Routing and Switching

Cisco Networking Academy
Routing and Switching Essentials

Case Study 2018

Overview and Objectives

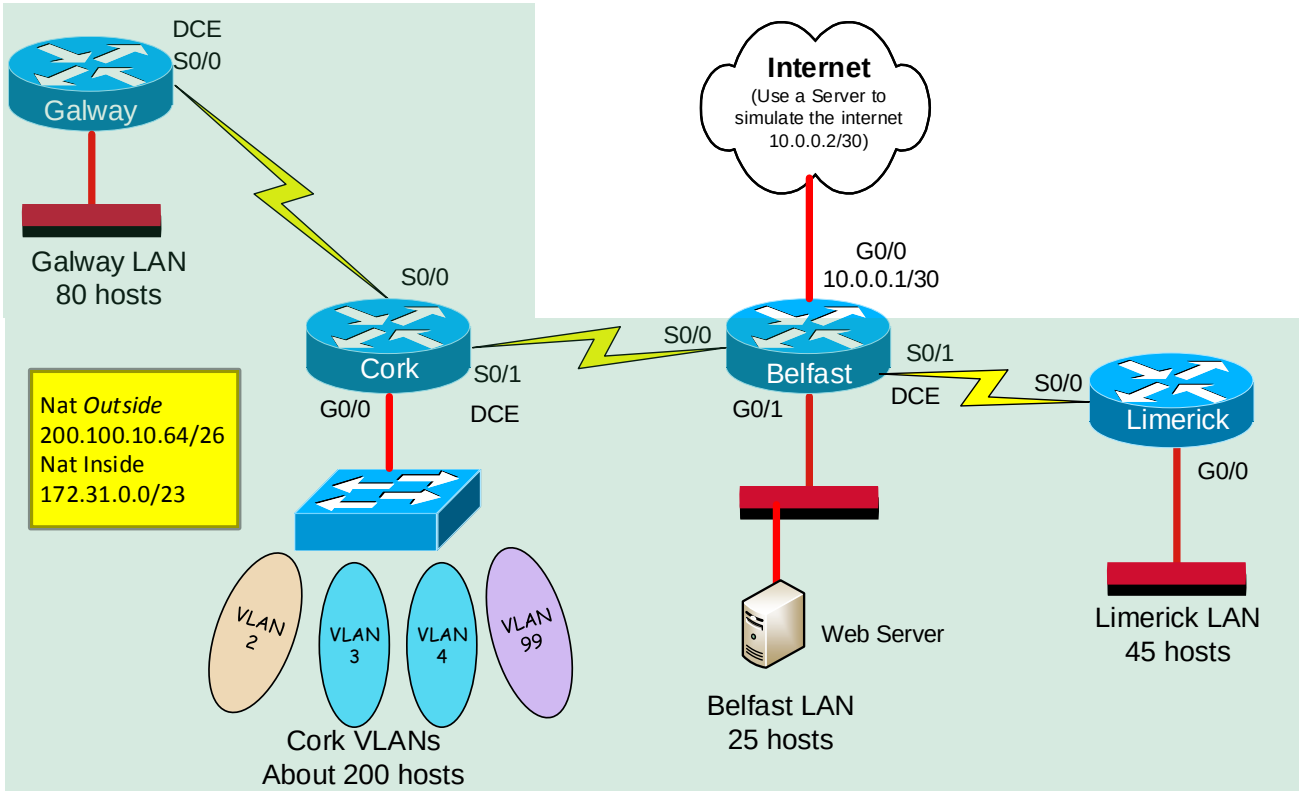
This case study allows students fully Design a complex network using skills gained throughout the course but build and configure only a **PROTOTYPE** as seen in the following diagram. This case study is not a trivial task. To complete it as outlined with all required documentation will be a significant 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 this case study:

- Set up the physical layout of the network using the diagram and accompanying narrative.
- Correctly configure Interfaces on all routers
- Correctly configure VLANS
- Correctly configure IEEE 802.1q trunking
- Correctly configure RIP Version 2 routing
- Correctly configure DHCP
- Correctly configure NAT
- Create and apply access control lists (ACL'S) on the appropriate routers and interfaces
- Test and verify that all devices are operational and functioning according to the scenario guidelines and this document.
- Provide detailed documentation in a prescribed form as listed in the deliverables sections.

Scenario

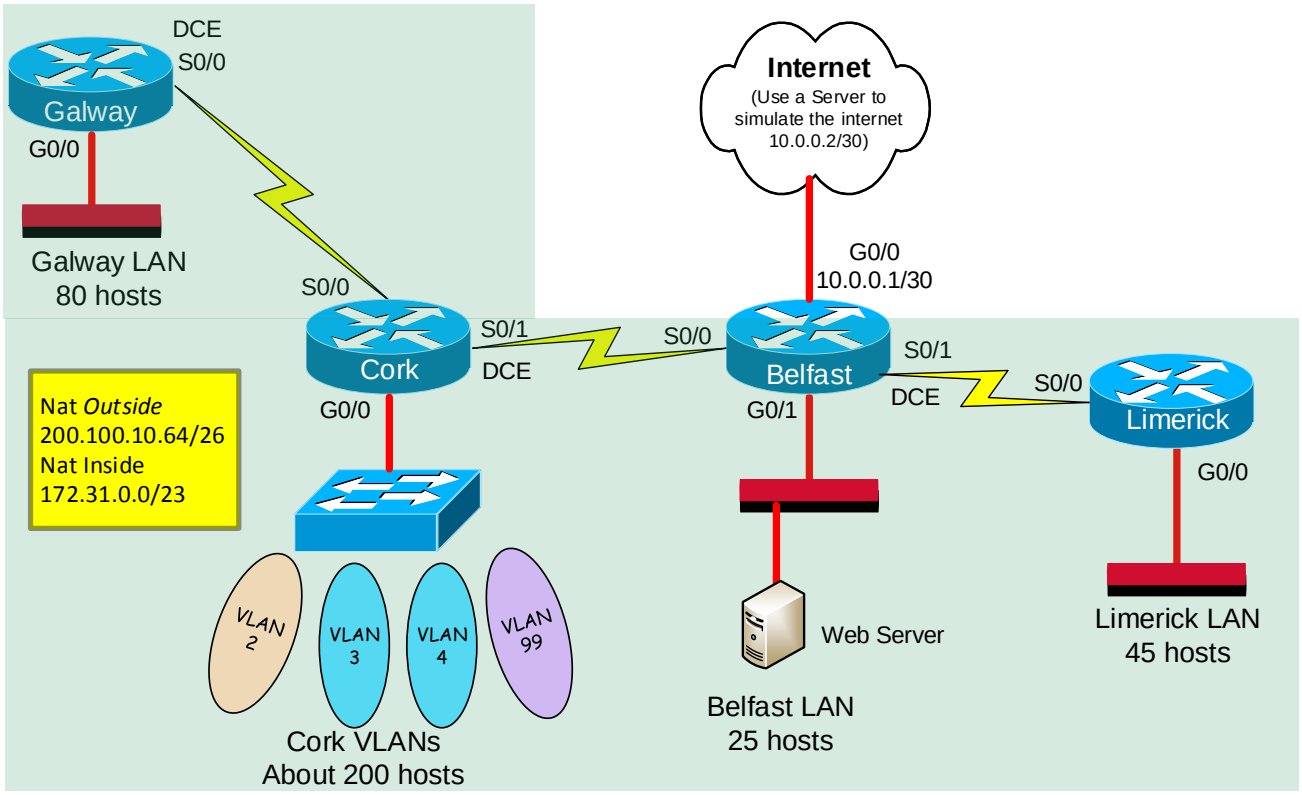


A company needs a network to be designed and implemented; the company has locations in four cities. All of the locations will be connected using leased-line (T1) serial links. The company has previously used RIP version 2; however, a default static route must be used and distributed to allow access to the internet.

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 throughout the Autonomous System, DHCP over most of the LAN segments, Static and Dynamic NAT implemented for Internet connectivity. The company also wishes to limit access to some LAN segments within the network.

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

Phase 1: Addressing the WANs, LANs & VLANs

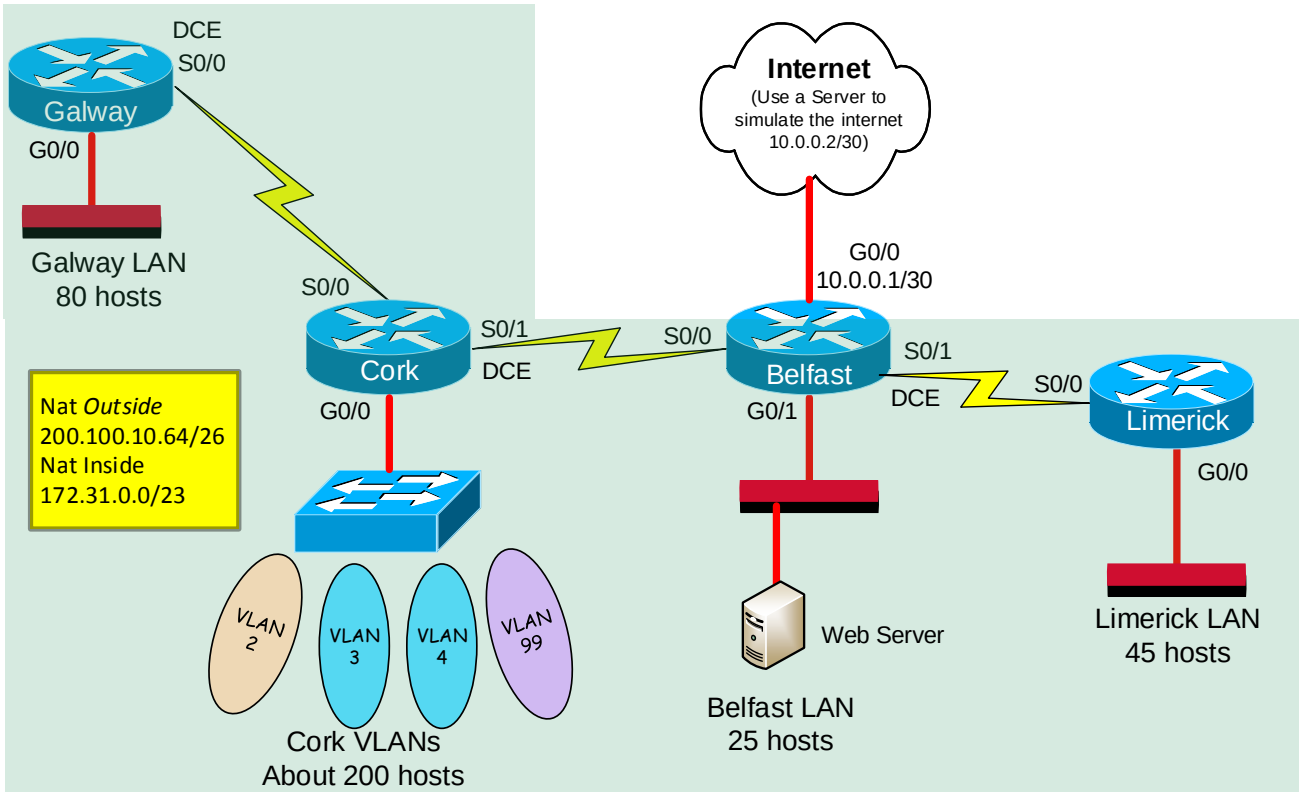


Use the following instructions to complete Phase 1:

- Use **172.31.0.0/23** for internal addressing.
- Apply **/30 subnets** on all serial interfaces, using the **last** available subnet.
- Assign an appropriately sized subnet for the **Cork** LAN, has about **200** devices:
  - VLAN 99: 25 devices (Management VLAN)
  - VLAN 2: 55 hosts (R&D)
  - VLAN 3: 20 hosts (HR)
  - VLAN 4: 100 hosts (Production)
- Assign the appropriately sized subnet to the **Limerick** LAN (**45** hosts).
- Assign an appropriately sized subnet for the **Belfast** LAN (**25** Hosts).
- Assign an appropriately sized subnet for the **Galway** LAN (**80** Hosts).
- Document the addressing scheme in tables.

Addresses will be assigned dynamically to hosts; refer to the DHCP section to this document for details.

Phase 2: Configuring Default Routes & RIP Routing

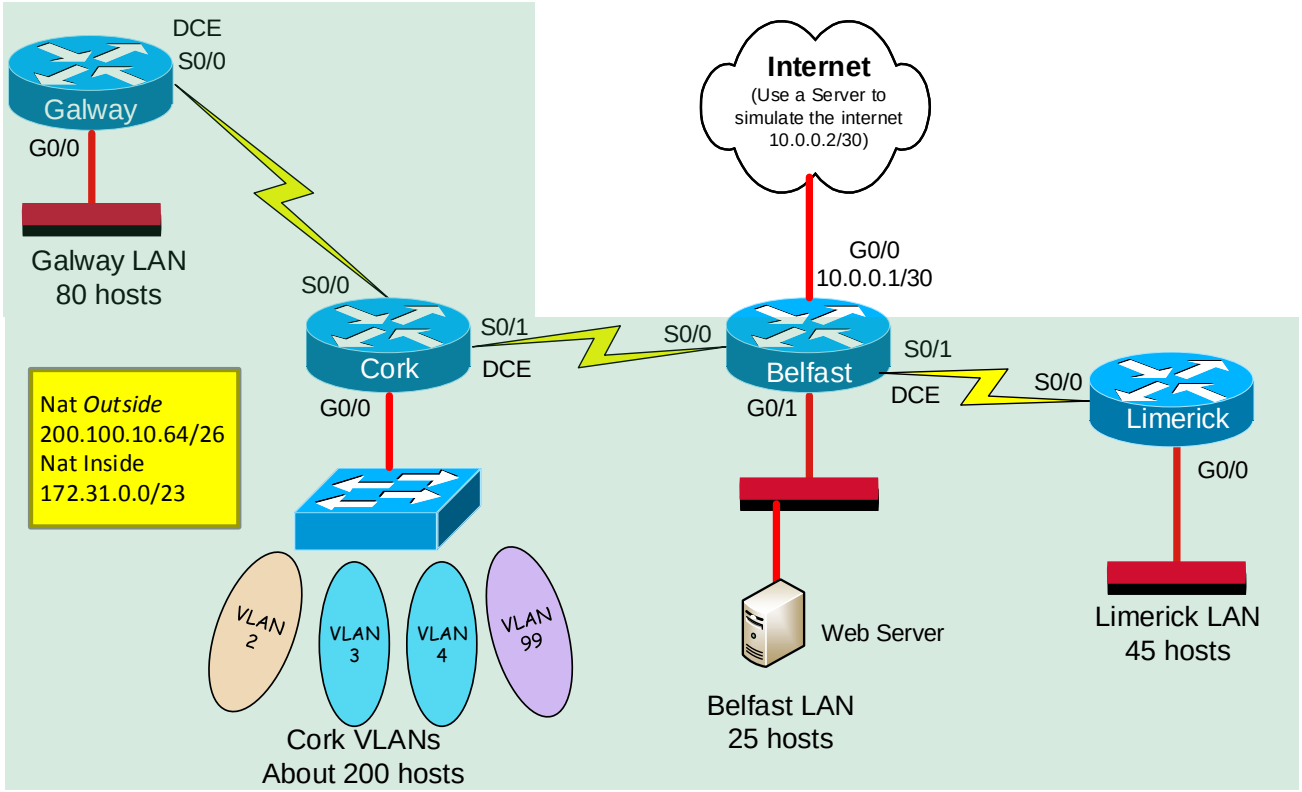


Use the following instructions to complete Phase 2:

- Configure all router with a hostname and required passwords.
- Configure the interfaces on all routers as documented in Phase 1.
- Configure RIP version 2 routing
  - Configure RIP on all Routers (Galway, Cork, Limerick, and Belfast).
  - Configure a Default Route (pointing to the ISP) on Belfast and redistribute the route into the RIP network.
  - Verify the operation of RIP
  - Verify that the Limerick, Belfast, Galway, Limerick 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. This document will serve as deliverable for phase 2

Phase 3: Configure VLANs, Trunks & Port Security

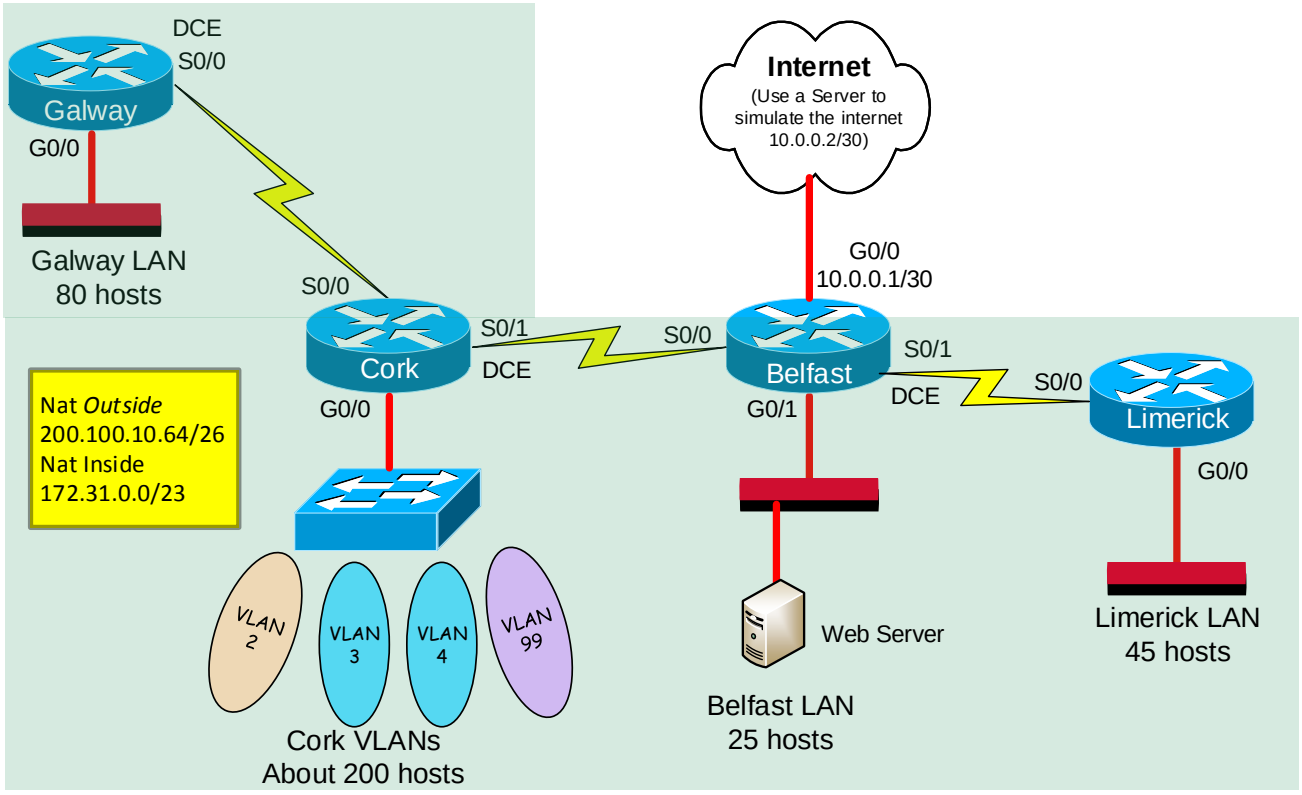


Use the following instructions to complete Phase 3:

1. Apply the basic switch configuration
    - Hostname, all 3 types of passwords (encrypted) and MOTD.
2. Configure the Cork Local Area Network switch as follows:
    - Create and name three Data and one Management VLAN, for a total of 4 VLANs.
        - VLAN 99: Management (Native)
        - VLAN 2: R&D
        - VLAN 3: HR
        - VLAN 4: Production.
    - Assign ports:
        - Ports G0/1-2 to trunk mode (802.1Q)
        - Ports 1-3 to VLAN 99
        - Ports 4-7 to VLAN 2
        - Ports 8-11 to VLAN 3
        - Ports 12-15 to VLAN 4
        - Disable all unused ports
    - **Connect G0/0 on the Cork router to the switch S1, port G0/1**
    - Connect one workstation per VLAN (for testing purposes).
    - Configure ports (1, 2 & 3) in VLAN 99 with port-security, set the maximum MAC addresses to 1 and the violation action to shutdown.

This documentation will serve as the deliverable item for Phase 3

Phase 4: Configuring ACLs



Use the following instructions to complete Phase 4:

1. Configure a **Standard ACL** to filter traffic.

   The ACL should:
   - Deny only the Limerick LAN access to VLAN 2 (R&D), permit all others

2. Configure a **Named Standard ACL** to filter traffic.

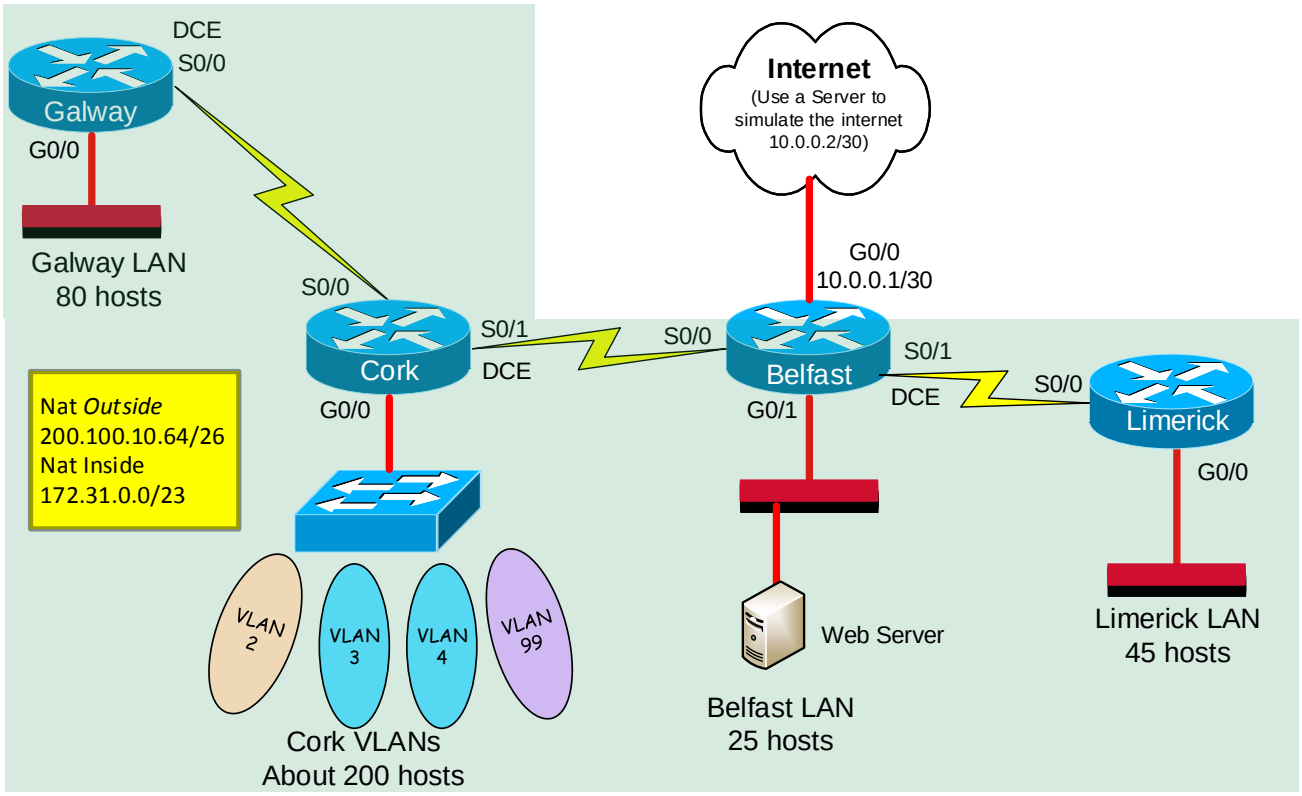
   The ACL should:
   - Permit the HR (VLAN 3) and Galway LAN users to access the Limerick LAN, deny all others.

3. Use an ACL to control VTY access to all routers.

   The ACL should:
   - Allow telnet session to all routers from the Management VLAN (VLAN 99) only; telnet from all other networks should be denied.

Document the ACL configuration in a chart. This chat will serve as the deliverable item in your documentation for Phase 4.

Phase 5: Configuring DHCP



DHCP Services

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, Default Gateway, Domain Name CaseStudy.edu and DNS server (10.0.0.2)

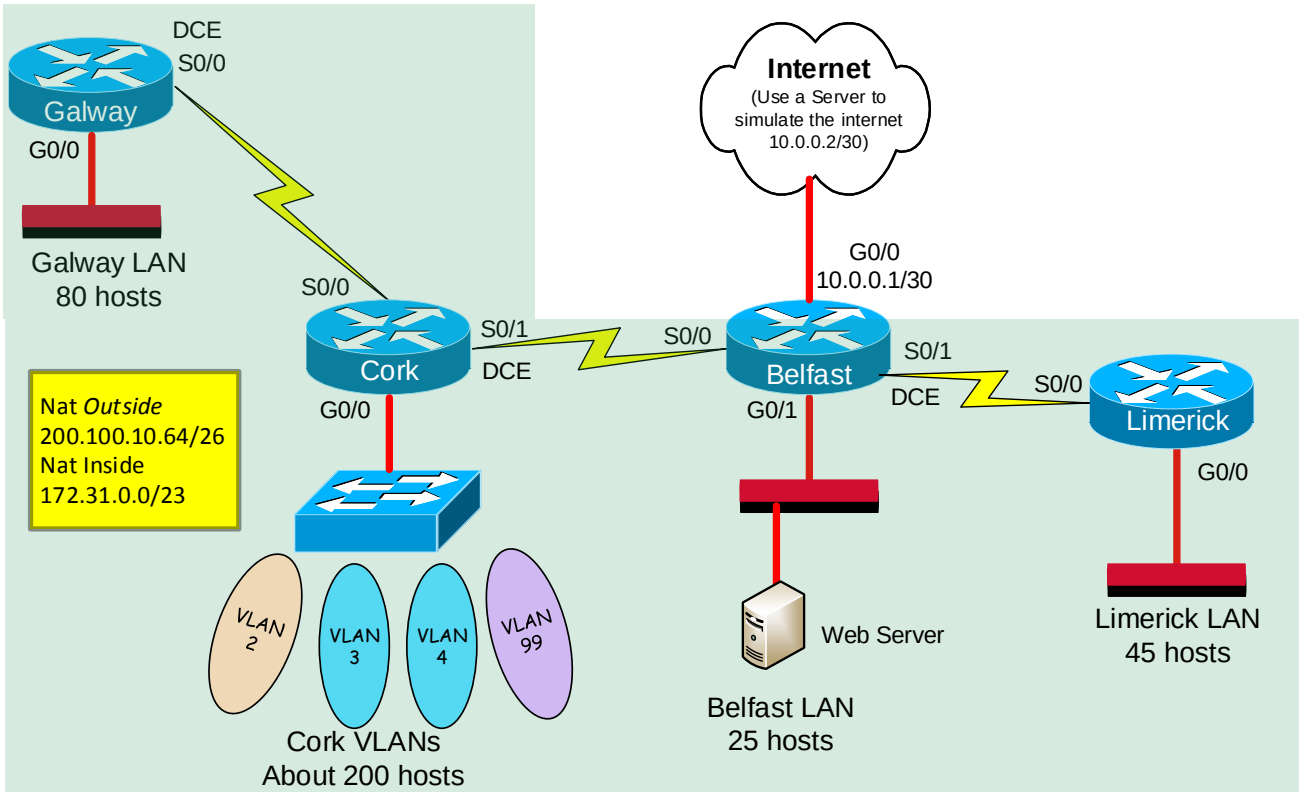
The Galway router will perform DHCP services. Configure the Galway using the DHCP pools documented in Phase 1.

Configure DHCP services on the Galway router as follows:

- G0/0 and sub-interfaces with the first useable address.
- Configure the DHCP pools on the Galway router.
- Exclude the first 10 IP addresses from each pool (to be used for printers and servers)
- Connect a workstation to G0/0 on Galway and VLANs 2-4 on the Cork LAN.
- Configure the workstation to obtain its IP address automatically.
- Verify the operation of DHCP

Recapture and save the Galway router configuration file. Edit the text file, and include comments in your documentation.

Phase 6: NAT



The Belfast router will perform NAT to allow the following:

1. Configure Static NAT to translate the public local IP address 200.10.10.65 to a private local IP address 172.31.X.X (the internal Web Server residing on the Belfast LAN)

2. Configure Dynamic NAT as follows:

    a) Define the NAT pool. The pool consists of public network address 200.100.10.64/26. Exclude first 10 addresses from this pool (to be use for servers, when required).

    b) Define an access control list, which will translate for all internal (172.31.0.0/23) addresses.

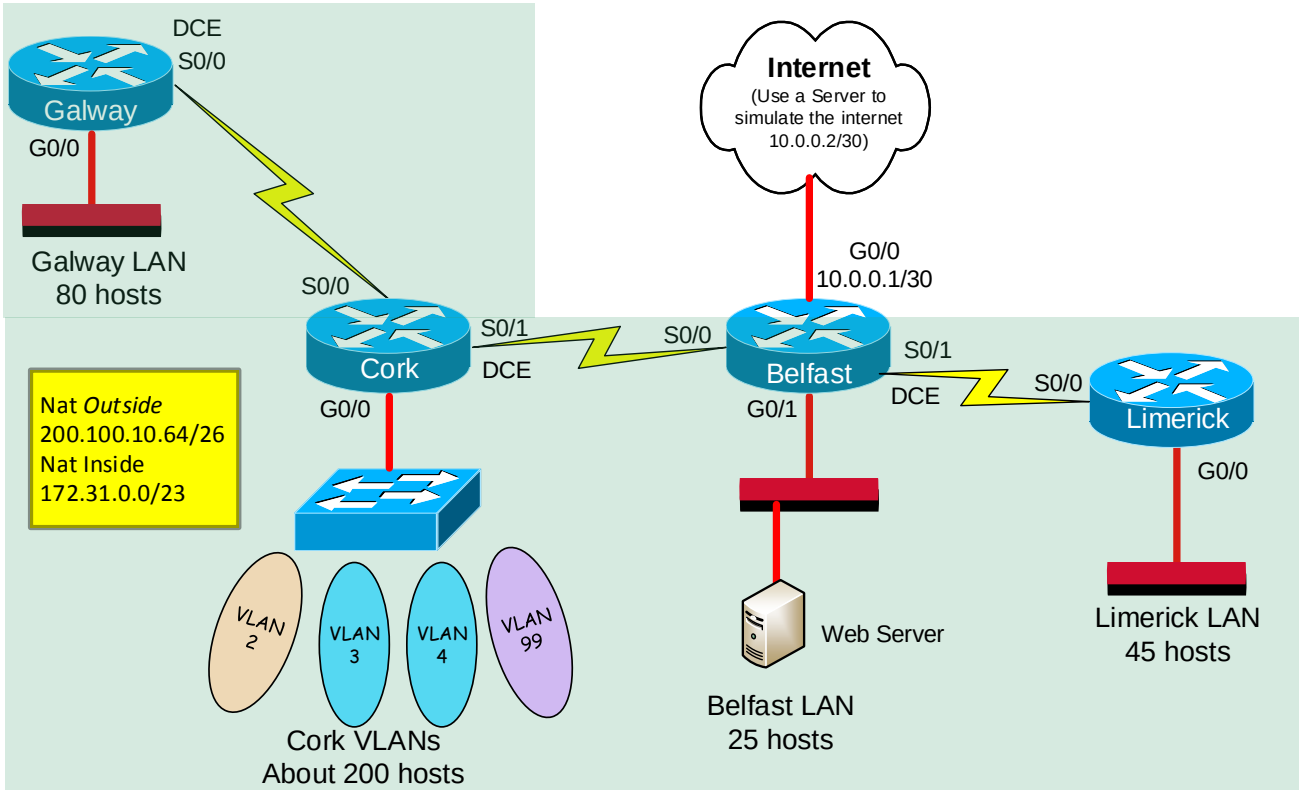
    c) Establish dynamic source translation, specifying the NAT pool and the ACL defined in the previous steps.

    d) Specify the inside and the outside NAT interfaces.

3. Connect a web server to Belfast's G0/0 port to simulate an ISP server. Configure this sever with an IP address, subnet mask and a default gateway
4. Connect a web server to G0/1, configure the server with an IP address, subnet mask and a default gateway.

NAT configurations and translations output will serve as the deliverable item for Phase 6

Phase 7: 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 and the Cork switch. Edit the text files, and include comments at the top of each file documenting the following:

   – Device name and type

   – The date of last modification

   – CCNA4 Case Study – Final Router Configuration

   – The router name that corresponds to each file.

This documentation, along with the completed tables from Phase 1, Phase 2, Phase 3, Phase4, Phase 5, Phase 6, and Phase 7, will serve as the final deliverable item for the case study.

Case Study Deliverables

Once the case study problem has been solved, the network has been successfully designed and the prototype implemented and tested, a final report must be provided to your instructor. This report will include thorough and well-organized documentation of the process. It is highly recommended that all tables be completed using a spreadsheet program such as Microsoft Excel. Cisco Network Designer, Visio or a paint program can be used for the network diagrams. Some of these tables and outputs should be used in your power point presentation

The following items must be included in the final report and presentation:

- Outline
- Summary of the Company and Network Requirements
- Discussion on the implementation of IP address and VLSM
- Discussion on the implementation of Routing
- Discussion on the implementation of VLANs and security on switches
- Discussion on the physical layer design and equipment
- Discussion on testing and verification strategies
- Recommendations for future network upgrades
- Logical Diagram
- Physical Diagram
- Subnetting Table
- IP Addressing Table
- Equipment Table including quantity, make and model (Routers & Switches ONLY)
- Show Commands outputs to verify connectivity:
  show ip route, show vlan, ping, telnet, etc.
- Router Configurations
- Switch Configuration

The documentation should be complete and should contain enough information to allow a third party to properly install, configure and troubleshoot the network without requesting additional information.