15-Day CCNA Medium Level Lab Guide

Day 1: Advanced VLAN Configuration & Trunking

Lab Objectives:

- Configure VLANs across multiple switches
- Implement 802.1Q trunking
- Configure VTP (VLAN Trunking Protocol)

Topology:

- 3 Switches (SW1, SW2, SW3) in a triangular topology
- 6 PCs distributed across switches

Tasks:

1. Create VLANs: VLAN 10 (Sales), VLAN 20 (Engineering), VLAN 30 (HR)
2. Configure trunk links between all switches
3. Set up VTP with SW1 as server, others as clients
4. Assign ports to appropriate VLANs
5. Verify VLAN database synchronization
6. Test connectivity within and between VLANs

Configuration Commands:

```
SW1(config)# vtp domain COMPANY
SW1(config)# vtp mode server
SW1(config)# vlan 10
SW1(config-vlan)# name Sales
SW1(config)# interface range fa0/1-2
SW1(config-if-range)# switchport mode trunk
SW1(config-if-range)# switchport trunk allowed vlan all
```

Day 2: Inter-VLAN Routing (Router-on-a-Stick)

Lab Objectives:

- Configure router subinterfaces for inter-VLAN routing
- Implement 802.1Q encapsulation
- Enable communication between VLANs

Topology:

- 1 Router (R1), 1 Switch (SW1), 3 PCs in different VLANs

Tasks:

1. Configure VLANs on switch
2. Create subinterfaces on router for each VLAN
3. Configure 802.1Q encapsulation
4. Assign IP addresses to subinterfaces
5. Configure default gateway on PCs
6. Test inter-VLAN connectivity

Configuration Commands:

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config)# interface g0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
```

Day 3: Static Routing with Redundant Paths

Lab Objectives:

- Configure static routes
- Implement floating static routes

- Test failover scenarios

Topology:

- 3 Routers (R1, R2, R3) with dual connections
- 2 LANs on R1 and R3

Tasks:

1. Configure IP addressing on all interfaces
2. Create primary static routes
3. Configure backup floating static routes (higher AD)
4. Test primary path connectivity
5. Simulate link failure
6. Verify automatic failover to backup path

Configuration Commands:

```
R1(config)# ip route 192.168.3.0 255.255.255.0 10.1.1.2
R1(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.2 5
```

Day 4: OSPF Single Area Configuration

Lab Objectives:

- Configure OSPF routing protocol
- Set router IDs
- Adjust OSPF costs and priorities

Topology:

- 4 Routers in a partial mesh topology
- Multiple LANs attached

Tasks:

1. Enable OSPF on all routers (Area 0)
2. Configure manual router IDs
3. Advertise all networks
4. Verify OSPF neighbor relationships
5. Manipulate DR/BDR election with priority
6. Analyze routing table and OSPF database

Configuration Commands:

```
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0
R1(config)# interface g0/0
R1(config-if)# ip ospf priority 100
```

Day 5: OSPF Multi-Area Configuration

Lab Objectives:

- Design and implement multi-area OSPF
- Configure ABRs (Area Border Routers)
- Summarize routes between areas

Topology:

- 5 Routers: 2 in Area 0, 2 in Area 1, 2 in Area 2
- ABRs connecting areas

Tasks:

1. Configure backbone Area 0
2. Establish Area 1 and Area 2
3. Configure ABRs with interfaces in multiple areas
4. Implement route summarization at ABRs
5. Verify inter-area routing
6. Compare routing tables in different areas

Configuration Commands:

```
ABR1(config)# router ospf 1
ABR1(config-router)# network 10.0.0.0 0.0.0.3 area 0
ABR1(config-router)# network 172.16.0.0 0.0.255.255 area 1
ABR1(config-router)# area 1 range 172.16.0.0 255.255.0.0
```

Day 6: EIGRP Configuration & Tuning

Lab Objectives:

- Configure EIGRP routing protocol
- Implement EIGRP authentication
- Tune EIGRP metrics

Topology:

- 4 Routers in a square topology
- Multiple LANs with varying bandwidth

Tasks:

1. Enable EIGRP with AS number 100
2. Configure all networks
3. Implement MD5 authentication on all links
4. Modify interface bandwidth to influence path selection
5. Configure passive interfaces for LAN segments
6. Verify feasible successors and successors

Configuration Commands:

```
R1(config)# router eigrp 100
R1(config-router)# network 192.168.0.0
R1(config-router)# no auto-summary
R1(config-router)# passive-interface g0/0
R1(config)# key chain EIGRP_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string Cisco123
R1(config)# interface s0/0/0
R1(config-if)# ip authentication mode eigrp 100 md5
R1(config-if)# ip authentication key-chain eigrp 100 EIGRP_KEY
```

Day 7: Access Control Lists (ACLs)

Lab Objectives:

- Configure standard and extended ACLs
- Implement ACLs for traffic filtering
- Apply ACLs in correct directions

Topology:

- 2 Routers, 2 Switches, 4 Subnets

Tasks:

1. Create standard ACL to block specific host
2. Configure extended ACL to filter HTTP traffic
3. Permit ICMP while denying other protocols
4. Apply ACLs on appropriate interfaces and directions
5. Test and verify ACL functionality
6. Review ACL hit counters

Configuration Commands:

```
R1(config)# access-list 10 deny host 192.168.1.50
R1(config)# access-list 10 permit any
R1(config)# interface g0/0
R1(config-if)# ip access-group 10 in

R1(config)# ip access-list extended WEB_FILTER
R1(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group WEB_FILTER out
```

Day 8: NAT Configuration (Static, Dynamic, PAT)

Lab Objectives:

- Configure static NAT
- Implement dynamic NAT
- Set up PAT (NAT overload)

Topology:

- 1 Router connecting internal network to ISP
- Internal network: 192.168.1.0/24
- Public IPs: 200.1.1.1-200.1.1.10

Tasks:

1. Configure static NAT for internal server
2. Set up dynamic NAT pool for 10 users
3. Configure PAT for remaining users
4. Define inside and outside interfaces
5. Test connectivity from internal hosts
6. Verify NAT translations

Configuration Commands:

```
R1(config)# ip nat inside source static 192.168.1.10 200.1.1.5
R1(config)# ip nat pool DYNAMIC_POOL 200.1.1.1 200.1.1.10 netmask 255.255.255.0
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)# ip nat inside source list 1 pool DYNAMIC_POOL
R1(config)# ip nat inside source list 1 interface g0/1 overload
R1(config)# interface g0/0
R1(config-if)# ip nat inside
R1(config)# interface g0/1
R1(config-if)# ip nat outside
```

Day 9: DHCP Server Configuration

Lab Objectives:

- Configure router as DHCP server
- Create multiple DHCP pools
- Implement DHCP relay agent

Topology:

- 2 Routers, 2 Switches, 3 VLANs
- R1 as DHCP server, R2 as relay agent

Tasks:

1. Configure DHCP pools for each VLAN
2. Exclude static IP ranges
3. Set default gateway and DNS options
4. Configure DHCP relay on remote router
5. Test dynamic IP assignment

6. Verify DHCP bindings

Configuration Commands:

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)# ip dhcp pool VLAN10
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 8.8.8.8
R1(dhcp-config)# lease 7

R2(config)# interface g0/0.10
R2(config-subif)# ip helper-address 10.1.1.1
```

Day 10: EtherChannel Configuration

Lab Objectives:

- Configure Layer 2 EtherChannel with LACP
- Implement PAgP EtherChannel
- Configure Layer 3 EtherChannel

Topology:

- 2 Switches with multiple connections
- 1 Switch to 1 Router with multiple links

Tasks:

1. Create LACP EtherChannel between switches
2. Configure PAgP channel (alternate method)
3. Set up Layer 3 EtherChannel to router
4. Verify load balancing
5. Test link failure scenarios
6. Monitor EtherChannel status

Configuration Commands:

```
SW1(config)# interface range f0/1-2
SW1(config-if-range)# channel-group 1 mode active
SW1(config-if-range)# exit
SW1(config)# interface port-channel 1
SW1(config-if)# switchport mode trunk

SW1(config)# interface range f0/3-4
SW1(config-if-range)# channel-group 2 mode desirable
```

Day 11: Spanning Tree Protocol Optimization

Lab Objectives:

- Configure PVST+ and Rapid-PVST+
- Manipulate root bridge election
- Implement PortFast and BPDU Guard

Topology:

- 4 Switches in redundant topology
- Multiple VLANs

Tasks:

1. Identify current root bridge per VLAN
2. Configure priority to control root election
3. Enable Rapid-PVST+
4. Configure PortFast on access ports
5. Enable BPDU Guard for security
6. Verify STP topology and port states

Configuration Commands:

```
SW1(config)# spanning-tree mode rapid-pvst
SW1(config)# spanning-tree vlan 10 root primary
SW1(config)# spanning-tree vlan 20 root secondary
SW1(config)# interface range f0/1-10
SW1(config-if-range)# spanning-tree portfast
SW1(config-if-range)# spanning-tree bpduguard enable
```

Day 12: Port Security & Switch Hardening

Lab Objectives:

- Implement port security
- Configure violation modes
- Secure unused ports

Topology:

- 2 Switches, 6 PCs

Tasks:

1. Configure maximum MAC addresses per port
2. Set sticky MAC learning
3. Define violation actions (shutdown, restrict, protect)
4. Disable unused ports
5. Test security violations
6. Recover from err-disabled state

Configuration Commands:

```
SW1(config)# interface f0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 2
SW1(config-if)# switchport port-security mac-address sticky
SW1(config-if)# switchport port-security violation shutdown

SW1(config)# interface range f0/20-24
SW1(config-if-range)# shutdown
SW1(config-if-range)# description UNUSED_PORTS

SW1# errdisable recovery cause psecure-violation
SW1# errdisable recovery interval 300
```

Day 13: PPP & GRE Tunneling

Lab Objectives:

- Configure PPP with authentication
- Implement GRE tunnels
- Route traffic through tunnels

Topology:

- 3 Routers with serial connections
- 2 remote LANs to be connected via GRE

Tasks:

1. Configure PPP encapsulation on serial links
2. Implement CHAP authentication
3. Create GRE tunnel between remote sites
4. Configure routing over tunnel
5. Test tunnel connectivity
6. Verify MTU considerations

Configuration Commands:

```
R1(config)# username R2 password Cisco123
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication chap

R1(config)# interface tunnel 0
R1(config-if)# ip address 10.10.10.1 255.255.255.0
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 200.2.2.2
R1(config-if)# tunnel mode gre ip
```

Day 14: IPv6 Addressing & Routing

Lab Objectives:

- Configure IPv6 addresses
- Implement static IPv6 routing
- Configure OSPFv3

Topology:

- 3 Routers, multiple IPv6 subnets

Tasks:

1. Assign IPv6 addresses (EUI-64 and manual)
2. Enable IPv6 routing
3. Configure static IPv6 routes
4. Implement OSPFv3 for dynamic routing
5. Test IPv6 connectivity
6. Verify neighbor discovery

Configuration Commands:

```
R1(config)# ipv6 unicast-routing
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:1:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown

R1(config)# ipv6 route 2001:db8:3::/64 2001:db8:2::2

R1(config)# ipv6 router ospf 1
R1(config-rtr)# router-id 1.1.1.1
R1(config)# interface g0/0
R1(config-if)# ipv6 ospf 1 area 0
```

Day 15: Network Troubleshooting Scenario

Lab Objectives:

- Diagnose complex multi-layer issues
- Apply systematic troubleshooting methodology
- Document findings and solutions

Topology:

- Complete network with intentional misconfigurations
- 5 Routers, 3 Switches, multiple VLANs, OSPF routing

Pre-configured Issues:

1. Incorrect VLAN assignments
2. Wrong subnet masks
3. OSPF network type mismatch
4. ACL blocking legitimate traffic
5. Native VLAN mismatch on trunk
6. Incorrect default gateway

Tasks:

1. Document reported problems
2. Use systematic troubleshooting (OSI layers)

3. Use commands: show, ping, traceroute, debug
4. Identify and fix all issues
5. Verify full network connectivity
6. Create troubleshooting report

Key Troubleshooting Commands:

```
# show running-config
# show ip interface brief
# show vlan brief
# show interfaces trunk
# show ip route
# show ip ospf neighbor
# show ip protocols
# show access-lists
# ping [destination]
# traceroute [destination]
# debug ip ospf events
```

Additional Resources

Recommended Tools:

- Cisco Packet Tracer
- GNS3
- EVE-NG

Study Tips:

1. Document each lab configuration
2. Break topology and troubleshoot
3. Recreate labs from memory
4. Time yourself on configurations
5. Practice verification commands

Next Steps:

- Practice under timed conditions
- Combine multiple technologies in single lab
- Explore advanced topics (QoS, WAN technologies)
- Take practice CCNA exams