Implementing Cisco IP Switched Networks (300-115)

Exam Description: Implementing Cisco IP Switched Networks (SWITCH 300-115) is a 120-minute qualifying exam with 45–55 questions for the Cisco CCNP and CCDP certifications. The SWITCH 300-115 exam certifies the switching knowledge and skills of successful candidates. They are certified in planning, configuring, and verifying the implementation of complex enterprise switching solutions that use the Cisco Enterprise Campus Architecture.

The SWITCH exam also covers highly secure integration of VLANs and WLANs.

The following topics are general guidelines for the content that is likely to be included on the exam. However, other related topics may also appear on any specific version of the exam. To better reflect the contents of the exam and for clarity, the following guidelines may change at any time without notice.

65% 1.0 Layer 2 Technologies

1.1 Configure and verify switch administration

1.1.a SDM templates

1.1.b Managing MAC address table

1.1.c Troubleshoot Err-disable recovery

1.2 Configure and verify Layer 2 protocols

1.2.a CDP, LLDP

1.2.b UDLD

1.3 Configure and verify VLANs

1.3.a Access ports

1.3.b VLAN database

1.3.c Normal, extended VLAN, voice VLAN

1.4 Configure and verify trunking

1.4.a VTPv1, VTPv2, VTPv3, VTP pruning

1.4.b dot1Q

1.4.c Native VLAN

1.4.d Manual pruning

1.5 Configure and verify EtherChannels

1.5.a LACP, PAgP, manual

1.5.b Layer 2, Layer 3

1.5.c Load balancing

1.5.d EtherChannel misconfiguration guard

1.6 Configure and verify spanning tree

1.6.a PVST+, RPVST+, MST

1.6.b Switch priority, port priority, path cost, STP timers

1.6.c PortFast, BPDUguard, BPDUfilter

1.6.d Loopguard and Rootguard

1.7 Configure and verify other LAN switching technologies

1.7.a SPAN, RSPAN

1.8 Describe chassis virtualization and aggregation technologies

1.8.a Stackwise

20% 2.0 Infrastructure Security

2.1 Configure and verify switch security features

2.1.a DHCP snooping

2.1.b IP Source Guard

2.1.c Dynamic ARP inspection

2.1.d Port security

2.1.e Private VLAN

2.1.f Storm control

2.2 Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

2.2.a AAA with TACACS+ and RADIUS

2.2.b Local privilege authorization fallback

15% 3.0 Infrastructure Services

3.1 Configure and verify first-hop redundancy protocols

3.1.a HSRP

3.1.b VRRP

3.1.c GLBP
