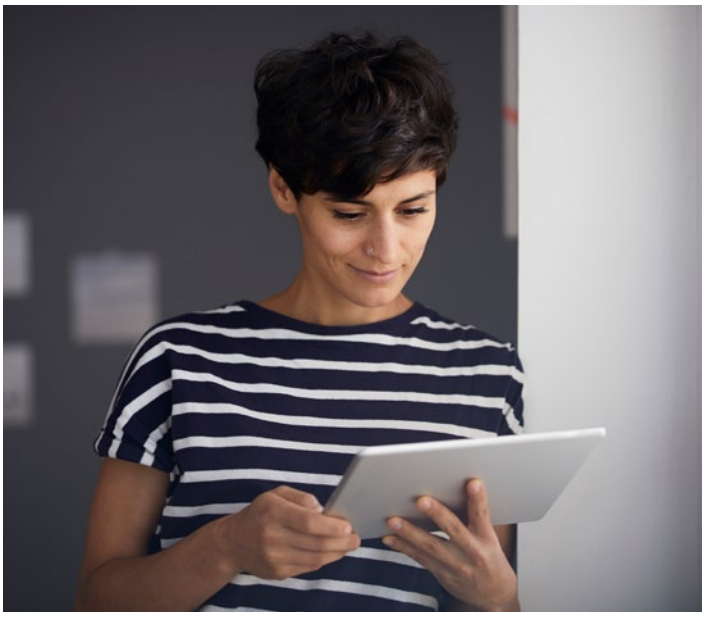
Top five challenges of managing SD-WAN and wifi in the modern branch office

IBM

Overview



For enterprise IT teams today, meeting the connectivity demands of their organizations' mobile-first employees and other users is an ongoing challenge. With more of their environments moving to the cloud, and with software-defined provisioning of virtualized network resources, the job of managing connectivity and access to network applications and services has grown a lot more complicated.

For teams tasked with handling those responsibilities for offices in distributed locations, that complexity can ratchet up significantly. Deploying new and complex network technologies at remote offices where there is usually little or no onsite IT support creates a whole range of challenges for enterprise networking teams.

To keep branch office users connected and productive, enterprise IT and NetOps teams are increasingly pursuing remote office modernization. In these initiatives, organizations entirely redesign their network infrastructures to match the mobile-first connectivity needs of their customers and regional office employees.

The overall goal is to provide reliable, high-quality connectivity at branch offices so that customers and staff have dependable access to applications and network services anywhere, any time and from any device.

Two technology mainstays that enterprises are now using in these projects are software-defined wide-area networks (SD-WANs) and next-generation wifi systems. Although these technologies can deliver the needed connectivity, they both create network monitoring challenges that have slowed their adoption in years past. More recently, however, modern network monitoring systems have emerged that offer the capabilities required to address and overcome those issues.

This white paper discusses the monitoring challenges that previously inhibited the use of SD-WAN and next-gen wifi for modernizing enterprises' remote offices. It also describes the new class of modern network monitoring solutions and how their advanced capabilities, along with their speed, scale and flexibility, let enterprises get past the old monitoring problems and on to successful branch office modernization.

The top five challenges created by SD-WAN and next-gen wifi

Following are brief discussions of the top five challenges that have held back broader adoption of SD-WAN and next-gen enterprise wifi. Also included are discussions of the specific ways modern network monitoring systems help enterprise IT and NetOps teams overcome these operational hurdles.

Challenge 1

Avoiding the temptation to over-provision

As enterprise connectivity models become more cloud-based, they get more complicated and difficult to monitor and manage, especially for team members without deep experience with cloud-based deployments. In outage or service degradation situations where there is tremendous pressure to address the problem, over-provisioning is a very tempting option. Even though they haven't figured out exactly what's going on or why it's happening, teams throw more cloud computing power at the problem, and it recedes. Do this two or three times, and it probably won't be an issue. But choose that option repeatedly, and networking teams watch their connectivity and cloud costs go through the roof.

With faster, more flexible and more scalable monitoring, along with fast and powerful analytics, teams can spot issues before they build into user-impacting episodes. They can also diagnose issues and problems more accurately and remediate them more effectively. All of these things help teams resist the temptation to simply over-provision their way around problems, which in turn helps them keep the costs under control and their budgets intact.

Challenge 2

Managing the change from static to dynamic connectivity

With traditional WANs, connections to branch offices are familiar entities to networking teams. Generally, they go from the data center over a few set hops, usually handled by a small set of well-recognized service provider liaisons, and then on to the specifically identified regional office — or the same in reverse direction. These connections are fixed and contractually arranged with service providers and offer little, if any, flexibility. If IT and NetOps teams were truck drivers, multiprotocol label switching (MPLS)-based WANs would be the same delivery routes they take every day — the same roads, on-ramps, off-ramps and the same destinations without variation, day after day.

Managing those static routes is a very different job than what it takes to watch over SD-WAN connections. That's because SD-WAN fundamentally changes an organization's network. The technology is designed to detect opportunities to change the way network traffic is delivered in terms of servicing priority locations, selecting particular links, opting for service providers, switching transport protocols and so on. This helps enterprises better meet policy directives for highest quality and reliability, lowest cost or some other operational parameters.

In the MPLS world, teams essentially have connectivity maps that they become familiar with and then use to guide their monitoring and problem resolution efforts: "Oh, it's that shaky link acting up again," or "Oh, that service provider is still having that problem."

With SD-WAN, things change rapidly and frequently, so the topological familiarity that teams could count on under the MPLS model goes out the window. They must monitor a much broader set of network traffic variables and do so dynamically. This ratcheting up of the complexity of both monitoring and management tasks for networking teams slowed down what could have been much faster adoption of SD-WAN.

Challenge 3

Reducing network monitoring inefficiency

SD-WANs and next-gen wifi systems are fast and fluid. Traffic flows are complex and dynamic, often involving more hops, service providers and transport types in between where network traffic originates and gets delivered — and all of those variables can and do change rapidly.

Part of the problem for NetOps and IT teams is the limited monitoring capabilities that come with most SD-WAN solutions. Most providers treat this functionality as a "checkbox" item rather than a real differentiator. The larger problem for these teams is that neither one of their network monitoring resources — their existing system or out-of-the-box SD-WAN tools — can monitor both their traditional and modern network environments. That results in split views that prevent teams from seeing full paths and create visibility gaps. Without unified and automated, end-to-end network path visibility, efficient monitoring and management remain an unattainable goal.

When network traffic flows traverse mixed WAN environments, it's difficult and time consuming for teams to stitch together views of the component parts of links, and to figure out if and how their two different network fabrics are impacting one another. By the time teams figure out why a problem happened, everything has changed, so their analysis isn't particularly helpful.

With this inefficiency, issues that should have been spotted and remediated in their early or building phases are missed and grow into larger disruptions that impact users. Performance degradations and outages cause business disruptions and productivity losses, and remediation or repair actions take too long to be effective.

Challenge 4

Gauging service reliability and quality with policy adherence

With SD-WANs and next-gen wifi systems, one way to measure service reliability and quality is through the lens of policy adherence. These technologies allow teams to set and configure policies that essentially direct how the service should operate. What's tricky is assessing policy adherence in these dynamic environments — and how well those policies are being adhered to by various involved parties and technologies. In the case of SD-WANs, this includes network operators and their contracted SLAs; private, public and hybrid cloud arrangements; and network resources that support virtual private networks (VPNs) and other types of access tunnels.

Policies are set up to ensure that entire mixed WAN infrastructures work in ways that align with the organization's operational priorities. Effective monitoring is therefore a critical requirement for determining whether or not policy benchmarks are being met.

With policy adherence monitoring, both lack of end-to-end visibility on the software-defined side and the visibility gaps between SD and MPLS segments again create operational challenges. Whether it's a telco service provider not reporting adequately on performance versus its SLA levels, or being unable to gain a service-level view for connectivity reliability to a priority location, the lack of policy adherence visibility makes overall WAN performance management difficult for IT and NetOps teams. It's yet another reason why such teams might prefer to put off their SD-WAN transitions.

Challenge 5

Achieving operational agility goals

Across all functional areas of enterprises today, one of the top goals is to find ways to conduct business with more flexibility and responsiveness while controlling costs. With their smart, software-driven ways of automatically finding and using the best connections — whether that means the fastest, most reliable, least expensive or best according to some other desired characteristic — SD-WANs should handle the changes teams need to meet their operational agility goals.

Whether it's managing new connectivity arrangements during a merger or acquisition, accommodating growth by provisioning connectivity to a new branch office, or handling temporary priority changes — such as a chief financial officer working at a regional office for an extended period — SD-WANs should make all of that easy.

Without flexible network monitoring with speed at scale, however, the desired operational agility with IT and networking operations often remains stubbornly out of reach. Device polling that's not fast or thorough enough, sluggish visualization and reporting tools that mask or delay views of what's really going on, upticks in manual interventions to address problems — these are just some of the ways that subpar network monitoring can bog down or derail efforts to boost an enterprise's business agility.

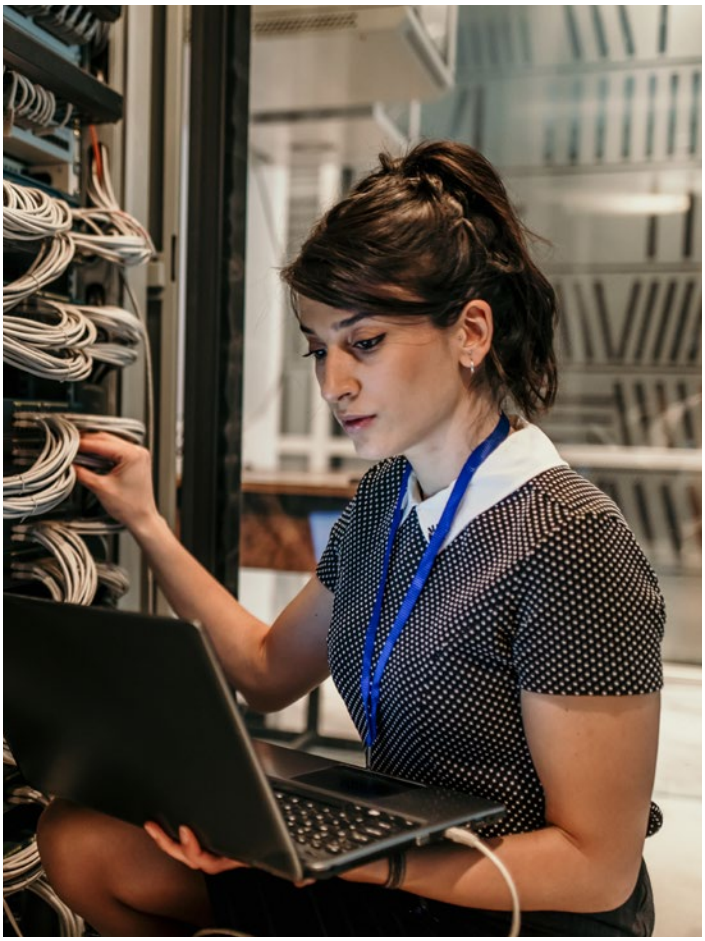
The top new monitoring features required

The new SD-WAN and wifi technologies being used to modernize branch office operations come with new monitoring requirements. Following are some of these must-haves:

SD-WAN flow/QoS analysis
In SD-WAN environments, the paths used between endpoints are dynamic rather than fixed, so the sessions are more fleeting and more elusive for those trying to monitor them. Being able to collect and analyze this dynamic flow of information is critical for networking teams. To manage bandwidth utilization and quality of service (QoS) with critical applications and services, networking teams must be able to see and understand what's going on with their SD-WAN–powered flows with integrated QoS insight in real time. Doing so requires monitoring capabilities that are just as fluid and dynamic as the SD-WAN paths. Broad coverage of all popular flow formats is also a must, as are detailed, real-time visibility into bandwidth utilization and simplified reporting. Only modern network monitoring solutions can deliver these dynamic capabilities.

SD-WAN tunnel views
VPN tunnels have been part of traditional WAN deployments for years. So, for networking teams, the tunnels themselves are nothing new. IT and NetOps teams would manually configure and manage these network tunnels, so they knew all about them, including where they originated and terminated, how their transport worked, and what their capacity and normal performance were. With this close-quarters support, teams basically had all the information and metrics they needed to effectively monitor and manage the tunnels and the traffic that traversed them.

What's new and challenging about VPN tunnels in SD-WAN deployments is that they are configured and managed automatically by the SD-WAN solution. Precisely as it's designed to do, this automation removes humans from the equation. Though that drives tremendous efficiency gains, it eliminates networking teams' familiarity with these resources. That lack of familiarity, combined with the changing nature of these connections, makes it much more difficult for teams to troubleshoot and resolve problems with the tunnels when they crop up. Only modern network monitoring systems — with the capabilities needed to keep up with SD-WAN tunnels as needed — enable IT and NetOps teams to avoid these issues and the major operational problems they can cause.



Synthetic indicators

Traditional monitoring systems have some metrics that IT and NetOps teams would like to see from their polled devices, but they are simply not available. For example, when polling interfaces, teams can view bytes in and bytes out, but polling total bytes is not an option. In SD-WAN and next-gen wifi deployments, there are lots of variations on metrics that would be informative and useful if they were available. The challenge is that traditional monitoring systems cannot produce them; only modern monitoring systems offer these capabilities. With synthetic indicator functionality, teams gain the ability to generate these types of performance metrics with added value, which can help them more quickly spot, diagnose and fix issues before they build into major problems.

Synthetic indicators work by performing simple math calculations on multiple metrics collected from a single monitored device. With synthetic indicators, teams can customize their monitoring to include this multifaceted and previously unavailable performance insight. Networking teams can create and generate these metrics. They can also combine, report on and generate alerts based on this "manufactured" data even though the values don't exist in the management information bases (MIBs) of the target devices.

Synthetic indicators open up many new and useful ways to view and assess network performance, and they're only available in modern network monitoring solutions.

Next-gen wifi visibility

Not so long ago, when enterprise users needed serious connectivity, they plugged into the Ethernet connections in their office walls. Enterprise wifi, on the other hand, was viewed by these users as "good when it's available, but don't rely on just that." In other words, it was a nice-to-have, and the monitoring of this source of network activity reflected its marginal status. In short, like wifi itself, the monitoring of it was "best efforts," not mission-critical.

> Successful remote offices require fast, flexible, powerful monitoring that only next-gen performance monitoring solutions can provide.

Fast-forward to today, and enterprise users aren't looking around for Ethernet connections. They need — and expect — reliable, full coverage wifi services so they can use their mobile devices anywhere across their enterprise campuses.

Next-generation wifi solutions are meeting these needs by incorporating new standards such as Wi-Fi 6 (802.11ax), using more of the available wireless spectrum, and borrowing some technologies from the cellular world. As a result, these next-gen wireless solutions are enabling mobile devices to use new wireless capabilities not just for better and broader coverage but also for higher speeds with fewer congestion headaches. This is what's making next-gen wifi a must-have.

With more traffic moving faster through more layers and a much broader array of devices, it takes more than a traditional monitoring system to keep up with next-gen wifi. It takes the faster, more flexible and more powerful monitoring provided only with next-gen network performance monitoring systems.

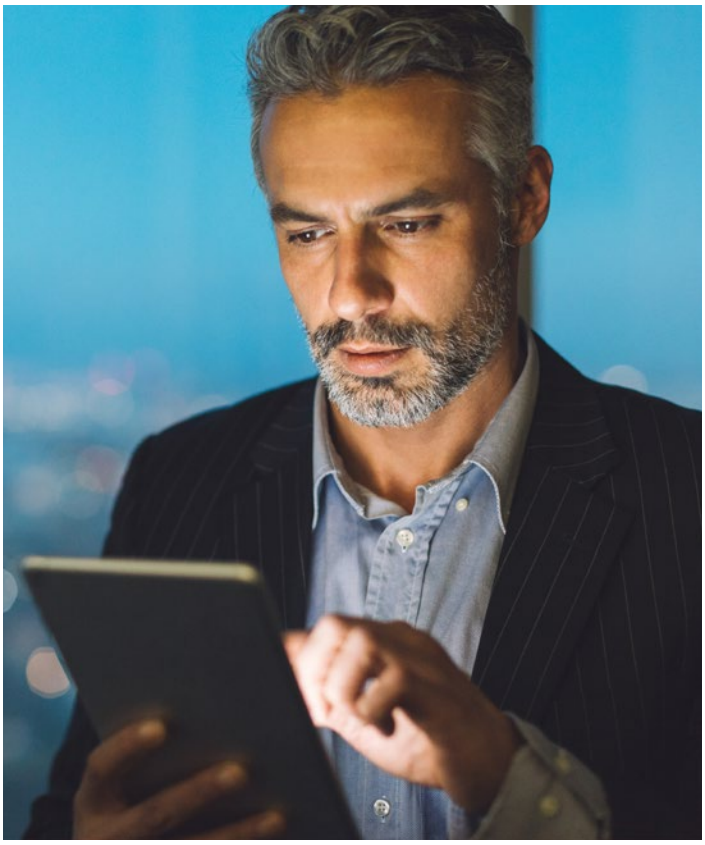
Conclusion

SD-WAN and next-gen wifi solutions are the obvious choice for modernizing connectivity at offices in distributed locations and providing users with more reliable access to network applications and services in these important locations. Less obvious, perhaps, but critical nonetheless is the need to pair these dynamic technologies with network monitoring capabilities that can keep up. For branch modernization strategies to succeed, networking teams need monitoring capabilities that are just as fast, dynamic and scalable as the new SD-WAN and wifi solutions they are deploying.

These requirements are well beyond the capabilities of traditional monitoring systems. Attempting to use them to keep tabs on network performance in modern remote offices is a recipe for failure.

A better, smarter strategy is to support these deployments with modern network monitoring. Properly managing SD-WAN and next-gen wifi connectivity requires speed, flexibility and scalability — but also simplicity and automation.

That's precisely what modern monitoring solutions deliver, and it's how they're enabling enterprise IT and NetOps teams to move forward effectively and successfully with their branch office modernization initiatives.



Why IBM?

IBM SevOne Network Performance Management (NPM) provides a single source of truth to help assure network performance across multivendor, enterprise, communication and managed services provider (MSP) networks.

Learn more about SevOne NPM and how it can help your organization monitor and manage the performance of both your existing and next-gen network and infrastructure resources more effectively.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
August 2022