

Transport-agnostic VPNs using Cisco SD-WAN

Use case scenario

The Cisco SD-WAN solution is a cloud-delivered overlay WAN architecture that enables digital and cloud transformation at enterprises. It significantly reduces WAN costs and time to deploy new services, and, builds a robust security architecture crucial for hybrid networks.

Executive summary

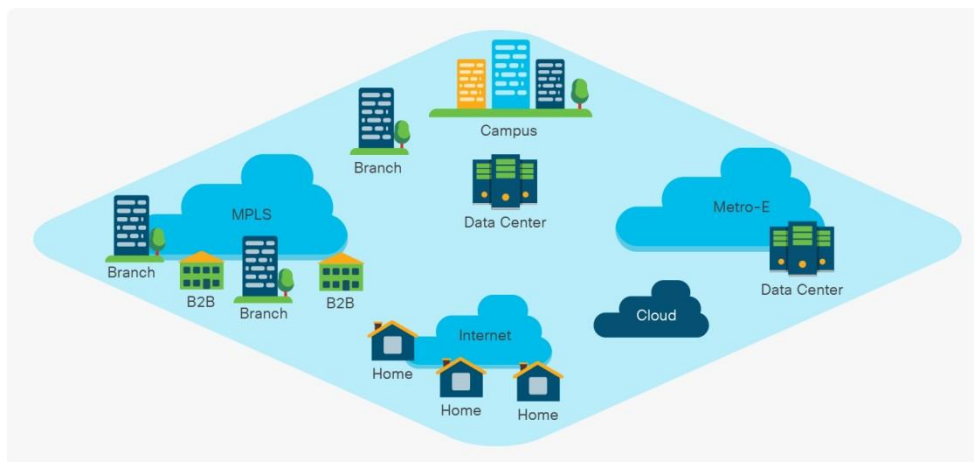
MPLS Layer 3 VPNs were designed for connectivity when most branch-office traffic flowed within an enterprise's perimeter. However, new applications and cloud service models are shifting traffic patterns. Today, most enterprise traffic flows to public clouds and the Internet. There is an increasing requirement for high bandwidth for new applications, and an agile operational model to support digital transformation. Networking teams need to support a hybrid WAN model that introduces new challenges for secure connectivity, real-time application performance, efficient cloud experience, and dynamic change control.

Cisco SD-WAN (based on Viptela) is a cloud-aware, overlay architecture that provides the benefits of MPLS VPN but across all kinds of hybrid transports like broadband, MPLS, LTE and more.

Current network design

Figure 1 shows a typical enterprise network architecture. Multiple networks are needed to connect various facilities — campus, data centers, branches, and business partners — because MPLS cannot solve the connectivity requirements of all these entities.

Figure 1. A typical enterprise network



The MPLS problem

MPLS Layer 3 VPNs were designed for private multisite connectivity. However, many challenges exist with this network infrastructure:

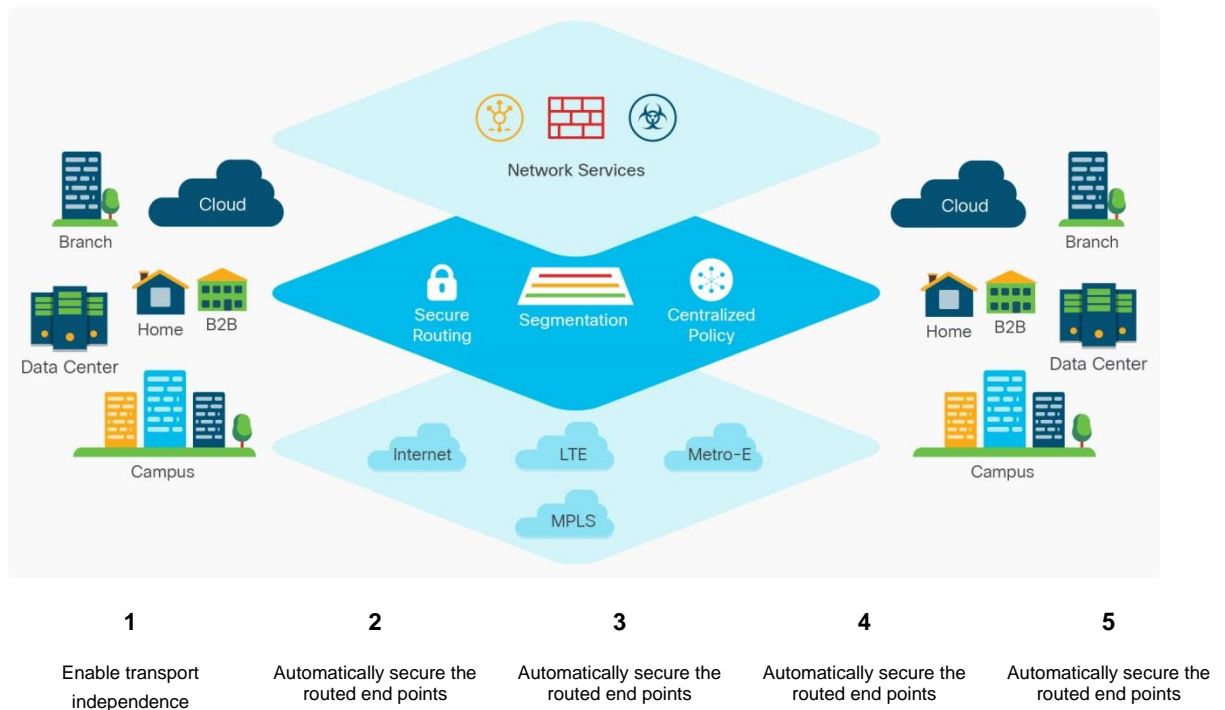
- No cost-effective option to deal with the increased capacity requirements for Virtual Desktop Infrastructure (VDI), video, and other high-bandwidth applications
- Poor user experience for cloud applications and Internet access because of the centralized DMZ architecture
- Security isolation is not guaranteed, so encryption is required
- No end-to-end network segmentation between lines of business and B2B partners
- Months of lead time to add new sites and business partners

A new approach is needed to address these problems.

Cisco SD-WAN approach

The Cisco SD-WAN solution based on Viptela technology provides enterprises with a single solution for secure, ubiquitous connectivity. It offers all the major benefits of MPLS Layer 3 VPN service and works over any underlying transport. This solution entails virtualizing the network and critical services in five steps shown below.

Figure 2. Five steps to virtualizing the network

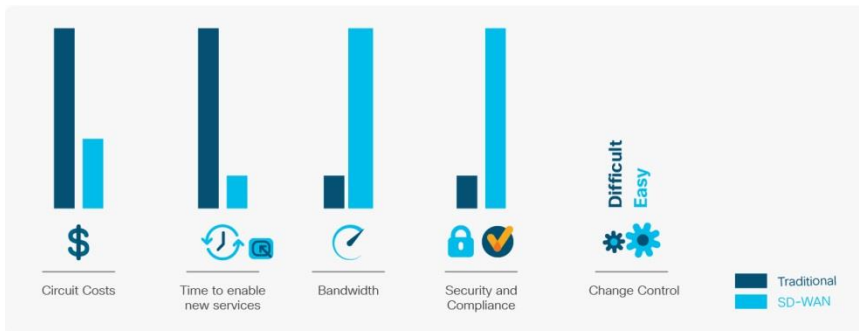


The Cisco SD-WAN solution helps enterprises:

- Provide secure connectivity anywhere
- Extend the benefits of virtualization outside the data center
- Rapidly deploy new services and applications

For the CIO, this translates to a savings of up to 80 percent in WAN Operating Expenses (OpEx), a significant improvement in time to deploy new services, and a consistent high level of security across the network.

Figure 3. SD-WAN ROI



Deployment options from MPLS to Cisco SD-WAN

Enterprises can deploy the Cisco SD-WAN solution in conjunction with an existing MPLS network, or alternatively, to completely replace MPLS Layer 3 VPNs.

Step 1

Backup for MPLS: You can initially deploy Cisco SD-WAN as a backup for MPLS at some or all sites. This topology helps to ensure that the enterprise sites are always connected. With any failure in the MPLS service, all sites seamlessly transition to the SD-WAN overlay network. That way, enterprises can take advantage of Internet and LTE connections for additional last-mile resilience.

Step 2

Traffic steering for high-bandwidth and cloud applications: High-bandwidth applications like video, VDI, Internet, and cloud applications are straining the low-bandwidth MPLS pipes. To address this situation, you can deploy the Cisco SD-WAN solution alongside MPLS VPNs to carry these high-bandwidth applications.

Step 3

New sites onto SD-WAN: Footprint limitations in the carrier's network introduce delays in bringing up new sites. An SD-WAN enabled site can be up and running immediately over the Internet or LTE, and provide secure, high-bandwidth integration into the rest of the MPLS network.

Step 4

Replace MPLS: The Cisco SD-WAN solution can completely replace MPLS VPNs, helping enterprises take advantage of high-bandwidth commodity links to build a secure overlay to all entities in the network. This solution greatly simplifies the entire network and provides the greatest cost savings.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)