WANs

Cisco Networking Academy Program
CCNA 4: WAN Technologies
Overview and Objectives

This final case study allows students to build and configure a complex network using skills gained throughout the course. This case study is not a trivial task. To complete it as outlined with all required documentation will be a significant accomplishment.

The case study scenario describes the project in general terms, and will explain why the network is being built. Following the scenario, the project is broken into a number of phases, each of which has a detailed list of requirements. It is important to read and understand each requirement to make sure that the project is completed accurately.

The following tasks are required to complete the case study:

- Set up the physical layout of the network using the diagram and accompanying narrative
- Correctly configure single-area OSPF
- Correctly configure VLANs and 802.1q trunking
- Correctly configure Frame Relay
- Correctly configure Point to Point (PPP) and CHAP Authentication
- Correctly configure DHCP
- Correctly configure NAT
- Create and apply access control lists (ACL’S) on the appropriate routers and interfaces
- Verify that all configurations are operational and functioning according to the scenario guidelines
- Provide detailed documentation in a prescribed form as listed in the deliverables sections
A company needs a network to be designed and implemented. The company has locations in four cities. Three of the locations will be connected using leased-line serial links. The fourth location, Galway, will be connected using Frame Relay because of cost considerations. The company has previously used RIP version 2 in this location and wishes to continue using it for now. However, the other three locations will use OSPF, so RIP routes must be redistributed into the OSPF routing process.

One location, Cork, has a large and complex LAN. Due to the size and complexity, the company wants to create VLANs to control broadcasts, enhance security, and logically group users. The company also wants to use private addresses and DHCP throughout the WAN. NAT must be implemented for Internet connectivity. The company also wishes to limit Internet access to Web traffic while allowing multiple protocols within its own WAN.

Although private addresses (RFC 1918) will be used, the company appreciates efficiency and address conservation in design. To minimize wasted address space, they have requested VLSM to be used when appropriate.
Phase 1: Addressing the WAN & LAN

Use the following instructions to complete Phase 1:

- Use **172.16.0.0/11** for internal addressing with IP subnet zero enabled.
- Apply **/30 subnets** on all serial interfaces, using the last available subnets.
- Assign an appropriately sized subnet for the Cork LAN, which has about **1000** devices (use a 1024 block subnet):
  - VLAN 99: 40 devices (Management VLAN)
  - VLAN 2: 100 hosts
  - VLAN 3: 200 hosts
  - VLAN 4: 500 hosts
- Assign the appropriately sized subnet to the Limerick LAN, which has **200** hosts.
- Assign an appropriately sized subnet for the Galway LAN, which has **500** devices.
- Document all of the addressing in the tables below.

**DHCP POOL**

Configure DHCP services on the Galway router. DHCP should provide services to the following LANs hosts:

- Galway LAN,
- Cork’s VLAN 2, VLAN 3 and VLAN 4

DHCP should pass the following parameters to the hosts:

- IP address, Subnet Mask and Default Gateway
### Name | Interface/Subnet Mask
--- | ---
Limerick S0 |  
Cork E1 |  
Cork S0 |  
Cork S1 |  
Galway E0 |  
Galway S0 |  
Belfast E0 |  
Belfast S0 |  
Belfast S1 |  

### Name | Address Pools
--- | ---
Galway DHCP Pool: |  
VLAN 2 DHCP Pool: |  
VLAN 3 DHCP Pool: |  
VLAN 4 DHCP Pool: |  
Phase 2: Configuring the Routers, Static Default Route & OSPF Routing

Use the following instructions to complete Phase 2:

- Configure each router with a hostname and passwords.
- Configure each interface on the four routers documented in Phase 1.
- Configure OSPF on the Cork, Limerick, and Belfast routers.
- Configure and redistribute a Default Route into the OSPF routing process
- Configure Static routing between OSPF area 0 and the Galway Router
- Verify that the Limerick, Belfast, Galway, and Cork routers have connectivity through Layers 1-7.
- Capture and save the four router configuration files. Edit the text files, and include comments at the top of each file documenting the following:
  - Your name
  - The date
  - CCNA4 Case Study – Phase 2
  - The router name that corresponds to each file.

This documentation will serve as the deliverable item for Phase 2.
Phase 3: Configuring NAT, Frame Relay, PPP with CHAP, and ACL’s

Use the following instructions to complete Phase 3:

1. The Belfast router will perform NAT. Configure the Belfast router as follows:
   - Define the NAT pool. The pool consists of only one address of 200.10.10.64/26. Exclude first 10 addresses from this pool (to be use for servers, when needed).
   - Define an access control list, which will permit traffic from all internal (172.16.0.0/16) addresses, and deny all other traffic.
   - Establish dynamic source translation, specifying the NAT pool and the ACL defined in the previous steps.
     - Specify the inside and the outside NAT interfaces.
     - Change the default NAT timeout value to 120 seconds.

2. Connect a workstation to Belfast’s E0 port to simulate an ISP server. Configure this workstation as follows:
   - Configure the IP address and subnet mask as 10.0.0.2/8.
   - Configure the default gateway.
   - Configure the workstation to act as a web server. Create a simple web page that will tell users that they have reached the ISP.
3. Configure the Frame Relay as follows:
   - Configure the serial interface on both the Cork router and the Galway router to use Frame Relay encapsulation.
   - Use Frame-Relay maps (disable Inverse-Arp)
4. Configure PPP encapsulation and CHAP authentication between:
   - The Belfast router and the Cork router
   - The Belfast router and the Limerick router
   - Configure CHAP authentication on all PPP links, password Cisco
5. On the Cork Router: configure an **Extended ACL** on the Cork router to filter traffic. The ACL should:
   - permit HTTP access to the Internet
   - permit E-mail
   - Permit ICMP (for the purpose of testing connectivity)
   - Deny all other access to the ISP.
   - Permit all traffic to all destinations within the Autonomous System.
6. Recapture and save the Belfast, Cork, and Galway router configuration files. Capture and save the Frame Relay switch router configuration file. Edit the text files, and include comments at the top of each file documenting the following:
   - Your name
   - The date
   - CCNA4 Case Study – Phase 3
   - The router name that corresponds to each file.

Document the NAT configuration and the ISP Server configuration in the chart. This documentation will serve as the deliverable item for Phase 3.
Phase 4: Configuring VLANs and DHCP

Use the following instructions to complete Phase 4:

1. Configure the Cork Local Area Network switch as follows:
   - Create three more VLANs, for a total of 4 Vlans.
   Assign port 1 to trunk mode (802.1Q)
   - Assign ports 2-4 to VLAN1.
   - Assign ports 5-6 to VLAN2.
   - Assign ports 7-8 to VLAN3
   - Assign ports 9-12 to VLAN4.
   - Connect E1 of the Cork router to port 1
   - Connect a workstation to each VLAN.
   - Configure the workstations with appropriate IP addresses.

2. The Galway router will perform DHCP. Configure the Galway router as follows:
   Using the DHCP pool documented in Phase 1, configure E0 with the first useable address.
   - Configure the DHCP pool on the router.
   - Connect a workstation to E0 on Galway and VLANs 2-4 on Cork router.
   - Configure the workstation to obtain its IP address automatically.

3. Recapture and save the Galway router configuration file. Edit the text file, and include comments at the top documenting the following:
   - Your name
   - The date
   - CCNA4 Case Study
   - Phase 4 – Galway router

This documentation will serve as the deliverable item for Phase 4.
Phase 5: Verification and Testing

Use the following instructions to complete Phase 5:

1. Verify communication between various hosts in the network. Troubleshoot and fix any problems in the network until it works properly. Document the results of the tests in a table.

2. Recapture and save the router configuration files for all four routers. Edit the text files, and include comments at the top of each file documenting the following:
   – Your name
   – The date
   – CCNA4 Case Study – Final Router Configuration –
   The router name that corresponds to each file.

This documentation, along with the completed tables from Phase 1, Phase3, and Phase 5, will serve as the final deliverable item for the case study.