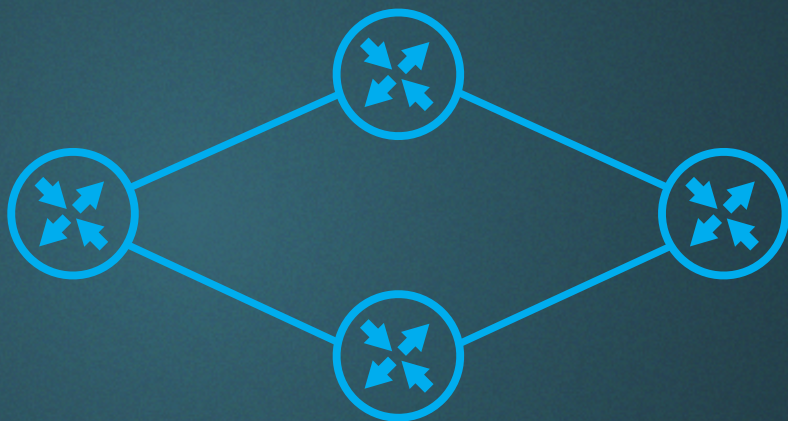


ThousandEyes for Enterprise

WAN and LAN Monitoring

ThousandEyes





Introduction

Enterprise network architectures have been changing rapidly over the last few years. Trends such as BYOD, telecommuting, server and desktop virtualization (VDI), VoIP, SaaS and Wi-Fi adoption bring new challenges and requirements to the underlying network infrastructure that connects branch offices and data centers. Dedicated MPLS circuits are now being replaced by shared infrastructure, the Internet. As more employees work remotely and applications get virtualized and more distributed in nature, the pattern of network access is changing from high-speed/low-latency LAN access to a low-speed/high-latency WAN access. As the Internet becomes the WAN backbone, Software-defined-WAN (SD-WAN) is gaining popularity. SD-WAN provides the flexibility to choose the most optimal transport and dynamically steer traffic over hybrid access networks.

These trends have resulted in reduced cost, faster service deployment, increased flexibility and improved application performance. However, it brings along some unique challenges. As traffic traverses multiple networks and third-party infrastructure, blind spots are more common. An infrastructure-agnostic, intelligent monitoring solution that can tie together service- and network-level data, providing a unified end-to-end view of user experience, will be critical for the Internet-centric enterprise.



Challenges in the Internet-Centric Enterprise

Each technology trend brings new challenges, creating newer approaches in the realm of network monitoring.

Responsibility without Ownership. Increased reliance on third-party networks has been the combined byproduct of different technology trends. SaaS adoption, telecommuting and 'cloud' data centers all rely on using the Internet as the network backbone. Traditional WAN architectures had most traffic staying inside the enterprise. Network and IT teams triaging problems had full control over the physical devices and the software applications. However, as increasing volumes of traffic go through the public Internet, those same IT teams are still responsible for managing application and service delivery. Troubleshooting routing changes or packet loss in peering and transit ISPs that invariably affect your employee's productivity is an arduous task.

Diverse Access Networks. As telecommuting becomes increasingly popular, there is a lot of variation in how remote users connect to data centers. While broadband internet is the underlying transport, IP/VPN and IPSec-based connections are common. Wi-Fi has surpassed Ethernet to become the ubiquitous mode of connectivity in the LAN. While it is the most convenient, it is definitely harder to debug. Bad quality 802.11 wireless access in the branch office is a common cause for application performance degradation, caused by interference or physical distance between the client and the access point. This is often a hard element to troubleshoot end-to-end since there is typically no access to this information without instrumenting the client or the access point.

Limited Visibility into Cloud Services. As enterprises adopt Infrastructure-as-a-Service (IaaS) and boost their SaaS consumption, application performance does not only depend on what happens inside the corporate network. Data traffic has to cross multiple third-party networks in the public Internet before being delivered to the end user. Troubleshooting a sluggish Office 365 or Salesforce login becomes challenging when you don't own the application or the underlying transport. Applications like voice and video, that are extremely sensitive to loss and latency, are now being delivered over the 'cloud' further complicating troubleshooting.

"The shift of employees to a telecommuter role gives us new challenges as we are delivery services over the public Internet, over a network we do NOT control."

Ivan Shepherd
Sr. Technical Manager
AIM Specialty Health



Heightened Expectations of User Experience. Telecommuting trends are skyrocketing with corporate employees no longer restricted by physical or geographical boundaries. Remote teams can access in-house applications by connecting directly to the data center via IP/VPN or can access SaaS-based applications like Office 365, Salesforce directly through the Internet. Bring-Your-Own-Network is a reality where IT and Network Engineers are tasked with providing the same flawless user experience irrespective of where an employee is connecting from. This causes an increase in the number of IT support tickets because of a gap in network visibility when it comes to managing third-party networks and end user experience.

Implementing New Hybrid Network Architectures. As SD-WAN drives the next generation of enterprise architecture, it is critical to benchmark and baseline the network for application performance and optimal user experience. Backhauling traffic from branch offices to the data center can create performance challenges for SaaS applications, increasing round-trip times. Local break-out from branch offices through upstream Internet Service Providers (ISPs) is another option. If maintaining SLAs and fast resolution during failure is critical, then backhauling traffic in spite of higher latency might be the best approach. Under such circumstances, a distributed data center model might be beneficial. Irrespective of the SD-WAN technology and path-determination algorithms that are dynamic, end-to-end visibility from a network and application perspective is important at all times.

Network Intelligence: Erasing the Blind Spots

Recognizing the problems of the modern enterprise, ThousandEyes' Network Intelligence platform bridges the gap in traditional network monitoring and visibility. Through a combination of vantage points ThousandEyes delivers visibility into every network the internet-centric enterprise relies on. Smart agents deployed across the Internet, enterprise and end-user laptops or desktops reveal network topologies, dependencies and behavior. Intuitive visualizations-powered by correlating application, network and routing layer data-vastly reduce mean time to resolution.

Monitoring the WAN and LAN with ThousandEyes

ThousandEyes has developed two vantage points from within the enterprise and one from outside the enterprise network to address the issues discussed earlier (Figure 1).

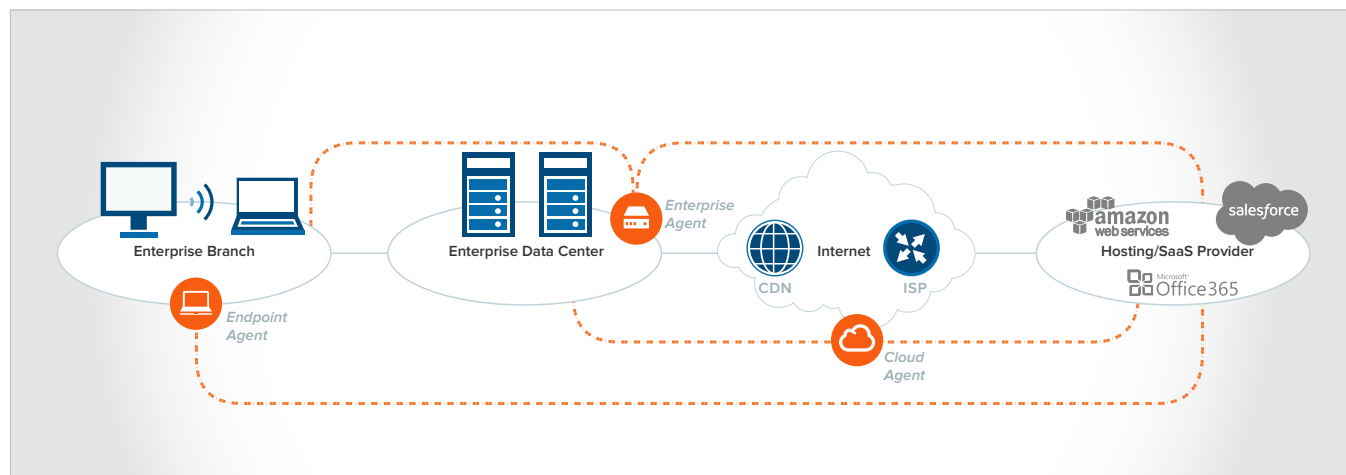


Figure 1: ThousandEyes Agents provide multiple vantage points to monitor the WAN and LAN

Enterprise Agents: Enterprise Agents are software appliances that probe the network at regular intervals to determine the health of infrastructure and performance of key applications. Available as virtual appliances, Linux and Docker containers, these agents perform periodic measurements to targets configured by the user. Targets might include internally hosted web-servers, SaaS applications like Salesforce.com and DNS servers. Data collected through these tests can be viewed across the application layer like HTTP or Voice and be correlated to network metrics like loss, latency at the same time. They are most commonly installed in branch sites and data centers to provide a detailed understanding of WAN and Internet connectivity.

Endpoint Agents: Endpoint Agents are deployed on end user desktops and laptops running Windows and OSX, extending visibility all the way till the end user. They bring a new way to measure user experience and collect network diagnostic data from all parts of the corporate network, as well as external networks employees use to access critical services. Endpoint Agents are software, installed on the OS and as a browser plugin so that Help Desk and Network Operations teams can easily solve application delivery issues with live data from end users and correlate delivery issues across the LAN, WAN and Internet.

Cloud Agents: Similar in functionality to Enterprise Agents, Cloud Agents are the third type of vantage points. Owned and maintained by ThousandEyes, these agents are geared towards solving the challenges faced by the enterprise but from an external perspective. They reside in Tier 2 and Tier 3 service provider networks and provide visibility into DNS servers, internally or externally hosted applications and also monitor your enterprise network during DDoS attacks.

Data without analysis is just wasted potential. Visual analysis capabilities bring together diverse data sources to give you meaningful new insights.

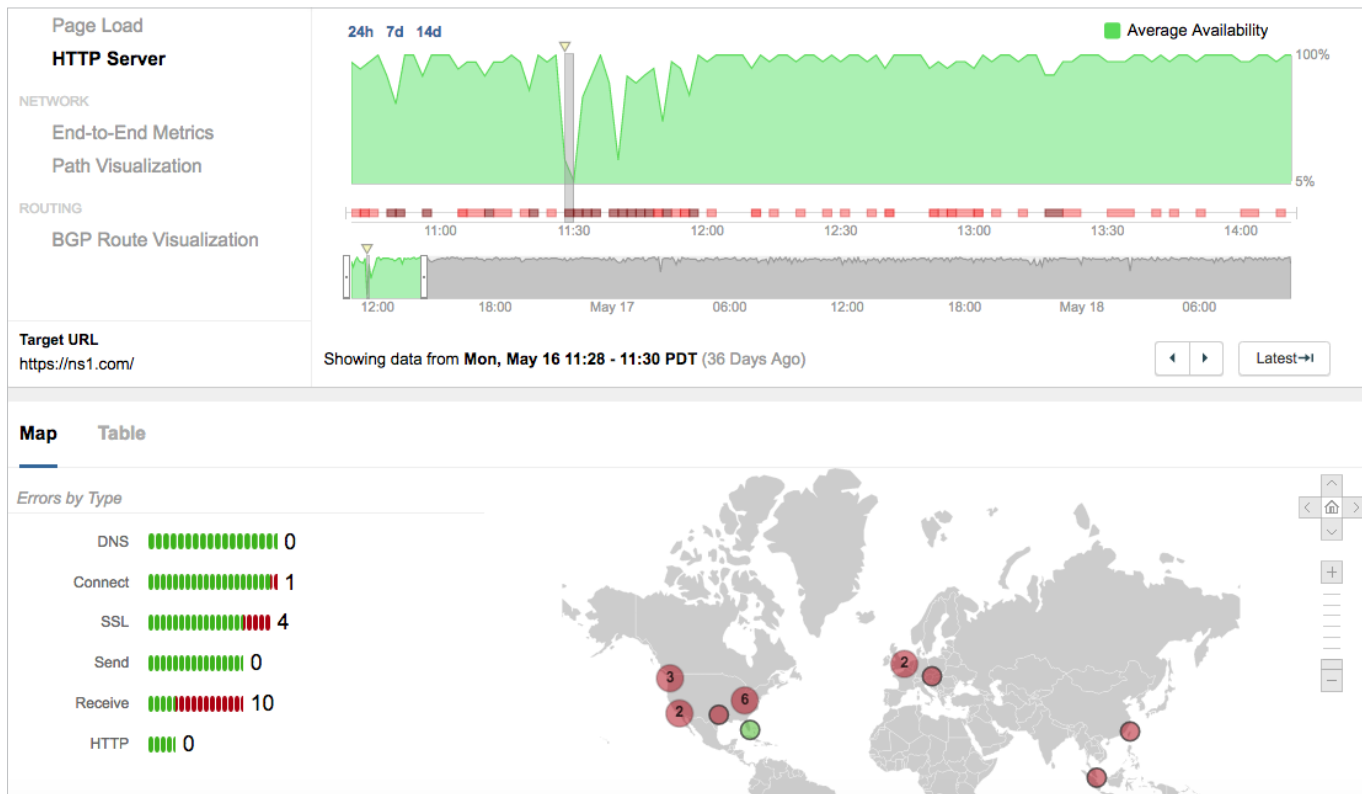


Figure 2: HTTP Server layer visualization indicating a drop in server availability and agents impacted (in red)

Solving The Challenges

Take Back Ownership: Any Network, Any Access, Any Application

Enterprise and Endpoint Agents send specially crafted network packets—TCP, UDP and ICMP—to map traffic paths and measure the performance of links and interfaces along the path. Path Visualization maps the internal WAN and external Internet, providing a hop-by-hop view of network performance. In parallel, Enterprise Agents also measure availability and response times of a variety of applications (HTTP, HTML pages, VoIP and FTP) irrespective of whether the application is hosted internally or in the cloud (Figure 2). Enterprise Agents also provide detailed visibility into MPLS networks including MPLS labels and DSCP markings, as shown in Figure 3. When deployed in a full mesh capacity, Enterprise Agents can map the entire WAN network.

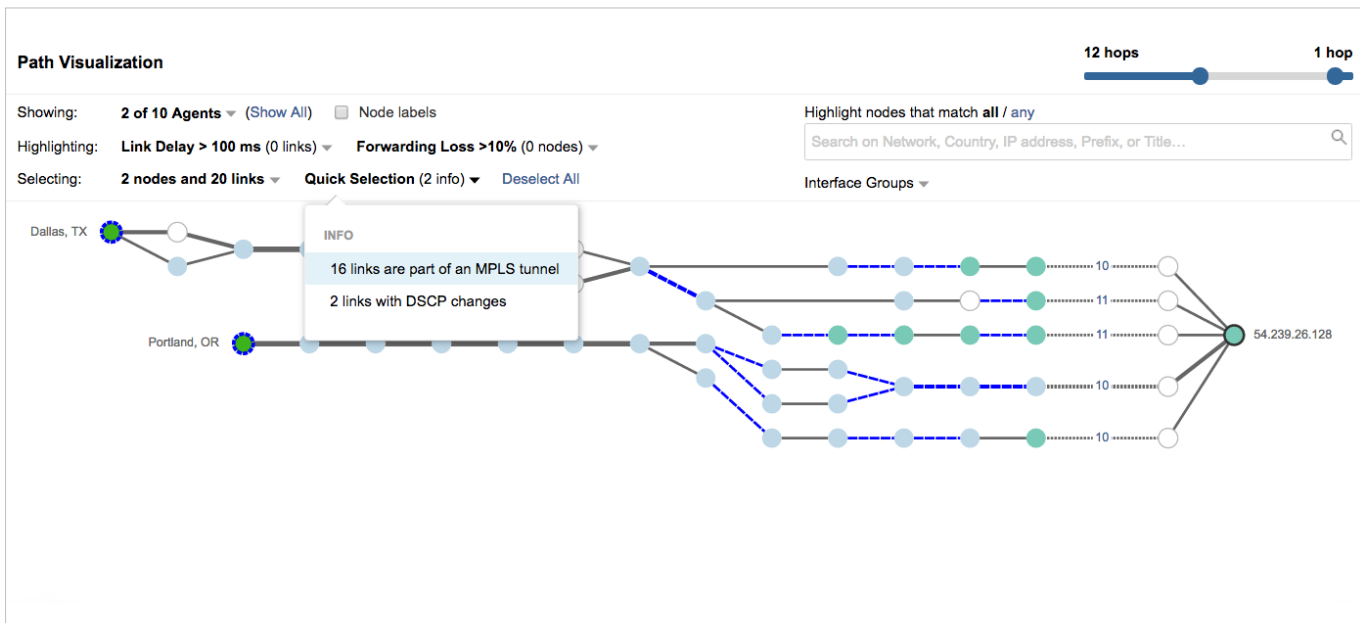


Figure 3: Visualize MPLS tunnels along with network measurements like loss, latency in your WAN

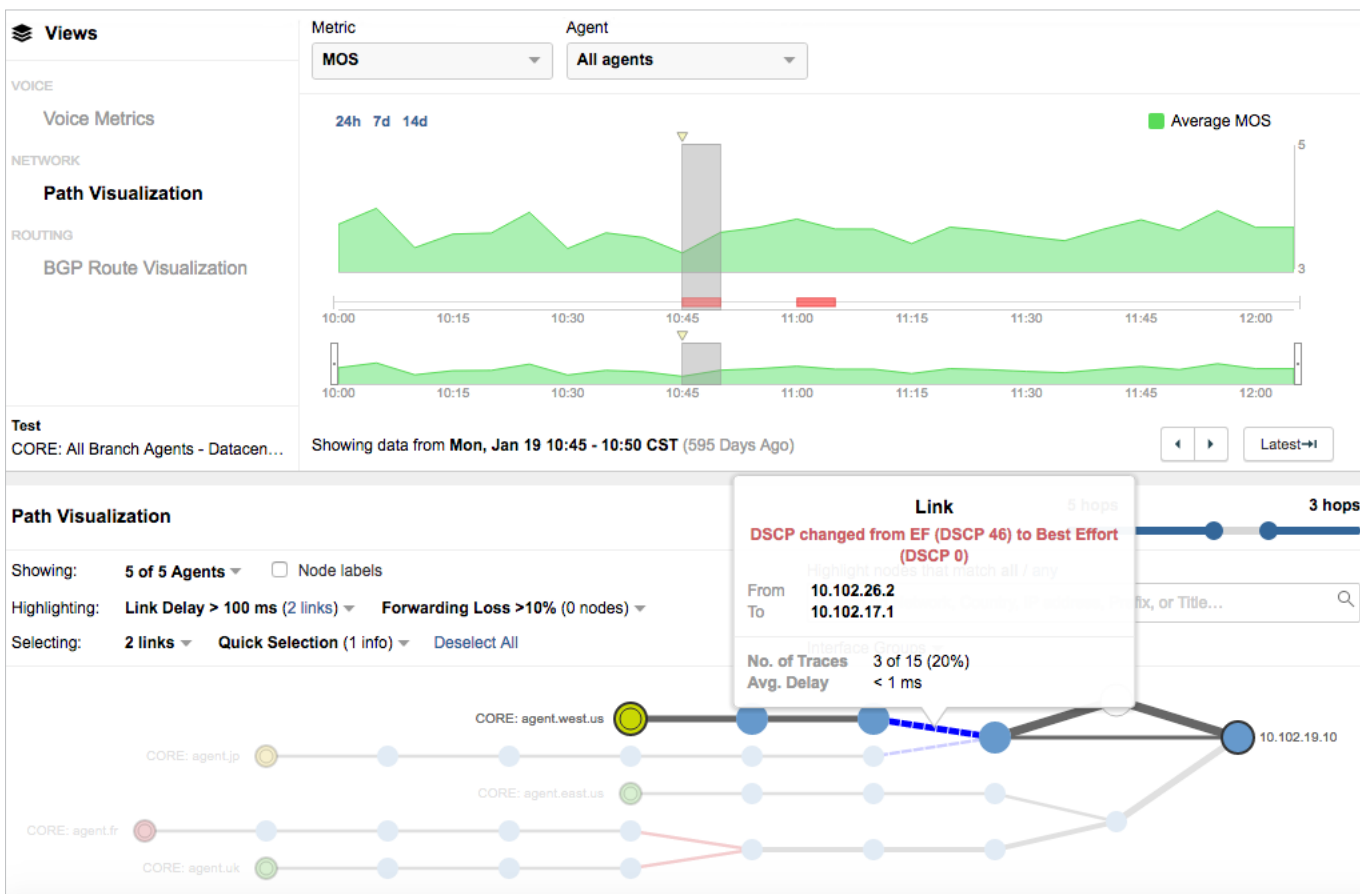


Figure 4: DSCP re-markings in VoIP traffic from a branch office to a data center

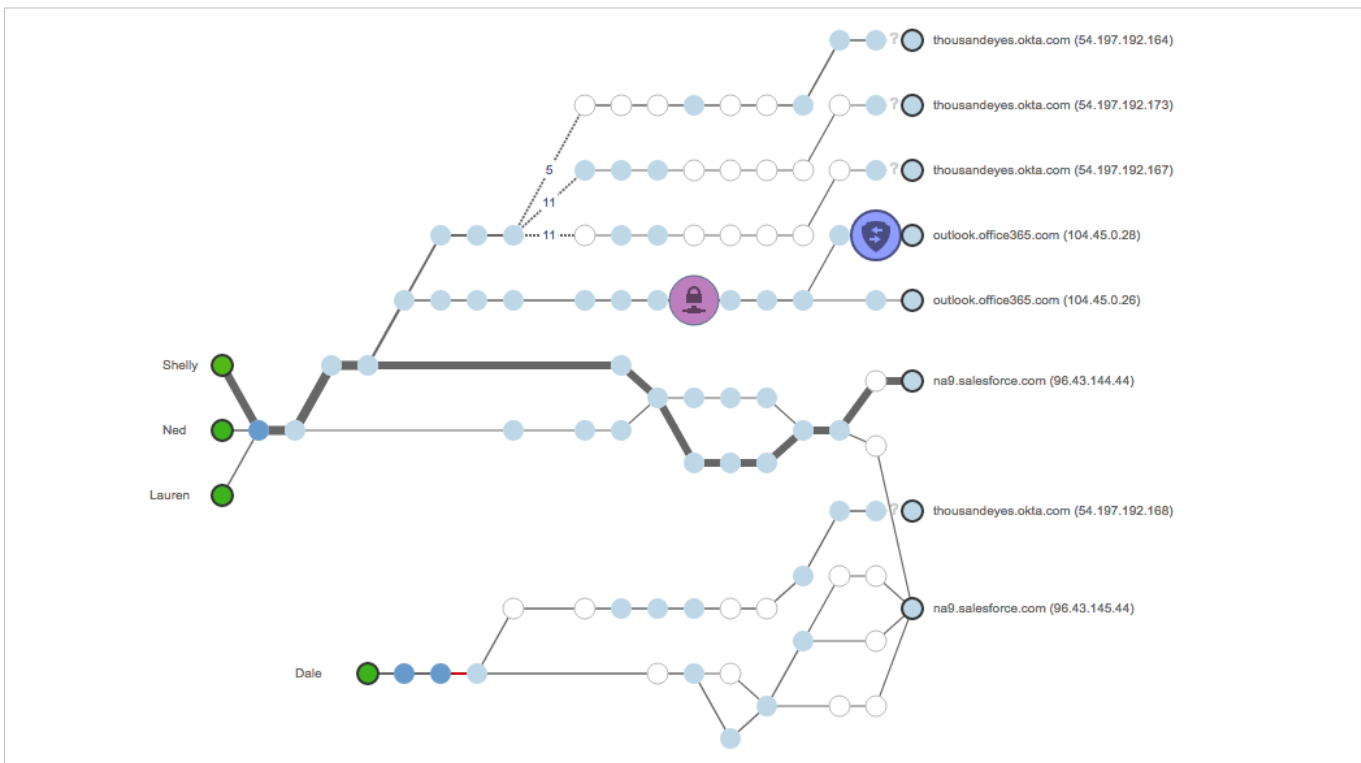


Figure 5: Endpoint Agents show network connectivity from the end user to a browser-based applications like Okta, Salesforce and Office 365

Monitor on-premises, hosted or UCaaS voice applications by instrumenting voice tests that show loss, delay, MOS and quality of service performance across the WAN and the public Internet (Figure 4). Leverage Endpoint Agents to track performance and user experience of browser-based internal and external applications, including Salesforce and Office 365. They make it possible to analyze hop-by-hop connectivity across the LAN, WAN and even the public Internet from each employee. And they can also measure performance of proxies, VPN gateways and access points along the path (Figure 5).

Know what Your SaaS Application Is Doing

Do not be in the dark when it comes to monitoring your SaaS applications anymore. Enterprise and Endpoint Agents can work in conjunction to triage SaaS performance by providing deep application visibility combined with network-level insights, including the performance of ISPs. Monitor SaaS applications like Salesforce or Office 365 with Enterprise Agents located within the data center DMZ or within branch offices (Figure 6). Gain visibility into application-level performance like page load times and server availability and create insights into network level bottlenecks or BGP routing issues within ISP.

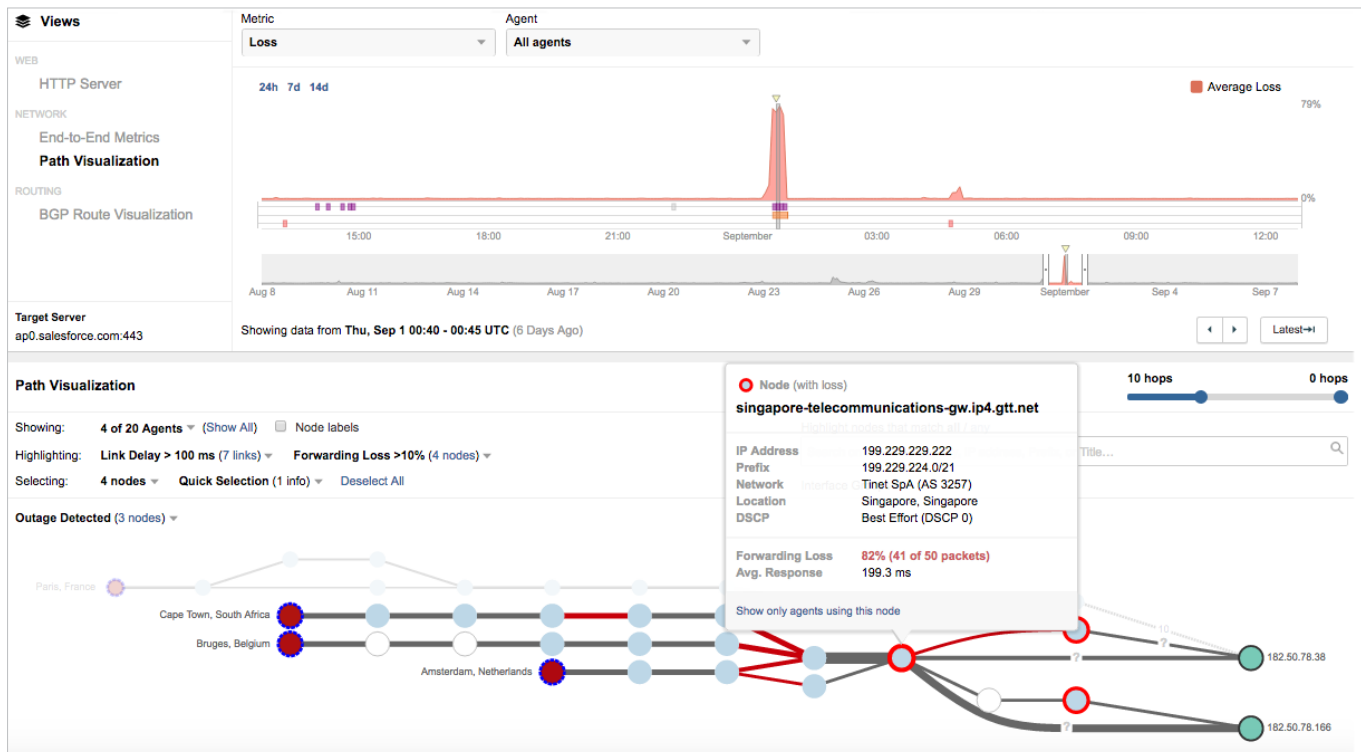


Figure 6: Service to Salesforce was interrupted due to an outage in Singaporean Internet Service Provider

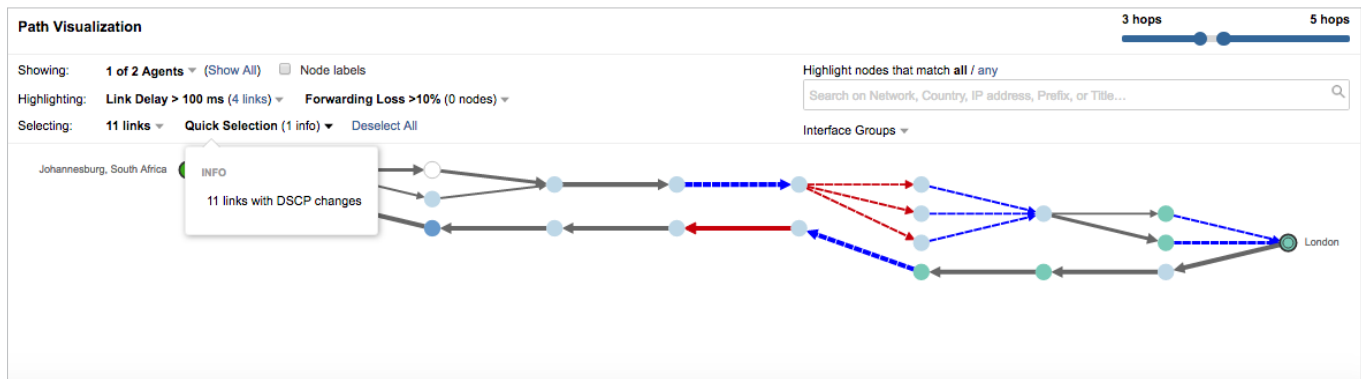


Figure 7: Monitor both forward and reverse path to understand the impact of both your upstream and downstream ISP provider

Routing in the Internet is often not symmetric. ThousandEyes maps out reverse paths to show the impact of your ISP providers on both the reverse and forward traffic paths. Visualizing bi-directional routes is critical as traffic might traverse different ISP's in either direction. Knowing where exactly a problem lies is the first step in successful troubleshooting. Capture reverse path data between Enterprise Agents and/or Cloud Agents, most likely located at the Internet edge of your data centers and in branch offices, as shown in Figure 7.

Extend network visibility further into the corporate network with Endpoint Agents. See the end-user experience of SaaS applications, including full page load data. Visually correlate user experience to network behaviour. Dig into the entire network connection quality through detailed diagnostics with views of VPN, proxy, gateway and wireless performance (Figure 8).



Manage End-User Experience

As your employees increasingly use a mix of applications from the office or the road, measuring and quantifying end user experience has become nearly impossible. Endpoint Agent tracks performance and user experience of browser-based internal and external apps, including SaaS applications such as Salesforce and Office 365. You can even monitor virtual desktops in your environment.

Detect performance patterns within your WAN and LAN across multi-vendor wired and wireless networks. Isolate issues that affect specific offices, networks or groups of devices. Compare performance across SSIDs, BSSIDs and wired networks across the corporate campus (Figure 9).

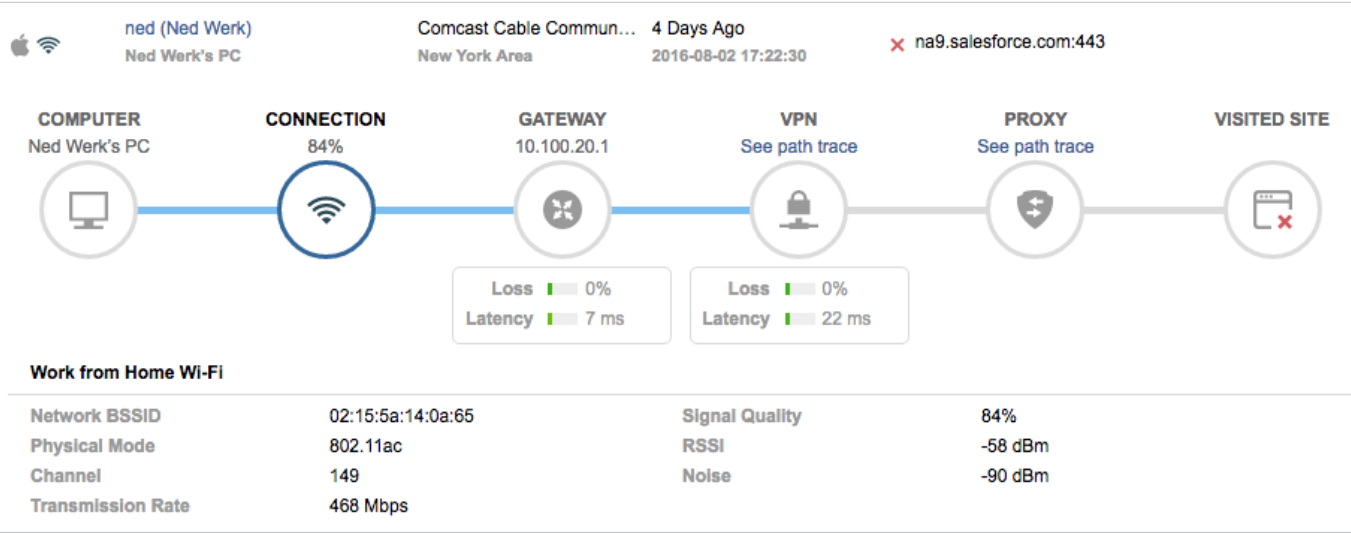


Figure 8: Visualize end-user experience of every user and every session

Data collected by Endpoint Agent can be calibrated using whitelisted networks as well as whitelisted domains, to control where and what is monitored. In addition, users can choose to manually capture data for specific sessions when an issue occurs. By extending network visibility up to last hop connections and locations without dedicated server rooms or hardware, IT teams now have more information about real user-experience to quickly resolve those support tickets.

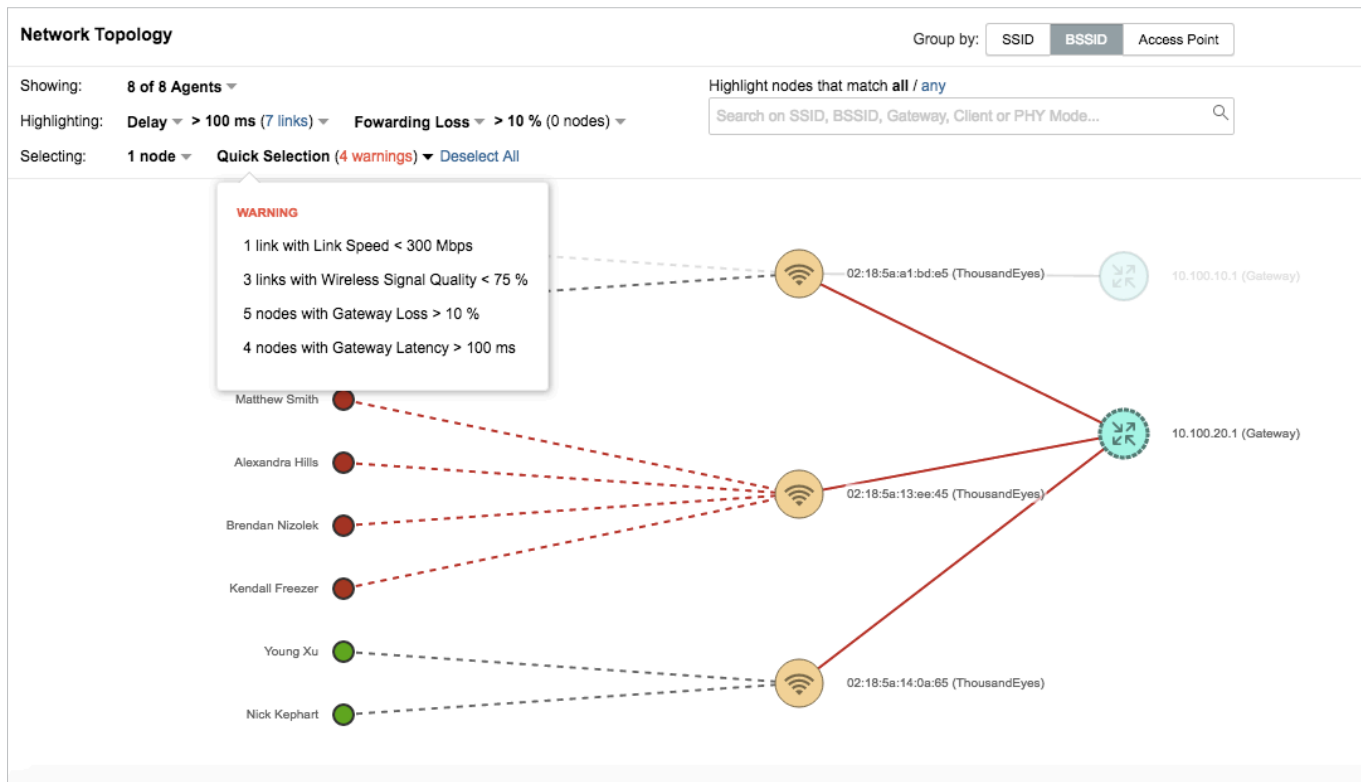


Figure 9: Aggregate wireless quality information to understand problems with network coverage, congestion or device faults

Plan Ahead to Architect the Internet-Centric Enterprise

Use ThousandEyes Enterprise Agents and Endpoint Agents to benchmark current architecture by measuring network loss, latency while accessing SaaS- or internally-hosted applications. Organizations typically rely on more than one ISP for redundancy while designing the SD-WAN network. Have the flexibility to choose your upstream ISP calibrated by average number of outages and failures. ThousandEyes agents can help your through the transition from MPLS-based WAN to an Internet-centric WAN by monitoring both MPLS, VPN links and also the Internet.

Enterprise Agents: Choosing the Right Deployment Model

Enterprise networks are complex in terms of both architecture and the type of devices present. And not every enterprise is alike. ThousandEyes Enterprise Agents are available in a wide range of software form factors to simplify deployment.



Deploying Enterprise Agents










Virtual Appliance	  	Easily deployable across the enterprise WAN and data center
Linux Package	  	
Docker Container		Locations with containerized monitoring and operations tools
Intel NUC Installer		For remote branches and stores with limited IT infrastructure
Cisco IOS Virtual Container		Branch and WAN routers (IOS XE 3.17+ on ASR 1000 and ISR 4000)

Figure 10: Enterprise Agents support multiple deployment options

Conclusion

The Internet-centric enterprise is not futuristic anymore. It is already here. With ThousandEyes, enterprises gain the end-to-end level of visibility required to troubleshoot problems inside and outside of their environment. ThousandEyes Enterprise and Endpoint Agents are lightweight software packages that can be installed and configured within minutes. Gain control of your borderless network, quickly isolate issues and engage the right teams. ThousandEyes can reduce the Mean Time to Resolution of infrastructure problems from hours to days to minutes—and when it comes to business, every second counts.



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.