eBook

Network Intelligence Planning Guide

Insights on net neutrality, cloud readiness, security and WAN transformation

ThousandEyes

Table of Contents

The Net Neutrality Debate Shows There's No Such Thing as Steady State in the Cloud

by **Alex Henthorn-Iwane**
VP Product Marketing, ThousandEyes

One of the trickiest mindset shifts that business leaders have to make in the era of the cloud is understanding the highly unpredictable nature of the Internet as compared to other infrastructure systems on which they've historically relied. Recently, the FCC ruling to overturn what has become known in the U.S. as Net Neutrality has thrown open an impassioned debate over how the Internet should work. This is an important public policy debate for the U.S. for many reasons. However, for business leaders, it also highlights the need to recalibrate how they view the Internet and what their organization needs to thrive in an Internet-connected world. Given that businesses are increasingly reliant on the Internet, both as a source of revenue and as a platform for nearly every form of IT communication and enablement, this is a matter of existential importance.

The Internet is Not a Traditional Infrastructure

Modern businesses take advantage of numerous publicly funded or governed infrastructures such as roads and highway systems, shipping lanes, and traditional utilities such as power, water, telecommunications and mobile networks. All of these historical infrastructure systems are centrally controlled in some fashion and exhibit slow rates of change. That relative stasis creates a helpful level of predictability for business investment.

Even though information technology has long exhibited a much higher rate of change than any other business discipline, IT infrastructure has historically been built and operated on the utility model, with high degrees of control and slow rates of change. Dissatisfaction with the inability of this model to cope with rapidly shifting business demands and the desire for greater agility has driven cloud adoption. And cloud adoption has been predicated on a multi-trillion dollar, two decades long build-out of the global Internet.

Due to the maturity of the Internet build-out, the fact that so many traditional telecommunication carriers are intrinsic participants in the Internet, and because these telecommunications brands are the most visible face of the Internet to consumers, most people assume that the Internet is similar to other traditional infrastructures as mentioned above. However, that assumption is wrong.

The Internet is a Living Organism

The Internet is unlike centrally controlled and slow-changing traditional infrastructures. It is more like a living organism that is continuously and rapidly evolving in response to a variety of stimuli.

The Internet is at its core comprised of tens of thousands of independent organizational networks, bound together not by a central controlling authority or edict but because of a common goal: the free flow of information.

There is shared DNA within the Internet—the most essential being routing protocols that determined how traffic flow and the Domain Name System (DNS) that translates human-readable URLs into routable IP addresses. Yet most rules on the Internet are not centrally enforced and can be at least partially broken by some Internet participants without breaking the whole. Internet routing works on implicit trust between "peer" networks, which means that an accidental misconfiguration or malicious act can create chaos, such as when the Russian ISP Rostelecom hijacked the addresses of multiple financial services websites in 2017.

The structure of the Internet and how traffic flows across it responds to a variety of stimuli including the supply and demand for information traffic flows, capital investments in search of returns, and government policies—whether in the domestic or geopolitical realm. Given the vast scale of the Internet, the number of such stimuli occurring at any given time is large, and the precise effects are very difficult if not impossible to predict.

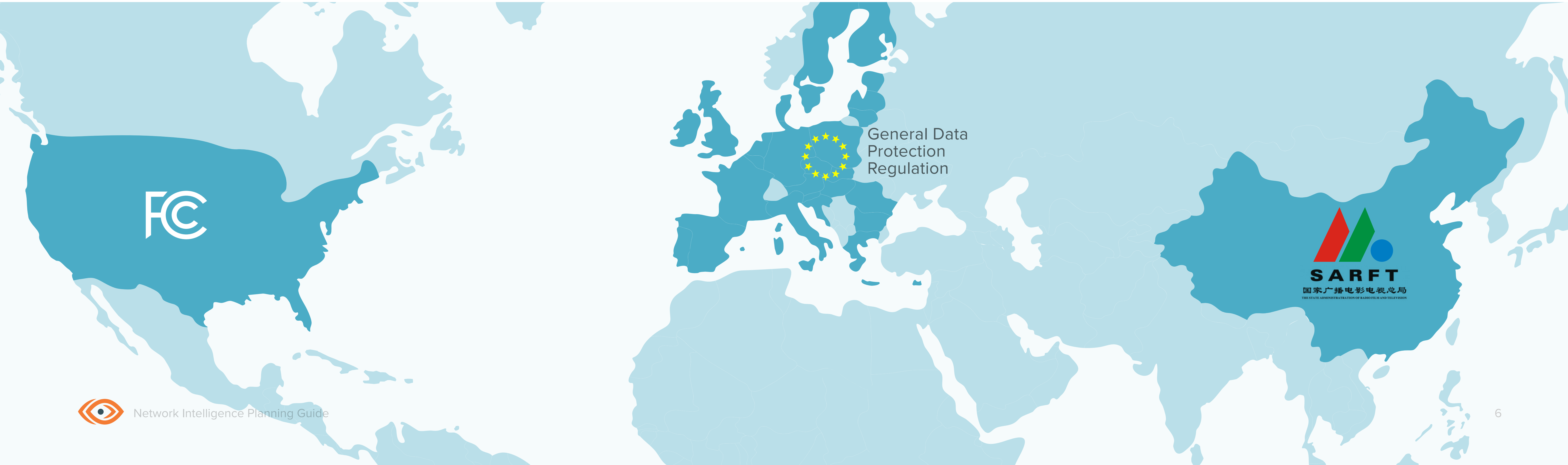
For example, carriers, ISPs, cloud providers, web enterprises, government agencies and educational institutions are continually updating and changing their network and data center infrastructures, as well as how their services operate. As they do so, all of these key players are continuously renegotiating contracts and setting up new paid or peer trading arrangements to carry traffic on behalf of one another. To draw on a traditional utility for an analogy, it's as if a water utility system was constantly relaying its pipes and where it pumps water from. There is no steady state in the cloud.

Policy Impacts on Internet Behavior

Aside from commercial stimuli, the Internet is also affected by public policies. For a long time, the trend in the U.S. has been towards supporting net neutrality—and regarding public opinion, that is still the dominant view. The possibility of the new FCC ruling taking effect has roiled the waters of the U.S. Internet scene because it introduces a whole new range of commercial possibilities for broadband providers based on differentiating content rather than treating all information traffic flows solely based on volumetrics. This could impact how various types of content, and particularly traffic that competes with home-grown services broadband provider offerings might be handled by broadband providers.

For online businesses, the impacts could include needing to pay extra for prioritized passage of web-based service traffic to customers connected to broadband networks. For mainstream enterprises, the impacts could include a change in how freely and flexibly broadband connections can be used for branch office Direct Internet Access (DIA) or replacement of MPLS circuits. Other impacts could be variable behavior or performance for home-based, remote or on the road employees trying to access business-critical cloud applications and services. As of the writing of this article, there are significant uncertainties on whether the FCC ruling will stand in the face of political opposition, and even if it does, how it will actually play out in practice.

The Net Neutrality change is not the only Internet-related policy that impacts business. For example, the advent of the European Union's General Data Protection Regulation (GDPR) means that corporations must now be very careful to ensure that European data is never transferred to data centers outside of the EU, or else they may face heavily punitive fines. In addition, the revelation of the breadth of the U.S. National Security Agency's exploits by Edward Snowden prompted many other governments to explore or even mandate that their Internet traffic flows avoid networks operated within the U.S. In China and other countries, alterations to how DNS and routing work to enforce politically motivated content controls often alter the behavior of Internet communications in unpredictable ways.


FCC
General Data Protection Regulation
SARFT
国家广播电影电视总局
THE STATE ADMINISTRATRATION OF RADIO FILM AND TELEVISION

The Need for Network Intelligence in an Unpredictable Internet

How do businesses deal with the unpredictability of relying on such a rapidly changing "organism" like the Internet? As with any unpredictable environment, visibility is critical to restoring control over the business outcomes that IT is responsible for.

The problem is that traditional network monitoring was built for networks, apps and services that are internally owned and controlled. Despite being useful data, it is simply not available from the Internet, including all the providers on which businesses rely. That's where Network Intelligence comes into play.

Network Intelligence refers to the data, technology, algorithms and techniques used to collect, analyze and visualize network information for the globally connected, digital world. The purpose of Network Intelligence is to optimize digital experiences everywhere, by understanding global network topologies, dependencies and behavior, and to support better IT decision making.

The FCC's repeal of Net Neutrality is an important public policy decision point. For businesses, the fact that the FCC could repeal a long-standing policy like Net Neutrality is a wake-up call to deploy Internet-aware Network Intelligence and regain control in the midst of greater reliance on the business-critical yet highly unpredictable Internet.

Cloud Readiness: Move Monitoring Left

by **Alex Henthorn-Iwane**
VP Product Marketing, ThousandEyes

In 2018, cloud migration will continue to pick up steam in enterprises. Most organizations are already using multiple SaaS applications, and multi-cloud and hybrid cloud architectures have become the de facto standard. According to Gartner, “in 2018, SaaS will become the dominant model for consuming new application software.”[1] Yet, too many organizations run the needless risk of encountering network performance issues with new cloud applications. Moving network performance monitoring and baselining left on your cloud migration project timeline is a critical element of cloud readiness and risk mitigation.

Move Monitoring Left

New Reality Bites

In the midst of planning cloud migration projects, it is easy for project teams to assume that the combination of new cloud apps and the Internet will "just work." This attitude stems from long-term experience with MPLS-based WANs that provided highly predictable performance characteristics supported by contractually enforced Service Level Agreements (SLAs). Development teams knew what to expect from the WAN and developed applications accordingly. Monitoring was typically an afterthought.

Those expectations no longer hold true in the cloud. SaaS applications are developed with different (higher) bandwidth assumptions in many cases, but more importantly the Internet is an unpredictable "new normal" communications environment that IT and cloud operations teams ignore at their peril. Take Office 365 as an example. Gartner found "20% of all organizations using Office 365 reporting service performance challenges and another 12% citing insufficient service availability. Based on Gartner inquiry findings, network issues are one of the leading causes, if not the foremost, of performance issues for Office 365. Consequently, through 2019, Gartner anticipates that more than half of all global-scale deployments of Microsoft Office 365 will experience network-related performance problems."[2]

ThousandEyes solutions and customer success teams have witnessed such network performance challenges first-hand with many organizations. An example is a Fortune 150 corporation that migrated its Microsoft Sharepoint application to the cloud. Previously, they had deployed SharePoint in their data center in the UK, with the expectation that the page load time for Sharepoint's home page from anywhere in the world should be 5 seconds. To achieve this goal, the network team deployed WAN accelerators to speed page delivery. However, when Sharepoint migrated to the cloud, the enterprise infrastructure solutions manager explained that the migration project team assumed that performance would be the same. "They did very limited testing from one location in the UK, so when the cloud migration was rolled out, employees began experiencing performance issues again." As a result, Sharepoint homepage load time increased to 20-30 seconds. In this case, it was a combination of network and application factors that contributed to the overall performance degradation.

Traditional Monitoring: More Hindrance than Help

Most large IT organizations already possess a portfolio of network and application monitoring tools. However, these tools are typically built for pre-cloud scenarios. Traditional network monitoring relies on passive data collection from network infrastructure devices such as switches and routers, via SNMP, packet capture, sFlow and NetFlow.

However, your team simply can't collect passive monitoring data from infrastructure owned and operated by ISPs, IaaS and SaaS providers. SaaS applications don't allow code injection, so many application performance management techniques such as Real User Monitoring (RUM), aren't applicable.

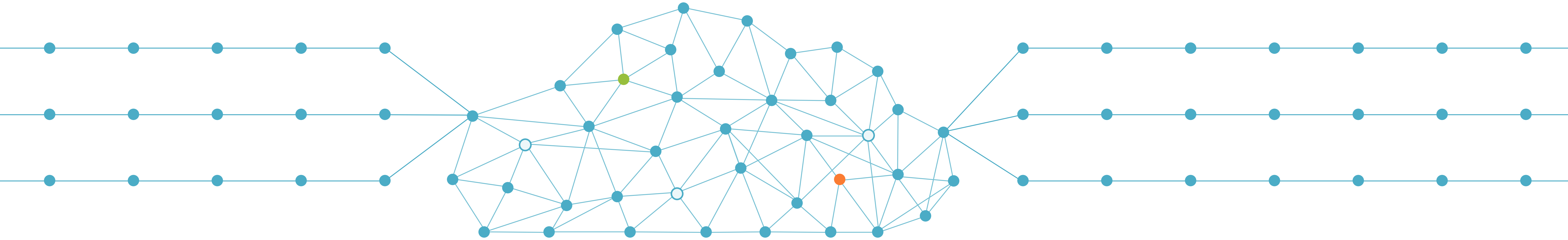
Not only does the ill-suitedness of traditional monitoring to cloud scenarios prevent project teams from proactively baselining performance to check upfront assumptions, the lack of actionable data hinders you from performing effective remediation work after projects encounter problems in the field.

Network Intelligence and Cloud Readiness

Network Intelligence refers to the data, technology, algorithms and techniques used to collect, analyze and visualize network information for a globally connected, cloud-oriented and Internet-centric world. Network Intelligence leverages a combination of active and passive monitoring techniques that provide insight into the linkage between cloud app and service performance, user experience, and underlying network topologies including the Internet. For example, Network Intelligence exposes information like page load and detailed web transaction timing and links that performance to underlying Layer 3 paths and hop-by-hop network performance metrics. With Network Intelligence, you can see the end-to-end performance of a SaaS provider from branch office sites, plus visualize complex paths from each site via multiple ISPs, through a secure web gateway (SWG) provider PoP, and ultimately through the SaaS network to the service instance. Network Intelligence allows IT and cloud operations teams to measure, monitor, baseline, troubleshoot and perform root cause analysis of cloud performance issues.

Know Before You Go

To avoid surprises and de-risk cloud projects, IT organizations should deploy Network Intelligence capabilities at the front end of their cloud migration timeline. It is advisable to obtain at least a month of performance data using active monitoring transactions from all branch sites to see if performance expectations can be reliably met, or find out if remediation steps need action ahead of rollout. Furthermore, at least a month should be allocated before deployment to perform service escalations supported by collected monitoring data. This period provides a performance baseline on which cloud operations SLAs can be built and communicated to all providers on which the user experience depends. Creating Network Intelligence-powered dashboards for operations teams, internal client organizations and service providers establishes a single point of "truth" to help service escalations and inter-team coordination proceed as rapidly as possible after rollout.



2018 Security Trends and Network Intelligence Implications

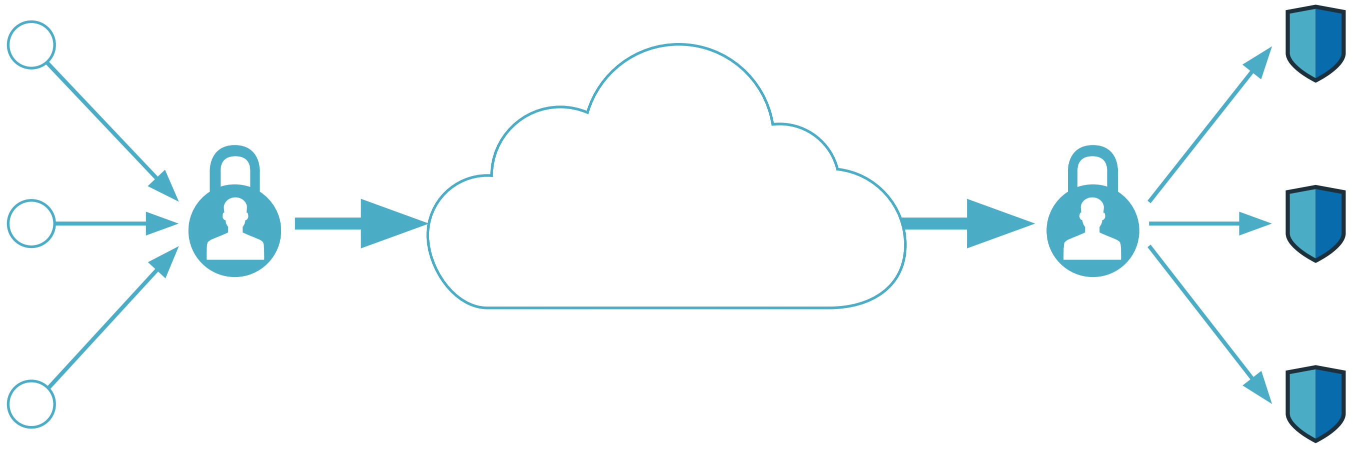
by **Alexander Anoufriev**

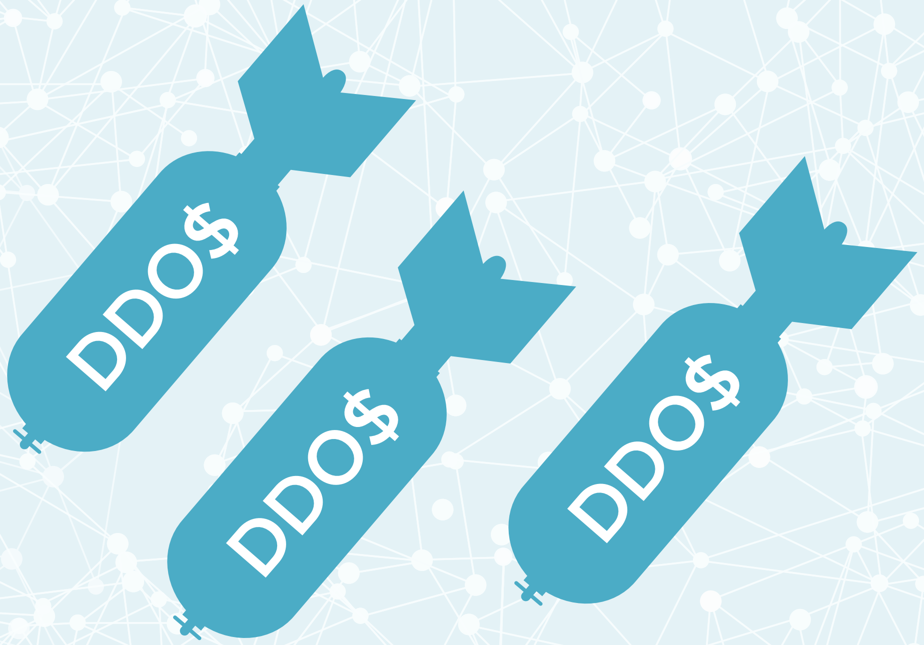
Chief Information Security Officer, ThousandEyes

Every year, security professionals must assess critical areas in which to make investments to ensure the integrity, confidentiality and availability of their organization’s information. However, this assessment doesn’t happen in a security-only vacuum. With business processes, systems, suppliers and partners increasingly interconnected via the Internet; there are substantial implications for and dependencies to master in the realm of Network Intelligence. Here are some key themes for 2018.

Strong Authentication and SAML

As businesses continue to move their IT applications and services into the cloud, one of the most critical security processes—authentication and authorization, now happens over a potentially unreliable and insecure medium: the Internet. When all services were located in a datacenter, users were connecting either directly from an internal network or over the Internet via VPN or reverse proxy technologies. Now that services are shifting to the cloud, users access the application over the Internet; they are instructed to authenticate using their company's Internet-facing identity provider; then they are redirected back to the application. It is essential not only to understand this change in the authentication process but also to be ready to plan for its implementation with reliable network performance data—specifically data on latency and end-to-end network paths. Those who perform baseline measurements of their network performance in relation to the authentication process before and after the shift to the cloud will notice a dramatic difference in both latency and paths, and they will be ready to set proper expectations and find service providers (both for network and applications) who can deliver the best results.





DDoS and Cyber-Crime Automation

DDoS attacks increased during 2017 and will continue to do so into 2018, facilitated by the growing number of insecure IoT devices, hacktivist activities and state-sponsored attacks. Before starting to plan a new deployment or improvements of DDoS mitigation services, companies should identify what their normal traffic is, set this as a baseline and monitor for deviations. Also as businesses continue moving from on-premises DDoS mitigation appliances to always-on, cloud-based services, such baselines will demonstrate not only the effectiveness but also the efficiency of a specific technology and chosen provider as compared to others. For an end-user, the service availability through mitigation is very important; they don't want to lose access to the network and services nor modify their settings. This could be validated by the service owners continually monitoring the availability of protected networks before, during and after an attack. To ensure the availability and consistency of routing information, businesses must exercise DDoS mitigation tests as part of their disaster recovery testing and capture all network-related data in their Network Intelligence platform for future reporting and analysis.

Network Intelligence applications allow you to define critical web application transactions, establish a performance baseline, compare the performance of this transaction to the SLA and report on all deviations.

The End of Vendor Trust

Wherever there's a lock, there's someone trying to get in. Even if you've accounted for and checked your own locks for proper operation, now you have to do the same for all your vendors. Four years after the Target breach, the importance of vendor management is still rising. For example, as part of European Union's General Data Protection Regulation (GDPR) Article 28(2) requirements, companies now have to not only disclose a list of their vendors who process Personally Identifiable Information (PII) (processors) but also request approval from their customers (controller) if any changes are planned for implementation in the vendor landscape. How can Network Intelligence help to reestablish trust? Trust, but verify ("Doveryai, no proveryai"). Establish verification procedures that would enable both sides to monitor compliance with the promised or expected service level agreement (SLA). Network Intelligence applications allow you to define critical web application transactions (for example login, purchase order entry, and logout), establish a performance baseline, compare the performance of this transaction to the SLA and report on all deviations. Sharing this data with your vendors on a monthly basis will help them to improve network and application performance and stay accountable for overall results.

Regulatory and Board Oversight

Information security and risk management are becoming an essential part of the management responsibilities for a company's board of directors. GDPR requires the Data Protection Officer to report to the highest management level within the organization. How do boards manage information security and privacy risks? They need to rely on qualitative or quantitative analysis provided by different sources, including business intelligence applications (or Network Intelligence in networking environments). For example, a company's network reachability during a DDoS attack with Vendor A may be 99.999% while Vendor B provides only 99.8%. Likewise, Vendor X may be able to complete a specific transaction within 3 seconds while same transactions take 5 seconds for Vendor Y. Obviously, the board of directors does not need this level of detail; however, they need to make sure those details exist, are available to and are being reviewed by their respective teams/owners. The board will rely on high-level dashboards with overall security and privacy risk status and compliance data.

Network Intelligence Supports Security Goals

A Network Intelligence platform can help security professionals manage information risks in more efficient ways:

Monitor and predict availability of critical network and application security resources like authentication and authorization portals

Learn from other companies regarding DDoS mitigation strategies and compare vendor performance

Compare network and application performance for defined business transactions across multiple systems and suppliers

Bring up valuable security metrics to the level of company’s board of directors

Internet-Centric Monitoring for Real-Time Intelligence in Cloud-Centric Enterprise WANs

by **Stephen Collins**
Principal Analyst, ACG Research

The Cloud is Transforming Enterprise WANs

Three dominant trends are driving business and IT transformation in the modern enterprise: rapid adoption of cloud-based applications and services; pervasive Internet connectivity; and widespread user mobility. These trends are extending the scope and increasing the complexity of traditional enterprise wide area networks (WANs), forcing enterprise IT managers to employ new tools and techniques for gaining real-time insights into the performance of public cloud applications delivered via a hybrid of public and private network connectivity.

The migration of enterprise IT applications to hybrid multi-cloud environments is shifting the center of gravity for network managers from traditional enterprise WANs and private data centers to the Internet and public clouds. Figure 1 depicts the emerging model for cloud-centric enterprise WANs. On the left is a diverse mix of end-users—employees, customers and partners—situated at many sites and locations. In the center are public and private networks: traditional WANs based on carrier services; the Internet, comprised of access, backbone and content distribution networks; and enterprise SD-WAN virtual overlays that utilize a hybrid of traditional WAN and Internet connectivity. On the right are multiple public and private clouds for delivering applications and services.

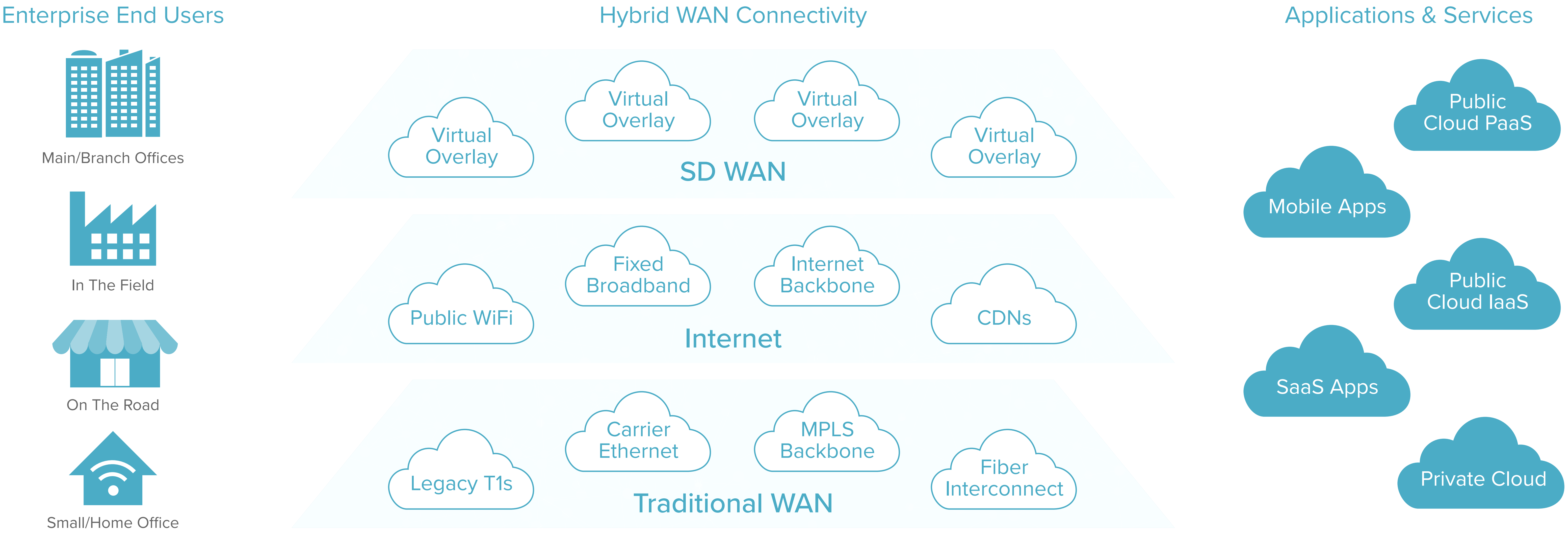


Figure 1 – Cloud-Centric Enterprise WAN for Hybrid Multi-Cloud Applications

The Challenge of Ensuring Quality of Experience for Cloud Applications

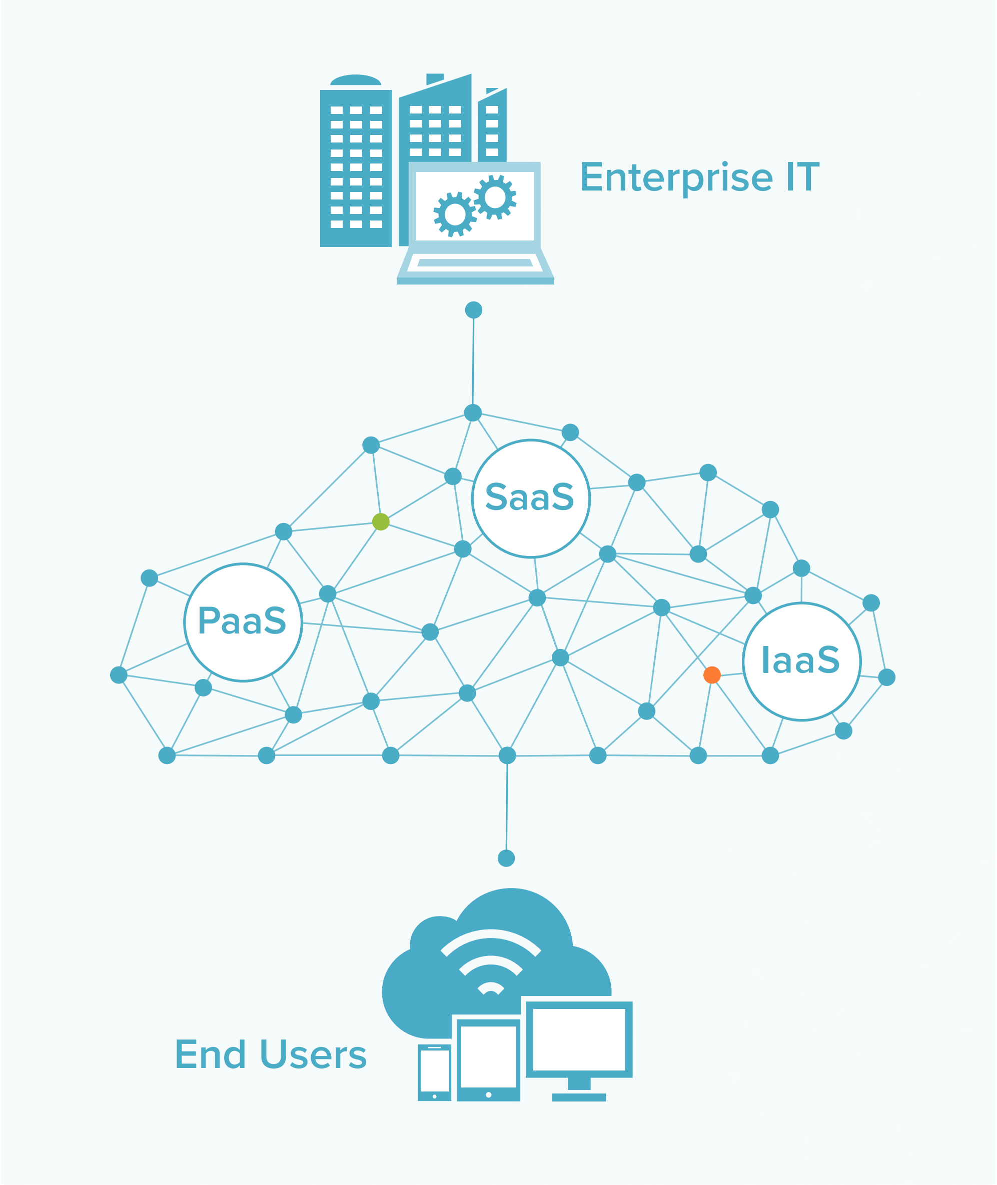
The overarching challenge for enterprise IT managers in this complex hybrid multi-cloud environment is ensuring end-user quality of experience when application traffic flows traverse virtual and physical networks spanning multiple domains: enterprise, carrier, Internet and cloud. Traditional enterprise WANs have evolved to incorporate multiple services: T1, Ethernet and 4G/LTE access; carrier MPLS backbones; direct fiber connections; and IP VPN overlays. The adoption of software-defined networking in the wide area has also enabled enterprise SD-WAN virtual overlays for dynamic routing of traffic over a blend of traditional WAN services and Internet connections based on application policies defined by security, bandwidth, latency, jitter and packet loss requirements. SD-WANs incorporate Internet connectivity for cost-effective WAN access from remote sites and for breakout connections from the WAN to common SaaS applications such as Salesforce and Office 365.

In the extended, cloud-centric enterprise WAN, users of cloud-based applications simply expect them to work. That means IT managers are on the hook for ensuring end-to-end performance and user quality of experience, even though the enterprise doesn't own or control much of the supporting network and application infrastructure. Enterprise IT managers need to apply tools and techniques for expanding the scope of application and network monitoring beyond the infrastructure the enterprise owns and operates. These tools will enable DevOps and NetOps teams to rapidly detect and identify problems impacting application performance caused by conditions in public network and cloud infrastructure outside of their direct control.

Managing application and service performance is further complicated by the distributed nature of cloud-based applications in which a single user transaction may invoke APIs for multiple services spanning multiple clouds. In addition, container-based run-time frameworks for microservices architectures are highly dynamic, spinning containers up and down on-demand, driven by workload requirements. As a result, application monitoring involves tracking a moving target and discovering the dependencies between services invoked within an application.

In terms of cloud providers, the hybrid multi-cloud environment is distributed and diverse. There are multiple leading providers offering Platform-as-a-Service and Infrastructure-as-a-Service, with data centers located across multiple continents. Many SaaS applications are based on public cloud services, but some are deployed from dedicated data centers. The trend is that many large enterprises rely on an array of business-critical applications delivered via multiple clouds distributed geographically across continents.

A final complicating factor is that the population of end users for enterprise IT applications has grown dramatically to encompass mobile and remote users, including employees, partners and large numbers of customers for enterprises embracing digital transformation. These users typically rely on Internet access from fixed and mobile service providers to reach cloud-based applications over connections that may traverse a hybrid of public and private networks. Integrating Internet access as a key component of the cloud-centric enterprise WAN places a premium on the ability of enterprise IT managers to rapidly detect and isolate Internet connectivity problems on the access side, in addition to the cloud.



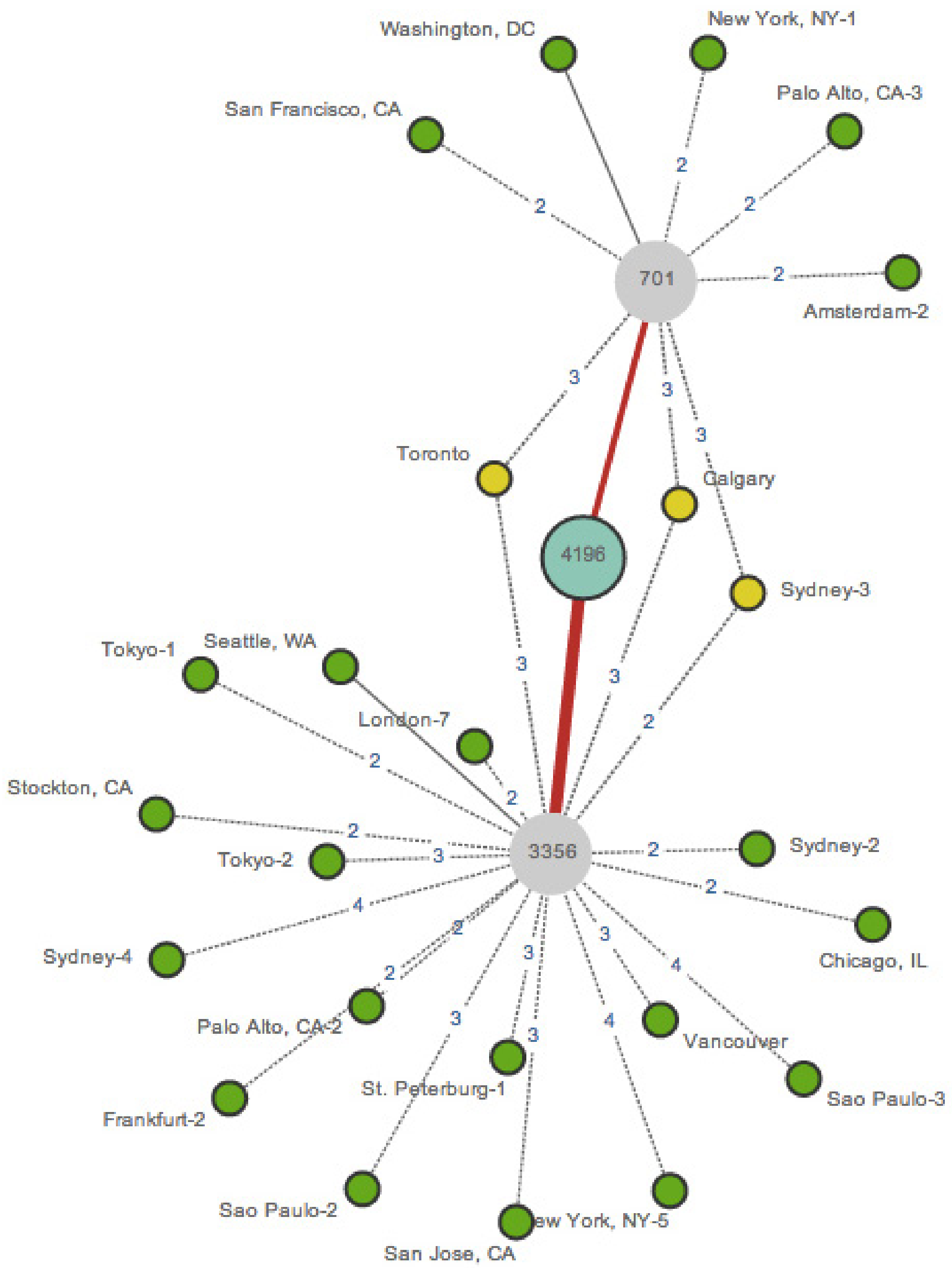
Active Monitoring for Internet and Cloud Performance Management

The monitoring tools and techniques that have served network managers well for years were not designed for visibility into network infrastructure not under the IT manager's direct control. Enterprise network management has been historically centered on passive monitoring techniques, such as gathering statistics using SNMP; analyzing packet data collected by passive probes; and capturing packet streams for offline analysis. Recently, passive monitoring is incorporating streaming telemetry for real-time intelligence, including flow metadata from switches and routers capable of exporting sFlow, NetFlow and IPFIX records. All of these techniques still retain validity and have their place in a well-rounded network management tool stack.

Within the borders of a traditional enterprise WAN, passive monitoring can effectively maintain an accurate view of network health and then quickly detect and isolate problems because it is straightforward to instrument and monitor network infrastructure that the enterprise owns and controls.

However, in the cloud-centric enterprise WAN, monitoring needs to be expanded to incorporate synthetic monitoring techniques for tracking application performance in the cloud, combined with active monitoring techniques for probing end-to-end connections through the underlying network infrastructure. Specifically, diagnosing performance problems in the cloud-centric WAN requires fine-grained, hop-by-hop monitoring of individual links along the entire network path from user to application, inclusive of Internet and cloud provider links that don't allow passive monitoring. For this, enterprise network managers are now employing active and synthetic monitoring.

Active network monitoring has been around a long time, but was largely confined to hardware probes used to test network connections for latency, jitter and packet loss, particularly to support voice and video applications. These approaches required that probes be deployed at both ends of the communication path, typically enterprise office or data center locations.



Web developers have long employed synthetic monitoring techniques to measure website performance and optimize end user page behavior based on web, application and database server performance. This type of monitoring is typically automated and script-based and periodically exercises web pages for various click streams while measuring round-trip performance end-to-end.

In the cloud-centric enterprise WAN, continuous synthetic monitoring of applications can be used to rapidly detect problems when they arise. It's important that synthetic monitoring be initiated from agents that are situated proximate to user populations. The growth of remote users and the importance of digital business customers using customer-facing websites and applications means agents are required in locations far afield of enterprise offices.

Synthetic monitoring can then be coupled with a combination of techniques to yield details of the precise network path for each user to application traffic flow. One such technique is active monitoring of the Internet path at the IP layer, which requires the agent to send and receive certain sequences of packets over TCP connections that terminate at intermediate points along the affected network path—segment by segment—from end user to application. This yields insights into latency, jitter and packet loss on a hop-by-hop basis. A further and more sophisticated technique involves integration of passive monitoring of BGP routing data to track the current network path and the networks it is traversing.

If a performance anomaly is suspected, then active monitoring at the IP layer can be used to isolate the specific link or network element that is the root cause. Active monitoring might also involve performing DNS queries and measuring response time or performing end-to-end monitoring of VoIP sessions to measure VoIP call quality.

Synthetic and active monitoring solutions today are mainly software-based, and involve deploying intelligent agents throughout the cloud-centric enterprise WAN: in user endpoint devices; in network infrastructure at primary data centers, branch offices and remote sites; and in the cloud.

Leading active monitoring vendor ThousandEyes also deploys software agents in over 150 co-location facilities that are distributed worldwide and serve as a proxy for enterprise end users located in those cities. Critically, for synthetic and active monitoring solutions to work for the cloud, they must be able to gain the aforementioned visibility without requiring deployment of agents on both ends of the communication path. The simple reason being that IT teams will simply not be able to deploy agents in SaaS datacenters.

Active monitoring is full stack, operating at multiple layers: applications and services; the supporting application infrastructure; and in multiple layers across the underlying networks. Active monitoring also spans multiple domains end-to-end from user to application: enterprise, carrier, Internet and cloud. The optimal approach for active monitoring is to test continually on a periodic basis that is frequent enough to quickly detect problems but not so often as to consume excessive network and application bandwidth.

New Monitoring Tools Needed for Hybrid Multi-Cloud Applications

Digital transformation and powerful economies of scale are driving the migration of enterprise IT applications to hybrid multi-cloud environments characterized by a new cloud-centric enterprise WAN that is a hybrid of traditional WAN services and Internet connectivity. IT managers now own user experience, whether they own the networks or not. Ensuring end user quality of experience in these environments requires enterprise IT managers to employ new tools and techniques for monitoring end-to-end application performance and gaining real-time visibility into the underlying network infrastructure across multiple layers and domains. Complementing passive monitoring techniques, synthetic and active monitoring are emerging as important techniques for managing the performance of applications and services delivered via the Internet from the cloud.

> IT managers now own user experience, whether they own the networks or not.

Learn More

Hundreds of leading organizations around the world utilize Network Intelligence to gain critical insights into digital experience, application delivery and network performance. ThousandEyes customers include 5 of the top 6 U.S. banks, 8 of the top 10 global software companies, 18 of the top 20 SaaS providers, 50+ of the Fortune 500 and 90+ of the Global 2000.

To learn more, read the "Guide to Network Intelligence" and explore further information resources including real-world user case studies and videos.

ThousandEyes
201 Mission Street, Suite 1700
San Francisco, CA 94105
(415) 513-4526

www.thousandeyes.com

References

1. Gartner "2018 Planning Guide for Cloud Computing," Cancila, Toombs, Waite, et al, September 2017.

2. Gartner "Network Design Best Practices for Office 365," Neil Rickard, Andrew Lerner, Bjarne Munch, December, 2017.

About ThousandEyes

ThousandEyes delivers performance visibility from every user to every application over any network, enabling you to successfully migrate to the cloud, modernize your WAN and deliver exceptional digital experiences.