|  |  |
| --- | --- |
| **ARU Cambridge Campus**  ATTEMPT: 1 |  |
| **ANGLIA RUSKIN UNIVERSITY** | |
| Assignment Coversheet | |
| **STUDENT DETAILS** | |
| Student Number: | **2179610** |
| **FACULTY** | |
| **Faculty of Science and Engineering** | |
| **ASSIGNMENT DETAILS** | |
| Module ref | **2023 MOD003262 TRI2 F01CAM** |
| Module Title | **Network Routing** |
| Module Element | **010 - Coursework (2000 words)[Part B]** |
| Submission date (by 2pm) | **EXT: 26 May 2024** |
| **WORD COUNT** | 1962 |

**Table of Contents**

**Executive Summary:**

* Overview of network proposal and challenges addressed
* Figure 1: Existing Network
* Table 1: Host per Site Breakdown

**Routing**

* IP Addressing
* Class A Network Addressing
* Subnetting and Network Segmentation
* Table 2: Proposed Subnets in the Network
* Table 3: Proposed IP Addresses for the 4 Sites
* 1.2………………………………….. Routing Protocol
* OSPF Advantages and Implementation
* Figure 2: Routing Table of London Router
* 1.2.1………………………………. Sample Router Running Configurations
* London Router Example
* Switching

**2.0 Switching Overview**

* Introduction and Benefits of Using Switches
* Hierarchical Model of Network Switch Installation
* 2.1……… …………………………………Advantages of VLANs
* VLAN Configuration and Management
* VLAN Implementation Strategy
* 2.2………………………………………… VLANs Implementation
* Detailed VLAN Configuration Across Sites
* Figure 3: VLAN Propagation by VTP
* 2.3…………………………………………... Sample Configurations
* Leicester Core Switch Configuration
* Access Control

**3.0 Access List and Controls**

* Role and Implementation of Access Lists
* Extended Access Lists
* Specific Access Control Measures

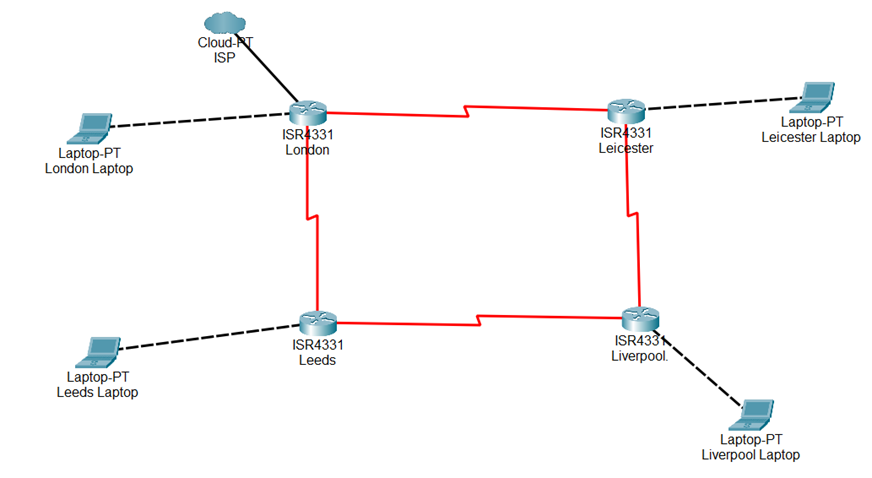
**Conclusion**

* Summary of Network Implementation and Benefits
* Figure 4: Logical Diagram of Implemented Network

**EXECUTIVE SUMMARY**

This report details the proposal for a new network for our company **FinTec** Inc and this design is aimed at addressing the various challenges the company is having with the existing network namely, **efficiency, security, resilience and capacity to expand the network.** Figure 1 depicts the existing network.

**Figure 1**



The essence of this report is to build on this network to address the current challenges focusing on three main areas namely:

1. Routing
2. Switching
3. Access Control

This consideration will cut across all Sites of the FinTech Inc offices in London, Leeds, Liverpool and Leicester with the table 1 depicting the host per site.

**Table 1**

|  |  |
| --- | --- |
| **Branch Name** | **Number of Hosts** |
| **London** | 1500 Hosts |
| **Leeds** | 500 Hosts |
| **Liverpool** | 900 Hosts |
| **Leicester** | 1200 Hosts |

1. **ROUTING**

**1.1 IP ADDRESSING**

In the consulting industry, it is generally accepted that, no matter how small the network, you should choose a Class A network address when putting up a corporate network since it offers you the greatest flexibility and growth choices.

(Todd lammle, 2016, p. 178). This rule is applicable to one of the challenges the company is trying to address, which is to ensure a network that has the capacity to grow.

A further subnetting a class A IP address helps to break the big network to smaller units which will ensure the company achieve the following which are the major limitations of the current design:

* Improve network performance.
* Ensure security.
* Aid organization and management.

The following details the Subnets that will be used for all 4 sites.

Network to be sub netted is 10.0.0.0/20 which can accommodate maximum of 4094 host and bear in mind the most needed host per site is 500 host as shown in table 1.

/20 is 255.255.240.0 gives us 12 bits of subnetting and leaves us 12 bits for host addressing. Subnets: 2 12 = 4096.

Hosts: 2 12 – 2 = 4094.

Valid subnets: 256 – 240 = 16. The subnets in the second octet are a block size of 1 and the subnets in the third octet are 0, 16, 32,64,80,96,112, etc.

**Table 2 Proposed subnets in the network**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Subnet | 10.0.0.0 | 10.0.16.0 | 10.0.32.0 | … | 10.255.240.0 |
| first host | 10.0.0.1 | 10.0.16.1 | 10.0.32.1 | … | 10.255.240.1 |
| Last host | 10.0.15.254 | 10.0.31.254 | 10.0.47.254 | … | 10.255.255.254 |
| Broadcast | 10.0.15.255 | 10.0.31.255 | 10.0.47.255 | … | 10.255.255.255 |

**Table 3 Proposed IP addresses for the 4 sites**

|  |  |  |
| --- | --- | --- |
| **Branch Name** | **Number of Hosts** | **Proposed Network address** |
| **London** | 1500 Hosts | 10.0.16.0 |
| **Leeds** | 500 Hosts | 10.0.32.0 |
| **Liverpool** | 900 Hosts | 10.0.48.0 |
| **Leicester** | 1200 Hosts | 10.0.64.0 |

**1.2 ROUTING PROTOCOL**

Because of some of its benefits, OSPF is typically taken into consideration by users. It operates by first creating a shortest path tree using the Dijkstra algorithm, then filling the routing table with the best pathways that emerge. Two other outstanding benefits that OSPF provides are:

1. It supports multiple, equal-cost routes to the same destination

2. Supports both IP and IPv6 routing protocols.

All four (4) sites will be configured with OSPF routing protocol and below figure depicts London router can communicate with all other Three(3) sites and the ISP

The routing table of London router is depicted in figure 2 which reflects the routing table of other routers.

**Figure 2**

A close-up of a white screen

Description automatically generated

**1.2.1 SAMPLE ROUTER RUNNING CONFIGS(London router)**

The proposed network was deployed in a test environment on the packet tracer to derive the above routing table and all routers had similar configurations with the London router. The configurations took into security and performance as seen in the below sample configurations

Current configuration : 1372 bytes

!

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname londonR

!

!

!

enable secret 5 $1$mERr$BzWXHJbL/8FCg3nYAD5SU.

!

!

ip dhcp excluded-address 10.0.16.1 10.0.16.20

!

ip dhcp pool London\_fintec\_inc

network 10.0.16.0 255.255.240.0

default-router 10.0.16.1

dns-server 10.0.16.1

domain-name fintech\_corp

!

!

!

ip cef

no ipv6 cef

!

!

!

!

!

!

!

!

!

!

!

!

spanning-tree mode pvst

!

!

!

!

!

!

interface GigabitEthernet0/0/0

ip address 10.0.16.1 255.255.240.0

duplex auto

speed auto

!

interface GigabitEthernet0/0/1

ip address 209.165.200.226 255.255.255.0

duplex auto

speed auto

!

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

!

interface Serial0/1/0

ip address 10.0.128.1 255.255.240.0

clock rate 2000000

!

interface Serial0/1/1

ip address 10.0.80.1 255.255.240.0

clock rate 2000000

!

interface Vlan1

no ip address

shutdown

!

router ospf 1

log-adjacency-changes

network 10.0.80.0 0.0.15.255 area 0

network 10.0.128.0 0.0.15.255 area 0

network 10.0.16.0 0.0.15.255 area 0

network 209.165.200.0 0.0.0.255 area 0

!

ip classless

!

ip flow-export version 9

!

!

!

banner motd ^CLONDON ROUTER NOT FOR UNAUTORISED ACCESS ^C

!

!

!

!

line con 0

password P@55word1

login

!

line aux 0

!

line vty 0 4

password [P@55word1](mailto:P@55word1)

login

transport input ssh

!

!

!

end

**1.3 DHCP CONFIGURATION**

A DHCP pool will be configured on all four routers to serve as the DHCP server for all devices, with exclusion of Ips for management of network devices as shown in the above configuration for London site(***ip dhcp pool London\_fintec\_inc***)

**2.0 SWITCHING**

The initial design didn’t utilize switches and all systems were connected directly to the router which made expansion difficult. This proposed design will utilize switches that will offer scalability to the network and the switches will be installed using the hierarchical model of installation of switches in a network i.e.;

1. Access Layer; First layer where switches connect directly to the end user devices

2.Distribution layer: middle layer where traffic us aggregated and distributed

3. Core Layer; The backbone of the network

The introduction of switches will also guarantee the deployment of VLANS, which provide complete control over all ports and network users by enabling the construction and creation of various broadcast groups. Therefore, the days of anyone being able to access network resources by simply plugging their workstations into any switch port are long gone.

**2.1 Advantages of VLANS**

1. VLANs can be created in line with a specific user’s need for the network resources.

2. Switches can be configured to inform a network management station

about unauthorized access to those vital network resources.

3. inter-VLAN routing can be implemented for communication between the permitted configurations between VLANs using the router

4. Restrictions to hardware, protocol, applications and other resourced can also be restricted to the permitted groups and personnel within the organization

5. Scalability and flexibility are two other important features that the VLAN provides. In essence, creating VLANs reduces the size of layer 2 broadcast domains. Consequently, broadcasts emanating from a node within a single VLAN will not be routed to ports set up to be part of an alternate VLAN. The broadcast will only be received by the users we want to allow into that broadcast domain, regardless of where they are physically located. The network will develop as the organisation does, thanks to the introduction of VLANs.

**2.2 VLANS IMPLMENTATION.**

The four sites will be configured for the following VLANs;

* "Finance” (VLAN 30),
* "Executive" (VLAN 40), and
* "Employers" (VLAN 50

The core switch will be configured with the VLANs itemized as a VTP server which will propagate the VLANs across all other switches that will be configured as VTP client. After the VLANs are propagated then all ports on all switches will be assigned to these VLANs to ensure implementation of policies.

The figure below reflects the VLANs that will be propagated by VTP in all sites;

***Figure3***

A close-up of a document

Description automatically generated

**Below shows the VTP on Leicester core switch**

leicestercore#sh vtp status

VTP Version capable : 1 to 2

VTP version running : 1

VTP Domain Name : fintec\_corp

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0002.1743.B000

Configuration last modified by 10.0.64.2 at 3-2-93 08:39:01

Local updater ID is 10.0.65.1 on interface Vl30 (lowest numbered VLAN interface found)

Feature VLAN :

--------------

VTP Operating Mode : Server

Maximum VLANs supported locally : 255

Number of existing VLANs : 9

Configuration Revision : 0

MD5 digest : 0x45 0x12 0x70 0x03 0xAB 0x56 0x65 0x56

0x83 0x4D 0xED 0xA2 0xF2 0x5E 0xC9 0x44

leicestercore#

**Below shows the VTP on Leicester distribution switch**

leicesterdist1#sh vtp status

VTP Version : 1

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 9

VTP Operating Mode : Client

VTP Domain Name : fintec\_corp

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x45 0x12 0x70 0x03 0xAB 0x56 0x65 0x56

Configuration last modified by 10.0.64.2 at 3-2-93 08:39:01

**2.3 SAMPLE CONFIGURATIONS**

The switch configurations will implement access control by allowing technicians to the devices as shown in the configurations.

**LEICESTER CORE SWITCH**

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname leicestercore

!

enable secret 5 $1$mERr$BzWXHJbL/8FCg3nYAD5SU.

!

!

!

ip ssh version 1

ip domain-name fintec\_corp

!

username Todd privilege 15 password 0 P@55word1

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

description connection to distribution2

switchport mode trunk

!

interface FastEthernet0/2

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/3

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/4

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/5

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/6

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/7

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/8

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/9

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/10

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/11

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/12

switchport access vlan 30

switchport mode access

!

interface FastEthernet0/13

switchport access vlan 40

!

interface FastEthernet0/14

switchport access vlan 40

!

interface FastEthernet0/15

switchport access vlan 40

!

interface FastEthernet0/16

switchport access vlan 40

!

interface FastEthernet0/17

switchport access vlan 40

!

interface FastEthernet0/18

switchport access vlan 40

!

interface FastEthernet0/19

switchport access vlan 40

!

interface FastEthernet0/20

switchport access vlan 50

!

interface FastEthernet0/21

switchport access vlan 50

!

interface FastEthernet0/22

switchport access vlan 50

!

interface FastEthernet0/23

switchport access vlan 50

!

interface FastEthernet0/24

switchport access vlan 50

!

interface GigabitEthernet0/1

description connection to router

switchport access vlan 99

switchport mode access

!

interface GigabitEthernet0/2

description connection to distribution1

switchport mode trunk

!

interface Vlan1

no ip address

shutdown

!

interface Vlan30

ip address 10.0.65.1 255.255.240.0

!

interface Vlan40

ip address 10.0.67.1 255.255.240.0

!

interface Vlan50

ip address 10.0.69.1 255.255.240.0

!

interface Vlan99

ip address 10.0.64.2 255.255.255.240

!

ip default-gateway 10.0.64.1

!

banner motd #leceistercore is not for unuathorised user#

!

!

!

line con 0

password P@55word1

login

!

line vty 0 4

password P@55word1

login local

transport input none

line vty 5 15

login local

transport input none

!

!

!

!

end

**3.0 ACCESS LIST AND CONTROLS**

When it comes to managing network traffic, access lists are quite helpful as they are just a set of criteria that classify packets. In these circumstances, the best instrument for decision-making would be an ACL. (Todd lammle, 2016, p. 459). The switch configurations will implement Extended access control.

Numerous additional fields in an IP packet's layer 3 and layer 4 headers can be evaluated by extended access lists. They can assess the port number in the Transport layer header, the Protocol field in the Network layer header, and the source and destination IP addresses. This allows traffic control decisions made by extended access lists to be much more precise.

Todd lammle, 2016, p. 460)

IP extended access lists are best placed as close to the source as possible. Since extended access lists can filter on very specific addresses and protocols, to optimize the network, the traffic shouldn’t traverse the entire network just to be denied.

Since The three sites( Leicester, Leeds and Liverpool) needs to be restricted from getting to the internet, access list will be configured at the outbound interfaces for this networks on the router has shown below;

**access-list 110 deny tcp any host 209.165.200.227 255.255.255.0 eq www**

Also on all switches, the list of allowed technicians to all network devices will be implemented with secret passwords with Telnet been disabled as shown in the switches configuration detailed below;

*‘username Todd privilege 15 password 0* [*P@55word1*](mailto:P@55word1)*’*

‘line vty 0 4

password P@55word1

login local

transport input none

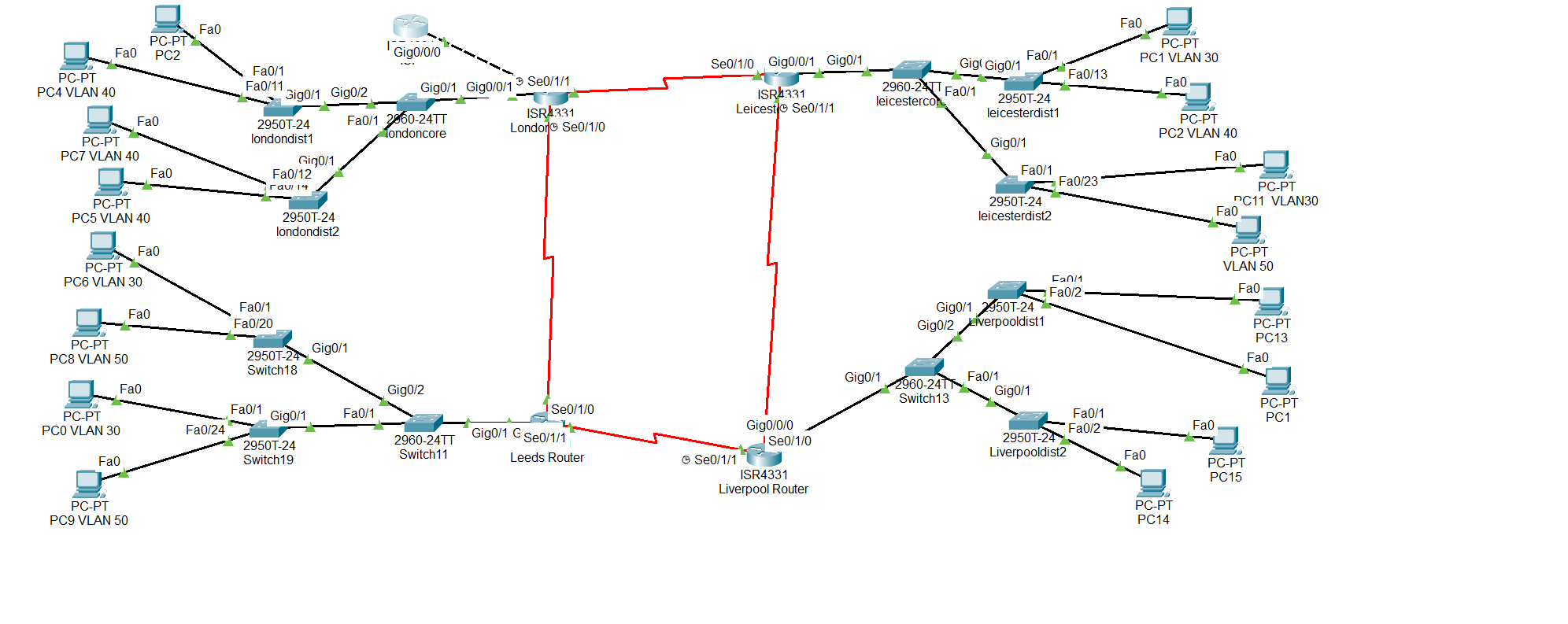
line vty 5 15

login local

transport input none

!

**CONCLUSION**

****

The network once implemented will have the logical diagram has shone on figure 4 and this implementation will solve all the current challenges the current toploy is experincing

**REFRENCE:**

1. Todd,L., 2016. *CCNA Routing and Switching complete study guide*. 2nd ed. America:Sybex

2. Lecture notes and LAB practicals.