception of performance extends well beyond the application itself — i.e. how well a SaaS provider is managing the app's functionality — into how the network is affecting the delivery of that application. Baselining performance before launching a service over DIA circuits or while accessing SaaS application will allow teams to assess faults and plan proactively.



Decentralizing the network without compromising control

Under the legacy WAN model that most enterprises followed, traffic travels from remote offices over the network through upstream ISP connections to a centralized data center. DIA takes this model apart, breaking out traffic from the branch offices instead of a data center at headquarters to create a highly-distributed network architecture.

Because DIA traffic isn't explicitly backhauled to an individual, centralized data center, teams need to extend security features that were once contained there to each remote location, including the implementation of gateways and firewalls at each office. This also reduces the latency incurred when users have to round-trip traffic through another company location before accessing the internet.

The problem here is that teams need solutions that have the ability to see behind these firewalls and gateways to get the local perspective into how apps are performing once these configurations are up and running.

It's at this stage of the planning process — once teams have set performance baselines and started accounting for decentralization — that SD-WAN solutions start becoming increasingly attractive in the context of DIA. That's because many of the “soft” management and operational benefits SD-WAN promises to help IT regain some of the control they may have lost when they ripped up their legacy architecture.

As part of SD-WAN implementation, SD-WAN-enabled edge routers need to be placed at each branch location on the WAN that will dictate each office's routing policies. A centralized SD-WAN controller pools these routing policies and sets a global standard for all traffic across the WAN that gives central IT a level of visibility across the enterprise footprint.

What's attractive about SD-WAN is that it doesn't force teams to solely seek DIA for all traffic, as IT may want to retain some MPLS connectivity. This can be practical in managing bandwidth-heavy VoIP flows, for instance, by steering them over MPLS circuits while less time-sensitive applications are routed over DIA tunnels.

From there, many SD-WAN providers collect relatively basic app performance measurements from the traffic that allow them to automatically redirect certain streams according to the controller's policies. But there's a wealth of granular data that the SD-WAN won't pass on to IT.

For instance, when traffic travels directly over the internet, most of the external characteristics of the delivery path — that is, the hops between DNS servers and other touch points along the public internet — aren't accounted for.

There may be dedicated VPN tunnels that transit traffic between branch offices, data centers, and the internet, for example. From the SD-WAN view, this tunnel appears to be a single hop from end-to-end. In reality, traffic could be transiting more than a dozen different routers or Autonomous Systems (AS) along its path. If performance isn't up to snuff over this tunnel, all the SD-WAN can deliver to enterprise IT is a binary good/bad response.

In a nutshell, these tools don't inherently collect any data about Internet routing tables, hop-by-hop metrics across, communication between ASs or any of the additional network infrastructure outside of the controller's purview. When this detail is missing, IT can't pinpoint which network organization within the Internet may be at the root of an issue, let alone culprit routers or detailed error metrics.

These are a lot of blind spots compared to the pre-DIA days when IT owned all of the connections and didn't need to account for a wealth of additional touchpoints.

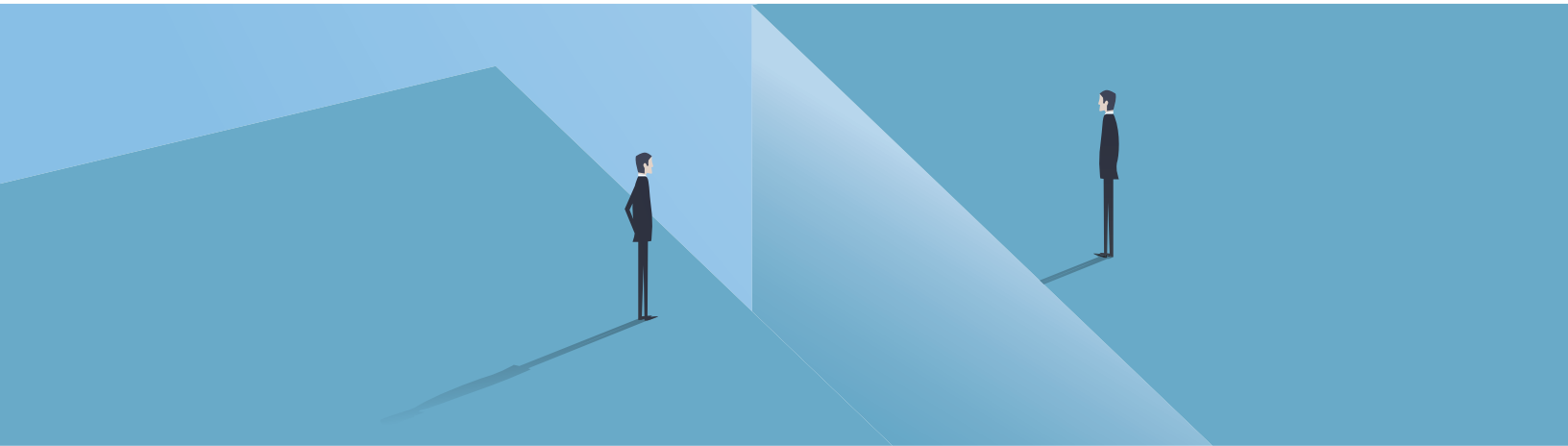
SD-WAN is also only limited to delivering even binary performance data as it relates to the WAN between edge routers, giving no local perspective into additional issues taking place at remote offices. Without additional insight on the LAN at each branch location, centralized IT could be completely blind to performance issues that don't originate on the path over the Internet.

Performance monitoring to bridge visibility gaps

It's essential that teams seek out a performance monitoring solution that can account for all of the blind spots that come about with DIA, including the lingering visibility needs that SD-WAN only begins to account for.

At the very least, IT needs a tool that can measure performance hop-by-hop across each network pathway in order to unpack that binary "good/bad" response they receive from their SD-WAN regarding delivery speed. But solutions also need to go beyond seeing just between the edge routers at each branch firewall and into the actual end-user perspective, looking both at the WAN and the LAN.

Without that additional layer of insight, an SD-WAN may report that network connectivity is "good" when local impacts on performance may be impacted. A SaaS app may have no problem regarding delivery across the WAN, for instance, but issues with the app itself that are impacting users locally will happen in isolation from IT without additional local context.



Lumped into all of this is assuring that networks actually perform better at the end of the day than they did before IT teams overhauled legacy networks. This goes beyond just setting performance baselines throughout the process of redesigning the network, but employing monitoring solutions that can deliver visibility without exhausting network capacity on an ongoing basis.

AppNeta is a comprehensive solution that actively and passively monitors all network pathways — end-to-end, across the WAN and into the LAN to gain the user perspective — with minimal network impact. Other solutions may offer similar features, but they might sap up network capacity in the process, themselves playing a part in hindering network performance.

AppNeta is a low-overhead solution that can act as the eyes and ears on all corners of the network without burdening network capacity. To learn more about how, schedule a demo today to see how our solution delivers deep visibility into the experience of the end user, acting as a critical partner in any network redesign.

ABOUT APPNETA

AppNeta is the only network performance monitoring solution that delivers deep, actionable, end-to-end network performance data from the end-user perspective. With AppNeta's SaaS-based solution, IT and Network Ops teams at large, distributed enterprises can quickly pinpoint issues that affect network and business-critical cloud application performance, regardless of where they occur. AppNeta is trusted by some of the biggest Fortune 1000 companies, including 3 out of the 5 largest corporations in the world, as well as 4 out of the 5 largest cloud providers.

1.800.508.5233 | SALES@APPNETA.COM | APPNETA.COM