CCNA 4: ACCESSING THE WAN

CASE STUDY
Overview and Objectives

This case study allows students to complete a network design, implementation, and troubleshooting project using the skills gained in CCNA 4. 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 tasks to make sure that all requirements are fulfilled. Each task 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 switch with a basic switch configuration.
- Correctly configure the switching features that the design requirements describe.
- Correctly configure WAN encapsulation with PPP and Frame Relay.
- Correctly configure the Network Address Translation (NAT) needed to communicate inside users to external Servers and external users to internal Servers.
- Correctly configure DHCP features to provide dynamic addressing.
- Correctly configure Access Control Lists (ACL) to filter some traffic.
- Troubleshoot and test the connectivity between all devices.
- Provide detailed documentation in a prescribed form, as listed in the deliverables section.
LaSalle Telecom is a company that has several people responsible for designing and implementing a new network for ABC Company. 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 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

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/0</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.10</td>
<td>192.168.10.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.20</td>
<td>192.168.20.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/0.99</td>
<td>192.168.99.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Se0/0</td>
<td>172.16.0.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Se0/1</td>
<td>172.16.0.9</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>Se0/0</td>
<td>172.16.0.5</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Se0/1</td>
<td>172.16.0.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/0</td>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
<td>10.10.10.2</td>
</tr>
<tr>
<td>R3</td>
<td>Se0/0</td>
<td>172.16.0.10</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Se0/1</td>
<td>172.16.0.6</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/0</td>
<td>192.168.30.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>SW</td>
<td>VLAN 10</td>
<td>192.168.10.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>VLAN 20</td>
<td>192.168.20.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>VLAN 99</td>
<td>192.168.99.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>ISP</td>
<td>Fa0/0</td>
<td>10.10.10.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1</td>
<td>200.200.200.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>PC1</td>
<td>NIC</td>
<td>192.168.10.100</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>Internal Server</td>
<td>NIC</td>
<td>192.168.20.100</td>
<td>255.255.255.0</td>
<td>192.168.20.1</td>
</tr>
<tr>
<td>PC3</td>
<td>NIC</td>
<td>192.168.30.100</td>
<td>255.255.255.0</td>
<td>192.168.30.1</td>
</tr>
<tr>
<td>External Server</td>
<td>NIC</td>
<td>200.200.200.100</td>
<td>255.255.255.0</td>
<td>200.200.200.1</td>
</tr>
</tbody>
</table>

*Table 1: Addressing Table*

### Port Assignments

<table>
<thead>
<tr>
<th>Switch</th>
<th>Ports</th>
<th>Assignment</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW</td>
<td>F0/1 - F0/2</td>
<td>802.1q Trunks (Native VLAN 99)</td>
<td>192.168.99.0/24</td>
</tr>
<tr>
<td></td>
<td>F0/3 - F0/6</td>
<td>VLAN 10 – Users</td>
<td>192.168.10.0/24</td>
</tr>
<tr>
<td></td>
<td>Fa0/7 – Fa0/10</td>
<td>VLAN 20 - Servers</td>
<td>192.168.20.0/24</td>
</tr>
</tbody>
</table>

*Table 2: Port Assignments Table*

### VLANs Information

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VLAN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 99 (Native)</td>
<td>Management</td>
</tr>
<tr>
<td>VLAN 10</td>
<td>Users</td>
</tr>
<tr>
<td>VLAN 20</td>
<td>Servers</td>
</tr>
</tbody>
</table>

*Table 3: VLANs Information Table*
Phase 2: Basic Configuration Requirements

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

1. **Basic configuration for R1, R2 and R3.**
   a. Passwords must have a **minimum length of 10 characters.**
   b. AAA authentication on Console 0 and VTY lines.
      - Create a list named `AUTH` for the authentication methods. The first authentication method is the **local database** and the second is the **enable password**.
      - The database contains a user named `Admin01` with a password `admin01pass`.
   c. **Only SSH access** is permitted to VTY lines with a crypto key of 1024 bits.
      - Domain name: `CCNA4CS.com`
      - SSH version 2
   d. Enable secret password: `ciscoenpa55`
   e. Banner MOTD:
      
      `**************************
      This is the <router_name> CLI. 
      **************************`
   f. Interfaces configuration.
      - IP addressing and subnet masking according to Table 1
      
      **NOTE:** Remember that R1’s Fa0/0 requires special attention (InterVLAN Routing)
   g. Descriptions in point-to-point interfaces:
      ```
      Link <router1_name> - <router2_name>
      ```
   h. Descriptions in LAN interfaces/subinterfaces:
      ```
      LAN <LAN_name>
      ```

2. **Basic configuration for ISP.**
   a. Passwords must have a **minimum length of 10 characters.**
   b. Console 0 password: `ciscoconpa55`
   c. Line VTY password: `ciscovtypa55`
   d. **Only Telnet access** is permitted to VTY lines.
   e. Enable secret password: `ciscoenpa55`
   f. Banner MOTD:
      ```
      **************************
      This is the <router_name> CLI. 
      **************************
      ```
   g. Interfaces configuration.
      - IP addressing and subnet masking according to Table 1
   h. Descriptions in LAN interfaces/subinterfaces:
      ```
      LAN <LAN_name>
      ```
3. Basic configuration for SW.
   a. Passwords must have a minimum length of 10 characters.
   b. Console 0 password: ciscoconpa55
   c. Line VTY password: ciscotypa55
   d. Enable secret password: ciscoenpa55
   e. Banner MOTD:
      ***************************
      This is the <switch_name> CLI.
      ***************************
   f. Configure SVIs (Switched Virtual Interfaces) according Table 1.
   g. Configure SW ports assigned to VLANs according Table 2.
   h. The Management VLAN has to be accessible from remote devices.

4. Device interface configuration.
   a. Configure IP addressing for PC1, Internal Server, External Server and PC3.
      Interfaces according Table 1.

5. Perform a basic checking.
   a. Connectivity between PC1 and R1.
   b. Connectivity between SW and R1 (all SVIs).
   c. Connectivity between SW and PC1.
   d. Connectivity between SW and Internal Server.
   e. Connectivity between Internal Server and R1.
   f. Connectivity between PC3 and R3.
   g. Connectivity between R1 and R2.
   h. Connectivity between R1 and R3.
   i. Connectivity between R2 and R3.
   j. Connectivity between ISP and R2.
   k. Connectivity between External Server and ISP.
   l. Access to all routers with passwords assigned (Enable, Console and VTY lines).

Phase 3: Routing Configuration Requirements

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

1. Routing Configuration.
   a. OSPF with the Process ID 10 for R1, R2 and R3.
   b. R1 propagates OSPF routing information about all its directly connected networks.
   c. R3 propagates OSPF routing information about all its directly connected networks.
   d. R2 propagates OSPF routing information about its directly connected networks on Se0/0 and Se0/1.
   e. R1 only sends and receives OSPF routing updates through Se0/0 and Se0/1 interfaces.
   f. R2 only sends and receives OSPF routing updates through Se0/0 and Se0/1 interfaces.
g. R3 only sends and receives OSPF routing updates through Se0/0 and Se0/1 interfaces.

h. R2 has a default gateway toward ISP.

i. R2 propagates default route information to R1 and R3.

j. **ISP is not inside the OSPF Process.** ISP only knows information about its directly connected networks.

2. **Perform a basic checking.**
   a. Connectivity between all devices inside OSPF process.
   b. Connectivity between External Server and remote devices. Is it successful or not? Why?

### Phase 4: WAN Configuration Requirements

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

1. The link between R1 and R2 is encapsulated with PPP.
   a. Authentication: **CHAP**
   b. Password: **pppchapenc**

2. The link between R2 and R3 is encapsulated with Frame Relay.
   a. Encapsulation: **IETF**
   b. DLCI: **203**

3. The link between R1 and R3 is encapsulated with Cisco HDLC (default).

4. Perform a basic checking.
   a. Make sure that the connectivity between routers is still successful and the routing tables are correct.

### Phase 5: NAT Configuration Requirements

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

1. Users within networks 192.168.10.0/24 and 192.168.30.0/24 gain access to Public Domain through a translation of internal IP addresses to the Fa0/0 interface of R2 and different ports.

2. Users in the Public Domain gain access to Internal Server sending the requests to 10.10.10.100/24.

3. Perform a basic checking.
   a. Connectivity from users inside Private Domain to External Server.
   b. Connectivity from users inside Public Domain to Internal Server.

### Phase 6: DHCP Configuration Requirements

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

1. R2 is the DHCP Server.

2. R2 serves IP addressing information to users in networks 192.168.10.0/24 and 192.168.30.0/24.
3. Exclude IP addresses that are yet assigned or being assigned in new DHCP requests.
4. Change the configuration of PC1 and PC3 to request IP addressing parameters to DHCP Server.
5. Perform a basic checking.
   a. Note the IP address of PC1:
   b. Note the IP address of PC3:
   c. Do they belong to the pools created?
   d. Check connectivity between PC1 and other devices in Private and Public Domains.
   e. Check connectivity between PC3 and other devices in Private and Public Domains.

**Phase 7: ACL Configuration Requirements**

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

1. Only users within network 192.168.10.0/24 have access to R2 VTY lines. **Use standard named ACLs.**
2. Only users within network 192.168.10.0/24 have FTP access to the External Server.
3. Only users within network 192.168.30.0/24 have HTTP access to the External Server.
4. Ping from PC1 to PC3 is successful but ping from PC3 to PC1 is unsuccessful.
5. **Configurations in ISP are not permitted.**
6. Perform a basic checking.
   a. Be sure that all requirements are fulfilled and there is still connectivity in the topology.

**Phase 8: Troubleshooting**

The technician is assigned to check the connectivity and performance of the network implemented.

1. Repeat the checking done before to be sure that the performance is correct and provide documentation that specifies how the checking was tested.
2. Explain and justify the results.
Phase 9: 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 ip route
- show ip protocols
- show interfaces <type_slot_port>
- show startup-config
- show frame-relay pvc <DLCI>
- show frame-relay map
- show ip ospf neighbor
- show ip nat statistics
- show ip nat translations
- show ip nat translations
- show ip dhcp binding
- show ip dhcp pool
- show ip access-lists

**Switches**

- show cdp neighbors
- show ip interface brief
- show interfaces trunk
- show interface vlan <vlan>
- show vlan brief
- show startup-config

**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 person 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. Microsoft Visio or any paint program could be used to draw the network (physical or logical topology).

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 end devices
- 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 ip route
  - show ip protocols
  - show interfaces <type_slot_port>
  - show startup-config
  - show frame-relay pvc <DLCI>
  - show frame-relay map
  - show ip ospf neighbor
  - show ip nat statistics
  - show ip nat translations
  - show ip dhcp binding
  - show ip dhcp pool
  - show ip access-lists

- Switch output from the following commands should be captured and placed into this documentation:
  - show cdp neighbors
  - show ip interface brief
  - show interfaces trunk
  - show interface vlan <vlan>
  - show vlan brief
  - show startup-config