Case Study

WANs

Cisco Networking Academy Program
CCNA 4: WAN Technologies v3.0
Overview and Objectives

This final case study shows you how to build and configure a complex network using the skills you have acquired throughout the course. This case study is not a trivial task, and completing it with all the required documentation will be a significant accomplishment.

The case study scenario describes the project in general terms and explains why the network is being built. Following the scenario, the project is then broken into a number of phases, each of which includes a detailed list of requirements. It is crucial that you read and understand each requirement to make sure that your project is complete.

This case study requires that you accomplish the following:

- 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 DHCP.
- Correctly configure NAT.
- Create and apply access control lists on the appropriate router(s) and interface(s).
- 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.
You are being asked to design and implement a network for a company that 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 you must redistribute RIP routes into the OSPF routing process.

One location, Cork, has a large and complex LAN; therefore, the company requests the creation of VLANs to control broadcasts, enhance security, and logically group users. The company also requests the use of private addresses and DHCP throughout the WAN, so you must properly implement NAT for Internet connectivity. Finally, the company wishes to limit Internet access to Web traffic while allowing multiple protocols within its own WAN.

Although private addresses (RFC 1918) will be used, VLSM should be used to minimize wasted address space for efficiency and elegance in design.
Phase 1: Addressing the WAN

Instructions:

- Use 172.16.0.0 for internal addressing with IP subnet zero enabled.
- Apply /30 subnets to all serial interfaces and to the link between Cork and Limerick, using the last available subnets.
- Assign an appropriately sized subnet for the DHCP pool on the Galway LAN, which has 512 devices.
- Assign an appropriately sized subnet for the Cork LAN, which has 750 devices.
- Document all addressing in the tables that follow this step. This documentation will serve as your deliverable item for Phase 1.

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limerick S0</td>
<td></td>
</tr>
<tr>
<td>Cork E1</td>
<td></td>
</tr>
<tr>
<td>Cork S0</td>
<td></td>
</tr>
<tr>
<td>Cork S1</td>
<td></td>
</tr>
<tr>
<td>Galway E0</td>
<td></td>
</tr>
<tr>
<td>Galway S0</td>
<td></td>
</tr>
<tr>
<td>Belfast E0</td>
<td></td>
</tr>
<tr>
<td>Belfast S0</td>
<td></td>
</tr>
<tr>
<td>Belfast S1</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Address Pools</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Galway DHCP Pool</td>
<td></td>
</tr>
<tr>
<td>Cork LAN</td>
<td></td>
</tr>
</tbody>
</table>
Phase 2: Configuring the Routers and OSPF

Instructions:

1. Configure each router with a hostname and password.
2. Configure each interface on the four routers that are documented in Phase 1.
3. Configure OSPF on the Cork, Limerick, and Belfast routers.
4. Configure RIP and redistribute through the OSPF tables.
5. Verify that the Limerick, Belfast, and Cork routers have connectivity through layers 1-7.
6. 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 your deliverable item for Phase 2.
Phase 3: Configuring NAT, Frame Relay Simulation, and Access Control List (ACLs)

Instructions:

1. The Belfast router will perform NAT. Configure the Belfast router as follows:
   - Define the NAT pool, which consists of only one address. This is the public address 192.168.1.6/30.
   - Define an access control list, which will permit traffic from all internal (172.16.0.0/24) addresses and deny all other traffic.
   - Establish dynamic source translation, specifying the NAT pool and the ACL, as defined in the previous steps.
   - Specify the interior and the exterior 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 inform users that they have reached the ISP.

3. Configure the Frame Relay simulator as follows:
   - Configure S0 on both the Cork router and the Galway router to use Frame Relay encapsulation.
- Configure the router between Cork and Galway to simulate a Frame Relay switch.

4. Configure an ACL to filter traffic from source addresses on the Galway LAN. The ACL should permit HTTP access to the ISP, deny all other access to the ISP, and permit all traffic to destinations within the WAN.

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 your NAT configuration and your ISP Server configuration in the following table. This documentation will serve as your deliverable item for Phase 3.

<table>
<thead>
<tr>
<th>Item</th>
<th>Configured Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belfast: Name of NAT pool</td>
<td></td>
</tr>
<tr>
<td>Belfast: ACL number</td>
<td></td>
</tr>
<tr>
<td>ACL Number for ACL filtering Galway LAN traffic</td>
<td></td>
</tr>
<tr>
<td>Router for ACL filtering Galway LAN traffic</td>
<td></td>
</tr>
<tr>
<td>Configured port for ACL filtering Galway LAN traffic</td>
<td></td>
</tr>
<tr>
<td>Configured direction for ACL filtering Galway LAN traffic</td>
<td></td>
</tr>
<tr>
<td>ISP Server IP address</td>
<td></td>
</tr>
<tr>
<td>ISP Server subnet mask</td>
<td></td>
</tr>
<tr>
<td>ISP Server default gateway</td>
<td></td>
</tr>
<tr>
<td>Filename of web page on ISP Server (including path)</td>
<td></td>
</tr>
</tbody>
</table>
Phase 4: Configuring VLANs and DHCP

Instructions:

1. Configure the Cork LAN switch as follows:
   - Create three VLANs.
   - Assign ports 1-4 to VLAN 1.
   - Assign ports 5-8 to VLAN 2.
   - Assign ports 9-12 to VLAN 3.
   - Connect E1 of the Cork router to a VLAN 1 port.
   - 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.
   - 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 your deliverable item for Phase 4.
Phase 5: Verification and Testing

Instructions:

1. Verify communication between various hosts in the network. Troubleshoot and fix any problems in the network until it works properly. Document your tests in the table below:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Expected Result</th>
<th>Date Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host on VLAN1</td>
<td>ISP</td>
<td>HTTP</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN1</td>
<td>Host on Galway LAN</td>
<td>Ping</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN1</td>
<td>Host on VLAN2</td>
<td>Ping</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN1</td>
<td>Host on VLAN3</td>
<td>Ping</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN2</td>
<td>Host on VLAN3</td>
<td>Ping</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN2</td>
<td>Host on Galway LAN</td>
<td>Ping</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN2</td>
<td>ISP</td>
<td>HTTP</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN3</td>
<td>Host on Galway LAN</td>
<td>Ping</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on VLAN3</td>
<td>ISP</td>
<td>HTTP</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>Host on Galway LAN</td>
<td>ISP</td>
<td>HTTP</td>
<td>Success</td>
<td></td>
</tr>
<tr>
<td>Host on Galway LAN</td>
<td>ISP</td>
<td>Telnet</td>
<td>Failure</td>
<td></td>
</tr>
</tbody>
</table>

4. Recapture and save the router configuration files for all five routers. Edit the text files, and include comments at the top of each file, documenting the following:
   - Your name
   - The date
- CCNA 4 Case Study: Final Router Configuration
- The router name that corresponds to each file

This documentation, along with the completed tables from Phase 1, Phase 3, and Phase 5, will serve as your final deliverable items for the case study.
Instructor Notes

Phase 1

VLSM can offer many solutions. Although they vary greatly in size, remember that /22 subnets are the only ones that can be used for the two LANs. Check that the students’ solutions are correct before they proceed to subsequent phases of the case study. In Phase 5, students should not troubleshoot errors in the addressing scheme.

Because this is the basis for a number of other parts of the case study, you need to make sure that students document their addresses and keep the documentation.

Following is one of several possible solutions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface/Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limerick S0</td>
<td>172.16.255.249/30</td>
</tr>
<tr>
<td>Cork E1</td>
<td>172.16.255.2/30</td>
</tr>
<tr>
<td>Cork S0</td>
<td>172.16.255.241/30</td>
</tr>
<tr>
<td>Cork S1</td>
<td>172.16.255.246/30</td>
</tr>
<tr>
<td>Galway E0</td>
<td>172.16.0.1/22</td>
</tr>
<tr>
<td>Galway S0</td>
<td>172.16.255.242/30</td>
</tr>
<tr>
<td>Belfast S0</td>
<td>10.0.0.1/8</td>
</tr>
<tr>
<td>Belfast E0</td>
<td>172.16.255.245/30</td>
</tr>
<tr>
<td>Belfast S1</td>
<td>172.16.255.250/22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Address Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Galway DHCP Pool</td>
<td>172.16.4.0/22</td>
</tr>
<tr>
<td>Cork LAN</td>
<td>172.16.0.0/22</td>
</tr>
</tbody>
</table>
Phase 2

Following is an example of the configuration on the Cork router. Remember to issue the `clockrate 56000` command in interface configuration mode on any serial DCE interfaces.

1.

```
Router> enable
Router# configure terminal
Router(config)# hostname Cork
Cork(config)# enable secret cisco
Cork(config)# line vty 0 4
Cork(config-line)# password cisco
```

2.

```
Cork(config)# interface serial 0
Cork(config-if)# ip address 172.16.255.241 255.255.255.252
Cork(config-if)# no shutdown
```

3.

```
Cork(config)# router ospf 1
Cork(config-router)# network 172.16.255.244 0.0.0.3 area 0
Cork(config-router)# network 172.16.255.2 0.0.0.3 area 0
Cork(config-router)# network 172.16.4.0 0.0.3.255 area 0
```

4.

```
Cork(config)# router rip
Cork(config-router)# version 2
Cork(config-router)# network 172.16.0.0
Cork(config-router)# exit
Cork(config)# router ospf 1
Cork(config-router)# redistribute rip subnets
```

You can verify layer 1-7 connectivity through Telnet. You can verify layer 1-3 through Ping.

Any line in a configuration file that begins with an exclamation point character is a comment line.
## Phase 3

The following table lists the answers to the configured values.

<table>
<thead>
<tr>
<th>Item</th>
<th>Configured Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belfast: Name of NAT pool</td>
<td>BelfastPool</td>
</tr>
<tr>
<td></td>
<td>(Can be any word consisting of letters and/or numbers)</td>
</tr>
<tr>
<td>Belfast: ACL number</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>(This can be any value between 1 and 99.)</td>
</tr>
<tr>
<td>ACL number for ACL filtering Galway LAN traffic</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>(This can be any value between 100 and 199.)</td>
</tr>
<tr>
<td>Router for ACL filtering Galway LAN traffic</td>
<td>Galway</td>
</tr>
<tr>
<td></td>
<td>(This is closest to the source for an extended ACL.)</td>
</tr>
<tr>
<td>Configured port for ACL filtering Galway LAN traffic</td>
<td>E0</td>
</tr>
<tr>
<td>Configured direction for ACL filtering Galway LAN traffic</td>
<td>In</td>
</tr>
<tr>
<td>ISP Server IP address</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>ISP Server subnet mask</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>ISP Server default Gateway</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td></td>
<td>(Must be the same value as Phase 1, Belfast E0; can be 10.0.0.1 or any value from 10.0.0.3-10.0.0.254.)</td>
</tr>
<tr>
<td>Filename of web page on ISP Server (including path)</td>
<td>c:...\htdocs\index.html</td>
</tr>
<tr>
<td></td>
<td>(If running Apache, the location of the htdocs subdirectory depends on the Apache directory tree installed; if you are running Windows NT server, the location will differ.)</td>
</tr>
</tbody>
</table>

1. After configuring the port addresses as specified in Phase 1, the following commands are used to configure NAT on the Belfast router:

   ```
   Belfast# configure terminal
   Belfast(config)# ip nat pool BelfastPool 192.168.1.6 192.168.1.6 netmask 255.255.255.252
   Belfast(config)# access-list 1 permit 172.16.0.0 0.0.0.255
   Belfast(config)# access-list 1 deny any
   Belfast(config)# ip nat inside source list 1 pool BelfastPool
   Belfast(config)# interface s0
   Belfast(config-if)# ip nat inside
   Belfast(config-if)# interface s1
   Belfast(config-if)# ip nat inside
   ```
Belfast(config-if)# interface e0
Belfast(config-if)# ip nat outside
Belfast(config-if)# exit
Belfast(config)# ip nat translation timeout 120

2. The following commands are used to configure the ISP Server workstation (assuming that it is a Windows PC):
   - Go to the Control Panel, and double-click Network.
   - Double-click TCP/IP.
   - Under the IP Address tab, select Specify an IP Address. Enter 10.0.0.2 as the IP address and 255.0.0.0 as the subnet mask.
   - Under the Gateway tab, enter the same IP address as configured on the E0 port of Belfast, and click Add.
   - Click OK twice, and reboot the PC.
   - If the ISP PC is running Windows NT, then it can be configured as an NT web server. Consult the operating system documentation for instructions.

   Alternatively, web server software (such as Apache) can be downloaded and installed.

   ■ The following link explains how to install Apache: http://perl.about.com/library/weekly/aa020502a.htm
   ■ The following link can be helpful in debugging the Apache installation: http://www.thesitewizard.com/archive/apache.shtml
   ■ Copy the HTML document that tells users that they have reached the ISP to the htdocs subdirectory in the Apache directory tree.
   ■ If the name of the HTML document is not index.html, search for a file named httpd.conf and open it in a text editor. Find the line in the file that begins with DirectoryIndex and add the filename between the word DirectoryIndex and the word index.html. The files listed after DirectoryIndex represent the prioritized order in which files are searched and opened.

3. The following commands configure the Cork router for Phase 3:

Cork# configure terminal
Cork(config)# interface s0
Cork(config-if)# encapsulation frame-relay

The following commands configure the Galway router for Phase 3. The ACL shown is one of several possible solutions.

Galway# configure terminal
Galway(config)# interface s0
Galway(config-if)# encapsulation frame-relay
Galway(config-if)# exit
Galway(config)# access-list 101 permit any 10.0.0.2 0.0.0.0 eq 80
Galway(config)# access-list 101 deny any 10.0.0.2 0.0.0.0
Galway(config)# access-list 101 permit any any
Galway(config)# interface e0
Galway(config-if)# ip access-group 101 in

The following commands configure the router simulating the Frame Relay switch:

FR# configure terminal
FR(config)# frame-relay switching
FR(config)# interface s0
FR(config-if)# no ip address
FR(config-if)# encapsulation frame-relay
FR(config-if)# clock rate 56000
FR(config-if)# frame-relay intf-type dce
FR(config-if)# frame-relay route 21 interface serial 1 20
FR(config-if)# no shutdown
FR(config-if)# interface s1
FR(config-if)# no ip address
FR(config-if)# encapsulation frame-relay
FR(config-if)# clock rate 56000
FR(config-if)# frame-relay intf-type dce
FR(config-if)# frame-relay route 20 interface serial 0 21
FR(config-if)# no shutdown
Phase 4

1. Use the following commands configure the Cork switch. These commands assume that the switch is reset to its default settings. To reset the switch, select [S] System from the Main Menu, and then select [R] Reset System.

   - Select [V] Virtual LAN Menu from the Main menu.
   - Select [A] Add VLAN from the Virtual LAN menu.
   - Enter [1] Ethernet; press Enter.
   - Select [S] Save and Exit. This creates VLAN 2, which will use the default VLAN name of VLAN0002. VLAN 1 is configured by default.
   - Select [A] Add VLAN from the Virtual LAN menu.
   - Enter [1] Ethernet; press Enter.
   - Select [S] Save and Exit. This creates VLAN 3.
   - Select [E] VLAN Membership.
   - Select [V] VLAN Assignment. Enter ports 5-8, and assign them to VLAN 2.
   - Select [V] VLAN Assignment again. Enter ports 9-12, and assign them to VLAN 3.
   - Select [X] Exit to the Previous menu.
   - Connect E1 on the Cork router to a VLAN1 port on the switch

2. After configuring the port addresses as specified in Phase 1, use the following commands to configure DHCP on the Galway router. In the network and default-router commands, use the network address for the E0 network on Galway from Phase 1.

   Galway# configure terminal
   Galway(config)# ip dhcp pool GalwayPool
   Galway(dhcp-config)# network x.x.x.x
   Galway(dhcp-config)# default-router x.x.x.x
Phase 5

Troubleshooting is a difficult process to learn. Encourage students to work systematically when troubleshooting. If communication that is expected to succeed fails, students should ping in a systematic manner beginning with the link closest to the source, and proceeding to the next link only when successful. There may be more than one problem preventing communication between the source and the destination; after a problem is found and fixed, the process should resume and continue until communication between the source and the destination is verified.

Use `winipcfg` or `ipconfig /all` to ensure the hosts are configured properly.

The following router commands are helpful when troubleshooting router configuration problems:

- `show running-config`
- `show protocol`
- `show interface`
- `show ip route`
- `show frame-relay`