

KHO BẠC NHÀ NƯỚC
BAN CÔNG NGHỆ THÔNG TIN VÀ CHUYỂN ĐỔI SỐ

TÓM TẮT THIẾT KẾ CHI TIẾT
DỰ ÁN “ĐẦU TƯ HỆ THỐNG MẠNG LAN CƠ
QUAN KHO BẠC NHÀ NƯỚC”

*(Đính kèm HSMT gói thầu: Đầu tư hệ thống mạng LAN cơ
quan Kho bạc Nhà nước)*

Hà Nội, 2025

8. THIẾT KẾ CHI TIẾT

8.1. Các chỉ tiêu kỹ thuật áp dụng trong triển khai lắp đặt, cài đặt, kiểm tra và hiệu chỉnh thiết bị

- Việc lắp đặt, cài đặt thực hiện theo tài liệu hướng dẫn lắp đặt, cài đặt của nhà sản xuất thiết bị.

- Phải đáp ứng các tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước ban hành theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông.

- Phải đáp ứng các tiêu chuẩn kỹ thuật theo quy định tại Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông Quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu và Thông tư số 23/2022/TT-BTTTT ngày 30 tháng 11 năm 2022 sửa đổi, bổ sung một số điều của thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 của Bộ thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với trung tâm dữ liệu.

- Việc lắp đặt, cài đặt không được làm ảnh hưởng đến hệ thống hiện có.

- Việc kiểm tra hiệu chỉnh thiết bị sử dụng các phần mềm kèm theo thiết bị của hãng cung cấp, đối chiếu với tiêu chuẩn kỹ thuật yêu cầu trong dự án nêu trên.

8.4. Chỉ dẫn biện pháp triển khai (đối với trường hợp triển khai phức tạp)

- Việc triển khai nâng cấp hệ thống mạng LAN phải đảm bảo đúng tiến độ, chất lượng theo kế hoạch đề ra và vừa đảm bảo không gián đoạn các hoạt động nghiệp vụ.

- Phải chuyển đổi và đảm bảo an toàn tuyệt đối đối với toàn bộ dữ liệu hệ thống, dữ liệu người dùng trong hệ thống.

- Nhằm đảm bảo hệ thống vận hành liên tục, không bị gián đoạn công việc chuyên môn của các cán bộ Khoa bạc Nhà nước, trong quá trình thực hiện dự án, các phương án dự phòng cần được thực hiện như sau:

+ Mọi công tác liên quan đến chuyển đổi hệ thống cũ sang hệ thống mới cần được thực hiện vào thời điểm ngoài giờ hành chính.

+ Quá trình chuyển đổi hệ thống cần được thực hiện theo từng module (hệ thống chuyển mạch vùng Server, các thiết bị tường lửa, hệ thống mạng Wireless, thiết bị chuyển mạch Core Switch, ...).

8.5. Biện pháp an toàn vận hành, phòng, chống cháy, nổ

8.5.1. Yêu cầu chung

Trang bị các phương tiện bảo hộ để tạo điều kiện thuận tiện cho người lao động, thích ứng với môi trường xung quanh và bảo đảm điều kiện lao động tốt nhất.

Các phương tiện bảo hộ cho người lao động không gây ra các yếu tố nguy hiểm và có hại trong quá trình lắp đặt.

Phương tiện bảo vệ cần đảm bảo hiệu quả cao và thuận tiện

Trong từng trường hợp của mỗi loại công việc, lựa chọn phương tiện bảo vệ tính đến yêu cầu an toàn cho từng công việc đó.

Các phương tiện bảo hộ đảm bảo các chỉ tiêu an toàn, vệ sinh lao động...

8.5.2. Yêu cầu về tuân thủ các tiêu chuẩn kỹ thuật

Thi công đúng theo yêu cầu kỹ thuật, đảm bảo chất lượng.

Một yếu tố quan trọng nữa là công cụ dùng để lắp đặt cũng phải là các thiết bị chuyên dụng và được sử dụng đúng chức năng.

Các thiết bị hệ thống mạng là các thiết bị chuyên dụng, đắt tiền do vậy trong quá trình thi công cần thực hiện đúng các quy trình, quy phạm của Ngành, bản vẽ thiết kế thi công xây lắp và tài liệu hướng dẫn của nhà sản xuất.

Quy trình đi dây phải đảm bảo đúng kỹ thuật, cẩn thận, chắc chắn ngay ngắn và có mỹ quan.

An toàn trong vận hành khai thác là một tiêu chí quan trọng của thiết kế kỹ thuật thi công công trình.

Đơn vị thi công cần lập phương án an toàn lao động để đảm bảo an toàn cho người lao động và thiết bị trong suốt quá trình thi công.

Khi làm việc trên cao cần dùng thang đảm bảo an toàn.

Khi thi công trong phòng có thiết bị thông tin đang khai thác cần có các phương án đảm bảo tuyệt đối không làm ảnh hưởng đến sự cố cho hệ thống thông tin.

Đảm bảo an toàn thông tin và an toàn dữ liệu của đơn vị khi chuyển đổi.

Trong quá trình thi công phải đảm bảo không làm ảnh hưởng đến vệ sinh môi trường ở khu vực thi công công trình và nơi công cộng.

8.5.3. An toàn điện, an toàn thiết bị

Khi thi công, bố trí cấp nguồn điện phải riêng rẽ để có khả năng cắt điện toàn bộ phụ tải điện trong phạm vi từng hạng mục công trình hay một số khu vực sản xuất.

Việc tháo dỡ dây dẫn, sửa chữa hiệu chỉnh thiết bị điện phải do công nhân điện có trình độ về kỹ thuật an toàn điện thích hợp với từng loại công việc tiến hành.

Các thiết bị điện di động, máy điện cầm tay và đèn điện xách tay khi nối vào lưới điện phải qua ổ cắm, phích cắm hoặc cầu dao điện. Việc đấu, nối phải thỏa mãn các yêu cầu về kỹ thuật an toàn điện.

Trước khi lắp ráp và sửa chữa điện hay thiết bị, phải cắt cầu dao cấp điện cho khu vực thao tác và tại cầu dao đó treo bảng “Cấm đóng điện! Có người làm việc”. Nếu cầu dao đó nằm ngoài trạm biến áp (cầu dao phân đoạn, rẽ nhánh) ngoài các biện pháp trên phải tiếp đất và ngắt mạch các pha phía đầu nguồn, các nguồn có khả năng dẫn dòng điện tới.

Các dụng cụ cầm tay: Khoan điện, đèn xách tay, máy biến áp, hạ áp, bộ biến đổi tần số... cần phải thực hiện các yêu cầu:

Trước khi cấp phát dụng cụ mới phải kiểm tra cách điện với vỏ, thông mạch nối đất, Xem cấu tạo bảo vệ có phù hợp với điều kiện sử dụng hay không. Nghiêm cấm sử dụng các dụng cụ điện cầm tay có dấu hiệu hư hỏng.

Trước khi sử dụng các dụng cụ điện cầm tay, công nhân phải thực hiện kiểm tra các mạch nối đất, các chi tiết quay, tình trạng của chổi than, vành góp.

Các cầu dao điện, máy tự ngắt phải có vỏ hoặc hộp bảo vệ, các phần dẫn điện của thiết bị điện cần được cách ly, có hàng rào che chắn, có biện pháp ngăn ngừa người không có phận sự tiếp xúc với nó.

Khi sử dụng thiết bị, đường dây điện cần tránh khả năng phát nóng do quá tải hoặc các mối nối không tốt.

8.5.4. An toàn thi công

Phổ biến kiến thức cho công nhân về vấn đề an toàn lao động, an toàn điện, an toàn cháy nổ. Nội quy công trường.

Trang bị cho công nhân các phương tiện bảo vệ cần thiết cho quá trình thi công.

Thường xuyên kiểm tra các phương tiện phòng hộ trước và trong khi sử dụng.

Trong quá trình thi công, phối hợp với các đơn vị khác để có biện pháp ngăn chặn hỏa hoạn, mất an toàn lao động.

8.5.5. Nội quy

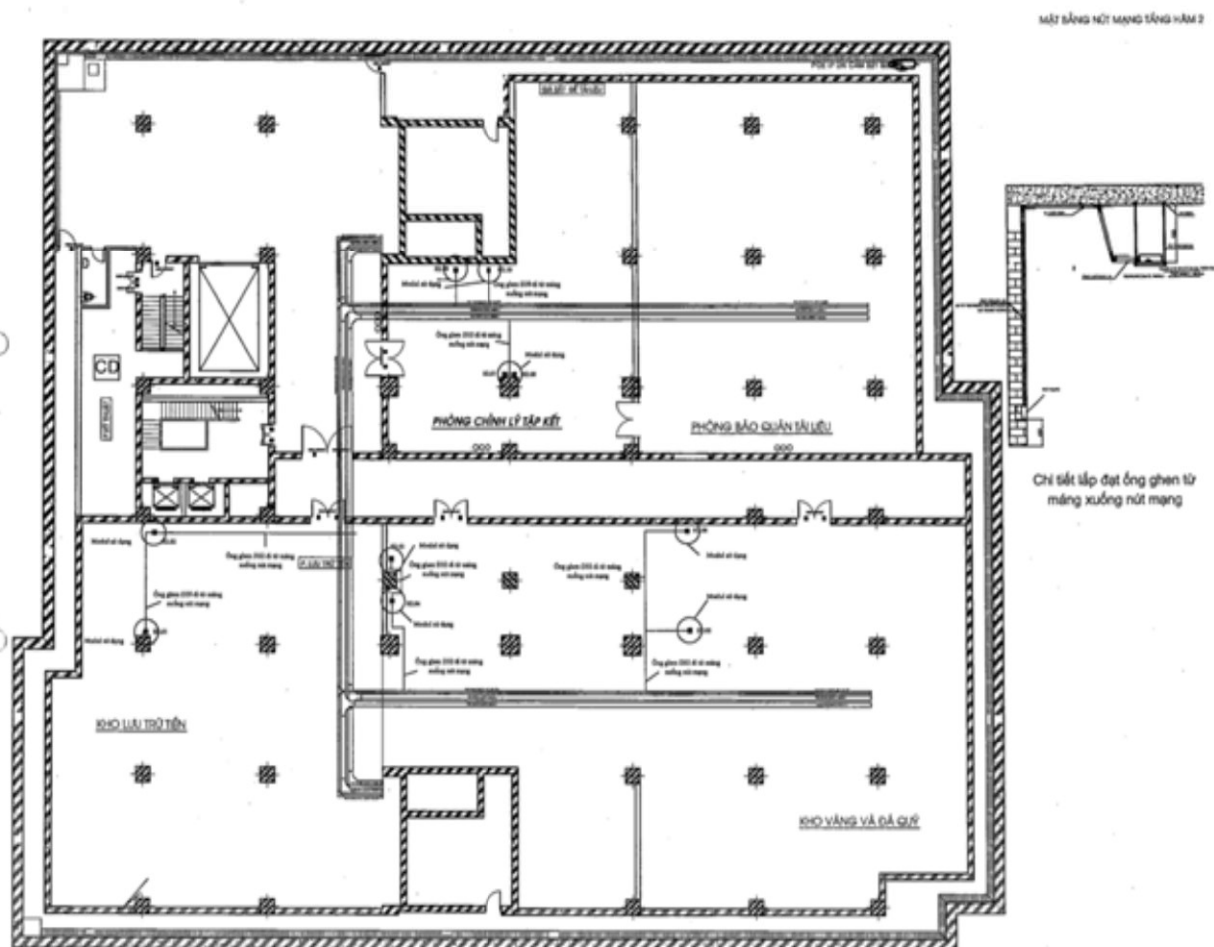
Phối hợp với chủ đầu tư trong công việc thực hiện nội quy chung

Xử lý sai phạm nội quy theo như quy định của công trình.

8.6. Sơ đồ mặt bằng hiện trạng

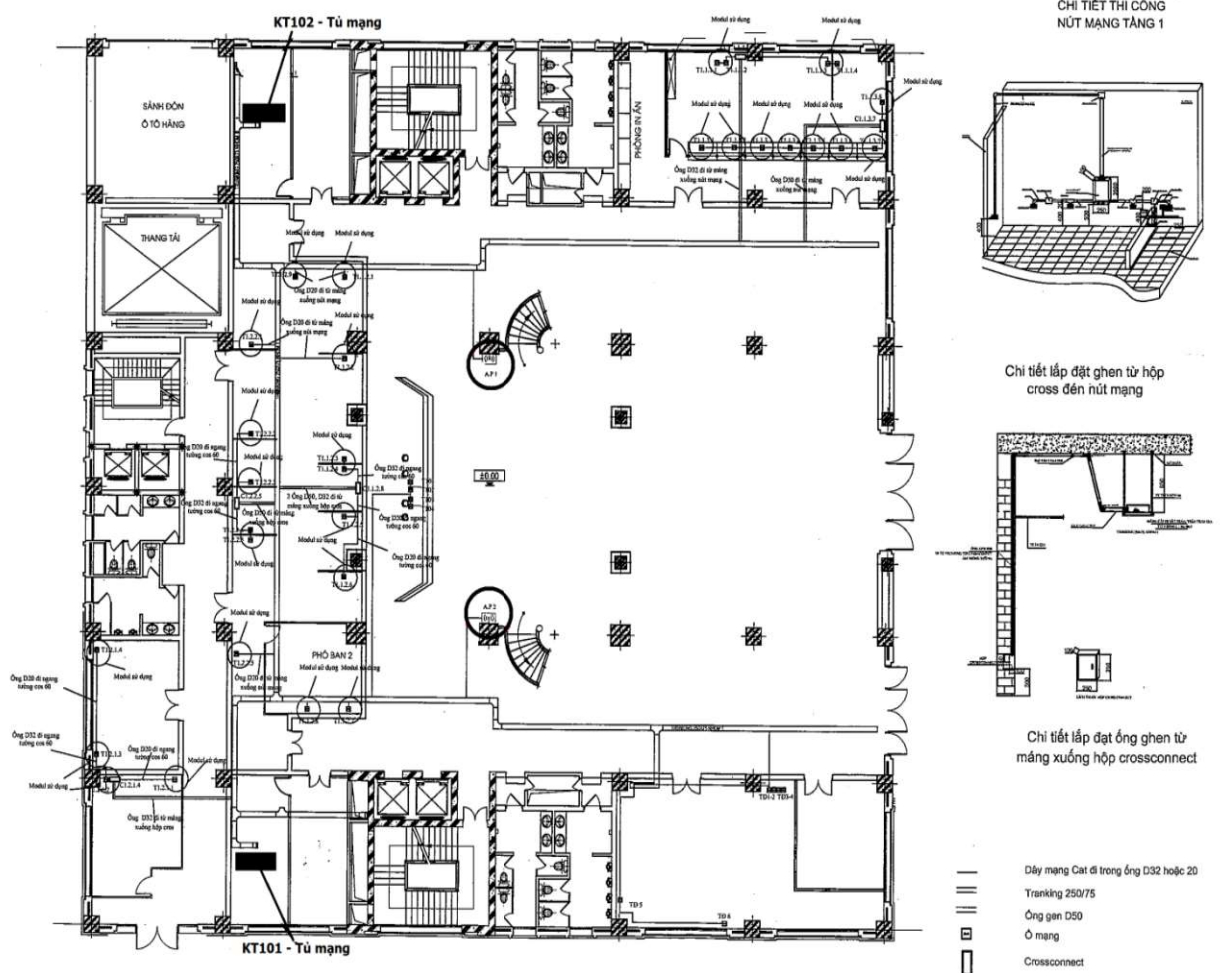
8.6.1. Hiện trạng mặt bằng tại các tầng cơ quan KBNN

8.6.1.1. Sơ đồ mặt bằng và kết nối mạng tại tầng hầm



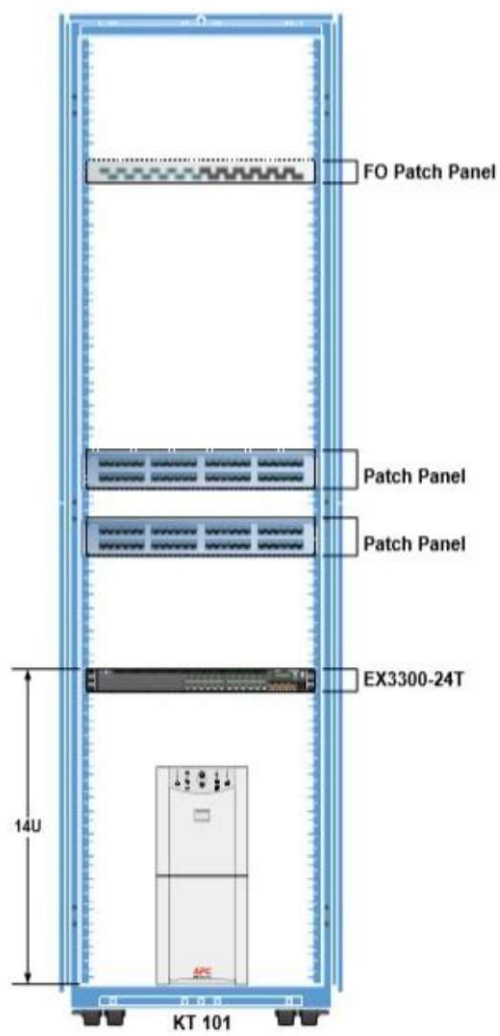
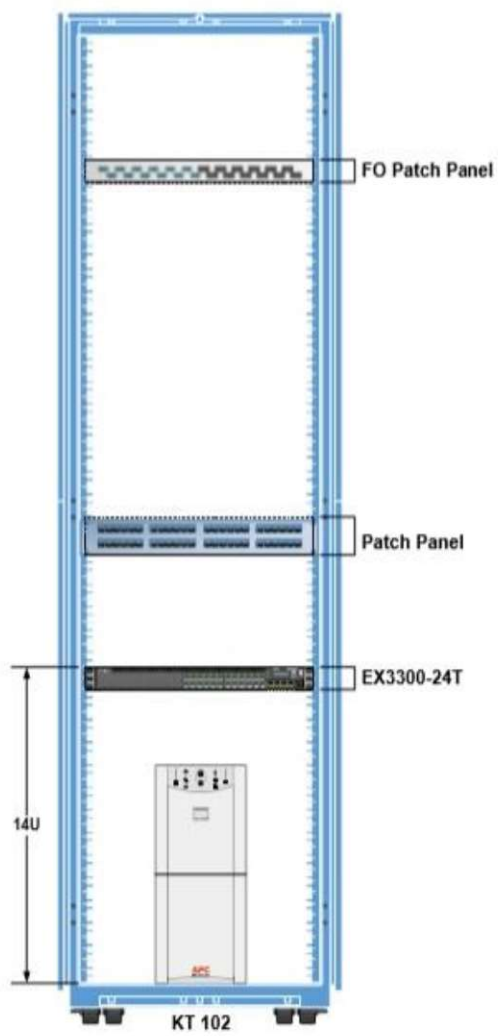
8.6.1.2. Sơ đồ mặt bằng và kết nối mạng tại tầng 1

Sơ đồ mặt bằng tầng 1:



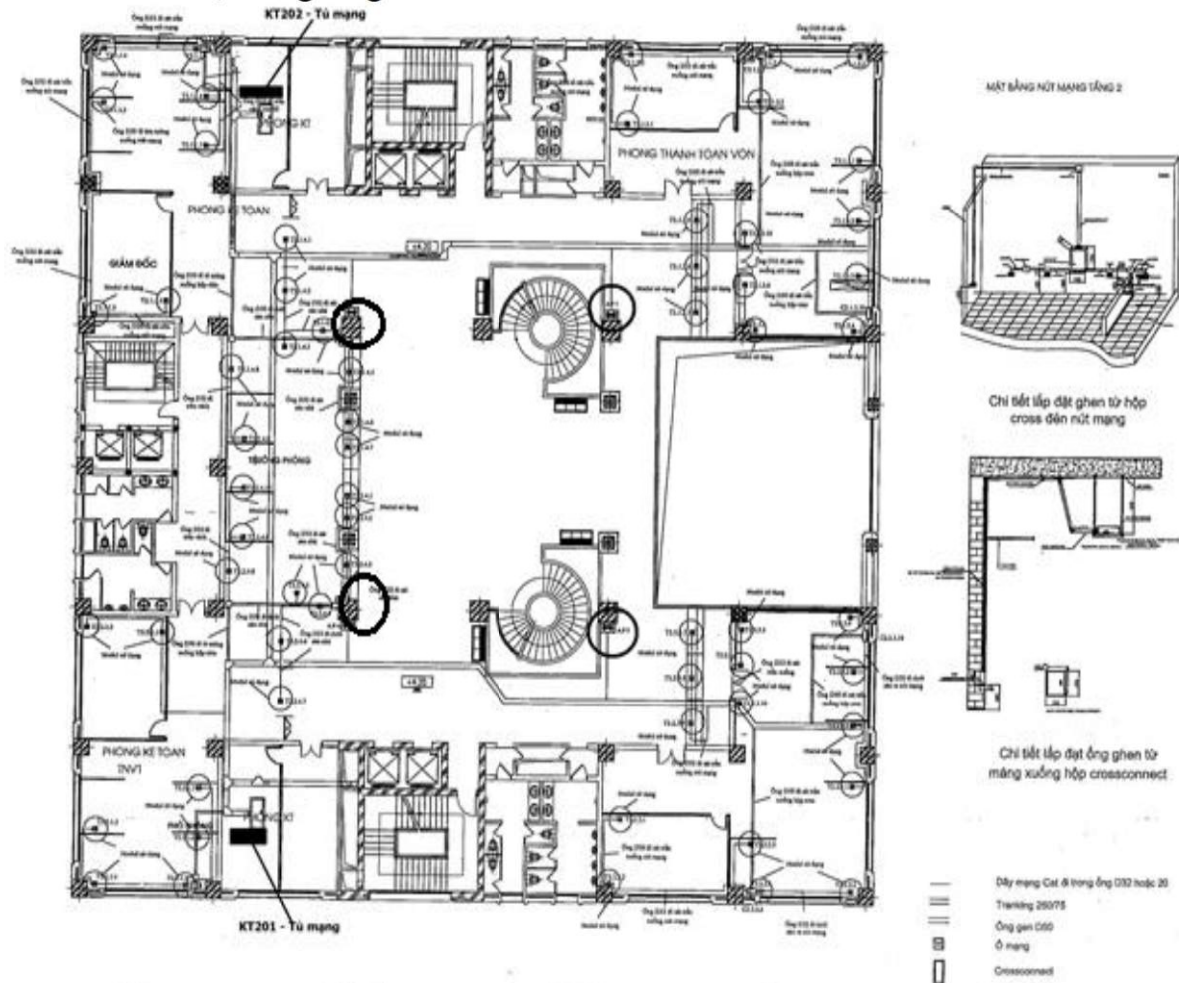
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 1:



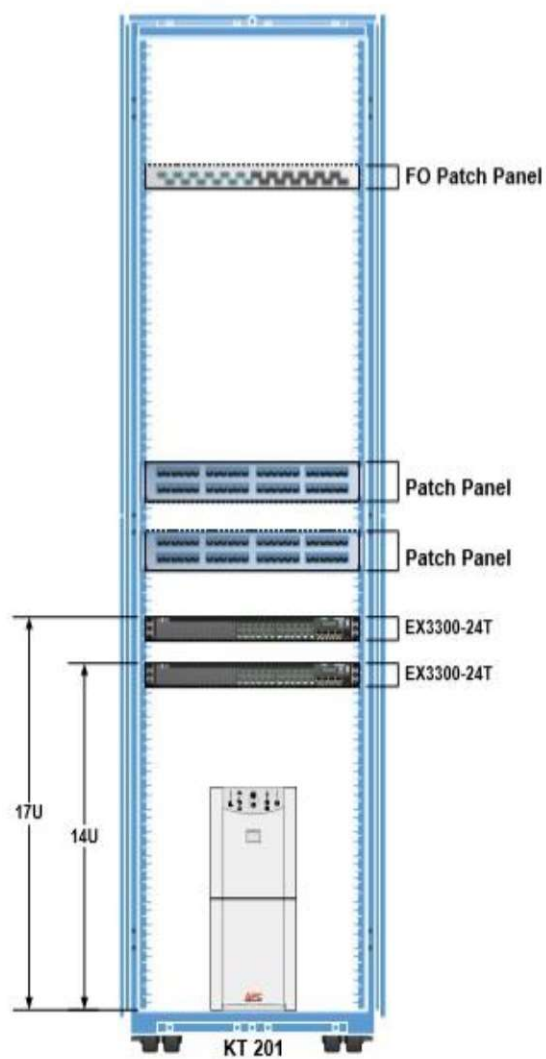
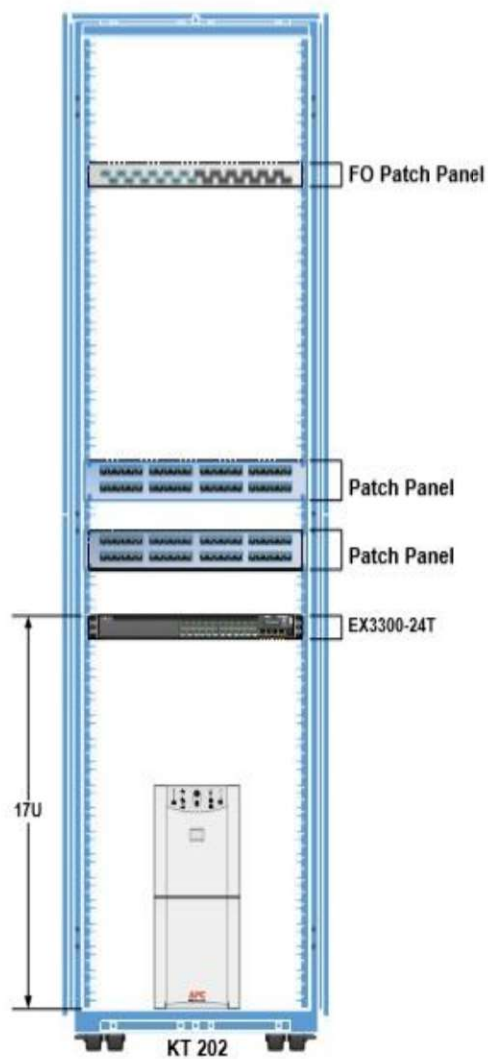
8.6.1.3. Sơ đồ mặt bằng và kết nối mạng tại tầng 2

Sơ đồ mặt bằng tầng 2:



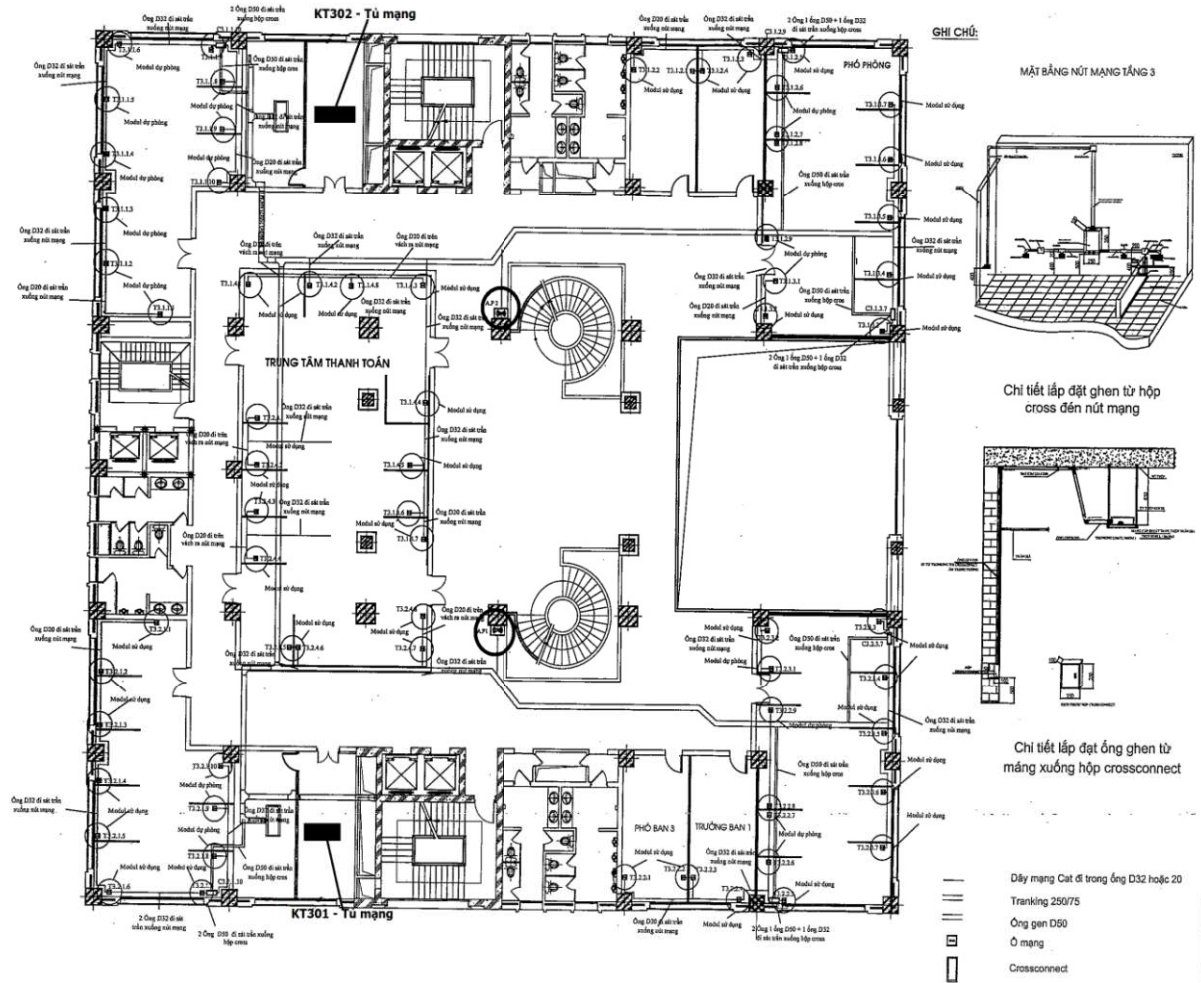
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 2:



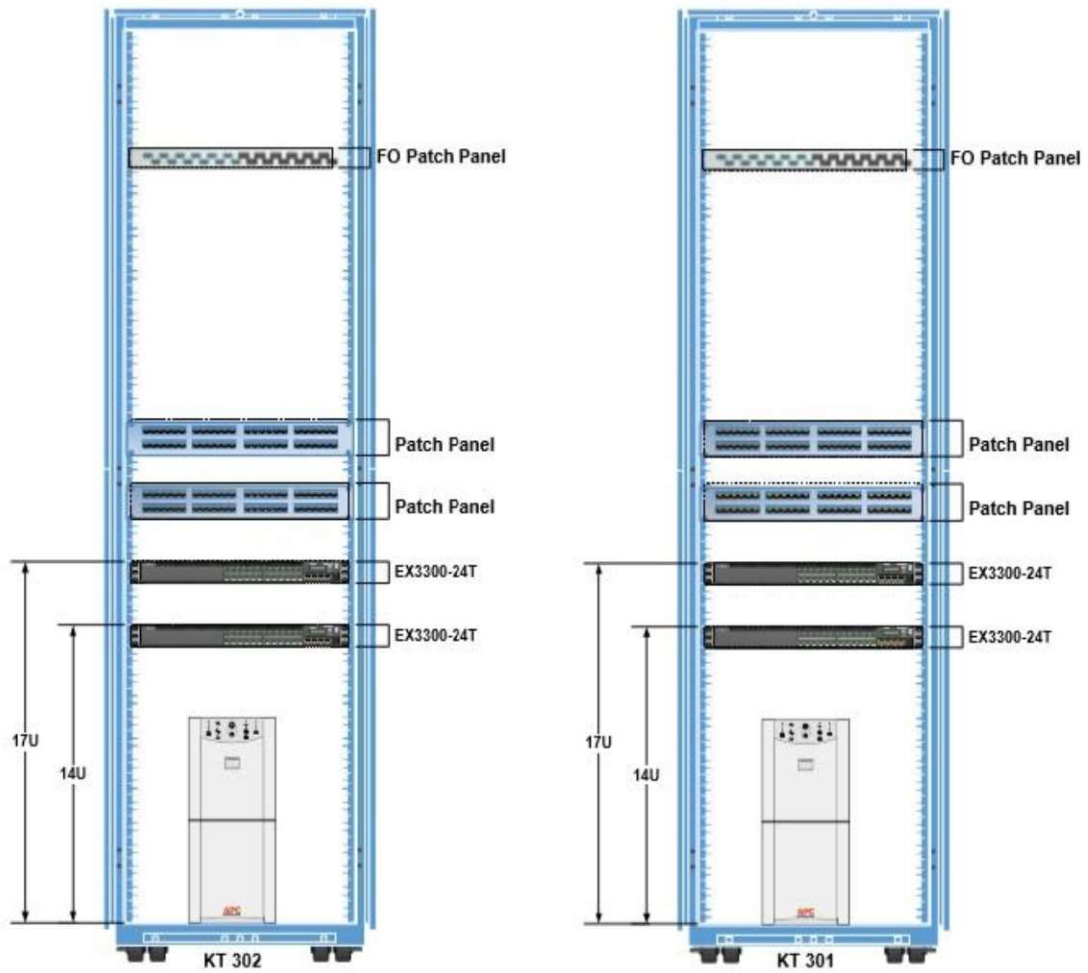
8.6.1.4. Sơ đồ mặt bằng và kết nối mạng tại tầng 3

Sơ đồ mặt bằng tầng 3:



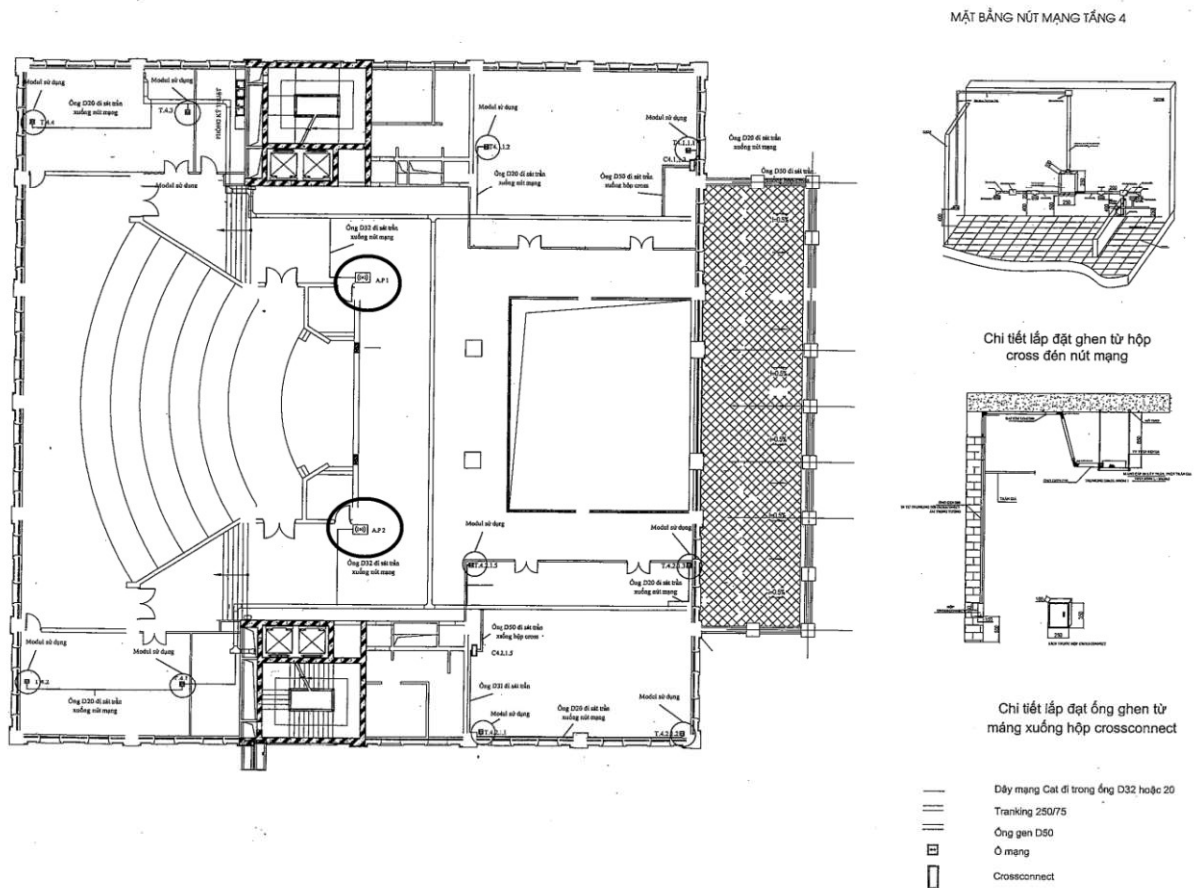
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 3:



8.6.1.5. Sơ đồ mặt bằng và kết nối mạng tại tầng 4

Sơ đồ mặt bằng tầng 4:

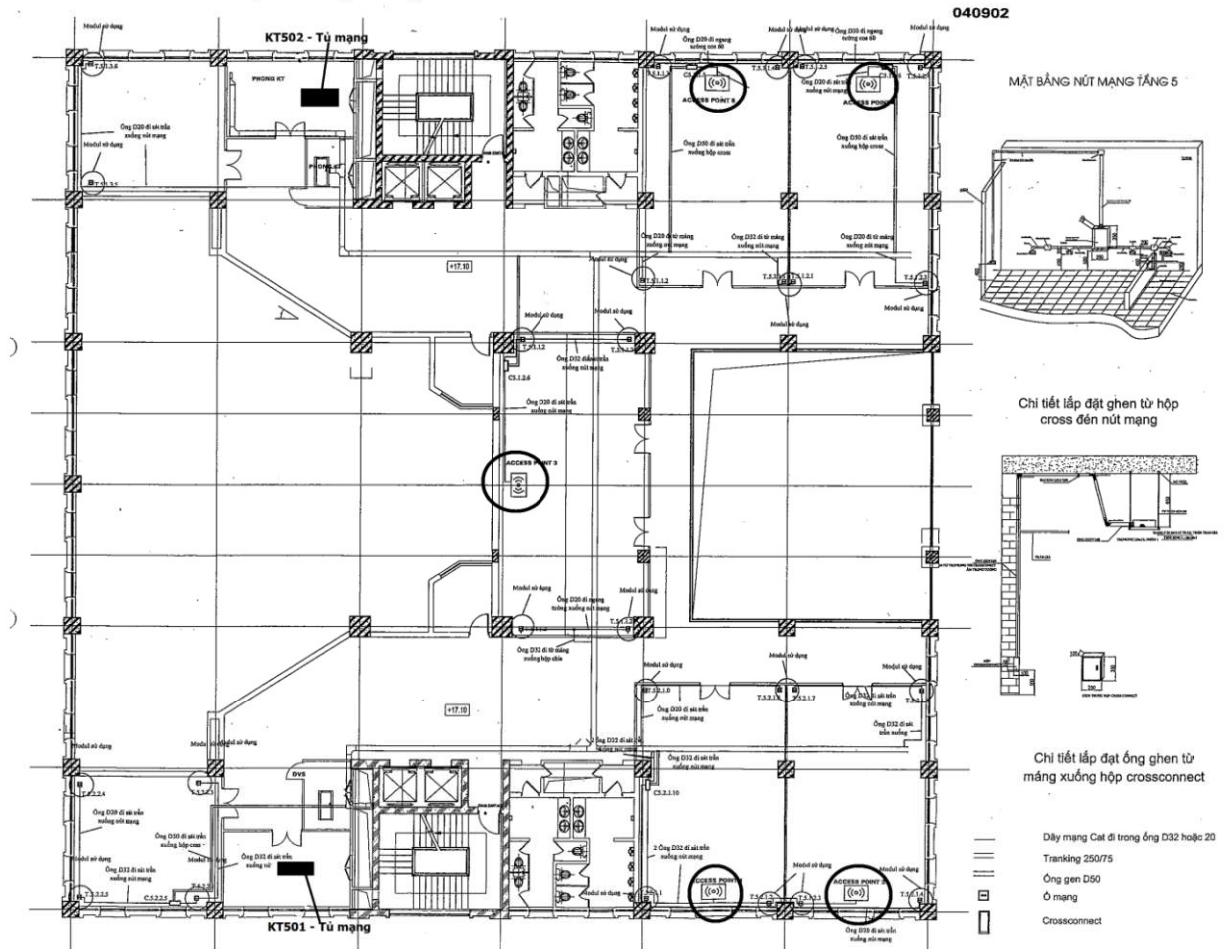


Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 4: Tại tầng 4 không đặt tủ mạng, các thiết bị đầu cuối kết nối mạng với tủ mạng đặt tại tầng 5

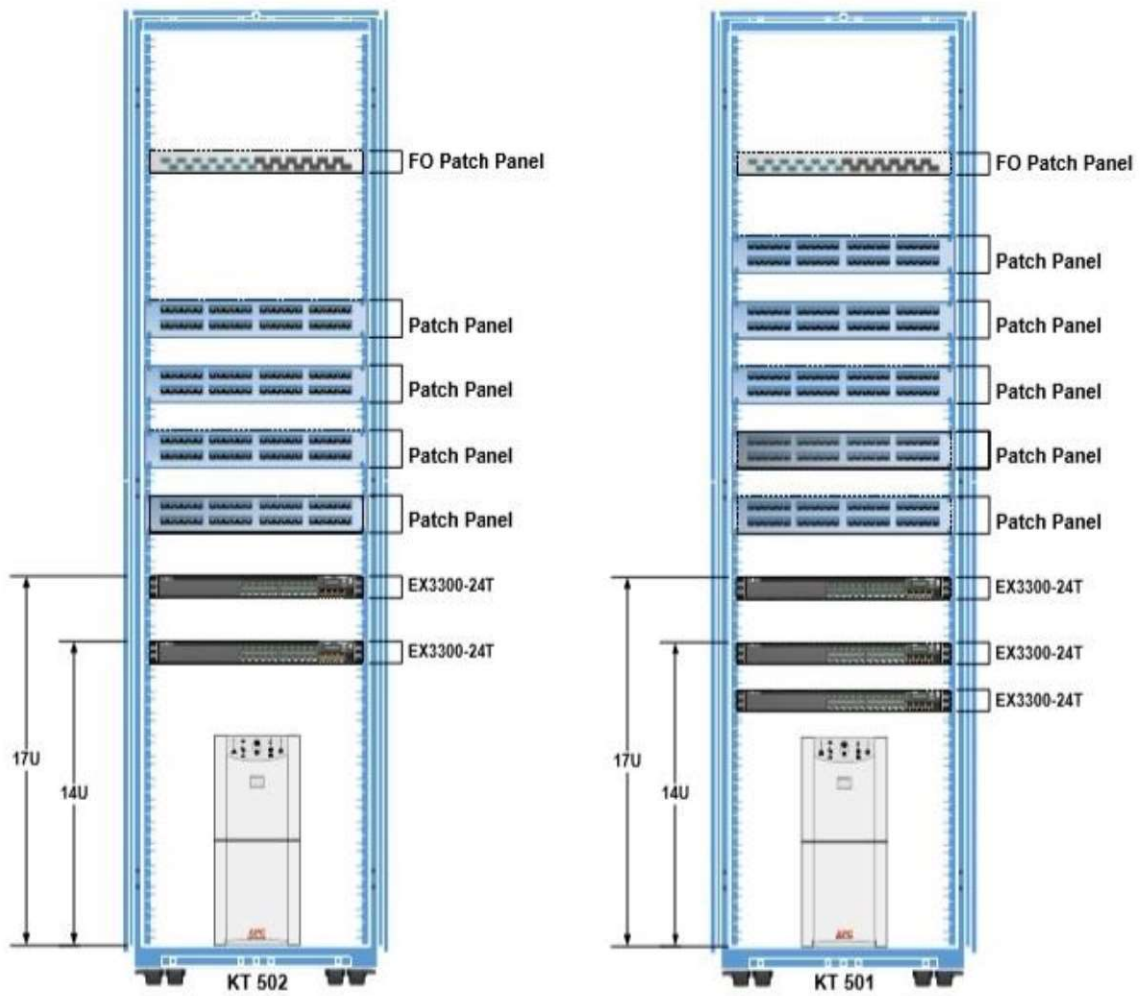
8.6.1.6. Sơ đồ mặt bằng và kết nối mạng tại tầng 5

Sơ đồ mặt bằng tầng 5:



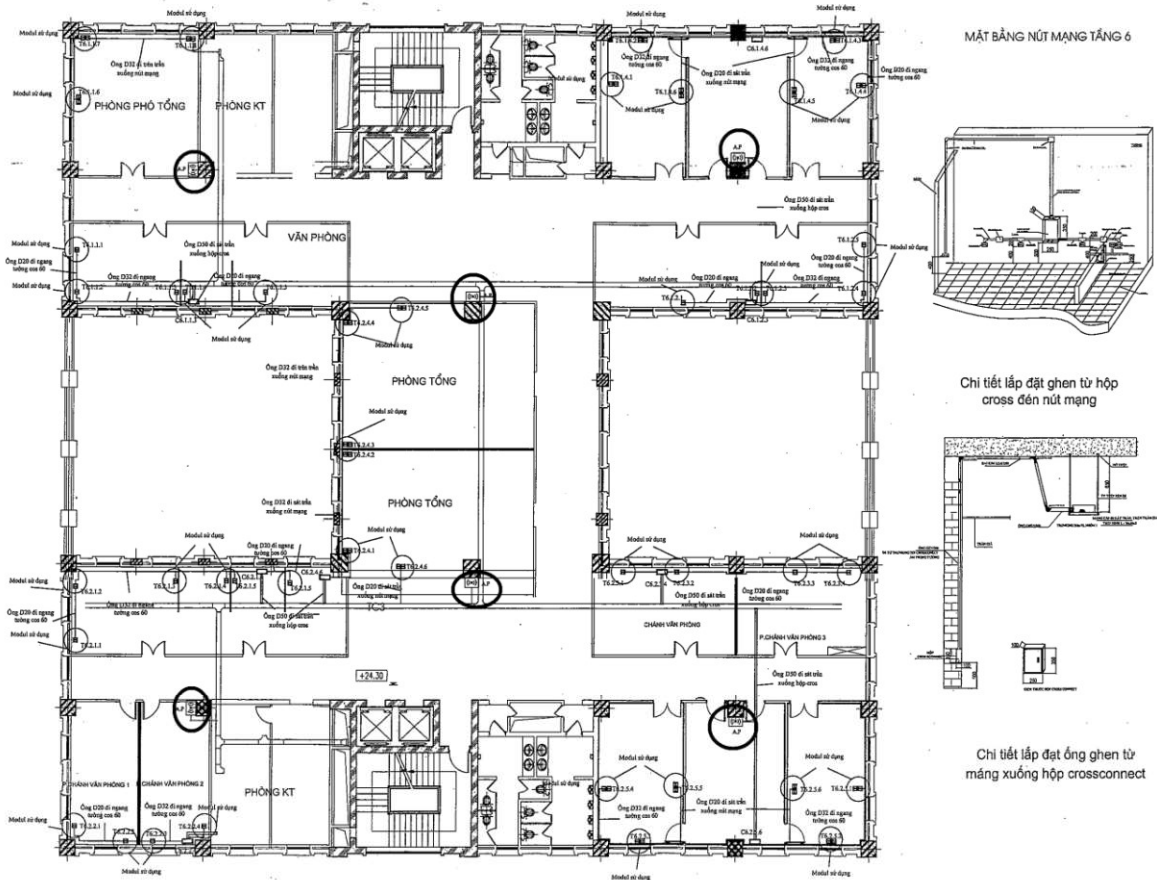
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 5:



8.6.1.7. Sơ đồ mặt bằng và kết nối mạng tại tầng 6

Sơ đồ mặt bằng tầng 6:

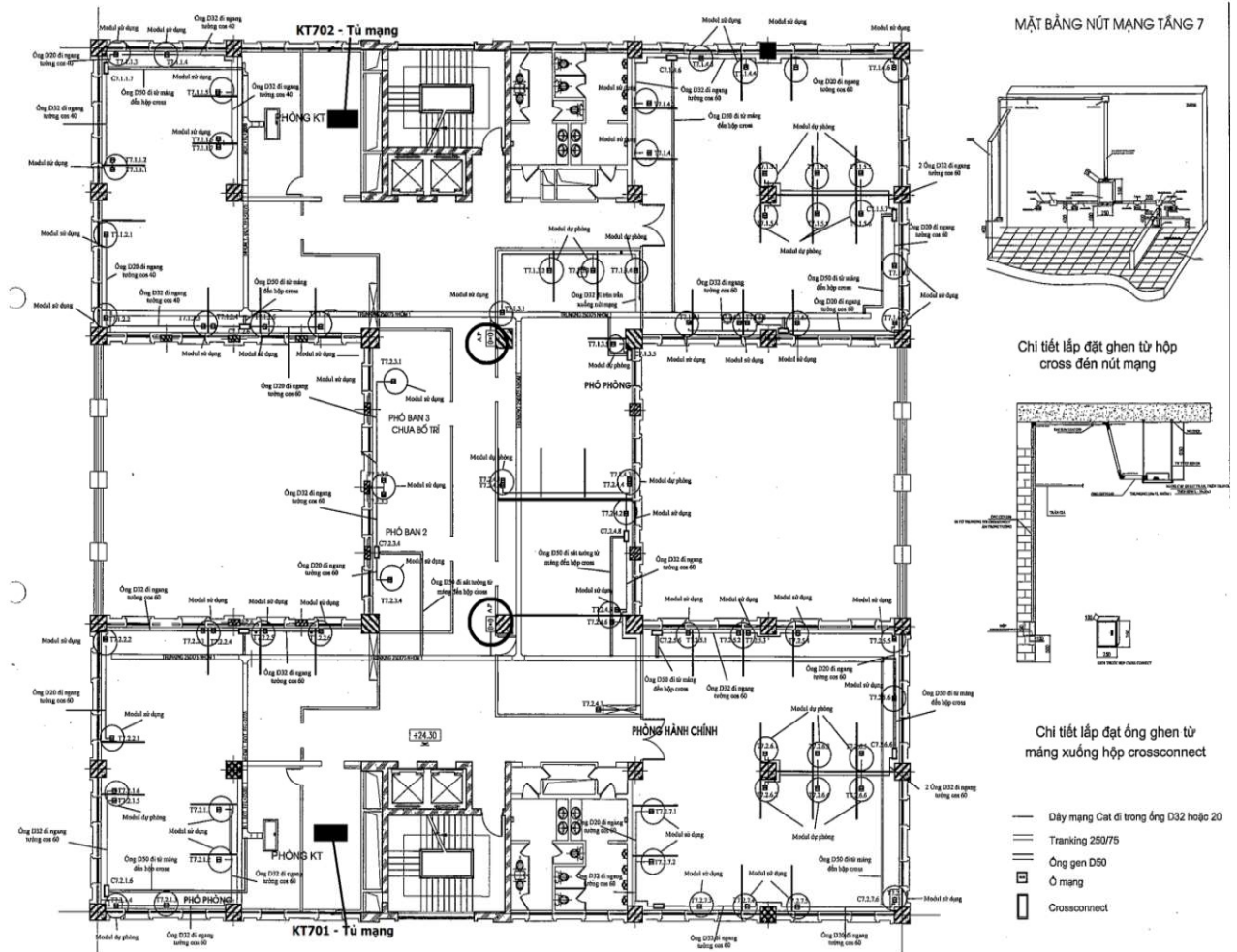


Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

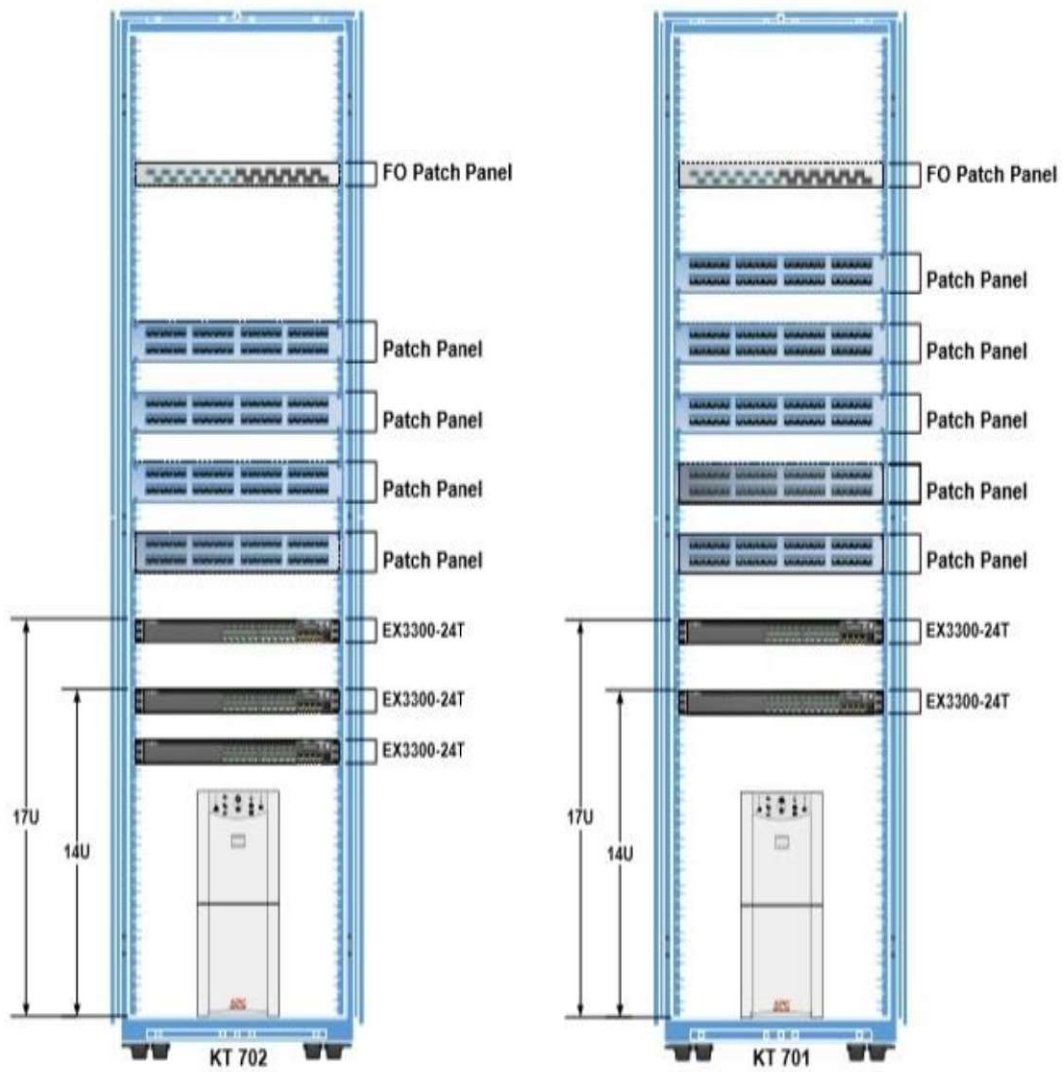
Sơ đồ tủ mạng tầng 6: Tại tầng 6 không đặt tủ mạng, các thiết bị đầu cuối kết nối mạng với tủ mạng đặt tại tầng 5

8.6.1.8. Sơ đồ mặt bằng và kết nối mạng tại tầng 7

Sơ đồ mặt bằng tầng 7:

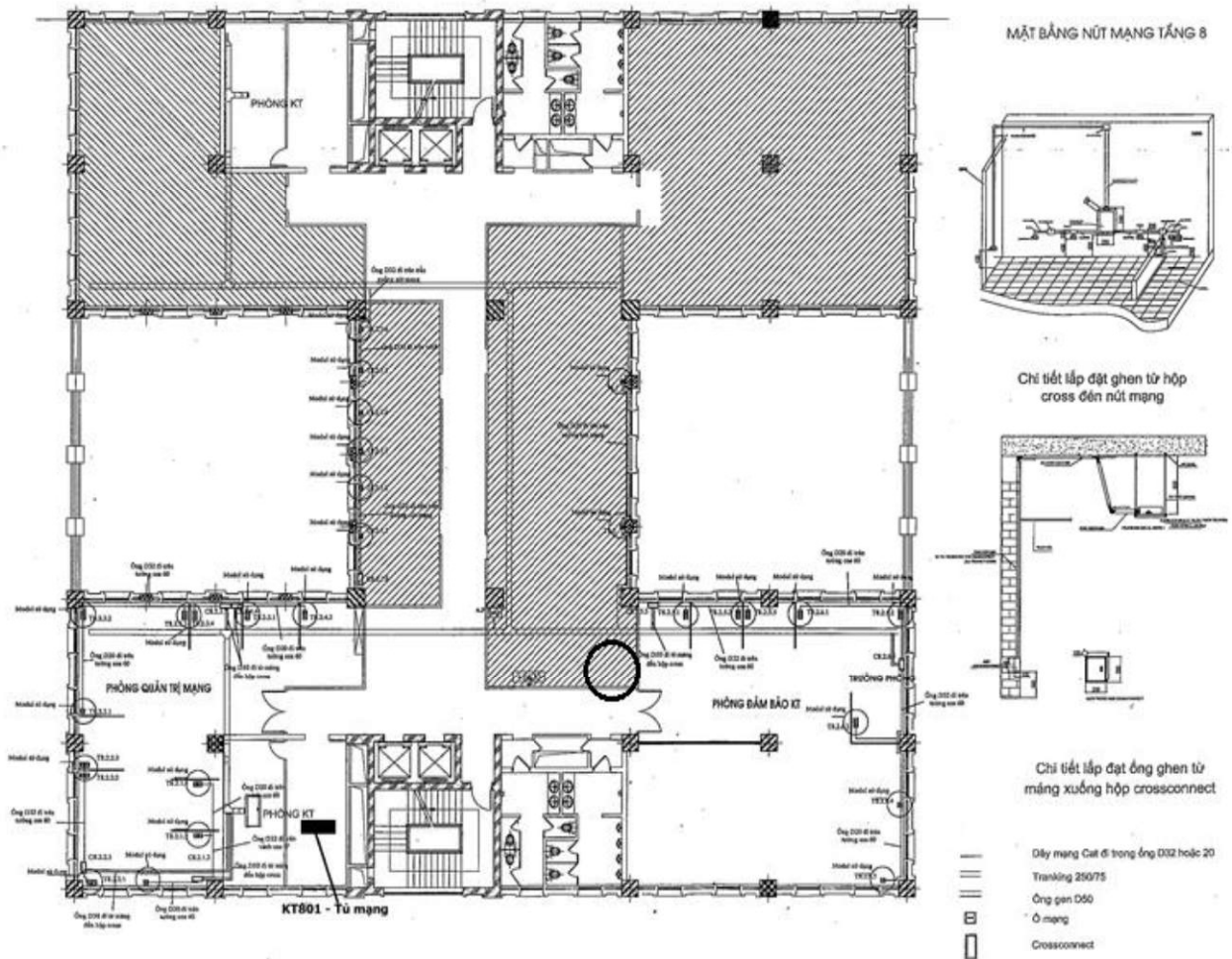


Sơ đồ tủ mạng tầng 7:



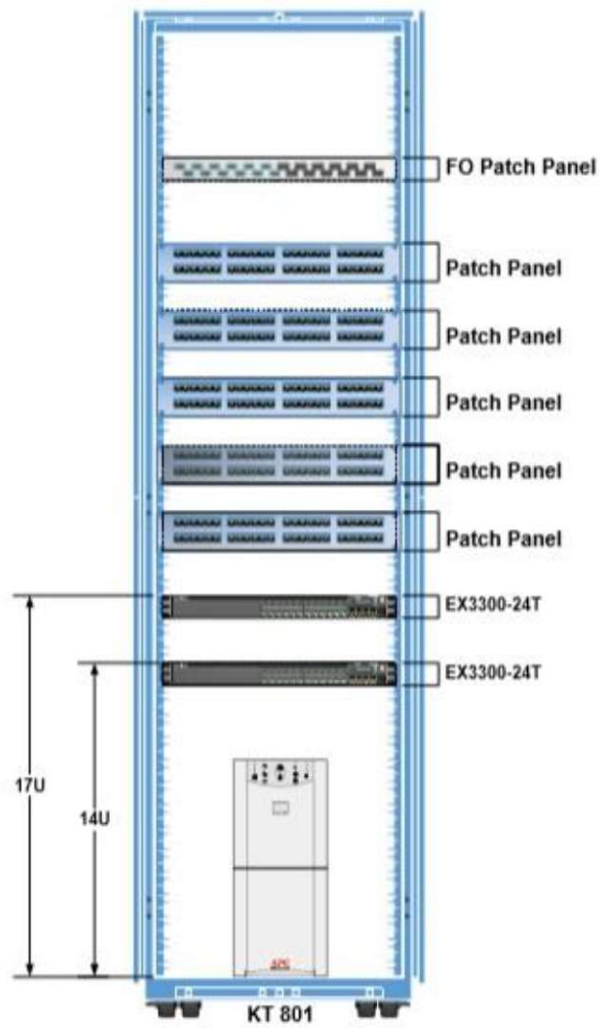
8.6.1.9. Sơ đồ mặt bằng và kết nối mạng tại tầng 8

Sơ đồ mặt bằng tầng 8:



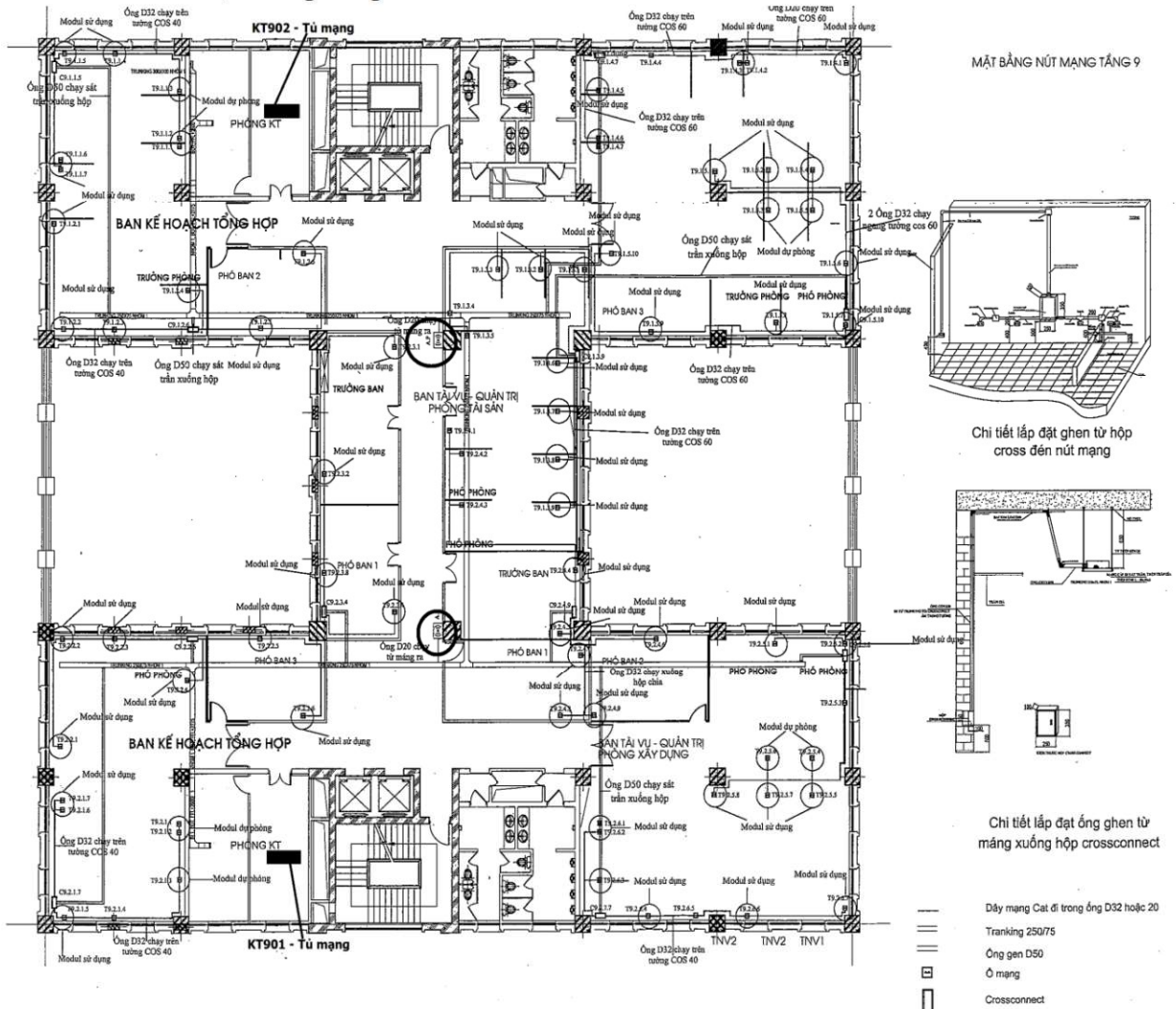
Trong đó: Phần khoanh tròn là vị trí đặt Access Point

Sơ đồ tủ mạng tầng 8:



8.6.1.10. Sơ đồ mặt bằng và kết nối mạng tại tầng 9

Sơ đồ mặt bằng tầng 9:

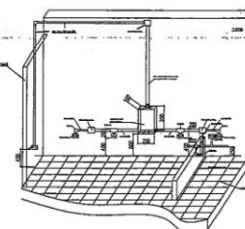


Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

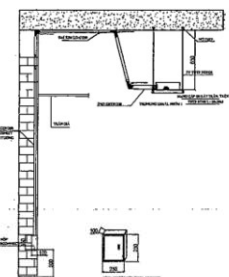
Sơ đồ tủ mạng tầng 9:








MẶT BẰNG NÚT MANG TẦNG 10



Chi tiết lắp đặt ghen từ hộp cross đến nút mạng

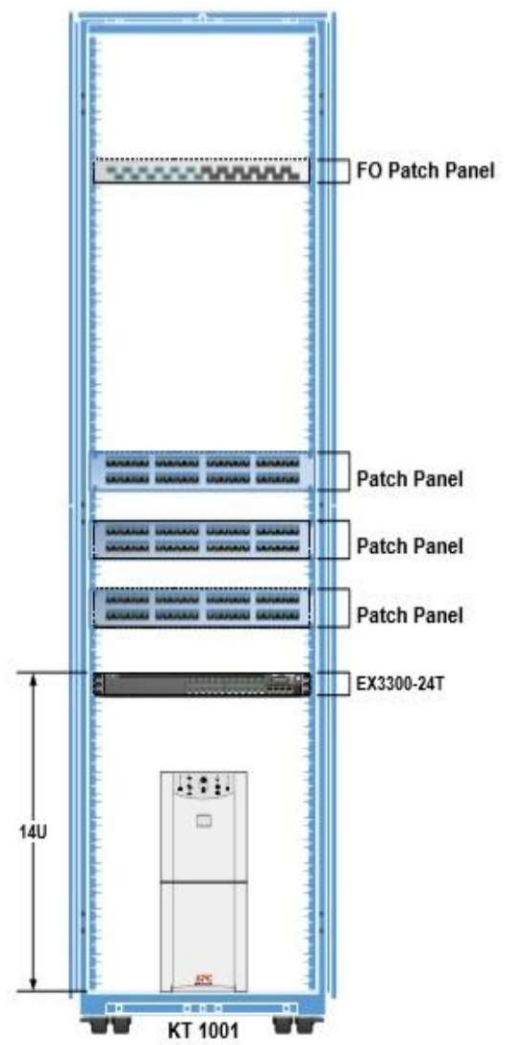
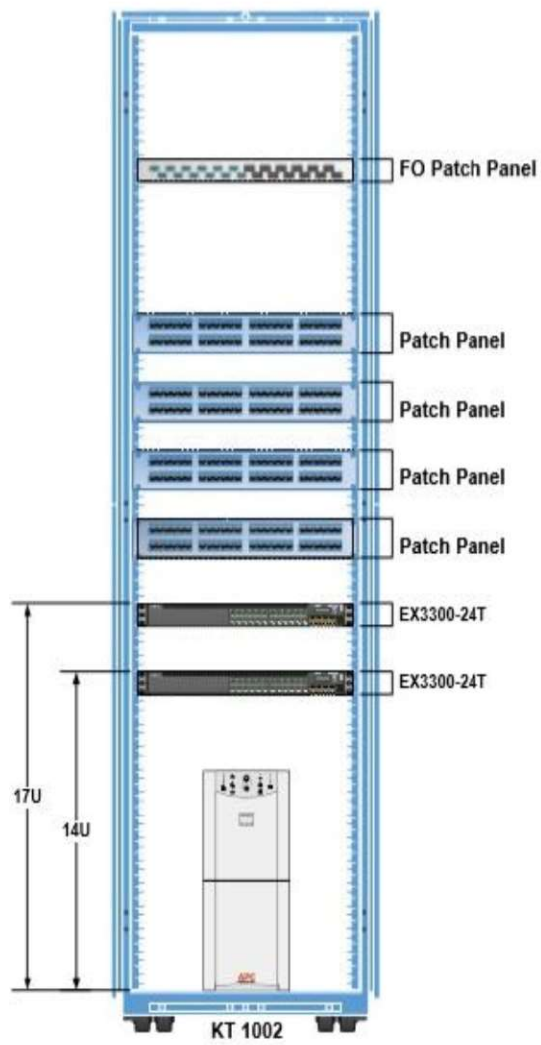


Chi tiết lắp đặt ống ghen từ
máng xuống hộp crossconnect

- | | |
|---|---------------------------------------|
|  | Dây mạng Cat đi trong ống D32 hoặc 20 |
|  | Trunking 250/75 |
|  | Ông gen D50 |
|  | Ổ mạng |
|  | Crossconnect |

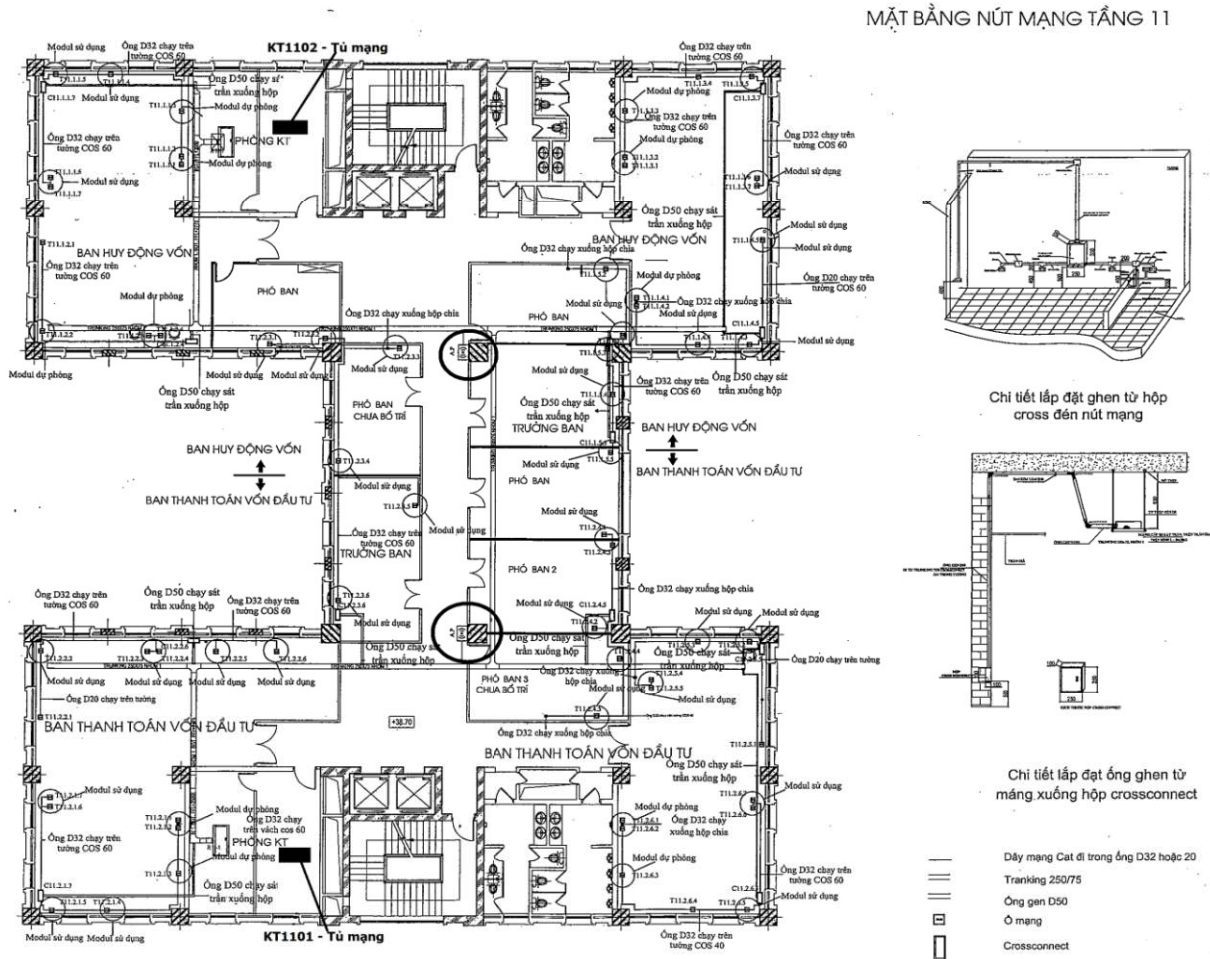
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 10:



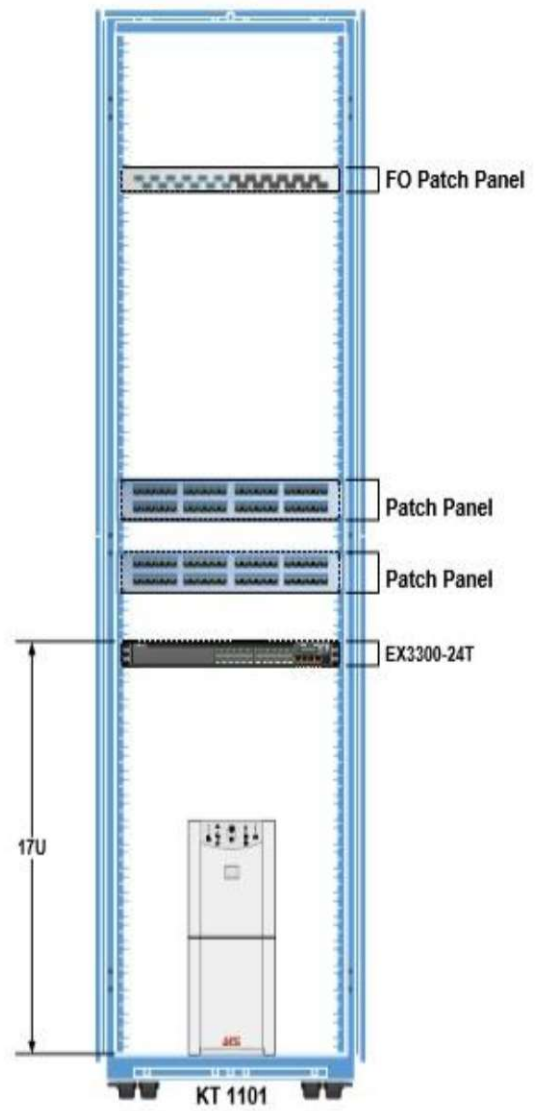
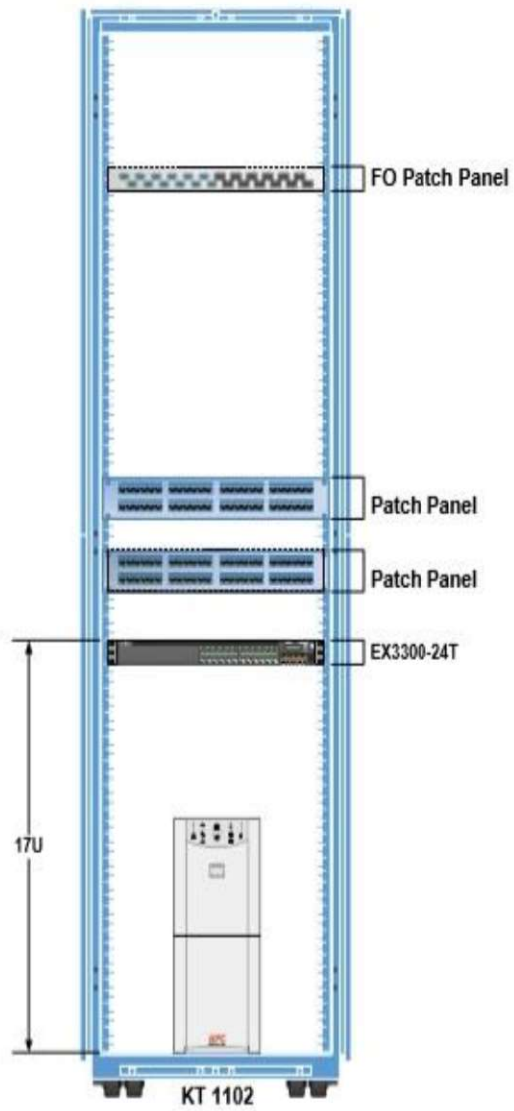
8.6.1.12. Sơ đồ mặt bằng và kết nối mạng tại tầng 11

Sơ đồ mặt bằng tầng 11:



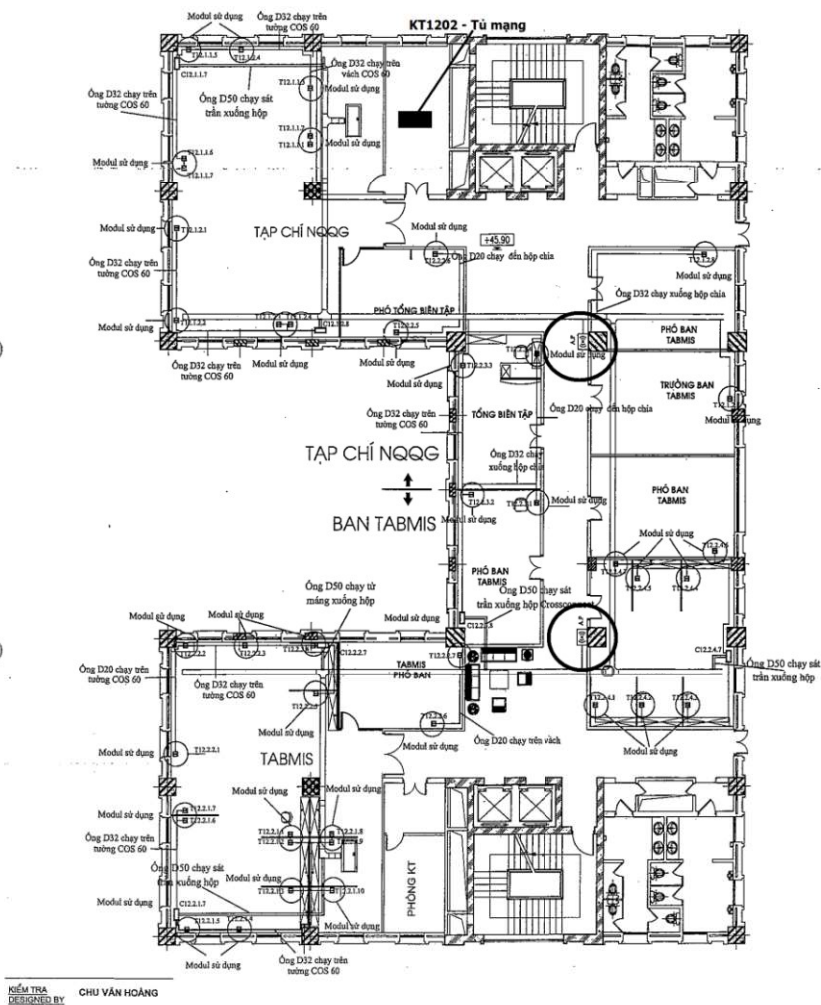
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 11:

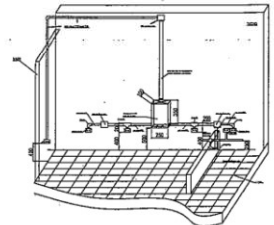


8.6.1.13. Sơ đồ mặt bằng và kết nối mạng tại tầng 12

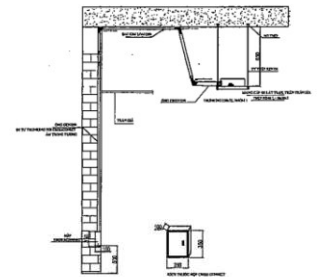
Sơ đồ mặt bằng tầng 12:



MẶT BẰNG NÚT MẠNG TẦNG 12



Chi tiết lắp đặt ghen từ hộp cross đến nút mạng

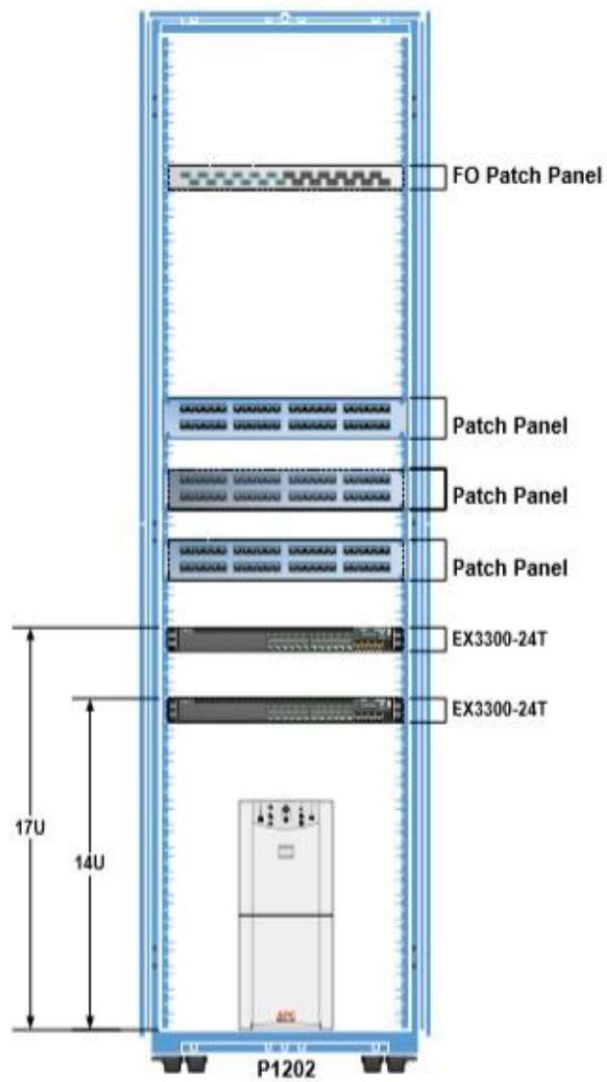


Chi tiết lắp đặt ống ghen từ máng xuống hộp crossconnect

- Dây mạng Cat 6 đi trong ống D32 hoặc 20
- Trunking 250/75
- Ống ghen D50
- Ô mạng
- Crossconnect

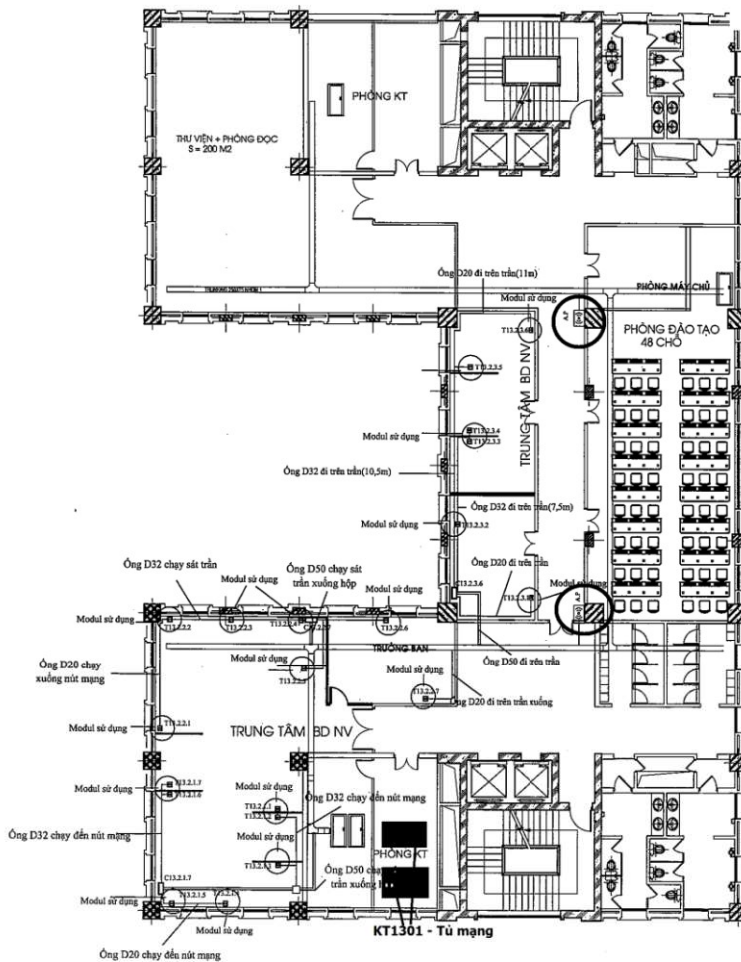
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 12:

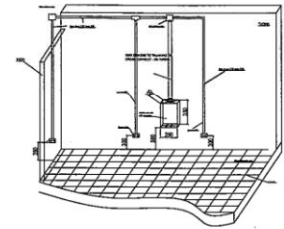


8.6.1.14. Sơ đồ mặt bằng và kết nối mạng tại tầng 13

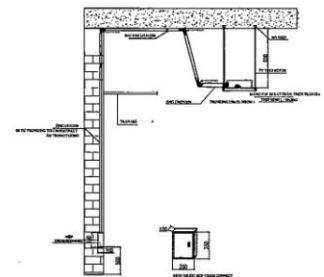
Sơ đồ mặt bằng tầng 13:



MẶT BẰNG NÚT MẠNG TẦNG 13



Chi tiết lắp đặt ghen từ hộp cross đến nút mạng

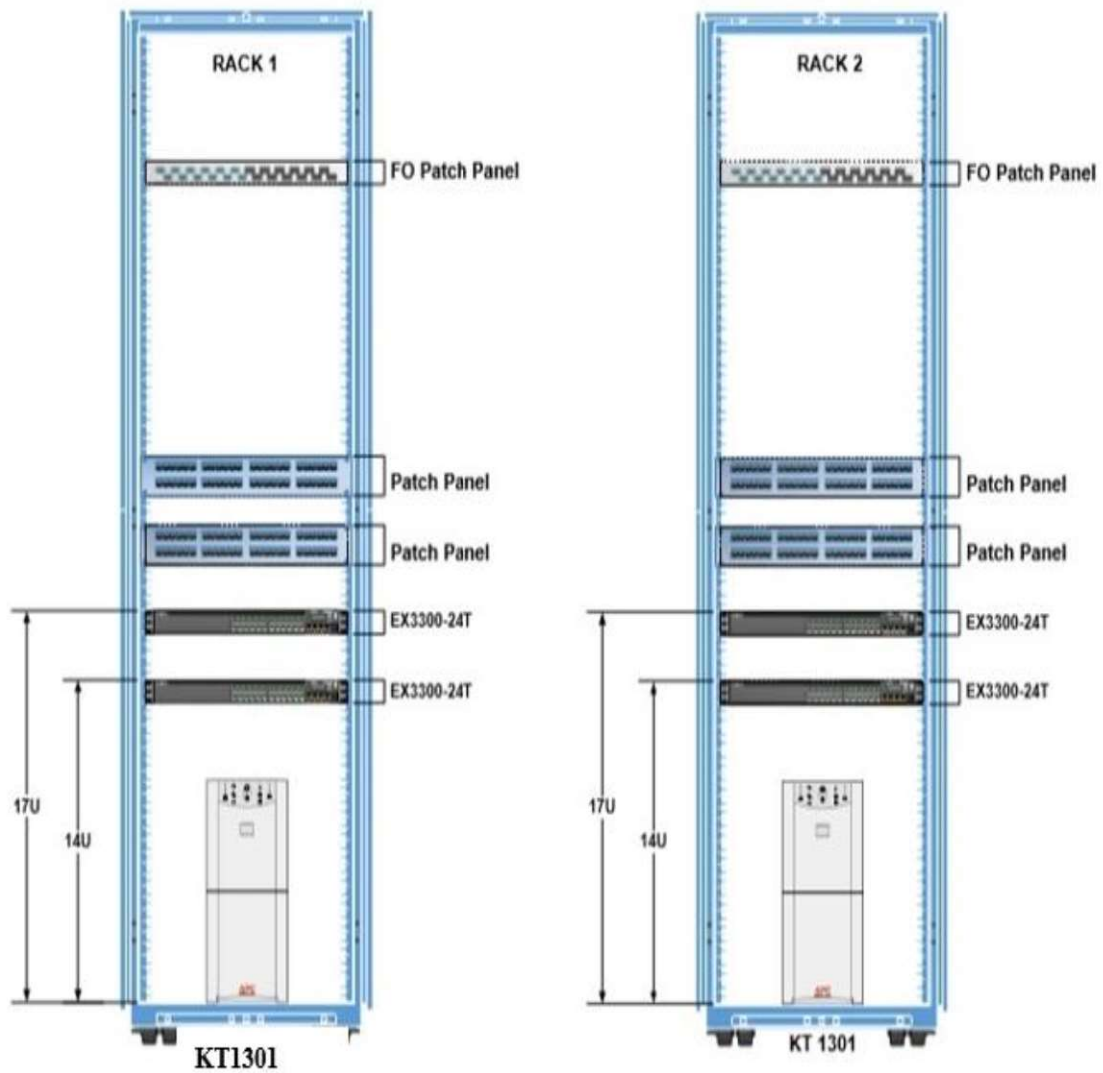


Chi tiết lắp đặt ống ghen từ máng xuống hộp crossconnect

- Dây mạng Cat đi trong ống D32 hoặc 20
- - - Trunking 250/75
- Ống gen D50
- ⊗ Ồ mạng
- ⊞ Crossconnect

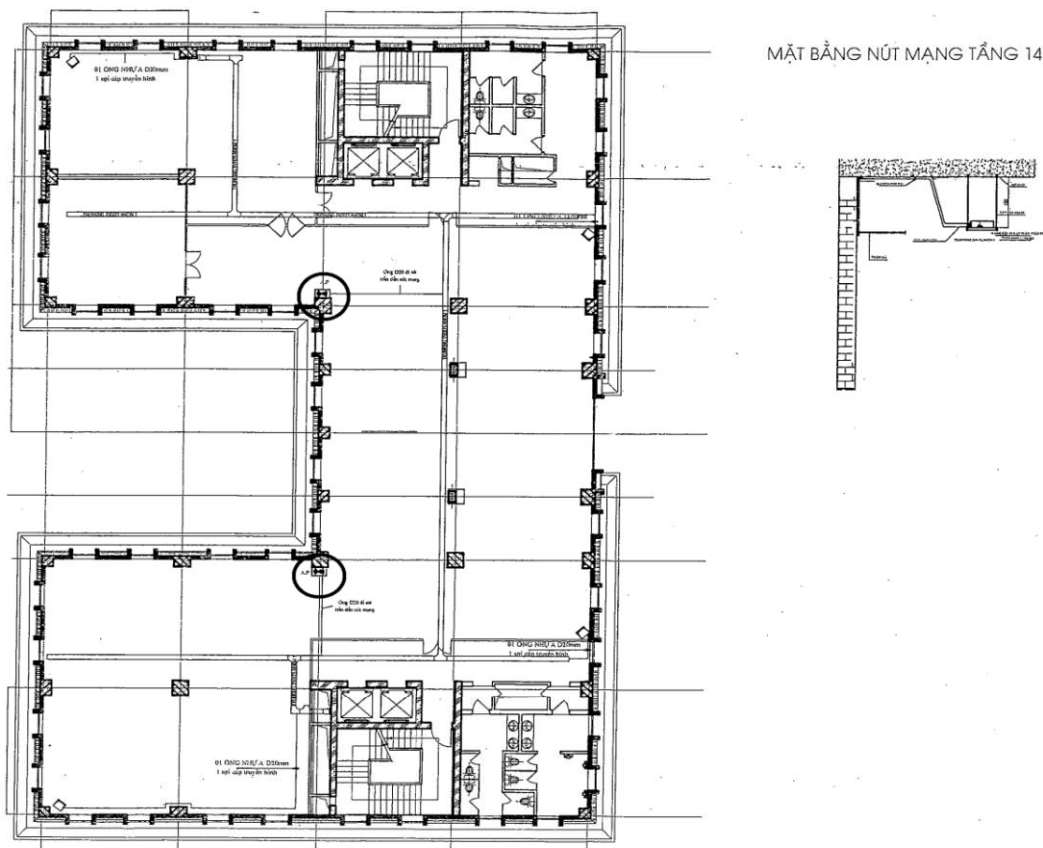
Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

Sơ đồ tủ mạng tầng 13:



8.6.1.15. Sơ đồ mặt bằng và kết nối mạng tại tầng 14

Sơ đồ mặt bằng tầng 14:



Trong đó: Phần khoanh tròn là vị trí đặt các Access Point

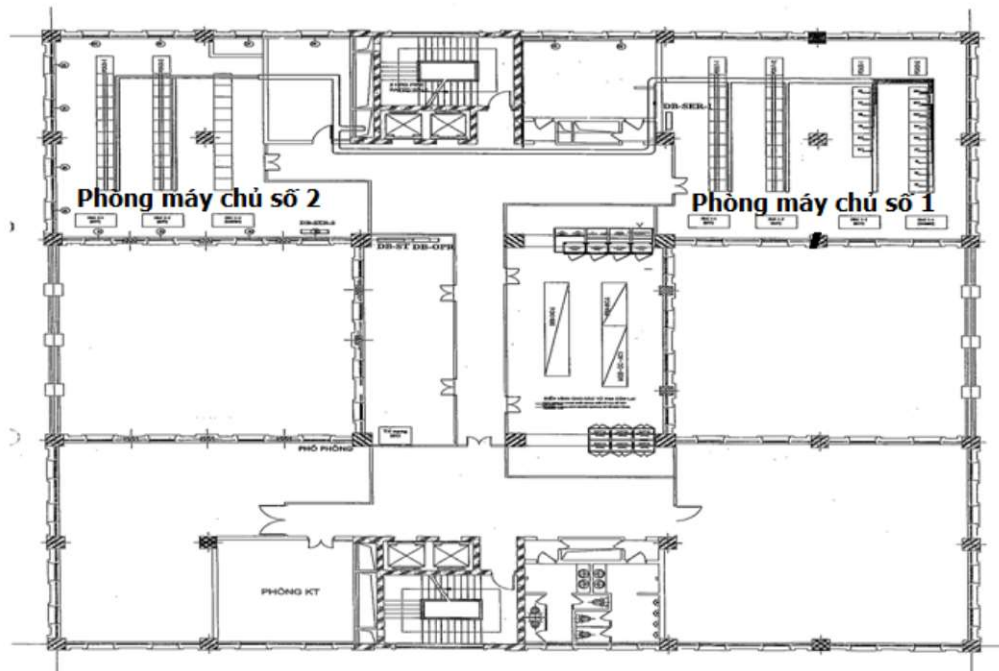
Sơ đồ tủ mạng tầng 14: Tại tầng 14 không đặt tủ mạng, các thiết bị Access point kết nối mạng với tủ mạng đặt tại tầng 13.

8.6.2. Hiện trạng hạ tầng Trung tâm dữ liệu

8.6.2.1. Hiện trạng mặt bằng TTDL

Trung tâm dữ liệu (TTDL) của KBNN đặt tại 32 Cát Linh, Hà Nội là nơi lắp đặt hệ thống các thiết bị CNTT, ứng dụng, dữ liệu chính của KBNN. TTDL của KBNN với diện tích gần 600m² và đưa vào sử dụng từ năm 2008. TTDL được bố trí hạ tầng đảm bảo cho hệ thống CNTT vận hành liên tục 24/24 phục vụ thường xuyên hoạt động nghiệp vụ của hệ thống KBNN.

TTDL của KBNN được bố trí tại tầng 8 của tòa nhà KBNN. Sơ đồ mặt bằng TTDL hiện tại như sau:



Sơ đồ mặt bằng khu TTDL

Hạ tầng TTDL bao gồm các hệ thống:

- Hệ thống Điện nguồn và UPS;
- Hệ thống Điều hòa không khí: gồm 02 hệ thống:
 - + Hệ thống điều hòa giải nhiệt nước (chiller) và máy lạnh chính xác;
 - + Hệ thống điều hòa cục bộ.
- Hệ thống an ninh (camera quan sát và kiểm soát ra vào);
- Hệ thống báo cháy sớm và chữa cháy khí Nitơ;
- Hệ thống kiến trúc và sàn nâng;
- Hệ thống giám sát môi trường và phát hiện chất lỏng.

TTDL có các khu vực chức năng chính như sau:

- Phòng giám sát (phòng Monitor) bố trí các màn hình giám sát để cán bộ quản trị TTDL có thể theo dõi việc đảm bảo an ninh trong TTDL (qua hệ thống camera), theo dõi tình trạng hoạt động của các hệ thống hạ tầng TTDL (điều hòa, điện nguồn và UPS, nhiệt độ và độ ẩm...), từ đó phát hiện được các sự cố kỹ thuật để kịp thời sửa chữa, khắc phục.

- Phòng Nguồn điện và UPS (phòng Power):

+ Hệ thống điện nguồn và UPS có dự phòng 2 hệ thống chạy song song với công suất mỗi hệ thống là 160KW. Hệ thống điện nguồn và UPS này đảm bảo cung cấp điện sạch phục vụ phòng máy chủ hoạt động liên tục 24/24.

+ Ngoài ra hệ thống điện nguồn Trung tâm dữ liệu được dự phòng cấp điện từ máy phát điện dự phòng (tự động bật lên khi mất điện lưới).

- **Phòng máy chủ số 1:** (diện tích 200m²), hiện đang đặt 36 tủ rack, cụ thể:

+ 16 tủ Rack thuộc hệ thống TABMIS: 13 tủ Rack được lắp đặt từ năm 2008, 03 tủ được lắp đặt từ năm 2018.

+ 20 tủ Rack được lắp đặt từ năm 2008, hiện đang chứa các thiết bị mạng, bảo mật, hạ tầng truyền thông, môi trường phát triển, hệ thống TCS.

+ Các tủ mạng bao gồm: Rack M01; M02; M03; M04; Rack 10, Rack 11



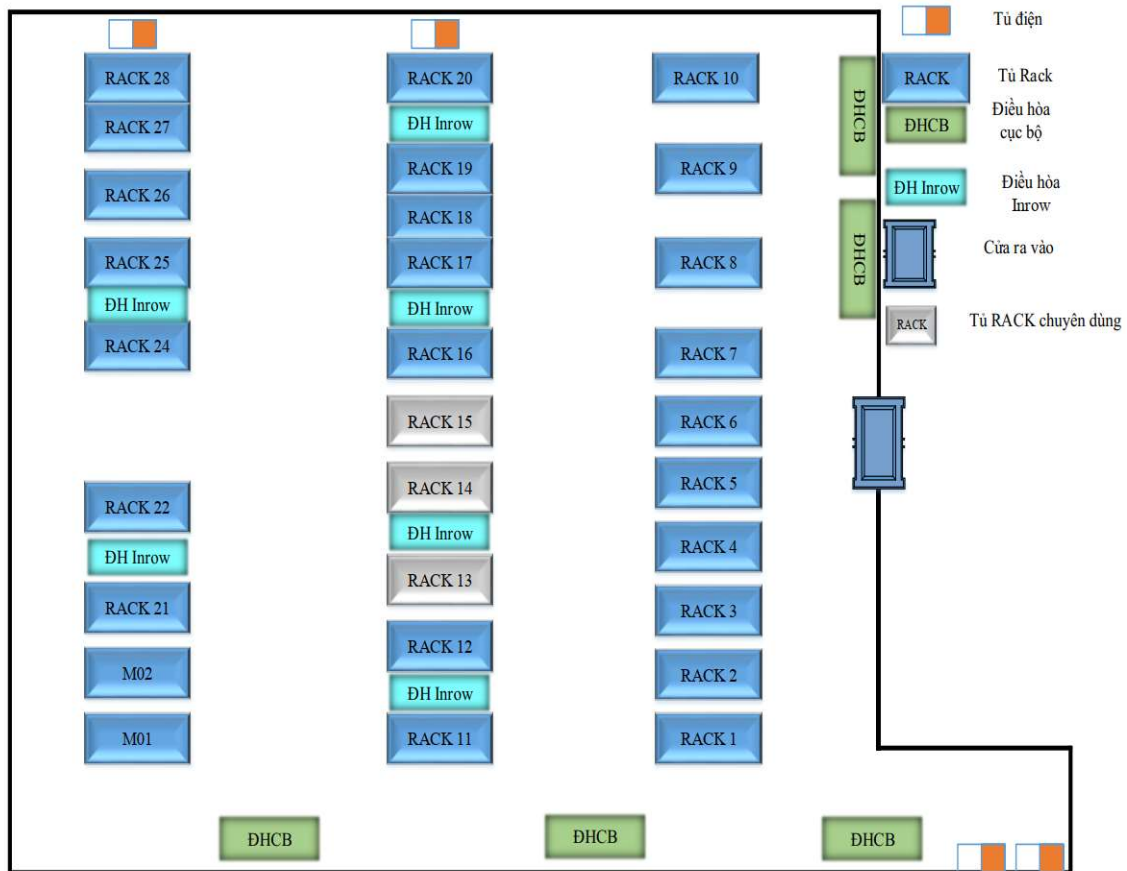
Sơ đồ mặt bằng bố trí thiết bị phòng máy chủ số 1

- **Phòng máy chủ số 2:** (diện tích 150m²): hiện đang đặt 29 Tủ Rack được lắp đặt từ năm 2013, trong đó:

+ 26 tủ Rack đang chứa các máy chủ, thiết bị mạng, bảo mật, thiết bị lưu trữ, thiết bị sao lưu tập trung.

+ 03 tủ Rack chuyên dụng lắp đặt thiết bị Lưu trữ, sao lưu tập trung cho các hệ thống: Thanh toán song phương, Thanh toán liên ngân hàng, Intranet, Dịch vụ công, Tổng kế toán, Kho dữ liệu; hệ thống máy chủ ảo hóa cài đặt các ứng dụng tại Trung ương...

+ Các tủ mạng bao gồm: M01, M02



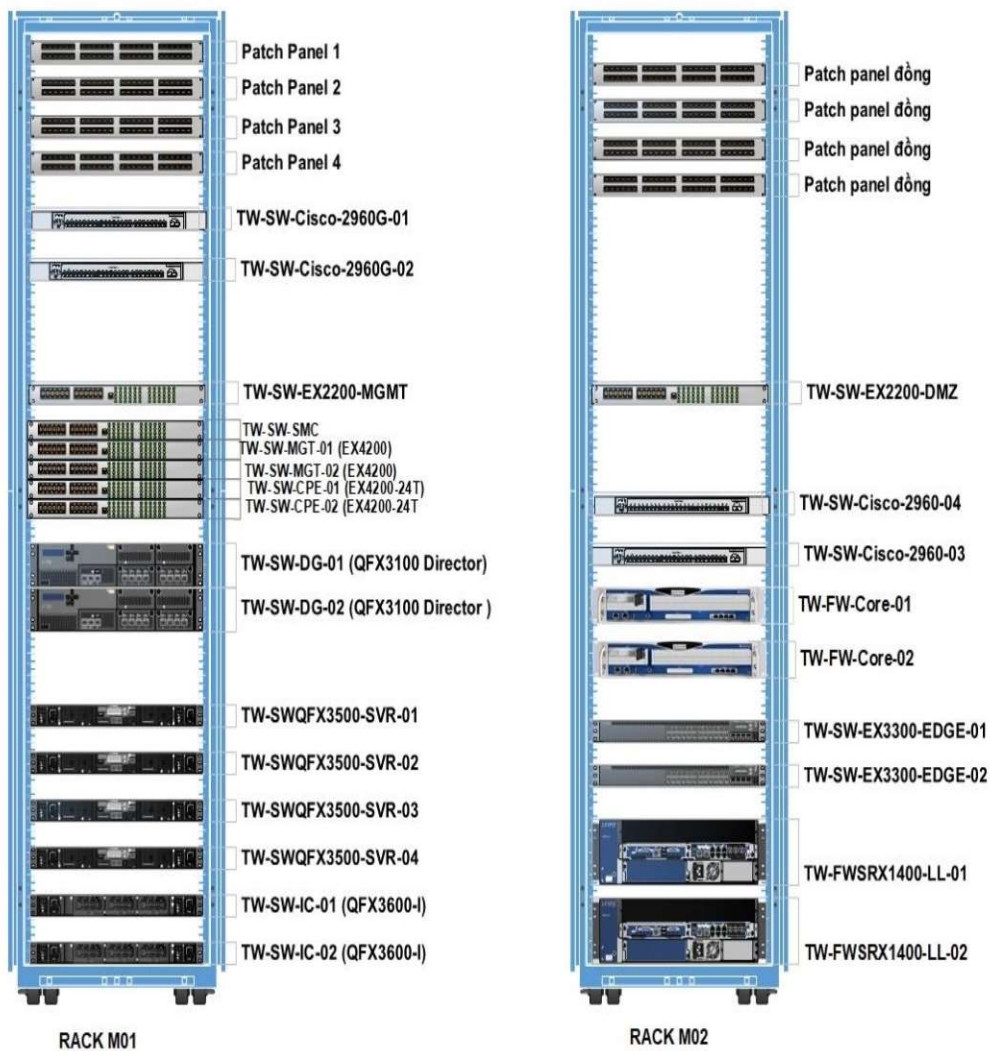
Sơ đồ mặt bằng bố trí thiết bị phòng máy chủ số 2

TTDL KBNN đang đặt các thiết bị thuộc môi trường sản xuất của các hệ thống quan trọng, hoạt động 24/7.

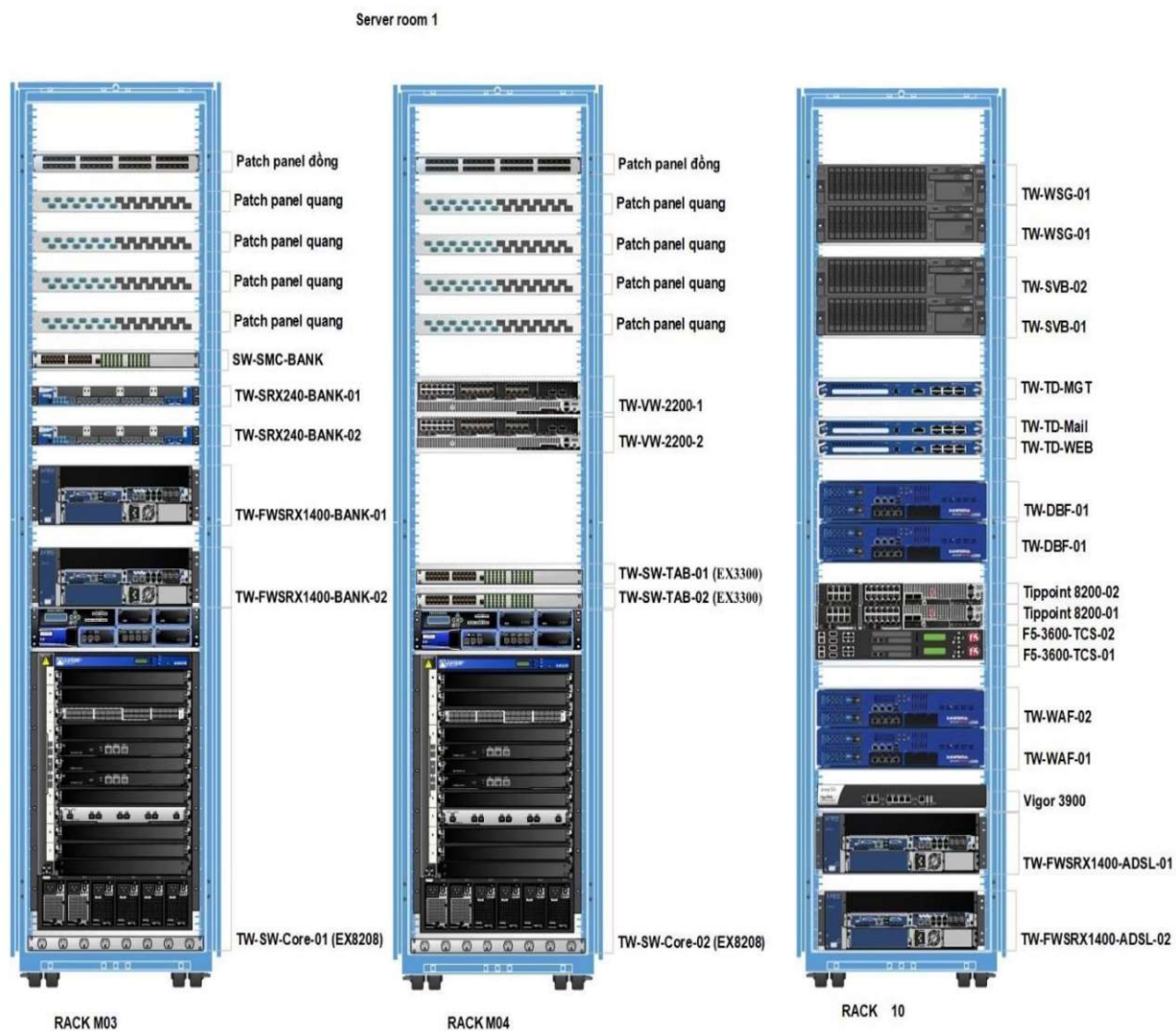
Các phòng giám sát, phòng nguồn và phòng máy chủ đều được lắp đặt điều hòa, các thiết bị phục vụ giám sát môi trường, các thiết bị báo cháy, chữa cháy tự động. Phòng máy chủ số 1 và 2 được lắp đặt hệ thống phát hiện chất lỏng.

8.6.2.2. Sơ đồ bố trí thiết bị mạng phòng máy chủ số 1

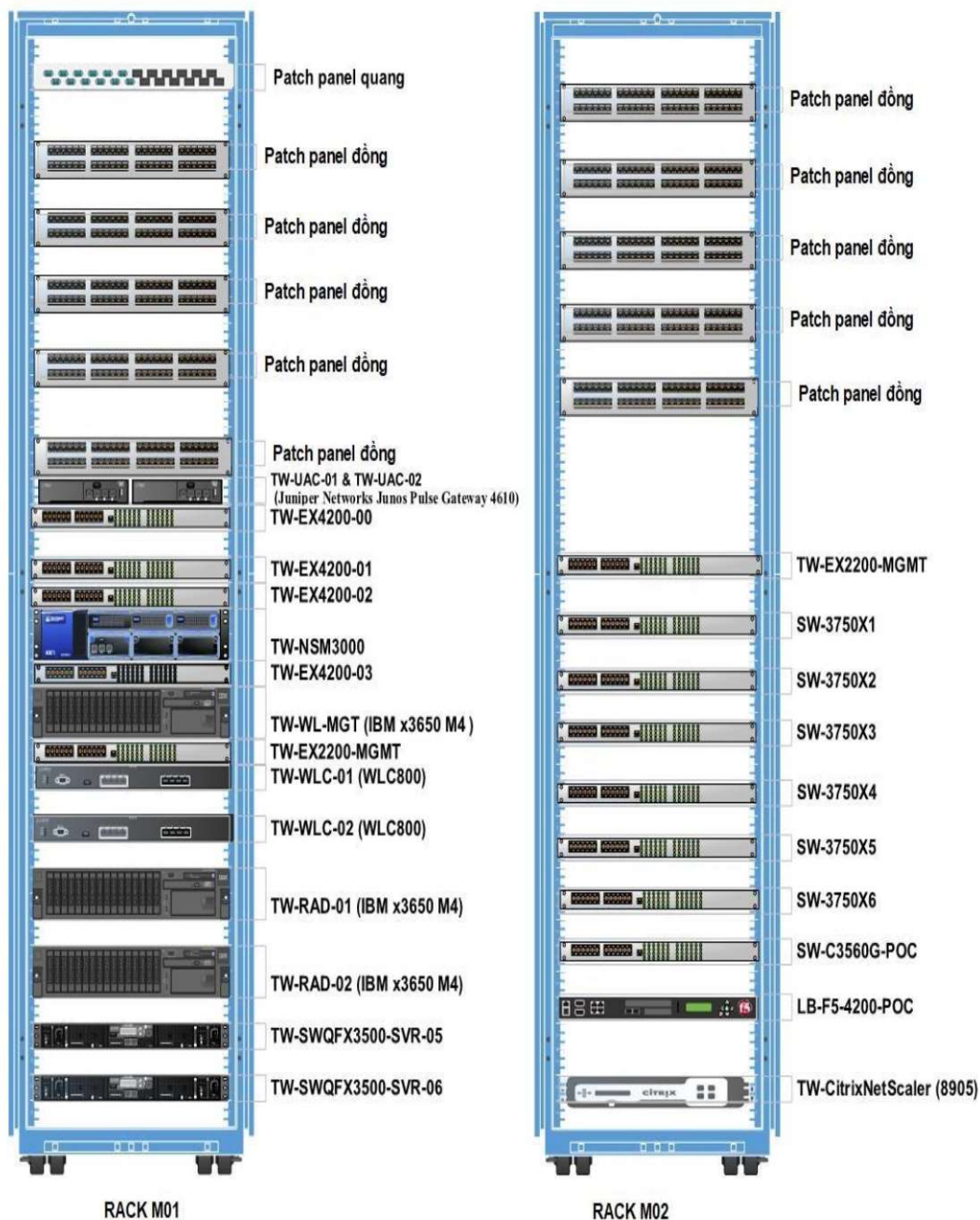
Sơ đồ bố trí thiết bị mạng phòng máy chủ số 1 trên các Rack: M01, M02:



Sơ đồ bố trí thiết bị mạng phòng máy chủ số 1 trên các Rack: M03, M04, Rack10:



Server room 2



8.7. Sơ đồ và thuyết minh chi tiết giải pháp thiết kế mạng, đường truyền, hạ tầng kỹ thuật, an toàn thông tin, cấp điện, chống sét, hệ thống làm mát, tính toán băng thông đường truyền

8.7.1. Sơ đồ thiết kế tổng thể

Hiện tại KBNN đang thực hiện các công việc để triển khai kế hoạch “Thuê trung tâm dữ liệu Kho bạc Nhà nước”. Do đó, dự án “Đầu tư hệ thống mạng LAN cơ quan Kho bạc Nhà nước” sẽ có 02 mô hình thiết kế tổng thể trong 02 trường hợp sau:

+ Trường hợp 1: TTDL chưa được di chuyển đến địa điểm thuê theo kế hoạch thuê TTDL KBNN

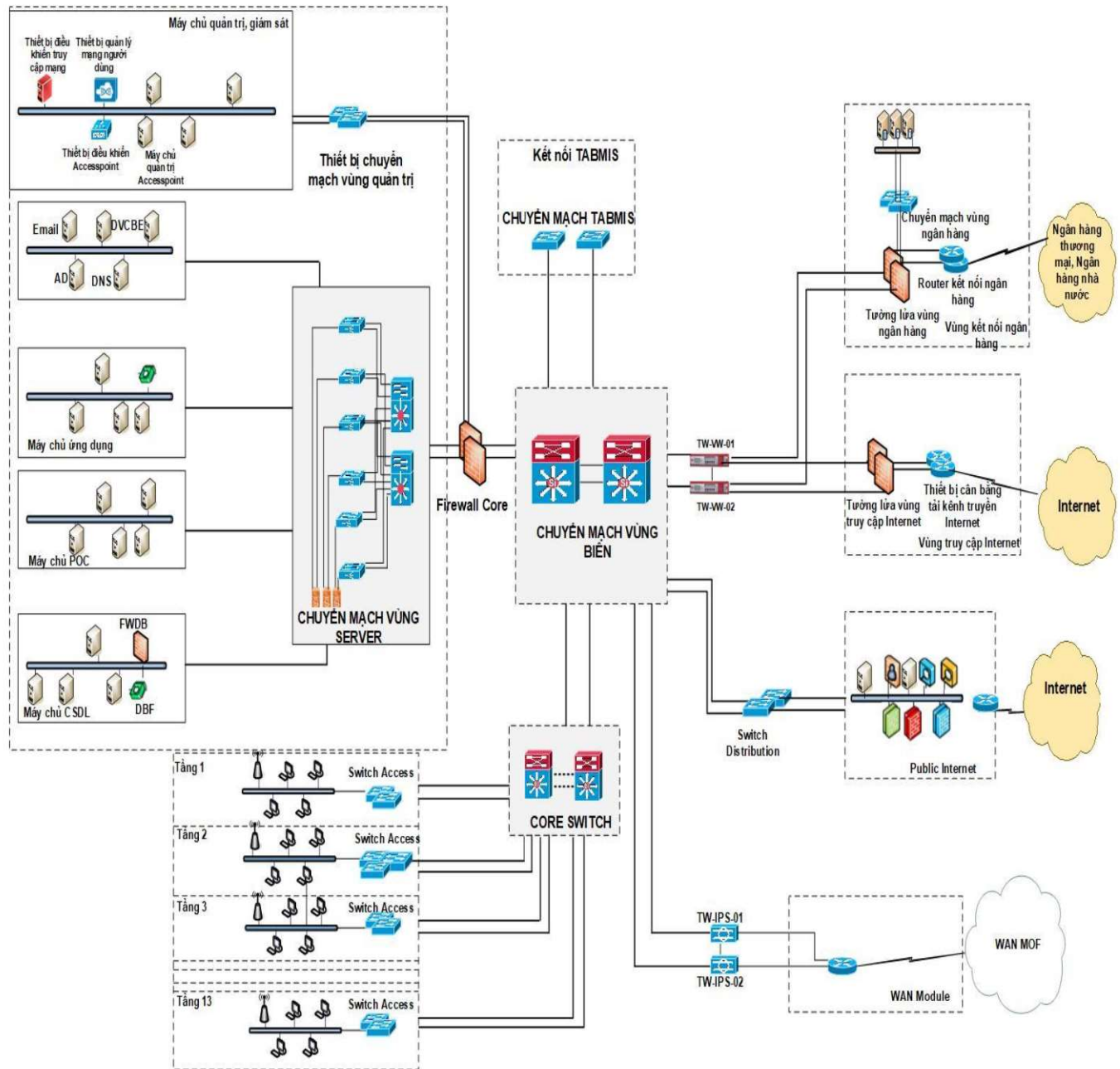
+ Trường hợp 2: TTDL đã được di chuyển đến địa điểm thuê theo kế hoạch thuê TTDL KBNN

Điểm khác nhau giữa 02 sơ đồ thiết kế tổng thể này là:

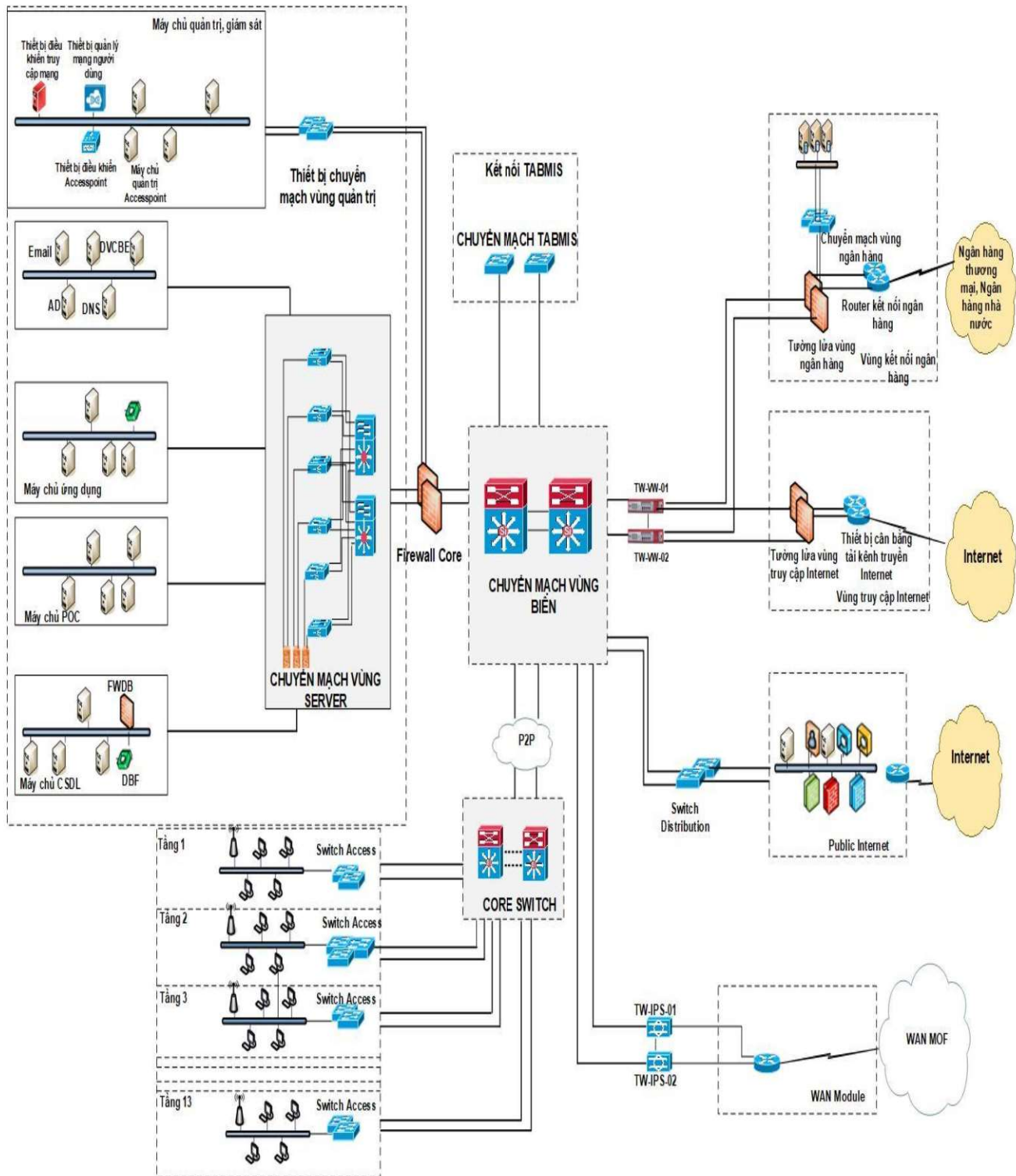
+ Sơ đồ thiết kế trường hợp TTDL chưa được di chuyển: Thiết bị chuyển mạch Core Switch sẽ kết nối trực tiếp qua cáp 10Gbps với thiết bị chuyển mạch vùng biên và cùng được lắp đặt trong TTDL đặt trụ sở cơ quan KBNN.

+ Sơ đồ thiết kế trường hợp TTDL đã được di chuyển đến địa điểm thuê: Thiết bị chuyển mạch Core Switch sẽ kết nối với thiết bị chuyển mạch vùng biên qua 02 kênh truyền của nhà cung cấp dịch vụ.

Sơ đồ tổng thể hệ thống sau khi nâng cấp trong trường hợp TTDL chưa được di chuyển đến địa điểm thuê theo kế hoạch thuê TTDL KBNN như sau:



Sơ đồ tổng thể hệ thống sau khi nâng cấp trong trường hợp TTDL đã được di chuyển đến địa điểm thuê theo kế hoạch thuê TTDL KBNN như sau:



Hệ thống mạng LAN KBNN sau khi nâng cấp bao gồm các hạng mục sau:

Hệ thống chuyển mạch vùng server: Được triển khai theo mô hình mạng được định nghĩa bằng phần mềm (Software-Defined Networking - SDN), cung cấp kết nối tốc độ cao cho hệ thống máy chủ KBNN.

Thiết bị chuyển mạch vùng biên: Cung cấp kết nối giữa các Ngân hàng thương mại, Ngân hàng nhà nước với hệ thống mạng TTDL; kết nối giữa vùng mạng NSD tại cơ quan KBNN với TTDL; kết nối giữa mạng LAN KBNN với Internet; kết nối giữa mạng LAN KBNN với hạ tầng truyền thông BTC; kết nối giữa LAN KBNN với hệ thống TABMIS; kết nối giữa TTDL môi trường sản xuất và TTDL môi trường dự phòng. Các thiết bị chuyển mạch vùng biên với khả năng ảo hóa sẽ có thể ghép lại với nhau để tạo thành 01 thiết bị logic duy nhất, giúp cho công tác quản trị vận hành của KBNN trở nên đơn giản hơn.

Thiết bị chuyển mạch vùng TABMIS: Cung cấp kết nối 1Gbps cho hệ thống TABMIS và đồng thời kết nối về hệ thống chuyển mạch biên với tốc độ 10Gbps.

Thiết bị chuyển mạch vùng quản trị: Cung cấp các kết nối 1Gbps phục vụ lưu thông quản trị cho các thiết bị mạng, bảo mật, lưu trữ, máy chủ.

Thiết bị chuyển mạch Core Switch: Đảm nhiệm vai trò chuyển mạch cho toàn bộ hệ thống mạng vùng người dùng tại cơ quan KBNN.

Thiết bị chuyển mạch lớp Access: Thiết bị cung cấp các kết nối GE cho các thiết bị đầu cuối như PC, Máy in, Photocopy, Access Points, Camera, ...

Thiết bị phát sóng Access point: là điểm kết nối không dây cho tất cả các thiết bị đầu cuối tương thích với chuẩn, 802.11n, 802.11ac, 802.11ax.

Thiết bị điều khiển Access point: Quản lý toàn bộ các Access point trong hạ tầng Wireless.

Hệ thống điều khiển truy cập mạng: giúp nhận diện các điểm cuối và thực thi chính sách cho dịch vụ. Hệ thống điều khiển truy cập mạng tích hợp thực thi chính sách với thiết bị quản lý mạng người dùng.

Thiết bị quản lý mạng người dùng: quản lý tập trung cấu hình và luồng dữ liệu, thực hiện cài đặt cấu hình toàn bộ thiết bị trong hệ thống SD-LAN, hồ sơ mạng cho các thiết bị vật lý, địa chỉ IP, quản lý, quyền truy cập của NSD.

Thiết bị tường lửa vùng ngân hàng: Kiểm soát thông tin trao đổi giữa các ngân hàng với dữ liệu của KBNN. Thiết bị bên cạnh tính năng tường lửa (Firewall) còn được trang bị khả năng phòng chống xâm nhập (IPS).

Thiết bị chuyển mạch vùng ngân hàng: Cung cấp các kết nối 1Gbps cho các thiết bị máy chủ, bảo mật vùng kết nối với ngân hàng.

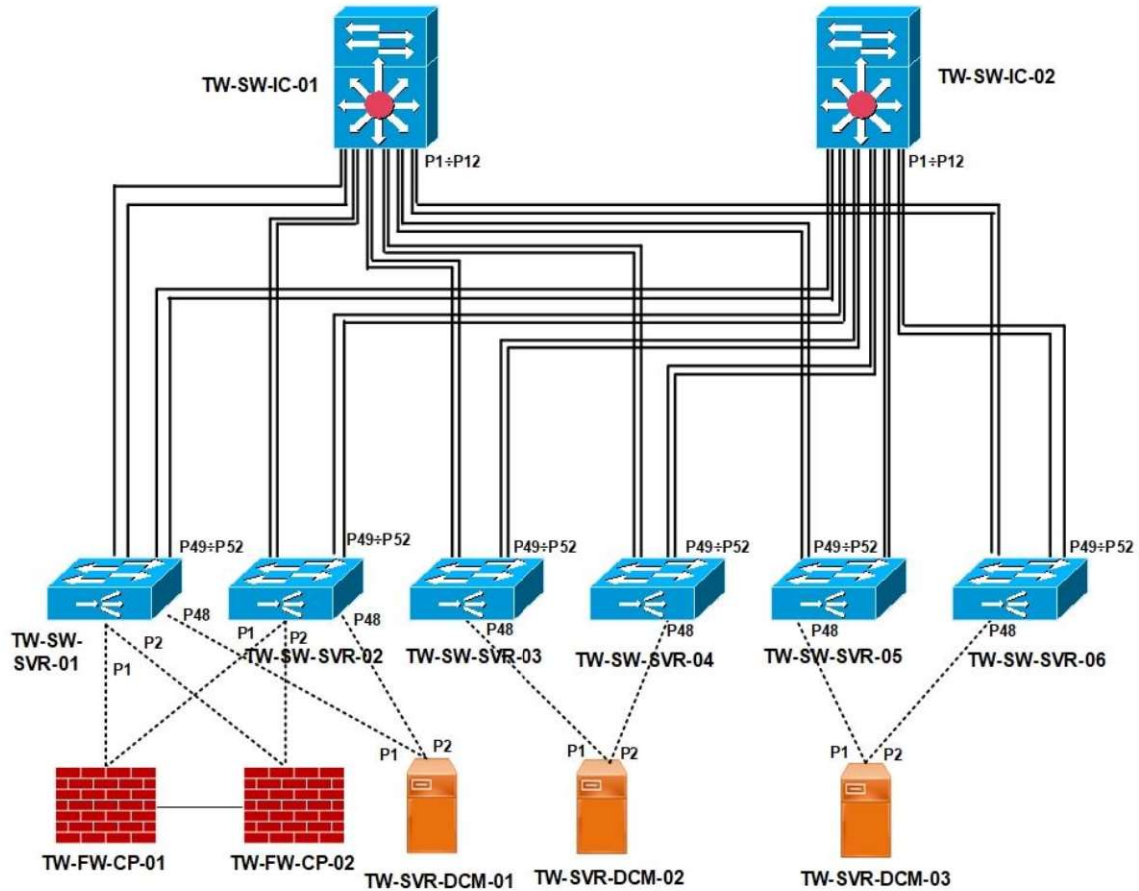
Thiết bị Router kết nối ngân hàng: Cung cấp kết nối từ KBNN sang Ngân hàng Nhà nước và các Ngân hàng Thương mại.

Thiết bị tường lửa vùng truy cập Internet: kiểm soát truy cập của người sử dụng trong mạng LAN KBNN kết nối Internet. Thiết bị bên cạnh tính năng tường lửa (Firewall) còn được trang bị khả năng phòng chống xâm nhập (IPS).

Thiết bị cân bằng tải kênh truyền Internet: có chức năng cân bằng tải các kết nối Internet.

8.7.2. Hệ thống chuyển mạch vùng server

8.7.2.1. Sơ đồ thiết kế



Chú thích:

TW-FW-CP-0x: Thiết bị Firewall hiện có
 TW-SW-IC-0x: Thiết bị Liên kết chuyển mạch vùng Server
 TW-SW-SVR-0x: Thiết bị Chuyển mạch vùng Server
 TW-SVR-DCM-0x: Thiết bị điều khiển chuyển mạch vùng Server

Px: Port

Cáp quang, tốc độ 10Gbps

—————

Cáp quang, tốc độ 100Gbps

8.7.2.2. Thuyết minh giải pháp

Hệ thống chuyển mạch vùng server của KBNN hoàn toàn dựa trên nền tảng là công nghệ SDN. Thiết kế hệ thống chuyển mạch vùng server bao gồm 03 thành phần chính:

- Thiết bị chuyển mạch vùng Server

Đây là các thiết bị chuyển mạch truy cập (Leaf switch) trong kiến trúc SDN.

Thiết bị chuyển mạch vùng Server là thiết bị chuyển mạch có mật độ cổng cao, độ trễ cực thấp, có nhiệm vụ cung cấp kết nối tới hệ thống server, hệ thống mạng vào ra cho hệ thống. Thành phần có khả năng thực hiện chuyển tiếp gói tin ở cả lớp 2 và lớp 3, thực hiện các chính sách QoS, quản trị ACL (Access Control List) và các tác vụ quản trị khác. Hệ thống chuyển mạch vùng Server bao gồm 06 thiết bị chuyển mạch vùng Server thay thế cho 06 thiết bị chuyển mạch vùng Server Juniper Networks QFX3500 hiện nay.

Thiết bị chuyển mạch vùng Server sẽ cung cấp giao tiếp 1 Gbps, 10 Gbps, 25 Gbps cho các thiết bị máy chủ và lưu trữ trong mạng, thiết bị mạng, bảo mật. Thiết bị chuyển mạch vùng Server kết nối với hệ thống Core Firewall hiện tại của KBNN thông qua giao tiếp 10GE, kết nối với hệ thống Firewall Cơ sở dữ liệu hiện tại thông qua giao tiếp 1GE. Bên cạnh đó, mỗi thành phần sẽ sử dụng các kết nối uplink tốc độ 100Gbps hoạt động trên cáp quang, mỗi thành phần sẽ có 04 đường uplink kết nối với thành phần liên kết chuyển mạch vùng Server.

- Hệ thống liên kết chuyển mạch vùng Server

Đây là các thiết bị chuyển mạch xương sống (Spine) chịu trách nhiệm liên kết tất cả các thiết bị chuyển mạch truy cập trong kiến trúc SDN.

Các thiết bị chuyển mạch vùng Server trao đổi dữ liệu với nhau thông qua thành phần liên kết chuyển mạch vùng Server bằng cách xây dựng lên một hình mạng ở dạng Mesh, sử dụng các liên kết quang tốc độ 100Gbps.

Thiết kế đề xuất sử dụng 02 hệ thống liên kết chuyển mạch trong mô hình hệ thống chuyển mạch vùng Server nhằm cung cấp khả năng dự phòng cả về mặt thiết bị lẫn liên kết. 04 liên kết uplink tốc độ 100Gbps từ mỗi thiết bị chuyển mạch vùng server sẽ được phân bố trên cả 02 thành phần Liên kết chuyển mạch vùng Server.

- Hệ thống thiết bị điều khiển chuyển mạch vùng Server (bộ điều khiển SDN)

Là thiết bị quản lý và điều khiển các thiết bị chuyển mạch, thực thi chính sách tập trung cho toàn bộ hệ thống mạng chuyển mạch vùng Server.

Mỗi thiết bị điều khiển chuyển mạch vùng Server sẽ kết nối với 02 thiết bị chuyển mạch vùng Server thông qua giao tiếp quang tốc độ 10GE để đảm bảo tính dự phòng.

Thiết kế đề xuất sử dụng 03 thiết bị điều khiển chuyển mạch vùng Server trong mô hình hệ thống chuyển mạch vùng Server nhằm cung cấp khả năng dự phòng cả về mặt thiết bị lẫn liên kết.

- Thiết bị liên kết chuyển mạch vùng Server TW-SW-IC-01: Cần 12 giao tiếp quang tốc độ 100Gbps kết nối với 06 thiết bị chuyển mạch vùng Server.

- Thiết bị liên kết chuyển mạch vùng Server TW-SW-IC-02: Cần 12 giao tiếp quang tốc độ 100Gbps kết nối với 06 thiết bị chuyển mạch vùng Server.

- Thiết bị chuyển mạch vùng Server TW-SW-SVR-0x:

- + 04 giao tiếp quang tốc độ 100Gbps kết nối với 02 thiết bị liên kết chuyển mạch vùng Server;

- + 01 giao tiếp quang tốc độ 10Gbps kết nối với 01 thiết bị điều khiển chuyển mạch vùng Server;

- + 24 giao tiếp quang 25GE, 19 giao tiếp 10GE, 2 giao tiếp 1GE đồng, 2 giao tiếp quang 1GE phục vụ cho các kết nối đến máy chủ, lưu trữ, thiết bị mạng, bảo mật khác.

Thiết bị điều khiển chuyển mạch vùng Server TW-SVR-DCM-0x: cần 02 giao tiếp quang 10GE kết nối với 02 thiết bị chuyển mạch vùng Server.

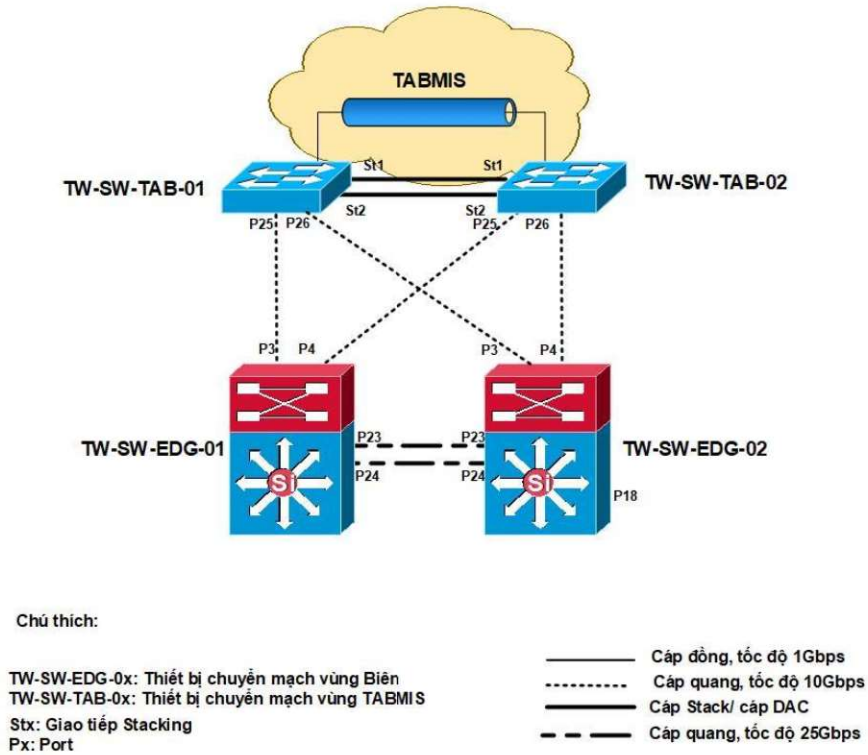
Phương án triển khai: 06 Thiết bị chuyển mạch vùng Server, 02 thiết bị liên kết chuyển mạch vùng Server, 03 thiết bị điều khiển chuyển mạch vùng Server sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

- + 02 port 10GE kết nối với 02 thiết bị Firewall Core
- + 04 port 1GE quang kết nối với 01 thiết bị Antivirus Gateway (VirusWall TippingPoint 2200)
- + 01 port 1Gbps đồng kết nối với 01 thiết bị IPS vùng hạ tầng truyền thông
- Thiết bị chuyển mạch vùng biên TW-SW-EDG-02:
- + 02 port 25GE kết nối với 02 thiết bị chuyển mạch vùng biên 01
- + 01 port 10GE kết nối với 01 thiết bị chuyển mạch vùng Core Switch
- + 02 port 10GE kết nối với 02 thiết bị chuyển mạch vùng TABMIS
- + 02 port 10GE kết nối với 02 thiết bị chuyển mạch Distribution
- + 02 port 10GE kết nối với 02 thiết bị Firewall Core
- + 04 port 1GE quang kết nối với 02 thiết bị Antivirus Gateway (VirusWall TippingPoint 2200)
- + 01 port 1GE đồng kết nối với 01 thiết bị IPS vùng hạ tầng truyền thông

Phương án triển khai: 02 thiết bị chuyển mạch vùng biên sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.4. Thiết bị chuyển mạch vùng TABMIS

8.7.4.1. Sơ đồ thiết kế



8.7.4.2. Thuyết minh giải pháp

- Theo thiết kế, cặp thiết bị chuyển mạch vùng TABMIS được cấu hình ảo hóa 02 thiết bị vật lý thành 01 switch logic (theo công nghệ xếp chồng). Cặp thiết bị sẽ thay thế 02 thiết bị Juniper EX3300-24T hiện có.

- Thiết bị sẽ kết nối với thiết bị chuyển mạch vùng biên thông qua các giao tiếp 10GE và kết nối vào hệ thống TABMIS thông qua giao tiếp 1GE. Mỗi thiết bị chuyển mạch vùng TABMIS sẽ cần có các kết nối sau:

+02 kết nối uplink 10Gbps quang phục vụ kết nối tới 02 thiết bị chuyển mạch vùng biên

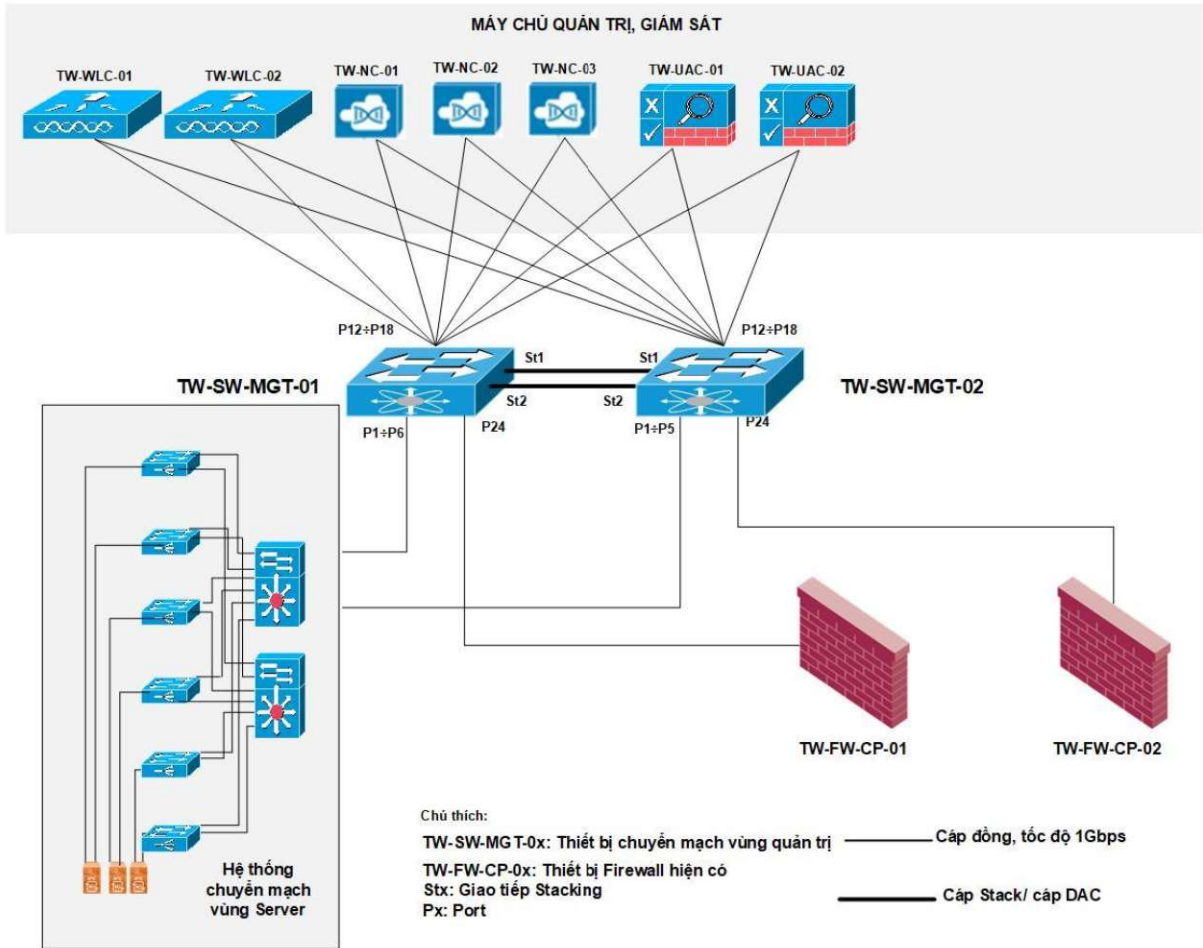
+02 giao tiếp phục vụ kết nối xếp chồng

+24 giao tiếp đồng 1GE phục vụ kết nối vào TABMIS

Phương án triển khai: 02 thiết bị chuyển mạch vùng TABMIS sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.5. Thiết bị chuyển mạch vùng quản trị

8.7.5.1. Sơ đồ thiết kế



8.7.5.2. Thuyết minh giải pháp

- Theo thiết kế, cặp thiết bị chuyển mạch vùng quản trị được cấu hình ảo hóa 02 thiết bị vật lý thành 01 switch logic (theo công nghệ xếp chồng).

- Cặp thiết bị chuyển mạch vùng quản trị cung cấp kết nối 1GE sử dụng cáp đồng tới toàn bộ các thành phần thuộc phân vùng máy chủ quản trị, giám sát, thành phần quản trị của các thiết bị mạng, bảo mật, máy chủ trong TTDL. Bên cạnh đó, 02 thiết bị kết nối tới Firewall nhằm bảo vệ cho mọi dữ liệu quản trị trước các cuộc tấn công. Lưu thông quản trị được giám sát thông qua thiết bị Firewall hiện có. Cặp thiết bị này sẽ thay thế cặp thiết bị Juniper EX4200-24T hiện có.

- Mỗi thiết bị chuyển mạch vùng quản trị cần 48 cổng 1GE, trong đó số kết nối cần thiết cho cặp thiết bị chuyển mạch vùng quản trị cần là:

+ 79 kết nối 1Gbps đồng theo hiện trạng (bao gồm 02 kết nối 1GE đến thiết bị Firewall Core)

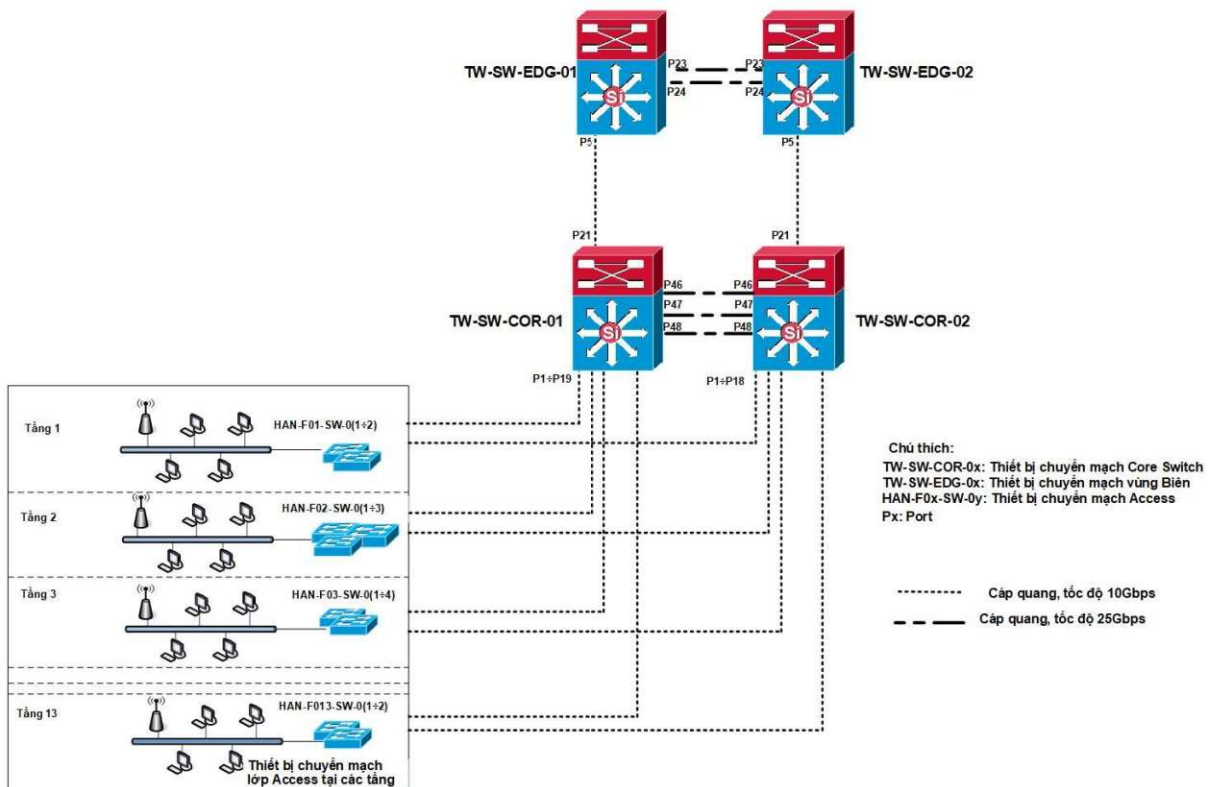
+ 14 kết nối 1Gbps đồng kết nối đến các thiết bị: 02 thiết bị điều khiển Access point, 03 thiết bị quản lý mạng người dùng, 02 thiết bị điều khiển truy cập mạng (mỗi thiết bị này sẽ có 02 kết nối đến 02 thiết bị chuyển mạch vùng quản trị sử dụng port group để tăng tốc độ và dự phòng kết nối)

+ 02 giao tiếp phục vụ kết nối xếp chồng

Phương án triển khai: 02 thiết bị chuyển mạch vùng quản trị sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.6. Thiết bị chuyển mạch Core Switch

8.7.6.1. Sơ đồ thiết kế



8.7.6.2. Thuyết minh giải pháp

- Thiết kế bao gồm 02 thiết bị chuyển mạch Core Switch để đảm bảo tính dự phòng. Cặp thiết bị này kết hợp với các thiết bị chuyển mạch Access tạo thành một mạng SD-LAN cho người sử dụng tại cơ quan KBNN, đồng thời là thiết bị định tuyến vùng mạng NSD với TTDL của KBNN.

- Mỗi thiết bị chuyển mạch Core Switch trong cặp thiết bị được cấu hình dự phòng đầy đủ:

- + Dự phòng điều khiển
- + Dự phòng module chuyển mạch
- + Dự phòng nguồn

Việc dự phòng này giúp cho hệ thống hoạt động liên tục 24/7, một cách suôn sẻ, ngay cả trong trường hợp bất kỳ thành phần nào của thiết bị gặp sự cố thì thành phần dự phòng đều được kích hoạt để đảm nhiệm vai trò.

Với thiết kế đề xuất ở trên, thiết bị chuyển mạch Core Switch cần có số lượng giao tiếp như sau:

Thiết bị chuyển mạch Core Switch TW-SW-COR-01:

- + 19 port 10GE kết nối với 19 thiết bị chuyển mạch lớp Access tầng
- + 01 port 10GE kết nối với 01 thiết bị chuyển mạch vùng biên
- + 03 port 25GE kết nối với thiết bị Core Switch 02

Thiết bị chuyển mạch Core Switch TW-SW-COR-02:

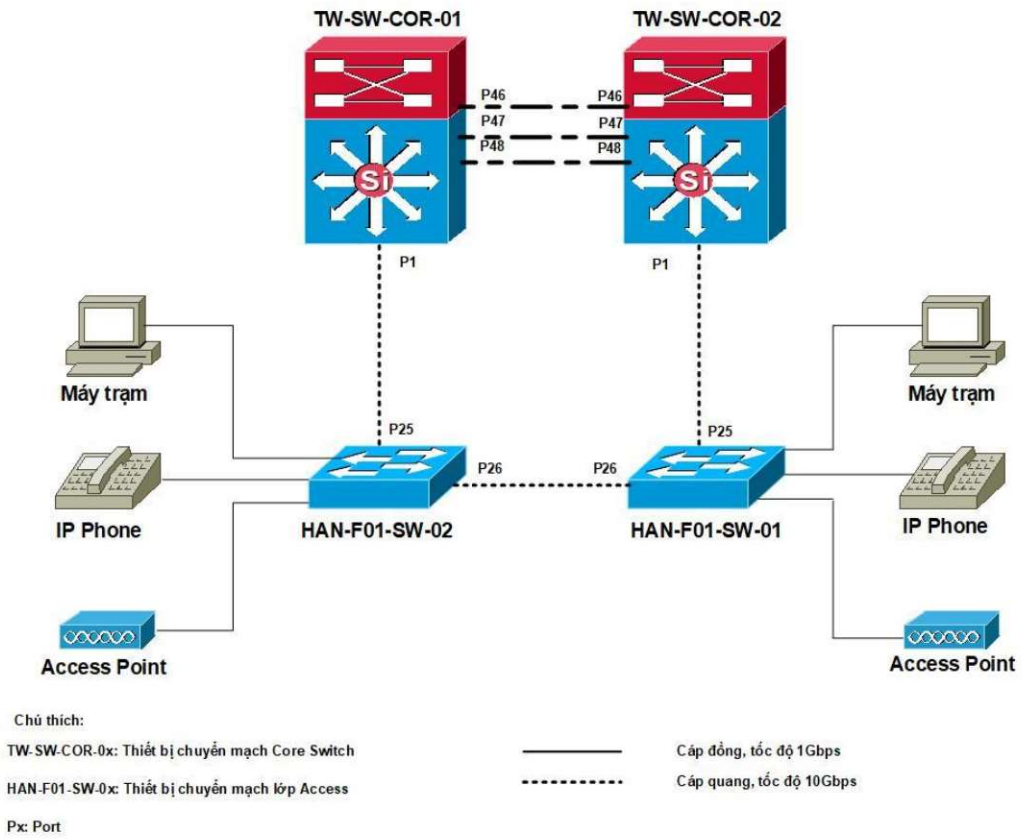
- + 18 port 10GE kết nối với 18 thiết bị chuyển mạch lớp Access tầng
- + 01 port 10GE kết nối với 01 thiết bị chuyển mạch vùng biên
- + 03 port 25GE kết nối với thiết bị Core Switch 01

Phương án triển khai: 02 thiết bị chuyển mạch Core Switch sẽ được triển khai tại trụ sở KBNN 32 Cát Linh. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

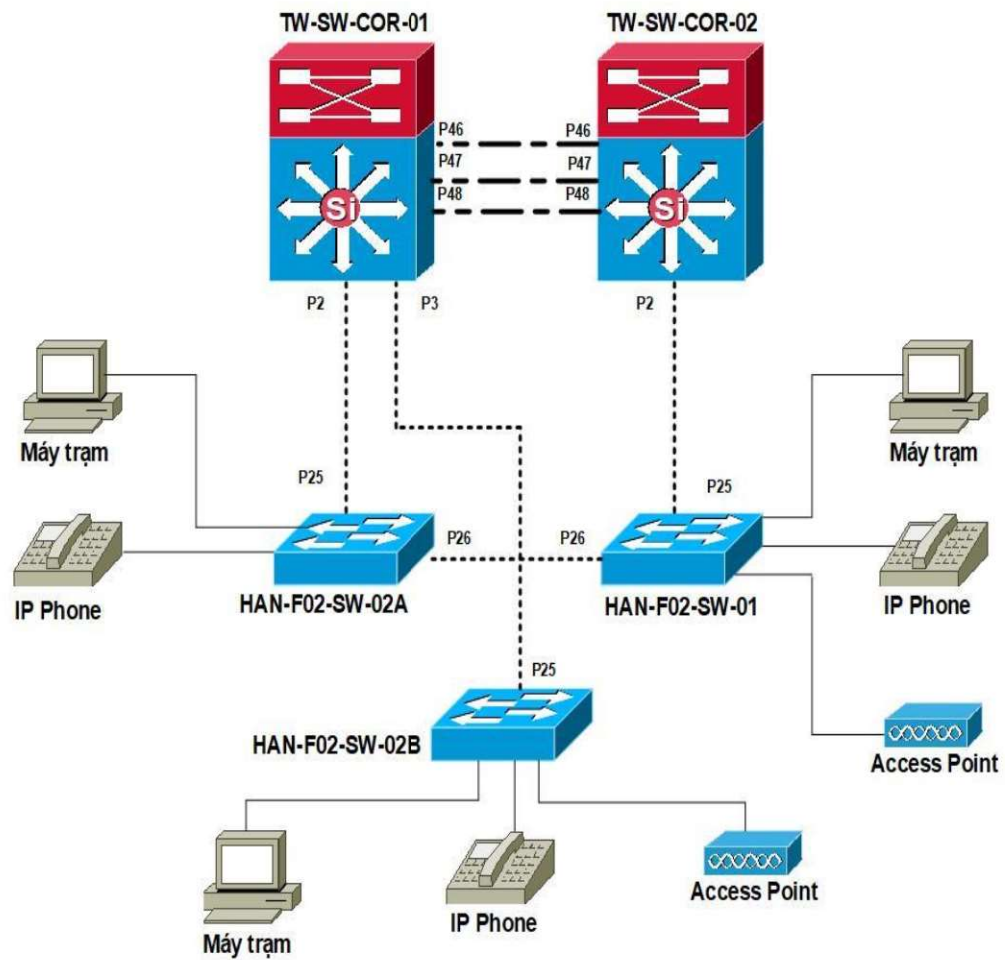
8.7.7. Thiết bị chuyển mạch lớp Access

8.7.7.1. Sơ đồ thiết kế

Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 1:



Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 2:

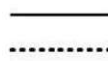


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch

HAN-F02-SW-0x: Thiết bị chuyển mạch lớp Access

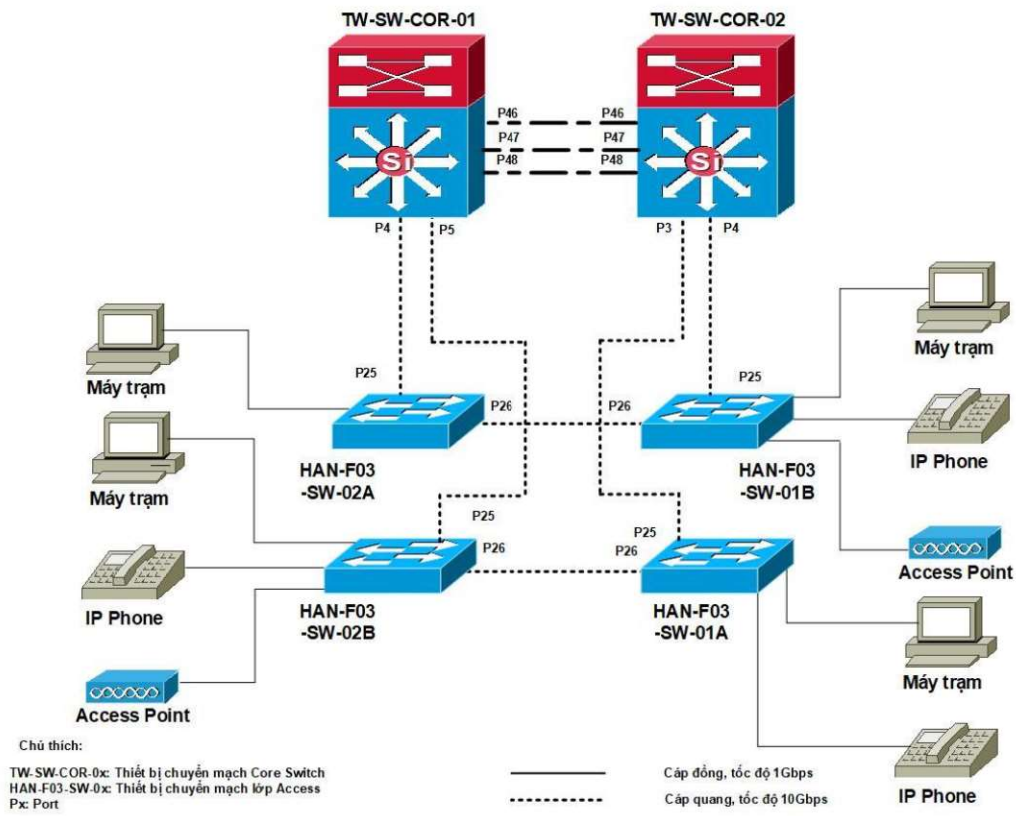
Px: Port



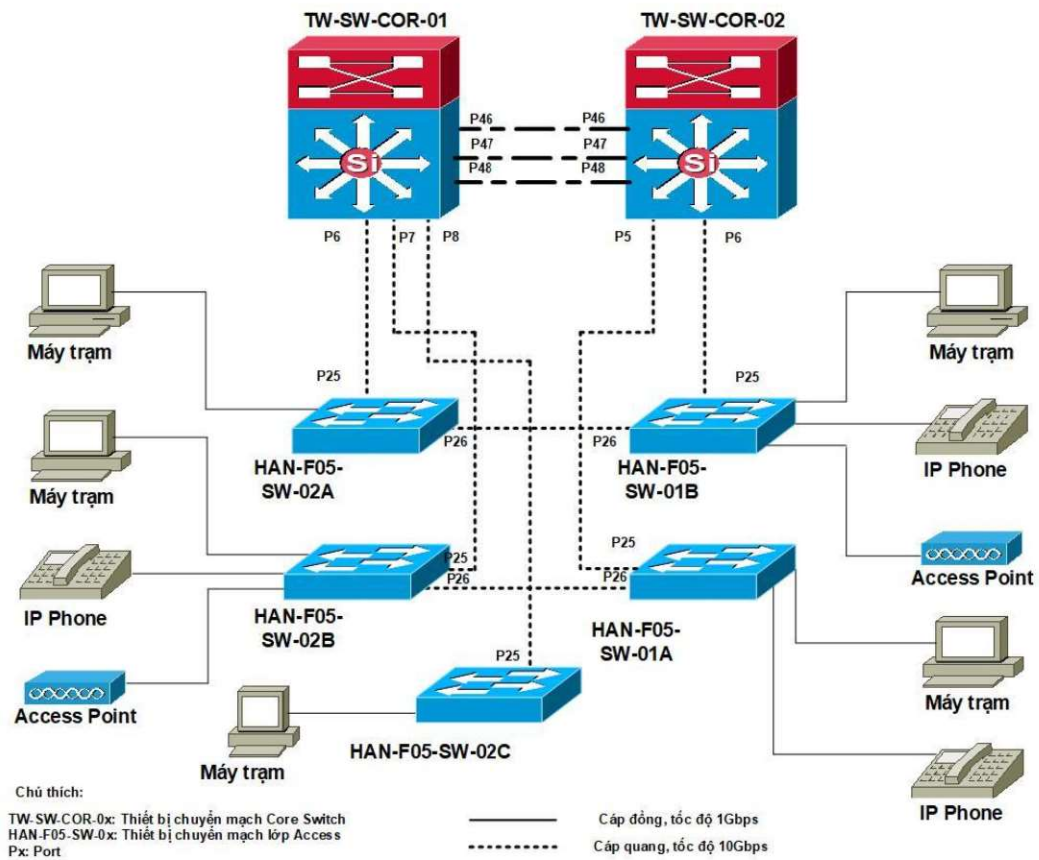
Cáp đồng, tốc độ 1Gbps

Cáp quang, tốc độ 10Gbps

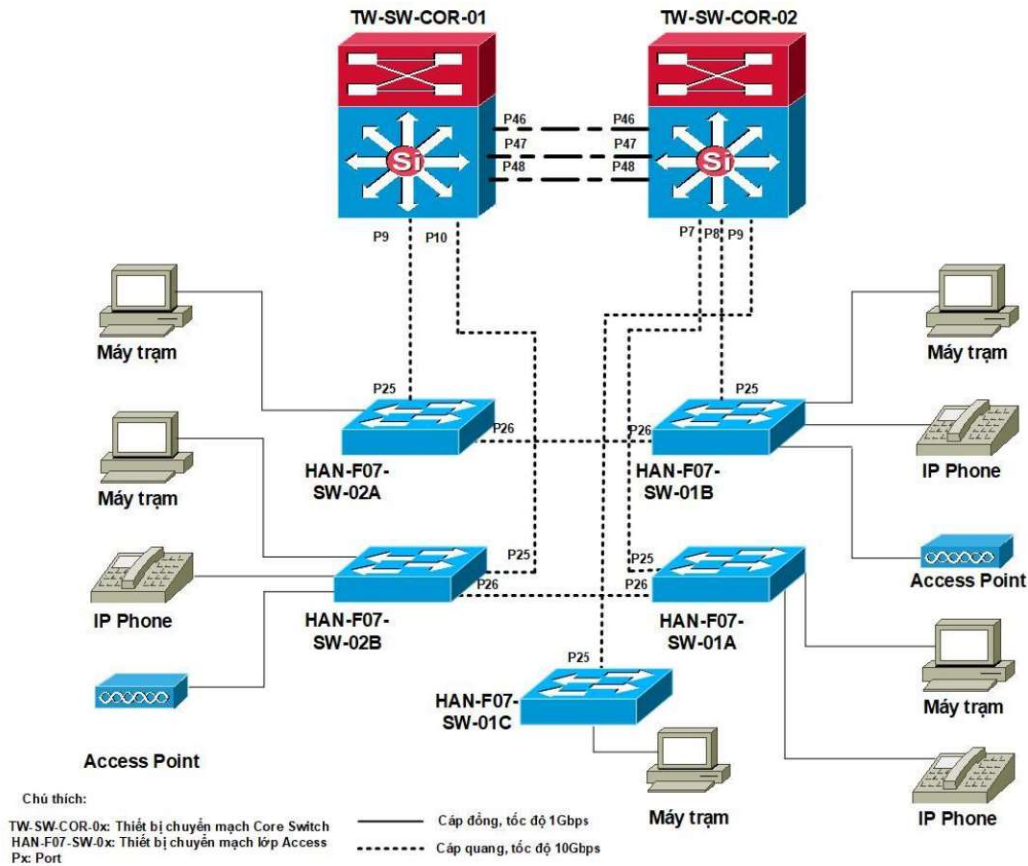
Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 3:



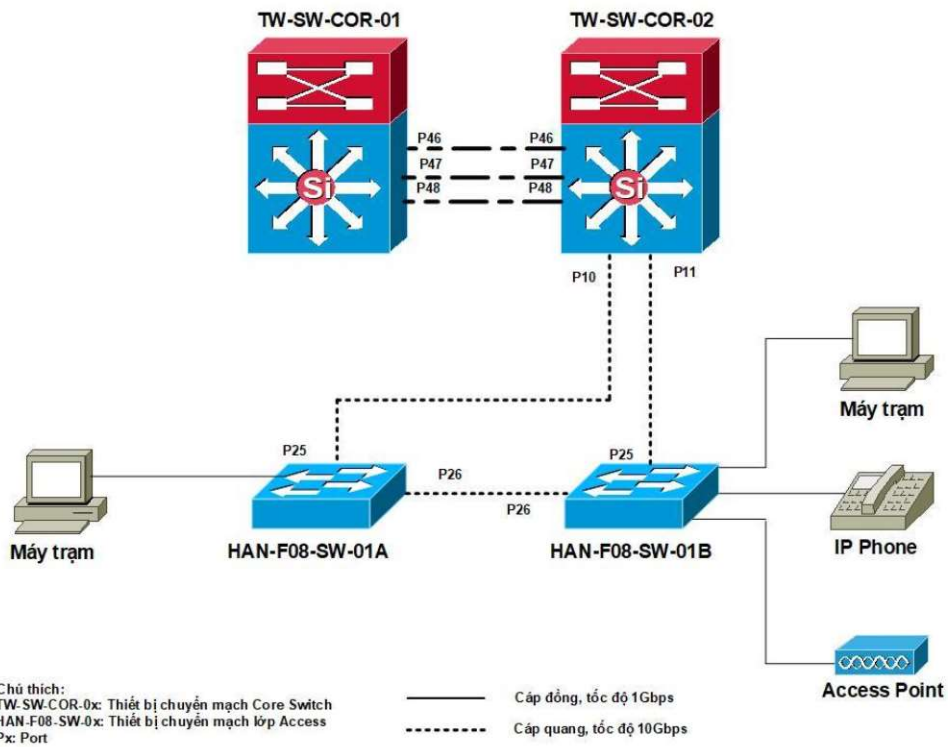
Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 5:



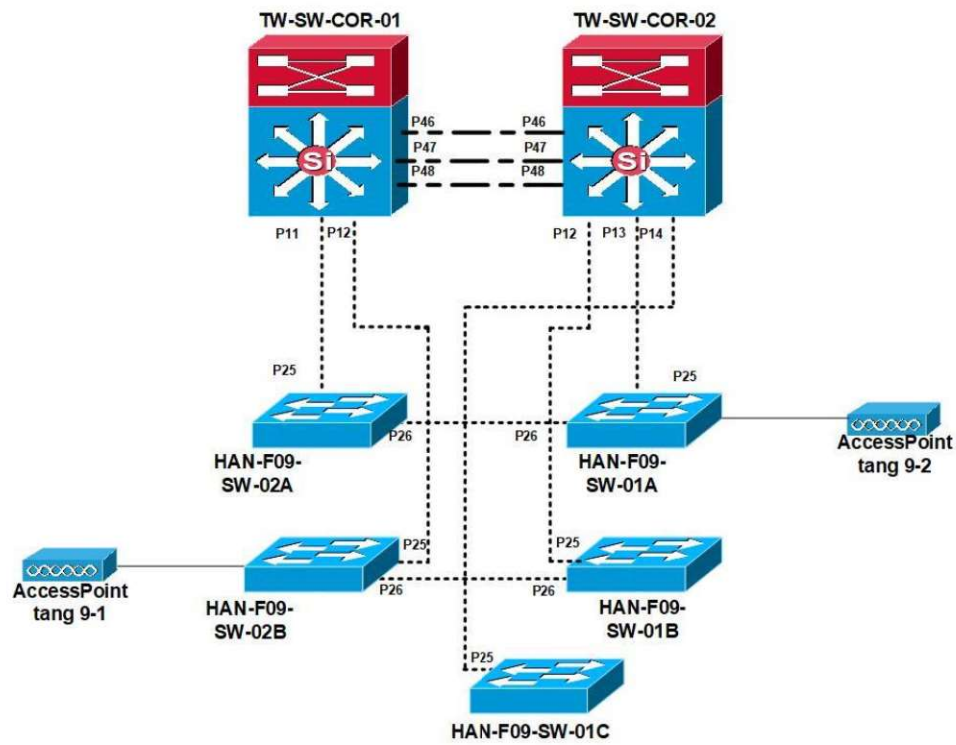
Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 7:



Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 8:



Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 9:



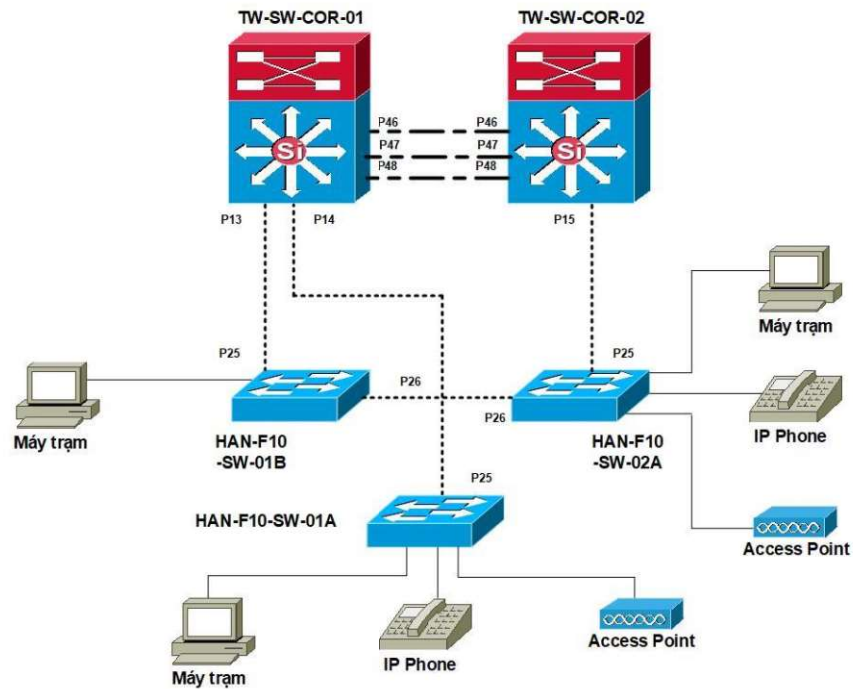
Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
HAN-F09-SW-0x: Thiết bị chuyển mạch lớp Access
Px: Port



Cáp đồng, tốc độ 1Gbps
Cáp quang, tốc độ 10Gbps

Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 10:

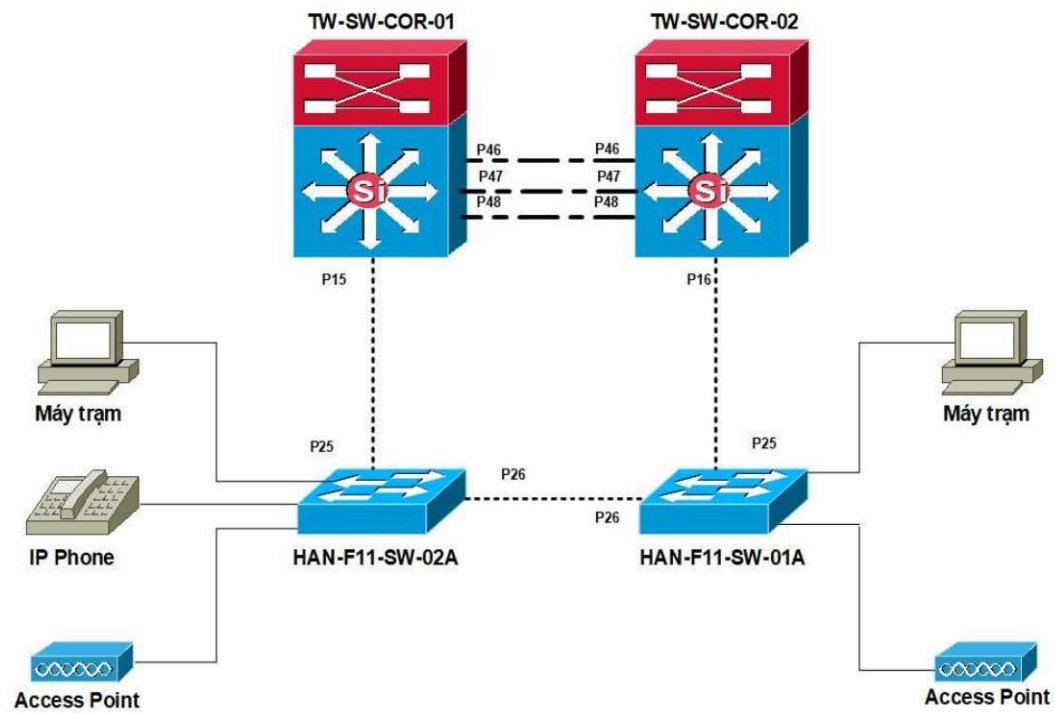


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
 HAN-F10-SW-0x: Thiết bị chuyển mạch lớp Access
 Px: Port

————— Cáp đồng, tốc độ 1Gbps
 - - - - - Cáp quang, tốc độ 10Gbps

Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 11:

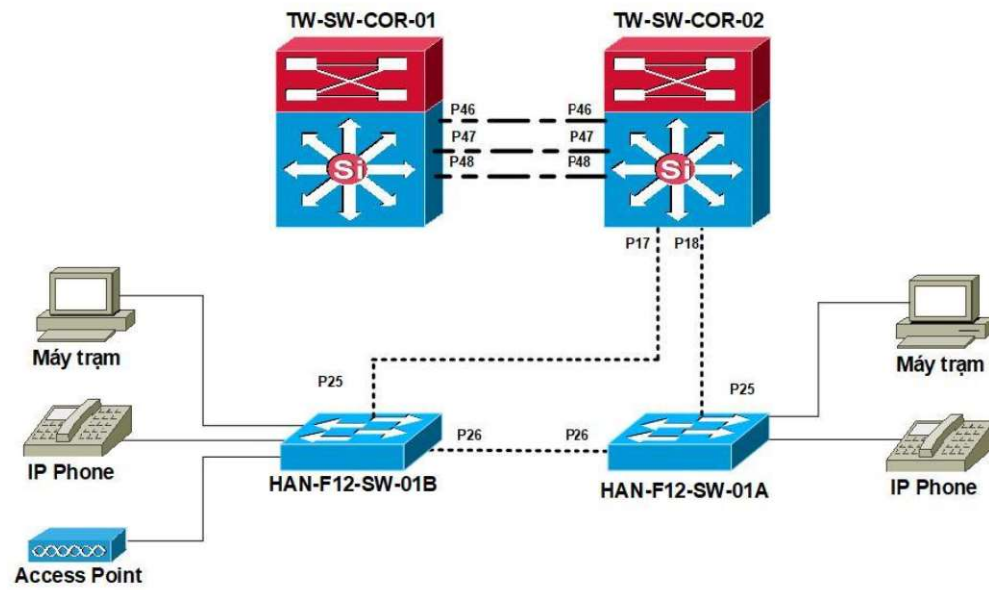


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
HAN-F11-SW-0x: Thiết bị chuyển mạch lớp Access
Px: Port

————— Cáp đồng, tốc độ 1Gbps
----- Cáp quang, tốc độ 10Gbps

Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 12:



Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch

HAN-F12-SW-0x: Thiết bị chuyển mạch lớp Access

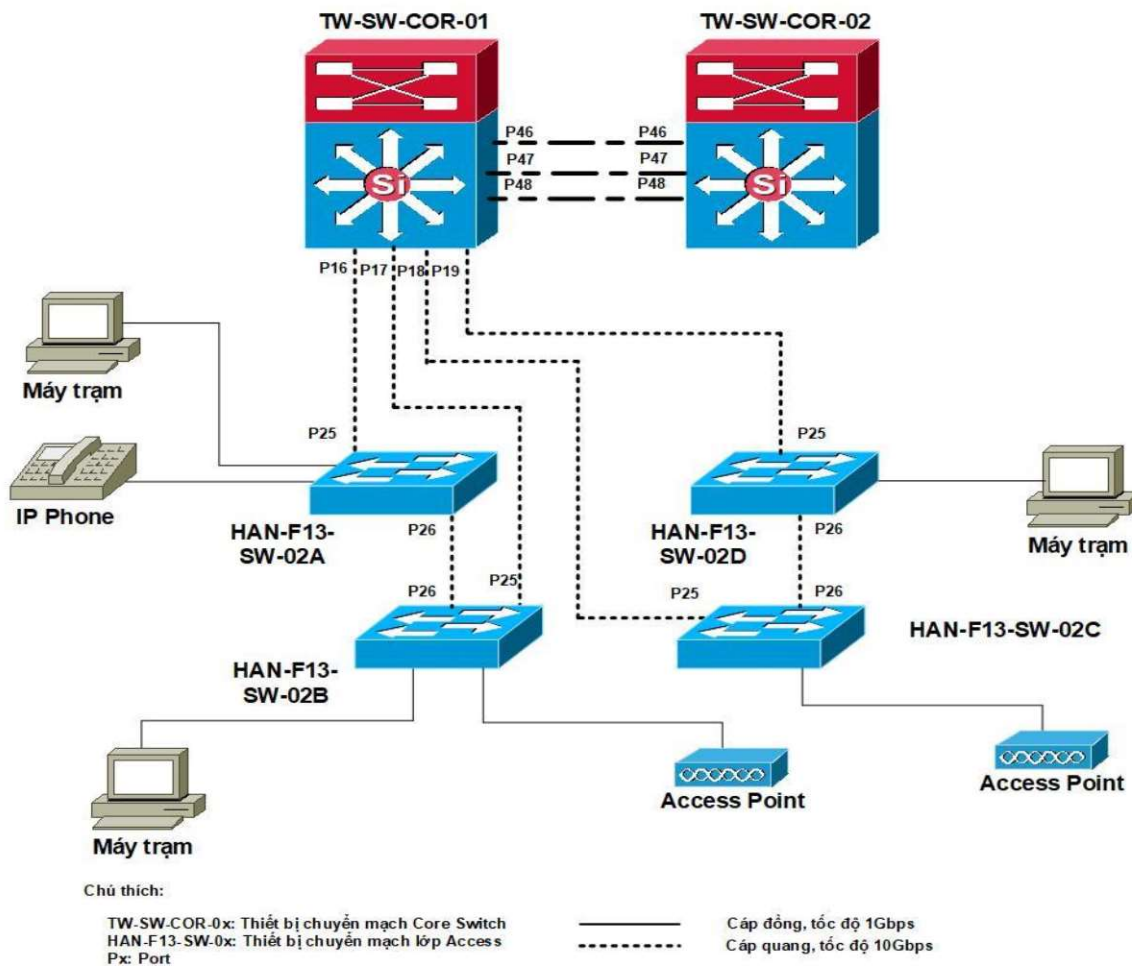
Px: Port

—————

Cáp đồng, tốc độ 1Gbps

Cáp quang, tốc độ 10Gbps

Mô hình thiết kế thiết bị chuyển mạch lớp Access – Tầng 13:



8.7.7.2. Thuyết minh giải pháp

Thiết kế cho khối chuyển mạch lớp Access bao gồm 37 thiết bị. Các thiết bị chuyển mạch Access sẽ thay thế cho 37 thiết bị Juniper EX3300-24T hiện tại.

Các thiết bị chuyển mạch lớp Access được phân bổ trên các tầng tại trụ sở KBNN, mỗi thiết bị chuyển mạch lớp Access sẽ bao gồm 01 kết nối uplink tốc độ 10Gbps quang đến hệ thống chuyển mạch Core Switch và 24 kết nối downlink 1Gbps đồng kết nối đến các thiết bị đầu cuối (như PC, Máy in, Access Point, v.v...)

Thiết bị chuyển mạch lớp Access được thiết kế kết nối với các thành phần bao gồm: thiết bị chuyển mạch Core Switch, thiết bị phát sóng Access point, thiết bị điều khiển Access point, hệ thống điều khiển truy cập mạng tạo thành một mạng SD-LAN cho người sử dụng tại cơ quan KBNN. Tất cả các thiết bị chuyển mạch lớp Access được giám sát, quản trị tập trung bởi thiết bị quản lý mạng người dùng.

Dưới đây là bảng phân bổ kết nối 10GE trên mỗi thiết bị chuyển mạch lớp Access:

| TT | Switch/Cổng | Kết nối tới | Tốc độ | Vị trí lắp đặt |
|----------|-----------------------|----------------------|--------|------------------------|
| 1 | HAN-F01-SW-01 | | | Tầng 01 – KT102 |
| | P25 | TW-SW-COR-02 (P1) | 10GE | |
| | P26 | HAN-F01-SW-02 (P26) | 10GE | |
| 2 | HAN-F01-SW-02 | | | Tầng 01 – KT101 |
| | P25 | TW-SW-COR-01 (P1) | 10GE | |
| | P26 | HAN-F01-SW-01 (P26) | 10GE | |
| 3 | HAN-F02-SW-01 | | | Tầng 02 – KT202 |
| | P25 | TW-SW-COR-02 (P2) | 10GE | |
| | P26 | HAN-F02-SW-02A (P26) | 10GE | |
| 4 | HAN-F02-SW-02A | | | Tầng 02 – KT201 |
| | P25 | TW-SW-COR-01 (P2) | 10GE | |
| | P26 | HAN-F02-SW-01 (P26) | 10GE | |
| 5 | HAN-F02-SW-02B | | | Tầng 02 – KT201 |
| | P25 | TW-SW-COR-01 (P3) | 10GE | |
| 6 | HAN-F03-SW-01A | | | Tầng 03 – KT302 |
| | P25 | TW-SW-COR-02 (P3) | 10GE | |
| | P26 | HAN-F03-SW-02B (P26) | 10GE | |
| 7 | HAN-F03-SW-01B | | | Tầng 03 – KT302 |
| | P25 | TW-SW-COR-02 (P4) | 10GE | |
| | P26 | HAN-F03-SW-02A (P26) | 10GE | |
| 8 | HAN-F03-SW-02A | | | Tầng 03 – KT301 |
| | P25 | TW-SW-COR-01 (P4) | 10GE | |
| | P26 | HAN-F03-SW-01B (P26) | 10GE | |

| | | | | |
|-----------|-----------------------|----------------------|------|------------------------|
| 9 | HAN-F03-SW-02B | | | Tầng 03 – KT301 |
| | P25 | TW-SW-COR-01 (P5) | 10GE | |
| | P26 | HAN-F03-SW-01A (P26) | 10GE | |
| 10 | HAN-F05-SW-01A | | | Tầng 05 – KT502 |
| | P25 | TW-SW-COR-02 (P5) | 10GE | |
| | P26 | HAN-F05-SW-02B (P26) | 10GE | |
| 11 | HAN-F05-SW-01B | | | Tầng 05 – KT502 |
| | P25 | TW-SW-COR-02 (P6) | 10GE | |
| | P26 | HAN-F05-SW-02A (P26) | 10GE | |
| 12 | HAN-F05-SW-02A | | | Tầng 05 – KT501 |
| | P25 | TW-SW-COR-01 (P6) | 10GE | |
| | P26 | HAN-F05-SW-01B (P26) | 10GE | |
| 13 | HAN-F05-SW-02B | | | Tầng 05 – KT501 |
| | P25 | TW-SW-COR-01 (P7) | 10GE | |
| | P26 | HAN-F05-SW-01A (P2) | 10GE | |
| 14 | HAN-F05-SW-02C | | | Tầng 05 – KT501 |
| | P25 | TW-SW-COR-01 (P8) | 10GE | |
| 15 | HAN-F07-SW-01A | | | Tầng 07 – KT702 |
| | P25 | TW-SW-COR-02 (P7) | 10GE | |
| | P26 | HAN-F07-SW-02B (P26) | 10GE | |
| 16 | HAN-F07-SW-01B | | | Tầng 07 – KT702 |
| | P25 | TW-SW-COR-02 (P8) | 10GE | |
| | P26 | HAN-F07-SW-02A (P26) | 10GE | |
| 17 | HAN-F07-SW-01C | | | Tầng 07 – KT702 |
| | P25 | TW-SW-COR-02 (P9) | 10GE | |
| 18 | HAN-F07-SW-02A | | | Tầng 07 – KT701 |

| | | | | |
|-----------|-----------------------|----------------------|------|-------------------------|
| | P25 | TW-SW-COR-01 (P9) | 10GE | |
| | P26 | HAN-F07-SW-01B (P26) | 10GE | |
| 19 | HAN-F07-SW-02B | | | Tầng 07 – KT701 |
| | P25 | TW-SW-COR-01 (P10) | 10GE | |
| | P26 | HAN-F07-SW-01A (P26) | 10GE | |
| 20 | HAN-F08-SW-01A | | | Tầng 08 – KT801 |
| | P25 | TW-SW-COR-02 (P10) | 10GE | |
| | P26 | HAN-F08-SW-01B (P26) | 10GE | |
| 21 | HAN-F08-SW-01B | | | Tầng 08 – KT801 |
| | P25 | TW-SW-COR-02 (P11) | 10GE | |
| | P26 | HAN-F08-SW-01A (P26) | 10GE | |
| 22 | HAN-F09-SW-01A | | | Tầng 09 – KT902 |
| | P25 | TW-SW-COR-02 (P13) | 10GE | |
| | P26 | HAN-F09-SW-02A (P26) | 10GE | |
| 23 | HAN-F09-SW-01B | | | Tầng 09 – KT902 |
| | P25 | TW-SW-COR-02 (P12) | 10GE | |
| | P26 | HAN-F09-SW-02B (P26) | 10GE | |
| 24 | HAN-F09-SW-01C | | | Tầng 09 – KT902 |
| | P25 | TW-SW-COR-02 (P14) | 10GE | |
| 25 | HAN-F09-SW-02A | | | Tầng 09 – KT901 |
| | P25 | TW-SW-COR-01 (P11) | 10GE | |
| | P26 | HAN-F09-SW-01A (P26) | 10GE | |
| 26 | HAN-F09-SW-02B | | | Tầng 09 – KT901 |
| | P25 | TW-SW-COR-01 (P12) | 10GE | |
| | P26 | HAN-F09-SW-01B (P26) | 10GE | |
| 27 | HAN-F10-SW-01A | | | Tầng 10 – KT1002 |

| | | | | |
|-----------|-----------------------|----------------------|------|-------------------------|
| | P25 | TW-SW-COR-01 (P14) | 10GE | |
| 28 | HAN-F10-SW-01B | | | Tầng 10 – KT1002 |
| | P25 | TW-SW-COR-01 (P13) | 10GE | |
| | P26 | HAN-F10-SW-02A (P26) | 10GE | |
| 29 | HAN-F10-SW-02A | | | Tầng 10 – KT1001 |
| | P25 | TW-SW-COR-02 (P15) | 10GE | |
| | P26 | HAN-F10-SW-01B (P26) | 10GE | |
| 30 | HAN-F11-SW-01A | | | Tầng 11 – KT1102 |
| | P25 | TW-SW-COR-02 (P16) | 10GE | |
| | P26 | HAN-F11-SW-02A (P26) | 10GE | |
| 31 | HAN-F11-SW-02A | | | Tầng 11 – KT1101 |
| | P25 | TW-SW-COR-01 (P15) | 10GE | |
| | P26 | HAN-F11-SW-01A (P26) | 10GE | |
| 32 | HAN-F12-SW-01A | | | Tầng 12 – KT1202 |
| | P25 | TW-SW-COR-02 (P18) | 10GE | |
| | P26 | HAN-F12-SW-01B (P26) | 10GE | |
| 33 | HAN-F12-SW-01B | | | Tầng 12 – KT1202 |
| | P25 | TW-SW-COR-02 (P17) | 10GE | |
| | P26 | HAN-F12-SW-01A (P26) | 10GE | |
| 34 | HAN-F13-SW-02A | | | Tầng 13 – KT1301 |
| | P25 | TW-SW-COR-01 (P16) | 10GE | |
| | P26 | HAN-F13-SW-02B (P26) | 10GE | |
| 35 | HAN-F13-SW-02B | | | Tầng 13 – KT1301 |
| | P25 | TW-SW-COR-01 (P17) | 10GE | |
| | P26 | HAN-F13-SW-02A (P26) | 10GE | |
| 36 | HAN-F13-SW-02C | | | Tầng 13 – KT1301 |

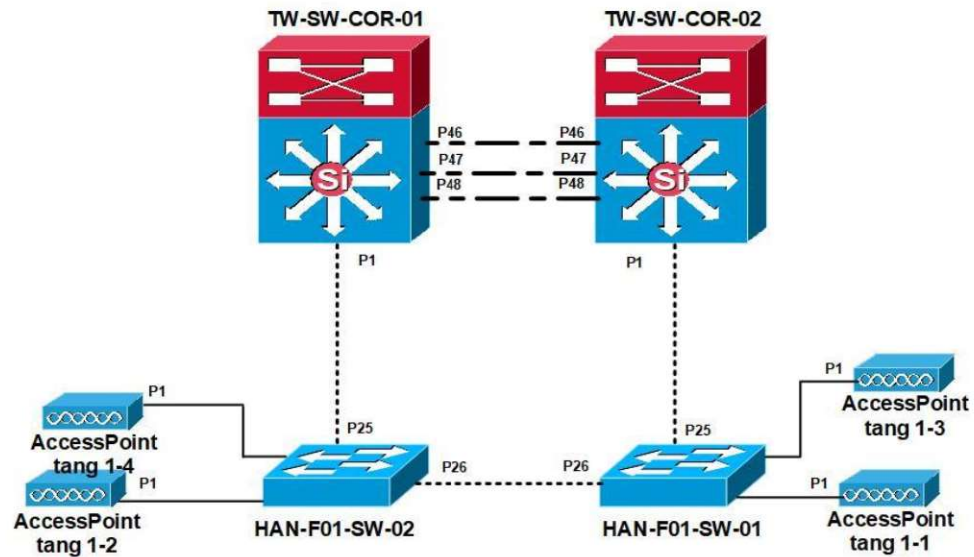
| | | | | |
|-----------|-----------------------|----------------------|------|-------------------------|
| | P25 | TW-SW-COR-01 (P18) | 10GE | |
| | P26 | HAN-F13-SW-02D (P26) | 10GE | |
| 37 | HAN-F13-SW-02D | | | Tầng 13 – KT1301 |
| | P25 | TW-SW-COR-01 (P19) | 10GE | |
| | P26 | HAN-F13-SW-02C (P26) | 10GE | |

Phương án triển khai: 37 thiết bị chuyển mạch lớp Access sẽ được triển khai tại các tầng ở trụ sở KBNN 32 Cát Linh. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.8. Thiết bị phát sóng Access point

8.7.8.1. Sơ đồ thiết kế

Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 1:



Chú thích:

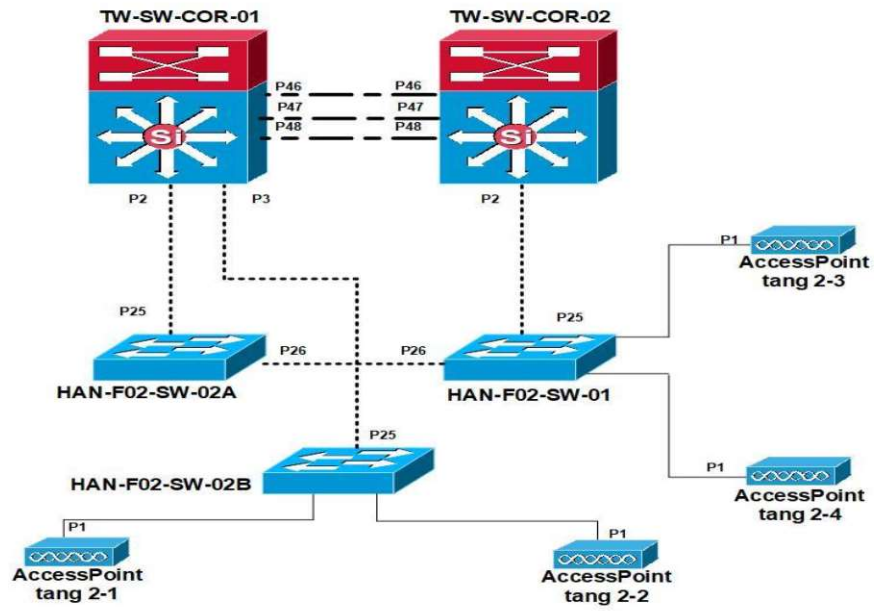
TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch

HAN-F01-SW-0x: Thiết bị chuyển mạch lớp Access

Px: Port

———— Cáp đồng, tốc độ 1Gbps
 - - - - - Cáp quang, tốc độ 10Gbps
 - - - - - Cáp quang, tốc độ 25Gbps

Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 2:

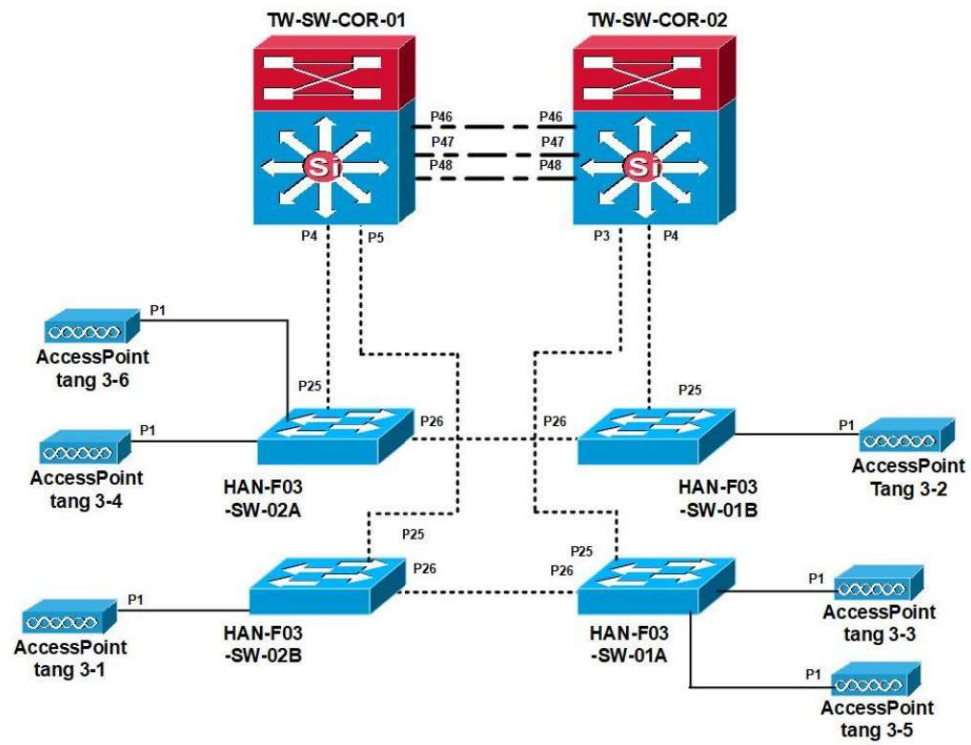


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
 HAN-F02-SW-0x: Thiết bị chuyển mạch lớp Access
 Px: Port

————— Cáp đồng, tốc độ 1Gbps
 - - - - - Cáp quang, tốc độ 10Gbps
 - . - . - Cáp quang, tốc độ 25Gbps

Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 3:

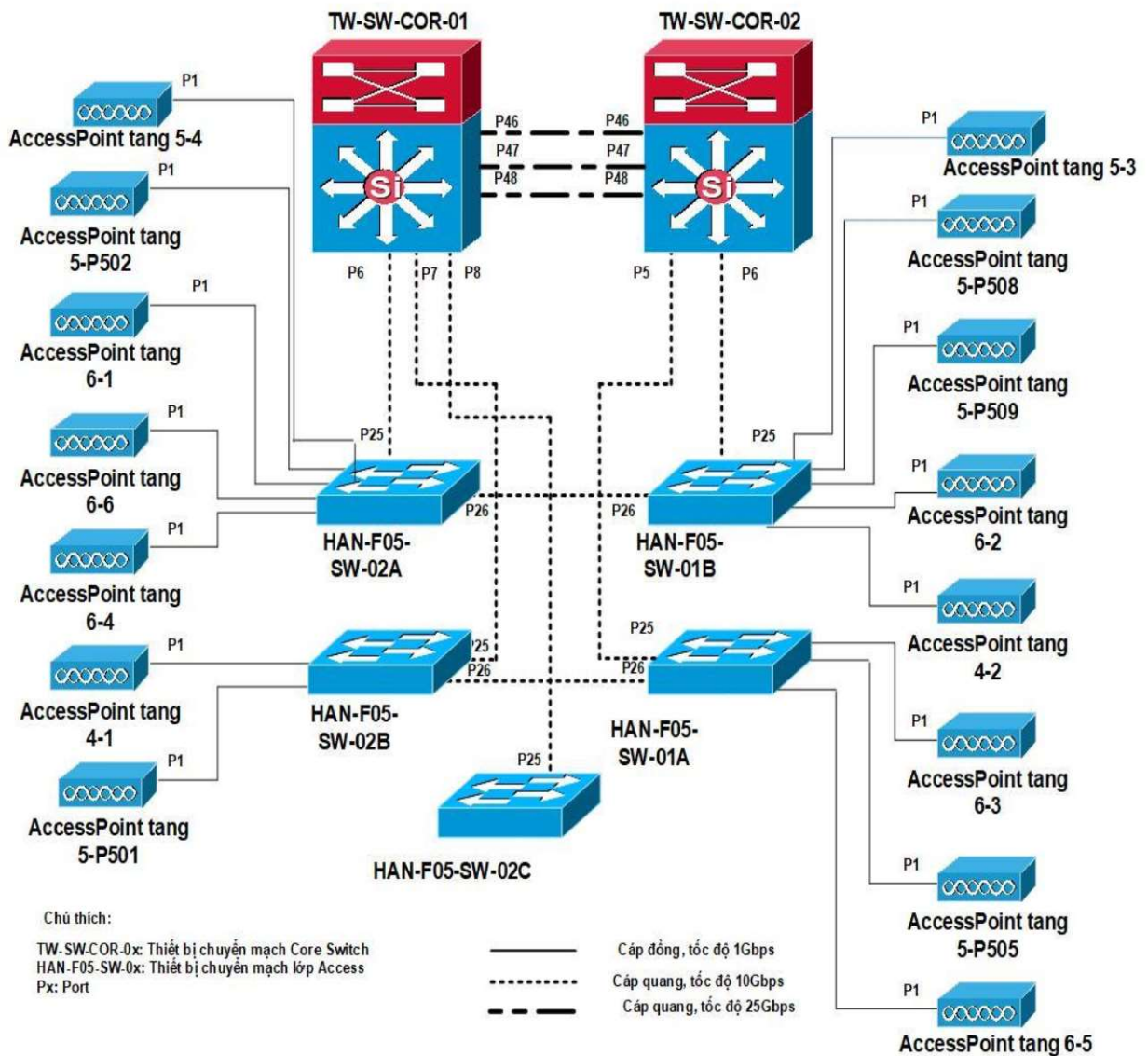


Chú thích:

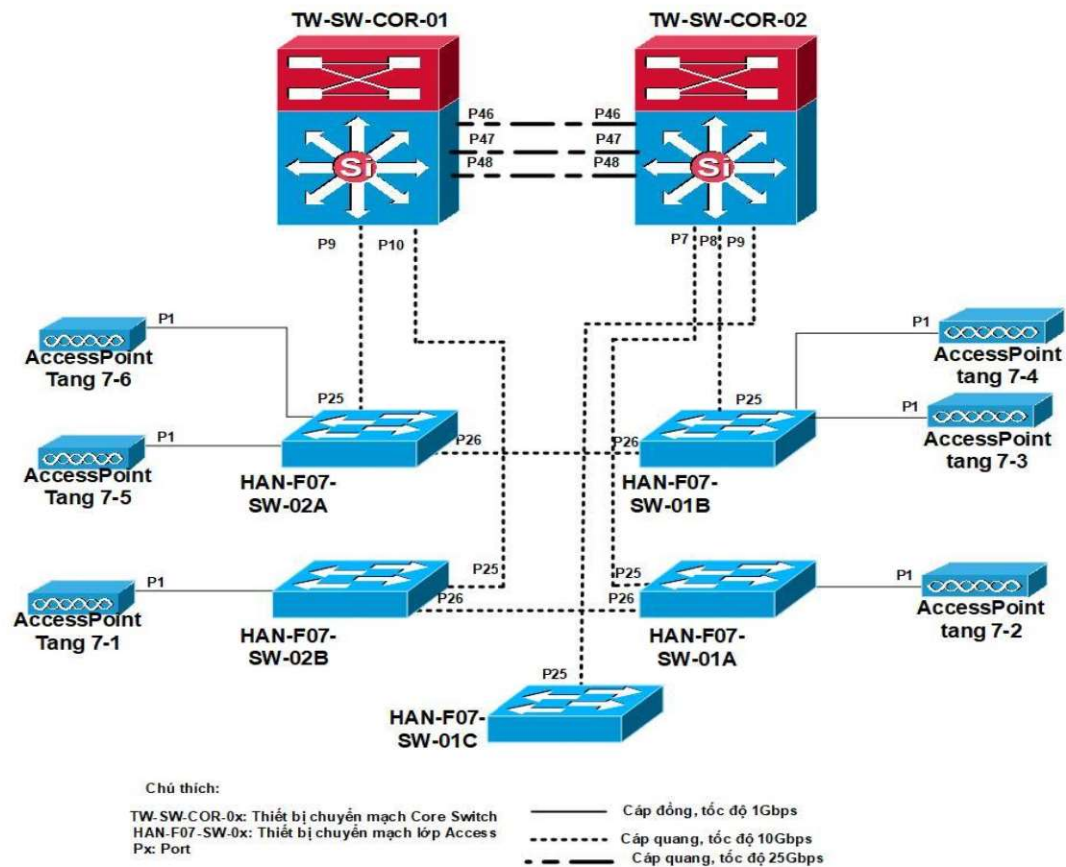
TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
HAN-F03-SW-0x: Thiết bị chuyển mạch lớp Access
Px: Port

————— Cáp đồng, tốc độ 1Gbps
----- Cáp quang, tốc độ 10Gbps
- . - . - Cáp quang, tốc độ 25Gbps

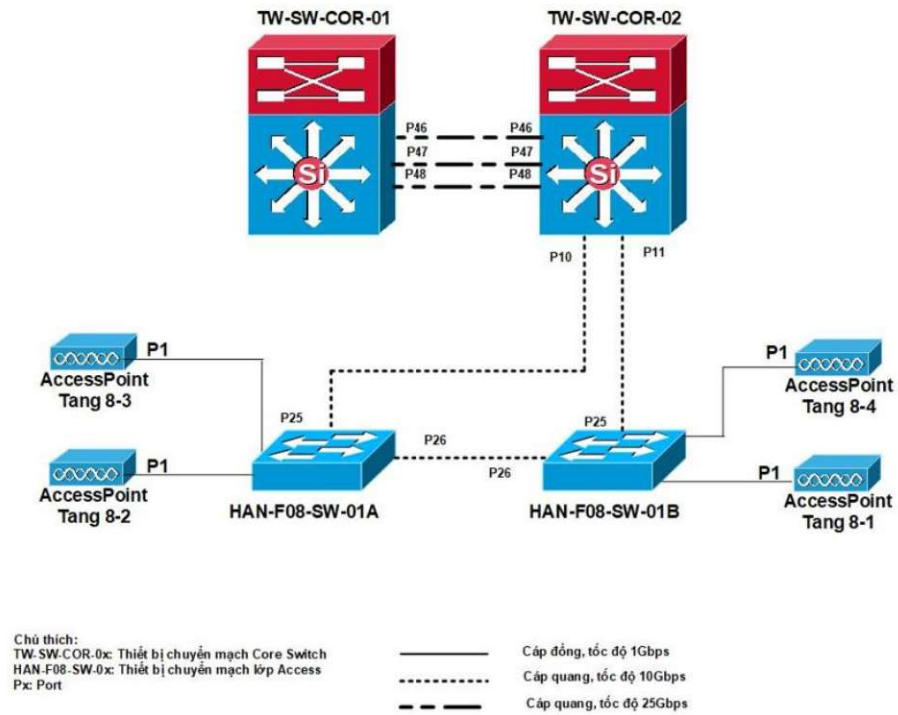
Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 4, 5, 6:



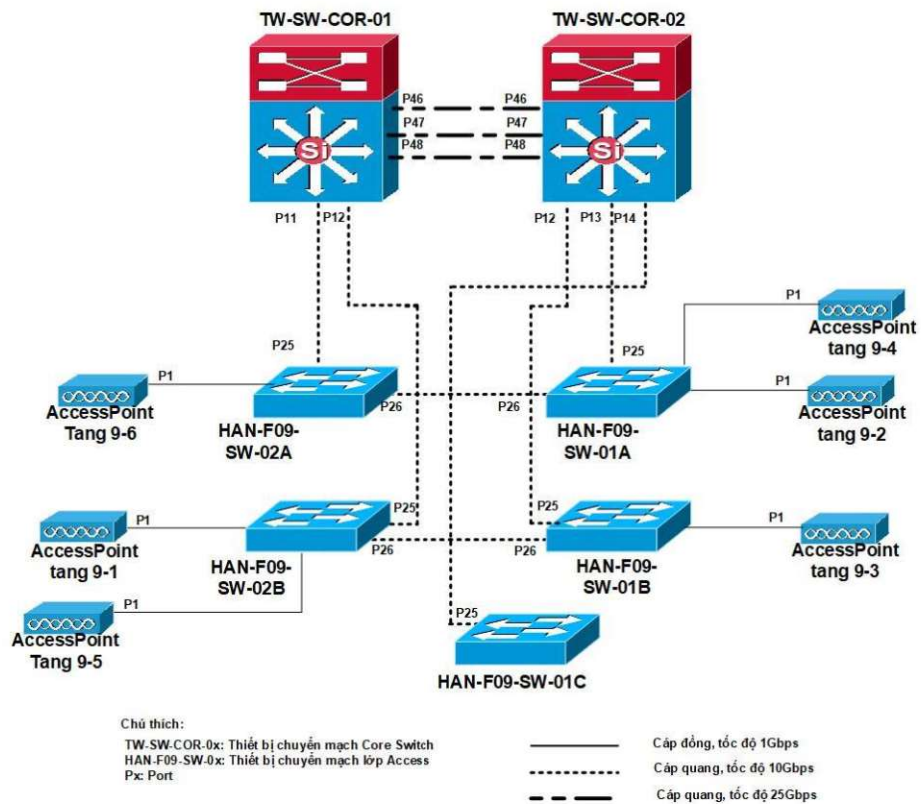
Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 7:



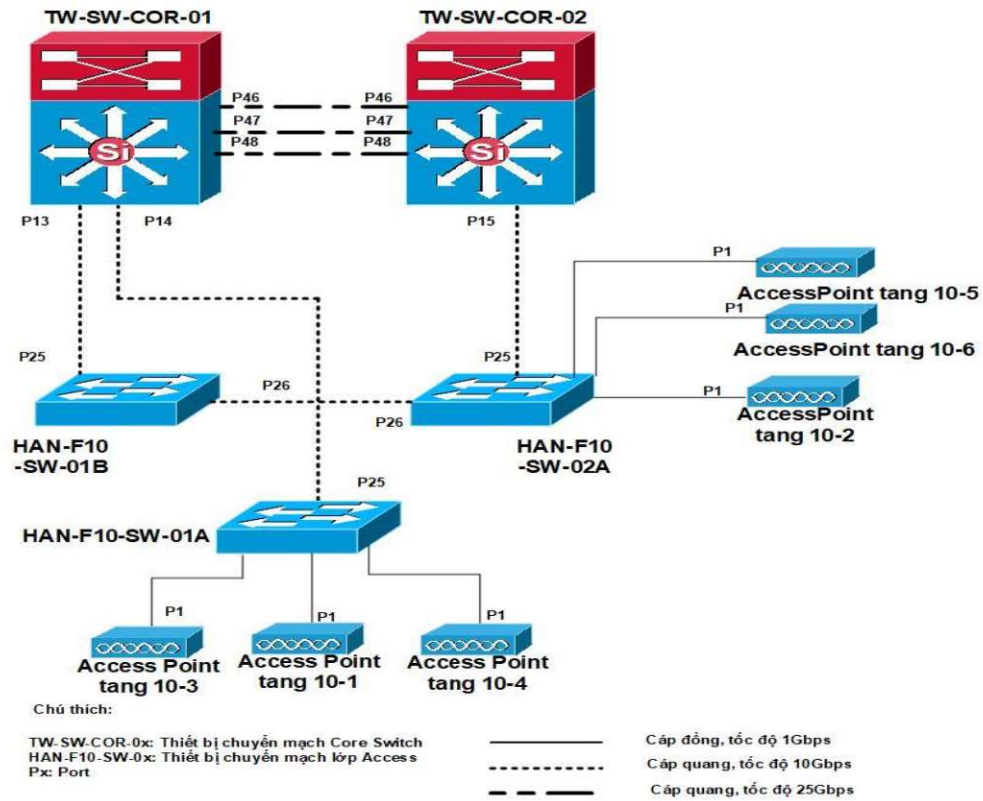
Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 8:



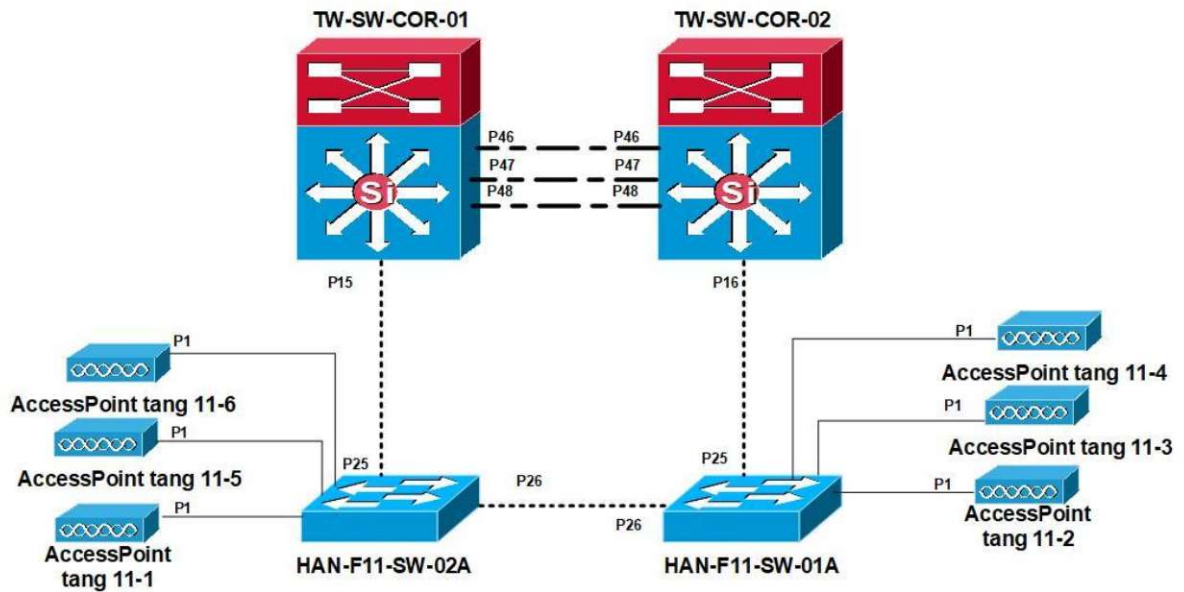
Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 9:



Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 10:



Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 11:

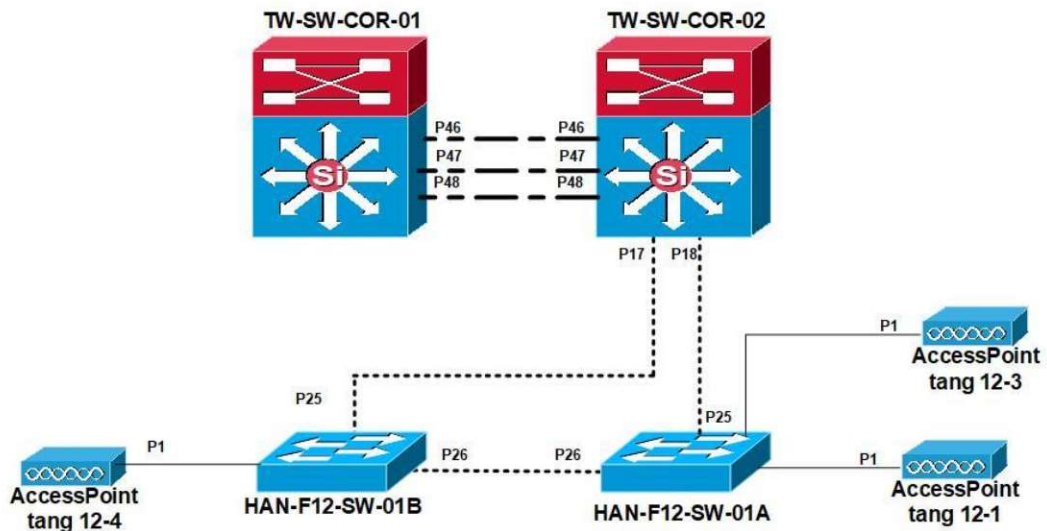


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
HAN-F11-SW-0x: Thiết bị chuyển mạch lớp Access
Px: Port

————— Cáp đồng, tốc độ 1Gbps
----- Cáp quang, tốc độ 10Gbps
- . - . - Cáp quang, tốc độ 25Gbps

Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 12:

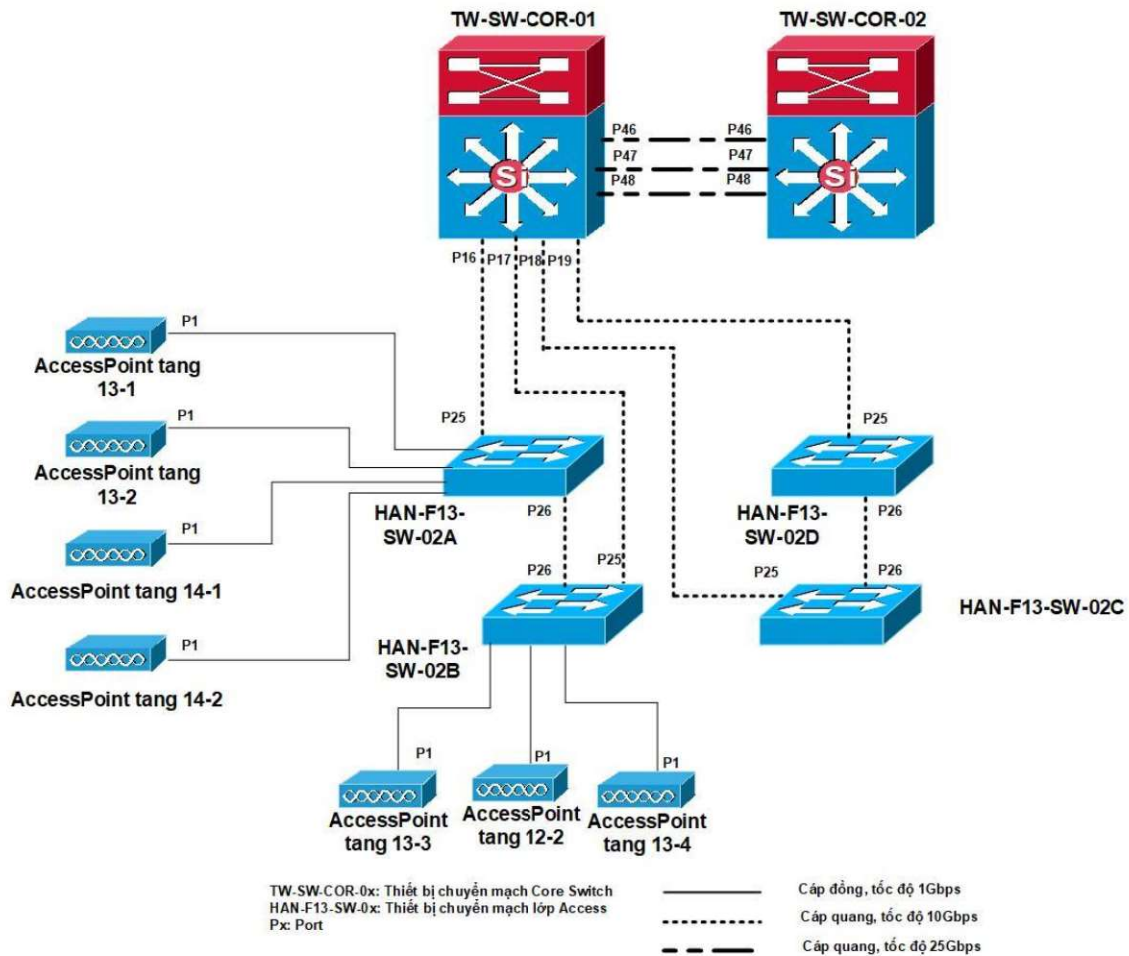


Chú thích:

TW-SW-COR-0x: Thiết bị chuyển mạch Core Switch
HAN-F12-SW-0x: Thiết bị chuyển mạch lớp Access
Px: Port

————— Cáp đồng, tốc độ 1Gbps
----- Cáp quang, tốc độ 10Gbps
- . - . - Cáp quang, tốc độ 25Gbps

Mô hình thiết kế thiết bị phát sóng Access Point – Tầng 13, 14:



8.7.8.2. Thuyết minh giải pháp

Thiết kế bao gồm 67 thiết bị phát sóng Access Point đóng vai trò là điểm kết nối không dây cho tất cả các thiết bị đầu cuối tương thích với chuẩn 802.11n, 802.11ac, 802.11ax. Các thiết bị này sẽ thay thế và bổ sung cho thiết bị Juniper WLA532 hiện tại. Các thiết bị này phải được điều khiển bởi thiết bị điều khiển Access point

Mỗi thiết bị phát sóng Access point sẽ gồm 01 giao tiếp tốc độ 10/100/1000BASE-T kết nối đến thiết bị chuyển mạch lớp Access. Dưới đây là bảng phân bổ thiết bị phát sóng Access point.

| STT | Thiết bị phát sóng Access Point | Kết nối tới | Vị trí lắp đặt thiết bị |
|-----|---------------------------------|-------------|-------------------------|
|-----|---------------------------------|-------------|-------------------------|

| | | | |
|----|--------------------------|----------------|--------|
| 1 | Access point tang 1-1 | HAN-F01-SW-01 | Tầng 1 |
| 2 | Access point tang 1-2 | HAN-F01-SW-02 | Tầng 1 |
| 3 | Access point tang 1-3 | HAN-F01-SW-01 | Tầng 1 |
| 4 | Access point tang 1-4 | HAN-F01-SW-02 | Tầng 1 |
| 5 | Access point tang 2-1 | HAN-F02-SW-02B | Tầng 2 |
| 6 | Access point tang 2-2 | HAN-F02-SW-02B | Tầng 2 |
| 7 | Access point tang 2-3 | HAN-F02-SW-01 | Tầng 2 |
| 8 | Access point tang 2-4 | HAN-F02-SW-01 | Tầng 2 |
| 9 | Access point tang 3-1 | HAN-F03-SW-02B | Tầng 3 |
| 10 | Access point tang 3-2 | HAN-F03-SW-01B | Tầng 3 |
| 11 | Access point tang 3-3 | HAN-F03-SW-01A | Tầng 3 |
| 12 | Access point tang 3-4 | HAN-F03-SW-02A | Tầng 3 |
| 13 | Access point tang 3-5 | HAN-F03-SW-01A | Tầng 3 |
| 14 | Access point tang 3-6 | HAN-F03-SW-02A | Tầng 3 |
| 15 | Access point tang 4-1 | HAN-F05-SW-02B | Tầng 4 |
| 16 | Access point tang 4-2 | HAN-F05-SW-01B | Tầng 4 |
| 17 | Access point tang 5-P501 | HAN-F05-SW-02B | Tầng 5 |
| 18 | Access point tang 5-P502 | HAN-F05-SW-02A | Tầng 5 |
| 19 | Access point tang 5-P505 | HAN-F05-SW-01A | Tầng 5 |
| 20 | Access point tang 5-P508 | HAN-F05-SW-01B | Tầng 5 |
| 21 | Access point tang 5-P509 | HAN-F05-SW-01B | Tầng 5 |
| 22 | Access point tang 5-3 | HAN-F05-SW-01B | Tầng 5 |
| 23 | Access point tang 5-4 | HAN-F05-SW-02A | Tầng 5 |
| 24 | Access point tang 6-1 | HAN-F05-SW-02A | Tầng 6 |
| 25 | Access point tang 6-2 | HAN-F05-SW-01B | Tầng 6 |
| 26 | Access point tang 6-3 | HAN-F05-SW-01A | Tầng 6 |

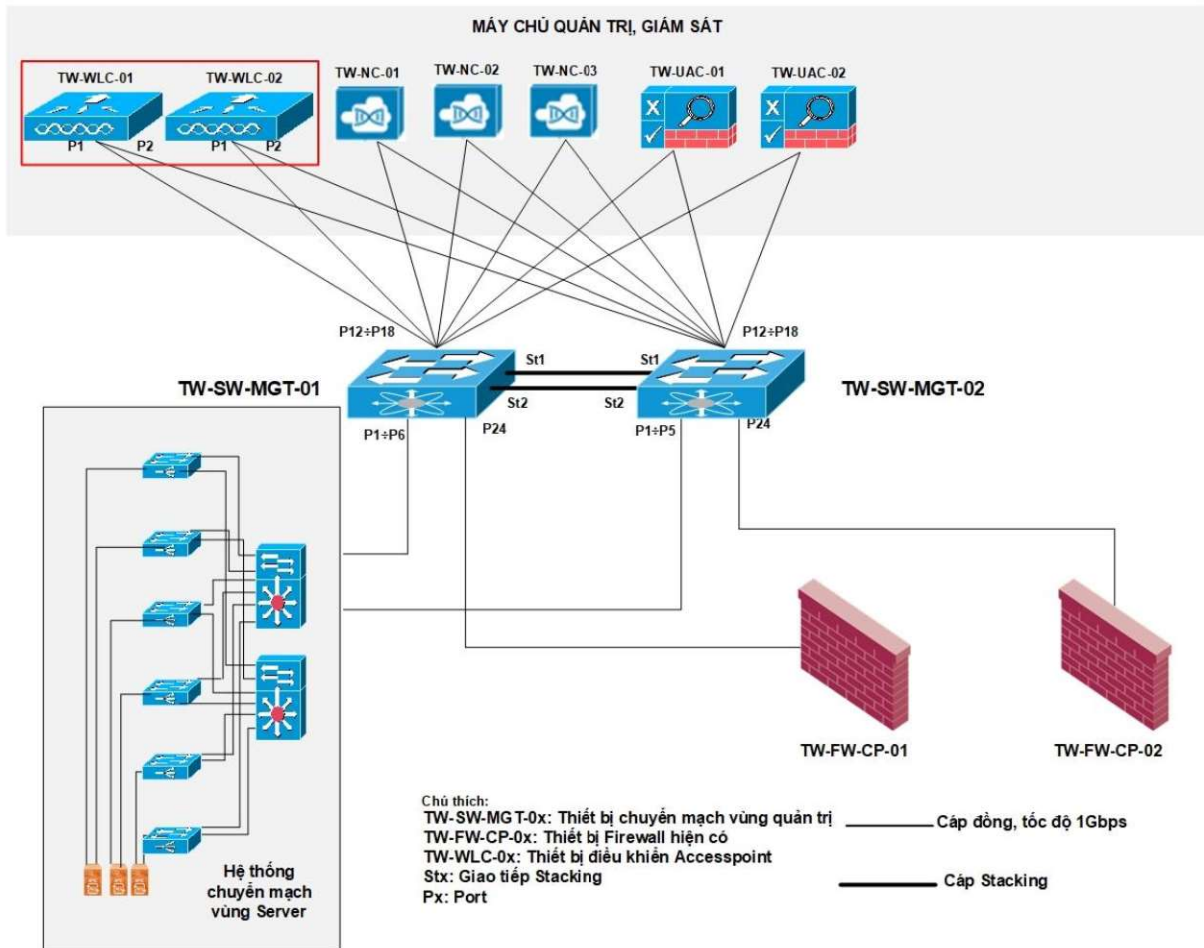
| | | | |
|----|------------------------|----------------|---------|
| 27 | Access point tang 6-4 | HAN-F05-SW-02A | Tầng 6 |
| 28 | Access point tang 6-5 | HAN-F05-SW-01A | Tầng 6 |
| 29 | Access point tang 6-6 | HAN-F05-SW-02A | Tầng 6 |
| 30 | Access point tang 7-1 | HAN-F07-SW-02B | Tầng 7 |
| 31 | Access point tang 7-2 | HAN-F07-SW-01A | Tầng 7 |
| 32 | Access point tang 7-3 | HAN-F07-SW-01B | Tầng 7 |
| 33 | Access point tang 7-4 | HAN-F07-SW-01B | Tầng 7 |
| 34 | Access point tang 7-5 | HAN-F07-SW-02A | Tầng 7 |
| 35 | Access point tang 7-6 | HAN-F07-SW-02A | Tầng 7 |
| 36 | Access point tang 8-1 | HAN-F08-SW-01B | Tầng 8 |
| 37 | Access point tang 8-2 | HAN-F08-SW-01A | Tầng 8 |
| 38 | Access point tang 8-3 | HAN-F08-SW-01A | Tầng 8 |
| 39 | Access point tang 8-4 | HAN-F08-SW-01B | Tầng 8 |
| 40 | Access point tang 9-1 | HAN-F09-SW-02B | Tầng 9 |
| 41 | Access point tang 9-2 | HAN-F09-SW-01A | Tầng 9 |
| 42 | Access point tang 9-3 | HAN-F09-SW-01B | Tầng 9 |
| 43 | Access point tang 9-4 | HAN-F09-SW-01A | Tầng 9 |
| 44 | Access point tang 9-5 | HAN-F09-SW-02B | Tầng 9 |
| 45 | Access point tang 9-6 | HAN-F09-SW-02A | Tầng 9 |
| 46 | Access point tang 10-1 | HAN-F10-SW-01A | Tầng 10 |
| 47 | Access point tang 10-2 | HAN-F10-SW-02A | Tầng 10 |
| 48 | Access point tang 10-3 | HAN-F10-SW-01A | Tầng 10 |
| 49 | Access point tang 10-4 | HAN-F10-SW-01A | Tầng 10 |
| 50 | Access point tang 10-5 | HAN-F10-SW-02A | Tầng 10 |
| 51 | Access point tang 10-6 | HAN-F10-SW-02A | Tầng 10 |
| 52 | Access point tang 11-1 | HAN-F11-SW-02A | Tầng 11 |

| | | | |
|----|------------------------|----------------|---------|
| 53 | Access point tang 11-2 | HAN-F11-SW-01A | Tầng 11 |
| 54 | Access point tang 11-3 | HAN-F11-SW-01A | Tầng 11 |
| 55 | Access point tang 11-4 | HAN-F11-SW-01A | Tầng 11 |
| 56 | Access point tang 11-5 | HAN-F11-SW-02A | Tầng 11 |
| 57 | Access point tang 11-6 | HAN-F11-SW-02A | Tầng 11 |
| 58 | Access point tang 12-1 | HAN-F12-SW-01A | Tầng 12 |
| 59 | Access point tang 12-2 | HAN-F13-SW-02B | Tầng 12 |
| 60 | Access point tang 12-3 | HAN-F12-SW-01A | Tầng 12 |
| 61 | Access point tang 12-4 | HAN-F12-SW-01B | Tầng 12 |
| 62 | Access point tang 13-1 | HAN-F13-SW-02A | Tầng 13 |
| 63 | Access point tang 13-2 | HAN-F13-SW-02A | Tầng 13 |
| 64 | Access point tang 13-3 | HAN-F13-SW-02B | Tầng 13 |
| 65 | Access point tang 13-4 | HAN-F13-SW-02B | Tầng 13 |
| 66 | Access point tang 14-1 | HAN-F13-SW-02A | Tầng 14 |
| 67 | Access point tang 14-2 | HAN-F13-SW-02A | Tầng 14 |

Phương án triển khai: Các thiết bị Access point sẽ được triển khai tại các tầng trong trụ sở KBNN 32 Cát Linh. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.9. Thiết bị điều khiển Access point

8.7.9.1. Sơ đồ thiết kế



8.7.9.2. Thuyết minh giải pháp

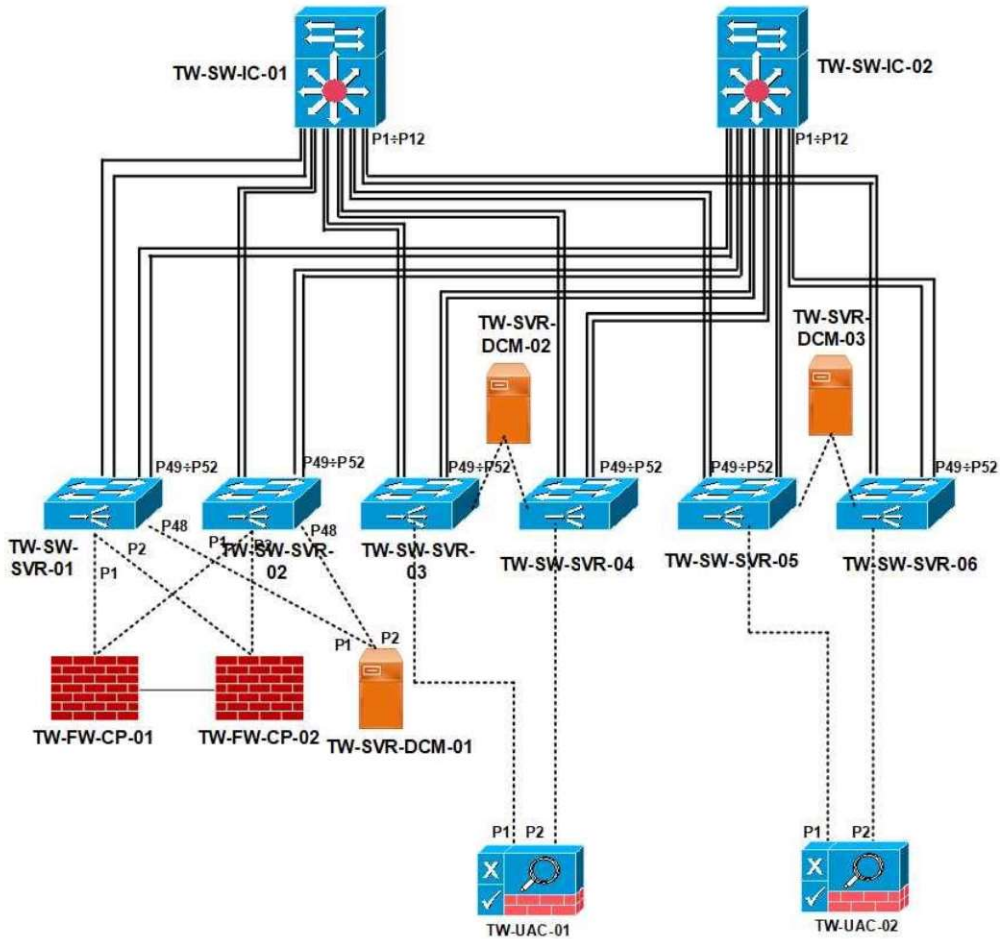
Thiết kế bao gồm 02 thiết bị điều khiển Access point cấu hình dự phòng 1+1. Nếu thiết bị chính ngưng hoạt động thì các Access point sẽ được phân phối lại sang thiết bị Controller còn lại. Chính nhờ khả năng này mà người dùng sẽ không hề nhận ra việc thiết bị trong mạng đang có sự cố do phiên làm việc của người dùng khi chuyển đổi sang thiết bị Controller còn lại không hề bị ngắt. Cập thiết bị điều khiển Access point thay thế cho cặp thiết bị Juniper Networks WLC800.

Mỗi thiết bị điều khiển Access point bao gồm 02 kết nối 10/100/1000 đến 02 thiết bị chuyển mạch vùng quản trị.

Phương án triển khai: 02 thiết bị điều khiển Access point sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.10. Hệ thống điều khiển truy cập mạng

8.7.10.1 Sơ đồ thiết kế



Chú thích:
 TW-FW-CP-0x: Thiết bị Firewall hiện có
 TW-SW-IC-0x: Thiết bị Liên kết chuyển mạch vùng Server
 TW-SW-SVR-0x: Thiết bị Chuyển mạch vùng Server
 TW-SVR-DCM-0x: Thiết bị điều khiển chuyển mạch vùng Server
 TW-UAC-0X: Thiết bị điều khiển truy cập mạng

Px: Port
 ----- Cáp quang, tốc độ 10Gbps
 ————— Cáp quang, tốc độ 100Gbps

8.7.10.2. Thuyết minh giải pháp

Thiết kế bao gồm 01 phần mềm điều khiển truy cập mạng được cài đặt trên 02 thiết bị điều khiển truy cập mạng. Giải pháp kết hợp với các thiết bị chuyển mạch lớp Access, Switch Core, Access Point, thiết bị quản lý mạng người dùng sẽ cung cấp tới người quản trị khả năng điều khiển mọi truy cập của người dùng trong mạng KBNN với bất kỳ phương thức kết nối nào (không dây hoặc có dây). Hệ thống điều khiển truy cập mạng tích hợp thực thi chính sách với thiết bị quản lý mạng người dùng.

Hệ thống điều khiển truy cập mạng chia làm nhiều ngữ cảnh và chính sách như danh tính người sử dụng và điểm cuối, giao thức xác thực (User, MAC address..), danh tính thiết bị và các thuộc tính khác. Giải pháp cung cấp nhiều tùy chọn kiểm soát truy cập, bao gồm danh sách kiểm soát truy cập (ACL), chỉ định VLAN ...

Người dùng trong hệ thống sẽ được chia thành các nhóm cụ thể (VD: Nhóm khách, nhóm Kỹ thuật, nhóm Quản trị, nhóm người dùng nội bộ, nhóm mạng có dây, nhóm mạng không dây, ...). Mỗi nhóm sẽ được định nghĩa với các quyền truy xuất dữ liệu cụ thể (VD: Nhóm khách sẽ chỉ có thể truy cập Internet; nhóm Quản trị có thể truy cập tới mọi thiết bị trong mạng qua Telnet hoặc SSH).

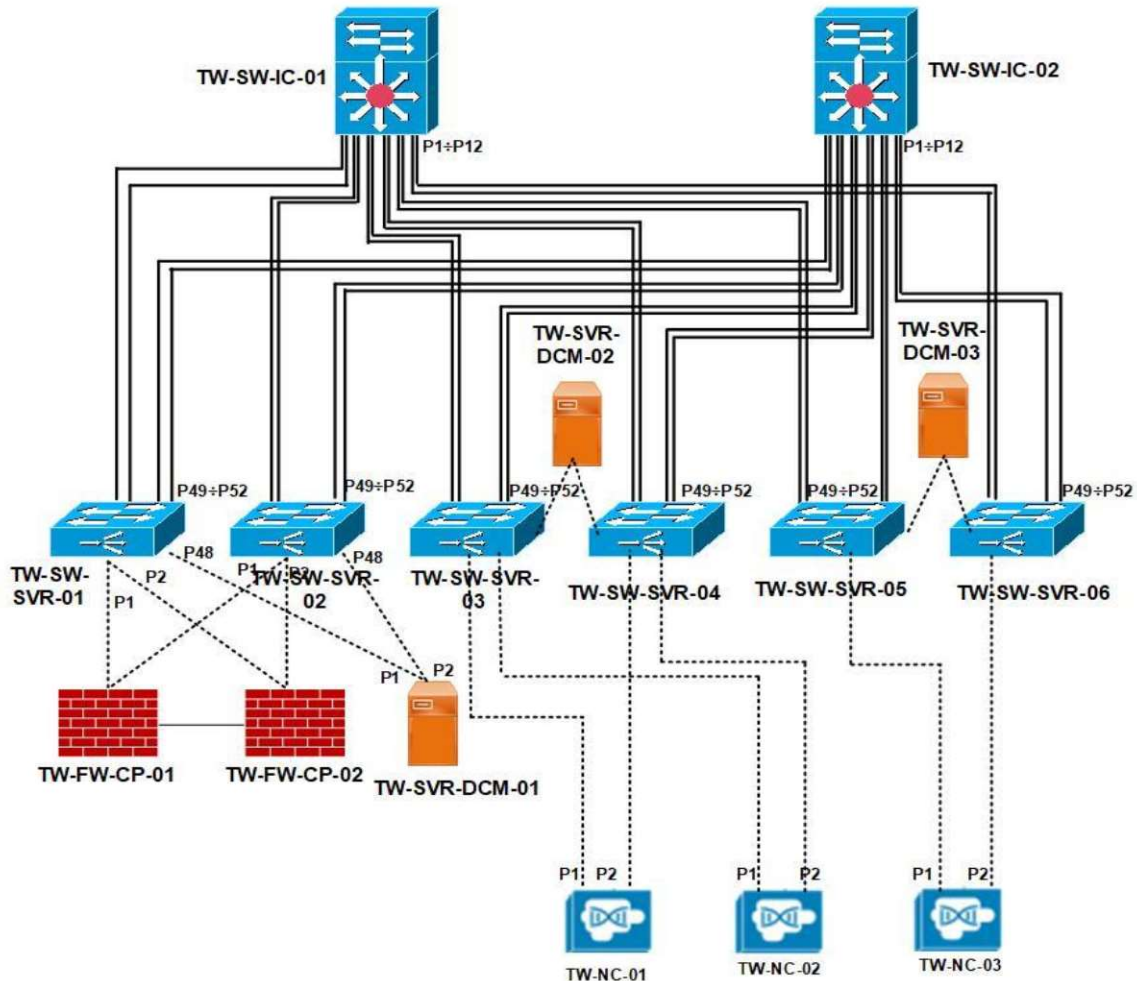
Khi người dùng kết nối vào hệ thống mạng LAN KBNN (qua mạng có dây hoặc không dây), trước khi có thể truy xuất hoặc truy cập tới bất kỳ tài nguyên nào thì người dùng sẽ được xác thực và thiết bị điều khiển truy cập sẽ xác định chính xác các quyền truy cập của người dùng trong hệ thống.

Mỗi thiết bị điều khiển truy cập người dùng sẽ cần 02 kết nối 10 Gbps đến 02 thiết bị chuyển mạch vùng Server.

Phương án triển khai: 02 thiết bị điều khiển truy cập mạng sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.11. Thiết bị quản lý mạng người dùng

8.7.11.1. Sơ đồ thiết kế



Chú thích:

TW-FW-CP-0x: Thiết bị Firewall hiện có
 TW-SW-IC-0x: Thiết bị Liên kết chuyển mạch vùng Server
 TW-SW-SVR-0x: Thiết bị Chuyển mạch vùng Server
 TW-SVR-DCM-0x: Thiết bị điều khiển chuyển mạch vùng Server
 TW-NC-0x: Thiết bị quản lý mạng người dùng

Px: Port

----- Cáp quang, tốc độ 10Gbps

———— Cáp quang, tốc độ 100Gbps

8.7.11.2. Thuyết minh giải pháp

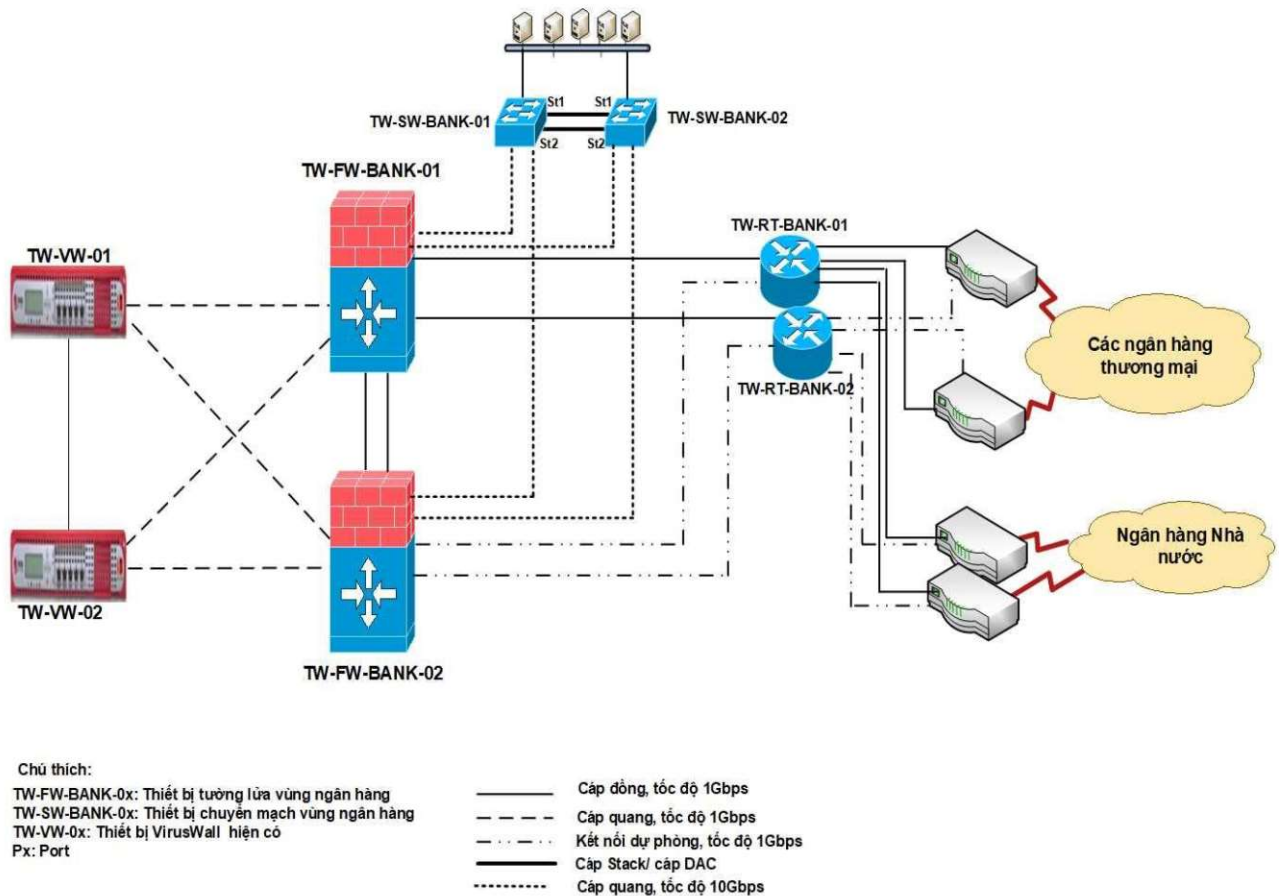
Giải pháp thiết bị quản lý mạng người dùng cung cấp môi trường quản lý duy nhất các thiết bị thuộc cấu trúc SD-LAN, theo dõi sức khỏe mạng, quản lý sự cố; cho phép giám sát, quản trị tập trung các thiết bị mạng LAN (có dây và không dây) cho NSD tại cơ quan KBNN giải quyết được bài toán quản trị phân tán trên từng thiết bị chuyển mạch, thiết bị điểm truy cập không dây tại các tầng riêng lẻ. Hệ thống thiết bị quản lý mạng người dùng được trang bị thêm để tích hợp, quản lý cấu trúc SD-LAN, hệ thống bao gồm 03 thiết bị để đảm bảo tính dự phòng.

Mỗi thiết bị quản lý mạng người dùng sẽ cần 02 kết nối 10Gbps quang đến 02 thiết bị chuyển mạch vùng Server.

Phương án triển khai: 03 thiết bị quản lý mạng người dùng sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.12. Thiết bị tường lửa vùng ngân hàng

8.7.12.1. Sơ đồ thiết kế



8.7.12.2. Thuyết minh giải pháp

Thiết kế bao gồm 01 cặp thiết bị tường lửa vùng ngân hàng hoạt động song song, nếu một trong 02 thiết bị gặp sự cố thì thiết bị còn lại sẽ đảm nhiệm tiếp tục vai trò. Cặp thiết bị này bao gồm tính năng Firewall kết hợp với IPS. 02 thiết bị tường lửa vùng ngân hàng được trang bị sẽ thay thế cho 02 thiết bị tường lửa Juniper Network SRX 1400 hiện tại.

Hệ thống tường lửa vùng ngân hàng có chức năng: Kiểm soát thông tin trao đổi giữa các ngân hàng (các Ngân hàng Thương mại, Ngân hàng Nhà nước) với dữ

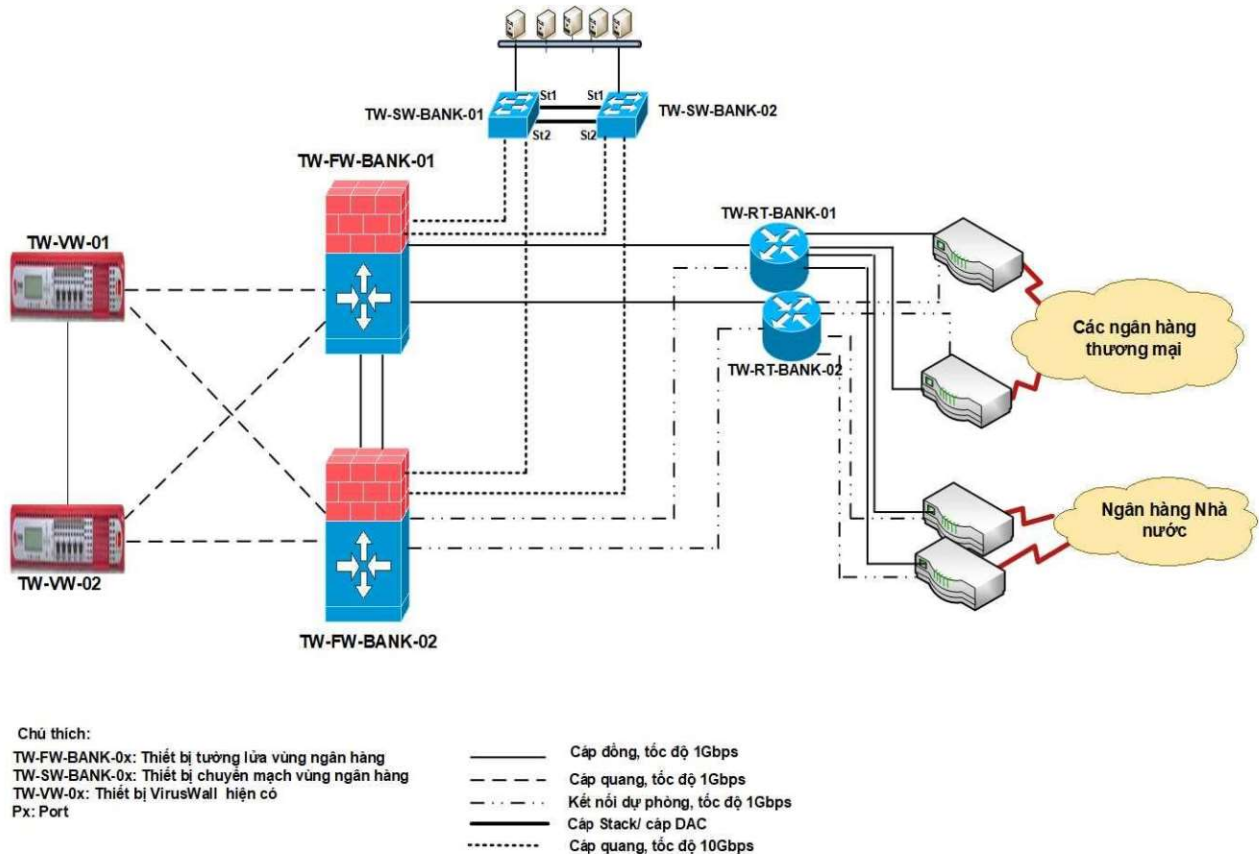
liệu của KBNN, chống lại các cuộc tấn công, xâm nhập trái phép phát sinh từ mạng ngoài (các ngân hàng).

- Mỗi thiết bị tường lửa vùng ngân hàng cần có các kết nối sau:
- + 02 port tốc độ 10Gbps quang kết nối với 02 thiết bị chuyển mạch vùng ngân hàng
- + 02 port tốc độ 1Gbps quang kết nối với 02 thiết bị Antivirus Gateway (VirusWall TippingPoint 2200)
- + 02 port tốc độ 1Gbps đồng kết nối với 02 thiết bị Router kết nối ngân hàng
- + 02 port tốc độ 1Gbps đồng kết nối HA giữa 02 thiết bị tường lửa vùng ngân hàng
- + 02 port tốc độ 1Gbps đồng dự phòng

Phương án triển khai: 02 thiết bị tường lửa vùng ngân hàng sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.13. Thiết bị Router kết nối ngân hàng

8.7.13.1. Sơ đồ thiết kế



8.7.13.2. Thuyết minh giải pháp

Thiết kế bao gồm 02 thiết bị Router kết nối ngân hàng để đảm bảo tính dự phòng, 02 thiết bị Router kết nối ngân hàng được trang bị này sẽ thay thế cho 02 thiết bị Router Juniper SRX 240 hiện tại. 01 thiết bị Router kết nối ngân hàng sẽ chạy chính và 01 thiết bị còn lại sẽ làm dự phòng nóng.

- Mỗi thiết bị Router kết nối ngân hàng cần có các kết nối sau:

- + 02 port tốc độ 1Gbps đồng kết nối kênh truyền sang các Ngân hàng Thương mại (1 kênh chính, 1 kênh dự phòng)

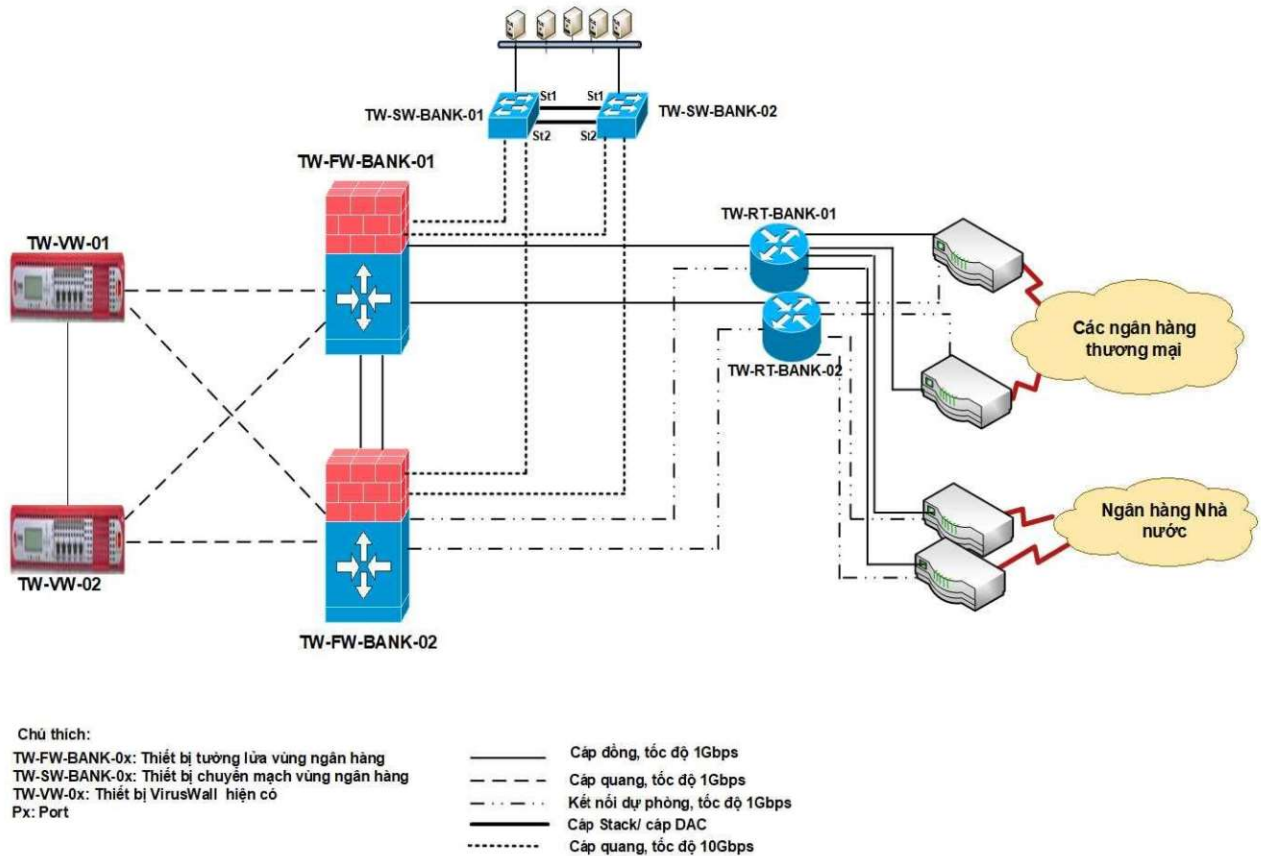
- + 02 port tốc độ 1Gbps đồng kết nối kênh truyền sang Ngân hàng Nhà nước (1 kênh chính, 1 kênh dự phòng)

- + 02 port tốc độ 1Gbps đồng kết nối với 02 thiết bị tường lửa vùng ngân hàng

Phương án triển khai: 02 thiết bị Router kết nối ngân hàng sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.14. Thiết bị chuyển mạch vùng ngân hàng

8.7.14.1. Sơ đồ thiết kế



8.7.14.2. Thuyết minh giải pháp

- Theo thiết kế, cặp thiết bị chuyển mạch vùng ngân hàng được cấu hình ảo hóa 02 thiết bị vật lý thành 01 switch logic (theo công nghệ xếp chồng). Cặp thiết bị sẽ thay thế 01 thiết bị switch SMC hiện có và bổ sung thêm 01 thiết bị switch để đảm bảo tính dự phòng.

- Thiết bị chuyển mạch vùng ngân hàng sẽ kết nối với thiết bị tường lửa vùng ngân hàng thông qua cổng uplink tốc độ 10Gbps quang. Mỗi thiết bị chuyển mạch vùng ngân hàng sẽ cần có các kết nối sau:

+02 kết nối uplink 10Gbps quang phục vụ kết nối tới 02 thiết bị tường lửa vùng ngân hàng

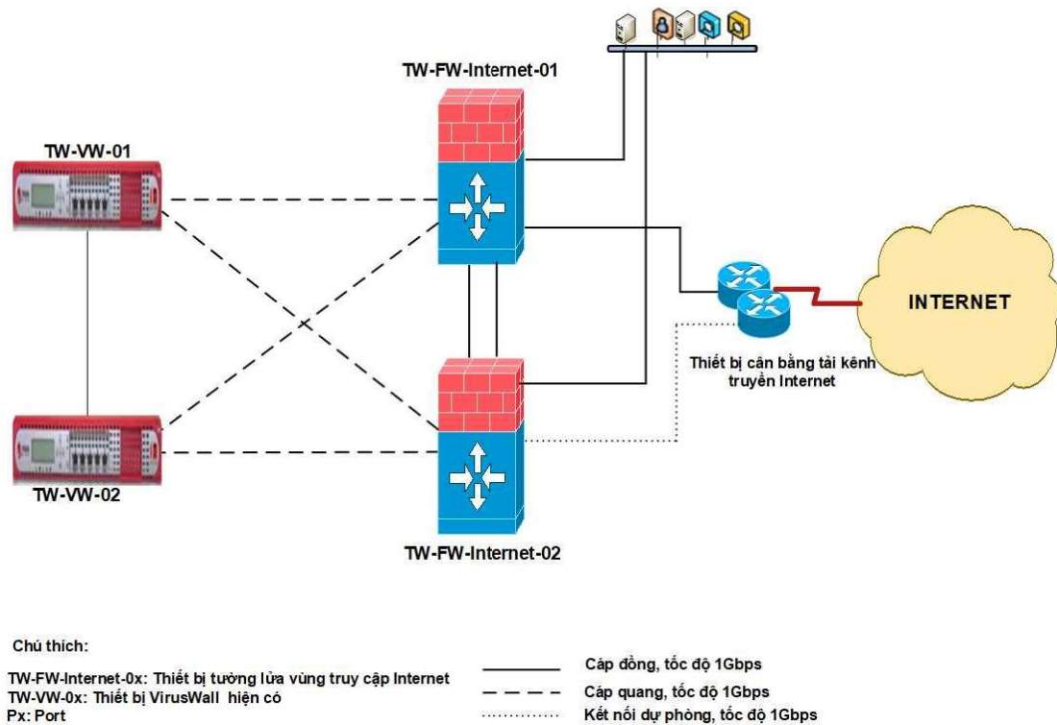
+24 port 1Gbps đồng kết nối với các máy chủ vùng ngân hàng

+02 giao tiếp phục vụ kết nối xếp chồng

Phương án triển khai: 02 thiết bị chuyển mạch vùng ngân hàng sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.15. Thiết bị tường lửa vùng truy cập Internet

8.7.15.1. Sơ đồ thiết kế



8.7.15.2. Thuyết minh giải pháp

- Thiết kế bao gồm 01 cặp thiết bị tường lửa vùng truy cập Internet hoạt động song song, nếu một trong 02 thiết bị gặp sự cố thì thiết bị còn lại sẽ đảm nhiệm tiếp tục vai trò. Cặp thiết bị này bao gồm tính năng Firewall kết hợp với IPS. 02 thiết bị tường lửa vùng truy cập Internet được trang bị sẽ thay thế cho 02 thiết bị tường lửa Juniper Network SRX 1400 hiện tại.

- Hệ thống tường lửa vùng truy cập Internet có chức năng: Kiểm soát truy cập của người sử dụng trong mạng LAN KBNN kết nối Internet. Thiết bị tường lửa có chức năng rà soát mọi dữ liệu vào/ra hệ thống qua đường Internet ADSL, có khả năng chống lại các cuộc tấn công, xâm nhập trái phép phát sinh từ Internet

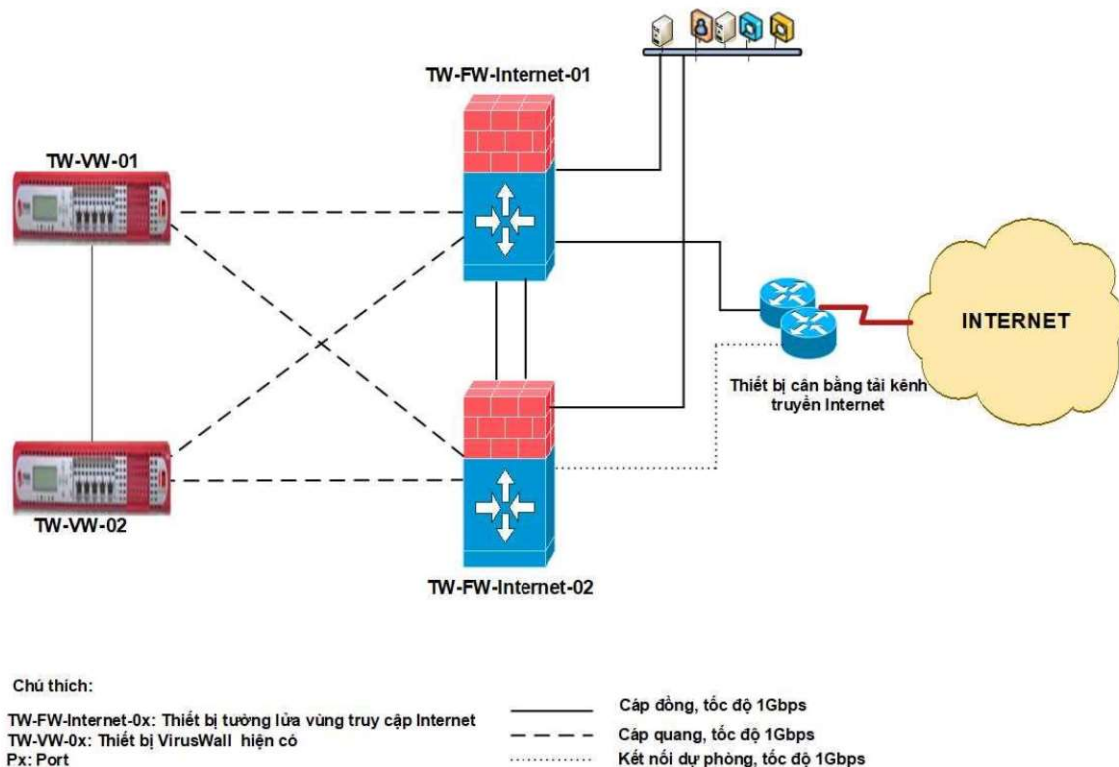
- Mỗi thiết bị tường lửa vùng truy cập Internet cần có các giao tiếp sau:

- + 02 port tốc độ 1Gbps quang kết nối với 02 thiết bị Antivirus Gateway (VirusWall TippingPoint 2200)
- + 01 port đồng tốc độ 1 GE kết nối với thiết bị cân bằng tải kênh truyền Internet
- + 01 port đồng tốc độ 1GE kết nối thiết bị Symantec WSG
- + 02 port đồng tốc độ 1GE kết nối HA giữa 02 thiết bị tường lửa vùng truy cập Internet

Phương án triển khai: 02 thiết bị tường lửa vùng truy cập Internet sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.16. Thiết bị cân bằng tải kênh truyền Internet

8.7.16.1. Sơ đồ thiết kế



8.7.16.2. Thuyết minh giải pháp

- Giải pháp thiết bị cân bằng tải kênh truyền Internet có chức năng cân bằng tải WAN, thiết bị phân phối lưu lượng giữa tất cả các WAN đang hoạt động và xác định trọng số cân bằng tải dựa trên việc sử dụng băng thông của mỗi giao diện. Thiết bị cho phép chạy đồng thời nhiều đường truyền Internet cùng lúc và cộng gộp băng thông các đường truyền. Thiết bị có khả năng kiểm soát và quản lý băng thông giúp

tối ưu hóa đường truyền Internet. Hệ thống cân bằng tải kênh truyền Internet bao gồm 02 thiết bị cân bằng tải kênh truyền Internet để đảm bảo tính dự phòng, 02 thiết bị này sẽ thay thế cho 02 thiết bị Draytek Vigor3900. 01 thiết bị cân bằng tải kênh truyền sẽ chạy chính, 01 thiết bị còn lại làm dự phòng nóng.

- Mỗi thiết bị cân bằng tải kênh truyền Internet cần có các giao tiếp sau:

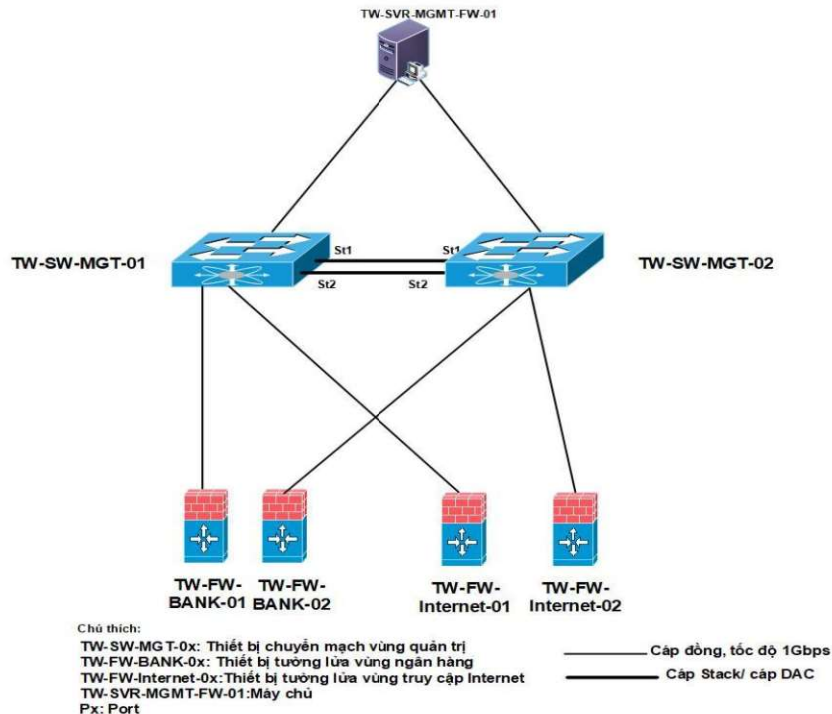
+ 01 port 1GE LAN kết nối với 01 thiết bị tường lửa vùng truy cập Internet

+ 03 port 1GE WAN port kết nối với các kênh truyền Internet

Phương án triển khai: 02 thiết bị cân bằng tải kênh truyền Internet sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.17. Máy chủ

8.7.17.1. Sơ đồ thiết kế



8.7.17.2. Thuyết minh giải pháp

Giải pháp máy chủ có chức năng cài đặt phần mềm quản trị thiết bị tường lửa để quản trị tập trung 02 thiết bị tường lửa vùng ngân hàng và 02 thiết bị tường lửa vùng Internet.

Với thiết kế ở trên, yêu cầu máy chủ cần có 02 kết nối 1Gbps đồng kết nối với 02 thiết bị chuyển mạch vùng quản trị để đảm bảo tính dự phòng.

Phương án triển khai: Máy chủ sẽ được triển khai tại Trung tâm dữ liệu KBNN. Việc thay thế thiết bị sẽ được tiến hành vào thời điểm thích hợp nhằm không ảnh hưởng tới hoạt động nghiệp vụ của KBNN.

8.7.18. Giải pháp an toàn thông tin, cấp điện, chống sét

8.7.18.1. Giải pháp về an toàn thông tin

- Việc thi công lắp đặt, cài đặt phải đảm bảo tính bí mật: thông tin không bị tiết lộ cho những người không có thẩm quyền.

- Việc thi công lắp đặt, cài đặt phải đảm bảo tính thống nhất, toàn vẹn: thông tin không bị thay đổi hay phá hủy.

Việc thi công phải đảm bảo tuân thủ theo phương án đảm bảo an toàn hệ thống thông tin theo cấp độ được phê duyệt.

8.7.18.2. Giải pháp về nguồn cấp điện

Giải pháp về nguồn cấp điện được nêu chi tiết theo mục: “8.5.3. An toàn điện, an toàn thiết bị”

8.12. Phương án bảo đảm an toàn thông tin dự án

KBNN đã có Quyết định số 4408/QĐ-KBNN ngày 29/8/2019 phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của cơ quan Kho bạc Nhà nước, đây là hệ thống mạng nội bộ cơ quan Kho bạc Nhà nước đang vận hành tại KBNN.

Theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 về đảm bảo an toàn hệ thống thông tin theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP, với hệ thống mạng LAN cơ quan Kho bạc Nhà nước đang được thiết kế theo Báo cáo kinh tế - kỹ thuật này, Hội đồng thẩm định hồ sơ đề xuất cấp độ đối với các hệ thống thông tin về hạ tầng của Kho bạc Nhà nước đã có ý kiến thẩm định hồ sơ đề xuất cấp độ “Hệ thống mạng LAN cơ quan Kho bạc Nhà nước” ngày 26/8/2025 và Ban Công nghệ thông tin và Chuyển đổi số có Tờ trình số 249/TTr-CNTT ngày 26/8/2025 về việc phê duyệt hồ sơ đề xuất cấp độ “Hệ thống mạng LAN cơ quan Kho bạc Nhà nước”, trong đó, các nội dung cơ bản sau:

- Sự phù hợp về việc đề xuất cấp độ: cấp độ an toàn thông tin là cấp độ 3
- Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong thiết kế: Phương án đảm bảo an toàn hệ thống thông tin phù hợp với thiết kế trong Báo cáo kinh tế - kỹ thuật của dự án
- Sự phù hợp của phương án bảo đảm an toàn hệ thống thông tin trong quá trình vận hành hệ thống theo cấp độ tương ứng: Phương án đảm bảo an toàn hệ thống thông tin trong tài liệu thuyết minh hồ sơ đề xuất cấp độ đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-BTTTT, phù hợp với hiện trạng hệ thống CNTT của Kho bạc Nhà nước và phù hợp với quá trình vận hành hệ thống theo cấp độ 3.