

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Khoa Công Nghệ Thông Tin

---o0o---



THIẾT KẾ HỆ THỐNG MẠNG NỘI BỘ CHO DOANH NGHIỆP

Học phần : Thiết kế mạng

Lớp : 18_4

Sinh viên

Trần Trung Hậu - 18120360
Lương Đức Trung - 18120100

Giảng viên

Nguyễn Thanh Quân
Nguyễn Thị Thanh Huyền

Mục Lục

Giai đoạn 1: Analyze Requirements:	3
1. Tổng quan.....	3
2. Bản vẽ thiết kế tòa nhà:.....	4
3. Yêu cầu Khách hàng:.....	7
Phần hạ tầng và thiết bị:	7
Phần Server và quản trị:.....	7
Giai đoạn 2: Logical Network Design	9
Giai đoạn 3: Physical Network Design	11
Giai đoạn 4: Simulation Model.....	15
Giai đoạn 5: Documenting	19
1. Thiết bị:	19
Danh sách thiết bị cần mua mới:	19
2. Công nghệ:.....	20
Danh sách công nghệ sử dụng:	20
3. Ưu khuyết điểm công nghệ, thiết bị:	20
4. Dịch vụ và thiết bị khác.....	21
5. Tổng chi phí	21
Tự đánh giá đề tài	22
Tài liệu tham khảo	23

❖ Thành viên nhóm:

MSSV	Họ Tên	Phân công
18120360	Trần Trung Hậu	Phân tích yêu cầu, mô hình vật lý, Documenting
18120100	Lương Đức Trung	Phân tích yêu cầu, mô hình logic, simulation model

❖ Thực hiện đề tài:

Giai đoạn 1: Analyze Requirements:

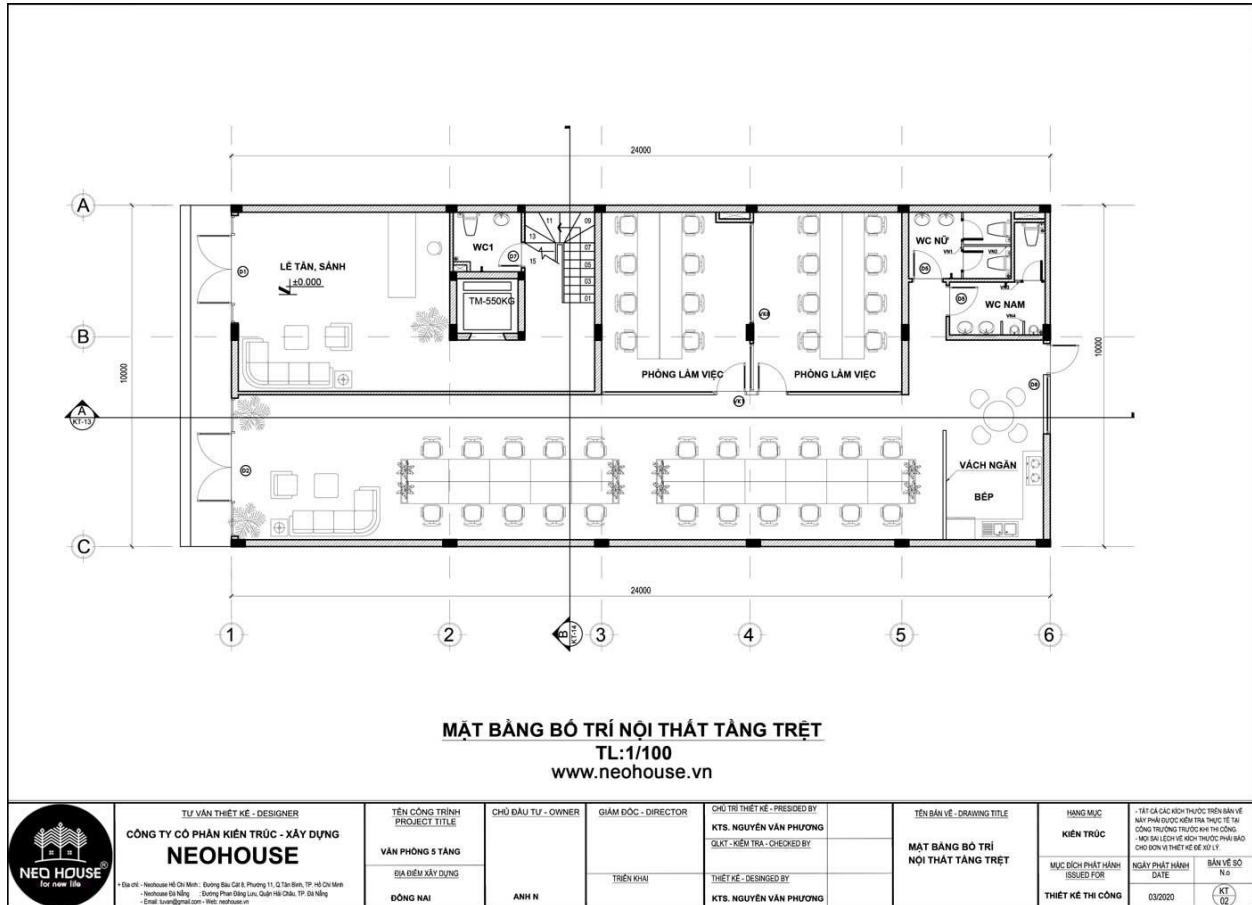
1. Tổng quan

- Khách hàng là doanh nghiệp kinh doanh dưới hình thức trung tâm khảo thí.
- Doanh nghiệp này muốn triển khai hệ thống mạng nội bộ cho công ty.

2. Bản vẽ thiết kế tòa nhà:

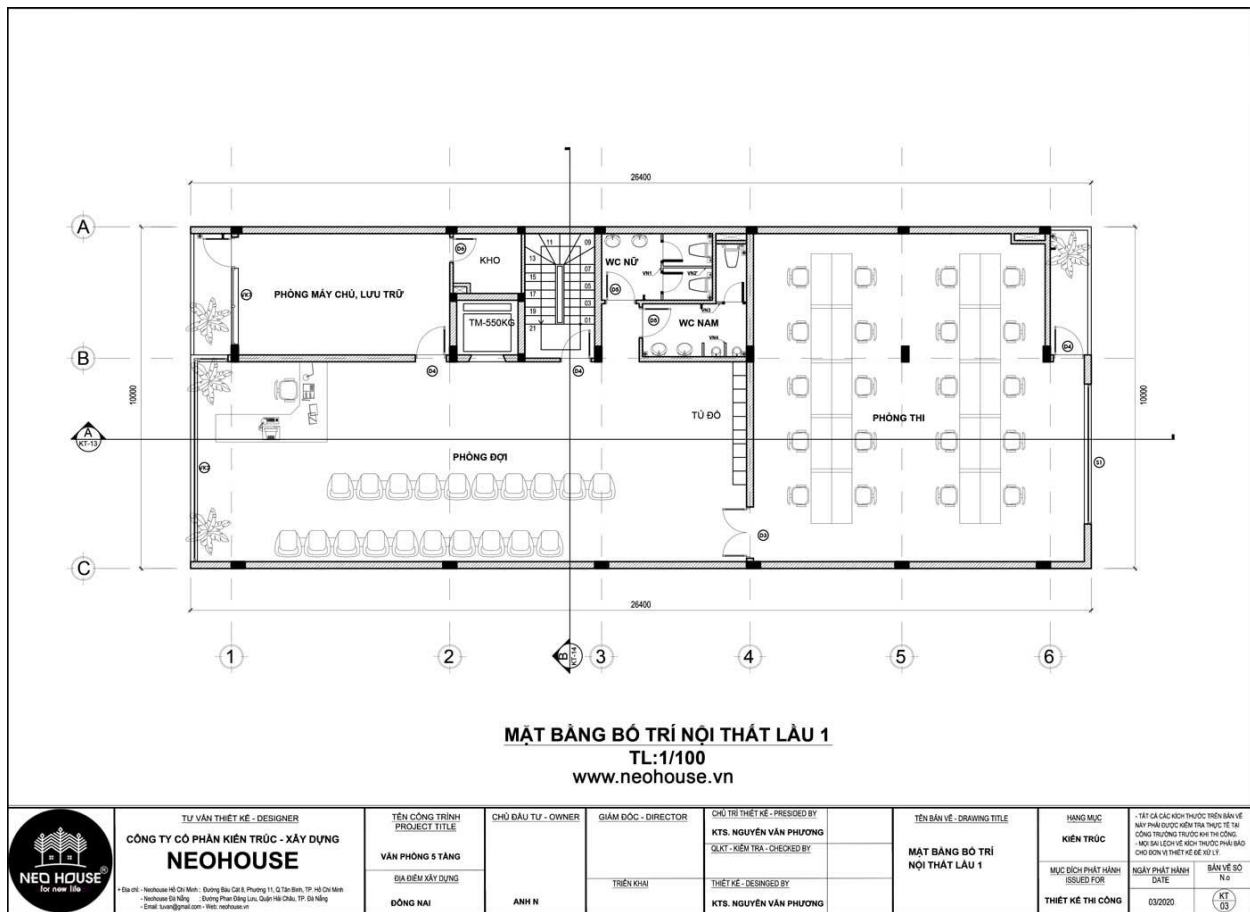
Tòa nhà này gồm 3 tầng:

Tầng trệt:



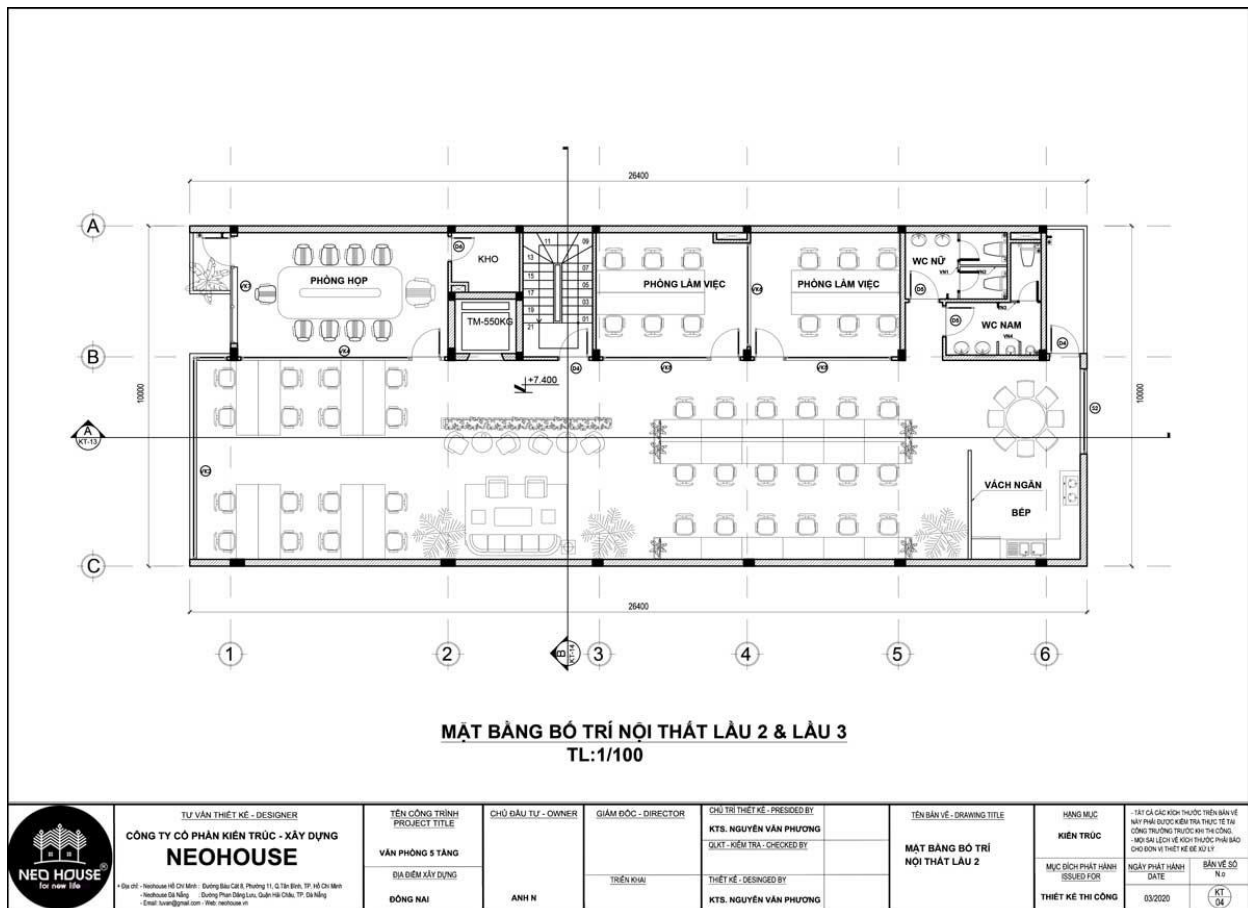
Mô tả: khu vực lễ tân, khu vực tiếp khách, 2 phòng làm việc (Phòng Marketing), 2 khu vực làm việc ngoài sảnh (Dành cho Telesales), phòng bếp và nhà vệ sinh nam – nữ.

Tầng 1:



Mô tả: khu vực đợi, 1 phòng thi, phòng máy chủ lưu trữ, nhà kho và nhà vệ sinh cho nam và nữ.

Lầu 2 & Lầu 3:



Mô tả lầu 2: Khu vực sảnh làm việc bên trái (Bộ phận đánh giá & chấm điểm), 2 phòng làm việc phía trên (Phòng nhân sự), chính giữa là không gian tiếp khách hay dùng để nghỉ ngơi. 1 phòng bếp và bàn ăn bên góc, đối diện là nhà vệ sinh nam – nữ, 1 phòng họp và nhà kho.

Mô tả lầu 3: Khu vực bên trái là của phòng phân tích thị trường, 2 phòng làm việc phía trên thuộc phòng kế toán, trong khi sảnh làm việc đối diện phòng kế toán sẽ là bộ phận kế hoạch & tổ chức khảo thí. Phòng họp và nhà vệ sinh ở các vị trí tương ứng như hình.

❖ Doanh nghiệp có thuê đường kết nối Internet đi vào tại tầng 1. Bảng thông kết nối Internet của mỗi tầng như sau:

- Tầng trệt: Tiếp tân, tư vấn (15 người - 15 máy), Truyền thông & Marketing (12 người - 12 máy): 4Mbps

- Tầng 1: Phòng kỹ thuật - Phòng máy chủ, lưu trữ (5 người – 5 máy) và phòng thi (21 người – 20 máy thí sinh & 1 máy giám khảo): 16Mbps
- Tầng 2: Quản lý nhân sự (9 người - 9 máy) và Bộ phận đánh giá & chấm điểm (12 người – 12 máy): 4Mbps
- Tầng 3: Phòng phân tích thị trường (16 người – 16 máy), kế toán (9 người – 9 máy), Kế hoạch & tổ chức khảo thí (18 người - 18 máy): 12Mbps
- ❖ Ngoài ra doanh nghiệp còn thuê thêm 1 đường mạng wifi cho khách hàng đi vào từ tầng trệt:
 - Băng thông của wifi:
 - Tối thiểu: 10Mbps
 - Tối đa: 30Mbps

3. Yêu cầu Khách hàng:

Phần hạ tầng và thiết bị:

- Công ty lắp đặt các camera ở mỗi tầng. Mỗi phòng có đều có camera. Riêng phòng thi có 2 camera và phòng đợi có 1 camera.
- Phòng kỹ thuật sẽ quản lý hệ thống camera.
- Công ty đã có các máy tính cá nhân (PC).
- Lắp đặt Wifi ở mỗi tầng: 1 đường wifi cho nhân viên và 1 đường wifi cho khách hàng. Đảm bảo có thể truy cập wifi kết nối tốt.
- Phòng máy chủ, lưu trữ phải có kết nối mạng ưu tiên với tốc độ cao, đồng thời đảm bảo về tính bảo mật cho dữ liệu.

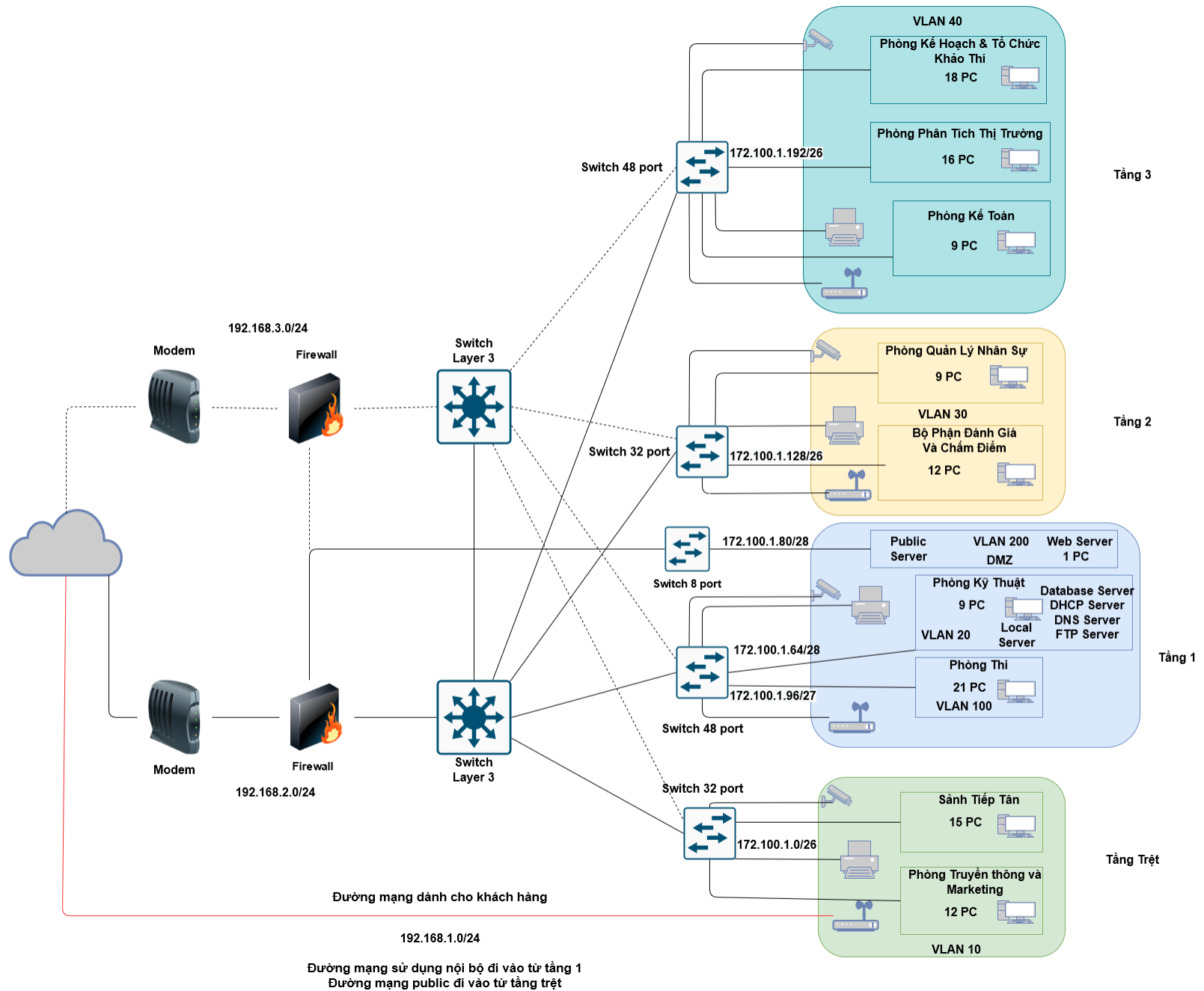
Phần Server và quản trị:

- Đảm bảo các máy tính nội bộ có thể liên lạc được với nhau.
- Mạng nội bộ:
 - Ở mỗi tầng sẽ sử dụng các đường mạng VLAN khác nhau, riêng phòng thi tầng 1 thì có 1 VLAN riêng biệt nối tất cả các máy trong phòng lại với nhau:
 - Tầng trệt: gồm 27 máy sẽ được nối vào Switch Layer 2, Switch Layer 2 nối vào Switch Layer 3 (VLAN 10).

- Tầng 1: 21 máy phòng thi tạo thành 1 VLAN (VLAN 100), tất cả các máy ở phòng kỹ thuật đều nằm trên 1 VLAN khác (VLAN 20).
- Tầng 2 & 3: Các máy ở mỗi tầng lần lượt thuộc VLAN 30 & VLAN 40.
- Phòng máy chủ, lưu trữ gồm có:
 - Database Server
 - DHCP Server
 - DNS Server
 - FTP Server
 - WEB Server
- Firewall: Công ty sẽ có một firewall để kiểm duyệt thông tin ra vào hệ thống. Người ngoài bao gồm cả khách hàng cần sự cho phép của firewall để truy cập dữ liệu của công ty.
- Mạng Internet:
 - Mô hình mạng đảm bảo cho các máy nội bộ có thể truy cập Internet.
 - Website của doanh nghiệp có thể truy xuất từ bên ngoài Internet.

Giai đoạn 2: Logical Network Design

Mô hình Logical, danh sách đường mạng (địa chỉ IP) của mỗi phòng.

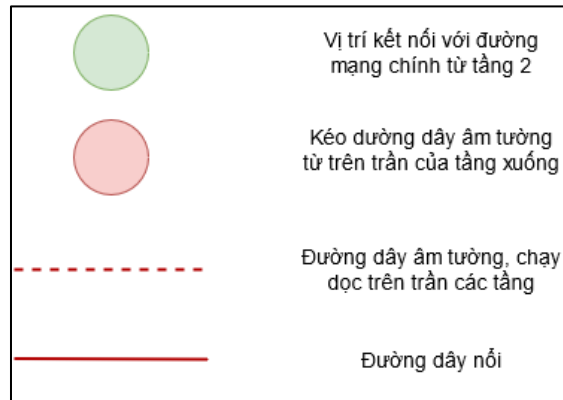
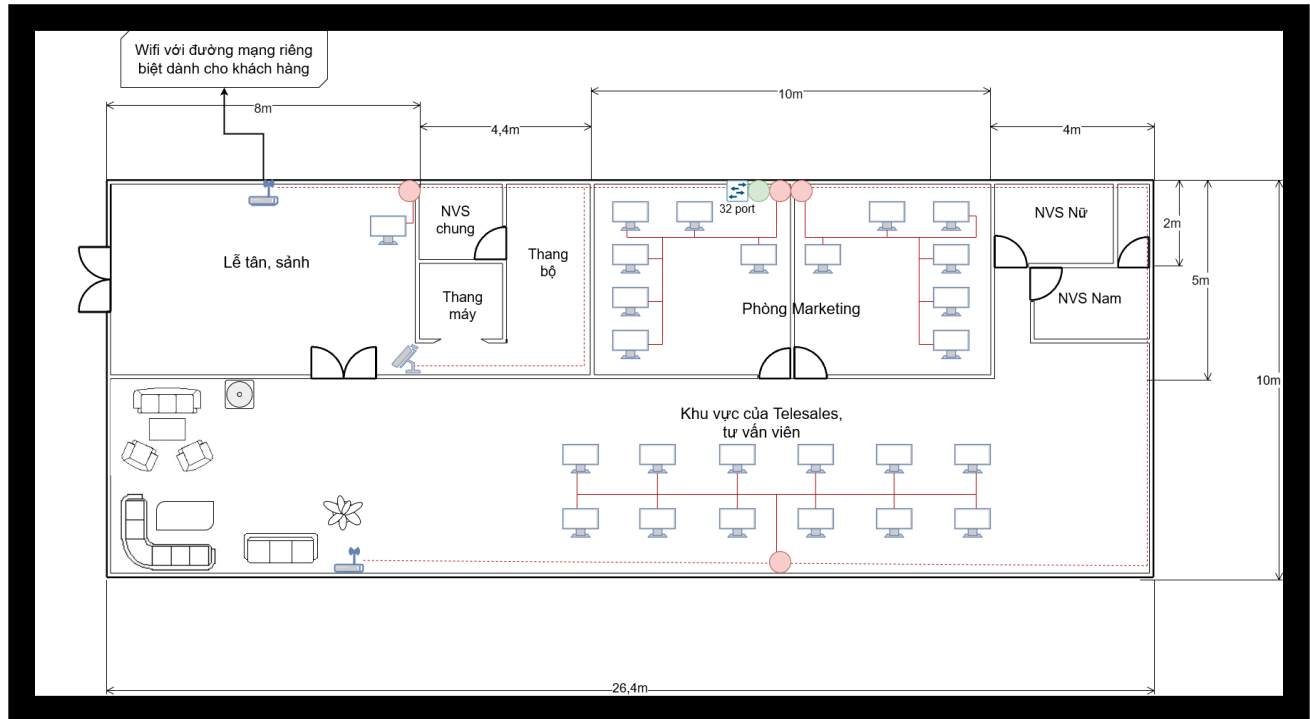


Bảng địa chỉ IP

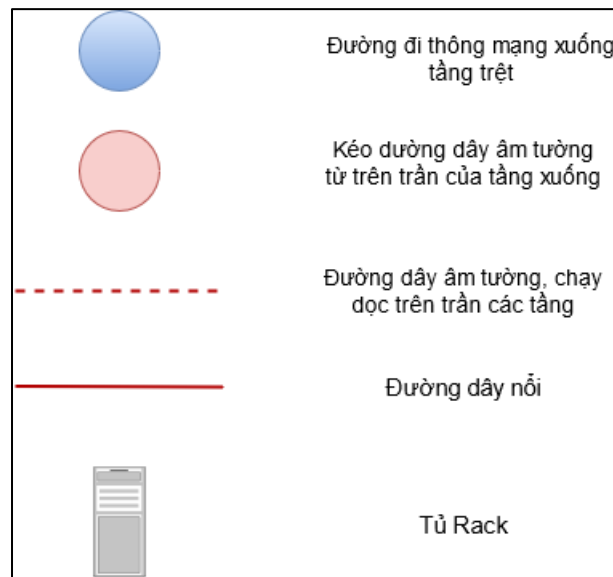
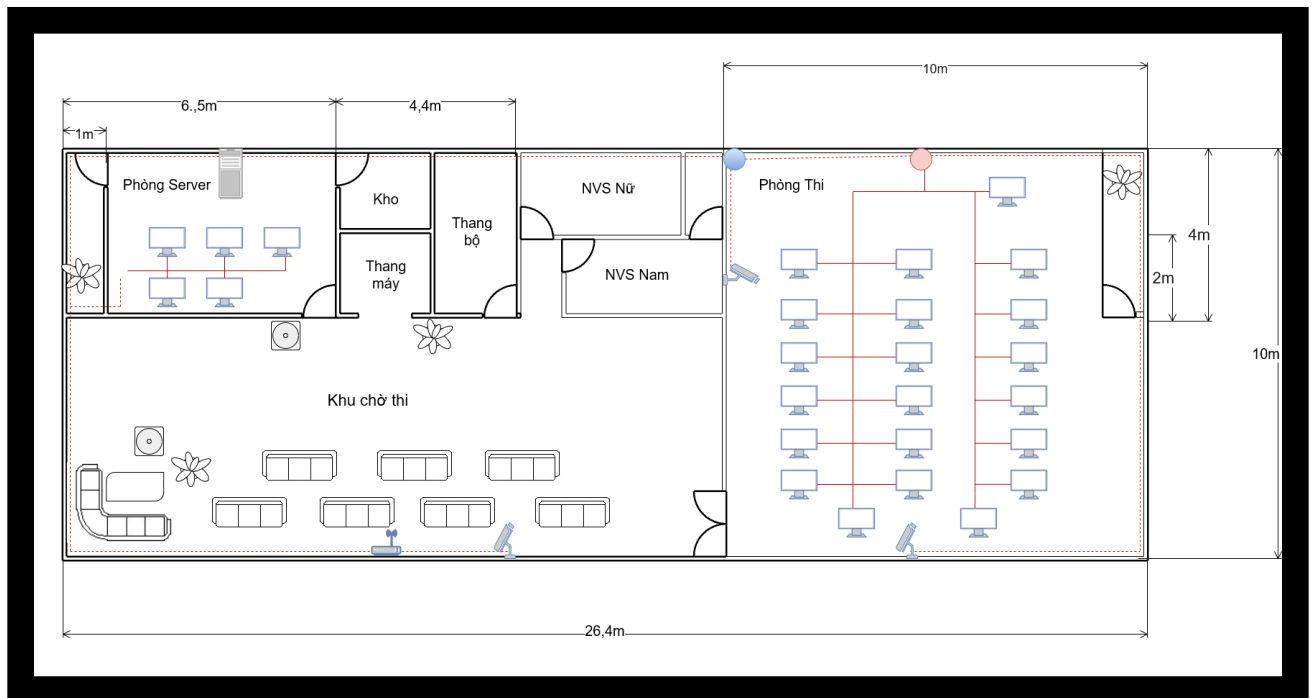
Phòng	Số máy	VLAN	Địa chỉ đường mạng
Sảnh Tiếp Tân	15 PC	VLAN 10	172.100.1.0/26
Phòng Truyền Thông & Marketing	12 PC	VLAN 10	172.100.1.0/26
Phòng Kỹ Thuật	Public Server: 1 Server	VLAN 200	172.100.1.80/28
	9 PC (8 PC & 1 Local Server)	VLAN 20	172.100.1.64/28
Phòng thi	21 PC	VLAN 100	172.100.1.96/27
Bộ Phận Đánh Giá & Chấm Điểm	12 PC	VLAN 30	172.100.1.128/26
Phòng Quản Lý Nhân Sự	9 PC	VLAN 30	172.100.1.128/26
Phòng Kế Toán	9 PC	VLAN 40	172.100.1.192/26
Phòng Phân Tích Thị Trường	16 PC	VLAN 40	172.100.1.192/26
Phòng Kế Hoạch & Tổ Chức Khảo Thí	18 PC	VLAN 40	172.100.1.192/26

Giai đoạn 3: Physical Network Design

❖ Tầng trệt:

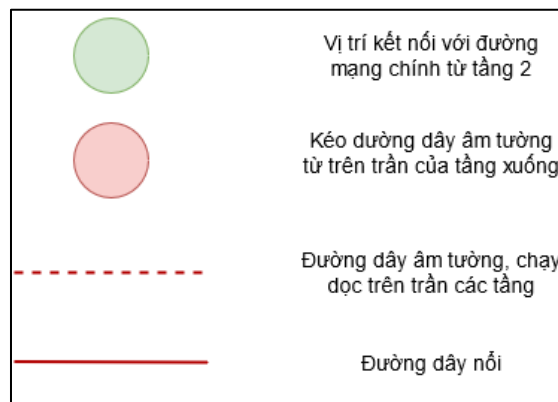
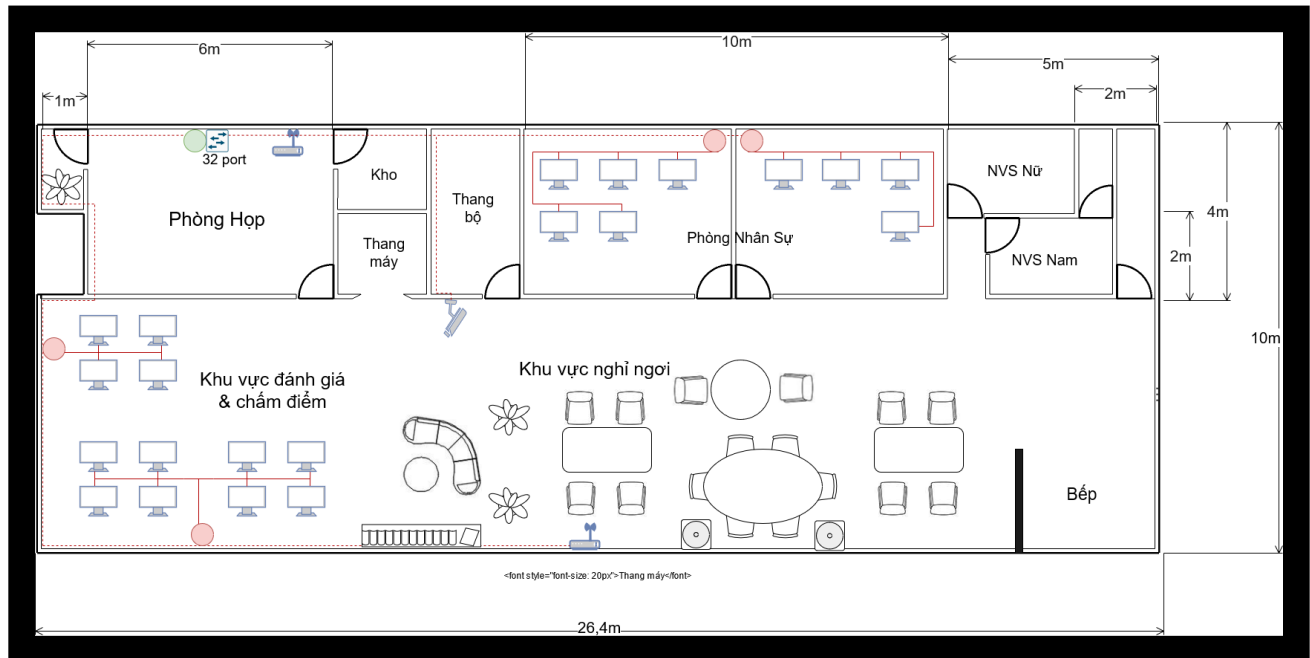


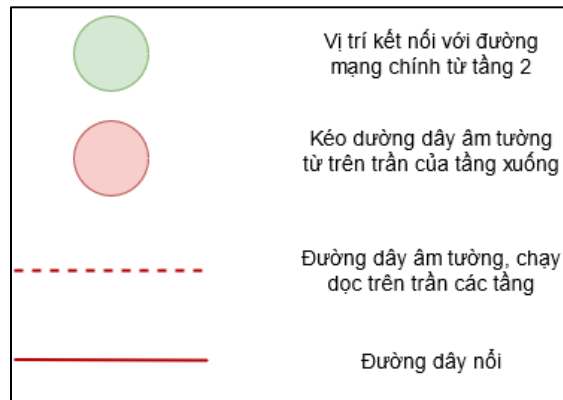
❖ Tầng 1:



Ghi chú: Để tránh các sự cố về bảo mật nên đường đi thông xuống tầng trệt mới nằm ở vị trí xanh dương như trên hình. Đối với các tầng còn lại đường thông mạng trùng vị trí tương ứng với tủ rack ở tầng 1 (kí hiệu màu xanh lá ở các hình dưới).

❖ Tầng 2:



[illegible]

Giai đoạn 4: Simulation Model

Các chính sách của firewall

- Cho phép các máy trên mạng nội bộ truy cập ra ngoài Internet.
- Chỉ cho phép các máy bên ngoài Internet truy cập vào server ở vùng DMZ thông qua giao thức http/https.

```
ciscoasa(config)#sh run
: Saved
:
ASA Version 9.6(1)
!
hostname ciscoasa
names
!
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 203.1.1.1 255.255.255.0
!
interface GigabitEthernet1/3
 nameif DMZ
 security-level 50
 ip address 172.100.1.81 255.255.255.240
!
```

```
object network DMZ
  subnet 172.100.1.80 255.255.255.240
object network INSIDE
  subnet 192.168.2.0 255.255.255.0
object network VLAN10
  subnet 172.100.1.0 255.255.255.192
object network VLAN100
  subnet 172.100.1.96 255.255.255.224
object network VLAN20
  subnet 172.100.1.64 255.255.255.240
object network VLAN30
  subnet 172.100.1.128 255.255.255.192
object network VLAN40
  subnet 172.100.1.192 255.255.255.192
object network WEB_SERVER
  host 172.100.1.82
```

```
route outside 0.0.0.0 0.0.0.0 203.1.1.2 1
route inside 172.100.1.0 255.255.255.192 192.168.2.2 1
route inside 172.100.1.64 255.255.255.240 192.168.2.2 1
route inside 172.100.1.128 255.255.255.192 192.168.2.2 1
route inside 172.100.1.192 255.255.255.192 192.168.2.2 1
route inside 172.100.1.96 255.255.255.224 192.168.2.2 1
route DMZ 172.100.1.80 255.255.255.240 172.100.1.82 1
!
access-list OUTSIDE-TO-DMZ extended permit tcp any object WEB_SERVER eq www
access-list OUTSIDE-TO-DMZ extended permit tcp any host 203.1.1.1 eq www
access-list INSIDE-TO-OUTSIDE extended permit ip 192.168.2.0 255.255.255.0 any
access-list INSIDE-TO-OUTSIDE extended permit icmp 192.168.2.0 255.255.255.0 any
!
!
access-group OUTSIDE-TO-DMZ in interface outside
```



```
object network DMZ
  nat (DMZ,outside) dynamic interface
object network INSIDE
  nat (inside,outside) dynamic interface
object network VLAN10
  nat (inside,outside) dynamic interface
object network VLAN100
  nat (inside,outside) dynamic interface
object network VLAN20
  nat (inside,outside) dynamic interface
object network VLAN30
  nat (inside,outside) dynamic interface
object network VLAN40
  nat (inside,outside) dynamic interface
object network WEB_SERVER
  nat (DMZ,outside) static 203.1.1.1
```

```
class-map inspection_default
  match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect tftp
policy-map global
  class inspection_default
    inspect http
    inspect icmp
policy-map web-server
  class inspection_default
    inspect http
    inspect icmp
!
service-policy global_policy global
service-policy global interface inside
service-policy web-server interface outside
```

```
router ospf 1
 log-adjacency-changes
 network 192.168.2.0 255.255.255.0 area 0
 network 172.100.1.80 255.255.255.240 area 0
```

Giai đoạn 5: Documenting

1. Thiết bị:

Danh sách thiết bị cần mua mới:

Thiết bị	Số lượng	Yêu cầu chức năng	Nhà sản xuất	Giá thành
Server Dell PowerEdge T440	4	Triển khai các dịch vụ cần thiết	Dell	55.900.000 VND/cái
Firewall ASA5506-K9 (Cisco ASA 5506-X)	2	Bảo vệ mạng LAN, điều khiển truy cập	Cisco	12.500.000 VND/cái
Modem ADSL TP-Link TD8840	2	Chuyển đổi tín hiệu	TP-Link	350.000 VND/cái
Switch Layer 3 Cisco WS-C3650-24TS-S	2	Trung gian kết nối Switch & Router	Cisco	42.350.000VND/Cái
Switch Cisco 48 port	2	Các thiết bị giao tiếp được với nhau trong cùng vlan	Cisco	15.000.000 VND/cái
Switch Cisco 32 port	2		Cisco	12.000.000 VND/cái
Switch Cisco 8 port	1		Cisco	1.200.000 VND/cái
Máy in đa năng HP Laser MFP 137fnw 4ZB84A	3	In ấn tài liệu	HP	3.990.000 VND/máy
Máy Photocopy Ricoh MP 5001	3		Ricoh	20.000.000 VND/máy
Cáp Cat5e UTP (2/2020)	3	Đường truyền tải mạng	COMMSCOPE	2.150.000 VND/thùng
Wifi Router	7	Kết nối mạng qua sóng vô tuyến	TP-Link	500.000 VND/Cái
Dây điện Cadivi 2.5	4	Cung cấp điện cho hệ thống		1.000.000 VND/cuộn (1 cuộn = 100m)
Tổng chi phí				475.150.000 VND

2. Công nghệ:

Danh sách công nghệ sử dụng:

Tên ứng dụng	Yêu cầu chức năng	Nhà sản xuất	Giá thành bản quyền (1 tháng/năm)
Windows Server 2016	Server quản lý các dịch vụ cần thiết của doanh nghiệp	Microsoft	10.000.000 VND/Tháng

3. Ưu khuyết điểm công nghệ, thiết bị:

- Ưu điểm: hầu hết đều là những công nghệ, thiết bị phổ biến, giá thành ổn
- Nhược điểm: Cần người có chuyên môn hỗ trợ về phần mềm và thiết bị, khó để mở rộng quy mô nếu như không mua thêm thiết bị mới.

4. Dịch vụ và thiết bị khác

Tên dịch vụ	Giá thành
Internet (Viettel)	7.700.000 VND/Tháng
Tên miền .vn	450.000 VND/Năm
Hosting	130.000 VND/Tháng
Tổng chi phí	8.280.000 VND/Tháng

5. Tổng chi phí

- Chi phí thiết bị: 475.150.000 VND
- Chi phí dịch vụ hàng tháng: 18.280.000 VND/Tháng

Tự đánh giá đề tài

Đối với đề tài này, nhóm tin rằng hệ thống mạng này có thể đáp ứng được cơ bản những yêu cầu của doanh nghiệp, dù vẫn còn đó những điểm chưa tốt vì thiếu kinh nghiệm thực tế.

Tài liệu tham khảo

Các bài làm mẫu và tài liệu tham khảo trên Moodle