



WAN Performance: Why It Matters and How to Improve It

The wide area network (WAN) has become more important than ever. The reliance on public WAN performance is now essential for businesses with remote locations of all kinds. That includes hospitals and doctors' offices, retail stores, hotels and anywhere employees are working from home or at a branch office.

The number of connected locations is increasing regardless of what industry you're in, but this increase lets IT centralize infrastructure for off-site branches or offices, since they can enable access from the home office or data center. Using the public internet makes server management easier and often allows for better bandwidth and faster connections. Plus, the provider of that WAN connection offers better support than the traditional approach of leased circuits and MPLS spokes.

The scale that modern business needs today combined with these benefits make it clear that the public WAN is now an essential piece of IT infrastructure. You can't ignore WAN performance, though it may seem complex and difficult to manage or improve. This is especially important because WAN connections exist to join remote offices—so it's likely you (or one or your IT counterparts) won't actually be on-site to see whether the WAN is serving users well.



Managing modern networks

Businesses are managing various types of networks today, including:

- LAN
- WAN
- SD-WAN
- MPLS
- SaaS provider network
- Cloud provider network
- Commodity internet
- WiFi

Historically, WAN could have meant any number of leased network lines with T1 or T3 connections. Either way, they were and still are expensive. Setting up a traditional WAN involves choosing a private circuit like MPLS, a business-specific broadband connection or a 4G or LTE connection. An enterprise might choose to spend money on a traditional WAN instead of just using a cheaper public internet connection. This method can get a more secure, faster dedicated connection to any office that's outside of your main data center. Users connecting over this traditional WAN can get a similar experience to employees working at a main office.

Like any technology, this historical approach to WAN comes with particular challenges. Along with choosing and paying for the connection, you'll also have to provision connectivity from carriers and providers and then track and manage bandwidth.

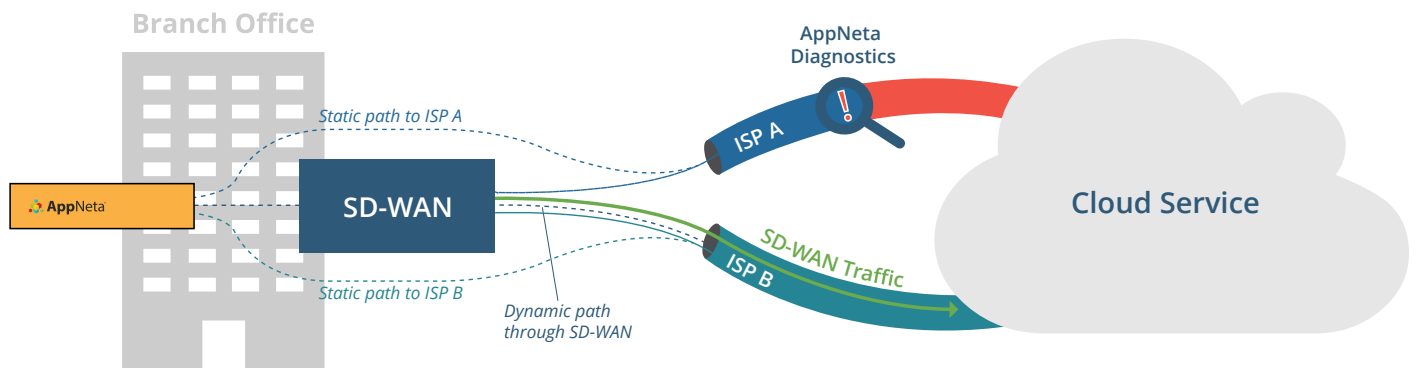
Plus, there's security and compliance to consider. If you'll be setting up and maintaining connections for multiple branch offices, you can set up benchmarks and policies for performance.

The limitations of the connections—the need for higher throughput and bandwidth management to keep up performance at lower cost, for example—led to the development of various WAN optimization techniques several years back. The idea was to make data flow more efficiently over the public internet, which would make deployment to new locations easier and also allow users fast access to critical applications. Those techniques take a few different forms: traffic shaping for prioritization and bandwidth allocation; deduplication to reduce the amount of data that's sent over the WAN in the first place; compression to shrink the size of the data at the get-go to reduce bandwidth use; and caching, which is local hosting of frequently used data.

SD-WAN Enters the Picture

WAN optimization, while still used, has now been joined by [SD-WAN technology](#) (and, in some cases, is included in SD-WAN tools). SD—software-defined—WAN aggregates multiple internet connections into a single virtual connection that's more reliable than those separate connections. It chooses the best connection at any moment to shape traffic in real time, and can help enterprises dealing with unreliable internet connections. Many SD-WAN products are adopting WAN optimization techniques to improve performance further.

SD-WAN technology cuts down on costs, too. There's less expense on hardware and software acquisition, and less support needed for the traditional WAN equipment. SD-WAN can also save on operational expenses needed to manage the traditional costs of tools like MPLS. Plus, branch office networks can be set up faster with SD-WAN technology, since it can use existing internet infrastructure.



SD-WAN technology picks the best network path at any given moment.

For IT, decisions around deploying SD-WAN will be in part about delivery method: choices include hardware appliance, virtual appliance or software, a combination of hardware and virtual appliances, or a managed service. There are lots of features to consider when shopping for an SD-WAN product, too. These could include application-based policy enforcement and path selection, central management from a cloud-based interface, ease of deployment at remote offices, encryption, hybrid connectivity, WAN optimization and more. As with any important piece of networking hardware, IT should match their company's needs (and future needs) with available features that are within budget.

Many existing corporate WAN connections are run via MPLS technology, though they can also be run over the public internet. One [study found that MPLS use isn't going away with the advent of SD-WAN](#), but that businesses are looking at using it more strategically to save money. For example, they may deploy SD-WAN so that they can use MPLS less when there's a need for speed, while short-term capacity growth can be handled by cheaper public internet.

One other SD-WAN feature to note is the ability to break out traffic into business-critical and recreational streams at a branch office, which results in lowered latency and frees up bandwidth for business applications running over the connections.

Take Good Care of Your WAN

Along with the technology moving these packets to your remote offices, there's plenty of process and infrastructure to manage. When a WAN connection has layers of other technologies on top of it, things can get complicated quickly.

You should really know what you're getting with your WAN with a good SLA. Remember, you won't find violations or room for improvement if you're [not actively monitoring SLA compliance](#). One reason a lot of companies choose a dedicated line or MPLS tunnel over public internet is that there are support and performance standards with an SLA—so take advantage of that. A WAN provider's SLA should offer some guarantees for performance, as well as

penalties if the provider fails to meet performance goals or guarantees. For example, your SLA might include capacity and packet loss thresholds, and QoS enforcement policies promised between locations. The SLA should also make it clear how and when you'll get reports from the provider on these metrics and performance. You should also note that if your ISP peers with any other provider, there should be some way of enforcing compliance with metrics like QoS. When ISPs pass traffic off to a peer, the QoS category can be reset, say from "expedited forwarding" to "best effort," so you'd see a big change. End-to-end monitoring can show you these details.

Shopping for SD-WAN

Here are some of the features you might consider when looking for SD-WAN technology:

- Application-based policy enforcement
- Application-based path selection
- Central management through cloud interface
- Zero-touch remote office deployment
- Encryption
- Hybrid connectivity
- WAN optimization functions
- Policy-based routing

Even with [SD-WAN technology, you have to track SLA compliance](#). If you've got a bunch of WAN connections through different ISPs, each with its own SLA, and you adopt SD-WAN technology, that provider's SLA should be the primary one you understand and track. SD-WAN can actually mask problems, since it automatically routes around network issues. While traffic is still flowing it may be relegated to your less-expensive, lower-performing connection. It can be hard to monitor, since it wasn't designed to report on application or user performance or show any application usage data. The service-level agreement can show you the necessary details or at least allow you to see more into current performance.

How to Make WAN Performance Better

Our cloud-connected world has made business easier, and remote offices more possible. The complexity the cloud brings can cost a business money and cause helpdesk tickets and other IT headaches.

When you monitor a WAN, you're looking for spikes in usage that could overwhelm the network. A slow WAN connection will translate into user complaints about applications that are slow to load. Depending on the root cause of the issue, you may or may not be able to pinpoint what's causing the user problem.

Keep these tips in mind to get the most out of your WAN.

Baseline network performance.

You have more control than you think, and you should be proactive about network performance related to the WAN. This will be especially important if you think your organization will be opening new offices down the road. Even if not, it's useful to understand the basics of any WAN connection under your control—how much data it handles, when it's used most and how much you're paying for it.

Use the right tool for the job.

Where there's a relatively modern enterprise today, there's some kind of complicated network infrastructure. Any enterprise using SaaS or cloud has likely added hardware and providers to the network mix. There's wired and wireless networking, and when remote offices are in play, there's MPLS, IPSec VPN and SSL VPN connections to consider. This will involve some fine print, but look at provider performance, both what you've tracked and what is promised, and consider user needs to get the right mix of technology.

Track the right metrics.

To get the information you need from your WAN on a regular basis, track the right network-oriented metrics. These may vary for your particular business, but there are a couple that can give you a big-picture look. These should also be included in a standard network provider SLA.

Latency:

This is the amount of time it takes for data to travel across a network between client and server. This is often coupled with RTT (round-trip time) for a WAN connection due to network asymmetry.

Capacity:

Measuring the connection from end user to application or from office-to-office is the only way to accurately compare performance. Bandwidth metrics can be used to size a new office, but connections with available and utilized capacity will allow for proactive alerting.

QoS:

Use a QoS strategy to categorize and prioritize application traffic, so the most important applications get to their destination first when capacity is scarce. QoS becomes an essential metric for streaming voice/video app delivery. This will involve setting up the QoS queue, then enforcing it hop-by-hop to make sure it works.

Packet loss:

Track this metric to see the percentage of network packets that are lost between source and destination. In small bursts, networks can handle loss, but if loss compounds, then it can have severe effects on end users.

Jitter:

With this measurement, you'll see the percentage of packets with delay variation between source and destination. This most often manifests as patchy video or choppy audio. It's important to monitor cloud-based voice, video and application traffic in order to accurately identify where jitter is occurring.

Test your WAN.

If WAN management involves guesswork, you'll hear about it from end users. When users are spread across distances, especially global, it's a challenge to make sure everyone's performance is consistent. Network monitoring tools let you perform single-ended tests to endpoints you may not own so you can see performance at those distant locations. Remember that automatic synthetic scripting can be sent from any location to add application context to your benchmarks, so a tool that can do that will be very useful.

A well-functioning WAN will help IT manage remote sites better and cut down on help desk tickets and support requests. It's a necessary network connection in a distributed world, and taking care of your WAN will be one important component in your arsenal of cloud tools.

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. For more information, visit www.appneta.com.

1.800.508.5233 | SALES@APPNETA.COM | APPNETA.COM

