CHƯƠNG TRÌNH NGHIÊN CỨU KHOA HỌC VÀ PHÁT TRIỂN
CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG KC.01

ĐỀ TÀI KC.01.02

NGHIÊN CỨU PHÁT TRIỂN VÀ ỨNG DỤNG CÔNG NGHỆ, DỊCH VỤ MẠNG IP TIẾP CẬN CÔNG NGHỆ IN-TƠ-NÉT (INTERNET) THẾ HỆ MỚI

Chủ nhiệm đề tài: GS.TSKH. Đỗ Trung Tá

QUYỂN 7

ĐỀ TÀI NHÁNH:

TRIỂN KHAI THỬ NGHIỆM MẠNG IPV6 VIỆT NAM VÀ KẾT NỐI MẠNG IPV6 QUỐC TẾ

Đơn vị thực hiện: Công ty Điện toán và Truyền số liệu -VDC
Chủ trì : Vũ Hoàng Liên

BỘ BƯU CHÍNH, VIỄN THÔNG
Hà Nội, 06-2004

CHƯƠNG TRÌNH NGHIÊN CỨU KHOA HỌC VÀ PHÁT TRIỂN
CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG KC.01
ĐỀ TÀI KC.01.02

TÀI LIỆU ĐÁNH GIÁ KẾT QUẢ TRIỂN KHAI KẾT NỐI VỚI IPV6 QUỐC TẾ

CÔNG TY ĐIỆN TOÁN VÀ TRUYỀN SỐ LIỆU - VDC
Hà Nội, 06-2004

BÀI TÓM TẮT ĐỀ TÀI

Đề tài này nghiên cứu tóm lược về không gian địa chỉ IPv6, cách thức chuyển đổi mạng IPv4 và IPv6. Trọng tâm của đề tài hướng tới việc xây dựng một mạng IPv6 Việt Nam kết nối quốc tế, do vậy tập trung vào việc chọn lựa phương thức chuyển đổi IPv4/IPv6 thích hợp, định cỡ mạng IPv6 Việt Nam, các phương thức kết nối quốc tế và kinh nghiệm cũng như triển khai thực tế. Ngoài ra, đề tài cũng triển khai một số các ứng dụng IPv6 trên nền mạng IPv6 Việt Nam có khả năng áp dụng trong thực tế, tiến tới làm chủ công nghệ và có những ứng dụng IPv6 của riêng mình trong tương lai.

Đề tài được cấu trúc gồm 3 chương, kết luận và phụ lục. Các chương được trình bày theo thứ tự và mục tiêu nghiên cứu cũng như triển khai của đề tài.

Chương I nghiên cứu về **Kế hoạch định cỡ và định tuyến mạng IPv6**. Mạng thử nghiệm IPv6 cần được định cỡ về mọi phương diện như địa chỉ mạng, định cỡ thiết bị mạng, định cỡ dịch vụ và ứng dụng, phân tách để triển khai từng bước, kết nối nội bộ, kết nối trên diện rộng và kết nối quốc tế. Mạng thử nghiệm IPv6 sẽ được xây dựng trên nền mạng IPv4, có nghĩa là các thành phần IPv6 sẽ được lưu thông và định tuyến thông qua bộ định tuyến cửa khẩu của mạng IPv4 trước khi đi ra ngoài quốc tế, ngoài ra cũng phải được định tuyến để có thể có khả năng tích hợp với mạng IPv4 hiện tại. Việc chuyển đổi mạng IPv4 dần dần sang mạng IPv6 phải tuân thủ các nguyên tắc như không được phá vỡ cấu trúc mạng thực tế đang có, các tiến trình sử dụng IPv4 không bị ảnh hưởng và giảm hiệu năng. Ngoài ra, mạng thử nghiệm IPv6 còn cần phải được định cỡ và định tuyến phù hợp với các tiêu chuẩn của quốc tế để được phép kết nối ra mạng IPv6 quốc tế.

Chương II nghiên cứu về việc **Áp dụng thử nghiệm kế hoạch chuyển đổi từ mạng IPv4 sang IPv6**. Chương này tập trung chủ yếu vào việc nghiên cứu sự khả thi và cần thiết của việc chuyển đổi, việc định cỡ và quản lý địa chỉ IPv6 trong và sau quá trình chuyển đổi. Chương II cũng nghiên cứu việc chuyển đổi địa chỉ IPv6 tại Việt Nam dựa trên việc xây dựng một mạng IPv6 song song với việc chuyển đổi dần dần địa chỉ IPv4/IPv6 từ mạng IPv4 hiện đang có. Sau đó là việc **Thử nghiệm các dịch vụ và ứng dụng IPv6**. Việc kết nối sử dụng không gian địa chỉ IPv6 về cơ bản nhằm mang lại cho người sử dụng cơ hội và khả năng sử dụng các dịch vụ và ứng dụng IPv6. Ngay trong quá trình thử nghiệm cũng như xây dựng mô hình, một số các dịch vụ IPv6 như DNS, Web Server, Mail Server, FTP Server... đã được thử nghiệm trong các mô hình mạng khác nhau và đã đem lại những kết quả khả quan so với việc sử dụng các dịch vụ này trong không gian địa chỉ IPv4. Các ứng dụng IPv6 cũng đã được bắt tay vào thử nghiệm để có thể thu thập được các kinh nghiệm cần thiết cũng như

bước đầu thử tiếp cận với môi trường bùng nổ của các thiết bị kết nối sử dụng giao thức TCP/IP. Đối với tầng mạng, các công cụ như Iperf, tcpdump... đã được thử nghiệm để nhằm mục đích thu thập kinh nghiệm đối với các ứng dụng có tác động tới quá trình xử lý trực tiếp địa chỉ IPv6. Đối với tầng ứng dụng, các công cụ video số đã được thử nghiệm nhằm mục đích thử nghiệm các ứng dụng xử lý các gói tin IPv6 với số lượng lớn, đồng thời cũng cân nhắc tới khía cạnh hữu dụng và phổ biến của các loại ứng dụng này.

Chương III tập trung vào việc **So sánh và đánh giá kết quả**. Các kết quả thử nghiệm đối với các dịch vụ cơ bản được đánh giá và so sánh đối với các kết quả tương tự được thực hiện trong môi trường IPv4. Chương này cũng nhắc lại về các mô hình kết nối thử nghiệm khác nhau để đánh giá kết quả kết nối đối với các mô hình này. Một số lộ trình triển khai của các ISP trong khu vực và các ISP tại châu Á cũng đã được xem xét tới để rút ra những kinh nghiệm trong việc triển khai tại Việt Nam

Đề tài được thực hiện trong một thời gian không dài, tuy vậy cũng đã có được những thành công nhất định, mà đặc biệt là việc triển khai thành công mạng thử nghiệm IPv6 diện rộng trong nước, sau đó kết nối với mạng IPv6 quốc tế, tạo tiền đề cho những nghiên cứu và triển khai chuyển đổi thật sự trong tương lai. Tuy còn gặp những khó khăn về thời gian và nhất là việc chưa có khách hàng thử nghiệm, đề tài đã đưa ra được những kết quả tương đối thuyết phục về việc thử nghiệm kết nối và hiệu năng của các dịch vụ/ứng dụng thử nghiệm trong không gian địa chỉ mới, địa chỉ IPv6.

MỤC LỤC

Danh mục hình vẽ

Danh mục bảng biểu

Lời mở đầu

Với sự phát triển của Internet về phạm vi cũng như loại hình ứng dụng, giao thức nền IPv4 chắc hẳn sẽ không thể đáp ứng được trong tương lai không xa. IPv6 đang được nghiên cứu và đưa ra như là sự lự chọn duy nhất cho sự phát triển tiếp tục của Internet.

Chuyển đổi hạ tầng từ IPv4 lên IPv6 là điều chắc chắn sẽ xảy ra. Tuy nhiên, chuyển đổi lên IPv6 phải đảm bảo hoạt động bình thường của mạng và đặc biệt phải trong suốt đối với người dùng đấu cuối. Quá trình chuyển đổi cần diễn ra dần dần, các tính năng mới được thiết kế chỉ là tuỳ chọn chứ không phải là yêu cầu bắt buộc để cho phép sự song song tồn tại của IPv4 và IPv6 trong quá trình chuyển đổi.

Đề tài nghiên cứu tóm lược về không gian địa chỉ IPv6, cách thức chuyển đổi mạng IPv4 và IPv6. Trọng tâm của đề tài hướng tới việc xây dựng một mạng IPv6 Việt Nam kết nối quốc tế, do vậy tập trung vào việc chọn lựa phương thức chuyển đổi IPv4/IPv6 thích hợp, định cỡ mạng IPv6 Việt Nam, các phương thức kết nối quốc tế và kinh nghiệm cũng như triển khai thực tế. Ngoài ra, đề tài cũng triển khai một số các ứng dụng IPv6 trên nền mạng IPv6 Việt Nam có khả năng áp dụng trong thực tế, tiến tới làm chủ công nghệ và có những ứng dụng IPv6 của riêng mình trong tương lai.

Chương 1: KẾ HOẠCH THỬ NGHIỆM ĐỊNH CỠ VÀ ĐỊNH TUYẾN MẠNG IPv6

Chương này nói về kế hoạch thử nghiệm định cỡ và định tuyến mạng IPv6 để kết nối trong các mô hình khác nhau, đặc biệt là mô hình kết nối với mạng IPv6 quốc tế. Chương này không đi sâu và chi tiết vào việc triển khai mà chỉ dừng lại ở mức định cỡ và đánh giá công nghệ cũng như thiết bị để triển khai.

1.1 Các phương pháp chuyển đổi từ IPv4 sang IPv6

Trong thời điểm hiện tại, việc ngừng sử dụng IPv4 để chuyển đổi sang sử dụng IPv6 trên diện rộng là điều không thể thực hiện được ngay lập tức. Đối với các mạng nhỏ sử dụng IPv4, chuyển đổi sang IPv6 là điều cần thiết, tuy nhiên cũng chỉ có thể thực hiện dần từng bước thay vì đồng loạt, điều đó đảm bảo không có sự đột biến trong việc tiếp cận công nghệ mới. Do vậy, các phương pháp chuyển đổi cho phép chuyển đổi từ cục bộ đến chuyển đổi tổng thể một hệ thống mạng đang sử dụng IPv4 sang IPv6 đã ra đời. Các giải pháp này được xây dựng trên cơ sở các nút mạng IPv4/IPv6 ngày càng tăng và IPv6 cùng tồn tại với IPv4, chuyển đổi dần dần các nút mạng IPv4 sang IPv6 và tiến dần tới mạng trục.

1.1.1 Sử dụng làn đôi IPv6/IPv4 (Dual-Layer)

Bản chất của việc sử dụng làn đôi IPv6/IPv4 cho phép hỗ trợ các kết nối giữa IPv4 và IPv6, cho phép các liên kết giữa IPv6 và IPv4 trao đổi với nhau theo nguyên lý ngăn xếp (stack). Phương pháp này cho phép nâng cao độ tin cậy trong việc nhận và gửi các gói tin IPv6 trên nền giao thức IPv4 đang hoạt động bình thường.

Khả năng này cho phép các trạm mới cài đặt IPv6 tương tác với các trạm IPv4 cũ một cách trực tiếp và dễ dàng. Giải pháp này cũng cho phép IPv6 dần dần trở nên phổ biến trên mạng trục mà các kết nối IPv4 cũ vẫn không hoàn toàn bị loại bỏ. Đây là giải pháp được sử dụng phổ biến cho các **thiết bị đầu cuối** và **thiết bị định tuyến**.

1.1.2 Sử dụng cấu hình đường ống thủ công IPv6 trên IPv4

Phương pháp này thường được áp dụng để thực hiện lưu thông IPv6 trên nền tảng mạng IPv4. Đường ống IPv6 trên IPv4 được sử dụng trong bốn trường hợp khác nhau: **tram-tram**; **tram-router**; **router-tram** và **router-router**. Để phù hợp với mô hình này, hai kỹ thuật chính hỗ trợ thiết lập cấu hình đường ống được đề xuất dựa trên cơ chế đóng gói các gói tin IPv6 trong các gói tin IPv4 sẵn có:

Tự động cấu hình: Phương pháp này thường được sử dụng khi một điểm cuối của đường ống

cũng chính là điểm đến của các gói tin IPv6, tức là áp dụng cho mô hình trạm trạm và router - trạm. Trong trường hợp này, địa chỉ IPv4 của trạm đích được tự động xác định trên địa chỉ đích IPv6 được đóng gói từ các gói tin IPv4.

Cấu hình đường ống: Được cấu hình khi đích đến của gói tin IPv6 không phải là điểm cuối của đường ống tới router. Trong trường hợp này, địa chỉ điểm cuối của đường ống được xác định thông qua địa chỉ của gói tin nguồn có trong gói tin gửi đi hoặc thông qua phép ánh xạ địa chỉ IPv4-IPv6.

Các giải pháp đường ống có thể bao gồm nhiều phương pháp khác nhau, tuỳ thuộc vào vị trí của hai đầu cuối:

Router đến Router: Các router IPv6/IPv4 liên nối với nhau trên nền IPv4 có thể gửi các gói tin IPv6 trong đường ống giữa chúng. Trong trường hợp này, đường ống chỉ bao gồm một đoạn trên đường đi giữa hai trạm.

Từ trạm đến router : Các trạm IPv6/IPv4 có thể gửi các gói tin IPv6 trong đường ống đến một router IPv6/IPv4 trung gian mà nó tới được thông qua cơ chế định tuyến của IPv4. Phương pháp đường ống này chỉ bao gồm đoạn đầu của đường đi nối hai trạm.

Từ trạm đến trạm : Các trạm IPv6/IPv4 được kết nối trên nền IPv4 có thể gửi các gói tin IPv6 trong đường ống giữa chúng. Đường ống này bao gồm toàn bộ đường đi giữa hai trạm.

Từ router đến trạm : Các router có thể gửi các gói tin IPv6 tới trạm đích cuối cùng (sử dụng IPv6/IPv4). Đường ống này chỉ bao gồm đoạn cuối của đường đi giữa hai trạm.

1.1.3 Cấu hình đường ống tự động 6over4

Phương pháp này sử dụng đường ống tự động ***IPv6 over IPv4*** sử dụng hạ tầng multicast có sẵn. Cơ chế thực hiện việc cấu hình tự động chủ yếu dựa trên khả năng sử dụng giao thức IPv6 Neighbor over IPv4, coi hạ tầng multicast có sẵn như một kết nối Ethernet ảo.

Phương thức này hầu như không được sử dụng do việc sử dụng hạ tầng multicast IPv4 tương đối phức tạp cũng như việc sử dụng các phương thức khác nhanh chóng và đơn giản hơn.

1.1.4 Cấu hình đường ống tự động sử dụng 6to4 relay router

Một phương thức cấu hình tự động khác được gọi với tên ***6to4***, trong đó một node mạng dual-stack tự động đóng gói các gói tin khi cần thiết và gửi chúng đi thông qua một router 6to4 mà không cần phải cấu hình thiết lập một đường ống cũng như điểm đầu cuối của đường ống.

Phương thức chuyển đổi này sử dụng địa chỉ /48 là con của TLA với tiếp đầu tố 2002::/16. Phương thức này cho phép người sử dụng kết nối IPv6 qua các thiết bị NAT với các bước cài đặt đơn giản. Người sử dụng chỉ cần chỉ ra một địa chỉ 6to4 router để thiết lập cấu hình.

1.1.5 Sử dụng các bộ chuyển đổi:

Khi mạng trục trở nên thuần IPv6, các lưu thông IPV4 còn lại vẫn có thể được xen vào bằng các bộ chuyển đổi header. Một bộ chuyển đổi đối xứng sẽ nhận các gói tin này và hướng chúng đến nút đích. Cơ chế này cũng tương đương với việc đánh địa chỉ IPv4 sang không gian địa chỉ IPv6.

1.2 Lựa chọn phương thức chuyển đổi cho mạng thử nghiệm

Dựa trên các phương pháp chuyển đổi giao thức trên, mạng thử nghiệm giao thức IPv6 sẽ được xây dựng dựa trên việc kết hợp các phương pháp nói trên như sau:

Các máy tram trong hệ thống sẽ sử dụng *IPv6 hoặc làn đôi IPv6/IPv4* (cơ chế thứ hai cho phép các máy này vẫn có khả năng truy nhập vào mạng IPv4 hiện tại)

Kết nối với mang quốc tế dựa trên các *phương thức đường ống* để có thể tận dụng các kết nối sẵn có của mạng VNN.

Các mang khác hoặc **các thuê bao** muốn kết nối vào mạng sẽ sử dụng:

hoặc kết nối IPv6,

hoặc bộ chuyển đổi địa chỉ nếu mạng đó đang sử dụng IPv4 và không muốn thay đổi địa chỉ.

hoặc sử dụng làn đôi IPv6/IPv4.

1.3 Kế hoạch chuyển đổi định tuyến từ IPv4 sang IPv6

Triển khai mạng IPv6 trên cơ sở từ mạng trục với yêu cầu thiết yếu đặt ra là phải đảm bảo việc truyền số liệu IPv6 ổn định trên nền mạng trục IPv4 hiện tại. Trên cơ sở đó, các phương pháp chủ yếu để triển khai mạng trục IPv6 trên mạng IPv4 như sau:

Thông qua các phương pháp đường ống IPv4

Thông qua các liên kết phân lớp 2 riêng biệt

Thông qua mạng trục MPLS IPv4

Sử dụng mạng trục Dual-stack .

Ngoài ra, trong giai đoạn đầu, để có thể triển khai IPv6 trong một môi trường IPv4, cần có các cơ chế chuyển đổi giao thức IPv4-IPv6 nhằm mục đích hỗ trợ chuyển đổi thông tin giữa các ứng dụng IPv4 và IPv6. Các cơ chế chuyển đổi giao thức chính có thể là:

NAT-PT (Network Address Translation – Protocol Translation)

TCP-UDP relay

BIS (Bump-in-the-Stack)

DSTM (Dual Stack Transition Mechanism)

SOCKS-Based Gateway.

Tích hợp giữa mạng IPv4 và IPv6 đòi hỏi phải có cơ chế chuyển đổi giao thức. Trong tương lai sẽ có những phần mềm hỗ trợ cơ chế NAT-PT, khi đó hai bộ định tuyến đặt tại hai nút Hà nội, Hồ chí Minh sẽ đóng vai trò 'Gateway' giữa 2 hệ thống giao thức.

Trên cơ sở mục tiêu kết nối với mạng IPv4, nhóm nghiên cứu khuyến nghị sử dụng 2 máy chủ mạng LAN có thêm nhiệm vụ hỗ trợ kết nối vào cả hai hệ thống mạng IPv4 và IPv6.

Như đã trình bày ở trên, các cơ chế chuyển đổi chính giữa các ứng dụng IPv4 và IPv6 có thể là:

NAT-PT (Network Address Translation – Protocol Translation)

TCP-UDP relay

BIS (Bump-in-the-Stack)

DSTM (Dual Stack Transition Mechanism)

SOCKS

Based Gateway.

Việc cấp địa chỉ được thực hiện tự động theo phương pháp cấu hình theo địa chỉ trên bộ định tuyến có trong LAN (Staless Auto-Configuration). Các dải địa chỉ cho các máy tại Hà nội và Tp Hồ Chí Minh như sau:

STT	Vị trí	Địa chỉ IPv6
1	IPv6 LAN Hà nội	3FFF:XXXX:0100::/40
2	IPv6 LAN Tp Hồ Chí Minh	3FFF:XXXX:0200::/40

Tại mạng LAN tại Hà nội và TP Hồ Chí Minh sẽ tiến hành thử nghiệm các dịch vụ như DNS, Web, FTP, Mail, Telnet, News, Chat, Directory, Multimedia trên nền IPv6. Ngoài ra, 2 máy chủ đó cũng đồng thời được sử dụng vào việc:

Thử nghiệm kết nối vào mạng IPv4

Triển khai các dịch vụ chuyển đổi IPv4/IPv6 như NAT-PT, TCP/UDP Relay giữa hai mạng.

1.4 Kế hoạch chuyển đổi nút mạng từ IPv4 sang IPv6

1.4.1 Cơ chế cấp phát địa chỉ trong không gian địa chỉ IPv6

Để quản lý không gian địa chỉ hiệu quả và hợp lý, các nhà thiết kế giao thức IPv6 đã đưa ra 2 cơ chế cấp phát địa chỉ như sau:

1.1.1.1 Cơ chế cấp phát chung:

Rút kinh nghiệm từ việc phân bổ địa chỉ của IPv4, các nhà thiết kế IPv6 đã xây dựng một cơ chế phân bổ địa chỉ hoàn toàn mở, nghĩa là nó không phụ thuộc vào giai đoạn ban đầu, hoàn toàn có thể thay đổi tuỳ thuộc vào những biến động trong tương lai về việc cấp phát và sử dụng địa chỉ cho các dịch vụ, các vùng khác nhau. Mặt khác, những người thiết kế IPv6 đã dự đoán trước những khả năng có thể phải sửa đổi một vài điểm như cấu trúc các loại địa chỉ, mở rộng một số loại địa chỉ ... trong tương lai. Điều này là hoàn toàn đúng đắn đối với một giao thức đang trong giai đoạn xây dựng và hoàn thiện.

Phân loại địa chỉ IPv6 không phải chỉ để cung cấp đầy đủ các dạng khuôn mẫu và dạng tiền tố của các loại địa chỉ khác nhau. Việc phân loại địa chỉ theo các dạng tiền tố một mặt cho phép các host nhận dạng ra các loại địa chỉ, mặt khác ứng với mỗi dạng địa chỉ sẽ có các cách xử lý khác nhau. Ví dụ với địa chỉ có dạng tiền tố **FE80::/16** host sẽ nhận dạng đó là địa chỉ link-local chỉ để kết nối các host trong cùng một mạng ...; hoặc với địa chỉ có dạng tiền tố **3FEE::/16** sẽ hiểu đó là địa chỉ của mạng 6Bone cung cấp. Mặt khác, với định dạng các địa chỉ theo tiền tố cũng cho phép đơn giản trong các bảng định tuyến vì khi đó các đầu vào của các bảng router sẽ là những tiền tố đơn giản, chiều dài của nó sẽ biến đổi từ 1 tới 128 bit. Chỉ có ngoại lệ duy nhất khi những địa chỉ đó liên quan là những địa chỉ đặc biệt. Các host và router thực sự phải nhận ra các địa chỉ "muticast", những địa chỉ này không thể được xử lý giống như các địa chỉ "unicast " và "anycast". Chúng cũng phải nhận ra các địa chỉ đặc biệt, tiêu biểu như địa chỉ "link local". Tài liệu cấu trúc cũng để dành tiền tố cho các địa chỉ địa lý cơ sở các địa chỉ tương thíc với NSAP (địa chỉ điểm truy nhập dịch vụ mạng: Network Service Access Point) và các địa chỉ tương thích IPX.3

Bảng cấp phát địa chỉ đã chỉ ra tỉ lệ sử dụng của các loại địa chỉ trong không gian địa chỉ. Phần chiếm không gian địa chỉ lớn nhất được sử dụng cho loại địa chỉ Global Unicast - dành cho các nhà cung cấp dịch vụ IPv6 - provider-based (phân theo nhà cung cấp) nhưng cũng chỉ chiếm một phần trăm của tổng không gian địa chỉ. Tất cả còn hơn 70% không gian còn

lại chưa được cấp phát, phần này có thể cung cấp những cơ hội phong phú cho việc cấp phát mới trong tương lai.

Cấp phát địa chỉ theo nhà cung cấp

Theo cấu trúc bảng phân bổ địa chỉ ở trên, một trong số những loại địa chỉ IPv6 quan trọng nhất là dạng địa chỉ Global Unicast với ý nghĩa phép định danh một giao diện trên mạng Internet (mạng IPv6) có tính duy nhất trên toàn cầu. Ý nghĩa loại địa chỉ này cũng giống như địa chỉ IPv4 sử dụng để định danh một host trong mạng Internet hiện nay. Không gian của dạng địa chỉ Global Unicast là rất lớn; để quản lý và phân bổ hợp lý các nhà thiết kế IPv6 đã đưa ra mô hình phân bổ địa chỉ theo cấp các nhà cung cấp dịch vụ Internet.

Dạng địa chỉ này gồm 3 bit tiền tố 010 theo sau bởi 5 thành phần mà mỗi thành phần này được quản lý bởi các nhà cung cấp dịch vụ theo các cấp độ khác nhau. Tuỳ theo việc phân bổ địa chỉ các thành phần này có một chiều dài biến đổi - điều này một lần nữa cho thấy tính "động" trong việc cấp phát và quản lý địa chỉ IPv6.

Bảng 1: Cấu trúc địa chỉ IPv6 dạng Global Unicast

3	**n bit**	**m bit**	**O bit**	**p bit**	**125-m-n-o-p bit**
010	ID đăng ký	ID của nhà cung cấp	ID của thuê bao	ID của mạng con	ID của giao tiếp

Thành phần đầu tiên là ID của các nhà cung cấp dịch vụ hàng đầu (Top Level "registry"). Cũng giống như IPv4, có một số các tổ chức chính quản lý việc cấp phát địa chỉ IPv6 có nhiệm vụ cấp phát các giá trị TLA ID đầu tiên. Cụ thể các tổ chức này như sau:

Khu vực Bắc Mỹ là Internet NIC (Network Information Center), tổ chức này điều khiển bởi NSI dưới một hợp đồng với U.S National Science Foundation.

Khu vực châu Âu là NCC (Network Coordinoction Center) của RIPE (hiệp hội mạng IP châu Âu).

Khu vực châu Á và Thái Bình Dương là tổ chức APINC.

Ngoài ra còn có một tổ chức chung có thể cấp phát địa chỉ cho các khu vực khác nhau là IANA.

Các nhà cung cấp dịch vụ Internet IPv6 phải có một "provides ID" (nhận dạng nhà cung cấp) từ những đăng ký trên. Theo kế hoạch cấp phát địa chỉ "Provider ID" là một số 16 bit. 8 bit tiếp theo sẽ được cho bằng 0 trong giai đoạn đầu – 8 bits này chưa sử dụng, được để dành

cho các mở rộng tương lai. Chi tiết về việc quản lý và phân bổ địa chỉ Global Unicast theo các cấp độ nhà cung cấp sẽ được trình bày trong phần Cấu trúc dạng địa chỉ Global Unicast.

Trong cấu trúc hiện tại, những điểm đăng ký chính được bổ xung bởi một số lớn các điểm đăng ký vùng hoặc quốc gia ví dụ French NIC quản lý bởi INRIA cho các mạng của Pháp. Những điểm đăng ký này sẽ không được nhận dạng bằng một số đăng ký. Thay vào đó họ sẽ nhận được phạm vi nhận dạng của các nhà cung cấp từ các cơ sở đăng ký chính.

Với cấu trúc dạng địa chỉ mới này cho phép các khách hàng lớn có thể có được các định danh ngắn hơn, và điều đó sẽ cho họ khả năng thêm vào các lớp mạng mới trong phân tầng mạng con của họ. Thực tế các khách hàng lớn còn có thể đòi được chấp nhận như nhà cung cấp của chính họ, lấy được ID nhà cung cấp từ các điểm đăng ký mà không phải lệ thuộc vào nhà cung cấp dịch vụ Internet IS

1.1.1.2 Phương pháp gán địa chỉ IPv6

Theo đặc tả của giao thức IPv6, tất cả các loại địa chỉ IPv6 được gán cho các giao diện, không gán cho các nodes (khác với IPv4). Một địa chỉ IPv6 loại Unicast (gọi tắt là địa chỉ Unicast) được gán cho một giao diện đơn. Vì mỗi giao diện thuộc về một node đơn do vậy, mỗi địa chỉ Unicast định danh một giao diện sẽ định danh một node.

Một giao diện đơn có thể được gán nhiều loại địa chỉ IPv6 (cho phép cả 3 dạng địa chỉ đồng thời Unicast, Anycast, Multicast). Nhưng nhất thiết một giao diện phải được gán một địa chỉ IPv6 dạng Unicast link-local. Các nhóm địa chỉ của dạng địa chỉ Unicast sẽ được trình bày ở phần sau. Để thực hiện các kết nối Point - to - point giữa các giao diện người ta thường gán các địa chỉ dạng Unicast link-local cho các giao diện thực hiện kết nối.

Đồng thời, IPv6 còn cho phép một địa chỉ unicast hoặc một nhóm địa chỉ unicast sử dụng để định danh một nhóm các giao diện. Với phương thức gán địa chỉ này, một nhóm giao diện đó được hiểu như là một giao diện trong tầng IP.

Theo thiết kế của IPv6, một host có thể định danh bởi các địa chỉ sau:

Một địa chỉ link-local cho mỗi giao diện gắn với host đó

Một địa chỉ Unicast được cung cấp bởi các nhà cung cấp dịch vụ

Một địa chỉ loopback

Một địa chỉ Multicast, mà host đó là thành viên trong nhóm có địa chỉ Multicast đó.

Một router nếu hỗ trợ IPv6 sẽ nhận biết được tất cả các loại địa chỉ mà host chấp nhận kể trên, ngoài ra nó còn có thể được gán các loại địa chỉ như sau:

Tất cả các địa chỉ Multicast được gán trên Router

Tất cả các địa chỉ Anycast được cấu hình trên Router

Tất cả các địa chỉ Multicast của về các nhóm thuộc về router quản lý.

1.4.2 Kế thừa địa chỉ IPv4

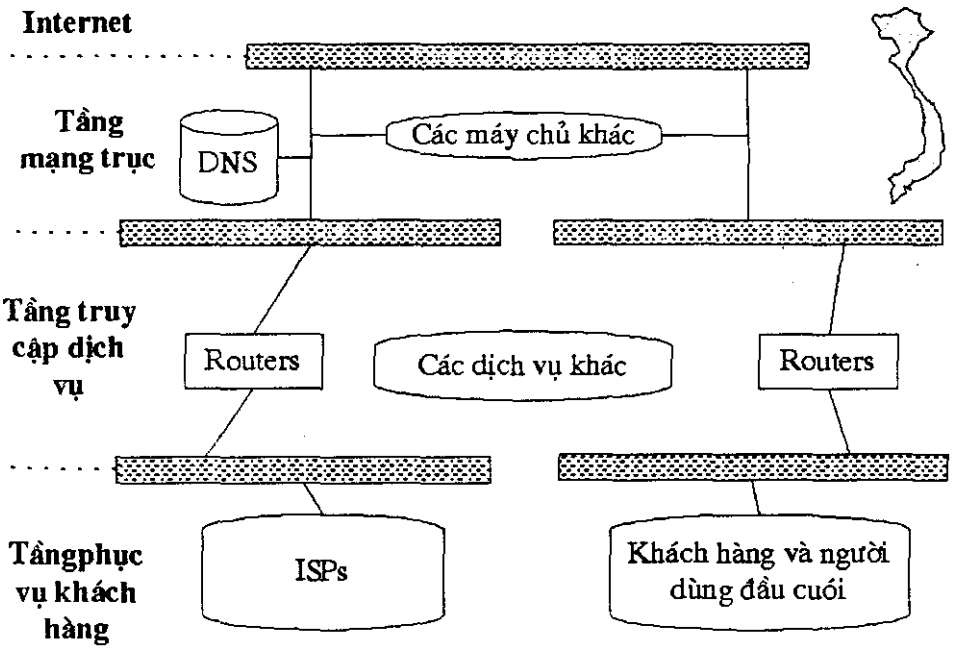
Do mạng lưới IPv4 của ta đã được xây dựng và đang hoạt động nên việc sử dụng kế thừa các phân hoạch sử dụng IPv4 là một yếu tố quan trọng tạo nên tính khả thi của phương án chuyển đổi. Hơn nữa việc chuyển đổi địa chỉ từ IPv4 sang IPv6 là một quá trình lâu dài vì ảnh hưởng đến toàn bộ mạng lưới và dịch vụ. Việc ứng dụng phương thức nào là tuỳ ở từng hoàn cảnh cụ thể, do các đặc điểm, ưu nhược điểm của từng phương thức như đã nêu. Cụ thể đối với mạng lưới của mạng trục quốc gia VNN, ta có thể thấy các vấn đề sau :

VDC là một nhà cung cấp dịch vụ Internet chính của Việt nam (IAP và ISP). Cũng như một ISP khác, hệ thống mạng lưới của VDC có thể được chia làm 3 vùng chính:

Mạng trung tâm - Core Network

Các kết nối của các ISP khác (như Netnam, FPT ...)

Các kết nối của các khách hàng



Hình 1 - Các lớp cần quy hoạch cho mạng IPv6

Để triển khai mạng IPv6, các vấn đề cần giải quyết đối với mỗi vùng này bao gồm:

Qui hoạch và cấp phát không gian địa chỉ IPv6 cho mỗi vùng

Kiến trúc lại các hệ thống thiết bị cho có khả năng hỗ trợ IPv6

Đăng ký các site IPv6

Cài đặt DNS server hỗ trợ IPv6.

1.4.3 Triển khai mạng IPv6 đối với mạng trung tâm (core) :

ISP cần phải xác định có nên cài đặt riêng biệt các router/host theo cơ chế dual-stack hay chỉ là những node thuần IPv6. Quyết định này dựa trên các kết nối tới mạng trung tâm; Các phương thức định tuyến cần được cài đặt để sao cho các gói tin IPv4 được định tuyến trên nền hạ tầng mạng IPv4; còn các gói tin IPv6 được định tuyến trên nền hạ tầng mạng IPv6 mới.

Hiện nay do mạng IPv6 mới chỉ phát triển rộng ở trên phạm vi thử nghiệm nên thực tế nhu cầu đối với các kết nối thuần IPv6 là chưa cao. Do đó sẽ tiết kiệm và hiệu quả hơn nếu sử dụng tối đa khả năng cung cấp song song dịch vụ trên cả IPv4 và IPv6, có nghĩa là đối với các dịch vụ cung cấp ở mạng trục thì việc sử dụng các cơ chế song song IPv4/IPv6 là cho hiệu quả tối đa.

Tuy vậy trong thực tế cũng có thể có các mạng mới có khả năng cung cấp dịch vụ thuần IPv6, ví dụ các mạng lưới phục vụ các dịch vụ di động thế hệ mới, các mạng cung cấp dịch vụ mạng thuần IPv6 như mạng DNS IPv6, mạng thử nghiệm IPv6 ... thì có thể thiết lập ngay dưới dạng thuần tuý IPv6. Lúc này mạng được xây dựng sẽ chỉ giao tiếp được với các mạng lưới khác thông qua các kết nối thuần IPv6 mà thôi.

Với các thiết bị chuyển mạch nằm giữa các miền giới hạn IPv4/IPv6: Sau khi giai đoạn các router chạy chế độ dual-stack ổn định. Các ISP có thể cấu hình các router trong mạng core là những router chạy dual-stack để định tuyến cả IPv6 và IPv4.

Giai đoạn tiếp tiếp theo là thực hiện các kết nối tới mạng IPv6 toàn cầu. Có thể làm các kết nối này thông qua các phương thức kết nối trực tiếp vào một mạng IPv6 toàn cầu (như mạng thử nghiệm 6Bone) hoặc thông qua cơ chế tunneling. Nếu mạng core hỗ trợ IPv6 và các ISP khác cũng hỗ trợ IPv6 thì có thể cấu hình các kết nối trực tiếp IPv6 mà không cần thông qua tunnel hoặc dual-stack

Đồng thời các ISP cũng phải quyết định sử dụng một hoặc một vài các router nằm ở "đường biên" trong quá trình chuyển đổi từ mạng IPv4 sang mạng IPv6. Khái niệm "đường biên" này

được hiểu như là các router là các gateway đóng vai trò là điểm chuyển tiếp giữa mạng IPv4 và mạng IPv6.

1.4.4 Triển khai mạng IPv6 đối với mạng truy nhập của khách hàng

Các khách hàng của mỗi ISP có thể truy nhập vào mạng qua đường dial-up (các khách hàng gián tiếp) hoặc qua đường leased-line (các khách hàng trực tiếp). Do vậy có các vấn đề cần giải quyết để triển khai mạng IPv6 như sau:

Cần phải nâng cấp các router để các router này hỗ trợ dual stack. Do vậy đảm bảo các các khách hàng IPv4 và khách hàng IPv6 đều các trả năng truy nhập vào mạng.

Hoặc cài đặt các router IPv4 và IPv6 riêng rẽ nhau. Sau đó thực hiện phân tách các khách hàng thuộc mạng IPv4 sẽ truy nhập qua router IPv4 cũ; còn các khách hàng mới sẽ truy nhập qua router IPv6. Những access router này phải hỗ trợ các kết nối tới mạng IPv6 toàn cầu. Nếu mạng core không hỗ trợ IPv6 cần phải cài đặt các cơ chế chuyển đổi (dual stack hay tunneling) trên các router IPv6.

Đối với các khách hàng là những site IPv6, các ISP cần phải cài đặt các cơ chế chuyển đổi để hỗ trợ khách hàng có thể truy nhập vào các node IPv4; có thể thông qua các cơ chế như NAT.

Như vậy đối với mạng khách hàng thì có thể ứng dụng các biến thể của tunnelling, NAT để cung cấp IPv6 trong quá trình chuyển tiếp. Như đã nghiên cứu, việc chuyển đổi dần sang chế độ native IPv6 sẽ được thực hiện tương đối đơn giản khi các thiết bị và phần mềm có khả năng hỗ trợ hoàn hảo.

Một giải pháp nữa không kém phần quan trọng trong quá trình chuyển đổi là việc kết nối với 6BONE. Thực chất việc kết nối này là cung cấp các kết nối thử nghiệm đối với IPv6 chứ không phải là các kết nối bền vững có thể sử dụng lâu dài cho việc cung cấp dịch vụ sau này (vì nó phá vỡ kiến trúc phân cấp địa chỉ IPv6 theo nhà cung cấp, và hạn chế các khả năng cũng như số lượng địa chỉ IPv6 có thể cấp phát). Tuy nhiên việc kết nối với 6BONE lại là một việc làm hết sức cần thiết, đặc biệt là đối với nhà cung cấp dịch vụ kết nối và dịch vụ như VDC, do :

6BONE cung cấp khả năng thử nghiệm IPv6 trên phạm vi toàn cầu

Là một yêu cầu bắt buộc nếu muốn tham gia vào các công cuộc nghiên cứu phát triển IPv6

Là yêu cầu bắt buộc để có thể được cấp phát các sub-TLA đầu tiên từ RIR

1.4.5 Triển khai địa chỉ IPv6 tại Việt Nam

Để có thể triển khai được sử dụng Internet IPv6 tại Việt nam, nhóm nghiên cứu đề xuất các bước thực hiện theo trình tự sau:

Bước 1 :

Muốn triển khai địa chỉ IPv6 trước hết cần có địa chỉ IPv6. Muốn được cấp địa chỉ IPv6, chúng ta cần phải tham gia thử nghiệm 6bone ít nhất 6 tháng (xem phần giới thiệu về phân cấp quản lý địa chỉ IPv6). Việc kết nối với 6BONE có thể được thực hiện thông qua một trong những giải pháp sau đây :

Kết nối với 6BONE thông qua kết nối transit do một đối tác cung cấp đường truyền trực tiếp nào đó. VDC cần thương lượng với các đối tác cung cấp đường truyền dữ liệu quốc tế để tìm hiểu khả năng thông qua kết nối quốc tế đó để tham gia vào 6BONE. Điều kiện là đối tác phải có kết nối sẵn với 6BONE, và tương thích về thiết bị

Kết nối với 6BONE thông qua các relay được cung cấp bởi đối tác, hoặc các relay công cộng (như của Microsoft, Cisco). Phương pháp này đơn giản nhưng chỉ cung cấp khả năng truy nhập vào 6BONE chứ không đủ năng lực và điều kiện để được chấp nhận như một site cung cấp dịch vụ IPv6, và do đó không đủ điều kiện do APNIC yêu cầu.

Bước 2 :

Sau thời gian thử nghiệm với kết quả khả quan, xúc tiến việc xin cấp các sub-TLA đầu tiên cho Việt nam. Việc phân bổ các sub-TLA này được thực hiện theo phần II ở trên.

Ta đã đề cập đến việc phân chia dải địa chỉ theo các ranh giới bit do APNIC quy định, cung cấp được (với sub-TLA đầu tiên) là 8192 networks, với 65536 giao diện trên một network như vậy. Tuy nhiên trong 13 bit sử dụng cho network nói trên ta nên phân chia cụ thể hơn theo các nhà cung cấp, cụ thể địa chỉ được phân cấp chủ yếu cho các nhà cung cấp dịch vụ cỡ lớn (như các ISP, IXP, ICP...). Việc phân hoạch tiếp theo được thực hiện trên ranh giới mạng con thuộc đơn vị đó quản lý, thực hiện theo phương pháp tương tự như phương pháp đã được minh hoạ ở trên.

Bước 3 :

Sau khi mạng trục đã hỗ trợ IPv6 thì có thể cung cấp các dịch vụ kết nối IPv6 thuần, dịch vụ kết nối qua tunnelling, qua NAT... Một trong các dịch vụ đầu tiên mà nhà cung cấp dịch vụ IPv6 phải cung cấp là dịch vụ tên miền IPv6 (DNS). Do đó nhà cung cấp phải xây dựng trước các máy chủ cung cấp dịch vụ này trước khi đưa ra dịch vụ. Việc xây dựng hệ thống này đã được mô tả trong phần thử nghiệm.

1.5 Kế hoạch định cỡ mạng IP v6

1.5.1 Định cỡ kiến trúc mạng IPv6

Mạng thử nghiệm IPv6 được thiết lập trên nền mạng IPv4, tức là các thành phần lưu thông của mạng IPv6 được định tuyến thông qua các bộ định tuyến cửa khẩu của mạng IPv4 trước khi chuyển tiếp đến mạng IPv6 quốc tế. Vì trong giai đoạn 2002-2003, mạng IPv6 tạm thời chỉ dừng lại ở vai trò là một mạng thử nghiệm thế hệ mới, do đó chưa cần thiết đầu tư các thiết bị mạng mới với cấu hình cao. Tuỳ theo khả năng mở rộng về sau, kết hợp với lộ trình phát triển mạng lưới Internet quốc gia nói chung và mạng dịch vụ thế hệ mới IPv6 nói riêng, các thiết bị phục vụ cho mạng IPv6 sẽ được điều chuyển hoặc nâng cấp trong tương lai.

Trước thực tế nhu cầu sử dụng dịch vụ Internet của xã hội đang ngày càng gia tăng, trong thời gian qua, mạng lưới của VNN liên tục được mở thêm kênh đi quốc tế tới hàng chục Mb/s. Mặc khác, đường trục Internet quốc gia cũng được nâng cấp lên tới trên dưới 300Mbps. Tới thời điểm này, tổng dụng lượng kênh Internet đi quốc tế của Việt nam đạt tới trên dưới 300Mbps, cao hơn nhiều so với các nước trong khu vực và xấp xỉ bằng Thái Lan.

Giải pháp chuyển đổi hệ thống dần từ giao thức IPv4 sang IPv6 được bắt đầu từ mạng nhánh, tiến tới mạng trục. Phương án này cho phép tiết kiệm được các chi phí đầu tư trong khi vẫn nhắm vào được nhu cầu ứng dụng trước mắt mà không cần thiết phải có sự nâng cấp toàn bộ hệ thống sang sử dụng giao thức IPv6 trong giai đoạn này. Trong quá trình chuyển đổi, các nhà hoạch định hệ thống có một môi trường thử nghiệm lý tưởng để có được các phân tích, đánh giá cần thiết cho việc vạch ra những hướng đi vững chắc của hệ thống mạng thông tin Việt nam.

Hệ thống thử nghiệm là hệ thống thu nhỏ của 1 hệ thống mạng quốc gia tổng thể trong tương lai có khả năng đáp ứng được sự phát triển nhanh chóng của Internet toàn cầu với việc hỗ trợ các công nghệ mới, sự gia tăng nhảy vọt về số lượng người sử dụng, các ứng dụng và dịch vụ trên mạng. Trên cơ sở đó, mạng IPv6 thử nghiệm cần đảm bảo được các khả năng sau:

Khả năng tích hợp với các hệ thống khác:

Mạng IPv6 có khả năng kết nối với mạng VNN4 hiện có, kết nối với hệ thống mạng quốc tế 6BONE và các mạng IPv6 khác trên thế giới(nếu có thể). Đảm bảo khả năng song song cùng tồn tại hai hệ thống IPv4 và IPv6 trong thời gian trước mắt.

Khả năng cung cấp dịch vụ

Cung cấp các dịch vụ kết nối thử nghiệm IPv6, dịch vụ giá trị gia tăng cho khách hàng:

- ✓ Trước mắt, triển khai các dịch vụ phổ biến như Web, FTP, e-mail,...
- ✓ Từng bước triển khai các dịch vụ băng thông rộng và chất lượng dịch vụ cao (ví dụ dịch vụ Video Conference,...)
- ✓ Có khả năng cung cấp khả năng truy cập các dịch vụ trên mạng IPv6 cho người sử dụng trên hệ thống IPv4 qua các phương thức chuyển đổi tự động và thủ công.

Khả Năng Mở Rộng và Nâng Cấp

Mạng có cấu trúc mở, độ tin cậy cao. Các thiết bị có tính mở, năng lực và đặc tính kỹ thuật phù hợp với dịch vụ thử nghiệm. Có khả năng thay thế, nâng cấp khi cần thiết.

Hỗ trợ việc nâng cấp phần mềm để đáp ứng sự phát triển về công nghệ, cho phép thử nghiệm các dịch vụ mới ra đời trong tương lai. Hỗ trợ các tiêu chuẩn kết nối quốc tế chung, không phụ thuộc vào nhà sản xuất cụ thể.

Đảm hiệu năng của hệ thống

Có độ linh hoạt và tính sẵn sàng phù hợp với quy mô thử nghiệm vừa và nhỏ. Tập trung thử nghiệm tại hai nút mạng Hà nội và Hồ chí Minh nhằm nâng cao hiệu quả sử dụng mạng lưới cũng như các chí phí khai thác, bảo dưỡng. Đảm bảo khả năng mở rộng bao phủ toàn quốc phù hợp với chiến lược phát triển trong giai đoạn tới.

Tạo nên một môi trường thử nghiệm cho việc triển khai dịch vụ, công nghệ mới - qua đó rút ra được những kinh nghiệm cần thiết cho việc xây dựng hệ thống mạng quốc gia tổng thể cho tương lai.

Đảm bảo an ninh hệ thống.

Đảm bảo độ tin cậy của các thông tin được trao đổi giữa các nút mạng thử nghiệm. Có khả năng bảo mật thông tin trao đổi giữa các nút mạng khi cần thiết.

1.5.2 Kiến Trúc hệ thống

Mạng thử nghiệm giao thức mới IPv6 sẽ được triển khai trong khuôn khổ một liên mạng khai thác kết nối toàn quốc. Trước mắt hệ thống sẽ được xây dựng trên nền mạng IPv4 hiện có, từng bước tiến hành chuyển đổi hệ thống IPv4 hiện tại sang IPv6 (*Native IPv6*), phù hợp với các nghiên cứu và thử nghiệm chung của các nước và tổ chức khác trong giai đoạn chuyển tiếp.

Giao Tiếp với Mạng 6BONE

Nút mạng Hà nội được kết nối với mạng thử nghiệm 6BONE quốc tế thông qua kết nối IPv4 hiện có, sử dụng phương án đường ống (*Tunnel*). Sau quá trình thử nghiệm và chạy IPv6, nút mạng này có thể được đăng ký để kết nối với các nút mạng IPv6 khác để trở thành nút mạng IPv6 chính thức.

Giao Tiếp với Mạng IPv4 hiện có.

Để đảm bảo cho việc song song cùng tồn tại hai hệ thống IPv4 và IPv6, mạng thử nghiệm IPv6 sẽ được kết nối với mạng VNN IPv4 hiện tại. Hệ thống phải có khả năng hỗ trợ cơ chế chuyển đổi giao thức giữa IPv4 và IPv6.

Giao tiếp với mạng LAN IPv6

Hai mạng LAN chạy IPv6 đặt tại 2 nút ban đầu là Hà Nội và Hồ Chí Minh. Hai mạng LAN này được kết nối thông qua mạng trục IPv4 hiện tại, sử dụng phương án đường ống (Tunnel) có băng thông tương đương 2xE1. Hai Router chạy dual-mode IPv4/IPv6 đặt tại hai đầu đảm bảo việc kết nối hai mạng IPv6 trên nền mạng IPv4.

Dịch vụ dial-up IPv6.

Tại nút mạng hai đầu Hà nội, Hồ Chí Minh, các Router với khả năng của Access Server sẽ cung cấp dịch vụ Dial-up IPv6 thử nghiệm cho khách hàng.

1.5.3 Định cỡ thiết bị mạng IPv6

Các thiết bị mạng dùng cho mạng thử nghiệm IPv6 bao gồm các bộ định tuyến (*router*), hệ thống chuyển mạch (*switch*), các máy chủ dịch vụ (*servers*) và các máy trạm thử nghiệm dịch vụ (*workstation*). Các thiết bị này vừa đảm bảo được yêu cầu tối thiểu là xây dựng một hệ thống mạng thử nghiệm trong phạm vi quốc gia nhưng cũng cần đảm bảo hội tụ được các đặc tính cho phép mở rộng phạm vi thử nghiệm thành một mạng IPv6 đủ khả năng cung cấp các dịch vụ trên nền mạng IPv6 cho các đối tượng khách hàng trên lãnh thổ Việt nam có nhu cầu sử dụng.

1.5.3.1 Bộ định tuyến

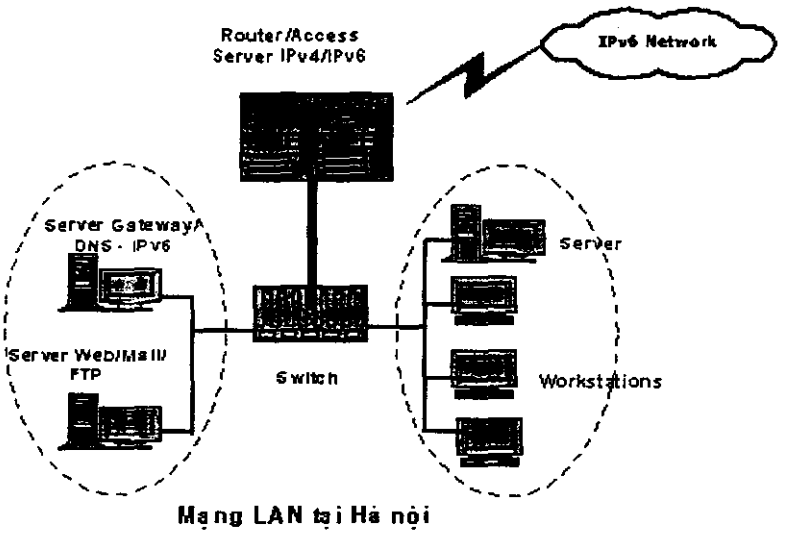
Với nhiệm vụ định tuyến các lưu thông trong mạng IPV6 qua các bộ định tuyến cửa khẩu của mạng IPV4, bộ định tuyến cho mạng IPV6 cần đảm bảo được các đặc tính của một hệ định tuyến mạng trục và hệ thống truy cập gián tiếp. Chức năng định tuyến đóng vai trò chuyển tiếp chính các lưu thông mạng trục giữa 2 đầu nút Bắc Nam và định tuyến di quốc tế. Chức năng truy cập gián tiếp được tích hợp trong bộ định tuyến để cung cấp các dịch vụ truy cập Internet từ xa qua mạng điện thoại.

Để xác định được năng lực của bộ định tuyến trên cơ sở căn cứ vào:

- ***Lưu thông mạng trục, quốc tế***
- ***Lưu thông mạng LAN tại mỗi đầu nút***
- ***Lưu thông cho các người dùng truy cập gián tiếp***

Ví dụ xét tại đầu nút Hà nội:

- Kênh kết nối quốc tế IPv6 Tunnel lên mạng 6BONE với băng thông 01xE1
- Đảm bảo đồng thời 8 kết nối (connections) cho người dùng đầu cuối
- Hỗ trợ 500 đến 1000 người dùng truy cập gián tiếp vào mạng IPv6



Hình 2 - Kiến trúc mạng LAN IPv6 tại Hà nội

Mặt khác, các dịch vụ chủ yếu được khai thác thử nghiệm trên mạng ngoài các ứng dụng truyền thống như Web, Mail, FTP còn bao gồm một số các ứng dụng băng thông rộng như VideoConference, MPEG... Theo trung bình thống kê, các traffic diễn ra trên mạng IP Internet mà dịch vụ Web-based, Mail (POP3 & SMTP) và dịch vụ khác như telnet, ftp, ...vv, lần lượt chiếm các tỷ lệ chiếm 70%, 20% và 10%. Tuy nhiên, trong trường hợp thử nghiệm các dịch vụ băng rộng, traffic cho các dịch vụ đó sẽ chiếm đến 80% lưu thông chính của mạng. Trong trường hợp mạng LAN có tốc độ 100Mbps, có thể hiểu traffic cho video luôn chiếm tới 80Mbps và traffic cho các dịch vụ truyền thống là 20% tương đương với 20Mbps.

Dịch vụ Mail được xếp vào loại dịch vụ mà tính kết nối là có trạng thái - stateful, băng thông dùng cho nó thường cao hơn mọi dịch vụ không trạng thái.

Vậy lưu lượng bit/giây (bps) dành cho hình thức truy cập gián tiếp sẽ là :

Dgt = (Pvideo+ Pkhác) x (8 bits/byte)

Trong đó :

Pweb=Pvideo x 80% x 2048 là lưu lượng do dịch vụ Video chiếm.

Pkhác=Pgt x 20% x 1024 là lưu lượng do dịch vụ truyền thống khác chiếm.

Pgt là số kết nối dành cho thuê bao gián tiếp.

Áp dụng quy tắc Clos cho xác định tốc độ chuyển mạch, không xung đột, tắc nghẽn

- Tốc độ chuyển mạch của bộ định tuyến vào khoảng 25 đến 35 Mbps hay hiệu năng chuyển tiếp gói tin vào khoảng 50 - 70 Mpps (các gói tin ở đây có kích thước chuẩn là 64Kbyte)

Chức năng định tuyến:

Hệ thống cần có kiến trúc đã xử lý, hỗ trợ các xử lý chính như: Truyền nhận các thông tin cập nhật về định tuyến của tất cả các giao thức định tuyến được cài đặt trên hệ thống. Quản lý chặt chẽ các thông tin định tuyến và trạng thái hoạt động môi trường của hệ thống.

Hệ thống cần có chế độ bảo mật tường lửa với truy nhập Internet/Intranet.

Chức năng truy cập gián tiếp:

Hỗ trợ truy cập gián tiếp có khả năng quản trị thiết bị thông qua các hệ thống giám sát trạng thái hoạt động như: thủ tục truyền thông, hiệu suất sử dụng, trạng thái kết nối modem với khách hàng,...v..v

Khả năng hỗ trợ tối đa các chuẩn kết nối thoại cho các loại modem phổ thông cho khách hàng đầu cuối.

Mô hình kết nối tại đầu nút Hà nội và TP Hồ Chí Minh về cơ bản là giống nhau. Riêng nút Hà nội còn có thêm 02 máy chủ dịch vụ kết nối thêm vào LAN. Do vậy, về cơ bản, 02 bộ định tuyến được trang bị giống nhau.

1.5.3.2 Bộ chuyển mạch

Bộ chuyển mạch có chức năng chuyển tiếp các lưu thông vào và ra tại các mạng LAN đặt tại 2 nút mạng chính. Cũng giống như bộ định tuyến, phần lớn toàn bộ các traffic đều được chuyển tiếp qua đây.

Cũng theo quy tắc Clos về đảm bảo chống tắc nghẽn băng thông chuyển mạch tại LAN, tốc độ chuyển mạch của bộ chuyển mạch tối thiểu cũng phải bằng được tốc độ chuyển mạch của bộ định tuyến và còn có khả năng mở rộng đến chuyển mạch Gigabit. Với các tiêu chí đó, bộ chuyển mạch cần đảm bảo các thông số:

- Tốc độ chuyển mạch tối thiểu 35Mbps và có thể mở rộng đến 8Gbps.
- Hiệu năng chuyển tiếp thông tin từ 70Kpps đến 7Mpps (tính theo kích thước gói tin 64kbps)
- Hỗ trợ các công nghệ FastEtherChannel, GigaEtherChannel phép tạo nên các kết nối tốc độ cao tới 4Gbps giữa các Switch, kết nối tới Router, cũng như tới các máy chủ.

1.5.3.3 Máy chủ

Có tổng cộng 04 máy chủ trên toàn mạng. Với mục tiêu đảm bảo cho số lượng người dùng đầu cuối truy cập gián tiếp khoảng từ 500 đến 1000 người, 04 máy chủ đó cần đảm bảo các tiêu trí:

- Hỗ trợ đa truy nhập, phân tải truy nhập.
- Hỗ trợ đa xử lý, phân tải đa xử lý.

Đối với các máy chủ gateway/DNS-IPv6 và máy chủ web/mail/FTP thì số lượng kết nối truy nhập sẽ biến thiên, phụ thuộc nhiều vào các truy nhập gián tiếp của người dùng. Tuy nhiên trong môi trường mạng LAN thì chính là nơi các dịch vụ băng thông rộng được thử nghiệm do vậy các kết nối ở đây đều là FastEthernet 100Mbps.

1.5.3.4 Định cỡ, lựa chọn hệ điều hành máy chủ

Hầu hết các hệ điều hành thông dụng hiện nay như Windows, Linux, Unix,... đều đã hỗ trợ các kết nối IPv6. Dưới đây, nhóm nghiên cứu phân tích, đánh giá và so sánh các ưu, khuyết của các hệ điều hành thông dụng, từ đó đưa ra được hệ điều hành phù hợp cho các máy chủ thử nghiệm.

Hệ điều hành UNIX

Hệ điều hành (HĐH) UNIX được xây dựng từ đầu những năm 70 và được sử dụng trong các hệ máy tính lớn. Tính đến thời điểm hiện tại, so với các hệ điều hành khác, UNIX là một trong những hệ thống có tính bảo mật cao vì đã trải qua thời gian dài xây dựng, khắc phục và bù lấp những lỗ hổng bảo mật. Hiện nay tồn tại nhiều dòng UNIX khác nhau như: HP UNIX, IBM AIX, Novell UNIXWARE....

Chúng ta có thể điểm qua những đặc điểm nổi bật của HĐH UNIX như:

- Là một hệ xử lý đa luồng, thích hợp cho các máy chủ lớn với một hệ thống lớn các trạm làm việc.
- Khả năng bảo mật cao vì các tính năng phân quyền, bảo mật và truyền tin nằm trong hạt nhân của HĐH UNIX luôn được bổ sung và khắc phục những lỗ hổng.
- Tính ổn định của UNIX cao.
- Hỗ trợ giao thức IPv6 trên nhiều dòng như: IBM(AIX 4.3); BSDI(BSD/OS 4.0); COMPAQ(Tru64 UNIX5.1); FreeBSD(FreeBSD 4.0); HP(HP-Ux 11i)...

Tuy nhiên, có những điểm hạn chế:

- UNIX chỉ thực sự phát huy sức mạnh trong các hệ thống lớn.
- Giá thành đầu tư cho UNIX tương đối lớn, đòi hỏi sự đồng bộ ở các cấu hình thiết bị phần cứng chuyên dụng, đắt tiền.
- Vận hành UNIX khá phức tạp, đòi hỏi người vận hành phải có kiến thức chuyên môn trình độ cao.

Hệ điều hành Linux

Linux ra đời dựa trên những tính năng cơ bản của UNIX, được thiết kế cho nền máy PC và tận dụng kiến trúc của máy tính với chíp Intel để có được hệ thống hoạt động với hiệu suất cao như UNIX. Linux là HĐH mã nguồn mở, do đó có nhiều hãng phát triển với các phiên bản Linux khác nhau như: RedHAT, Trubo, SuSE,... Lí do càng ngày càng nhiều người sử dụng Linux:

- Môi trường làm việc Linux cho phép tìm hiểu được UNIX, đây thực sự là môi trường thử nghiệm tuyệt vời với giá cả hợp lý và gần như là miễn phí hoàn toàn.
- Linux cho phép tận dụng gần như hết hiệu suất của các thiết bị phần cứng với cơ chế quản lý mạnh và có tính ổn định cao.
- Linux là HĐH cho phép cung cấp các dịch vụ Internet như Web, Mail, FTP... với chất lượng dịch vụ đảm bảo và độ tin cậy cao.
- Linux kernel 2.2.x trở đi bắt đầu hỗ trợ IPv6.

Hệ điều hành Windows

HĐH Windows được phát triển bởi công ty Microsoft nổi tiếng. Hiện nay, tại Việt nam, Windows được sử dụng khá phổ biến . Các dòng sản phẩm cho người dùng đầu cuối có chức năng HĐH mạng như WindowsNT, Windows 2000,... thường được lựa chọn cho các ứng dụng đầu cuối của người sử dụng. Sử dụng Windows cũng có những ưu nhược điểm như:

- HĐH Windows hỗ trợ phần lớn các giao thức mạng phổ dụng.
- Giao diên người dùng thân thiện trong cài đặt và sử dụng.
- Có khả năng kết nối với HĐH khác.
- Chi phí thấp hơn so với UNIX nhưng độ bảo mật thấp hơn so với UNIX.

Microsoft đã phát triển các package hỗ trợ IPv6 cho các HĐH: Windows 95/98/NT; Windows 2000/XP;Windows 2003.

Lựa chọn hệ điều hành Linux cho các máy chủ

Trong giai đoạn thử nghiệm với mục đích tiết kiệm chi phí và tăng cường khả năng phát triển hệ thống, giải pháp sử dụng đồng thời một số phần mềm miễn phí và mã nguồn mở vừa đảm bảo được tính kinh tế và khả năng mở rộng của hệ thống thử nghiệm. Trên thực tế, nhiều nhóm nghiên cứu tại các trung tâm nghiên cứu và trường đại học trên thế giới, đặc biệt trong các dự án thử nghiệm cũng lựa chọn giải pháp sử dụng Linux. Với vai trò là HĐH giống UNIX, hệ thống thử nghiệm sẽ có được những ưu điểm:

- Khả năng đa luồng và đa xử lý cho hệ thống lớn.
- Tính ổn định, bảo mật kết hợp với phân quyền người sử dụng mức cao.
- Có tính tương thích cao với các hệ thống khác, có khả năng nâng cấp theo yêu cầu sử dụng.
- Tiết kiệm 10-20% chi phí dự án.

Với hệ thống thử nghiệm, việc sử dụng HĐH mã nguồn mở cho phép nhóm nghiên cứu có khả năng phát triển HĐH mới theo ý mình dựa trên mã nguồn mở của nhân HĐH (kernel). Ngoài ra, với việc đầu tư cho hệ thống thử nghiệm trong khoảng thời gian từ 3-5 năm với HĐH UNIX và các trang thiết bị đồng bộ đi kèm sẽ là không hiệu quả. Nhất là đối với các thiết bị máy chủ hiện tại với thời gian khấu hao từ 5-7 năm, việc lựa chọn Linux thay cho UNIX là hợp lí.

Lựa chọn hệ điều hành Windows cho các máy trạm

Đối với các máy trạm, việc sử dụng đồng nhất một hệ điều hành có hỗ trợ sẵn các ứng dụng Multimedia, đảm bảo được việc cấu hình kết nối IPv6 cũng như có được giao diện người dùng phù hợp cho các thử nghiệm Multimedia sau này. Mặt khác, các ứng dụng multimedia chưa thực sự được phát triển mạnh trên nền Linux. Bên cạnh đó, việc sử dụng Windows trở thành phổ biến cho các máy trạm tại Việt nam nhất là với những người sử dụng đầu cuối thông thường.

Tuy nhiên, tùy thuộc vào điều kiện thực tế của quá trình thử nghiệm, có thể sử dụng các phần mềm HĐH khác thay thể cho một số máy sử dụng Windows với mục đích đa dạng hệ thống thử nghiệm.

1.5.3.5 Định cỡ, lựa chọn dịch vụ thử nghiệm

Trong giai đoạn thử nghiệm trên mạng IPv6, một số dịch vụ cơ bản như: Web, Mail, FTP,... cần thiết được thử nghiệm dưới nền giao thức IPv6. Việc lựa chọn dịch vụ thử nghiệm đồng nghĩa với việc xây dựng các phương pháp đánh giá, kiểm tra chất lượng và tính hiệu quả của các dịch vụ trên nền giao thức mới IPv6. Chi tiết thông tin về các phương pháp đánh giá mạng thử nghiệm trên các dịch vụ cụ thể được trình bày chi tiết trong chương V và chương VI của đề tài.

a. Dịch vụ Web

Trong số các dịch vụ cơ bản trên Internet, World Wide Web thực sự là dịch vụ được cả thế giới biết tới. Các trang Web hiện nay ngày càng được mở rộng các tính năng, phát triển về số lượng để thoả mãn như cầu trao đổi thông tin trên mạng của người sử dụng. Với các hệ thống khác nhau, người dùng luôn có thể tham gia vào hệ thống mạng toàn cầu, thiết lập máy chủ dịch vụ và thiết kế trang Web cho mình. Với các hệ điều hành hiện tại dùng cho máy chủ hay máy trạm, các ứng dụng dịch vụ thường được tích hợp luôn bên trong hệ điều hành.

Hiện tại, Apache là phần mềm máy chủ dịch vụ Web được sử dụng phần lớn trên các hệ thống máy chủ dịch vụ Web trên thế giới. Lý do được sử dụng thông dụng là vì Apache hỗ trợ các đặc tính mở của một web server, có nhiều phiên bản cho các nền hệ điều hành khác nhau. Với HĐH Linux, Apache được sử dụng như một webserver chuẩn. Trong thời gian đầu, Apache chưa hỗ trợ IPv4, nhưng sau dự án KAME, Apache đã được chính thức hỗ trợ IPv6 bắt đầu từ phiên bản 1.3.6, phiên bản Apache chuẩn được cung cấp bởi Apache Software Foundation. Việc sử dụng Apache cho phép người dùng có thể cấu hình được các thông số của máy chủ web, kiểm soát các thông tin truy nhập. Mặt khác, ứng dụng Apache chuẩn được nhiều hãng phát triển trên nền mã nguồn mở, do đó phù hợp với mô hình thử nghiệm, phát triển và tự xây dựng các ứng dụng hỗ trợ kèm theo.

b. Dịch vụ Mail

Hệ thống email của Linux có hai thành phần: tác nhân người dùng email (MUA – Mail User Agent) và tác nhân gửi email (MTA – Mail Transfer Agent). MUA đóng vai trò giao diện người dùng đối với trình nhận/gửi mail; MTA đóng vai trò nhận và chuyển tiếp mail. Trên HĐH Linux, có hai MTA phổ biến là sendmail và smail. Còn trên các HĐH khác nhau luôn có sẵn

các MUA với tính năng và giao diện phong phú, trên Windows của Microsoft có Outlook Express, trên Linux có XMail, Netscape mailm,...

Sendmail là MTA được sử dụng phổ biến nhất, vì đây là hệ thống được xây dựng trên nền MTA của đại học Berkeley ở California. Sendmail đáp ứng được cho các hệ thống lớn, có khả năng xử lý linh hoạt và cho phép thiết lập cấu hình với nhiều lựa chọn.

Do tính linh hoạt và khá mạnh trong xử lý, sendmail trở nên phức tạp trong cấu hình. Chính vì thế, sendmail thường kết hợp với công cụ IDA để trở thành một sản phẩm nối tiếp Sendmail+IDA. IDA làm cho sendmail trở nên dễ sử dụng hơn, trên thực tế, sendmail được cài đặt trên HĐH Linux là phổ biến. Phiên bản 8.11.6 của Sendmail đã có hỗ trợ giao thức IPv6.

Trong khuôn khổ mạng thử nghiệm, HĐH sử dụng là Linux, trình Sendmail đã được nhúng vào trong Linux, do vậy việc cài đặt và cấu hình không còn thực sự phức tạp.

c. Dịch vụ DNS

DNS là dịch vụ cho phép chuyển đổi địa chỉ IP sang địa chỉ tên miền. DNS góp phần giải quyết bài toán phân bố cơ sở dữ liệu địa chỉ mạng. Với một địa chỉ IP nhưng cho phép có nhiều tên miền khác nhau, người dùng không cần thiết ghi nhớ địa chỉ IP để biết xem vị trí địa lý của máy đang truy nhập mà chỉ quan tâm đến phần tên gợi nhớ của địa chỉ IP đó được ghi nhận trong cơ sở dữ liệu. Cấu trúc địa chỉ tên mền có dạng cây, nút cao nhất là gốc, các nút thấp hơn tương đương với các sub-domain được chia theo địa lý (lãnh thổ quốc gia) và các lĩnh vực hoạt động (kinh tế, giáo dục,...).

Trong hệ thống máy chủ Linux, BIND là công cụ hữu dụng hỗ trợ dịch vụ DNS. BIND cũng do nhóm Đại học Berkeley phát triển nên được sử dụng rộng rãi trên thế giới. Với tính năng cung cấp nhiều đặc tính mạnh, ổn định, an toàn và định hướng mở, việc sử dụng BIND trong giai đoạn thử nghiệm là hợp lý. Phiên bản BIND 9.x hỗ trợ quản lý địa chỉ IPv6 được sử dụng trong hệ thống.

d. Dịch vụ FTP

Giống như Web và Mail, FTP là một trong những dịch vụ khá thông dụng trên Internet. FTP cho phép truyền và nhận các tập tin giữa các máy tính được kết nối với nhau trên nền giao thức TCP/IP.

Trên HĐH Linux có công cụ FTP-Wu-FTP hỗ trợ IPv6. Với quy mô vừa và nhỏ, việc sử dụng công cụ này trong phạm vi thử nghiệm là hoàn toàn hợp lý. Ngoài ra, chúng ta cũng có thể tham khảo các phần mềm dịch vụ FTP server của các nhóm phát triển khác.

Chương 2: KẾT QUẢ ÁP DỤNG THỬ NGHIỆM KẾ HOẠCH CHUYỂN ĐỔI

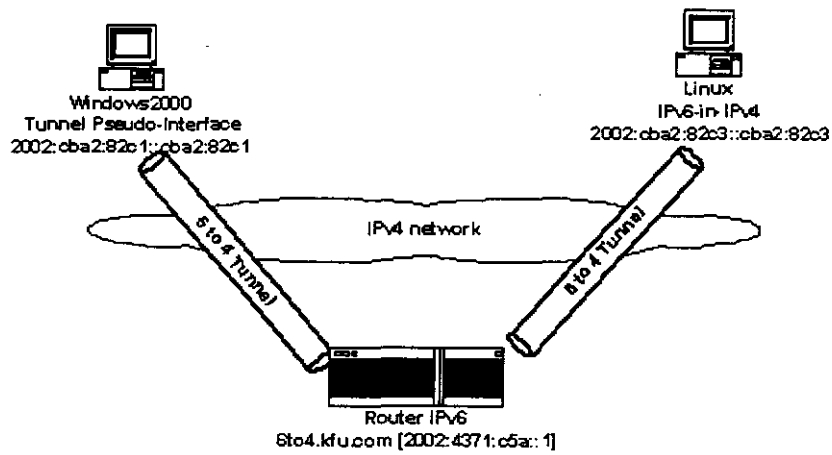
2.1 Thử nghiệm kết nối mô hình mạng cục bộ

2.1.1 Mục tiêu

Trong quá trình triển khai nghiên cứu, thử nghiệm giao thức IPv6 trên diên rộng, việc tiếp cận, làm chủ công nghệ là điều cần thiết. Để có được cái nhìn từ chi tiết đến tổng thể của toàn bộ quá trình thử nghiệm, nhóm nghên cứu đã có những thử nghiệm nhỏ trên mô hình mạng cục bộ, bước đầu có được những đánh giá, rút ra được những bài học cho việc nghiên cứu, thử nghiệm trên hệ thống mạng diện rộng sẽ được trình bày trong phần sau.

2.1.2 Mô hình thực hiện

Tiến hành thiết lập một mạng IPv6 đơn giản bao gồm hai máy tính đang sử dụng trong mạng IPv4 hiện tại, định tuyến với nhau thông qua một bộ định tuyến công cộng (public IPv6 router).



Hình 3 - Mô hình kết nối mạng thử nghiệm nhỏ

Thiết lập địa chỉ IPv6 cho 2 máy trong mạng nội bộ đang sử dụng thuần giao thức IPv4. Hai máy này có địa chỉ thực IPv4.

Máy I : 203.162.130.195.

Máy II: 203.162.130.193

Thiết lập cấu hình 02 đường ống IPv6 trên nền mạng IPv4 đến cùng 01 router hỗ trợ chuyển đổi 6to4.

Trên thế giới, tương ứng mỗi vùng địa lý khác nhau có các tổ chức tự xây dựng các router 6to4 nhằm hỗ trợ thiết lập và thử nghiệm các kết nối IPv6 tạm thời.

Bảng 2 - Danh sách định tuyến chuyển tiếp kết nối tạm thời

Địa chỉ bộ định tuyến	**Quốc gia**	**Băng thông kết nối**	**Chú ý**
2002:c058:6301::	Toàn cầu	n/a	Trong RFC 3068. Đây là địa chỉ *anycast* cho các relay router gần nhất.
Bắc Mỹ			
6to4.ipv6.microsoft.com	Redmond, WA? / -	?	Mở cho các thử nghiệm
6to4.kfu.com	Santa Clara, CA / Pacific Bell	128 kbps	Mở cho các thử nghiệm
ipv6-lab-gw.cisco.com	San Jose / Sprint?	100 mbps	Có yêu cầu, điều lệ cụ thể, tham khảo tại website của Cisco.
Châu Á Thái Bình Dương			
6to4.ipv6.aarnet.net.au	Sydney, Australia	100 mbps	Chỉ hỗ trợ tại Australia
kddilab.6to4.jp	Tokyo, Japan / ?	100 mbps	Mở cho các thử nghiệm, hỗ trợ bởi KDDI LAB
6to4.ipv6.ascc.net	Taipei, Taiwan / ?	100 mbps	Mở bởi Trung tâm tính toán Viện Sinica, hỗ trợ thử nghiệm.
Châu Phi			
6to4.ipng.unix.za.net	Cape Town, South Africa / ?	48 mbps	Mở thử nghiệm
Châu Âu			
6to4.ipv6.bt.com	Adastral Park, UK / ?	10 mbps	Mở thử nghiệm

skbys-00-00.6to4.xs26.net	Banska Bystrica, Slovakia	34 mbps	Mở thử nghiệm
6to4.ipv6.uni-leipzig.de	Leipzig, Germany	100 mbps	Mở với mục đích thử nghiệm
6to4.ipv6.fh-regensburg.de	Regensburg, Germany	34 mbps	Mở với mục đích thử nghiệm
6to4.ipng.nl	The Netherlands / AMS-IX	100 mbps	Mở thử nghiệm

2.1.3 Phần cứng - Hệ điều hành

Trước hết, việc sử dụng hai máy tính IBM PC có cấu hình phần cứng giống nhau đảm bảo được tính nhất quán trong thử nghiệm (1Ghz, 10GB HDD, FastEthernet 10/100 Mbps.). Tuy nhiên, trong tương lai, mô hình thử nghiệm diện rông đòi hỏi sử dụng những phần mềm HĐH khác ngoài Windows, do đó việc cài đặt một máy sử dụng HĐH Linux và máy còn lại cài đặt HĐH Windows 2000.

2.1.4 Yêu cầu

Hai máy phải nhìn thấy nhau thông qua giao thức IPv6. Chúng ta có thể kiểm tra bằng cách sử dụng những công cụ kiểm tra đường truyền đơn giản đối với giao thức IPv6 (cũng tương tự như IPv4) : ping6, traceroute6.

2.1.5 Thiết lập cấu hình

Thiết lập địa chỉ IPv6 trên máy Windows

```
ipv6 rtu 2002::/16 2
ipv6 adu 2/2002:CBA2:82C1::CBA2:82C1
ipv6 rtu ::/0 2/::202.255.45.5 pub life 1800
ping6 www.6bone.net
```

ipv6 rtu 2002::/16 2

Thiết lập giao diện thứ 02 làm giao diện đánh địa chỉ IPv6 với định dạng (prefix) kiểu 6to4.

ipv6 adu 2/2002:CBA2:82C1::CBA2:82C1

Nhập địa chỉ IPv6 cho giao diện số 02. Giá trị số hex gán cho địa chỉ lấy từ địa chỉ IPv4 tương ứng là 203.162.130.196.

ipv6 rtu ::/0 2/::202.255.45.5 pub life 1800

Thiết lập tunnel đến router kddilab.6to4.jp [202.255.45.5] với thời gian tồn tại (time to live) cho kết nối tạm thời này là 1800 giây = 30'.

Kết quả khi thử ping đến website của 6bone

```
C:\>ping6 www.6bone.net –t

Pinging 6bone.net [3ffe:b00:c18:1::10] with 32 bytes of data:

Reply from 3ffe:b00:c18:1::10: bytes=32 time=724ms

Reply from 3ffe:b00:c18:1::10: bytes=32 time=740ms

Reply from 3ffe:b00:c18:1::10: bytes=32 time=748ms
```

Kết quả khi traceroute đến webserver chính của mạng 6bone

```
C:\>tracert6 www.6bone.net

Tracing route to 6bone.net [3ffe:b00:c18:1::10] over a maximum of 30 hops:

1  808 ms  824 ms  811 ms  2002:4371:c5a::1

2  572 ms  579 ms  577 ms  digital-ca-tunnel.ipv6.cisco.com [3ffe:c00:8023:13::2]

3  657 ms  667 ms   *     3ffe:c00:8023:6::2

4  722 ms  716 ms   *     rap.ipv6.viagenie.qc.ca
                    [3ffe:b00:c18:1:290:27ff:fe17:fc0f]

5   *     722 ms  737 ms  www.6bone.net [3ffe:b00:c18:1::10]

Trace complete.
```

Thiết lập giao diện IPv6 trên máy Linux:

```
ifconfig sit0 up
ifconfig sit0 add 2002:cba2:82c3::cba2:82c3/16
route -A inet6 add 2000::/3 gw ::202.255.45.5 dev sit0
```

ifconfig sit0 up

Kích hoạt giao diện dùng cho IPv6, ở đây là **sit0**.

ifconfig sit0 add 2002:cba2:82c3::cba2:82c3/16

Đặt địa chỉ cho giao diện đó, địa chỉ sử dụng ở đây được lấy giá trị từ giá trị của địa chỉ IPv4 tương ứng là 203.162.130.195 => chuyển đổi sang IPv6 là CBA2:82C3. Ta hoàn toàn có thể lấy một địa chỉ khác để gán cho giao diện này, tuy nhiên để có được địa chỉ thống nhất và thuận tiện, dễ nhớ, chúng tôi chọn phương pháp này.

route -A inet6 add 2000::/3 gw ::202.255.45.5 dev sit0

Thiết lập cấu hình đường ống 6to4 đến public router chuyển đổi 6to4 có địa chỉ IPv4 là 202.255.45.5. Giao diện được gán địa chỉ này mặc định là sit0.

Kết quả khi thử ping đến một website thuộc 6BONE: **6to4.kfu.com**

```
[root@IPV6 root]# ping6 6to4.kfu.com
PING 6to4.kfu.com(2002:4371:c5a::1) 56 data bytes
64 bytes from 2002:4371:c5a::1: icmp_seq=6 ttl=64 time=269 ms
64 bytes from 2002:4371:c5a::1: icmp_seq=9 ttl=64 time=325 ms
64 bytes from 2002:4371:c5a::1: icmp_seq=10 ttl=64 time=329 ms
64 bytes from 2002:4371:c5a::1: icmp_seq=11 ttl=64 time=304 ms
--- 6to4.kfu.com ping statistics ---
4 packets transmitted, 11 received, 0% loss, time 10039ms
rtt min/avg/max/mdev = 188.120/292.484/433.440/59.509 ms
```

Kết quả khi traceroute đến website đó

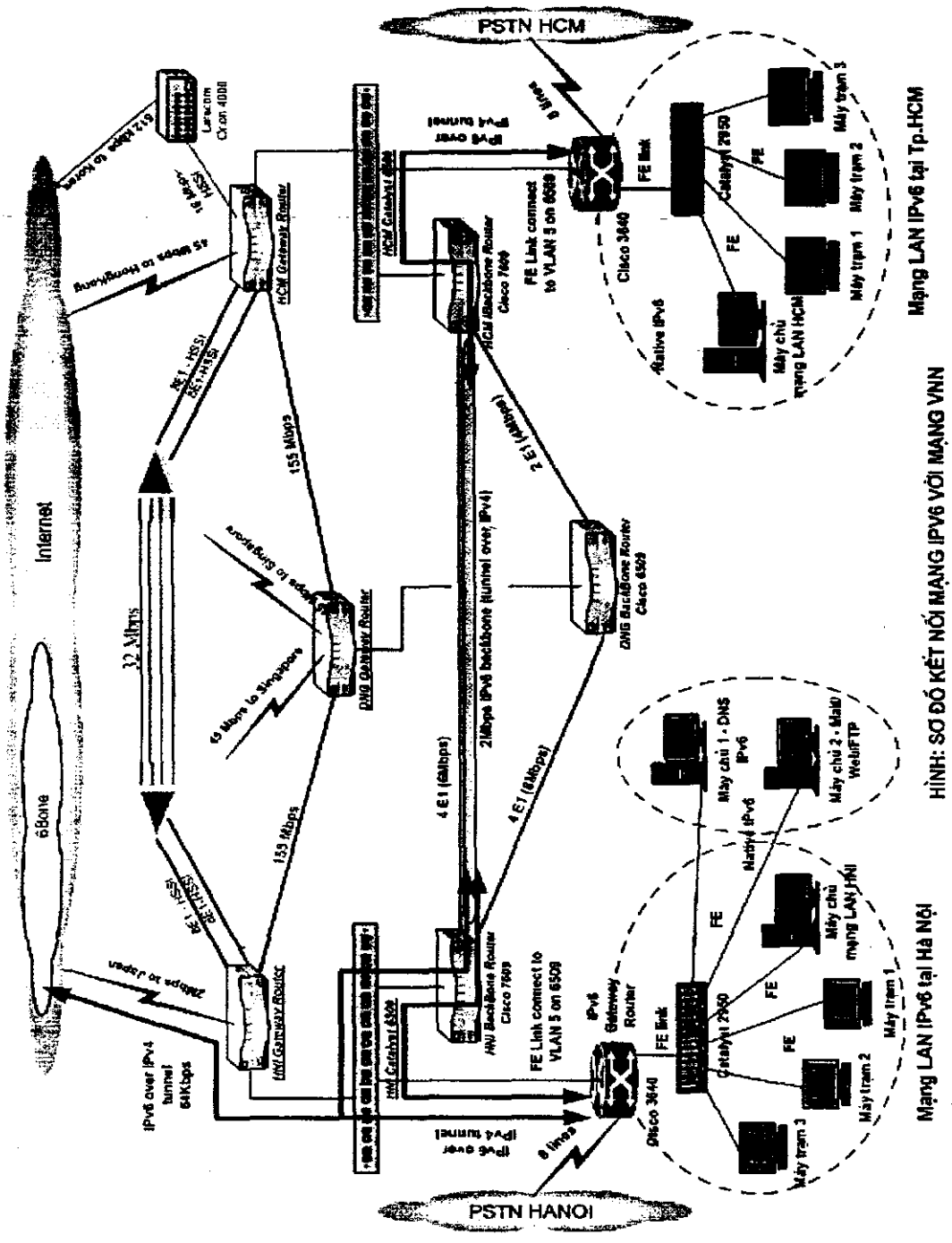
```
[root@IPV6 root]# traceroute6 6to4.kfu.com
traceroute to 6to4.kfu.com (2002:4371:c5a::1) from 2002:cba2:82c3::cba2:82c3, 30 hops max, 16 byte packets
 1  2002:4371:c5a::1 (2002:4371:c5a::1)  188.227 ms  337.819 ms  261.427 ms
```

2.2 Thử nghiệm kết nối mô hình mạng diện rộng trong nước

2.2.1 Mô hình mạng diện rộng

Được sự đồng ý và hỗ trợ của Tổng Công ty Bưu chính Viễn Thông, công ty VDC đang triển khai dự án "Triển khai mạng thử nghiệm IPv6 kết nối VNN" với mô hình tương tự như mô hình lý thuyết đã được nghiên cứu (trong phần II, tài liệu Báo cáo đề tài nghiên cứu Triển khai thử nghiệm mạng IPv6 Việt Nam và kết nối với mạng IPv6 quốc tế), nhằm phục vụ cho việc hiện thực hóa và triển khai các nghiên cứu về IPv6.

Dưới đây là mô hình mạng thử nghiệm kết nối VNN



Hình 4 : Sơ đồ đấu nối mạng IPv6 Hà Nội-TP Hồ Chí Minh và VNN4

Việc triển khai mô hình này được tiến hành theo 3 bước

Triển khai các mạng LAN thuần tại hai đầu Hà Nội và Thành phố Hồ Chí Minh. Mỗi mạng LAN này bao gồm một Gateway Router 3640 IOS IP Plus kết nối với một Cisco Catalyst 2950 qua giao diện Fast Ethernet và các Server Mail, Web, FTP, các máy trạm sử dụng giao thức thuần IPv6. Các mạng LAN thuần này được kết nối tới mạng VNN4 thông qua kết nối Fast Ethernet từ Gateway Router 3640 tới VLAN5 main Switch 6509(VLAN cho các thiết bị quản trị, người quản trị mạng và thử nghiệm các công nghệ mới).

Triển khai các kết nối IPv6 Backbone và quốc tế. Sử dụng đường ống IPv6 trên nền IPv4 dựa trên mạng trục IPv4 tạo tunel ảo với tốc độ 2Mbps để làm backbone IPv6. Các tunel ảo được thiết lập giữa hai Router hai đầu Hà Nội – Thành phố Hồ Chí Minh và thiết lập giữa Router đầu Hà Nội ra mạng quốc tế. (router đối tác mà mạng VNN kết nối vào)

Triển khai các kết nối cho khách hàng Dialup và Leased Line.

2.2.2 Cấu hình thiết bị và phần mềm

Dưới đây là bảng cấu hình Router hai đầu Hà Nội-Thành phố Hồ Chí Minh sau khi đã thực hiện bước 1 .

2.2.2.1 Router Hà Nội

```
HANOI(6to4)#show run
Building configuration...

Current configuration : 2989 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HANOI(6to4)
!
```

```
boot system flash c3640-p7-mz.122-15.T2.bin
logging queue-limit 100
enable secret 5 $1$ODgb$/iUoaOAT.sFu1UzJU8bQn/
!
username ... password ... ipv6-vdc
aaa new-model
!
!
aaa authentication login default local
aaa accounting connection default none
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip name-server 3FFE:FFFF:8000:2003::3
!
ipv6 unicast-routing
mpls ldp logging neighbor-changes
!
!
!
!
!
!
!
```

```
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
interface Loopback0
 no ip address
 ip broadcast-address 0.0.0.0
 ipv6 address 3FFE::1/64
!
interface Tunnel0
 description Connection_TO_HCM
 no ip address
 ip broadcast-address 0.0.0.0
 ipv6 unnumbered FastEthernet0/0
 ipv6 rip ipv6_vdc enable
 tunnel source FastEthernet0/0
 tunnel destination 203.162.4.117
 tunnel mode ipv6ip
!
interface FastEthernet0/0
```

```
 ip address 203.162.175.39 255.255.255.224
 ip broadcast-address 0.0.0.0
 duplex auto
 speed auto
 ipv6 address 3FFE:FFFF:8000:2004::1/64
 ipv6 rip ipv6_vdc enable
 no cdp enable
!
interface Serial0/0
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
 clockrate 2000000
!
interface FastEthernet0/1
 description LAN_SERVER
 no ip address
 ip broadcast-address 0.0.0.0
 duplex auto
 speed auto
 ipv6 address 3FFE:FFFF:8000:2003::1/64
 ipv6 enable
 ipv6 rip ipv6_vdc enable
 no cdp enable
!
interface Serial0/1
```

```
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
 clockrate 2000000
!
interface Serial2/0
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/1
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/2
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/3
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/4
```

```
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/5
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/6
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Serial2/7
 no ip address
 ip broadcast-address 0.0.0.0
 shutdown
!
interface Group-Async1
 no ip address
 ip broadcast-address 0.0.0.0
 encapsulation ppp
 ipv6 unnumbered Loopback0
 ipv6 rip ipv6_vdc enable
 async mode interactive
```

```
 peer default ipv6 pool HAN
 no keepalive
 ppp authentication pap chap ms-chap
 group-range 33 40
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 203.162.175.33
!
!
!
ipv6 local pool HAN 3FFE:FFFF:8000:2008::/64 16
ipv6 router rip ipv6_vdc
!
!
!
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
```

```
!
!
!
line con 0
line 33 40
 no flush-at-activation
 modem Dialin
 modem autoconfigure discovery
 autoselect during-login
 autoselect ppp
 flowcontrol hardware
line aux 0
line vty 0 4
 password ...
!
!
end


HANOI(6to4)#
```

2.2.2.2 Router Thành phố Hồ Chí Minh

```
TPHCM6to4#sh running-config
Building configuration...


Current configuration : 2757 bytes
!
```

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname TPHCM6to4
!
logging queue-limit 100
enable secret 5 $1$fCm3$RSex/yZYCQ9vLzahOrW4z0
!
username test password 7 1403171818
ip subnet-zero
!
!
ip domain name NAME1
ip name-server 3FFE:FFFF:8000:2003::3
!
ipv6 unicast-routing
mpls ldp logging neighbor-changes
!
!
voice call carrier capacity active
!
!
!
!
```

```
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
!
interface Loopback0
 no ip address
 ip broadcast-address 0.0.0.0
 ipv6 address 3FFE::2/64
!
interface Loopback1
 no ip address
!
interface Loopback2
 ip address 1.1.1.1 255.255.255.0
!
interface Tunnel0
 description Tunnel to HANOI6to4
 no ip address
 ipv6 unnumbered FastEthernet0/1
```

```
 ipv6 rip ipv6_vdc enable
 tunnel source FastEthernet0/1
 tunnel destination 203.162.175.39
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 description Connection to LAN (IPv6)
 no ip address
 duplex auto
 speed auto
 ipv6 address 3FFE:FFFF:8000:2005::1/64
 ipv6 enable
 ipv6 rip ipv6_vdc enable
!
interface Serial0/0
 no ip address
 shutdown
 clockrate 2000000
!
interface FastEthernet0/1
 description Connection to HANOI6to4 (tunnel) and VNN
 ip address 203.162.4.117 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 3FFE:FFFF:8000:2006::1/64
 ipv6 enable
```

```
 ipv6 rip ipv6_vdc enable
!
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
interface Serial2/4
 no ip address
 shutdown
```

```
!
interface Serial2/5
 no ip address
 shutdown
!
interface Serial2/6
 no ip address
 shutdown
!
interface Serial2/7
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 rip ipv6_vdc enable
 async mode interactive
 peer default ipv6 pool HCM
 ppp authentication pap chap ms-chap
 group-range 33 40
!
```

```
ip default-gateway 203.162.4.172
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
ip route 192.168.0.0 255.255.255.0 FastEthernet0/1
!
!
!
logging 203.162.47.238
ipv6 local pool HCM 3FFE:FFFF:8000:2007::/64 16
ipv6 router rip ipv6_vdc
!
!
!
call rsvp-sync
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
!
```

```
line con 0
line 33 40
 no flush-at-activation
 login local
 modem InOut
 modem autoconfigure discovery
 autocommand  ppp
 transport input all
 autoselect arap
 autoselect during-login
 autoselect ppp
 flowcontrol hardware
line aux 0
line vty 0 4
 password ...
 login
!
!
end

TPHCM6to4#
```

2.2.2.3 Cấu hình DNS tại Server DNSv6

A.File named.conf

```
## named.conf - configuration for bind
#
# Generated automatically by redhat-config-bind, alchemist et al.
# Any changes not supported by redhat-config-bind should be put
# in /etc/named.custom
#
# controls {
#       inet 127.0.0.1 allow { localhost; } keys { rndckey; };
# };

key "rndc-key" {
        algorithm hmac-md5;
        secret "VOKSm3OnVyMK4MEW1HJWAw==";
};

// include "/etc/named.custom";

// include "/etc/rndc.key";

options {
        directory "/var/named/";
        listen-on-v6 { any; };
};

zone  "0.0.127.in-addr.arpa" {
        type master;
        file  "0.0.127.in-addr.arpa.zone";
```

```
};

zone "localhost" {
        type master;
        file "localhost.zone";
};
zone "ipv6.vnn.vn." {
        type master;
        file "ipv6.vnn.vn.zone";
};
```

B.File ipv6.vnn.vn.zone

```
$TTL 3D
$ORIGIN ipv6.vnn.vn.
@       IN      SOA     ns.ipv6.vnn.vn. postmaster.ipv6.vnn.vn. (
                        2003053011; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

                NS      ns.ipv6.vnn.vn.
                IN      MX      10      mail.ipv6.vnn.vn.
;
;
```

home IN CNAME www

www IN AAAA 2001:C20:2001:1101::2

mail IN AAAA 2001:C20:2001:1101::2

ftp IN AAAA 2001:C20:2001:1101::1

dns IN AAAA 2001:C20:2001:1101::1

files-server IN AAAA 2001:C20:2001:1101::3

hcm IN AAAA 2001:C20:2001:2101::1

2.3 Thử nghiệm kết nối mô hình mạng diện rộng quốc tế

2.3.1 Kết nối với mạng 6BONE

Mạng thử nghiệm VNN6 đã được kết nối thực tế với mạng 6BONE qua đối tác SingTel với các địa chỉ được phân như sau :

Địa chỉ do SingTel cấp :

2001:C20:2001::/48

Các địa chỉ được phân tiếp cho VDC1(tại Hà Nội) và VDC2(Tại Thành phố HCM) như sau:

Tại VDC1:

2001:C20:2001:1000::/64 ----> Địa chỉ kết nối

2001:C20:2001:1101::/64 ----> LAN IPv6 Server

2001:C20:2001:1102::/64 ----> LAN IPv6 Workstation

2001:C20:2001:1103::/64 ----> IPv6 Dial-Up VDC1

Tại VDC2:

2001:C20:2001:2000::/64 ----> Địa chỉ kết nối

2001:C20:2001:2101::/64 ----> LAN IPv6 Server (hiện tại chưa có Server, để dành cho Server trong tương lai)

2001:C20:2001:2102::/64 ----> LAN IPv6 Workstation

Backbone HN-HCM Tunnel:

HNI:

203.162.175.39 / 27 (địa chỉ IPv4)

2001:C20:2001:0::1 /127 (địa chỉ IPv6)

HCM:

203.162.4.117 / 27 (địa chỉ IPv4)

2001:C20:2001:0::2 /127 (địa chỉ IPv6)

HNI-SINGTEL Tunnel:

HNI:

203.162.175.39 / 27 (địa chỉ IPv4)

2001:C20:0:E::15 / 127 (địa chỉ IPv6)

SINGTEL:

220.255.0.2 /27 (địa chỉ IPv4)

2001:C20:0:E::14 / 127 (địa chỉ IPv6)

Sau khi được cấu hình kết nối với SingTel, Router 3640 tại Hà Nội đã được thay đổi cấu hình như sau :

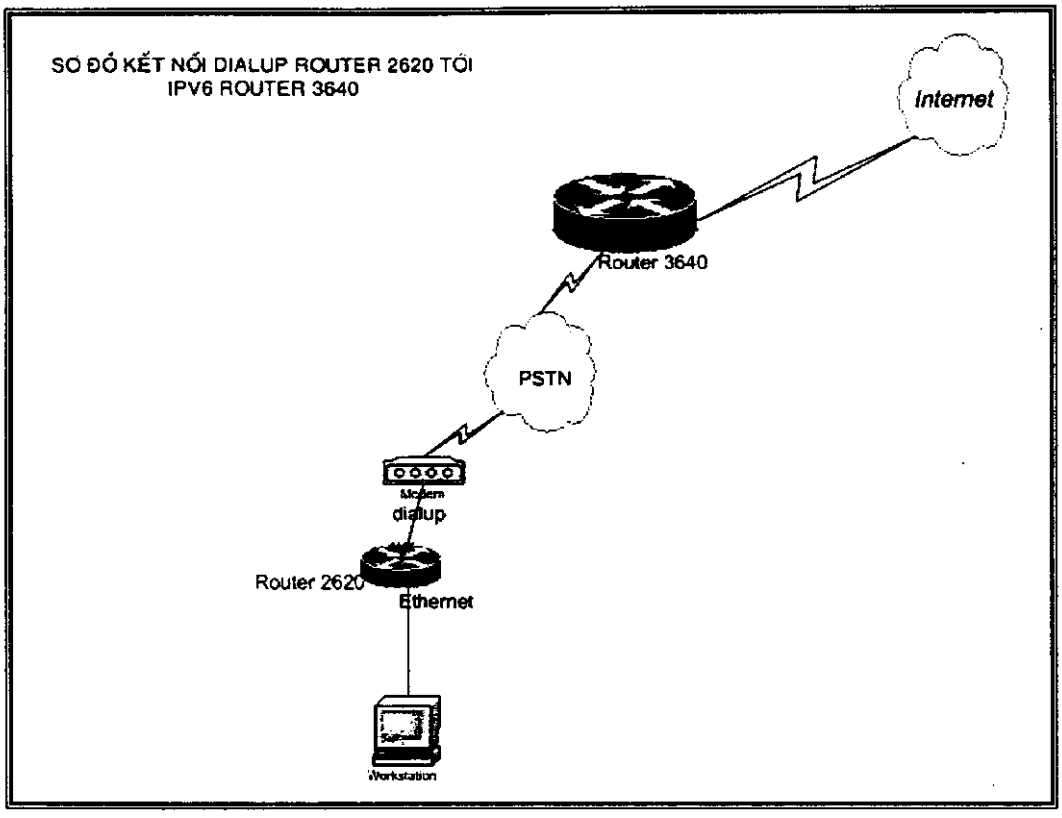
```
interface Tunnel0
 description Connection_TO_HCM
 no ip address
 ipv6 unnumbered FastEthernet0/0
 ipv6 rip ipv6_vdc enable
 tunnel source FastEthernet0/0
 tunnel destination 203.162.4.117
 tunnel mode ipv6ip
```

```
!
interface Tunnel1
 description Connection_TO_SINGTEL
 no ip address
 ipv6 unnumbered FastEthernet0/0
 ipv6 rip ipv6_vdc enable
 tunnel source FastEthernet0/0
 tunnel destination 220.255.0.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
ip address 203.162.175.39 255.255.255.224
 duplex auto
 speed auto
 ipv6 address 3FFE:FFFF:8000:2004::1/64
 ipv6 rip ipv6_vdc enable
 no cdp enable
!
interface Serial0/0
 no ip address
 shutdown
 clockrate 2000000
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
```

```
 speed auto
 ipv6 enable
 no cdp enable
!
interface FastEthernet0/1.1
 description LAN_WORKTATION
 encapsulation dot1Q 5
ipv6 address 3FFE:FFFF:8000:2002::1/64
 ipv6 rip ipv6_vdc enable
 no cdp enable
!
interface FastEthernet0/1.2
 description LAN_SERVER
 encapsulation dot1Q 3
 ipv6 address 3FFE:FFFF:8000:2003::1/64
 ipv6 rip ipv6_vdc enable
 no cdp enable
!
```

2.4 Mô hình dịch vụ Dial-up

Nhóm thử nghiệm cũng đã thử nghiệm dịch vụ dial-up và đã dial-up thành công với địa chỉ IPv6. Do có những khó khăn trong việc phiên bản phần mềm của Router 3640 trong dự án chưa hỗ trợ chức năng dial-up, nhóm thử nghiệm đã thử nghiệm dial-up qua Router 2620 và đã thành công. Trong tương lai gần, sau khi Router 3640 được nâng cấp phiên bản phần mềm mới, người sử dụng có thể dial-up từ máy trạm. Dưới đây là mô hình dịch vụ dial-up :



Hình 5: Sơ đồ kết nối Dial Up Router 2620 tới IPV6 Router 3640

2.5 Thử nghiệm cung cấp dịch vụ và công cụ phát triển đối với IPv6

2.5.1 Xây dựng phương pháp đánh giá chất lượng dịch vụ cơ bản trên Internet

2.5.1.1 Các kiểu đo kiểm dịch vụ mạng

Đối với các dịch vụ mạng, để kiểm tra độ tin cậy của từng dịch vụ, có nhiều nhóm nghiên cứu trên thế giới đã đề xuất các phương pháp đo khác nhau. IETF đã tổng hợp và phân loại thành hai kiểu đo chính là ***đo chủ động (Active measurement)*** và ***đo thụ động (Passive measurement)***. Việc sử dụng phương pháp đo nào tùy thuộc vào mục đích của quá trình đo và các yếu tố khác nhau trong quá trình vận hành mạng. Tuy nhiên nếu áp dụng kết hợp đồng thời được hai phương pháp đo đồng thời trong cùng một phép đo thì sẽ nâng cao tính chính xác và ý nghĩa của quá trình đo nói riêng và cả quá trình đánh giá hiệu năng mạng nói chung.

Đo kiểu chủ động

Định nghĩa cho các phép đo chủ động dựa trên cơ sở thực hiện các phiên truyền thông bằng cách gửi các gói tin thăm dò lên trên môi trường mạng đang hoạt động, từ đó xác định được các đáp ứng, kích thích của các dịch vụ mạng tương ứng.

Đối với các dịch vụ trên nền giao thức IP nói chung, việc sinh ra các gói tin, yêu cầu và gửi đến các máy chủ dịch vụ tương ứng cho phép xác định được khả năng đáp ứng và tính sẵn sàng của dịch vụ. Tương ứng với các gói tin, yêu cầu gửi đến máy chủ, tiến hành kiểm tra số lượng, tính chính xác của các đáp ứng của các máy chủ gửi về dưới dạng các gói tin, các trả lời phản hồi. Thông qua đó đưa ra đánh giá về máy chủ. Tuy nhiên, để phép đo thực sự có ý nghĩa, phản ánh được thực trạng của môi trường mạng, các gói tin, yêu cầu dò tìm gửi đến máy chủ dịch vụ cần được dựa trên số liệu truyền thông thực của người sử dụng. Trong những trường hợp mà những điều kiện trên không thể thực hiện được, chúng ta có thể phải thực hiện thêm những phép đo khác đồng thời phải duy trì sự tương ứng giữa các điều kiện thực hiện đo kiểm với phép đo.

Một ví dụ minh hoạ khi thực hiện các phép đo kiểm tra dịch vụ như web, mail, ftp, khi thực hiện thiết lập kết nối thông qua các socket, cần thiết tính đến tương quan thời gian trả lời các yêu cầu xác định tên máy chủ phản hồi từ máy chủ DNS. Nếu máy chủ DNS đó nằm trong cùng một mạng với máy chủ dịch vụ cần đo thì không có sự cách biệt lớn. Điều này cho thấy chỉ sử dụng duy nhất phương pháp đo chủ động cũng có thể không thu được kết quả chính xác như mong muốn nếu như không tính đến các yếu tố khác như cấu trúc mạng, khả năng phân tải và đáp ứng của các thành phần mạng khác nhau.

Bản chất của phép đo bằng phương pháp chủ động là đưa các lưu thông giám sát vào trong quá trình lưu thông chính của các luồng dữ liệu trong mạng. Chính yếu tố này cũng có thể gây nên những sai số nhất định trong quá trình đo nếu như không có một kế hoạch đo được hoạch định từ trước. Những phiên truyền thông giám sát gia tăng đột biến có thể làm ảnh hưởng chính đến chất lượng dịch vụ mà ta đang đánh giá, do đó mất đi ý nghĩa của quá trình đo. Mặt khác, những yếu tố ngầm định đối với phép đo này cũng có thể ảnh hưởng đến chất lượng dịch vụ cần đo. Ví dụ như trong nhiều trường hợp, các thiết bị đo không nằm trong kiểm soát của nhà cung cấp dịch vụ, do vậy quá trình đăng nhập vào các hệ thống con khác nhau trên một hệ thống tổng thể thường không được đề cập đến, và do vậy, phép đo vẫn tồn tại những hạn chế.

Đo kiểu thụ động

Đo kiểm kiểu thụ động là phương pháp đo dựa trên những thiết bị sẵn có trên mạng kết hợp với các công cụ đo kiểm mạng. Một điểm khác biệt quan trọng của phương pháp này là không sử dụng đến những lưu thông giám sát đưa thêm vào trong mạng, do vậy không làm

ảnh hưởng đến các lưu thông thực tế cần đo. Các quá trình đo kiểm của các nhà cung cấp dịch vụ lớn thường được tiến hành trên cả hai phương pháp đo chủ động và bị động, tuy nhiên, trên diện rộng, với mạng lưới phức tạp, giảm thiểu sự tác động đến hệ thống thì kiểu đo này có nhiều ưu điểm.

Kiểu đo này tận dụng những thiết bị sẵn có trong mạng, máy chủ, thiết bị mạng và các ứng dụng dịch vụ mạng để thực hiện đo kiểm. Bởi vì không cần phải thực hiện những tác động tới quá trình truyền thông nên nó sẽ giảm tối thiểu sự tác động đến hệ thống của ISP, do đó kiểu đo này tỏ ra thích hợp đối với những nhà cung cấp dịch vụ lớn. Kiểu đo này cũng phản ánh chân thực chất lượng dịch vụ nhận được từ phía người sử dụng. Ngoài ra, đo kiểu thụ động cũng cung cấp cho chúng ta nhiều thông tin rất hữu ích cho qúa trình phát hiện lỗi và lập kế hoạch phát triển như lượng tài nguyên và dịch vụ được sử dụng.

Kiểu đo thụ động có thể được thực hiện trên nhiều kiểu thiết bị khác nhau:

- **Máy chủ**: Web, email và các dịch vụ mới có thể được thực hiện dựa trên giao thức TCP, đây là giao thức đảm bảo tin cậy do phía client có thể gửi những phản hồi về phía server. Dựa trên thông điệp phản hồi, các ứng dụng dịch vụ có thể nhận biết được cả hai quá trình bắt đầu và kết thúc của một giao dịch tại client. Cùng với các chức năng thông thường, các ứng dụng dịch vụ cũng có thể ghi nhận được sự thay đổi về hoạt động của dịch vụ thông qua thời gian chờ đợi phản hồi từ một giao dịch khác. Các thông tin này thường được lưu trong các file log hay được phân tích và thống kê chi tiết hơn bởi chức năng quản lý của bản thân ứng dụng. Để đánh giá hoạt động của hệ thống, chúng ta có thể khai thác nguồn thông tin này. Ngoài ra, chúng ta cũng có thể thu nhận được thông tin bằng cách tự thu thập dựa trên các quy tắc quản lý thông tin mà các dịch vụ tuân theo.
- **Máy trạm:** Thành phần kiểm tra của dịch vụ web phía client có thể sử dụng những phương pháp đo để đánh giá khả năng hoạt động của ứng dụng phía client sử dụng những công cụ phần mềm đặc biệt, trong môi trường mạng thử nghiệm, ta có thể dùng các công cụ hỗ trợ chuyên dụng cho mạng IPv6 như COLD, Ethereal, MRTG...
- **Những thiết bị kiểm tra đặc biệt :** Những thiết bị kiểm tra đặc biệt có thể được dùng để theo dõi quá trình truyền thông trên mạng và phân tích những gói tin để đưa ra đánh giá về chất lượng mạng và dịch vụ.

2.5.2 Các dịch vụ thử nghiệm

Đo kiểm dịch vụ Mail

Kiểu đo

Dịch vụ thư điện tử là một trong những dịch vụ phổ thông trong các dịch vụ mạng. Điều đó có nghĩa, thư điện tử là dịch vụ có tần suất sử dụng cao hơn so với các dịch vụ khác như FTP, telnet. Do vậy, khi đánh giá chất lượng dịch vụ trên kết quả đo đối với dịch vụ này, ta cần chú ý tới hai tiêu trí chính. Thứ nhất là khả năng tương tác giữa một người sử dụng với nhiều người sử dụng khác nhau và sử dụng dịch vụ thư điện tử của các nhà cung cấp khác nhau. Thứ hai là tính ổn định và tin cậy của người dùng đó khi sử dụng dịch vụ thư điện tử của một nhà cung cấp với tần suất sử dụng lớn.

Khi thực hiện đánh giá và tiến hành đo thử dịch vụ thư điện tử, ta vẫn cần tính đến những ảnh hưởng của hệ thống mạng hiện tại lên hệ thống đang tiến hành đo thử nghiệm. Đối với việc kiểm tra các ảnh hưởng đó, sử dụng kiểu đo bị động để đánh giá là phù hợp.

Mỗi người sử dụng dịch vụ mail có thể gửi nhận mail tới nhiều địa chỉ khác nhau, mỗi địa chỉ đó được đặc tả bởi các hệ thống mạng khác nhau. Điều đó có nghĩa là hệ thống mạng của người gửi và nhận mail có thể giống nhau hoặc có thể sẽ khác nhau, ở đây bao gồm cả các thiết bị phần cứng, hệ thống đường truyền cũng như phần mềm điều khiển và cơ chế định tuyến, chuyển tiếp giữa các tên miền. Do vậy, nếu sử dụng phương pháp đo bị động để đánh giá chất lương dịch vụ thư điện tử sử dụng cùng một giao thức, ví dụ giao thức SMTP/POP3, thì sẽ phải sử dụng đến tất cả các phần mềm giám sát đặt tại các máy chủ thư điện tử tại các mạng khác nhau. Trên thực tế, điều đó là không thể với mô hình mạng diện rộng. Tuy nhiên, với mô hình mạng diện rộng nhưng số lượng nút mạng không nhiều như mạng thử nghiệm IPv6, việc sử dụng phương pháp đo kiểu bị động vẫn có thể chấp nhận được.

Mặt khác, nếu thay vì sử dụng một phần mềm đánh giá chất lượng dịch vụ thư điện tử, ta sử dụng các phần mềm gửi nhận thư điện tử khác nhau tại các máy trạm; đồng thời tiến hành gửi và nhận đến các địa chỉ khác nhau tương ứng với các máy chủ thư điện tử khác nhau, trên cơ sở đó, đánh giá được năng lực hoạt động của máy chủ thư điện tử, đường truyền, khả năng đáp ứng,.. và như vậy, đánh giá được chất lượng dịch vụ mạng đối với dịch vụ thư điện tử.

Tóm lại, với dịch vụ thư điện tử, sử dụng được đồng thời cả hai phương pháp đo kiểu chủ động và bị động sẽ thu được những kết quả đo chính xác hơn so với việc sử dụng một trong hai phương pháp đo. Tuy nhiên, nếu so sánh hai phương pháp trong trường hợp này thì kiểu đo chủ động có nhiều ưu điểm hơn, trong đó nổi bật là khả năng triển khai đo thực tế dễ dàng hơn. Phần tiếp theo sẽ trình bày chi tiết các phương pháp, cách thức đo dịch vụ thư điện tử trên cơ sở đánh giá chất lượng đáp ứng dịch vụ của mail server và người sử dụng dịch vụ tương ứng.

Phương pháp đo

Quá trình gửi mail

Các tham số quan trọng sau ảnh hưởng trực tiếp đến quá trình gửi nhận thư:

- Thời gian thiết lập liên kết TCP.
- Thời gian thiết lập liên kết giữa bên nhận và bên gửi mail.
- Thời gian truyền dữ liệu.

Thông qua các tham số này, ta có thể đánh giá được khả năng đáp ứng của hệ thống máy chủ mail khi tiếp nhận một số lượng lớn các yêu cầu phục vụ từ các tài khoản truy nhập khác nhau.

Bằng cách sử dụng một ứng dụng mail client hỗ trợ IPv6 trên Linux như FetchMail 5.9.0 hoặc NTEmacs trên Windows, phần mềm này gửi các message đến các máy chủ mail khác nhau theo giao thức SMTP. Tiến hành ghi nhận lại thời gian gửi thư, số lượng thư gửi đi và số lượng thư nhận được, từ đó đưa ra đánh giá hệ thống dựa trên các kết quả thống kê đó.

Ta có thể tóm tắt quá trình đo như sau:

a. Gửi 100 đến 300 thư cùng một lúc từ nhiều trạm đến cùng một địa chỉ thư.

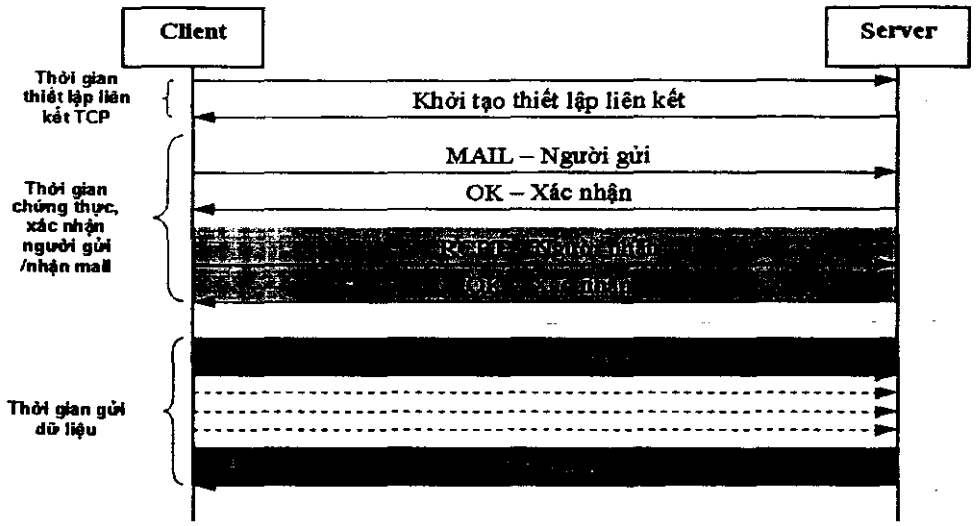
b. Kiểm soát các thư nhận được, đánh giá số lượng thư nhận được, thống kê và phân loại chúng.

c. Từ đó xây dựng tham số thông qua các thư nhận thành công:

   + Thời gian thiết lập kết nối với máy chủ qua cổng 25 với giao thức SMTP, tính đến khi nhận được trả lời từ server sau lệnh HELO.

   + Thời gian chuẩn bị truyền dữ liệu, tính từ lúc máy chủ tiếp nhận thành công lệnh MAIL từ phía client.

   + Thời gian truyền dữ liệu, tính từ lúc kết thúc lệnh DATA cho đến lúc đóng phiên truy nhập.



Hình 6 - Quá trình gửi thư

Quá trình nhận mail

Trong trường hợp này, các tham số dùng để đánh giá dựa trên cơ sở giao thức POP3.

- Thời gian thiết lập kết nối với máy chủ qua cổng 110 với giao thức POP3.
- Thời gian chờ phản hồi ACK từ máy chủ.
- Thời gian nhận toàn bộ dữ liệu mail.

Cũng tương tự như đánh giá các tham số trong quá trình gửi mail với giao thức SMTP, cũng sử dụng các ứng dụng trên để đồng thời nhận và gửi mail trên nền giao thức IPv6. Thông qua các ứng dụng này, người dùng cũng thực hiện các phiên đăng nhập vào hệ thống, chứng thực người dùng. Từ phía người dùng, ta đánh giá được khả năng đáp ứng của máy chủ, tốc độ truyền dữ liệu, đỗ trễ nhận / gửi mail.

Tóm tắt quá trình đo như sau:

a. Đăng nhập hòm thư bằng tài khoản.

b. Đánh giá kết quả đăng nhập, tổng số thời gian đăng nhập, sô lần đăng nhập không thành công.

c. Đối với lần đăng nhập thành công, thực hiện đo các tham số:

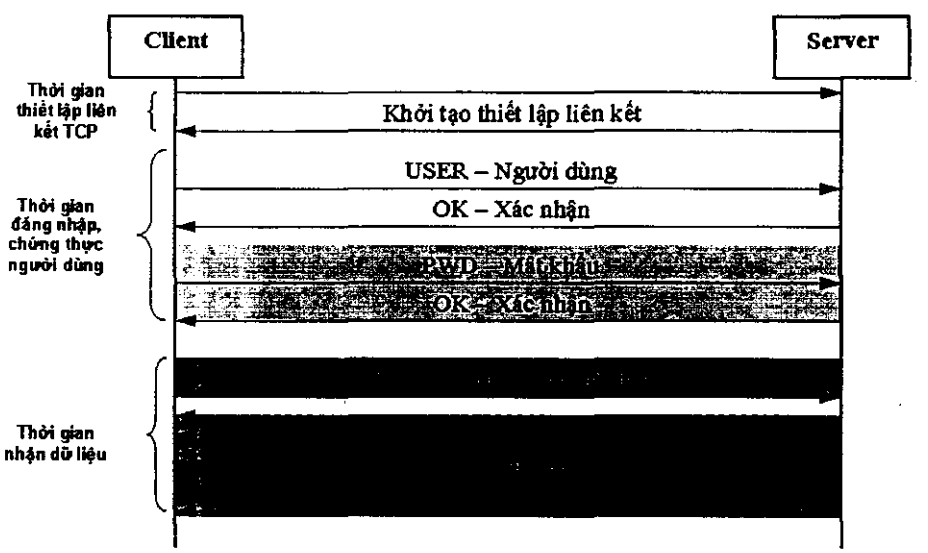
+ Thời gian thiết lập kết nối với máy chủ qua cổng 110 với giao thức POP3. Đây là khoảng thời gian cần thiết để thiết lập một liên kết TCP. Giá trị thời gian này quyết định

thời gian đáp ứng của máy chủ, từ đó có thể xác định được máy chủ này có đáp ứng được yêu cầu dịch vụ của hệ thống hay không.

+ Thời gian chờ trả lời của máy chủ khi tiếp nhận yêu cầu thực hiện kết nối. Khoảng thời gian này được xác định từ lúc máy chủ chấp nhận yêu cầu thiết lập liên kết TCP và gửi thông báo ACK về cho máy trạm.

+ Thời gian đăng nhập hệ thống, kiểm soát, chứng thực người dùng. Khoảng thời gian này được xác định từ lúc người dùng gửi thông tin tài khoản của mình (username/password) tới chứng thực tại máy chủ cho đến lúc máy chủ trả lời về máy trạm là chấp nhận hoặc không chấp nhận người dùng đó. Tương đương với thời gian giữa lúc bắt đầu gửi lệnh USER và lúc nhận trả lời lệnh PASS.

+ Thời gian nhận thư được xác định là khoảng thời gian từ từ lúc bắt đầu nhận dữ liệu cho đến lúc kết thúc quá trình nhận dữ liệu. Ở đây, một khối dữ liệu được hiểu là một đoạn dữ liệu tương ứng một bức thư. Tương đương với thời gian giữa lúc bắt đầu gửi lệnh RETR và lúc nhận toàn bộ dữ liệu.



Hình 7 - Quá trình nhận thư

Đo kiểm dịch vụ Web

Kiểu đo

Kể từ lúc một người sử dụng gửi đi yêu cầu sử dụng một dịch vụ web cho đến khi máy chủ của ISP cung cấp được dịch vụ đến tận web browser của người sử dụng đó là một quá trình gồm rất nhiều công đoạn khác nhau. Mỗi công đoạn đều có thể gây ra những ảnh hưởng

nhất định tới chất lượng của dịch vụ Web. Ví dụ khả năng xử lý của web browser, khả năng của thiết bị kết nối của người sử dụng, chất lượng đường truyền, khả năng xử lý của máy chủ cung cấp dịch vụ, vv. Do đó nếu chúng ta chỉ dùng một trong hai kiểu đo chủ động hoặc bị động, kết quả đo của chúng ta có thể không phản ánh chính xác được chất lượng dịch vụ.

Có một giải pháp là sử dụng kết hợp cả hai kiểu đo. Trong đó chúng ta sẽ sử dụng kiểu đo chủ động để giả lập ra các yêu cầu dịch vụ web gửi tới máy chủ web của ISP. Sau đó tiến hành ghi nhận thời gian nhận được các phản hồi từ phía máy chủ.

Đồng thời chúng ta cũng sử dụng phương pháp đo bị động để đánh giá khả năng hoạt động của liên kết mạng như đo round trip delay -độ trễ kể từ khi gửi một gói tin đến khi nhận được phản hồi, tỷ lệ dữ liệu được gửi đi, tỷ lệ mất gói tin,..Đây là các tham số đo đã được nhóm làm việc IPPM (IP Performance Metrics workgroup) của IETF nghiên cứu phát triển để soạn thảo các tiêu chuẩn cho Internet như RFC 2678, RFC 2026...

Phương pháp đo

Đo các tham số HTTP: Sử dụng một phần mềm giám sát đặt tại các client của web server. Phần mềm này sẽ sử dụng phương pháp đo chủ động để đánh giá khả năng hoạt động và khả năng sẵn sàng của web server. Giống như một web client thông thường, phần mềm giám sát dịch vụ sẽ thực hiện các bước sau để gửi những yêu cầu dịch vụ tới web server:

- Từ địa chỉ URL của web server, xác định địa chỉ IP
- Thiết lập một liên kết TCP với web server
- Gửi yêu cầu GET URL tới web server để yêu cầu truy nhập đến một trang web xác định
- Nhận lại phản hồi HTTP từ phía web server.

Bằng cách phân tích thông tin trong phần header của gói tin HTTP trả lại từ web server, chúng ta có thể xác định được khả năng thực sự của web server.

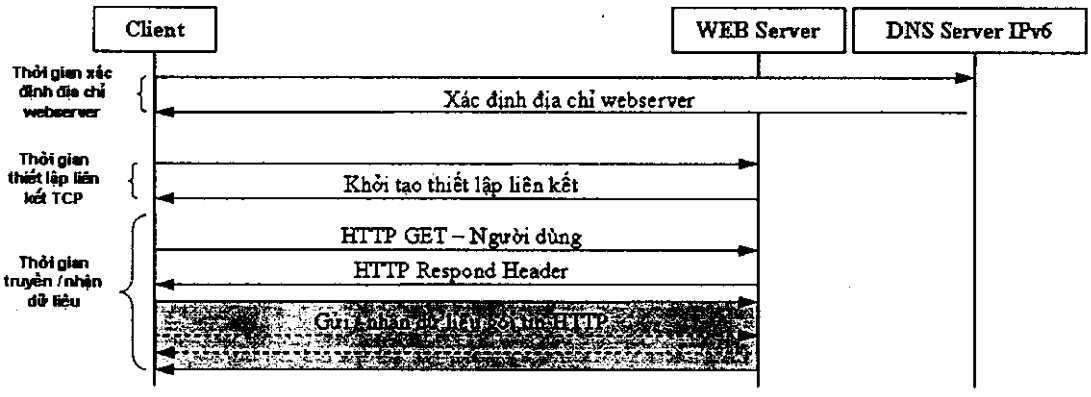
Quá trình đo có thể được mô tả như sau:

a. Từ phía một client bất kỳ, thực hiện các kết nối đến 100 website IPv6 của nước ngoài, các website được phân loại theo khu vực địa lý nếu tính tương đối các kết nối đến mạng 6BONE. Chi tiết danh sách các kết nối đến 6BONE tham khảo chi tiết tại phụ luc A.

b. Đánh giá kết quả kết nối, thống kê số web site không thực hiện kết nối được, phân xem chúng thuộc loại nào trong các loại web site đã đề cập ở trên.

c. Đối với các web site kết nối thành công, thực hiện bài đo dịch vụ web và đánh giá các tham số đo nhận được trong bài đo. Những tham số này bao gồm:

- Thời gian phân tích và chuyển đổi địa chỉ DNS: Đây là thời gian cần thiết để nhận được địa chỉ IPv6 tương ứng với địa chỉ URL mà người sử dụng truy nhập tới thông qua web browser. Như đã trình bày ở trên, các tham số liên kết mạng có ảnh hưởng trực tiếp đến giá trị thời gian này. Chính vì vậy chúng ta phải tiến hành đo song song cả khả năng hoạt động của liên kết mạng và so sánh với thời gian phân tích và chuyển đổi địa chỉ DNS để xác định thời gian xử lý DNS thực (*không phụ thuộc vào chất lượng mạng*). Tuy nhiên nếu giá trị này vẫn còn ở mức cao thì chúng ta có thể kết luận là hệ thống DNS có vấn đề.
- Thời gian thiết lập liên kết TCP. Thời gian cần thiết để thiết lập một liên kết TCP-IP (RFC 793). Nếu tham số này có giá trị lớn, chúng ta có thể kết luận là máy chủ web server có tính năng hoạt động kém hay đang có tắc nghẽn xảy ra tại máy chủ. (Sở dĩ như vậy vì mặc dù các liên kết TCP được thiết lập tại các cổng TCP và ứng dụng cung cấp dịch vụ sẽ thực hiện chờ tại các cổng này, nhưng việc thiết lập liên kết TCP lại thuộc về kernel của hệ điều hành máy chủ).
- Thời gian chờ phản hồi từ server: Thời gian kể từ lúc gửi yêu cầu GET URL cho tới khi nhận được byte đầu tiên của phần HTTP header phản hồi lại theo giao thức HTTP. Trong hầu hết các máy chủ, tham số này tương ứng với lượng thời gian cần thiết để định thời các yêu cầu, chuẩn bị các trang web trong bộ nhớ và thời gian gửi thông tin.
- Thời gian truyền dữ liệu : Đây là khoảng thời gian tính từ lúc nhận được phần header trả lời theo giao thức HTTP cho tới lúc quá trình nạp trang web đã hoàn tất.

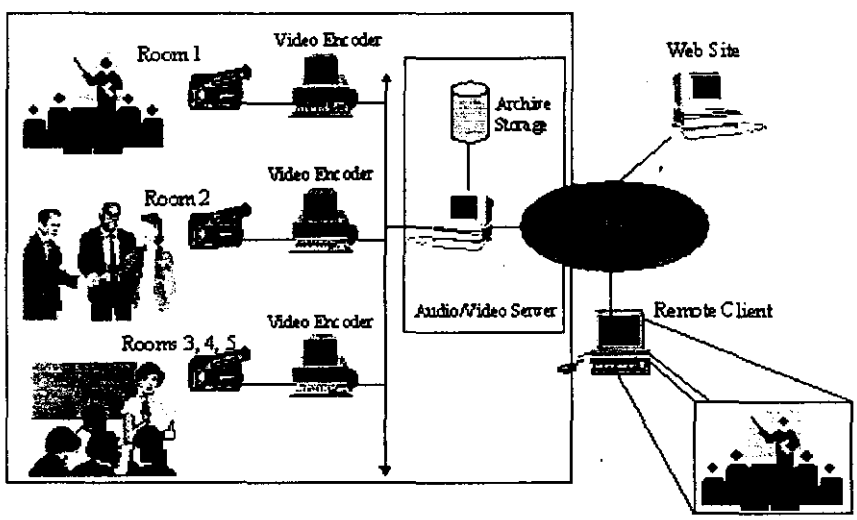


Hình 8 – Quá trình hoạt động của dịch vụ WEB

2.5.3 Công cụ phát triển tầng ứng dụng

Việc cài đặt thử nghiệm một số dịch vụ cơ bản nhằm mục đích đưa mạng thử nghiệm vào hoạt động ổn định. Vì IPv6 là giao thức thế hệ mới, nhiều công nghệ mới sẽ được triển khai trên nền tảng giao thức này. Mạng Ipv6 là một môi trường thuận lợi cho việc triển khai và phát triển các ứng dụng liên mạng, điều này mở ra một hướng đi mới trong việc phát triển các ứng dụng truyền thông nói chung và ứng dụng cho mạng thế hệ mới IPv6 nói riêng. Trong số đó, các nổi lên là các ứng dụng truyền thông multimedia.

Trên cơ sở hệ thống tương tác client – server dưới dạng lưu thông hình ảnh video số (Video Streaming) cho phép chuyển tiếp các dòng dữ liệu âm thanh hoặc hình ảnh tới các máy tính đã được cài đặt các ứng dụng Multimedia. Các ứng dụng multimedia tiếp nhận các lưu thông âm thanh/hình ảnh đó, giải nén và trình diễn. Kỹ thuật điều khiển luồng dữ liệu còn cho phép người dùng máy tính nghe âm thanh qua card âm thanh, từng phần hoặc toàn bộ dòng dữ liệu âm thanh đó.



Hình 9 - Mô hình ứng dụng Video trên nền IPv6

Các sản phẩm của các ứng dụng tương tác multimedia đó có thể là:

Lưu thông trình diễn hình ảnh trên Internet.

Các dịch vụ mã hoá tín hiệu số

Đào tạo, khám chữa bệnh từ xa

Truyền hình thương mại

Giới thiệu sản phẩm qua mạng Internet.

2.5.3.1 Ứng dụng Video LAN

VideoLAN là công cụ xử lý các lưu thông video số trên mô hình client – server. Các phiên bản của VideoLAN được xây dựng trên mã nguồn mở bằng C++ trên môi trường HĐH Linux, do vậy việc phát triển tiếp trên nền ứng dụng cũ là hoàn toàn khả thi. Tất nhiên VideoLAN cũng được phát triển trên nền các HĐH khác như BE OS, Windows và Mac OS X.

Một điểm quan trọng là VideoLAN có hỗ trợ IPv6, tuy nhiên bước đầu chỉ dừng lại ở thử nghiệm unicast, các thử nghiệm cho multicast chưa có đảm bảo sẽ đạt hiệu quả tốt. ứng dụng VideoLAN server tiếp nhận dòng Video đầu vào dưới dạng đĩa DVD, card Satellite, card mã hoá MPEG 2 hoặc dạng file MPEG-1 và MPEG-2. Chuẩn MPEG4/DivX được hỗ trợ trên bản Client, tuy nhiên việc xây dựng chuẩn MPEG4/DivX trên server là việc chưa thể triển khai ngay trong tương lai gần vì nhiều lý do khác nhau.

Ứng dụng VideoLan hiện tại hỗ trợ cho IPv6, do vậy mới chỉ được xây dựng và thử nghiệm trên mô hình điểm - điểm (*unicast*). Trong trước mắt, VideoLan chưa hỗ trợ đa điểm (*multicast*). Ứng dụng VideoLan-server có thể xử lý được các loại dữ liệu khác nhau như DVD, card mã hoá MPEG-2 hoặc MPEG-1 hoặc xử lý các files MPEGs. Tương ứng, các phiên bản dành cho máy trạm cũng đã hỗ trợ MPEG-4/DivX. Trong tương lai, ứng dụng máy chủ cũng sẽ hỗ trợ DivX.

Cài đặt VideoLAN

Được cài đặt trên cơ sở một ứng dụng mã nguồn mở, để chạy được ứng dụng, nhất thiết phải tiến hành cài đặt. Cú pháp lệnh cấu hnh và cài đặt VideoLAN như sau:

./configure
./make
./make install

VideoLAN sẽ hoạt động sau khi quá trình cấu hình và cài đặt được hoàn tất. Trong một số trường hợp, một số ứng dụng cụ thể sẽ đòi hỏi các thư viện nhất định, phù hợp với đặc tả các ứng dụng đó. Nếu không, một số chức năng sẽ không được kích hoạt. Ví dụ như với lưu thông DVD, nếu không có đầu đọc DVD tại máy chủ thì không nhất thiết cần đến gói thư viện hỗ trợ DVD đi kèm, ta có thể bỏ qua lựa chọn này trong cài đăt.

Cấu hình Server

VideoLAN chia làm hai pha chính là Client và Server, đối với phía server, cần thiết phải cấu hình lại cho phù hợp với hệ thống hiện tại.

Có hai files cấu hình chính là: vls.cfg và input.cfg. Trên Linux, hai files này trong thư mục **/usr/local/etc/videolan/vls/** sau khi cài đặt. File vls.cfg bao gồm các cấu hình chính của Server còn input.cfg chứa các cấu hình đầu vào cho lưu thông multimedia tới server, cấu hình kiểu lưu thông video tương ứng.

Chi tiết file cấu hình server tham khảo trong phụ lục của báo cáo.

Kích hoạt lưu thông multimedia

Để khởi tạo phiên lưu thông video, trước hết cần kết nối với ứng dụng điều khiển VideoLAN bằng telnet qua cổng đã được chỉ ra trong file vls.cfg (*mặc định là 9999*). Tên truy nhập và mật khẩu đã được khai báo chi tiết trong file cấu hình. Mỗi lần đăng nhập vào hệ thống, lệnh **help** sẽ được gửi đến server và nhận được các danh sách lệnh thực hiện tương ứng: **help, logout, start, stop, suspend, shutdown, browse, resume.**

Ví dụ, bắt đầu khởi tạo film1 tới máy trạm client1 từ máy chủ server1, cú pháp lệnh như sau:

Start film1 client1 server1

Lưu thông sẽ bắt đầu bằng việc xác định địa chỉ, cổng kết nối từ file cấu hình.

Ở phía client, kích hoạt VideoLAN Client nghe ở địa chỉ IPv6, cú pháp lệnh như sau:

Vlc udp6

Ngoài giao diện telnet, hiện tại, nhóm phát triển VideoLAN đã xây dựng website viết bằng ngôn ngữ Perl cho phép quản lý và điều khiển lưu thông dễ dàng hơn.

2.5.3.2 Ứng dụng MPEG4IP

MPEG4IP là ứng dụng mã nguồn mở có sẵn trên Internet tại địa chỉ ..... Ứng dụng này kết hợp các chức năng của một ứng dụng multimedia cung cấp các lưu thông audio-video trên nền giao thức IPv4/IPv6 sử dụng công nghệ mã hoá MPEG4.

Các gói tin của ứng dụng này bao gồm:

Phần mềm mã hoá/ chuyển đổi cung cấp nội dung hình ảnh và âm thanh theo yêu cầu.

Mp4live: module mã hoá MPEG4 theo thời gian thực. Với giao diện đồ hoạ, module này cho phép dễ dàng gửi / nhận các lưu thông video trên nền giao thức IPv4/IPv6 theo giao thức thời gian thực (RTP) và ghi nhận các lưu thông đó.

Mp4layer: module thực hiện việc chơi các file âm thanh và video trên mạng.

Cài đặt MPEG4IP

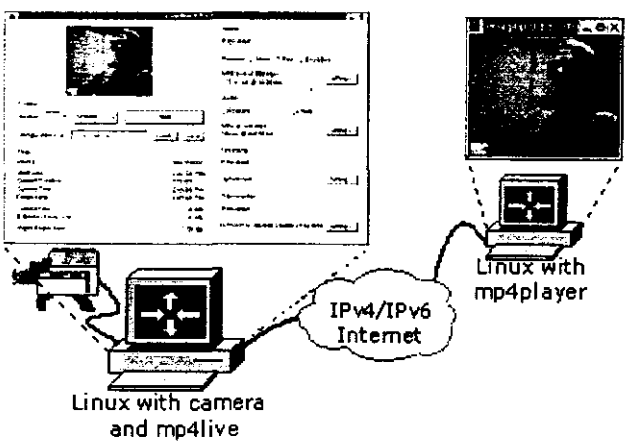
Bộ ứng dụng đóng gói của MPEG4IP tương thích với HĐH RedHat Linux 7.3, nhóm nghiên cứu của ISMA đã xây dựng và thử nghiệm thành công trên các HĐH khác như MacOS, BSD song nhóm khuyến cáo sử dụng Linux RedHat làm cơ sở chính cho các thử nghiệm. Gói ứng dụng MPEG4IP đã tích hợp các thư viện cần thiết để cài đặt và chạy chương trình thay vì phải tải các thư viện khác để hỗ trợ cài đặt. Để cài đặt, ta thực hiện các lệnh theo quy trình sau:

 # ./bootstrap --enable-ipv6

 # make

 # make install

Chú ý: Nếu không thêm tham số hỗ trợ IPv6 thì ứng dụng sẽ ngầm định giao thức hỗ trợ là IPv4.

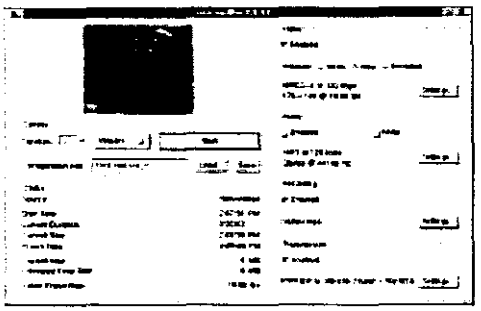


Hình 10 - Mô hình thử nghiệm của ISMA với MPEG4IP (MP4Live và MP4Player)

Sử dụng MPEG4IP

MPEG4IP là gói ứng dụng bao gồm hai thành phần chính là: MP4Live và MP4Player.

Sau khi kích hoạt MP4Live, giao diện cửa sổ đồ hoạ sẽ có dạng như minh hoạ dưới, ứng dụng cho phép cấu hình tất cả các tham số hỗ trợ dịch vụ như: tỉ lệ khung hình / giây, băng thông đường truyền, kích thước ảnh, địa chỉ máy đích,... MP4Live hỗ trợ cấu hình đơn giản (*fastconfig*) qua một nút Start, cho phép tự động tối ưu hoá các tham số.



Hình 11 - Giao diện đồ hoạ của MP4Live

Dưới đây là ba cách kích hoạt MPEG4IP với các tham số khác nhau:

MP4Player được dùng để chạy một file mp4 thông thường

 # mp4player capture.mp4

A. MP4Player nhận dòng video (*videostream*) từ MP4Live bằng cách đặc tả file xử lí tín hiệu số (*sdp – singal digital processing*) được tự động sinh ra bởi ứng dụng. File này phải được MP4Live kích hoạt từ trước. Sau khi khởi tạo truyền, MP4Player sẽ nhận file này như một bus dữ liệu và hiển thị nội dung của dòng dữ liệu lên màn hình.

 # mp4player capture.sdp

RSTP là giao thức phù hợp cho các truyền thông multimedia được phát triển bởi RealNetwork. Giao thức này xây dựng dựa trên cơ sở giao thức FTP hỗ trợ truyền nhận các file có kích thước lớn.

Darwin Streaming Server là ứng dụng mã nguồn mở phát triển bởi QuickTime sử dụng giao thức RTSP cho các lưu thông multimedia.

MP4Player nhận các lưu thông RTSP từ Darwin Server và hiển thị lên màn hình theo cú pháp:

 # mp4player rtsp://[ipv6_address]/capture.mp4

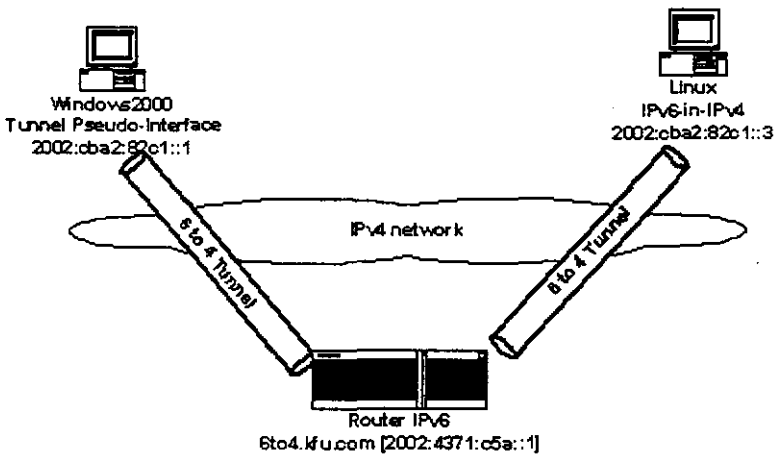
2.5.4 Công cụ phát triển tầng mạng

2.5.3.1. Ứng dụng DNS

DNS là một trong những dịch vụ quan trọng trên Internet. Như đã phân tích ở trên, ứng dụng BIND DNS phiên bản 9.0 trở lên đã hỗ trợ bản ghi AAAA đối với địa chỉ IPv6. Vì giao thức IPv6 chưa được sử dụng một cách chính thức trên mạng Internet nên phần lớn các lưu thông IPv6 đều được thực hiện trên nền IPv4. Dịch vụ DNS được thử nghiệm trên hai mô hình mạng : Mạng nhỏ và mạng diện rộng.

Mạng nhỏ

Hai máy tính kết nối với nhau thông qua một router chuyển tiếp IPv6/IPv4. Các kết nối đường ống IPv6 over IPv4 được cấu hình trên từng máy.



Hình 12 - Mô hình mạng nhỏ

Máy Linux được cài đặt phần mềm BIND DNS phiên bản 9.1.3. Ta giả định tên miền là ipv6.vnn.vn cho các giao dịch IPv6. Một điểm đáng lưu ý là sự giống nhau về cấu trúc của các dịch vụ DNS được sử dụng đồng thời trên IPv4 và IPv6, do vậy ở đây, các máy chủ DNS chạy IPv4 chỉ cần upgrade chế độ làm việc với bản ghi AAAA.

Mạng diện rộng

Một điểm quan trọng rằng trên thực tế, các máy chủ DNS đều được sử dụng để chạy đồng thời hai giao thức IPv4 và IPv6. Do đó, một vấn đề sẽ nảy sinh khi đưa IPv6 vào sử dụng, đó là phần lớn lưu thông các giao dịch được thông qua IPv4.

Việc cấu hình BindDNS được thực hiện chính trong file **/etc/namebd/named.conf**; đây là nơi lưu cấu hình các bản ghi địa chỉ tên miền. Ở đây có hai điểm đánh lưu ý là: cài file đặt tên miền và file tham chiếu ngược tên miền, hai files này quyết định việc kích hoạt dịch vụ IPv6. Dưới đây là một phần cấu hình bản ghi tên miền của file named.conf

```
zone "ipv6.vnn.vn" {
        type master;
        file "/var/named/ipv6.vnn.vn";
```

```
        };
    zone "2.A.B.C.2.0.0.2.IP6.INT" {
        type master;
        file "/var/named/2002.CBA2.ip6.int";
    };
```

Trước tiên, file ipv6.vnn.vn sẽ được gọi và nếu tạm thời, ta để cả địa chỉ IPv4 cho tên miền đó thì đồng thời cả hai địa chỉ IPv4 và IPv6 đều trỏ tới tên miền đó.

```
$TTL    38400
$ORIGIN ipv6.vnn.vn.
@       IN      SOA     ns.ipv6.vnn.vn. root.ns.ipv6.vnn.vn. (
                        2000000000      ;
                        10800           ;
                        1800            ;
                        864000          ;
                        86400 )         ;
                NS      ns.ipv6.vnn.vn.
                MX      10 mail.ipv6.vnn.vn.
localhost       A       127.0.0.1
                AAAA    0000:0000:0000:0000:0000:0000:0000:0001
ipv6-localhost  CNAME   localhost
unassigned      AAAA    0000:0000:0000:0000:0000:0000:0000:0000
ipv6-unassigned CNAME   unassigned

web6                    A       192.168.xxx.xxx
web6                    AAAA    2002:CBA2:82C3::1
web6                    A6      0 2002:CBA2:82C3::1
```

```
mail6           A       192.168.xxx.xxx
mail6           AAAA    2002:CBA2:82C3::1
mail6           A6      0 2002:CBA2:82C3::1

dns6            A       192.168.xxx.xxx
dns6            AAAA    2002:CBA2:82C3::1
web6            A6      0 2002:CBA2:82C3::1

office1v6       A       192.168.xxx.xxx
office1v6       AAAA    2002:CBA2:82C3::1
office1v6       A6      0 2002:CBA2:82C3::1

office2v6       A       192.168.xxx.xxx
office2v6       AAAA    2002:CBA2:82C1::1
office2v6       A6      0 2002:CBA2:82C1::1
```

File 2002.CBA2.82C1.ip6.int chứa các bản ghi tham chiếu ngược các địa chỉ IPv6 với các tên miền tương ứng.

```
$TTL    38400
$ORIGIN 2.A.B.C.2.0.0.2.IP6.INT.
@       IN      SOA     ns.ipv6.vnn.vn.     root.ipv6.vnn.vn. (
                        2000000000      ;
                        10800           ;
                        1800            ;
                        864000          ;
                        86400 )         ;
```

```
        IN    NS    ns.ipv6.vnn.vn.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0. 0.0.0.0.0.0.0.0.1.C.2.8   IN PTR  web6.ipv6.vnn.vn.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0. 0.0.0.0.0.0.0.0.1.C.2.8   IN PTR  mail6.ipv6.vnn.vn.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0. 0.0.0.0.0.0.0.0.1.C.2.8   IN PTR  dns6.ipv6.vnn.vn.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0. 0.0.0.0.0.0.0.0.1.C.2.8 IN PTR  office1v6.ipv6.vnn.vn.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0. 0.0.0.0.0.0.0.0.3.C.2.8 IN PTR  office2v6.ipv6.vnn.vn.
```

Để cho Bind DNS có thể đảm bảo được đáp ứng được đồng thời các yêu cầu và trả lời tra cứu tên miền, trong file named.conf cần bổ sung thêm dòng lựa chọn sau:

listen-on-v6 {any;};

trong phần các lựa chọn.

2.5.3.2. Ứng dụng Tcpdump – đo chất lượng dịch vụ mạng

Trên HĐH Linux, **tcpdump** là một ứng dụng kiểm soát lưu thông gói tin khá hiệu quả. Từ phiên bản 3.6 trở đi, **tcpdump** hỗ trợ IPv6.

Tcpdump sử dụng các biểu thức để lọc gói tin với ảnh hưởng của lưu thông kiểm soát gói tin nhỏ nhất. Đầu ra của **tcpdump** là header của các gói tin trên giao diện thỏa mãn những biểu thức lọc gói tin. Chúng ta có thể lấy một số ví dụ các bộ lọc gói tin mà **tcpdump** cung cấp :

- **icmp6**: bộ lọc thuần nhất các lưu thông ICMPv6
- **ip6:** bộ lọc thuần nhất các lưu thông IPv6 (đã bao gồm cả ICMPv6)
- **proto ipv6**: bộ lọc lưu thông đường ống IPv6-in-IPv4.
- **not port ssh**: hạn chế các gói tin trong chế độ SSH.
- Các dạng biểu thức bộ lọc gói tin(3 dạng) :
    - Type : host, net, port. Ví dụ "host ipv6.vdc.com.vn", "net ::1", "port 20". Mặc định của dạng thức là host.
    - Dir : chiều kết nối cần lọc gói tin. Bao gồm các biểu thức : src, dst, src or dst, src and dst. Ví dụ "dst ipv6.vdc.com.vn" capture tất cả các gói tin đi đến địa chỉ ipv6.vdc.com.vn

- Proto : các loại giao thức. **tcpdump** hỗ trợ các giao thức **ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp** và **udp**. Ví dụ : `ether src foo', `arp net 128.3', `tcp port 21'

Một số lệnh cơ bản cho phép kiểm soát và hiển thị các gói tin thông qua các gói tin ICMPv6:

- **"-s 512":** tăng kích thước của gói tin dò tìm lên 512 bytes
- **"-vv":** chi tiết các kết quả đầu ra

IPv6 ping tới 3ffe:ffff:100:f101::1 thông qua kết nối thông thường

 # tcpdump -t -n -i eth0 -s 512 -vv ip6 or proto ipv6

tcpdump: listening on eth0

3ffe:ffff:100:f101:2e0:18ff:fe90:9205 > 3ffe:ffff:100:f101::1: icmp6: echo

¬ request (len 64, hlim 64)

3ffe:ffff:100:f101::1 > 3ffe:ffff:100:f101:2e0:18ff:fe90:9205: icmp6: echo

¬ reply (len 64, hlim 64)

IPv6 ping tới 3ffe:ffff:100::1 định tuyến thông qua đường ống IPv6-in-IPv4

Các giá trị 1.2.3.4 và 5.6.7.8 là những điểm cuối đường ống (*tất cả các địa chỉ ở đây là giả định cho thử nghiệm*)

 # tcpdump –t -n -i ppp0 -s 512 -vv ip6 or proto ipv6

tcpdump: listening on ppp0

1.2.3.4 > 5.6.7.8: 2002:ffff:f5f8::1 > 3ffe:ffff:100::1: icmp6: echo request

¬ (len 64, hlim 64) (DF) (ttl 64, id 0, len 124)

5.6.7.8 > 1.2.3.4: 3ffe:ffff:100::1 > 2002:ffff:f5f8::1: icmp6: echo reply (len

¬ 64, hlim 61) (ttl 23, id 29887, len 124)

1.2.3.4 > 5.6.7.8: 2002:ffff:f5f8::1 > 3ffe:ffff:100::1: icmp6: echo request

¬ (len 64, hlim 64) (DF) (ttl 64, id 0, len 124)

5.6.7.8 > 1.2.3.4: 3ffe:ffff:100::1 > 2002:ffff:f5f8::1: icmp6: echo reply (len

¬ 64, hlim 61) (ttl 23, id 29919, len 124)

2.5.3.3 Ứng dụng IPerf đo băng thông và các đặc trưng mạng

IPerf là công cụ đo các thông số đặc trưng hiệu năng mạng. Dựa trên nền tảng phát triển của công cụ **ttcp**, **IPerf** cũng được phát triển dựa trên đánh giá hiệu năng băng thông gói tin TCP và UDP. **IPerf** đánh giá được giá trị cực đại của băng thông đường truyền và các tham số khác như độ trễ đường truyền (delay jitter) và tỉ suất mất gói tin.

IPerf có hỗ trợ cho các hệ điều hành khác nhau như Windows, Linux, FreeBSD, Sunsolaris,... do vậy thuận tiện trong việc cài đặt thử nghiệm tại các máy trạm. Mặt khác, từ phiên bản 1.6.2, **IPerf** đã hỗ trợ đầy đủ cho địa chỉ IPv6 mà không cần đòi hỏi các thư viện phức tạp khác.

Iperf là công cụ đo kiểm chủ động đòi hỏi cấu hình theo mô hình client/server. Dưới đây là cấu hình và kết quả ví dụ khi thử nghiệm ứng dụng **Iperf** với hai máy Server (Win2000, địa chỉ thử nghiệm 2002:cba2:82c4::cba2:82c4) và máy Client (SuSe Linux 8.0, địa chỉ thử nghiệm 2002:cba2:82c3::cba2:82c3).

Lần 1 :

Server chạy chế độ mặc định theo giao thức TCP

>Iperf –s –V

Server listening on TCP port 5001

TCP window size: 8.00 KByte (default)

---

[192] local [2002:cba2:82c4::cba2:82c4] port 5001 connected with
[2002:cba2:82c3::cba2:82c3] port 32937

[ID] Interval Transfer Bandwidth

[192] 0.0-10.0 sec 23.5 MBytes ***19.8 Mbits/sec***

Client kết nối tới server :

>Iperf –c 2002:cba2:82c4::cba2:82c4 –V

Lần 2 :

Server chạy chế độ mặc định theo giao thức UDP

>iperf -s -u -l 32K -w 128K -i 1

Server listening on UDP port 5001

Receiving 32768 byte datagrams

UDP buffer size: 128 KByte

---

[140] local [2002:cba2:82c4::cba2:82c4] port 5001 connected with [2002:cba2:82c3::cba2:82c3] port 32771

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[140] 0.0- 1.0 sec	1.69 MBytes	18.9 Mbits/sec	8.915 ms	0/ 54 (0%)
[140] 1.0- 2.0 sec	1.72 MBytes	19.4 Mbits/sec	8.878 ms	0/ 55 (0%)
[140] 2.0- 3.0 sec	1.69 MBytes	19.2 Mbits/sec	8.619 ms	0/ 54 (0%)
[140] 3.0- 4.0 sec	1.69 MBytes	19.2 Mbits/sec	9.636 ms	0/ 54 (0%)
[140] 4.0- 5.0 sec	1.72 MBytes	19.4 Mbits/sec	10.760 ms	0/ 55 (0%)
[140] 5.0- 6.0 sec	1.69 MBytes	19.2 Mbits/sec	8.585 ms	0/ 54 (0%)
[140] 6.0- 7.0 sec	1.72 MBytes	19.2 Mbits/sec	9.005 ms	0/ 55 (0%)
[140] 0.0- 7.0 sec	11.9 MBytes	19.2 Mbits/sec	9.799 ms	0/ 382 (0%)

Chương 3: ĐÁNH GIÁ KẾT QUẢ

3.1 Kết quả thử nghiệm các dịch vụ và công cụ phát triển

3.1.1 Kết quả thử nghiệm các dịch vụ cơ bản

3.1.1.1 Dịch vụ Web Server

Bảng 3 : Kết quả thử nghiệm dịch vụ Web

Lần thử	Dung lượng file (KB)	Thời gian download (IPv6-tính bằng giây)	Tốc độ download (IPv6-KBps)	Thời gian download (IPv4-tính bằng giây)	Tốc độ download (IPv4)
1	512	25	20.48	26	19.69
2	512	26	19.69	24	21.33
3	512	26	19.69	24	21.33
4	1024	51	20.08	49	20.90
5	1024	50	20.48	50	20.48
6	1024	53	19.32	52	19.69
7	2048	102	20.08	102	20.08
8	2048	101	20.28	103	19.88
9	2048	102	20.08	100	20.48
10	4096	203	20.18	203	20.18
11	4096	206	19.88	204	20.08
12	4096	204	20.08	201	20.40
13	16384	810	20.18	812	20.18
14	16384	805	20.35	803	20.40
15	16384	806	20.33	803	20.40
16	32768	1630	20.10	1626	20.15
17	32768	1624	20.18	1630	20.10

18	32768	1624	20.18	1633	20.07
19	65536	3251	20.16	3259	20.11
20	65536	3284	19.96	3285	19.95
			20.09		**20.29**

Phần mềm sử dụng : **Apache-2.0.45 for Linux**

Tỉ lệ kết nối thành công : 100%

Download file trên 500K (20 lần/files/máy tính) : thành công 100%

Tốc độ download trung bình IPv6 : 20.09 KB/s

Tốc độ download trung bình IPv4 : 20.29 KB/s

Nhận xét : Dịch vụ Web Server chạy tốt, kết nối được với các website có địa chỉ IPv6 trong nước cũng như nước ngoài. Hiệu năng của dịch vụ này không thua kém so với dịch vụ Web Server của IPv4, đáp ứng được đầy đủ các chức năng của dịch vụ tương tự được chạy trên nền IPv4.

3.1.1.2 Dịch vụ FTP

Bảng 4: kết quả thử nghiệm dịch vụ FTP

Lần thử	Dung lượng file (KB)	Thời gian download/upload (IPv6-tính bằng giây)	Tốc độ (IPv6-KBps)	Thời gian download/upload (IPv4-tính bằng giây)	Tốc độ (IPv4-KBps)
1	512	43	11.91	45	11.38
2	512	44	11.64	42	12.19
3	512	43	11.91	44	11.64
4	1024	85	12.05	85	12.05
5	1024	89	11.51	84	12.19
6	1024	87	11.77	85	12.05
7	2048	169	12.12	170	12.05

8	2048	165	12.41	172	11.91
9	2048	167	12.26	167	12.26
10	4096	342	11.98	343	11.94
11	4096	339	12.08	340	12.05
12	4096	335	12.23	338	12.12
13	16384	1342	12.21	1346	12.17
14	16384	1350	12.14	1349	12.15
15	16384	1333	12.29	1340	12.23
16	32768	2670	12.27	2677	12.24
17	32768	2681	12.22	2675	12.25
18	32768	2675	12.25	2667	12.29
19	65536	5350	12.25	5353	12.24
20	65536	5370	12.20	5364	12.22
			12.08		12.08

Phần mềm sử dụng : **Proftpd-1.2.8 for Linux (cho server)**

WS_FTP Pro 7.04 (cho client-WINDOWS)

NC_FTP-3.1.5 (cho client-Linux)

Tỉ lệ kết nối thành công : 100%

Download/Upload các file có kích thước lớn hơn 5MB(20 lần /Địa chỉ/ Máy tính) : thành công 100%

Tốc độ upload/download trung bình IPv6 : 12.08 KB/s

Tốc độ upload/download trung bình IPv4 : 12.08 KB/s

Nhận xét : Dịch vụ FPT Server chạy tốt, cho phép thực hiện các chức năng download và upload với tốc độ tương đương trên môi trường IPv4. Ngoài ra, hệ thống cũng đáp ứng được các chức năng thông thường khác của một phần mềm FTP server và client, do các chức năng này không phụ thuộc vào địa chỉ IPv6 hay IPv4(phân quyền, các lệnh FTP...)

3.1.1.3 Dịch vụ Mail

Bảng 5: Kết quả thử nghiệm dịch vụ Mail

Lần thử	Dung lượng file (KB)	Thời gian gửi/nhận (IPv6)	Tốc độ (IPv6-KBps)	Thời gian gửi/nhận (IPv4)	Tốc độ (IPv4-KBps)
1	200	34	5.88	35	5.71
2	200	35	5.71	33	6.06
3	200	34	5.88	33	6.06
4	400	70	5.71	70	5.71
5	400	71	5.63	69	5.80
6	400	70	5.71	72	5.56
7	800	139	5.76	141	5.67
8	800	142	5.63	140	5.71
9	800	143	5.59	141	5.67
10	1600	285	5.61	286	5.59
11	1600	286	5.59	281	5.69
12	1600	284	5.63	284	5.63
13	3200	566	5.65	570	5.61
14	3200	567	5.64	561	5.70
15	3200	566	5.65	566	5.65
16	6400	1126	5.68	1127	5.68
17	6400	1128	5.67	1123	5.70
18	6400	1124	5.69	1120	5.71
19	12800	2246	5.70	2240	5.71
20	12800	2249	5.69	2250	5.69
			5.69		5.72

Phần mềm sử dụng : **SendMail-8.9.3 for Linux (cho server)**

NTEmacs (cho client-WINDOWS)

FetchMail-5.9.0 (cho client – LINUX)

Tỉ lệ gửi nhận thành công : 100%

Gửi/nhận email liên tục 20 lần, mỗi lần attach một file có kích thước lớn hơn 200KB : thành công 100%

Tốc độ gửi/nhận trung bình IPv6 : 5.69 KB/s

Tốc độ gửi/nhận trung bình IPv4 : 5.72 KB/s

Nhận xét : Dịch vụ Mail-Server chạy tốt, cho phép gửi nhận mail có file đính kèm với hiệu năng tương đương với dịch vụ trong môi trường IPv4. Ngoài ra, hệ thống cũng đáp ứng được các chức năng thông thường khác của một phần mềm Mail server và client, do các chức năng này không phụ thuộc vào địa chỉ IPv6 hay IPv4(phân quyền, các lệnh Mail...)

Với các kết quả thử nghiệm này, chúng ta có thể thấy rằng các dịch vụ cơ bản chạy thuần môi trường IPv6 có tốc độ và hiệu năng trung bình không thua kém các ứng dụng tương tự trong môi trường IPv4. Ngoài ra, môi trường IPv6 chỉ ảnh hưởng tới việc đánh địa chỉ trong tầng Network mà không ảnh hưởng tới các tầng dịch vụ ở trên, do vậy các chức năng khác của các dịch vụ cơ bản không liên quan tới việc đánh địa chỉ đều không bị ảnh hưởng và chạy tốt trong môi trường IPv6.

3.1.2 Kết quả thử nghiệm tầng ứng dụng

Kết quả thử nghiệm tầng ứng dụng tập trung chủ yếu vào việc thử nghiệm các ứng dụng Video số. Nhìn chung, các ứng dụng này đều hoạt động được trong môi trường IPv6, xử lý tốt các vấn đề liên quan tới địa chỉ IPv6, tuy vậy còn khá nhiều những điểm cần khắc phục vì các ứng dụng này cũng đang trong giai đoạn thử nghiệm (ví dụ, ứng dụng **VideoLAN** chưa hỗ trợ multicast mà mới chỉ hỗ trợ unicast).

Đối với tầng ứng dụng, có thể nói là hiện tại chưa có một phân lớp ứng dụng nào đối với Internet lại bắt buộc cần IPv6 để có thể chạy (do các ứng dụng IPv6 hiện tại chủ yếu là viết lại các ứng dụng đã có trên nền IPv4 để phù hợp với IPv6). Hiện tại các ứng dụng này có thể phân chia thành các nhóm sau :

- Wrapper đối với ứng dụng IPv4
- Truyền File (FTP,TFTP,RSYNC...)
- Email (Webmail, Mail Tranfer Agents và Mail User Agents, Mailbox deamon...)
- Domain Name System (DNS)

- HTTP (HTTP,HTTPS...)
- News (NNTP)
- Chat (IRC)
- LDAP
- Security
- Remote Access
- Proxy and Cache
- Multimedia
- Các ứng dụng khác...

Việc chọn các ứng dụng media, mà cụ thể là các ứng dụng Video số chủ yếu nhằm vào mục đích thử nghiệm các công cụ mới (chưa hoàn thiện đối với ngay cả môi trường IPv4) và đòi hỏi xử lý một lượng gói tin khá lớn, cũng như xử lý một khối lượng địa chỉ IPv6 khá lớn. Ngoài ra các ứng dụng khác cũng đã được các nhóm nghiên cứu khác thử nghiệm thành công, nhưng không hội tụ đủ hai tính chất nói trên nên không được nhóm thử nghiệm đưa vào nghiên cứu.

Hiện tại, với các thử nghiệm tại mạng cục bộ và mạng thử nghiệm kết nối VNN (phần VI.1.2) tại hai đầu Hà Nội-Thành phố Hồ Chí Minh đều cho chất lượng Video trực quan (tốc độ khung hình) tương đương với các thử nghiệm thuần IPv4. Kết quả này cho chúng ta kết luận khả quan về phương diện kết nối và chuyển dữ liệu qua mạng thuần IPv6, tuy vậy còn cần phải có nhiều thử nghiệm thêm với các mô hình multicast mới có thể đánh giá được thực sự năng lực xử lý dữ liệu đối với các nhóm địa chỉ multicast qua mô hình IPv6 diện rộng.

Ngoài các ứng dụng đã thử nghiệm nói trên, hiện tại trên thế giới cũng đã có những thử nghiệm multicast khác đối với IPv6, ví dụ như các trò chơi qua mạng, IRC (Internet Relay Chat). Do thời gian và môi trường thử nghiệm còn hạn hẹp, nhóm thử nghiệm chưa có những đánh giá chính thức được về các ứng dụng này (quy mô trao đổi dữ liệu nhỏ) , tuy vậy sơ bộ khi sử dụng cũng đã mang lại những kết quả tốt.

3.1.3 Kết quả thử nghiệm tầng mạng :

Việc thử nghiệm tầng mạng tập trung vào các ứng dụng có liên quan tới việc xử lý các gói tin IPv6. Các ứng dụng **tcpdump** và **Iperf** qua quá trình thử nghiệm đều thực hiện được đầy đủ các chức năng can thiệp tới tầng Network (phân tích gói tin để lấy địa chỉ, tạo gói tin mới với địa chỉ định trước...), tầng sử dụng các địa chỉ IPv6 làm đầu vào cho các chức năng của mình. Với việc làm chủ được các công cụ này, ít nhất chúng ta cũng có các công cụ chuẩn trong môi trường IPv6 để thực hiện các tác vụ liên quan tới tầng Network, sau đó với mạng

IPv6 thử nghiệm triển khai hoàn thành, có thể xây dựng tiếp các ứng dụng tùy theo yêu cầu cần thiết.

Ví dụ :

- Với mô hình capture gói tin như **tcpdump**, chúng ta có thể xây dựng các công cụ để debug, quản lý gói tin (proxy), thống kê các gói tin, một số vấn đề liên quan tới topology mạng...
- Với mô hình sử dụng ICMPv6 và các kỹ thuật tạo gói tin như trong **Iperf**, chúng ta có thể xây dựng và áp dụng các thuật toán đang được nghiên cứu trên thế giới để tạo ra các công cụ đo kiểm mạng, test các thông số của mạng, một số vấn đề liên quan tới topology mạng....

Trong thời điểm hiện tại, kết quả thử nghiệm tầng mạng cho chúng ta thấy việc can thiệp tới địa chỉ mạng như trong môi trường IPv4 là hoàn toàn khả thi và không quá khó khăn. Với các công cụ như trên, nếu chúng ta xây dựng một ứng dụng phân tích và tác động tới tầng mạng như trên với đồng thời cả hai môi trường IPv4/IPv6 thì sẽ rất hữu ích cho việc debug trong quá trình chuyển đổi IPv4 sang IPv6.

3.2 Đánh giá kết quả thử nghiệm

Với đề tài nghiên cứu này, nhóm nghiên cứu đã có những bước áp dụng lý thuyết vào việc triển khai các mô hình mạng IPv6 khác nhau, thu được một số kết quả nhất định. Cho đến nay, nhóm nghiên cứu đã làm chủ được các kỹ thuật triển khai IPv6 trên mạng cục bộ, một số kinh nghiệm triển khai mạng diện rộng và đặc biệt là triển khai đối với mạng IPv6 quốc tế, các kỹ thuật chuyển đổi IPv4/IPv6. Việc triển khai được tiến hành theo đúng trình tự và mô hình từ nhỏ đến lớn, từ đơn giản đến phức tạp để có thể rút kinh nghiệm sau mỗi lần triển khai áp dụng vào các mô hình lớn hơn (mô hình mạng cục bộ -> mô hình mạng diện rộng trong nước -> mô hình mạng diện rộng kết nối với quốc tế).

Đối với mô hình mạng cục bộ, nhóm thử nghiệm đã thử nghiệm thành công mô hình kết nối đường ống 6to4 giữa hai máy qua một Router IPv6 hỗ trợ 6to4. Ngoài ra, trong đề tài "Triển khai mạng thử nghiệm IPv6 kết nối VNN", nhóm thử nghiệm cũng đã triển khai mạng thuần IPv6 cục bộ tại mỗi đầu Hà Nội – Thành phố Hồ Chí Minh, thử nghiệm thành công một số ứng dụng trên nền IPv6.

Đối với mô hình mạng diện rộng kết nối trong nước, nhóm thử nghiệm đã kết nối thành công các mạng cục bộ tại hai đầu, làm chủ các kỹ thuật cấu hình router kết nối các mạng thuần IPv6 qua môi trường IPv4. Ngoài ra, nhóm thử nghiệm cũng đã kết nối thành công mạng thử nghiệm IPv6 với mạng VNN4 chạy trên nền giao thức IPv4. Việc thử nghiệm thành công chức năng dial-up, tuy còn một số khó khăn cần giải quyết nhưng bước đầu đã chứng tỏ khả năng thay thế của IPv6 đối với IPv4 trong mảng cung cấp dịch vụ dial-up này.

Đối với mô hình mạng diện rộng kết nối quốc tế, nhóm thử nghiệm đã triển khai mô hình lý thuyết kết nối với mạng thử nghiệm 6BONE quốc tế. Nhóm thử nghiệm cũng đã kết nối thành công với đối tác Singtel, qua đó kết nối thử nghiệm với mạng 6BONE quốc tế, đi theo đúng lộ trình đã nêu ở trên. Các dịch vụ cũng đã được từng bước thử nghiệm trên diện rộng quốc tế. Việc cấu hình các thiết bị để đấu nối quốc tế không quá khó khăn vì hầu hết các hệ điều hành chạy trên các thiết bị này (router,switch...) đều hỗ trợ tốt đối với IPv6. Hy vọng nhóm thử nghiệm sẽ tiếp tục được thực hiện các bước kết nối với mạng IPv6 trong các bước tiếp theo để sớm thúc đẩy mạng IPv6 Việt Nam cũng như có được các kinh nghiệm trên mạng diện rộng quốc tế.

Việc triển khai thử nghiệm các mô hình IPv6 đã đi được bước đầu thành công, tuy vậy cần nhanh chóng thực hiện tiếp các bước trong lộ trình kết nối mạng quốc tế để chuẩn bị cho việc hình thành mạng IPv6 của Việt Nam sau này. Ngoài ra cũng cần phải chú trọng tới việc thử nghiệm các dịch vụ và ứng dụng để cung cấp cho khách hàng và người sử dụng, từng bước thay thế và mở rộng mạng VNN4 hiện tại.

Kết luận và khuyến nghị

Sau quá trình nghiên cứu và thử nghiệm triển khai kết nối mạng IPv6, nhóm đề tài đã đưa ra phương án và kế hoạch chuyển đổi từ mạng IPv4 lên IPv6 trong đó sử dụng phương pháp làn sóng đôi (Dual-Layer) cho phép IPv6 và IPv4 chạy song song và phương pháp đường ống thủ công cho phép IPv6 chạy trên IPv4.

Quá trình thử nghiệm đã đạt được một số kết quả rất khả quan như:

- Kết nối mạng IPv6 với Singtel
- Kết nối mạng IPv6 của Việt Nam với mạng IPv6 của 6bone thông qua Singtel
- Kết nối mạng IPv6 là vnn4 giữa Hà Nội và thành phố Hồ Chí Minh
- Đang hoàn tất thủ tục cấp địa chỉ IPv6

Nhóm đề tài cũng đã thử nghiệm một số loại hình dịch vụ truyền thống như: Web Server, Mail, FTP và đánh giá chất lượng dịch vụ mà IPv6 cung cấp cũng tương đương với IPv4. Qua đó có thấy, ngoài những ưu điểm vượt trội như khả năng mở rộng địa chỉ, bảo mật và chất lượng dịch vụ, IPv6 còn đáp ứng tốt được các yêu cầu của IPv4.

Đề tài được thực hiện trong một thời gian không dài, tuy vậy cũng đã có được những thành công nhất định, mà đặc biệt là việc triển khai thành công mạng thử nghiệm IPv6 diện rộng trong nước, sau đó kết nối với mạng IPv6 quốc tế, tạo tiền đề cho những nghiên cứu và triển khai chuyển đổi thật sự trong tương lai. Tuy còn gặp những khó khăn về thời gian và nhất là việc chưa có khách hàng thử nghiệm, đề tài đã đưa ra được những kết quả tương đối thuyết phục về việc thử nghiệm kết nối và hiệu năng của các dịch vụ/ứng dụng thử nghiệm trong không gian địa chỉ mới, địa chỉ IPv6.