Cisco Catalyst SD-WAN

Design, Deploy, and Secure Your WAN

Second Edition

ANASTASIYA VOLKOVA
CCIE® X2 (ENT & SEC) NO. 54378
OSVALDO SALAZAR TOVAR
CONSTANTIN MOHOREA
CCIE® X2 (ENT, SEC) NO. 16223, CCDE® NO. 20170054
DUSTIN SCHUEMANN
CCIE® (ENT) NO. 59235

ciscopress.com

Cisco Catalyst SD-WAN: Design, Deploy, and Secure Your WAN

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, and more!

To access the companion website, simply follow these steps:

1. Go to **www.ciscopress.com/register**.
2. Enter the **print book ISBN:** 9780138313906.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

Finally, for the underlay backup architecture to work correctly, it is important to do some filtering at the data center. To ensure that remote branch routes are learned and preferred through the overlay (and asymmetry or route looping is avoided), create an outbound filter toward the WAN Edge router to limit the learned routes to those originating from the data center. Make sure to also advertise a default route or summary routes into the overlay. Figure 5-44 shows this design option.

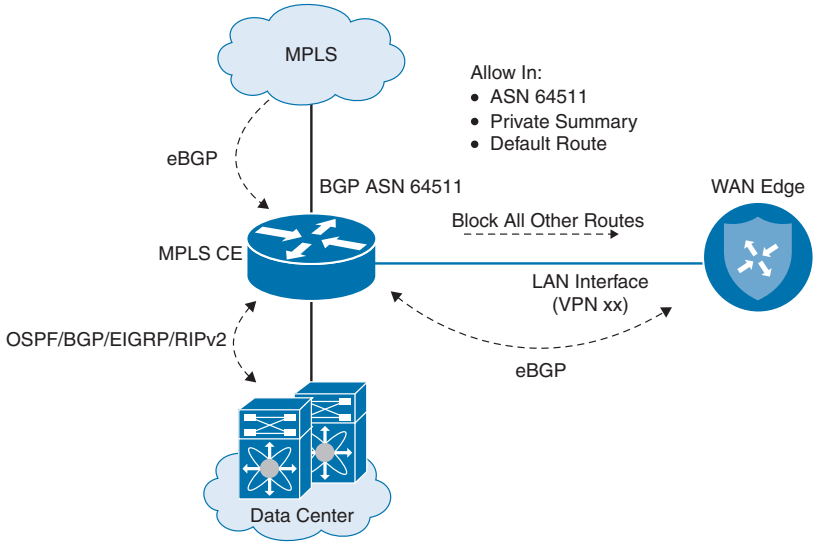

Figure 5-44 *Overlay with Underlay Backup: Data Center Considerations*

Figure 5-45 reviews the traffic flow patterns experienced when using an overlay with an underlay backup design.

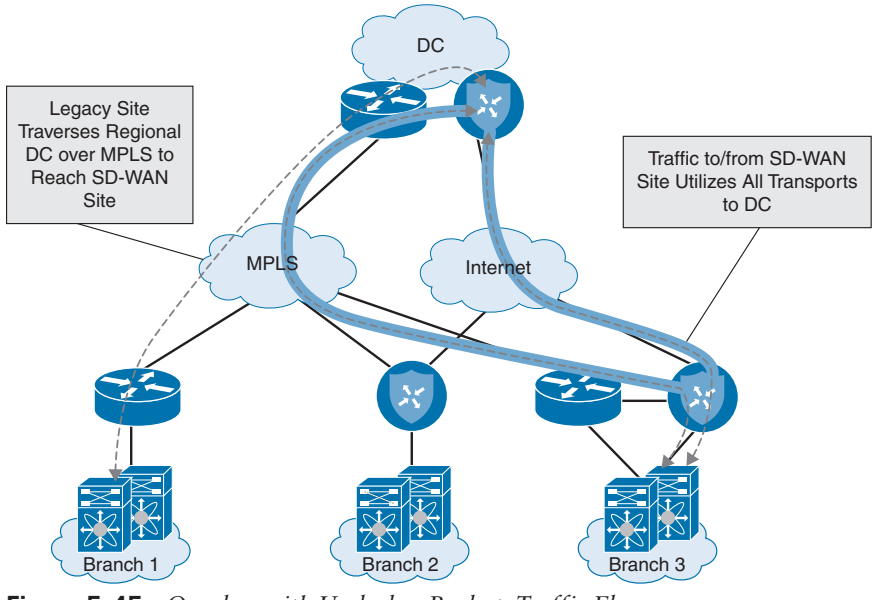

Figure 5-45 *Overlay with Underlay Backup Traffic Flow*

It is also important to see the traffic flow during a failover condition. This helps visualize the path the traffic will take during a failure scenario. Figure 5-46 highlights the backup traffic flow during a failover event.

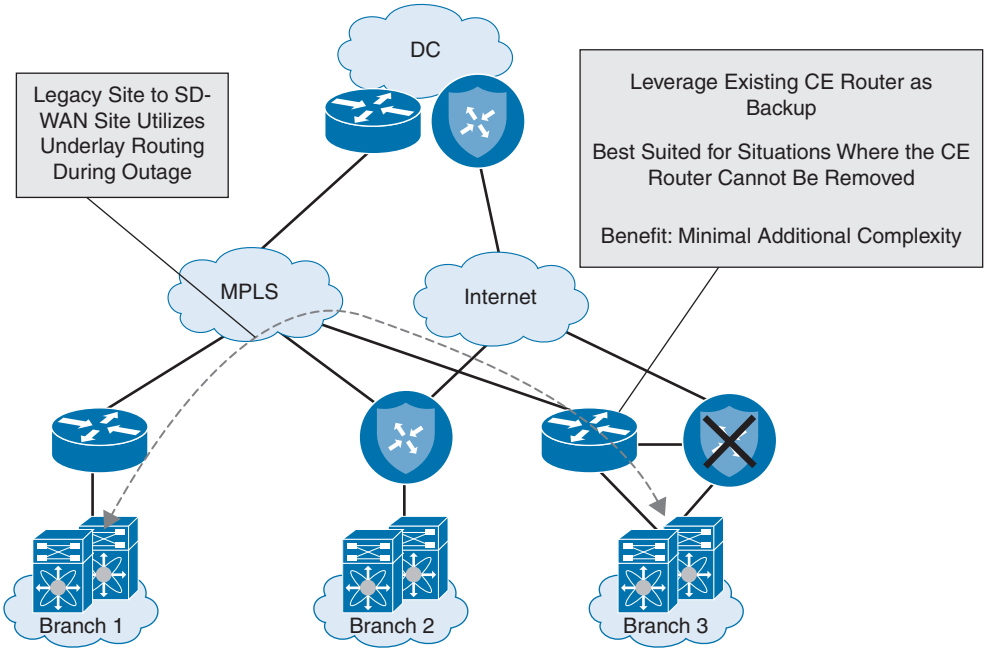

Figure 5-46 *Overlay with Underlay Backup Traffic Flow During Failover*

Full Overlay and Underlay Integration

For some organizations, due to strict application latency requirements, certain branches migrated to Cisco SD-WAN may need to communicate directly with non-migrated branches through a lower-latency underlay path. For example, CIFS traffic, which is relatively sensitive to latency, may suffer from going through additional hops at the data center for transit to another site. To address this latency requirement, SD-WAN network can be architected to use the overlay path for communication with migrated sites and the underlay path for communication with non-migrated sites, enabling full overlay and underlay integration. Figure 5-47 shows routing from a non-SD-WAN site to a Cisco SD-WAN site in this scenario. Figure 5-48 illustrates the traffic flow between two Cisco SD-WAN sites while leveraging a full overlay and underlay integration design.

NOTE In most cases, configuring full overlay and underlay integration at every site will add a significant amount of routing complexity to the network and, in some environments, can be a challenge to scale and control. Typically, voice applications can handle 300 ms of round-trip latency, and therefore this design might not even be required.

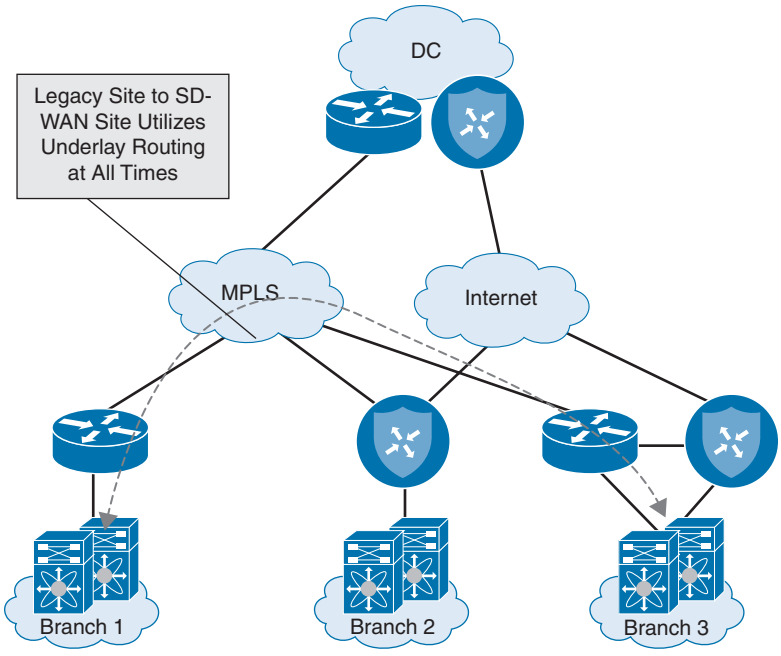

Figure 5-47 *Full Overlay with Underlay Routing: Legacy Site to SD-WAN Site Traffic Flow*

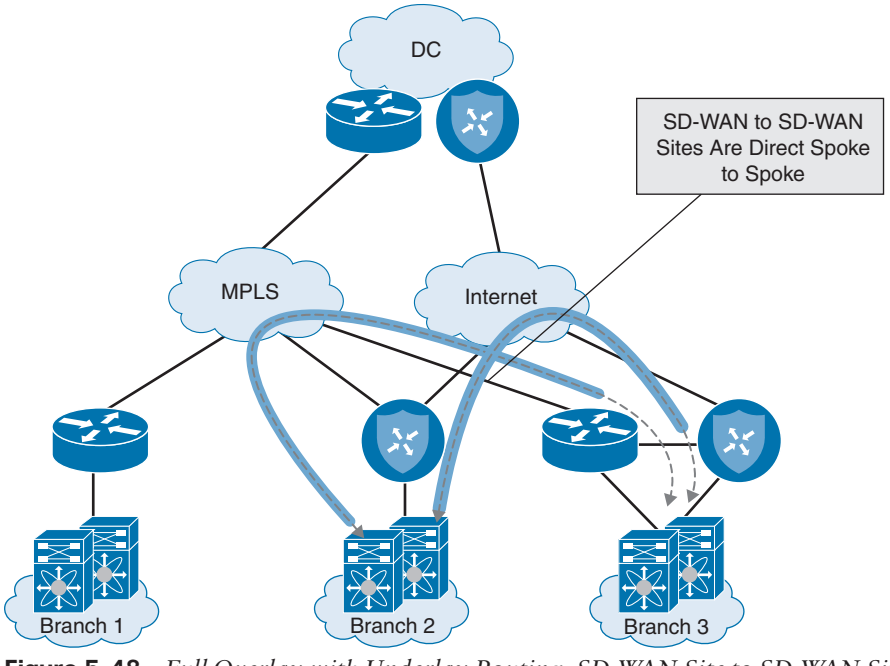

Figure 5-48 *Full Overlay with Underlay Routing: SD-WAN Site to SD-WAN Site Traffic Flow*

One way to implement full overlay and underlay integration at a branch is through the use of an existing MPLS CE router. This design is similar to the MPLS CE router integration solution discussed previously, with the difference being that the CE router continues to advertise the site prefixes into the MPLS underlay while the WAN Edge router simultaneously advertises the site prefixes into the overlay. Both the MPLS CE router and WAN Edge router advertise prefixes from the WAN into the LAN. However, the WAN Edge router should advertise SD-WAN migrated site prefixes (including data center prefixes) with a more attractive metric to retain traffic symmetry and to force Cisco SD-WAN sites to talk to each other via the overlay. While any routing protocol can be used to achieve this design, BGP is recommended for its native anti-transit logic. If any other routing protocol is used, tagging and filtering mechanisms should be used to avoid making the branch into a transit site. Figure 5-49 shows this design option.

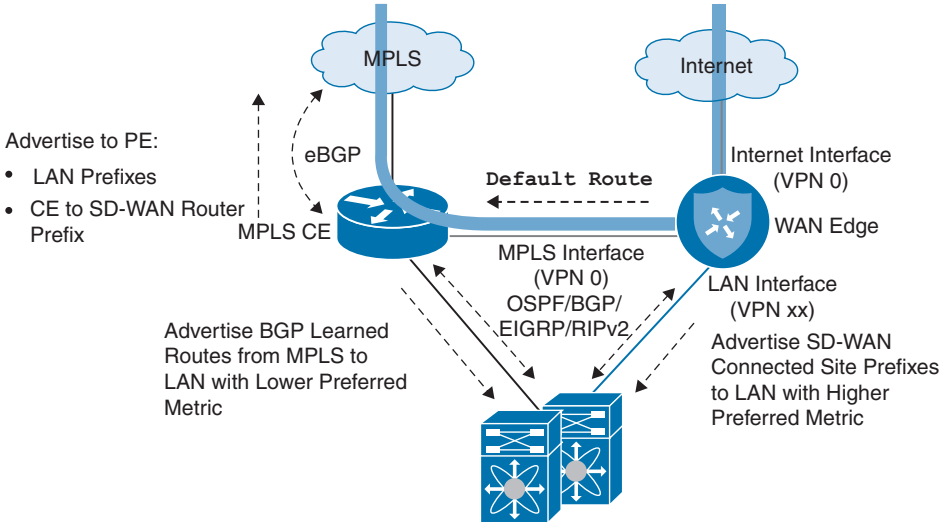

Figure 5-49 *Full Overlay with Underlay Routing: CE Integration*

Figure 5-50 shows the traffic flow for a branch with two transports. Traffic can flow directly through an Internet interface as well as through an interface that is connected to an existing MPLS CE router.

Full overlay and underlay integration can also be achieved without a dedicated MPLS CE router when only a WAN Edge router exists at the branch. The same principles apply as if there were a separate MPLS CE router; however, TLOC termination on the WAN Edge router is a bit different. Instead of configuring the TLOC on the physical interface connected to the MPLS carrier, a loopback interface is created in VPN 0, bound to the physical WAN interface, and configured as the TLOC. This configuration is required to remove TLOC configuration, along with the associated implicit ACL, from the physical interface. Without it, non-SD-WAN transit traffic received on MPLS from legacy sites will be dropped.

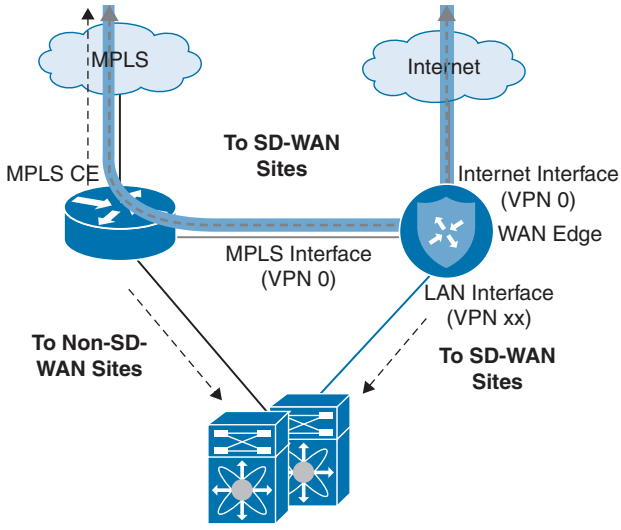

Figure 5-50 *Full Overlay with Underlay Routing: CE Integration Traffic Flow*

A routing protocol is configured between the WAN Edge router and the carrier in order to advertise the loopback interface IP address for control and data plane tunnel termination. A VPN 0 interface is then configured and connected to a downstream (LAN-side) Layer 3 switch. Finally, a routing protocol can be configured on this transit link to learn and advertise overlay routes. This configuration, in effect, creates a route leak between VPNs. Figure 5-51 shows this design option.

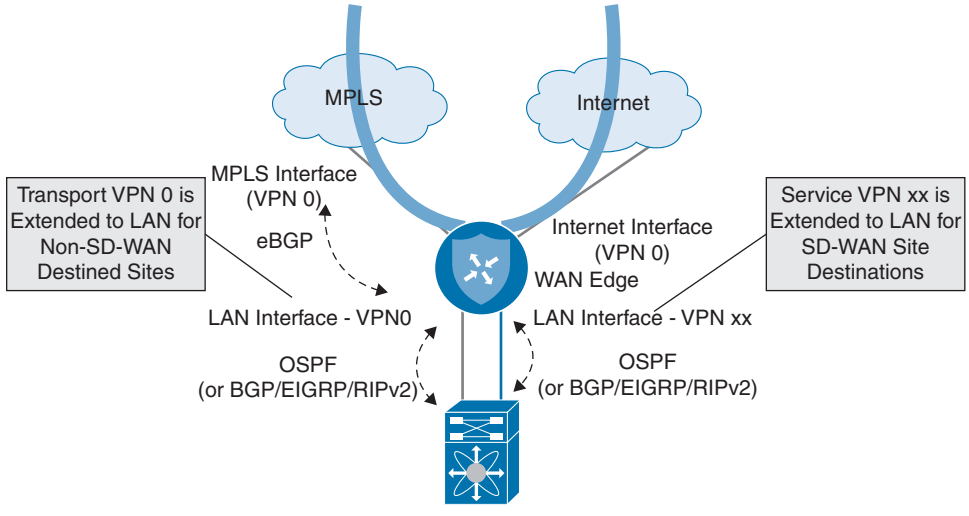

Figure 5-51 *Full Overlay with Underlay Routing: Without CE Integration*

Figure 5-52 illustrates the traffic flow for a site location with no integration with a CE device.

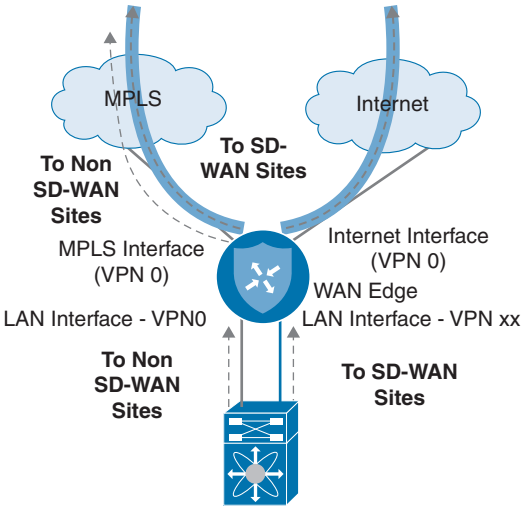

Figure 5-52 *Full Overlay with Underlay Routing: Without CE Integration Traffic Flow*

NOTE Additional tagging, filtering, and best path manipulation may be required at both the data center and the remote sites participating in full overlay/underlay connectivity, depending on how routing between the overlay and underlay is accomplished. From a routing perspective, there are many valid ways to achieve full overlay and underlay integration. Each of these options deserves special attention to avoid routing loops and suboptimal routing. Every environment has unique complexities and caveats, so it's important to think through all the different possible scenarios specific to your organization's network that could affect the flow of traffic during and after migration.

Summary

This chapter covers the design methodology recommended for the implementation of Cisco SD-WAN. It discusses the importance of migration preparation, validated data center and branch designs, and overlay and underlay integration techniques. Cisco SD-WAN implementation requires a solid discovery and design period in which ample time is spent understanding the existing network thoroughly while also thinking about its future state. Preparation prior to deploying the Cisco SD-WAN network is key in ensuring that data center and branch cutovers are executed flawlessly. Understanding the benefits and caveats of all the supported data center and branch designs allows a network architect to select a design that meets the requirements of the business and provides additional Cisco SD-WAN functionalities while maintaining resiliency and performance. Every network has some degree of complexity, and the goal is to implement Cisco SD-WAN gracefully without increasing the complexity.

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 5-4 lists these key topics and the page number on which each is found.