



How To Migrate From
MPLS To SD-WAN Internet

A step-by-step guide to a successful SD-WAN migration

The old adage “the devil is in the details” certainly reigns true in IT. From the most tenured of IT professionals to the newbies just out of college, the obvious answer to overcoming and preparing for a big change is to develop a thorough and well-documented migration plan.

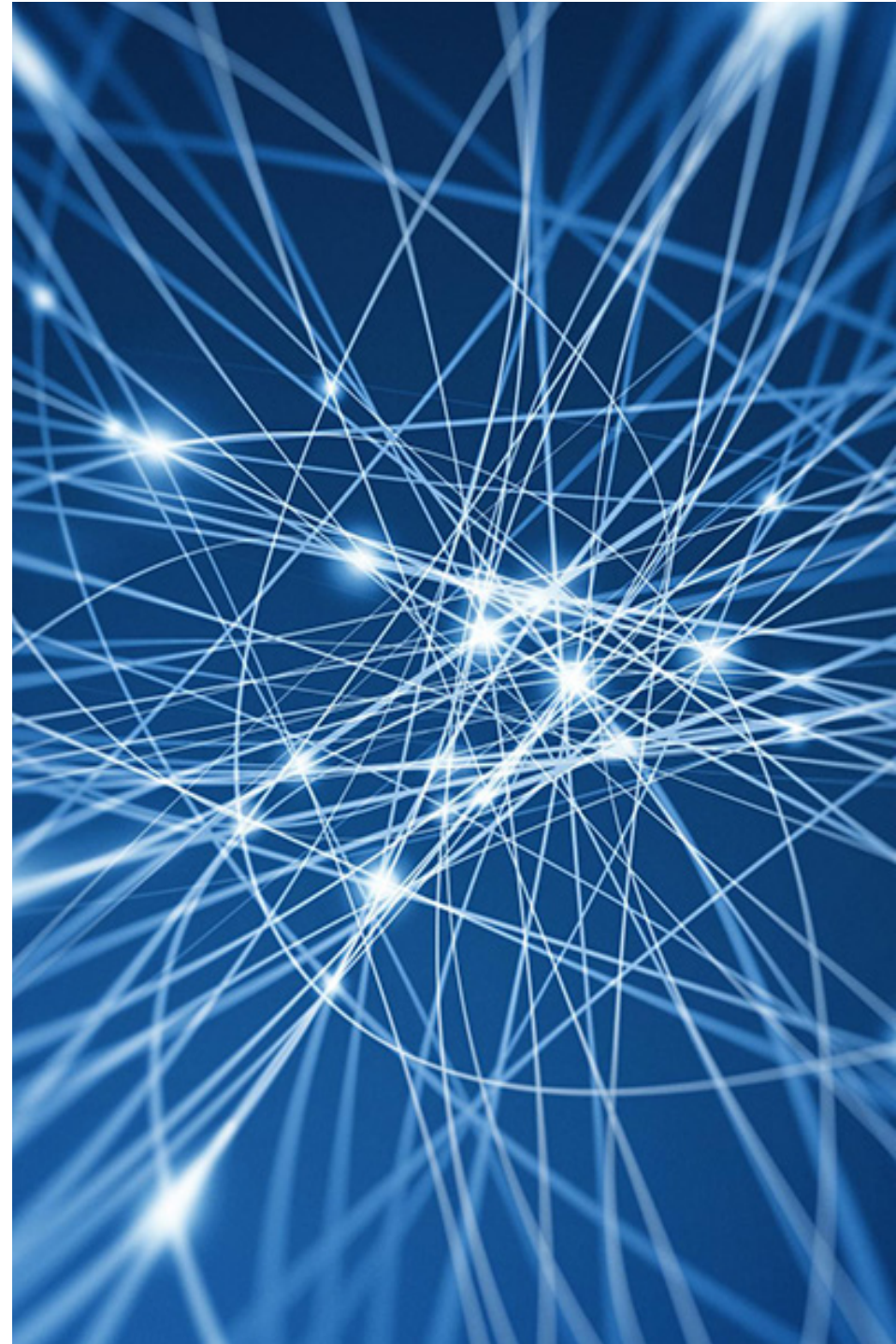
When migrating your network from one carrier to another, some thought has clearly already gone into the potential impact such a change will have on the organization and how to mitigate risk of disruption to your end-users.

If you aren’t yet comfortable with the idea of migrating to SD-WAN (or even if you are), this article will give a detailed overview of what needs to be considered, requested and fulfilled when building your plan to migrate from MPLS to an SD-WAN controlled internet environment.

Pre-Installation Planning Phase

Prior to deploying your [SD-WAN solution](#), orders must be placed with the appropriate carrier or carriers to insure you have connectivity to roll off of your existing MPLS internet solution to a dual internet solution.

Another best practice is to have both diverse carriers and paths. Diverse technologies ensure redundancy to the internet from the corporate HQ or the remote sites.



After you've confirmed diverse connectivity, start by following these steps:

Step 1: Take an inventory

You must know exactly what you have in order to replace it, so it's important to conduct a thorough inventory of the services, equipment and IP addressing schemes you will need.

Keep in mind that the role of SD-WAN in this environment is to centralize the control function so traffic can be directed securely and intelligently across the WAN. That said, your SD-WAN device may physically connect to routers, firewalls, LAN(s) and DMZs.

For this reason, you'll need to develop a thorough network diagram as well as create a pre-install document identifying the following by sight:

- Data LAN networks
- Voice LAN networks
- Core router/ Switch IP
- Routing Protocol
- Firewall External IP
- SD-WAN LAN IP
- SD-WAN #1 IP
- SD WAN #1 Gateway IP
- SD-WAN #2 IP
- SD-WAN #2 Gateway IP



Step 2: Define the cut-over process

Consult with your SD-WAN provider to determine exactly what the cutover process is going to look like based on the current architecture and what you want the final outcome of the architecture to look like by doing the following:

- Provide a current network diagram.
- The SD-WAN provider will provide pre-install documents.
- The SD-WAN provider will provide a remote network survey and comprehensive review of your premise network edge.
- Review the IP addressing and make sure your SD-WAN device has the right IP addressing scheme based on where it will be in the design.
- Hold pre-deployment meetings (including whiteboard sessions and diagrams) to outline the complete installation, deployment and support of the SD-WAN solution.
- Both teams must work together to identify what will go into staging, configuration, testing, installs, turn-up and ongoing hardware/software/GUI training.
- Finally, monitor the SD-WAN device.

Equipment Staging & Configuration Phase

Our recommendations for configuring and placing your new SD-WAN device include:

- Review your IP addressing scheme to ensure SD-WAN appliance. Then, have your SD-WAN provider review your IP addressing scheme to determine proper placement of SD-WAN equipment into the network.
- Conduct proper inbound and outbound policy routing procedures.
- Configure network circuit with SD-WAN appliance layered into updated network diagram.
- Have your SD-WAN provider review your premise network edge.
- Identify client applications including (but not limited to) VPN tunnels, voiceover IP, premise-based web servers, email servers, cloud applications and any other critical application servers.
- Both your engineers and the SD-WAN provider's engineer(s) should come to an agreement on the configuration and then set an installation date.
- The project manager should track the order and delivery of equipment as noted in the equipment list.
- Prior to shipping, make sure the SD-WAN provider tests all units, including:
 - 48-hour hardware traffic test for all network interface cards
 - Software confirmation and integrity testing
 - Dual-power test configuration
 - Pre-set configuration (if requested)
 - Failover unit testing (if requested)



Installation & Deployment Phase

Step 1: Physical install and configuration of first three sites

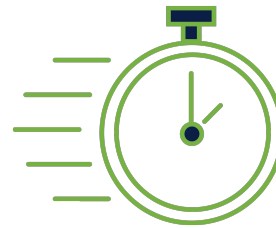
The SD-WAN provider typically assists with powering up the units to assure hardware and connectivity is functioning normally. This includes testing connectivity to other network appliances, including:



Routers



Firewalls



LAN



DMZ



Step 2: Test and turn-up

Network WAN

- Ping each WAN interface.
- Ping each router through SD-WAN appliance.
- Ping SD-WAN appliance to the internet.

Network MPLS (if necessary)

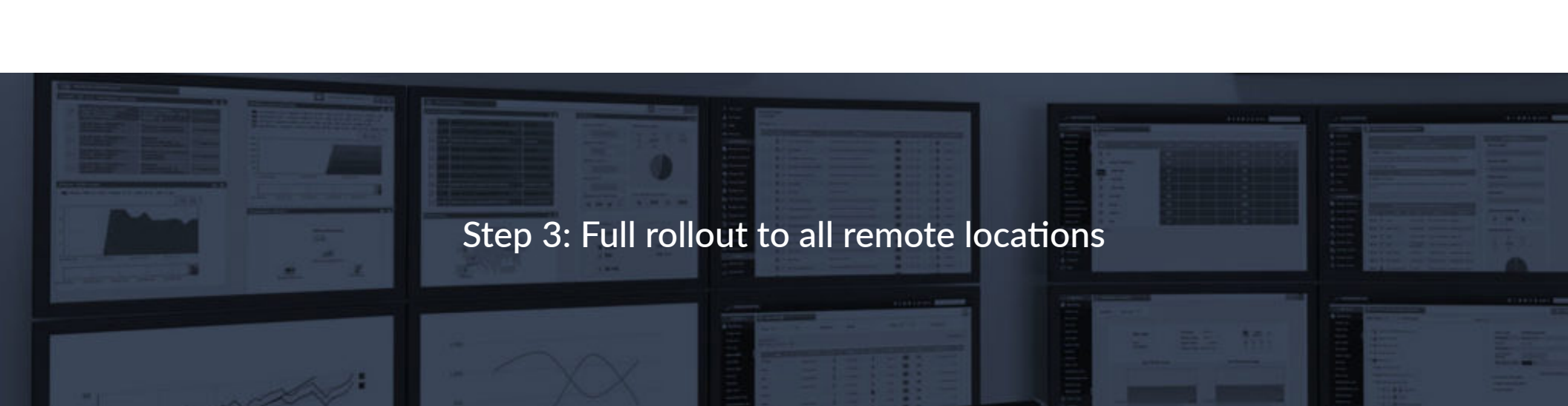
- Ping each WAN interface of MPLS circuits.
- If MPLS routers are retained, ping each MPLS router to assure SD-WAN appliance to router connection.
- Ping SD-WAN appliance to SD-WAN appliance (site-to-site) connection is fully meshed.

Network LAN

- Conduct IP addressing to assure LAN devices can ping SD-WAN appliance.
- Test to make sure Admin can connect to the SD-WAN appliance and access the user interface for device configuration.

Functionality

- Test internet traffic to insure LAN devices can access the web without errors and to ensure traffic is flowing across all internet connections.
- Test that emails can be received and sent.
- Test that internal servers can be accessed from the internet.
- Test any specific applications that were defined at pre-install.



Step 3: Full rollout to all remote locations

Note: For the sake of choosing a path, we've chosen to outline turning up the SD-WAN solution in conjunction with the existing MPLS environment. Depending on your specific circumstances, this can be considered a best practice when it makes sense. It certainly mitigates the potential for risk of downtime since the goal is to fit the SD-WAN appliance into the current architecture, you just slip it in and out in the event of issues with no changes on the existing network environment. This means everything runs as normal, regardless of whether or not you have the SD-WAN appliance in the network.

- The rest of the rollout should be considered “zero-touch” for your SD-WAN device as you have tested the configuration in the lab and now tested in production.
- Be prepared for anomalies and to implement your roll-back plan (removing the SD-WAN device) in the event of issues at the remote locations.
- Confirm the appropriate routes for accessing the MPLS-only subnets (when applicable).
- Acceptance test at all remote sites with a tech on-site in case of anomalies.

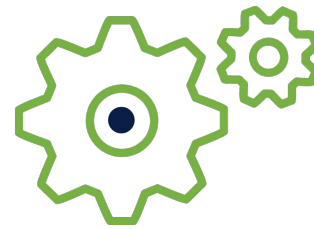
Step 4: MPLS turn-down



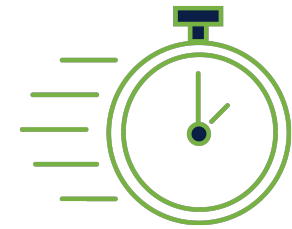
Turn-down the MPLS connections at data centers.




Remove all MPLS bridging routes if any have been added.



Turn-down connections at the remote sites.



Run final acceptance testing at all sites to confirm connectivity.



Step 5: Admin training and testing

- Introduce and train network administration staff on network management tools and assist in setting up accounts in the SD-WAN GUI.
- Put all helpdesk, escalation points, and contacts in a single document for your team's review and answer any questions in regards to how they can be assisted with issues or questions.
- Request all configuration templates and guidelines for restoration in the event of a total loss of the configuration.



Step 6: Monitoring and ongoing management

- Set-up monitoring parameters and thresholds to provide alarms and determine who/where those alarms will need to go.
- Allow admin access to view network, routers, speed meter, speed charts, and status of connections.
- Offload to SNMP and send traps to select SNMP management stations.
- Offload to reporting software and send/report system logs to a log server (if necessary).



Step 7: NextGen firewall setup (if necessary)

Configure and test the following:

- Intrusion prevention
- DDoS blocker
- Anti-virus filtration
- Anti-spam filtration
- Web content filtering
- Web application security services
- VPN encryption / concentration services
- DHCP server



Step 8: On-going training

- Identify the groups that need continued training, what curriculum is available, how often an individual will need to be trained, and what the training will consist of.
- Check and double-check how to open tickets in the event you need help for your SD-WAN network solution.

Conclusion

As you can see, with a plan anything is possible. As a human species, we've proven that anything is possible by putting man on the moon and by going to the depths of our ocean floors. Here at EnableIP, our [managed SD-WAN solutions](#) allows us to simplify the migration process for businesses of all sizes.

About Enable IP

EnableIP is a telecom solutions provider founded by Wired Networks' founder Jeremy Kerth and head engineer Steve Roos after they realized there was a deep market need for helping mid-size businesses establish better uptime rates for their Wide Area Networks (WANs). Armed with the best-in-class carriers and partners, Jeremy and Steve set out with a bold plan: **Guarantee better uptime rates than the industry standard of only 99.5%.**

Their bold plan became a reality. EnableIP's solutions guarantee clients 99.99% (even 99.999%) network uptime. But we don't stop there. Many telecom providers promise high availability network solutions but fail to deliver because they're in the business of providing services, not solutions.

That's the EnableIP difference: We deliver highly available networks by providing a complete system (called "Cloud Assurance") that ensures 99.99% or above uptime.

We deliver this bold promise by:

- Owning the entire customer experience. From pricing, contracting, ordering and provisioning to installing, servicing and billing—we do it all! This means no stressful negotiations, confusing setups, or finger pointing if something goes wrong. We actually *deliver* on our promise.
- We manage the entire system, and monitor and manage issues as they occur so you can focus on your business—not your network.

The Enable IP solution is like no other. [Contact us](#) to get started and experience the difference of a system that truly delivers on its 99.99% network uptime promise.