BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

------🙢⯎🙠*------*

A blue logo with a flower and a planet

Description automatically generated

**BÁO CÁO ĐỒ ÁN**

**THIẾT KẾ MẠNG**

**THIẾT KẾ HỆ THỐNG MẠNG CHO TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

GIẢNG VIÊN HƯỚNG DẪN: **ThS. Lê Anh Tuấn**

NHÓM SINH VIÊN THỰC HIỆN:

**Bùi Thành Đạt 21520689**

**Tạ Hoàng Long 21522307**

**Lê Văn Tuyến 21522778**

**Nguyễn Anh Khoa 19520638**

MỤC LỤC

*Trang*

[MỤC LỤC ii](#_Toc154775247)

[Lời mở đầu iii](#_Toc154775248)

[CHƯƠNG I: GIỚI THIỆU TỔNG QUAN 4](#_Toc154775249)

[1.1. Mục đích và tổng quan 4](#_Toc154775250)

[1.2. Phân tích yêu cầu 4](#_Toc154775251)

[1.2.1. Yêu cầu 4](#_Toc154775252)

[1.2.2. Bảng phân tích nhu cầu sử dụng 5](#_Toc154775253)

[1.3. Các công nghệ mạng khả dụng 5](#_Toc154775254)

[1.3.1. WiFi 5](#_Toc154775255)

[1.3.2. Routing 6](#_Toc154775256)

[1.3.3. Server 9](#_Toc154775257)

[1.3.4. Cloud 10](#_Toc154775258)

[CHƯƠNG II: THIẾT KẾ HỆ THỐNG MẠNG 12](#_Toc154775259)

[2.1. Thiết kế mô hình mạng logic 12](#_Toc154775260)

[2.2. Mô hình địa chỉ IP cho hệ thống mạng 13](#_Toc154775261)

[2.2.1. Bảng dải địa chỉ IP 13](#_Toc154775262)

[2.2.2. Cấu hình port 14](#_Toc154775263)

[2.2.3. Các bước cấu hình 15](#_Toc154775264)

[2.3. Cấu hình hệ thống mạng 28](#_Toc154775265)

[2.3.1. Sơ đồ logic 28](#_Toc154775266)

[2.3.2. Thiết kế phân chia vùng mạng 29](#_Toc154775267)

[2.3.2.1. Trụ sở chính 29](#_Toc154775268)

[2.3.2.2. Chi nhánh 30](#_Toc154775269)

[2.4. Chi phí hệ thống 30](#_Toc154775270)

[2.4.1. Các thiết bị dùng trong hệ thống 30](#_Toc154775271)

[2.4.2. Chi phí thuê dịch vụ 31](#_Toc154775272)

[KẾT LUẬN VÀ KIẾN NGHỊ 33](#_Toc154775273)

[tài liệu tham khảo 34](#_Toc154775274)

[Lời cảm ơn 35](#_Toc154775275)

Lời mở đầu

Lời đầu tiên, chúng em xin phép gửi lời cảm ơn tới thầy *Lê Anh Tuấn* đã tận tình giảng dạy và chỉ bảo chúng em trong quá trình học tập cũng như thực hiện đồ án. Với sự tâm huyết của mình, không chỉ là kiến thức trong sách vở, thầy còn truyền đạt cho chúng em những kiến thức thực tế, kỹ năng mềm khác.

Chúng em đã nỗ lực và cố gắng hoàn thành đề tài được giao một cách tốt nhất trong khả năng của bản thân, nhưng vì vẫn còn thiếu sót về mặt kiến thức nên không thể tránh được những sai sót cũng như những hạn chế trong quá trình hoàn thành đồ án. Dù vậy chúng em vẫn cố gắng và hoàn thiện từng ngày trong quá trình hoàn thành đồ án vừa qua, vậy nên em mong Thầy thông cảm với những thiếu sót của chúng em và góp ý cũng như chỉ bảo để giúp chúng em hoàn thiện hơn.

Một lần nữa, nhóm chúng em xin chân thành cảm ơn và xin được gửi lời chúc đến thầy *Lê Anh Tuấn.* Kính chúc thầy luôn tiến tới, thành công trong sự nghiệp theo đuổi tri thức của thầy và mong rằng thầy sẽ luôn giữ được sự tâm huyết của mình đối với sinh viên.

CHƯƠNG I: GIỚI THIỆU TỔNG QUAN

1.1. Mục đích và tổng quan

Bài viết này cung cấp giải pháp thiết kế mạng cho trường đại học Công nghệ Thông tin UIT với 2 chi nhánh.

Tổng quan đề án cần xây dựng giải pháp thiết kế mạng và deploy theo kiểu greenfield cho một hệ thống theo yêu cầu cho trước.

1.2. Phân tích yêu cầu

1.2.1. Yêu cầu

*Trụ sở chính:*

* Giảng viên và các phòng ban có máy bàn có thể truy cập Internet để làm việc.
* Một hệ thống server với khả năng lưu trữ lớn để lưu trữ dữ liệu và các khóa học của sinh viên.
* Một hệ thống server để triển khai máy ảo phục vụ nghiên cứu.
* Một hệ thống wifi chứng thực cho sinh viên, giảng viên và cán bộ trong trường. Một hệ thống wifi public với đường kết nối Internet riêng.
* Hỗ trợ VPN cho các cán bộ và giảng viên khi làm việc tại nhà

*Chi nhánh:*

* Nhân viên phòng đào tạo từ xa sử dụng máy bàn để truy cập hệ thống quản lý trường và internet để làm việc.
* Hệ thống wifi public với đường kết nối Internet riêng cho học viên và nhân viên.
* Hỗ trợ VPN site-to-site để nhân viên phòng đào tạo truy cập vào hệ thống quản lý đặt tại Trụ sở chính.

Ngoài những yêu cầu quá trình xây dựng và thiết kế chúng ta cần tuân thủ những yêu cầu về mặt kỹ thuật, cấu trúc đặt ra như:

* Yêu cầu về hiệu năng, ứng dụng.
* Yêu cầu tính thông suốt của hệ thống mạng.
* Yêu cầu về mặt quản lý mạng như phân vùng, phân quyền.
* Yêu cầu an ninh an toàn mạng.

Để triển khai được yêu cầu, chúng ta cần phải thực hiện các công việc:

* Khảo sát thực trạng ở cả 2 cơ sở của trường Đại học Công nghệ Thông tin.
* Khảo sát nhu cầu của khách hàng.
* Nghiên cứu công nghệ mạng phù hợp.
* Thiết kế và xây dựng hệ thống mạng ứng dụng phù hợp với yêu cầu khách hang

1.2.2. Bảng phân tích nhu cầu sử dụng

Hiện nay trường đại học Công nghệ Thông tin có tổng số hơn 6000 sinh viên, học viên cao học, nghiên cứu sinh và giảng viên. Do đó chúng ta sẽ phải chia số lượng sử dụng mạng ra thành các nhóm tùy theo nhu cầu cũng như khối lượng tiêu thụ mạng của các nhóm đó.

* Trụ sở chính:

|  |  |  |
| --- | --- | --- |
| **Nhóm** | **Số lượng truy cập đồng thời** | **Băng thông** |
| Giảng viên, sinh viên, khách | 3000 | 15 Gbps |
| Các thiết bị khác | 300 | 5 Gbps |

* Cơ sở quận 3:

|  |  |  |
| --- | --- | --- |
| **Nhóm** | **Số lượng truy cập đồng thời** | **Băng thông** |
| Giảng viên, sinh viên, khách | 100 | 15 Gbps |
| Các thiết bị khác | 30 | 5 Gbps |

1.3. Các công nghệ mạng khả dụng

1.3.1. WiFi

* *GPON:* GPON là viết tắt của "Gigabit Passive Optical Network" là mạng quang thụ động gigabit. GPON sử dụng cơ chế truy cập điểm-tới-đa điểm. Đặc điểm chính của nó là sử dụng các bộ tách thụ động trong mạng lưới phân phối chất xơ, cho phép một sợi đơn ăn từ văn phòng trung tâm của nhà cung cấp để phục vụ cho nhiều ngôi nhà và các doanh nghiệp nhỏ.
* *Extranet:* Extranet là một mạng công nghệ nội bộ dựa trên giao thức TCP/IP, cho phép truy cập vào các đối tác, nhà cung cấp hoặc một nhóm khách hàng. Nó cũng được xem như là một mạng riêng chia sẻ một cách an toàn thông tin nội bộ cũng như hoạt động của doanh nghiệp với người ở bên ngoài đã được uỷ quyền. Muốn truy cập thành công, người dùng bắt buộc phải có ID, mật khẩu và các cơ chế xác thực khác để truy cập.
* *802.11n:* thường được biết đến là Wi-Fi 4, là một tiêu chuẩn Wi-Fi được phát triển để cải thiện hiệu suất và khả năng của mạng không dây so với các chuẩn trước đó. Chuẩn 802.11n được sử dụng công nghệ MIMO (Multiple-Input Multiple-Output), cho phép hỗ trợ tốc độ tối đa lên tới 600Mbps, đồng thời có thể chạy trên cả 2 băng tần là 2.4 GHz và 5 GHz, phạm vi kết nối lên đến 250m tùy thuộc vào môi trường.

1.3.2. Routing

* *VRF:* Virtual Routing and Forwarding (VRF) là một công nghệ mạng máy tính dựa trên giao thức IP, hoạt động ở Layer trong mô hình OSI cho phép người dùng cấu hình nhiều bảng định tuyến để tồn tại đồng thời trong cùng một router. Các địa chỉ IP trùng lặp có thể được sử dụng mà không gặp xung đột vì các instance được định tuyến độc lập với nhau và sẽ được chọn các đường ra ở các interface khác nhau.
* *Load Balancing:* Load balancing là một thành phần quan trọng của cơ sở hạ tầng thường được sử dụng để cải thiện hiệu suất và độ tin cậy của các trang web, các ứng dụng, cơ sở dữ liệu và các dịch vụ khác bằng cách phân phối khối lượng công việc trên nhiều máy chủ. Khi máy chủ gặp sự cố, lưu lượng truy cập sẽ được tự động chuyển đến máy chủ còn lại. Nhờ đó, trong hầu hết mọi trường hợp, sự cố bất ngờ có thể được phát hiện và xử lý kịp thời, không làm gián đoạn các truy cập của người dùng.
* *Inter-VLAN routing:* Inter-VLAN routing là quá trình định tuyến (routing) giữa các VLAN khác nhau trên một thiết bị định tuyến hoặc một switch có khả năng định tuyến (router-on-a-stick). Khi bạn có nhiều VLAN trên mạng, để cho phép các thiết bị trong các VLAN này giao tiếp với nhau, bạn cần một cơ chế để định tuyến dữ liệu giữa chúng. Khi các thiết bị trong các VLAN gửi dữ liệu đến địa chỉ IP trong mạng của VLAN khác, router sẽ thực hiện chức năng định tuyến và chuyển tiếp dữ liệu giữa các VLAN, cho phép giao tiếp giữa chúng. Inter-VLAN routing là một phần quan trọng trong việc quản lý mạng hiệu quả, đặc biệt là trong các môi trường có nhiều phòng ban hoặc ứng dụng đòi hỏi tính cô lập*.*
* *802.11Q:* IEEE 802.1Q, thường được gọi là Dot1q, là một chuẩn trong lớp 2 (Data Link Layer) của mô hình OSI, được sử dụng để triển khai VLAN (Virtual LAN) trong các mạng Ethernet, cho phép chia nhỏ mạng thành phần để dễ dàng quản lý đồng thời giảm độ trễ. 802.1Q sử dụng VLAN tagging để đặt thông tin về VLAN vào khung Ethernet. Mỗi gói dữ liệu được thêm vào một thẻ VLAN (VLAN tag) để xác định VLAN của nó. Các thẻ này chứa tất cả các thông tin về VLAN đó.
* *FHRP:* First Hop Redundancy Protocol là một nhóm các giao thức được sử dụng trong mạng máy tính để cung cấp tính sẵn sàng và độ tin cậy cao cho các thiết bị chuyển mạch (switch) khi chúng phải làm việc như là "first hop" (cổng đầu tiên) cho các thiết bị kết nối vào mạng. Hay nói một cách đơn giản hơn là giao thức này cho phép việc dự phòng gateway. Ví dụ trong một mô hình mạng của công ty, ngoài mạng cục bộ, phần quan trọng tiếp theo mà họ cần xử lý là default gateway. Nếu cổng down, thì quyền truy cập vào toàn bộ subnet cũng sẽ down. Do đó, công nghệ FHRP xuất hiện để giúp giải quyết bài toán này.
* *EIGRP:* Enhance Interio Gateway Routing Protocol là giao thức định tuyến mở rộng của IGRP, IGRP là giao thức dạng Classfull, còn EIGRP là giao thức dạng Classless, nghĩa là có mang theo subnetmask trong các lần cập nhật EIGRP là giao thức định tuyến lai (Hybrid Routing), là sự kết hợp của Distance Vector và Link States. EIGRP là một giao thức định tuyến theo vector khoảng cách nâng cao nhưng khi cập nhật và bảo trì thông tin láng giềng và thông tin định tuyến thì nó làm việc giống như một giao thức định tuyến theo trạng thái đường liên kết. Ưu điểm của giao thức này:
  + Khả năng hội tụ nhanh: vì chúng sử dụng DUAL. DUAL bảo đảm hoạt động không bị lặp vòng khi tính toán đường đi, cho phép mọi Router trong hệ thống mạng thực hiện đồng bộ cùng lúc khi có sự thay đổi xảy ra.
  + Bảo tồn băng thông và sử dụng băng thông một cách hiệu quả: vì nó chỉ gửi thông tin cập nhật một phần và giới hạn chứ không gửi toàn bộ bảng định tuyến. Nhờ vậy nó chỉ tốn một lượng băng thông tối thiểu khi hệ thống mạng đã ổn định. Điều này tương tự như hoạt động cập nhật của OSPF, Router EIGRP chỉ gửi thông tin cập nhật một phần cho Router nào cần thông tin đó mà thôi chứ không gửi mọi Router khác trong vùng như OSPF. Chính vì hoạt động cập nhật theo chu kỳ, các Router EIGRP giữ liên lạc với nhau bằng các gói hello rất nhỏ. Việc trao đổi các gói hello theo định kỳ không chiếm nhiều băng thông đường truyền.
  + Hỗ trợ VLSM (Veriable Length Subnet Mask) và CIDA (Classles Inter Domain Routing). Không giống như IGRP,EIGRP có thể trao đổi thông tin ở các IP khác lớp mạng
  + Hỗ trợ IP, IPX, Apple talk: vì Talk nhờ có cấu trúc từng phần theo giao thức (PDMs – Protocok dependent modules). EIGRP có thể phân phối thông tin của IPX,RIP để cải tiến hoạt động toàn diện. Trên thực tế, EIGRP có thể điều khiển giao thức này. Router EIGRP nhận thông tin định tuyến và dịch vụ, chỉ cập nhật cho các Router khác khi thông tin trong bảng định tuyến thay đổi.
  + Chạy trực tiếp trên IP và protocol number là 88
  + Load balancing trên tất cả các cost không bằng nhau
  + Hỗ trợ tất cả các giao thức và cấu trúc dữ liệu ở layer 2
  + Không dùng broadcast và dùng Multicast hoặc Unicast trong từng trường hợp cụ thể
  + Hỗ trợ việc chứng thực
  + Manual Summary trên bất kỳ interface nào
* *ACL:* Access Control List là một cơ chế quản lý quyền truy cập được sử dụng trong hệ thống mạng để kiểm soát và giám sát quyền truy cập vào các tài nguyên. ACL được áp dụng tại cấp giao diện của thiết bị mạng, chẳng hạn như router hoặc switch, để quyết định liệu gói tin có thể đi qua hay không. Một ACL có thể được sử dụng để kiểm soát các yếu tố như địa chỉ IP nguồn/đích, cổng đích/nguồn, giao thức, hoặc các tiêu chí khác để xác định liệu một gói tin có quyền đi qua một giao diện hay không.
* *VPN site-to-site:* VPN site-to-site (Virtual Private Network site-to-site) là một kiểu kết nối mạng ảo giữa hai (hoặc nhiều) địa điểm vật lý khác nhau thông qua Internet hoặc một mạng công cộng khác. Mục tiêu của VPN site-to-site là tạo ra một kênh an toàn để truyền dữ liệu giữa các địa điểm này, giống như việc chúng ta có một mạng riêng tư được mở rộng qua Internet. Các VPN site-to-site thường được triển khai trong môi trường doanh nghiệp để kết nối các chi nhánh, văn phòng, hoặc trung tâm dữ liệu khác nhau với nhau. Điều này cho phép các vị trí khác nhau của một tổ chức có thể giao tiếp với nhau một cách an toàn, bảo vệ dữ liệu khỏi sự can thiệp bên ngoài.
* *VLSM****:*** Variable Length Subnet Masking (VLSM) tương đương với việc chia subnet (mạng con). Điều đó có nghĩa là VLSM cho phép các kỹ sư mạng phân chia một không gian địa chỉ IP thành một hệ thống các subnet có kích thước không giống nhau, giúp tạo ra những subnet với số lượng host rất khác nhau, mà không làm lãng phí số lượng lớn địa chỉ IP.

1.3.3. Server

* *DMZ:* DMZ là vùng mạng trung lập giữa mạng nội bộ và mạng Internet. Vai trò của DMZ nhằm tăng cường bảo mật hệ thống và giảm thiểu các rủi ro từ các cuộc tấn công mạng. Trong một hệ thống mạng, DMZ thường được sử dụng để đặt các máy chủ như web server, mail server hoặc các ứng dụng khác có thể được truy cập từ Internet. Các máy chủ này được đặt trong DMZ để đảm bảo rằng các cuộc tấn công từ bên ngoài chỉ có thể tác động tới DMZ và không thể tiếp cận các máy chủ nội bộ trong mạng nội bộ.
* *RADIUS:* Radius là từ viết tắt của Remote Authentication Dial In User Service. Đây là giao thức mạng hoạt động theo mô hình máy khách (client) – máy chủ (server) chạy trong lớp ứng dụng. Giao thức này sử dụng một máy chủ Radius và nhiều máy khách Radius. Radius thực hiện việc xác định quyền truy cập của người sử dụng mạng internet bằng mô hình máy khách và máy chủ. Thực tế, yêu cầu truy cập được xuất phát từ máy khách và hệ thống máy người dùng hay điểm truy cập Wifi, sau đó chúng sẽ đến điểm xác thực của hệ thống máy chủ Radius. Các Radius Server thường kết hợp để thiết lập thành hệ thống tạo, duy trì, quản lý tất cả thông tin được nhận dạng. Đồng thời, nó cung cấp dịch vụ xác thực riêng biệt. Vì vậy, bất kỳ người dùng internet nào muốn truy cập vào hệ thống mạng đã được giao thức Radius bảo vệ, thì họ bắt buộc phải cung cấp các thông tin xác thực.
* *Rate-limiting:* Rate Limit tức là hạn chế (limit) số lượng request gửi/nhận (rate) đến hệ thống. Việc này sẽ giúp phòng tránh việc server bị DDOS cũng như là giới hạn số lượng request để phù hợp với số lượng mà server có thể xử lý.

1.3.4. Cloud

* *AWS:* Amazon web services là một nền tảng điện toán đám mây phát triển toàn diện được cung cấp bởi Amazon.com. Dịch vụ Web đôi khi được gọi là dịch vụ đám mây hoặc các dịch vụ điện toán từ xa. Các dịch vụ AWS đầu tiên đã được đưa ra vào năm 2006 để cung cấp các dịch vụ trực tuyến cho các trang web và các ứng dụng phía máy khách. Để giảm thiểu việc bị mất điện đột ngột và đảm bảo tính mạnh mẽ của hệ thống, AWS đa dạng về địa lý theo khu vực. Các khu vực này có trung tâm ở Đông Mỹ, Tây Mỹ (hai địa điểm), Brazil, Ireland, Singapore, Nhật Bản và Úc. Mỗi khu vực bao gồm nhiều khu vực địa lý nhỏ hơn được gọi là vùng sẵn có.

CHƯƠNG II: THIẾT KẾ HỆ THỐNG MẠNG

2.1. Thiết kế mô hình mạng logic

A map of a town

Description automatically generated

*Trụ sở chính:*

* Tòa A: Tầng 1 có các phòng ban và thư viện nên sẽ đặt 5 access point để đảm bảo các kết nối lưu thông và tiến độ làm việc không bị gián đoạn giữa các phòng ban. Tầng 2 là thư viện cũng sẽ và một số ít các phòng ban khác nên chỉ cần 3 access point là đủ. Tầng 3 là 3 giảng đường thì cũng sẽ được bố trí 3 access point bởi vì số lượng sinh viên ở giảng đường sẽ rất đông. 2 phòng ban sẽ dùng chung 1 switch.
* Tòa B: Mỗi tầng sẽ có 3 access point đặt ở đầu, cuối và giữa mỗi tầng để đảm bảo toàn vẹn độ phủ sóng. Với tầng 7, tầng 8 và tầng 9 mỗi tầng chỉ cần 1 access point vì ở đây chỉ có 3 phòng nên không cần số lượng quá nhiều. Mỗi tầng sẽ có 1 switch để chia VLAN. Mỗi phòng máy sử dụng 1 switch. Còn các phòng học với mỗi tầng sẽ có 1 switch, riêng từ tầng 7 tới tầng 9 sẽ chỉ cần 1 switch để chia VLAN.
* Tòa C: vì số lượng phòng học không quá nhiều nên chỉ cần 2 access point đặt ở đầu và cuối dãy mỗi tầng. Có 5 phòng máy mỗi phòng 1 switch. Còn các phòng học mỗi tầng dùng chung 1 switch để chia VLAN.
* Tòa D: chi có 1 văn phòng đoàn ở đây nên sẽ chỉ cần 1 access point để tránh lãng phí.
* Tòa E: tầng 1 là trung tâm ngoại ngữ nên chỉ cần 1 access point, các tầng còn lại sẽ có 2 access point ở đầu và cuối mỗi tầng. Với mỗi tầng sẽ có 1 switch. Có 3 phòng lab thì mỗi phòng sẽ có 1 switch riêng.
* Chi tiết thiết bị từng tòa:

|  |  |
| --- | --- |
| Tòa | Số lượng |
| A | 11 APs, 7 switches |
| B | 18 APs, 33 switches |
| C | 6 APs, 8 switches |
| D | 1 AP |
| E | 24 APs, 15 switches |

2.2. Mô hình địa chỉ IP cho hệ thống mạng

2.2.1. Bảng dải địa chỉ IP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Toà | Tên | VLAN | Host | Dải IP |
| A | Server | 2 | 10 | 192.168.2.0/28 |
| Tổ chức hành chính | 20 | 30 | 192.168.20.0/27 |
| Kế hoạch – tài chính | 30 | 30 | 192.168.30.0/27 |
| Công tác sinh viên | 40 | 30 | 192.168.40.0/27 |
| Dữ liệu và công nghệ thông tin | 50 | 30 | 192.168.50.0/27 |
| Thư viện | 60 | 10 | 192.168.60.0/28 |
| Đào tạo đại học | 10 | 30 | 192.168.10.0/27 |
| Bộ môn toán lý | 70 | 10 | 192.168.70.0/28 |
| B | Khoa học và kỹ thuật thông tin | 110 | 100 | 192.168.110.0/25 |
| Hệ thống thông tin | 120 | 100 | 192.168.120.0/25 |
| Mạng máy tín và truyền thông | 130 | 100 | 192.168.130.0/25 |
| Công nghệ phần mềm | 140 | 100 | 192.168.140.0/25 |
| Kỹ thuật máy tính | 150 | 100 | 192.168.150.0/25 |
| Khoa học máy tính | 160 | 100 | 192.168.160.0/25 |
| ALL |  | 999 |  |  |

2.2.2. Cấu hình port

|  |  |  |  |
| --- | --- | --- | --- |
| Thiết bị | Interfaces | Mode | IP |
| SW Core 1 | F0/24 |  | 10.0.10.2/24 |
| F0/23 |  | 10.0.30.1/24 |
| F0/1-14 | trunk |  |
| SW Core 2 | F0/24 |  | 10.0.20.2/24 |
| F0/23 |  | 10.0.30.2/24 |
| F0/1-14 | trunk |  |
| R-GW-1 | F0/0 |  | 10.0.10.1/24 |
| S2/0 |  | 10.0.1.1/24 |
| R-GW-2 | F0/0 |  | 10.0.20.1/24 |
| S2/0 |  | 10.0.2.1/24 |
| INTERNET | S2/0 |  | 10.0.1.2/24 |
| S3/0 |  | 10.0.2.2/24 |
| S4/0 |  | 10.0.3.2/24 |
| Lo0 |  | 8.8.8.8/32 |
| R-chinhanh | F0/0 |  | 192.168.500.1/24 |
| S2/0 |  | 10.0.3.1/24 |
| SW ACCESS | F0/1-2 | Trunk |  |
| F0/3-10 | access |  |
| F0/11-22 | access |  |

2.2.3. Các bước cấu hình

* Cấu hình vlan và trunk:
  + Cấu hình trunk cho liên kết giữa SW CORE và SW ACCESS
  + Cấu hình VTP server tại và các vlan tại core 1, VTP client tại các sw còn lại
  + Trên sw access cấu hình cho f0/1-2 trunk, f0/3-10 access vlan theo yêu cầu. port còn lại cấu hình access vlan 999
  + Đổi native vlan 999
  + Core 1:

//

en

conf t

vtp domain UIT-campus

vtp mode server

vlan 10

name DTDH

vlan 20

name TCHC

vlan 30

name KHTC

vlan 40

name CTSV

vlan 50

name DL-CNTT

vlan 60

name THUVIEN

vlan 2

name SERVER

vlan 110

name K\_KHKTTT

vlan 120

name K\_HTTT

vlan 130

name K\_MTT\_TT

vlan 140

name K\_CNPM

vlan 150

name K\_KTMT

vlan 160

name K\_KHMT

vlan 70

name BMTL

vlan 999

name Unuse

end

wr

//

* + SW còn lại:

//

en

conf t

vtp domain UIT-campus

vtp mode client

end

wr

//

* Cấu hình spanning-tree:
  + Core 1 là root cho vlan toà A, Core 2 là root cho vlan toà B
  + Đổi switch chạy giao thức RSTP
  + Cấu hình port access là portfast và bật DBU Guard
  + CORE 1:

//

en

conf t

spanning-tree mode rapid

spanning-tree vlan 10 root primary

spanning-tree vlan 20 root primary

spanning-tree vlan 30 root primary

spanning-tree vlan 40 root primary

spanning-tree vlan 50 root primary

spanning-tree vlan 60 root primary

spanning-tree vlan 70 root primary

spanning-tree vlan 2 root primary

spanning-tree vlan 110 root secondary

spanning-tree vlan 120 root secondary

spanning-tree vlan 130 root secondary

spanning-tree vlan 140 root secondary

spanning-tree vlan 150 root secondary

spanning-tree vlan 160 root secondary

end

wr

//

* + CORE 2:

//

en

conf t

spanning-tree mode rapid

spanning-tree vlan 10 root secondary

spanning-tree vlan 20 root secondary

spanning-tree vlan 30 root secondary

spanning-tree vlan 40 root secondary

spanning-tree vlan 50 root secondary

spanning-tree vlan 60 root secondary

spanning-tree vlan 70 root secondary

spanning-tree vlan 2 root secondary

spanning-tree vlan 110 root primary

spanning-tree vlan 120 root primary

spanning-tree vlan 130 root primary

spanning-tree vlan 140 root primary

spanning-tree vlan 150 root primary

spanning-tree vlan 160 root primary

end

wr

//

* + SW:

//

en

conf t

spanning-tree mode rapid

end

wr

//

* Cấu hình trunk – vlan: Tạo vtp server-client để tự cập nhật vlan
  + Cấu hình trunk CORE 1:

//

en

conf t

hostname CORE-1

int range f0/1-14

sw trunk encap dot1q

sw mode trunk

sw trunk native vlan 999

end

wr

//

* + Cấu hình trunk Switch:

//

en

conf t

hostname SW-DTDH

int range f0/1-2

sw mode trunk

sw trunk native vlan 999

exit

int range f0/3-10

sw mode access

sw access vlan 10

exit

int range f0/11-24

sw mode access

sw access vlan 999

end

wr

//

* Cấu hình IP:
  + Cấu hình ip cho vlan trên 2 core
  + Cấu hình ip cho các port layer 3 và router
  + CORE 1:

//

en

conf t

int vlan 10

ip add 192.168.10.1 255.255.255.224

no shut

exit

int vlan 20

ip add 192.168.20.1 255.255.255.224

no shut

exit

int vlan 30

ip add 192.168.30.1 255.255.255.224

no shut

exit

int vlan 40

ip add 192.168.40.1 255.255.255.224

no shut

exit

int vlan 50

ip add 192.168.50.1 255.255.255.224

no shut

exit

int vlan 60

ip add 192.168.60.1 255.255.255.240

no shut

exit

int vlan 70

ip add 192.168.70.1 255.255.255.240

no shut

exit

int vlan 2

ip add 192.168.2.1 255.255.255.240

no shut

exit

int vlan 110

ip add 192.168.110.1 255.255.255.128

no shut

exit

int vlan 120

ip add 192.168.120.1 255.255.255.128

no shut

exit

int vlan 130

ip add 192.168.130.1 255.255.255.128

no shut

exit

int vlan 140

ip add 192.168.140.1 255.255.255.128

no shut

exit

int vlan 150

ip add 192.168.150.1 255.255.255.128

no shut

exit

int vlan 160

ip add 192.168.160.1 255.255.255.128

no shut

end

wr

//

* + CORE 2: thay địa chỉ IP từ .1 thành .2
* Gán địa chỉ ip cho port layer 3
* Cấu hình IP router
  + R-GW-1:

//

en

conf t

hostname R-GW-1

int f0/0

ip add 10.0.10.1 255.255.255.0

no shutdown

exit

int S2/0

ip add 10.0.1.1 255.255.255.0

no sh

end

wr m

//

* Giả lập Internet
  + R-INTERNET:

//

en

conf t

hostname INTERNET

int s2/0

ip add 10.0.1.2 255.255.255.0

no shutdown

exit

int s3/0

ip add 10.0.2.2 255.255.255.0

no shutdown

exit

int S4/0

ip add 10.0.3.2 255.255.255.0

no sh

int lo0

ip add 8.8.8.8 255.255.255.255

no shutdown

end

wr

//

* Cấu hình HSRP cho sw core và tạo dự phòng: Vlan toà A ưu tiên đi qua core 1, toà B đi core 2, các phòng lab chia đôi.
  + CORE 1:

//

en

conf t

int vlan 10

standby 1 ip 192.168.10.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 20

standby 1 ip 192.168.20.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 30

standby 1 ip 192.168.30.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 40

standby 1 ip 192.168.40.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 50

standby 1 ip 192.168.50.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 60

standby 1 ip 192.168.60.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 70

standby 1 ip 192.168.70.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 2

standby 1 ip 192.168.2.5

standby 1 priority 105

standby 1 preempt

exit

int vlan 110

standby 1 ip 192.168.110.5

standby 1 preempt

exit

int vlan 120

standby 1 ip 192.168.120.5

standby 1 preempt

exit

int vlan 130

standby 1 ip 192.168.130.5

standby 1 preempt

exit

int vlan 140

standby 1 ip 192.168.140.5

standby 1 preempt

exit

int vlan 150

standby 1 ip 192.168.150.5

standby 1 preempt

exit

int vlan 160

standby 1 ip 192.168.160.5

standby 1 preempt

end

wr

//

* + CORE 2: đảo lại vị trí standby 1 priority 105 cho các vlan còn lại
* Cấu hình SW Core track port f0/24 cho các vlan active trên nó
  + CORE 1:

//

conf t

int vlan 10

standby 1 track f0/24

exit

int vlan 20

standby 1 track f0/24

exit

int vlan 30

standby 1 track f0/24

exit

int vlan 40

standby 1 track f0/24

exit

int vlan 50

standby 1 track f0/24

exit

int vlan 60

standby 1 track f0/24

exit

int vlan 70

standby 1 track f0/24

exit

int vlan 2

standby 1 track f0/24

end

wr

//

* + CORE 2:

//

conf t

int vlan 110

standby 1 track f0/24

exit

int vlan 120

standby 1 track f0/24

exit

int vlan 130

standby 1 track f0/24

exit

int vlan 140

standby 1 track f0/24

exit

int vlan 150

standby 1 track f0/24

exit

int vlan 160

standby 1 track f0/24

end

wr

//

* Cấu hình DHCP:
  + Có 2 cách cấu hình DHCP cho vlan. Cấu hình trên Core Switch và cấu hình DHCP server chung
  + ở đây ta thực hiện cách 2 để dễ quản lý
  + trong phòng server(vlan 2) đặt server và bật DHCP trên phần service
  + gán địa chỉ ip tĩnh cho DHCP server và tạo các pool DHCP theo yêu cầu
  + DNS server cũng được gắn ip tĩnh

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

* + Trên Core và Switch ta gắn ip-helper là ip DHCP server cho các vlan

//

en

conf t

int vlan 10

ip helper-address 192.168.2.7

exit

int vlan 20

ip helper-address 192.168.2.7

exit

int vlan 30

ip helper-address 192.168.2.7

exit

int vlan 40

ip helper-address 192.168.2.7

exit

int vlan 50

ip helper-address 192.168.2.7

exit

int vlan 60

ip helper-address 192.168.2.7

exit

int vlan 70

ip helper-address 192.168.2.7

exit

int vlan 2

ip helper-address 192.168.2.7

exit

int vlan 110

ip helper-address 192.168.2.7

exit

int vlan 120

ip helper-address 192.168.2.7

exit

int vlan 130

ip helper-address 192.168.2.7

exit

int vlan 140

ip helper-address 192.168.2.7

exit

int vlan 150

ip helper-address 192.168.2.7

exit

int vlan 160

ip helper-address 192.168.2.7

end

wr

//

* + Cấu hình dns vlan toà A trên C1, toà B trên C2
  + IP bắt đầu từ .11
  + Dùng c++ để in các code cần thiết

//

int main()

{

cout<<"en\nconf t\n";

for(int i=1;i<7;i++)

{

cout << "ip dhcp pool 192.168."<<i<<"0.0\n";

cout << " network 192.168."<<i<<"0.0 255.255.255.0\n";

cout << " default-router 192.168."<<i<<"0.5\n";

cout << " dns 192.168.2.11\n exit\n";

cout << "ip dhcp exclude 192.168."<<i<<"0.1 192.168."<<i<<"0.10\n";

cout << "ip dhcp exclude 192.168."<<i<<"0.41 192.168."<<i<<"0.254\n\n";

}

cout <<"end\nwr\n";

return 0;

}

//

* + Thay đổi 1 số thông số phù hợp với số host rồi chạy trên CORE SW
  + Làm tương tự cho các vlan nhà B
* Routing:
  + Sử dụng giao thức định tuyến EIGRP để định tuyến động sao cho mạng bên trong ping được 8.8.8.8. bao gồm 2 SW CORE, 2 R-GW, R-INTERNET, R-CHINHANH
  + CORE 1:

//

en

conf t

ip routing

router eigrp 1

network 10.0.10.0

network 10.0.30.0

network 192.168.0.0 0.0.255.255

passive-interface vlan 1

passive-interface vlan 10

passive-interface vlan 20

passive-interface vlan 30

passive-interface vlan 40

passive-interface vlan 50

passive-interface vlan 60

passive-interface vlan 70

passive-interface vlan 2

passive-interface vlan 110

passive-interface vlan 120

passive-interface vlan 130

passive-interface vlan 140

passive-interface vlan 150

passive-interface vlan 160

end

wr m

//

* + CORE 2: ta đổi vùng mạng còn lại giữ nguyên
  + ROUTER 1:

//

en

conf t

router eigrp 1

network 10.0.1.0

network 10.0.10.0

end

wr m

//

* + ROUTER INTERNET:

//

en

conf t

router eigrp 1

network 10.0.1.0

network 10.0.2.0

network 10.0.3.0

network 8.8.8.8

end

wr m

//

* + ROUTER 2 và ROUTER CHINHANH ta đổi vùng mạng còn lại giữ nguyên
  + Một số L3 switch không cho phép định tuyến mặc định nên ta thêm lệnh ip routing.
* Tạo default router:
  + Trên R-GW-1 tạo ip route main cho phép tất cả dải mạng ra internet: ip rout 0.0.0.0 0.0.0.0 10.0.1.2
  + Gán ip route này vào eigrp để quảng bá xuống Core
  + R-GW-1/2:

//

conf t

router eigrp 1

redistribute static metric 1000 10 255 1 1500

end

wr m

//

* Cấu hình NAT:
  + Cho mạng nội bộ trong R1-2 ra ngoài
  + Trên mạng chi nhánh ta cấu hình thêm source ip route 0.0.0.0 0.0.0.0 s2/0

//

conf t

access-list 1 permit any

ip nat inside source list 1 interface s2/0 overload

int s2/0

ip nat outside

exit

int f0/0

ip nat inside

end

//

* + Cho phép máy chi nhánh truy cập Web và FTP

//

conf t

ip nat inside source static tcp 192.168.2.10 80 203.162.1.2 8080

ip nat inside source static tcp 192.168.2.10 443 203.162.1.2 8443

ip nat inside source static tcp 192.168.2.9 21 203.162.1.2 8021

end

wr m

//

2.3. Cấu hình hệ thống mạng

2.3.1. Sơ đồ logic

A diagram of a network

Description automatically generated

2.3.2. Thiết kế phân chia vùng mạng

2.3.2.1. Trụ sở chính

Mô hình mạng được phân chia thành 3 lớp *Core, Distribution* và *Access:*

* *Core:* Bao gồm 2 router ở đầu ra internet để cấu hình load balancing, 2 server DMZ. 2 router sẽ được cấu hình thêm VPN site-to-site để có thể liên kết với hệ thống ở chi nhánh. Trước 2 router sẽ có 2 firewall để nhằm bảo mật, và nó sẽ được kết nối với nhau để chia sẻ lưu lượng. Khi 1 firewall có vấn đề thì ngay lập tức sẽ chuyển lưu lượng cũng như sẽ ngắt đường ra internet ở firewall bị trục trặc và chuyển sang firewall còn lại. 2 server DMZ cũng sẽ có 2 firewall vì đây là vùng vô cùng quan trọng, vì các dịch vụ đều nằm ở đây. Vì thế mỗi server DMZ sẽ kết nối với 1 switch layer 3 riêng để khi 1 server có vấn đề thì sẽ không bị ảnh hưởng đến server còn lại. Ngoài ra còn 3 vùng mạng riêng của Wifi để chia đối tượng sử dụng mạng. Mạng Public sẽ có 1 đường mạng riêng, sử dụng dịch vụ OLT riêng của nhà mạng, không kết nối vào hệ thống mạng nhằm mục đích bảo mật, tránh để hệ thống bị xâm nhập thông qua đường mạng này. 2 mạng UIT và UIT GUEST sẽ nằm ở trong hệ thống mạng nhằm quản lý các tài khoản truy cập.
* *Distribution:* Bao gồm 2 switch layer 3 làm nhiệm vụ tổng hợp traffic từ lớp Access. Các VLAN sẽ sử dụng SVI để chọn default gateway trên 2 switch này. 2 switch này sẽ liên tục hoạt động ở trạng tháiActive-Active (mỗi Switch sẽ gánh một phần lưu lượng, nếu 1 Switch down, Switch còn lại sẽ gánh toàn bộ lưu lượng chờ khắc phục).
* *Access:* Bao gồm các switch ở các tòa nhà. Các switch sẽ được đấu nối theo mô hình Mess để cung cấp truy cập tới các WLAN: UIT Public, UIT và UIT GUEST. Ngoài ra các PC cũng sẽ được kết nối trực tiếp tới switch ở các tầng. Ở mỗi tòa nhà sẽ có 1 Wireles Controller để tập trung quản lý cũng như giám sát các access point.
* *Data center:* Gồm 3 server có các chức năng khác nhau:
  + Server 1 có cấu hình mạnh, độ sẵn sàng lớn và tốc độ xử lý cao, dùng để phục vụ cho nghiên cứu và ảo hóa.
  + Server 2 ưu tiên khả năng lưu trữ lớn dùng lưu dữ liệu, thông tin sinh viên.
  + Server 3 dùng để chạy các tác vụ, dịch vụ quản trị hệ thống mạng.

Trong data center còn có các PC để quản lý các server. Trước các server cũng sẽ có 2 firewall phân chia lưu lượng và nhằm bảo vệ vùng này ở mức cao nhất vì đây là nơi quan trọng nhất của hệ thống mạng.

Ngoài ra cũng sẽ có dịch vụ cloud của Amazon để lưu trữ thông tin cũng như phục vụ cho một số hoạt động khác.

2.3.2.2. Chi nhánh

Tại chi nhánh cũng sẽ có 1 router và một firewall để bảo mật. Tuy nhiên router này sẽ đảm nhận nhiều chức năng hơn như là load balancing, VPN site-to-site, … Dưới đó sẽ là PC quản lý chi nhánh và các access point để có thể phủ sóng mạng cho cả chi nhánh. Ngoài ra cũng sẽ có 1 vùng mạng riêng để làm WiFi public cho chi nhánh. Và có thêm 1 wireless controller để quản lý và giám sát các access point.

2.4. Chi phí hệ thống

2.4.1. Các thiết bị dùng trong hệ thống

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Thiết bị | Tên thiết bị | Số lượng | Đơn giá (VND) | Thành tiền (VND) |
| Multilayer switch | Cisco WS-C3650-24TS-E | 2 | 52.500.000 | 105.000.000 |
| Firewall | FortiGate FG-40F | 5 | 11.340.000 | 56.700.000 |
| Router | CISCO2901/ K9 | 4 | 33.000.000 | 132.000.000 |
| Switch | Cisco CBS220-24T-4G-EU | 63 | 5.690.000 | 358.470.000 |
| Access Point | Cisco C9105AXI-EWC-S | 60 | 11.800.000 | 708.000.000 |
| Server | Emerson 10KVA GXT MT+ Online UPS | 1 | 41.000.000 | 41.000.000 |
| Dell PowerEdge R650xs | 2 | 56.000.000 | 112.000.000 |
| Dell PowerEdge T350 (Basic) | 1 | 55.430.000 | 55.430.000 |
| Tổng | | | | 1.568.600.000 |

Tổng chi phí cho thiết bị dự kiến: 1.568.600.000 VND (*một tỷ năm trăm sáu mươi tám triệu sáu trăm nghìn đồng*)

2.4.2. Chi phí thuê dịch vụ

|  |  |  |
| --- | --- | --- |
| Dịch vụ | Tên dịch vụ | Đơn giá (VND/năm) |
| Gói cước Internet | SUPER SOC | 97.500.000 |
| Gói IP tĩnh | Đi cùng SUPER SOC | 14.400.000 |
| Cloud | AWS EC2 t3.2xlarge | 3.738.768 |
| Microsoft | Microsoft 365 Business Basic | 1.309.500.000 |

* Microsoft 365

Sẽ bao gồm dịch vụ Microsoft Teams và Microsoft Office 365 với giá thuê được quy đổi sang VND là 200.062 VND/người/tháng. Với ước tính 1500 sinh viên và giảng viên một năm thì chi phí sẽ là 72.750\* 1500 \* 12 = 1.309.500.000VND/năm.

* Tổng chi phí cho dịch vụ trong 1 năm là 1.425.138.768 VND/năm (*một tỷ bốn trăm hai mươi lăm triệu một trăm ba mươi tám nghìn bảy trăm sáu mươi tám đồng*).

2.4.1.3. Bảng dự trù kinh phí

|  |  |  |
| --- | --- | --- |
| STT | Hạng mục | Giá tiền |
| 1 | Chi phí thiết bị | 1.376.630.000 VND |
| 2 | Chi phí dây dẫn | 50.000.000 VND |
| 3 | Chi phí dịch vụ | 1.425.138.768 VND/năm |

KẾT LUẬN VÀ KIẾN NGHỊ

Kết luận

Đây là thiết kế hệ thống mạng của trường Đại học Công nghệ Thông tin với 2 chi nhánh. Hệ thống đã đảm bảo được các yếu tố và yêu cầu của đề tài, đem lại hiệu quả cho hệ thống.

Nhóm sẽ tiếp tục nghiên cứu chuyên sâu vào vấn đề bảo mật mạng để đảm bảo quản trị hệ thống mạng hoàn chỉnh và tăng mức độ an toàn.

Trong tương lai sẽ liên tục cập nhật hệ thống (nâng cấp, mở rộng).

Kiến nghị

Vì budget còn hạn chế nên không thể triển khai hệ thống một cách hoàn thiện hơn. Nếu budget có thể mở rộng hơn thì sẽ có thể sử dụng nhiều dịch vụ cũng như các thiết bị cao cấp hơn.

tài liệu tham khảo

[1] *Priscilla Oppenheimer, (2010). “Top – Down Network Design”, 3th ed, Cisco Press*

[2] *Jame F. Kurose – Keith W. Ross, (2017).”Computer Networking”, 7th ed, PEARSON*

[3] *Wayne Lewis – Ph.D, (2008), “Lan Switch and Wireless”, Cisco Press*

[4] *Michaela Goss (2023), “12 common network protocols and their functions explained”,* [*https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained*](https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained)*.*

[5] *Amazon, “AWS Documentation”,* [*https://docs.aws.amazon.com/*](https://docs.aws.amazon.com/)

Lời cảm ơn

Trước tiên chúng em xin cảm ơn sâu sắc đến cha mẹ đã cổ vũ, động viên, hỗ trợ về tinh thần cũng như tạo mọi điều kiện thuận lợi cho em hoàn thành tốt tiểu luận này.

Chúng em xin chân thành cảm ơn thầy *Lê Anh Tuấn* đã luôn quan tâm chỉ dạy, theo dõi, giúp đỡ tận tình trong suốt khoảng thời gian em thực hiện tiểu luận.

Và hơn hết, chúng em xin bày tỏ lòng biết ơn trân trọng đến quý thầy cô *trường Đại học Công nghệ Thông tin* đã tận tình chỉ dạy, truyền đạt những kiến thức quý báo cho chúng em trong thời gian vừa qua để chúng em có đủ kiến thức, điều kiện để thực hiện đề tài này. Đồng thời chúng em cũng rất biết ơn các cán bộ trực ở thư viện ệ, phòng máy... đã hỗ trợ giúp đỡ chúng em trong thời gian qua.

Đồng cảm ơn đến các tác giả trong các quyển sách báo, internet, anh chị đi trước đã tìm tòi, nghiên cứu đúc kết kinh nghiệm làm tài liệu để em có thể tham khảo trong quá trình thực hiện đề tài.

Sau cùng tôi xin cảm ơn các bạn cùng nhóm 3 lớp NT113.O12 đã tận tình giúp đỡ, hỗ trợ cho tôi thực hiện tiểu luận này.

**HẾT**