

**SPVI****Implementing Cisco Service Provider VPN Services**

40 horas

Service Provider

Cisco

**Cisco Continuing Education Credits****40 CE Credits****INTRODUÇÃO**

The Implementing Cisco Service Provider VPN Services (SPVI) v1.0 course prepares you to manage end-customer Virtual Private Network (VPN) environments built over a common service provider Multiprotocol Label Switching (MPLS) backbone. You will complete hands-on labs to reinforce MPLS VPN fundamental concepts, benefits, and classification, MPLS components, MPLS control plane and data plane operations, MPLS VPN routing using Virtual Routing and Forwarding (VRF), Layer 2 and Layer 3 MPLS VPNs, IPv6 MPLS VPN implementations, IP Multicast VPNs, and shared services VPNs. The course also covers solutions for deploying MPLS VPN crossing multiple Service Provider domains that improve the use of network bandwidth.

This course prepares you for the 300-515 Implementing Cisco® Service Provider VPN Services (SPVI) exam. By passing this exam, you earn the Cisco Certified Specialist - Service Provider VPN Services Implementation certification, and you satisfy the concentration exam requirement for the CCNP® Service Provider certification. This course also earns you 40 Continuing Education (CE) credits towards recertification.

This course will help you:

- Gain valuable skills in reinforcing MPLS VPN fundamental concepts, benefits, and classifications;
- Learn to configure optional paths for traffic to avoid network congestion;
- Prepare to take the 300-515 SPVI exam.

The 300-515 SPVI exam certifies your knowledge of implementing service provider VPN services including Layer 2, Layer 3, and IPv6. After you pass 300-515 SPVI, you earn the Cisco Certified Specialist - Service Provider VPN Services Implementation certification, and you satisfy the concentration exam requirement for the CCNP Service Provider certification.

## OBJETIVO DO CURSO

---

After taking this course, you should be able to:

- Describe VPN concepts and operation in a Service Provider environment;
- Implement Layer 3 MPLS VPN operations in a Service Provider environment;
- Implement Layer 3 Inter-domain MPLS VPN services traversing multiple Service Providers;
- Implement Layer 3 Multicast MPLS VPN operations in a Service Provider environment;
- Troubleshoot typical issues in Layer 3 MPLS VPN environments;
- Implement Layer 2 VPN operations in a Service Provider environment;
- Troubleshoot Layer 2 VPN issues in a Service Provider network;
- Implement MPLS VPN solutions for IPv6 environments;
- Troubleshoot MPLS VPN solutions for IPv6 environments.

## PÚBLICO-ALVO

---

This course is for network professionals who need to learn the techniques to implement, configure, monitor, and support Service Provider VPN solutions based on MPLS backbones.

- Network administrators
- Network engineers
- Network supervisors
- Network managers
- Network Operations Center (NOC) personnel
- Network designers
- Network architects
- Channel partners

## PRÉ-REQUISITOS

---

Before taking this course, you should have Service Provider knowledge at the professional level, equivalent to the material in the following Cisco courses:

- Building Cisco Service Provider Next-Generation Networks Part 1 (SPNGN1) v1.2;
- Building Cisco Service Provider Next-Generation Networks Part 2 (SPNGN2) v1.2;
- Deploying Cisco Service Provider Network Routing (SPROUTE).

In the new certification program, foundational material is covered in these courses:

- Implementing and Administering Cisco Solutions (CCNA®)  
Understanding Cisco Service Provider Network Foundations (SPFNDU);
- Implementing and Operating Cisco Service Provider Network Core Technologies (SPCOR).

## Introducing VPN Services

VPN Fundamentals

MPLS VPN Control Plane Operation

## Troubleshooting MPLS VPN Underlay

Troubleshoot Core Interior Gateway Protocol (IGP)

Troubleshoot Border Gateway Protocol (BGP)

## Implementing Layer 3 MPLS VPNs

Multiprotocol BGP (MP-BGP) Routing Requirements in MPLS VPNs

Provider Edge to Customer Edge (PE-to-CE) Routing Requirements in Layer 3 MPLS VPNs

## Implementing Layer 3 Interdomain MPLS VPNs

Inter-Autonomous System (AS) for Layer 3 MPLS VPNs

Content Security and Control (CSC) for Layer 3 MPLS VPNs

## Implementing Layer 3 Multicast MPLS VPNs

Multicast VPN (MVPN) Fundamentals

Implement Intranet MVPN

## Troubleshooting Intra-AS Layer 3 VPNs

Troubleshoot PE-CE Connectivity

Troubleshoot PE-to-Route Reflector

## Implementing Layer 2 VPNs

Layer 2 Service Architecture and Carrier Ethernet Services

Refresh on Traditional Ethernet LAN (E-LAN), E-Line, and E-Tree Solutions

## Troubleshooting Layer 2 VPNs

Troubleshoot Common Issues for Traditional E-Line, E-LAN, and E-Tree Ethernet Solutions

Troubleshoot Common Issues for Ethernet VPN (EVPN) Native, EVPN Virtual Private Wire Service (VPWS), and EVPN Integrated Routing and Bridging (IRB) Solutions

## Implementing Layer 3 IPv6 MPLS VPNs

Classical Solutions for Deploying IPv6 over IPv4 Environments

Using 6VPE to Deploy IPv6 Connectivity over MPLS Environment

## Troubleshooting Layer 3 IPv6 MPLS VPNs

Troubleshooting PE-to-PE Connectivity

## Lab outline

Verify the Service Provider Backbone Operation for MPLS VPN

Work with VRF Instances

Troubleshoot the MPLS VPN Backbone

Configure MP-BGP as the PE-CE Routing Protocol

Configure and Verify PE-to-CE Routing Requirements

Enable Shared Services VPN

Deploy Internet Access as a VPN Service

Troubleshoot Layer 3 MPLS VPN End-Customer Connectivity

Implement Different EVPN Solutions

Troubleshoot EVPN VPWS

Implement IPv6 VPN Provider Edge Router (6VPE)