# Setting Goals for SD-WAN

## *Don't Leave Any Benefits on the Table*

by Bob Nerz

**What is SD-WAN?**

SD-WAN is an acronym for "software-defined networking in a wide area network (WAN)." Unlike predecessor devices with command line interfaces, SD-WAN devices provides a browser-based interface for both configuration and management. With easier configuration and more intuitive management, SD-WAN enables higher-performance WANs by leveraging low-cost Internet access. It reduces or eliminates the dependence on expensive single-carrier solutions such as MPLS. Gartner predicts that 40% of WAN refresh initiatives in 2018 will incorporate SD-WAN edge devices. By 2020 they predict that 60% of branch offices will have direct Internet access.

**Recommended Goals**

Well-established hardware vendors and carriers are rebranding their offerings to align with SD-WAN. Many aggressive young companies are also providing attractive new offerings. These offering are not all the same. As an independent consultant, my job is to find the ideal solution for my clients based on their needs, priorities and current situation. There is no one "cookie cutter" solution. Every network transformation is different. However, there are some goals I would encourage all organizations to consider as part an SD-WAN transformation:

**#1 Increase Performance while Reducing Cost**
**#2 Increase Reliability and Redundancy**
**#3 Reduce the Number and Types of Edge Devices**
**#4 Automate Network Management**
**#5 Revamp the Plumbing**
**#6 Consider New Carriers and Bandwidth Types**
**#7 Don't Forget the Backend Processes**

**Bob Nerz**

**About the Author:** Bob Nerz founded Network Technology Consulting (NTC) and serves as its principal consultant. NTC focuses on the needs of large companies making complex IT transitions to address changing technology, expanding business needs, and cost reduction. Prior to NTC, Bob had over a decade of experience with hardware and software companies in the computer-networking field including: Motorola Codex, Concord Communications, and American Power Conversion. Bob holds both a B.S. in Engineering and an MBA.

**#1 Increase Performance while Reducing Cost:**

Since the advent of the cable modem, end users have been coming to work and saying: "Why is the network so slow? It's much faster at home." IT departments have tried various explanations, but what the end the users inevitably *hear* is "the network is slow because with our carrier we have to pay more to get less bandwidth." That's hardly a winning argument. Migration to SD-WAN is an opportunity to end the rationing of bandwidth. Bandwidth has become more of a commodity and SD-WAN provides the tools to reduce dependence on expensive MPLS and old-line carriers. More affordable bandwidth can be so plentiful that congestion becomes a thing of the past. With SD-WAN tools, prioritization also becomes less critical while at the same time easier to implement. Redundancy also becomes more affordable, so it may be reasonable to have backup links as large as the primary links. For the risk averse with a matched set of links from a single carrier, it's important to *try new things* ahead of establishing goals for an SD-WAN transformation. Without a diverse experience base with multiple carriers and bandwidth types, IT groups are likely to give into their definition of risk avoidance and choose undersized links from an expensive carrier. I recommend that the optimization guideline be "with a *fixed budget*, how can we get the *most performance* (most bandwidth and lowest latency) and *reliability* (automated failover and right-sized redundancy)".

***Depending upon the starting point, it may be reasonable to set a specific goal such as: Double the end-user bandwidth and add redundant links of a useful size, while reducing the total cost of bandwidth by 30%. Apply these savings to pay for the cost of the project.***

**#2 Increase Reliability and Redundancy:**

SD-WAN devices generally make it easier to implement automated failover or Active-Active load sharing. Prior to SD-WAN, failover or load-sharing may have required a highly skilled network engineer and a long conversation about routing protocols and convergence times. SD-WAN also facilitates vendor neutrality, so there is no reason not have a large cable modem link from the local cable company as your passive (or active) redundant link.

Not to harp on a point, but if your network experiences frequent congestion due to undersized links, in the eyes of the end users, that's also a "reliability" issue. They can't get their work done if the network is slow. So, if a different carrier can eliminate congestion by providing larger links at a lower cost, that increases "reliability" in the eyes of the users.

*Setting goals for redundancy is completely dependent on the requirements of the organization. Some cannot tolerate any downtime or reduced performance; their users require full performance, even when a primary link fails. Some can tolerate the chance of reduced performance and can size backup links at half the size of the primary. Some can tolerate "limp along" performance for the duration of a primary link outage, so a backup link can be much smaller than the primary. Some organizations consciously rely on their users to provide their own redundancy, namely their smart phones can provide access to email and cloud apps during an outage or can act as Wi-Fi hot spots.*

***Your Reliability and Redundancy goals should be in tune with both the needs and budget of your company.***

**#3 Reduce the Number and Types of Edge Devices:**

Over the last decade, there has been a proliferation of new devices at the edge of the network. At one time, a Cisco router was the only edge device at a branch office. Over time, there have been more and more devices added to the branch office edge including firewalls, path optimizers, compression/acceleration devices, and traffic monitoring devices. All these functions could have been incorporated into a Cisco router (software upgrades for firewall and security, performance routing (Cisco PfR) for load-sharing and path control, WAAS hardware modules for compression and acceleration, and NetFlow for traffic monitoring). A fully loaded Cisco router essentially would have been an SD-WAN device, but not likely "best-in-class" for any function except routing. So one-by-one, purpose-built devices were added at the edge and it can now be a complex mess with multiple vendors, multiple support and update processes, multiple management interfaces, and multiple skill sets required for network engineers. The expense of maintaining these devices can be a substantial and sometimes overlooked contributor to the total cost of network ownership. Added devices also increase the chances of a hardware failure or a security vulnerability.

SD-WAN is an opportunity to get back to one or two devices at the network edge. This requires being realistic about requirements. For example, many organizations struggle to keep up with firewall updates and never fully implement the threat signature subscription services for the platforms they choose. Or they fail to acknowledge that users take devices off their network and use them at home and on the road outside the corporate perimeter. In other words, it may be time to outsource your outbound firewalls to a third-party because they can do a better job of keeping up with the rapidly changing threat environment and usage patterns. Some carriers offer firewall-in-the-cloud. Other service providers offer hosted web proxies in the cloud (e.g. Forcepoint -Websense or Zscaler). Email remains a likely vector for an attack and there are multiple 3rd party screening services (e.g. Mimecast and Proofpoint) and user awareness training companies (e.g. SANS Institute and KnowBe4).

***Set a goal to reduce the number of devices at the network edge, especially in branch offices. Reducing devices reduces cost and complexity and increases the ability of your team to maintain and secure your network. Many carriers offer a managed SD-WAN device as part of their offering, so there is no longer a need for separate capital purchases or maintenance contracts. Consider using a 3rd party service as part of your security solution to reduce the need for complex gear at the office edge. Some 3rd party services can offer full protection of road warrior devices as well as remote access back into the corporate net.***

**#4 Automate Network Management:**

How often have you requested traffic statistics to analyze a specific network situation only to hear "we can turn on collection now" or "we haven't added that site to the management console yet" or "we need a license upgrade to do that level of analysis". To be a useful tool, network management must cover every edge device and collect fundamental stats automatically … and *before* you need them for forensic analysis. Some SD-WAN offerings include a centralized network management console hosted in the cloud. While most SD-WAN vendors focus only on the edge device, some can also fold other network devices into the same management platform including Ethernet/PoE switches and wireless access points (Wi-Fi WAPs).

**Migration to SD-WAN is an opportunity to review your current network management platform and decide whether to keep it and incorporate SD-WAN devices, or replace/augment it with a new solution, possibly one hosted by the SD-WAN provider.**

**#5 Revamp the Plumbing:**

Some organizations are still backhauling or "hair pinning" Web browsing traffic over MPLS to a centralized firewall at their main data center. This practice is increasingly hard to defend. Most users direct 80% or more of their traffic to the public internet. With solutions like Office 365, even Email and intra-company File Sharing are accessed over the Internet. Generally, less than 10% of a user's traffic is targeted at applications hosted in a corporate data center. Your usage pattern could be different, but do you have a clear picture? In the future, more and more corporate apps will be hosted in the cloud vs. a corporate data center. Migration to SD-WAN is time to align your network with the needs of the users. They need a direct exit to the Internet. For some it is a giant leap to allow branch offices to have direct access to the Internet. The key to making that leap may be realizing that the security task of allowing outbound web traffic is a very specialized subset of the many *inbound* and outbound traffic patterns that a data center firewall may have to enable.

**Migration to SD-WAN is an opportunity to enable direct exit to the Internet at all branch offices for all users.**

**#6 Consider New Carriers and Bandwidth Types:**

Many network folks are biased against bandwidth that's asymmetric, a different speed for upload and download. Asymmetric is used by cable companies and some carriers, not because of technological reasons, but because most users are happier with 100 Down and 10 Up than with 25 Down & 25 Up. While symmetric bandwidth may be mandatory at your data center, a 5:1 or 10:1 asymmetric ratio makes perfect sense for branch offices where the traffic patterns are typically asymmetric by 10:1 or more. It's also simple to prioritize traffic in the Upload direction relying on the SD-WAN edge device, so voice and video are not reasons to avoid asymmetric bandwidth.

SLAs and SLA penalties are another area of bandwidth bias. Some may never give up the security blanket of an SLA with a financial penalty, but there is a very high cost for that. Most SLAs are designed with the same philosophy as the three-clawed stuffed animal machine at the restaurant you take your kids to. It may look possible to collect, but it's much more difficult than it looks. Collecting financial penalties requires access to *both network management information and billing information*. It's time consuming and may not be the best use of your staff's time to collect modest sums. *Why not collect big savings every month instead?* Ironically, carriers that offer the best SLAs typically have the most difficult contracts to cancel for non-performance. Carriers that have no SLAs, sometimes have no or low penalty for cancellation, i.e. they believe you'll like their product whether or not you are contractually obligated. My experience is that cable companies are very reliable in a business setting, more so than in a residential setting. That's because more of the service path is fiber and because the service path tends to be underground or in a climate controlled building, rather than hanging off a telephone poll in harsh weather.

**Migration to SD-WAN is an opportunity to deploy new bandwidth types. Try some, you may like them.**

**#7 Don't Forget the Backend Processes:**

SD-WAN enables carrier neutrality. Low-cost backup links may also result in a few more carriers and many more invoices. For example, most cable companies issue one invoice per site. So if you have 20 backup links, you'll receive 20 invoices. That could be a nightmare, but there are some easy solutions. Bandwidth aggregators or agents can combine multiple invoices into a single monthly statement. Another solution is to set all small invoices to auto-pay against a company credit or debit card dedicated to that purpose only. Hiring a telecom expense management firm (TEM) is another option. Corporate accounts payable groups frequently loose invoices or deliberately pay late to primp up cash at the end of a quarter, thereby generating a late fee. Whoever pays your carrier invoices should have an "invoice calendar" and know when every invoice is expected, how much it should be, and if it was paid on time.

Aside from paying invoices, there is also the need to track account information such as account numbers, circuit IDs, static IP assignments, device serial numbers, support numbers, PINs, etc. This is best treated as something that needs to be included in and an overall configuration management process.

**Migration to SD-WAN presents new requirements for backend processes such as invoice payment, support access, and configuration management. With proper planning and attention, these challenges can easily be met.**

**Network Technology Consulting** tm

508-698-1000
800-653-4182
bob@nerz.net