CCNA 4: CONNECTING NETWORKS

CASE STUDY

Overview and Objectives

This case study allows students to complete a network design, implementation, and troubleshooting project using the skills gained in all modules of the CCNA course. 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 phases to make sure that all requirements are fulfilled. Each phase 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, including IGP and EGP routing protocols.
- Correctly configure the switches with a basic switch configuration.
- Correctly configure the switching features that the design requirements describe, including security features and redundancy characteristics.
- Correctly configure PPP as data link layer encapsulation protocol.
- Correctly configure redundancy protocols such as HSRP.
- Correctly configure the *Network Address Translation* (NAT) needed to provide communications between inside and outside networks.
- Correctly configure GRE tunneling to provide internal connectivity between two remote sites.
- Correctly configure DHCP features to provide dynamic addressing.
- Correctly configure *Access Control Lists* (ACL) to filter some traffic.
- Correctly configure monitoring tools.
- 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

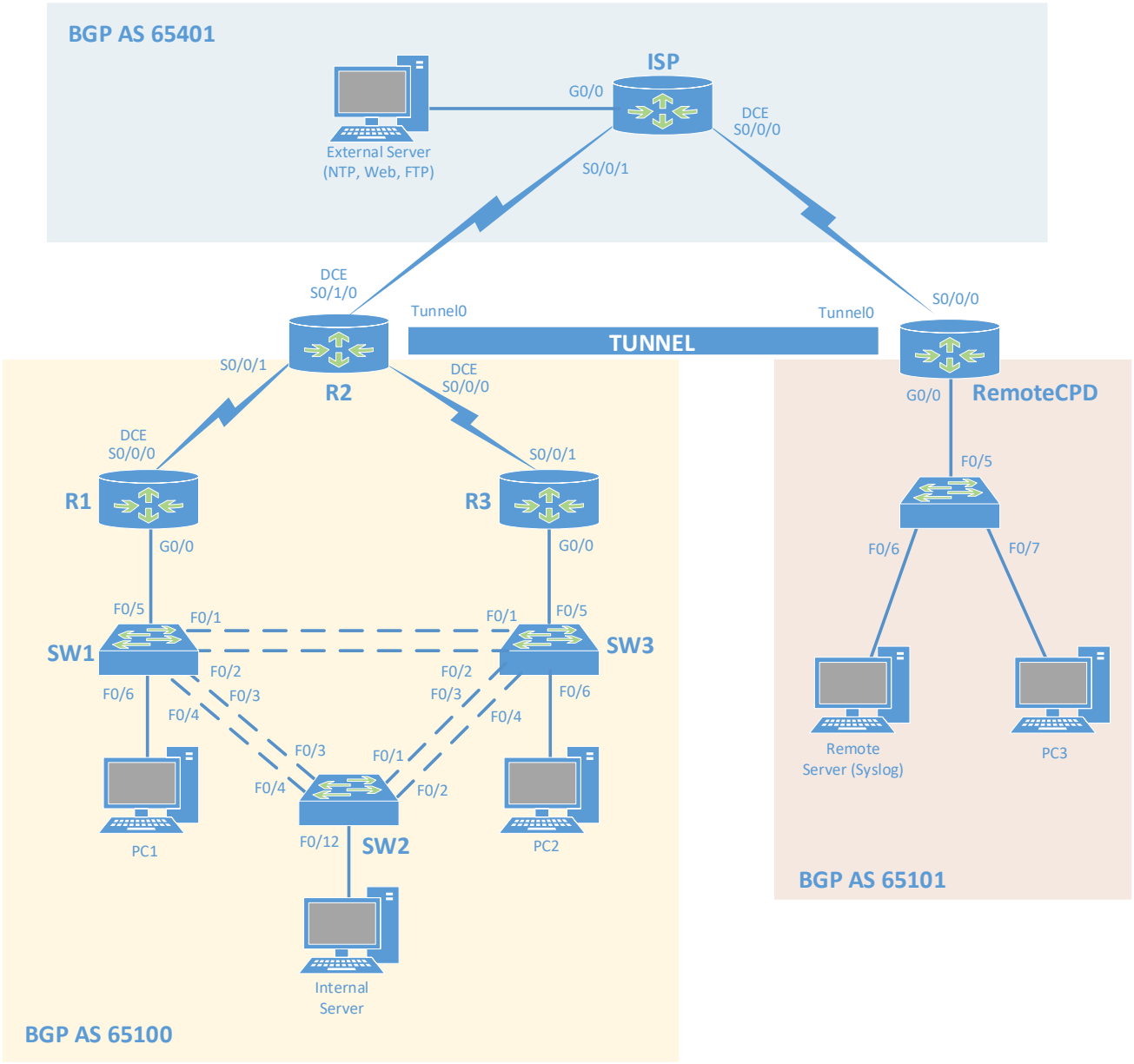

Figure 1: Topology diagram

LaSalle Telecom is a company that has several people responsible for designing and implementing the switched infrastructure of the university Campus and the connection to the Remote site. 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 (Figure 1).

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	N/A	N/A	N/A
	G0/0.10	172.16.10.1	255.255.255.0	N/A
	G0/0.20	172.16.20.1	255.255.255.0	N/A
	G0/0.99	172.16.99.1	255.255.255.0	N/A
	Lo0	172.16.1.1	255.255.255.0	N/A
	Lo1	172.16.2.1	255.255.255.0	N/A
	Lo2	172.16.3.1	255.255.255.0	N/A
	S0/0/0	172.16.123.1	255.255.255.252	N/A
R2	S0/0/0	172.16.123.5	255.255.255.252	N/A
	S0/0/1	172.16.123.2	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.252	N/A
	Tunnel0	172.17.1.1	255.255.255.252	N/A
R3	G0/0	N/A	N/A	N/A
	G0/0.10	172.16.10.3	255.255.255.0	N/A
	G0/0.20	172.16.20.3	255.255.255.0	N/A
	G0/0.99	172.16.99.3	255.255.255.0	N/A
	Lo4	172.16.4.1	255.255.255.0	N/A
	Lo5	172.16.5.1	255.255.255.0	N/A
	Lo6	172.16.6.1	255.255.255.0	N/A
	S0/0/1	172.16.123.6	255.255.255.252	N/A
SW1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.2
SW2	VLAN 99	172.16.99.12	255.255.255.0	172.16.99.2
SW3	VLAN 99	172.16.99.13	255.255.255.0	172.16.99.2
ISP	G0/0	200.200.200.1	255.255.255.0	N/A
	S0/0/0	209.165.200.229	255.255.255.252	N/A
	S0/0/1	209.165.200.226	255.255.255.252	N/A
RemoteCPD	G0/0	172.18.10.1	255.255.255.0	N/A
	S0/0/0	209.165.200.230	255.255.255.252	N/A
	Tunnel0	172.17.1.2	255.255.255.252	N/A
PC1	NIC	172.16.10.10 or DHCP	255.255.255.0	172.16.10.2
PC2	NIC	172.16.10.11 or DHCP	255.255.255.0	172.16.10.2
PC3	NIC	172.18.10.10 or DHCP	255.255.255.0	172.18.10.1
Internal Server	NIC	172.16.20.20	255.255.255.0	172.16.20.2
Remote Server	NIC	172.18.10.100	255.255.255.0	172.18.10.1
External Server	NIC	200.200.200.100	255.255.255.0	200.200.200.1

Table 1: Addressing Table

Port Assignments

Switch	Ports	Assignment	Network
SW1	F0/1 - F0/5	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/6 - F0/11	VLAN 10 – Sales	172.16.10.0/24
	F0/12 - F0/17	VLAN 20 – Servers	172.16.20.0/24
SW2	F0/1 - F0/4	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/6 - F0/11	VLAN 10 – Sales	172.16.10.0/24
	F0/12 - F0/17	VLAN 20 – Servers	172.16.20.0/24
SW3	F0/1- F0/5	802.1q Trunks (Native VLAN 99)	172.16.99.0/24
	F0/6 - F0/11	VLAN 10 – Sales	172.16.10.0/24
	F0/12 - F0/17	VLAN 20 – Servers	172.16.20.0/24

Table 2: Port Assignments Table

VLANs Information

VLAN	VLAN Name
VLAN 99 (Native)	Management
VLAN 10	Sales
VLAN 20	Servers

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 R1, R2, R3, and Remote CPD.**
    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_CS4.com**
        iii. Username: **adminSSH**
        iv. Password: **adminSSHpass**

    ***Note**: If SSH is not supported, configure telnet with local database access.*
    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 SW1, SW2 and SW3.

a. IP domain lookup deactivated.
b. Encrypt all passwords.
c. Console access password: **ciscoconpa55**
d. **Only Telnet access** is permitted to VTY lines.
    i. Username: **remote**
    ii. Password: **ciscovtypa55**
e. Enable secret password: **ciscoenpa55**
f. Banner MOTD:
    ****
    This is the <switch_name> CLI.
    ****
g. Packets can traverse between VLANs, inter-VLAN Routing.
h. The Management VLAN has to be accessible from any other device inside the topology.
i. All ports between switches and between switches and routers, will create a trunk unconditionally.
j. SW1 is performing VTP server functions and SW3 is a VTP client. SW2 is configured in VTP transparent mode.
    i. VTP domain: **CSCCNA4**
    ii. VTP password: **VTPccna4pass**
k. Every switch has different ports assigned to VLANs according the table presented in Phase 1.
l. The links that interconnect SW1 to SW3 are bundled together forming an Etherchannel unconditionally, without negotiation.
m. The links that interconnect SW1 to SW2 are bundled together forming an Etherchannel.
    i. Ports F0/3 and F0/4 on SW1 are configured in an active negotiating state, in which each port starts negotiations with other ports by sending PAgP packets.
    ii. Ports F0/3 and F0/4 on SW2 are configured in a passive negotiating state, in which each port responds to PAgP packets it receives but does not start PAgP packet negotiation.

n. The links that interconnect SW2 to SW3 are bundled together forming an Etherchannel.
    i. Ports F0/3 and Fa0/4 on SW3 are configured in an active negotiating state in which each port starts negotiations with other ports by sending LACP packets.
    ii. Ports F0/1 and Fa0/2 on SW2 are configured in a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.

o. Spanning Tree Protocol:
    i. Mode: Rapid PVST+.
    ii. SW1 has a priority of 24576 for VLAN 20 and 99 and is the secondary root bridge for VLAN 10.
    iii. SW3 is the primary root bridge for VLAN 10 and has a priority of 28672 for VLAN 20 and 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 port Fa0/12 on SW2:
    i. Port Fa0/12 can learn 3 different MAC addresses.
    ii. Port Fa0/12 learns the MAC of Internal Server 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 F0/12 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.

3. Basic configuration for ISP.

a. Console access password: **ciscoconpa55**
b. Enable secret password: **ciscoenpa55**
c. Banner MOTD:
    ****
    This is the <router_name> CLI.
    ****
d. Interfaces configuration.
    i. IP addressing and subnet masking according to Table 1.

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. Users in Sales network prefer R3 as their default gateway and if the path through R3 doesn't work properly they use R1 to exit the network.
2. Users in Servers network prefer R1 as their default gateway and if the path through R1 doesn't work properly they use R3 to exit the network.
3. Users in Management network prefer R1 as their default gateway and if the path through R1 doesn't work properly they use R3 to exit the network.
4. The router with the highest priority immediately becomes the active router.

Phase 5: Encapsulation of external links

Change the encapsulation on external links to meet the following requirements:

1. **Link between R2 and ISP.**
    a. Encapsulation: PPP
    b. Authentication: PAP
        i. Password: pppPAPencap
2. **Link between RemoteCPD and ISP.**
    a. Encapsulation: PPP
    b. Authentication: CHAP
        i. Password: pppCHAPencap

NOTE**: Save your work now. Copy the running-configuration to startup-configuration. Also, copy the running-configuration of all devices to a notepad and save the file with the name **CCNA_CS4_<login>_basic_conf.txt** (backup). If you perform the exercise in PT, save the file as **CCNA_CS4_<login>_basic_conf.pkt.

Phase 6: Basic Checking

1. **Perform a basic checking.**
    a. Connectivity between PC1 and R1.
    b. Connectivity between PC1 and R3.
    c. Connectivity between PC1 and PC2.
    d. Connectivity between PC1 and SW1, SW2 and SW3.
    e. Connectivity between PC1 and Internal Server.
    f. Connectivity between PC1 and its default gateway.
    g. Connectivity between PC2 and its default gateway.
    h. Connectivity between Internal Server and R1.
    i. Connectivity between Internal Server and R3.
    j. Connectivity between Internal Server and its default gateway.
    k. Connectivity between SW1 and R1 (all subinterfaces).

l. Connectivity between SW3 and R3 (all subinterfaces).
m. Connectivity between switches.
n. Connectivity between R1 and R2.
o. Connectivity between R2 and R3.
p. Connectivity between ISP and R2.
q. Connectivity between ISP and RemoteCPD.
r. Connectivity between PC3 and RemoteCPD.
s. Connectivity between Remote Server and RemoteCPD.
t. Connectivity between External Server and ISP.
u. Access to all routers with passwords assigned (Enable, Console and VTY lines).
v. Check port security on SW2.

Phase 7: NAT Configuration Requirements

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

1. Users within Sales network gain access to External Networks through a translation of internal IP addresses to the following range and using **different ports**.
    a. IP address range: **From 1.1.1.1 to 1.1.1.2**
    b. Network mask: **255.255.255.248**
2. Users in External networks gain access to Internal Server sending the requests to **1.1.1.4**.
3. Users within network attached to RemoteCPD gain access to External Networks through a translation of internal IP addresses to the following range and using **different ports**.
    a. IP address range: **From 2.2.2.1 to 2.2.2.2**
    b. Network mask: **255.255.255.248**
4. Users in External networks gain access to Remote Server sending the requests to **2.2.2.4**.

Phase 8: Routing Configuration

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

1. Internal Site
    a. OSPF with the Process ID 10 for R1, R2 and R3.
    b. R1 requirements:
        i. R1 is an *Area Border Router* (ABR).
        ii. Router ID: 1.1.1.1
        iii. R1 propagates OSPF routing information about all its directly connected networks.
        iv. R1 only sends and receives routing updates through serial interface.
        v. G0/0.X and S0/0/0 are inside area 0.
        vi. Loopback interfaces are inside area 1.
        vii. R1 summarizes area 1 routes to propagate the information to other areas.
    c. R2 requirements:
        i. R2 is an *Autonomous System Boundary Router* (ASBR).
        ii. Router ID: 2.2.2.2

iii. R2 is inside area 0 and propagates information of networks attached to S0/0/0 and S0/0/1.
iv. R2 sends and receives OSPF routing updates through S0/0/0 and S0/0/1 interfaces.
v. R2 has a default gateway toward ISP.
vi. R2 propagates default route information to R1 and R3.

d. R3 requirements:
i. R3 is an *Area Border Router* (ABR).
ii. Router ID: 3.3.3.3
iii. R3 propagates OSPF routing information about all its directly connected networks.
iv. R3 only sends and receives routing updates through serial interface.
v. G0/0.X and S0/0/1 are inside area 0.
vi. Loopback interfaces are inside area 2.
vii. R3 summarizes area 2 routes to propagate the information to other areas.

e. The cost reference bandwidth is adjusted to the fastest link of the topology.
f. The routers authenticate its identity with MD5 using the password ***routingOSPF***.
g. Routers send Hello packets every 5 seconds.
h. Routers break any adjacency with a neighbor if they don't receive a hello packet from that neighbor within 20 seconds.

2. External routing

a. BGP is the routing protocol used between Autonomous Systems (ASs).
b. R2 and ISP are eBGP neighbors.
c. RemoteCPD and ISP are eBGP neighbors.
d. R2 propagates the proper network via BGP to allow communication between AS 65100 users and external users.
e. RemoteCPD propagates the proper network via BGP to allow communication between AS 65101 users and external users.

3. Remote Site

a. RemoteCPD has a default gateway toward ISP.

4. Checking

a. Ping between all devices inside AS 65100. Successful? _____
b. Ping between Sales users and External Server. Successful? _____
c. Ping between RemoteCPD network users and external users. Successful? _____
d. Ping from External Server to Internal Server and to Remote Server. Successful? _____
e. Ping between networks inside AS 65100 and RemoteCPD network (AS 65101) (via private IP addresses). Successful? _____
f. Are all pings successful? Why or why not?

_____
_____
_____

5. **WAN connection**
    a. Connect AS 65100 and AS 65101 via a GRE tunnel between R2 and RemoteCPD.
    b. Configure a static route to 172.18.0.0/16 in R2 crossing the tunnel.
    c. Configure a static route to 172.16.0.0/16 in RemoteCPD crossing the tunnel.
    d. Check again the connectivity between networks inside AS 65100 and RemoteCPD network (AS 65101) via internal IP addresses. Successful? Why or why not?

    _____
    _____
    _____

Phase 9: DHCP Configuration Requirements

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

1. RemoteCPD is the DHCP Server.
   RemoteCPD serves IP addressing information to users in Sales network (172.16.10.0/24) and users directly attached to this router (172.18.10.0/24).
2. Exclude IP addresses that are yet assigned of being assigned in new DHCP requests (routers, servers, etc).
3. Change the configuration of PC1, PC2 and PC3 to request IP addressing parameters to DHCP Server.
4. DNS server is 200.200.200.100.
5. Perform a basic checking.
    a. Note the IP address of PC1: _____
    b. Note the IP address of PC2: _____
    c. Note the IP address of PC3: _____
    d. Do they belong to the pools created? _____
    e. Check connectivity between PC1 and other devices in internal and external networks.
    f. Check connectivity between PC2 and other devices in internal and external networks.
    g. Check connectivity between PC3 and other devices in internal and external networks.

Phase 10: Monitoring Requirements

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

1. External Server is the NTP server used to synchronize devices.
    a. Configure External Server as the NTP server for R1, R2, R3, RemoteCPD, SW1, SW2 and SW3.

    ***NOTE**: If any device does not support NTP commands, do the task theoretically for this device.*

b. Do all devices synchronize its time with External Server? Why or why not?

_____

_____

_____

2. Remote Server is the Syslog Server to centralize logs.
    a. Configure Remote Server as the Syslog server for R1, R2, R3, RemoteCPD, SW1, SW2 and SW3.
    b. Message Logging Level: Debugging
    c. Do all devices send the logs to Remote Server? Why or why not?

_____

_____

_____

Phase 11: ACL Configuration Requirements

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

1. Only users within Servers network have access to R1 VTY lines.
2. Only users within Sales network have access to Web service allocated in External Server.
3. Only users within RemoteCPD network have access to FTP service allocated in External Server.
4. The ping from Remote Server to Sales users is permitted but the ping from Sales users to Remote Server is prohibited.
5. The rest of the traffic (like other icmp traffic, routing updates, etc) is permitted.
6. **Apply ACLs carefully.**
7. **Configurations in ISP are not permitted.**
8. Perform a basic checking.
    a. Be sure that all requirements are fulfilled and there is still connectivity in the topology.

NOTE**: Copy the running-configuration of all devices to a notepad and save the file with the name **CCNA4_CS_<login>_vOSPF.txt.** If you perform the exercise in PT, save the file as **CCNA4_CS_<login>_vOSPF.pkt.

Phase 12: Routing challenge (optional)

Configure EIGRP as IGP routing protocol:

1. Erase OSPF routing configuration from R1, R2 and R3.
2. EIGRP with the *Autonomous System* number 20 for R1, R2 and R3.
3. R1 requirements:
    a. Router ID: 1.1.1.1
    b. R1 propagates EIGRP routing information about all its directly connected networks.
    c. R1 only sends and receives updates through its S0/0/0 interface.
    d. R1 does not have any Null0 route to a major class network in its routing table.
    e. R1 sends a summary route of the networks directly connected to its loopback interfaces.
4. R2 requirements:
    f. Router ID: 2.2.2.2
    g. R2 propagates EIGRP routing information about networks connected to its S0/0/0 and S0/0/1 interfaces.
    h. R2 does not have any Null0 route to a major class network in its routing table.
    i. R2 has a default gateway toward ISP.
    j. R2 propagates default route information to R1 and R3.
5. R3 requirements:
    k. Router ID: 3.3.3.3
    l. R3 propagates EIGRP routing information about all its directly connected networks.
    m. R3 only sends and receives updates through its S0/0/1 interface.
    n. R3 does not have any Null0 route to a major class network in its routing table.
    o. R3 sends a summary route of the networks directly connected to its loopback interfaces.
6. The percentage of bandwidth that may be used by EIGRP is up to 60%.
7. The routers authenticate its identity with MD5 using the password ***routingEIGRP***.
8. Routers send Hello packets every 10 seconds.
9. Routers break any adjacency with a neighbor if they don't receive a hello packet from that neighbor within 30 seconds.

NOTE*: Copy the running-configuration of all devices to a notepad and save the file with the name* ***CCNA4_CS_<login>_vEIGRP.txt.*** *If you perform the exercise in PT, save the file as* ***CCNA4_CS_<login>_vEIGRP.pkt.***

Phase 13: 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 (**physical and logical 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

The technical documentation has to include router output from the following commands (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
- 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

- show ip bgp summary
- show ip bgp
- For EIGRP optional part:
    - show ip route
    - show ip protocols
    - show ip eigrp neighbors
    - show ip eigrp topology
- show ip nat statistics
- show ip nat translations
- show ip dhcp binding
- show ip dhcp pool
- show ip access-lists
- show ntp status
- show logging

The technical documentation has to include switch output from the following commands (for each switch):

- show cdp neighbors
- show ip interface brief
- show version
- show startup-config
- show interfaces trunk
- show interface vlan <management vlan>
- show vlan brief
- show vtp status
- show spanning-tree
- show port-security
- show port-security interface <secured port>
- show etherchannel
- show etherchannel summary
- show logging