Conversational SD-WAN

A ConversationalGeek® Book

Sponsored by MASERGY

Learn about:

- What SD-WAN is and how it differs from traditional WANs
- How SD-WAN can improve application performance
- How SD-WAN can make more efficient use of your bandwidth

By Ben Piper (IT Author and Consultant)

Sponsored by Masergy

Masergy is a provider of fully-managed hybrid WAN, security, and unified communications solutions for enterprises around the globe. Our offerings are based on our patented Software Defined Platform, the largest independent solution of its kind that enables a modern, programmatic approach to hybrid wide area networks that delivers optimum application performance.

For close to two decades Masergy has focused on providing custom-engineered WAN solutions that meet clients' highest expectations for performance, resiliency, and customer experience. Our hybrid WAN approach lets customers leverage SD-WAN solutions into their broader network architecture to support new application performance requirements and cloud connectivity requirements.

The Hybrid WAN portfolio includes managed network functions such as routers, firewalls and encryption, supported as on-premises, software and cloud options. These agile network solutions provide customers with visibility, control and analytics associated with their networks' performance.

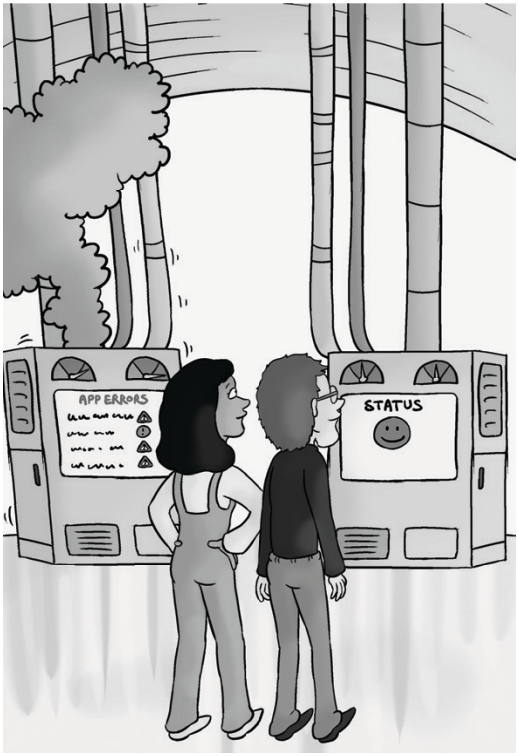
In addition to offering the highest quality solutions to enterprise customers, Masergy is also committed to consistently delivering outstanding customer service to our clients in close to 80 countries. All solutions are fully managed 24x7x365 by certified experts. When customers call our network operations center, they speak directly to our engineers who help resolve their issues on the spot.

Masergy has one of the highest customer retention rates in the industry at 99%, and an industry-best Net Promoter Score (NPS) of 74. (NPS gauges customer satisfaction and willingness to recommend a provider to others.) Customers view us as a trusted partner and valued member of their extended IT teams.

www.masergy.com

Conversational SD-WAN

By Ben Piper



ConversationalGeek®

Conversational SD-WAN

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Ben Piper
Project Editor:	J. Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer:	Karla Reina

Note from the Author

Greetings, and welcome to Conversational SD-WAN!

I'm Ben Piper, tech author and IT consultant. Over the years, I've seen the prevailing WAN technology shift from slow, low-speed data links to gigabit speed networks. SD-WAN isn't a new WAN technology. Instead, it builds on top of the WAN technology you use every day. And it's a hot topic right now.

SD-WAN brings all of your WAN and Internet connections together, both in terms of bandwidth and management. You can centrally manage your WAN from a single system, regardless of carrier, connection type, or location. You can combine bandwidth and granularly define how to route traffic, all from a point-and-click interface.

Perhaps you're considering SD-WAN, but want to know if it lives up to the hype. Or maybe you (or your boss) have already decided to implement SD-WAN. Either way, you've got some choices to make. Which SD-WAN features will you use (or not use)? Will you implement it in one fell swoop or in phases? Will you use your in-house networking experts or engage outside help? Will you use a managed service or build your own? These are the questions this booklet will help you answer.

Leveraging SD-WAN isn't easy, but it can be rewarding. And it doesn't have to be painful! With a clear understanding of what SD-WAN can (and can't) do, you can come up with a solid plan. This book is meant to arm you with actionable information to help you make the best choice for your company.

Ben Piper

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Why SD-WAN?

SD-WAN. You want it. You know you do. But do you really *need* it? To answer this question, it helps to understand the traditional WAN problems SD-WAN was designed to solve. Once you understand the "why" behind SD-WAN, you'll have a good idea whether an SD-WAN solution might be right for you. I say "might" because implementing any SD-WAN solution comes with some challenges, and we'll cover those thoroughly in the next chapter.

The WAN Primer

Before jumping into the problems with traditional WANs, let's clarify what the term "WAN" means. The acronym "WAN"

stands for Wide Area Network. Generally, people use it to refer to *private* connectivity between sites over distance (which could be 5 miles or 5,000 miles). This connectivity can take different forms: MPLS (the de facto successor to frame relay), virtual private LAN service (VPLS), or point-to-point leased lines. *Private* means the traffic stays within the telecom carrier's network and doesn't hit the Internet. A single organization may use multiple carriers for its WAN links.

Wide Area Networks have served enterprises well for decades to connect corporate headquarters, data centers and branch offices using MPLS, VPN, etc. Organizations use one or multiple carriers for their WAN links. Companies are increasingly adopting "Hybrid WANs", which consists of traditional private WAN links *and* site-to-site virtual private network (VPN) connectivity over the *public* Internet. This also includes VPN connectivity to cloud-based resources.

Functionally, a WAN and hybrid WAN achieve the same goal: to get your organization's important traffic from one location to another. So, for the sake of brevity, I'll use the term "WAN" to refer to both traditional (private) and hybrid (mixed private/public) WANs.

SD-WAN blurs the line between public and private networks. With SD-WAN, any link that carries traffic over distance can become part of your WAN!

Traditional WAN Problems

There are four major problems that nearly all traditional WANs suffer from. You can probably think of more, but for brevity, I'll list just four and then discuss each one. See if any of these sounds familiar!

1. Not enough bandwidth
2. Long deployment times for new sites
3. Application performance problems are difficult to monitor and troubleshoot
4. Full mesh VPNs are complex

A Typical Traditional WAN Scenario

To illustrate these problems, let's take a typical WAN scenario. Imagine you have two data centers and multiple offices, all connected in a full mesh via an MPLS network. You also have additional, high-bandwidth point-to-point links between the data centers. Finally, each site has its own Internet connection.

It's common for an organization to have different types of WAN links. While this is often done for resiliency and redundancy, that's not the only reason. Each WAN link is often built with a specific business purpose in mind. Using the scenario I just laid out, let's divvy up our connections according to a purpose:

The full-mesh MPLS network carries traffic for your company's enterprise applications (housed at its data centers, cloud providers, and SaaS providers), as well as voice over IP (VoIP), video, data, streaming media, etc. The full-mesh topology allows interoffice dialing, interoffice networking and MPLS' inherent low latency (usually) ensures calls go through quickly and sound good. And if your enterprise applications aren't bandwidth hungry, you should see fairly low utilization.

The point-to-point link between your data center carries replication traffic, which tends to be continuous and bandwidth intensive. By keeping this on a dedicated link, you avoid competing for bandwidth with your enterprise or cloud applications. Point-to-point links also tend to be low latency, so

you can use this one as a backup if the MPLS at one of your data centers goes down.

At each site, an Internet circuit enables business-related surfing, guest Wi-Fi, and access to cloud-based apps. This spares the MPLS from taking on additional load from users streaming cat videos. If the MPLS goes down, you can use the Internet circuit to route traffic over a site-to-site VPN.

Don't forget your cloud-based apps! Any connection to your SaaS or IaaS provider *is* WAN connectivity!

This doesn't sound so bad! You've separated business traffic from non-business traffic and bandwidth hungry replication traffic from time-sensitive voice traffic. This carefully architected configuration can work fine indefinitely, provided nothing changes.

But what happens when you need to add more heads, offices, or applications? That's when you might encounter the first problem: running out of bandwidth!

Problem #1: Not enough bandwidth!

There are normally two reasons you'll run out of bandwidth: adding more applications and adding more users.

Adding newer, more demanding applications like Big Data Analytics, videoconferencing, IoT devices, or IP security cameras, and pushing them over your WAN can send your utilization skyrocketing. If you acquire a new office through a company merger, you may easily find yourself with a couple of hundred new users on your WAN! (Adding new sites to your WAN has other challenges, which we'll get to shortly.)

Regardless of the cause, when you run out of bandwidth in a traditional WAN, you have a few options:

- WAN optimization: This requires an appliance at each end of the WAN link you want to optimize. This means scheduling downtime, configuring the appliance, installing, and testing it. At the very least, this can take days.

- Quality of Service (QoS): This improves performance for the applications you specify by giving them priority over everything else. It will buy you some time, at best, but it's not a permanent solution.

- Rerouting traffic: You can manually move some traffic off a congested link onto one that has room to spare. But this requires careful planning, scheduled downtime, and doesn't ensure optimal bandwidth utilization. It's a "good enough" solution that you may have to revisit every time you add more users or applications.

- Adding more bandwidth: This is probably the most expensive option. If you have an Ethernet handoff, this may be as simple as calling your carrier and requesting more. But Ethernet isn't available everywhere, and for legacy serial lines, this process can take weeks and even require a scheduled outage.

It may be tempting to route critical traffic over a high-bandwidth Internet VPN, but Internet connections are high latency, which can cause problems with delay-sensitive apps such as VoIP.

Problem #2: Long deployment times for new sites

Whether you're just opening a new site or adding an existing one acquired from a company merger, getting a new WAN link installed can take a long time.

First, you have to wait for the physical circuit to be installed and tested, which in some markets can take 90+ days. Next, you must configure a router and install it onsite. Once it's all connected, you have to verify that routing is configured properly, and that the new site has connectivity to all the network resources it needs. This often involves reconfiguring routers at existing sites.

But that's just for basic connectivity. What if you need to monitor application performance at the new site? That's the next problem.

Problem #3: Application performance problems are difficult to monitor and troubleshoot

If you want to monitor application performance over the WAN, you can configure each of your WAN routers to send information about source and destination IP addresses, protocols, and ports to a piece of monitoring software called a flow collector. The flow collector aggregates this information and makes it searchable and reportable, so you can easily see how much bandwidth each application is using on each WAN link.

But this comes with a big drawback. The more data you're pushing across the WAN, the more flow information you'll have, and sending that flow information across the WAN to the flow collector *uses more bandwidth!* If you're not careful, something as innocuous as application reporting can make your bandwidth woes worse.

And there's another issue. If you're connecting to cloud applications over the Internet, you may have no application

performance visibility at all, because that traffic doesn't pass through your WAN routers and hence doesn't get collected.

Problem #4: Full mesh VPNs are complex

Suppose you want a full mesh of VPN tunnels connecting all your sites, and you want to use them concurrently with your other WAN connections. In theory, this sounds simple. But let's look at what it takes to achieve this.

First, simply getting the tunnels established can be a challenge. Instead of just building one tunnel between two sites, you have to build a tunnel between each pair of sites. If you have 7 sites, that's 21 tunnels! And many firewalls aren't exactly known for their user-friendly configuration! (Incidentally, each time you add a new site, you have to create additional tunnels, which adds even more time to what's already a slow process.)

Also, as I mentioned earlier, you can steer certain traffic across VPN tunnels to achieve an active-active setup. But to be resilient, your firewalls must support dynamic routing protocols, which not all do. Also, because the Internet is inherently a high-latency medium, your VPN performance can go from blazing fast to unbearably slow and back again in a matter of seconds. Dynamic routing protocols can't overcome that.

How can SD-WAN help you?

Now that you've got a clear picture of the problems traditional WANs face, let's get to the important question: how can SD-WAN solve them?

An SD-WAN fundamentally does two things:

- Utilizes all WAN connections simultaneously - MPLS, Broadband Internet, DIA, Metro Ethernet, T1/E1 private lines, etc. - while intelligently steering traffic to optimize application performance.

- Gives you the agility to add new WAN connections and sites quickly and without downtime

Next, let's talk about exactly *how* SD-WAN accomplishes this.

Implementing SD-WAN: Features, Choices, and Challenges

"Thank goodness he has SD-WAN!"

Implementing SD-WAN is anything but simple. The number of decisions you have to make before, during, and after implementation can be overwhelming.

It's critical to consider all your options up front and be absolutely certain the SD-WAN solution you choose meets your business requirements. That's what this chapter is all about.

Enterprise or managed?

The first decision is whether to purchase a self-managed enterprise solution or go with a managed service provider. If you have the networking expertise in-house, you may be comfortable with an enterprise solution you fully own and manage. But if you don't have network staff (or you do and

they're overworked), you can engage a managed service provider to implement and manage an SD-WAN solution for you. There are advantages and disadvantages to each, and those will become apparent as we walk through what's involved in the implementation process.

Some managed service providers offering SD-WAN also offer connectivity to their own private MPLS cloud. This can be a bonus if you're looking to replace your carrier, or just add a new one for redundancy. If redundancy is important, make sure they can provide you last-mile diversity. Also, if you have offices globally, make sure they can hook you into their network in those other countries.

One more thing: some SD-WAN managed service providers offer SLA-backed direct connectivity to cloud providers like Amazon AWS and Microsoft Azure, giving you a faster and more reliable connection than you'd get with a site-to-cloud VPN.

Performance and resiliency

The next decision is around the level of performance and resiliency you need at each site. How much downtime or poor application performance can you tolerate at a two-person sales office? What about headquarters? This will give you clues as to how much redundancy you need to build into your SD-WAN implementation.

SD-WAN Components

An SD-WAN consists of at least two components: an appliance at each site, and a centralized management portal.

The SD-WAN Appliance

The SD-WAN appliance sits between your WAN links and your local area network (LAN) at each site. It typically has multiple Gigabit Ethernet ports, but may have fiber ports as well. On the

outside, it looks and feels much like a WAN optimization appliance, with separate ports for WAN and LAN.

Having all your WAN links run through a single appliance may sound risky because it's a single point-of-failure. If the appliance at a site goes down, you lose all WAN connectivity there. Some SD-WAN solutions allow you to run multiple appliances in a high availability (HA) configuration. This way, if one appliance goes down, the other one will take over. If you require this level of robust resiliency, be sure the solution you choose supports it.

As of this writing, appliances from different SD-WAN vendors aren't compatible, so you can't buy Vendor A's super cheap appliance for the two-person sales office and expect it to work with your top-of-the-line SD-WAN box at your data centers. (This will hopefully change in the future once SD-WAN vendors adopt interoperability standards.)

Some vendors offer virtual SD-WAN appliances you deploy in the cloud. This lets you seamlessly connect your cloud infrastructure to your WAN as if it were any other site.

The centralized management portal

All SD-WAN's offer centralized management from a single pane of glass, which is usually delivered via a web portal. This is where you configure exactly how you want your SD-WAN to route and prioritize traffic and which features you want to use (we'll discuss features are in a moment.) It's also where you can view network and application performance data for your entire WAN.

Here's how it works. Rather than configuring each SD-WAN appliance individually (as you might do with a router), all configuration is done on the management portal and pushed

out to the appliances. This is sometimes called policy orchestration.

In addition to receiving configuration from the management portal, the appliances collect and send various metrics back to it. The portal aggregates this data and makes it available for analysis and reporting.

Here's the rub: the configuration management portal runs on a server. If you go with a self-managed enterprise solution, you'll have to manage that server yourself, perform upgrades, and fix any problems that arise. Also, if you lose that server, you may also lose configuration and reporting capability. And as with any centralized system, it's a single point-of-failure. If you want high availability, make sure that the solution you choose can support it.

With a managed solution, the vendor will likely host the server in their own data center or cloud. They'll also have the responsibility of handling upgrades and ensuring that it stays available. Another advantage of using a managed service is that they can jump in and "see" your WAN (if you want them to), which can be helpful when troubleshooting.

If you go with a managed solution, find out whether you get your own server instance, or if you're sharing it with multiple customers in a multi-tenant fashion. Also, ask about the resolution SLA for outages. If you lose access to the portal, you lose access to reporting and configuration! You'll also want to see what level of visibility & control the solution provider offers via the customer portal. In some cases, providers have 'bolted on' a portal login that is not integrated with the rest of their network portal, which is not ideal. So there is much to look for.

SD-WAN Features

Given the term "Software-defined WAN", it probably doesn't surprise you that the bulk of your SD-WAN configuration is

done in software, on the centralized management portal. In fact, deciding what features to use and how to configure them are among the most important decisions you'll make regarding your SD-WAN. And these choices will be based on the types of applications and cloud services you're using, as well as the type of branch offices and connectivity being used.

Here are some of the most common features:

- Active-active links
- Quality of Service
- Advanced error correction
- WAN optimization
- Automatic VPN tunnels
- Integration with dynamic routing protocols

Active-active links

Being able to combine all your bandwidth is arguably the biggest selling point of SD-WAN. The SD-WAN appliance aggregates your WAN links into a single logical connection. This is called an active-active or dual-active configuration.

In a traditional WAN, you have to answer questions like, "Which WAN link do I use for voice traffic? Which do I use for backup and replication?" With SD-WAN, you don't have to choose. You can use all available connections, all the time.

WAN connections don't have to be the same type or speed. You can combine a 10 Mbps MPLS link, a 4.5 Mbps private line, and a broadband Internet connection, and efficiently utilize their combined bandwidth. That's the power of SD-WAN!

Running an active-active configuration is optional. If you want to use MPLS for your primary transport and an VPN as a backup, you can still do that. But you don't have to. And because configuration management is centralized, you can switch between active-active and active-passive configurations with the flip of a switch.

It goes without saying that running a dual-active configuration requires you to have multiple WAN links. If you're thinking of saving money by dumping some of your WAN connections, don't get too excited. To ensure resilient connectivity, you'll have to have multiple connections, preferably with some last-mile diversity.

This doesn't just mean having multiple Internet circuits. Contrary to some marketing hype, SD-WAN is not an "MPLS killer." The Internet is a high-delay medium, and with broadband, you're sharing a common medium with other users.

Also, broadband is asymmetrical, meaning your upload speed is significantly less than your download speed. If your download speed is 300 Mbps, your upload speed will probably be around 20 Mbps. That means you're still wasting bandwidth! You just can't go all-Internet and expect great results.

Although some ISPs offer dedicated Internet access with symmetric, guaranteed bandwidth, latency, and uptime, this only applies within their own network. It doesn't guarantee end-to-end performance. The Internet is always best effort!

Quality of Service

Quality of Service (QoS) was originally developed to improve performance of networked applications over congested or high-latency links. On a traditional WAN, this is done by sorting traffic into queues (usually no more than 6), with each queue having a different priority and bandwidth allocation. For example, voice traffic may go into the highest-priority queue, but be limited to only a fraction of the available bandwidth. Line-of-business applications get a lower priority than voice, but they're guaranteed a minimum bandwidth allocation. Bulk file transfers may be given the lowest priority, getting only whatever bandwidth is leftover.

SD-WAN provides the same type of queue-based QoS, but it goes one better. SD-WAN continually monitors bandwidth utilization, packet loss, and latency, and dynamically selects the best path according to whatever parameters you choose. For example, the best path for voice traffic would be a low-latency, low-loss link. The best path for bulk data transfers would be any underutilized, high-bandwidth link. By continually monitoring and readjusting, SD-WAN ensures that you always get the best application performance possible.

When shopping around, find out exactly how each SD-WAN solution prioritizes traffic. Some let you prioritize at the application level (port and protocol), while others only let you do it by subnet. Also, if you're using traditional queue-based QoS, find out whether your SD-WAN solution will honor the QoS markings you're already using.

If you go with a managed service provider, ask if they can help you discover all the applications in use on your network. You can't prioritize them if you don't know they're there!

Forward error correction

Forward error correction (FEC) is a way of reconstructing missing or corrupt packets without retransmitting them. This is especially important for locations where you have shoddy physical connectivity, such as ancient T1/E1 copper lines that take on errors every time it rains.

FEC can be important for MPLS as well. The manner in which carriers handle traffic engineering can vary widely. To better understand your risk, ask your MPLS provider about their oversubscription and traffic engineering policies.

A few packet drops here and there may not seem significant, but it's a big deal for TCP-based applications. As soon as TCP begins losing packets, its congestion avoidance feature slows down the rate of transmission, making application performance even worse. Even with UDP-based applications, such as voice and video, packet loss can result in choppy calls or missing video frames.

FEC works by inserting sending or more parity packets across the WAN. The more parity packets, the more packet loss it can overcome. But the drawback of this is that it requires more bandwidth. With static FEC, the number of parity packets is the same, regardless of actual packet loss. With adaptive (sometimes called dynamic) FEC, the number of parity packets varies depending on actual packet loss. If you want to maximize your bandwidth, make sure the SD-WAN solution you choose supports adaptive FEC.

WAN optimization

WAN optimization lets you squeeze a little more out of your WAN links by deduplicating and compressing data before it traverses the WAN. It's perfectly suited for situations where you're pushing the same data across the WAN over and over. Think of distributed file systems, backups, and system images.

It's not so good, however, for delay-sensitive traffic. In fact, some applications crash gloriously if you try to optimize them. Also, most encrypted traffic isn't going to benefit from compression and deduplication. Only optimize those apps which can benefit from it, and test thoroughly!

High latency on WAN links can be caused by congestion (not enough bandwidth), packet loss, or just the distance packets travel. Traditional QoS and WAN optimization only help with high latency caused by congestion. But SD-WAN can help overcome congestion, packet loss, *and* high latency!

Automatic VPN tunnels

One of the most exciting features of SD-WAN is its ability to automatically create secure VPN tunnels across all available WAN links, including the Internet, MPLS, and leased lines! This means no more manually configuring site-to-site VPN tunnels. Because everything is centrally managed, bringing up a new tunnel is a quick point-and-click operation.

Imagine that you're opening a new office. The broadband circuit is installed, but the MPLS circuit won't arrive for another 2 weeks. With SD-WAN, you can overnight an appliance, fire up a VPN tunnel, and get the office online in a day. When the MPLS circuit is ready, you simply plug it into the appliance and start using it. No downtime necessary!

As exciting as this is, there are some things to consider. If you currently have a VPN connection to an IaaS cloud provider, check whether your SD-WAN solution has a virtual appliance you can deploy so you can take advantage of automatic VPN building between your on-premises sites and your cloud.

If you require all WAN traffic to be encrypted, make sure your solution supports end-to-end VPN tunnels over MPLS. Some only allow VPN tunnels over Internet circuits, leaving all other WAN traffic unencrypted.

Integration with dynamic routing protocols

In order to route traffic properly, your SD-WAN has to know the location of all your subnets. Unfortunately, not all solutions currently support dynamic routing protocols such as BGP or OSPF. If you choose one that doesn't, you'll have to program static routes.

Although that sounds like a time-consuming and error-prone process, it's really not. Remember that you manage all of your SD-WAN from a single pane of glass. That means you just program your static routes in one place, and the centralized management system takes care of the rest.

When you think about it, it's similar to how dynamic routing protocols work in a traditional WAN. You configure a route on only one router, and it propagates to the rest of them.

Because the SD-WAN appliance at each site knows about all the WAN links, it makes sense to make it the default gateway. Remember that when considering appliance redundancy!

When is SD-WAN not right for you?

You've spent some time reading about all the cool features of SD-WAN. But are there good reasons why SD-WAN might not be appropriate for you?

It might not be right for you if…

- You have few WAN connections that perform well and don't require any maintenance, and you don't plan to add any more. SD-WAN is not well suited to organizations that upgrade their WAN once every 10 years and never add new sites.

- You only want one WAN connection at each location. SD-WAN can still give you WAN optimization, forward error correction, and centralized management, but a pure WAN optimization solution can net you the same features at a lower cost. Note: You can use dual links at larger sites while being single threaded at the remote. This is still a valid use case to move forward with SD-WAN.

The Budgeting Question: Capex or Opex?

From an IT budgeting standpoint, the decision to go with a self-managed enterprise solution or a managed service comes down to capital expenditure (capex) vs operational expenditure (opex). Let's briefly talk about each option.

Capex

If you go with an enterprise solution, you'll have to purchase the appliances, licenses, and support contracts, which can put a big ding in your IT budget. This may be worth it if you want full control over your SD-WAN. If you purchase a solution and

decide you don't like the features or interface, or if the ongoing support costs get too high, you can change vendors. You decide when to perform upgrades and maintenance, rather than being at the mercy of a service provider's scheduled downtime. (Although a good managed service provider will work with you and won't schedule outages at inconvenient times.)

There's another reason to consider the enterprise approach. If you've already got a WAN optimization solution you're happy with, your vendor may offer SD-WAN functionality as an add-on. Going this route may be as simple as purchasing additional licenses.

Opex

Even if you've got plenty of room in your IT budget, there are still some reasons to consider engaging a managed service for SD-WAN.

You may not want to shoulder the risk of things going wrong. Even with skilled and experienced networking staff, you may feel more comfortable using a managed service provider that implements SD-WAN's every day. That means getting your SD-WAN running faster and with fewer headaches.

Look for managed service providers that can seamlessly integrate SD-WAN with traditional WAN solutions, allowing you to customize your environment for your specific business objectives.

You may also want to conserve your IT budget for other projects. Or perhaps you've already invested a lot in WAN routers and optimization, and don't want any awkward

conversations about why you need to buy more WAN appliances.

The Big Takeaways

As you've gathered by now, SD-WAN isn't a product you buy and install in a day. It requires a keen understanding of the performance requirements of each and every single application your organization uses (cloud apps included!). Don't even think of implementing a solution you aren't 100% sure will meet those requirements!

As you're considering SD-WAN options, take your time to choose wisely. Walk through the provisioning and configuration process of a new site. Test what happens when a link goes down. This might seem like overkill, but an SD-WAN solution isn't something you'll stick in the corner and touch every few months. It brings all your WAN connections under one roof, and will become *the* way you manage and monitor your WAN going forward.

SD-WAN isn't standardized yet, so every vendor has their own lingo. Always ask them to clearly explain unfamiliar terms and concepts.

Vendor Sponsor: Masergy

I'm going to tell you about Masergy Managed SD-WAN. This isn't a "Product Pitch," but a conversational, jargon-free discussion of how their SD-WAN offerings can help you. If you go to Masergy's website, you can see that Managed SD-WAN is one of many solutions that comprise their main Hybrid Networking solution category. To better understand the Masergy Managed SD-WAN, it's helpful to understand some foundational elements of their broader Hybrid Networking solution and their solution customization approach to address the unique application environments and business objectives for each client.

Masergy's global platform is pretty unique. All of its Hybrid Networking solutions are modular and extensible, which facilitates its "customizable by design" nomenclature -- think Lego blocks. The company's "traditional" private networking (MPLS, VPLS) solutions are not really traditional. Clients can "spin-up" an unlimited number of MPLS, VPLS, and other enterprise-grade wide area networking (WAN) environments as

virtual instances just like you create virtual server instances in the cloud. Masergy allows you to create an unlimited number of these virtual network instances at no additional charge. Every virtual instance includes embedded real-time analytics and service controls so you can provision and modify these environments on the fly.

Masergy allows you to “spin-up” an unlimited number of MPLS, VPLS, and other enterprise-grade WAN environments as virtual instances at no additional charge.

Like many service providers, they have directly interconnected their global platform with leading cloud service providers to simply establish private, secure connections. Unlike most providers, Masergy extends their service level agreement (SLA) guarantees of performance directly to these cloud service providers. They offer a full complement of managed network functions like routers, firewalls, and enterprise session border controllers which can all be deployed via three different models: premise based, cloud based, and as virtual customer premises equipment (vCPE) where network functions are downloaded to a server-like device.

Unlike most providers, Masergy extends their service level agreement (SLA) guarantees of performance directly to cloud service providers like Amazon AWS and Microsoft Azure.

Masergy's objective here was to create a modular and extensible software defined network platform that delivers both inherent customization with real-time agility.

Enter Masergy Managed SD-WAN.

Masergy had long offered a Network as a Service (NaaS) solution allowing customers to leverage broadband Internet connectivity for creating secure tunnels into their private network environments. Most clients used the service to connect small/remote locations or for cost effective resiliency. For Masergy, SD-WAN was a logical evolution of NaaS. Originally launched in 2016 as a managed network function, Managed SD-WAN has evolved into a feature-rich solution that is natively integrated with all of their Hybrid Networking solutions.

Like most SD-WAN offerings, you can deploy SD-WAN utilizing only Internet connections or you can combine a variety of access methods including Internet, MPLS, and 4G. The real difference with Masergy Managed SD-WAN is that you don't have to deploy it everywhere. You can deploy SD-WAN to certain locations while retaining MPLS at other locations and all interoperation between the technologies takes place within Masergy's global platform.

With that backdrop, let's look at the key features that enable the flexibility enterprises need to design a network solution customized for their unique application environments:

Hybrid WAN Ready

Masergy Managed SD-WAN is seamlessly integrated with the company's global Software Defined Network Platform allowing you to deploy SD-WAN at certain locations without the need to design a "terminating" location like a data center. This simplifies WAN designs because all interoperation between

Managed SD-WAN and other Masergy networking technologies like MPLS happens in their platform.

Direct Cloud Connect with SLAs

If you choose to leverage Masergy's global Software Defined Network Platform, you can take advantage of its direct connectivity to cloud partners including Amazon AWS and Microsoft Azure. Direct Cloud Connections include industry-leading SLA's to the cloud service providers.

Zero Touch Provisioning

Rapid deployment and centralized policy management are key characteristics of the solution. To speed up deployment of new sites, Masergy's Zero Touch Provisioning allows a new SD-WAN appliance to automatically grab preconfigured settings from the Masergy Intelligent Service Control (ISC) customer portal. Customers simply log into their ISC account, type in the IP address their new Masergy Managed SD-WAN appliance will use, and it is automatically configured. The appliance works as expected from day one!

Active - Active Configurations

For years, WANs have leveraged the concept of active-passive links for resiliency. Two or more links are deployed at a given location, but only the primary link is active and passing traffic. The backup link only becomes active only if the primary link fails. That makes sense, but it's inefficient as enterprises with this configuration pay for more bandwidth than they actually use. Managed SD-WAN enables robust active-active configurations, meaning you can now use all available bandwidth while also realizing resiliency.

Dynamic Path Control

This feature intelligently steers IP traffic over public and private WAN links to maximize available bandwidth. Dynamic Path Control is important because most companies have multiple WAN links for redundancy's sake, but limitations in routing

protocols have made enabling the simultaneous use of multiple WAN links complex. Again, when you have an active-passive setup, the idle connection used as a backup wastes perfectly-good bandwidth that could be used for business apps.

With Dynamic Path ControI, if you experience a network outage on one link, the system automatically steers network traffic to a secondary connection in less than a second. When all links are active, all available bandwidth is utilized. Dynamic Path Control, like Masergy's, allows you to set policies on various links and apps. This helps to fully use all available bandwidth--public and private--to boost performance on the company's various business applications.

Agnostic Access

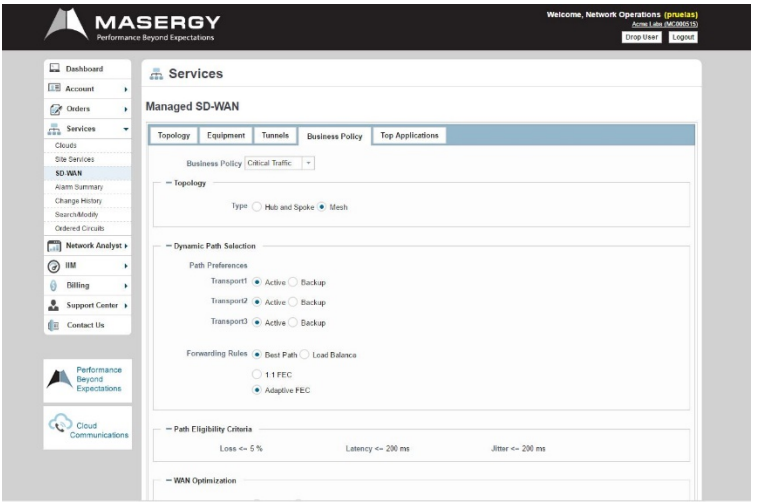
How you choose to connect to Masergy's platform is up to you. Unlike large telcos, Masergy doesn't force you to use a specific type of connection to get onto the network. Their Software Defined Platform is access agnostic, meaning each site can connect to the platform using the method that makes sense from a price-performance standpoint. For large offices and corporate data centers, you'll probably want dedicated private access. For connecting smaller or remote sites, you can leverage dedicated Internet access or broadband Internet access. And you can mix and match multiple public and private connections to balance price, performance, and resiliency. For public connectivity, you can source it yourself (literally "bring your own bandwidth" or BYOB) or have Masergy source it for you. Masergy will even monitor BYOB connections used with its Managed SD-WAN.

Application-Based and Policy-Based Routing

Managed SD-WAN delivers on both fronts, and includes an integrated router to make it happen. Policy-based routing is a "table stakes" feature for any enterprise SD-WAN. With policy-based routing you can control how IP traffic is routed based on a general rule you set. For example, you can create a policy to

ensure traffic in your VoIP network always takes a low-latency, low-loss link.

Unlike policy-based routing, which lets you route traffic based on subnet, application-based routing lets you control routing on a per-application basis. For example, you may have Citrix and file-sharing traffic on the same subnet. With application-based routing, you can prioritize those applications individually.



Configuring policies for critical business traffic.

Secure Encrypted Tunnels.

All Masergy Managed SD-WAN solutions employ encrypted tunnels to securely and dynamically route WAN traffic across the public Internet, dedicated broadband, private links, and Masergy's global network platform.

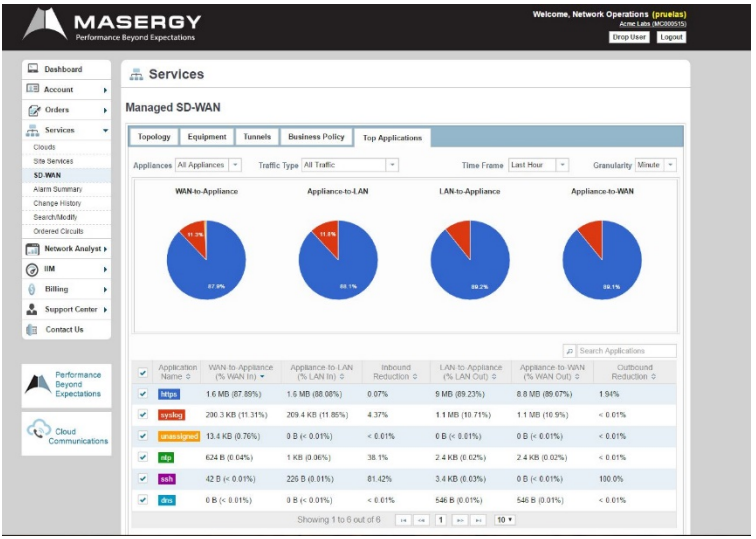
Secure Local Internet Offload.

Masergy Managed SD-WAN device includes an integrated router and a next-generation firewall with Unified Threat Management (UTM), making it easy to directly and securely

route traffic to the internet without stacking multiple devices at a given location.

Application Performance Visibility

One of the most hyped advantages of SD-WAN is its ability to provide visibility into the network. Analytics on an SD-WAN connection are especially crucial when utilizing the public Internet for primary connectivity. Masergy built in a layer of analytics and service controls directly into its Software Defined Platform for both “traditional” network services and Managed SD-WAN. From a single pane of glass, you get forensic network and application intelligence regardless of the connection types being utilized.

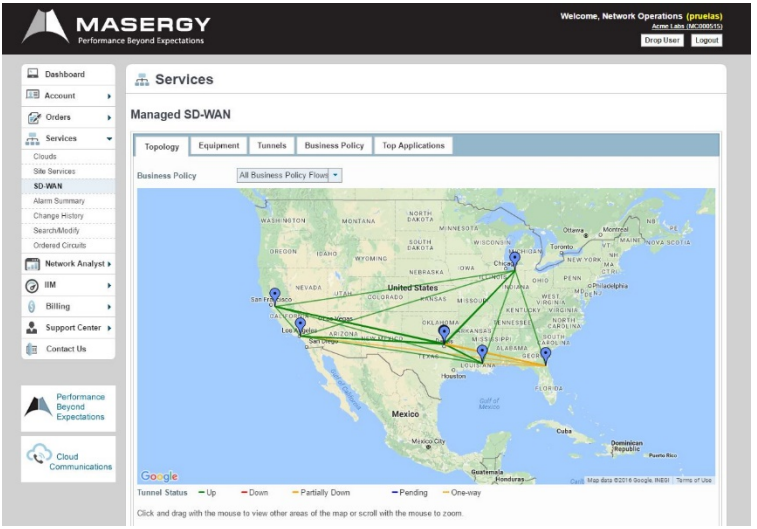


Viewing application top-talkers in the Masergy ISC

The Intelligent Service Control Portal

Masergy’s centralized management portal, the Intelligent Service Control Portal (ISC), is where you’ll spend most of your time managing and monitoring all Masergy solutions including Managed SD-WAN. Here you can provision new deployments,

make configuration changes, get the status of all your WAN links, and see how your applications are performing.



The Masergy Intelligent Service Control Portal

WAN Optimization

WAN Optimization is designed to improve the performance of traffic moving between a branch office and larger sites such as the corporate headquarters, data centers, or the cloud. Masergy Managed SD-WAN offers an additional WAN Optimization feature to reduce the overall amount of data being transferred which speeds up data replication, data center consolidation, virtualization, and big data transfers to and from the cloud.

The Big Takeaways

Much of the initial marketing hype surrounding SD-WAN led folks to believe the decision between SD-WAN and, say MPLS, was a binary decision--SD-WAN vs. MPLS. Don't believe the hype! As discussed in this book, MPLS and SD-WAN most certainly can, and in most enterprise use cases, should coexist.

When plotting your path to SD-WAN, understand that the feature comparison checklist is only part of the equation. Understand the entire scope of the solutions available from any given provider and how they can interoperate. Stay focused on your mission: striking the optimal balance between price, performance, and resiliency to ensure your applications deliver the right experience to your users.

Masergy's approach to Hybrid Networking is unique. Check out their website for more details. While you're there, you can also look into Masergy's other managed services, including Security, Unified Communications as a Service (UCaaS), and Cloud Contact Center. The company also offers professional security services for penetration and compliance testing.


MASERGY
Performance Beyond Expectations
SD-WAN
ACCESS AGNOSTIC. FULLY INTEROPERABLE.
www.masergy.com | sales@masergy.com | 866.588.5885

Easily “converse” and understand SD-WAN

SD-WAN isn’t a solution you purchase and install in day. It takes a bit of effort to review your environment and make an educated decision on the use of SD-WAN in your environment. In this book, we first explore the problems inherent in traditional WAN scenarios and help explain how SD-WAN can resolve those issues. We then dive into the various features of SD-WAN, the choices before you and the challenge of determining if SD-WAN right for you.

About Ben Piper

Ben Piper is a hands-on IT consultant and author of Learn Cisco Network Administration in a Month of Lunches. He holds numerous Cisco, Citrix, and Microsoft certifications, including the Cisco CCNA and CCNP. He has over 18 Pluralsight courses covering networking, cloud, devops, and server administration.
Email him at ben@benpiper.com