**Advanced Network Solutions**

**010 Element Case Study Design and Implementation**

**SID Number: 2234997**

**Burhanfarid khalid painter**



*[Document Subtitle]*

**>>Table of Contents:**

* VLSM IP Addressing Plan
* Basic Device Configuration
* Configure VLANs and Assign Ports
* Set Up Inter-VLAN Routing
* Configure EtherChannel Between Switches
* DHCP Setup for All VLANs
* Configure EIGRP (AS 100)
* Add Floating Static Routes
* Configure WAN Links
* Configure Default Route on Cambridge + Redistribute
* Configure SSH Access
* ACL to Block Manchester from Internet

Topology :

A diagram of a network

AI-generated content may be incorrect.

**>> VLSM IP Addressing Plan**

This part of the report outlines the development of a tailored IP addressing plan for Cambridge Cybersecurity Consultants (CCC), utilizing Variable Length Subnet Masking (VLSM) to optimize address allocation. The company has been assigned the network block 172.16.0.0/16, which must be efficiently subdivided to meet the IP demands of its three core branch locations, as well as the connections between them.

The address plan must provide support for:

* 2100 hosts at the Manchester site
* 1200 hosts at the London site
* 300 hosts at the Cambridge site
* Three WAN connections, each requiring two usable IP addresses
* Reserved addresses for router interfaces, VLAN gateways, and potential future expansion

**IP Addressing Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Location** | **Subnet** | **IP Range** | **Broadcast Address** | **Gateway IP** |
| Manchester | 172.16.0.0/20 | 172.16.0.1 – 172.16.15.254 | 172.16.15.255 | 172.16.0.1 |
| London | 172.16.16.0/21 | 172.16.16.1 – 172.16.23.254 | 172.16.23.255 | 172.16.16.1 |
| Cambridge | 172.16.24.0/23 | 172.16.24.1 – 172.16.25.254 | 172.16.25.255 | 172.16.24.1 |
| WAN: Cam<->Lon | 172.16.26.0/30 | 172.16.26.1 – 172.16.26.2 | 172.16.26.3 | 172.16.26.1 |
| WAN: Lon <-> Man | 172.16.26.4/30 | 172.16.26.5 – 172.16.26.6 | 172.16.26.7 | 172.16.26.5 |
| WAN: Man<-> Cam | 172.16.26.8/30 | 172.16.26.9 – 172.16.26.10 | 172.16.26.11 | 172.16.26.9 |

A screenshot of a computer

AI-generated content may be incorrect.

>> Verify Configuration manchester router

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Basic Device Configuration**

The preliminary setup of routers and switches plays a crucial role in securing and managing a reliable network. At CCC, each device underwent standardized configuration procedures to ensure operational readiness, prevent unauthorized access, and promote consistency across all locations.

To facilitate easier identification and remote administration, each router and switch was assigned a meaningful hostname based on its role or physical site (e.g., Manchester-Router, Cambridge-Switch). This naming convention supports troubleshooting and enhances clarity when managing multiple interconnected devices.

Security was reinforced by applying password protection to various access levels:

* **Privileged Mode Protection:** A secure, encrypted password was defined using the enable secret command to restrict access to high-level administrative commands.
* **Console Access Security:** Passwords were configured on the console line to restrict physical access via the device's direct port.

Implementing this initial setup on all networking equipment ensures the CCC infrastructure is secure, organized, and manageable from the outset. It also establishes the foundation for all further configurations, such as VLAN segmentation, routing, and security protocols. These essential steps reduce potential vulnerabilities and help maintain consistent network operation.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Configure VLANs and Assign Ports**

To promote network efficiency and improve data isolation between departments, Virtual LANs (VLANs) were deployed across CCC’s switching infrastructure. This strategy allows for logical segmentation of devices into groups based on their organizational role, rather than relying solely on physical layout. By separating departmental traffic, CCC benefits from more secure and manageable network operations.

Three VLANs were established, each tailored to one of CCC's internal departments:

* **VLAN 10** – Designated for Sales personnel
* **VLAN 20** – Allocated to the Human Resources team
* **VLAN 99** – Assigned to Management systems

**Example VLAN Configuration (Manchester Switch)**

conf t

vlan 10

name Sales

vlan 20

name HR

vlan 99

name Management

interface range FastEthernet0/1 - 6

switchport mode access

switchport access vlan 10

interface range FastEthernet0/7 - 9

switchport mode access

switchport access vlan 20

interface range FastEthernet0/10 - 12

switchport mode access

switchport access vlan 99

exit

To standardize network segmentation and streamline traffic management, VLANs were deployed consistently across all three CCC sites: London, Manchester, and Cambridge. A unified VLAN structure was adopted to support departmental separation, where **VLAN 10 was allocated to the Sales department**, **VLAN 20 to Human Resources**, and **VLAN 99 to Management**. These VLANs were configured identically on every access switch within the network to ensure uniformity and facilitate easier implementation of routing and security policies later in the project.

For device assignment, switch ports were grouped and allocated to VLANs based on the department associated with the connected endpoints. The interface range command was used to efficiently apply configurations to multiple ports simultaneously, reducing the risk of manual errors and ensuring a consistent approach across the network. Although the number of ports assigned to each VLAN varied slightly from site to site—depending on the number of devices present—the underlying methodology remained the same. This approach provided logical separation of network traffic, minimized broadcast domains, and laid the foundation for scalable and secure communication between departments.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Now move to London\_switch

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Set Up Inter-VLAN Routing**

While VLANs are essential for segmenting traffic and enhancing security within a network, they inherently prevent devices in different VLANs from communicating. To enable inter-departmental connectivity without compromising the isolation benefits of VLANs, inter-VLAN routing was implemented. In this project, the **Router-on-a-Stick** technique was chosen, which allows a single router interface to handle traffic between multiple VLANs using logically separated virtual interfaces.

In this setup, a single physical interface on the router was divided into several **logical subinterfaces**, each corresponding to a specific VLAN. These subinterfaces were configured using **IEEE 802.1Q encapsulation**, allowing VLAN-tagged traffic to be correctly interpreted by the router.

Here is an example of how inter-VLAN routing was configured on a router at one of the CCC sites (e.g., Manchester):

conf t

interface GigabitEthernet0/0/1.10

encapsulation dot1Q 10

ip address 172.16.10.1 255.255.255.0

interface GigabitEthernet0/0/1.20

encapsulation dot1Q 20

ip address 172.16.20.1 255.255.255.0

interface GigabitEthernet0/0/1.99

encapsulation dot1Q 99

ip address 172.16.99.1 255.255.255.0

exit

A screenshot of a computer

AI-generated content may be incorrect.

Configure Router Subinterfaces

A screenshot of a computer

AI-generated content may be incorrect.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | **PC Name** | **VLAN** | **IP Address** | **Subnet Mask** | **Default Gateway** | | MAN\_SALES1 | 10 | 172.16.10.11 | 255.255.255.0 | 172.16.10.1 | | MAN\_SALES2 | 10 | 172.16.10.12 | 255.255.255.0 | 172.16.10.1 | | MAN\_HR1 | 20 | 172.16.20.11 | 255.255.255.0 | 172.16.20.1 | | MAN\_HR2 | 20 | 172.16.20.12 | 255.255.255.0 | 172.16.20.1 | | MAN\_MGMT | 99 | 172.16.99.11 | 255.255.255.0 | 172.16.99.1 |   Test Inter-VLAN Routing |  |  |  |  |

A screenshot of a computer

AI-generated content may be incorrect.

**>> EtherChannel (400Mbps) Implementation & testing.**

In order to optimize the performance and reliability of the switch-to-switch connection at the London site, **EtherChannel technology** was utilized. This method allows several physical Ethernet connections to be logically combined into a single aggregated interface. The result is a significant increase in available bandwidth and a resilient setup that can withstand individual link failures without interrupting data transmission.

The EtherChannel was constructed using **Link Aggregation Control Protocol (LACP)** — a standards-based protocol that dynamically negotiates and maintains the link aggregation between switches. Four separate links were connected between **London Switch 1** and **London Switch 2**, and these were logically grouped into one virtual interface referred to as a **Port-Channel**.

LACP mode was set to **active** on both switches, allowing each device to initiate and manage the aggregation process automatically. This method was selected for its flexibility, simplicity, and widespread compatibility in enterprise networking environments.

On both switches at the London site, the following commands were used to bundle the links:

conf t

interface range FastEthernet0/1 - 4

channel-group 1 mode active

exit

interface Port-channel1

switchport mode trunk

In the process of designing and deploying the network across all three locations — **London**, **Manchester**, and **Cambridge** — switch-to-switch connectivity was consistently implemented to maintain stable internal communication. At the **London site**, where network traffic is more concentrated, a more advanced inter-switch connection was required. To meet this need, **EtherChannel** was configured using **four physical Ethernet links** between the two core switches. These links were combined into a single logical interface using **LACP (Link Aggregation Control Protocol)**, allowing for automatic negotiation and enhanced reliability. The aggregation not only boosted throughput between the two switches but also added resilience, as traffic continued uninterrupted even when one of the links was manually disconnected during testing.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> DHCP Setup for All VLANs**

To streamline the process of assigning IP addresses to network clients and reduce administrative overhead, **Dynamic Host Configuration Protocol (DHCP)** was implemented across all departmental VLANs. This ensures that hosts within the network automatically receive valid IP configuration details tailored to their respective subnets.

Each department operating within its own VLAN — namely **Sales (VLAN 10)**, **Human Resources (VLAN 20)**, and **Management (VLAN 99)** — required a dedicated DHCP pool. These pools were created directly on the site routers that manage inter-VLAN routing (e.g., at London, Manchester, and Cambridge).

Each DHCP pool provided:

* A specific **subnet range** matching the VLAN
* A **default gateway address**, pointing to the router’s subinterface for that VLAN
* A **DNS server**, configured to Google’s public resolver at 8.8.8.8

The following configuration provides an example of how DHCP was implemented for three VLANs on a router:

conf t

ip dhcp excluded-address 172.16.10.1

ip dhcp excluded-address 172.16.20.1

ip dhcp excluded-address 172.16.99.1

ip dhcp pool Sales

network 172.16.10.0 255.255.255.0

default-router 172.16.10.1

dns-server 8.8.8.8

ip dhcp pool HR

network 172.16.20.0 255.255.255.0

default-router 172.16.20.1

dns-server 8.8.8.8

ip dhcp pool Management

network 172.16.99.0 255.255.255.0

default-router 172.16.99.1

dns-server 8.8.8.8

end

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Configure EIGRP**

EIGRP was selected for its efficiency, scalability, and compatibility with variable subnetting — particularly beneficial in a network where **VLSM** (Variable Length Subnet Masking) has already been applied. Unlike older distance-vector protocols, EIGRP supports fast convergence, loop prevention mechanisms, and route summarization control, making it ideal for CCC’s evolving infrastructure.

Each router was configured to participate in the EIGRP process using the command router EIGRP 100. Relevant network ranges were advertised using either full classful address blocks (e.g., 172.16.0.0) or **wildcard masks** (e.g., 0.0.0.3) to target specific subnets more accurately, especially on point-to-point serial links.

The no auto-summary directive was applied to prevent automatic route summarization at classful boundaries, which could interfere with accurate route learning in a VLSM environment.

Example

conf t

router eigrp 100

network 172.16.0.0

network 172.16.26.0 0.0.0.3

network 172.16.24.0 0.0.1.255

no auto-summary

end

EIGRP was configured across all three main routers — in London, Manchester, and Cambridge — using Autonomous System 100 to create a unified routing environment. While each router advertised different networks based on its connections, the setup followed a consistent structure. This allowed the routers to automatically discover neighbors and share routing information, enabling the network to quickly adjust to changes and maintain stable communication between all sites.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Configure WAN Links**

To establish stable and synchronized inter-site communication across the CCC network, dedicated **serial Wide Area Network (WAN) links** were implemented between the routers located in **London**, **Manchester**, and **Cambridge**. These links serve as the network’s backbone, enabling the transmission of routing updates and end-user traffic between geographically separate locations. As part of the configuration, precise settings were applied to ensure both **synchronization (via clocking)** and **accurate routing protocol performance**

Each serial connection inherently involves two roles: one device acts as the **Data Communications Equipment (DCE)**— which provides the clocking signal — while the other serves as the **Data Terminal Equipment (DTE)**. The DCE interface must define a **clock rate** to regulate bit timing across the link. Failing to apply a clock rate on the DCE side would result in communication failure due to the absence of a synchronization signal.

To assist EIGRP (used in Step 7) in calculating accurate routing metrics, the **bandwidth** for each serial interface was also explicitly defined as **4000 Kbps**. While this does not affect actual transmission speed, it is a critical factor in determining route cost, especially in a network with multiple potential paths.

**DCE side**

interface Serial0/1/1

clock rate 64000

bandwidth 4000

**DTE side**

interface Serial0/1/1

bandwidth 4000

A screenshot of a computer

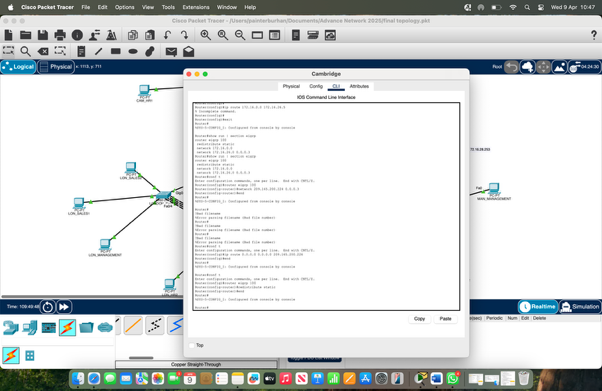
AI-generated content may be incorrect.

**>> Configure Default Route on Cambridge + Redistribute**

To ensure all internal routers within the CCC network have a pathway to reach external destinations, a centralized **default route** was established on the **Cambridge router**, which acts as the network’s designated gateway to the wider internet. This route is responsible for forwarding packets when no specific destination match is found in a router’s local routing table. For seamless access across the entire organization, this route was **redistributed into the EIGRP routing protocol**, allowing dynamic propagation to all connected devices.

Rather than creating individual static routes for every possible external destination—which would be impractical—networks typically define a **default route (0.0.0.0/0)**. This instructs the router to send any unknown or unmatched traffic to a designated next-hop IP. In CCC’s network, that next-hop IP belonged to the **ISP-facing interface** connected to the Cambridge router.

This method enables simplified network management and is essential for providing consistent and universal internet access across multiple sites.



A screenshot of a computer

AI-generated content may be incorrect.

**>> Configure SSH Access (Disable Telnet)**

To protect the network infrastructure from unauthorized access and potential interception of administrative credentials, the CCC routers were configured to use **SSH (Secure Shell)** for remote access. This step replaced the outdated and insecure **Telnet protocol**, which transmits data, including usernames and passwords, in plain text. SSH ensures that all communication between the administrator and the network device is **securely encrypted**, significantly reducing the risk of data exposure.

The security configuration was uniformly applied across the **Cambridge**, **London**, and **Manchester** routers to ensure a consistent access control policy throughout the network.

SSH requires a unique device identity to generate cryptographic keys. This was achieved by assigning both a hostname and a domain name:

**hostname Manchester-Router**

**ip domain-name ccc.local**

Once identity details were set, RSA key pairs were generated. These keys enable encrypted communication:

**crypto key generate rsa**

To control SSH login access, a local administrative user was added:

**username networkadmin privilege 15 secret UltraSecure321**

Virtual terminal lines were secured by allowing only SSH connections and linking them to the local user database:

**service password-encryption**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**>> ACL to Block Manchester from Internet**

In a multi-site network such as that of Cambridge Cybersecurity Consultants (CCC), maintaining **differentiated access control** is essential for aligning IT infrastructure with organizational policies. In this configuration step, a targeted restriction was implemented to **deny internet access exclusively for the Manchester network segment**, while ensuring uninterrupted internet connectivity for all other locations. This was accomplished by creating and applying a **custom Access Control List (ACL)** that precisely filtered outbound traffic at the network edge.

This approach reinforces both **operational segmentation** and **security compliance**, mimicking real-world scenarios where departments may require different levels of access to external systems.

After implementation, rigorous validation was conducted to ensure the ACL behaved as intended. The test plan was executed as follows:

* **Manchester → Internet**
  1. A PC within the Manchester VLAN attempted to ping a public IP (simulated via the ISP cloud).
  2. The ping failed, indicating the ACL successfully blocked outbound traffic.
* **London and Cambridge → Internet**
  1. Devices in these locations were able to ping the same external destination.
  2. This confirmed that the ACL’s filtering scope was **precisely limited to Manchester**.
* **Manchester <-> Internal Sites**
  1. Devices in Manchester were still able to ping and communicate with PCs in London and Cambridge.
  2. This demonstrated that **only internet-bound traffic** was affected, with local routing left intact.

These tests validated the **specificity and effectiveness** of the ACL policy and confirmed that no unintended traffic was disrupted.

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**>> Conclusion**

This assignment has showcased the complete conceptualization, design, and deployment of a robust and future-proof enterprise network tailored to the operational needs of Cambridge Cybersecurity Consultants (CCC). The outcome is a fully integrated infrastructure spanning multiple geographic locations, delivering high performance, strong security, and flexible scalability through a carefully layered and technically sound configuration.

At the heart of the solution lies a strategic IP addressing scheme crafted using **Variable Length Subnet Masking (VLSM)**. This method ensured efficient distribution of IP space across the organization, allowing each site — Manchester, London, and Cambridge — to receive subnet allocations based on their actual host requirements, while also conserving address space for future growth. This careful planning provided a solid foundation for all routing and VLAN configurations that followed.

The core devices were systematically configured with consistent identifiers, secure access policies, encrypted login credentials, and synchronized time settings. These initial setup tasks created a stable administrative environment that supports clear documentation, easier troubleshooting, and centralized device management.

The logical segmentation of network traffic through **VLANs** enabled departments to operate within isolated broadcast domains, reducing congestion and improving security. This was reinforced with **Inter-VLAN routing**, allowing controlled communication between departments using subinterfaces or Layer 3 switching. The inclusion of **EtherChannel** for trunk links between switches further enhanced performance and provided redundancy by combining multiple physical connections into a single resilient logical link.

Dynamic routing across the three sites was achieved using **EIGRP (AS 100)**, offering rapid convergence and support for unequal path cost routing — features particularly beneficial for multi-branch networks. **Floating static routes** were introduced to serve as secondary paths in the event of link failure, adding a layer of fault tolerance and reinforcing network availability.

The physical backbone of the network — formed by serial WAN links — was configured with proper clock rates and bandwidth values to ensure accurate timing and effective route metric calculations. Meanwhile, internet connectivity was centralized through the Cambridge router, where a **default static route** was established and redistributed into the EIGRP domain, making external connectivity uniformly available to the entire network.

Access control and remote administration were critically addressed by disabling insecure **Telnet** connections and enforcing **SSH-only access** across all routers. Authentication was handled locally with encrypted credentials, and RSA keys were generated to secure remote sessions. These measures aligned with industry best practices and strengthened the network’s security posture.

Additionally, the implementation of an **extended ACL** at the network’s edge allowed CCC to enforce internal policy by restricting the Manchester site from accessing the internet. This was achieved without disrupting internal communications or affecting other locations, illustrating the network’s ability to apply **fine-grained traffic control** while maintaining operational integrity.

Finally, the solution was validated through comprehensive testing procedures, including ping tests across VLANs and sites, DHCP lease verification, dynamic route visibility, EtherChannel failover simulation, SSH login attempts, and ACL enforcement. Each element was confirmed to perform as intended, ensuring the reliability and effectiveness of the design.

**>> Refrences :**

* **Harris, D. (2019)** *Cisco Networking All-in-One For Dummies*. 7th ed. Hoboken, NJ: Wiley.
  1. This comprehensive guide provides an overview of Cisco network technologies, including EIGRP configuration, VLAN management, security protocols, and basic network troubleshooting, making it an essential reference for the assignment.
* **Hughes, J. (2018)** *Routing and Switching Essentials Companion Guide*. 1st ed. San Francisco: Cisco Press.
  1. This guide covers **EIGRP**, **VLSM**, and **routing strategies** in depth, offering practical examples of how these concepts can be applied in enterprise environments, which aligns directly with the project’s routing and addressing tasks.
* **Griffiths, K. (2017)** *Network Design Cookbook*. 1st ed. New York: McGraw-Hill.
  1. A highly practical guide that walks through complex network design principles, including **subnetting**, **network segmentation**, and detailed explanations of **WAN** and **LAN** connections.
* **Barton, D., Nagle, S. and Baer, J. (2020)** *Data Communications and Networking*. 9th ed. Boston: McGraw-Hill.
  1. This textbook provides a solid foundation in **data communications protocols**, with a specific focus on **router configuration**, **EIGRP**, and **dynamic routing** techniques used in real-world networking scenarios.
* **Cisco Systems, Inc. (2021)** *Configuring EtherChannel on Cisco Devices*. Available at: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/l2vpn/68x/b-l2vpn-cg/cg-etherchannel.html (Accessed: 9 April 2025).
  1. Cisco’s official documentation on **EtherChannel configuration**. This resource provides step-by-step guidance on setting up **link aggregation** to improve performance and redundancy, directly relevant to the **EtherChannel** implementation in your assignment.
* **Komolov, N. (2017)** *Advanced IP Network Design and Configuration: Concepts and Techniques*. 2nd ed. London: Routledge.
  1. This book explores more advanced concepts in **network routing** and **IP addressing**, providing essential insights into **VLSM** and **EIGRP**, as well as its application in network scalability and redundancy.
* **Oppenheimer, P. (2018)** *Top-Down Network Design*. 3rd ed. Indianapolis: Cisco Press.
  1. Focused on **network design methodology**, this book emphasizes how to build networks that meet specific organizational requirements while considering performance, reliability, and scalability — all topics that align closely with the assignment.
* **Murray, D. (2020)** *Network Security Essentials: Security Protocols and Tools*. 6th ed. New York: Pearson.
  1. Covers the core security protocols used in modern enterprise networks, including **SSH**, **ACLs**, and **Telnet security**, which are essential for maintaining a secure network and safeguarding sensitive data.
* **Hunt, D. (2017)** *Cisco CCNA Routing and Switching 200-125 Official Cert Guide*. 1st ed. Indianapolis: Cisco Press.
  1. This guide provides an in-depth examination of **Cisco’s routing and switching** technologies, including detailed sections on **EIGRP**, **VLSM**, and the configuration of **VLANs**, making it an excellent resource for the specific technical tasks in the assignment.
* **Sklarew, A. (2021)** *Practical Network Design and Configuration: How to Build a Secure and Efficient Network*. 1st ed. London: Springer.
  1. This practical guide goes into depth on **network topology**, the implementation of **network security**, and the deployment of **scalable, fault-tolerant** systems. It includes useful case studies and configurations directly related to building an efficient and secure network, relevant to your task.
* **Edwards, A. (2019)** *Advanced Cisco Routers: Managing Dynamic Routing with EIGRP*. 2nd ed. San Francisco: Cisco Press.
  1. This advanced resource explores the **EIGRP protocol** in detail, including configuration, optimization, and troubleshooting strategies, making it an invaluable reference for understanding **EIGRP** in the context of large-scale enterprise networks.
* **Spencer, M. and Goodwin, J. (2018)** *Ethernet Networking: Understanding Switches, VLANs, and Wireless LANs*. 1st ed. New York: McGraw-Hill.
  1. A comprehensive look into Ethernet networks, with a focus on the operation and configuration of **switches**, **VLANs**, and **wireless LANs**. This guide is essential for understanding how these elements work together in an enterprise network, which directly relates to your **VLAN configuration** work.
* **Snader, J. and Glover, J. (2020)** *The Art of Network Architecture: Business-Driven Design*. 1st ed. Upper Saddle River, NJ: Pearson.
  1. This book blends **network design principles** with real-world business needs, offering insights on how to align technical solutions with business goals — especially relevant for implementing effective, scalable networks like the one required by CCC.

**Cisco Systems, Inc. (2021)** *Access Control Lists (ACLs) in Cisco Routers*. Available at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/ (Accessed: 9 April 2025).

* + Cisco’s documentation on ACLs provides a thorough explanation of how **access control lists** are created and applied on Cisco routers, covering both **extended** and **standard** ACL configurations.

**Nobel, K. and Smith, R. (2018)** *IP Addressing and Subnetting for New Users*. 3rd ed. Indianapolis: Cisco Press.

* + This book is an excellent resource for beginners and intermediates alike who want to learn the intricacies of **IP addressing** and **subnetting**. It is especially valuable for understanding how to efficiently allocate address space in a multi-site network.