CCDE v3.0 Unified Exam Topics

Exam Description: The exam topics below are general guidelines for the content likely to be included on both the CCDE Written (400-007) and the CCDE Practical exam.

The **CCDE v3.0 Written exam (400-007)** is a two-hour, multiple choice test with 90-110 questions, that focuses on core Enterprise network architectures and technologies.

The **CCDE v3.0 Practical Exam** is an 8-hour scenario-based exam, that focuses on core Enterprise network architectures and technologies, as well as on your selected area of expertise.

Both exams validate your knowledge, skills, and abilities throughout the entire network design lifecycle. Both exams are closed book and no outside reference materials are allowed.

Your knowledge, skills, and abilities of recommending, building, validating, optimizing, and adapting technologies/solutions in the context of complex high-level network designs will be tested throughout the exam:

- Recommend technologies or solutions that align with the stated requirements.
- Justify why a given decision was made.
- Make design choices and fully design solutions that complies with the stated requirements.
- Validate existing designs to ensure they are compliant with all requirements, as well as suggesting design changes to accommodate for changed specifications or requirements in the network.
- Perform optimizations of existing network designs to fix issues or mitigate risks.
- Build high-level implementation plans/steps.
- Recommend, build, or justify strategies.

Both the Written and Practical exams are designed with dual stack in mind, so both IPv4 and IPv6 should be expected across every exam topic and technology.

For more information about the exam format and the technologies covered within your exam, please refer to:

- CCDE v3.0 Written and Practical Exam Format
- Core - technology list
- Workforce Mobility - technology list
- On-Prem and Cloud Services - technology list
- Large Scale Networks - technology list

15% 1.0 Business Strategy Design

1.1 Impact on network design, implementation, and optimization using various customer project management methodologies (for instance waterfall and agile)

1.2 Solutions based on business continuity and operational sustainability (for instance RPO, ROI, CAPEX/OPEX cost analysis, and risk/reward)

25% 2.0 Control, data, management plane and operational design

2.1 End-to-end IP traffic flow in a feature-rich network

2.2 Data, control, and management plane technologies

2.3 Centralized, decentralized, or hybrid control plane

2.4 Automation/orchestration design, integration, and on-going support for networks (for instance interfacing with APIs, model-driven management, controller-based technologies, evolution to CI/CD framework)

2.5 Software-defined architecture and controller-based solution design (SD-WAN, overlay, underlay, and fabric)

30% 3.0 Network Design

3.1 Resilient, scalable, and secure modular networks, covering both traditional and software-defined architectures, considering:

- 3.1.a Technical constraints and requirements
- 3.1.b Operational constraints and requirements
- 3.1.c Application behavior and needs
- 3.1.d Business requirements
- 3.1.e Implementation plans
- 3.1.f Migration and transformation

15% 4.0 Service Design

4.1 Resilient, scalable, and secure modular network design based on constraints (for instance technical, operational, application, and business constraints) to support applications on the IP network (for instance voice, video, backups, data center replication, IoT, and storage)

4.2 Cloud/hybrid solutions based on business-critical operations

- 4.2.a Regulatory compliance
- 4.2.b Data governance (for instance sovereignty, ownership, and locale)
- 4.2.c Service placement
- 4.2.d SaaS, PaaS, and IaaS
- 4.2.e Cloud connectivity (for instance direct connect, cloud on ramp, MPLS direct connect, and WAN integration)
- 4.2.f Security

15% 5.0 Security Design

5.1 Network security design and integration

- 5.1.a Segmentation
- 5.1.b Network access control
- 5.1.c Visibility
- 5.1.d Policy enforcement
- 5.1.e CIA triad
- 5.1.f Regulatory compliance (if provided the regulation)