CP1402/CP1802 Assignment

Networking Case Study

Introduction

This case study has been divided into four components.

You are to design a network, research and source appropriate devices justifying choices (feasibility, efficiency, etc.), subnet the network using VLSM, and assign IP addresses to the appropriate devices. You will also be required to implement security by applying access control lists to filter traffic.

Note: This is ***not*** a group project. Each student must individually complete all parts of their submission.

Students ***must*** start with a ***new document*** and they must not have another person's file in their possession at any time. Students may discuss the task with each other, but each student must write their assignment independently and not show their work to other students.

Deliverables

1. A single **Word document** (.docx) – containing all parts

Assignment breakdown

Scenario

A major Australian data analytics company has asked you to assess and redesign their network. They are opening new branches in Brisbane and Adelaide, which will require new equipment. They have existing contracts and hardware to maintain fibre optic leased line WAN links between sites.

PART 1 - Network specifications and diagram

PART 2 - Subnet the network using VLSM, and assign IP addresses to the appropriate devices

PART 3 - Research and source appropriate devices justifying choices (feasibility, efficiency, etc.) with a Weighted Scoring Model (WSM) and documented report

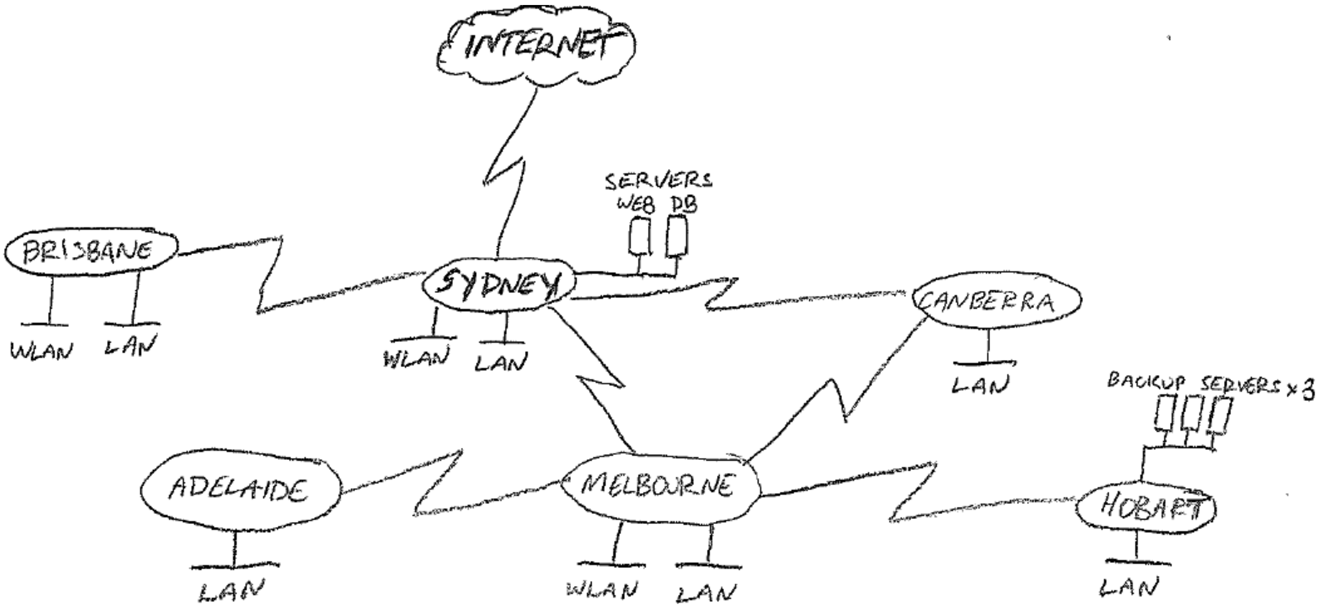
PART 4 - Security by applying Access Control Lists (ACLs) to filter traffic

PART 1 - Network specifications and diagram

Network Specifications

You have been given a rough sketch of the network topology below. You are to draw the network using Visio, subnet the network (see case study part 2), and assign port numbers and IP addresses to ports.

Network Structure



Hardware

- Only include one switch in you diagram for each LAN and one wireless access point for each WLAN (even if more are required)
- The Internet router port address is 104.200.16.26/30
- The Sydney router is connected to the Internet, and provides access to the ***public backbone containing a web server and a database server.***

PART 2 - Subnet the network using VLSM, and assign IP addresses to the appropriate devices.

Each location has the following number of hosts

Sydney, Melbourne, and Brisbane each include a wireless LAN for clients to use.

Location	Workstations	WLAN addresses
Sydney	910	14
Melbourne	200	6
Brisbane	40	6
Canberra	120	
Adelaide	70	
Hobart	20	

Subnetting

Use VLSM to subnet the network topology using a public class B network. You are to use the table format below to provide the subnet details.

Table 1. Subnets (including WAN subnets)

Spreadsheet Columns: Subnet name, subnet address, subnet mask (in slash format), first useable address, last useable address, broadcast address, static address range and DHCP address range (all addresses to be in dotted decimal notation)

Table 2. Router Interfaces

Spreadsheet Columns: Location, interface, IP address, subnet mask (in slash format)

Table 3. Servers

Spreadsheet Columns: Location, server name, IP address, subnet mask (in slash format)

Additional requirements:

- Choose one public B class network address for the entire network and subnet this block of addresses to optimise spare addresses for future expansion.
- Place the WAN subnets in the blocks directly following the LAN address space.
- Add 100% to each subnet to allow for growth in the number of hosts specified for each LAN (i.e. workstations × 2). Do not allow for any growth in the number of servers or size of WLANs
- DHCP will to be used for IP address allocation for hosts in each subnet and these ranges are to be allocated for each LAN.
- Static IP addresses are to be allocated where appropriate.
- The ISP has given us an IP address of 104.200.16.26/30 for our Internet connection at Sydney.
- **You must also provide your working to show how you calculated the subnet sizes and determined the appropriate addresses and ranges. Do not include working in your tables, present it after the tables.**

PART 3 - Research and source appropriate devices justifying choices (feasibility, efficiency, etc.)

You are to research and submit a project procurement plan for the Adelaide and Brisbane networks. The devices you must include are routers, switches, and wireless access points. Make sure the devices you select can handle the number of workstations required at each site, and provide a good quality of service to wired and wireless users.

Your project plan and final recommendations should be based on a Weighted Decision Matrix (similar to the WDM you did in the Procurement Practical). You are to compare five (5) devices from each category and to base the decision on reasonable and well-justified attributes.

The budget for all procurement is $10,000. You may exceed this if you can justify it well.

Your project plan is to contain the following components:

Executive summary

- Briefly describe the goals of the procurement plan

Weighted Decision Matrix - hardware resource requirements analysis

- Include a written justification for priorities and attributes given in the matrix
- Create your WDMs in Excel and copy and paste them into your Word doc

Budget

- Create a well-presented table of the prices of all devices and the total cost
- Include hardware only, not labour

PART 4- Security by applying access control lists to filter traffic

Write ACL tables, in the format taught in the lectures, to address the following security requirements.

Requirements for all ACLs

- ACLs are to be placed in the optimal position to minimise bandwidth unless the location of the ACL is specified
- You are **not** to rely on the implicit deny any any.
- No ACL is required on a port where all traffic is permitted.
- Create one ACL table per router.

a) Access to the Internet and public backbone:

Apply these ACL/s to serial 0/0 on the Sydney Router

1. ***External*** hosts outside the organisation (on the Internet) must only be able to access the Sydney Web server on the public backbone using HTTP and HTTPS.
2. No other ***external*** access is permitted into the organisation from the Internet.
3. ***Internal*** hosts must only be able to communicate out to the Internet using HTTP and HTTPS (Hint: established connections must be allowed to communicate back into the private network).

b) Sydney and Melbourne

4. The Sydney and Melbourne LANs should have unrestricted access to the Internet, and to the Sydney servers.
5. The Sydney and Melbourne WLANs should have HTTP and HTTPS access to the Internet, and to the Sydney Web server, but no access to anywhere else on the corporate network.
6. The Sydney Web server should have unrestricted communication via HTTP and HTTPS, and be able to respond to ping requests from internal hosts.
7. The Sydney Database server should be able to respond to established connections via port 1433.

c) Brisbane, Adelaide, and Canberra

8. The Brisbane, Adelaide, and Canberra WANs should have HTTP and HTTPS access to the Internet and to the Sydney Web server
9. The Brisbane WLAN should have HTTP and HTTPS access to the Internet, and to the Sydney Web server, but no access to anywhere else on the corporate network.

d) Hobart

10. The Hobart servers should be able to initiate connections anywhere within the corporate network without restriction.
11. Only traffic from established connections and from the Hobart LAN is permitted to reach the Hobart servers. All other access should be blocked.
12. The Hobart LAN should have unrestricted access to the Internet, the Sydney servers, and the Hobart servers.