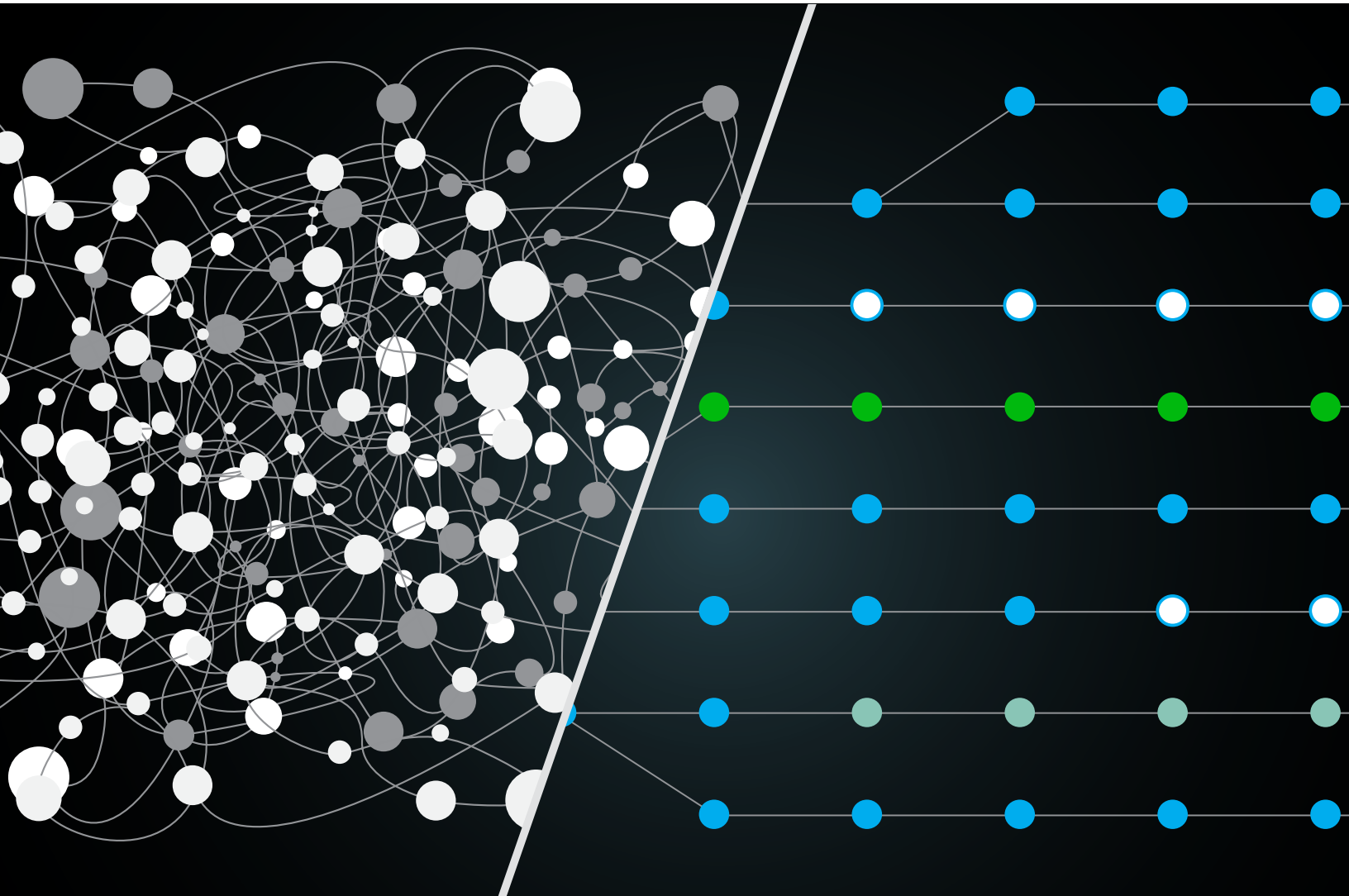
ThousandEyes

The Evolution of Network Monitoring
From Data Center to Cloud

White Paper



ThousandEyes

White Paper

Summary

In the last 10 years we've seen a radical change in the way applications are delivered in enterprise environments. Mobile devices such as phones and tablets as well as thin clients have begun to replace traditional workstations and desktops. Most enterprises are far along the process of virtualizing bare metal servers and consolidating them into centralized data centers. And entire classes of applications that used to be in the data center are now served from the cloud, including CRM, email and IT ticketing systems.

The enterprise data center that used to be the hub for application delivery is now just another segment in the application delivery chain. The cloud has become the new hub, connecting myriad clients to an ever growing number of SaaS applications. Network monitoring technologies that worked in the 2000s, most of them clunky boxes, now have a diminished role in this new paradigm. Current environments are much more complex, diverse and distributed, and require a new way to do network monitoring.

"ThousandEyes has become one of the key tools in our operations center for troubleshooting network and application performance problems."

Ivan Batanov
VP Engineering
ServiceNow

servicenow

10 Years Ago: The Data Center as the Hub

The network enterprise architectures of a decade ago were simple. Employees in branch offices and campuses used workstations to access applications hosted in the enterprise data center. Branch offices connected directly to data centers through point-to-point T1 links. When connection to the Internet was required, traffic flowed through data centers with centralized security services to upstream Internet Service Providers (ISPs).[1] Critical applications were all deployed on-premises, often requiring a heavy investment in hardware. These applications were siloed, rarely interacting with other applications and/or the Internet (Figure 1).

In this environment, most of the network flows only had to travel a small number of hops on the journey from the client to the server. This made fault isolation easier since:

- the number of hops traversed by packets were few
- network traffic stayed within the same administrative domain
- clients were static, mostly workstations connected through wired Ethernet cables

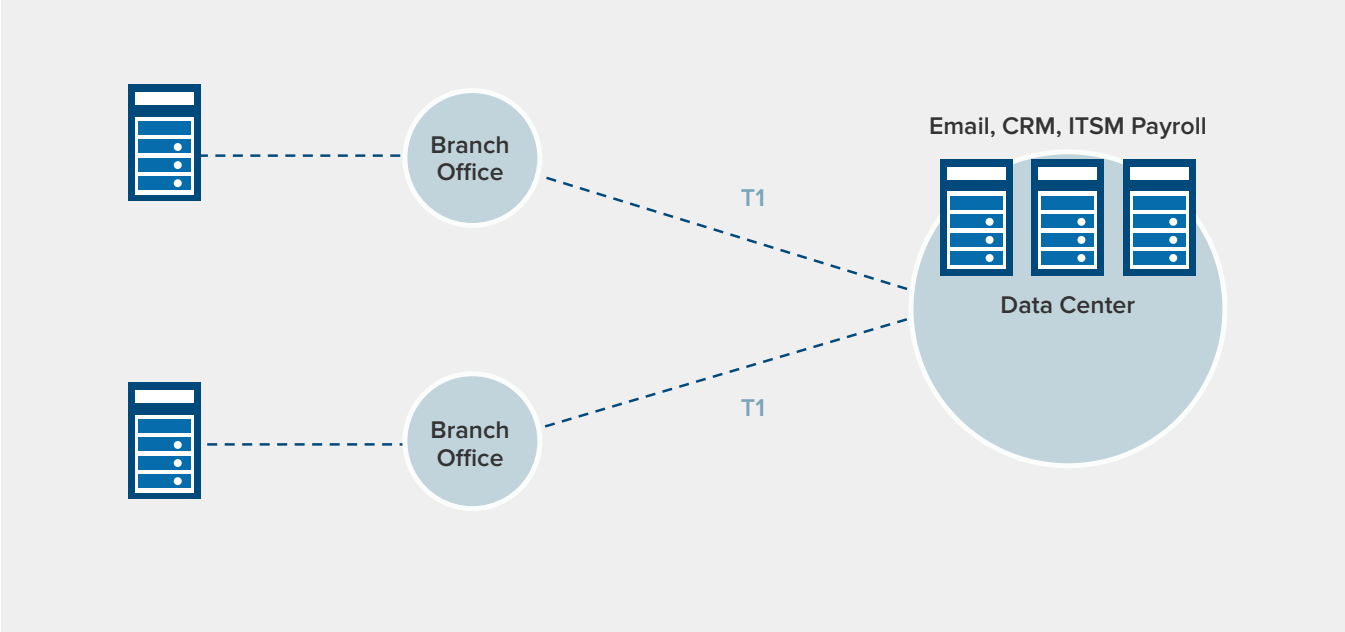


Figure 1: Enterprise network ten years ago

1 Gartner, April 2013. Optimize Enterprise Networks to Improve SaaS Performance.

Legacy Network Monitoring

Even though application flows were simpler in the enterprise networks of a decade ago, the monitoring solutions themselves were hard to use and install. Legacy solutions required multiple hardware boxes to cover an enterprise network, at least one per data center. Configuring and provisioning the monitoring instances was difficult because of the lack of centralized management. Deployment required multiple engineers over several weeks and was capex intensive. Software upgrades, including bug fixes, had to be deployed manually by the customer.

These solutions worked in silos, lacking correlation between data sets and network segments, making network troubleshooting a daunting task. SNMP-based solutions provided a network device-centric view of the network, not necessarily aligned with application performance.

For example, if a switch interface went down, an alert would be triggered, even if there was no critical traffic passing through the interface. This type of device-centric alerting gets very noisy and detached from real application performance. In most cases, network engineers had to manually correlate the end-to-end performance inferred from traffic analysis, such as Netflow, with per-device data provided by SNMP, often involving different vendors.

One of the main drawbacks of these solutions was the lack of application context. The main metrics reported were mostly related to the network (packet loss, latency, jitter), lacking the correlation to the overlaying application. This type of alerting creates high levels of noise because the same application can have sessions with dozens of flows and network level issues are not always perceptible to the application user.

Today: The Cloud as the Hub

Fast forwarding to today, the picture of the enterprise network is radically different. Applications are more frequently hosted in consolidated data centers or by external SaaS and IaaS vendors. Application users, both employees and customers, now rely heavily on mobile

Network Monitoring Primer

Network monitoring solutions come in different variants depending on what they measure and how they collect the data:

- **Active Probing:** service-centric approach that collects data based on synthetic measurements such as ICMP Echo Requests, HTTP GET requests or specially crafted packets. Often these measurements are trying to measure properties of the network that would be impossible to capture from pure passive measurements and are arguably the only way to measure service availability.
- **Device Polling:** device-centric approach that queries devices typically using SNMP (Simple Network Management Protocol), collecting interface status information, traffic volumes, device load, CPU, etc.
- **Flow Collection:** solutions that collect traffic information from network devices such as routers/switches; traffic is aggregated in flows using e.g. Cisco Netflow and stored in disk for post-analysis. Flow data it's easier to analyze and process than packet data, but provides less granular information.
- **Packet Analysis:** usually involves a SPAN port from a switch or a network tap and extracts information from individual packets, including information from payloads through DPI (Deep Packet Inspection).
- **Log Analysis:** solutions that collect machine-generated data typically in the form of log files (e.g. syslog) and present a query interface to correlate events across different types of systems, e.g. routers, web servers, load balancers.

> "ThousandEyes provides us with the unique ability to understand complex network issues that impact the performance of our customers' applications. Our customers can not only react to problems faster but also improve their network architectures to optimize global performance."
>
> **Brian Lille**
> *CIO*
> *Equinix*

EQUINIX

devices. And network architectures are changing to adapt to increasing bandwidth requirements and narrower budgets. A much more complex enterprise network has emerged, with the Internet at its center (Figure 2).

More Complex, Cloud-Based Applications

Applications that were hosted in the data center are now increasingly served in the cloud by SaaS providers. Recent surveys show that 75% of enterprises are investigating or using SaaS applications and 48% are investigating or using IaaS to host their applications.[2] The most common SaaS applications in enterprises are HR (Workday), CRM (Salesforce), email and collaboration (Office365).[3]

Applications are now much more complex and dependent on multiple third-party components. The number of requests per webpage increased 28% to 96 requests from 2010 to 2014 while the total transfer size increased 150% to more than 1.8MBs.[4]

Clients Are Mobile and Can Be Anywhere

For a world dominated by workstations, end devices now include mobile phones and tablets (Figure 3). By 2017, Gartner predicts that more than 40% of enterprises will encourage the use of personal mobile devices and more than 70% of professionals will conduct work on them.[5] Forrester currently finds that 48% of workers use a mobile phone and 21% use a tablet for work, with high rates of use at home, while traveling and while commuting.[6] Employees increasingly telecommute from their home office, with nearly 20% of Americans reporting working from home.[7]

Mobile devices typically connect to the enterprise network using WiFi or via the Internet from mobile carriers. Telecommuting employees most often connect directly to the corporate network via Internet and their local ISP, or work from public WiFi hotspots. These changes in application hosting and consumption have led to a new network architecture (Figure 4).[8]

The Rise of Internet Traffic

According to Cisco, 70% of business IP traffic currently crosses the Internet and 6% of that Internet traffic traverses mobile networks.[9] In most cases, enterprises still backhaul traffic through the corporate data center via VPN tunnels. Cloud providers are commonly accessed from the Internet; few enterprises have created dedicated connections to their SaaS or IaaS vendors (Figure 5).[10]

To improve scalability and network capacity, most enterprises have replaced T1 point-to-point circuits with multi-hop MPLS WAN (Figure 6).[11] Still others have begun to implement WAN optimization controllers such as Talari or Aryaka or WAN hubs such as Equinix (Figure 7).[12]

2 PCConnection, 2013. Cloud Survey Results
3 Forrester, May 2014. Application Adoption Trends: The Rise of SaaS
4 HttpArchive from November 15 2010 to July 15 2014
5 Gartner, April 2014. Defining BYOD Ownership and Support Expectations in Contracts Ensures Successful Implementation. Gartner, November 2013. Containing Mobile Security Risks with the 80/20 Rule.

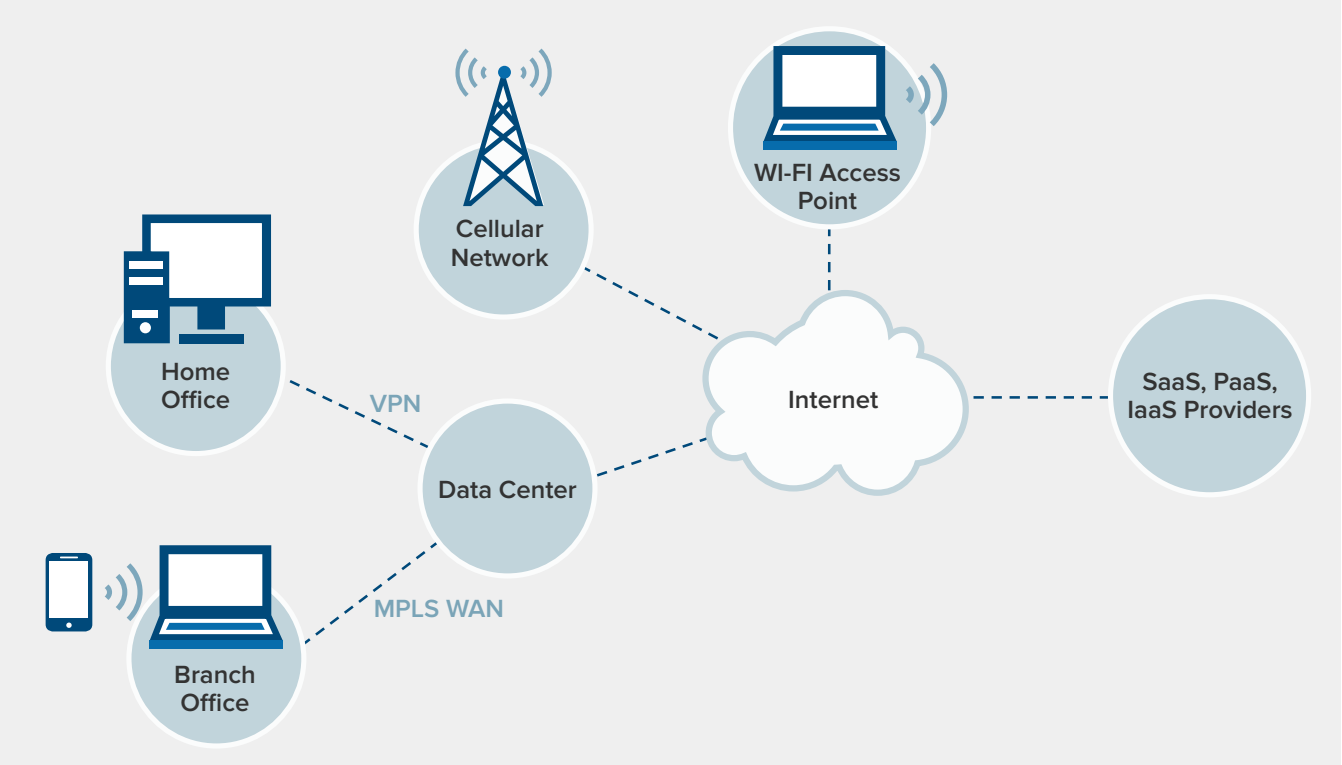


Figure 2: Enterprise network today.

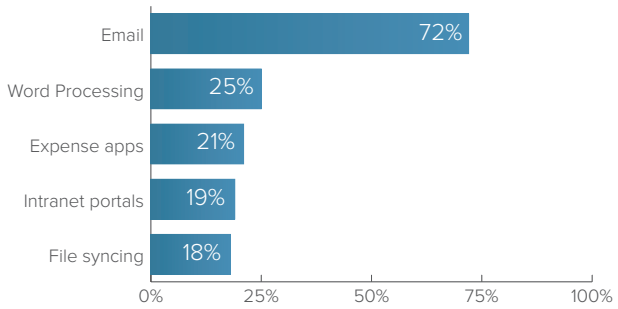


Figure 3: Most commonly used enterprise apps on mobile devices

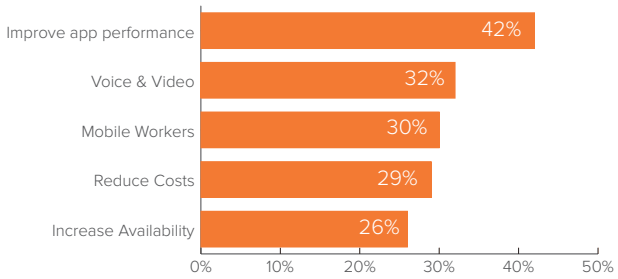


Figure 4: Top factors impacting WAN implementations over the next three years

Losing a Grasp on the Network

Network monitoring solutions from 10 years ago are no longer suitable for this new environment where application endpoints, both clients and servers, can be anywhere. Network paths are now much longer and complex, and include segments out of control of the enterprise domain (Figure 8).

Network fault isolation for modern enterprise environments requires visibility beyond the four walls of the data center and can only be achieved by multiple types of instrumentation. This includes instrumentation of client devices, the corporate data center and the Internet. Modern network monitoring solutions need to be application-aware and able to single out underlying problems that actually impact user experience. This is a major difference over monitoring solutions from the past that missed application context and only provided visibility into the network layer or over individual devices.

6 Forrester, February 2013. 2013 Mobile Workforce Adoption Trends
7 Forbes, February 2013. One in Five Americans Work from Home, Numbers Seen Rising Over 60%
8 Ashton, Metzler & Associates. The 2014 State of the WAN Report.
9 Cisco Visual Networking Index, June 2014.
10 Ashton, Metzler & Associates. The 2014 State of the WAN Report.
11 TechTarget, May 2011. T1 Circuit or MPLS Network: How to Choose.
12 NetworkWorld, September 2011. Enterprise WAN connectivity: MPLS VPN vs. Public Internet. Gartner, May 2014. Communications Hubs Improve WAN Performance

The shift in monitoring techniques is being accompanied by an expansion in the scope of responsibilities of network operations teams. In the past, most teams would argue that fixing services that traversed the Internet is largely beyond the control of Operations teams. And in the case of SaaS applications, isolating network faults or service degradation outside the corporate perimeter was treated as the job of the SaaS provider. However, with more and more critical services traveling across the public Internet and being served up in a SaaS model, more and more operations teams are taking on responsibilities to track down issues outside of their own environments.

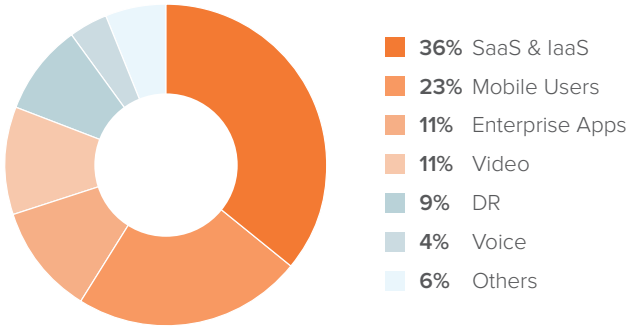


Figure 5: Biggest drivers of increasing Internet traffic

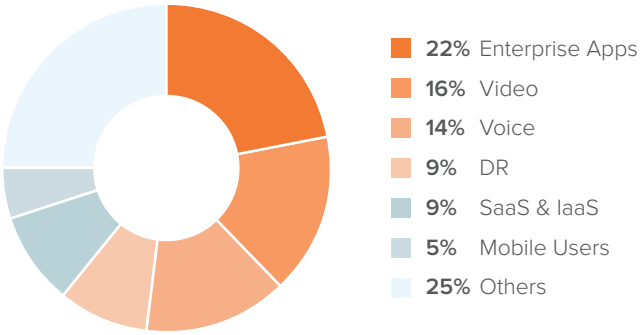


Figure 6: Biggest drivers of increasing WAN traffic

Combining Monitoring Techniques for Broad and Deep Visibility

Passive monitoring has long been used in enterprise network environments. Techniques such as SNMP polling, packet capture, log file analysis and flow monitoring are important to discover and provide diagnostics on users and devices in the local

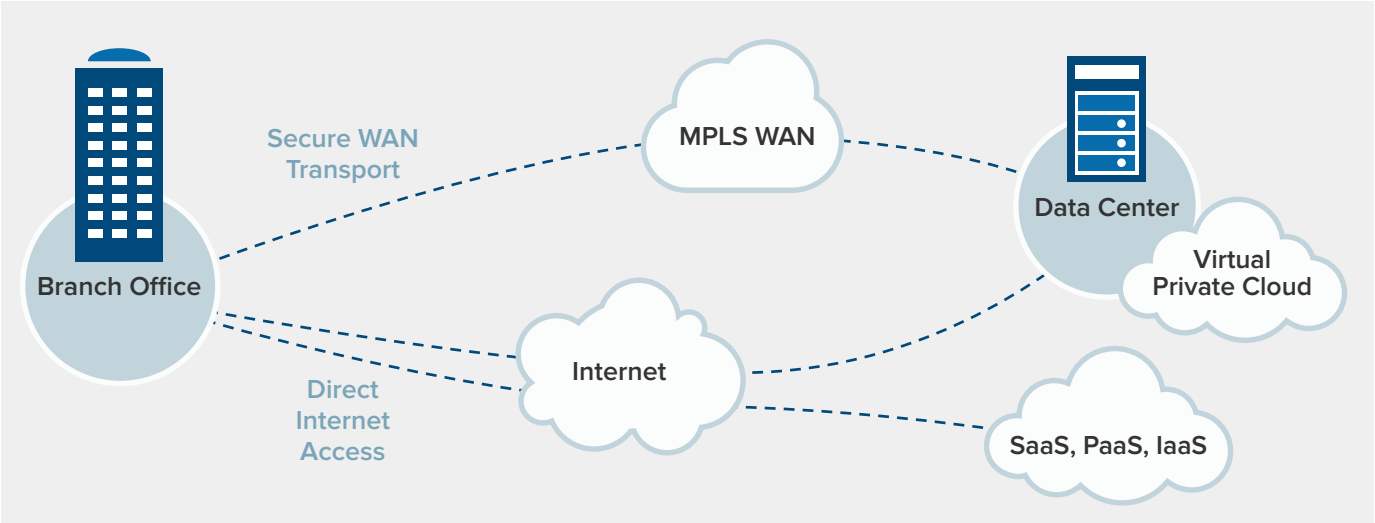


Figure 7: Changing network topology due to WAN optimization and hubs

> "ThousandEyes has provided us with visibility into global network status that we haven't found with other tools. Easy analysis of BGP state changes and full path visualization tools have routinely reduced our troubleshooting time and resulted in real answers as to what happened."

Steve Loyd
Director of Operations
Zendesk

zendesk

environment. They can also be used to better understand the actual user experience. However, passive monitoring often falls short when proactively detecting availability issues, reproducing issues for troubleshooting or offering visibility outside of the local environment.

Active probing has become a key monitoring technique to provide a complete hop-by-hop picture of performance between clients and servers, or among clients. Using active tests makes it easier to detect issues quickly, reproduce issues and troubleshoot in external environments. Because the root cause of problems can be anywhere along the path, the troubleshooting process does not depend only on the enterprise team anymore, but is rather a joint effort that also involves ISPs, third-party IaaS providers and SaaS application providers.

In combination, active and passive techniques provide complementary functionality and coverage for monitoring and troubleshooting. These two techniques extend visibility within and outside the enterprise network, enable detailed forensics and make it possible to proactively resolve network faults and degradation.

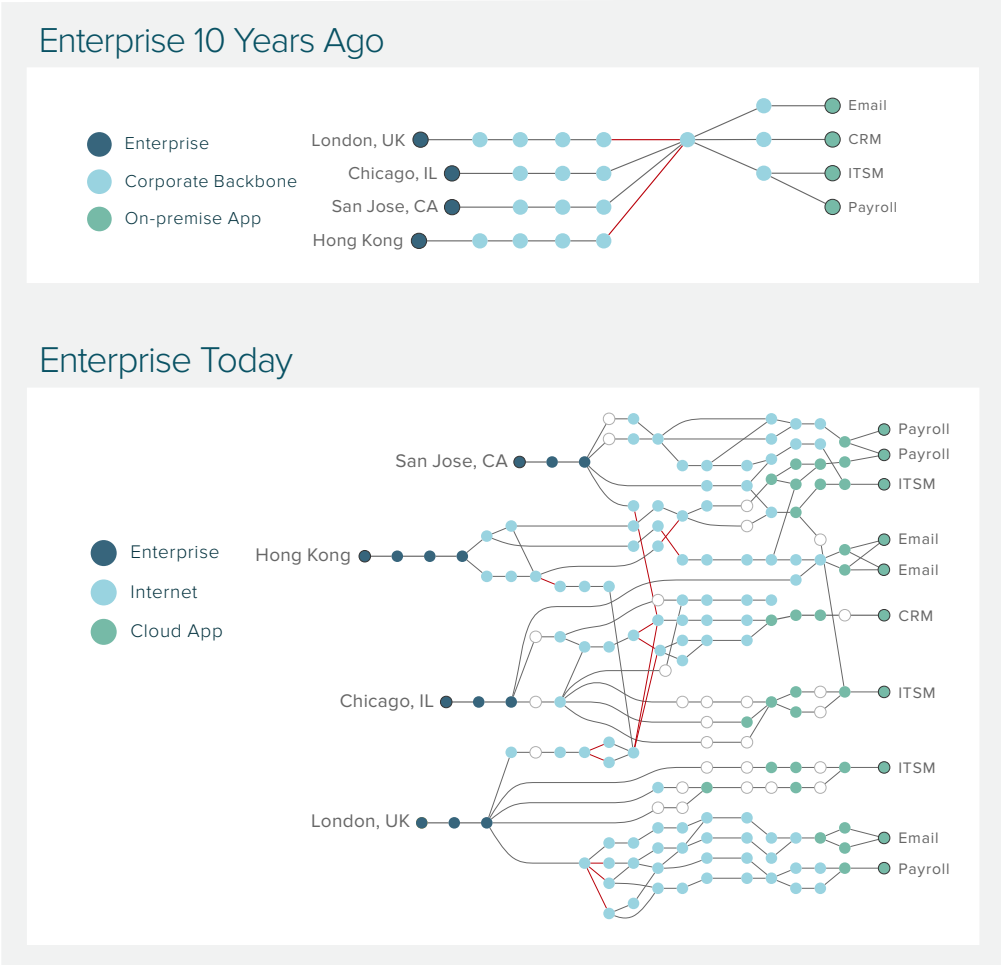


Figure 8: Network paths are more complex than ever

A New Way to Do Network Monitoring in the Cloud

In the same way that the focus of application delivery shifted from the data center to the cloud, modern network monitoring solutions need to become cloud-based themselves in order to catch up. Monolithic monitoring solutions that lived within the four walls of data centers fall short in capturing the highly distributed nature and complexity of the modern enterprise. Even though instrumentation is still required in the branch and/or data center, this is mostly in the form of “dummy“ collection agents that pre-process the data and export aggregates to be processed elsewhere. This approach brings multiple advantages including centralized management, better support, faster and more frequent version releases, and easier deployment.

Capability	On-Premises Solutions	Cloud-Based Solutions
Data collection	Mostly traffic captured in DC or SNMP polling of devices	Distributed collection agents covering endpoints, branch, DC and cloud using a mix of active and passive measurement techniques
Application metrics	Limited , especially with encrypted traffic	Application-aware and tightly integrated with network layers
Data sharing & collaboration	Siloed and lacking sharing capabilities	Enabled in the cloud
User interface	On-premises, often per network segment	Cloud
Management (collection, user access, configuration)	Per instance local config	Centralized cloud management
Local environment discovery	Mostly manual input from the user	Auto-discovery
Software updates	Local, manual trigger	Frequent auto-updates

Putting New Monitoring Techniques into Practice

For most organizations that have already invested in on-premises monitoring tools, the next few years will be transitional, with increasing use of cloud-based monitoring. Consider evolving your network monitoring technologies when:

- Adopting new SaaS applications such as Salesforce, Office365 and RingCentral.
- Rearchitecting your network, lessening use of MPLS circuits, consolidating data centers or implementing WAN hubs.
- Implementing BYOD or telecommuting policies among your employees.
- Replacing existing monitoring appliances that require major capex commitments.

This shift will first focus on additional visibility into external networks and distributed applications. A second wave of change will come as on-premises systems reach their end-of-life and are replaced with new, lighter weight cloud-based solutions for troubleshooting, traffic analysis and packet inspection.

Learn more about cloud-based monitoring solutions for that give you visibility across networks at www.thousandeyes.com.

ThousandEyes

201 Mission Street, 17th Floor
San Francisco, CA 94105
(415) 513-4526

www.thousandeyes.com

About ThousandEyes

ThousandEyes is a network intelligence platform that delivers visibility into every network your organization relies on, enabling you to resolve issues faster, improve application delivery and run your business smoothly.