

**Bộ Giáo Dục Và Đào Tạo**  
**Trường Đại Học Ngoại Ngữ - Tin Học Thành Phố Hồ Chí Minh**  
**Khoa Công Nghệ Thông Tin**



**ĐỒ ÁN MÔN HỌC: ĐỒ ÁN MẠNG**  
**ĐỀ TÀI: Xây dựng hệ thống mạng cho Viện Giáo Dục Quốc Tế**  
**HUFLIT**

**GVHD: Đỗ Phi Hưng**

**SV: Trần Ngọc Vinh – 21DH113413**

**SV: Nguyễn Hoàng Phúc – 21DH114014**

**SV: Lê Thành Ân – 21DH112304**

**TP. HỒ CHÍ MINH, 2023**

[illegible]

## LỜI MỞ ĐẦU

Ngày nay, việc ứng dụng công nghệ thông tin đã trở nên phổ biến trong hầu hết mọi cơ quan, doanh nghiệp, trường học đặc biệt là việc áp dụng các giải pháp tin học trong công tác quản lý hoặc để xây dựng những hệ thống phục vụ cho một mục đích nào đó. Với sự phát triển vượt bậc của công nghệ ngày một được đưa vào đời sống của chúng ta nhiều hơn, có thể nói rằng hầu hết mọi công việc, tác vụ hoặc giải trí đã và đang ngày một được gói gọn trong những thiết bị sử dụng hằng ngày.

Công nghệ thông tin trở thành một ngành học, một lĩnh vực không thể thiếu để áp dụng vào nhiều lĩnh vực khác liên quan đến mọi ngành nghề, giúp cho đời sống của chúng ta ngày một dễ dàng, tiện lợi và nhanh chóng hơn. Tuy rằng công việc tự học của học sinh, sinh viên trong lĩnh vực này là vô cùng quan trọng nhưng như thế vẫn là chưa đủ. Việc kết hợp yếu tố giảng dạy từ những giáo viên và người khác thì tốc độ tiếp tục và áp dụng kiến thức của chúng ta sẽ được tăng lên rất nhiều, giúp chúng ta có tính tư duy, vận dụng, tính sáng tạo cũng như kế thừa để phát huy những ưu điểm của người giảng dạy. Bởi vì những yếu tố ấy, để bắt kịp với tốc độ phát triển của xã hội, những kiến thức có được nhờ việc đi học đầy đủ trên giảng đường là vô cùng quan trọng đối với chúng em.

## LỜI CẢM ƠN

Trong thời gian làm đề án bộ môn Đồ Án Mạng, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành cảm ơn thầy Đỗ Phi Hưng - giảng viên Bộ môn Đồ Án Mạng của trường đại học Ngoại Ngữ - Tin Học (HUFLIT) người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm khoá luận.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường nói chung, các thầy cô của chuyên ngành An Ninh Mạng thuộc Công Nghệ Thông Tin nói riêng đã dạy dỗ cho em kiến thức về các môn đại cương cũng như các môn chuyên ngành, giúp em có được cơ sở lý thuyết vững vàng và tạo điều kiện giúp đỡ em trong suốt quá trình học tập.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành khoá luận tốt nghiệp.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế của một học viên, luận văn này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để tôi có điều kiện bổ sung, nâng cao ý thức của mình, phục vụ tốt hơn công tác thực tế sau này.

# MỤC LỤC

<b>CHƯƠNG I: MÔ TẢ ĐỒ ÁN .....</b>	<b>9</b>
------------------------------------	----------

<b>CHƯƠNG II: CƠ SỞ LÝ THUYẾT .....</b>	<b>11</b>
---	-----------

<b>1. Hệ điều hành mạng (NOS):.....</b>	<b>11</b>
---	-----------

<b>1.1/ Đánh giá các loại NOS.....</b>	<b>11</b>
--	-----------

a/ So sánh và lựa chọn các loại NOS:.....	11
---	----

b/ Lựa chọn NOS phù hợp với dự án: .....	13
--	----

c/ Các dịch vụ mạng cần triển khai (Network services: DHCP, DNS, Domain Controller ...).....	14
--	----

<b>1.2/ Khả năng dự phòng, phục hồi hệ thống hoạt động liên tục .....</b>	<b>16</b>
---	-----------

a/ Lưu trữ đám mây (Cloud Storage):.....	16
--	----

b/ Lưu trữ trên thiết bị mạng (NAS): .....	18
--	----

c/ Lưu trữ trực tiếp (DAS):.....	20
----------------------------------	----

d/ Các kiểu RAID : .....	21
--------------------------	----

e/ Các loại kiểu Back-up: .....	25
---------------------------------	----

<b>1.4/ Các dịch vụ tường lửa : .....</b>	<b>28</b>
---	-----------

a/ Tường lửa ứng dụng (Application Firewall):.....	29
--	----

b/ Tường lửa gói tin (Packet-filtering Firewall): .....	30
---	----

c/ Tường lửa kết nối (Stateful Firewall): .....	32
---	----

<b>1.5/ Các hệ thống phát hiện xâm nhập : .....</b>	<b>34</b>
---	-----------

a/ Hệ thống phát hiện xâm nhập dựa trên chữ ký (Signature-based IDS):.....	34
--	----

b/ Hệ thống phát hiện xâm nhập dựa trên hành vi (Behavior-based IDS):.....	36
--	----

<b>1.6/ Các hệ thống giám sát Mạng : .....</b>	<b>39</b>
--	-----------

a/ Nagios:.....	40
-----------------	----

b/ Zabbix: .....	42
------------------	----

c/ PRTG Network Monitor:.....	44
-------------------------------	----

<b>2. Kế hoạch triển khai: .....</b>	<b>46</b>
--------------------------------------	-----------

<b>2.1. Thiết kế hệ thống: .....</b>	<b>46</b>
--------------------------------------	-----------

a/ Chọn các phần mềm cần triển khai và chức năng (File, Backup, Firewall, IDS,...) .....	46
--	----

b/ Yêu cầu thiết bị: .....	46
----------------------------	----

<b>2.2. Triển khai: .....</b>	<b>47</b>
-------------------------------	-----------

a/ Thiết lập Domain và các máy Client: .....	47
--	----

c/ Logical topology và Physical topology, IP Table: .....	48
---	----

<b>3. Triển Khai .....</b>	<b>51</b>
<b>3.1. Cài đặt môi trường EVE-NG:.....</b>	<b>51</b>
<b>3.2. Cấu hình và test lỗi:.....</b>	<b>52</b>
<b>a/ Phòng máy Server: .....</b>	<b>52</b>
<b>b/ Phòng máy Client: .....</b>	<b>56</b>
<b>3.3. Đánh giá kết quả thực hiện:.....</b>	<b>62</b>
<b>4. Quản trị hệ thống: .....</b>	<b>63</b>
<b>4.1. Đánh giá và lựa chọn network monitoring tool (SNMP, PRTG...): .....</b>	<b>63</b>
<b>a/ Đánh giá và lựa chọn Network Monitoring Tool .....</b>	<b>63</b>
<b>4.2. Các báo cáo nhận được .....</b>	<b>65</b>
 <b>CHƯƠNG III. ĐÁNH GIÁ KẾT QUẢ:.....</b>	 <b>67</b>
 <b>BẢNG PHÂN CÔNG CÔNG VIỆC.....</b>	 <b>69</b>

## DANH MỤC HÌNH ẢNH

Hình 1. Cloud Storage .....	16
Hình 2. Network Attached Storage .....	18
Hình 3. Direct- Attached Storage .....	20
Hình 4. RAID 0 .....	22
Hình 5. RAID 1 .....	23
Hình 6. RAID 5 .....	24
Hình 7. Full Backup .....	26
Hình 8. Incremental Backup.....	27
Hình 9. Differential Backup .....	27
Hình 10. Application Firewall.....	29
Hình 11. Packet-filtering Firewall.....	31
Hình 12. Stateful Firewall .....	32
Hình 13. Infection Detection System .....	34
Hình 14. Signature-based IDS.....	35
Hình 15. Behavior-based IDS .....	37
Hình 16. Network Monitoring System.....	39
Hình 17. Nagios.....	41
Hình 18. Zabbix.....	42
Hình 19. PRTG Network Monitor.....	44
Hình 20. Sơ đồ Logic .....	48
Hình 21. Sơ đồ vật lý.....	49
Hình 22. Cài đặt và test EVE-NG trên VMWare .....	52
Hình 23. Cấu hình của máy chủ Server_DC_DHCP_DNS .....	52
Hình 24. Thông tin về IP đầu tiên và IP đầu cuối của scope1 trong DHCP .....	53
Hình 25. Địa chỉ IP của máy chủ Server_DC_DHCP_DNS .....	53
Hình 26. Ổ đĩa E chứa file lưu trữ gốc để thử nghiệm BackUp dữ liệu.	54

Hình 27. Thông tin của ổ cứng E về lần BackUp tiếp theo .....	54
Hình 28. Thông tin của ổ cứng F – nơi lưu trữ những dữ liệu sẽ được BackUp bởi dữ liệu từ ổ cứng E.....	55
Hình 29. Thông tin về PC tầng trệt đã tham gia vào domain của máy chủ Server_DC_DHCP_DNS .....	56
Hình 30. Địa chỉ IP của máy và test ping sang domain của máy chủ Server_DC_DHCP_DNS .....	56
Hình 31. Thông tin về PC tầng 1 đã tham gia vào domain của máy chủ Server_DC_DHCP_DNS .....	57
Hình 32. Địa chỉ IP của máy và test ping sang domain của máy chủ Server_DC_DHCP_DNS .....	57
Hình 33. Thông tin về PC tầng 2 đã tham gia vào domain của máy chủ Server_DC_DHCP_DNS .....	58
Hình 34. Địa chỉ IP của máy và test ping sang domain của máy chủ Server_DC_DHCP_DNS .....	58
Hình 35. Thông tin về PC tầng 3 đã tham gia vào domain của máy chủ Server_DC_DHCP_DNS .....	59
Hình 36. Địa chỉ IP của máy và test ping sang domain của máy chủ Server_DC_DHCP_DNS .....	59
Hình 37. Thông tin về các port có trong sơ đồ hệ thống mạng của EVE-NG .....	60
Hình 38. Sử dụng port mạng 1 làm địa chỉ IP Static để chỉnh sửa tường lửa trực tiếp trên trình duyệt web .....	61
Hình 39. Giao diện tùy chỉnh các chế độ của tường lửa sau khi cấu hình thành công .....	61



## **CHƯƠNG I: MÔ TẢ ĐỒ ÁN**

Bạn là kỹ sư Network của Công ty Hudo, chuyên các giải pháp Mạng công nghệ cao, có các chi nhánh ở các thành phố HCM, HN, DN, CT.

Công ty vừa có hợp đồng triển khai mạng cho Viện Giáo Dục Quốc Tế HUFLIT.  
Cụ thể như sau:

Nhân sự: 400 sinh viên, 30 giảng viên, 20 nhân viên marketing và giáo vụ, 5 quản lý cao cấp bao gồm giám đốc chương trình và quản lý đào tạo, 3 nhân viên quản trị Mạng.

Thiết bị: 60 máy tính cho phòng Lab, 35 máy tính cho nhân viên, 3 máy in, chưa tính số lượng Server.

Tòa nhà: gồm 3 tầng, máy tính và máy in đặt ở tầng trệt, ngoại trừ phòng thực hành IT: 1 phòng ở tầng 1 và 1 phòng khác ở tầng 2 và tầng 3.

=> Viện Giáo Dục yêu cầu triển khai hệ thống Mạng đáp ứng số người dùng như trên, Lưu trữ tập trung, có khả năng Backup và Restore dữ liệu, Phủ sóng Wifi toàn bộ 3 tầng, có hệ thống tường lửa bảo mật, phát hiện xâm nhập, giám sát hệ thống Mạng.

## CHƯƠNG II: CƠ SỞ LÝ THUYẾT

### 1. Hệ điều hành mạng (NOS):

Hệ điều hành mạng (NOS) là hệ điều hành trên máy tính, thiết kế dùng để hỗ trợ máy tính cá nhân, máy trạm và các thiết bị cũ hơn có thể kết nối được với mạng LAN hay mạng cục bộ. Sau hệ điều hành có một phần mềm, cho phép các thiết bị giao tiếp và thực hiện chức năng chia sẻ tài nguyên.

Phần cứng sử dụng NOS sẽ bao gồm máy in, máy tính cá nhân, máy chủ và file server (máy chủ tập tin) với mạng LAN có thể kết nối chúng lại với nhau. NOS cũng sẽ là nhà cung cấp dịch vụ, hỗ trợ yêu cầu đầu vào khi có nhiều người dùng cùng lúc. Vì các phiên bản trước của hệ điều hành NOS không thiết kế để sử dụng mạng nên việc sử dụng hệ điều hành sẽ là giải pháp thích hợp nhất cho máy tính của một người dùng.

#### 1.1/ Đánh giá các loại NOS

##### a/ So sánh và lựa chọn các loại NOS:

Giao diện người dùng (User Interface):

- Windows: Có giao diện người dùng đa dạng từ Windows 7, Windows 8, đến Windows 10 với môi trường người dùng đồ họa. Windows 11 cũng đã được giới thiệu.
- Linux: Giao diện người dùng có thể đa dạng, tùy thuộc vào phiên bản distro và môi trường đồ họa (GNOME, KDE, Xfce, vv.).
- macOS: Có giao diện người dùng đặc biệt và hiện đại, được thiết kế bởi Apple.

Khả năng tùy chỉnh (Customization):

- Windows: Cho phép tùy chỉnh đáng kể với nhiều ứng dụng và giao diện người dùng bên ngoài.
- Linux: Linh hoạt và tùy chỉnh cao với sự linh hoạt của hệ điều hành mã nguồn mở, cho phép người dùng điều chỉnh hầu hết mọi thứ.
- macOS: Có một số tùy chỉnh, nhưng Apple giới hạn để duy trì trải nghiệm người dùng thống nhất.

#### Ứng dụng và tương thích phần cứng:

- Windows: Đa dạng ứng dụng và tương thích rộng rãi với nhiều loại phần cứng.
- Linux: Có sẵn nhiều ứng dụng mã nguồn mở, nhưng cần nỗ lực hơn để cài đặt và tương thích phần cứng.
- macOS: Hỗ trợ nhiều ứng dụng chất lượng cao, nhưng giới hạn về phần cứng và tương thích.

#### An ninh và ổn định:

- Windows: An ninh đã cải thiện trong các phiên bản gần đây, nhưng còn tồn tại các vấn đề bảo mật. Stabilitiy tốt nhưng cần cập nhật thường xuyên.
- Linux: An ninh cao hơn do tính mở mã nguồn và cộng đồng quan tâm. Stabilitiy tùy thuộc vào distro, nhưng nói chung tốt.
- macOS: Được thiết kế với kiến trúc an toàn và ổn định, nhưng cũng cần cập nhật định kỳ.

#### Giá cả và giấy phép:

- Windows: Có giá bán và phải mua giấy phép. Có phiên bản miễn phí như Windows 10 Home.
- Linux: Miễn phí và mã nguồn mở. Không cần mua giấy phép.

- macOS: Miễn phí cho các máy Mac mới mua, nhưng không chạy được trên phần lớn các máy tính cá nhân.

Hỗ trợ cộng đồng và tài liệu:

- Windows: Có một cộng đồng lớn và nhiều tài liệu hướng dẫn.
- Linux: Có cộng đồng lớn, và tài liệu hướng dẫn phong phú nhưng phụ thuộc vào distro.
- macOS: Hỗ trợ từ Apple và cộng đồng sáng tạo nhưng ít phong phú hơn.

Hiệu suất và tài nguyên hệ thống:

- Windows: Yêu cầu tài nguyên hệ thống cao hơn so với Linux và macOS.
- Linux: Có thể được tùy chỉnh để chạy trên nhiều loại phần cứng và có thể tiết kiệm tài nguyên.
- macOS: Hiệu suất cao và tối ưu cho máy Mac, nhưng có thể không tận dụng tốt trên phần cứng không phải của Apple

## **b/ Lựa chọn NOS phù hợp với dự án:**

Chúng em quyết định chọn hệ điều hành Windows để triển khai đồ án vì những lý do sau đây:

- Hỗ trợ ứng dụng phong phú: Windows có một hệ sinh thái phong phú của ứng dụng và phần mềm, đặc biệt là trong lĩnh vực văn phòng như Microsoft Office. Điều này có nghĩa là bạn có thể dễ dàng truy cập và sử dụng các ứng dụng cần thiết cho đồ án của mình.
- Tương thích phần cứng: Windows thường tương thích với nhiều loại phần cứng khác nhau. Nếu bạn cần sử dụng phần cứng đặc biệt cho đồ án (ví dụ: thiết bị đo lường, máy in, hoặc phần mềm độc quyền chỉ chạy trên

Windows), thì việc sử dụng Windows có thể giúp bạn tránh các vấn đề tương thích.

- Giao diện người dùng dễ sử dụng: Windows thường được đánh giá là dễ sử dụng với giao diện người dùng đồ họa trực quan. Điều này có thể giúp bạn tiết kiệm thời gian và tập trung vào công việc thay vì phải mất nhiều thời gian để tìm hiểu về hệ thống.
- Hỗ trợ tài liệu và cộng đồng lớn: Windows có một cộng đồng lớn, và có nhiều tài liệu hướng dẫn trực tuyến và sách về việc sử dụng và triển khai các phần mềm và dự án trên hệ điều hành này. Điều này có thể giúp bạn giải quyết vấn đề nhanh chóng và dễ dàng.
- Hỗ trợ cho việc phát triển ứng dụng: Nếu bạn cần phát triển phần mềm hoặc ứng dụng cho đồ án, Windows cung cấp môi trường phát triển phong phú với nhiều công cụ và tài liệu hỗ trợ.

### **c/ Các dịch vụ mạng cần triển khai (Network services: DHCP, DNS, Domain Controller...)**

Dịch vụ mạng DHCP (Dynamic Host Configuration Protocol) là một dịch vụ quan trọng trong mạng máy tính, được sử dụng để tự động cấu hình địa chỉ IP và thông tin mạng khác cho các thiết bị trong mạng. Dịch vụ DHCP giúp đơn giản hóa quá trình quản lý và triển khai mạng, đặc biệt là trong các môi trường lớn.

Dịch vụ mạng DNS (Domain Name System) là một dịch vụ quan trọng trong mạng máy tính, được sử dụng để chuyển đổi tên miền (domain names) dễ đọc của các trang web và dịch vụ mạng thành địa chỉ IP, giúp thiết bị trong mạng máy tính có thể tìm thấy và kết nối với các máy chủ và dịch vụ trên internet.

Dịch vụ mạng Domain Controller (DC) là một thành phần quan trọng trong mô hình quản lý và xác thực người dùng và tài nguyên trong một mạng máy tính dựa

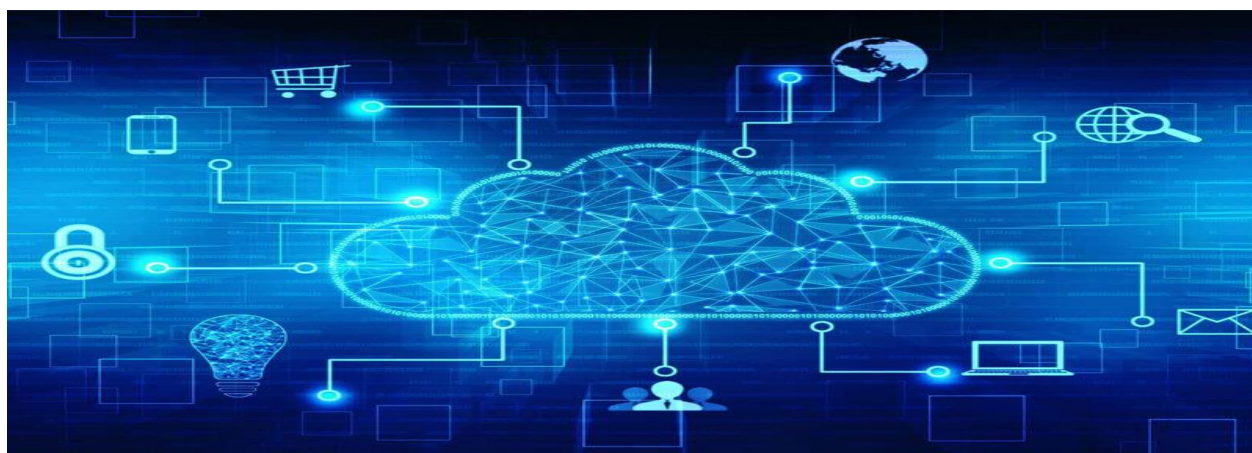
trên Windows. Domain Controller hoạt động trong một mô hình mạng dựa trên Windows, thường được sử dụng trong môi trường doanh nghiệp hoặc tổ chức lớn

## 1.2/ Khả năng dự phòng, phục hồi hệ thống hoạt động liên tục

Hiện nay có nhiều hệ thống lưu trữ tập trung và sau đây là một số ví dụ :

### a/ Lưu trữ đám mây (Cloud Storage):

Lưu trữ đám mây: Đây là phương pháp lưu trữ trên các dịch vụ đám mây như Amazon S3 ,Google Cloud Storage ,Icloud.... Dữ liệu được lưu trữ trên hệ thống máy chủ của nhà cung cấp dịch vụ đám mây và có thể truy cập từ bất kỳ địa điểm nào qua mạng Internet.



*Hình 1. Cloud Storage*

Lưu trữ đám mây (cloud storage) có nhiều ưu điểm và nhược điểm. Dưới đây là một số điểm mạnh và yếu của dịch vụ lưu trữ đám mây:

Ưu điểm:

- **Tiện lợi và dễ sử dụng:** Lưu trữ đám mây cho phép người dùng lưu trữ, truy cập và chia sẻ dữ liệu từ bất kỳ nơi nào chỉ với một kết nối Internet. Điều này giúp tiết kiệm thời gian và công sức so với việc lưu trữ dữ liệu trên các thiết bị cục bộ.
- **Khả năng mở rộng linh hoạt:** Với lưu trữ đám mây, người dùng có thể dễ dàng mở rộng không gian lưu trữ theo nhu cầu. Nếu cần thêm dung lượng,



người dùng có thể tăng cấp bằng cách mua thêm không gian lưu trữ từ nhà cung cấp dịch vụ.

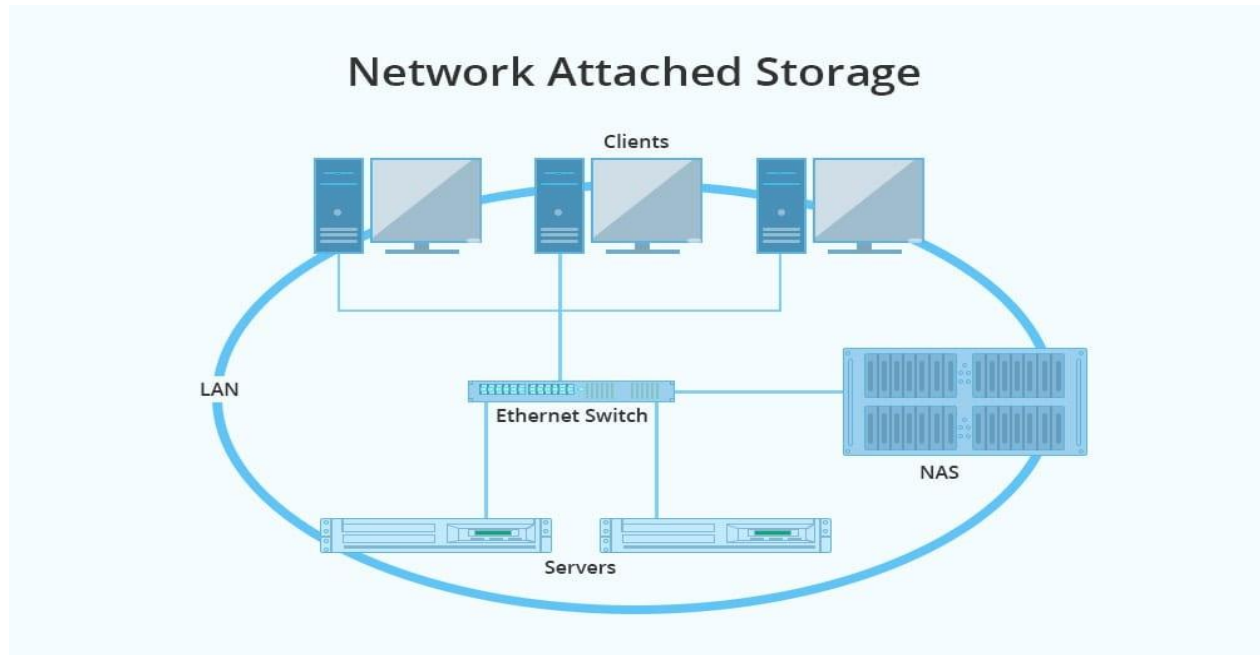
- Bảo mật và sao lưu tự động: Các dịch vụ lưu trữ đám mây thường áp dụng các biện pháp bảo mật mạnh mẽ như mã hóa dữ liệu và chứng chỉ SSL để đảm bảo an toàn cho dữ liệu của người dùng. Hơn nữa, hầu hết các dịch vụ cung cấp tính năng sao lưu tự động, giúp người dùng bảo vệ dữ liệu khỏi mất mát hoặc hỏng hóc.
- Cộng tác dễ dàng: Lưu trữ đám mây cho phép người dùng chia sẻ dữ liệu một cách dễ dàng với người khác và cộng tác trực tuyến trên các tài liệu. Điều này rất hữu ích khi làm việc nhóm hoặc chia sẻ thông tin với đối tác, khách hàng.

Nhược điểm:

- Phụ thuộc vào kết nối Internet: Để truy cập và quản lý dữ liệu trong lưu trữ đám mây, người dùng cần có kết nối Internet ổn định. Nếu mất kết nối hoặc tốc độ Internet chậm, việc truy cập và làm việc với dữ liệu có thể gặp khó khăn.
- Bảo mật dựa vào nhà cung cấp dịch vụ: Dữ liệu được lưu trữ trên đám mây phụ thuộc vào các nhà cung cấp dịch vụ. Mặc dù nhiều nhà cung cấp áp dụng các biện pháp bảo mật, nhưng người dùng vẫn phải tin tưởng rằng dữ liệu của họ được bảo mật và không bị truy cập trái phép.
- Chi phí: Một số dịch vụ lưu trữ đám mây miễn phí có giới hạn dung lượng. Để có nhiều dung lượng hơn hoặc tính năng cao cấp hơn, người dùng có thể phải trả phí hàng tháng hoặc hàng năm. Việc chi trả liên tục này có thể tạo ra chi phí dài hạn.
- Quản lý dữ liệu: Số lượng dữ liệu trong lưu trữ đám mây có thể tăng nhanh chóng

## **b/ Lưu trữ trên thiết bị mạng (NAS):**

Network Attached Storage (NAS) là một loại hệ thống lưu trữ tập trung nơi dữ liệu được lưu trữ và quản lý trong các thiết bị lưu trữ đặt trên mạng. NAS cho phép người dùng kết nối và truy cập vào dữ liệu từ xa thông qua mạng LAN hoặc Internet.



*Hình 2. Network Attached Storage*

Một số ưu điểm của Network Attached Storage bao gồm:

- Dễ dàng sử dụng: NAS cung cấp giao diện đơn giản, rõ ràng và dễ sử dụng cho việc quản lý và truy cập dữ liệu. Người dùng có thể truy cập và chia sẻ dữ liệu một cách thuận tiện thông qua giao diện web hoặc ứng dụng di động.
- Chia sẻ dữ liệu: NAS cho phép nhiều người dùng cùng truy cập vào dữ liệu từ xa. Nó hỗ trợ việc chia sẻ file, thư mục và tài nguyên mạng, giúp tăng cường sự cộng tác trong tổ chức.
- Dung lượng mở rộng linh hoạt: NAS có khả năng mở rộng dung lượng lưu trữ bằng cách thêm ổ cứng hoặc dùng các hình thức RAID (Redundant Array

of Independent Disks). Điều này cho phép người dùng mở rộng không gian lưu trữ theo nhu cầu của họ.

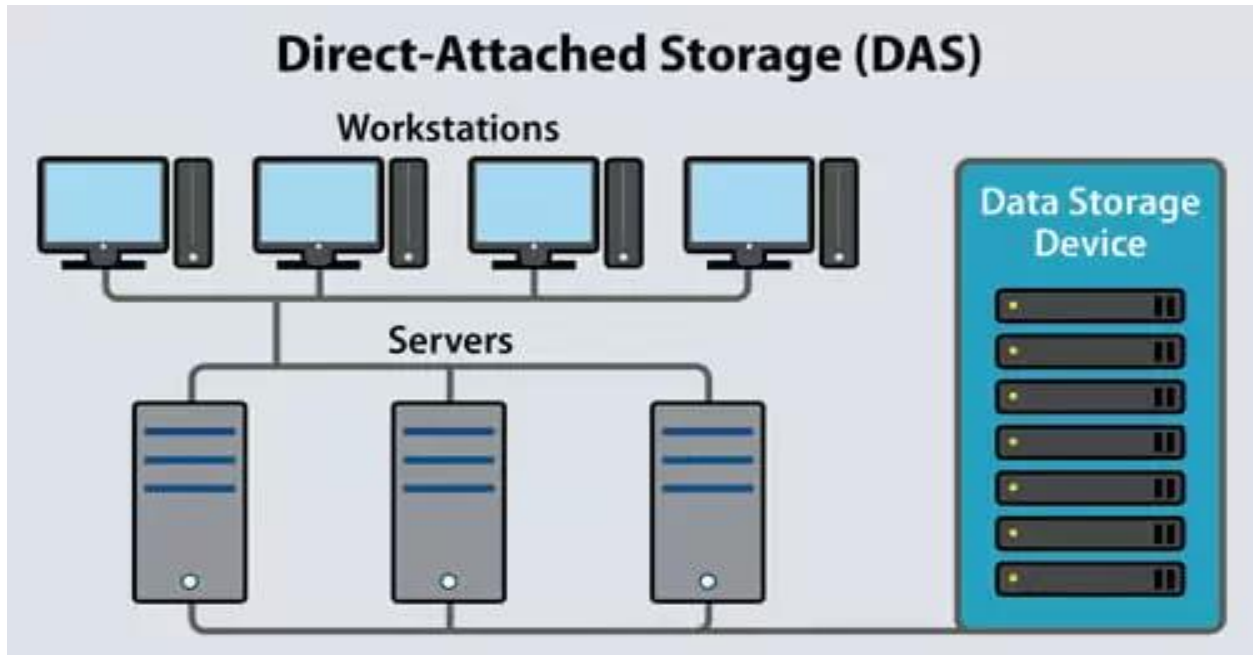
- Bảo mật dữ liệu: NAS hỗ trợ các tính năng bảo mật như mã hóa dữ liệu, quản lý quyền truy cập, và sao lưu dữ liệu định kỳ để đảm bảo an toàn cho dữ liệu.

Tuy nhiên, NAS cũng có một số hạn chế như:

- Hiệu suất hạn chế: NAS thường không có hiệu suất cao như các hệ thống lưu trữ khác như Storage Area Network (SAN). Điều này có thể ảnh hưởng đến tốc độ truy cập và xử lý dữ liệu trong một số trường hợp sử dụng tải lớn.
- Giới hạn trong việc mở rộng quyền truy cập: NAS có giới hạn về quyền truy cập và kiểm soát người dùng. Trong môi trường doanh nghiệp lớn hoặc yêu cầu bảo mật cao, hệ thống quản lý quyền truy cập phức tạp hơn có thể là lựa chọn tốt hơn.
- Network Attached Storage (NAS) thích hợp cho việc lưu trữ và chia sẻ dữ liệu trong môi trường gia đình, doanh nghiệp nhỏ hoặc các nhóm làm việc nhỏ. Nó cung cấp sự đơn giản, linh hoạt và tiện ích trong việc quản lý dữ liệu qua mạng.

### c/ Lưu trữ trực tiếp (DAS):

DAS (Direct-Attached Storage) là một hình thức lưu trữ dữ liệu trong đó các ổ cứng được kết nối trực tiếp với một máy tính hoặc máy chủ thông qua giao diện như SATA, SCSI hoặc USB. DAS đơn giản và dễ sử dụng, không yêu cầu mạng hoặc thiết bị trung gian.



*Hình 3. Direct- Attached Storage*

Các đặc điểm chính của DAS bao gồm:

- Hiệu suất cao: Vì DAS kết nối trực tiếp với máy tính hoặc máy chủ, nó cung cấp hiệu suất truy xuất dữ liệu nhanh và đáng tin cậy.
- Đơn giản và chi phí thấp: DAS không yêu cầu cơ sở hạ tầng mạng riêng và không có khả năng chia sẻ dữ liệu cho nhiều người dùng. Do đó, nó thường rẻ hơn so với các giải pháp lưu trữ mạng khác như NAS hoặc SAN.
- Dễ dàng mở rộng: DAS cho phép dễ dàng mở rộng dung lượng lưu trữ bằng cách thêm ổ cứng mới vào hệ thống. Việc này giúp người dùng linh hoạt trong việc mở rộng không gian lưu trữ theo nhu cầu của họ.

Tuy nhiên, DAS cũng có một số hạn chế:

- Hạn chế trong việc chia sẻ: Vì DAS không phải là một hệ thống lưu trữ mạng, nó không cho phép chia sẻ dữ liệu với nhiều người dùng đồng thời như NAS hoặc SAN.
- Quản lý phức tạp: Với nhiều hệ thống DAS, quản lý và kiểm soát quyền truy cập dữ liệu có thể trở nên phức tạp, đặc biệt khi hệ thống mở rộng. DAS thích hợp cho các ứng dụng cá nhân hoặc nhóm làm việc nhỏ có nhu cầu lưu trữ dữ liệu riêng tư và không cần chia sẻ rộng rãi. Nó cung cấp hiệu suất cao và giải pháp lưu trữ đơn giản và chi phí thấp. Tuy nhiên, nếu bạn cần chia sẻ dữ liệu cho nhiều người dùng hoặc có yêu cầu mở rộng phức tạp hơn, các giải pháp lưu trữ mạng khác như NAS hoặc SAN có thể phù hợp hơn.

#### **d/ Các kiểu RAID :**

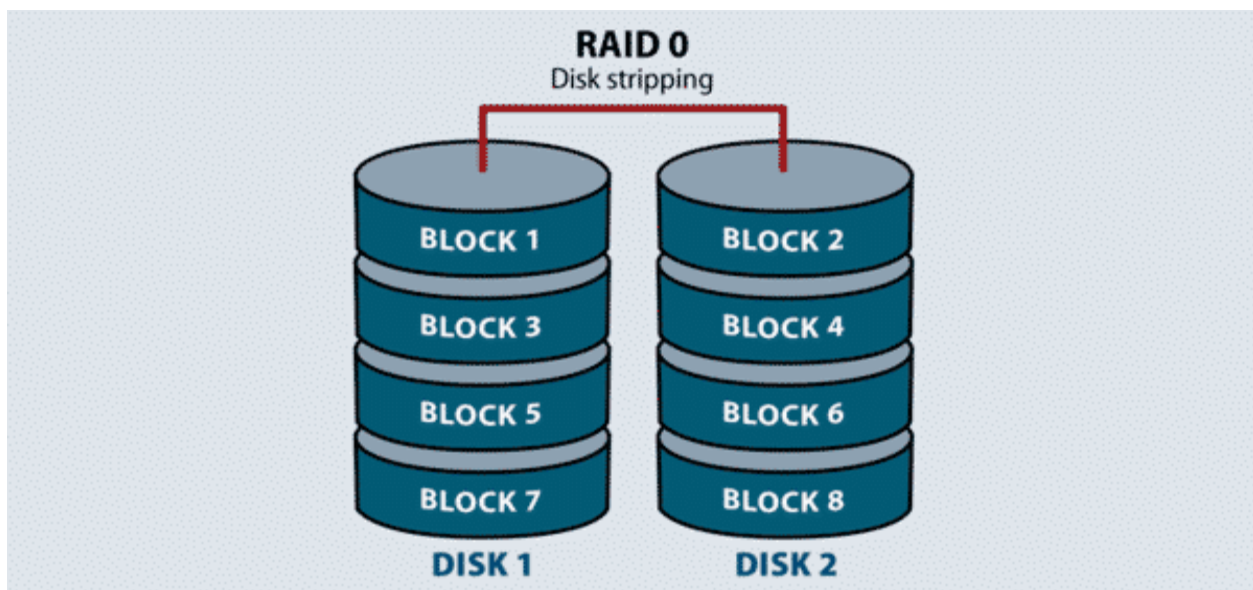
RAID là viết tắt của Redundant Array of Independent Disks, được sử dụng ban đầu như một giải pháp bảo vệ dữ liệu bằng cách cho phép ghi dữ liệu lên nhiều đĩa cứng cùng lúc. Sau đó, RAID đã phát triển nhiều biến thể khác nhau để đảm bảo an toàn và tăng tốc độ truy xuất dữ liệu từ đĩa cứng. Dưới đây là năm loại RAID phổ biến mà chúng ta có thể tìm hiểu.

Một số đặc tính của RAID:

- RAID nên sử dụng các ổ cứng có dung lượng bằng nhau.
- Việc sử dụng RAID sẽ tốn nhiều ổ cứng hơn so với không sử dụng, nhưng đổi lại dữ liệu sẽ được bảo vệ tốt hơn.
- RAID có thể hoạt động trên nhiều hệ điều hành như Windows 98, Windows 2000, Windows XP, Windows 10, Windows Server 2016, MAC OS X, Linux,...

Các loại RAID điển hình như là:

RAID 0: Là loại RAID khá phổ biến và được nhiều người sử dụng hiện nay. Do có khả năng nâng cao hiệu suất tốc độ đọc ghi trao đổi dữ liệu của ổ cứng. Để tiến hành setup Raid 0 thì server cần tối thiểu 2 ổ đĩa (Disk 0, Disk 1). RAID 0 sẽ lưu trữ như sau. Giả sử bạn có 1 file A dung lượng 100MB. Khi tiến hành lưu trữ thay vì file A sẽ được lưu vào 1 ổ cứng duy nhất. Raid 0 sẽ giúp lưu vào 2 ổ đĩa disk 0, disk 1 mỗi ổ 50MB (Striping) giúp giảm thời gian đọc ghi xuống 1 nửa so với lý thuyết.



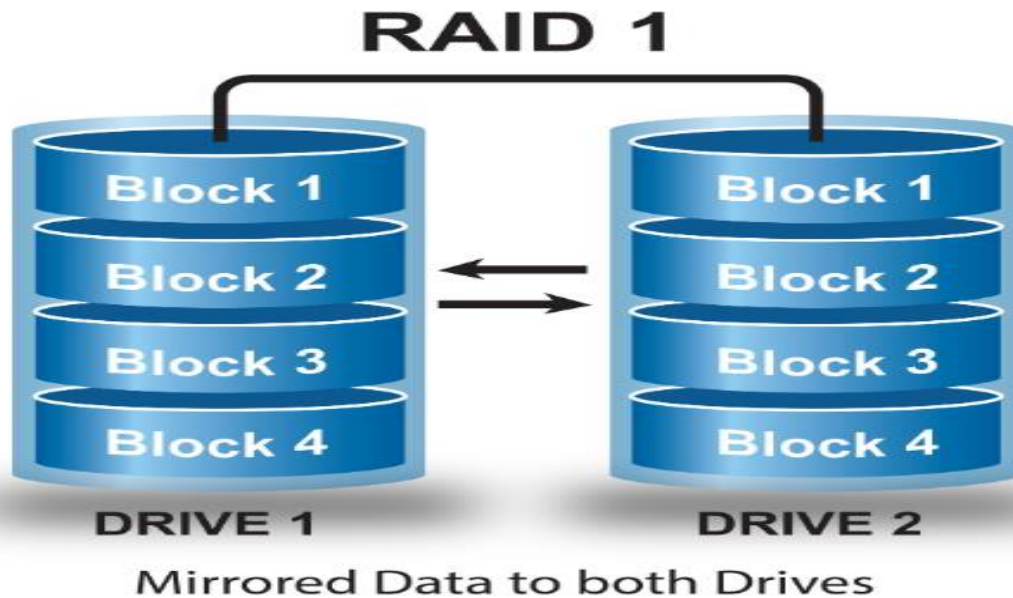
*Hình 4. RAID 0*

Ưu điểm: Tốc độ đọc ghi nhanh (gấp đôi bình thường theo lý thuyết).

Nhược điểm: Tiềm ẩn rủi ro về dữ liệu. Lý do dữ liệu được chia đôi lưu trên 2 ổ đĩa. Trường hợp 1 trong 2 ổ đĩa bị hỏng thì nguy cơ mất dữ liệu rất cao. Về ổ cứng yêu cầu phải 2 ổ cùng dung lượng, nếu 2 ổ khác dung lượng thì lấy ổ thấp nhất.

RAID 1: Là loại RAID cơ bản được sử dụng khá nhiều hiện nay do khả năng đạt an toàn về dữ liệu. Để tiến hành setup RAID 1 thì cũng giống như RAID 0, server

cần tối thiểu 2 ổ cứng để lưu trữ. Không giống như Raid 0, Raid 1 đảm bảo an toàn hơn về dữ liệu do dữ liệu được ghi vào 2 ổ giống hệt nhau (Mirroring).

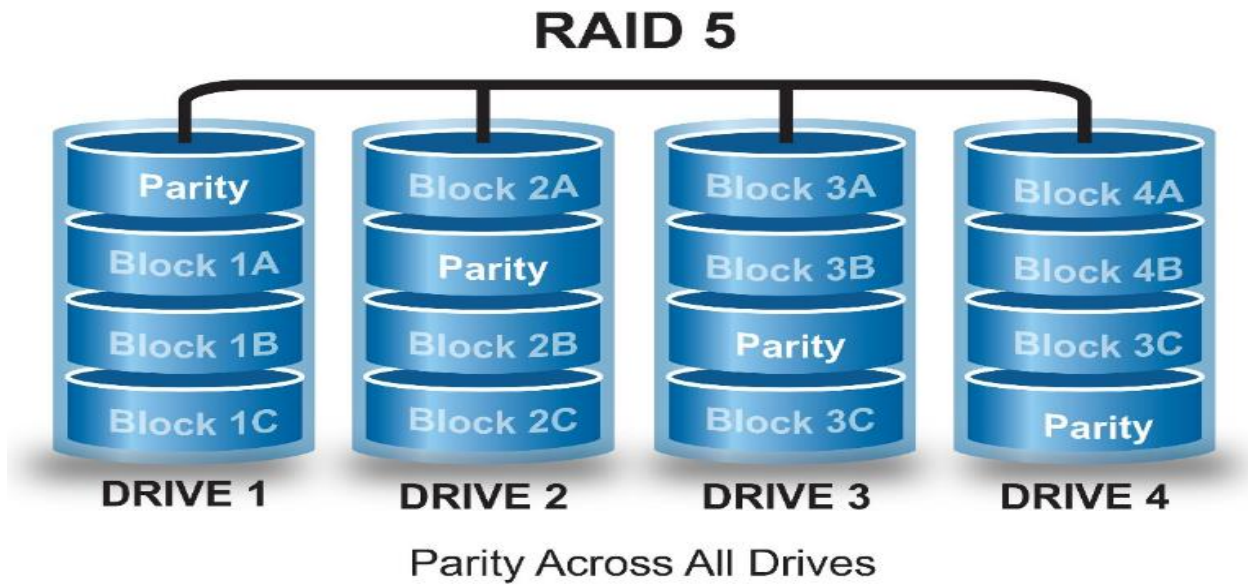


*Hình 5. RAID 1*

Ưu điểm: An toàn về dữ liệu, trường hợp 1 trong 2 ổ đĩa bị hỏng thì dữ liệu vẫn có khả năng đáp ứng dịch vụ.

Nhược điểm: Hiệu suất không cao, Nâng cao chi phí (giả sử khách hàng sử dụng 2 ổ cứng 500GB. Khi sử dụng Raid 1 thì dung lượng lưu trữ có thể sử dụng chỉ được 500GB). Về ổ cứng yêu cầu phải 2 ổ cùng dung lượng, nếu 2 ổ khác dung lượng thì lấy ổ thấp nhất.

RAID 5: Là một loại RAID được phổ biến khá rộng rãi. Nguyên tắc cơ bản của RAID 5 cũng gần giống với 2 loại raid lưu trữ truyền thống là RAID 1 và RAID 0. Tức là cũng có tách ra lưu trữ các ổ cứng riêng biệt và vẫn có phương án dự phòng khi có sự cố phát sinh đối với 1 ổ cứng bất kì trong cụm. Để setup Raid 5 ta cần tối thiểu 3 ổ cứng.



*Hình 6. RAID 5*

Ưu điểm: Nâng cao hiệu suất, an toàn dữ liệu, tiết kiệm chi phí hơn so với hình thức lưu trữ Raid 10.

Nhược điểm: Chi phí phát sinh thêm 1 ổ so với hình thức lưu trữ thông thường.



### **e/ Các loại kiểu Back-up:**

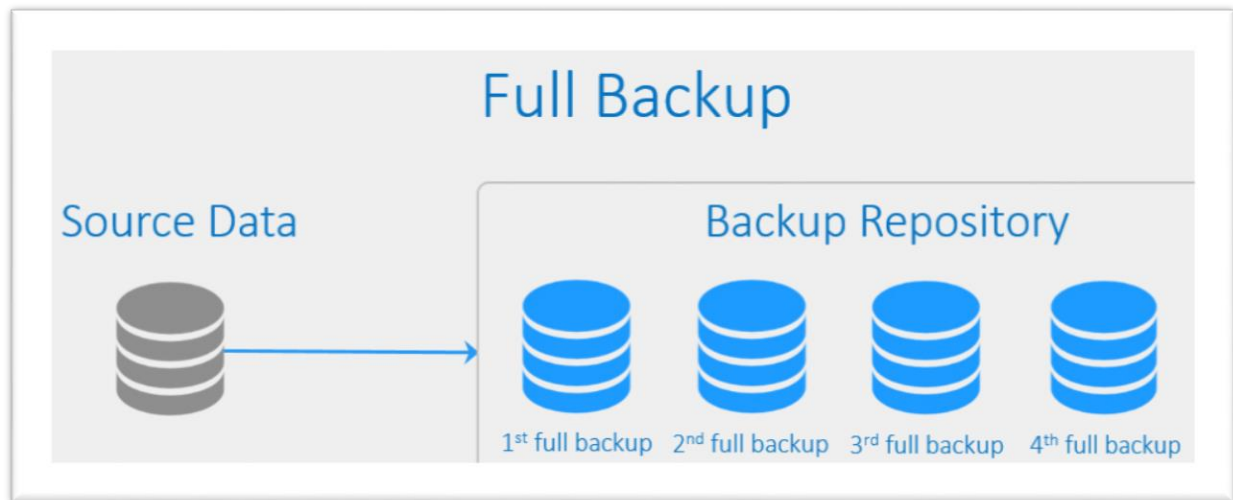
Back-up hay (sao lưu) dữ liệu là hình thức bạn copy lại toàn bộ đoạn dữ liệu trong máy tính, máy chủ, server... hay bất cứ thiết bị nào có khả năng nhớ và lưu trữ của bạn và lưu trữ nó ở một hoặc nhiều thiết bị có chức năng lưu trữ khác để làm dữ liệu dự phòng. Khi thiết bị nhớ chính của chúng ta bị mất dữ liệu trong khi hoạt động do hư hỏng, hacker, sập nguồn.... Chúng ta vẫn còn dữ liệu để restore lại, hạn chế thiệt hại và mất mát về nguồn tài nguyên dữ liệu này.

Việc sao lưu dữ liệu và vô cùng quan trọng vì dữ liệu là tài sản quý giá đối với mỗi cá nhân và mỗi doanh nghiệp. Nếu bạn không muốn một hôm đẹp trời nào đó toàn bộ dữ liệu của mình lưu trên máy tính cá nhân, máy tính bảng hay thậm chí điện thoại di động bốc hơi mất vì máy bị hỏng hay mất trộm thì bạn cần phải back-up dữ liệu. Đặc biệt, các hệ thống máy chủ ngày nay của các công ty doanh nghiệp là một ví dụ điển hình cho câu trả lời vì sao chúng ta cần backup dữ liệu. Trong quá trình thực hiện vận hành lưu trữ cho toàn bộ hệ thống kinh doanh đồ sộ cho các doanh nghiệp. Các loại máy chủ là nơi tổng hợp vô số các loại dữ liệu bảo mật cực kỳ quan trọng. Chỉ cần một sự cố xảy ra như ổ cứng máy chủ bị hư, sập nguồn gây lỗi mất dữ liệu, virus mã hóa toàn bộ thì dữ liệu của chúng ta có nguy cơ bị mất trắng. Lúc này, biện pháp duy nhất để cứu vãn tình thế là chúng ta phải phục hồi lại dữ liệu từ nguồn backup (sao lưu) trước đó.

Các loại Back-up điển hình như

- Full Backup – Sao lưu toàn bộ: Sao lưu toàn bộ tạo ra một bản sao toàn bộ dữ liệu cũ lên một thiết bị lưu trữ mới, chẳng hạn như đĩa cứng. Ưu điểm của cách này là lưu trữ toàn bộ dữ liệu của hệ thống lên một thiết bị duy nhất. Dễ tìm kiếm và sử dụng. Việc khôi phục dữ liệu cũng dễ dàng và ít tốn thời gian hơn. Nhược điểm: Bởi vì sao lưu một lượng lớn dữ liệu nên thời gian sao chép dữ liệu rất lâu. Đòi hỏi không gian lưu trữ lớn. Việc sao lưu

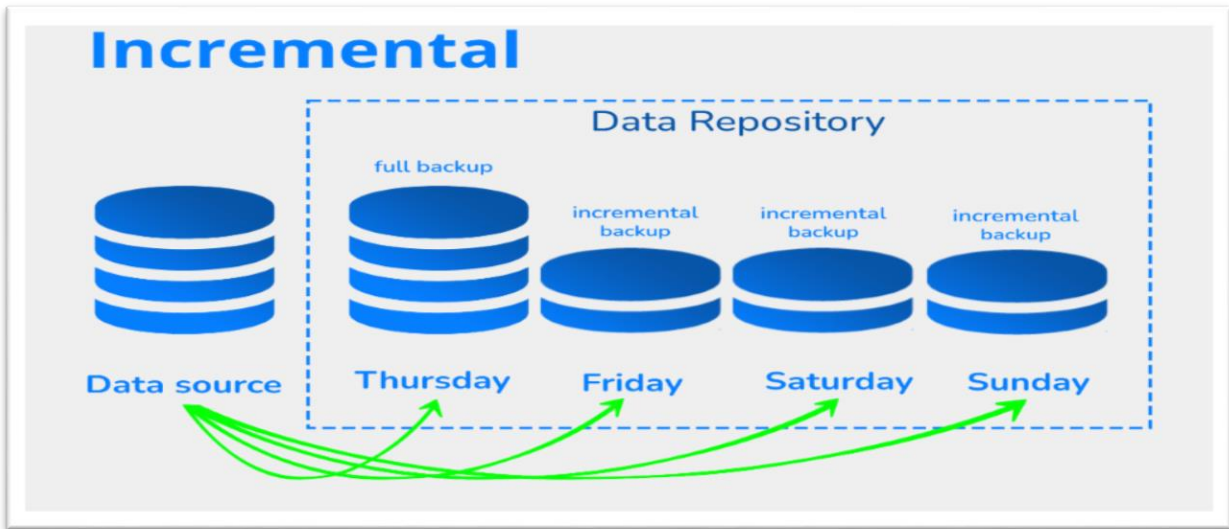
toàn bộ cần thực hiện thường xuyên, định kỳ. Nếu dữ liệu của bạn không có nhiều, có thể tiến hành sao lưu hàng ngày hoặc hàng tuần. Sao lưu toàn bộ đảm bảo an toàn cho những dữ liệu quan trọng của bạn trong trường hợp rủi ro xảy ra.



*Hình 7. Full Backup*

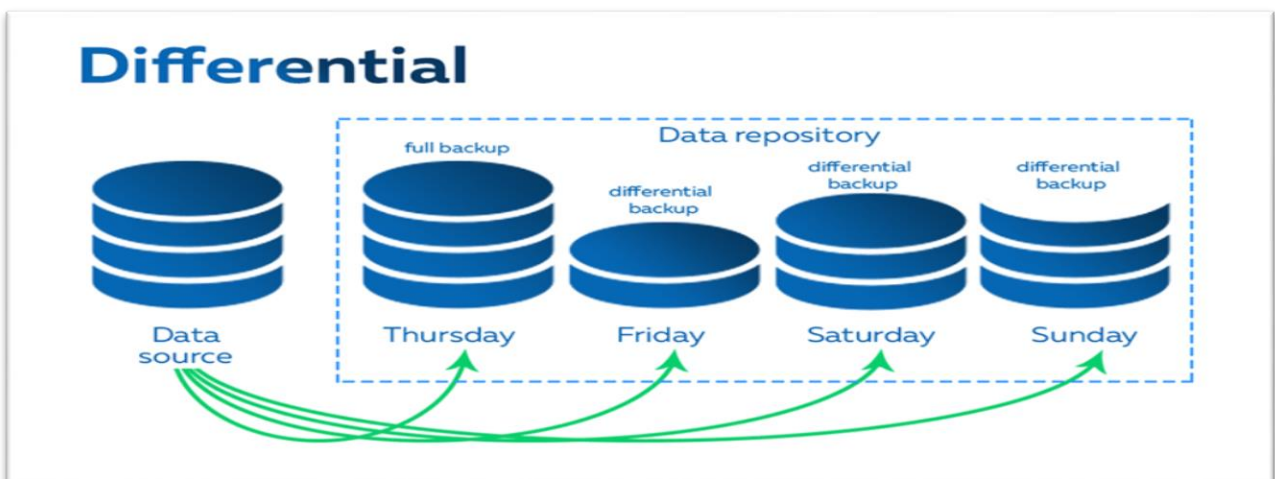
Thông thường, sao lưu toàn bộ được thực hiện cùng với một trong hai phương pháp còn lại : Sao lưu gia tăng và sao lưu khác biệt.

- Sao lưu gia tăng (Incremental Backup): Điểm khác biệt của sao lưu gia tăng với sao lưu dữ liệu toàn bộ là nó chỉ sao lưu lại những dữ liệu được chỉnh sửa cuối cùng của một tệp dữ liệu. Bạn có thể thực hiện rất nhiều chỉnh sửa trên tệp đó và hệ thống chỉ lưu lại những dữ liệu gần nhất. Thông thường, ngày giờ mà các hoạt động sao lưu, sửa đổi xảy ra cũng được ghi chép lại. Bởi vì mỗi lần chỉ sao chép một lượng dữ liệu nhỏ nên tốc độ sao lưu nhanh. Không gian lưu trữ dữ liệu không cần quá lớn.



*Hình 8. Incremental Backup*

- Sao lưu khác biệt (Differential Backup): Cách sao lưu dữ liệu này cũng giống sao lưu gia tăng. Thế nhưng, thay vì chỉ lưu lại dữ liệu của lần thay đổi cuối cùng. Nó sẽ lưu lại toàn bộ dữ liệu của cả những lần sao lưu trước đó. So với sao lưu gia tăng, phương pháp này tốn nhiều không gian lưu trữ dữ liệu hơn. Tuy nhiên, nó vẫn không là gì sao với sao lưu toàn bộ.



*Hình 9. Differential Backup*

#### **1.4/ Các dịch vụ tường lửa :**

Dịch vụ tường lửa (firewall service) là một phần quan trọng của hệ thống bảo mật mạng, đảm bảo an toàn và bảo vệ dữ liệu khỏi các mối đe dọa từ bên ngoài. Dịch vụ tường lửa có thể bao gồm các chức năng và tính năng sau:

- **Quản lý quy tắc truy cập:** Dịch vụ tường lửa cho phép người quản trị xác định và thiết lập các quy tắc để kiểm soát truy cập vào mạng hoặc hệ thống. Các quy tắc này có thể được cấu hình để cho phép hoặc từ chối truy cập dựa trên các thông tin như địa chỉ IP nguồn/đích, cổng và giao thức.
- **Giám sát và ghi nhật ký lưu lượng mạng:** Dịch vụ tường lửa theo dõi và ghi lại lưu lượng mạng đi qua hệ thống để phát hiện và cảnh báo về các hoạt động không mong muốn hay bất thường. Log này có thể hỗ trợ trong việc phân tích sự cố, điều tra và tuân thủ quy định.
- **Bảo vệ chống tấn công mạng:** Dịch vụ tường lửa có thể được cấu hình để chống lại các loại tấn công mạng như DoS (Denial of Service), DDoS (Distributed Denial of Service), SYN flood và ICMP flood. Nó giúp ngăn chặn hoặc giảm thiểu ảnh hưởng của các cuộc tấn công này đến mạng và hệ thống.
- **Kiểm soát ứng dụng và giao thức:** Một số dịch vụ tường lửa cung cấp khả năng kiểm soát và quản lý lưu lượng ứng dụng và giao thức. Chúng có thể xác định và kiểm soát các ứng dụng hoặc giao thức không an toàn hoặc không mong muốn trong mạng.
- **VPN (Virtual Private Network):** Một số dịch vụ tường lửa cung cấp tính năng VPN, cho phép thiết lập kết nối an toàn và riêng tư từ xa vào mạng nội bộ. Điều này giúp bảo vệ thông tin truyền qua mạng công cộng và cho phép người dùng từ xa truy cập vào tài nguyên nội bộ của mạng.

Các dịch vụ tường lửa có thể được triển khai trên phần cứng tường lửa (firewall hardware) hoặc phần mềm tường lửa (firewall software). Chúng có thể được cấu hình, quản lý và giám sát từ một giao diện điều khiển trung tâm để đảm bảo an toàn và hiệu suất của mạng và hệ thống.

Một số dịch vụ tường lửa phổ biến:

**a/ Tường lửa ứng dụng (Application Firewall):**

Tường lửa ứng dụng (Application Firewall) là một loại tường lửa nhằm giám sát và kiểm soát lưu lượng mạng dựa trên các ứng dụng và giao thức cụ thể. Nó tập trung vào việc bảo vệ các ứng dụng mạng khỏi các cuộc tấn công phần mềm độc hại và lỗ hổng bảo mật.



*Hình 10. Application Firewall*

Các tính năng chính của tường lửa ứng dụng bao gồm:

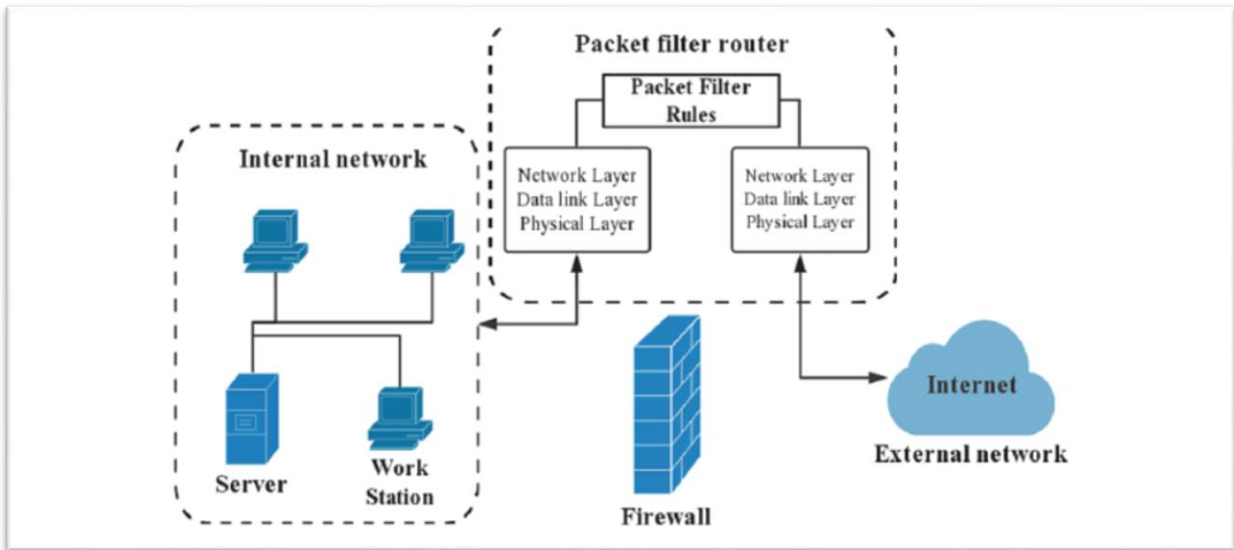
- Phân biệt hoạt động ứng dụng: Tường lửa ứng dụng có hiểu biết về các loại ứng dụng cụ thể được sử dụng trong mạng và theo dõi lưu lượng mạng để xác định hoạt động của từng ứng dụng. Điều này cho phép nó áp dụng các quy tắc kiểm soát truy cập dựa trên các luồng dữ liệu và hoạt động cụ thể của ứng dụng.

- Kiểm tra và ngăn chặn các cuộc tấn công ứng dụng: Tường lửa ứng dụng có khả năng phát hiện và ngăn chặn các cuộc tấn công phần mềm độc hại như SQL injection, cross-site scripting (XSS), remote code execution và các lỗ hổng bảo mật khác liên quan đến ứng dụng. Nó sử dụng các quy tắc và chữ ký để phát hiện các hoạt động không mong muốn và ngăn chặn chúng trước khi gây hại cho hệ thống.
- Quản lý chính sách bảo mật: Tường lửa ứng dụng cho phép người quản trị cấu hình các chính sách bảo mật cho từng ứng dụng, bao gồm quy tắc kiểm soát truy cập, quản lý chứng chỉ SSL/TLS, xác thực người dùng và kiểm soát thông tin nhạy cảm. Điều này giúp tăng cường an ninh và tuân thủ quy định về bảo mật trong môi trường mạng.
- Ghi nhật ký và phân tích: Tường lửa ứng dụng có khả năng ghi lại các sự kiện và lưu lượng mạng đi qua hệ thống. Nhật ký này có thể được sử dụng để phân tích, giám sát và điều tra sự cố bảo mật, cũng như để tuân thủ quy định về báo cáo và tuân thủ quyền riêng tư.

Tường lửa ứng dụng thường được triển khai trong môi trường doanh nghiệp và các hệ thống mạng quan trọng. Nó giúp bảo vệ các ứng dụng mạng khỏi các cuộc tấn công phần mềm độc hại và lỗ hổng bảo mật, đồng thời giám sát và kiểm soát việc sử dụng ứng dụng trong mạng.

#### **b/ Tường lửa gói tin (Packet-filtering Firewall):**

Tường lửa gói tin (Packet-filtering Firewall) là một loại tường lửa mạng hoạt động dựa trên các quy tắc cấu hình để kiểm tra và quyết định xem một gói tin mạng có được chuyển tiếp hay không. Nó là một thành phần quan trọng của hệ thống bảo mật mạng và giúp ngăn chặn các cuộc tấn công từ bên ngoài.



*Hình 11. Packet-filtering Firewall*

Các tính năng chính của tường lửa gói tin bao gồm:

- Kiểm tra thông tin gói tin: Tường lửa gói tin xem xét các thông tin cơ bản như địa chỉ IP nguồn/đích, cổng và giao thức trong gói tin mạng. Dựa trên các quy tắc đã được cấu hình, nó sẽ quyết định xem gói tin được chuyển tiếp hay bị từ chối.
- Quy tắc kiểm soát truy cập: Tường lửa gói tin cho phép người quản trị thiết lập các quy tắc kiểm soát truy cập để xác định loại lưu lượng mạng được phép đi qua. Các quy tắc này có thể được dựa trên địa chỉ IP nguồn/đích, cổng, giao thức hoặc các tiêu chí khác để từ chối hoặc cho phép truy cập.
- Thiết lập một chiều (stateless): Tường lửa gói tin thường được thiết lập dựa trên các quy tắc không có khái niệm về trạng thái kết nối. Nó xem xét từng gói tin cá nhân mà không biết về các gói tin trước đó đã đi qua hay sẽ đi qua.
- Hiệu suất cao: Vì tường lửa gói tin chỉ kiểm tra các thông tin cơ bản trong gói tin mạng, nên nó có thể đạt được hiệu suất cao và xử lý lưu lượng mạng nhanh chóng.

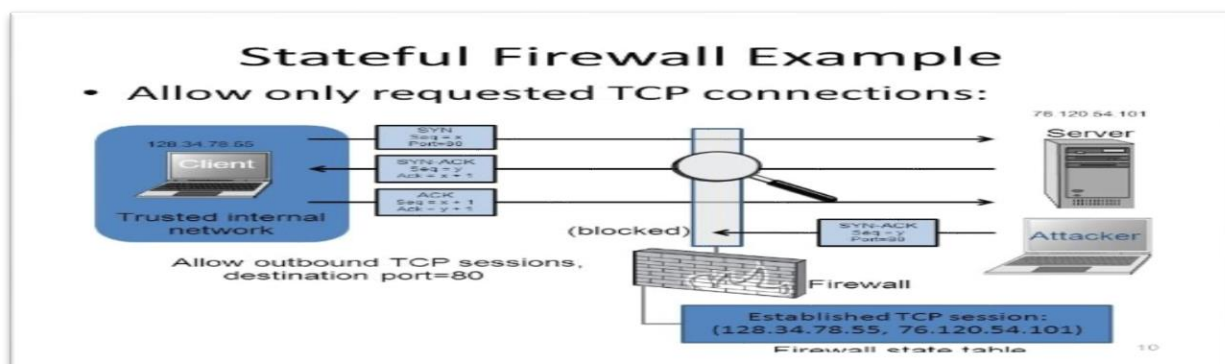
Tuy nhiên, tường lửa gói tin có một số hạn chế:

- Không xác định trạng thái kết nối: Do thiếu khái niệm về trạng thái kết nối, tường lửa gói tin không thể theo dõi trạng thái của các kết nối mạng như TCP/IP. Điều này có thể làm giảm hiệu suất và khả năng kiểm soát truy cập.
- Không xác định ứng dụng: Tường lửa gói tin chỉ xem xét các thông tin cơ bản trong gói tin mạng và không xác định được loại ứng dụng cụ thể đang sử dụng. Điều này làm hạn chế trong việc kiểm soát và bảo vệ các ứng dụng mạng.

Tường lửa gói tin thường được triển khai ở mức cơ bản và là một phần quan trọng của hệ thống bảo mật mạng. Nó giúp ngăn chặn các cuộc tấn công từ bên ngoài bằng cách kiểm soát lưu lượng mạng dựa trên các quy tắc cấu hình.

### c/ Tường lửa kết nối (Stateful Firewall):

Tường lửa kết nối (Stateful Firewall) là một dạng tường lửa mạng tiên tiến hơn so với tường lửa gói tin truyền thống, có khả năng theo dõi trạng thái kết nối của các gói tin mạng và áp dụng các quy tắc kiểm soát truy cập dựa trên trạng thái này, cho phép xác định được các kết nối hợp lệ và chỉ cho phép lưu lượng mạng liên quan đến các kết nối đã được thiết lập.



Hình 12. Stateful Firewall



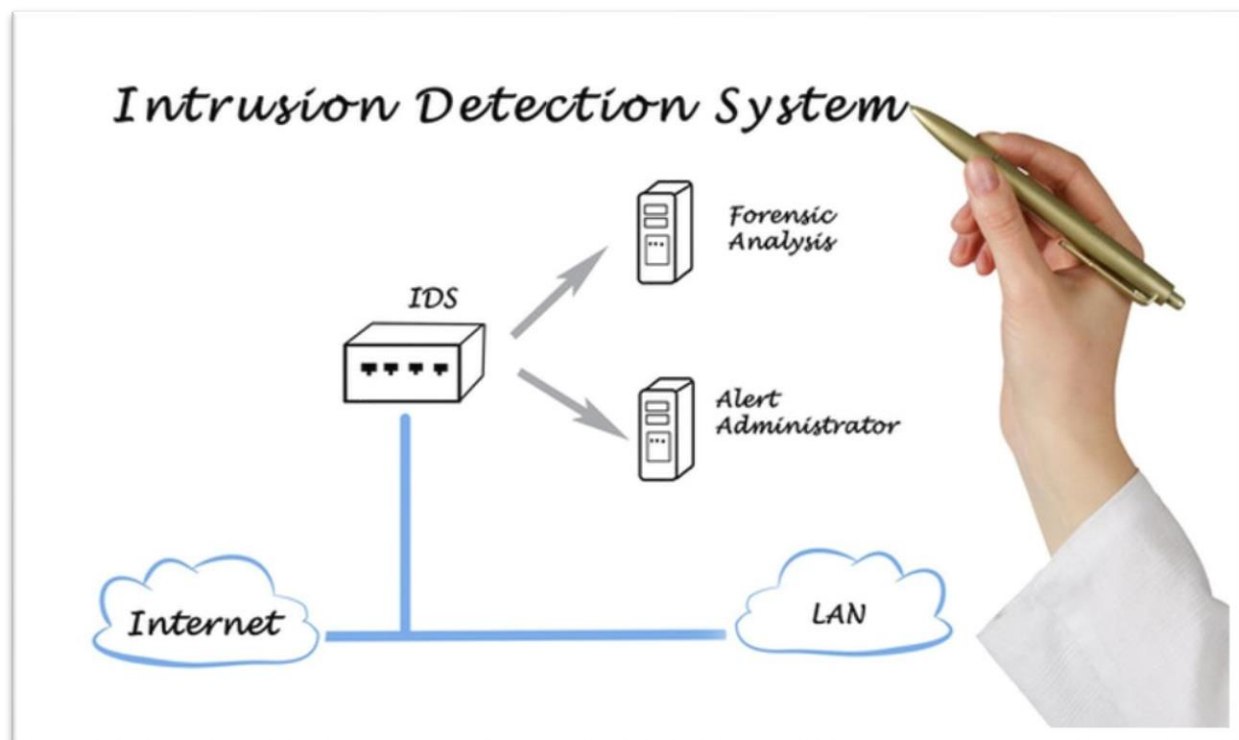
Các tính năng chính của tường lửa kết nối bao gồm:

- Theo dõi trạng thái kết nối: Tường lửa kết nối lưu giữ thông tin về trạng thái của các kết nối mạng, như trạng thái kết nối mới, kết nối đã thiết lập hoặc kết nối đã đóng. Nhờ đó, nó có thể phân biệt lưu lượng mạng hợp lệ và từ chối các gói tin không thuộc về kết nối đang diễn ra.
- Quy tắc kiểm soát truy cập dựa trên trạng thái: Tường lửa kết nối sử dụng các quy tắc kiểm soát truy cập dựa trên trạng thái kết nối. Các quy tắc này xác định cách xử lý gói tin theo trạng thái của chúng, bao gồm cho phép, từ chối hoặc giới hạn lưu lượng mạng.
- Hiểu biết về giao thức: Tường lửa kết nối có hiểu biết sâu về các giao thức mạng như TCP/IP. Nó có khả năng kiểm tra tính toàn vẹn và xác thực của các gói tin trong kết nối để ngăn chặn các cuộc tấn công như TCP SYN flood hay các cuộc tấn công khác liên quan đến việc thiếu thông tin giao thức cần thiết.
- Ghi nhật ký và phân tích: Tường lửa kết nối có khả năng ghi lại các sự kiện và lưu lượng mạng đi qua hệ thống. Nhật ký này có thể được sử dụng để phân tích, giám sát và điều tra sự cố bảo mật, cũng như để tuân thủ quy định về báo cáo và tuân thủ quyền riêng tư.

Tường lửa kết nối cung cấp một cơ chế bảo mật mạnh mẽ hơn so với tường lửa gói tin truyền thống. Nó giúp ngăn chặn các cuộc tấn công mạng bằng cách kiểm soát lưu lượng dựa trên trạng thái kết nối và khả năng hiểu biết về giao thức. Các tính năng này làm cho tường lửa kết nối trở thành một lựa chọn phổ biến trong việc bảo vệ hệ thống mạng.

### 1.5/ Các hệ thống phát hiện xâm nhập :

Các hệ thống phát hiện xâm nhập (IDS - Intrusion Detection Systems) là công cụ được sử dụng để giám sát và phát hiện các hoạt động xâm nhập vào mạng hoặc hệ thống. Chúng có khả năng phát hiện và báo cáo về những hành vi không mong muốn, nguy hiểm hoặc gian lận trong mạng.

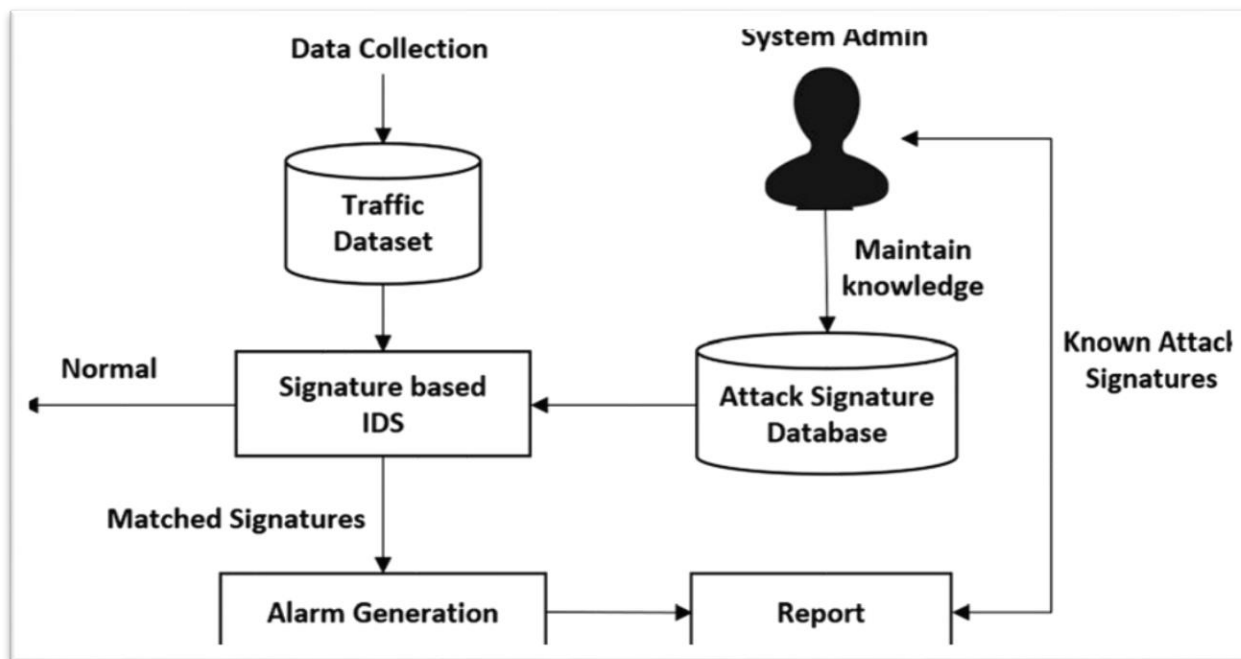


Hình 13. Infection Detection System

Một số loại hệ thống phát hiện xâm nhập phổ biến:

#### a/ Hệ thống phát hiện xâm nhập dựa trên chữ ký (Signature-based IDS):

Đây là loại IDS sử dụng cơ sở dữ liệu các chữ ký đã biết trước để so sánh với các gói tin hoặc hành vi trong mạng. Nếu có sự khớp, hệ thống sẽ cảnh báo người quản trị về nguy cơ xâm nhập. Tuy nhiên, hệ thống này có thể bị vượt qua bởi các cuộc tấn công mới mà chưa có chữ ký tương ứng.



Hình 14. Signature-based IDS

Cách hoạt động của hệ thống phát hiện xâm nhập dựa trên chữ ký như sau:

- **Xây dựng cơ sở dữ liệu chữ ký:** Hệ thống phải có một cơ sở dữ liệu chứa các chữ ký của các cuộc tấn công đã biết trước. Các chữ ký này được tạo ra từ các mẫu gói tin, mã độc hay các thuật toán xâm nhập được biết đến.
- **So sánh và phát hiện chữ ký:** Khi nhận được gói tin hoặc các hoạt động trong mạng, hệ thống sẽ so sánh chúng với cơ sở dữ liệu chữ ký đã xây dựng. Nếu có sự khớp, hệ thống sẽ kích hoạt cảnh báo và thông báo rằng có một cuộc tấn công xảy ra.

Ưu điểm của hệ thống phát hiện xâm nhập dựa trên chữ ký bao gồm:

- **Hiệu suất cao:** Vì các chữ ký đã biết được sử dụng để so sánh, hệ thống này có thể phát hiện và báo cáo nhanh chóng về các loại cuộc tấn công đã biết trước.

- Đáng tin cậy: Với việc sử dụng cơ sở dữ liệu chữ ký, hệ thống có thể giảm thiểu số lượng false positive (cảnh báo sai) và false negative (không phát hiện cuộc tấn công).

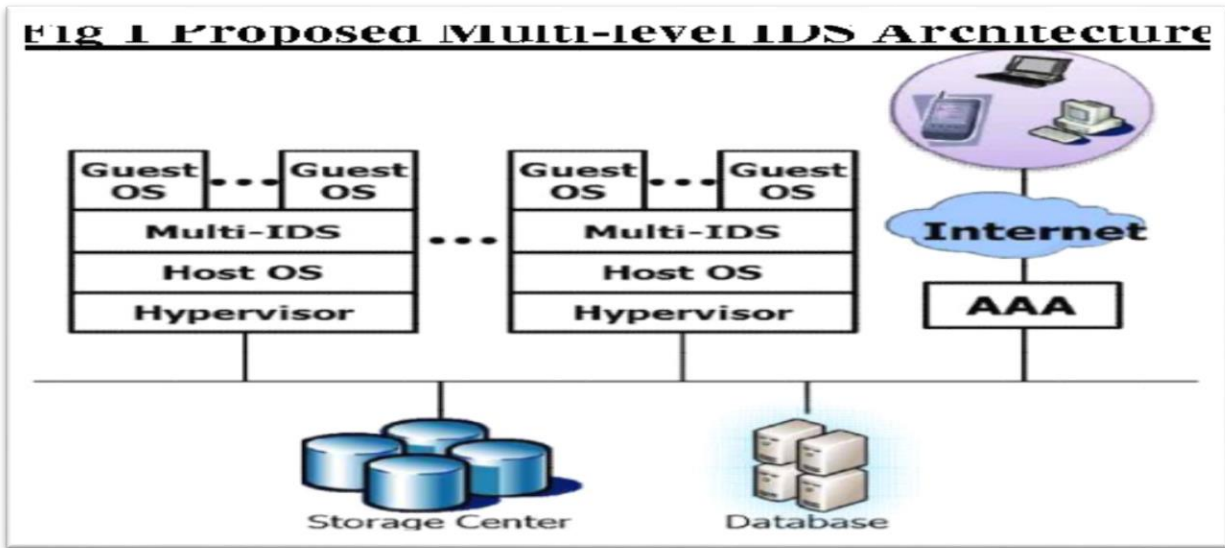
Tuy nhiên, hệ thống phát hiện xâm nhập dựa trên chữ ký cũng có một số hạn chế:

- Không thể phát hiện cuộc tấn công mới: Nếu một cuộc tấn công mới mà không có chữ ký tương ứng trong cơ sở dữ liệu, hệ thống sẽ không phát hiện được.
- Dễ bị đánh lừa: Kẻ tấn công có thể sửa đổi hoặc mã hóa lại gói tin để tránh bị phát hiện bởi hệ thống dựa trên chữ ký.

Vì các hạn chế này, các hệ thống phát hiện xâm nhập dựa trên chữ ký thường được sử dụng như một phần trong một hệ thống phát hiện xâm nhập tổng thể, kết hợp với các phương pháp khác như hệ thống phát hiện xâm nhập dựa trên hành vi.

#### **b/ Hệ thống phát hiện xâm nhập dựa trên hành vi (Behavior-based IDS):**

Loại IDS này theo dõi hoạt động của mạng và xác định các hành vi bất thường hoặc không phù hợp. Thay vì chỉ dựa trên chữ ký, hệ thống này sẽ phân tích các mô hình hành vi thông qua thu thập dữ liệu và xác định các hoạt động không bình thường. Điều này giúp nó phát hiện được những cuộc tấn công mới mà chưa có chữ ký tương ứng.



*Hình 15. Behavior-based IDS*

Cách hoạt động của hệ thống phát hiện xâm nhập dựa trên hành vi như sau:

- Thu thập dữ liệu: Hệ thống phải thu thập thông tin về các hoạt động trong mạng, bao gồm lưu lượng mạng, sự tương tác giữa người dùng và hệ thống, cấu hình hệ thống và các dữ liệu khác liên quan.
- Xây dựng mô hình hành vi chính xác: Dựa trên dữ liệu thu thập được, hệ thống sẽ phân tích và xây dựng các mô hình hành vi bình thường của người dùng và hệ thống. Đây là những mô hình mô tả hành vi chính xác đã được xác định trước.
- Phát hiện hành vi không bình thường: Khi có hoạt động mới trong mạng hoặc hành vi không phù hợp so với những mô hình đã xây dựng, hệ thống sẽ cảnh báo và thông báo về một tiềm năng xâm nhập hoặc hành vi đáng ngờ.

Ưu điểm của hệ thống phát hiện xâm nhập dựa trên hành vi bao gồm:

- Khả năng phát hiện cuộc tấn công mới: Bởi vì hệ thống phân tích các mô hình hành vi, nó có khả năng phát hiện các cuộc tấn công mới mà chưa có chữ ký tương ứng.

- Độ tin cậy cao: Hệ thống phát hiện xâm nhập dựa trên hành vi giúp giảm thiểu số lượng false positive và false negative.
- Phù hợp với môi trường biến đổi: Vì không dựa vào chữ ký, hệ thống này có thể phát hiện các loại tấn công và hành vi xâm nhập trong một môi trường mạng biến đổi.

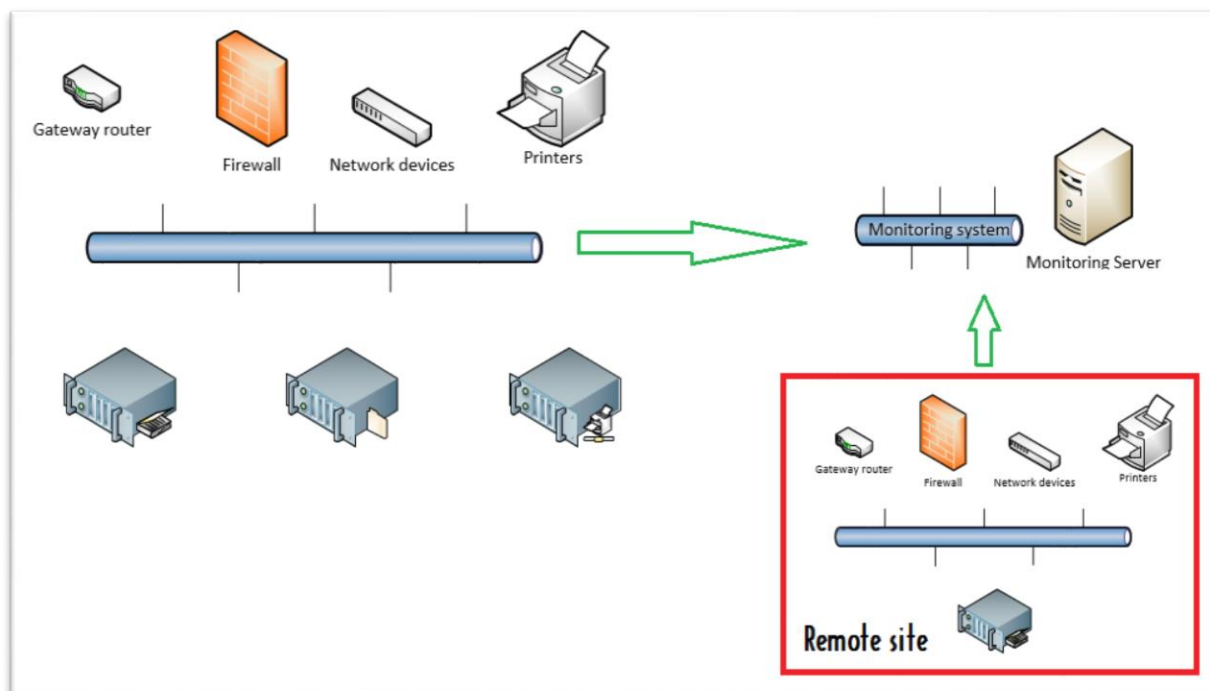
Tuy nhiên, hệ thống phát hiện xâm nhập dựa trên hành vi cũng có một số hạn chế:

- Cần nhiều dữ liệu để xây dựng mô hình: Hệ thống yêu cầu phải có đủ dữ liệu để xác định và xây dựng mô hình hành vi bình thường, điều này có thể tốn thời gian và tài nguyên.
- Có thể phát sinh false positive: Hệ thống có thể cảnh báo với những hành vi không phù hợp nhưng không phải là cuộc tấn công thực sự, dẫn đến false positive.

Tổng quát, hệ thống phát hiện xâm nhập dựa trên hành vi là một phương pháp quan trọng trong việc phát hiện và ngăn chặn các hoạt động xâm nhập trong mạng. Kết hợp với các phương pháp khác như hệ thống phát hiện xâm nhập dựa trên chữ ký, nó có thể cung cấp một lớp bảo mật toàn diện cho mạng và hệ thống.

## 1.6/ Các hệ thống giám sát Mạng :

Hệ thống giám sát mạng (Network Monitoring System) là một phần mềm hoặc hệ thống quản lý được sử dụng để giám sát, theo dõi và quản lý hoạt động của mạng máy tính. Nó cung cấp thông tin chi tiết về các thành phần của mạng như máy chủ, thiết bị mạng, ứng dụng, giao thức, băng thông và các yếu tố khác.



*Hình 16. Network Monitoring System*

Các chức năng chính của hệ thống giám sát mạng bao gồm:

- **Giám sát trạng thái:** Theo dõi hoạt động của các thiết bị mạng, bao gồm máy chủ, bộ định tuyến, công tắc, tường lửa và các thiết bị khác. Hệ thống giám sát mạng cung cấp thông tin về trạng thái hoạt động, tải trọng, sự cố và hiệu suất của các thiết bị này.
- **Giám sát kết nối và băng thông:** Theo dõi lưu lượng mạng và đánh giá việc sử dụng băng thông trong mạng. Hệ thống giám sát mạng cho phép người

quản trị xem kết nối mạng hiện tại, đưa ra cảnh báo khi có sự cố và phân tích việc sử dụng băng thông của các ứng dụng và dịch vụ.

- Ghi nhật ký và phân tích: Hệ thống giám sát mạng có khả năng ghi nhật ký (log) các sự kiện quan trọng trong mạng và phân tích chúng để xác định nguyên nhân gốc rễ của các sự cố, hiệu suất yếu và các vấn đề khác.
- Thông báo và cảnh báo: Hệ thống giám sát mạng có thể cung cấp cảnh báo qua email, tin nhắn văn bản hoặc thông báo trực tuyến khi có sự cố, trạng thái không bình thường hoặc vượt quá ngưỡng được định trước. Điều này giúp người quản trị mạng có thể phản ứng kịp thời để khắc phục vấn đề.
- Báo cáo và thống kê: Hệ thống giám sát mạng cung cấp tính năng tạo báo cáo và thống kê về hiệu suất, sự cố và các chỉ số quan trọng khác của mạng. Những thông tin này có thể được sử dụng để đánh giá và cải thiện hiệu suất mạng.

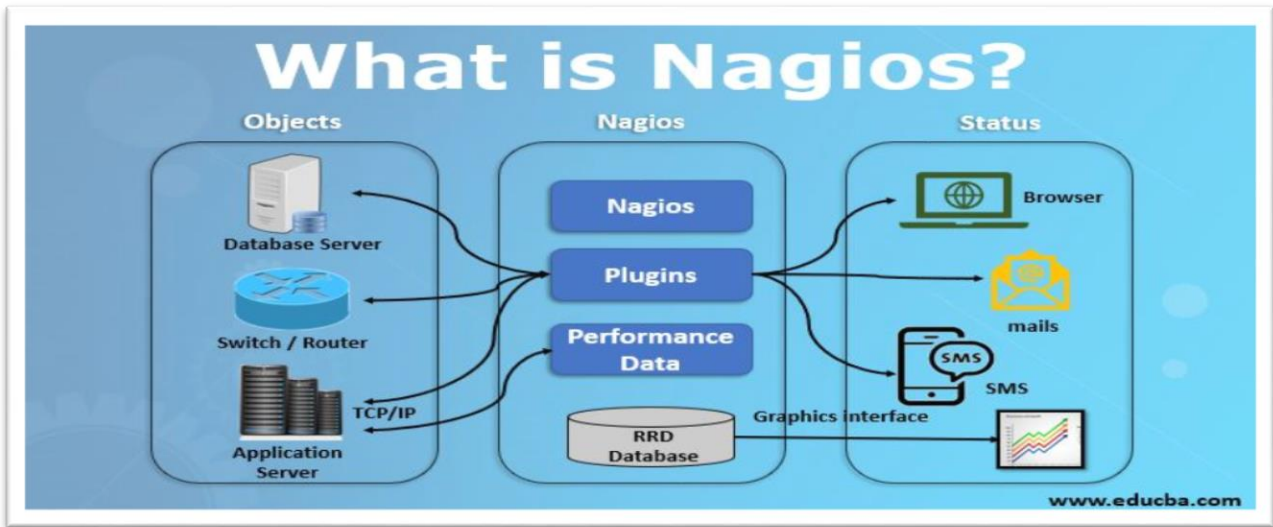
Hệ thống giám sát mạng đóng vai trò quan trọng trong việc duy trì và quản lý mạng máy tính một cách hiệu quả, đảm bảo hoạt động liên tục, tăng cường bảo mật và giảm thời gian không hoạt động.

Các loại hệ thống giám sát mạng phổ biến:

**a/ Nagios:**

Là một hệ thống giám sát mạng mã nguồn mở phổ biến được sử dụng rộng rãi cho việc giám sát và quản lý hệ thống. Nó đã tồn tại từ năm 1999 và đã trở thành một công cụ quan trọng trong lĩnh vực giám sát mạng.





*Hình 17. Nagios*

Các đặc điểm và chức năng chính của Nagios bao gồm:

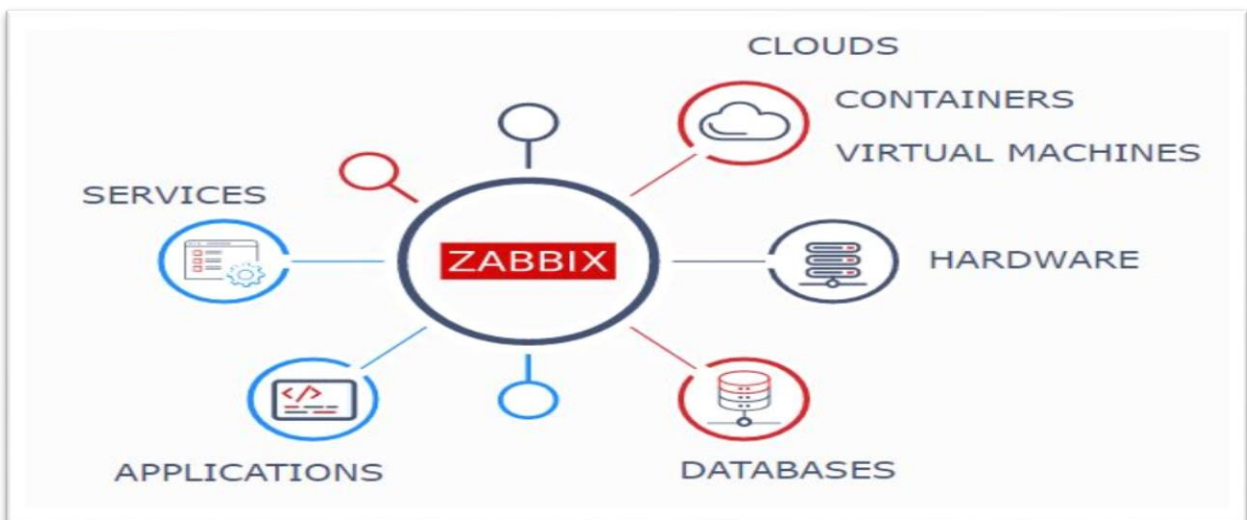
- **Giám sát đa nền tảng:** Nagios có khả năng giám sát các thành phần mạng khác nhau trên nhiều nền tảng, bao gồm máy chủ, thiết bị mạng, ứng dụng và dịch vụ. Nó hỗ trợ các giao thức như SNMP, ICMP, SSH, SMTP, HTTP và nhiều giao thức khác.
- **Cấu hình linh hoạt:** Nagios cho phép người dùng tùy chỉnh cấu hình theo yêu cầu cụ thể của mình. Người dùng có thể xác định các mục tiêu giám sát, kiểm tra chu kỳ, ngưỡng cảnh báo và các thông số khác để đáp ứng nhu cầu riêng.
- **Giao diện đồ họa:** Nagios cung cấp một giao diện web đồ họa cho phép người dùng xem trạng thái của hệ thống mạng và các thông báo cảnh báo. Giao diện này dễ sử dụng và cho phép người dùng tùy chỉnh theo ý muốn.
- **Cảnh báo và thông báo:** Nagios có khả năng gửi cảnh báo qua nhiều phương tiện, bao gồm email, tin nhắn văn bản và thông báo push. Người dùng có thể đặt các ngưỡng cảnh báo và điều kiện để nhận thông báo khi sự cố xảy ra hoặc trạng thái không bình thường được phát hiện.

- Ghi nhật ký và phân tích: Nagios lưu trữ các thông tin giám sát trong các tập tin nhật ký, cho phép người dùng xem lại và phân tích các sự cố, xu hướng hoạt động và hiệu suất của hệ thống.
- Mở rộng bằng plugin: Nagios cho phép mở rộng chức năng của nó thông qua việc sử dụng các plugin. Có sẵn một số lượng lớn các plugin đã được phát triển bởi cộng đồng người dùng, cho phép Nagios giám sát các thành phần cụ thể hoặc tích hợp với các công cụ và hệ thống khác.

Nagios là một giải pháp mạnh mẽ và linh hoạt để giám sát mạng và hệ thống. Nó đã trở thành một công cụ quan trọng cho các tổ chức và nhà quản trị hệ thống trong việc theo dõi và đảm bảo hoạt động ổn định của mạng và các thành phần liên quan.

#### **b/ Zabbix:**

Zabbix là một phần mềm mã nguồn mở và hệ thống giám sát mạng được sử dụng rộng rãi để theo dõi và quản lý hoạt động của các thành phần mạng, máy chủ và ứng dụng. Nó cung cấp các công cụ mạnh mẽ cho việc thu thập dữ liệu, phân tích và báo cáo về hiệu suất, trạng thái và sự cố trong môi trường mạng.



*Hình 18. Zabbix*

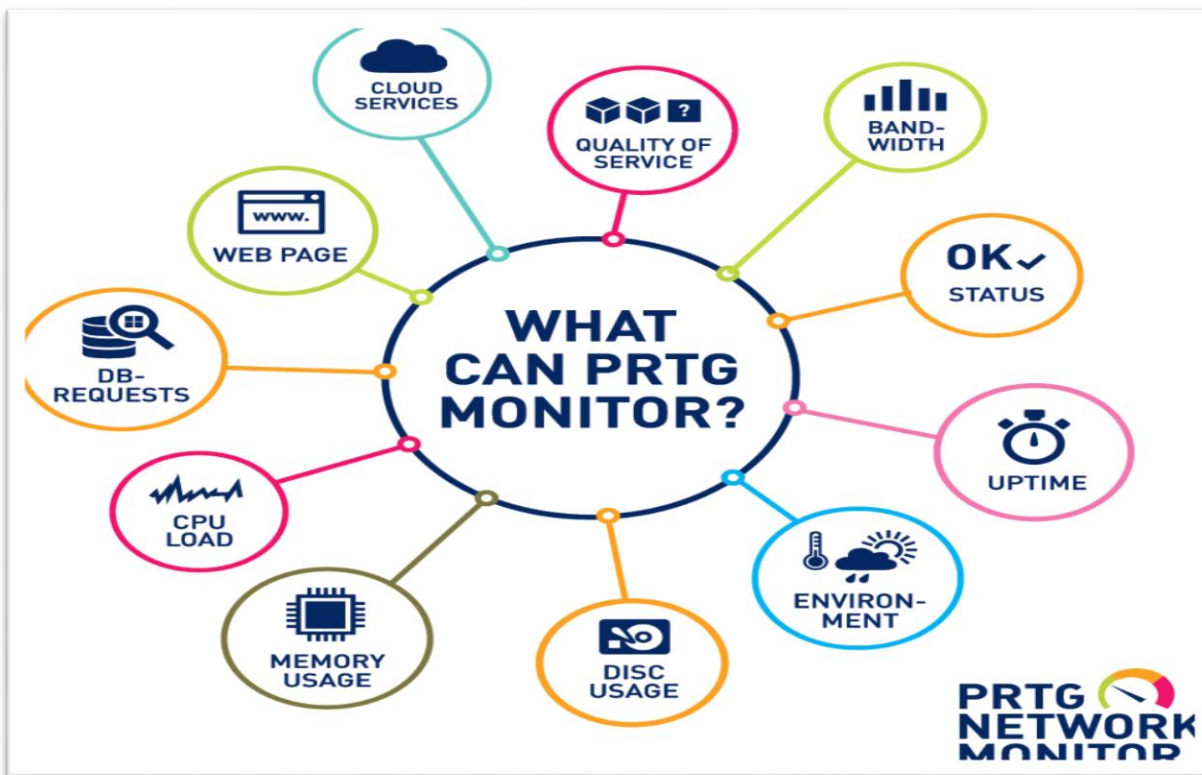
Các đặc điểm và chức năng chính của Zabbix bao gồm:

- **Giám sát đa nền tảng:** Zabbix có khả năng giám sát các thiết bị và hệ thống trên nhiều nền tảng, bao gồm Linux, Unix, Windows, macOS và nền tảng mạng khác nhau. Nó hỗ trợ nhiều giao thức giám sát như SNMP, ICMP, TCP, UDP, IPMI và các phương thức tùy chỉnh khác.
- **Giám sát linh hoạt:** Zabbix cho phép người dùng tùy chỉnh cấu hình giám sát theo yêu cầu cụ thể của môi trường mạng. Người dùng có thể xác định các thông số giám sát, ngưỡng cảnh báo, kiểm tra chu kỳ và cách nhận thông báo.
- **Giao diện đồ họa:** Zabbix cung cấp giao diện web đồ họa dễ sử dụng để xem trạng thái của các thành phần mạng và hiển thị các biểu đồ, bảng điều khiển và báo cáo chi tiết về hiệu suất và sự cố.
- **Cảnh báo và thông báo:** Zabbix cho phép cấu hình các ngưỡng cảnh báo và phương tiện thông báo khi có sự cố xảy ra hoặc trạng thái không bình thường được phát hiện. Các thông báo cảnh báo có thể được gửi qua email, tin nhắn văn bản, Slack và nhiều phương tiện khác.
- **Phân tích và báo cáo:** Zabbix có khả năng thu thập và lưu trữ dữ liệu giám sát trong cơ sở dữ liệu, từ đó phân tích và tạo báo cáo về hiệu suất, xu hướng và sự cố của mạng. Nó cung cấp các công cụ và tính năng mạnh mẽ để phân tích dữ liệu và tạo báo cáo theo yêu cầu.

Zabbix là một công cụ mạnh mẽ và linh hoạt để giám sát mạng và hệ thống. Nó cung cấp khả năng giám sát đa nền tảng, cấu hình linh hoạt, giao diện đồ họa và khả năng phân tích dữ liệu. Với Zabbix, người quản trị mạng có thể theo dõi và quản lý mạng một cách hiệu quả để duy trì hoạt động ổn định và tăng cường bảo mật.

### c/ PRTG Network Monitor:

Là một công cụ giám sát mạng và hệ thống phổ biến được phát triển bởi Paessler AG. Nó cung cấp các tính năng mạnh mẽ để giám sát, phân tích và báo cáo về hiệu suất và trạng thái của mạng, máy chủ, ứng dụng và các thiết bị khác.



*Hình 19. PRTG Network Monitor*

Các đặc điểm và chức năng chính của PRTG Network Monitor bao gồm:

- Giám sát đa nền tảng: PRTG có thể giám sát và thu thập dữ liệu từ các hệ điều hành khác nhau như Windows, Linux, Unix và macOS. Nó hỗ trợ nhiều giao thức giám sát như SNMP, WMI, SSH, ICMP và các giao thức tùy chỉnh khác.
- Cấu hình linh hoạt: PRTG cho phép người dùng dễ dàng cấu hình các thông số giám sát, ngưỡng cảnh báo, kiểm tra chu kỳ và cách nhận thông báo.

- Người dùng có thể tạo ra các cảnh báo tức thì, cảnh báo theo lịch trình và cảnh báo dựa trên các ngưỡng được xác định.
- Giao diện đồ họa: PRTG cung cấp một giao diện đồ họa trực quan và dễ sử dụng để xem trạng thái của mạng và các thành phần giám sát. Nó cung cấp biểu đồ, bảng điều khiển và giao diện người dùng linh hoạt để theo dõi và hiển thị thông tin chi tiết về hiệu suất và sự cố.
- Cảnh báo và thông báo: PRTG cho phép cấu hình các ngưỡng cảnh báo và thông báo tự động khi có sự cố xảy ra hoặc trạng thái không bình thường được phát hiện. Thông báo cảnh báo có thể được gửi qua email, tin nhắn văn bản, ứng dụng di động, Slack và nhiều phương tiện khác.
- Phân tích và báo cáo: PRTG thu thập dữ liệu giám sát và cung cấp công cụ để phân tích dữ liệu và tạo báo cáo về hiệu suất, xu hướng và sự cố của mạng. Người dùng có thể tạo báo cáo tùy chỉnh hoặc sử dụng các báo cáo mẫu có sẵn để hiển thị thông tin cần thiết.

PRTG Network Monitor là một công cụ mạnh mẽ và dễ sử dụng để giám sát mạng và hệ thống. Nó cung cấp khả năng giám sát đa nền tảng, cấu hình linh hoạt, giao diện đồ họa và các tính năng phân tích dữ liệu. Với PRTG, người quản trị mạng có thể theo dõi và quản lý mạng một cách hiệu quả để đảm bảo hoạt động ổn định và tối ưu hóa hiệu suất.

## **2. Kế hoạch triển khai:**

### **2.1. Thiết kế hệ thống:**

#### **a/ Chọn các phần mềm cần triển khai và chức năng (File, Backup, Firewall, IDS,...)**

Chúng em sẽ sử dụng những hệ thống bao gồm:

- Hệ thống lưu trữ: Sử dụng 2 hệ thống backup cloud là office 365 và bizfly cloud và dùng hệ thống Raid để full backup.
- Hệ điều hành: Sử dụng windows sever 2016 với các tính năng là DHCP, DNS, DC, ...
- Hệ thống tường lửa: Sử dụng firewall của hệ windows server đã được tích hợp sẵn.
- Các hệ thống phát hiện xâm nhập: Wireshark phân tích và xác định các vấn đề có liên quan đến mạng, trong đó bao gồm kết nối chậm, rò rỉ gói tin hoặc các nguồn truy cập bất thường
- Hệ thống giám sát mạng : PRTG Network Monitor giúp quản lý cơ sở hạ tầng, có khả năng tự động phát hiện các thiết bị và có khả năng cấu hình tự động.

#### **b/ Yêu cầu thiết bị:**

Sau đây là danh sách các thiết bị cần có để triển khai dự án :

- Mô hình văn phòng: Tòa nhà bao gồm 4 tầng, máy tính và máy in đặt ở tầng trệt, ngoại trừ phòng thực hành IT: 1 phòng ở tầng 1 và 1 phòng khác ở tầng 2 và tầng 3.
- Máy tính cho phòng lab :60 máy và được cấu hình vừa phải.
- Máy tính cho nhân viên :35 máy và cần được cấu hình cao.

- Sever: 1 server chính đảm nhiệm Domain chính chứa DHCP, 1 server Backup data, 1 server IDS IPS.
- Dây mạng RJ45 ADC ước tính khoảng 500 m
- Switch: bao gồm 5 switch thường, 1 switch tổng dẫn ra các tầng

## 2.2. Triển khai:

Sau khi cài đặt thành công EVE-NG trên phần mềm máy ảo VMWare và thiết lập các bước cơ bản để có thể tạo lab trên trình duyệt web thông qua địa chỉ IP, cần phải thêm các thiết bị Node vào EVE-NG để có thể giả lập sử dụng các thiết bị và sắp xếp mô hình của chúng tương ứng với kế hoạch vật lý đã lập ra từ ban đầu. Ta có thể tham khảo và làm theo hướng dẫn cách thêm thiết bị thông qua đường link: <https://www.eve-ng.net/index.php/documentation/> của đồng sáng lập nên phần mềm này.

### a/ Thiết lập Domain và các máy Client:

Domain hay còn được gọi là máy chủ Domain là một máy chủ đảm nhiệm công việc quản lý các tên miền và chuyển đổi chúng thành địa chỉ IP tương ứng. Điều này giúp người dùng truy cập các trang web thông qua tên miền dễ nhớ thay vì phải ghi nhớ địa chỉ IP phức tạp. Đối với yêu cầu của doanh nghiệp hiện đang được sử dụng làm đề tài của đồ án, nhóm của chúng em đã chia ra và thiết lập 1 domain chính (DHCP-DNS) và 2 domain phụ (IPS-IDS và BackUp).

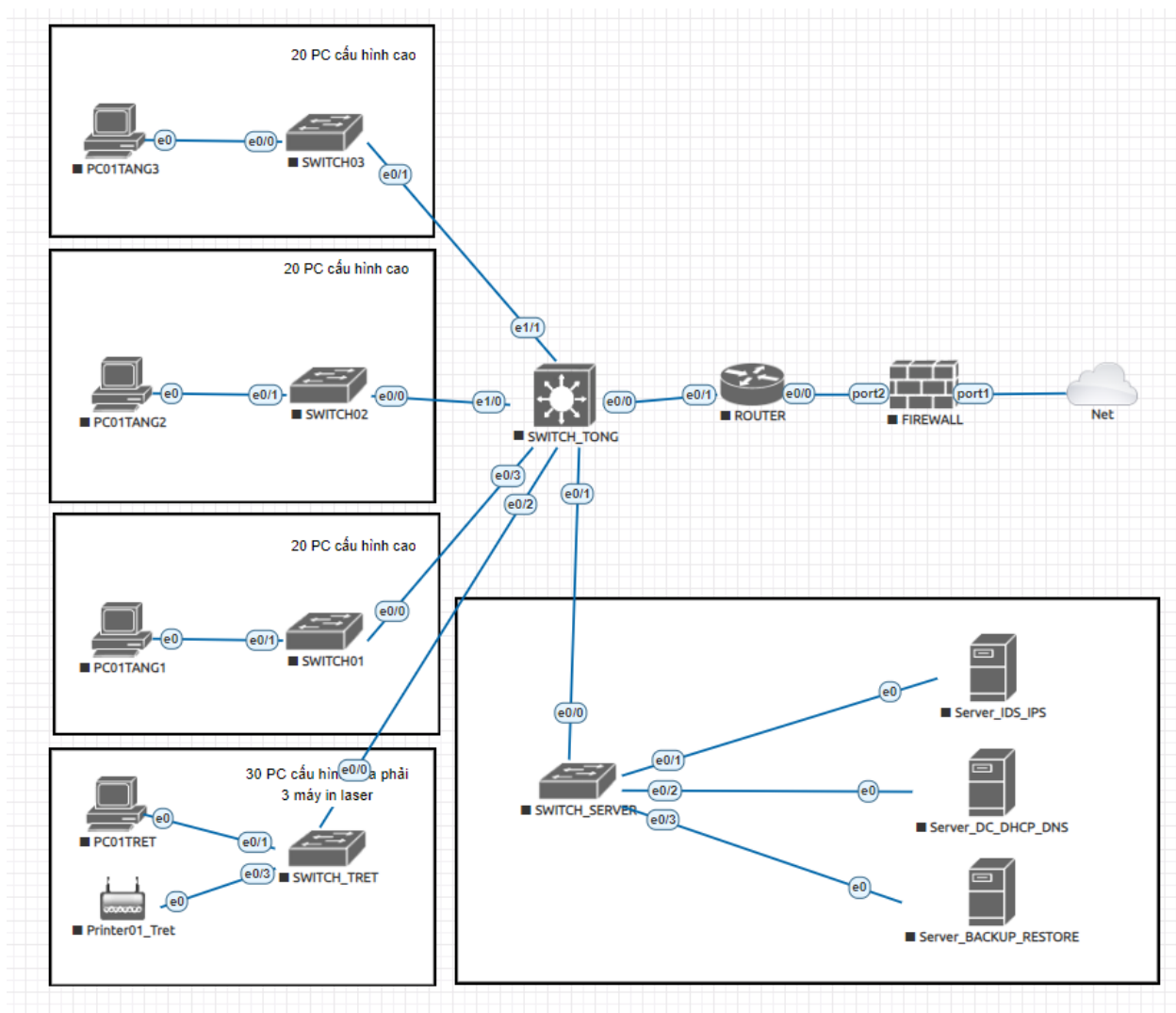
Sau đây là ví dụ về việc thiết lập và cài đặt từ một máy Windows Server 2019 thành một máy chủ Domain:

- Mô hình văn phòng: Tòa nhà bao gồm 4 tầng, máy tính và máy in đặt ở tầng trệt, ngoại trừ phòng thực hành IT: 1 phòng ở tầng 1 và 1 phòng khác ở tầng 2 và tầng 3.
- Máy tính cho phòng lab :60 máy và được cấu hình vừa phải.

- Máy tính cho nhân viên :35 máy và cần được cấu hình cao.
- Sever: Ước tính cần 3 sever, 2 sever Backup, 1 sever cung cấp dịch vụ mạng.
- máy in dạng laser
- Dây mạng RJ45 ADC ước tính khoảng 500 m
- Switch: bao gồm 7 switch chứa 14 port

### c/ Logical topology và Physical topology, IP Table:

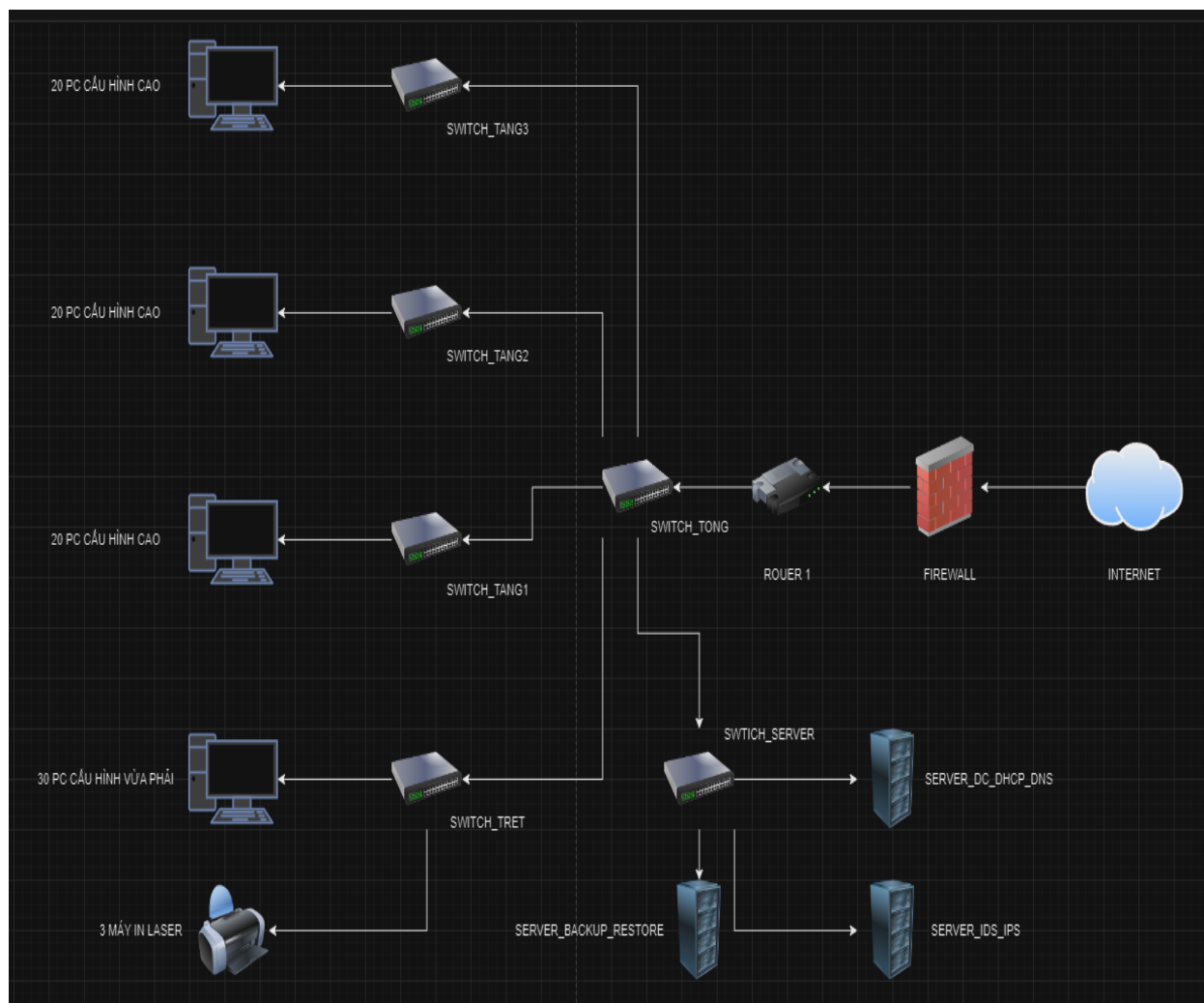
Sơ đồ logic (Logical topology):



Hình 20. Sơ đồ Logic



Sơ đồ vật lí (Physical topology):



Hình 21. Sơ đồ vật lý

Quy hoạch địa chỉ IP, chia subnet:

STT	DEVICE	IP	SUBNET MASK	NOTE
1	3 máy Server: DC_DHCP_DNS; IDS_IPS; BACKUP_RESTORE	192.168.1.100 – 200/24	255.255.255.0	IDS_IPS; BACKUP_RESTORE đều phải vào domain của DC_DHCP_DNS
2	TẦNG TRỆT: 35 PC CẤU HÌNH VỪA PHẢI VÀ 3 MÁY IN LASER	192.168.1.100 – 200/24	255.255.255.0	Đều phải vào domain của DC_DHCP_DNS
3	TẦNG 1: 20 PC CẤU HÌNH CAO	192.168.1.100 – 200/24	255.255.255.0	Đều phải vào domain của DC_DHCP_DNS
4	TẦNG 2: 20 PC CẤU HÌNH CAO	192.168.1.100 – 200/24	255.255.255.0	Đều phải vào domain của DC_DHCP_DNS
5	TẦNG 3: 20 PC CẤU HÌNH CAO	192.168.1.100 – 200/24	255.255.255.0	Đều phải vào domain của DC_DHCP_DNS

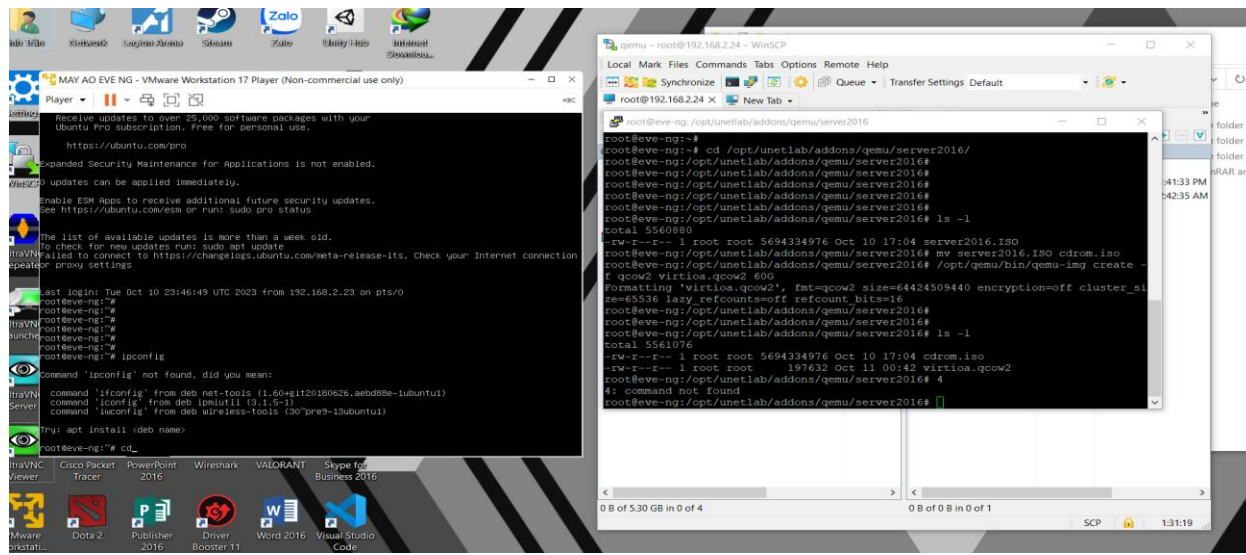
### **3. Triển Khai**

#### **3.1. Cài đặt môi trường EVE-NG:**

Giới thiệu sơ lược về công cụ EVE-NG

Đầu tiên ta giới thiệu sơ về UNetLab, UNetLab viết tắt cho Unified Networking Lab, là một bản phân phối của Linux cho phép bạn xây dựng hệ thống các bài lab network. UNetLab có thể xem như là một hypervisor cho các image thường chạy trên các thiết bị mạng vật lý hoặc các máy ảo tách biệt bên trong. Nó cho phép triển khai giả lập các thiết bị mạng như switch, router, firewall, ... và các thiết bị cuối để kiểm tra thiết kế, kiểm thử các hoạt động của mô hình lab thực tế. Điều tuyệt vời về UnetLab (và do đó cũng về EVE-NG) là tất cả mọi thứ được chứa trong một máy ảo, và bạn sử dụng một giao diện web để tạo và quản lý các bài lab bạn. Chỉ cần đẩy image vào đó (EVE-NG hỗ trợ rất nhiều image các thiết bị từ nhiều nhà cung cấp khác nhau), và từ đó cấu hình bắt đầu lab. EVE-NG (Emulated Virtual Environment – Next Generation) là một trong các công cụ giả lập (emulator) mạnh nhất hiện nay. Thừa hưởng các tính năng của UnetLab, EVE-NG cũng có thể giả lập được rất nhiều loại thiết bị mạng đang được sử dụng rộng rãi, với nhiều nền tảng hệ điều hành khác nhau: router/switch của Cisco (sử dụng Cisco IOL hoặc IOS trên nền Dynamip Server), thiết bị mạng của Juniper, nhiều loại firewall thông dụng.

## Cài đặt môi trường EVE-NG:



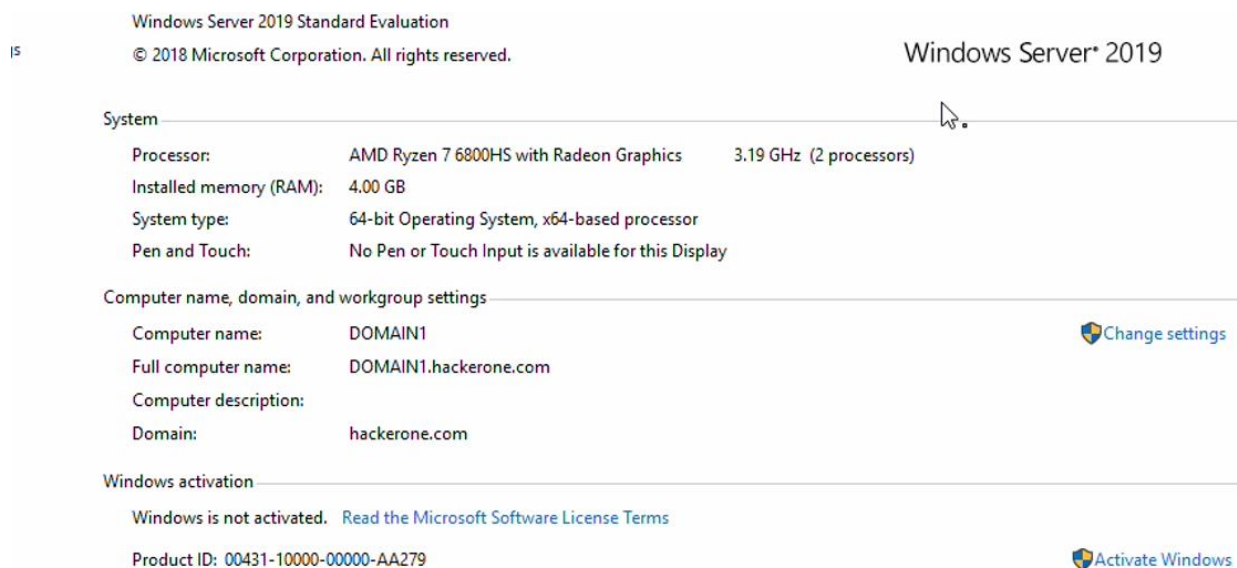
Hình 22. Cài đặt và test EVE-NG trên VMWare

## 3.2. Cấu hình và test lỗi:

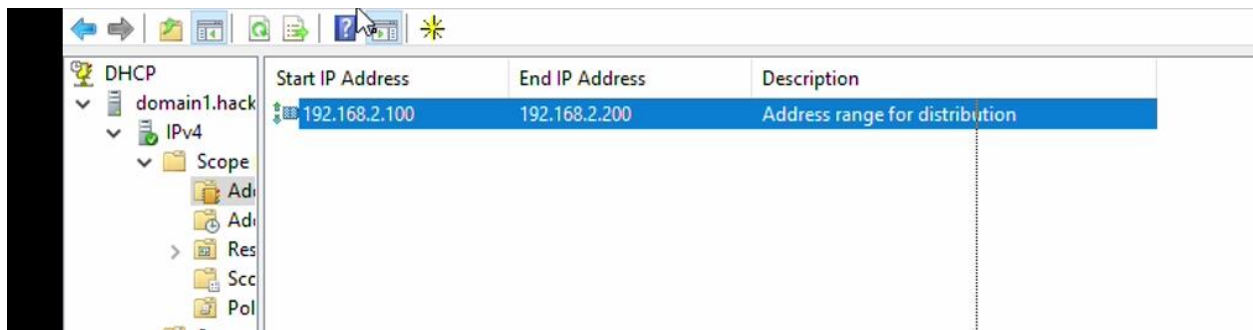
### a/ Phòng máy Server:

Server\_DC\_DHCP\_DNS:

Cấu hình Domain Controller:

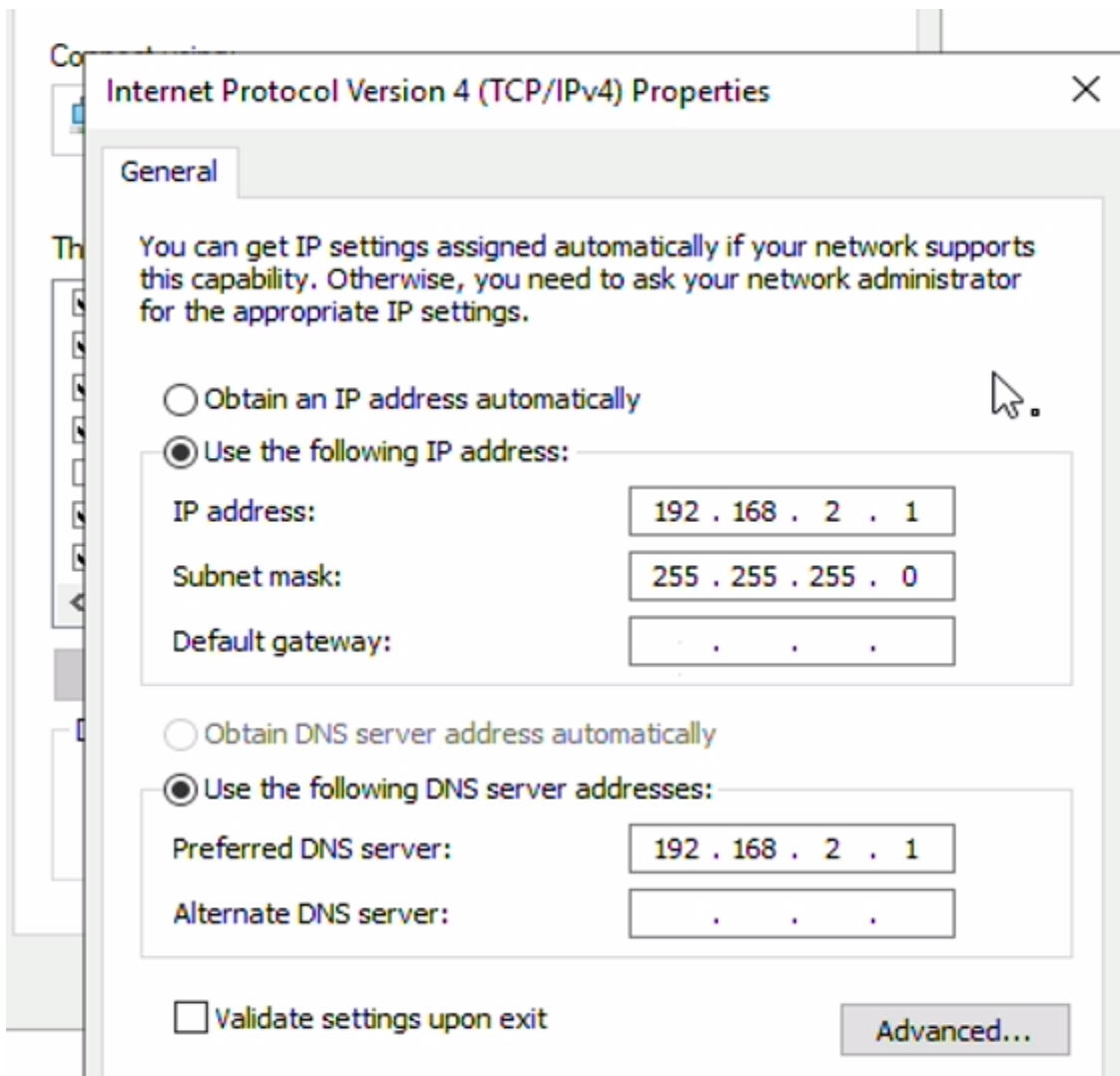


Hình 23. Cấu hình của máy chủ Server\_DC\_DHCP\_DNS



Start IP Address	End IP Address	Description
192.168.2.100	192.168.2.200	Address range for distribution

Hình 24. Thông tin về IP đầu tiên và IP đầu cuối của scope1 trong DHCP



**Internet Protocol Version 4 (TCP/IPv4) Properties**

**General**

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 2 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 1

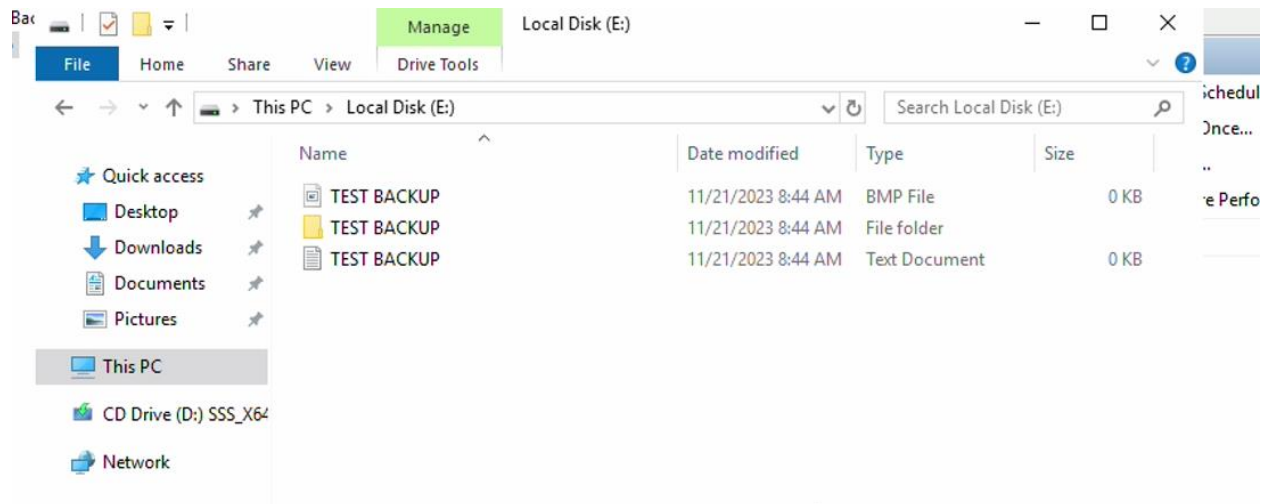
Alternate DNS server: . . .

☐ Validate settings upon exit

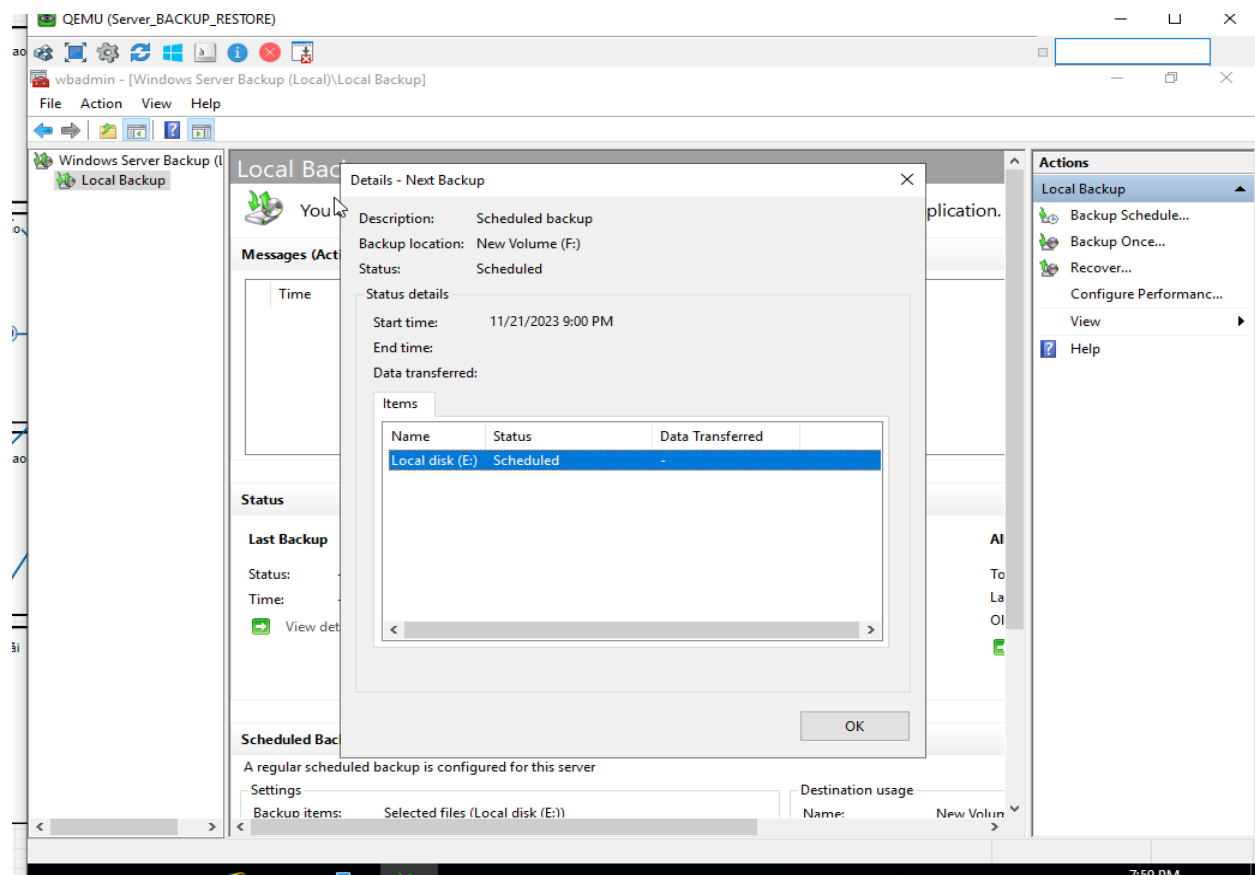
Advanced...

Hình 25. Địa chỉ IP của máy chủ Server\_DC\_DHCP\_DNS

## Server\_BACKUP\_RESTORE:

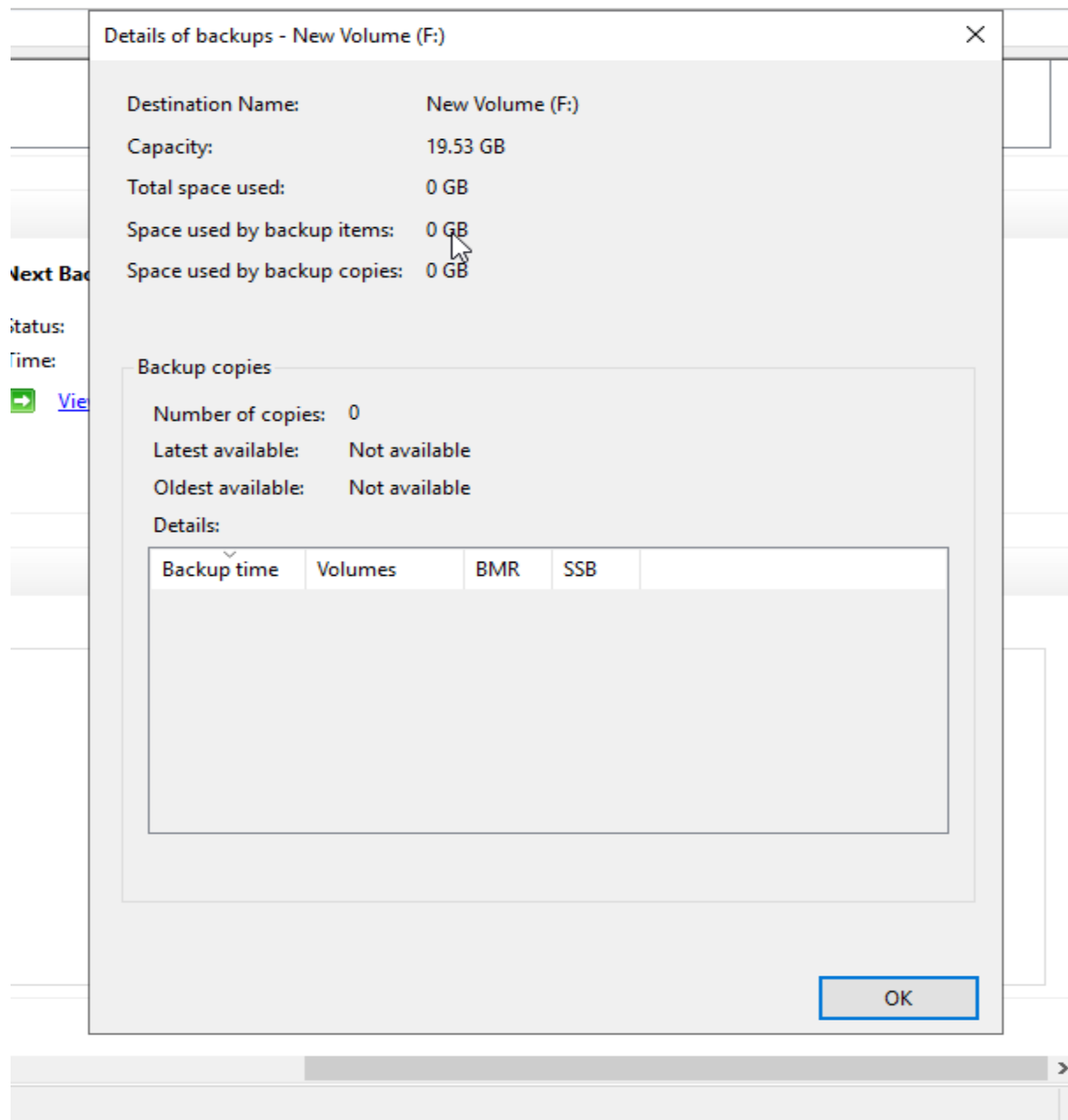


Hình 26. Ổ đĩa E chứa file lưu trữ gốc để thử nghiệm BackUp dữ liệu



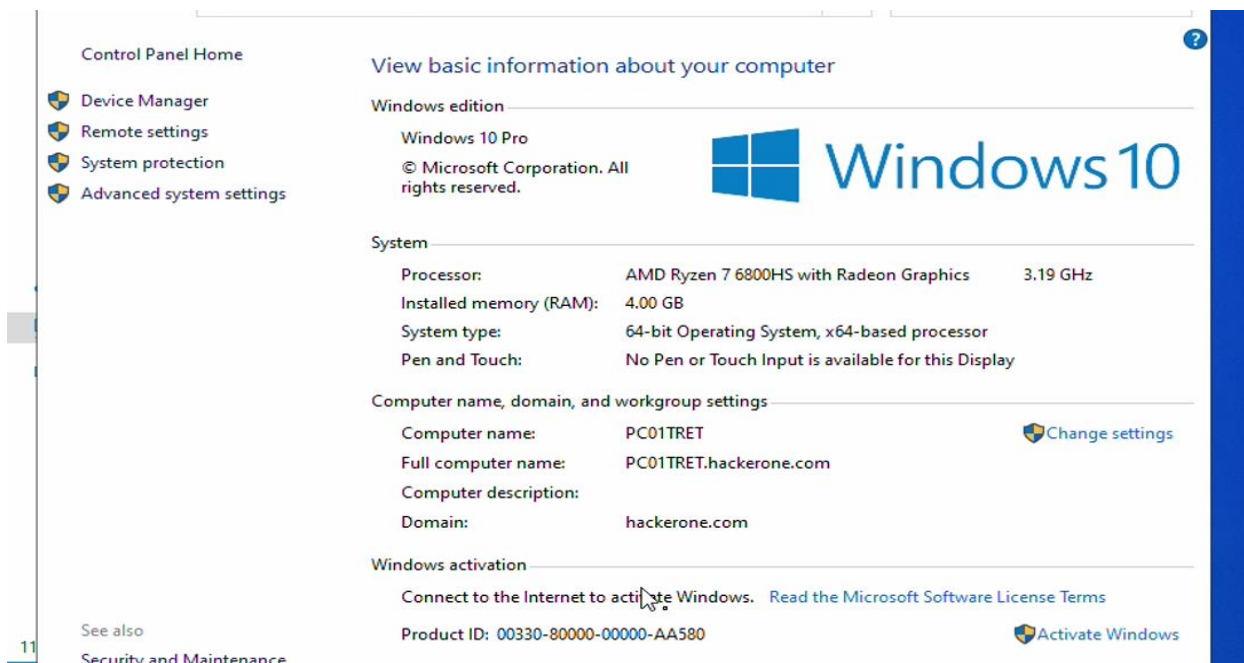
Hình 27. Thông tin của ổ cứng E về lần BackUp tiếp theo

p (Local)\Local Backup]

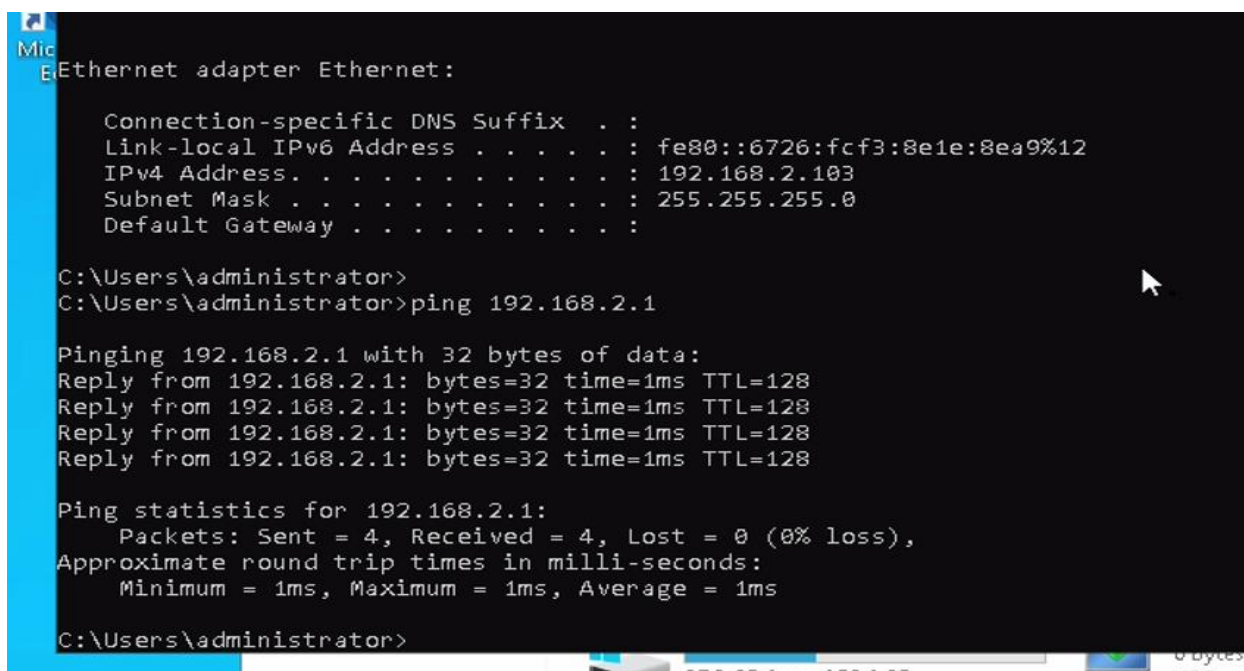


Hình 28. Thông tin của ổ cứng F – nơi lưu trữ những dữ liệu sẽ được BackUp bởi dữ liệu từ ổ cứng E

**b/ Phòng máy Client:**  
**PC tăng trệt:**



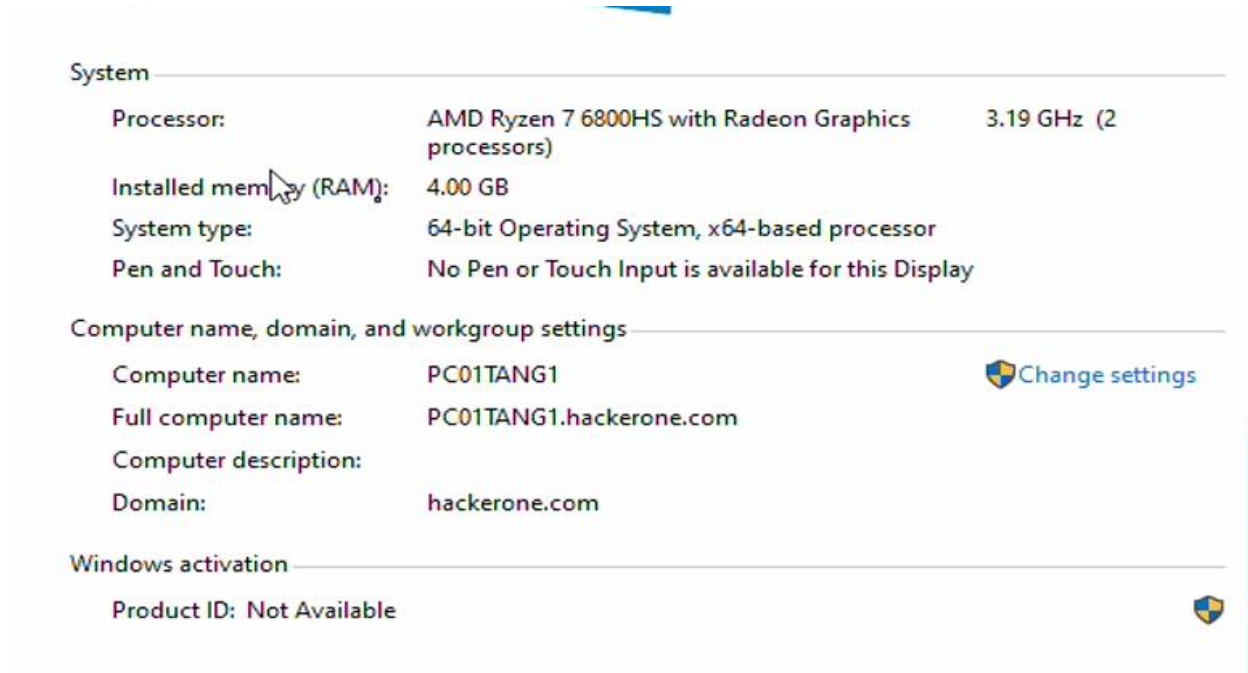
*Hình 29. Thông tin về PC tăng trệt đã tham gia vào domain của máy chủ  
Server\_DC\_DHCP\_DNS*



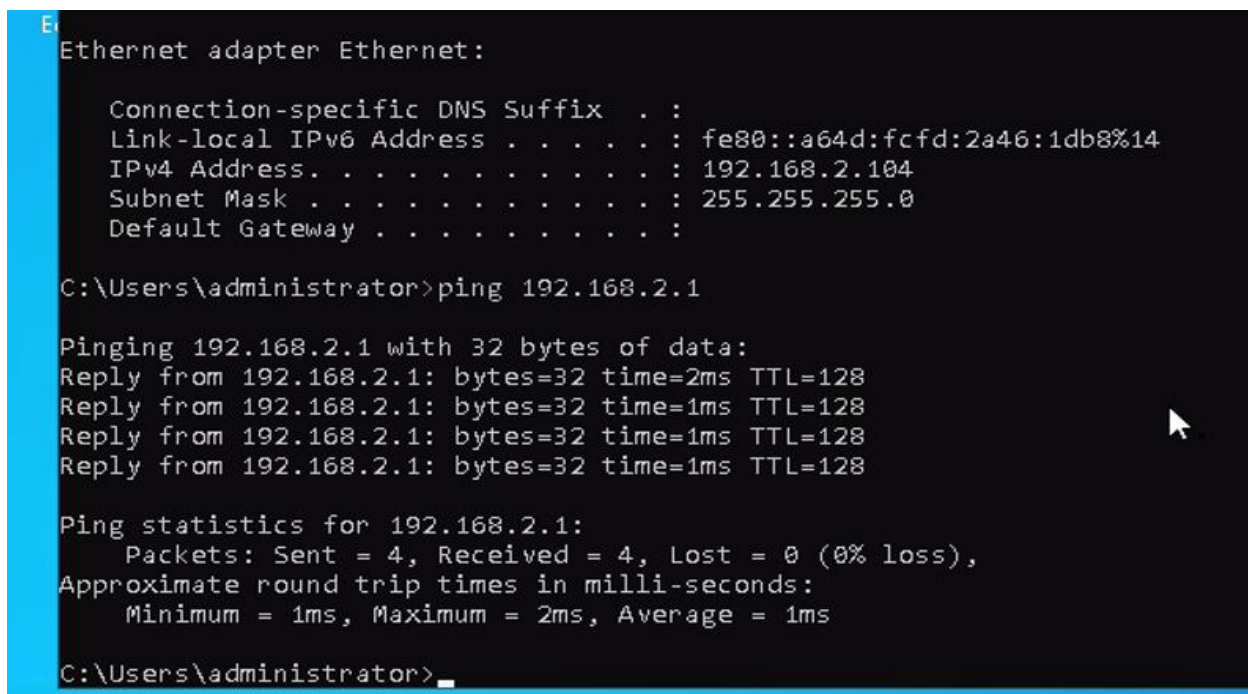
*Hình 30. Địa chỉ IP của máy và test ping sang domain của máy chủ  
Server\_DC\_DHCP\_DNS*



## PC tầng 1:

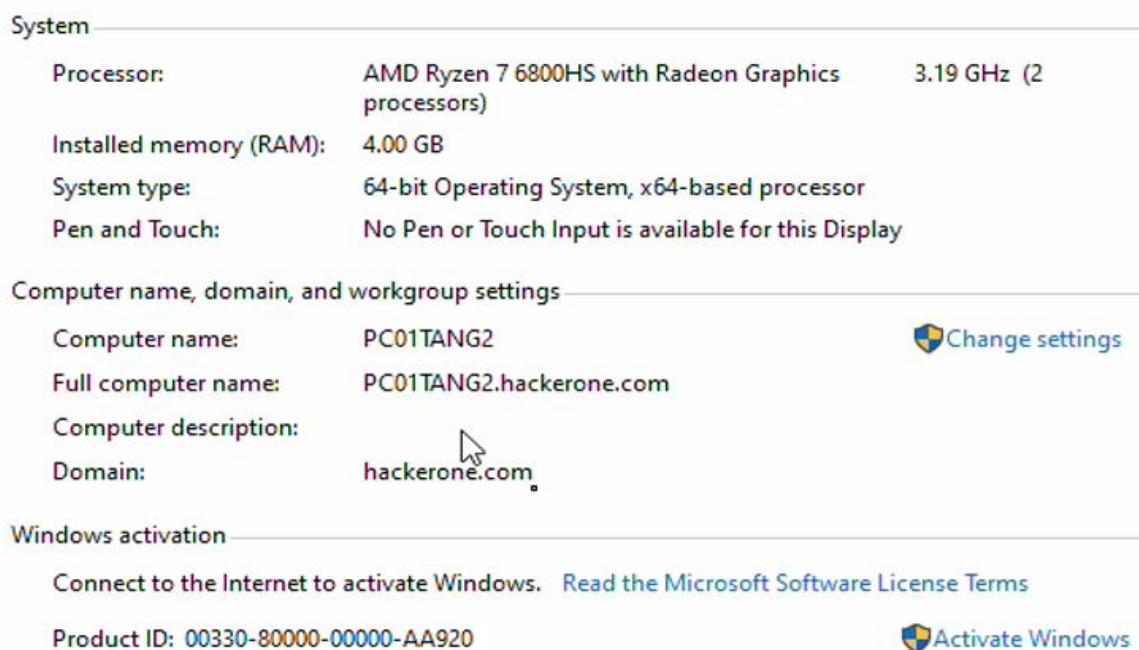


Hình 31. Thông tin về PC tầng 1 đã tham gia vào domain của máy chủ  
Server\_DC\_DHCP\_DNS



Hình 32. Địa chỉ IP của máy và test ping sang domain của máy chủ  
Server\_DC\_DHCP\_DNS

## PC tầng 2:



Hình 33. Thông tin về PC tầng 2 đã tham gia vào domain của máy chủ  
Server\_DC\_DHCP\_DNS

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::2fe5:3b1a:dc70:cd1%6
IPv4 Address. . . . . : 192.168.2.105
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

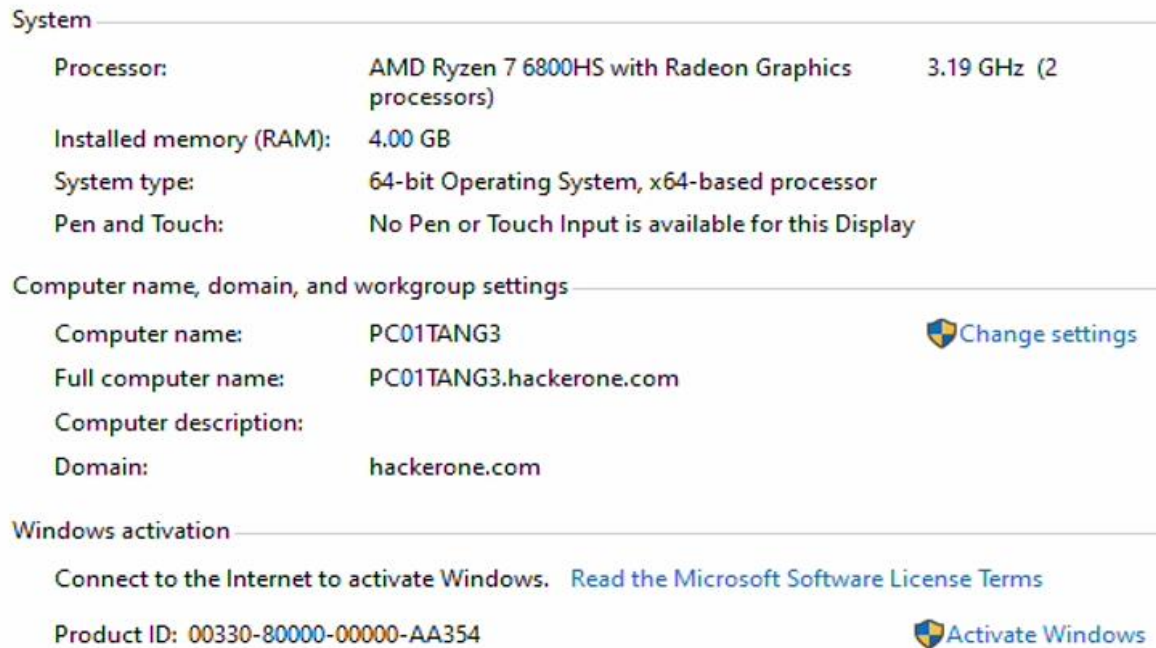
C:\Users\administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=7ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms
```

Hình 34. Địa chỉ IP của máy và test ping sang domain của máy chủ  
Server\_DC\_DHCP\_DNS

### PC tầng 3:



Hình 35. Thông tin về PC tầng 3 đã tham gia vào domain của máy chủ  
Server\_DC\_DHCP\_DNS

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::4097:40b6:9593:7ecf%8
IPv4 Address. . . . . : 192.168.2.106
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

C:\Users\administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=2ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Hình 36. Địa chỉ IP của máy và test ping sang domain của máy chủ  
Server\_DC\_DHCP\_DNS

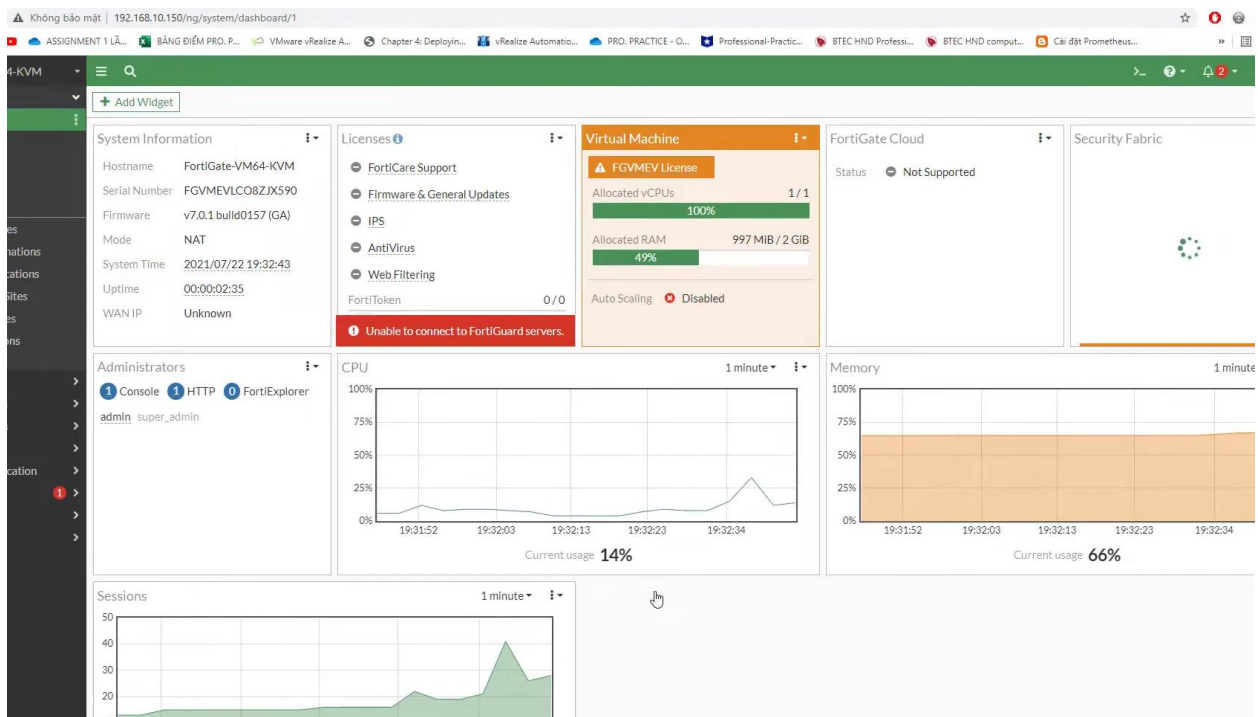
## FIREWALL:

```
FortiGate-VM64-KVM #
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh fgfm
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set type physical
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set type physical
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "naf.root"
        set vdom "root"
        set type tunnel
        set src-check disable
        set snmp-index 5
    next
    edit "l2t.root"
        set vdom "root"
        set type tunnel
        set snmp-index 6
    next
    edit "ssl.root"
        set vdom "root"
        set type tunnel
        set alias "SSL VPN interface"
        set snmp-index 7
    next
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set lldp-reception enable
        set lldp-transmission enable
        set snmp-index 8
    next
```

Hình 37. Thông tin về các port có trong sơ đồ hệ thống mạng của EVE-NG

```
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # show system interface port1
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.10.150 255.255.255.0
    set allowaccess ping https ssh http
    set type physical
    set snmp-index 1
  next
end
```

Hình 38. Sử dụng port mạng 1 làm địa chỉ IP Static để chỉnh sửa tường lửa trực tiếp trên trình duyệt web



Hình 39. Giao diện tùy chỉnh các chế độ của tường lửa sau khi cấu hình thành công

### **3.3. Đánh giá kết quả thực hiện:**

Kết quả của đề tài này là việc xây dựng thành công hệ thống mạng cho Viện Giáo dục Quốc tế HUFLIT. Hệ thống mạng đã được triển khai, đảm bảo hoạt động ổn định và đáng tin cậy Mạng LAN và WAN đã được kết nối và cung cấp băng thông cao, đáp ứng nhu cầu truy cập thông tin của sinh viên và nhân viên.

Chúng em cũng đã đảm bảo tính bảo mật thông tin và bảo vệ mạng khỏi các mối đe dọa từ bên ngoài. Hệ thống bảo mật đã được triển khai, bao gồm tường lửa, phần mềm diệt virus, hệ thống phát hiện xâm nhập và các biện pháp bảo mật khác để đảm bảo an toàn cho dữ liệu và thông tin quan trọng.

Ngoài ra, chúng em đã triển khai các dịch vụ và công nghệ tiên tiến như hệ thống giám sát mạng, sao lưu dữ liệu và khôi phục, hệ thống quản lý truy cập, và các dịch vụ đi kèm khác Các dịch vụ này đáp ứng tốt nhu cầu của Viện Giáo dục Quốc tế HUFLIT và giúp nâng cao hiệu suất và quản lý mạng.



## **4.Quản trị hệ thống:**

### **4.1. Đánh giá và lựa chọn network monitoring tool (SNMP, PRTG...):**

#### **a/ Đánh giá và lựa chọn Network Monitoring Tool**

PRTG Network Monitor là một công cụ phổ biến được sử dụng để giám sát mạng và cung cấp thông tin chi tiết về hiệu suất và sự hoạt động của các thiết bị mạng.

PRTG Network Monitor cung cấp các tính năng sau:

**Giám sát thiết bị mạng:** Công cụ này cho phép bạn giám sát các thiết bị mạng như máy chủ, switch, router, tường lửa và điểm truy cập không dây. Bạn có thể theo dõi trạng thái hoạt động, khả năng phản hồi, tài nguyên sử dụng (CPU, bộ nhớ) và thông lượng mạng của các thiết bị này.

**Giám sát mạng LAN và WAN:** PRTG Network Monitor cho phép bạn theo dõi các thông số mạng như băng thông, độ trễ, gói tin mất và gói tin hủy. Bạn có thể xác định các vấn đề về hiệu suất mạng, đánh giá sự ổn định và tìm hiểu nguyên nhân gây ra sự cố mạng.

**Giám sát ứng dụng:** Công cụ này cung cấp khả năng giám sát ứng dụng và dịch vụ mạng chạy trên hệ thống. Bạn có thể theo dõi các thông số như tài nguyên sử dụng, thời gian phản hồi và khả năng phục hồi của ứng dụng. Điều này giúp bạn xác định các vấn đề hoạt động của ứng dụng và đảm bảo rằng chúng hoạt động một cách hiệu quả.

**Báo cáo và cảnh báo:** PRTG Network Monitor cho phép tạo báo cáo tự động về hiệu suất mạng và các sự cố liên quan. Bạn có thể tùy chỉnh các báo cáo này để phù hợp với yêu cầu của bạn. Ngoài ra, công cụ này có khả năng cảnh báo thông qua email, tin nhắn hoặc thông báo trực tiếp khi phát hiện sự cố hoặc vượt ngưỡng được xác định.

Giao diện đồ họa và dễ sử dụng: PRTG Network Monitor có giao diện đồ họa thân thiện và dễ sử dụng. Bạn có thể tùy chỉnh giao diện để xem thông tin mạng theo cách bạn muốn và theo dõi từ xa thông qua giao diện web hoặc ứng dụng di động.

Đánh giá:

PRTG Network Monitor là một công cụ giám sát mạng rất phổ biến và có nhiều ưu điểm đáng kể. Dưới đây là một số đánh giá về PRTG Network Monitor:

- Dễ cài đặt và cấu hình: PRTG Network Monitor được đánh giá cao về tính dễ cài đặt và cấu hình. Giao diện người dùng thân thiện và trực quan giúp người dùng nhanh chóng thiết lập các thiết bị mạng và cấu hình các thông số giám sát một cách dễ dàng.
- Đa dạng tính năng giám sát: PRTG Network Monitor cung cấp một loạt các tính năng giám sát mạnh mẽ. Bạn có thể giám sát các thiết bị mạng, mạng LAN và WAN, ứng dụng và dịch vụ mạng. Công cụ cung cấp thông tin chi tiết về hiệu suất, tài nguyên sử dụng và sự hoạt động của các thành phần mạng, giúp người dùng nắm bắt tình trạng mạng và xử lý sự cố một cách hiệu quả.
- Báo cáo và cảnh báo linh hoạt: PRTG Network Monitor cho phép tạo báo cáo tự động về hiệu suất mạng và các sự cố liên quan. Bạn có thể tùy chỉnh các báo cáo này để phù hợp với yêu cầu của bạn. Ngoài ra, công cụ cung cấp cảnh báo linh hoạt thông qua email, tin nhắn hoặc thông báo trực tiếp khi phát hiện sự cố hoặc vượt ngưỡng được xác định.
- Hỗ trợ đa nền tảng: PRTG Network Monitor hỗ trợ nhiều hệ điều hành và nền tảng, bao gồm Windows, Linux và macOS. Điều này giúp công cụ phù hợp với nhiều môi trường mạng và cho phép người dùng giám sát từ xa thông qua giao diện web hoặc ứng dụng di động.



- Hỗ trợ khách hàng tốt: PRTG Network Monitor có một cộng đồng người dùng lớn và hỗ trợ khách hàng chuyên nghiệp. Bạn có thể tìm thấy tài liệu hướng dẫn chi tiết, diễn đàn thảo luận và tư vấn từ nhóm hỗ trợ để giúp giải quyết các vấn đề và tận dụng tối đa các tính năng của công cụ.

## **4.2. Các báo cáo nhận được**

PRTG Network Monitor cung cấp các báo cáo tự động về hiệu suất mạng và các sự cố liên quan.

Dưới đây là một số báo cáo mà bạn có thể nhận được từ PRTG Network Monitor:

- Báo cáo hiệu suất mạng: Báo cáo này cung cấp thông tin chi tiết về tình trạng hiệu suất mạng. Nó bao gồm thông số như băng thông sử dụng, độ trễ, gói tin mất và gói tin hủy. Báo cáo này giúp bạn đánh giá tình trạng mạng và xác định các vấn đề về hiệu suất.
- Báo cáo tài nguyên mạng: Báo cáo này cung cấp thông tin về tài nguyên sử dụng của các thiết bị mạng như CPU, bộ nhớ, ổ đĩa và giao diện mạng. Bạn có thể theo dõi việc sử dụng tài nguyên của các thiết bị và xác định các vấn đề liên quan đến tài nguyên.
- Báo cáo sự cố mạng: Báo cáo này liệt kê các sự cố mạng đã xảy ra trong một khoảng thời gian cụ thể. Nó bao gồm thông tin chi tiết về thời gian xảy ra sự cố, thiết bị liên quan và mô tả về sự cố. Báo cáo này giúp bạn nhanh chóng nhận biết và giải quyết các sự cố mạng.
- Báo cáo khả năng phục hồi: Báo cáo này cung cấp thông tin về thời gian phục hồi của các thiết bị mạng sau khi xảy ra sự cố. Nó giúp bạn đánh giá hiệu suất và thời gian phục hồi của các thành phần mạng và xác định các vấn đề về khả năng phục hồi.

- Báo cáo sử dụng ứng dụng: Báo cáo này cung cấp thông tin về hiệu suất và sử dụng của các ứng dụng và dịch vụ mạng. Nó bao gồm thông tin về tài nguyên sử dụng, thời gian phản hồi và khả năng phục hồi của các ứng dụng. Báo cáo này giúp bạn đánh giá và tối ưu hóa hiệu suất của các ứng dụng và dịch vụ mạng.

### **CHƯƠNG III. ĐÁNH GIÁ KẾT QUẢ:**

Sau quá trình nghiên cứu và thực hiện, đề tài này nhằm mục đích cung cấp một giải pháp toàn diện và hiệu quả cho viện giáo dục trong việc xây dựng và quản lý hệ thống mạng.

Trước hết, chúng tôi đã phân tích và hiểu rõ các yêu cầu và nhu cầu của Viện Giáo dục Quốc tế HUFLIT về mạng máy tính. Chúng tôi đã tiến hành thiết kế một kiến trúc mạng phù hợp, bao gồm các thành phần như máy chủ, mạng LAN và WAN, hệ thống bảo mật và quản lý mạng.

Kết quả của đề tài này là việc xây dựng thành công hệ thống mạng cho Viện Giáo dục Quốc tế HUFLIT. Hệ thống mạng đã được triển khai, đảm bảo hoạt động ổn định và đáng tin cậy. Mạng LAN và WAN đã được kết nối và cung cấp băng thông cao, đáp ứng nhu cầu truy cập thông tin của sinh viên và nhân viên.

Chúng tôi cũng đã đảm bảo tính bảo mật thông tin và bảo vệ mạng khỏi các mối đe dọa từ bên ngoài. Hệ thống bảo mật đã được triển khai, bao gồm tường lửa, phần mềm diệt virus, hệ thống phát hiện xâm nhập và các biện pháp bảo mật khác để đảm bảo an toàn cho dữ liệu và thông tin quan trọng.

Ngoài ra, chúng tôi đã triển khai các dịch vụ và công nghệ tiên tiến như hệ thống giám sát mạng, sao lưu dữ liệu và khôi phục, hệ thống quản lý truy cập, và các dịch vụ đi kèm khác. Các dịch vụ này đáp ứng tốt nhu cầu của Viện Giáo dục Quốc tế HUFLIT và giúp nâng cao hiệu suất và quản lý mạng.

Từ kết quả đạt được, chúng tôi nhận thấy rằng đề tài "Xây dựng hệ thống mạng cho Viện Giáo dục Quốc tế HUFLIT" đã mang lại những lợi ích đáng kể cho viện giáo dục. Hệ thống mạng mới đã cung cấp một môi trường học tập và làm việc hiện đại, tăng cường khả năng kết nối và truy cập thông tin, đồng thời đảm bảo an ninh và bảo mật thông tin.

Tuy nhiên, chúng tôi cũng nhận thấy rằng việc duy trì và nâng cấp hệ thống mạng là một quá trình liên tục. Chúng tôi khuyến nghị viện giáo dục tiếp tục theo dõi và đánh giá hiệu suất mạng, đồng thời thực hiện các biện pháp bảo trì, cập nhật và nâng cấp định kỳ để đảm bảo hệ thống mạng hoạt động tốt nhất.

Tổng kết lại, kết quả đề tài "Xây dựng hệ thống mạng cho Viện Giáo dục Quốc tế HUFLIT" đã mang lại những thành tựu đáng kể trong việc cung cấp một hệ thống mạng hiệu quả, an toàn và tin cậy cho Viện Giáo dục Quốc tế HUFLIT. Chúng tôi hi vọng rằng kết quả này sẽ góp phần nâng cao chất lượng giảng dạy và học tập tại viện giáo dục và tạo ra một môi trường học tập và làm việc tiên tiến. Chân thành cảm ơn quý thầy cô và các bạn đã tin tưởng và hỗ trợ chúng tôi trong quá trình nghiên cứu và thực hiện đề tài này

## **BẢNG PHÂN CÔNG CÔNG VIỆC**

Họ và tên	MSSV	Công việc
Trần Ngọc Vinh	21DH113413	Cài đặt, cấu hình và thiết lập mô hình doanh nghiệp, bao gồm Server, Client, Switch...
Lê Thành Ân	21DH112304	Lên kế hoạch và triển khai đồ án, hoàn thành sơ đồ vật lý
Nguyễn Hoàng Phúc	21DH114014	Triển khai và hoàn thành mục báo cáo đồ án trên Word