CCDP

Cisco Certified Design Professional (CCDP) certification is for senior network design engineers, senior analysts, and principal systems engineers, who discuss, design, and create advanced addressing and routing, security, data center, and IP multicast multi-layered enterprise architectures. This includes virtual private networking and wireless domains and it focuses on the design components of larger networks. The CCDP curriculum includes building scalable internetworks and multilayer-switched networks, and designing network service architecture.

Prerequisites: Valid Cisco CCDA and CCNA Routing and Switching or any Cisco CCIE certification can act as a prerequisite**.**

Recommended Training: Implementing Cisco IP Routing (ROUTE), Implementing Cisco IP Switched Networks (SWITCH), Designing Cisco Network Service Architectures (ARCH)

Exams : 642-902 ROUTE, 642-813 SWITCH, 642-874 ARCH

Syllabus:

642-902 ROUTE

1.0 Implement an EIGRP Based Solution, given a Network Design and a set of Requirements

- 1.1 Determine network resources needed for implementing EIGRP in a network
- 1.2 Create an EIGRP implementation plan
- 1.3 Create an EIGRP verification plan
- 1.4 Configure EIGRP routing
- 1.5 Verify EIGRP solution was implemented properly using show and debug commands
- 1.6 Document the results of EIGRP implementation and verification

2.0 Implement a Multi-Area OSPF Network, given a Network Design and a set of Requirements

- 2.1 Determine network resources needed for implementing OSPF in a network
- 2.2 Create an OSPF implementation plan
- 2.3 Create an OSPF verification plan
- 2.4 Configure OSPF routing
- 2.5 Verify OSPF solution was implemented properly using show and debug commands
- 2.6 Document the results of OSPF implementation and verification

3.0 Implement an eBGP Based Solution, given a Network Design and a set of Requirements

- 3.1 Determine network resources needed for implementing eBGP in a network
- 3.2 Create an eBGP implementation plan
- 3.3 Create an eBGP verification plan
- 3.4 Configure eBGP routing
- 3.5 Verify eBGP solution was implemented properly using show and debug commands
- 3.6 Document the results of eBGP implementation and verification

4.0 Implement an IPv6 Based Solution, given a Network Design and a set of Requirements

- 4.1 Determine network resources needed for implementing IPv6 in a network
- 4.2 Create an IPv6 implementation plan
- 4.3 Create an IPv6 verification plan
- 4.4 Configure IPv6 routing
- 4.5 Configure IPv6 interoperation with IPv4
- 4.6 Verify IPv6 solution was implemented properly using show and debug commands
- 4.7 Document the results of IPv6 implementation and verification

5.0 Implement an IPv4 or IPv6 Based Redistribution Solution, given a Network Design and a set of Requirements

- 5.1 Create a redistribution implementation plan based upon the results from a redistribution analysis
- 5.2 Create a redistribution verification plan
- 5.3 Configure a redistribution solution
- 5.4 Verify that a redistribution was implemented
- 5.5 Document results of a redistribution implementation and verification plan
- 5.6 Identify the differences between implementing an IPv4 and IPv6 redistribution solution

6.0 Implement Layer 3 Path Control Solution

- 6.1 Create a Layer 3 path control implementation plan based upon the results of the redistribution analysis
- 6.2 Create a Layer 3 path control verification plan
- 6.3 Configure Layer 3 path control
- 6.4 Verify that a Layer 3 path control was implemented
- 6.5 Document results of a Layer 3 path control implementation and verification plan

7.0 Implement Basic Teleworker and Branch Services

- 7.1 Describe broadband technologies
- 7.2 Configure basic broadband connections
- 7.3 Describe basic VPN technologies
- 7.4 Configure GRE
- 7.5 Describe branch access technologies

642-813 SWITCH

1.0 Implement VLAN Based Solution, given a Network Design and a set of Requirements

- 1.1 Determine network resources needed for implementing a VLAN based solution on a network
- 1.2 Create a VLAN based implementation plan
- 1.3 Create a VLAN based verification plan
- 1.4 Configure switch-to-switch connectivity for the VLAN based solution
- 1.5 Configure loop prevention for the VLAN based solution

2.0 Implement a Security Extension of a Layer 2 Solution, given a Network Design and a set of Requirements

- 2.1 Determine network resources needed for implementing a security solution
- 2.2 Create a implementation plan for the security solution
- 2.3 Create a verification plan for the security solution
- 2.4 Configure port security features
- 2.5 Configure general switch security features
- 2.6 Configure private VLANs
- 2.7 Configure VACL and PACL
- 2.8 Verify the Security based solution was implemented properly using show and debug commands
- 2.9 Document results of security implementation and verification

3.0 Implement Switch Based Layer 3 Services, given a Network Design and a set of Requirements

- 3.1 Determine network resources needed for implementing a Switch based Layer 3 solution
- 3.2 Create an implementation plan for the Switch based Layer 3 solution
- 3.3 Create a verification plan for the Switch based Layer 3 solution
- 3.4 Configure routing interfaces
- 3.5 Configure Layer 3 Security
- 3.6 Verify the Switch based Layer 3 solution was implemented properly using show and debug commands
- 3.7 Document results of Switch based Layer 3 implementation and verification

4.0 Prepare infrastructure to Support Advanced Services

- 4.1 Implement a Wireless Extension of a Layer 2 solution
- 4.2 Implement a VoIP support solution
- 4.3 Implement video support solution

5.0 Implement High Availability, given a Network Design and a set of Requirements

- 5.1 Determine network resources needed for implementing High Availability on a network
- 5.2 Create a High Availability implementation plan
- 5.3 Create a High Availability verification plan

- 5.4 Implement first hop redundancy protocols
- 5.5 Implement switch supervisor redundancy
- 5.6 Verify High Availability solution was implemented properly using show and debug commands
- 5.7 Document results of High Availability implementation and verification

642-874 ARCH

1.0 Design Advanced Enterprise Campus Networks

- 1.1 Design for high availability in enterprise networks
- 1.2 Design Layer 2 and Layer 3 campus infrastructures using best practices
- 1.3 Describe enterprise network virtualization considerations
- 1.4 Design for infrastructure services
- 1.5 Identify network management capabilities in Cisco IOS Software

2.0 Design Advanced IP Addressing and Routing Solutions for Enterprise Networks

- 2.1 Create summarizable and structured addressing designs
- 2.2 Describe IPv6 for campus design considerations
- 2.3 Create stable and scalable routing designs for EIGRP for IPv4
- 2.4 Describe IPv4 multicast routing
- 2.5 Create IPv4 multicast services and security designs
- 2.6 Create stable and scalable routing designs for OSPF for IPv4
- 2.7 Create stable and scalable routing designs for BGP for IPv4

3.0 Design WAN Services for Enterprise Networks

- 3.1 Describe Layer 1 - 3 WAN connectivity options
- 3.2 Describe IPsec VPN technology options
- 3.3 Evaluate WAN service provider design considerations
- 3.4 Create site-to-site VPNs designs with appropriate technologies, scaling, and topologies

4.0 Design an Enterprise Data Center

- 4.1 Describe data center network infrastructure best practices
- 4.2 Describe the components and technologies of a SAN network
- 4.3 Describe integrated fabric designs using Cisco Nexus technology
- 4.4 Describe network and server virtualization technologies for the data center
- 4.5 Create an effective e-commerce design
- 4.6 Design a high availability data center network that is modular and flexible

5.0 Design Security Services

- 5.1 Create firewall designs
- 5.2 Create NAC appliance designs
- 5.3 Create IPS/IDS designs
- 5.4 Create remote access VPN designs for the teleworker