CCIE Routing and Switching

Expansion of Routing and Switching Lab v4.0 Blueprint

Detailed Checklist of Topics to Be Covered

Please be advised that this topic checklist is not an all-inclusive list of Cisco CCIE Routing and Switching lab exam subjects. Instead, we provide this outline as a supplement to the existing lab blueprint to help candidates prepare for their lab exams. Other relevant or related topics may also appear in the actual lab exam.

We would like to get your feedback please comment and/or rate this document.

1.0	**Implementing Layer 2 Technologies -** Configuring and Troubleshooting Layer 2 Technologies	√
1.0	Frame Relay	
1.01.1	Frame Relay Multipoint Links on a Physical Interface Using Inverse ARP	
1.01.2	Frame Relay Multipoint Links on a Physical Interface Without Using Inverse ARP	
1.01.3.	Frame Relay Multipoint Link on a Subinterface Using Inverse ARP	
1.01.4.	Frame Relay Multipoint Link on a Subinterface Without Using Inverse ARP	
1.01.5.	Frame Relay Point-to-Point Subinterfaces	
1.01.6.	PVC with a Multipoint Interface on One Side and a Subinterface on the Other Side	
1.01.7.	Authentication on a Frame Relay Link Using PPP	
1.2	Catalyst Configuration	
1.2.01.	Trunks Using an Industry-Standard Encapsulation	
1.2.02.	Trunks Using a Cisco Proprietary Encapsulation	
1.2.03.	Creating, Deleting, and Editing VLANs	
1.2.04.	VTP in Client/Server Mode	
1.2.05.	VTP in Transparent Mode	
1.2.06.	VTP Authentication	
1.2.07.	VTP Pruning	
1.2.08.	Controlling VLANs That Cross a Trunk	
1.2.09.	Optimizing STP by STP Timers	
1.2.10.	PortFast	
1.2.11.	Loop Guard	
1.2.12.	BPDU Guard	
1.2.13.	BPDU Filters	
1.2.14.	UplinkFast	
1.2.15.	BackboneFast	
1.2.16.	MSTP	
1.2.17.	Selecting the Root Bridge for VLANs in a PVST Environment	
1.2.18.	Selecting the Root Bridge for an MST Instance in an MST Environment	
1.2.19.	Setting the Port Priority to Designate the Forwarding Ports	
1.2.20.	EtherChannel Using an Industry-Standard Protocol	
1.2.21.	EtherChannel Using a Cisco Proprietary Protocol	
1.2.22.	Disabling Protocols on the EtherChannel	
1.2.23.	Load-Balancing Type on the EtherChannel	
1.2.24.	SNMP Management on the Switch	
1.2.25.	Telnet and SSH Management on the Switch	

1.2.26.	Controlling Inbound and Outbound Telnet on the Switch	
1.2.27.	Regular and Smart Macros	
1.2.28.	Switch Banners	
1.2.29.	UDLD	
1.2.30.	Switch Virtual Interfaces (SVIs) for IP Routing	
1.2.31.	Router on a Stick	
1.2.32.	SPAN	
1.2.33.	RSPAN	
1.2.34.	IP Routing on the Switch Using RIPv2, EIGRP, OSPF, and BGP	
1.2.35.	IP Phones to Connect to the Catalyst Switch	
1.2.36.	Dot1q Tunneling	
1.3	Other Layer 2 Technologies	
1.3.1.	HDLC	
1.3.2.	PPP	
1.3.3.	PPP over Ethernet	
2.0	**Implementing IPv4 -** Configuring and Troubleshooting IPv4	
2.1.	IPv4 Addressing	
2.1.1.	IPv4 Addressing	
2.1.2.	IPv4 Subnetting	
2.1.3.	IPv4 VLSM	
2.2.	OSPFv2	
2.2.01.	OSPF on a Broadcast Multicast Access Network (Ethernet)	
2.2.02.	OSPF over a Frame Relay Multipoint Network by Changing Network Types	
2.2.03.	OSPF over a Frame Relay Multipoint Network by Using the neighbor Command	
2.2.04.	OSPF over a Frame Relay Point-to-Point Network	
2.2.05.	Virtual Links	
2.2.06.	Stub Areas	
2.2.07.	Totally Stubby Areas	
2.2.08.	NSSA Areas	
2.2.09.	NSSA and Stub Areas	
2.2.10.	NSSA and Totally Stubby Areas	
2.3.	EIGRP	
2.3.1.	Basic EIGRP	
2.3.2.	Passive Interfaces	
2.3.3.	EIGRP Stub on Routers and Switches	
2.3.4.	EIGRP Update—Bandwidth Control	
2.3.5.	Changing the Administrative Distance of EIGRP	
2.3.6.	Unequal-Cost Load Balancing for EIGRP	
2.4.	Filtering, Redistribution, and Summarization	
2.4.01.	Route Filtering for OSPF Within the Area Using a Distribute List with an ACL and Prefix	
2.4.02.	Route Filtering for OSPF Between Areas	
2.4.03.	Summarization of OSPF Routes Between Areas	
2.4.04.	Summarization of External Routers Within OSPF	
2.4.05.	Filtering with a Distribute List Using an ACL and Prefix Lists	
2.4.06.	Using Advanced ACLs and a Prefix List for Filtering Routes	
2.4.07.	Summarizing Routes with EIGRP	

2.4.08.	Route Summarization for RIP	
2.4.09.	Redistribution Between OSPF and EIGRP	
2.4.10.	Redistribution Between RIP and EIGRP	
2.4.11.	Redistribution Between RIP and OSPF	
2.4.12.	Redistribution of Directly Connected Routes	
2.4.13.	Redistribution of Static Routes	
2.4.14.	Redistribution with Filtering Using ACLs and Prefix Lists	
2.4.15	Redistribution with Filtering Using Route Tagging	
2.5.	IBGP	
2.5.1.	IBGP Peering	
2.5.2.	Advertising Routes in BGP	
2.5.3.	Next-Hop Attribute	
2.5.4.	Route Reflectors	
2.5.5.	Redundancy by Neighbor Relationships Based on Loopbacks	
2.6.	EBGP	
2.6.1.	EBGP Peering	
2.6.2.	EBGP Peering Based on Loopbacks	
2.7.	BGP Advanced Features	
2.7.01.	Filtering Using ACLs	
2.7.02.	Filtering Using Prefix Lists	
2.7.03.	Filtering Using AS Path Filters	
2.7.04.	Redistributing Connected Routes into BGP	
2.7.05.	Redistributing Dynamic Routing Protocols into BGP	
2.7.06.	BGP Aggregation	
2.7.07.	BGP Aggregation with the Summary Only Parameter	
2.7.08.	BGP Aggregation with Suppress Maps	
2.7.09.	BGP Aggregation with Unsuppress Maps	
2.7.10.	BGP Best-Path Selection – Weight	
2.7.11.	BGP Best-Path Selection – Local Preference	
2.7.12.	BGP Best-Path Selection – MED	
2.7.13.	BGP Communities – No-Export	
2.7.14.	BGP Communities – No-Advertise	
2.7.15.	BGP Confederation	
2.7.16.	BGP Local AS	
2.7.17.	Working with Private AS Numbers	
2.7.18.	Route Dampening	
2.7.19.	Conditional Advertising	
2.7.20.	Peer Groups	
2.8	Performance Routing (PfR) and Cisco Optimized Edge Routing (OER)	
3.0	**Implementing IPv6 -** Configuring and Troubleshooting IPv6	
3.1.	IPv6	
3.1.1.	IPv6 Addresses	
3.1.2	RIPng	
3.1.3	OSPFv3	
3.1.4	EIGRPv6	
3.1.5	IPv6 Tunneling	

3.1.6	IPv6 on a Frame Relay Network – Multipoint	
3.1.7.	IPv6 on a Frame Relay Network – Point-to-Point	
3.1.8	Route Filtering with a Distribute List Using an ACL and Prefix Lists	
3.1.9	Route Redistribution Between OSPFv3 and EIGRPv6	
4.0	**Implementing MPLS -** Configuring and Troubleshooting MPLS	
4.1.	MPLS Unicast Routing	
4.1.1.	MPLS Unicast Routing Using LDP	
4.1.2.	Controlling Label Distribution	
4.2.	MPLS VPN	
4.2.1.	MPLS VPN Using Static Routing Between PE-CE	
4.2.2.	MPLS VPN Using EIGRP as the PE-CE Routing Protocol	
4.2.3.	MPLS VPN Using OSPF as the PE-CE Routing Protocol	
4.2.4.	MPLS VPN Using EBGP as the PE-CE Routing Protocol	
4.2.5.	Controlling Route Propagation Using the Route Target with Import and Export Maps	
4.3.	VRF-Lite	
4.3.1.	VRFs at the Customer Sites Using VRF-Lite	
5.0	**Implementing IP Multicast -** Configuring and Troubleshooting IP Multicast	
5.1.	PIM and Bidirectional PIM	
5.1.1.	PIM Dense Mode	
5.1.2.	PIM on an NMBA Network	
5.1.3.	PIM Sparse Mode – Static Rendezvous Point	
5.1.4.	PIM Sparse Mode – Multiple Static Rendezvous Points	
5.1.5.	PIM Sparse Mode – Auto Rendezvous Point	
5.1.6.	PIM Sparse Mode with Multiple Rendezvous Points Using the Auto Rendezvous Point	
5.1.7.	Bidirectional PIM	
5.2.	MSDP	
5.2.1.	MSDP	
5.2.2.	MSDP to an Anycast Rendezvous Point	
5.3.	Multicast Tools	
5.3.1.	Multicast Rate Limiting	
5.3.2.	IGMP Filtering on the Switch	
5.3.3.	Use of the Switch to Block Multicast Traffic	
5.3.4.	Multicasting Through a GRE Tunnel	
5.3.5.	Multicast Helper Address	
5.4.	IPv6 Multicast	
5.4.1.	IPv6 Multicast Routing Using PIM	
5.4.2.	IPv6 Multicast Listener Discovery (MLD) Protocol	
6.0	**Implementing Network Security -** Configuring and Troubleshooting Network Security	
6.1.	AAA and Security Server Protocols	
6.1.1.	Use of a Router to Authenticate Against a AAA Server Using TACACS+	
6.1.2.	Use of a Router to Authenticate Against a AAA Server Using RADIUS	
6.1.3.	Local Privilege Authorization	
6.1.4.	Accounting to a AAA Server Using TACACS+	
6.1.5.	Accounting to a AAA Server Using RADIUS	
6.2.	Access Lists	
6.2.1.	Standard Access Lists	

6.2.2.	Extended Access Lists	
6.2.3.	Time-Based Access Lists	
6.2.4.	Reflexive Access Lists	
6.3.	Routing Protocol Security	
6.3.1.	Routing Protocol Authentication for EIGRP	
6.3.2.	Routing Protocol Authentication for OSPF – Area-Wide	
6.3.3.	Routing Protocol Authentication for OSPF – Interface-Specific	
6.3.4.	Routing Protocol Authentication for OSPF Virtual Links	
6.3.5.	Routing Protocol Authentication for BGP	
6.4.	Catalyst Security	
6.4.1.	Storm Control	
6.4.2.	Switch Port Security	
6.4.3.	Dot1x Authentication	
6.4.4.	Dot1x Authentication for VLAN Assignment	
6.4.5.	VLAN Access Maps	
6.4.6.	DHCP Snooping	
6.4.7.	DAI	
6.4.8.	IP Source Guard	
6.4.9.	Private VLANs	
6.5.	Cisco IOS and Zone-Based Firewalls	
6.5.1.	Basic Cisco IOS Firewall	
6.5.2.	DoS Protection on a Cisco IOS Firewall	
6.5.3.	Basic Zone-Based Firewall	
6.5.4.	Zone-Based Firewall with Deep Packet Inspection	
6.6.	NAT	
6.6.1.	Dynamic NAT	
6.6.2.	PAT	
6.6.3.	Static NAT	
6.6.4.	Static PAT	
6.6.5.	Policy-Based NAT	
6.7.	Other Security Features	
6.7.1.	Configuring the TCP Intercept Feature	
6.7.2.	Configuring Blocking of Fragment Attacks	
6.7.3.	Configuring Switch Security Features	
6.7.4.	Configuring Antispoofing Using an ACL	
6.7.5.	Configuring Antispoofing Using uRPF	
6.7.6.	SSH on Routers and Switches	
6.7.7.	Cisco IOS IPS	
6.7.8.	Controlling Telnet and SSH Access to the Router and Switch	
7.0	**Implementing Network Services -** Configuring and Troubleshooting Network Services	
7.1.	DHCP	
7.1.1.	Configuring DHCP on a Cisco IOS Router	
7.1.2.	Configuring DHCP on a Switch	
7.1.3.	Using a Router and a Switch to Act as a DHCP Relay Agent (Helper Address)	
7.2.	HSRP	
7.2.1.	HSRP Between Two Routers	

7.2.2.	Pre-empt for HSRP	
7.2.3.	Authentication for HSRP	
7.2.4.	VRRP	
7.2.5.	GLBP	
7.3.	IP Services	
7.3.1.	Use of the Router for WCCP	
7.3.2.	Use of the Router to Generate an Exception Dump Using TFTP	
7.3.3.	Use of the Router to Generate an Exception Dump Using FTP	
7.3.4.	Use of the Router to Generate an Exception Dump Using RCP	
7.3.5.	Broadcast Forwarding for Protocols	
7.4.	System Management	
7.4.1.	Telnet Management on the Router and Switch	
7.4.2.	SSH Management on the Router and Switch	
7.4.3.	Disabling Telnet and the SSH Client on the Switch	
7.4.4.	HTTP Management on the Router and Switch	
7.4.5.	Controlling HTTP Management on the Router and Switch	
7.5.	NTP	
7.5.1.	NTP Using the NTP Master and NTP Server Commands	
7.5.2.	NTP Without Using the NTP Server	
7.5.3.	NTP Using NTP Broadcast Commands	
8.0	**Implementing QoS -** Configuring and Troubleshooting QoS	
8.1.	Classification	
8.1.1.	Marking Using DSCP	
8.1.2.	Marking Using IP Precedence	
8.1.3.	Marking Using CoS	
8.2.	Congestion Management and Congestion Avoidance	
8.2.1.	Priority Queuing	
8.2.2.	Custom Queuing	
8.2.3.	Weighted Fair Queuing	
8.2.4.	WRED	
8.2.5.	RSVP	
8.3.	Policing and Shaping	
8.3.1.	CAR Using Rate Limiting Under the Interface	
8.3.2.	Frame Relay Traffic Shaping Using Map Classes	
8.3.3.	Discard Eligible List	
8.4.	Link Efficiency Mechanisms	
8.4.1.	Compression	
8.4.2.	Link Fragmentation and Interleaving (LFI) for Frame Relay	
8.5.	Modular QoS CLI	
8.5.1.	Policing	
8.5.2.	Class-Based Weighted Fair Queuing (CB-WFQ)	
8.5.3.	Low Latency Queuing (LLQ)	
8.5.4.	Shaping Using MQC	
8.5.5.	Random Early Detection Using MQC	
8.5.6.	WRED Using MQC	
8.5.7.	Using NBAR for QoS	

8.5.8.	Discard Eligible Marking Using MQC	
8.6.	Catalyst QoS	
8.6.1.	SRR on the Catalyst Switch	
9.0	**Troubleshooting a Network -** Troubleshooting Network-Wide Connectivity Issues	
9.1.	Troubleshooting Layer 2 Problems	
9.1.1.	Troubleshooting Catalyst Switch Network Issues	
9.1.2.	Troubleshooting Frame Relay Network Issues	
9.2.	Troubleshooting Layer 3 Problems	
9.2.1.	Troubleshooting IP Addressing Network Issues	
9.2.2.	Troubleshooting Routing Protocol Network Issues	
9.2.3.	Troubleshooting Routing Protocol Loop Issues	
9.3.	Troubleshooting Application Problems	
9.3.1.	Determining Which Aspects of the Network to Troubleshoot to Determine Network	
9.4.	Troubleshooting Network Services	
9.4.1.	Troubleshooting Misconfigured NTP Setup	
9.4.2.	Troubleshooting Misconfigured DHCP Setup	
9.4.3.	Troubleshooting Misconfigured Telnet and SSH Setup	
9.4.4.	Troubleshooting Misconfigured SNMP Setup	
9.5.	Troubleshooting Security Services	
9.5.1.	Troubleshooting Misconfigured ACLs	
9.5.2.	Troubleshooting Misconfigured NAT	
9.5.3.	Troubleshooting Misconfigured AAA Services	
10.0	**Optimizing a Network -** Configuring and Troubleshooting Optimization of a Network	
10.1.	Logging In	
10.1.1.	Logging into a Remote Syslog Server	
10.1.2.	Logging into the Internal Buffer	
10.2.	SNMP	
10.2.1.	Use of a Router to Communicate to an SNMP Management Station	
10.2.2.	Use of a Router to Generate SNMP Traps	
10.3.	RMON	
10.3.1.	Use of a Router to Generate SNMP Traps Using RMON	
10.4.	Accounting	
10.4.1.	IP Accounting	
10.5.	SLA	
10.5.1.	IP SLA	
10.6.	Implementing Network Services on the Routers	
10.6.1.	Use of a Router as an FTP Server	
10.6.2.	Use of a Router as a TFTP Server	
10.6.3.	Cisco IOS Embedded Event Manager	
10.6.4.	NetFlow	
10.6.5.	HTTP and HTTPS on a Router	
10.6.6.	Telnet on a Router	
10.6.7.	Implementing Secure Copy Protocol (SCP) on a Router	