CCIE Service Provider

Introduction

Software, networking, and infrastructure grow more and more interconnected every day. Applications deliver exciting new experiences, and with intent-based networking, service providers can take advantage of automation to scale and secure their infrastructure. With CCIE Service Provider certification, your opportunities to help maximize that potential are boundless. Just ask hiring managers: 71% of them say that certifications increase their confidence in an applicant's abilities.

CCIE Service Provider certification helps you position yourself as a technical leader in the ever-changing landscape of service provider networking. The certification covers core technology areas and validates your end-to-end lifecycle skills in complex service provider networking, from planning and design to operating and optimizing.

Exams and Recommended Training

1. 350-501 SPCOR: Implementing and Operating Cisco Service Provider Network Core Technologies

The Implementing and Operating Cisco Collaboration Core Technologies (CLCOR) v1.0 course helps you prepare for advanced-level roles focused on the implementation and operation of Cisco collaboration solutions. You will gain the knowledge and skills needed to implement and deploy core collaboration and networking technologies, including infrastructure and design, protocols, codecs, and endpoints, Cisco Internetwork Operating System (IOS®) XE gateway and media resources, call control, Quality of Service (QoS), and additional Cisco collaboration applications. This course earns you 64 Continuing Education (CE) credits towards recertification.

Duration

5 Days

Course Objectives

- Describe the Service Provider network architectures, concepts, and transport technologies
- Describe the Cisco Internetwork Operating System (Cisco IOS®) software architectures, main IOS types, and their differences
- Implement Open Shortest Path First (OSPF) in the Service Provider network
- Implement Integrated Intermediate System-to-Intermediate System (IS-IS) in the Service Provider network
- Implement Border Gateway Protocol (BGP) routing in Service Provider environments
- Implement route maps and routing policy language
- Describe IPv6 transition mechanisms used in the Service Provider networks
- Implement high-availability mechanisms in Cisco IOS XR software
- Implement traffic engineering in modern Service Provider networks for optimal resource utilization
- Describe segment routing and segment routing traffic engineering concepts
- Describe the VPN technologies used in the Service Provider environment
- Configure and verify Multiprotocol Label Switching (MPLS) L2VPN in Service Provider environments
- Configure and verify MPLS L3VPN in Service Provider environments
- Implement IP multicast services

- Describe the Quality of Service (QoS) architecture and QoS benefits for SP networks
- Implement QoS in Service Provider environments
- Implement control plane security in Cisco devices
- Implement management plane security in Cisco devices
- Implement data plane security in Cisco devices
- Describe the Yet Another Next Generation (YANG) data modeling language
- Implement automation and assurance tools and protocols
- Describe the role of Cisco Network Services Orchestrator (NSO) in Service Provider environments
- Implement virtualization technologies in Service Provider environments

Prerequisites

- Intermediate knowledge of Cisco IOS or IOS-XE
- Familiarity with Cisco IOS or IOS XE and Cisco IOS XR Software configuration
- Knowledge of IPv4 and IPv6 TCP/IP networking
- Intermediate knowledge of IP routing protocols
- Understanding of MPLS technologies
- Familiarity with VPN technologies

Target Audience

- Network administrators
- Network engineers
- Network managers
- System engineers
- Project managers
- Network designers

Course Outline

- Describing Service Provider Network Architectures
- Describing Cisco IOS Software Architectures
- Implementing OSPF
- Implementing IS-IS
- Implementing BGP
- Implementing Route Maps and Routing Protocol for LLN [Low-Power and Lossy Networks] (RPL)
- Transitioning to IPv6
- Implementing High Availability in Networking
- Implementing MPLS
- Implementing Cisco MPLS Traffic Engineering
- Describing Segment Routing
- Describing VPN Services
- Configuring L2VPN Services
- Configuring L3VPN Services
- Implementing Multicast
- Describing QoS Architecture
- Implementing QoS
- Implementing Control Plane Security
- Implementing Management Plane Security
- Implementing Data Plane Security
- Introducing Network Programmability
- Implementing Automation and Assurance
- Introducing Cisco NSO
- Implementing Virtualization in Service Provider Environments

Lab Outline

- Deploy Cisco IOS XR and IOS XE Basic Device Configuration
- Implement OSPF Routing
- Implement Integrated IS-IS Routing
- Implement Basic BGP Routing
- Filter BGP Prefixes Using RPL
- Implement MPLS in the Service Provider Core
- Implement Cisco MPLS Traffic Engineering (TE)
- Implement Segment Routing
- Implement Ethernet over MPLS (EoMPLS)
- Implement MPLS L3VPN
- Implement BGP Security
- Implement Remotely Triggered Black Hole (RTBH) Filtering

2. CCIE Service Provider (v5.0) Exam Topics (Practical Exam)

The Cisco CCIE Service Provider (v5.0) Practical Exam is an eight-hour, hands-on exam that requires a candidate to plan, design, implement, operate, and optimize dual-stack solutions (IPv4 and IPv6) of complex service provider networks.

Candidates are expected to program and automate the network within their exam, as per the exam topics below.

The following topics are general guidelines for the content likely to be included in the exam. Your knowledge, skills, and abilities on these topics will be tested throughout the entire network lifecycle unless explicitly specified otherwise within this document.

The exam is closed book and no outside reference materials are allowed.

Duration

8 Hours

Prerequisites

There are no formal prerequisites for CCIE Service Provider, but you should have a thorough understanding of the exam topics before taking the exam.

CCIE candidates are recommended to have five to seven years of experience with designing, deploying, operating, and optimizing service provider technologies and solutions prior to taking the exam.

Course Outline

1. **Core Routing (25%)**

    1.1 Interior Gateway Protocol

        1.1.a IS-IS
        1.1.b OSPFv2 and OSPFv3
        1.1.c Optimize IGP scale and performance
        1.1.d IS-IS segment routing control plane for IPv4 and IPv6
        1.1.e OSPFv2 and OSPFv3 segment routing control plane

    1.2 Border Gateway Protocol

        1.2.a IBGP, EBGP, and MP-BGP

- 1.2.b BGP route policy enforcement
- 1.2.c BGP path attribute
- 1.2.d BGP scale and performance
- 1.2.e BGP segments, BGP Labeled Unicast, and Linked State

1.3 Multicast

- 1.3.a Design PIM (PIM-SM, PIM-SSM, and PIM-BIDIR)
- 1.3.b Design RP (Auto-RP, BSR, Static, Anycast RP, and MSDP)
- 1.3.c Design IGMP and MLD
- 1.3.d MLDP
- 1.3.e P2MP RSVP-TE
- 1.3.f Tree-sid

1.4 Multiprotocol Label Switching

- 1.4.a MPLS forwarding and control plane mechanisms
- 1.4.b LDP
- 1.4.c LDP scale and performance
- 1.4.d SR (SRGB and Max Labels Depth)
- 1.4.e LDP and SR Interworking - Segment routing mapping server

1.5 MPLS Traffic Engineering

- 1.5.a ISIS and OSPF extensions
- 1.5.b RSVP-TE
- 1.5.c MPLS TE policy enforcement
- 1.5.d MPLS LSP attributes
- 1.5.e SR-TE
- 1.5.f PCE and PCEP technology
- 1.5.g Flexible Algorithm
- 1.5.h Optimize MPLS TE scale and performance

2. Architectures and Services (25%)

2.1 Virtualized Infrastructure

- 2.1.a Design NFVI
- 2.1.b Design Cloud scale networking Infrastructure
- 2.1.c Design IaaS (Openstack) underlay architecture using Bare metal and Virtual Machines
- 2.1.d Design convergence, virtual scaling, network Slicing, edge distribution, in 5G Architecture

2.2 Large scale MPLS Architecture

- 2.2.a Unified MPLS
- 2.2.b Multi-domain Segment Routing with SR-PCE
- 2.2.c SLA based on IGP/TE metrics and Disjoint Paths

2.3 Carrier Ethernet

- 2.3.a E-LINE, E-LAN, and E-TREE.
- 2.3.b VPWS, VPLS and H-VPLS
- 2.3.c EVPN, EVPN-VPWS, EVPN-IRB
- 2.3.d L2VPN service auto-steering into segment routing policy

2.4 L3VPN

- 2.4.a L3VPN
- 2.4.b Inter-AS L3VPN
- 2.4.c Shared services, for example: Extranet and Internet access
- 2.4.d L3VPN service auto-steering into segment routing policy

2.5 Internet service

- 2.5.a IPv4 translation mechanism, for example: NAT44, CGNAT
- 2.5.b IPv6 transition mechanism, for example: NAT64, 6RD, MAP, and DS Lite
- 2.5.c Internet peering route and transit policy enforcement

2.6 Multicast VPN

- 2.6.a Rosen mVPN
- 2.6.b NG mVPN

2.7 Quality of Service for Core, Distribution, and Access

- 2.7.a Classification and marking
- 2.7.b Congestion management and scheduling

2.7.c Congestion avoidance
2.7.d MPLS QoS models (Pipe, Short Pipe, and Uniform)
2.7.e MPLS TE QoS (MAM, RDM, CBTS, PBTS, and DS-TE)

3. Access Connectivity (10%)

3.1 Layer-2 Connectivity
3.1.a IEEE 802.1ad (Q-in-Q), IEEE 802.1ah (Mac-in-Mac), and ITU G.8032, REP
3.1.b Spanning-Tree Access Gateway (MST-AG and PVST-AG)
3.1.c Design and Operate MC-LAG
3.2 Layer-3 Connectivity
3.2.a PE-CE routing protocols (OSPF, ISIS, and BGP)
3.2.b Loop prevention techniques in multihomed environments

4. High Availability and Fast Convergence (10%)

4.1 High Availability
4.1.a (SS0/NSF, NSR, and GR)
4.2 Routing/fast convergence
4.2.a IGP convergence
4.2.b LDP convergence
4.2.c BGP convergence - Prefix Independent Convergence (BGP-PIC)
4.2.d BFD
4.2.e LFA-FRR (LFA, Remote LFA, and TI-LFA)
4.2.f MPLS TE FRR

5. Security (10%)

5.1 Control plane security
5.1.a Control plane protection techniques (LPTS and CoPP)
5.1.b Routing Protocol and LDP authentication and security
5.1.c BGP prefix-based and attribute-based filtering
5.1.d BGP-RPKI (Origin AS validation)
5.2 Management plane security
5.2.a Implement and troubleshoot device management (MPP, SSH, and VTY)
5.2.b Implement and troubleshoot logging and SNMP security
5.2.c Implement and troubleshoot AAA
5.3 Infrastructure security
5.3.a ACL
5.3.b uRPF
5.3.c RTBH and Router Hardening
5.3.d BGP Flowspec

6. Assurance and Automation (20%)

6.1 Network Assurance
6.1.a Syslog and logging functions
6.1.b SNMP traps and RMON
6.1.c NetFlow and IPFIX
6.1.d Segment Routing OAM and MPLS OAM
6.1.e Segment Routing Data Plane monitoring
6.1.f IP/MPLS Performance monitoring (TCP, UDP, ICMP, and SR)
6.1.g Ethernet OAM (Y.1564 and Y.1731)
6.2 Network Automation
6.2.a Design, deploy and optimize NSO service packages (Yang model, template-based, python-based, fast map, reactive fast map, CLI NEDs, NETCONF NEDs, NSO northbound integration using REST and RESTCONF).
6.2.b Design NFV orchestration (NFVO) using NSO and ESC in an ETSI NFV architecture.

6.2.c Design and deploy Model-driven telemetry on XR devices (Yang models, gRPC, GPB, device configuration, collection architecture)
6.2.d Deploy and Optimize Ansible playbook scripts that interact with NSO, IOS-XE, and IOS-XR devices