**BỘ GIÁO DỤC VÀ ĐÀO TẠO**
**TRƯỜNG ĐẠI HỌC HOA SEN**
**KHOA KHOA HỌC VÀ CÔNG NGHỆ**

# KHÓA LUẬN TỐT NGHIỆP

*Tên đề tài:*

## Vyatta, giải pháp thay thế Cisco cho doanh nghiệp

Giảng viên hướng dẫn : Đinh Ngọc Luyện

Nhóm sinh viên thực hiện : Trần Thanh Hùng – 061372

: Ngô Trọng Nghĩa - 060440

Lớp : VT062

Tháng 12 /năm 2010

# TRÍCH YẾU

Trong những năm trở lại đây, sự bùng nổ mạnh mẽ của Công Nghệ Thông Tin đã có những tác động nhất định đến mọi mặt của đời sống xã hội. Đặc biệt là sự ra đời của các công nghệ mạng máy tính đã thực sự làm thay đổi mọi thứ. Đối với các doanh nghiệp, việc triển khai hệ thống mạng được xem như là yếu tố quyết định then chốt đến việc hoạt động và bảo mật thông tin của cả công ty. Để việc triển khai được đạt hiệu quả cao nhất, việc lựa chọn các thiết bị mạng cho hệ thống cũng đòi hỏi sự kỹ lưỡng và cẩn thận sao cho phù hợp với tài chính và cơ sở vật chất hiện hành. Cisco luôn là lựa là lựa chọn hàng đầu đối với các nhà quản trị mạng bởi tính ổn định và bảo mật cao. Có thế nói trong lĩnh vực này, Cisco luôn dẫn đầu. Tuy nhiên trong một vài năm trở lại đây, sự xuất hiện của hệ thống router mã nguồn mở Vyatta đã làm cho ngành công nghệ mạng sôi nổi trở lại. Với giá cả rẻ hơn nhiều lần so với Cisco, tính ổn định và có đầy đủ các tính năng, cơ chế bảo mật khiến cho Vyatta nhanh chóng được chú ý là được đánh giá sẽ trợ thành đối thủ nặng kí cho Cisco. Trong qua các kiến thức đã học được ở trường, tìm hiểu thêm thông tin trên các diễn đàn trong và ngoài nước, cũng như sự sự tình giúp đỡ của giáo viên hướng dẫn. Nhóm chúng tôi đã nghiên cứu về hệ thống mã nguồn mở Vyatta nhằm giúp cho mọi người có có thêm cái nhìn tổng quan, rộng hơn về router mã nguồn mở Vyatta. Các tính năng của router Vyatta khá nhiều và gần như tương đương với router Cisco. Do thời gian và tài liệu về sản phẩm có hạn nên nhóm chúng tôi sẽ  nghiên cứu về các vấn đề sau

- Tổng quan về các sản phẩm mà Vyatta hiện đang có
- Tính năng trên các interfaces
- Tính năng về các services
- Tính năng về availability
- Tính năng về routing
- Tính năng về security

# MỤC LỤC

# LỜI CẢM ƠN

Do thời gian và kiến thức có hạn nên bài viết còn hạn chế, nhóm sinh viên rất mong nhận được sự góp ý của quý thầy cô, cùng các bạn sinh viên để hoàn thiện thêm kiến thức trong lĩnh vực này.

Qua đây, nhóm sinh viên bày tỏ lòng tri ân sâu sắc đến:

- Thầy Đinh Ngọc Luyện đã giúp đỡ và nhiệt tình hướng dẫn, tạo điều kiện để nhóm sinh viên hoàn thành khoá luận tốt nghiệp này
- Các thầy cô và cách anh kỹ thuật phòng thực hành đã hỗ trợ máy để thực hiện các bài Lab phục vụ cho đề tài

# NHẬP ĐỀ

Công nghệ ngành mạng máy tính trong những năm gần đây đã trở nên phát triển mạnh mẽ hơn bao giờ hết. Các công ty hay các tổ chức hiện nay đang rất xem trọng công tác triển khai hạ tầng mạng cho hệ thống của mình. Trong ngành công nghiệp ngành mạng, Cisco gần như không có đối thủ trong lĩnh vực này. Tuy nhiên với chi phí khá cao khiến cho một số công ty hay tổ chức phải e ngại và tìm kiếm một phương án thay thế khác. Năm 2005, công ty Vyatta thành lập và cung cấp đến ngành mạng những sản phẩm router mã nguồn mở với các tính năng tương đương với router Cisco, chi phí rẻ hơn rất nhiều. Việc xuất hiện của router Vyatta mã nguồn mở đã khiến cho ngành công nghiệp mạng sôi nổi hơn bao giờ hết. Ngay từ khi xuất hiện phiên bản đầu tiên, các nhà giải pháp mạng nổi tiếng trên thế giới đánh giá rất cao và xác định rằng Vyatta thực sự sẽ trở thành đối thủ cạnh tranh trực tiếp với Cisco trong lĩnh vực thiết bị mạng router. Vyatta có thể còn khá xa lạ với các nhà quản trị mạng tại Việt Nam.

Với mong muốn được nắm rõ hơn về sản phẩm router mã nguồn mở Vyatta này và nhằm đưa ra được giải pháp giúp cho doanh nghiệp có thể thay thế hoàn toàn các thiết bị Cisco, nhóm chúng tôi đã cùng nhau tìm tòi, nghiên cứu và cuối cùng cũng đã đạt được những kết quả cụ thể. Nhóm chúng tôi hi vọng bài báo cáo này sẽ giúp cho bạn đọc có thêm được thông tin cũng như nắm rõ về sản phẩm này.

## I. Giới thiệu

Công ty Vyatta được thành lập vào năm 2005, điều hành bởi Kelly Herrell, Tổng Giám Đốc điều hành đồng thời cũng là thành viên của Hội Đồng Quản Trị công ty và hiện đang nằm trong top 50 người có quyền lực nhất thế giới mạng do tạp chí Network World bầu chọn. Công ty Vyatta có trụ sở nằm ở Belmont, một thành phố ở Califonia. Công ty với khoảng 50 nhân viên, cung cấp các sản phẩm chủ yếu về hệ thống mạng. Các thành viên sáng lập Vyatta gồm nhiều chuyên gia trong lĩnh vực hệ thống mạng. Không giống như những công ty khác, đội ngũ Vyatta sở hữu những kiến thức tổng hợp về các thiết bị mạng, các mã nguồn mở trên thị trường và các nền tảng về mạng. Đồng thời với kiến thức về hệ thống mạng rộng khắp và kinh nghiệm dồi dào về mã nguồn mở và về các thiết bị mạng có được từ các công ty nổi tiếng như Cisco, Nortel, Redhat, BlueCoat Systems, Sun Microsystems, Redback Networks, Digital Island, Level 3, Internap, Hewlett-Packard, Oracle, AMD… Vào tháng 3 năm 2006, công ty đã tung ra thị trường phiên bản Vyatta chạy trên nền Linux miễn phí đầu tiên cho phép download đã xuất hiện.


Logo của Vyatta

Vyatta chạy dựa trên phần mềm mã nguồn mở, và chạy trên phần cứng tiêu chuẩn x86. Vyatta có bộ định tuyến và cơ chế bảo mật như các phần cứng router thông dụng, các tính năng cơ bản là: Ipv4, Ipv6, Ripv2, OSPFv3, BGP4, DHCP server/client, 802.1Q Vlan, WAN hỗ trợ với DSL, hỗ trợ kết nối Lan đến 10GbE, cân bằng tải WAN, Voip QoS, Firewall, VPN web-to-site, Nat, xác thực RADIUS và TACACS+…Ngoài các tính năng tương đương như một router Cisco, Vyatta chạy trên nền tảng mã nguồn mở vốn được các chuyên gia đánh giá cao, bên cạnh đó giá thương mại các sản phẩm của Vyatta cũng là một trong những yếu tố hấp dẫn nhất đối với các nhà quản trị mạng. Một số sản phẩm của Vyatta chỉ có giá chỉ bằng một phần

năm so với router của Cisco. Chính vì vậy ngay sau khi tung ra thị trường, các chuyên gia về mạng đánh giá rằng đây sẽ là một đối thủ cạnh tranh đáng gờm đối với hãng danh tiếng Cisco. Khi vừa thành lập, hãng dự định sẽ tập trung tiếp thị router mã nguồn mở tới các doanh nghiệp cỡ vừa và các văn phòng chi nhánh của những tập đoàn đa quốc gia. Trên thực tế thì Vyatta chỉ là một trong số nhiều công ty đang cố gắng tấn công vào thị trường cực kì béo bở này. Nhưng đây là thị trường có trị giá lên đến 4 tỷ USD và hiện đang nằm trong sự thống trị mạnh mẽ của Cisco. Vyatta đã rất mạo hiểm khi theo đuổi dự án này. Bởi từ trước đến giờ, chưa có bất kì dự án nào lại đầy táo bạo như của Vyatta: vượt qua mặt cả Cisco. Tổng Giám Đốc điều hành Kelly Herrell cho rằng cần phải cố gắng nhiều hơn nữa và đã phát biểu rằng "chúng tôi chỉ là những con cá trong một bể đầy cá mập", " mục tiêu của chúng tôi khi khởi đầu Vyatta là thách thức các nhà cung cấp về giá cả, hiệu năng và giá trị tổng thể…". Sự cố gắng của đội ngũ Vyatta đã được đền đáp xứng đáng khi đoạt được giải thưởng InfoWorld Bossie "phần mềm mạng mã nguồn mở tốt nhất" vào tháng 8 năm 2010 và đây là giải thưởng Bossie thứ 3 liên tiếp cho những nỗ lực của các thành viên Vyatta. Và cũng trong tháng 8 này, Vyatta được xếp vào trong top 10 các Linux Server hàng đầu về các tính năng: dễ sử dụng, tính thương mại, độ tin cậy trung tâm dữ liệu, sau khi vượt qua mặt cả CentOS chiếm ở vị trí thứ 8.


Kelly Herell – Giám đốc điều hành Vyatta

Forrester – đã phát biểu rằng: "Các sản phẩm mã nguồn mở ngày nay đã trở nên phổ biến, bên cạnh đó việc hạn hẹp ngân sách thì việc lựa chọn Vyatta sẽ thuận lợi hơn rất nhiều". Ngay cả David Davis, một chuyên gia tại TechRepublic đã đạt được các

chứng chỉ của Cisco như CCNA, CCNP, CCIE cho biết: "Bất cứ điều gì bạn muốn làm với một router Cisco, bạn đều có thể làm hầu hết với Vyatta…".

Đúng như dự đoán về một tương lai tươi sáng từ các chuyên gia. Chỉ trong vòng vài năm từ khi tung ra thị trường, Vyatta đã cho thấy mình xứng đáng là một đối thủ đáng gồm đối với các nhà mạng khác. Cụ thể rằng hiện nay Vyatta đã có những đối tác chiến lược lớn cực kì quan trọng nhằm phục vụ cho chiến lược của mình: Citrix Ready, Cloud.com, Extreme Networks, Hyperic, IBM, Intel, NEC Network & System intergration Corporation (NESIC), Openstack, OpenVPN, Riverbed, Sangoma Technologies và đặc biệt là sự cộng tác với hãng VMWare. Sự kết hợp độc đáo với VMWare nhằm cung cấp thêm tính năng ảo hoá giúp hỗ trợ thêm cho các trường học và doanh nghiệp.

Hiện nay Vyatta đang được sử dụng cho việc kết nối 100.000 sinh viên, 10.000 giảng viên và 18 cơ quan giáo dục trên toàn Quận Mark Hoffman. Đại học Florida đã lựa chọn Vyatta phục vụ cho môi  trường mạng ảo của mình. Vyatta hiện nay đang là sự lựa chọn số một tại thành phố Portland, toà án chính phủ của New Mexico, công ty Skybeam, và một Data Center tại Tây Nam nước Mỹ… Nhóm iParadigms là một nhóm gồm nhiều chuyên gia tại các lĩnh vực khác nhau được thành lập để cùng nhau làm việc ngăn ngừa việc đạo văn và bảo vệ việc sở hữu trí tuệ, đã thực hiện công cuộc cải cách hệ thống mạng của mình khi lựa chọn Vyatta thay thế cho router Cisco 7200 đã được sử dụng trước đây.

Vào năm 2009, Công ty Vyatta có 2 sự kiện lớn gây thu hút rất nhiều người. Đầu tiên là việc chính thức tham gia EDUCAUSE vào tháng 7, đây một hiệp hội phi lợi nhuận chỉ tập trung vào việc thúc đẩy giáo dục đại học bằng cách đưa công nghệ thông tin vào. Sự kiện đáng chú ý thứ 2 đó là việc thành lập trường đại học Vyatta vào tháng 12. Đại học Vyatta có hỗ trợ học online và sẽ đào tạo chuyên sâu về mạng, về các thiết bị và phần mềm Vyatta. Động thái này cho thấy quyết tâm mở rộng thị trường của Vyatta và đồng thời cũng gây sức ép lên đối thủ Cisco. Sức nóng của ngành công nghiệp mạng ngày một tăng lên ngay từ khi có sự xuất hiện của Vyatta bởi việc thách thức các nhà mạng. Đến tháng 10 năm 2009, Vyatta lại một lần nữa đã tạo nên một

cơn sốt khi đưa ra chương trình khuyến mãi tất cả dịch vụ mạng trong tháng 11. Sẽ không có gì đáng chú ý nếu như Vyatta không đưa ra chương trình khuyến mãi dựa trên tổng lãi xuất doanh thu của Cisco. Đây gần như là lời thách thức đối với nhà mạng khổng lồ Cisco vốn có tổng lãi suất lớn nhất trong ngành công nghiệp IT.

Trước những bước đi mạnh mẽ đầy táo bạo này các chuyên gia bắt đầu đặt ra một câu hỏi: liệu rằng Vyatta có thể thay thế được hoàn toàn Cisco hay không?

Hãng Cisco đã thực sự tự làm khó mình khi chỉ cung ứng các sản phẩm phần cứng riêng biệt của hãng. Chính vì việc sử dụng phần cứng riêng biệt nên giá thành của các thiết bị phần cứng Cisco luôn ở mức giá khá cao. Do đó khiến các công ty có quy mô vừa và nhỏ cũng không dám nghĩ tới. Còn Vyatta chạy trên nền tảng mã nguồn mở trên phần cứng tiêu chuẩn x86, điều này rất thuận lợi bởi không bị gò bó ở phần cứng và tạo nên sự linh hoạt hơn về giá cả.

Vào ngày 17/3/2008, nhà mạng Vyatta đã làm một cuộc thử nghiệm khá thú vị được thực hiện bởi nhóm Tolly nhằm so sánh giữa Vyatta và thiết bị Cisco 7200 Series. Cuộc khảo sát chỉ tập trung vào giao thức định tuyến BGP và kết quả cho thấy Vyatta đạt được hiệu suất cao gấp 2 đến 3 lần so với router Cisco 7200 Series nhưng chi phí khi sử dụng Vyatta lại thấp hơn 70%. Đây là một thông số rất đáng để chú ý.

- Nếu sử dụng Vyatta thì chi phí là 7.952 USD trong khi giá của Cisco là 35.756
- Vyatta hỗ trợ bản route có kích thước lên đến 4.5 triệu đường, gấp 3 lần so với Cisco 7204-G1 và gấp 1.5 lần so với Cisco 7204-G2
- Thời gian hội tụ BGP nhiều gấp 3 lần so với Cisco 7204-G1 và gấp 2 so với Cisco 7204-G2

Ông Simon Woodhead - Giám đốc tại Simwood eSMS Limited, nhà cung cấp dịch vụ Voip cho các sân bay, các doanh nghiệp và các ISP - đã cho biết: “Hiệu suất, tính ổn định và tính sẵn sàng của hệ thống mạng không chỉ rất quan trọng đối với chúng tôi mà còn cho khách hàng. Chúng tôi đã có xem qua rất nhiều lựa chọn cho việc xây

dựng hệ thống mạng, đặc biệt là Cisco nhưng cuối cùng chúng tôi đã chọn Vyatta. Bởi vì Vyatta có hiệu suất làm việc tương đương nhưng có giá không cao…", sau một thời gian hoạt động, ông khẳng định rằng: "Việc lựa chon Vyatta là một quyết định đúng đắn".

## II. Các sản phẩm của Vyatta

Đến nay, Vyatta đã tung ra thị trường các dòng sản phẩm như sau: Vyatta Core ,Vyatta Subscription Edition Software , Subscription Edition for Virtualization, Vyatta Appliances


**Vyatta Core (VC)**: là bản open-source hoàn toàn miễn phí,có thể download về và cài đặt phần cứng X86. Với bản VC này chúng ta hoàn toàn chịu trách nhiệm về việc sử trên dụng Vyatta của mình, tức là chúng ta sẽ không nhận dược hỗ trợ có tính ràng buộc nào từ Vyatta trong quá trình sử dụng. Tuy nhiên chúng ta có thể nhận được sự giúp đỡ nhiệt tình từ forum của Vyatta, wiki, và các diễn đàn khác. Phiên bản này dành cho các nhà tester, nhà phát triển sản phẩm, các doanh nghiệp có quy mô vừa và nhỏ.

Các tính năng của Vyatta Core: Routing, Firewall, NAT, VPN, IPS, URL, Filter, QOS, Wan loadbalacing, IPv6, Ethernet only. Phiên bản mới nhất của Vyatta core là 6.1-2010.08.20, trong phiên này một số tính năng mới được bổ sung bao gồm:

- *Stateful failover for NAT and firewall:*Vyatta core cung cấp 2 giải pháp failover cho Vyatta core bao gồm: Clustering và VRRP. Trong phiên bản này, hệ thống Vyatta sẽ theo dõi quá trình Nat và các kết nối qua Firewall và sẽ đồng bộ chúng đến hệ thống clustering hoặc VRRP standby, điều này giúp cho hệ thống standby có thể hoạt động với việc không thiết lập lại kết nối nếu như Primary fails

- *LLDP support* :Vyatta trong phiên bản này cung cấp cơ chế Link Layer Discovery Protocol (LLDP). LLDP cho phép các hệ thống Vyatta có thể quảng bá thông tin cho nhau và định danh các hệ thống Vyatta khác trong cùng một physical network.

- *Port mirroring and redirection*: Những gói tin inbound trên các interface Ethernet có thể được mirror lại. Tính năng này rất hữu dụng cho việc mirror packet cho IDS xử lý. Ngoài ra Vyata phiên bản này còn cung cấp thêm tính năng Redirect, cho phép redirect các gói tin chiều inbound từ nhiều interface Ethernet đến 1 interface. Dựa vào tính năng này có thể áp dụng duy nhất 1 policy QOS cho tất cả các gói dữ liệu

- *IPv6 BGP support*: phiên bản này hổ trở thêm ipV6 cho BGP

- Ngoài ra còn cung cấp thêm các tính năng sau: DHCPv6, SNMP for IPv6


**Vyatta Subscription Edition (SE):** Ngược lại với bản VC, bản SE là thương phẩm của Vyatta. Ở phiên bản này, Vyatta đã sửa lỗi tất cả các bug do cộng đồng phát hiện trong quá trình dùng VC. Họ đóng gói phiên bản đã được test kỹ này kèm với một số tính năng có giá trị gia tăng để tạo nên phiên bản SE. Với phiên bản này chúng ta sẽ nhận được sự hỗ trợ trực tiếp từ phía Vyatta.

Các tính năng của Vyatta Subscription Edition: Ngoài các tính năng sẵn có của Vyatta core, bản SE còn có thêm các tính năng: TACACS+, WAN/SERIAL DRIVERS, VPN CLIENT MANAGER, CONFIG SYNCH, RIVERBED RSP, Vyatta Remote Access API

Trong phiên bản 6.1 này Vyatta Subscription Edition bổ sung thêm các tính năng

- *TACACS+ IPv4 AAA Support* : Phiên bản này hổ trợ IPv4 AAA thông qua một Server chứng thực TACACS+ trung tâm.

- *Configuration synchronization*: Vyatta Subscription Edition cho phép đồng bộ cấu hình giữa những hệ thống Vyatta được chỉ định

**Subscription Edition for Virtualization**: là phiên bản thiết kế chạy trên nền ảo hóa Citrix XenServer, VMware, Xen and Redhat KVM. Đây là một phiên bản đặc biệt của Vyatta , rất linh hoạt trong việc backup và phục hồi từ hệ thống này sang hệ thống khác, tận dụng hết khả năng của hệ thống, giúp tiết kiệm chi phí.

**Vyatta PLUS Snort VRT service:** Dịch vụ này cung cấp các rules của Snort được đưa ra bởi các chuyên gia bảo mật hang đầu thế giới và đã được kiểm tra chặt chẽ , giúp cho hệ thống IPS và IDS của Vyatta hoạt động một cách hoàn hảo nhất bằng cách truy cập các bảng cập nhật Sourcefire VRT rule-base trực tiếp từ Vyatta

**Vyatta Appliances**: Đây là dòng sản phẩm các thiết bị phần cứng rất ổn định và đáng tin cậy mà Vyatta đã sản xuất. Tolly - một công ty chuyên về benmarking của Phần lan - đã tiến hành những cuộc thử nghiệm thú vị để so sánh Vyatta 2500 với Cico 2821, cũng như so sánh Vyatta 3500 với Cisco 7200. Phần thắng nghiên về phía Vyatta trên mặt hiệu năng làm việc lẫn chi phí. Thật ra các thiết bị Vyatta giống như một máy tính được thu nhỏ, lược bỏ các thành phần không cần thiết để trở thành một thiết bị phần cứng chuyên dụng kết hợp chặt chẽ với phần mềm tạo nên một hệ thống hoàn chỉnh.

Các sản phẩm Vyatta Appliances hiện tại:

- Vyatta 514 appliance : có cấu hình như sau


| | |
|---|---|
| Hardware | Model 514 |
| Memory | 512MB, upgradeable to 1GB |
| Compact Flash | 2GB |
| I/O Channels | Four onboard 10/100 Ethernet |
| WAN Expansion | One PCI-32 slot |
| Interfaces | » Linux-supported Ethernet cards<br>» ADSL<br>» T1/E1 1 port, 2 port<br>» Synchronous Serial Cards V.35, X.21, RS-422, or EIA530<br>» 3G Modem |

| | |
|---|---|
| Serial Console | One RS-232 D89 |
| USB | Dual USB 2.0 Connectors |
| LEDs | » Power and storage<br>» Ethernet port activity and link<br>» Ethernet port speed |
| Power Supply | 60W power adapter |
| Dimensions | Height: 1.97” (50 mm)<br>Width: 8.86” (225 mm)<br>Depth: 8.07” (205 mm) |
| Weight | 2.6 lbs (1.2kg) |
| Operating Temp | 41 to 113°F (5 to 40°C) |
| Storage Temp | 32 to 158°F (5 to 70°C) |
| Certifications | UL/CE/FCC Class B |

- Hiệu suất làm việc:

| Performance | Model 514 |
|---|---|
| L3 Forwarding | 70,000 PPS |
| VPN Forwarding | 113 Mbps IPSec |
| Max VPN Tunnels | 1500 |

- Vyatta 2500 Series Appliance : gồm 2 model 2051 và 2052


| Hardward | Model 2501 | Model 2502 |
|---|---|---|
| Processor | Single Core Intel | Dual Core Intel |

| | | |
|---|---|---|
| Memory | 1GB | 2GB |
| Dimensions | Height: 1.68” (4.27 cm)<br>Width: 17.60” (44.70 cm)<br>Depth: 21.50” (54.61 cm) | Height: 1.68” (4.27 cm)<br>Width: 17.60” (44.70 cm)<br>Depth: 21.50” (54.61 cm) |
| Form Factor | 1U rack height | 1U rack height |
| Hard Drives | Single 250GB SATA hard drive | Dual 250GB SATA w/ RAID |
| Onboard Interfaces | 2X Gigabit Ethernet | 2X Gigabit Ethernet |
| Expansion Slots | PCI-X slot (64bit,133MHz)<br>PCI Express x8 slot | PCI-X slot (64bit,133MHz)<br>PCI Express x8 slot |
| Power Supply | 345W non-redundant | 345W non-redundant |
| Interfaces | » 10/100/1000 Ethernet<br>» 10Gb Ethernet<br>» 3G Modem<br>» ADSL<br>» T1/E1 1 port<br>» T1/E1 2 port<br>» T1/E1 4 port<br>» T3<br>» X.21 and V.35 | » 10/100/1000 Ethernet<br>» 10Gb Ethernet<br>» 3G Modem<br>» ADSL<br>» T1/E1 1 port<br>» T1/E1 2 port<br>» T1/E1 4 port<br>» T3<br>» X.21 and V.35 |

- Hiệu suất làm việc:

| Performance | Model 2501 | Model 2502 |
|---|---|---|
| Layer 3 Forwarding | 500,000 PPS | 1,000,000 PPS |
| VPN Forwarding | 420 Mbps | 515 Mbps |
| Max VPN Tunnels | 2000 | 3000 |

- Vyatta 3500 Series Appliance: gồm 2 model 3510 và 3520


| Hardware | Model 3510 | Model 3520 |
|---|---|---|
| Processor | Quad Core Intel | Quad Core Intel |
| Memory | 2GB | 3GB |
| Dimensions | Height: 3.4” (8.6 cm)<br>Width: 19” (48.2 cm) with rack latches<br>Depth: 28.4” (72.1 cm) with bezel | Height: 3.4” (8.6 cm)<br>Width: 19” (48.2 cm) with rack latches<br>Depth: 28.4” (72.1 cm) with bezel |
| Form Factor | 2U rack height | 2U rack height |
| Hard Drives | 2 x 250GB SATA w/ RAID-1 | 2 x 250GB SATA w/ RAID-1 |
| Onboard Interfaces | 4 x Gigabit Ethernet | 4 x Gigabit Ethernet |
| Expansion Slots | 2 Gen-2 PCI Express x8 slots<br>1 full height Gen-2 PCI Express x4 slot<br>1 low profile Gen-2 PCI Express x4 slot | 2 Gen-2 PCI Express x8 slots<br>1 full height Gen-2 PCI Express x4 slot<br>1 low profile Gen-2 PCI Express x4 slot |
| Power Supply | 570W non-redundant<br>Redundant power supply available | 570W non-redundant<br>Redundant power supply available |
| Interfaces | » 10/100/1000 Ethernet<br>» 10Gb Ethernet<br>» 3G Modem<br>» T1/E1 1 port<br>» T1/E1 2 port | » 10/100/1000 Ethernet<br>» 10Gb Ethernet<br>» 3G Modem<br>» T1/E1 1 port<br>» T1/E1 2 port |

| | | |
|---|---|---|
| | » T1/E1 4 port<br>» X.21 and V.35 | » T1/E1 4 port<br>» X.21 and V.35 |

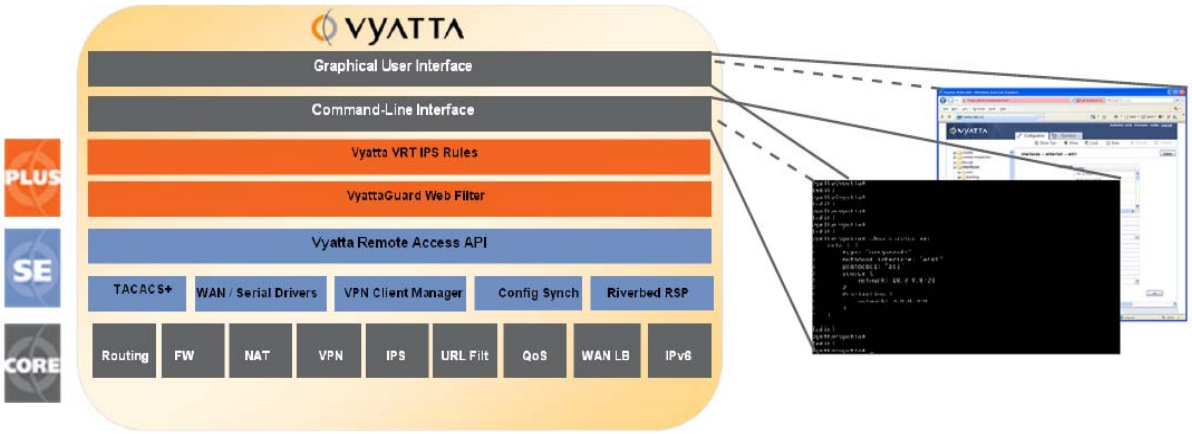
- Hiệu suất làm việc

| Performance | Model 3510 | Model 3520 |
|---|---|---|
| Layer 3 Forwarding | 2,000,000 pps | 3,000,000 pps |
| VPN Forwarding | 700 Mbps | 900 Mbps |
| Max VPN Tunnels | 6000 | 8000 |

**Bảng so sánh các sản phẩm phần mềm của Vyatta**

| Phiên bản | Tính năng | Hỗ trợ | Ứng dụng |
|---|---|---|---|
| CORE | - Basic Routing<br>- Stateful Firewall<br>- IPSec and SSL-Based OpenVPN<br>- WAN Load Balancing | Không hổ trợ | Test/Development/SOHO<br>Router<br>Firewall |
| SE | - Vyatta Remote Access API<br>- Configuration Synch<br>- IPv6 Ready Certified<br>- WAN Device Drivers DSL/T1/T3<br>- VPN Client Auto-Configuration<br>- TACACS+ | Vyatta hỗ trợ (24x7) | Enterprise/xPS/cloud<br>Router<br>Firewall<br>VPN<br>IPS<br>Web Filter<br>…. |

| | | | |
|---|---|---|---|
| | - Integrated Hardware Appliances<br>- Optimized Virtual Machines<br>- Riverbed RSP Ready | | |
| PLUS | - VyattaGuard Web Filtering<br>- Vyatta Snort VRT IDS/IPS Rules | Vyatta hỗ trợ 24/7 | Enterprise/xPS/Cloud<br>Threat Mitigation<br>HR Compliance<br>Productivity<br>Managing Bandwidth |



**Bảng giá của Vyatta Software SubScriptions so với Cisco**

| Vyatta Software Subscriptions | | | | | |
|---|---|---|---|---|---|
| Vyatta on 1-2 Core Processors | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 1800 Series | Cisco 2800 Series | Cisco ASA 5510 |
| $747 | $997 | $1,197 | $1,000 - $3,500 | $1,800 - $5,500 | $2,400 - $8,000 |
| Vyatta on 3-4 Core Processors | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 3800 Series | Cisco 7200 Series | Cisco ASA 5520 / 5550 |
| $1,120 | $1,495 | $1,795 | $6,500 - $13,500 | $25,000 - $40,000 | $5,500 - $60,000 |
| Vyatta on 5+ Core Processors | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 7200 Series | Cisco ASR 1000 Series | Cisco ASA 5550 |
| $2,988 | $3,988 | $4,788 | $25,000 - $40,000 | $45,000 - $100,000 | $13,500 - $60,000 |
| Vyatta for Virtual Environments | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | None | None | None |
| $934 | $1,246 | $1,496 | n/a | n/a | n/a |

**Bảng giá của Vyatta Hardware Appliances so với Cisco**

| Vyatta Hardware Appliances | | | | | |
|---|---|---|---|---|---|
| Vyatta 514 Appliance | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 1800 Series | Cisco ASA 5505 | |
| $797 | $897 | $947 | $1,000 - $3,500 | $600 - $2,300 | |
| Vyatta 2501 Appliance | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 2800 Series | Cisco 3800 Series | Cisco ASA 5510 / 5520 |
| $2,347 | $2,597 | $2,797 | $1,800 - $8,500 | $6,500 - $13,500 | $2,400 - $11,500 |
| Vyatta 2502 Appliance | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 2800 Series | Cisco 3800 Series | Cisco ASA 5510 / 5520 |
| $2,747 | $2,997 | $3,197 | $1,800 - $8,500 | $6,500 - $13,500 | $2,400 - $11,500 |
| Vyatta 3510 Appliance | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 7200 Series | Cisco ASR 1000 Series | Cisco ASA 5550 |
| $4,595 | $4,970 | $5,270 | $25,000 - $40,000 | $45,000 - $100,000 | $13,500 - $60,000 |
| Vyatta 3520 Appliance | | | Cisco Equivalent | | |
| Vyatta Professional Subscription | Vyatta Enterprise Subscription | Vyatta Premium Subscription | Cisco 7200 Series | Cisco ASR 1000 Series | Cisco ASA 5550 |
| $6,495 | $6,870 | $7,170 | $25,000 - $40,000 | $45,000 - $100,000 | $13,500 - $60,000 |

**Bảng so sánh tính năng của Vyatta OS và Cisco OS**

| The New Network Requirements | | |
|---|---|---|
| **Features** | **Vyatta Network OS** | **Cisco IOS** |
| Multifunction | Yes | Yes |
| Hardware Scalability | Seamless across x86 Cores | Cisco Limited |
| Software Performance | Unlimited | Platform Limited |
| Virtual Machine Availability | Yes (VMware, Xen, XenServer, KVM) | No |
| Open Management API | Yes | No |
| Integration into Edge Devices | Yes | No |
| Cloud Readiness | Yes | No |

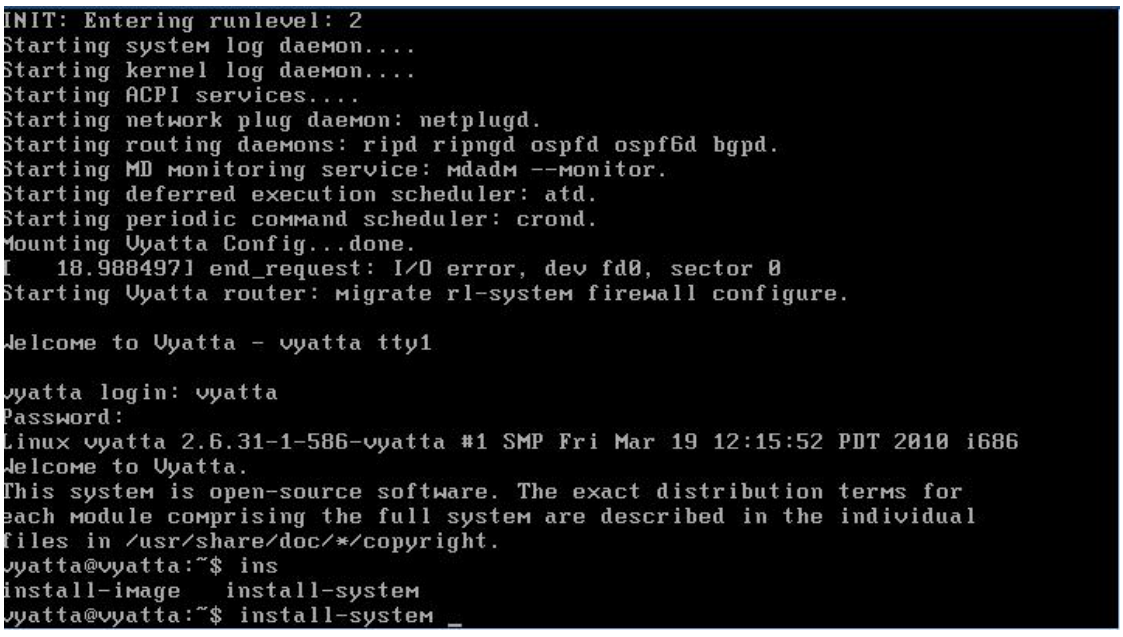
## III. Các tính năng của Vyatta

### 1. Installation

**Cài đặt từ các thiết bị phần cứng ngoài**

Đây là một kiểu cài đặt theo kiểu truyền thống từ trước đến nay. Để cài đặt hệ thống Vyatta người quản trị mạng có thể dùng đĩa CD chứa file image cài đặt, hoặc dùng một thiết bị phần cứng khác là USD, ổ cứng ngoài… Vyatta có thể được cài đặt và chạy được rất tốt trên hầu hết các server trên nền tảng phần cứng chuẩn X86 và trên PC.

Yêu cầu cho việc cài đặt Vyatta đòi hỏi ổ cứng còn trống khoảng 1GB (yêu cầu đề nghị là 2GB trống cho ổ cứng), 256MB RAM, có ít nhất 2 card mạng.




Hình: bước đầu thực hiện cài đặt

Mặc định trong hệ thống Vyatta , những gì chúng ta cấu hình sẽ được lưu trong config.boot, khi chúng ta cài đặt Vyatta trên ổ cứng thì config.boot nằm trong đường dẫn /opt/vyatta/etc/config, ta có thể dễ dàng backup lại file cấu hình bằng thiết bị lưu trữ ngoài như usb

Để lưu cấu hình Vyatta trong file mặc định config.boot ta dùng lệnh Save trong chế độ configuration mode.

```
vyatta@vyatta# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
vyatta@vyatta# _
```

Để lưu cấu hình khác với file mặc định config.boot ta dùng lệnh sau: Save tenfile

```
vyatta@vyatta# save nghia-hung
Saving configuration to '/opt/vyatta/etc/config/nghia-hung'...
Done
[edit]
vyatta@vyatta# _
```

Thuận lợi:

- Các cấu hình sau khi hoàn thành các thao tác xong sẽ được lưu vào trong hệ thống. Sau khi hệ thống khởi động lại thì các cấu hình sẽ vẫn còn được lưu giữ. Phương thức cài đặt này thích hợp dành cho việc triển khai hệ thống mạng cho doanh nghiệp.

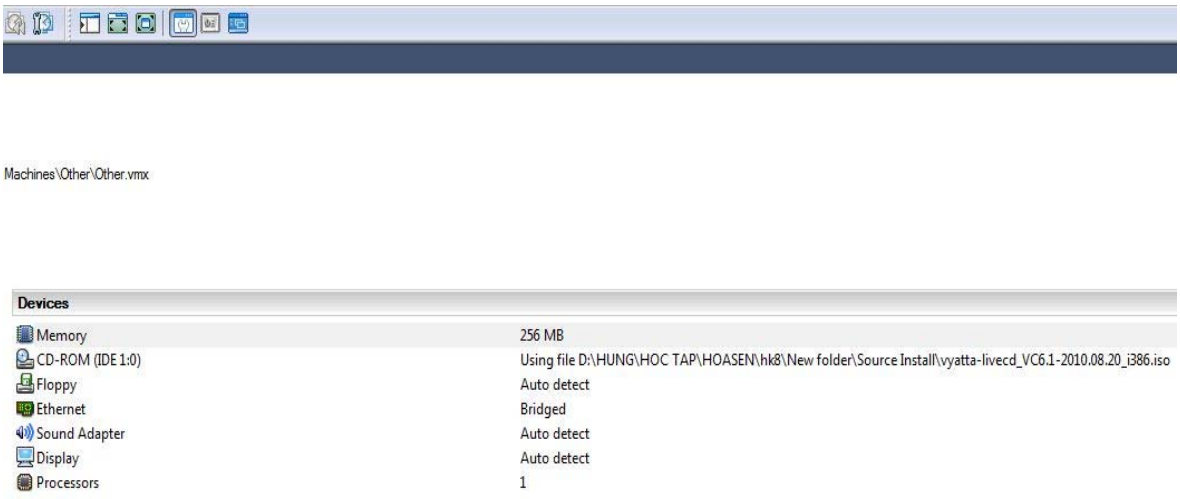
- Hệ thống Vyatta có thể cài đặt trên nền tạng phần cứng tiêu chuẩn X86 nên sẽ không bị hạn chế các thiết bị phần cứng nhiều. Khi sử dụng, doanh nghiệp vẫn có thể dễ dàng nâng cấp thiết bị.

**Hệ thống Vyatta hoạt động trực tiếp từ liveCD**

Đây là một trong những tính năng độc đáo của Vyatta trong việc hoạt động và triển khai hệ thống mạng.

Trên trang chủ Vyatta có cung cấp đường dẫn để download file image của hệ thống Vyatta xuống. Người dùng có thể burn file này ra một đĩa CD. File image này có tác dụng giúp cho hệ thống có thể chạy trực tiếp mà không cần phải có một ổ cứng cài đặt. Phương thức hoạt động này giúp người sử dụng có thể làm việc, cấu hình, triển khai hệ thống một cách nhanh chóng, linh hoạt và tiện lợi.

Khi khởi động máy lên, người sử dụng cho đĩa vào và hệ thống sẽ tự động boot đĩa lên và chạy ngay mà không cần thiết phải có ổ cứng. Trong quá trình sử dụng, mọi hoạt động, cấu hình của người sử dụng đều sẽ được đưa lên bộ nhớ Ram để lưu trữ. Nhưng sau khi tắt máy, tất cả cấu hình đều sẽ không được lưu giữ. Người sử dụng có thể save các file đã cấu hình vào đĩa mềm hoặc TFTP server. Khi sử dụng Vyatta dưới hình thức liveCD thì file cấu hình config.boot nằm trong đường dẫn /media/floppy/config.




Hình: giả lập chạy bằng Vmware – chỉ cần ổ CD để boot, không cần ổ cứng


Hình: chỉ cần mở máy và boot CD, hệ thống Vyatta đã sẵn sàng hoạt động

Đây là một phương thức hoạt động rất hay của Vyatta rất có ích cho công việc ước lượng, kiểm tra hệ thống trước khi hoạt động chính thức, rất phù hợp cho việc nghiên cứu và học tập.

Thuận lợi

- Không đòi hỏi máy phải có phần cứng
- Giúp người sử dụng có thể làm việc linh động và không mất nhiều thời gian cho việc cài đặt
- Rất tiện lợi cho việc nghiên cứu và học tập của các sinh viên ngành mạng

Không thuận lợi:

- Các cấu hình không được lưu sau khi khởi động

**Cài đặt trên mỗi trường ảo hóa**

Hiện nay, Vyatta có hỗ trợ cài đặt trong môi trường ảo hóa là VMware và XenServer

VMware: hiện tại Vyatta hỗ trợ chạy trên VMware ESX và ESXi. Giống như các nền tảng ảo hóa khác, VMware cho phép có thể chạy nhiều hệ thống Vyatta trên cùng một thiết bị phần cứng. Việc download có thể truy cập vào trang www.vytta .com/support/software và trang www.vyatta .com/downloads

XenServer: Citrix Xenserver là một server chạy trên nền tảng ảo hóa, giúp việc chạy nhiều hệ thống trên cùng một phần cứng tiêu chuẩn.Vyatta template được thiết kế để làm việc trên XenServer 5.5 và XenCenter 5.5. Để có thể dùng template cần phải: download, import template vào XenServer và cuối cùng là tạo ra các máy ảo từ template đó. Trước khi cài Vyatta template, XenServer 5 phải được cài trên Server và XenCenter 5 phải được cài trên máy tính mà người quản trị mạng quản lí. XenCenter là hệ thống quản lí các XenServer, cho phép quản lí nhiều server vât lí đang chạy XenServer.

## 2. Interfaces

### 2.1 Frame Relay

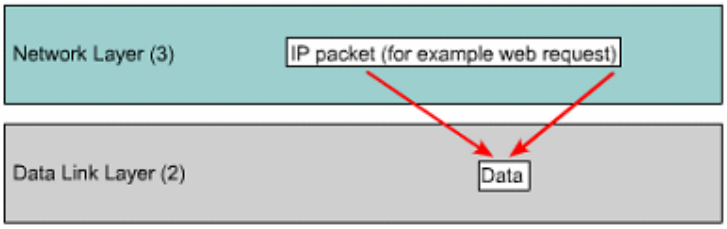
Tính năng hoạt động của Frame Relay chỉ hỗ trợ trên phiên bản Vyatta Subscription Edition (SE). Ở phiên bản Vyatta Core sẽ không có hỗ trợ tính năng này

Frame Relay là một dịch vụ truyền tải trong mạng Wan theo phương thức chuyển mạch tốc độ cao. Frame Relay hoạt động tại lớp Physical và lớp Data Link trong mô hình OSI. Các giao thức mà Frame Relay hỗ trợ là: Ip, DECnet, Apple Talk, Xerox Network Service (XNS), Novell IPX, Commectionless Network Service (CLNS), International Organization for Standards (ISO), Banyan Vines, Transparent bridging. Frame Relay thực hiện truyền frame giữa thiết bị DTE (Data Terminal Equipment) và thiết bị DCE (Data Circuit-Terminating Equipment). Được sử dụng để nối các mạng Lan. Mỗi Router biên của mạng Lan là một DTE. Sẽ được nối trực tiếp đến một thiết bị DCE gần nhất của nhà cung cấp dịch vụ.

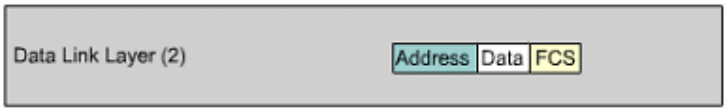
Các kết nối ảo VC trên cùng một đường truyền vật lý vẫn được phân biệt với nhau vì mỗi VC có một chỉ số DLCI riêng. Chỉ số DLCI (Data Link Connection Identifier) được ghi trong mỗi frame dữ liệu truyền đi. Chỉ số này chỉ có ý nghĩa trong nội bộ, nghĩa là nó chỉ có duy nhất trong kênh vật lý mà nó thuộc về. Do đó thiết bị ở đầu bên kia có thể sử dụng một chỉ số khác để quy ước cho cùng một kết nối ảo VC.

Đóng gói Frame Relay thực hiện theo phân lớp như sau: nhận dữ liệu từ tầng Network sau đó đóng thành các frame của Frame Relay, sao đó chuyển các frame xuống tầng vật lý để truyền đi

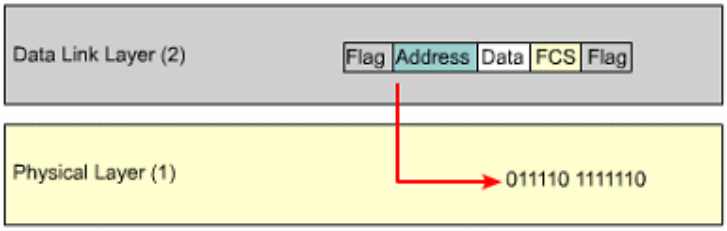
Frame của Frame Relay sử dụng một phần định dạng của frame HDLC. Do đó cũng có phần cờ 01111110. Phần FCS (Frame Check Sequence) được sử dụng để kiểm tra lỗi của frame. Giá trị FCS được tính ra trước khi truyền frame đi và được ghi vào phần FCS của frame. Thiết bị nhận frame cũng tính lại giá trị FCS và so sánh với giá trị FCS trong frame đã nhận. Nếu 2 giá trị giống nhau thì frame được tiếp tục xử lý. Nếu hai giá trị khác nhau thì có nghĩa là frame đã bị lỗi, frame này sẽ bị huỷ bỏ và không báo cho thiết bị nguồn của frame.




Nhận dữ liệu từ tầng network




Gắn thêm địa chỉ và phần FCS vào




Cuối cùng là cờ Flag có phần thêm giá trị là 01111110

Nếu hệ thống mạng chỉ cần kết nối 2 mạng với nhau bằng kết nối point to point thì lợi ích khi sử dụng Frame relay chưa rõ ràng lắm. Frame Relay sẽ rất có lợi về mặt chi phí nếu chúng ta liên kết nhiều mạng với nhau. Như đã biết, cấu trúc mạng Wan thường được liên kết theo cấu trúc hình sao. Dịch vụ chính được đặt ở một mạng trung tâm và mỗi mạng ở xa cần truy cập dịch vụ thì kết nối vào mạng trung tâm. Với cách kết nối như vậy chi phí sẽ được giảm rất nhiều

Trong bất kì cấu trúc Frame Relay nào, khi chúng ta sử dụng một cổng để kết nối nhiều mạng khác nhau thì có thể gặp phải sự cố không đến được mạng đích. Sự cố này do đặc tính đa truy cập không quảng bá (NBMA – nonbroadcast multiaccess) của Frame Relay gây ra. Các giao thức định tuyến sử dụng kỹ thuật Split horizon để tránh

tình trạng gây ra vòng lặp. Split horizon không cho phép truyền ra một cổng những thông tin định tuyến vừa nhận vào từ cổng đó. Khi có nhiều PVC trên cùng một cổng vật lý thì Split horizon lại gây ra một rắc rối về mặt cập nhật định tuyến.

**Hoạt động**

Nhờ vào cấu trúc inverse ARP, các router trong vùng Frame relay có thể map được địa chỉ giữa lớp data-link và lớp network lại với nhau

Các router trong mạng Frame relay khi khởi động, các gói tin LMI sẽ được gửi đi để kiểm trả trạng thái hoạt động của mạng.

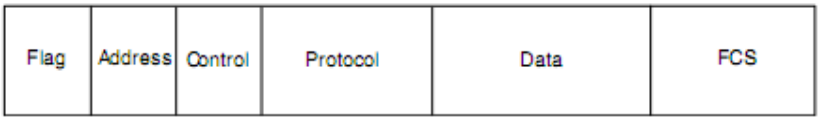
Các router sẽ thực hiện việc kiểm tra trạng thái của mạng theo chu kì lặp lại nhưng những lần sau này nó chỉ nhận được trả lời về những thay đổi trạng thái mới xảy ra. Sau một số lần nhất định như vậy mạng sẽ gửi lại một lần đầy đủ các thông tin về trạng thái mạng.

Nếu router cần ánh xạ giữa VC và địa chỉ lớp mạng thì nó sẽ gửi gói tin Inverse ARP ra mỗi VC. Thông điệp Inverse ARP trả lời sẽ cho phép router có thể ánh xạ giữa địa chỉ mạng và DLCI tương ứng. Nếu trong mạng có chạy nhiều giao thức lớp mạng khác nhau thì gói tin Inverse ARP được gửi đi nhiều lần tương ứng với mỗi giao thức lớp mạng khác nhau.

## 2.2 PPP

PPP (Point-to-point protocol) là một giao thức nằm tại tầng Data Link thường được dùng trên các cổng bất đồng bộ (dial-up) hay cổng đồng bộ (ISDN) và dùng LCP (Link Control Protocol) để triển khai và duy trì trên một kết nối Wan.

Mục đích cơ bản của PPP là vận chuyển các gói tin tại lớp 3 xuống lớp 2 và thông qua liên kết point-to-point.

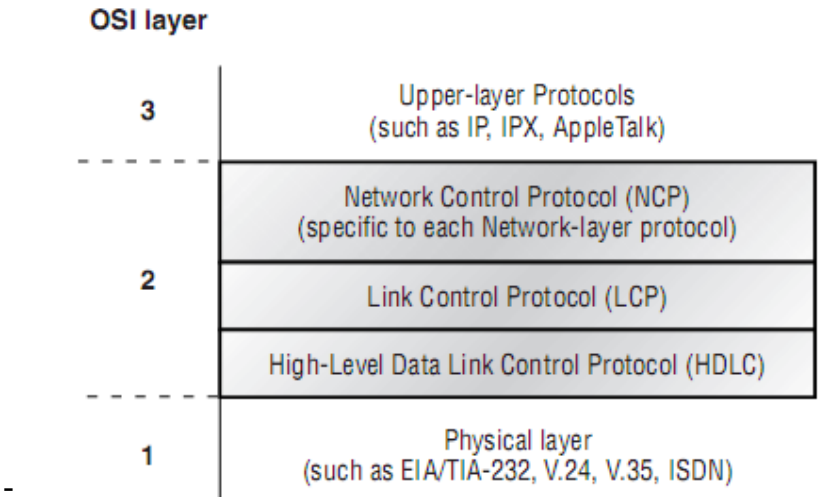


Trong một frame PPP gồm có:

- Flag: có kích thước 1 byte, cờ flag cho biết bắt đầu và kết thúc của một frame. Cờ này bao gồm 1 chuỗi nhị phân 01111110
- Address: có kích thước 1 byte, gồm 1 chuỗi số nhị phân 11111111, đây là địa chỉ broadcast. PPP không chỉ định địa chỉ riêng chọn trạm.
- Control: có kích thước 1 byte bao gồm chuỗi nhị phân 00000011, là dịch vụ truyền thông kết nối tương tự như LLC (Logical Link Control) loại 1, truyền dữ liệu không theo 1 chuỗi.
- Protocol: chiều dài 2 byte cho biết giao thức nào được đóng gói trong frame
- Data: có chiều dài từ 0 byte trở lên và chứa dữ liệu của các lớp ở trên.chiều dài tối đa của phần dữ liệu là 1500 byte
- FCS: thông thường có chiều dài 2 byte được dùng để kiểm tra lỗi của frame

PPP bao gồm 4 thành phần

- E1A/TIA-232-C: Đây là chuẩn quốc tế của truyền tín hiệu tại lớp vật lý
- HDLC: một phương thức đóng gói dữ liệu thông qua cổng liên kết serial
- LCP: một phương thức để thiết lập, cấu hình, duy trì và huỷ bỏ kết nối point-to-point
- NCP: là một phương thức để thiết lập và cấu hình các giao thức khác nhau tại lớp mạng. PPP được thiết kế để có thể sử dụng nhiều giao thức khác nhau tại lớp mạng cùng một lúc. Ví dụ như là IPCP (Internet Protocol Control Protocol) và IPXCP (Internetwork Packet Exchange Control Protocol)




Link Control Protocol (LCP) có thêm nhiều tuỳ chọn cho việc đóng gói dữ liệu:

- Xác thực (Authentication): phía bên thiết lập phải send thông tin người dùng để xác định. 2 phương thức xác thực người dùng được dùng ở đây là PAP và CHAP.

- Nén (Compression): sẽ nén frame khi truyền kết nối PPP, giúp giảm lưu lượng truyền tải. Bên kia khi nhận được frame dữ liệu sẽ được giải nén. Cisco dùng 2 phương thức để thực hiện nén là Stacker và Predictor

- Phát hiện lỗi (Error detection): PPP dùng thông số Quality và Magic để đảm bảo đường truyền không bị loop và độ tin cậy của đường truyền

- Multilink: bắt đầu ở Cisco IOS phiên bản 11.1, chức năng Multilink mới được đưa vào trong router Cisco. Dùng để chia sẽ đường truyền thông qua 2 hay nhiều đường dây song song với nhau.

**Thiết lập phiên kết nối PPP**

Khi kết nối PPP được thiết lập thì sẽ trải qua 3 phiên làm việc

- Phiên thiết lập kết nối: mỗi thiết bị PPP sẽ gửi gói tin LCP để cấu hình và kiểm tra liên kết. Gói tin LCP có một trường được gọi là Configuration Option cho phép các thiết bị có thể thoả thuận với nhau để thực hiện các cấu hình trên đường truyền như là kích thước của dữ liệu, kiểu nén dữ liệu và

phương thức xác thực. Nếu không có trường Configuration Option thì các cấu hình mặc định sẽ được dùng

- Phiên xác thực: PAP, CHAP là 2 phương thức được sử dụng trong việc xác thực. Việc xác thực sẽ diễn ra trước khi các thông tin giao thức tại lớp mạng được xem xét.
- Phiên cấu hình giao thức lớp mạng: PPP dùng NCP để cho phép nhiều giao thức tại lớp mạng được đóng gói và gửi thông qua liên kết PPP.

Phiên kết nói PPP sẽ ngưng kết nối khi

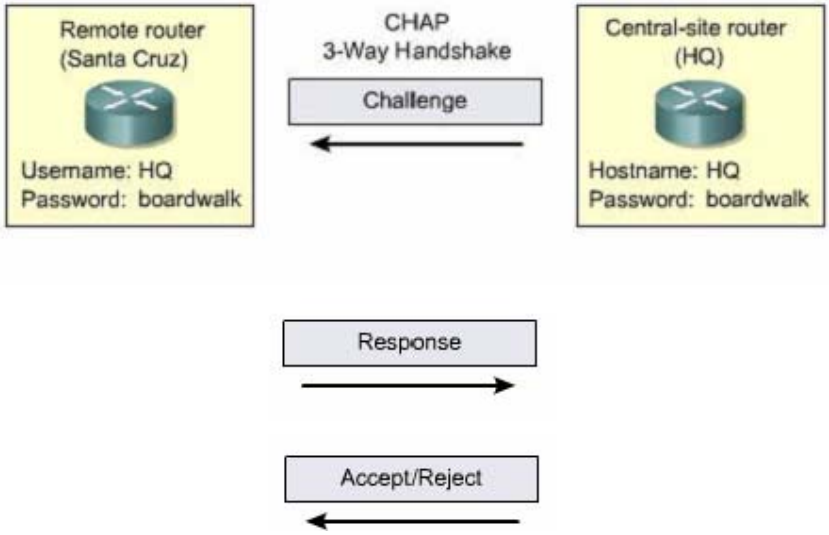
- Frame LCP đóng đường truyền
- Hết thời gian chờ
- Có sự can thiệp của người dùng

**Các phương thức xác thực trong PPP**

Có 2 phương thức xác thực được dùng trong PPP là Password Authentication Protocol (PAP) và Challenge Handshake Authentication Protocol (CHAP)

Password Authentication Protocol (PAP): PAP là phương thức xác thực ít bảo mật hơn CHAP. PAP cung cấp một cơ chế xác thực đơn giản sử dụng quá trình bắt tay 2 bước. Password sẽ được gửi đi ở dạng clear text, chính vì vậy rất dễ bị tấn công và lấy được password. Khi liên kết PPP được thiết lập xong, bên thiết lập kết nối sẽ nhận được username và password từ router kia gửi sang cho đến khi xác nhận được.

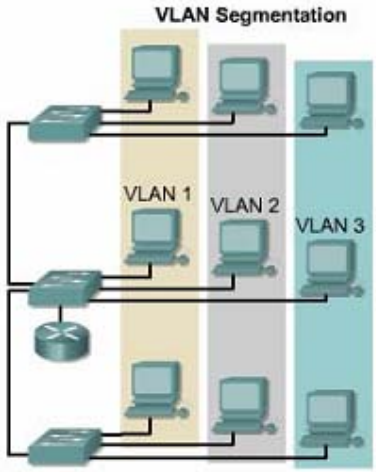
Challenge Handshake Authentication Protocol (CHAP): Sau khi hoàn thành bước thiết lập đầu tiên, router muốn thiết lập liên kết sẽ gửi gói tin challenge đến router bên kia. Router bên kia sau khi nhận được gói tin challenge, sẽ dùng thông số này kết hợp với password để tạo ra một giá trị thông qua thuật toán MD5 và gửi sang cho router thiết lập kết nối. Gói tin này là Response. Sau khi nhận được gói tin Respone. Sau khi nhận được gói tin Respone. Router sẽ tính toán và đưa ra một giá trị dựa trên thông số của gói tin Respone đã nhận trước đó. Nếu kết quả trùng với giá trị của gói tin challenge thì sẽ bắt đầu xác nhận.



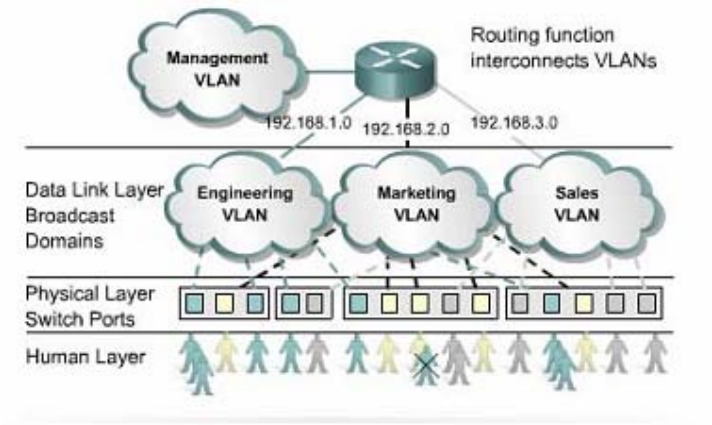

## 2.3 Vlan

Vlan là một nhóm logic các thiết bị mạng hay các user trong môi trường mạng cục bộ, các thiết bị hay các user thuộc Vlan nào thì chỉ liên lạc trong nội vùng Vlan của nó. Điều này giúp cho người quản trị dễ dàng quản lí và đặt ra các chính sách bảo mật cho từng Vlan khác nhau. Để các Vlan có thể liên lạc với nhau thì cần phải có một router đứng ra đảm nhận vai trò định tuyến giữa các Vlan đó. Trong một hệ thống mạng lớn đòi hỏi việc phân chia Vlan là rất cần thiết. Các công ty hay tổ chức thường sử dụng Vlan để tạo thành các nhóm logic mà không cần phải quan tâm đến địa lí vật lí của các thiết bị hay user trong nhóm đó. Với việc sử dụng Vlan sẽ giúp cho mạng có khả năng phát triển, bảo mật và quản lí tốt hơn. Bởi việc hạn chế các gói tin broadcast

gửi phát đi toàn mạng. Có thể nói Vlan là một công cụ rất mạnh và cần thiết trong thiết kế và cấu hình mạng.




Hình: chia các nhóm thành các vlan khác nhau mà không cần quan tâm đến vị trí thiết bị

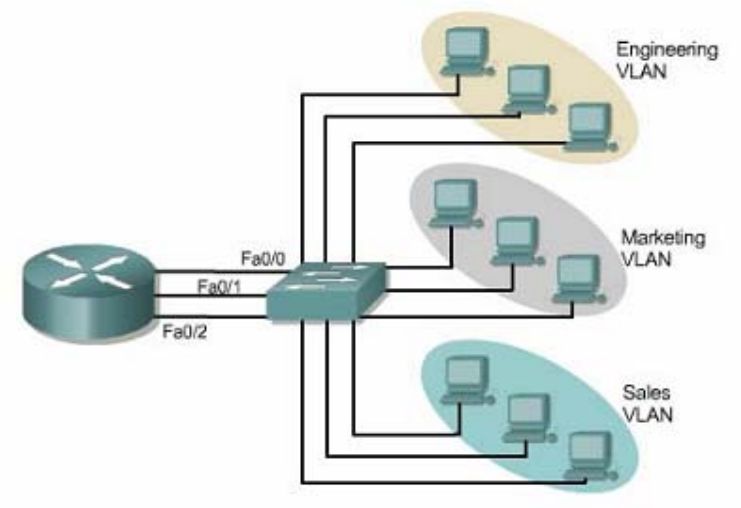



Hình: dùng một thiết bị router để thực hiện định tuyến cho các vlan

**Hoạt động của Vlan**

Trên switch sẽ tạo các Vlan tương ứng mà người quản trị mạng muốn, sau đó các Vlan vừa tạo ra sẽ đước áp đặt lên các interface của switch đó. Các thiết bị nào cắm vô port nào thuộc vlan nào sẽ trở thành thành viên của vlan đó. Các thành viên của vlan

nào chỉ có thể liên lạc với nhau qua và không thể liên lạc sang vlan khác. Để làm được điều này cần phải có một thiết bị lớp 3 hỗ trợ. Router Vyatta có hỗ trợ tính năng định tuyến giữa các vlan với nhau.




Trong ảnh ví dụ về Vlan, mỗi bộ phận được đưa vào mỗi Vlan hoàn toàn khác nhau. Nếu một thành viên trong Vlan sales gửi một gói tin đến cho thành viên khác cũng trong Vlan sales thì gói tin đó sẽ có dest MAC address là MAC của thành viên muốn gửi đến. Khi gói tin này đến switch, switch sẽ nhận thấy gói tin này xuất phát từ Vlan sales nên sẽ tìm địa chỉ MAC trong Vlan sales.

Nếu một thành viên trong Vlan sales gửi một gói tin đến Vlan marketing thì cần phải có một thiết bị router hỗ trợ cho việc định tuyến giữa các Vlan. Lúc này gói tin được gửi từ Sale sẽ có dest MAC address là MAC address của router đứng ra làm vai trò định tuyến. Khi gói tin này đến switch, nhận thấy MAC address này không thuộc Vlan sales nên gửi gói tin đến router. Router sẽ thực hiện chuyển gói tin này đến Vlan marketing.

Để cho việc liên lạc giữa các Vlan khác nhau, các interface của router Vyatta phải được cấu hình trỏ về 1 Vlan. Như mô hình ở trên thì interface Fa0/0 của Router sẽ được trỏ về Vlan engineering, interface Fa0/1 trỏ về Vlan marketing, interface Fa0/2 trỏ về Vlan sales. Các máy thuộc Vlan nào sẽ đặt default gateway trỏ về interface của router có Vlan tương ứng với Vlan của mình.

**Lợi ích của Vlan**

Khi sử dụng Vlan trong hệ thống mạng, người quản trị có thể tổ chức mạng theo ý muốn và dễ dàng quản lí hơn:

- Nhóm các thành viên trong mạng thành một group Vlan với nhau mà không cần quan tâm đến vị trí của các máy
- Thêm hay xóa bỏ các thành viên trong Vlan dễ dàng
- Hạn chế việc phát broadcast, tăng hiệu năng của hệ thống mạng

## 3. Services

### 3.1 Cấu hình

**Giao diện command**

Khi khởi động hệ thống vyatta thì đây là giao diện mặc định khi cấu hình. Trong hệ thống cấu hình bằng command line sẽ có 2 chế độ: operational và configuration mode

Operational mode cho phép hiển thị và xóa thông tin, enable va disable debug, loading và saving cấu hình, khởi động lại hệ thống

```
vyatta@vyatta:~$ show version
Version   :    3.0.2
Copyright:    2006-2008 Vyatta, Inc.
Built by :    autobuild@vyatta.com
Built on :    Wed Apr 16 08:26:33 UTC 2008
Build ID :    080416082620a705a
Boot via :    livecd
Uptime   :   14:22:45 up 35 min,  2 users,  load average:
0.00, 0.00, 0.00
vyatta@vyatta:~$
```

Configuration mode cho phép tạo, chỉnh sửa, xóa, commit và hiển thị thông tin cấu hình

```
vyatta@R1# set interfaces ethernet eth1 address
192.168.1.61/24
[edit]
vyatta@R1# commit
[edit]
vyatta@R1#
```

Khi chúng ta log on vào hệ thống Vyatta , thì hệ thống mặc định là operational mode

Để chuyển mode từ operational mode sang configuration mode , dùng lệnh **configure**

```
vyatta@vyatta:~$ configure
[edit]
```

Nếu chúng ta đang ở configuration mode muốn chuyển sang operational mode dùng lệnh exit

```
vyatta@vyatta# exit
exit
vyatta@vyatta:~$
```

**CLI help**

Vyatta cung cấp 2 loại command: Command của hệ điều hành Linux và command xây dựng cho Vyatta, tuy nhiên CLI của Linux chi đươc sử dụng ở mode Operate

ở chế độ command line interface, Vyatta cung cấp một hệ thống help cực kì linh hoạt

help: hiển thị tất cả dòng lệnh của shell command

help command: hiển thị ý nghĩa dòng lệnh và các tham số dòng lệnh được chỉ định

<TAB>?: Đối với user không có quyền root sẽ hiển thị tất cả command của Vyatta và cung cấp hoàn thành câu lệnh, Đối với user có quyền root hiển thị tất cả các command của Vyatta và shell command, cung cấp hoàn thành câu lệnh

**Thêm vào cấu hinh Vyatta**

Để thêm vào cấu hình Vyatta, ta dùng lệnh Set trong chế độ configuration mode.

Ví dụ để cấu hình ip cho card mạng eth0 ta dung lệnh sau

```
vyatta@vyatta# set interfaces ethernet eth1 address 192.168.2.3/24
[edit]
vyatta@vyatta# _
```

**Chỉnh sửa cấu hình**

Để chỉnh sửa cấu hình ta cũng dung lệnh set tương tự như them mới cấu hình

**Xóa cấu hình**

Để xóa 1 lệnh trong Vyatta ta dung lệnh delete thay cho lệnh set

```
vyatta@vyatta# delete interfaces ethernet eth1 address 192.168.2.3/24
[edit]
vyatta@vyatta# _
```

**Sao lưu cấu hình**

Trong Vyatta , những phần ta cấu hình sẽ không được lưu cho đến khi ta dung lệnh commit

```
vyatta@vyatta# delete interfaces ethernet eth1 address 192.168.2.3/24
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# _
```

**Không lưu câu lệnh vào Vyatta**

Thay vì dung lệnh delete để xóa từng câu lệnh trước đó để xóa toàn bộ cấu hình, ta có thể dung lệnh Discard hoặc exit discard

```
vyatta@vyatta# discard
Changes have been discarded
[edit]
vyatta@vyatta# _
```

```
vyatta@vyatta# exit discard
exit
vyatta@vyatta:~$ _
```

Mặc định Vyatta load file cấu hình config.boot khi hệ thống được khởi động, Để load file cấu hình khác nằm trong đường dẫn mặc định ta dung lệnh sau

Load ten file

```
vyatta@vyatta# load testconfig
Loading configuration file
/opt/vyatta/etc/config/testconfig...
No configuration changes to commit
Done
[edit]
vyatta@vyatta#
```

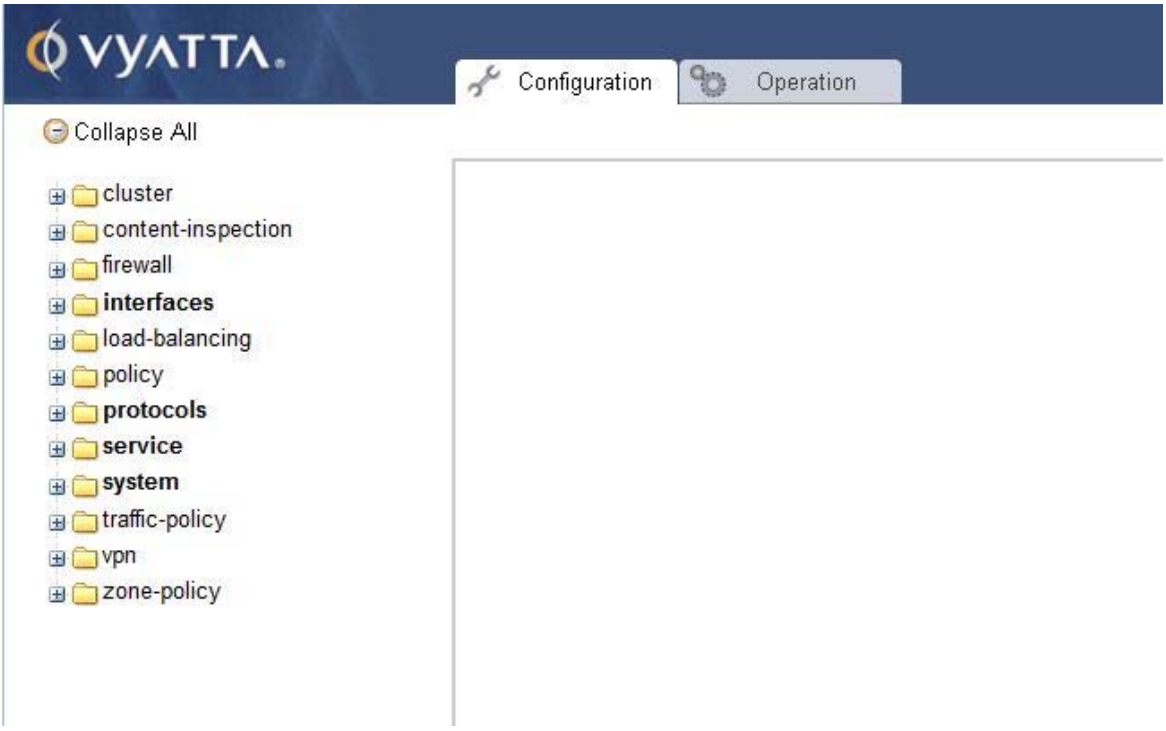
**Giao diện web**

Phần cấu hình bằng giao diện web mặc định là hệ thống vyatta khi vừa khởi động sẽ bị disable tính năng này. Chính vì vậy người quản trị cần phải enable tính năng này lên. Một điều cần lưu ý ở đây chính là Vyatta chỉ hỗ trợ cấu hình bằng giao diện web bằng giao thức https.

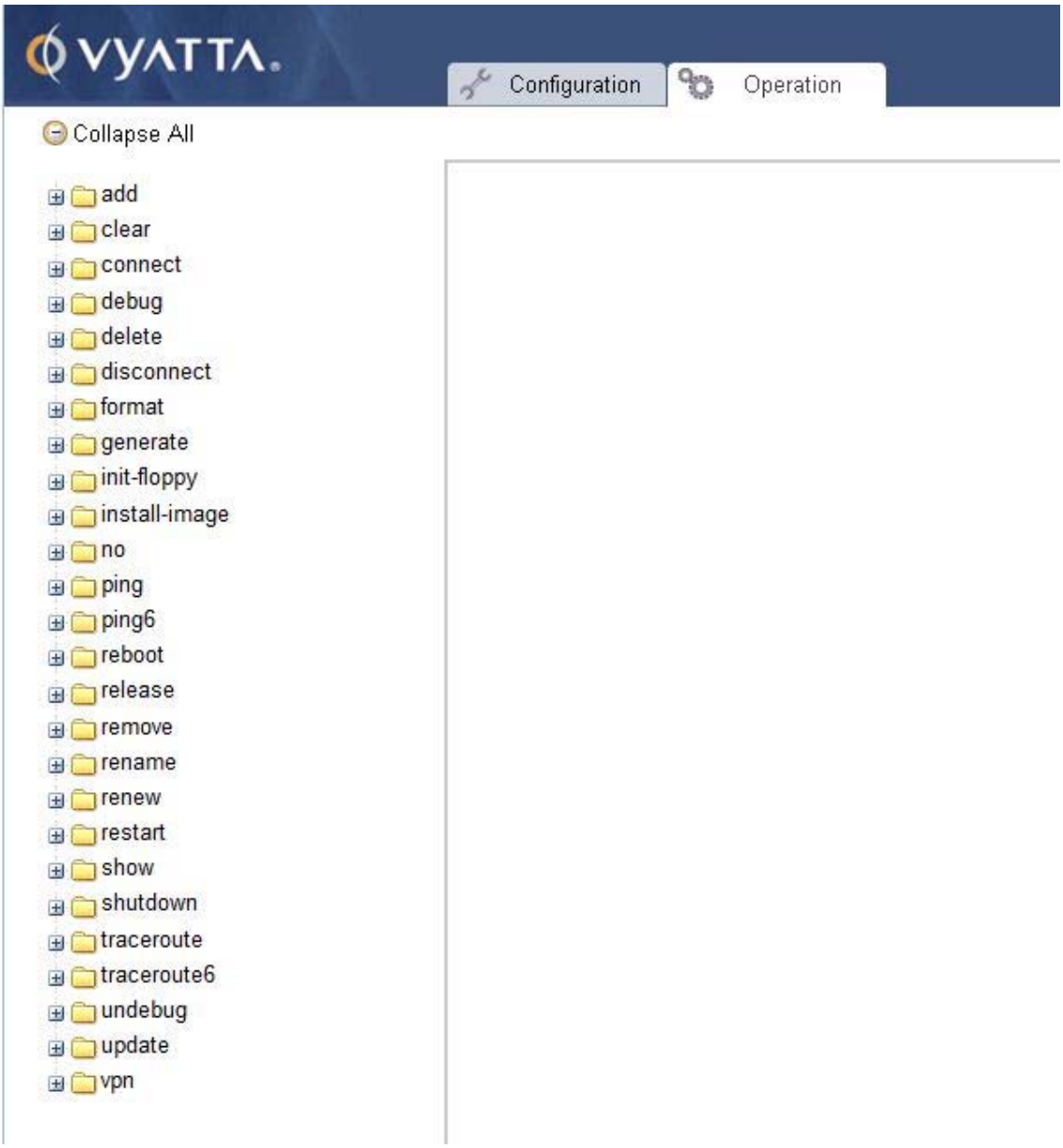

Đây là hình ảnh ban đầu khi vừa truy cập vào địa chỉ của Vyatta

Ở chế độ giao diện web thì cũng có 2 mode: operation và configuration mode

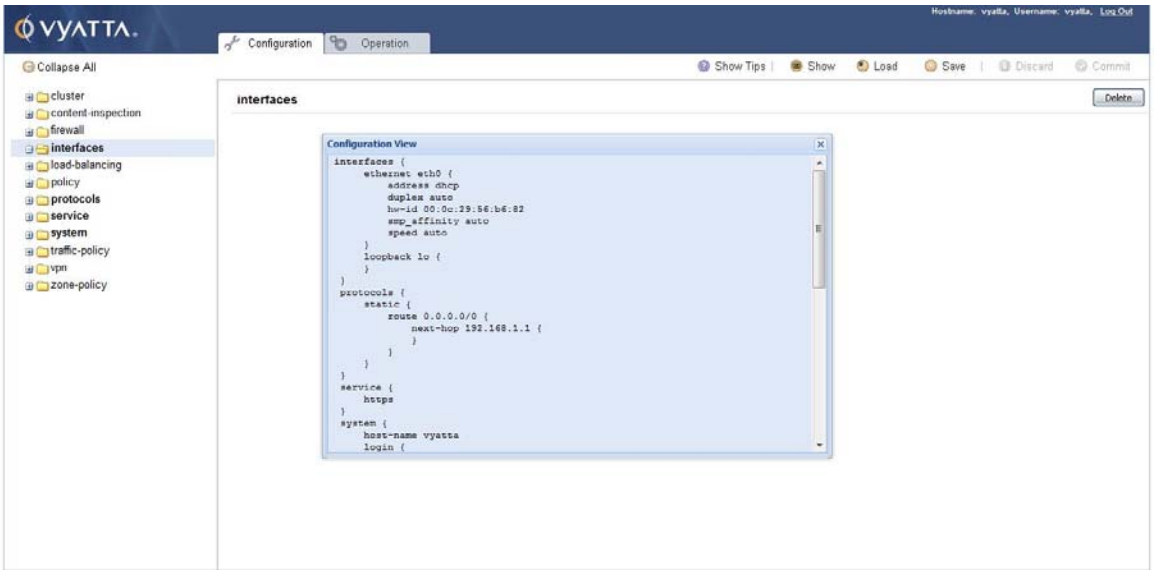
Chế độ mode configuration của giao diện web, ở mode này ta có thể tác động đến các dịch vụ về hệ thống như Nat, DHCP, System, Firewall… Dưới đây là hình ảnh minh họa ở chế độ Configuration và Operation mode trên giao diện cấu hình bằng web của Vyatta




Hình ảnh: cấu hình ở mode Configuration




Hình ảnh: cấu hình ở mode Operation của giao diện web




Thậm chí ta có thể show lên những cấu hình mà ta đã thao tác và được lưu lại ở dạng file system của Vyatta

Với 2 chế độ cấu hình bằng giao diện command và giao diện web sẽ hỗ trợ rất nhiều đối với người quản trị mạng. Nếu thao tác không quen ở các dòng lệnh khá rắc rối và phức tạp, người quản trị hoàn toàn có thể thao tác dễ dàng với giao diện khá trực quan mà Vyatta cung cấp

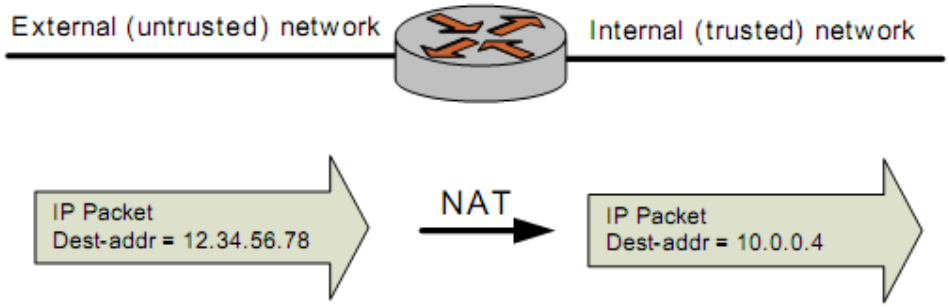
### 3.2 Telnet, SSH

Cũng như các dòng Router khác trên thị trường, Vyatta cũng hỗ trợ các dịch vụ cấu hình từ xa như Telnet và SSH (Secure Shell). Giúp cho việc linh động cấu hình các dịch vụ, hệ thống mà không cần phải đến tân nơi router để cấu hình.

### 3.3 NAT

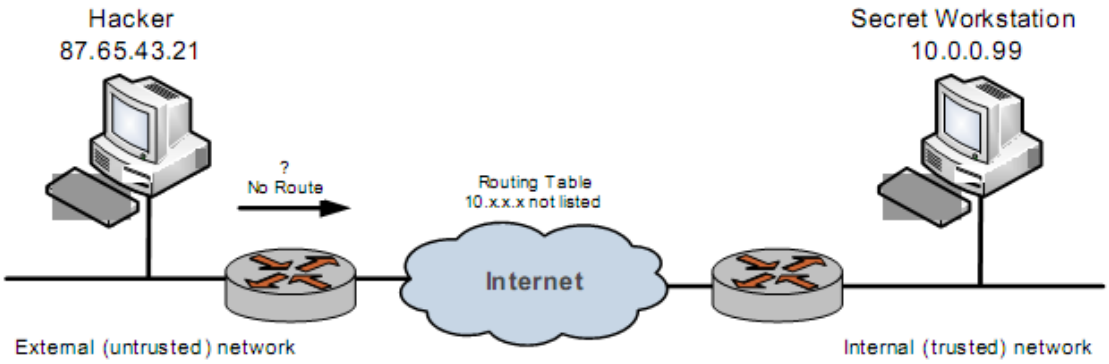
Trong hệ thống mạng, mỗi máy tính đều sẽ có 1 địa chỉ IP. Hiện nay hầu hết các máy tính đều giao tiếp với nhau bằng Ipv4. Các máy tính sử dụng trong mạng cục bộ sẽ sử dụng địa chỉ IP Private (là những địa chỉ IP không cần phải đăng kí và chỉ có giá trị trong mạng cục bộ). Nếu các máy này có nhu cầu truy cập internet thì cần phải có một địa chỉ IP Public (địa chỉ IP Public là những địa chỉ IP duy nhất và được sử dụng trên toàn thế giới, có để dùng trong routing trên internet). Chính vì vậy cần phải sử dụng đến NAT

Network Address Translation (NAT) là một dịch vụ chuyển đổi từ địa chỉ IP này sang địa chỉ IP khác khi gói tin đi qua thiết bị hay máy tính có cài dịch vụ NAT. Địa chỉ IP của thiết bị hay máy tính cài đặt NAT có thể là địa chỉ nguồn, có thể là địa chỉ đích của gói tin.



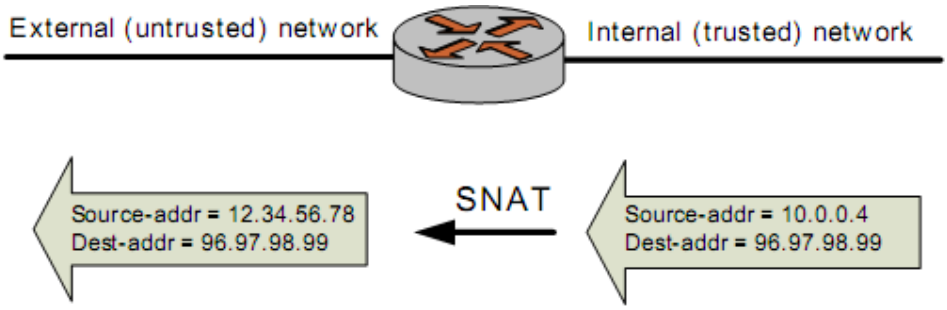

Hình ảnh minh họa về NAT

NAT giúp tăng khả năng bảo mật trong hệ thống mạng bởi việc che giấu địa chỉ IP trong mạng cục bộ và thay bằng địa chỉ IP public. Giúp cho các hacker khó hơn trong việc tấn công mạng. Tuy nhiên chỉ mang tính tương đối nên không phải là tuyệt đối nên không thể so sánh với Firewall

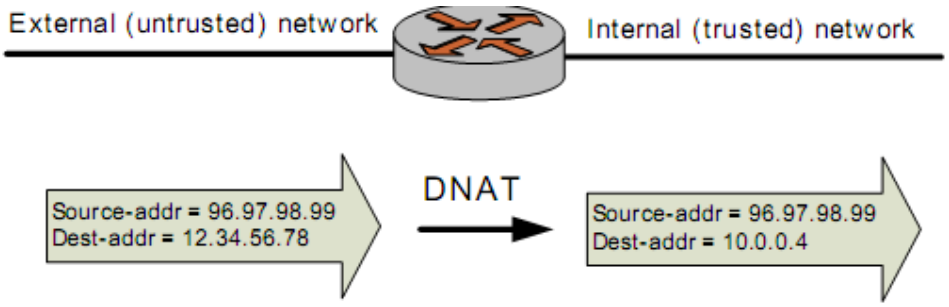



**Các dạng của NAT**

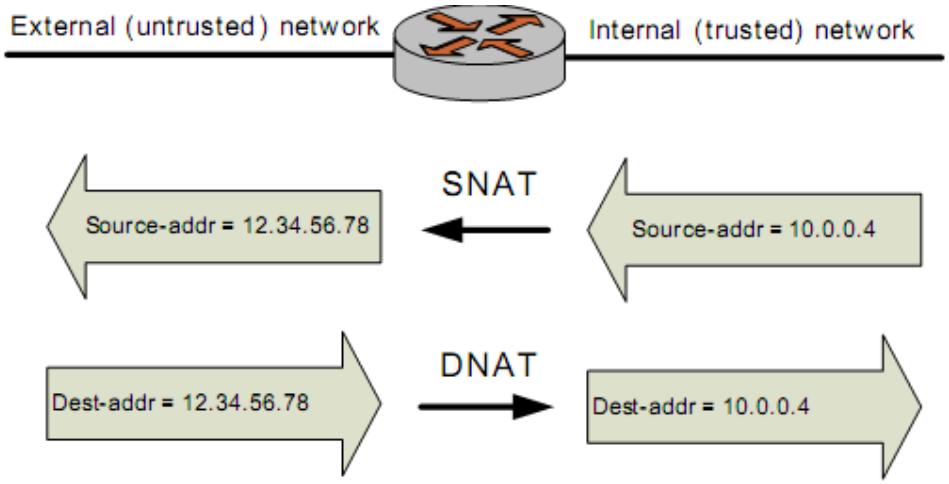
- Source NAT: còn được gọi là SNAT. Đây là một dạng NAT khả phổ biến. SNAT được dùng khi các máy tính ở mạng bên trong cần truy cập ra bên ngoài. Khi đó các gói tin đều sẽ bị thay đổi địa chỉ nguồn thành một địa chỉ public khi nó đi qua thiết bị NAT router Vyatta. "Masquerade" NAT là một dạng thủ thuật đặc biệt của SNAT. Khi một gói tin từ bên trong gửi ra ngoài, NAT router sẽ chuyển đổi IP private thành 1 IP public duy nhất, nhưng sẽ có thêm số port. Ví dụ rằng máy có địa chỉ IP 192.168.1.10 muốn truy cập trang web google.com có địa chỉ là 209.85.132.104. Khi đó NAT router sẽ nhận được gói tin có thông tin nguồn là 192.168.1.10:1204, thông tin đích là 209.85.132.104:80. Lúc này Router sẽ đổi địa chỉ nguồn thành IP public, ví dụ như là 113.22.165.133:26314. Sau đó sẽ lưu dữ liệu này vào bảng masquerade. Khi có gói tin trả lời từ trang web google.com thì router sẽ nhận được một gói tin có thông tin nguồn là209.85.132.104:80 đến địa chỉ đích là 113.22.165.133:26314. NAT router sẽ dựa vào bảng masquerade để đổi đích của gói tin thành 192.168.1.10:1204 và gửi về cho máy có địa chỉ 192.168.1.10.



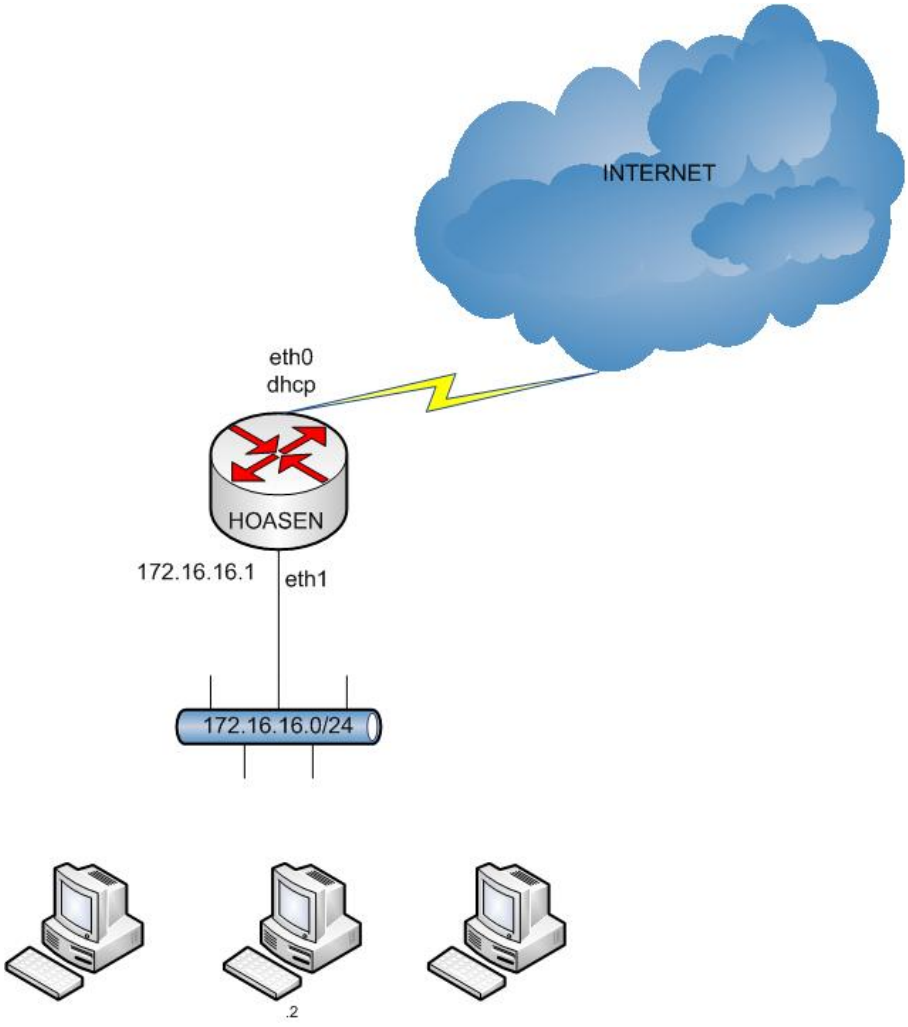

- Destination NAT: còn được gọi là DNAT. Trong khi SNAT đổi địa chỉ nguồn của gói tin thì DNAT lại đổi địa chỉ đích của gói tin khi đi qua thiết bị NAT router. DNAT được dùng khi có một yêu cầu kết nối từ mạng bên ngoài vào 1 máy bên trong của hệ thống.




- Bidirectional NAT (NAT song song): khi cả SNAT và DNAT được cấu hình hoàn chỉnh, nó sẽ được gọi là Bidirectional NAT. Bidirectional NAT được sử dụng khi các máy của mạng bên trong có nhu cầu muốn truy cập vào hệ thống mạng bên ngoài và các máy bên ngoài có nhu cầu truy cập các máy bên trong mạng.


External (untrusted) network
Internal (trusted) network
SNAT
Source-addr = 12.34.56.78
Source-addr = 10.0.0.4
DNAT
Dest-addr = 12.34.56.78
Dest-addr = 10.0.0.4

**Ví dụ về SNAT:**


INTERNET
eth0
dhcp
HOASEN
172.16.16.1
eth1
172.16.16.0/24
.2

```
configure
set system host-name HOASEN
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1

set service nat rule 1 source address 172.16.16.0/24
set service nat rule 1 outbound-interface eth0
set service nat rule 1 type masquerade
commit
```

Ở ví dụ này, hệ thống dùng dạng masquerade NAT để thực hiện NAT cho các máy client truy cập web

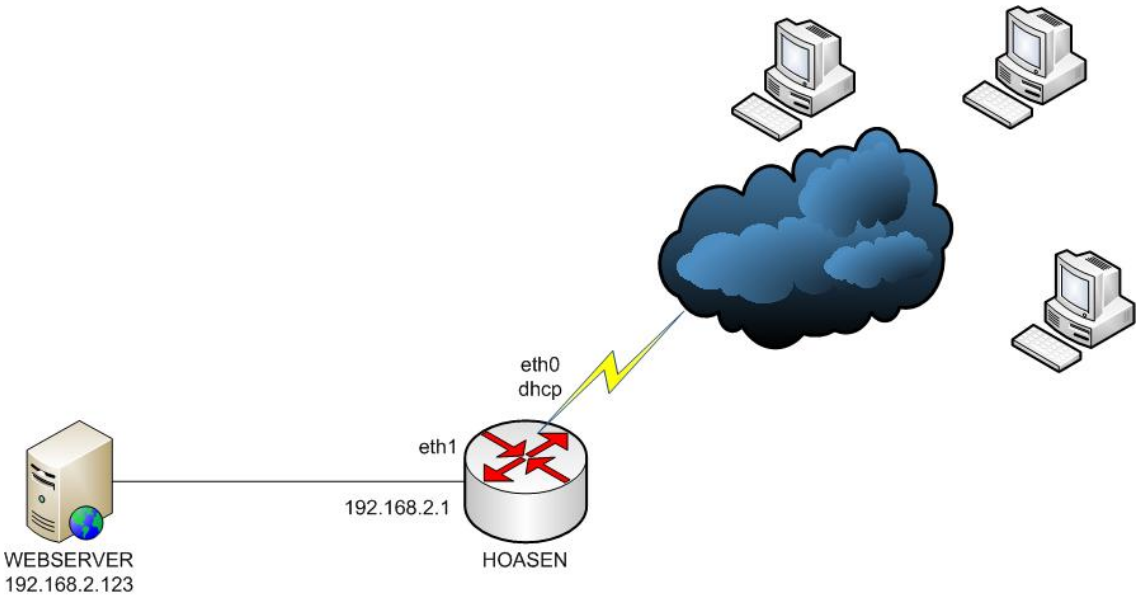
```
vyatta@vyatta:~$ show nat rules

Type Codes:  SRC - source, DST - destination, MASQ - masquerade
             X at the front of rule implies rule is excluded

rule   type  intf     translation
----   ----  ----     -----------
1      MASQ  eth0     saddr 172.16.16.0/24 to 192.168.1.42
    proto-all         sport ANY
```

Kết quả sau khi cấu hình, dùng lệnh “show nat rules” để xem dạng nat mà người quản trị đã cấu hình

```
vyatta@vyatta:~$ show nat translations
Pre-NAT              Post-NAT             Type  Prot  Timeout
vyatta@vyatta:~$ show nat translations
Pre-NAT              Post-NAT             Type  Prot  Timeout
172.16.16.2          192.168.1.42         snat  icmp  29
172.16.16.2          192.168.1.42         snat  udp   13
```

Khi bất cứ máy nào thực hiện một kết nối với bên ngoài đều sẽ được hệ thống ghi nhận lại

**Ví dụ về DNAT**




Ở hình này, hệ thống Vyatta sẽ thực hiện DNAT để cấu hình cho các client từ bên ngoài internet có thể truy cập được vào webserver.

```
configure
set system host-name HOASEN
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1

set service nat rule 1 type destination

set service nat rule 1 inbound-interface eth0
set service nat rule 1 protocol TCP
set service nat rule 1 source address 0.0.0.0/0
set service nat rule 1 destination address "ip ETH0"
set service nat rule 1 destination port 80
set service nat rule 1 inside-address address 172.16.16.2
```

```
vyatta@vyatta:~$ show nat translations
Pre-NAT             Post-NAT            Type  Prot  Timeout
192.168.1.42        192.168.2.123       dnat  tcp   431983
```

```
vyatta@vyatta:~$ show nat rules

Type Codes:  SRC - source, DST - destination, MASQ - masquerade
             X at the front of rule implies rule is excluded

rule   type  intf     translation
----   ----  ----     -----------
1      DST   eth0     daddr 192.168.1.42 to 192.168.2.123
    proto-tcp        dport 80

                     when saddr 0.0.0.0/0, sport ANY
```

Khi bất cứ client nào truy cập vào hệ thống webserver đều sẽ được ghi nhận session

lại ngay trên hệ thống Vyatta.

### 3.4 DHCP

The Dynamic Host Configuration Protocol (DHCP) là một giao thức được thiết kế để làm giảm thời gian cấu hình cho mạng TCP/IP bằng cách gán tự động các thông số cần thiết cho các client khi tham gia vào mạng.

Trong môi trường mạng, server DHCP sẽ giữ vai trò quản lý tập trung địa chỉ IP cho client và cung cấp địa chỉ IP và các thông số khác như subnet mask, default gateway, DNS cho client trong một khoảng thời gian nhất định, khoảng thời gian này được gọi là "lease". Trong khoảng thời gian này máy chủ DHCP sẽ không phân phối lại địa chỉ đã phân phối cho client. Sau hết khoảng thời gian này, user sẽ phải xin thông số IP khác. Để cho server cung cấp IP cho client, ta phải tạo các dãy các địa chỉ IP. Mỗi dãy IP phải có subnet trùng giống như subnet của interface của DHCP Server. Mỗi dãy địa chỉ khi cung cấp IP cho client sẽ có thời gian giới hạn mặc định là 24 giờ.

**Các bước cấp DHCP**

- Đầu tiên máy client sẽ phát broadcast gói tin DHCP DISCOVER, trong gói tin này có chứa địa chỉ nguồn MAC là địa chỉ MAC của client. Nếu sau 4 lần truy vấn DHCP nếu không thành công thì máy client sẽ tự phát sinh cho chính mình 1 địa chỉ IP nằm trong dãy 169.254.0.0 đến 169.254.255.255.

- Sau khi nhận được gói tin DHCP DISCOVER từ client thì DHCP server sẽ trả lời bằng gói tin broadcast DHCP OFFER. Gói tin sẽ chứa địa chỉ IP mà server sẽ cấp cho client. Trong quá trình thương thuyết này, DHCP server sẽ không cấp phát IP này cho máy nào khác

- Khi nhận được gói tin trả lời từ DHCP server, máy client sẽ gửi tiếp gói tin broadcast DHCP REQUEST đồng ý với địa chỉ IP do DHCP server cung cấp

- Cuối cùng thì DHCP server sẽ gửi gói tin DHCP ACK có thông tin xác nhận là client được cấp địa chỉ IP và các thông số khác.

```
vyatta@vyatta:~$ show dhcp leases

IP address       Hardware Address   Lease expiration     Pool          Client N
ame
----------       -----------------  ----------------     ----          --------
---
10.0.0.10        02:00:4c:4f:4f:50  2010/11/15 15:10:39  DHCP          minh
10.0.0.11        00:0c:29:a3:de:fd  2010/11/15 15:10:49  DHCP          hung-7bf
c3ac305
```

Hình ảnh: show kết quả cấp DHCP ở chế độ operational mode ta sẽ thấy được IP nào đang được cấp cho máy nào và có computername là gì

```
vyatta@vyatta:~$ show dhcp statistics pool DHCP

pool                                pool size   # leased    # avail
----                                ---------   --------    -------
DHCP                                10          2           8
```

Hình ảnh: đây là kết quả show pool sẽ cho ta biết có bao nhiêu địa chỉ đã cấp cho client

```
vyatta@R1# show service dhcp-server shared-network-name DHCP subnet 10.0.0.0/24
 default-router 10.0.0.1
 dns-server 8.8.8.8
 exclude 10.0.0.15
 start 10.0.0.10 {
     stop 10.0.0.20
 }
[edit]
```

Hình ảnh: đây là kết quả show ở mode configure, ta sẽ thấy được những thông tin ta đã cấu hình đã được thành dạng file system

**DHCP Relay**

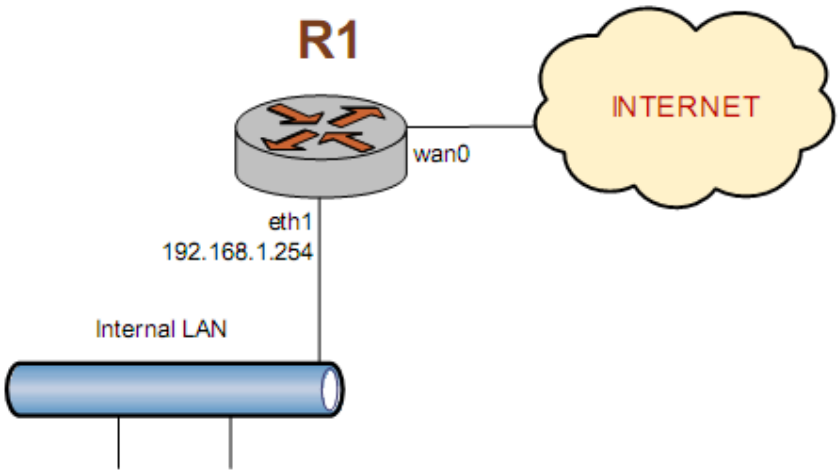
Hệ thống Vyatta cũng có hỗ trợ DHCP relay. Một DHCP relay agent sẽ nhận gói tin yêu cầu cấp DHCP từ client và chuyển thông tin yêu cầu đó đến DHCP server. DHCP relay agent được sử dụng khi mà DHCP client và DHCP server nằm ở vùng mạng khác nhau

Khi trong hệ thống có một DHCP relay agent thì quá trình cấp DHCP từ server đến một client nằm ở vùng mạng có subnet khác thì cần thông qua DHCP relay agent. Để

xin DHCP thì cũng thông qua 4 bước như trên. Client sẽ gửi các gói tin để xin IP tới DHCP relay agent bằng các gói tin DHCP DISCOVER, DHCP OFFER, DHCP REQUEST, DHCP ACK. Các gói tin này sẽ được trung chuyển đến DHCP server bằng các gói tin unicast từ DHCP relay agent.

### 3.5 Web caching

Hệ thống Vyatta có cơ chế để có thể cấu hình và hoạt động như là một web proxy server, hỗ trợ cho việc caching web và lọc URL.



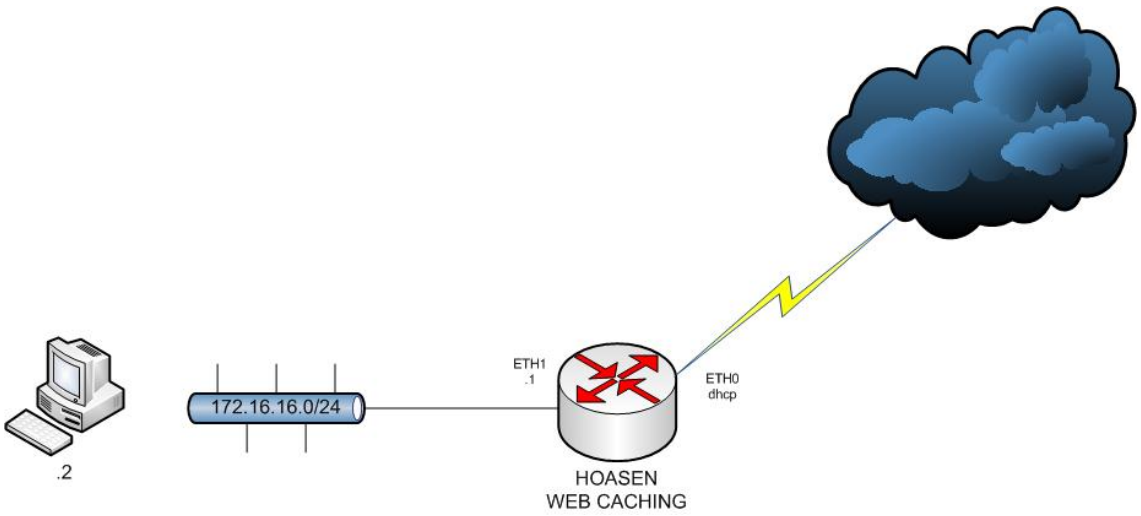

Client có thể gửi yêu cầu truy cập 1 trang web bất kì đến hệ thống Vyatta và hệ thống sẽ giúp kết nối đến webserver thay mặt cho client. Trang web sau khi được hệ thống Vyatta kết nối đến sẽ được lưu vào trong cache. Nếu trong mạng có một client khác muốn truy cập đến trang web đó thì hệ thống Vyatta sẽ lấy trang web đó từ trong cache ra và gửi về client. Điều này sẽ giúp cho việc tiết kiệm băng thông và thời gian hơn rất nhiều. Giúp hiệu năng làm việc tăng cao hơn.

Mặc định khi khởi động tính năng này, Vyatta sẽ hoạt động như là một proxy server trong suốt, hệ thống sẽ tự động chuyển đổi thành port 80 tới web proxy server. Tuy nhiên người quản trị  vẫn có thể thay đổi điều này. Để thay đổi, người quản trị phải

thiết lập bằng tay, đưa thông tin về địa chỉ proxy, port  trên trình duyệt web của client. Thuận lợi khi sử dụng dạng proxy không trong suốt là clent có thể biết chính xác được rằng proxy server nào mà mình đang sử dụng. Hơn thế nữa, có thể giúp ngăn chặn các trang web quảng cáo ở trên mạng.

Vyatta đã đưa ra khuyến cáo cho các nhà quản trị rằng không nên sử dụng dịch vụ web caching trên các máy sử dụng bộ nhớ flash làm thiết bị lưu trữ, vì việc ghi và xóa dữ liệu liên tục sẽ làm giảm tuổi thọ của thiết bị, chỉ nên dùng ở thiết bị có 1 ổ cứng riêng để lưu trữ. Mặc định cache lưu trữ là 100MB và port dùng là 3128, các luồng traffic web sẽ được chuyển sang port này.

**Ví dụ về Web caching**




Ở mô hình này, Vyatta router sẽ đóng vài trò là một webproxy server.

```
configure
set system host-name HOASEN

set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1

set service nat rule 1 source address 172.16.16.0/24
set service nat rule 1 outbound-interface eth0
set service nat rule 1 type masquerade
commit


set service webproxy listen-address 172.16.16.1
set service webproxy cache-size 200
```


Vyatta sẽ lắng nghe trên interface của mình, bất cứ yêu cầu nào đến thì Vyatta sẽ thay mặt client truy cập đến web server. Mọi truy cập đều sẽ được ghi nhận lại toàn bộ và lưu lại. Khi có yêu cầu khác truy cập đến trang này nữa thì Vyatta sẽ lấy trong hệ thống trả lời lại client

**Kết luận về các services có trong Vyatta:** các tính năng của phần mềm router mã nguồn mở Vyatta đều tương đương với một router Cisco bất kì. Các định nghĩa trong một số tính năng của Vyatta được nêu theo dạng linux bởi do Vyatta hoạt động trên nên tảng linux. Tuy nhiên về cách thức hoạt động vẫn không có gì thay đổi.

Đặc biệt về dịch vụ webcaching, Vyatta sẽ làm tốt hơn so với Cisco, bởi do hoạt động trên nền tảng X86 nên hệ thống Vyatta sẽ có một ổ cứng giúp cho việc caching được nhiều hơn hẳn so với Cisco.

## 4. Routing

### 4.1 Static route

Định tuyến là quá trình mà router thực hiện để chuyển gói dữ liệu tới mạng đích.

Static route là dạng định tuyến mà người quản trị phải nhập các thông tin về đường đi cho router. Các route được người quản trị thêm đường đi vào trong mỗi bảng routing table của từng router. Nếu trong hệ thống mạng có thêm một mạng mới thêm vào hoặc

thay đổi thì người quản trị phải xóa hay thêm đường đi vào bảng routing của từng router. Nếu trong một hệ thống mạng lớn thì việc quản lí bảng định tuyến là rất khó khăn vì mỗi khi có một sự thay đổi trong hệ thống mạng thì người quản trị rất mất thời gian và công sức. Trong môi trường mạng nhỏ thì việc dùng static route sẽ dễ dàng quản lí hơn.

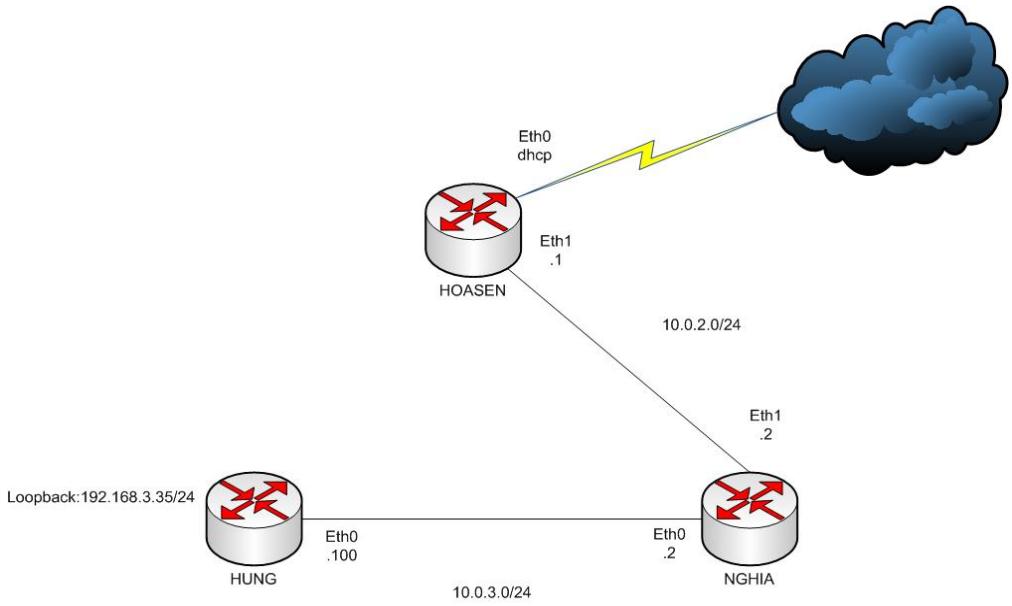
Thuận lợi khi dùng statis route:

- Không tiêu tốn tài nguyên CPU để xử lí việc lựa chọn đường đi tốt nhất
- Không tốn băng thông nhiều giữa các router vì không trao đổi thông tin bảng routing
- Bảo mật (vì chỉ có người quản trị mới cho phép routing tới các mạng bảo đảm)

Không thuận lợi:

- Người quản trị phải hiểu rõ về cấu trúc hệ thống mạng và cấu hình của từng router trong hệ thống.
- Nếu có thêm một mạng được thêm vào, người quản trị phải thêm vào đường route tới mạng này cho tất cả router.
- Không phù hợp khi sử dụng trong mạng lớn vì sẽ rất mất thời gian cho người quản trị.

**Ví dụ Static route**




```
vyatta@vyatta:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

C>* 10.0.2.0/24 is directly connected, eth1
C>* 10.0.3.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
S>* 192.168.3.0/24 [1/0] via 10.0.3.100, eth0
```

Sau khi cấu hình hoàn tất, dùng lệnh show ip route để xem kết quả: S> là viết tắt của static route. C> là các interface đang kết nối trực tiếp với router.

### 4.2 RIP (Routing Information Protocol)

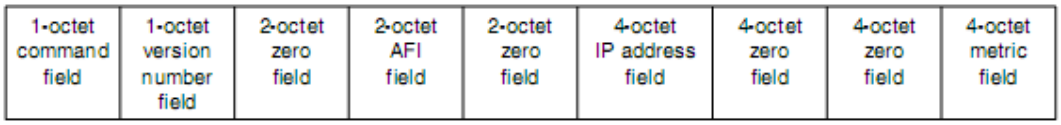
RIP là một giao thức định tuyến distance vector xuất hiện sớm nhất và được sử dụng khá rộng rãi trên thế giới. Dù còn nhiều điểm yếu nhưng RIP dựa trên chuẩn mở, sử dụng và cấu hình tương đối đơn giản nên vẫn được các nhà quản trị mạng tin dùng.

Đặc điểm của giao thức định tuyến theo distance vector là cứ đến một chu kì nhất định, các router sẽ gửi thông tin routing của mình với nhau để cập nhật. Chu kì của Rip là 30s. Nhưng mỗi khi cập nhật thì các router sẽ gửi toàn bộ bảng thông tin routing cho láng giềng học. Chính vì vậy sẽ dẫn đến việc hội tụ của các router cũng sẽ bị chậm đi. Điều này sẽ kéo theo tình trạng lặp vòng (loop) khi bảng định tuyến của các router chưa cập nhật kịp do quá trình hội tụ chậm xảy ra khi có sự cố.

Ban đầu khi vừa thực hiện tiến trình, các router RIP sẽ gửi gói tin request ra các cổng

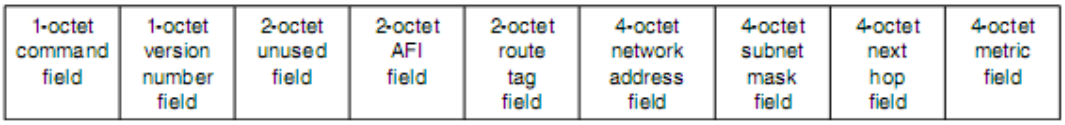
router. Gói tin này yêu cầu các neighbor gửi update thông tin bảng routing. Khi nhận được gói tin request thì các router sẽ gửi lại gói tin response chứ thông tin routing để trả lời. Tiếp đến Rip sẽ dùng thuật toán Bellman-Ford để xây dựng bảng routing.

Một gói tin RIP gồm có 9 trường




- Command: cho biết đây là gói tin request hay là respone
- Version: cho biết phiên bảng của RIP
- Address Family Identifier (AFI): có giá trị bằng 2 nếu là địa chỉ IP
- Ip Address: là địa chỉ đích của đường đi
- Metric: là giá trị hop count

Gói tin RIPv2




- Command: cho biết đây là gói tin request hay là respond
- Version: phiên bản của RIP, tại đây là 2
- Unused: có một giá trị là 0
- Router tag: cung cấp cách phân biệt giữa internal route (học bởi RIP) và external route (học từ các giao thức khác)
- Ip address: Ip của mạng cần đi
- Subnetmask: subnet của mạng cần đi

- Next hop: địa chỉ Ip của hop tiếp theo gói tin sẽ chuyển đến
- Metric: đây là giá trị hopcount

**Các phương thức chống vòng lặp của RIP**

Việc lặp vòng như trên sẽ lặp đến vô tận nếu không có tiến trình nào cắt đứt nó. Chính vì vậy giao thức định tuyến distance vector đã sử dụng thông số hop count để tránh dẫn đến việc lặp vô tận. Mỗi khi thông tin bảng routing chuyển từ router này sang router khác thì số lượng hop sẽ tăng lên 1. Giá trị tối đa mà giá trị hop có thể đạt được là 15. Như vậy khi có tình trạng lặp vòng xảy ra, nó sẽ chỉ lặp vòng đến giá trị hop là 15, nếu đến giá trị 16 thì gói tin cập nhật sẽ bị hủy bỏ. Khi giá trị đó vượt qua mức tối đa thì các router xem như mạng đó không thể đến được.

Một trong những nguyên nhân gây ra lặp vòng khi sử dụng giao thức định tuyến RIP đó là các router sau khi gửi các thông tin cập nhật bảng routing thì nó lại nhận lại thông tin mà nó vừa gửi đi từ các router láng giềng. Để tránh tình trạng này, slipt-horizon là cơ chế sẽ giúp cho các router sẽ không nhận lại thông tin cập nhật bảng routing từ cổng mà nó đã gửi gói tin cập nhật. Slipt-horizon đã giúp cho việc cập nhật thông tin sai của các router.

Route poisoning cũng được sử dụng để tránh vòng lặp. Trong hệ thống mạng ngay khi có sự cố trục trặc thì router ngay chỗ sự cố sẽ lập tức gửi gói tin thông báo cho các router láng giềng của nó với gói tin có thông số hop là 16. Vì gói tin cập nhật bảng định tuyến nào có số hop vượt quá 15 thì sẽ ngầm hiểu rằng con đường đến mạng đó không thể truy cập được.

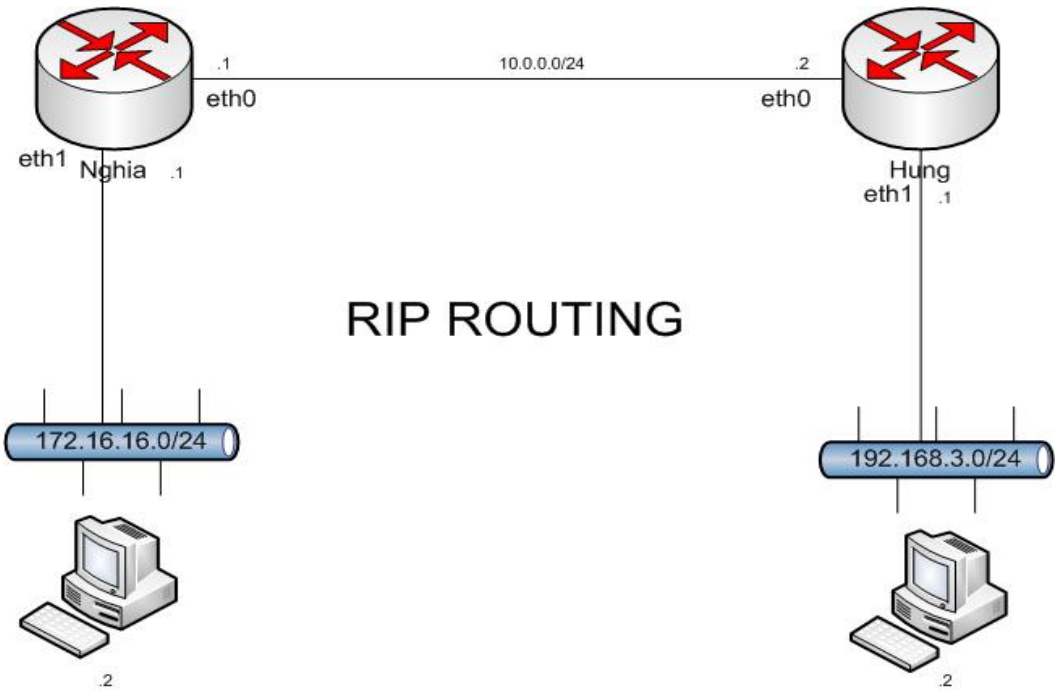
RIP có sử dụng holddown timer để xác định sự thay đổi trong hệ thống. Khi một router trong hệ thống gửi gói tin update tình trạng của nó đang thay đổi thì holddown timer sẽ bắt đầu. Trong quá trình holddown timer diễn ra, nó sẽ không cập nhật hay quảng bá đường này để tránh việc học sai thông tin. Sau khoảng thời gian đó, router sẽ nhận và gửi thông tin về tuyến đường này. Mặc định holddown timer là 180 giây.

Nếu trong hệ thống mạng có nhiều đường để cùng đến 1 đích thì RIP sẽ dựa vào số

lượng hop để tìm đường đi. RIP sẽ dựa vào đường đi nào có số hop ít nhất. Chính vì vậy một số con đường mà RIP chọn để đi không hẳn là con đường nhanh nhất. Do để tránh việc vòng lập vô tận khi cập nhật bảng routing, Rip đã giới hạn số hop tối đa là 15 hop. Do đó nếu một mạng khác nằm ngoài 15 hop đó sẽ không thể cập nhật được bảng định tuyến và không thể đến được mạng đó. Điều này làm hạn chế khả năng mở rộng của RIP rất nhiều.

RIP đến nay đã có 2 phiên bản chính. Ripv1 dùng classful routing. Nghĩa là khi gửi thông tin update về mạng, sẽ không gửi theo subnetmask của mạng. Ripv1 là giao thức được sử dụng khác phổ biến vì đa số mọi router đều có hỗ trợ giao thức này. Trong khi Ripv2 lại dùng cơ chế classless routing. Ripv2 khi gửi thông tin cập nhật định tuyến sẽ gửi kèm theo subnet của mạng.. Do đó Ripv2 có hỗ trợ VLSM và CIDR.

**Ví dụ về RIP**




Ở mô hình này, các router sẽ chạy giao thức định tuyến Rip version 2 và thực hiện quản bá thông tin mạng cho nhau.

```
R1

configure
set system host-name HUNG
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1/24

set protocols rip network 192.168.1.0/24
set protocols rip network 172.16.16.0/24



****************************************


R2

configure
set system host-name NGHIA
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 192.168.3.0/24

set protocols rip network 192.168.1.0/24
set protocols rip network 192.168.3.0/24
```

Đây là những cấu hình cần thiết để hoạt động và trao đổi định tuyến RIP. Lệnh network trong câu lệnh set protocols rip network có ý nghĩa cho phép gửi và nhận thông tin định tuyến trên các interface mà có địa chỉ mạng đã định nghĩa. Cho phép quảng bá các interface cạnh nó mà có subnet được định nghĩa.

```
C>* 10.0.0.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
R>* 172.16.16.0/24 [120/2] via 10.0.0.1, eth0, 00:00:43
C>* 192.168.3.0/24 is directly connected, eth1
```

### 4.3 OSPF (Open Shortest Path First)

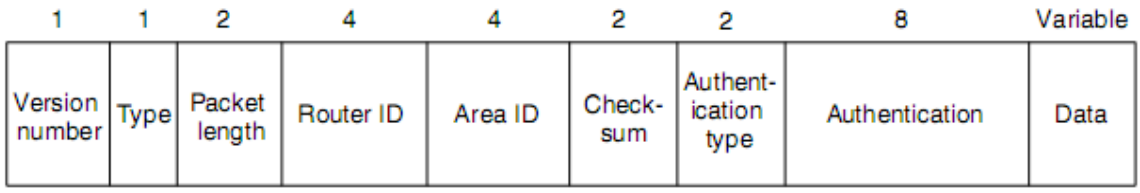
OSPF là một giao thức định tuyến theo kiểu link-state, là giao thức được triển khai theo chuẩn mở. Tức là OSPF hoàn toàn không có tính độc quyền và cho phép sử dụng rộng rãi.

Nếu so sánh với RIPv1 và RIPv2 thì OSPF là một giao thức tốt hơn bởi khả năng mở rộng. Bởi RIP đã bị giới hạn bởi số hop, có độ hội tụ chậm, tiêu hao băng thông. OSPF ra đời đã khắc phục được những yếu điểm tồn tại trong RIP. Nhờ không bị giới hạn số hop nên OSPF có khả năng mở rộng mạng, điều này rất phù hợp với các hệ thống mạng lớn và hiện đại.

Trong hệ thống mạng OSPF, mỗi router đều sẽ nắm rõ về cấu trúc sơ đồ mạng. Bởi các router OSPF thực hiện thu thập thông tin về trạng thái về các liên kết thông qua các router láng giềng. Sau khi nhận được thông tin, nó sẽ quảng bá thông tin các liên kết của nó và chuyển tiếp thông tin này cho các láng giềng khác. Router sau khi nhận được thông tin sẽ xử lý để xây dựng một cơ sở dữ liệu về trạng thái các đường liên kết trong cùng một AS. Do đó mọi thông tin về các đường liên kết của các router trong cùng một AS sẽ giống nhau. Để trao đổi thông tin các liên kết, các router sẽ gửi gói tin LSA (link-state advertisement), gói tin này sẽ chứa thông tin về các liên kết trong một vùng AS. Nhờ vào đặc điểm này mà OSPF giải quyết được vấn đề hội tụ chậm của RIP. Trong một hệ thống mạng lớn, RIP mất vài phút để có thể hội tụ được bởi mỗi router sẽ trao đổi bảng định tuyến theo mỗi chu kì. Còn OSPF chỉ cần phát ra thông tin khi về sự thay đổi trong hệ thống mạng.

Đối với RIP, khi trao đổi bảng thông tin route với láng giềng thì số hop sẽ tăng lên một. Từ đó các router sẽ lựa chọn đường nào thích hợp nhất dựa vào số hop. Chính vì vậy việc chọn lựa đường đi của RIP không dựa vào băng thông hay tốc độ của đường truyền. Việc chọn đường đi của Rip tương đối đơn giản nên không đòi hỏi nhiều bộ nhớ và khả năng xử lí của router. Nhưng OSPF sử dụng thuật tìm đường đi SPF (shortest path first) để tìm đường đi ngắn nhất. Nó sử dụng thuật toán của nhà khoa học máy tính Hà Lan Edsger Wybe Dijkstra, thuật toán này có tên là Dijkstra. Thuật toán này xem các router như là những điểm (nodes) và giữa các điểm liên kết với nhau có một chi phí nhất định. Thuật toán này là từ một điểm nhất định làm gốc sẽ tìm đường đi nào có chi phí tốt nhất để đi được đến đích. Đây là một thuật toán khá phức tạp nên đòi hỏi khả năng xử lý và bộ nhớ của router cao hơn so với RIP.

Tất cả gói tin OSPF đều có header gồm 24 byte



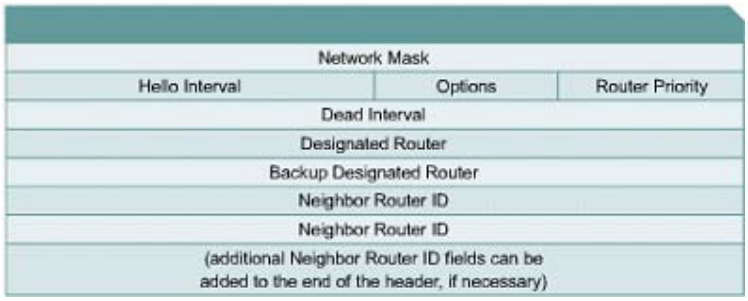

- Version number: Xác định version của OSPF

- Type: xác định dạng gói tin của OSPF với các thông số sau:
    - Hello: thiết lập và duy trì mối quan hệ neighbor
    - Database description: có dữ liệu topology, gói tin này được trao đổi với nhau khi OSPF chuẩn bị làm việc
    - Link-state request: yêu cầu cập nhật dữ liệu mô hình mạng về router neighbor. Nhưng thông tin này được trao đổi sau khi router phát hiện ra trong hệ thống mạng có sự thay đổi.
    - Link-state update: đáp trả lại gói tin link-state request
    - Link-state acknowledgment: báo nhận được gói tin update
- Packet length: chiều dài của gói tin, bao gồm cả header của OSPF
- Router ID: xác định nguồn gốc của gói tin
- Area ID: xác định khu vực truyền gói tin.
- Checksum: kiểm tra lại sự toàn vẹn của gói tin khi truyền đi
- Authentication Type: chứa dạng chứng thực OSPF.
- Authentication: chứa thông tin để chứng thực
- Data: chứa các dữ liệu đã được đóng gói lại tại các lớp trên.

**Quá trình thiết lập mối quan hệ giữa các router OSPF**

- Khi vừa khởi động tiến trình OSPF, lúc này các router vẫn chưa thiết lập bất cứ neighbor nào với các router khác. Các router sẽ gửi gói tin hello ra các cổng cấu hình theo địa chỉ multicast 224.0.0.5. Đây là địa chỉ chỉ đến các router OSPF, các router OSPF sử dụng gói tin này để thiết lập mối quan hệ neighbor. Mặc định gói hello sẽ được gửi cứ 10s một lần trong mạng broadcast và 40 s trong mạng nonbroadcast. Sau khi nhận được gói tin hello từ neighbor, router

sẽ kiểm tra các thông tin trong gói hello bao gồm: Router ID, Hello và Dead intervals timer, Neighbors, area ID, Router priority, DR Ip address, BDR Ip address, authentication password, Stub area flag. Nếu các thông số Hello và dead intervals timer, area ID, authentication password và cờ stub giống nhau thì router mới có thể trở thành neighbor của nhau.




Header của gói hello

- Các router nhận được gói tin hello sau khi kiểm tra sẽ đưa router đó vào danh sách neighbor. Sau đó nó sẽ gửi lại gói tin multicast reply cho router đã gửi gói tin hello.

- Đến lúc này các router đã thiết lập mối quan hệ neighbor với nhau, nếu có update các router sẽ trao đổi được với nhau. Nhưng như vậy sẽ tiêu hao một lượng băng thông rất lớn vì một con router sẽ trao đổi với các con còn lại. Như vậy ta sẽ có n(n-1)/2 mối quan hệ với nhau. Chính vì để tránh việc này, OSPF đã thực hiện việc bầu cử router đại diện BDR và DR cho việc thiết lập các mối quan hệ giữa các router OSPF trong cùng một vùng AS. Ban đầu OSPF sẽ chọn bất kì một router nào trong hệ thống để kiểm tra bảng danh sách neighbor của hệ thống. Bước này được thực hiện sau khi các router đã trao đổi gói tin hello với nhau, tức là tất cả các router đều có một danh sách neighbor giống nhau nên OSPF chỉ cần chọn ra một router bất kì để kiểm tra. Nó sẽ kiểm tra xem có router nào có priority là 0 hay không, nếu có thì nó sẽ loại router này ra khỏi danh sách bầu cử. Sao khi có được danh sách thì sẽ tiến hành bầu cử. Việc bầu cử router nào làm DR và BDR sẽ dựa vào độ ưu tiên priority cao nhất, nếu vẫn không chọn được DR và BDR từ priority thì sẽ lựa chọn router có chỉ số

Router-ID cao nhất, nếu vẫn không được thì sẽ dựa vào địa chi IP loopback cao nhất, tiếp đến và địa chỉ vật lý cao nhất. Sau khi bầu cử thành công DR và BDR, giả sử DR gặp sự cố thì BDR sẽ hiển nhiên trở thành DR và thực hiện bầu cử một BDR khác. Nhưng nếu khi router đảm nhận vai trò DR trước đó nếu hoạt động bình thường trở lại sẽ không thực hiện chiếm quyền trở lại.

- Từ lúc này, khi đã bầu được DR và BDR, các router thành viên khi có một bất cứ sự thay đổi gì thì các router sẽ gửi thông tin update đến DR/BDR thông qua địa chỉ multicast 224.0.0.6. Và router DR/BDR sẽ gửi lại thông tin update đến cho các thành viên khác thông qua địa chỉ multicast 224.0.0.5.

**OSPF Multi area**

Nếu trong một hệ thống mạng có số lượng router tham gia định tuyến OSPF nhiều, thì mỗi router sẽ phải nắm giữ toàn bộ cấu trúc đường đi của hệ thống mạng. Điều này dẫn đến việc các router phải làm việc quá tải. Để tránh điều này xảy ra. OSPF sử dụng multi area. Tức là các route sẽ chia vùng với nhau để quản lí. Trong đó area 0 là vùng backbone area. Các area khác sẽ phải kết nối với vùng này. Các router giao giữa 2 area khác nhau được gọi là router biên (ABR) và nó sẽ nắm giữ thông tin định tuyến của 2 vùng, còn những router nằm giao giữa giao thức định tuyến OSPF và giao thức định tuyến khác (như RIP, BGP) được gọi la ASBR (Autonomous System Boundary Router). Khi phân chia thành các area khác nhau, cũng cần quan tâm đến gói tin LSA khi trao đổi thông tin với nhau.

- LSA Type 1: gói tin này chứ thông tin router-id, dùng để cập nhật trạng thái của đường link (gói tin này gửi đến router ABR thì ngưng lại)

- LSA Type 2: gói tin này do router DR sinh ra. Chứa địa chỉ ip của interface tham gia vào mạng của chính nó. Để quảng bá cho các router khác biết nó là router DR.

- LSA Type 3: gói tin này chứa thông tin những lớp mạng nào ngoài area của nó. Gói tin này do router ABR sinh ra.

- LSA Type 4: chứa thông tin router-id của con ASBR và do router ABR sinh ra. (router ASBR khi trao đổi thông tin LSA với các router trong area của nó sẽ có thêm 1 bit e trong đó. Router ABR sẽ nhận thấy bit này và đẩy đi cho các ABR tại các area khác.

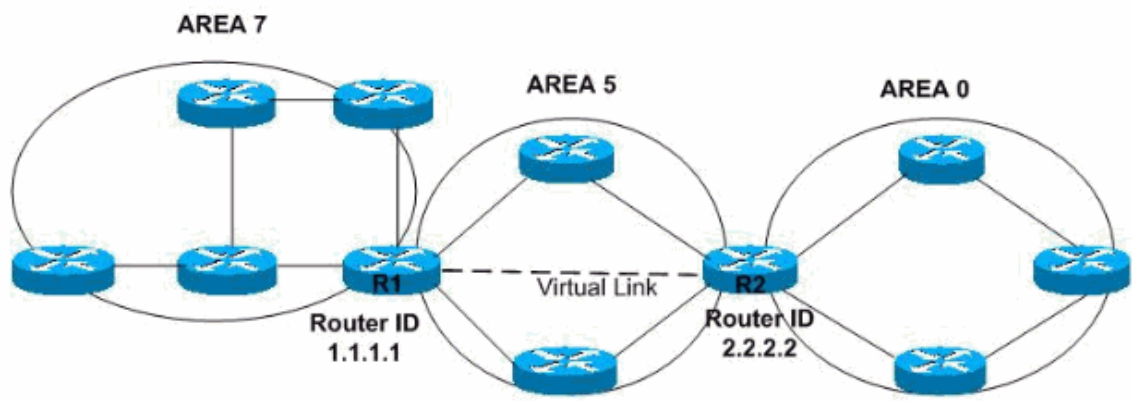
- LSA Type 5: chứ thông tin lớp mạng ngoài vùng OSPF do router ASBR gửi.

- LSA Type 7: NSSA External LSA (stub). Đây là gói tin để hạn chế các gói tin gửi update đến nó. Gói tin này sẽ được gửi từ router ASBR. Router ABR đầu tiên nhận được gói tin này sẽ gửi Type 5 đến các router còn lại. Các router khác sẽ nghĩ rằng router ABR này chính là router ASBR nên sẽ không cần biết thông tin định tuyến đến router ASBR thật. Các thông tin đều sẽ đi đến router ABR này.

**Virtual link**

Như đã nêu, area 0 là backbone area. Do đó mọi area khác đều phải được kết nối trực tiếp đến area này.

Tuy nhiên trong một vài trường hợp, có thể là do nguyên nhân khách quan trong lúc triển khai hệ thống. Người quản trị muốn tạo một area khác nữa nhưng không thể nào kết nói được với area 0 được nữa. Lúc này cơ chế Virtual link đã ra đời

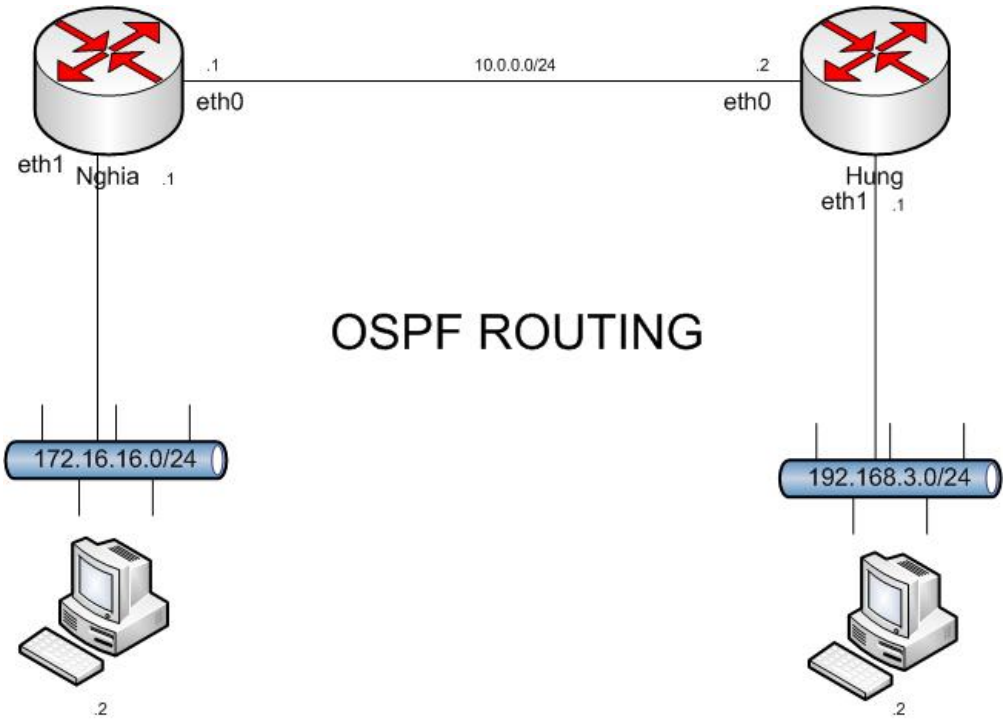


Như hình vẽ, Area 7 sẽ không thể thiết lập được neighbor hay trao đổi thông tin định tuyến với các router trong area 0. Do đó, vùng area 7 sẽ nhờ vào area 5 để tạo một virtual link kết nối đến area 0.

Virtual link sẽ được thực hiên ngay trên router ABR của 2 vùng area 7-5, area 5-0

Hãng Cisco đã từng đưa ra kiến nghị về giải pháp này. Họ cho rằng việc virtual link nên hạn chế dùng. Đây là giải pháp cứu cánh cho các hệ thống mạng không thể thay đổi được cấu trúc.

**Ví dụ về OSPF**



```
R1

configure
set system host-name HUNG
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1/24
set protocols ospf parameters router-id 10.0.0.1
set protocols ospf area 0.0.0.0 network 192.168.1.0/24
set protocols ospf redistribute connected

*****************************************

R2

configure
set system host-name NGHIA
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 192.168.3.1/24
set protocols ospf parameters router-id 10.0.0.2
set protocols ospf area 0.0.0.0 network 192.168.1.0/24
set protocols ospf redistribute connected
```

Đây là phần cấu hình cho OSPF, 2 interface 10.0.0.0/24 thực hiện trao đổi thông tin định tuyến với nhau và thiết lập neighbor.

```
vyatta@vyatta:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O   10.0.0.0/24 [110/10] is directly connected, eth0, 00:00:53
C>* 10.0.0.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.16.0/24 [110/20] via 10.0.0.1, eth0, 00:00:02
C>* 192.168.3.0/24 is directly connected, eth0
```

```
vyatta@vyatta:~$ show ip ospf  neighbor

    Neighbor ID Pri State           Dead Time Address         Interface
   RXmtL RqstL DBsmL
11.0.0.1          1 Full/Backup       37.249s 10.0.0.1        eth0:10.0.0.2
      0     0     0
```

### 4.4 BGP (Border Gateway Protocol)

Border Gateway Protocol (BGP) là 1 giao thức định tuyến được sử dụng trên Internet. Các nhà cung cấp dịch vụ Internet (Internet Service Providers - ISP) thực hiện trao đổi thông tin định tuyến giữa các mạng ngoài internet và bất cứ sự giao tiếp nào giữa những mạng ngoài internet này đều được hoàn thành thông qua BGP.

- An autonomous system (AS): chỉ số AS được đưa ra trong BGP để dễ dàng quản lí. AS là một số 16 bit, chạy từ 0-65535
    - Số 0: không dùng
    - Số 65535: không dùng
    - Số từ 64512 – 65532: là dãy số dành cho private. Khách hàng có thể dùng những AS này để thực hiện chạy giao thức BGP trong mạng nội vùng của họ
    - Các số còn lại được dùng cho public
- Pear: khi 2 router chạy cùng giao thức BGP và thiết lập một kết nối TCP giữa chúng, thì chúng được coi là Pear.
- EBGP (External Gateway Protocol): là giao thức định tuyến được sử dụng để trao đổi thông tin định tuyến giữa các router chạy BGP có các AS khác nhau.
- IBGP (Internal Gateway Protocol): là giao thức định tuyến được sử dụng để trao đổi thông tin định tuyến giữa các router chạy BGP trong cùng một AS.

**Những tính năng nổi bật của BGP**

BGP là 1 distance vector protocol với những cải tiến

BGP dùng TCP như là giao thức vận chuyển TCP port 179. BGP không thực hiện việc thiết lập neighbor một cách tự động như các giao thức định tuyến nội vùng khác. Người quản trị phải thiết lập bằng tay các neighbor của nhau.

Khi dùng BGP, cần lưu ý rằng BGP sẽ không cập nhật theo chu kỳ mà chỉ đơn thuần là keepalive theo chu kỳ để kiểm tra sự kết nối TCP.

BGP hiện có 3 cơ chế update thông tin định tuyến: Full update, partial update (cho phép người quản trị muốn update những tuyến đường mà mình muốn), default route.

Trong cấu trúc lệnh command của BGP, lệnh network sẽ hoàn toàn khác với các giao

thức định tuyến nội vùng khác như RIP hay OSPF về mặt ý nghĩa. Lệnh network trong RIP hay OSPF có ý nghĩa là sẽ thực hiện trao đổi thông tin định tuyến trên các interface mà có địa chỉ mạng theo cấu hình và cho phép quản bá interface của router có subnet như cấu hình. Còn của BGP thì hoàn toàn khác. Lệnh network có ý nghĩa là BGP sẽ đưa dò trong bảng định tuyến địa chỉ ip khi thực hiện lệnh network có nằm ở trong bảng định tuyến của nó hay không. Nếu có sẽ gửi thông tin đó cho neighbor của nó học. Đây cùng là một lưu ý rất quan trọng trong việc cấu hình triển khai BGP.

**Thiết lập phiên kết nối BGP**

Như đã nêu, BGP không thể phát hiện neighbors một cách tự động. Giao thức BGP được truyền trong một phiên kết nối TCP. Để thiết lập được neighbor, tất cả router phải được cấu hình thủ công, đưa từng neighbor vào cấu hình BGP. Sau khi cả 2 đầu router cấu hình hoàn chỉnh thì mới thiết lập neighbor được.

Các trạng thái khi thực hiện bắt tay với nhau:

- Idle: Khi router cấu hình BGP xong và xung quanh nó không có bất cứ neighbor nào để thiết lập mối quan hệ thì trạng thái của nó lúc này là Idle.
- Connect: Sau khi router được cấu hình BGP hoàn tất và chuẩn bị cho việc thiết lập mối quan hệ láng giềng. Đây chính là quá trình bắt tay 3 bước. Tuy nhiên giai đoạn này diễn ra khá nhanh. Thường người quản trị mạng sẽ không thấy được giai đoạn này. Nếu show kết quả ra mà vẫn thấy tình trạng này, có nghĩa rằng hệ thống đang có vấn đề
- Active: Sau quá trình bắt tay 3 bước thành công. Trạng thái active sẽ xuất hiện báo rằng cả 2 router chạy BGP sẵn sàng thiết lập kết nối
- Opensent: đây gần giống như là gói tin hello của các giao thức định tuyến nội vùng khác
- Open confirm: đây là gói tin trả lời xác nhận của gói opensent
- Established: trạng thái này chỉ xuất hiện khi 2 router trở thành neighbor của

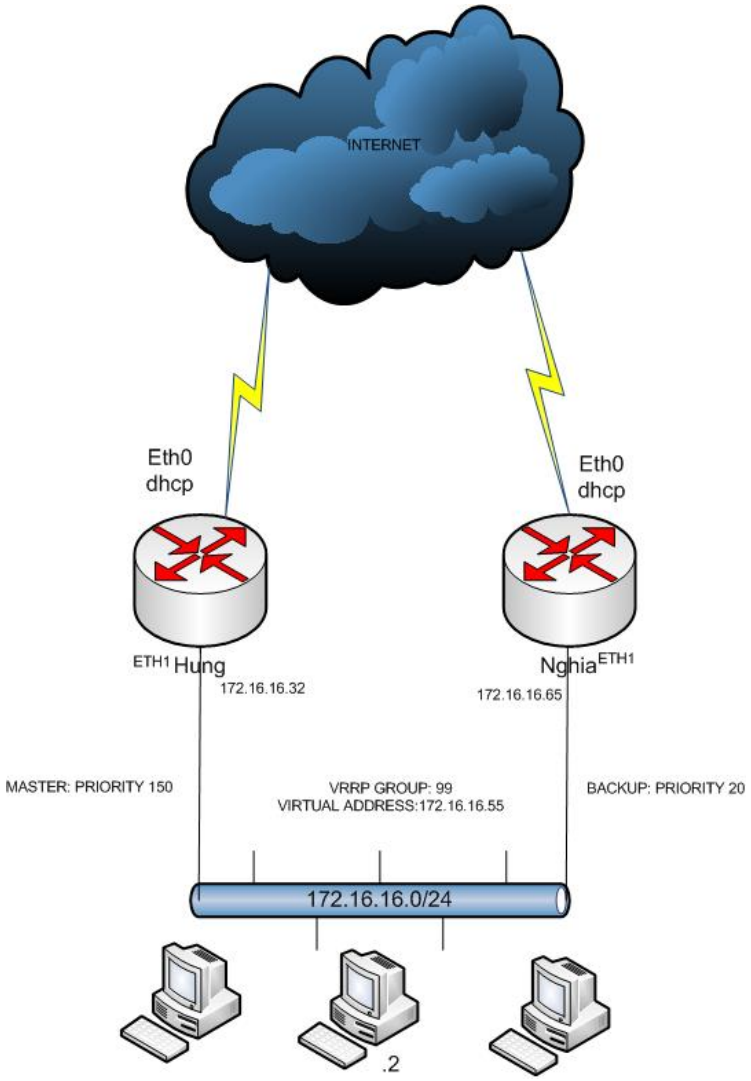
nhau và có thể trao đổi thông tin định tuyến qua lại với nhau.

**Kết luận:** Có thể nói các tính năng, khái niệm về Routing của hệ thống Vyatta về cơ bản là tương đương với các dòng router khác, đặc biệt là Cisco. Với giao diện command line giúp người quản trị mạng vốn đã quen thuộc với môi trường shell càng trở nên dễ dàng hơn. Bên cạnh đó Vyatta còn hỗ trợ thêm phần giao diện web giúp cho người quản trị dễ dàng hơn trong việc thiết lập và xây dựng.

## 5. Availability

### 5.1 VRRP

Virtual Router Redundancy Protocol (VRRP) là giao thức cho phép nhóm nhiều router thành một router ảo. VRRP là một chuẩn của IEEE (RFC 2338). VRRP được thiết kế với mục đích làm tăng khả năng chịu lỗi của các kết nối khi có sự cố xảy ra.




**Đặc điểm của VRRP**

VRRP Group: dùng để chỉ một nhóm các Router được sử dụng cùng hệ thống mạng và giữa chúng sẽ dùng 1 địa chỉ IP ảo để làm đại diện cho tất cả nhóm Router này. Địa chỉ IP ảo này sẽ link đến địa chỉ MAC của con Router làm master để khi có dữ liệu truyền qua thì sẽ đi qua con Router master. Khi con Router master gặp sự cố thì địa chỉ IP ảo đó sẽ được link đến con Router master. Điều này có thể làm được dễ dàng nhờ vào việc gửi các gói tin gratuitous ARP. Để các Router có thể nhóm với nhau thành một group VRRP thì trước hết mỗi Router phải được định nghĩa thông số VRRP group là giống nhau và địa chỉ IP ảo phải giống nhau. Địa chỉ IP ảo này phải cùng subnet với các interface của các Router trong VRRP group nhưng không nên để

địa chỉ IP ảo này trùng với địa chỉ IP thật của một trong các Router trong group.

```
vyatta@vyatta:~$ show interfaces
Interface    IP Address          State       Link   Description
eth0         192.168.1.50/24     up          up
eth1         10.0.0.1/24         up          up
eth1         10.0.0.100/24       up          up
lo           127.0.0.1/8         up          up
lo           ::1/128             up          up
```

Hình ảnh: Router master khi show interface ra sẽ thấy địa chỉ IP ảo của VRRP group

**Phương thức bầu chọn master và backup Router.**

Các Router sẽ bầu chọn master và backup dựa vào thông số priority. Đây là thông số quyết định xem ai sẽ được bầu chọn để làm Router chính để truyền dữ liệu. Thông số priority mặc định nếu không cấu hình sẽ bằng 1. Số priority sẽ chạy từ 1 đến số 255. Nếu các Router có cùng chỉ số priority thì sẽ xét đến thông số thứ 2 là địa chỉ IP. Router nào có địa chỉ IP tốt hơn hiển nhiên sẽ trở thành master. Nếu con Router master gặp sự cố thì interface nào tham gia vào group VRRP nếu có độ ưu tiên cao hơn sẽ được chọn làm master. Nhờ vào gratuitous ARP message nên khi có thay đổi ở Router master thì địa chỉ IP ảo của VRRP group sẽ được link đến địa chỉ MAC thích hợp. Có một điều cần lưu ý đó là Vyatta khuyến cáo nếu hệ thống có thể có nhiều Router đóng vai trò backup thì nên đặt các thông số priority khác nhau.

```
vyatta@vyatta:~$ show vrrp
Physical interface: eth1, Source Address 10.0.0.1
  Interface state: up, Group 1, State: master
  Priority: 100, Advertisement interval: 1, Authentication type: none
  Preempt: true, VIP count: 1, VIP: 10.0.0.100/24
  Master router: 10.0.0.1
  Last transition: 3m33s
```

```
vyatta@vyatta:~$ show vrrp
Physical interface: eth1, Source Address 10.0.0.10
  Interface state: up, Group 1, State: backup
  Priority: 99, Advertisement interval: 1, Authentication type: none
  Preempt: true, VIP count: 1, VIP: 10.0.0.100/24
  Master router: 10.0.0.1 [00:0C:29:35:D4:4E], Master Priority: 100
  Last transition: 12s
```

Hình ảnh: Router có priority 100 cao hơn con Router còn lại nên được làm master

Các Router trong VRRP group sẽ liên lạc với nhau bằng địa chỉ multicast 224.0.0.18 port 112. Trong một thời gian nhất định thì Router giữ vai trò làm master sẽ gửi gói tin đến địa chỉ multicast này để các Router backup còn lại nhận biết rằng tình trạng của Router master vẫn còn hoạt động. Gói tin này được gọi là heartbeat packets. Nếu sau một thời gian cố định gọi là dead interval mà các Router backup vẫn chưa nhận được gói tin heartbeat của Router master thì ngay lập tức việc bầu chọn sẽ diễn ra ngay lập tức giữa các Router backup. Và thời gian gửi gói tin định kì mặc định là 1 giây

Giao thức VRRP là một giao thức có đặc điểm là có thể chiếm quyền. Nếu tính năng này được enable trong hệ thống Vyatta thì nếu một Router mới tham gia vào mạng mà có chỉ số priority cao hơn với Router master hiện tại thì nó có thể được chiếm quyền làm master. Tính năng này mặc định được kích hoạt trong Router Vyatta.

## 5.2 Wan Load Balancing

Hệ thống Vyatta cho phép hỗ trợ cơ chế cân bằng tải tự động cho luồng dữ liệu theo chiều outbound trên 2 hay nhiều cổng interface. Cơ chế cân bằng tải giúp cho tính sẵn sàng của hệ thống lên cao, hiệu năng làm việc và băng thông khi truyền dữ liệu sẽ được tăng lên đáng kể. Load balancing trên hệ thống Vyatta chỉ hỗ trợ cho luồng dữ liệu di chuyển theo chiều outbound

**Thuật toán cân bằng tải**

Việc cân bằng tải cần có ít nhất 2 đường truyền trở lên. Việc dữ liệu sẽ truyền trên đường nào nhiều hơn hay ít hơn sẽ phụ thuộc vào thông số weight của mỗi đường do Router định ra. Nếu sau khi cấu hình load balancing trên Router vyatta, mặc định là các chỉ số weight của các tuyến đường sẽ ngang nhau và tỉ lệ dữ liệu truyền đi sẽ là ngang nhau. Nếu tuyến đường nào có chỉ số weight cao hơn thì các gói tin dữ liệu truyền đi sẽ đi qua đường đó cao hơn.

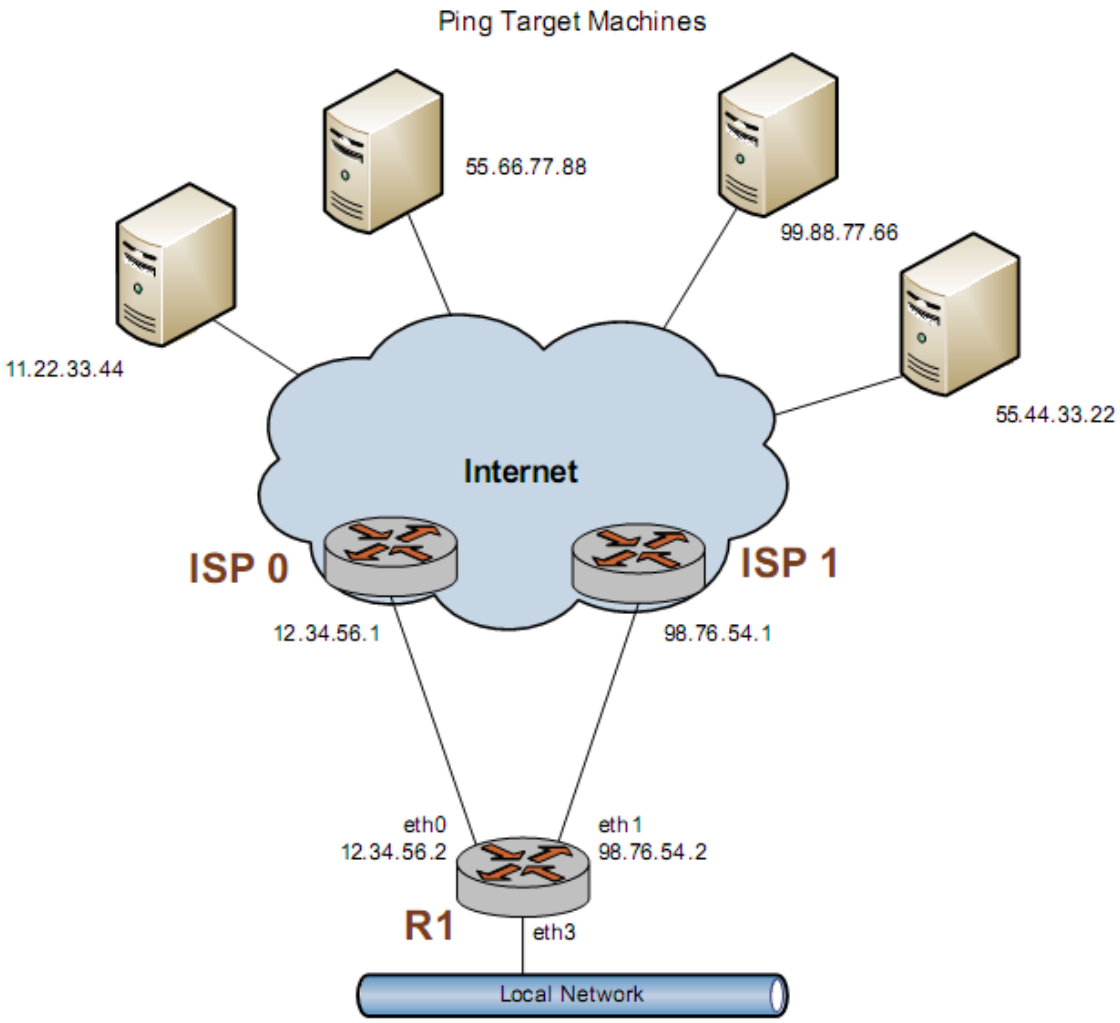
Ví dụ hệ thống mạng hiện có 2 đường truyền và 1 đường có chỉ số weight là 1, đường còn lại là 2. Thì đường có weight cao hơn sẽ có lượng dữ liệu truyền là 67%.

**Load Balancing Rules**

Khi xây dựng cơ chế load balancing trên hệ thống vyatta, các thiết lập trên các interface, và các thông số weight đặt ra cho mỗi interface, đó gọi là load balancing rule. Khi một luồng dữ liệu đi đến hệ thống thì nó sẽ kiểm tra thông tin luồng dữ liệu này có trùng khớp với rule được đề ra hay không. Nếu trùng với các thông số đưa ra thì luồng dữ liệu sẽ được xử lí. Nếu không khớp thì hệ thống sẽ đưa thông tin của dữ liệu xuống rule tiếp theo để xử lí. Nếu đến cuối cùng vẫn không có rule nào trùng với thông tin luồng dữ liệu thì nó sẽ dựa theo bảng routing table trong hệ thống để quyết định.

Cần chú ý là trong Vyatta, số thứ rule sẽ không thể thay đổi khi cấu hình. Do đó khi cấu hình người quản trị cần chú ý đặt các số của rule có một khoảng cách nhất định, như là 5,10,15… để có thể thêm các rule vào.

**Health Checking**




Trong hệ thống cân bằng tải, các interface phải luôn ở trạng thái là một active member. Trạng thái của các interface sẽ được giám sát bằng việc các gói tin ICMP echo request trong 1 khoảng thời gian nhất định tới các địa chỉ ở xa (ví dụ như trong hình là địa chỉ: 11.22.33.44, 55.66.77.88…). Nếu nhận được gói ICMP echo reply từ các địa chỉ từ xa thì sẽ cho hệ thống biết rằng interface này đang có thể truyền và nhận được các gói tin từ internet. Nếu interface đó không ổn định trong việc kiểm tra trạng thái thì sẽ bị loại bỏ khỏi danh sách các interface được truyền dữ liệu.

Khi thiết lập cơ chế cân bằng tải thì trên các interface phải được cấu hình luôn các tiêu chuẩn để đánh giá trạng thái của interface, bao gồm số lần kiểm tra trạng thái không thành công (không nhận được gói tin echo reply từ mạng xa)

## 5.3 RAID 1

Raid là công nghệ sử dụng một hay hay nhiều ổ cứng để giúp làm tăng tốc độ truy suất dữ liệu, tăng dung lượng lưu trữ, và đặc biệt là làm tăng khả năng chịu lỗi của hệ thống, tránh việc bị mất dữ liệu khi có sự cố về ổ cứng xảy ra. Hiện nay công nghệ Raid có rất nhiều dạng như Raid0, Raid1… Vyatta chỉ hỗ trợ Raid 1 cho hệ thống của mình.

Raid 1 cần ít nhất phải có 2 ổ cứng trở lên để cấu hình. Khi sử dụng Raid 1, các ổ cứng đều sẽ có dữ liệu giống nhau. Khi dữ liệu được ghi vào ổ cứng, các sector của ổ cứng này sẽ được duplicate đến ổ cứng khác. Nếu trong quá trình sử dụng, 1 trong những ổ cứng gặp sự cố và không thể hoạt động được thì dữ liệu sẽ vẫn được bảo toàn bởi các ổ còn lại.

Hệ thống Vyatta chỉ hỗ trợ công nghệ Raid theo phần mềm và chỉ hỗ trợ cho 2 ổ đĩa cứng. Tính năng khi sử dụng công nghệ Raid trên hệ thống Vyatta là:

- Khi có một sự cố xảy ra, hệ thống sẽ gửi thông báo tới người quản trị
- Khi có sự cố về ổ đĩa, hệ thống vẫn hoạt động tiếp tục
- Hệ thống vẫn có thể khỏi động bình thường nếu có ổ đĩa bị trục trặc
- Có thể giám sát quá trình sao chép dữ liệu sau khi có ổ cứng mới thêm vào.

Các ổ cứng trong hệ thống khi cấu hình Raid sẽ có những trạng thái khác nhau khi kết giao mối quan hệ

- Active: đây là trạng thái hoạt động bình thường của các ổ cứng, nếu hệ thống xảy ra sự cố thì hệ thống đòi hỏi người quản trị phải khởi động lại để thay đổi thiết bị ổ cứng bị hỏng. Khi vừa khởi động (nếu đã thay thế ổ cứng hỏng), hệ thống sẽ thực hiện đồng bộ dữ liệu lại giữa các ổ cứng
- Clean: sau khi quá trình chép dữ liệu hoàn tất thì hệ thống sẽ ở trạng thái clean

- Degraded: trạng thái này chỉ xảy ra nếu hệ thống bị lỗi, do Vyatta chỉ hỗ trợ raid 1 với 2 ổ cứng, nên tình trạng này xảy ra khi chỉ còn 1 ổ cứng dùng được
- Recovering: khi người quản trị đưa ổ cứng mới khác vào thì sẽ tiến hành sao chép dữ liệu từ thành viên còn lại. Ổ cứng mới thêm vào sẽ chưa thể dùng được nếu quá trình này chưa hoàn tất. trạng thái này chỉ xảy ra sau khi trải qua trạng thái Degraded
- Resyncing: đây là tình trạng đồng bộ giữa 2 ổ cứng. Do khi mới thêm vào, ổ cứng mới cần thiết lập lại các mối liên hệ kết giao với ổ cứng còn lại. Quá trình này sẽ không diễn ra đồng thời với trạng thái degraded và recovering.

Ví dụ về trạng thái của các ổ đĩa khi dùng Raid

```
State:    clean
Number    Major  Minor  RaidDevice    State
0         8      2      0             active sync   /dev/sda2
1         8      18     1             active sync   /dev/sdb2
```

Khi các ổ đĩa ở trạng thái bình thường thì các ổ đĩa sẽ có trạng thái là active và tình trạng hệ thống là clean

```
State:    clean, degraded
Number    Major  Minor  RaidDevice    State
0         0      0      0             removed       /dev/sda2
1         8      18     1             active sync   /dev/sdb2
```

Nếu có 1 ổ cứng trục trặc thì ổ cứng sẽ sẽ có tình trạng là remove và hệ thống sẽ xuất hiện tình trạng degraded

```
State:    clean, degraded, recovering
Rebuild status: 3% complete

Number    Major  Minor  RaidDevice    State
2         8      18     0             spare rebuilding/dev/sda2
1         8      18     1             active sync   /dev/sdb2
```

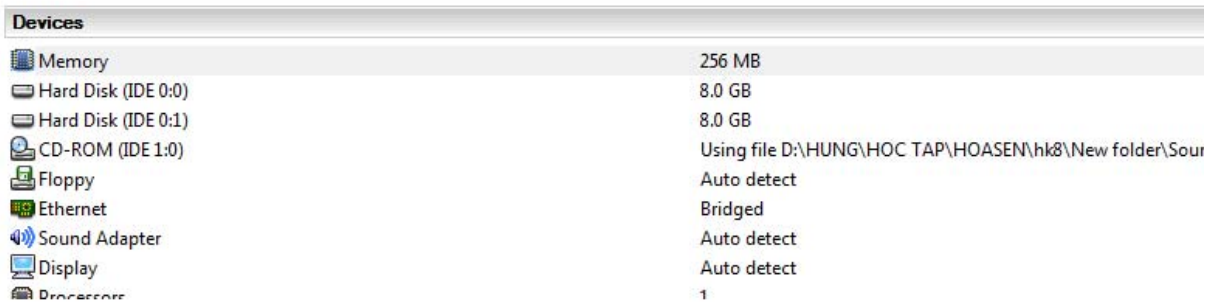
Sau khi thêm ổ cứng mới vào, bắt đầu tiến trình recovering, tình trạng của ổ cứng mới thêm vào là "spare rebuilding". Trạng thái này sẽ không thay đổi sao khi quá trình sao chép dữ liệu từ ổ cứng cũ sang mới hoàn tất.

```
State:    active, resyncing
Rebuild status: 3% complete

Number    Major  Minor  RaidDevice    State
2         8      2      0             active sync   /dev/sda2
1         8      18     1             active sync   /dev/sdb2
```

Sau khi sao chép dữ liệu hoàn tất, các ổ đĩa sẽ trở về trạng thái active và bắt đầu thực hiên reysncing. Sau đó là hoàn tất và hệ thống có thể hoạt động bình thường.

Điểm hay của Vyatta là dù chỉ hoạt động với những tính năng của một thiết bị Router, nhưng nó cũng hỗ trợ nên tính năng Raid 1. Đây là điểm mà Cisco không có. Có thể nói đây là một lợi thế khi sử dụng Vyatta. Tuy nhiên chỉ hỗ trợ công nghệ Raid ở mức đơn giản, chỉ hỗ trợ 2 ổ cứng nên không thể dùng để lưu trữ dữ liệu nhiều được.

**Ví dụ về RAID1**




Ban đầu, 2 ổ cứng sẽ được sử dùng trên cùng 1 hệ thống

```
vyatta@vyatta:~$ install-system
Welcome to the Vyatta install program.  This script
will walk you through the process of installing the
Vyatta image to a local hard drive.

Would you like to continue? (Yes/No) [Yes]: yes
Probing drives: OK
Looking for pre-existing RAID groups...none found.

You have two disk drives:
        sda     8590 MB
        sdb     8590 MB
Would you like to configure RAID-1 mirroring on them? (Yes/No) [Yes]:This proces
s will erase all data on both drives.
Are you sure you want to do this? (Yes/No) [No]: _
```

Khi vừa khởi động hệ thống, dùng cấu trúc lệnh install-system để thực hiện cấu hình RAID1

```
Erasing any previous RAID metadata that may exist on /dev/sda2
mdadm: Unrecognised md component device - /dev/sda2
Erasing any previous RAID metadata that may exist on /dev/sdb2
mdadm: Unrecognised md component device - /dev/sdb2
Creating RAID-1 group on partitions: /dev/sda2 /dev/sdb2
mdadm: array /dev/md0 started.
RAID-1 group created successfully:
        md0 : active (auto-read-only) raid1 sdb2[1] sda2[0]
              8267456 blocks [2/2] [UU]
                resync=PENDING
Creating filesystem on /dev/md0: OK
Mounting /dev/md0
Copying system files to /dev/md0:
 24% [=============>                                        ]
```

Quá trình thực hiện copy dữ liệu sẽ diễn ra

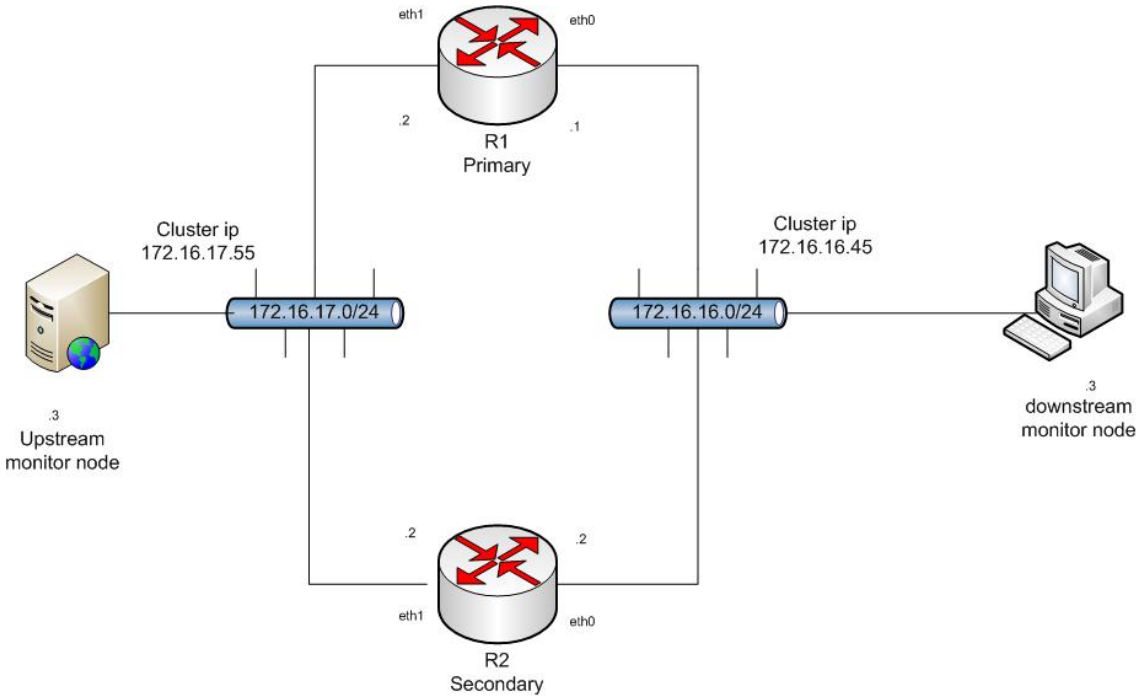
## 5.4 Cluster

Clustering là một kiến trúc nhằm đảm bảo nâng cao khả năng sẵn sàng cho các hệ thống mạng máy tính. Cluster là một hệ thống bao gồm nhiều máy chủ được kết nối với nhau theo dạng song song hay phân tán và được sử dụng như một tài nguyên thống nhất. Nếu một máy chủ ngừng hoạt động do bị sự cố hoặc để nâng cấp, bảo trì, thì toàn bộ công việc mà máy chủ này đảm nhận sẽ được tự động chuyển sang cho một máy chủ khác (trong cùng một cluster) mà không làm cho hoạt động của hệ thống bị ngắt hay gián đoạn. Quá trình này gọi là "fail-over"; và việc phục hồi tài nguyên của một máy chủ trong hệ thống (cluster) được gọi là "fail-back".

Việc thiết kế và lắp đặt các cluster cần thoả mãn các yêu cầu sau:

- Yêu cầu về tính sẵn sàng cao (High availability). Các tài nguyên mạng phải luôn sẵn sàng trong khả năng cao nhất để cung cấp và phục vụ các người dùng cuối và giảm thiểu sự ngưng hoạt động hệ thống ngoài ý muốn.
- Yêu cầu về độ tin cậy cao (reliability). Độ tin cậy cao của cluster được hiểu là khả năng giảm thiểu tần số xảy ra các sự cố, và nâng cao khả năng chịu đựng sai sót của hệ thống.
- Yêu cầu về khả năng mở rộng được (scalability). Hệ thống phải có khả năng dễ dàng cho việc nâng cấp, mở rộng trong tương lai. Việc nâng cấp mở rộng bao hàm cả việc thêm các thiết bị, máy tính vào hệ thống để nâng cao chất lượng dịch vụ, cũng như việc thêm số lượng người dùng, thêm ứng dụng, dịch vụ và thêm các tài nguyên mạng khác.

Trên hệ thống Vyatta, Clustering có thể được sử dụng cho failover để cung cấp khả năng High Availability. Cluster sẽ theo dõi những node đang cung cấp những dịch vụ được chỉ định. Nếu hệ thống phát hiện node fail, hoặc liên kết mạng fail, hệ thống sẽ chuyển cả dịch vụ và địa chỉ IP đến node Backup




**Các thành phần của một Cluster**

Primary Cluster node: Đây là một router ở trạng thái active trong cluster. Nó là một router cung cấp những dịch vụ

Secondary Cluster node:Đây là một Backup Router trong cluster.Nếu Primary Cluster node trong cluster bị fail thì Secondary Cluster node sẽ đảm nhận vai trò của Primary Cluster node

Monitor nodes: Primary va Secondary node sẽ kiểm tra kết nối mạng của nó bằng cách "ping" các thiết bị upstream và downstream trên network. Những thiết bị như thế gọi là monitor nodes. Bản thân monitor node không tham gia vào hệ thống clustering, một điều kiện tất yếu cho các monitor node là phải trả lời lại các gói tin ICMP Echo Request.

**Một cluster cung cấp failover gồm 2 loại tài nguyên:**

Cluster Ip address: là địa chị Ip được chia sẽ giữa những node trong một cluster. Ban đầu ip này được gán cho Primary node. Nếu primary node bị fail, hệ thống cluster sẽ chuyển cluster ip đến secondary node. Lưu ý: Cluster ip address được xem như một

service.

Services: là những dịch vụ cùng với cluster ip sẽ được cluster theo dõi và sẽ được di chuyển qua secondary node nếu primary node fail

Cluster node, cluster ip address, services phải thuộc cùng một group, hiện tại Vyatta chỉ hổ trợ một group

**Phát Hiện quá trình failure trong cluster**

- Node Failure: Primary va Secondary trong cluster trao đổi với nhau thông điệp heartbeat thông qua các interface. Nếu một node trong cluster không nhận được thông điệp heartbeat từ node khác, thì nó xem như node đó không còn tồn tại. Nếu secondary node xác định primary node không còn hoạt động, thì secondary node sẽ tiến hành quá trình failover và lấy lại các tài nguyên của cluster

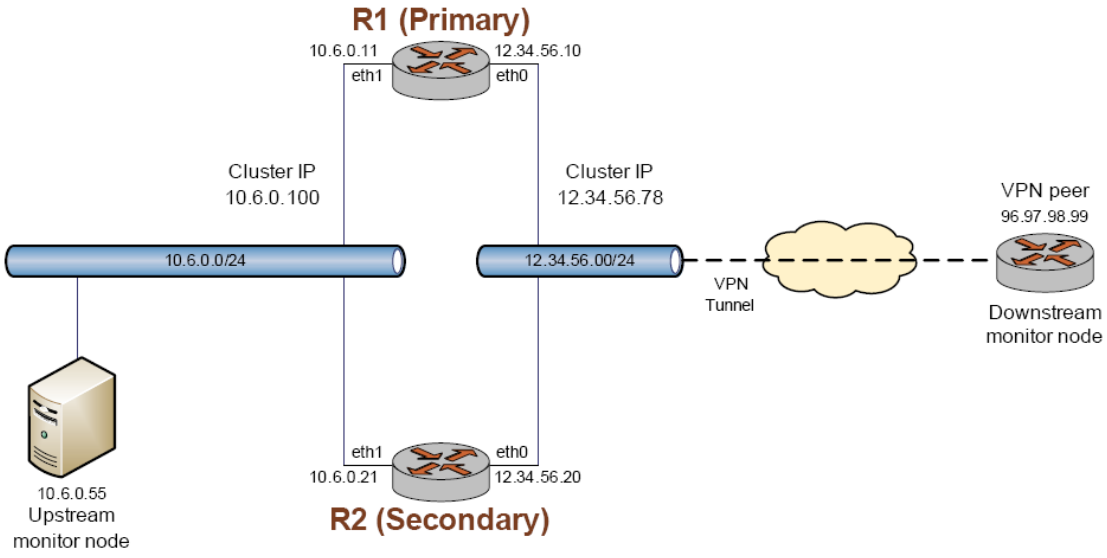
- Connectivity Failure: Primary và secondary node sẽ theo dõi kết nối mạng của nó bằng cách ping những monitor node được chỉ định. Quá Trình Failover thì được kích hoạt khi kết nối bị mất

Nếu trên router ta cấu hình auto-failback khi primary node fail, sau đó phục hồi trở lại, lúc này primary node tự động lấy lại các service và trở lại primary node. Nếu không cấu hình auto-failback cho dù primary node phục hồi trở lại thì nó cũng không lấy lại được các service. Mặc định auto-failback  không được cấu hình

**Kỹ Thuật Heartbeat trong Clustering**

Ngay sau khi cấu hình Vyatta được commit, node bắt đầu gửi thông điệp heatbeat, mặc định kỹ thuật  heatbeat chờ 120s phản hồi từ các node khác. Nếu thông điệp heatbeat nhận được trong khoảng thời gian chờ này thì các service trong cluster sẽ được khởi động trên primary node, và secondary node sẽ trở thành một active standby router.Nếu thông điệp heartbeat không nhận được trong khoảng thời gian chờ này thì node gửi thông điệp sẽ điều khiển các server trong cluster

Sau đây là một ví dụ về một cluster




Router R1 , R2 là cluster node, R1 là primary node, R2 là secondary node

Cluster ip address là 12.34.56.78 và 10.6.0.100, 2 ip này được xem là service. Và kết nối VPN thông qua ip sec cũng được xem là một service

Host 10.6.0.55 là monitor node upstream dùng với mục đích kiểm tra tình trạng mạng cho cluster node R1 và R2

VPN Peer là monitor node downstream dùng với mục đích kiểm tra tình trạng mạng

## 6. Security

### 6.1 Web filtering

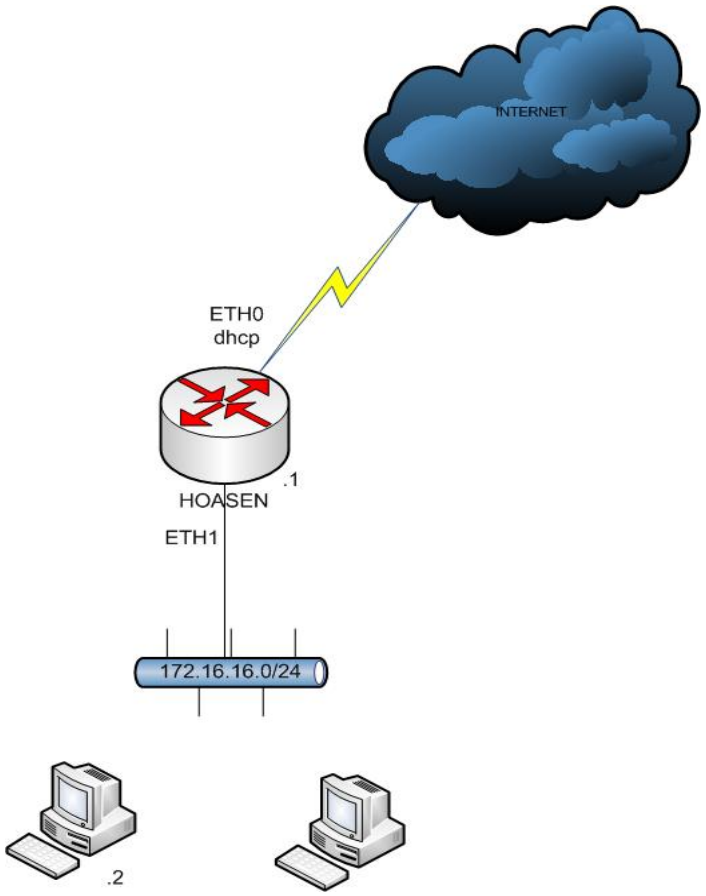
Vyatta có thể được cấu hình như là một web proxy server cho việc caching và lọc web. Đây là một trong những tính năng quan trọng trong việc quản lí truy cập các trang web có nội dụng không lành mạnh, trang web chứa mã độc (virus, Trojan…). Tuy nhiên không như những phần mềm hay phần cứng chuyên dụng khác, Vyatta chỉ hỗ trợ cho việc lọc web ở mức độ cơ bản. Để có thể nâng cao khả năng lọc web ở mức cao hơn, người quản trị có thể sử dùng bộ Vyatta Plus. Database của Vyatta Plus sẽ

lớn hơn nhiều nên đòi hỏi dung lượng ổ cứng khi cài đặt tối thiểu là 2Gb.

Với bản Vyatta Core, các chế độ lọc web tương đối đơn giản và cơ bản, các chế độ thực hiện là:

- Local-ok
- Local-block
- Allow-ipaddr-url
- Block-category
- Allow-categpry
- Local-block-keyword
- Default-action

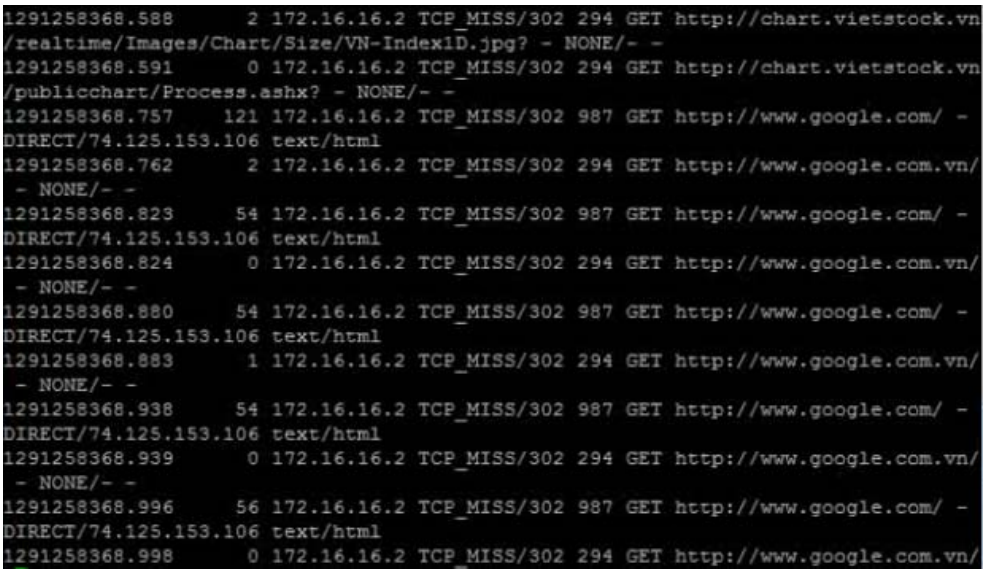
**Ví dụ về WebFiltering**




Ở mô hình này, sẽ có 1 router Vyatta đứng ra làm vai trò của một WebFiltering. Bất cứ yêu cầu truy cập mạng nào từ client đều sẽ bị kiểm tra xem có hợp lệ hay không. Bất cứ yêu cầu truy cập nào không đúng sẽ bị block

```
configure
set system host-name HOASEN

set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1

set service nat rule 1 source address 172.16.16.0/24
set service nat rule 1 outbound-interface eth0
set service nat rule 1 type masquerade
commit


set service webproxy listen-address 172.16.16.1
set service webproxy url-filtering squidguard local-block vnexpress.net
set service webproxy url-filtering squidguard local-block facebook.com
set service webproxy url-filtering squidguard local-block-keyword ".vn"
```

Hệ thống sẽ thực hiện việc chặn các trang facebook.com và vnexpress.net. Bất cứ trang nào có keyword nào ".vn" đều sẽ bị chặn




Tất cả mọi traffic đều sẽ được ghi nhận lại quá trình truy cập

## 6.2 Firewall

Trong một hệ thống mạng doanh nghiệp, việc thiết lập các cơ chế bảo mật là một bước không thể thiếu trong quá trình triển khai xây dựng. Bởi đó sẽ là yếu tố quan trọng sống còn của một hệ thống khi triển khai. Nếu người quản trị thiết lập một chính sách bảo mật không tốt thì nguy cơ tiềm ẩn cho hệ thống mạng là rất cao. Còn nếu như một chính sách bảo mật cao và chặt được đưa ra sẽ giúp tránh được các nguy cơ tiềm ẩn khác.

Cũng như các Router của hãng khác, đặc biệt là Cisco, Router Vyatta cung cấp một số tính năng của một basic firewall trên phiên bản Vyatta Core và Vyatta Subscription Edition.

**Firewall Rule**

Rules là những chính sách do người quản trị đưa ra sao cho phù hợp với hệ thống mạng hiện hành. Khi hoạt động, bất kì luồng dữ liệu nào khi đi ngang qua hệ thống firewall đều sẽ được kiểm tra xem có thông tin trùng với rule đã đưa ra hay không. Nếu trùng thì firewall sẽ lập tức thực thi lệnh dựa trên rule đã đề ra.

Nội dung của một rule để kiểm tra thông tin luồng dữ liệu khi đi qua firewall là: địa

chỉ nguồn, địa chỉ đích của gói tin, cổng kết nối của nguồn gửi, cổng kết nối của nguồn nhận, giao thức sử dụng.

Các hành động mà rule sẽ thực hiện nếu thông tin của dữ liệu truyền đi trùng với chính sách đã đề ra:

- Accept: dữ liệu sẽ được phép đi qua firewall
- Drop: dữ liệu khi đến router sẽ bị chặn lại và sẽ không phản hồi thông tin cho người gửi
- Reject: dữ liệu sẽ bị chặn lại và báo cho người gửi biết bằng TCP reset
- Inspect: dữ liệu sẽ được kiểm tra với hệ thống IPS

Những rule sẽ được thực thi theo thứ tự rule number. Tức là sẽ được xét theo thứ tự từ trên xuống dưới, nếu thông tin gói dữ liệu trùng với rule thì sẽ được thực thi, còn nếu không trùng thì sẽ được đẩy xuống các rule tiếp theo cho đến hết. Các rule sau khi được đặt ra và cấu hình bởi người quản trị mạng, hệ thống Vyatta sẽ ngầm mặc định có 1 rule reject all ở cuối tất cả các rule. Rule này sẽ thực hiện loại bỏ hết tất cả các luồng dữ liệu mà không trùng với bất cứ rule nào ở bên trên. Người quản trị vẫn có thể thay đổi mặc định này nếu muốn.

**Kiểm tra hướng đi của luồng dữ liệu**

Các rule sau khi cấu hình hoàn tất vẫn chưa thể hoạt động được. Bởi hệ thống firewall cần phải xác định chính xác các rule đó sẽ được áp đặt lên interface nào và theo chiều nào. Khi dữ liệu đi ngang qua firewall, hệ thống sẽ xác định chiều của luồng dữ liệu là như thế nào và bắt đầu thực thi các rule đã cấu hình. Cũng như các basic firewall khác, firewall của Vyatta định nghĩa rằng khi dữ liệu đi qua firewall, sẽ có 3 hướng.

- In: nếu firewall được thiết lập việc kiểm tra theo chiều in trên interface thì chỉ có những luồng dữ liệu đi vào interface đó mới được kiểm tra dựa theo các rule đã áp đặt trước đó.

- Out: nếu firewall được thiết lập việc kiểm tra theo chiều out trên interface thì chỉ có những luồng dữ liệu đi ra interface đó mới được kiểm tra dựa theo các rule đã áp đặt trước đó. Những gói tin này có thể là gói tin từ một nguồn gửi nào đó hoặc từ chính router gửi ra

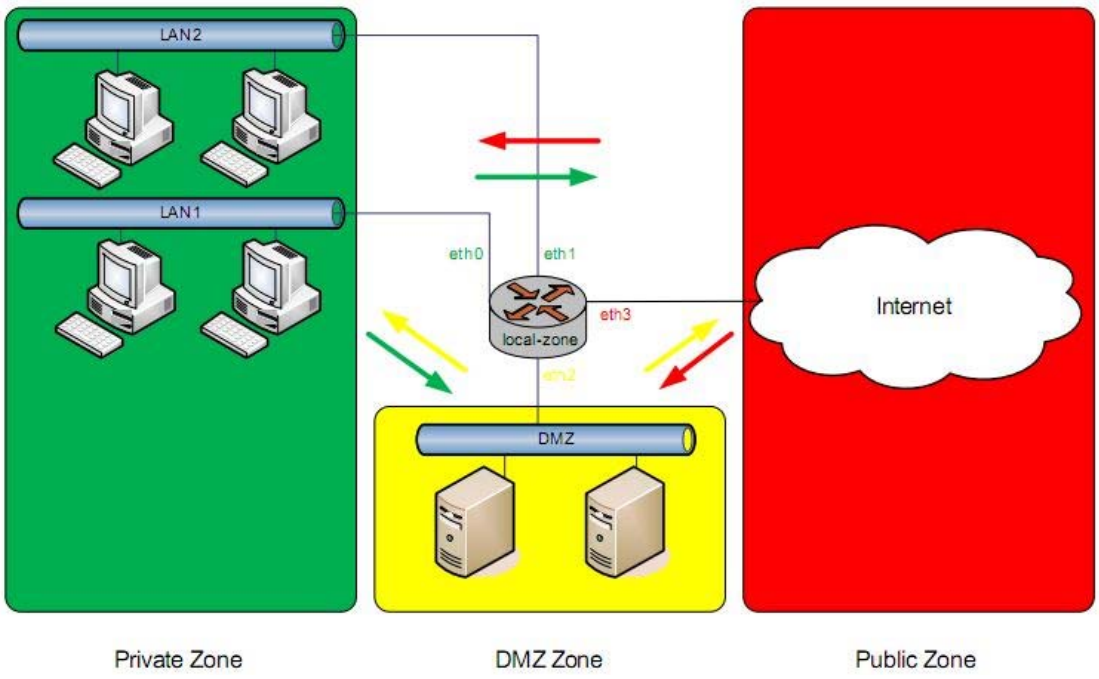
- Local: nếu firewall được thiết lập việc kiểm tra theo local trên interface thì chỉ có những luồng dữ liệu đi đến router đó mới được kiểm tra dựa theo các rule đã áp đặt trước đó.

Như vậy hệ thống Vyatta định nghĩa ra 3 hướng đi của dữ liệu khi áp đặt các rule lên các interface.

**Zone-based firewall**

Ở các dạng firewall trước đây, các rule của firewall sẽ được thiết lập trên mỗi interface (cơ bản là để lọc gói tin trên các interface đó). Như vậy nếu firewall có càng nhiều interface khác nhau thì đòi hỏi người quản trị phải áp đặt các rule lên tất cả các interface đó, như vậy khiến cho việc quản lí rất khó khăn, phức tap và rất mất thời gian. Nhất là khi firewall có nhu cầu phải đưa thêm 1 interface vào nữa thì sẽ rất khó khăn cho việc thiết lập các chính sách.

Để khắc phục tình trạng này, Vyatta đã đưa thêm tính năng zone-based vào hệ thống firewall của mình. Tính năng này giúp cho người quản trị đỡ mất thời gian hơn và dễ dàng hơn trong việc áp chính sách bảo mật lên từng interface của router firewall. Với tính năng này, các rule sẽ không còn được thiết lập trên từng interface nữa. Mà người quản trị sẽ thiết lập các rule cho các zone khác nhau. Sau đó chỉ cần lên các interface và đưa interface đó vào zone nào thích hợp, ngay lập tức các rule trên các zone đã cấu hình trước đó sẽ áp vào các interface.




Hình: ví dụ minh họa về zone-based

- Có 3 zone được tạo ra trong hệ thống mạng ở hình bên trên: Private zone (eth0 và eth1), DMZ zone (eth2), Public zone (eth3).

- Eth0 và eth1 cùng thuộc Private zone, vì vậy router firewall sẽ không thực hiện lọc gói tin khi dữ liệu trao đổi của 2 interface này với nhau.

- Ngoài ra còn 1 zone khác trong hệ thống nữa, đó là local zone. Zone này chính là router firwall. Mặc định rằng khi các dữ liệu đi qua zone này đều được cho phép. Tuy nhiên nếu muốn, người quản trị vẫn có thể thay đổi mặc định này.

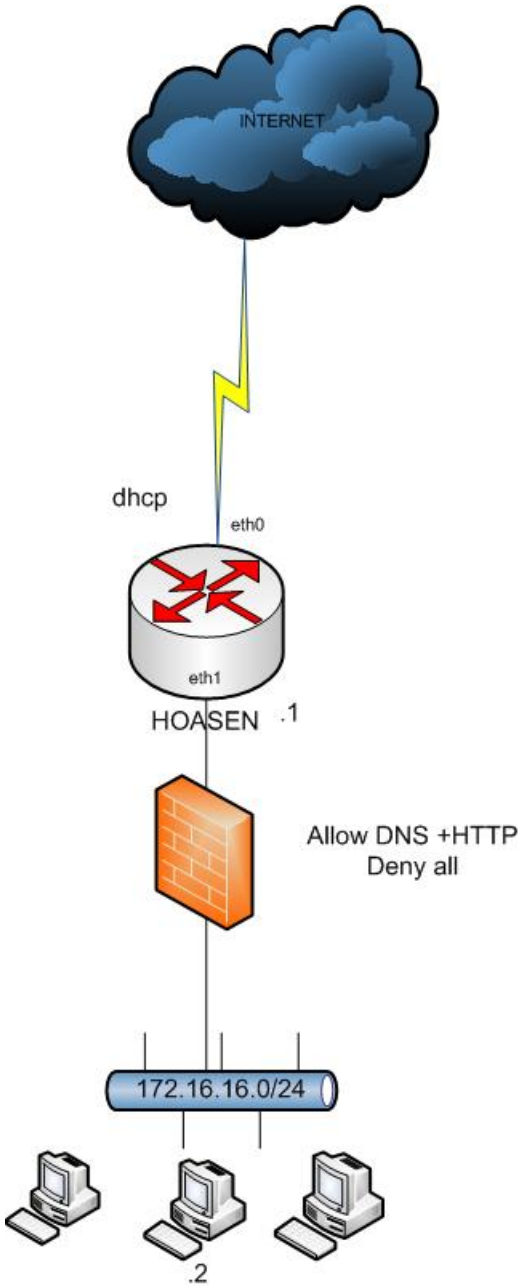
Các chú ý về zone-based firewall

- Mỗi một interface chỉ có thể liên kết được với 1 zone

- Khi các interface được cấu hình tham gia vào một zone nào thì sẽ không thể áp đặt trực tiếp các rule lên các interface này nữa. Các rule sẽ cấu hình trên từng zone, khi interface đó tham gia vào zone nào thì các rule của zone đó sẽ được áp tự động lên interface.

- Những interface không thuộc bất cứ zone nào, thì các rule được cấu hình trên interface sẽ được áp dụng
- Những luồng dữ liệu nào mà không trùng với bất cứ chính sách nào của zone sẽ bị chặn ngay lập tức
- Các chính sách trong zone-based firewall sẽ được áp dụng theo từng cặp đôi. Cặp đôi đó được định nghĩa theo nguồn gửi (from zone) và nguồn nhận (to zone)
    - From Private to DMZ
    - From Public to DMZ
    - From Private to Public
    - From DMZ to Public
    - From Public to Private
    - From DMZ to Private

**Ví dụ về firewall**




Đây mà một mô hình mạng dùng router Vyatta để làm một basic firewall.

Người quản trị chỉ muốn cho phép client truy cập ra ngoài internet bằng HTTP và DNS. Tất cả mọi truy cập khác đều sẽ bị chặn lại.

```
configure
set system host-name HOASEN
set system domain-name hoasen.edu.vn

set service ssh protocol-version all
set interfaces ethernet eth0 address dhcp
set interfaces ethernet eth1 address 172.16.16.1/24

set service nat rule 1
set service nat rule 1 type masquerade
set service nat rule 1 outbound-interface eth0
set service nat rule 1 protocol all
set service nat rule 1 source address 172.16.16.0/24


set firewall name ALLOWDNSHTTP rule 1
set firewall name ALLOWDNSHTTP rule 1 action accept
set firewall name ALLOWDNSHTTP rule 1 state established enable
set firewall name ALLOWDNSHTTP rule 1 state related enable

set firewall name ALLOWDNSHTTP rule 10
set firewall name ALLOWDNSHTTP rule 10 action accept
set firewall name ALLOWDNSHTTP rule 10 source address 172.16.16.0/24
set firewall name ALLOWDNSHTTP rule 10 protocol udp
set firewall name ALLOWDNSHTTP rule 10 destination port 53

set firewall name ALLOWDNSHTTP rule 20
set firewall name ALLOWDNSHTTP rule 20 action accept
set firewall name ALLOWDNSHTTP rule 20 source address 172.16.16.0/24
set firewall name ALLOWDNSHTTP rule 20 protocol tcp
set firewall name ALLOWDNSHTTP rule 20 destination port 80

set interfaces ethernet eth1 firewall in name ALLOWDNSHTTP
```

Sau khi các rule được cấu hình hoàn tất, dùng lệnh show firewall để kiểm tra nội dung các rules đã tạo trước đó

```
vyatta@vyatta:~$ show firewall
------------------------------------------------------------------------------
--------
IPv4 Firewall "ALLOWDNSHTTP":

 Active on (eth1,IN)

(State Codes: E - Established, I - Invalid, N - New, R - Related)

rule  action  source           destination        proto     state
----  ------  ------           -----------        -----     -----
10    ACCEPT  172.16.16.0/24   0.0.0.0/0          udp       any
                               dst ports: 53
20    ACCEPT  172.16.16.0/24   0.0.0.0/0          tcp       any
                               dst ports: 80
10000 DROP    0.0.0.0/0        0.0.0.0/0          all       any
```

Ứng với các rules, client có thể truy vấn DNS bất cứ trang web nào. Khi thực hiện ping google.com sẽ bị chặn ngay lập tức

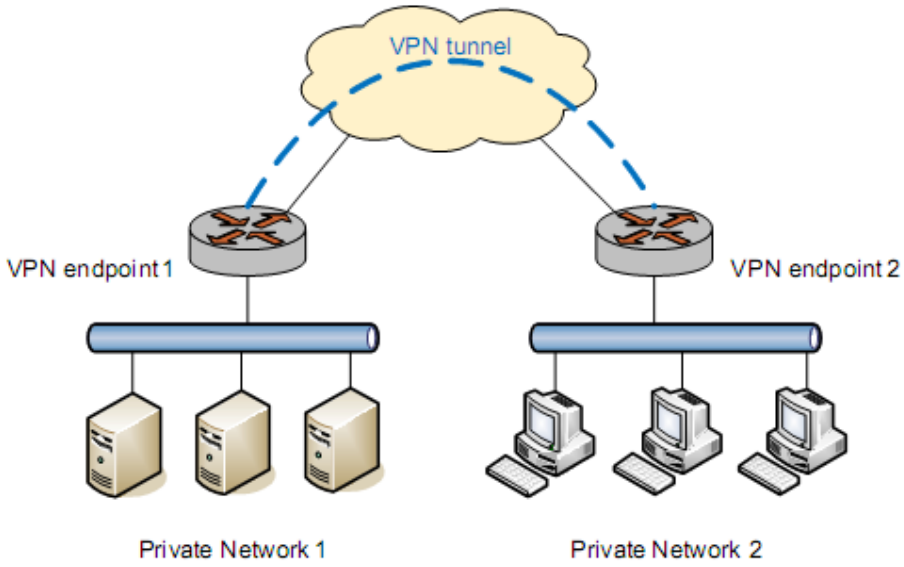
```
> vnexpress.net
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    vnexpress.net
Addresses:  210.245.31.22, 210.245.86.184, 118.69.251.6, 210.245.86.193
          210.245.86.175, 210.245.31.21, 118.69.251.4, 210.245.86.192

> ^C
C:\Documents and Settings\Administrator>ping google.com

Pinging google.com [74.125.71.147] with 32 bytes of data:

Request timed out.
```

### 6.3 VPN

VPN (Virtual private network) là công nghệ xây dựng hệ thống mạng riêng ảo thông qua môi trường internet để kết nối từ xa đến một mạng

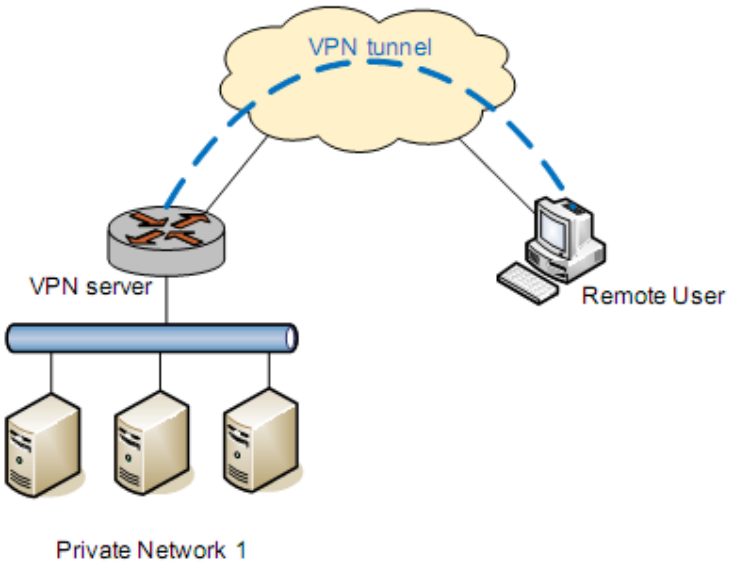
Hệ thống Vyatta hỗ trợ hai dạng VPN trên các phiên bản của mình

- Site to site VPN: cho phép kết nối hai hay nhiều mạng riêng lẻ trong mạng WAN lại với nhau thành một mạng. Site to site sẽ dùng cơ chế tunnel để truyền dữ liệu




Hình: ví dụ về site to site VPN dùng tunnel

- Remote access VPN: đây là kết nối giữa người dùng đến một mạng trong môi trường mạng WAN để người dùng có thể sử dụng tài nguyên bên trong của hệ thống mạng. Một VPN tunnel sẽ được thiết lập giữa user ở xa và VPN server.



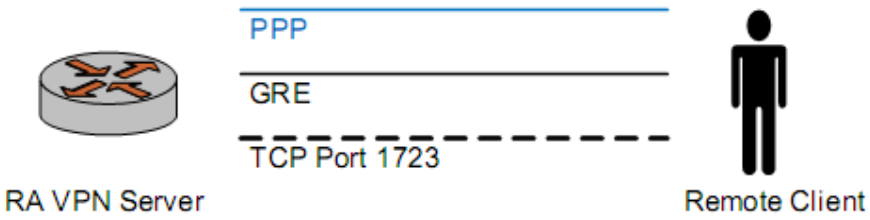

Hình: ví dụ về remote access VPN dùng VPN tunnel

Nhìn chung cả hai dạng kết nối VPN này tương đối giống nhau, đều tạo ra một VPN tunnel để kết nối giữa hai thiết bị đầu cuối. Điểm khác nhau giữa hai dạng là cách thức thiết lập tunnel.

**Các dạng mà hệ thống Vyatta hỗ trợ**

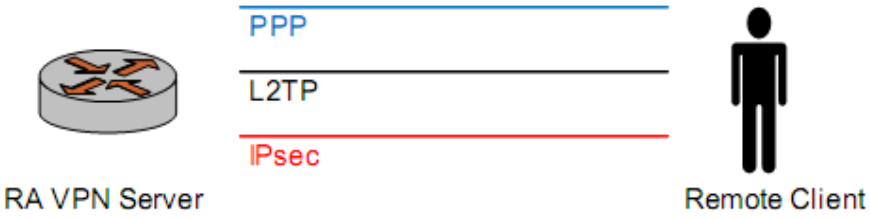
Site to site dùng IPSec

Remote access dùng PPTP



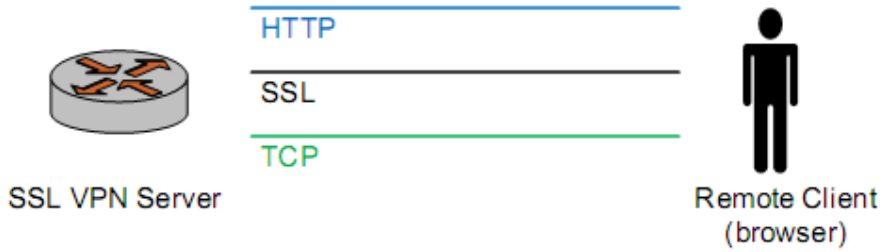

- PPTP client thiết lập một kênh kết nối TCP tới server dùng port 1723
- Thông qua kết nối ở trên, PPTP client và server thiết lập một GRE (Generic routing encapsulation) tunnel
- Sau khi GRE tunnel được thiết lập, một PPP (point to point) sessiong sẽ được thiết lập. Các gói tin PPP sẽ được đóng gói và gửi đi bên trong GRE tunnel

Remote access dùng L2TP và IPSec (tính năng này chỉ hỗ trợ trên phiên bản Vyatta Subcrisption Edition)




- Client từ xa sẽ thiết lập một IPSec tunnel với VPN server
- L2TP client và server sẽ thiết lập một L2TP tunnel ở bên trên IPSec tunnel
- Cuối cùng, PPP session được thiết lập ở trên L2TP tunnel. Các gói tin được đóng gói PPP sẽ truyền và nhận ở trong L2TP tunnel

Site to site và remote access dùng Open VPN

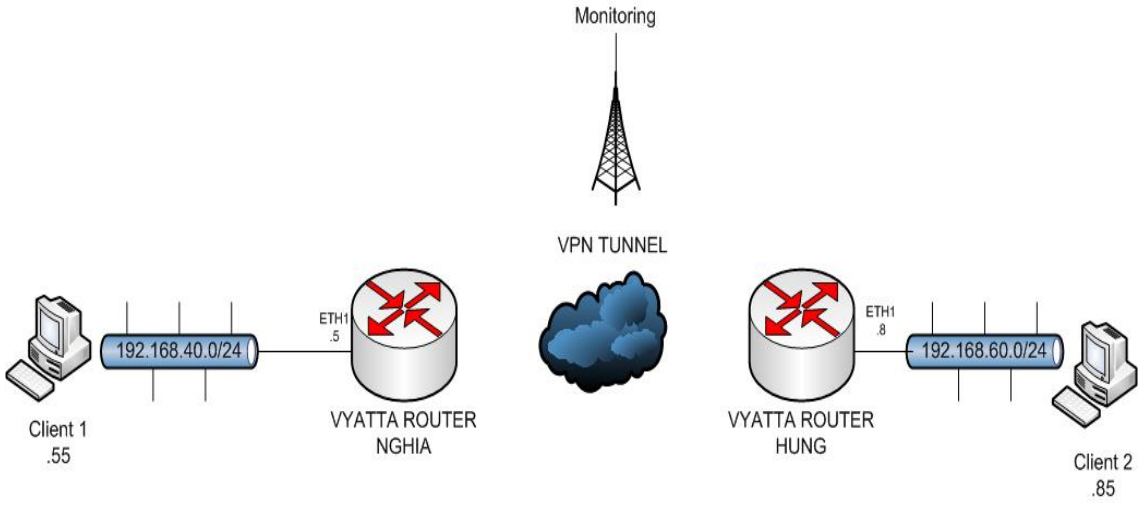



Open VPN là một phương pháp mã nguồn mỡ được sử dụng cho cả site to site và remote access VPN.

Trước tiên, remote user sẽ tạo một kết nối TCP đến server. Sau đó giao thức SSL sẽ chạy trên kết nối này. Cuối cùng là một session HTTP sẽ nằm bên trên session SSL. Session SSL cung cấp một tunnel bảo mật cho việc chứng thực của HTTP session. Cũng giống như là việc đăng nhập vào hệ thống web bảo mật của ngân hàng.

Sau khi đăng nhập thành công, trình duyệt sẽ đòi hỏi phải thực hiện download một đoạn code trên máy client để chạy trương trình (giống như là ActiveX)

**Ví dụ VPN site-to-site**



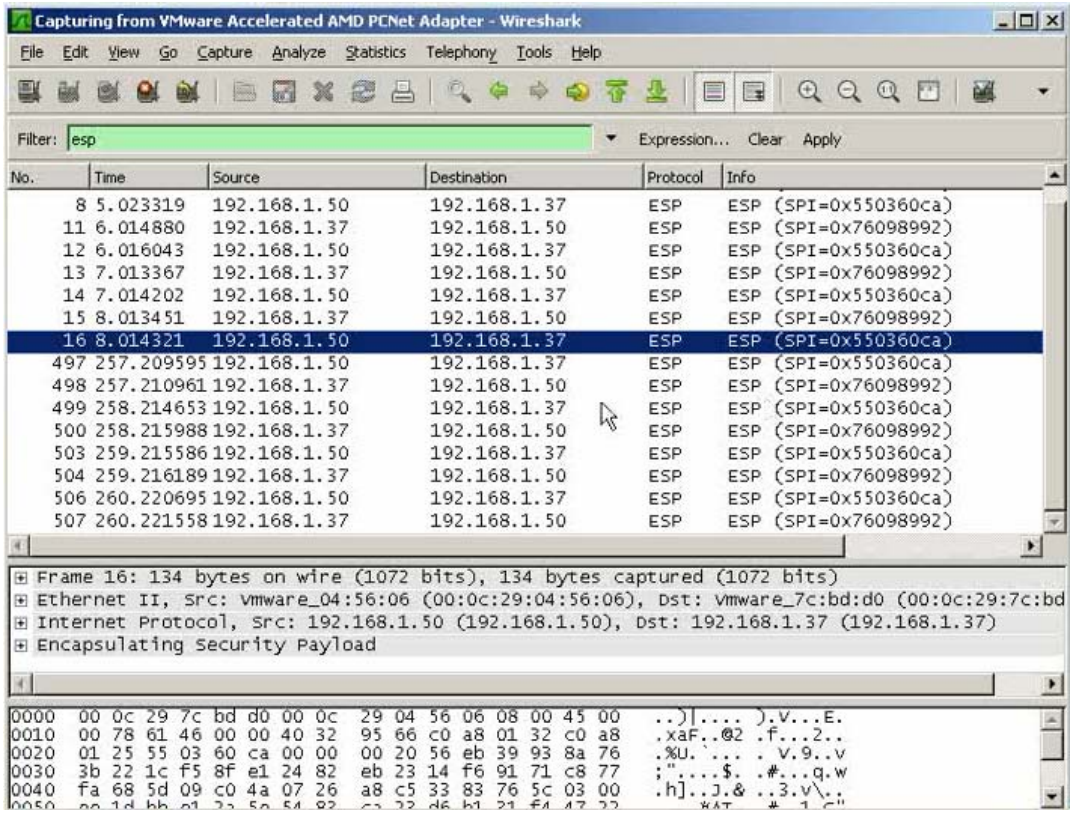
```
************************************************************
Configure EAST

************************************************************
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec ike-group IKE-1W proposal 1
set vpn ipsec ike-group IKE-1W proposal 1 encryption aes256
set vpn ipsec ike-group IKE-1W proposal 1 hash sha1
set vpn ipsec ike-group IKE-1W proposal 2 encryption aes128
set vpn ipsec ike-group IKE-1W proposal 2 hash sha1
set vpn ipsec ike-group IKE-1W lifetime 3600

set vpn ipsec esp-group ESP-1W proposal 1
set vpn ipsec esp-group ESP-1W proposal 1 encryption aes256
set vpn ipsec esp-group ESP-1W proposal 1 hash sha1
set vpn ipsec esp-group ESP-1W proposal 2 encryption 3des
set vpn ipsec esp-group ESP-1W proposal 2 hash md5
set vpn ipsec esp-group ESP-1W lifetime 1800
set vpn ipsec site-to-site peer 192.168.4.38 authentication mode pre-shared-secret
edit vpn ipsec site-to-site peer 192.168.4.38
set authentication pre-shared-secret test_key_1
set ike-group IKE-1W
set local-ip 192.168.4.37
set tunnel 1 local-subnet 192.168.40.0/24
set tunnel 1 remote-subnet 192.168.60.0/24
set tunnel 1 esp-group ESP-1W
top

************************************************************
Configure EAST
************************************************************
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec ike-group IKE-1E proposal 1
set vpn ipsec ike-group IKE-1E proposal 1 encryption aes256
set vpn ipsec ike-group IKE-1E proposal 1 hash sha1
set vpn ipsec ike-group IKE-1E proposal 2 encryption aes128
set vpn ipsec ike-group IKE-1E proposal 2 hash sha1
set vpn ipsec ike-group IKE-1E lifetime 3600

set vpn ipsec esp-group ESP-1E proposal 1
set vpn ipsec esp-group ESP-1E proposal 1 encryption aes256
set vpn ipsec esp-group ESP-1E proposal 1 hash sha1
set vpn ipsec esp-group ESP-1E proposal 2 encryption 3des
set vpn ipsec esp-group ESP-1E proposal 2 hash md5
set vpn ipsec esp-group ESP-1E lifetime 1800

set vpn ipsec site-to-site peer 192.168.4.37 authentication mode pre-shared-secret
edit vpn ipsec site-to-site peer 192.168.4.37
set authentication pre-shared-secret test_key_1
set ike-group IKE-1E
set local-ip 192.168.4.38
set tunnel 1 local-subnet 192.168.60.0/24
set tunnel 1 remote-subnet 192.168.40.0/24
set tunnel 1 esp-group ESP-1E
top
```

Sau khi cấu hình hoàn tất, để kiểm chứng các cấu hình, người quản trị có thể dùng lệnh “show vpn ipsec sa”, “show vpn ipsec status”

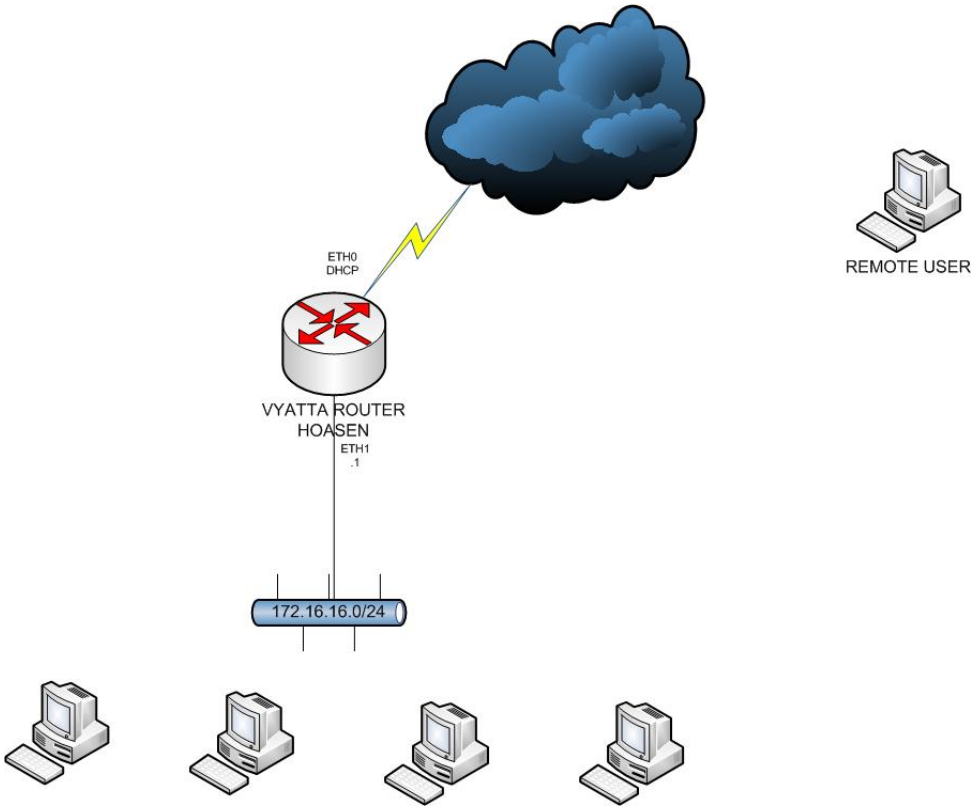
```
vyatta@vyatta:~$ show vpn ipsec sa
Peer            Tunnel# Dir SPI      Encrypt    Hash       NAT-T A-Time L-Time
-------         ------- --- ---      -------    ----       ----- ------ ------
192.168.1.37    1       in  4d726403 aes256     sha1       No    411    1800
192.168.1.37    1       out a6abc4b6 aes256     sha1       No    412    1800

vyatta@vyatta:~$ show vpn ipsec sa statistics
Peer            Dir SRC Network         DST Network         Bytes
-------         --- -----------         -----------         -----
192.168.1.37    in  192.168.60.0/24     192.168.40.0/24     0
192.168.1.37    out 192.168.40.0/24     192.168.60.0/24     0
```

```
vyatta@vyatta:~$ show vpn ipsec status
IPSec Process Running PID: 3987

1 Active IPsec Tunnels

IPsec Interfaces :
        eth0    (192.168.1.50)
```

Khi thực hiện site-to-site, dùng wireshark để kiểm tra thông tin trên đường truyền.



**Ví dụ VPN remote access**




Ở mô hình này, người quản trị mạng thực hiện cấu hình VPN remote access dùng PPTP

```
configure
set system host-name HOASEN
set system domain-name hoasen.edu.vn
set interface ethernet eth0 address dhcp
set interface ethernet eth1 address 172.16.16.1


set vpn pptp remote-access outside-address 192.168.1.25
set vpn pptp remote-access client-ip-pool start 192.168.100.101
set vpn pptp remote-access client-ip-pool stop 192.168.100.110
set vpn pptp remote-access authentication mode local
set vpn pptp remote-access authentication local-users username nghiahung password nghiahung
```

```
vyatta@vyatta:~$ show vpn remote-access
Active remote access VPN sessions:

User       Time      Proto Iface Remote IP       TX pkt/byte   RX pkt/byte
---------- --------- ----- ----- --------------- ------ ------ ------ ------
nghiahung  00h00m38s PPTP  ppp0  192.168.100.101     12    332     34   3.4K
```

## IV. Nhận xét và đánh giá của nhóm

### Điểm mạnh

Hiện nay Vyatta cung cấp hệ thống router mã nguồn mở theo hai dạng: software và hardware. Điều này giúp cho các quản trị mạng có thêm sự lựa chọn khi triển khai các giải pháp hạ tầng mạng của mình. Các sản phẩm của Vyatta trên thị trường hiện nay:

- Vyatta Core: đây là phiên bản miễn phí do Vyatta cung cấp và nhận được sự hưởng ứng khá nhiều từ cộng đồng mạng. Sản phẩm này rất phù hợp trong môi trường học tập và trong công việc nghiên cứu, kiểm tra hệ thống mạng (chạy thử). Tuy nhiên cũng còn rất nhiều hạn chế trong phiên bản này. Không được sự hỗ trợ trực tiếp từ Vyatta khi gặp sự cố và một số tính năng quan trọng không được hỗ trợ (Frame Relay, PPP…)

- Vyatta subscription Edition: đây là sản phẩm thương mại chính của Vyatta. Sản phẩm này tích hợp đầy đủ các tính năng của một router Cisco nhưng giá sản phẩm lại rẻ hơn nhiều. Khi đăng kí sử dụng sản phẩm này, người quản trị mạng có thể gọi điện trực tiếp đến bộ phận hỗ trợ của Vyatta khi có sự cố về mạng xảy ra

- Vyatta Applicance có giá bằng ¼ giá thành so với Cisco nhưng so sánh với cisco không hề thua kém bất cứ điểm nào

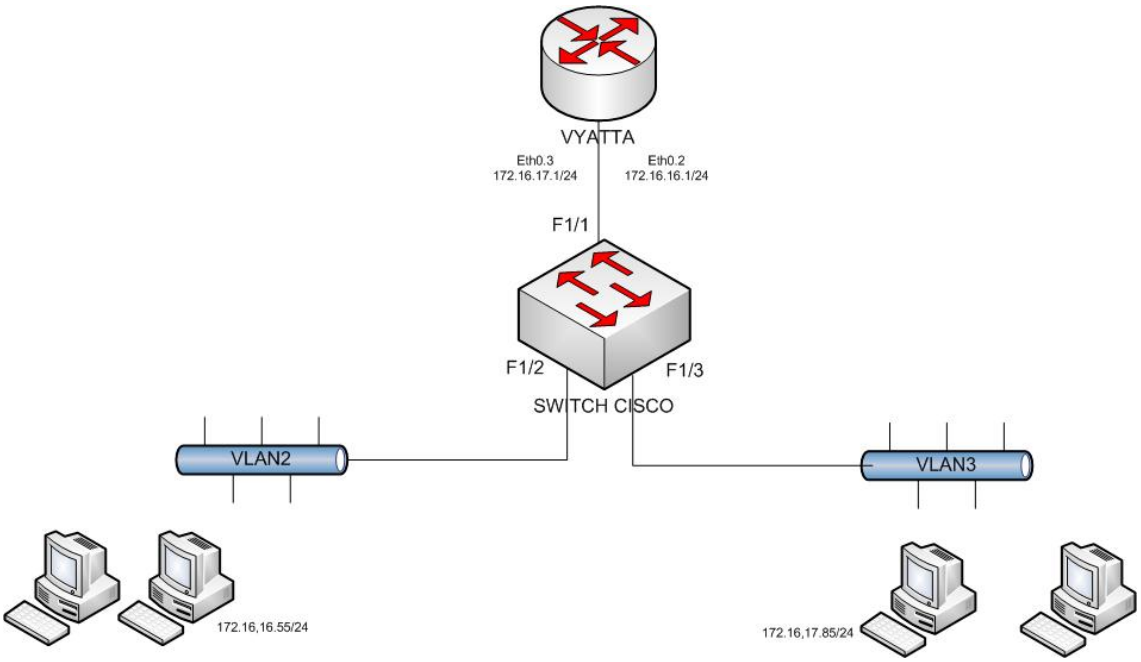
Các sản phẩm software router đều được chạy trên nền tảng X86, cho nên việc lựa chọn, thay thế hay nâng cấp thiết bị phần cứng tương đối dễ dàng. Đây là một thuận lợi to lớn của các sản phẩm Vyatta khi tung ra thị trường.

Khả năng tương thích với các thiết bị khác là rất cao. Các sản phẩm software router được chạy trên nền tảng X86, cho nên việc lựa chọn, thay thế hay nâng cấp thiết bị phần cứng tương đối dễ dàng, khả năng mở rộng linh hoạt, Backup đơn giản. Vyatta đòi hỏi nền tảng phần cứng không quá cao vì vậy doanh nghiệp sẽ tiết kiệm được nhiều chi phí khi triển khi hệ thống của mình bằng Vyatta.Điểm nổi bật ở Vyatta còn ở khả năng ảo hóa giúp Vyatta vô cùng linh hoạt trong việc backup hơn hẳn các thiết bị phần cứng khác, ngoài ra Vyatta còn thừa hưởng sức mạnh của hệ điều hành Linux

và khả năng Raid 1 cực kỳ ấn tượng, giúp cho hệ thống mạng luôn luôn sẵn sàng khi có sự cố xảy ra

**Các ví dụ về khả năng tương thích cao của Vyatta với các sản phẩm của hãng khác**

Dùng router Vyatta để định tuyến Vlan (kết hợp với switch Cisco)



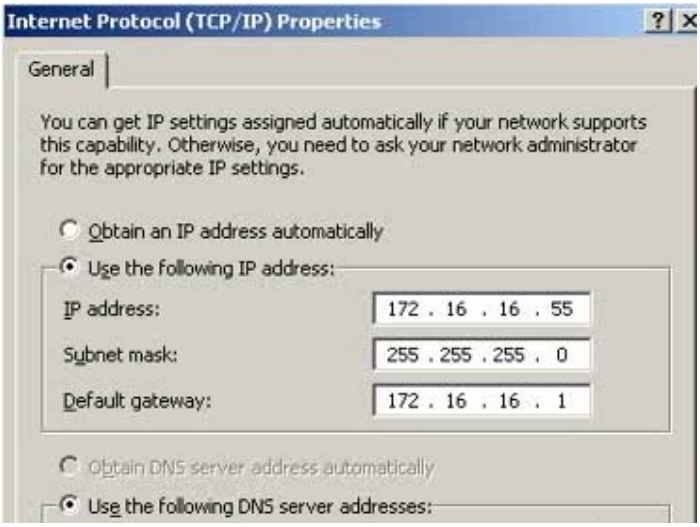
```
Switch Cisco
************************************************
conf t

vlan database
vlan 2 name net2
vlan 3 name net3

int f1/2
switchport mode access
switchport access vlan 2
no shut
exit

int f1/3
switchport mode access
switchport access vlan 3
no shut
exit

int f1/1
switchport mode trunk
no shut
exit



************************************************
Vyatta

configure
set system host-name HOASEN
set system domain-name hoasen.edu.vn

set interfaces ethernet eth0 vif 2 address 172.16.16.1/24
set interfaces ethernet eth0 vif 3 address 172.17.16.1/24
```

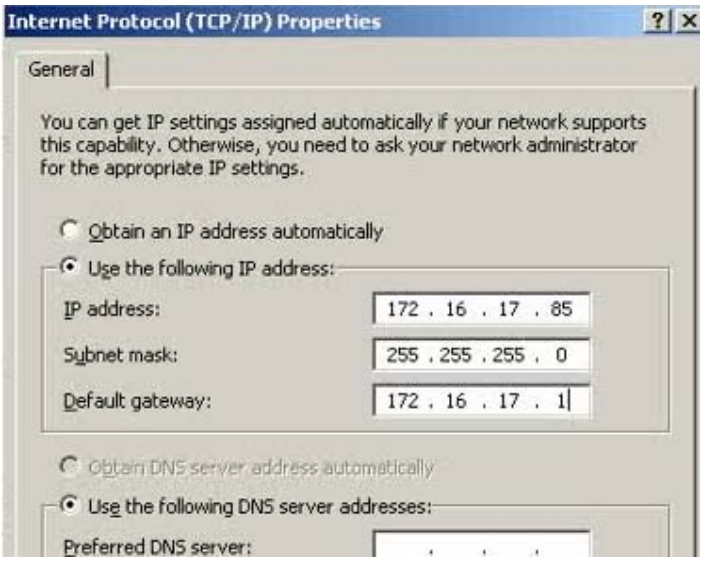
Ở mô hình mạng này, switch của router cisco sẽ tạo ra 2 vlan 2 và vlan 3 tương ứng với tên là net2 và net3. Sau khi tạo xong vlan, switch phải đưa các interface f1/2, f1/3 vào vlan 2 và 3 cho phù hợp. Interface của switch nối với router Vyatta là f1/1 sẽ được cấu hình đường trunk.

Trên Router của Vyatta sẽ tạo 2 ip trên một interface là 172.16.16.1 và 172.17.16.1 và đưa vào từng vlan sao cho phù hợp với mô hình mạng.

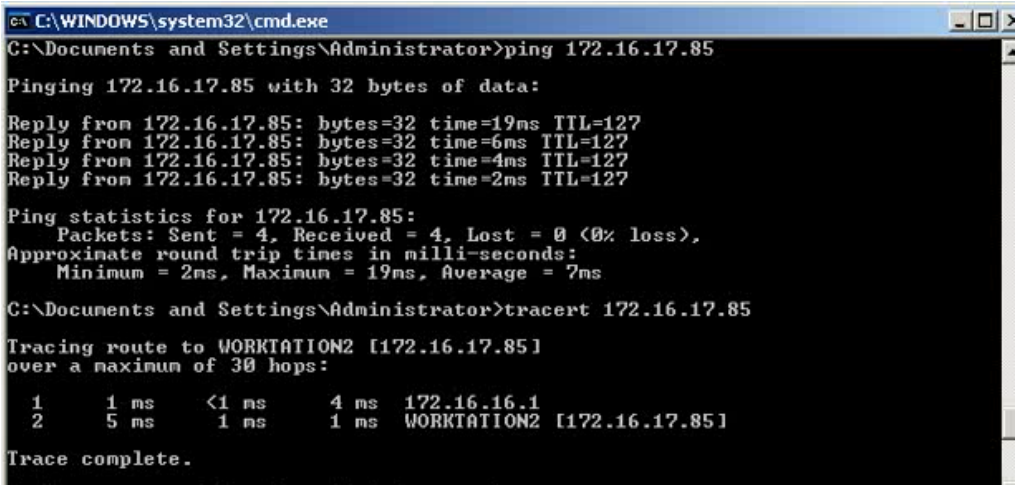
```
SWI#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/4, Fa1/5, Fa1/6
                                                Fa1/7, Fa1/8, Fa1/9, Fa1/10
                                                Fa1/11, Fa1/12, Fa1/13, Fa1/14
                                                Fa1/15
2    net2                             active    Fa1/2
3    net3                             active    Fa1/3
```

Các client khi được kết nối vào interface nào của switch sẽ tham gia vào vlan tương ứng với interface đó. Từ đó đặt default gateway trỏ đến ip của interface router Vyatta.

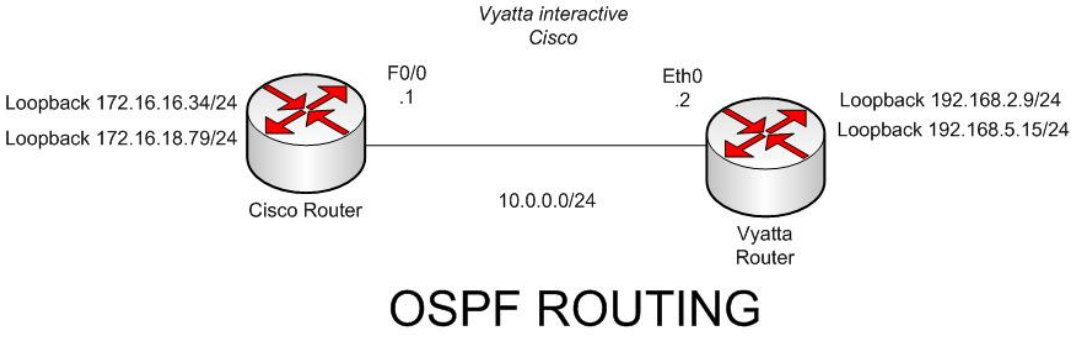



Cuối cùng, thực hiện cấu trúc lệnh tracert để kiểm tra



**Ví dụ 2: thực hiện định tuyến OSPF giữa 2 router Cisco và Vyatta**




```
Vyatta

configure
set system host-name HOASEN

set interfaces ethernet eth0 address 10.0.0.2/24
set interfaces loopback lo address 192.168.2.9/24
set interfaces loopback lo address 192.168.5.15/24

set protocols ospf parameters router-id 11.0.0.1
set protocols ospf area 0.0.0.0 network 10.0.0.0/24
set protocols ospf area 0.0.0.0 network 192.168.2.0/24
set protocols ospf area 0.0.0.0 network 192.168.5.0/24

*****************************************
Cisco

hostname Cisco
ip domain-name hoasen.edu.vn

int fa0/0
ip add 10.0.0.1 255.255.255.0
no shu
exit

int loop 0
ip add 172.16.16.34 255.255.255.0
no shut
exit

int loop 1
ip add 172.16.18.79 255.255.255.0
no shut
exit

router ospf 100
network 10.0.0.1 0.0.0.0 area 0
network 172.16.16.34 0.0.0.0 area 0
network 172.16.18.79 0.0.0.0 area 0
```

Mô hình mạng này, mỗi router sẽ tạo 2 loopback để thử hiện việc kiểm tra thiết lập neighbor, trao đổi hello bảng định tuyến.

Sau khi thiết lập, các router nhận ra các tuyến đường của nhau một cách bình thường và nhanh chóng

```
Cisco#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.16.0 is directly connected, Loopback0
C       172.16.18.0 is directly connected, Loopback1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.15 [110/20] via 10.0.0.2, 00:00:06, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/0
     192.168.2.0/32 is subnetted, 1 subnets
O       192.168.2.9 [110/20] via 10.0.0.2, 00:00:06, FastEthernet0/0
Cisco#
```

```
vyatta@vyatta:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

O   10.0.0.0/24 [110/10] is directly connected, eth0, 00:01:19
C>* 10.0.0.0/24 is directly connected, eth0
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.16.34/32 [110/11] via 10.0.0.1, eth0, 00:00:30
O>* 172.16.18.79/32 [110/11] via 10.0.0.1, eth0, 00:00:22
C>* 192.168.2.0/24 is directly connected, lo
C>* 192.168.5.0/24 is directly connected, lo
```

```
Cisco#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
11.0.0.1          1   FULL/DR         00:00:36    10.0.0.2        FastEthernet0/
0
Cisco#
```

Các ví dụ trên cho thấy khả năng tương thích khi chạy cùng các thiết bị khác là rất dễ dàng thực hiện cấu hình. Khả năng tương thích cao cũng là một trong những lợi thế rất lớn của Vyatta.

**Điểm Yếu**

Ngoài phiên bản Vyatta Core là phiên bản miễn phí, không có bất cứ một chương trình nào khác để thực hiện giả lập. Vì phiên bản Vyatta Core tuy rất được nhiều nhà quản trị mạng đón nhận nồng nhiệt, nhưng lại thiếu đi khá nhiều tính năng quan trọng và không hỗ trợ nhiều. Do đó đôi khi router Vyatta thực hiện cho công việc nghiên cứu và kiểm tra sự ổn định của hệ thống đôi khi vẫn còn hạn chế rất nhiều

Tài liệu về các sản phẩm của Vyatta rất ít. Mặc dù trên trang chủ có toàn bộ đầy đủ các tài liệu về từng tính năng của các dòng sản phẩm. Nhưng các tài liệu chỉ ở mức độ

tham khảo, định nghĩa chứ không giải thích và nêu sâu hơn về cơ chế hoạt động như nhà khổng lồ Cisco. Hơn nữa, tài liệu của Vyatta hầu như không có diễn đàn nào đề cập đến, ngay cả diễn đàn do chính Vyatta quản lí. Để có thể hiểu rõ hơn về các hoạt động, người quản trị mạng có thể đăng kí khóa đào tạo dưới hình thức online do Vyatta tổ chức và phải trả phí.

# KẾT LUẬN

Vyatta là một sản phẩm mã nguồn mở có đầy đủ tính năng tương đương với một router Cisco và với một mức giá phù hợp. Vyatta thực sự là cái tên đáng được chú ý nhiều nhất đối với các nhà quản trị mạng trong công cuộc tìm kiếm một sản phẩm có thể thay thế hoàn toàn Cisco với một chi phí khá cao. Trong quá trình nghiên cứu về sản phẩm router mã nguồn mở Vyatta. Nhóm chúng tôi đã thu lại được các kết quả như sau:

- Nắm được một cách tổng thể về các sản phẩm router của Vyatta, từ software router đến các Vyatta appliance.
- Nắm rõ hơn về cơ chế hoạt động của các tính năng trong router Vyatta.
- Nắm được cách cấu hình trên các rotuer software Vyatta để từ đó có thể áp dụng và việc triển khai các mô hình mạng thực tế
- Nắm được các điểm mạnh và điểm yếu của Vyatta trong quá trình nghiên cứu.

Tuy nhiên các kiến thức về sản phẩm của Vyatta là vô cùng rộng và đòi hỏi phải có rất nhiều thời gian để nghiên cứu. Bài báo cáo của chúng tôi có thể sẽ vẫn còn tồn tại một vài thiếu sót. Vì thế nhóm rất mong muốn nhận được các góp ý từ bạn bè và thầy cô.

# TÀI LIỆU THAM KHẢO

[1] Cisco Systems, Building Scalable Cisco Internetwork vol 1, 2006

[2] Cisco Systems, Building Scalable Cisco Internetwork vol 2, 2006

[3] Website www.vnpro.com

[4] Website www.Vyatta.com

[5] Website www.Vyatta.org

[6] Website www.Vyatta.vn

[7] Website www.cisco.com

[8] Website www.nhatnghe.com