BỘ THÔNG TIN VÀ TRUYỀN THÔNG	**CỘNG HOÀ XÃ H[illegible]Ủ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 273 /BTTTT - CBĐTW V/v hướng dẫn mô hình tham chiếu về kết nối mạng cho bộ, ngành, địa phương	*Hà Nội, ngày 31 tháng 01 năm 2020*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Uỷ ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17/02/2017 của Chính phủ về việc Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Nghị quyết số 17/NQ-CP ngày 07/3/2019 của Chính phủ về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019-2020, định hướng đến 2025;

Căn cứ Quyết định số 1739/QĐ-BTTTT ngày 18/10/2019 của Bộ Thông tin và Truyền thông về việc phê duyệt kế hoạch tổ chức triển khai thực hiện các nhiệm vụ phát triển Chính phủ điện tử đến năm 2020,

Bộ Thông tin và Truyền thông hướng dẫn mô hình tham chiếu về kết nối mạng cho bộ, ngành, địa phương. Toàn văn văn bản hướng dẫn được đăng tải trên Cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: https://www.mic.gov.vn.

Đề nghị Quý cơ quan nghiên cứu, tổ chức triển khai tại cơ quan, đơn vị mình.

Trong quá trình thực hiện, nếu có điều gì vướng mắc, đề nghị Quý Cơ quan phản ánh về Bộ Thông tin và Truyền thông, qua Cục Bưu điện Trung ương để được hướng dẫn giải quyết./.

Nơi nhận:
- Như trên;
- Thủ tướng Chính phủ (để b/c);
- Phó Thủ tướng Vũ Đức Đam (để b/c);
- Bộ trưởng và các Thứ trưởng;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở TTTT các tỉnh, TP trực thuộc TW;
- Các Doanh nghiệp Viễn thông;
- Lưu: VT, CBĐTW, VNNIC.

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

TÀI LIỆU HƯỚNG DẪN MÔ HÌNH THAM CHIẾU VỀ KẾT NỐI MẠNG CỦA BỘ, NGÀNH, ĐỊA PHƯƠNG

(Kèm theo Công văn số 273 /BTTTT-CBĐTW ngày 31 tháng 01 năm 2020 của Bộ Thông tin và Truyền thông)

I. Phạm vi và đối tượng áp dụng

1. Phạm vi áp dụng

Tài liệu này hướng dẫn về các mô hình tham chiếu kết nối mạng của bộ, ngành, địa phương vào mạng truyền số liệu chuyên dùng phục vụ cơ quan Đảng, Nhà nước.

2. Đối tượng áp dụng

Các Bộ, cơ quan ngang Bộ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương.

II. Danh mục từ viết tắt:

1. Mạng TSLCD: Mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước.

2. CPĐT: Chính phủ điện tử

3. TTDL: Trung tâm dữ liệu

4. DNVT: Doanh nghiệp viễn thông

5. CQNN: Cơ quan Nhà nước

6. BNĐP: Bộ, ngành, địa phương

7. CBCC: Cán bộ công chức

8. ATTT: An toàn thông tin

9. HTTT: Hệ thống thông tin

10. DNS: Hệ thống phân giải tên miền

11. WAN: Mạng diện rộng

12. LAN: Mạng nội bộ

III. Nguyên tắc chung

1. Mạng TSLCD được sử dụng làm hạ tầng truyền dẫn căn bản trong kết nối các HTTT CPĐT và liên thông, chia sẻ dữ liệu.

2. Kết nối từ người dân, doanh nghiệp vào HTTT của Chính phủ, BNĐP qua hạ tầng mạng công cộng.

3. Hệ thống máy chủ ứng dụng tại phân hệ kết nối mạng TSLCD được phân tách với phân hệ kết nối mạng công cộng.

IV. Các mô hình tham chiếu về kết nối mạng của BNĐP: quy định chi tiết tại Phụ lục kèm theo

1. Mô hình tổng quan

2. Các mô hình tham chiếu mạng BNĐP

2.1. Mô hình kết nối TTDL vào mạng TSLCD

Mô hình 01: kết nối phân vùng TTDL của DNVT phục vụ BNĐP về trụ sở BNĐP.

Mô hình 02: kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD.

Mô hình 03: kết nối TTDL của BNĐP vào mạng TSLCD.

Mô hình 04: kết nối Internet tại TTDL.

2.2. Mô hình 05: kết nối mạng WAN của bộ, ngành vào mạng TSLCD

2.3. Kết nối mạng WAN của địa phương vào mạng TSLCD

Mô hình 06: tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương.

Mô hình 07: chỉ tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương.

Mô hình 08: tập trung lưu lượng WAN về điểm quản lý tập trung của DNVT.

2.4. Mô hình 09: kết nối mạng LAN của đơn vị trực thuộc BNĐP vào mạng TSLCD

2.5. Mô hình hệ thống DNS

Mô hình 10: Hệ thống DNS quản lý tên miền <abc>.gov.vn của BNĐP

Mô hình 11: Hệ thống máy chủ tên miền đệm (DNS Caching)

3. Mô hình mục tiêu

V. Hướng dẫn triển khai

1. Các Bộ, cơ quan ngang Bộ, UBND các tỉnh, thành phố trực thuộc Trung ương

a) Tham khảo các mô hình kết nối mạng tại Phụ lục khi xây dựng, triển khai, quản lý, vận hành hệ thống mạng của BNĐP và kết nối giữa các BNĐP với nhau và với Chính phủ.

b) Chỉ đạo đơn vị phụ trách về công nghệ thông tin phối hợp với các đơn vị thuộc Bộ Thông tin và Truyền thông trong quá trình kết nối mạng diện rộng của BNĐP vào mạng TSLCD.

c) Chủ trì, phối hợp Cục Bưu điện Trung ương trong việc triển khai biện pháp giám sát trạng thái, lưu lượng kết nối đến các đơn vị sử dụng mạng WAN của BNĐP.

2. Bộ Thông tin và Truyền thông

a) Cục Bưu điện Trung ương

- Chủ trì, hướng dẫn mô hình kết nối mạng WAN của BNĐP vào mạng TSLCD.

- Đảm bảo chất lượng đường truyền mạng TSLCD cấp I phục vụ các bài toán CPĐT.

- Quản lý, quy hoạch tài nguyên địa chỉ IP cho các kết nối mạng TSLCD.

- Chủ trì, giám sát trạng thái, lưu lượng kết nối đến các đơn vị sử dụng mạng WAN của BNĐP.

b) Cục An toàn thông tin

- Chủ trì, hướng dẫn về các yêu cầu an toàn cơ bản đối với TTDL của DNVT phục vụ CQNN.

c) Trung tâm Internet Việt Nam (VNNIC)

- Chủ trì, hướng dẫn mô hình kết nối tại phân hệ HTTT kết nối Internet, hệ thống máy chủ tên miền DNS của BNĐP.

- Quản lý, quy hoạch tài nguyên số hiệu mạng AS, địa chỉ IP dùng để kết nối, định tuyến Internet (IP public) cho các BNĐP.

3. Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương

a) Tham mưu cho UBND tỉnh, thành phố mô hình kết nối mạng hiệu quả, đáp ứng các yêu cầu triển khai các bài toán CPĐT của địa phương.

b) Phối hợp với Cục Bưu điện Trung ương, Cục An toàn thông tin, Cục Tin học hóa, VNNIC đánh giá tình hình triển khai mạng WAN tại địa phương, định kỳ hàng năm báo cáo về Bộ Thông tin và Truyền thông (Cục Bưu điện Trung ương).

4. Các doanh nghiệp viễn thông

a) Hỗ trợ Sở Thông tin và Truyền thông trong quá trình triển khai các mô hình kết nối mạng tại các địa phương.

b) Chủ trì, phối hợp Cục Bưu điện Trung ương trong việc triển khai biện pháp giám sát trạng thái, lưu lượng kết nối đến các đơn vị sử dụng mạng WAN của BNĐP.

c) Triển khai điểm quản lý Internet tập trung cho các kết nối Internet của CQNN tại các địa phương.

PHỤ LỤC:
CÁC MÔ HÌNH THAM CHIẾU VỀ KẾT NỐI MẠNG CỦA BỘ, NGÀNH, ĐỊA PHƯƠNG

I. Mô hình tổng quan

Hình vẽ mô hình tổng quan được trình bày tại Hình 1.

Phân hệ TTDL của BNĐP:

- Kết nối mạng: kết nối trực tiếp vào mạng TSLCD qua hạ tầng mạng truyền tải của DNVT hoặc kết nối về trụ sở BNĐP.

- Tổ chức TTDL: phân thành phân vùng HTTT chuyên dùng và HTTT công cộng:

+ HTTT chuyên dùng: kết nối vào mạng TSLCD để đồng bộ CSDL giữa các HTTT chuyên dùng và kết nối từ cán bộ, công chức lên HTTT.

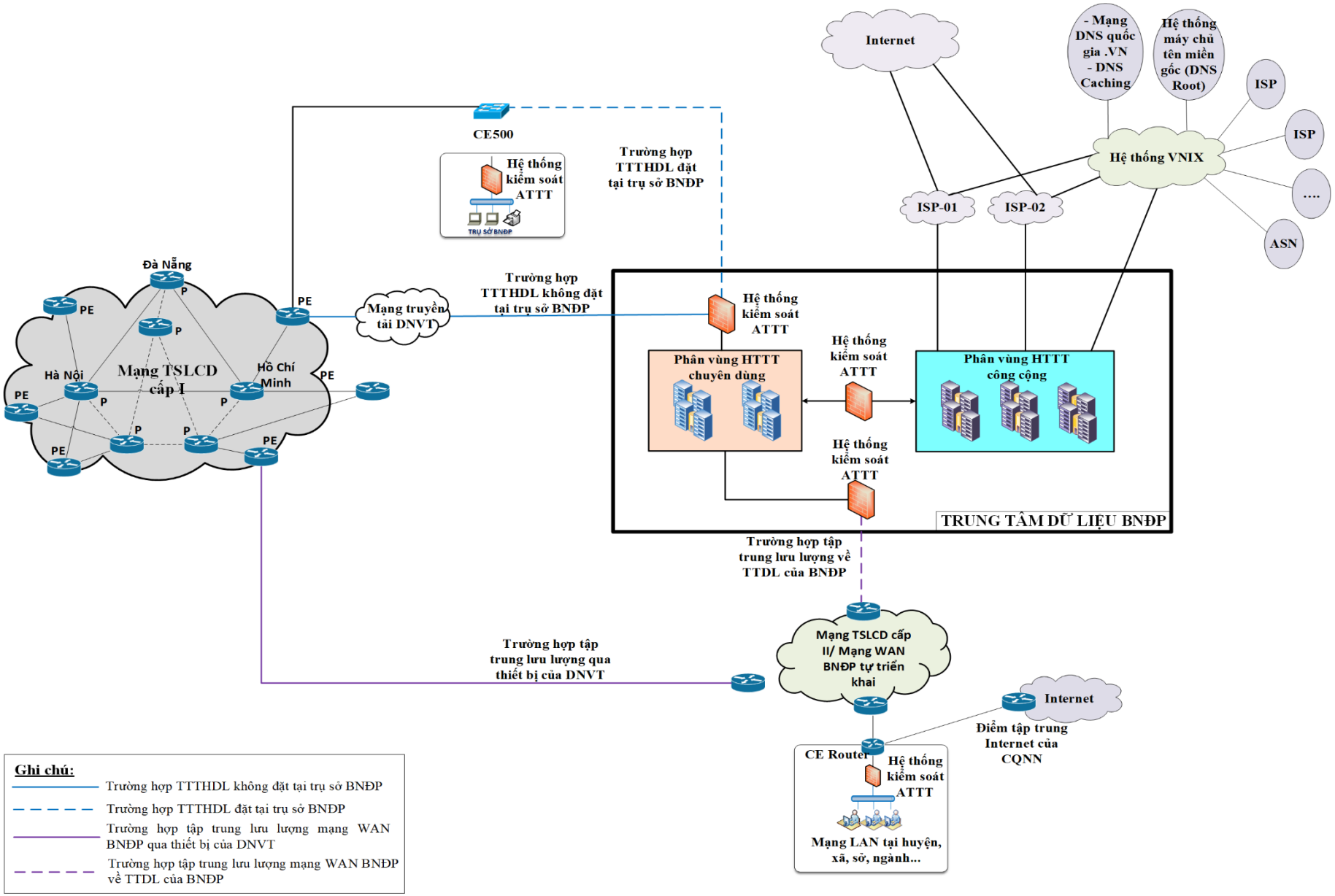
+ HTTT công cộng: kết nối multi-home qua các ISP và VNIX để người dân, doanh nghiệp truy cập vào HTTT.

Phân hệ mạng WAN của BNĐP: kết nối tập trung lưu lượng về TTDL của BNĐP hoặc qua thiết bị tập trung của DNVT.

Phân hệ mạng LAN của đơn vị trực thuộc BNĐP: có 2 kết nối:

- Kết nối mạng TSLCD cấp II hoặc qua kết nối WAN BNĐP tự triển khai.

- Kết nối Internet qua điểm tập trung Internet của CQNN tại DNVT hoặc tập trung tại TTDL của BNĐP.

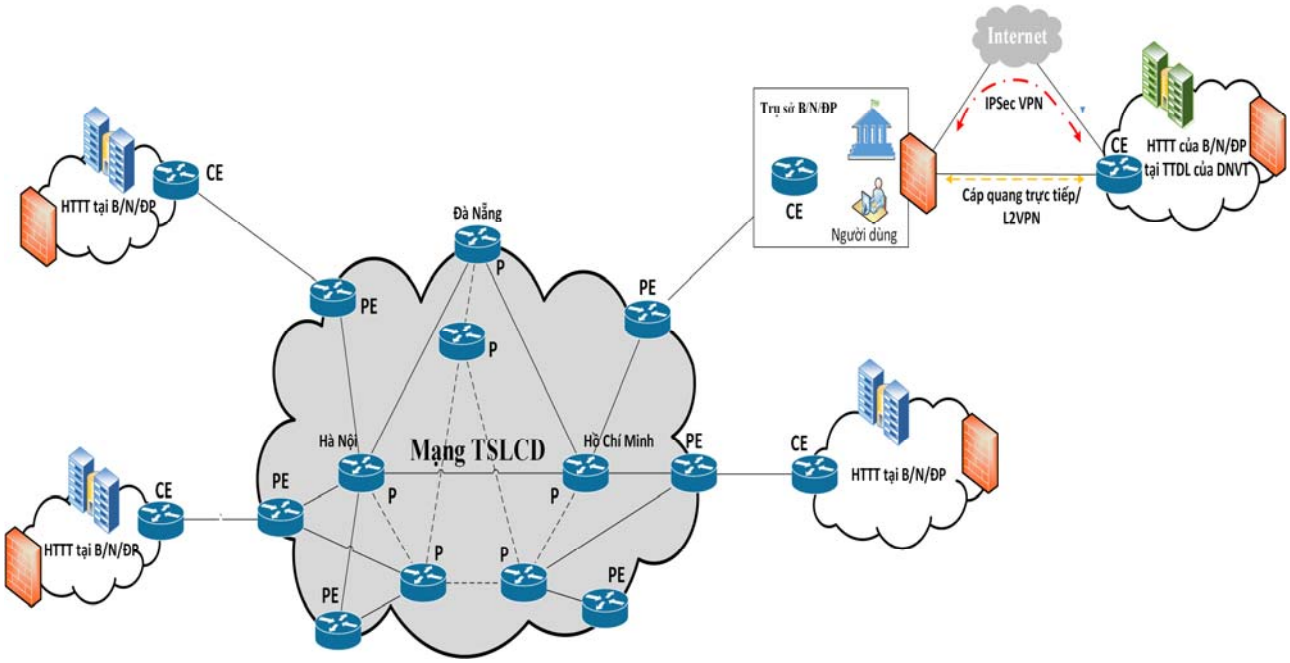


Hình 1. Mô hình tổng quan kết nối mạng LAN, WAN, Trung tâm dữ liệu

II. Các mô hình tham chiếu kết nối mạng BNĐP

2.1. Mô hình kết nối TTDL vào mạng TSLCD

2.1.1. Mô hình 01: kết nối phân vùng TTDL của DNVT phục vụ BNĐP về trụ sở BNĐP



Hình 2. Kết nối phân vùng TTDL của DNVT phục vụ BNĐP về trụ sở BNĐP

Mô hình kết nối phân vùng TTDL của DNVT phục vụ BNĐP về trụ sở BNĐP là mô hình sử dụng trong trường hợp TTDL của DNVT chưa đủ điều kiện kết nối trực tiếp vào mạng TSLCD.

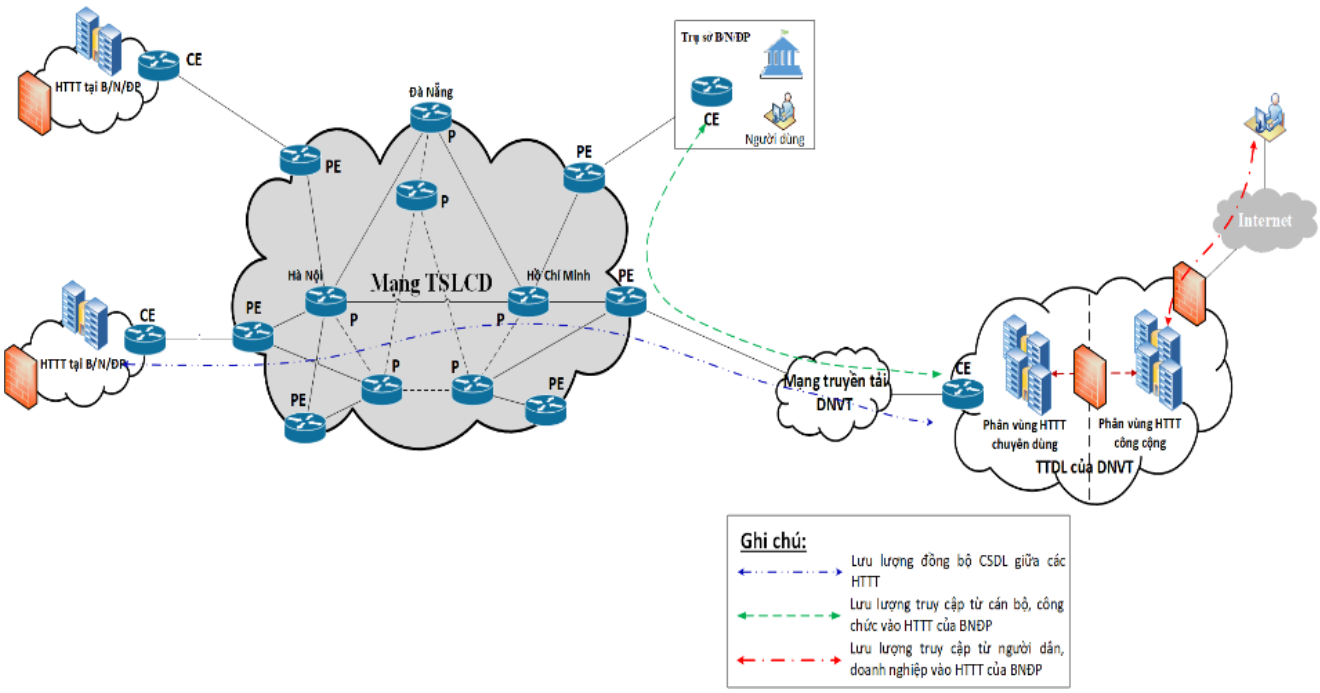
Để triển khai mô hình này, DNVT cần triển khai kênh kết nối bằng cáp quang trực tiếp, qua thiết lập kênh L2/L3VPN qua hạ tầng mạng của DNVT hoặc kênh IPSec VPN qua Internet từ TTDL của DNVT về trụ sở BNĐP.

Các yêu cầu cơ bản:

- BNĐP cần đáp ứng các quy định tại Điều 6 Thông tư số 27/2017TT-BTTTT ngày 20/10/2019 về quản lý, vận hành, kết nối, sử dụng và bảo đảm ATTT trên mạng TSLCD và Phụ lục 1 Thông tư số 12/2019/TT-BTTTT ngày 5/11/2019 về sửa đổi, bổ sung một số điều của Thông tư số 27/2017TT-BTTTT ngày 20/10/2019 về quản lý, vận hành, kết nối, sử dụng và bảo đảm ATTT trên mạng TSLCD.

- BNĐP chịu trách nhiệm các vấn đề liên quan đến an toàn bảo mật khi kết nối vào mạng TSLCD.

2.1.2. Mô hình 02: kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD



Hình 3. Kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD

Mô hình kết nối trực tiếp phân vùng TTDL của DNVT phục vụ BNĐP vào mạng TSLCD là mô hình sử dụng trong trường hợp TTDL của DNVT đủ điều kiện kết nối trực tiếp vào mạng TSLCD.

Để triển khai mô hình này, DNVT cần triển khai kênh kết nối bằng cáp quang trực tiếp vào mạng TSLCD cấp I hoặc qua kết nối trung kế với mạng TSLCD cấp I của Cục BĐTW.

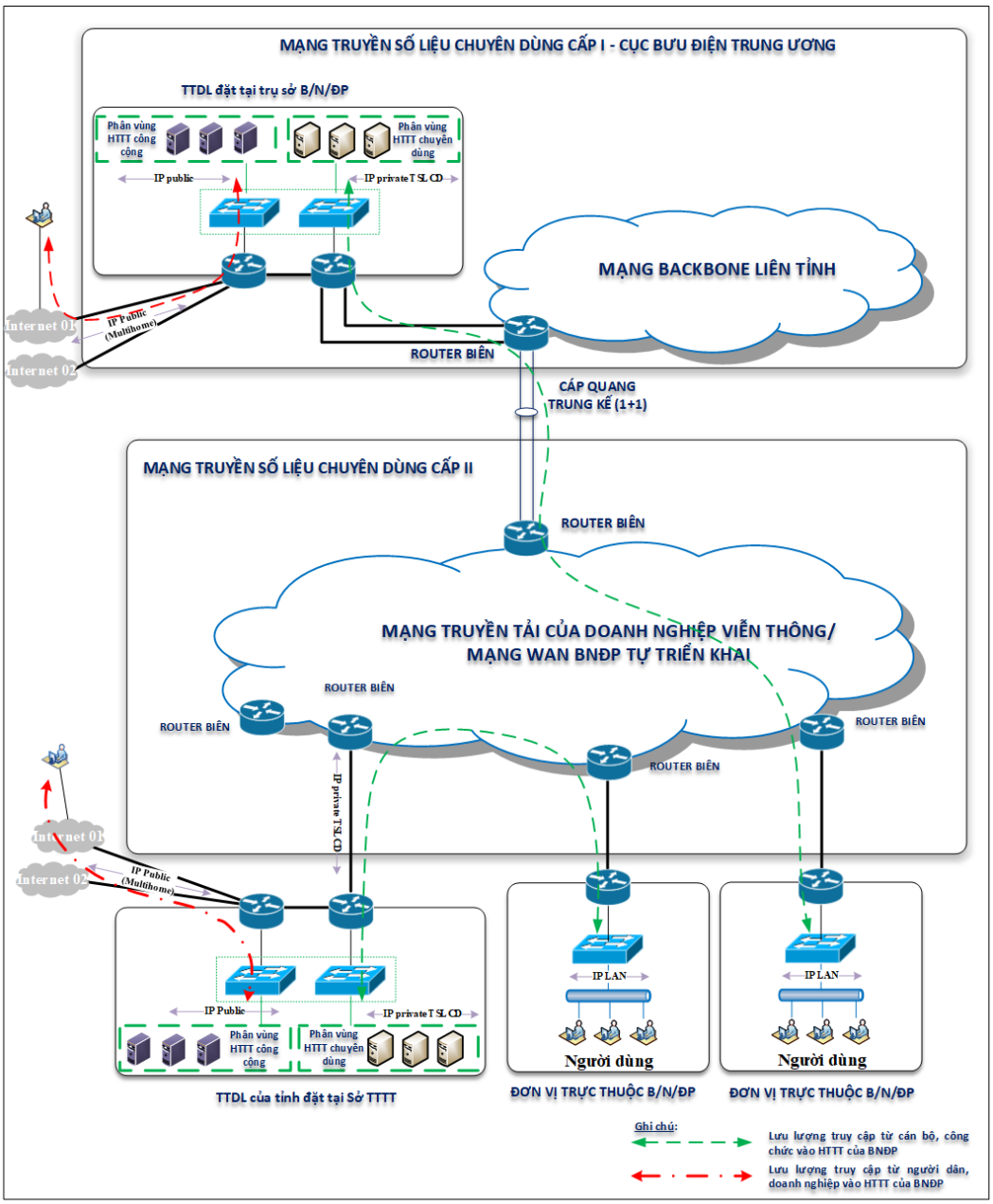
Các yêu cầu cơ bản:

- TTDL của DNVT cần đáp ứng các quy định về TTDL phục vụ BNĐP.

- DNVT cần phân tách khu vực riêng tại TTDL phục vụ BNĐP với khu vực tại TTDL phục vụ mục đích thương mại cho người dân, tổ chức, doanh nghiệp.

- Tại khu vực TTDL phục vụ BNĐP: cần phân tách phân vùng HTTT chuyên dùng và phân vùng HTTT công cộng.

2.1.3. Mô hình 03: kết nối TTDL của BNĐP vào mạng TSLCD



Hình 4. Kết nối TTDL của BNĐP vào mạng TSLCD

Mô hình kết nối TTDL của BNĐP vào mạng TSLCD là mô hình sử dụng trong trường hợp các BNĐP có TTDL riêng đặt tại trụ sở của BNĐP. Kết nối từ TTDL của BNĐP vào mạng TSLCD sử dụng kênh truyền mạng TSLCD sẵn có của BNĐP.

Các yêu cầu cơ bản:

- BNĐP cần phân tách phân vùng HTTT chuyên dùng và phân vùng HTTT công cộng.

- Đối với phân vùng HTTT chuyên dùng:

+ Kết nối vào mạng TSLCD sử dụng IP private do Cục BĐTW quy hoạch (Trong trường hợp bị trùng IP thì có phương án phối hợp xử lý đối với BNĐP).

+ Phân vùng HTTT chuyên dùng để đồng bộ cơ sở dữ liệu với HTTT của Chính phủ, BNĐP khác và kết nối từ cán bộ, công chức đến HTTT chuyên dùng.

- Đối với phân vùng HTTT công cộng:

+ Phân vùng HTTT công cộng phục vụ người dân, tổ chức, doanh nghiệp truy cập đến HTTT công cộng.

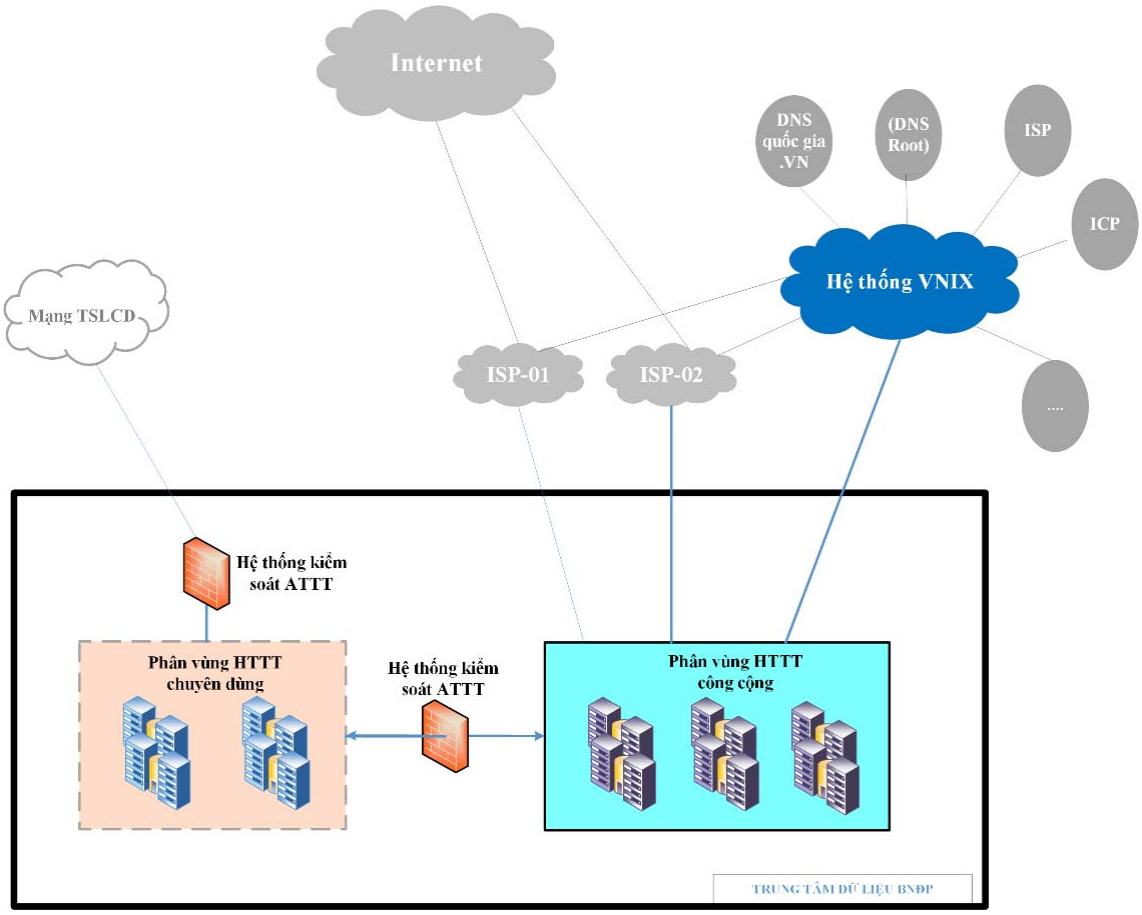
+ Sử dụng AS/IP độc lập do VNNIC cấp, kết nối Internet theo cơ chế multi-home tới một hoặc nhiều ISP, kết nối vào VNIX.

(Chi tiết xem mô hình, hướng dẫn tại mục số 2.1.4 dưới đây)

2.1.4. Mô hình 04: kết nối Internet tại TTDL

a) Mô hình kết nối Internet của TTDL

Phân hệ Internet của TTDL quy hoạch cung cấp các dịch vụ chung cho các hoạt động của BNĐP, bao gồm các ứng dụng, cổng thông tin BNĐP, các dịch vụ web khác, cơ sở dữ liệu, các hệ thống thông tin dùng chung như DNS, thư điện tử (email)…



Hình 5. Kết nối Internet tại TTDL

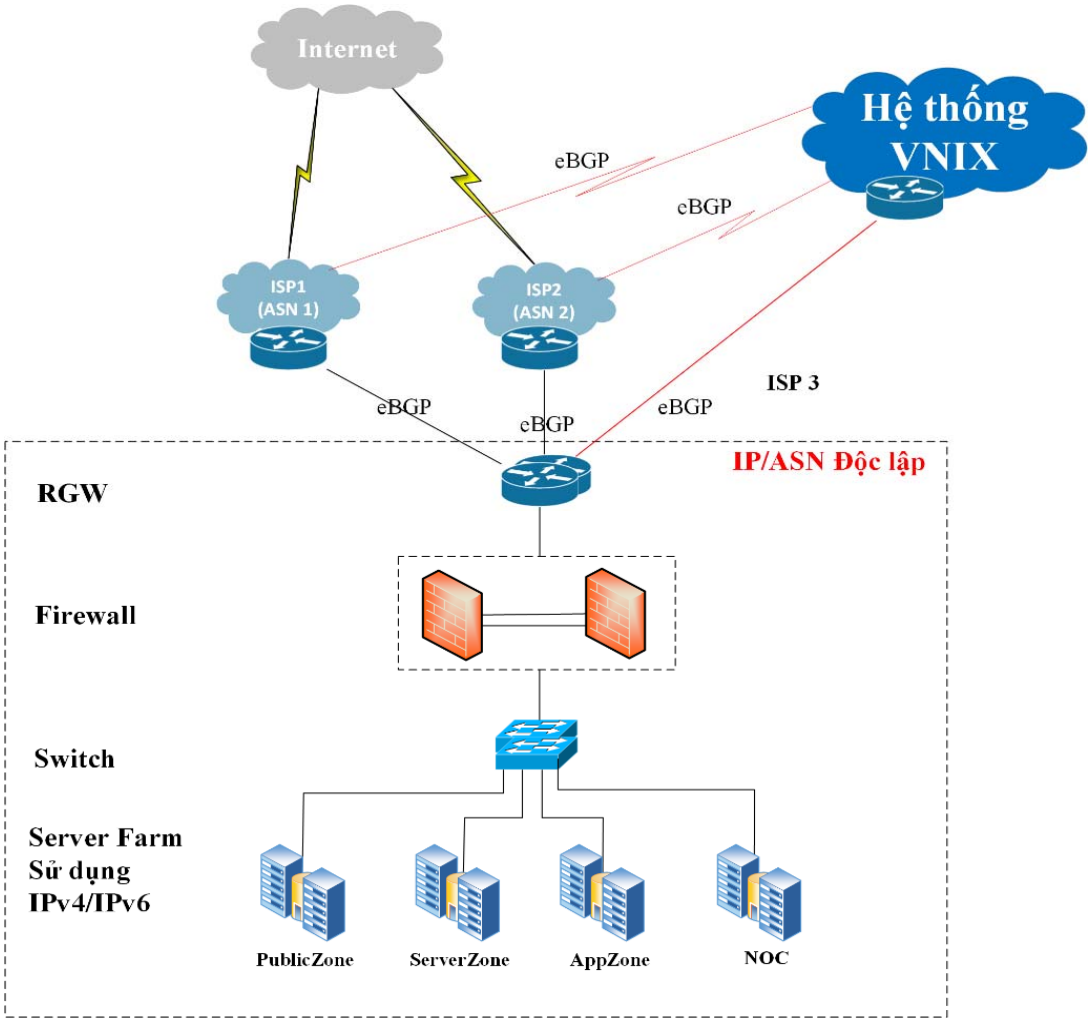
Phân hệ Internet cần được quy hoạch theo kiến trúc của một mạng độc lập, kết nối đa hướng (multi-home), từng bước chuyển đổi IPv6:

- Mạng độc lập: là mạng sử dụng vùng địa chỉ IP mạng Public và số hiệu mạng ASN độc lập. Tại Việt Nam địa chỉ IP và ASN được quản lý cấp phát bởi Trung tâm Internet Việt Nam (VNNIC), Bộ Thông tin và Truyền thông (Tham khảo quy trình đăng ký tại https://vnnic.vn/diachiip).

- Kết nối đa hướng (multi-home): một hệ thống mạng độc lập sẽ có khả năng kết nối nhiều hướng (peering hoặc transit) với các mạng độc lập khác, với các DNVT (ISP) khác để kết nối vào mạng Internet, khi có sự cố hướng này sẽ tự động chạy theo hướng khác và ngược lại mà không bị gián đoạn dịch vụ, đồng thời có thể linh hoạt trong điều hướng để sử dụng hiệu quả băng thông kết nối trên các kênh truyền theo nhu cầu.

- Chuyển đổi IPv6: Quy hoạch mạng đảm bảo hoạt động song song IPv4, IPv6, có lộ trình từng bước chuyển đổi từ IPv4 sang IPv6, tiến tới dừng sử dụng IPv4.

b) Giải pháp kết nối đa hướng với ISP và Trạm trung chuyển Internet quốc gia VNIX



Hình 6. Kết nối đa hướng với ISP và VNIX

Hệ thống mạng TTDL kết nối Internet cần được thiết kế theo mô hình phân tầng, bao gồm các khối như sau :

- Tầng định tuyến: khối Router Gateway kết nối định tuyến đa hướng cho toàn bộ hệ thống mạng với các ISP, trạm trung chuyển Internet quốc gia VNIX.

- Tầng an toàn an ninh: khối Firewall/IPS đảm bảo an toàn tổng thể cho hệ thống mạng, bảo vệ hệ thống mạng và các phân vùng quản lý phía trong mạng.

- Tầng chuyển mạch: khối Hệ thống chuyển mạch (Switch) kết nối giữa các tầng, các phân vùng quản lý và các hệ thống thiết bị máy chủ.

- Tầng máy chủ: khối Server farm là các máy chủ, ứng dụng, thiết bị lưu trữ, sao lưu…

Các phương án để kết nối Internet TTDL như sau:

- Phương án kết nối Internet qua các DNVT (ISP): phân hệ Internet của TTDL kết nối (peering, transit) với một hoặc hoặc nhiều các ISP để trao đổi lưu lượng hoặc transit đi Internet theo nhu cầu.

- Phương án đấu nối VNIX[1]: Hệ thống trạm trung chuyển Internet quốc gia VNIX được quản lý bởi Trung tâm Internet Việt nam (VNNIC), hiện tại được triển khai tại 3 điểm Hà Nội, Đà Nẵng và Tp. Hồ Chí Minh. VNIX cho phép các mạng cơ quan, tổ chức, doanh nghiệp sử dụng số hiệu mạng ASN và địa chỉ IP độc lập do VNNIC cấp phát kết nối đến để trao đổi lưu lượng Internet. Đối với phân hệ Internet của TTDL có thể kết nối VNIX theo 2 mô hình như sau:

+ Kết nối đa phương MLPA để trao đổi lưu lượng Internet trong nước: Với mô hình này khi kết nối với VNIX phân hệ Internet của TTDL chỉ cần thiết lập một kênh kết nối vật lý, cấu hình định tuyến eBGP ngang hàng (peering) với thiết bị quản lý định tuyến (route server) của VNIX là có thể kết nối trao đổi lưu lượng trực tiếp với tất cả các thành viên khác, hiện có 21 thành viên là các ISP, ICP, IDC, mạng của cơ quan nhà nước, chính phủ, mạng DNS quốc gia, DNS ROOT … đang kết nối VNIX.

+ Kết nối song phương BLPA: Trên cơ sở kênh kết nối vật lý tới VNIX, ngoài việc kết nối đa phương MLPA như trên thì BNĐP có thể thỏa thuận kết nối song phương BLPA với các thành viên khác hiện có tại VNIX để trao đổi lưu lượng riêng hoặc transit qua mạng khác. Có thể thoả thuận với các ISP đang kết nối vào VNIX để transit lưu lượng Internet quốc tế ngay tại VNIX thay vì phải thuê thêm kênh vật lý đến ISP.

[1] https://vnnic.vn/vnix

Có thể kết hợp hai phương án kết nối trên (qua ISP và VNIX) đảm bảo tính sẵn sàng cho hệ thống, tiết kiệm chi phí đường truyền và tăng chất lượng kết nối dịch vụ cho hệ thống phân mạng kết nối Internet cho các tổ chức BNĐP.

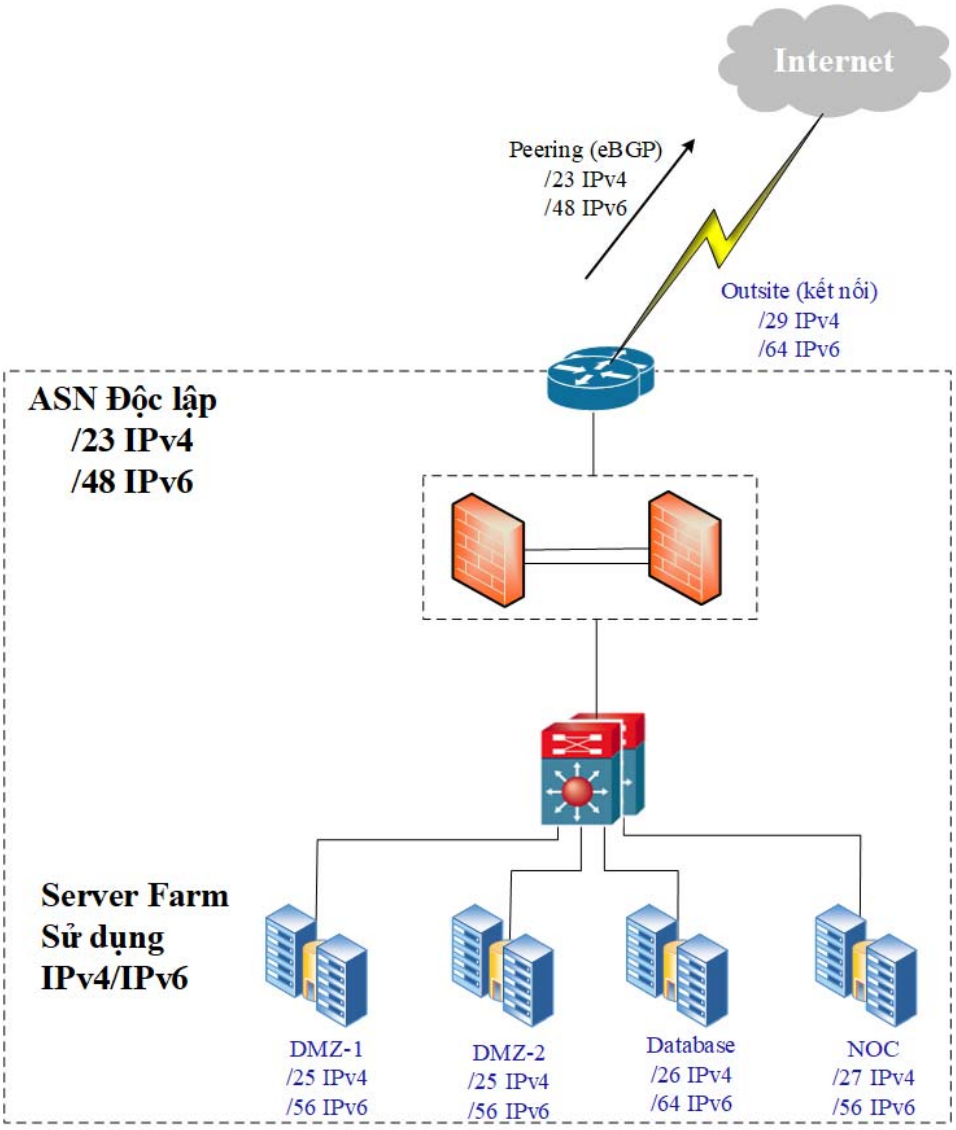
c) Quy hoạch địa chỉ IP (IPv4/IPv6):

Hệ thống mạng BNĐP cần phải phân vùng với mục đích, mức độ an toàn khác nhau để quản lý; và quy hoạch địa chỉ IP cho toàn bộ hạ tầng CNTT đảm bảo hiệu quả, liên tục, tránh bị phân mảnh, đáp ứng nhu cầu sử dụng trong từng khối và đảm bảo khả năng mở rộng trong tương lai mà không cần quy hoạch, thay đổi lại địa chỉ và chính sách định tuyến.

Sử dụng địa chỉ IPv4, IPv6 và số hiệu mạng độc lập (ASN) do VNNIC cấp để quy hoạch, phân bổ trong phân hệ Internet của TTDL, không dùng địa chỉ IP private kết hợp với NAT để cung cấp các dịch vụ ra Internet. BNĐP sẽ đăng ký với VNNIC 01 số hiệu mạng, 01 vùng địa chỉ IPv4 (2^16 = 512 địa chỉ) và 01 vùng địa chỉ IPv6 /32 hoặc /48 (tương đương với 2^32 địa chỉ hoặc 2^48 địa chỉ). Từ đó có thể chia thành các vùng địa chỉ nhỏ hơn tuỳ theo nhu cầu, ví dụ như sau (tham khảo trên website của VNNIC[2]):

- Các phân vùng mạng cho các ứng dụng kết nối trực tiếp Internet: DMZ-1, DMZ-2: /25 địa chỉ IPv4 (2^7 = 128 địa chỉ), /56 địa chỉ IPv6
- Các phân vùng CSDL, Middleware: /26 địa chỉ IPv4 (2^6=64 địa chỉ), /64 địa chỉ IPv6.
- Phân vùng NOC/SOC: /27 địa chỉ IPv4, /64 địa chỉ IPv6.
- Phân vùng kết nối bên ngoài tới các ISP: /29 địa chỉ IPv4, /64 địa chỉ IPv6.
- Dự phòng địa chỉ cho các phân vùng có thể phát sinh trong tương lai.

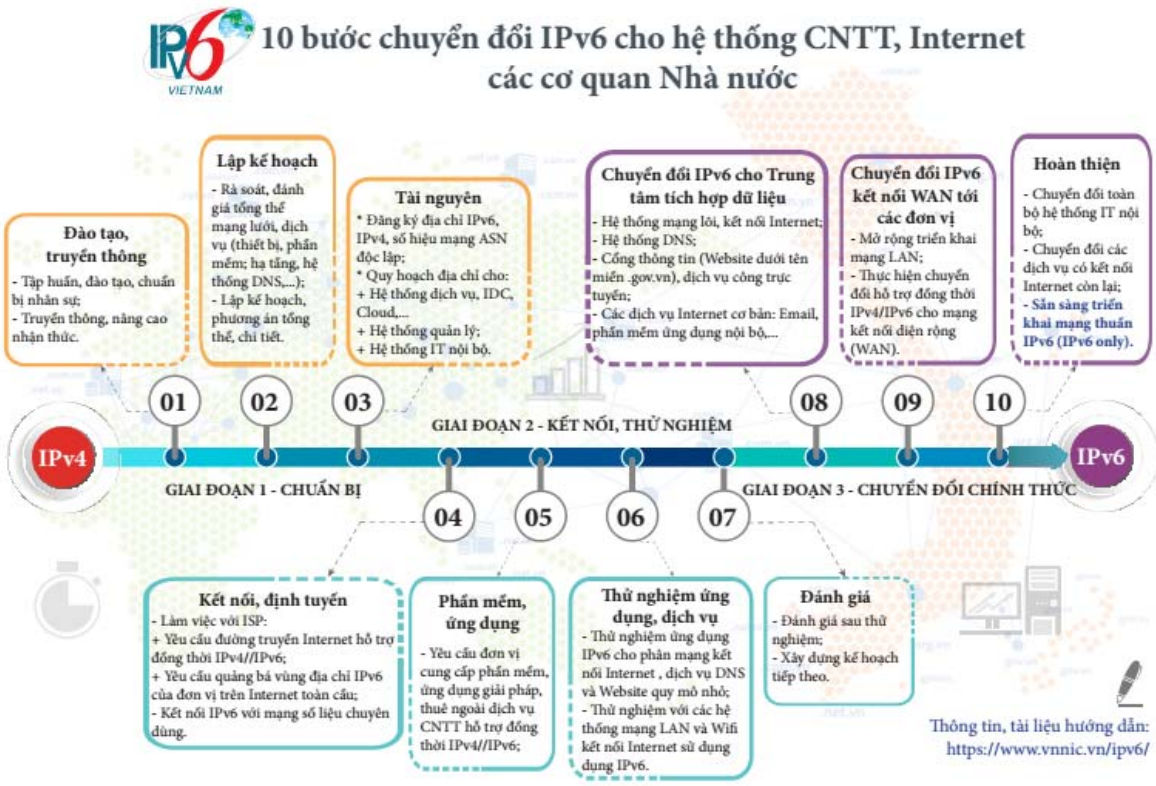
[2]https://www.vnnic.vn/sites/default/files/tailieu/VNNIC_TaiLieuHuongDanQuiHoachQuanLySuDungIPv6.pdf



Hình 7. Quy hoạch IPv4/IPv6

d) Chuyển đổi IPv6:

Địa chỉ IPv4 đã hết, không còn đủ để phát triển mạng Internet, vì vậy cần phải chuyển đổi sang IPv6. Việc triển khai chuyển đổi IPv6 khuyến nghị theo phương án song song IPv4/IPv6 (dual-stack), sau này tiến tới chỉ dùng IPv6 (IPv6 only). Chi tiết tham khảo tại địa chỉ: https://vnnic.vn/ipv6forgov.



Hình 8. Lộ trình chuyển đổi IPv6 cho các cơ quan Nhà nước

Về cơ bản CQNN thực hiện theo lộ trình chuyển đổi 3 giai đoạn, 10 bước[3] theo khuyến nghị của VNNIC được mô tả như sau:

(1) Giai đoạn I – Giai đoạn chuẩn bị:

Bước 1: Đào tạo, truyền thông: Tổ chức tập huấn, đào tạo, chuẩn bị nhân sự; Truyền thông nội bộ, nâng cao nhận thức cho các Lãnh đạo cơ quan, đơn vị và các đơn vị, cá nhân liên quan.

Bước 2: Lập kế hoạch: Rà soát tổng thể, đánh giá thực trạng mạng lưới và dịch vụ cho việc chuyển đổi ; Đánh giá phạm vi, quy mô chuyển đổi cho hệ thống máy chủ, dịch vụ, phần mềm và máy tính văn phòng để hỗ trợ IPv6. Lập kế hoạch, phương án tổng thể, chi tiết.

Bước 3: Chuẩn bị tài nguyên địa chỉ: Đăng ký địa chỉ IPv4, IPv6, ASN độc lập từ Trung tâm Internet Việt Nam – Bộ Thông tin và Truyền thông. Quy hoạch địa chỉ cho: hệ thống dịch vụ, IDC, Cloud ...; Hệ thống quản lý; Hệ thống IT nội bộ.

(2) Giai đoạn II – Kết nối, thử nghiệm:

[3] https://www.vnnic.vn/sites/default/files/tailieu/brochureIPv6-coquannhanuoc-final.pdf

Bước 4: Kết nối, định tuyến: Làm việc với ISP, VNIX về kết nối định tuyến Internet hỗ trợ đồng thời IPv4/IPv6; Làm việc với Cục Bưu điện Trung ương để triển khai kết nối IPv6 với mạng TSLCD.

Bước 5: Phần mềm, ứng dụng: Làm việc với các đơn vị cung cấp dịch vụ, phần mềm giải pháp, các đơn vị cung cấp dịch vụ CNTT thuê ngoài đảm bảo hỗ trợ IPv4/IPv6

Bước 6: Thử nghiệm ứng dụng, dịch vụ: Thử nghiệm ứng dụng IPv6 cho phân mạng kết nối Internet, dịch vụ DNS và Website quy mô nhỏ; các hệ thống LAN và Wifi kết nối Internet sử dụng IPv6.

Bước 7: Đánh giá: Đánh giá sau thử nghiệm; các vấn đề gặp phải, cách giải quyết, rút kinh nghiệm trước khi triển khai chính thức. Xây dựng kế hoạch tiếp theo.

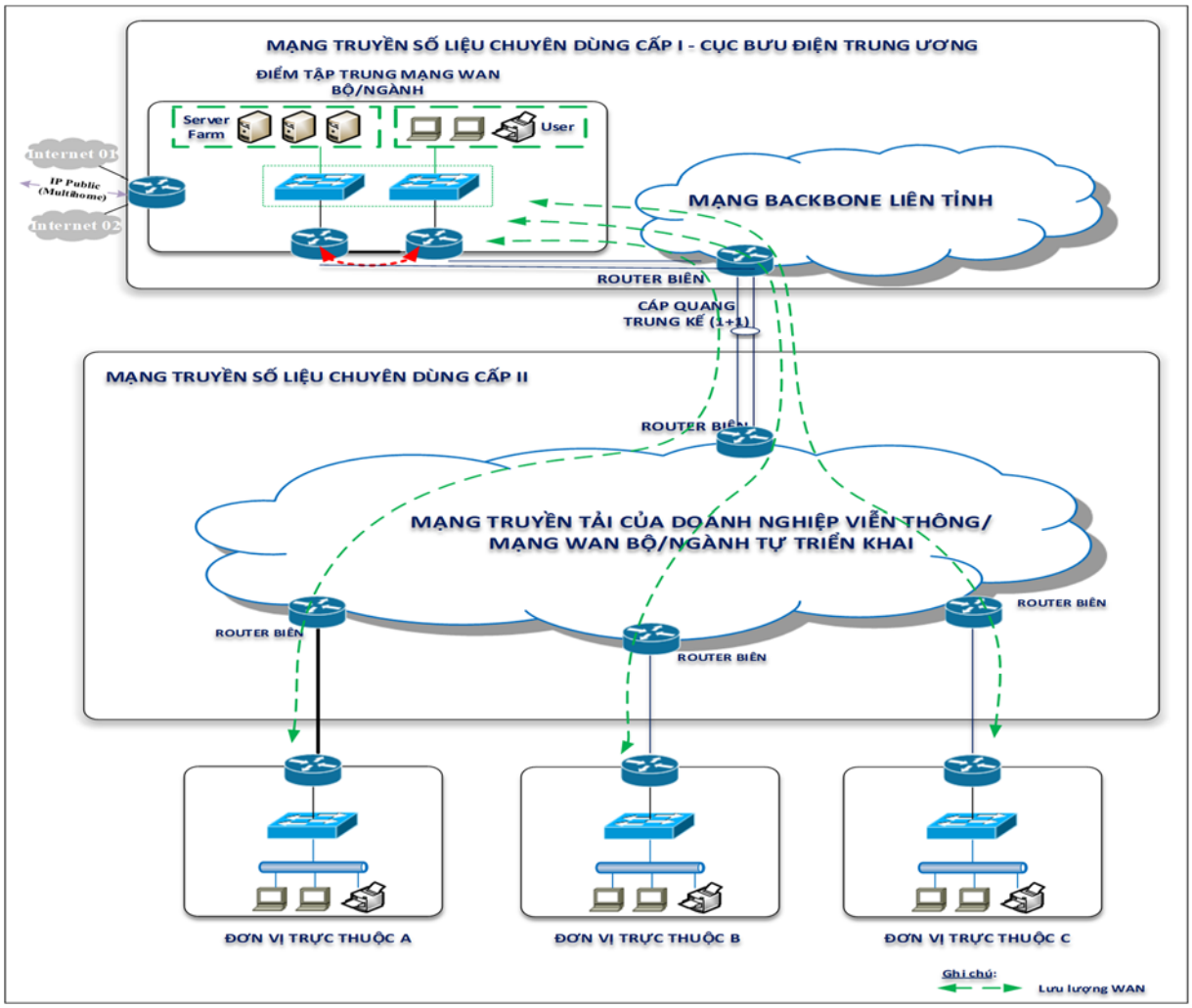
(3) Giai đoạn III – Chuyển đổi chính thức

Bước 8: Chuyển đổi IPv6 cho TTDL: Thực hiện chuyển đổi chính thức các hệ thống, dịch vụ: Hệ thống mạng lõi, mạng kết nối Internet; Hệ thống DNS; Cổng thông tin điển tử (đặc biệt là Website dưới tên miền .gov.vn), dịch vụ công trực tuyến; Các dịch vụ Internet cơ bản: Email, phần mềm ứng dụng nội bộ...

Bước 9: Chuyển đổi IPv6 kết nối WAN tới các đơn vị: Mở rộng triển khai IPv6 cho mạng LAN,WAN.

Bước 10: Hoàn thiện công tác chuyển đổi IPv6: Chuyển đổi các hệ thống IT nội bộ; Chuyển đổi các dịch vụ có kết nối Internet còn lại; Sẵn sàng triển khai mạng thuần IPv6 (IPv6 only).

2.2. Mô hình 05: kết nối mạng WAN của Bộ, ngành vào mạng TSLCD



Hình 9. Mô hình kết nối mạng WAN của Bộ, ngành vào mạng TSLCD

Mô hình kết nối mạng WAN của bộ, ngành vào mạng TSLCD là mô hình kết nối trực tiếp các đơn vị trực thuộc bộ, ngành lên điểm tập trung mạng WAN của bộ, ngành (thông thường là trụ sở chính hoặc TTDL của bộ, ngành).

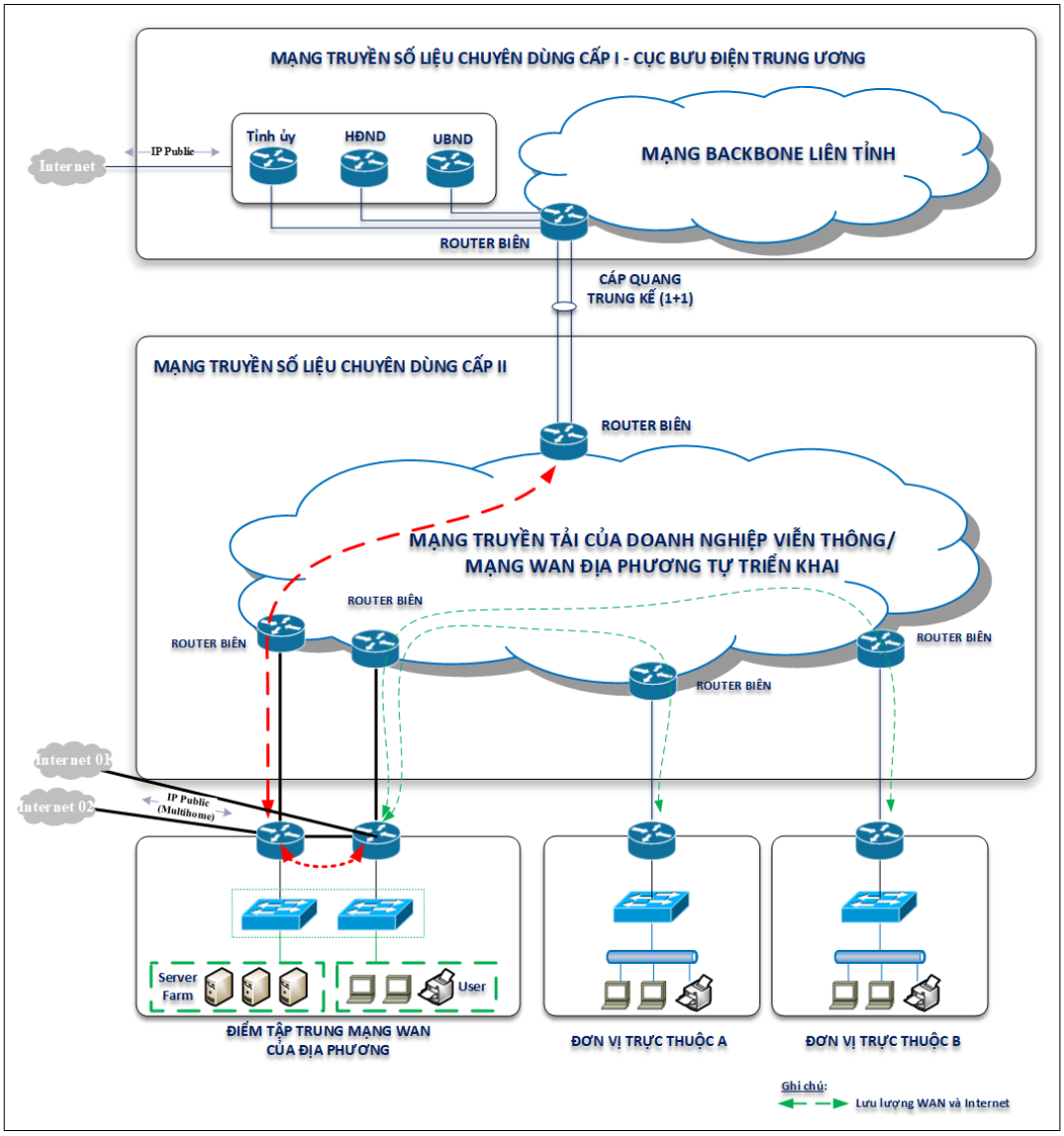
Các yêu cầu cơ bản:

- Trên hạ tầng mạng TSLCD cấp II (trong trường hợp bộ, ngành và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của bộ, ngành (trong trường hợp bộ, ngành tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của bộ, ngành.

- Tại điểm tập trung mạng WAN của bộ, ngành: thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của bộ, ngành.

2.3. Kết nối mạng WAN của địa phương vào mạng TSLCD

2.3.1. Mô hình 06: tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương



Hình 10. Mô hình tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương

Mô hình tập trung lưu lượng WAN và Internet về điểm quản lý tập trung của địa phương là mô hình sử dụng trong trường hợp các địa phương có nhu cầu triển khai Internet tập trung cho các đơn vị trực thuộc.

Các yêu cầu cơ bản:

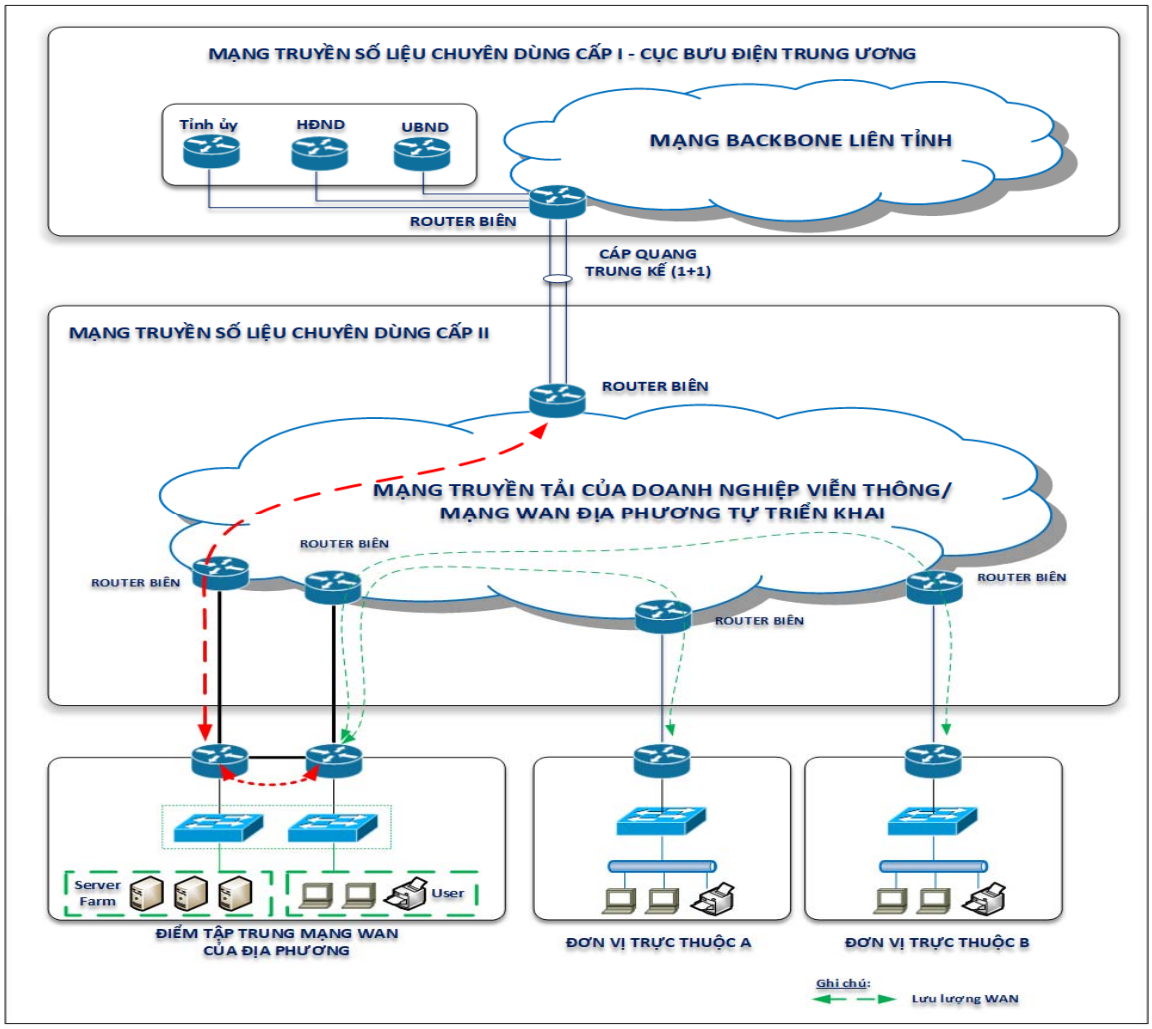
- Trên hạ tầng mạng TSLCD cấp II (trong trường hợp địa phương và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của địa phương (trong trường hợp địa phương tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương.

- Tại điểm tập trung mạng WAN của địa phương thực hiện:

+ Chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương.

+ Chuyển tiếp lưu lượng kết nối Internet của các đơn vị trực thuộc qua kênh kết nối Internet tại điểm tập trung.

2.3.2. Mô hình 07: chỉ tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương



Hình 11. Mô hình chỉ tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương

Mô hình tập trung lưu lượng WAN về điểm quản lý tập trung của địa phương là mô hình sử dụng trong trường hợp các địa phương không có nhu cầu triển khai Internet tập trung cho các đơn vị trực thuộc.

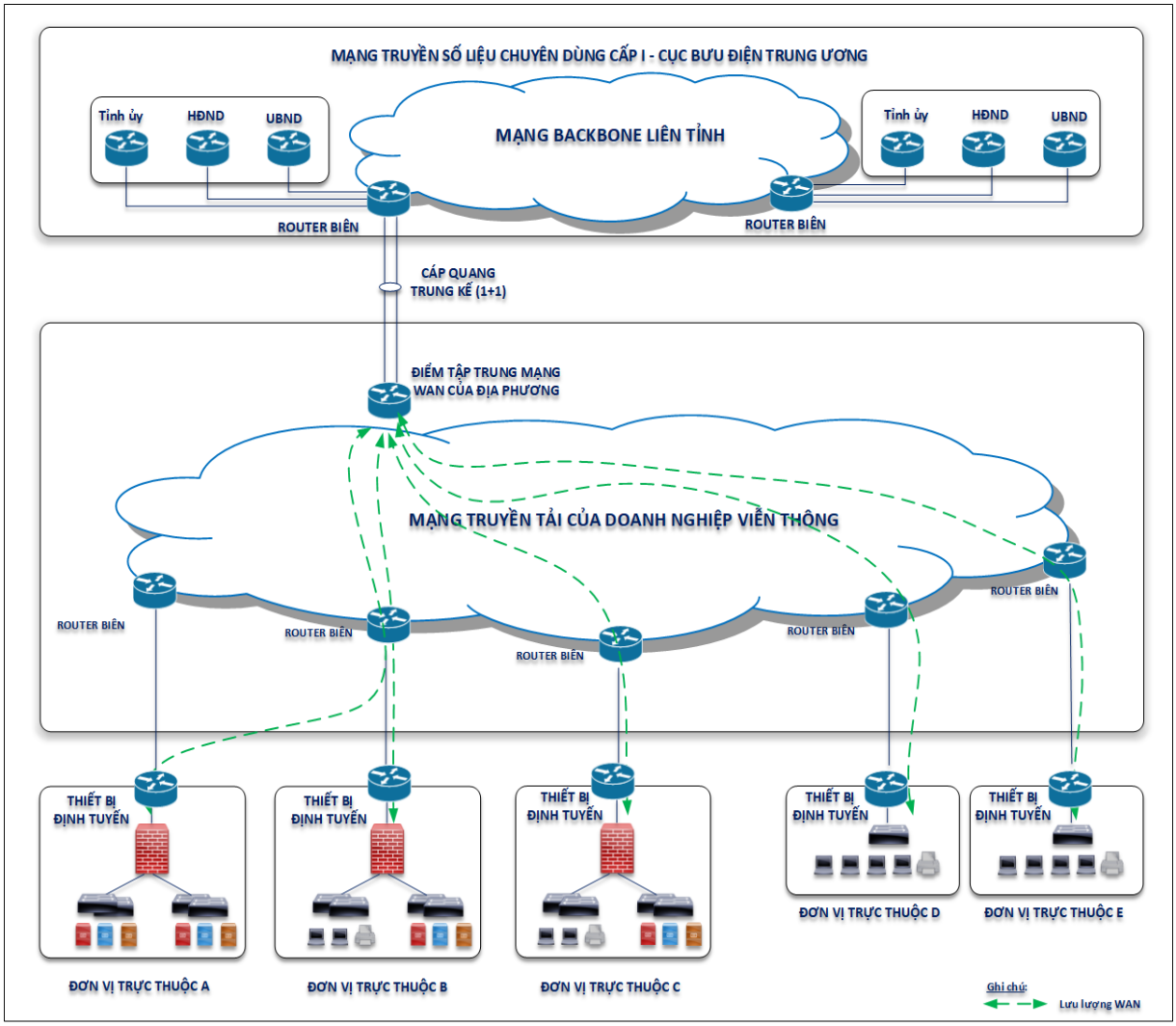
Các yêu cầu cơ bản:

- Trên hạ tầng mạng TSLCD cấp II (trong trường hợp địa phương và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của địa phương (trong trường hợp địa phương tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương.

- Tại điểm tập trung mạng WAN của địa phương thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương.

- Đối với lưu lượng Internet: thực hiện rẽ nhánh trực tiếp tại cổng kết nối của các đơn vị trực thuộc.

2.3.3 Mô hình 08: tập trung lưu lượng về điểm quản lý tập trung của DNVT



Hình 12. Tập trung lưu lượng về điểm quản lý tập trung của DNVT

Mô hình tập trung lưu lượng WAN về điểm quản lý tập trung của DNVT là mô hình sử dụng trong trường hợp các địa phương không có đủ trang thiết bị để thiết lập điểm tập trung mạng WAN của địa phương.

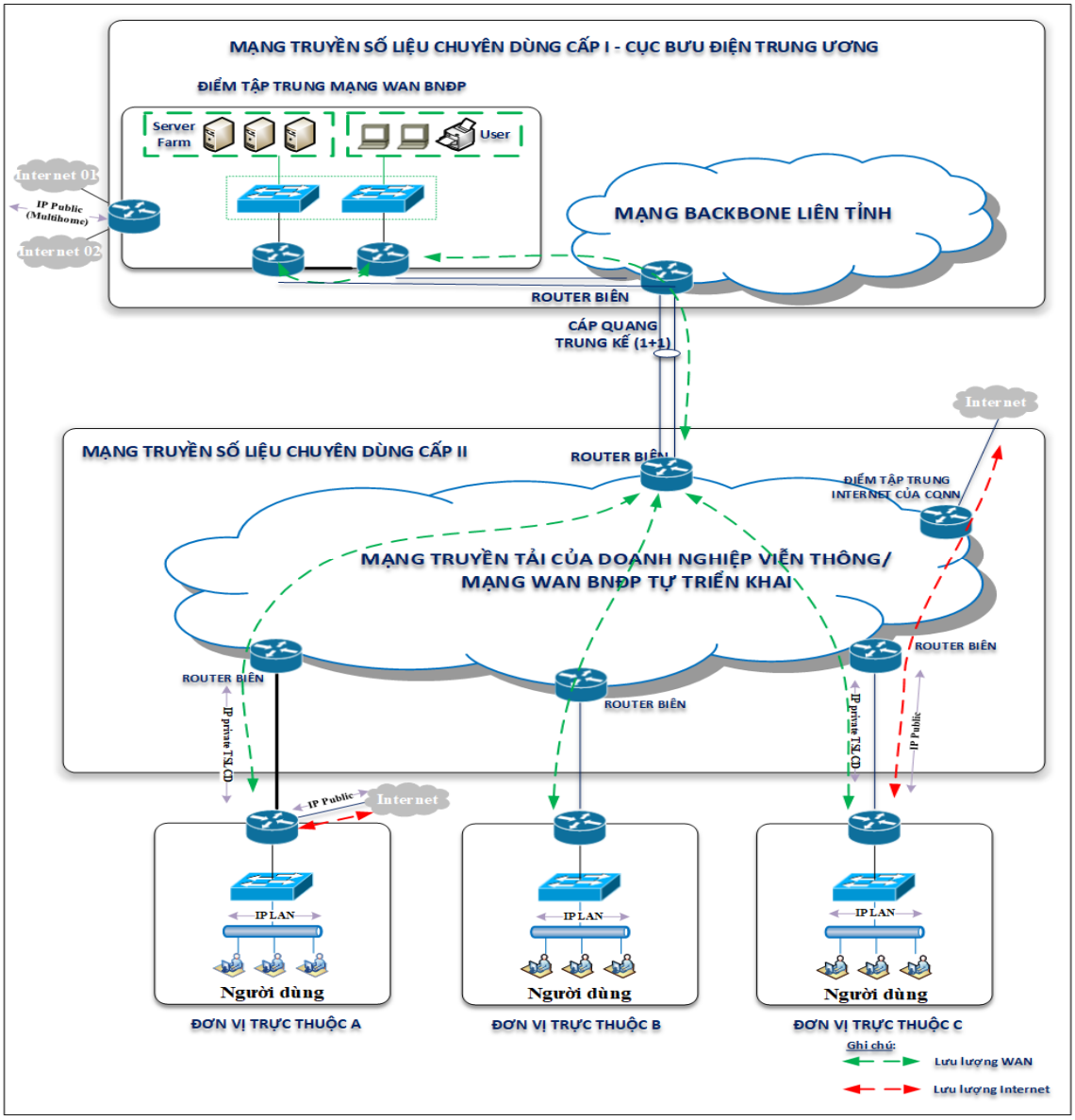
Các yêu cầu cơ bản:

- Trên hạ tầng mạng TSLCD cấp II: tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của địa phương tại DNVT.

- Tại điểm tập trung mạng WAN của địa phương tại DNVT thực hiện chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại TTDL của địa phương.

- Đối với lưu lượng Internet: thực hiện rẽ nhánh trực tiếp tại cổng kết nối của các đơn vị trực thuộc.

2.4. Mô hình 09: kết nối mạng LAN của đơn vị trực thuộc BNĐP vào mạng TSLCD:



Hình 13. Kết nối mạng LAN của đơn vị trực thuộc BNĐP vào mạng TSLCD:

Mô hình kết nối mạng LAN vào mạng TSLCD là mô hình sử dụng trong trường hợp các đơn vị không có HTTT (thường là các điểm quận/huyện, xã/phường).

Các yêu cầu cơ bản:

- Tại cổng kết nối của đơn vị: thực hiện tách riêng phân hệ kết nối Internet (IP Public do VNNIC quy hoạch) và phân hệ kết nối mạng TSLCD (IP private do Cục BĐTW quy hoạch). Cổng kết nối tại đơn vị cần đáp ứng các yêu cầu tại Phụ lục 1 Thông tư 12/2019/TT-BTTTT.

- Tại phân hệ LAN: 1 máy tính sử dụng đồng thời 2 kết nối Internet và TSLCD (IP do đơn vị sử dụng quy hoạch).

- Trên hạ tầng mạng của DNVT cung cấp kết nối Internet cho đơn vị: cần triển khai điểm tập trung Internet cho các CQNN để quản lý tập trung lưu lượng Internet của các CQNN tại địa phương.

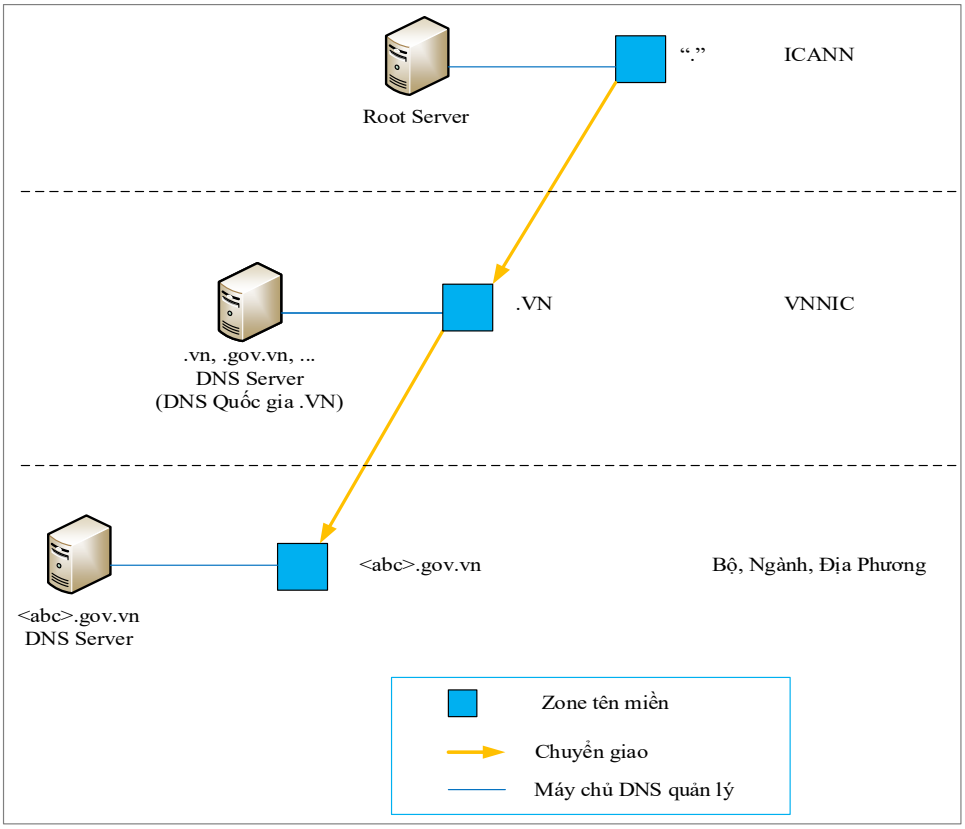
2.5. Mô hình hệ thống DNS

2.5.1. Mô hình 10: Hệ thống DNS quản lý tên miền <abc>.gov.vn của BNĐP

a) Phân cấp tên miền và máy chủ quản lý tên miền:

- Các BNĐP đều có tên miền <abc>.gov.vn để triển khai các dịch vụ: email, cổng thông tin, dịch vụ công trực tuyến, 1 cửa điện tử, …

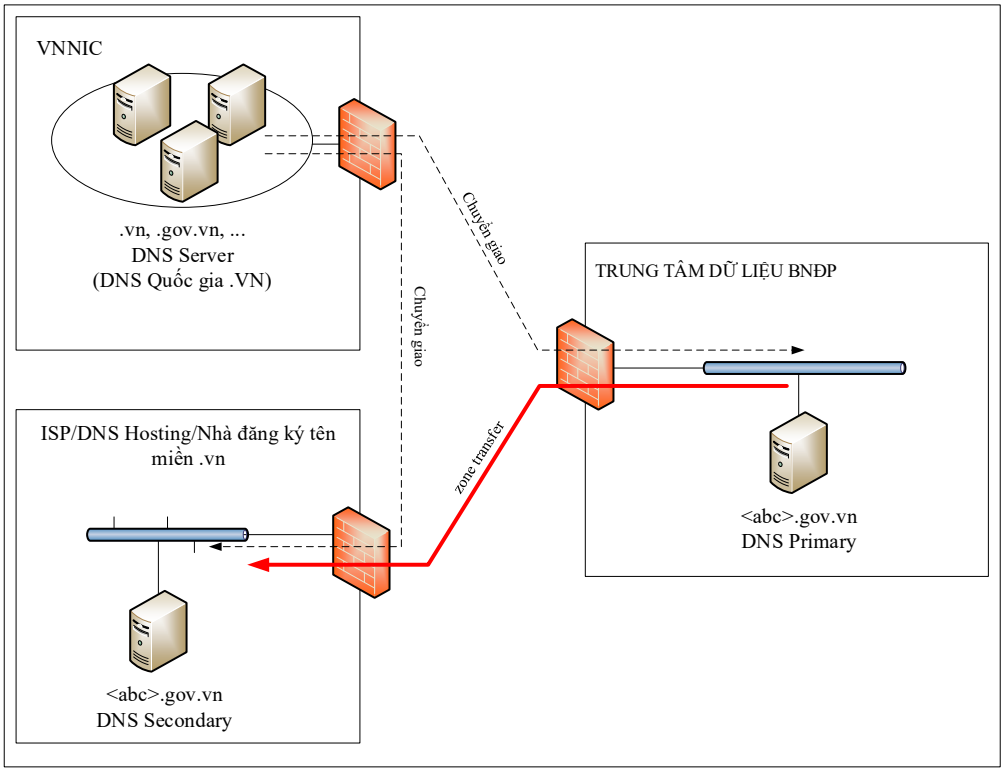
- Các BNĐP cần có hệ thống máy chủ tên miền DNS để quản lý các tên miền của mình theo hình vẽ dưới đây:



Hình 14. Hệ thống DNS quản lý tên miền <abc>.gov.vn của BNĐP

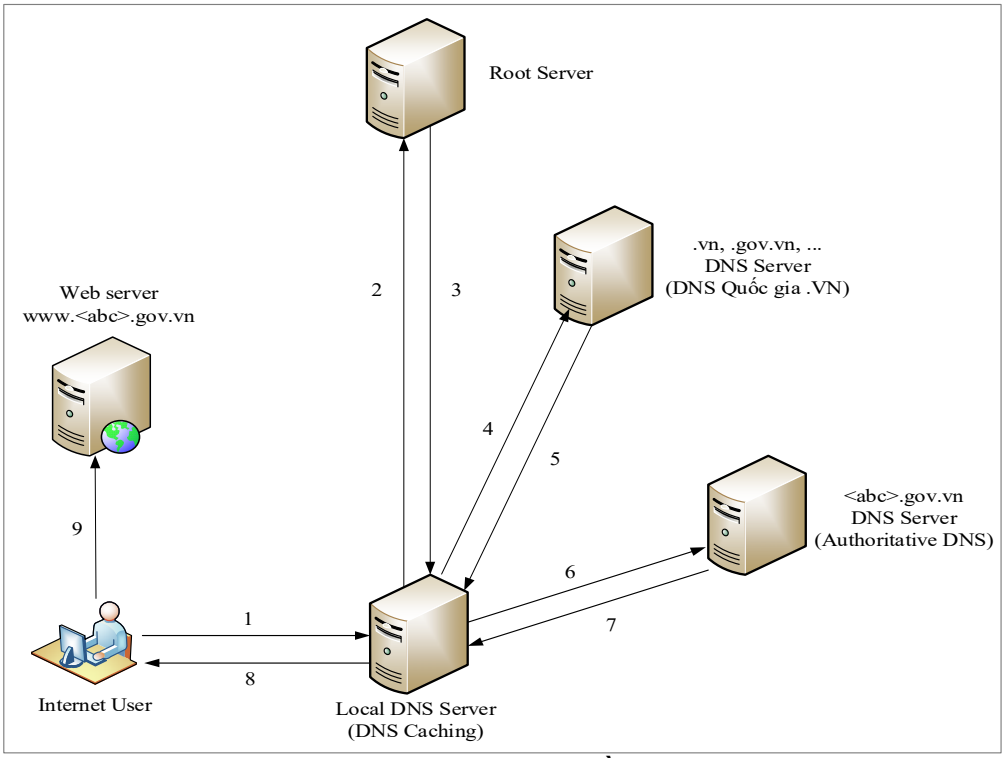
b) Mô hình khuyến nghị:

Khuyến nghị mô hình tổng thể về DNS quản lý tên miền <abc.gov.vn> theo hình vẽ như sau:



Hình 15. Mô hình tổng thể DNS quản lý tên miền <abc.gov.vn>

BNĐP sẽ có tối thiểu 02 máy chủ DNS để quản lý tên miền, máy chủ chính (Master) đặt tại TTDL, máy chủ phụ (secondary) đặt thuê tại ISP/Đơn vị cung cấp dịch vụ DNS Hosting. Hoạt động truy cập tên miền www.<abc>.gov.vn như sau:



Hình 16. Hoạt động truy cập tên miền www.<abc.gov.vn>

Chương trình trên máy người sử dụng (máy client) gửi yêu cầu tìm kiếm địa chỉ IP ứng với tên miền <abc>.gov.vn tới máy chủ quản lý tên miền cục bộ Local DNS Server (DNS Caching) thuộc mạng của nó. Máy chủ DNS Caching sẽ thực hiện quá trình truy vấn đệ quy tìm kiếm thông tin địa chỉ IP của tên miền và trả lời cho client để truy cập website www.<abc>.gov.vn.

c) Khai báo, quản lý tên miền ngược:

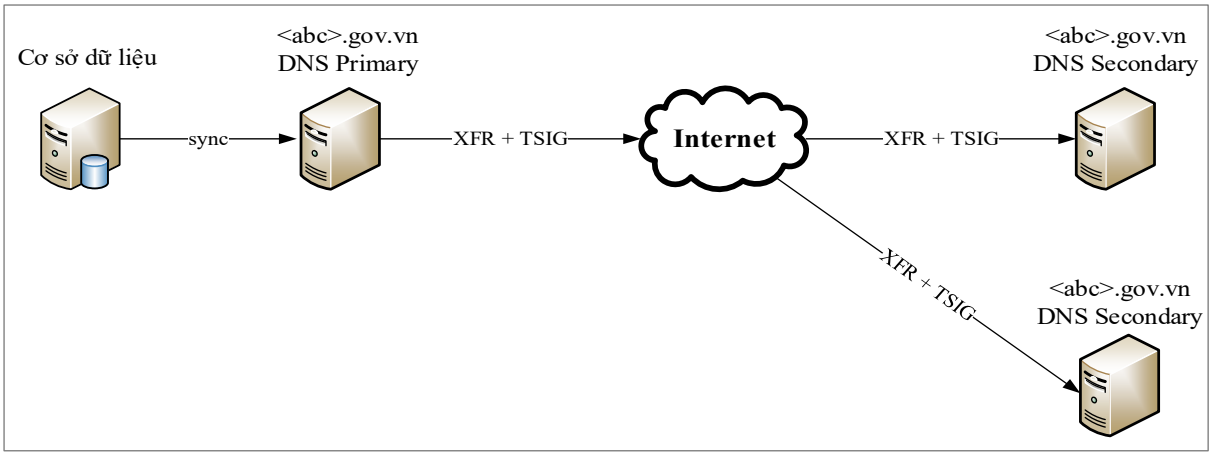
BNĐP được cấp phát địa chỉ IP từ VNNIC, khi đưa vào sử dụng cần khai báo tên miền ngược trên máy chủ DNS của mình, chi tiết tham khảo hướng dẫn tại địa chỉ sau: https://www.vnnic.vn/diachiip/hotro/thamkhao/.

d) Các yêu cầu cụ thể:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS với địa chỉ IP khác nhau quản lý tên miền đặt ở 02 mạng độc lập khác nhau: tại TTDL của BNĐP và tại các đơn vị cung cấp dịch vụ như ISP, DNS Hosting hoặc nhà đăng ký tên miền .vn.

- 01 máy chủ DNS Primary (Master) quản lý dữ liệu chính, toàn bộ khai báo các bản ghi dịch vụ như <www, mail, edoc>.gov.vn được thực hiện trên máy chủ này.

- 01- 02 máy chủ DNS Secondary (Slave): được đồng bộ với máy chủ master theo cơ chế zone transfer, sử dụng TSIG để đảm bảo an toàn (XFR + TSIG). Cơ chế TSIG (transaction signature) là quá trình sử dụng chung mã bảo mật chia sẻ giữa máy chủ DNS Primary và DNS Secondary để đảm bảo giao tiếp giữa các máy chủ DNS được xác thực.

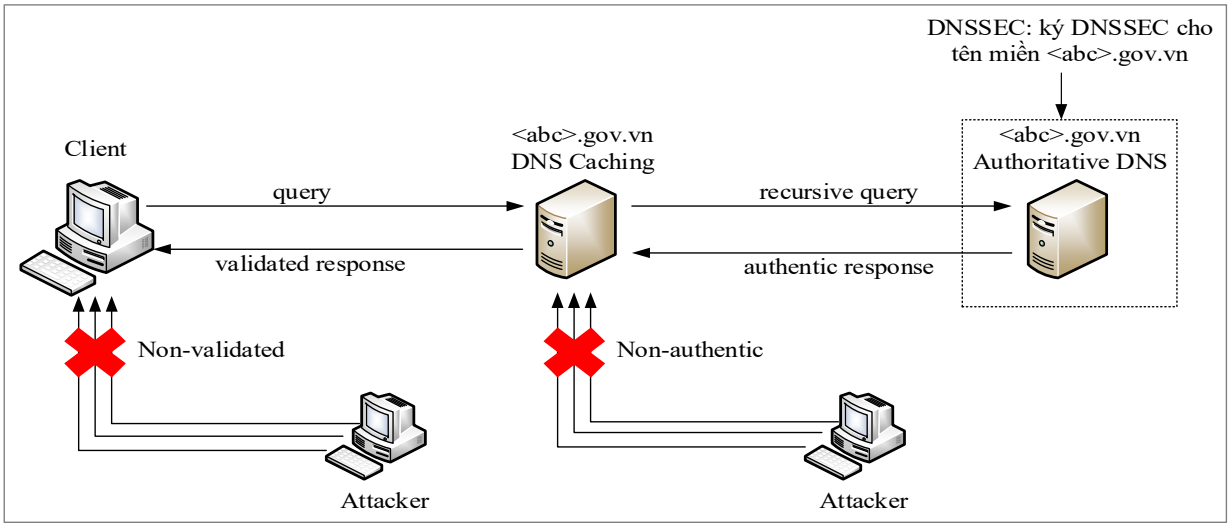


Hình 17. Đồng bộ CSDL máy chủ DNS Primary và Secondary

- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.

- Triển khai DNSSEC, đóng vai trò ký DNSSEC cho tên miền để đảm bảo an toàn tên miền. Các công việc thực hiện sẽ là tạo ra các khóa DNSSEC và ký lên zone tên miền <abc>.gov.vn. Gửi cập nhật đăng ký bản ghi chuyển giao

(Deligation Signer - DS) lên hệ thống DNS quốc gia do VNNIC quản lý thông qua các nhà đăng ký tên miền .vn.



Hình 18. Triển khai DNSSec

Tham khảo hướng dẫn: https://vnnic.vn/sites/default/files/tailieu/VNNIC-TaiLieuHuongDanTrienKhaiDNSSEC-DHP-Final.pdf

- Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack).

- Khai báo các bản ghi AAAA cho các tên miền như <www, mail, edoc>.gov.vn để hoạt động được trên mạng Internet IPv6.

- Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS0 (truy vấn DNS hỗ trợ IPv6, DNSSEC).

- Các phần mềm tham khảo: BIND 9.x, NSD.

2.5.2. Mô hình 11: Hệ thống máy chủ tên miền đệm (DNS Caching)

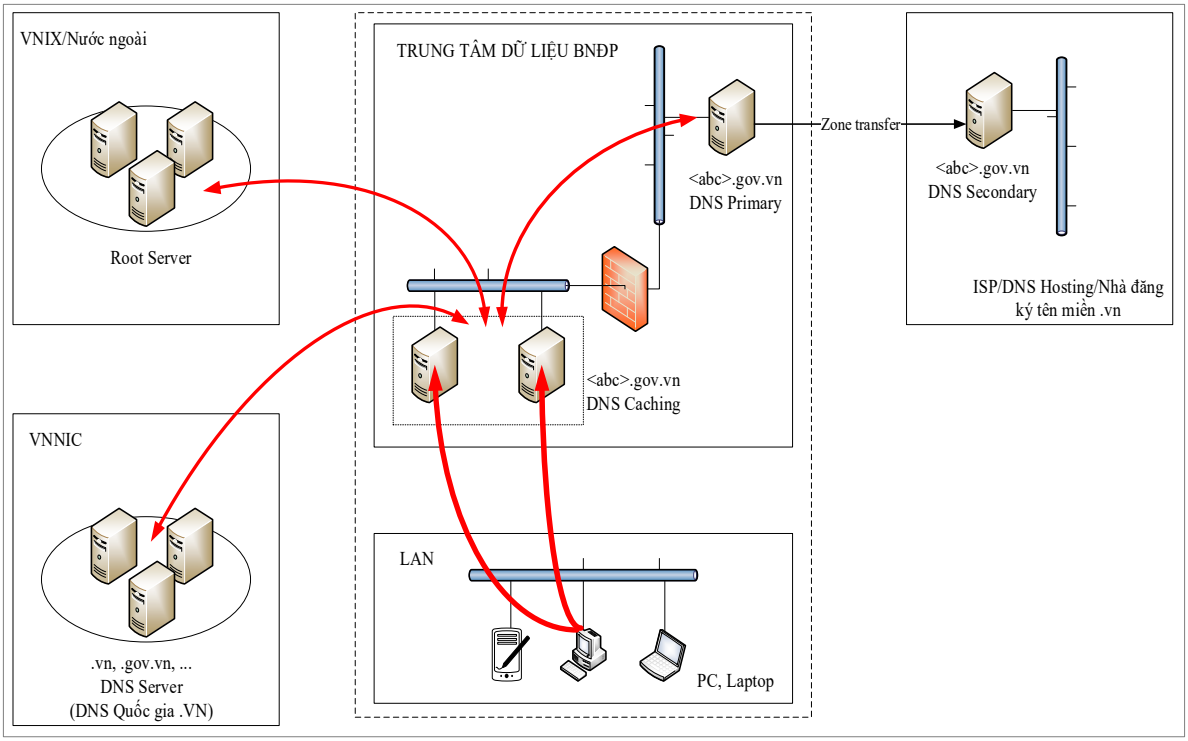
a) Sự cần thiết:

Phục vụ truy cập các dịch vụ Internet sử dụng tên miền, truy vấn tên miền .VN và tên miền quốc tế của các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động…) trong mạng của các đơn vị (BNĐP).

Quản lý thiết lập chính sách truy cập tên miền tập trung, hệ thống DNS Caching có thể kết hợp với các hệ thống ATTT khác để bảo vệ chống mã độc, botnet….

b) Mô hình khuyến nghị:

Khuyến nghị mô hình tổng thể về DNS Caching cho BNĐP như sau:



Hình 19. Mô hình tổng thể DNS Caching cho BNĐP

- Các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, …) trong mạng của các đơn vị (BNĐP) trước khi kết nối sử dụng dịch vụ (nội bộ hoặc trên Internet) thì việc đầu tiên là phải kết nối, truy vấn tên miền để tìm kiếm thông tin địa chỉ IP của dịch vụ cần kết nối đến.

- Hệ thống DNS Caching sẽ đi tìm kiếm và trả lời các thông tin về tên miền cho các thiết bị trong mạng của các đơn vị đang yêu cầu như hình vẽ trên.

c) Các yêu cầu cụ thể:

- Máy chủ DNS: tối thiểu 02 máy chủ DNS Caching với địa chỉ IP khác nhau đặt tại trung tâm TTDL của BNĐP. 02 máy chủ hoạt động Active-Active, đảm bảo khả năng dự phòng nóng, khi 01 máy chủ bị lỗi hoặc hỏng hóc vẫn còn 01 máy chủ còn lại hoạt động, đảm bảo không bị gián đoạn.

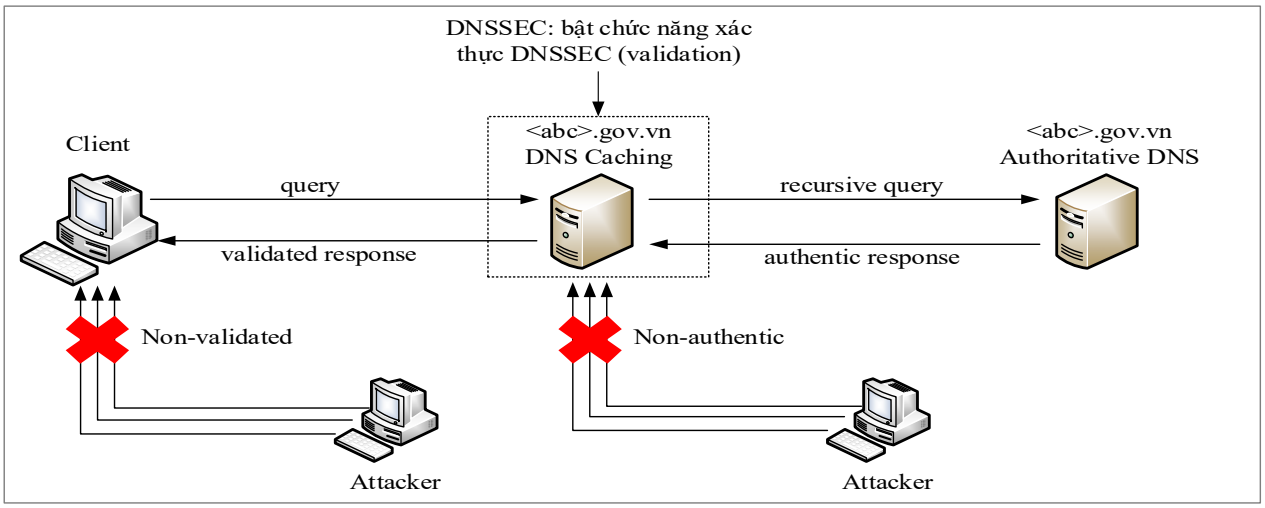
- Hệ thống có thể được thiết lập theo cơ chế đệ quy (recursive), tức là sẽ đi tìm kiếm câu trả lời từ các máy chủ DNS khác để trả lời cho máy trạm (client). Hoặc hệ thống có thể được thiết lập theo cơ chế caching forwarder (chuyển tiếp) để chuyển tiếp toàn bộ kết nối, truy vấn tên miền đến hệ thống DNS Caching khác.

- Hệ thống chỉ phục vụ các truy vấn tên miền từ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị di động, …) trong mạng của các đơn vị, không tiếp nhận phục vụ các truy vấn tên miền từ bên ngoài.

- Toàn bộ các thiết bị (máy tính để bàn, máy tính xách tay, thiết bị động, …) trong mạng của đơn vị phải được cấu hình để sử dụng hệ thống DNS Caching này.

- Ghi nhật ký hoạt động, phần mềm giám sát DNS, phân tích log DNS.

- Triển khai DNSSEC, đóng vai trò xác thực (validation) để đảm bảo an toàn tên miền: DNS Caching hỗ trợ DNSSEC có vai trò rất quan trọng, giúp bảo vệ người sử dụng, chống lại việc giả mạo các phản hồi truy vấn tên miền thông quan việc xác thực chữ ký số trên các bản ghi DNS có trong câu trả lời truy vấn tên miền.



Hình 20. Triển khai DNSSec

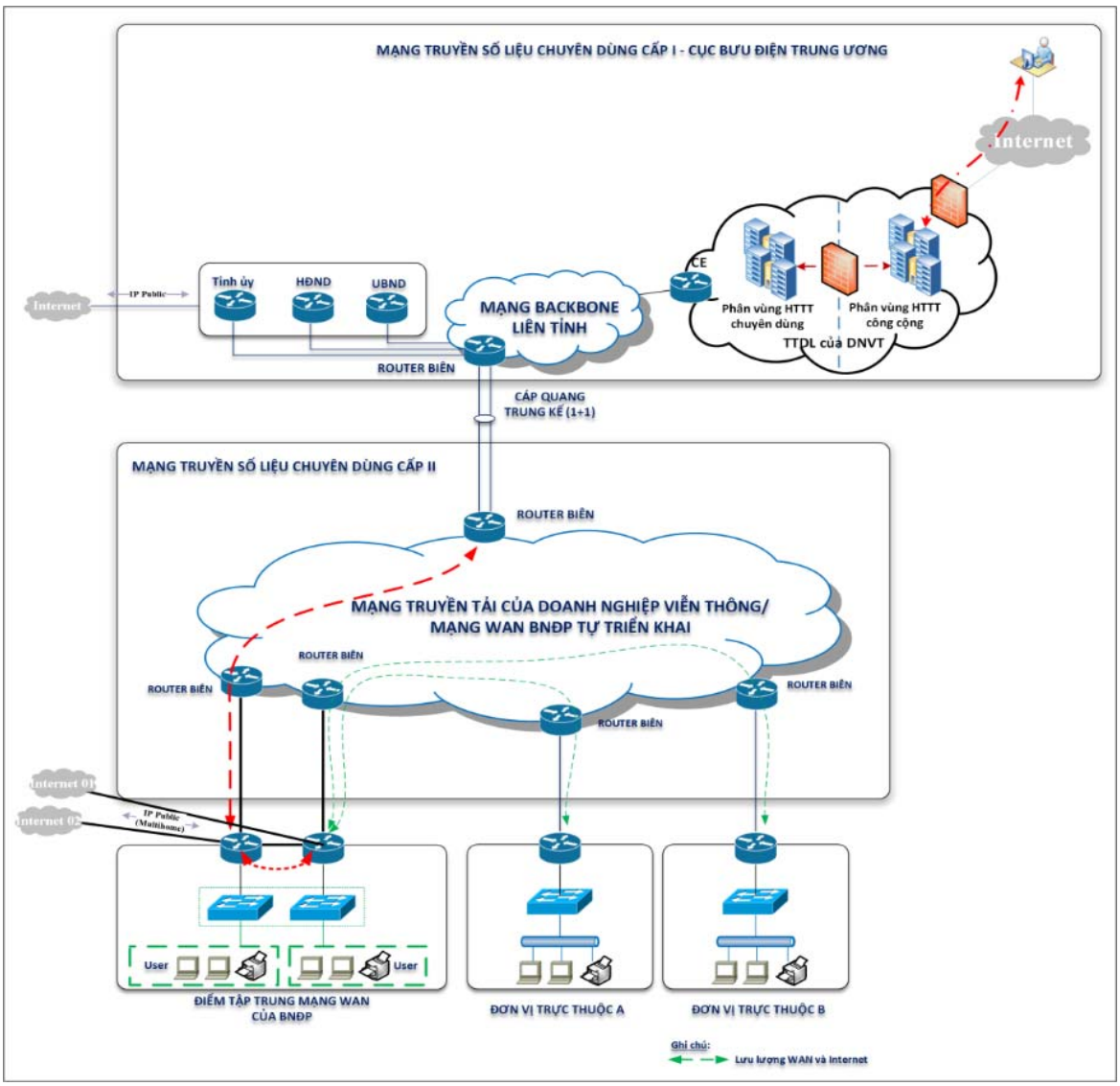
Tham khảo hướng dẫn: https://vnnic.vn/sites/default/files/tailieu/VNNIC-TaiLieuHuongDanTrienKhaiDNSSEC-ISP-Final.pdf

- Triển khai máy chủ DNS chạy song song IPv4, IPv6 (dual-stack), hỗ trợ kết nối, truy vấn từ các máy trạm trên mạng Internet IPv6.

- Thiết lập chính sách tường lửa (firewall): UDP-53, TCP-53 (truy vấn DNS); cho phép truy vấn EDNS0 (truy vấn DNS hỗ trợ IPv6, DNSSEC).

- Các phần mềm tham khảo: BIND 9.x, Unbound.

III. Mô hình mục tiêu



Hình 21. Mô hình mục tiêu

Mô hình mục tiêu là mô hình chuẩn, đáp ứng các yêu cầu về ATTT, được sử dụng trong trường hợp các BNĐP có đầy đủ các điều kiện, trang thiết bị để triển khai.

Các yêu cầu cơ bản:

- Trên hạ tầng mạng TSLCD cấp II (trong trường hợp BNĐP và các đơn vị trực thuộc có kết nối mạng TSLCD cấp II) hoặc hạ tầng mạng WAN của BNĐP (trong trường hợp BNĐP tự triển khai hạ tầng mạng WAN riêng): tạo kết nối điểm – đa điểm từ các đơn vị trực thuộc về điểm tập trung mạng WAN của BNĐP.

- Tại điểm tập trung mạng WAN của BNĐP thực hiện:

+ Chuyển tiếp lưu lượng từ các đơn vị trực thuộc đến các ứng dụng tại HTTT chuyên dùng của BNĐP đặt tại TTDL của DNVT.

+ Chuyển tiếp lưu lượng kết nối Internet của các đơn vị trực thuộc qua kênh kết nối Internet tại điểm tập trung.