Case Study

WANs

Cisco Networking Academy Program

CCNA 4: WAN Technologies v3.1

Overview and Objectives

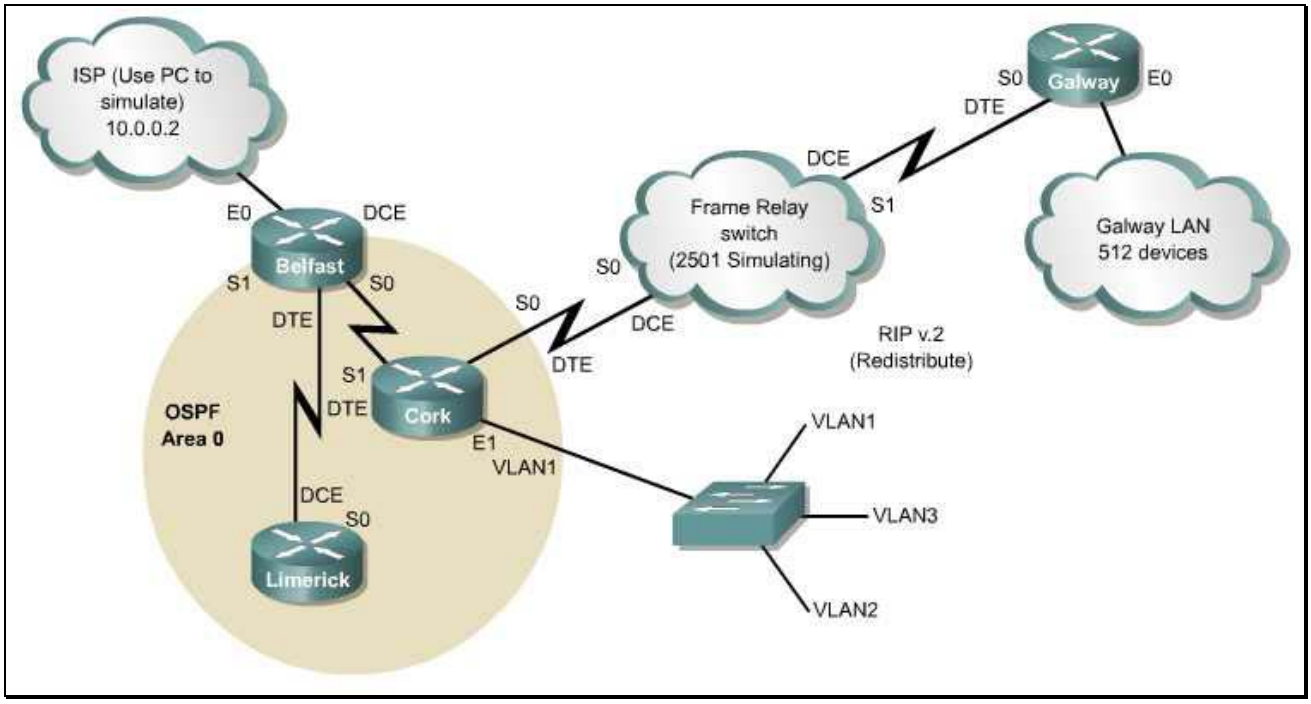
This final case study allows students to build and configure a complex network using skills gained throughout the course. This case study is not a trivial task. To complete it as outlined with all required documentation will be a significant accomplishment.

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 DHCP
- Correctly configure NAT
- Create and apply access control lists 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

Scenario

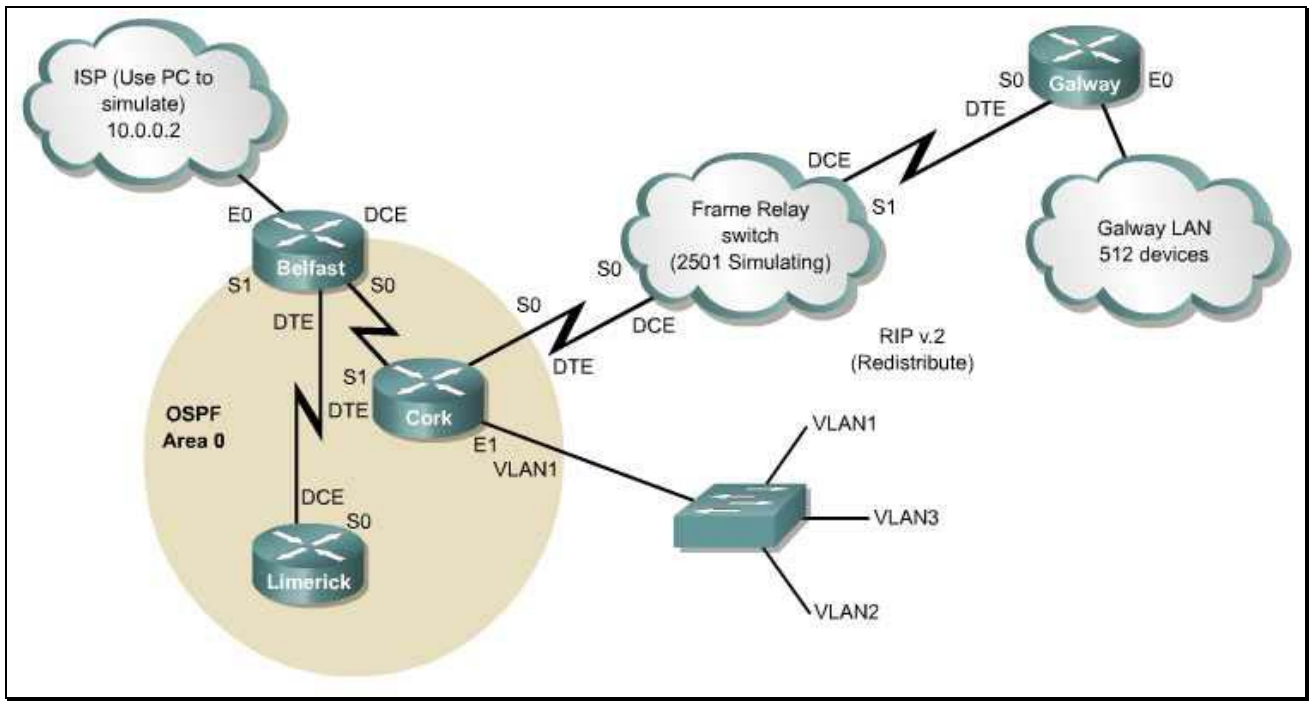


A company needs a network to be designed and implemented. The company has locations in four cities. Three of the locations will be connected using leased-line serial links. The fourth location, Galway, will be connected using Frame Relay because of cost considerations. The company has previously used 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



Use the following instructions to complete Phase 1:

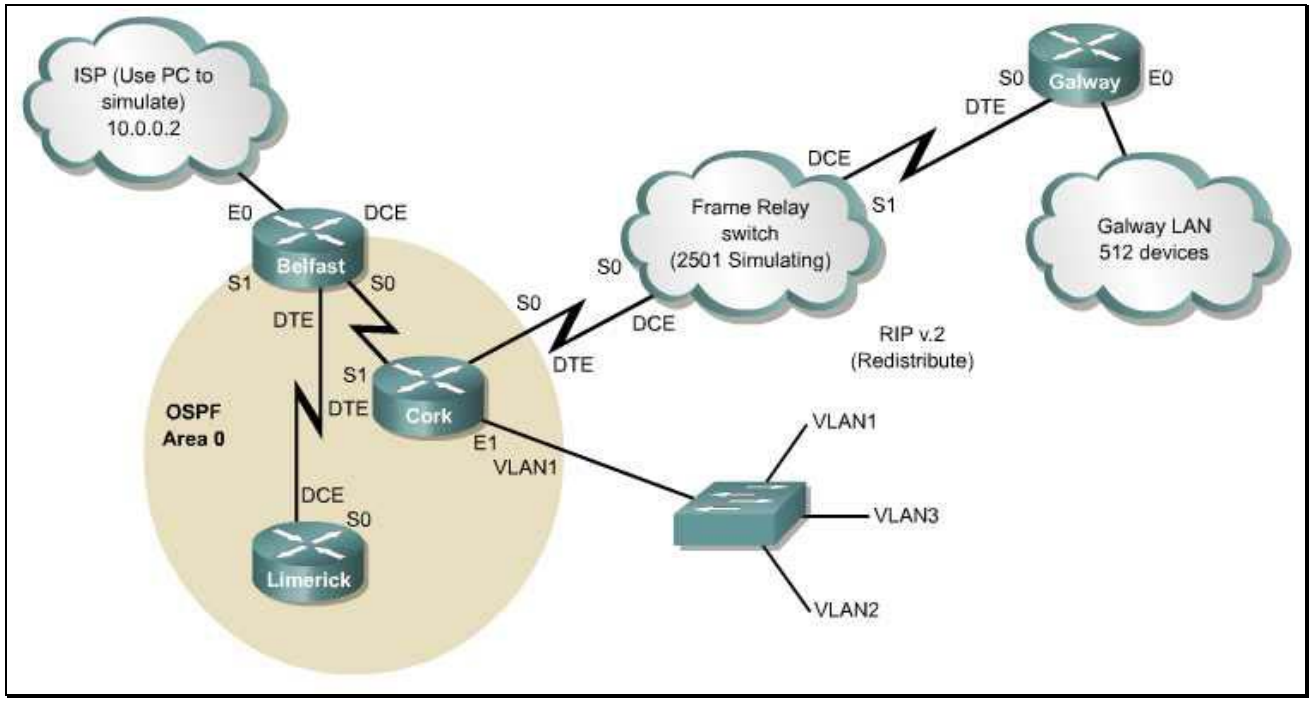
- Use 172.16.0.0 for internal addressing with IP subnet zero enabled.
- Apply /30 subnets on all serial interfaces, using the last available subnets.
- Assign an appropriately sized subnet for the DHCP pool on the Galway LAN, which has 512 devices.
- Assign an appropriately sized subnet for the Cork LAN, which has 750 devices.
- Document all of the addressing in the tables below.

This documentation will serve as the deliverable item for Phase 1.

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	
Cork LAN	

Phase 2: Configuring the Routers and OSPF

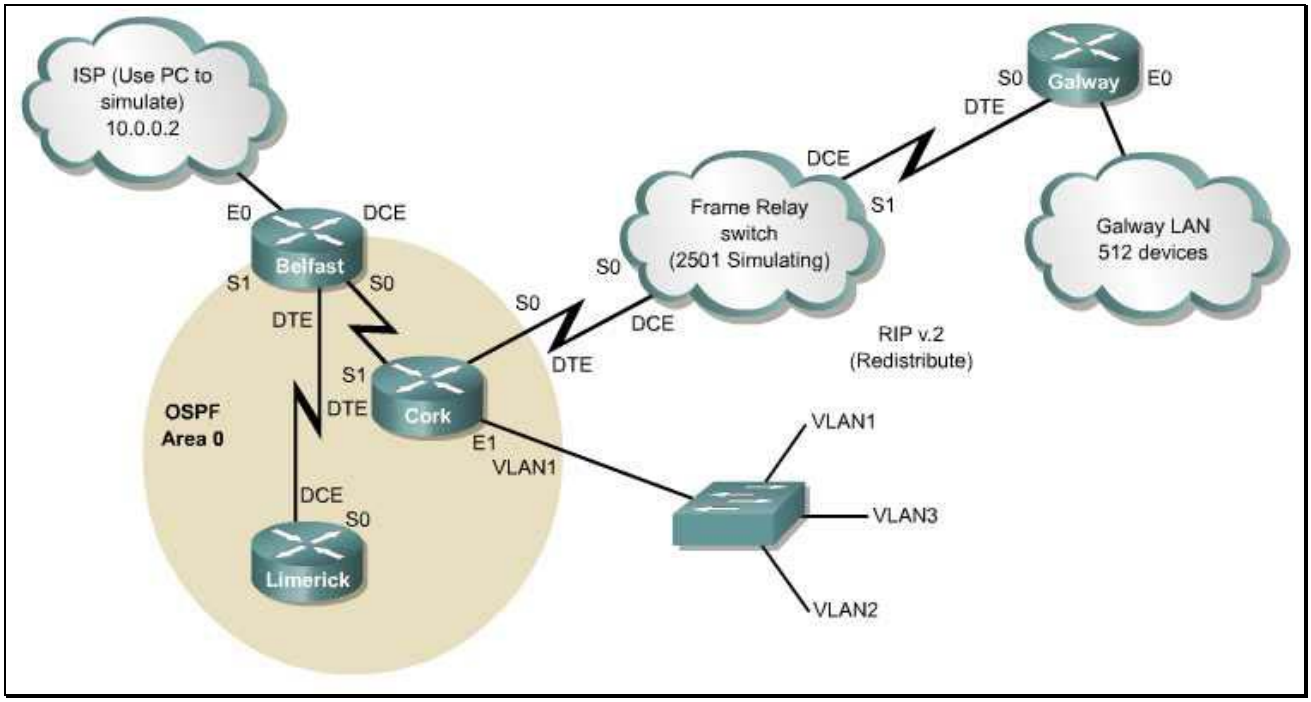


Use the following instructions to complete Phase 2:

- 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 RIP into the OSPF routing process
- 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 Simulation, and ACLs



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 192.168.1.6/30.
   - 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.

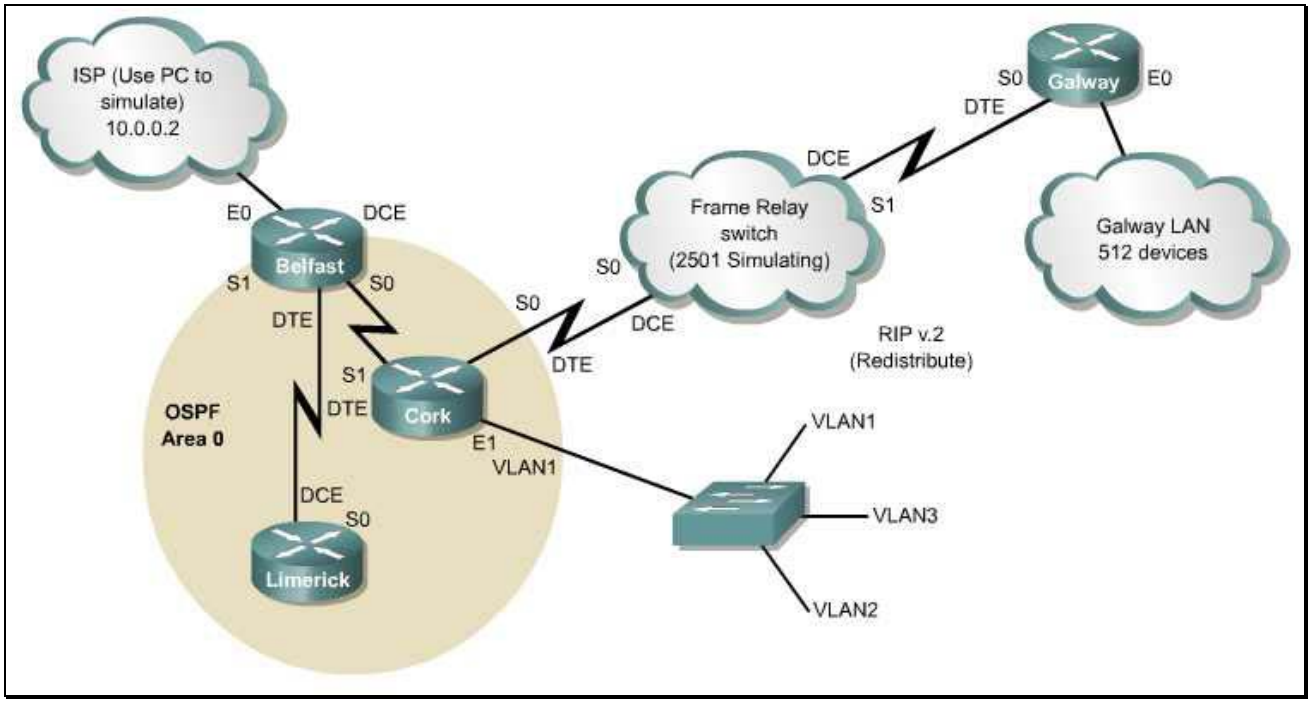
3. Configure the Frame Relay simulator as follows:
   - Configure S0 on both the Cork router and the Galway router to use Frame Relay encapsulation.
   - Configure the router between Cork and Galway to simulate a Frame Relay switch.
4. Configure an ACL to filter traffic from source addresses on the Galway 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.
5. 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 below.

This documentation will serve as the deliverable item for Phase 3.

Item	**Configured Values**
Belfast: Name of NAT Pool	
Belfast: ACL Number	
ACL Number for ACL Filtering Galway LAN Traffic	
Router for ACL Filtering Galway LAN Traffic	
Configured Port for ACL Filtering Galway LAN Traffic	
Configured Direction for ACL Filtering Galway LAN Traffic	
ISP Server IP Address	
ISP Server Subnet Mask	
ISP Server Default Gateway	
Filename of web page on ISP Server (include path)	

Phase 4: Configuring VLANs and DHCP



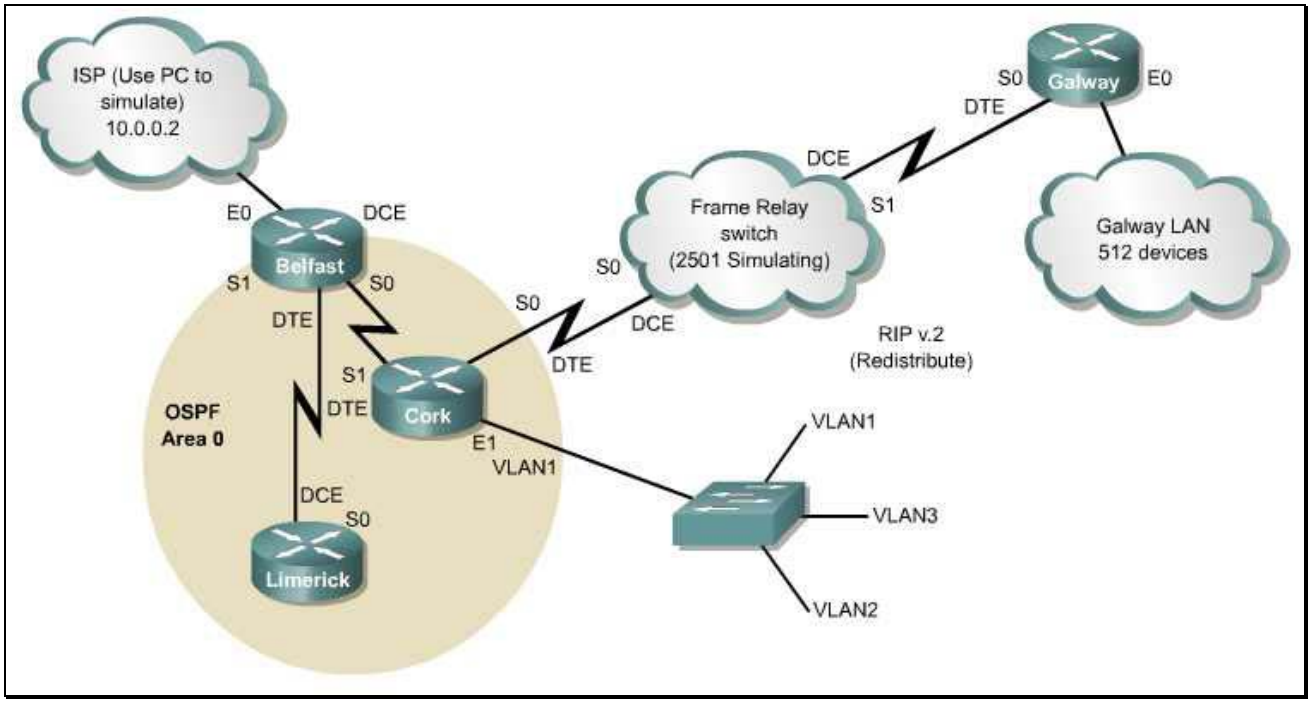
Use the following instructions to complete Phase 4:

1. Configure the Cork Local Area Network switch as follows:
   - Create three VLANs.
   - Assign ports 1-4 to VLAN1.
   - Assign ports 5-8 to VLAN2.
   - Assign ports 9-12 to VLAN3.
   - Connect E1 of the Cork router to a VLAN1 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 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 the table below:

Source	Destination	Protocol	Expected Result	Date Verified
Host on VLAN1	ISP	HTTP	Success	
Host on VLAN1	Host on Galway LAN	Ping	Success	
Host on VLAN1	Host on VLAN2	Ping	Failure	
Host on VLAN1	Host on VLAN3	Ping	Failure	
Host on VLAN2	Host on VLAN3	Ping	Failure	
Host on VLAN2	Host on Galway LAN	Ping	Failure	
Host on VLAN2	ISP	HTTP	Failure	
Host on VLAN3	Host on Galway LAN	Ping	Failure	
Host on VLAN3	ISP	HTTP	Failure	
Host on Galway LAN	ISP	HTTP	Success	
Host on Galway LAN	ISP	Telnet	Failure	

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.

