CCNA 3: SCALING NETWORKS

CASE STUDY (PACKET TRACER)

Overview and Objectives

This case study allows students to complete a network design, implementation, and troubleshooting project using the skills gained in CCNA 3. Students will use the skills that have already been developed to use, make and connect the proper cabling to the appropriate devices.

It is crucial to read and understand the scenarios to make sure that all requirements are fulfilled. Each scenario guides the student through the proper steps to ensure that the project is completed properly.

This case study requires the student to accomplish the following tasks:

- Set up the physical layout of the network using the diagram and accompanying narrative
- Correctly configure the routers with a basic router configuration
- Correctly configure the routing features that the design requirements describe
- Correctly configure the switches with a basic switch configuration
- Correctly configure the switching features that the design requirements describe
- Troubleshoot and test the connectivity between all devices
- Provide detailed documentation in a prescribed form, as listed in the deliverables section

Scenario and Phase 1: Project Description

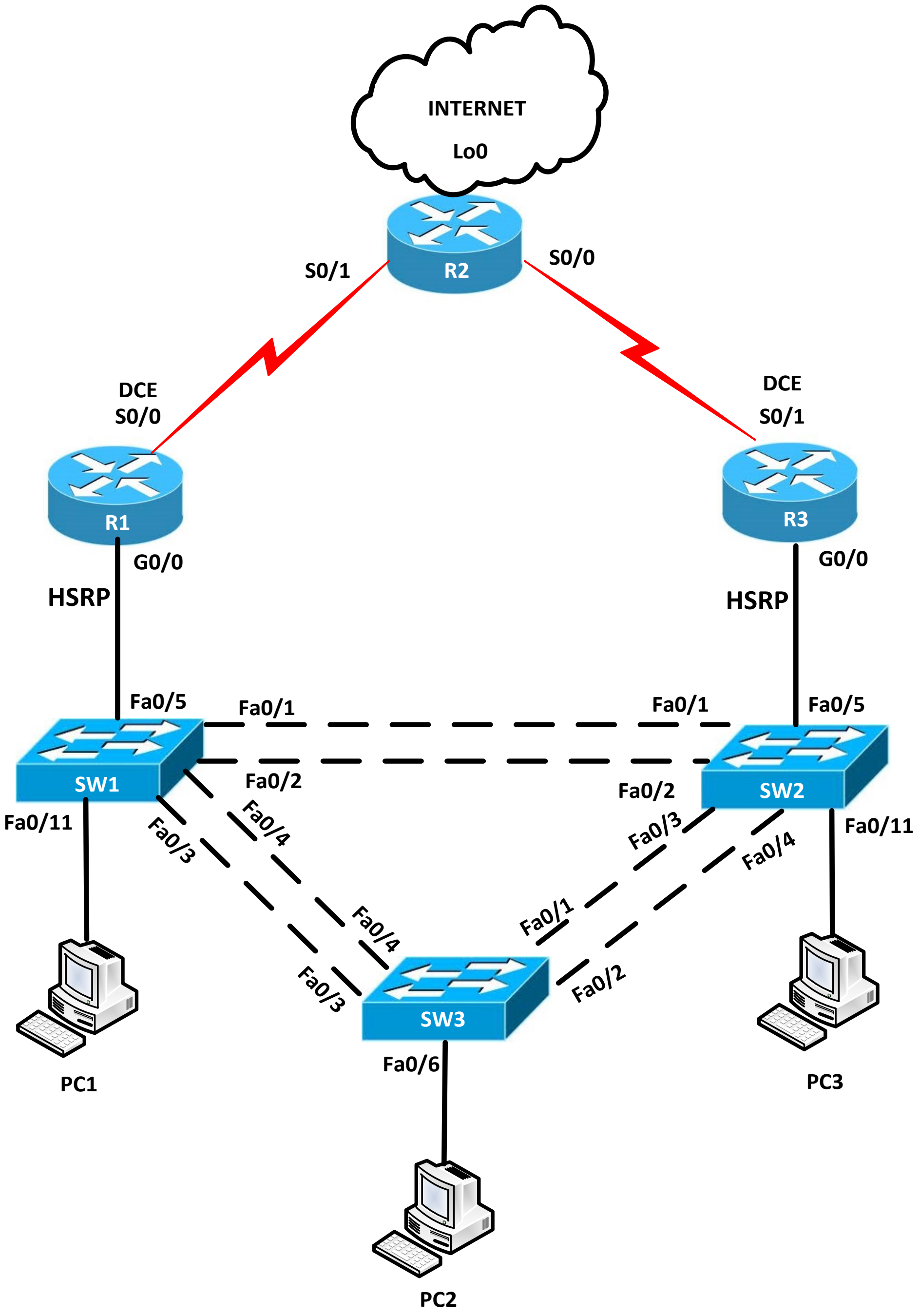

Figure 1: Topology diagram

LaSalle Telecom is a company that has several people responsible for designing and implementing the switched infrastructure of the university Campus. Many technicians are involved in the upgrading process.

A technician is given the task to complete this design and implementation knowing that the final network has the topology of the exhibit.

After deploying the solution, it is important that any documentation explaining the purpose, design, implementation or troubleshooting is recorded for further upgrade.

Below are the necessary information related to the implementation of the topology.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.10.1	255.255.255.0	N/A
	S0/0	209.165.100.1	255.255.255.252	N/A
R2	S0/0	209.165.100.5	255.255.255.252	N/A
	S0/1	209.165.100.2	255.255.255.252	N/A
	Lo0	200.200.200.1	255.255.255.0	N/A
R3	G0/0	172.16.10.3	255.255.255.0	N/A
	S0/1	209.165.100.6	255.255.255.252	N/A
SW1	VLAN 99	172.16.99.11	255.255.255.0	N/A
SW2	VLAN 99	172.16.99.12	255.255.255.0	N/A
SW3	VLAN 99	172.16.99.13	255.255.255.0	N/A
PC1	NIC	172.16.10.11	255.255.255.0	172.16.10.2
PC2	NIC	172.16.10.12	255.255.255.0	172.16.10.4
PC3	NIC	172.16.10.13	255.255.255.0	172.16.10.4

Table 1: Addressing Table

Port Assignments

Switch	Ports	Assignment	Network
SW1	F0/1 - F0/4	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/5 - F0/16	VLAN 10 – Sales	172.16.10.0/24
SW2	F0/1 - F0/4	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/5 - F0/16	VLAN 10 – Sales	172.16.10.0/24
SW3	F0/1- F0/4	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/5 - F0/16	VLAN 10 – Sales	172.16.10.0/24

Table 2: Port Assignments Table

VLANs Information

VLAN	VLAN Name
VLAN 99 (Native)	Management
VLAN 10	Sales

Table 3: VLANs Information Table

Phase 2: Basic Configuration Requirements

The technician is assigned to create a basic configuration that meets the following requirements:

1. **Basic configuration for all routers.**
    a. IP domain lookup deactivated.
    b. Minimum password length: **10 characters**
    c. Encrypt all passwords.
    d. Console access.
        i. Local database access.
        ii. Username: **admin01**
        iii. Password: **admin01pass**
    e. VTY lines access.
        i. Only SSH access is permitted.
        ii. Domain name: **CCNA_CS3.com**
        iii. Username: **adminSSH**
        iv. Password: **adminSSHpass**
    f. Enable secret password: **ciscoenpa55**
    g. Banner MOTD:

        ```
        ***************************
        This is the <router_name> CLI.
        ***************************
        ```
    h. Interfaces configuration.
        i. IP addressing and subnet masking according to the Addressing Table presented in Phase 1.
        ii. Descriptions in point-to-point interfaces:

            Link <router1_name> - <router2_name>
        iii. Descriptions in LAN interfaces:

            LAN <LAN_name>
2. **Basic configuration for all switches.**
    a. IP domain lookup deactivated.
    b. Encrypt all passwords.
    c. Console access.
        i. Local database access.
        ii. Username: **admin01**
        iii. Password: **admin01pass**
    d. VTY lines access.
        i. Only SSH access is permitted.
        ii. Domain name: **CCNA_CS3.com**
        iii. Username: **adminSSH**
        iv. Password: **adminSSHpass**
    e. Enable secret password: **ciscoenpa55**

f. Banner MOTD:
   ****
   This is the <switch_name> CLI.
   ****
g. The Management VLAN is not accessible and not routable.
h. SW1 is performing VTP server functions and SW2 is a VTP client. SW3 is configured in VTP transparent mode.
   i. VTP domain: CCNA3_CS
   ii. VTP password: VTPccna3
i. Every switch has different ports assigned to VLANs according the table presented in Phase 1.
j. Ports F0/1, F0/2, F0/3 and F0/4 on SW1, ports F0/1 and F0/2 on SW2, and ports F0/3 and F0/4 on SW3 will create a trunk when connected to any other port except one that is configured as an access port.
k. Ports F0/1, F0/2 on SW3 and ports F0/3 and F0/4 on SW2 will create a trunk unconditionally.
l. The links that interconnect SW1 to SW3 are bundled together forming an Etherchannel (use PAgP).
m. The links that interconnect SW2 to SW3 are bundled together forming an Etherchannel (use LACP).
n. The links that interconnect SW1 to SW2 are bundled together forming an Etherchannel (no protocol used).
o. Spanning Tree Protocol:
   i. Mode: Rapid PVST+.
   ii. SW1 has a priority of 24576 for VLAN 99 and is the secondary root bridge for VLAN 10.
   iii. SW2 is the primary root bridge for VLAN 10 and has a priority of 28672 for VLAN 99.
   iv. All ports in access mode transitioning directly to forwarding state.
   v. BPDU guard feature is activated where is necessary.
p. Configure security on switchports:
   i. Port Fa0/11 of SW1 can learn 2 different MAC addresses.
   ii. Port Fa0/11 of SW1 learns the MAC of PC1 statically and the rest dynamically. If the switch reboots for any reason, the end devices that can be connected have to be the same.
   iii. Port F0/11 of SW1 drops packets with unknown source addresses until the number of secure MAC addresses drops below the maximum value.
   iv. Port Fa0/6 of SW3 can learn 3 different MAC addresses.
   v. Port Fa0/6 of SW3 learns the MAC of PC2 statically and the rest dynamically. If the switch reboots for any reason, the end devices that can be connected have to be the same.

vi. Port F0/6 of SW3 drops packets with unknown source addresses until the number of secure MAC addresses drops below the maximum value and causes the Security Violation counter to increment.

Phase 3: Workstation Configuration Requirements

Configure IP Addresses of end devices according to the Addressing table presented in Phase 1.

Phase 4: Configuring Hot-Standby Routing Protocol

The technician is assigned to create a configuration that meets the following requirements:

1. PC1 prefers R1 as their default gateway and if the path through R1 doesn't work properly it uses R3 to exit the network.
2. PC2 and PC3 prefer R3 as their default gateway and if the path through R3 doesn't work properly they use R1 to exit the network.
3. The router with the highest priority immediately becomes the active router after reboot conditions.

NOTE**: Save your work now with the name **CCNA_CS3_basic_conf.pkt

Phase 5: Routing Configuration

The technician is assigned to create a configuration that meets the following requirements:

1. OSPF with the Process ID 10 for R1, R2 and R3.
2. R1 requirements:
   a. R1 is an *Area Border Router* (ABR).
   b. Router ID: 1.1.1.1
   c. R1 propagates OSPF routing information about all its directly connected networks.
   d. G0/0 is inside area 1.
   e. S0/0 is inside area 0.
3. R2 requirements:
   a. R2 is an *Autonomous System Boundary Router* (ASBR).
   b. Router ID: 2.2.2.2
   c. R2 is inside area 0.
   d. R2 sends and receives OSPF routing updates through S0/0 and S0/1 interfaces.
   e. R2 has a default gateway toward Internet.
   f. R2 propagates default route information to R1 and R3.

4. R3 requirements:
    a. R3 is an *Area Border Router* (ABR).
    b. Router ID: 3.3.3.3
    c. R3 propagates OSPF routing information about all its directly connected networks.
    d. G0/0 is inside area 1.
    e. S0/1 is inside area 0.
5. The cost reference bandwidth is adjusted to the fastest link of the topology.
6. The routers authenticate its identity with MD5 using the password ***routingOSPF***.
7. Routers send Hello packets every 5 seconds.
8. Routers break any adjacency with a neighbor if they don't receive a hello packet from that neighbor within 20 seconds.

NOTE: *If a command does not work on Packet Tracer, do this task theoretically.*

NOTE*: Save your work now with the name* ***CCNA3_CS_vOSPF.pkt***

Phase 6: Troubleshooting OSPF implementation

NOTE*: Do not save changes on the configuration for this phase. Only perform the properly changes and provide information to probe the new requirements.*

The technician is assigned to check the connectivity and performance of the network implemented with OSPF routing protocol:

1. Ping between all devices has to be successful.
2. Remote access to all devices has to be successful.
3. Packets destined from R1 to 209.165.100.4/30 go through R2 (not through the LAN network).
    a. If that requirement is not accomplished, make configuration changes to get this behavior. Justify your answer.
4. Packets destined from R3 to 209.165.100.0/30 go through R2 (not through the LAN network).
    a. If that requirement is not accomplished, make configuration changes to get this behavior. Justify your answer.
5. If the link between R1 and SW1 fails:
    a. Is there connectivity between devices in VLAN 10? Justify your answers.
    b. Do all VLAN 10 devices have connectivity to the outside? Justify your answers.
6. If the link between R3 and SW2 fails:
    a. Is there connectivity between devices in VLAN 10? Justify your answers.
    b. Do all VLAN 10 devices have connectivity to the outside? Justify your answers.

7. Check that load balancing is implemented.
   a. Follow the path of packets from PC1 to Internet and to other devices on the network.
   b. Follow the path of packets from PC2 to Internet and other devices on the network.
   c. Follow the path of packets from PC3 to Internet and other devices on the network.
8. Check DR and BDR elections.
   a. Which router is the DR? And the BDR? Justify your answers.
   b. Imagine that the elections of DR and BDR are incorrect. How do you change or force those elections? Probe it and justify your answers.
9. Adjust the bandwidth of R1's S0/0 and R2's S0/1 to 64kbps and the bandwidth of R2's S0/0 and R3's S0/1 to 128kbps.
   a. What changes do you appreciate? Justify your answers.
   b. Change the cost of the links with another technic (different from bandwidth configuration) and check that the results are the same.
10. Check port security in switches.

The technician provides documentation that specifies how the checking was tested.

NOTE: *If a command does not work on Packet Tracer, do this task theoretically.*

Phase 7: Modifying Routing Configuration

NOTE: *Restore the basic configuration to perform this phase.*

The technician is assigned to create a configuration that meets the following requirements:

1. EIGRP with the *Autonomous System* number 20 for R1, R2 and R3.
2. R1 requirements:
   a. Router ID: 1.1.1.1
   b. R1 propagates EIGRP routing information about all its directly connected networks.
   c. R1 does not have any Null0 route to a major class network in its routing table due to auto-summarization.
3. R2 requirements:
   a. Router ID: 2.2.2.2
   b. R2 propagates EIGRP routing information about networks connected to its serial interfaces.
   c. R2 does not have any Null0 route to a major class network in its routing table due to auto-summarization.
   d. R2 has a default gateway toward Internet.
   e. R2 propagates default route information to R1 and R3.

4. R3 requirements:
    a. Router ID: 3.3.3.3
    b. R3 propagates EIGRP routing information about all its directly connected networks.
    c. R3 does not have any Null0 route to a major class in its routing table due to auto-summarization.
5. The percentage of bandwidth that may be used by EIGRP is up to 60%.
6. The routers authenticate its identity with MD5 using the password ***routingEIGRP***.
7. Routers send Hello packets every 10 seconds.
8. Routers break any adjacency with a neighbor if they do not receive a hello packet from that neighbor within 30 seconds.

NOTE*: Save your work now with the name* ***CCNA3_CS_vEIGRP.pkt***

NOTE: *If a command does not work on Packet Tracer, do this task theoretically.*

Phase 8: Troubleshooting EIGRP Implementation

NOTE*: Do not save changes on the configuration for this phase. Only perform the properly changes and provide information to probe the new requirements.*

The technician is assigned to check the connectivity and performance of the network implemented with EIGRP routing protocol:

1. Ping between all devices has to be successful.
2. Remote access to all devices has to be successful.
3. Packets destined from R1 to 209.165.100.4/30 go through R2 (not through the LAN network).
    a. If that requirement is not accomplished, make configuration changes to get this behavior. Justify your answer.
4. Packets destined from R3 to 209.165.100.0/30 go through R2 (not through the LAN network).
    a. If that requirement is not accomplished, make configuration changes to get this behavior. Justify your answer.
5. If the link between R1 and SW1 fails:
    a. Is there connectivity between devices in VLAN 10? Justify your answers.
    b. Do all VLAN 10 devices have connectivity to the outside? Justify your answers.
6. If the link between R3 and SW2 fails:
    a. Is there connectivity between devices in VLAN 10? Justify your answers.
    b. Do all VLAN 10 devices have connectivity to the outside? Justify your answers.

7. Check that load balancing is implemented.
    a. Follow the path of packets from each PC to Internet and to other devices on the network.
8. Adjust the bandwidth of R1’s S0/0 and R2’s S0/1 to 64kbps and the bandwidth of R2’s S0/0 and R3’s S0/1 to 128kbps.
    a. What changes do you appreciate? Justify your answers.

The technician provides documentation that specifies how the checking was tested.

NOTE: *If a command does not work on Packet Tracer, do this task theoretically.*

Phase 9: Compare the results

The technician has implemented the same topology with two different routing protocols and now he/she has to decide which routing protocol is most suitable for the company.

1. Compare the results obtained with both implementations.
2. Which routing protocol do you prefer for the company? Justify your answer.

Phase 10: Documenting the Network

In order to support the network properly, documentation is required. Create documentation that is logically organized to make troubleshooting simpler:

- **Routers**
    - show cdp neighbors
    - show ip interface brief
    - show interface <type_slot_port>
    - show version
    - show startup-config
    - show standby
    - show standby brief
    - ***CCNA3_CS_<login>_vOSPF:***
        - show ip route
        - show ip protocols
        - show ip ospf
        - show ip ospf neighbors
        - show ip ospf database
        - show ip ospf interface <interface>
        - show ip ospf interface brief

    - ***CCNA3_CS_<login>_vEIGRP:***
        - show ip route
        - show ip protocols
        - show ip eigrp neighbors
        - show ip eigrp topology
- **Switches**
    - show cdp neighbors
    - show ip interface brief
    - show interfaces trunk
    - show interface vlan <management vlan>
    - show vlan
    - show spanning-tree
    - show port-security
    - show port-security interface <secured port>

Case Study Deliverables

The key lesson of this case study is the importance of thorough and clear documentation. There should be two types of documentation completed.

General Documentation:

- A complete narrative of the project should be typed using word processing software.
- Since the scenarios break up the entire task into pieces, take care to address each scenario task so that any layperson could understand that particular task.
- Microsoft Excel or another spreadsheet program could be used to simply list the equipment and serial numbers.
- Microsoft Visio or any paint program could be used to draw the network.
- Provide documentation that specifies how the connectivity was tested.

Technical Documentation:

The technical documentation should include details of the network topology. Visio or any paint program could be used to draw the network.

The technical documentation has to include a table or tables with the following details:

- IP addressing of all interfaces
- DCE/DTE information
- Router passwords
- Banner MOTD
- Interface descriptions
- IP addressing and gateway assignments for all PCs

- Router output from the following commands should be captured and placed into this documentation (for each router):
    - show cdp neighbors
    - show ip interface brief
    - show interface <type_slot_port>
    - show version
    - show startup-config
    - show standby
    - show standby brief
    - ***CCNA3_CS_<login>_vOSPF:***
        - show ip route
        - show ip protocols
        - show ip ospf
        - show ip ospf neighbors
        - show ip ospf database
        - show ip ospf interface <interface>
        - show ip ospf interface brief
    - ***CCNA3_CS_<login>_vEIGRP:***
        - show ip route
        - show ip protocols
        - show ip eigrp neighbors
        - show ip eigrp topology
- Switch output from the following commands should be captured and placed into this documentation (for each switch):
    - show cdp neighbors
    - show ip interface brief
    - show interfaces trunk
    - show interface vlan <management vlan>
    - show vlan
    - show spanning-tree
    - show port-security
    - show port-security interface <secured port>