ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Thiết kế mạng IP

Chương 2: Mạng nội bộ (Private network)

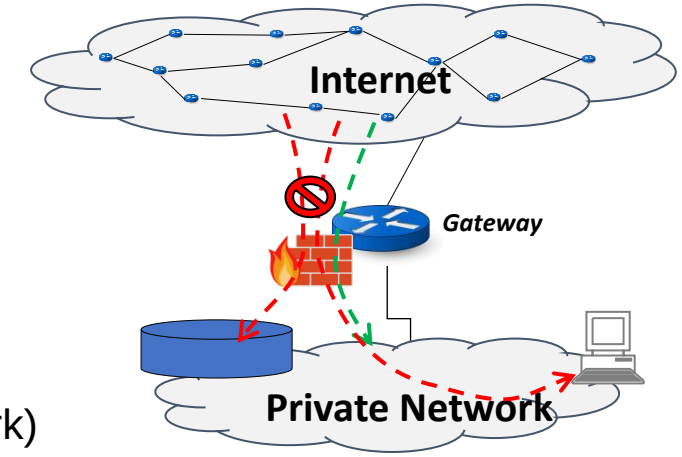
Phạm Huy Hoàng - SoICT/HUST
hoangph@soict.hust.edu.vn

Nội dung

- Khái niệm & định nghĩa
- Private network đơn giản: LAN, virtual LAN & inter-LAN
- Kết nối tầng IP giữa mạng nội bộ và Internet
  - Qui hoạch gateway cho private network
  - Địa chỉ IP cho private network
  - DHCP
  - NAT, NAPT & Port Forwarding
- Mạng nội bộ ảo – Virtual Private Network (VPN)
- Kết nối dịch vụ giữa private network và public Internet: DNS, Email, Web, FTP
- Đảm bảo an toàn mạng nội bộ
  - Qui hoạch các vùng an toàn trong mạng nội bộ
  - Tường lửa bảo vệ (firewall)
  - Hệ thống phát hiện xâm nhập IDS

Khái niệm & định nghĩa

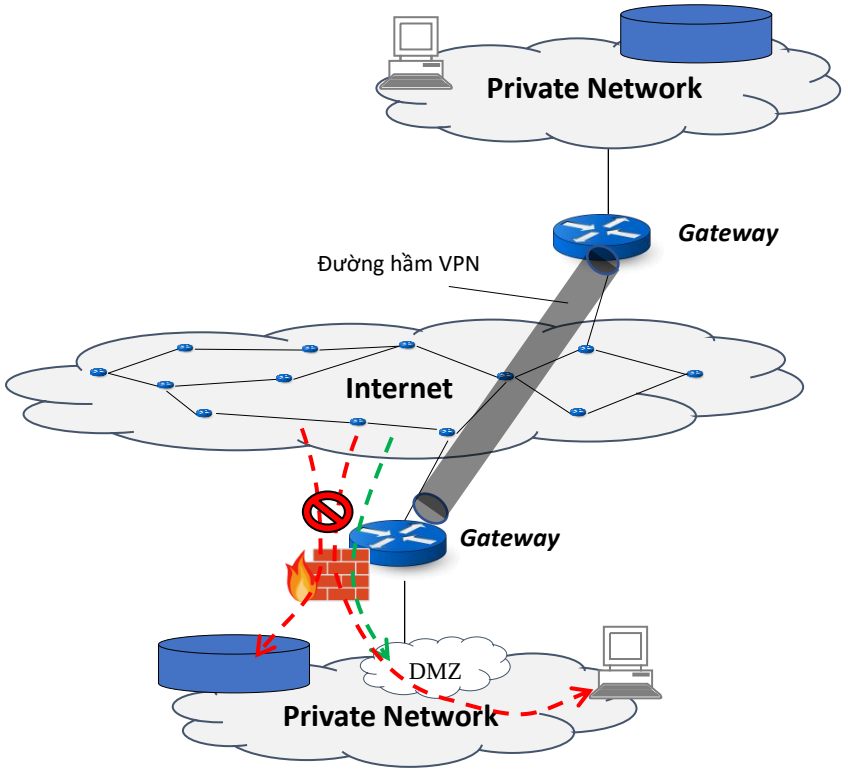
- Wikipedia[1]: *"In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments."*
- Techopedia định nghĩa theo phương diện an toàn thông tin[2]: *"A private network is any connection within a specified network wherein restrictions are established to promote a secured environment. This type of network can be configured in such a way that devices outside the network cannot access it."*
- Private (riêng tư) Network
  - Thiết lập cho mục đích sử dụng riêng (phân biệt với mạng public, mạng Internet)
  - Chứa các tài nguyên riêng, được bảo vệ không cho phép truy nhập từ bên ngoài
  - Có kết nối với public bên ngoài
  - Sử dụng dải địa chỉ IP private (xin địa chỉ IP phức tạp và mất nhiều thời gian)
  - Sử dụng IP public, hoặc mạng public làm công cụ (Virtual Private Network)



[1] https://en.wikipedia.org/wiki/Private_network
[2] https://www.techopedia.com/definition/26423/private-network

Kiến trúc tổng thể

- Private Network > < Public Network (Internet)
- Internet: mạng kết nối các private network
  - Đường truyền
  - Router
  - BGP/IGP routing protocol
- Private Network
  - Gateway kết nối public: router kết nối đường truyền trong mạng private với public
  - Tài nguyên & các host trong mạng private được bảo vệ khỏi truy nhập từ public bằng các luật xử lý gói tin trên gateway ➔ tường lửa (firewall)
  - Khu vực đặc biệt cho phép truy nhập có kiểm soát từ public ➔ DMZ zone[1] (Demilitarized Zone)
  - Các host trong private network sử dụng dải địa chỉ IP riêng để trao đổi thông tin. Khi truy nhập public cần cơ chế hỗ trợ trên Gateway (NAT & Port forwarding)
  - Các mạng private xa nhau sử dụng mạng public Internet để chia sẻ tài nguyên với nhau một cách an toàn (ví dụ, sử dụng cơ chế đường hầm IP – IP tunnelling[2] – giữa 2 gateway) tạo nên một mạng private to hơn ➔ Virtual Private Network



[1] https://en.wikipedia.org/wiki/DMZ_(computing)
[2] https://en.wikipedia.org/wiki/IP_tunnel

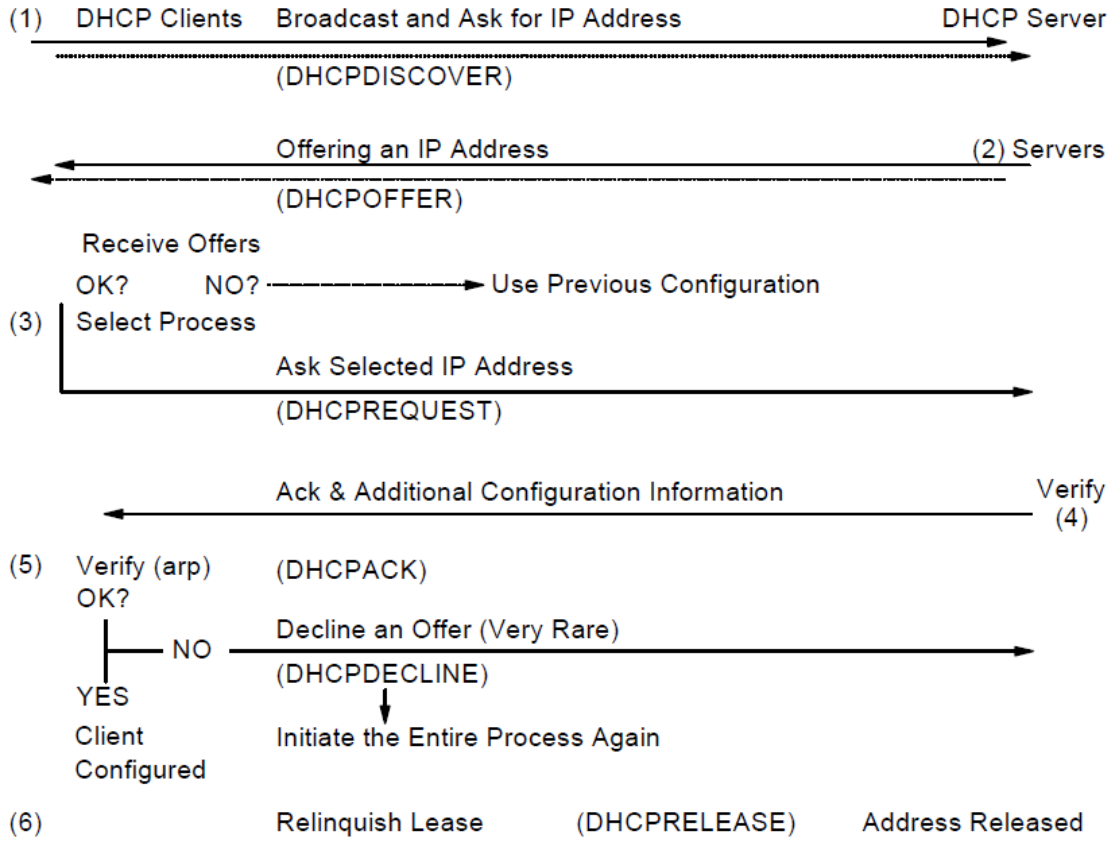
Private Network đơn giản nhất: LAN

- Local Area Network
  - Mạng nội bộ đơn giản nhất
  - Hoạt động tầng 2 (thậm chí là tầng 1)
  - Dễ dàng share resource (thư mục, file, máy in, v.v..)
  - Quản lý tài nguyên tập trung (đây mới là yếu tố xác định LAN)

- Cấu hình địa chỉ cho máy trạm
  - Địa chỉ IP của trạm để liên lạc (gửi/nhận gói tin IP) với các trạm khác
  - Địa chỉ IP gateway để gửi gói tin IP ra bên ngoài mạng LAN
  - Gán các địa chỉ IP tính hoặc tự động (khi máy kết nối mạng) bằng DHCP
  - DHCP kết hợp static IP – phân vùng địa chỉ IP
  - DHCP với địa chỉ IP đặt trước (reserved IP address)

Giao thức DHCP

1. Client broadcast DHCPDISCOVER message (gói trong UDP) trên mạng vật lý mà nó vừa kết nối để xin cấp địa chỉ IP
2. (các) DHCP server trả lời bằng DHCPOFFER message chứa một địa chỉ IP sẽ được gán cho client (có thể cùng với các thông số cấu hình khác như địa chỉ gateway, địa chỉ DNS server)
3. Client chấp nhận DHCPOFFER và gửi (quảng bá) DHCPREQUEST message để (các) DHCP server biết lựa chọn của client
4. DHCP Server mà được client lựa chọn gửi lại thông điệp DHCPACK để xác nhận với client
5. Client thiết lập cấu hình địa chỉ cho mình & ghi lại thời gian có hiệu lực của cấu hình hiện tại
6. Message DHCPRELEASE được gửi đi khi client muốn kết thúc sử dụng địa chỉ IP hiện tại



➔ DHCP không có cơ chế xác thực & lựa chọn server, dẫn đến khả năng client bị "fake DHCP"

Các thông điệp DHCP

DHCPDISCOVER message

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67

OP = 0x01	HTYPE = 0x01	HLEN = 0x06	HOPS = 0x00
XID = 0x3903F326			
SECS = 0x0000		FLAGS = 0x8000	
CIADDR (Client IP address) = 0x00000000			
YIADDR (Your IP address) = 0x00000000			
SIADDR (Server IP address) = 0x00000000			
GIADDR (Gateway IP address) = 0x00000000			
CHADDR (Client hardware address) = ...			
DHCP Options:			

st Subnet Mask (1), Router (3),

DHCPREQUEST message

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67

OP = 0x01	HTYPE = 0x01	HLEN = 0x06	HOPS = 0x00
XID = 0x3903F326			
SECS = 0x0000		FLAGS = 0x0000	
CIADDR (Client IP address) = 0x00000000			
YIADDR (Your IP address) = 0x00000000			
SIADDR (Server IP address) = 192.168.1.1			
GIADDR (Gateway IP address) = 0x00000000			
CHADDR (Client hardware address) = ...			
DHCP Options: DHCP option 53: DHCP Request DHCP option 50: 192.168.1.100 requested DHCP option 54: 192.168.1.1 DHCP server			

DHCPOFFER message

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68

OP = 0x02	HTYPE = 0x01	HLEN = 0x06	HOPS = 0x00
XID = 0x3903F326			
SECS = 0x0000		FLAGS = 0x0000	
CIADDR (Client IP address) = 0x00000000			
YIADDR (Your IP address) = 192.168.1.100			
SIADDR (Server IP address) = 192.168.1.1			
GIADDR (Gateway IP address) = 0x00000000			
CHADDR (Client hardware address) = ...			
DHCP Options: DHCP option 53: DHCP Offer DHCP option 1: 255.255.255.0 subnet mask			

DHCPACK message

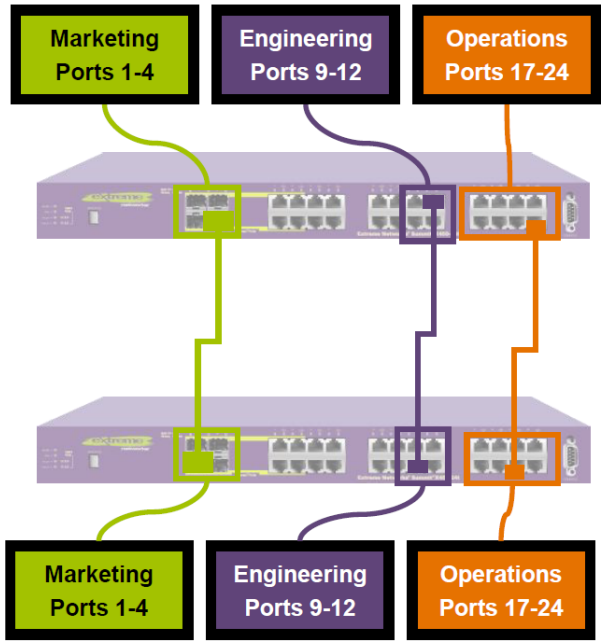
UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68

OP = 0x02	HTYPE = 0x01	HLEN = 0x06	HOPS = 0x00
XID = 0x3903F326			
SECS = 0x0000		FLAGS = 0x0000	
CIADDR (Client IP address) = 0x00000000			
YIADDR (Your IP address) = 192.168.1.100			
SIADDR (Server IP address) = 192.168.1.1			
GIADDR (Gateway IP address) = 0x00000000			
CHADDR (Client hardware address) = ...			
DHCP Options: DHCP option 53: DHCP ACK (value=5) or DHCP NAK (value=6) DHCP option 1: 255.255.255.0 subnet mask DHCP option 3: 192.168.1.1 router DHCP option 51: 86400s (1 day) IP address lease time DHCP option 54: 192.168.1.1 DHCP server DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18			

thực hành: # Thiết lập DHCP cho LAN

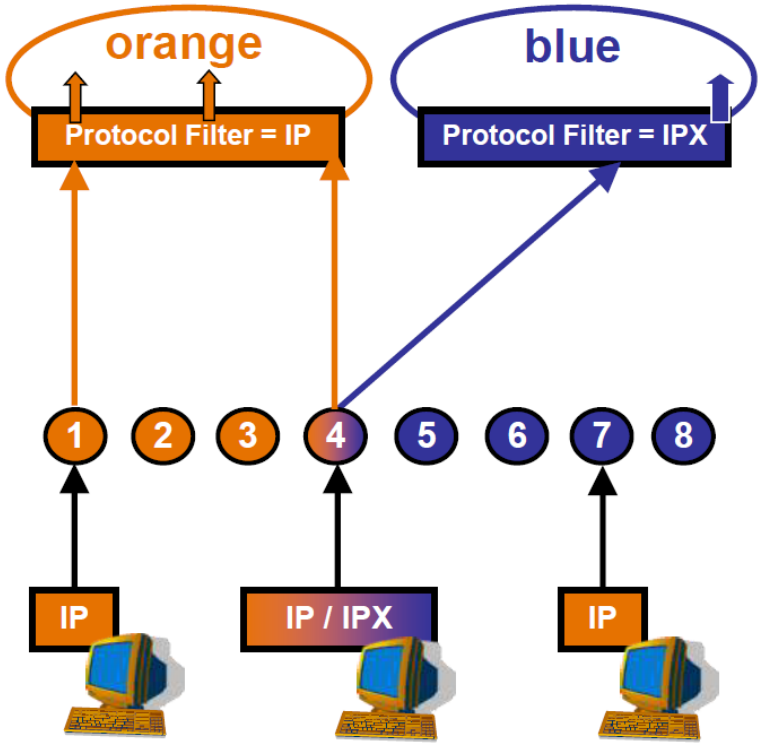
Inter-LAN & Virtual LAN (nhắc lại)

- LAN ➔ Inter-LAN:
  - Nhu cầu tăng kích thước mạng nội bộ: số host, khoảng cách giữa các host
  - Yêu cầu bảo mật theo từng vùng: phòng ban chia sẻ tài nguyên nội bộ & đảm bảo bên ngoài phòng ban không truy cập được
  - *lưu ý:* Yêu cầu bảo mật theo từng vùng có thể xử lý bằng việc kiểm soát tài nguyên tập trung, nhưng phức tạp & cần có sự tham gia của Admin
- LAN ➔ Virtual LAN
  - Có sự phân tán địa lý của vùng bảo mật
  - Phòng ban gồm nhiều địa điểm cách xa nhau nhưng vẫn muốn áp dụng cơ chế bảo mật đơn giản theo broadcast zone (LAN)
  - LAN (VLAN) được khai báo với các host phân tán trên nhiều switch. Các switch phối hợp để vận hành broadcast zone phù hợp
  - Trunk port là cổng đặc biệt, thực hiện vận chuyển các frame của nhiều VLANs
- VLAN technology:
  - Port-based (Untagged) VLAN
  - Protocol-based VLAN
  - 802.1Q Tagged VLAN



Port-based & Protocol-based VLAN

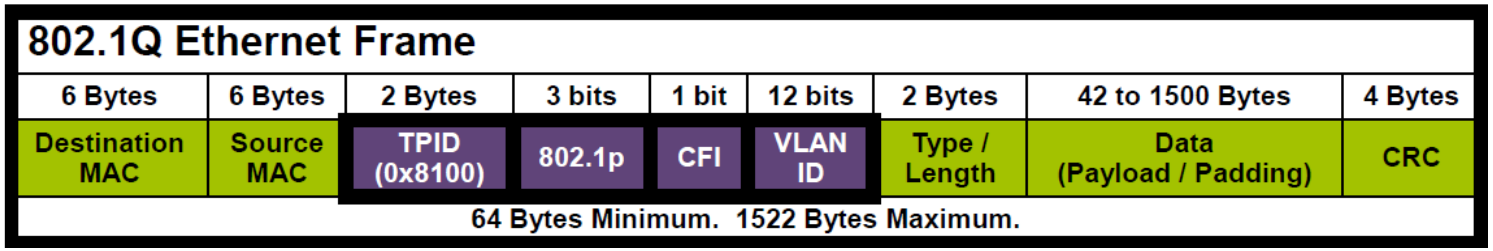
- Port-based:
  - VLAN được xây dựng bằng cách gán các cổng của switch với số hiệu VLAN.
  - Mỗi cổng switch được gán với duy nhất 1 VLAN
  - Ethernet frame nhận được từ 1 cổng
    ➔ chỉ switch sang các cổng thuộc cùng VLAN
- Protocol-based:
  - Admin khai báo “packet filter” tại switch, dựa trên các tiêu chí matching để xác định frame thuộc VLAN nào.
  - Các tiêu chí matching có thể dựa trên trường Type, LLC hoặc SNAP trong frame
  - Khai báo 1 cổng có thể tham gia nhiều VLAN. Vận hành sẽ xác định ethernet frame hiện tại thuộc VLAN nào để xử lý switch



Ethernet Frame						
6 Bytes	6 Bytes	2 Bytes	3 Bytes	5 Bytes	38 to 1492 Bytes	4 Bytes
Destination MAC	Source MAC	Type	LLC (Logical Link Control)	SNAP (Sub network Access Protocol)	Data (Payload / Padding)	CRC
64 Bytes Minimum. 1518 Bytes Maximum.						

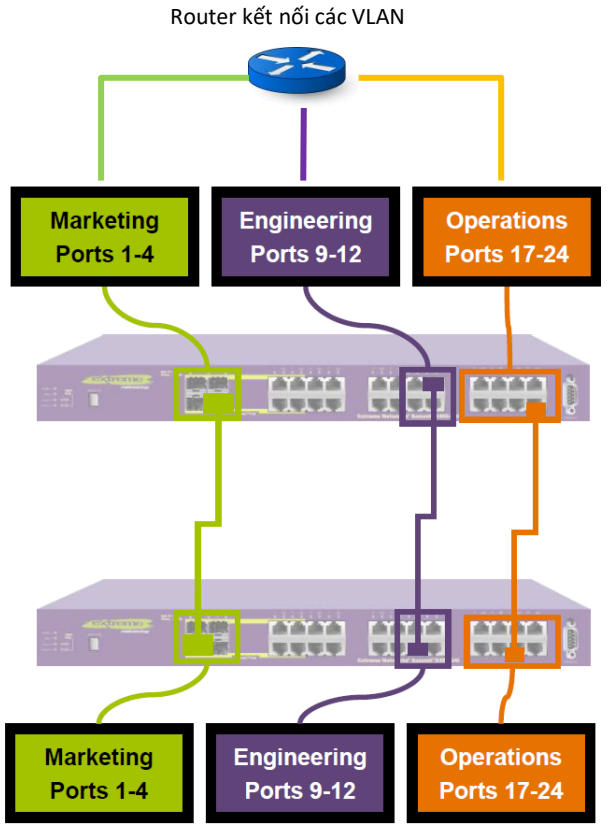
802.1Q Tagged VLAN

- Hoạt động tương tự cơ chế dựa trên Protocol, nhưng được IEEE chuẩn hóa (802.1)
- 802.1Q VLAN membership is based upon the VLAN ID in the 802.1Q field in the incoming packet.
- The 801.Q Tag contains four fields:
  - Tag Protocol ID (TPID)
  - User Priority
  - Canonical Format Indicator (CFI)
  - VLAN Identifier (VID)



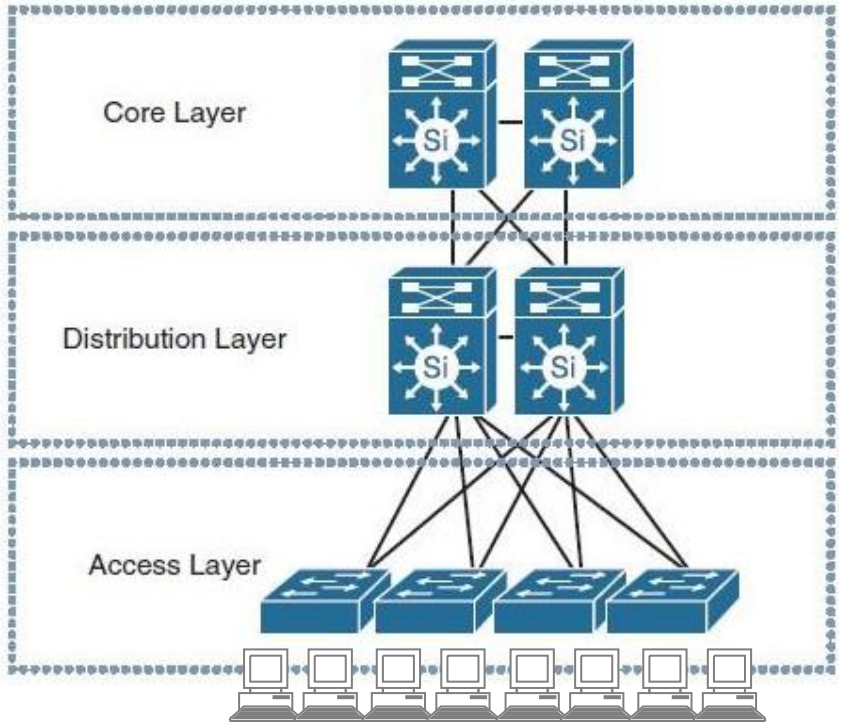
VLAN & IP

- Các hoạt động trên tầng IP (cấp địa chỉ với DHCP, gửi/nhận gói tin IP) hoạt động không phân biệt tầng 2 của máy trạm hiện đang chạy VLAN hay không
- VLAN bản chất là chỉnh sửa broadcast zone, thay vì toàn bộ mạng LAN thì chia ra làm nhiều vùng, mỗi vùng bao gồm các máy trạm phân tán và được gán chung một broadcast zone
- Cơ chế ARP (để ánh xạ địa chỉ IP sang địa chỉ MAC) sử dụng qui tắc hỏi đáp kiểu broadcast tương tự như DHCP. Phạm vi broadcast zone trong VLAN bị hẹp lại so với LAN ban đầu ➔ các máy trạm thuộc VLAN khác nhau không ánh xạ được IP sang địa chỉ MAC và không thể gửi frame tầng 2 cho nhau theo kiểu broadcast ➔ phải liên lạc bằng tầng IP (giống như liên lạc của 2 máy trạm tại 2 LAN khác nhau)
- Kết nối inter-VLAN như vậy có thể được triển khai bằng router giống như kết nối inter-LAN, nhưng hiện nay thường được xử lý với layer 3-switching của Cisco



Private Network với Cisco layer 3 switch

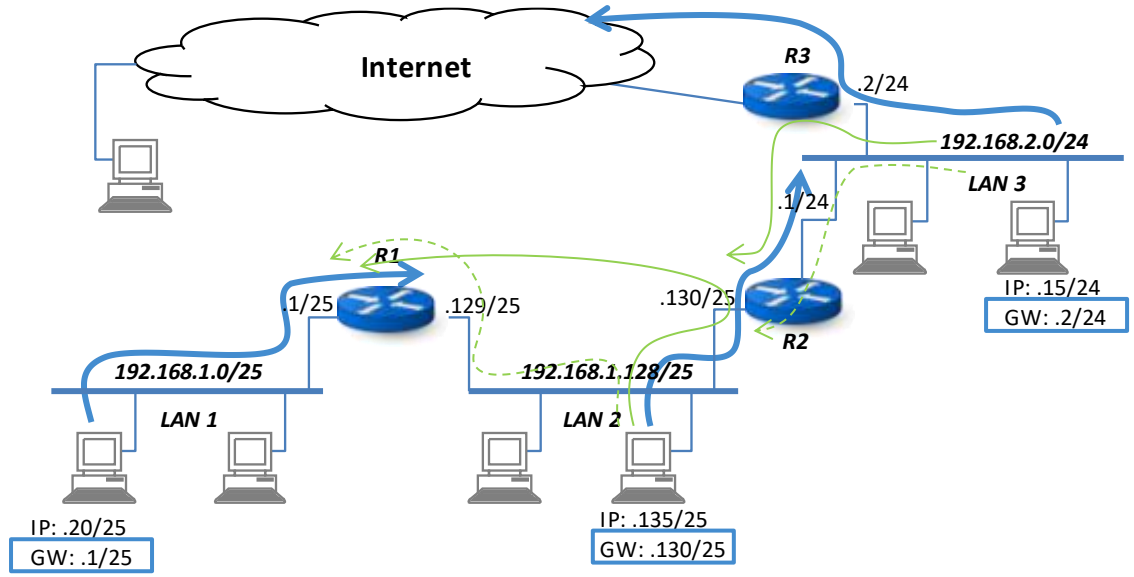
- Mạng private cỡ vừa đến lớn (mức độ trường đại học) hiện nay được xây dựng trên các hệ thống switch và hầu như đều đòi hỏi sử dụng VLAN
- Cisco nắm bắt xu hướng này và cung cấp các switch hoạt động cả ở tầng 2 và tầng 3 để hỗ trợ kết nối inter-VLAN rất đơn giản (gọi là switch layer-3)
- Mô hình mạng inter-VLAN toàn switch được Cisco đưa ra với 3 tầng kết nối switch: core, distribution và access
- Các máy trạm làm việc được kết nối với tầng access, distribution và core được sử dụng ở các kết nối chịu tải lớn (như các mạng backbone, hay gateway đi ra Internet)
- Các Cisco switch cũng hỗ trợ thêm các kết nối với nhau để hỗ trợ quản trị tài nguyên tập trung, vốn là đặc tính sử dụng của mạng private



Kết nối tầng IP với Internet

Inter-LAN và qui hoạch default gateway

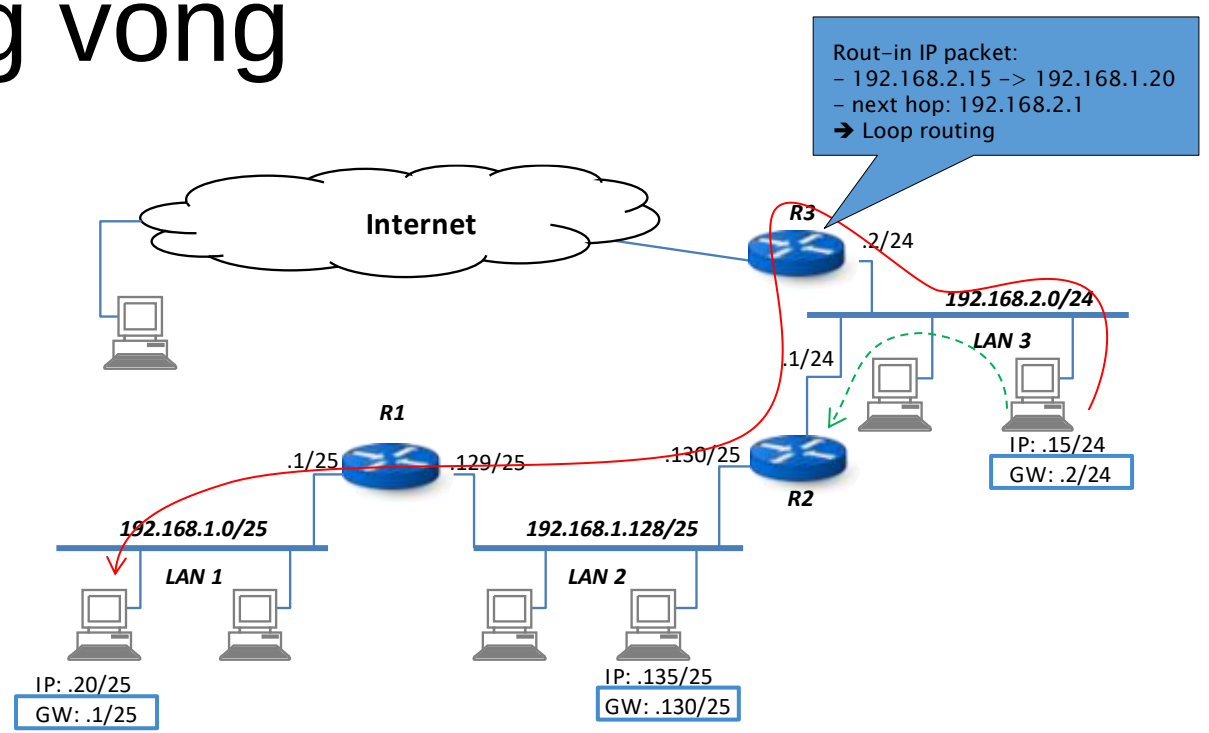
- Gateway đối với Private Network được hiểu là trạm (router) kết nối mạng private này với mạng public Internet
- Khi mạng private được thiết lập bằng nhiều LAN, mỗi trạm trong LAN cần được thiết lập default gateway ➔ Gateway của LAN là trạm (router) kết nối LAN với phần còn lại của mạng private
- Khi LAN có duy nhất 1 router kết nối ➔ router đó mặc nhiên là gateway của LAN
- Khi LAN có nhiều router để kết nối với các LAN khác trong mạng private ➔ lựa chọn router nào làm gateway cho LAN theo hướng ưu tiên lưu lượng kết nối
- Đối với các kết nối ra ngoài LAN mà không theo hướng nhiều lưu lượng kết nối ➔ đi vòng qua 2 router ➔ ICMP redirect



➔ Do lưu lượng hướng đi màu blue nhiều hơn màu green nên LAN2 và LAN3 qui hoạch default gateway tương ứng là R2 và R3, phù hợp với các hướng giao thông chính

ICMP Redirect & routing vòng

- Cấu hình default gateway cho mạng LAN có nhiều hơn 2 kết nối ra phần còn lại của mạng privare sẽ xảy ra tình huống gói tin phải đi vòng. Ví dụ khi ping từ máy trong mạng LAN3 sang máy trong LAN1, gói tin đi vòng qua gateway R3 rồi chuyển sang R2
- Tình trạng gói tin đi vòng có thể xảy ra khi các bảng routing được cấu hình không đồng bộ tạo nên đường vòng (loop routing) mà các routing protocol thường phải xử lý
- Router R3 phát hiện có loop routing ngoài việc xử lý gói tin IP theo bảng routing, nó kích hoạt gói ICMP Redirect[1] gửi về cho trạm phát
- Xử lý: các máy trạm có thể thiết lập nhiều gateway thay vì một default gateway. Khi nhận được ICMP redirect, máy trạm sẽ áp dụng gateway phù hợp với trường "nexthop" trong gói tin ICMP Redirect



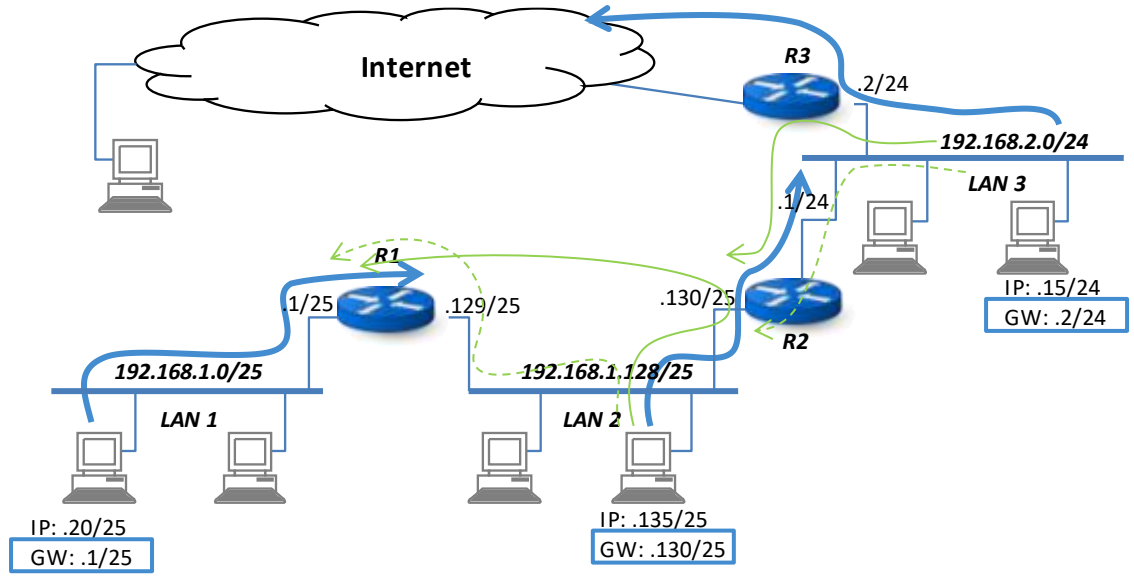

```
> ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
From 192.168.2.2: icmp_seq=1 Redirect Host(New nexthop:
192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=1 ttl=62 time=4.24 ms
From 192.168.2.2: icmp_seq=2 Redirect Host(New nexthop:
192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=5.05 ms
From 192.168.2.2: icmp_seq=3 Redirect Host(New nexthop:
192.168.2.1)
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=1.90 ms
```


[1] https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol#Redirect

thực hành:

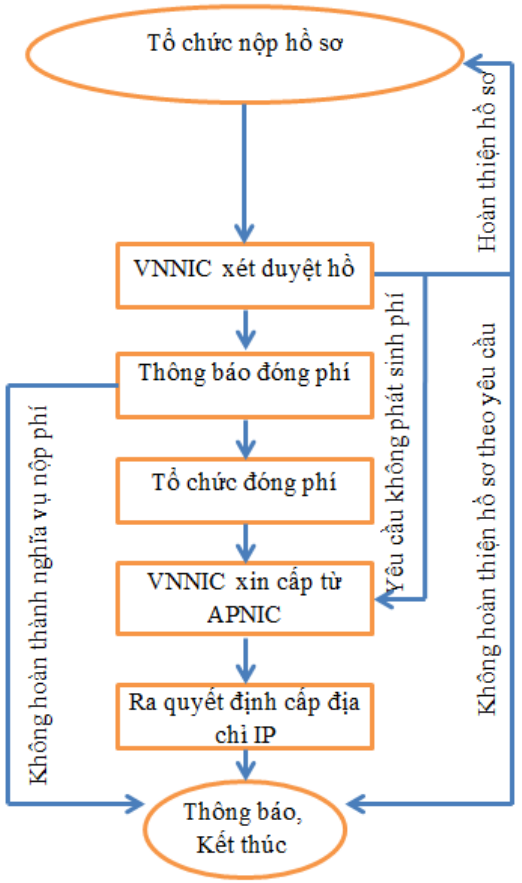
Qui hoạch gateway cho LAN & Private Net.

- Cấu hình host & gateway cho các LAN theo ưu tiên lưu lương
- Ping kiểm tra từ LAN3 sang LAN1 để xuất hiện ICMP Redirect
- Khai báo thêm gateway cho LAN3 và kiểm tra ping lại sang LAN1



Quản lý tài nguyên địa chỉ IP

- Trạm làm việc cần 1 địa chỉ IP (duy nhất!) để gửi & nhận gói tin IP
- Quản lý tài nguyên địa chỉ IP toàn cầu:
  - American Registry for Internet Numbers (ARIN): Bắc Mỹ, Nam Mỹ, Caribbean & châu Phi
  - Reseaux IP Europeans (RIPE): châu Âu, Trung Đông & một số bộ phận của châu Phi.
  - Asia Pacific Network Information Centre (APNIC): Châu Á Thái Bình Dương (gồm Việt Nam)
- Quản lý tài nguyên địa chỉ IP tại Việt Nam:
  - Trung Tâm Internet Việt Nam[1] (VNNIC) thuộc Bộ TT&TT
  - Cấp địa chỉ IP theo qui trình/qui định[2]: thường áp dụng cho các cơ quan tổ chức tương đối lớn cần một lượng địa chỉ IP phục vụ cho hoạt động của mình
  - Small Office & Home Office (Soho): kết nối Internet qua ISP và được cấp IP theo qui định của ISP này, thường là 01 địa chỉ IP không cố định. Tùy vào hợp đồng giữa Soho và ISP, địa chỉ IP cố định có thể được cấp cho Soho network
  - Thực tế là ISP xin VNNIC cung cấp một dải địa chỉ IP và sử dụng tài nguyên này để cấp cho các Soho network

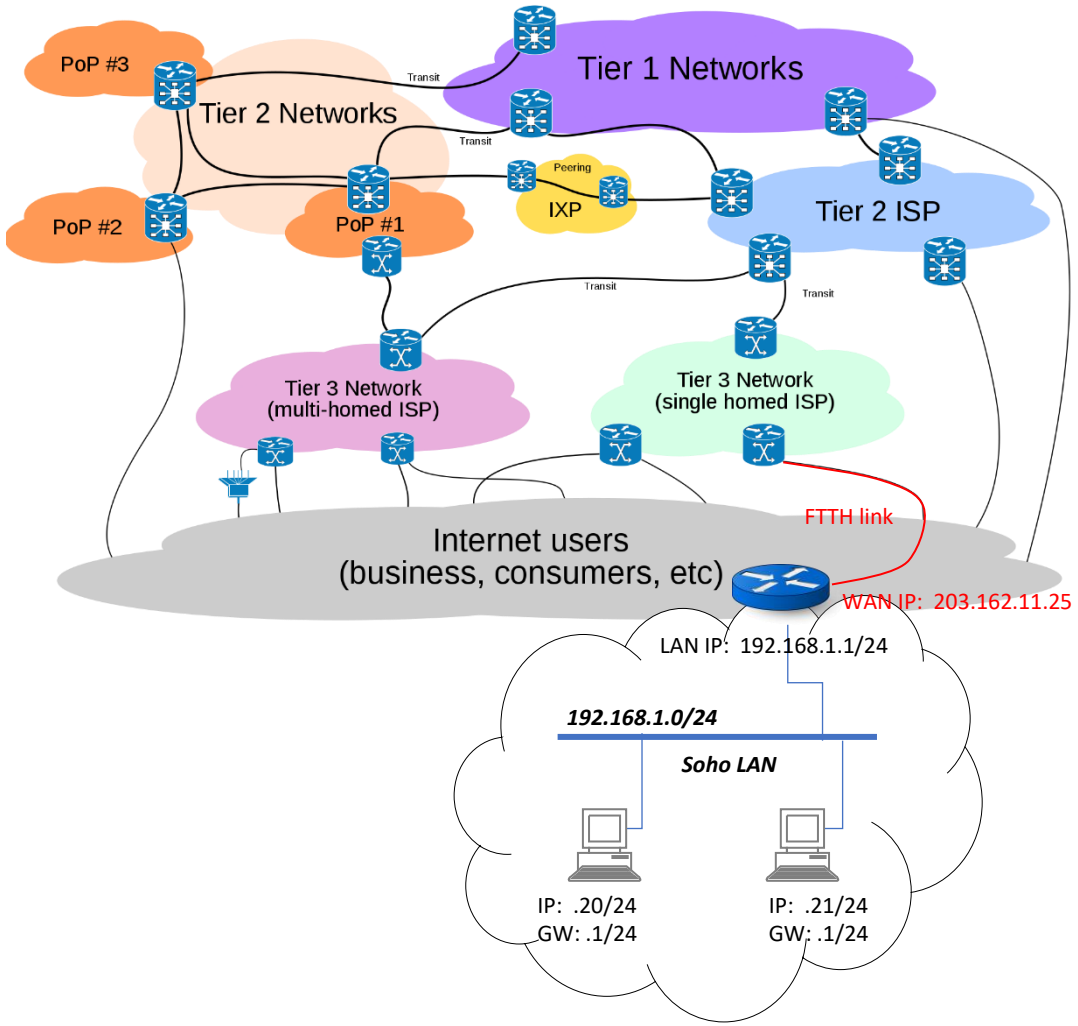


Qui trình cấp địa chỉ IP – nguồn VNNIC

[1] https://vnnic.vn
[2] https://vnnic.vn/diachiip/chinhsach/quy-trinh-dang-ky-cap-phan-bo-ipv4-ipv6-dang-ky-dia-chi-ip-va-doi-ten-thanh-vien

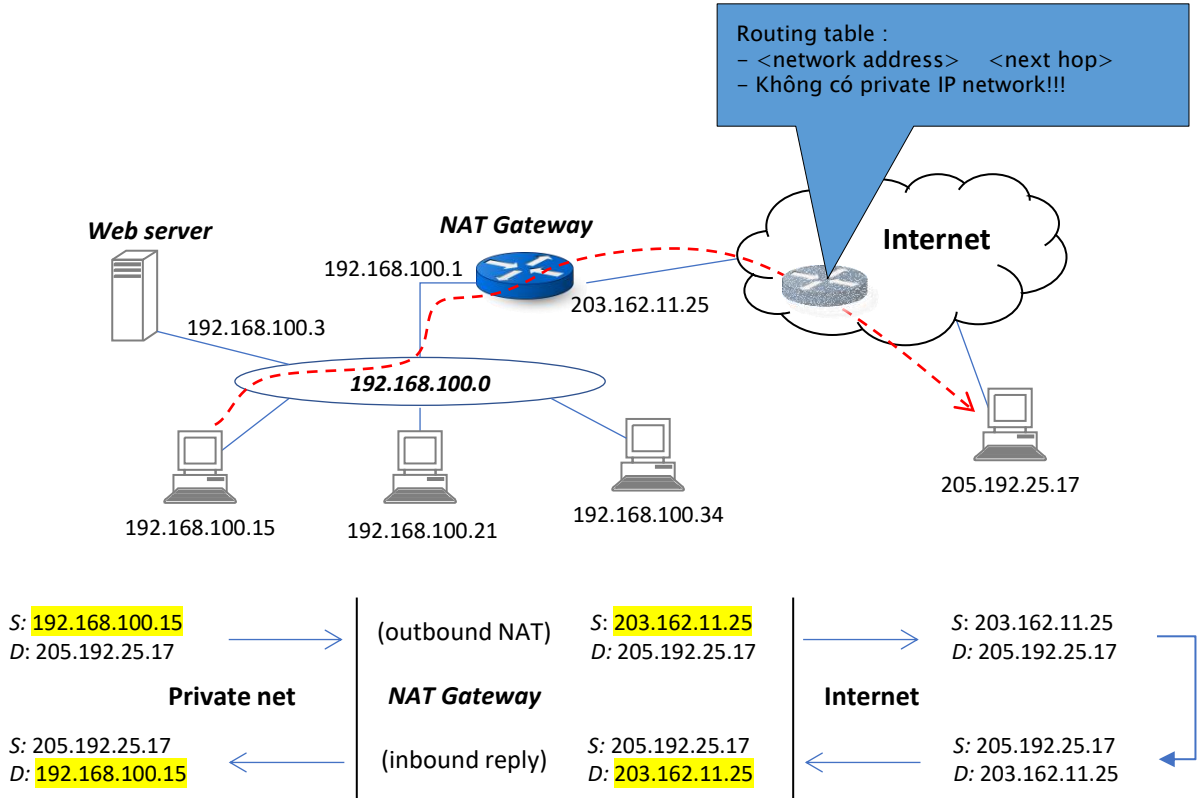
Vai trò của private IP addresses

- Soho network nết nối mạng ISP (ví dụ FTTH) bằng thiết bị router do ISP cung cấp (phù hợp với đường truyền) và được gán địa chỉ IP bằng DHCP của ISP (gọi là địa chỉ WAN IP – địa chỉ mặt ngoài)
- ISP router kết nối với Soho network và được gán một địa chỉ IP (gọi là LAN IP – địa chỉ mặt trong). Nó đóng vai trò là gateway cho Soho network đi ra Internet (thực tế là đi vào ISP network).
- Soho network sử dụng private IP address:
  - 10.x.x.x/8, 172.16-31.x.x/16, 192.168.x.x/24
  - Không cần thủ tục xin cấp phát
  - Đáp ứng yêu cầu kỹ thuật để kết nối IP các trạm trong Soho network
- Kết nối Soho network với bên ngoài:
  - Dùng NAT khi cần kết nối với một trạm bên ngoài Soho network (sử dụng địa chỉ IP public)
  - Dùng Port forwarding để nhận các kết nối từ bên ngoài vào Soho network



Network Address Translation (NAT)

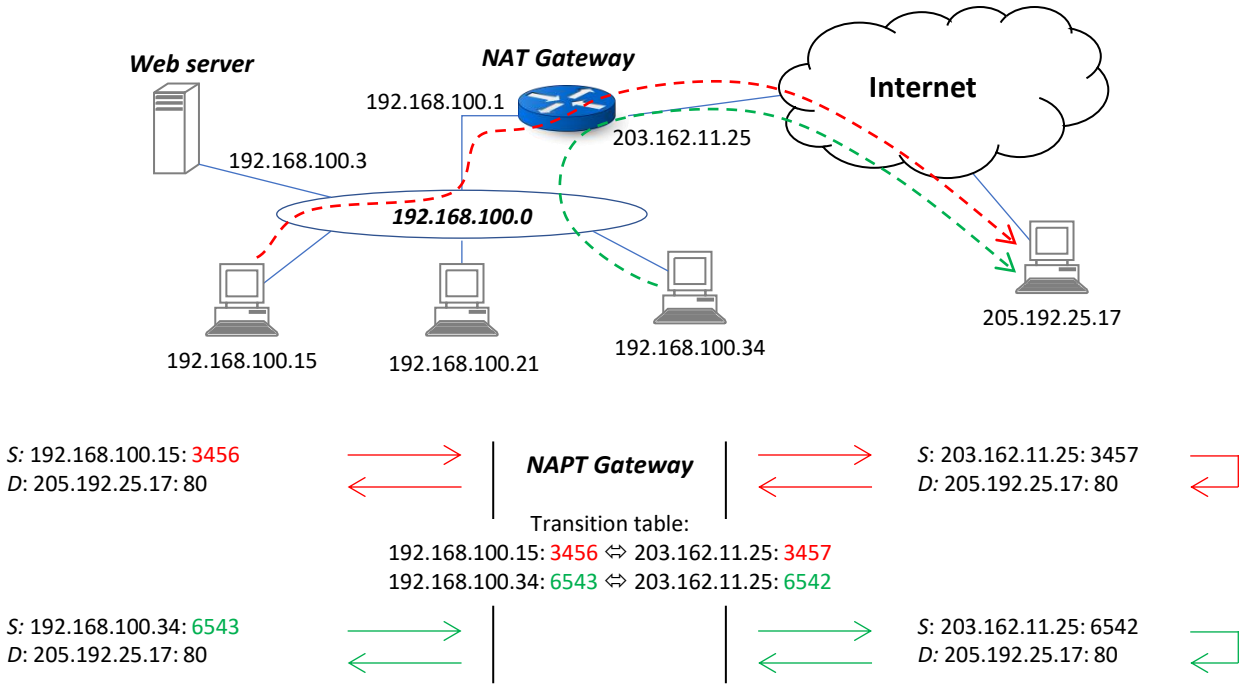
- Về mặt kỹ thuật, các router xử lý không phân biệt địa chỉ IP public và private
- Về mặt quản lý, không tồn tại địa chỉ IP private trong "giao thông" trên mạng Internet public
- Các router Internet public (backbone, tier, ISP, v.v..) được cấu hình các bảng routing không chứa các địa chỉ IP private
- Network Address Translation[1] (NAT) hoạt động tại tầng IP của private network gateway, hỗ trợ xử lý các gói tin IP của private net để có thể tham gia giao thông trên mạng public Internet
- Cơ chế hoạt động cơ bản (Basic NAT):
  - Xác định 1 trạm private net được kết nối public Internet
  - Thay địa chỉ IP nguồn bằng địa chỉ mặt ngoài của gateway cho các gói tin đi ra từ private network
  - Thay địa chỉ IP đích bằng địa chỉ trạm trong private network cho các gói tin đi từ public Internet vào private network



[1] https://en.wikipedia.org/wiki/Network_address_translation

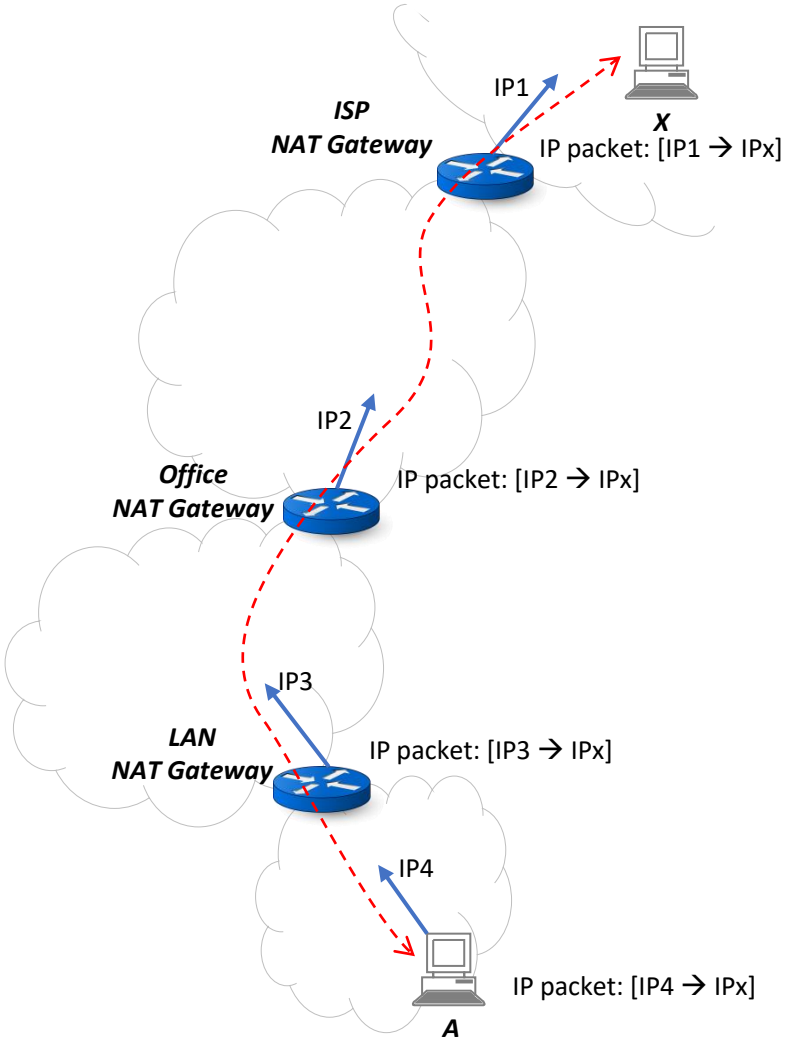
One-to-many NAT: NAPT

- Ngoài mục tiêu cho phép máy trạm trong private network truy nhập public Internet, NAT còn hỗ trợ nhiều máy trạm sử dụng các private IP address cùng chia sẻ một public IP address
- Network Address and Port Translation:
  - Basic NAT hoạt động ở tầng 3, chuyển đổi địa chỉ IP trong tất cả gói tin IP thành gói tin gửi đi từ địa chỉ mặt ngoài của gateway ➔ chỉ hỗ trợ 1 trạm private network kết nối public Internet
  - One-to-many NAT (NAPT) hoạt động ở tầng 4, chuyển đổi địa chỉ IP trong gói tin IP và trường Port trong gói tin TCP/UDP
  - Các gói tin TCP/UDP gửi đi từ nhiều trạm trong private network được chuyển đổi tương ứng thành các gói tin TCP/UDP gửi đi từ 1 địa chỉ IP mặt ngoài của gateway và với các Port khác nhau ➔ hỗ trợ đồng thời nhiều trạm trong private network kết nối public Internet



NAT lồng nhau (nested)

- Vì vấn đề thiếu địa chỉ IP (IPv6 đang xử lý bằng cách tăng độ dài lên gấp 4 lần, tức là tăng không gian địa chỉ IP lên gấp 2^{24} lần) ➔ ISP cũng dùng NAT để kết nối các thuê bao của mình ra Internet với địa chỉ IP_1
- Office kết nối ISP và sử dụng NAT với địa chỉ IP_2
- Mạng LAN của một phòng ban nào đó bên trong Office dùng NAT để kết nối ra bên ngoài với IP_3 (ví dụ trong bài thực hành, hệ thống mạng ảo kết nối với máy host và dùng NAT để kết nối Internet thông qua máy host)
- NAT lồng nhau:
  - Máy A kết nối với máy X thì gói tin IP được áp dụng NAT lần lượt tại các gateway
  - NAT lồng nhau trong suốt đối với các máy trạm, và không bị giới hạn số mức lồng nhau

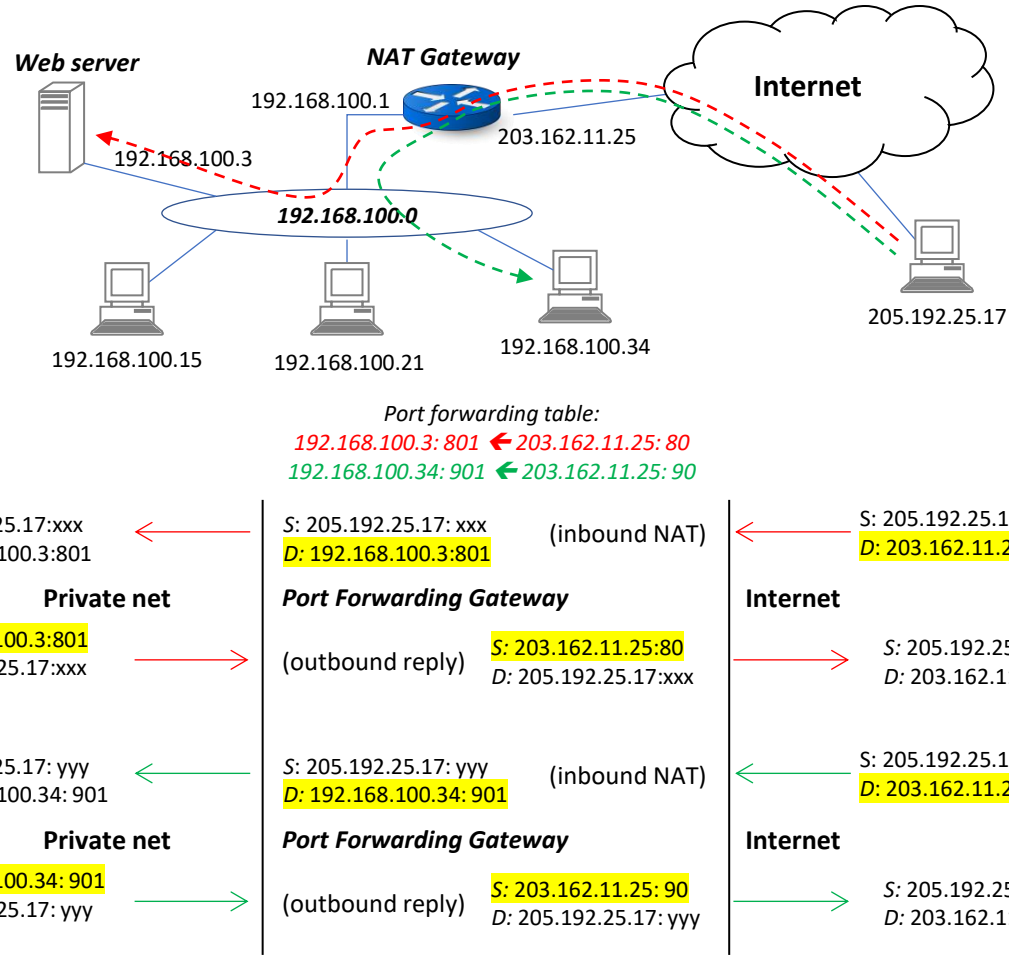


NAT & NAPT Discussion

- NAT & NAPT hoạt động ở tầng 3&4 ➔ độc lập với tầng ứng dụng (cho phép mọi ứng dụng kết nối từ private network ra public Internet)
- Cơ chế chuyển đổi địa chỉ IP và Port nằm trong header của các gói tin ➔ trong suốt với ứng dụng (vốn chỉ quan tâm đến gửi/nhận phần dữ liệu của gói tin)
- Đối với các ứng dụng có xử lý liên quan đến Port hay IP address (ví dụ FTP có cơ chế tạo kênh truyền dữ liệu và thông báo thông số kênh truyền này bằng gói tin FTP) ➔ NAT & NAPT không đáp ứng được
- NAT & NAPT chỉ hỗ trợ kết nối ra (outbound) cho private network. Tức là một trạm bên trong private network chủ động gửi gói tin đến trạm ngoài public Internet và nhận gói tin trả lời. Đối với các kết nối từ public Internet vào private network (inbound), ví dụ kết nối từ trạm ngoài public Internet vào một server đặt trong private network, NAT & NAPT không đáp ứng được

NAT Port Forwarding

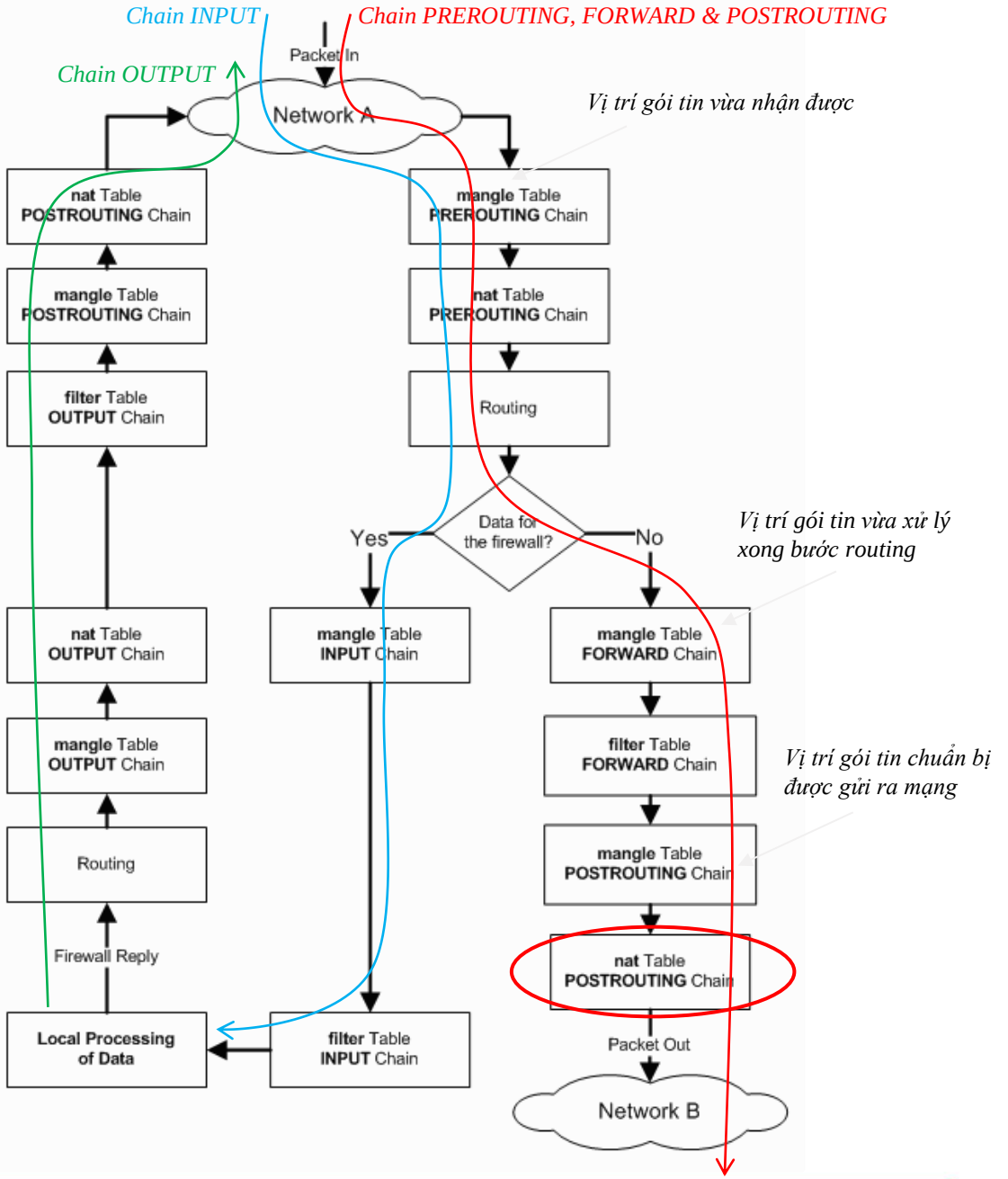
- Cho phép triển khai kết nối chủ động từ bên ngoài public Internet tới bên trong private network ➔ thường áp dụng khi private network có dịch vụ cần cung cấp cho bên ngoài public Internet sử dụng (ví dụ một web server)
- Port Forwarding (còn gọi là “Port Mapping”) hoạt động theo cơ chế ánh xạ một cổng dịch vụ trên mặt ngoài của gateway đến cổng một dịch tại một trạm nội bộ private network
- Cấu hình port forwarding được thiết lập trước trên gateway. Khi xuất hiện gói tin đi vào private network từ public Internet, luật anh xạ phù hợp sẽ được gateway áp dụng để thay đổi địa chỉ IP đích và Port khi chuyển tiếp gói tin từ mặt ngoài vào mặt trong



Linux *iptables* (nhắc lại)

- Cài đặt sẵn trong kernel Linux, xử lý gói tin theo dòng (chain) đi vào card mạng #1 & đi ra card mạng #2
- Chain:
  - INPUT, OUTPUT
  - PREROUTING, FORWARD, POSTROUTING
- Các luật (rule) được khai báo tại các vị trí trên chain để áp dụng để xử lý gói tin
- Rule có thể là cấm (reject), ghi lại thông tin (log), sửa đổi địa chỉ IP – NAT, v.v…
- Các rule được gộp với nhau theo mục đích sử dụng tạo thành các bảng (table)
- Table:
  - nat !!!

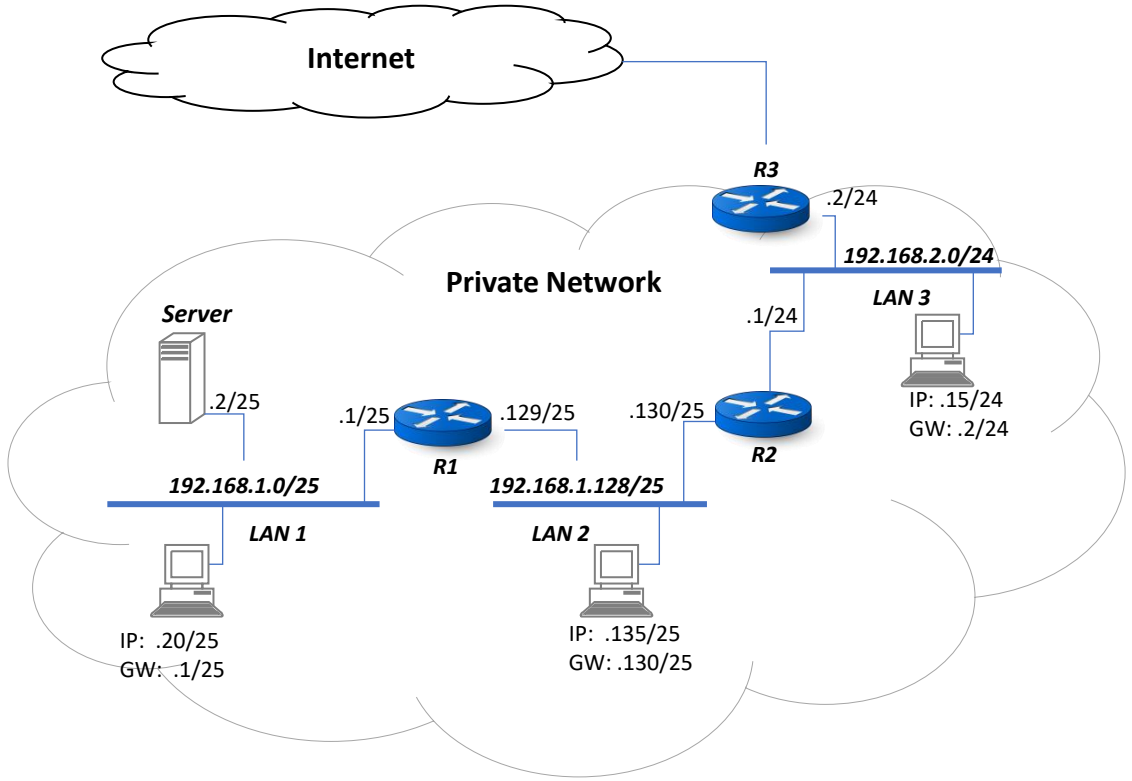
MASQUERADE là action cài đặt sẵn trong iptables thực hiện cơ chế NAT. Để bật action này tại vị trí POSTROUTING trên kết nối mạng eth1:
> iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE



thực hành:

NAT & Port Forwarding

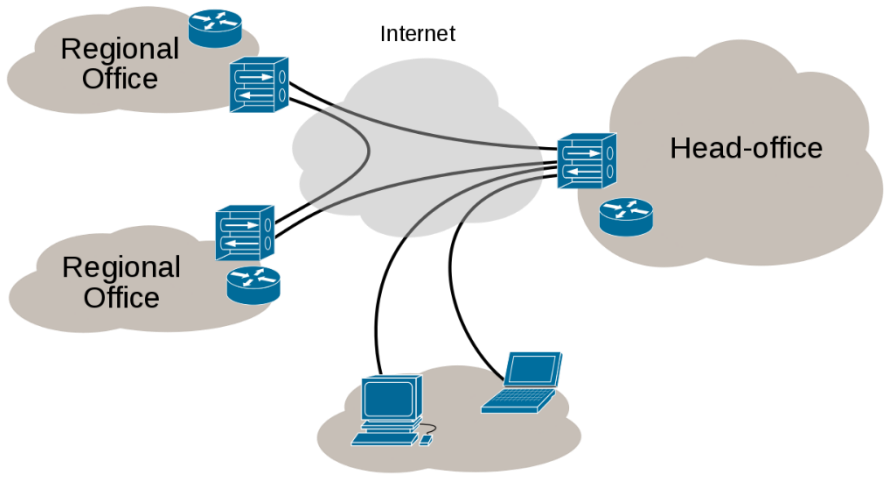
- Cấu hình R3 trong VirtualBox có một Network Adapter kiểu NAT để kết nối được với Internet qua máy host
- Cấu hình hệ thống private network gồm có các router R1, R2 liên kết các LAN như. Kiểm tra các trạm trên các LAN liên lạc được với nhau và lấy R3 làm gateway cho private network
- Cấu hình NAT trên R3 để tất cả các trạm trong LAN1, LAN2, LAN3 đều kết nối được Internet
- Cấu hình Port Forwarding trên R3 để máy host (đóng vai trò là một trạm làm việc bên ngoài private network) truy nhập đến server nằm trong LAN1



Virtual Private Network (VPN)

Virtual Private Network (VPN)

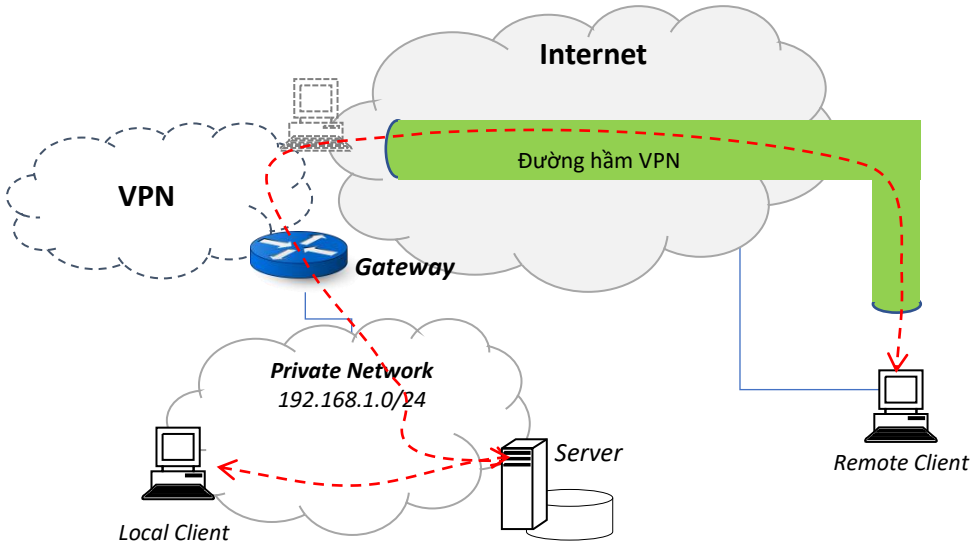
- Nhu cầu làm việc từ xa, làm việc tại mọi nơi mọi lúc, v.v.. trở nên khả thi với việc Internet có mặt khắp nơi. Vấn đề cần giải quyết là người sử dụng cần truy nhập được đến các tài nguyên của họ, vốn được lưu trữ và bảo vệ tại private network nơi họ làm việc ➔ VPN là giải pháp
- Mạng riêng ảo VPN được hình dung như là một mạng riêng (private network) của một tổ chức nào đó, mà sử dụng mạng công cộng để kết nối các trạm làm việc ở xa hoặc các chi nhánh tổ chức ở xa, với các tiêu chí :
  - *Bảo mật (confidentiality):* Dữ liệu của private network truyền trên mạng public phải được mã hóa, tránh bị nghe trộm gói tin và có thể giải mã để đánh cắp dữ liệu.
  - *Xác thực (authentication):* Đảm bảo quyền truy cập của người dùng vào các tài nguyên trong private network, đồng thời ngăn chặn giả mạo truy cập vào tài nguyên của private network.
  - *Toàn vẹn (integrity):* Chống giả mạo dữ liệu, hoặc thay đổi dữ liệu của private network khi di chuyển trên mạng công cộng



Mạng riêng ảo (VPN) sử dụng mạng công cộng Internet nguồn: Wikipedia

Host-to-net VPN

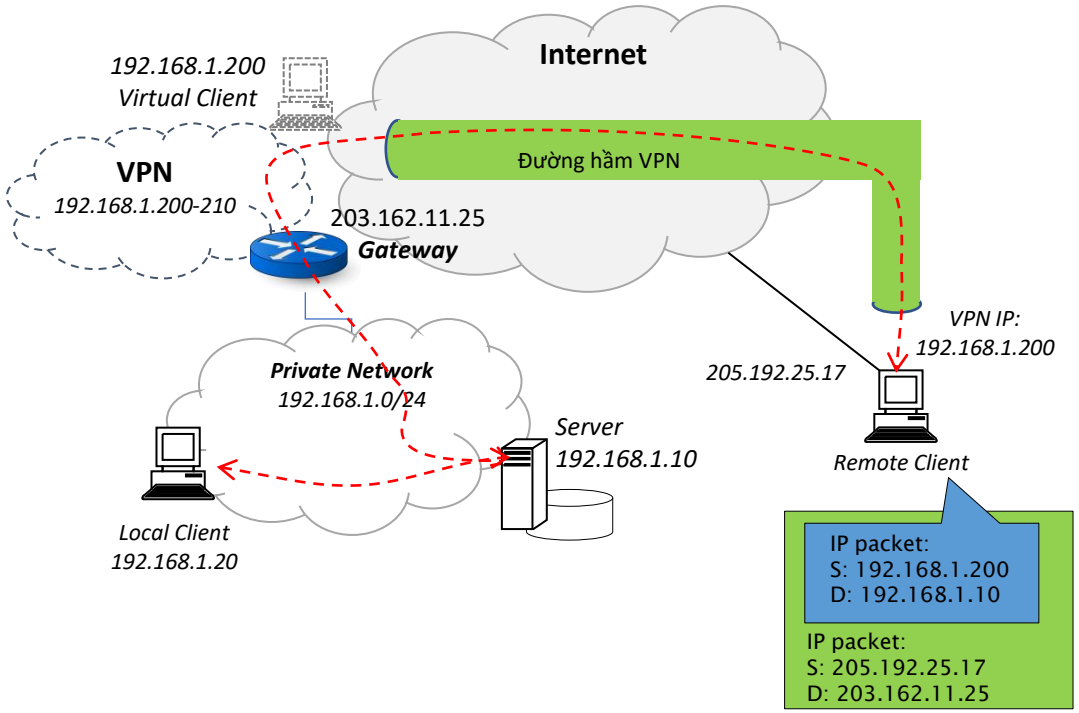
- Mục đích sử dụng của host-to-net VPN là hỗ trợ người dùng đơn lẻ ở xa, kết nối vào private network thông qua mạng công cộng
- Công nghệ phổ biến của host-to-net là tạo ra một mạng ảo (VPN) nằm phía trong gateway, đồng thời gateway hỗ trợ thêm chức năng truy nhập từ xa (remote access). Remote client khi remote access vào gateway được đại diện bằng một "virtual client" nằm trong VPN
- Server quản lý tài nguyên của private network không phân biệt local client với VNP client (kết nối với VPN) do các client này đều nằm phía trong gateway ➔ truy nhập đến private resource được cho phép
- Cơ chế đường hầm[1] (tunnel) được sử dụng để kết nối an toàn giữa virtual client với remote client trên mạng public Internet nhằm tự động vận chuyển tất cả các gói tin nội bộ private network đến remote client



[1] https://en.wikipedia.org/wiki/IP_tunnel

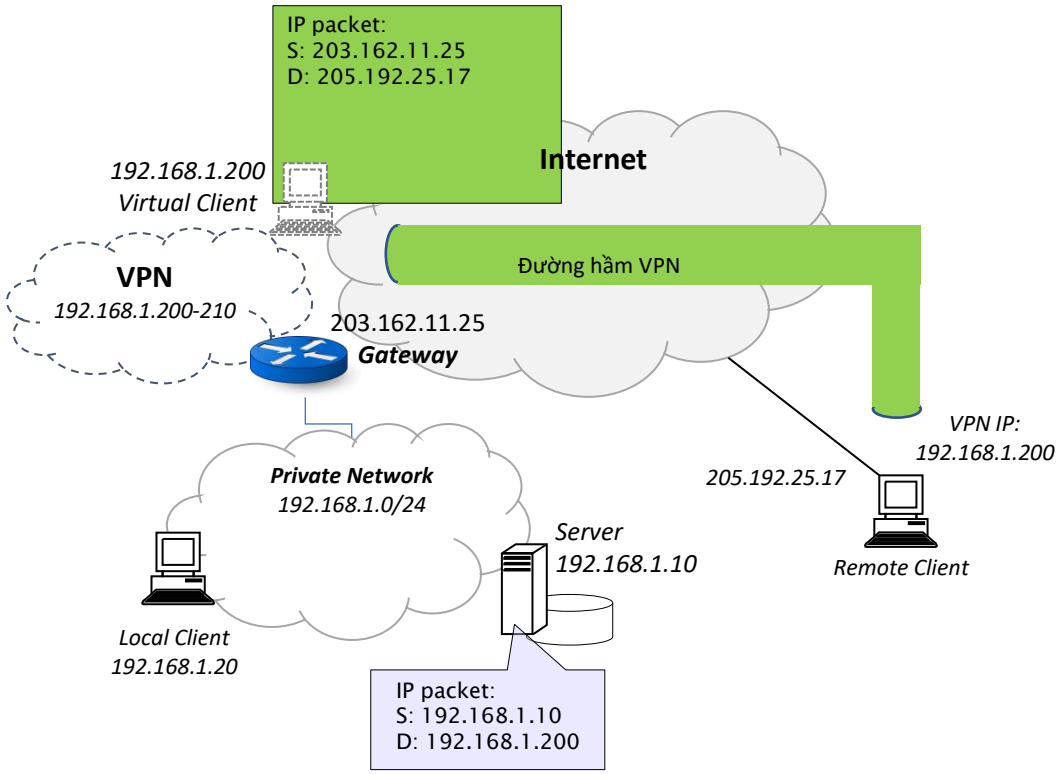
Host-to-net VPN demo

1. Private network kết nối Internet qua gateway. Cấu hình một phần địa chỉ IP phục vụ remote access và thiết lập VPN theo dải địa chỉ này
2. Remote client kết nối Internet & remote access gateway để login vào VPN
3. Login VPN thành công ➔ remote client được gán thêm một địa chỉ IP trong dải VNP IP đã chuẩn bị (gọi là VPN IP) để truy nhập đến các tài nguyên của private network. Phía VPN, gateway sau khi cấp địa chỉ VPN IP sẽ tạo ra một "agent" (virtual client) có đia chỉ trùng với VPN IP này để nhận các gói tin trong private network mà gửi đến remote client
4. Gateway và remote client thiết lập một đường hầm IP để chuyển tiếp các gói tin private network đến remote client thôn qua mạng public Internet
5. Remote client sử dụng VNP IP để gửi yêu cầu truy nhập đến private resource như một trạm trong private network.
6. Yêu cầu này được "bọc" trong một gói tin IP có địa chỉ nguồn là remote client và đích là gateway để chuyển qua Internet đến private network
7. Gói tin IP được mã hóa (phần data) và gửi qua Internet đến gateway ➔ cơ chế đường hầm
8. Gateway mở gói tin, lấy phần data ➔ nhận được gói tin remote client đã gửi để yêu cầu truy nhập đến resource trong private network
9. Chuyển gói tin vào private network để đến được server quản lý resource
10. Server nhận gói tin, xử lý yêu cầu của remote VPN client như một client trong private netwrok



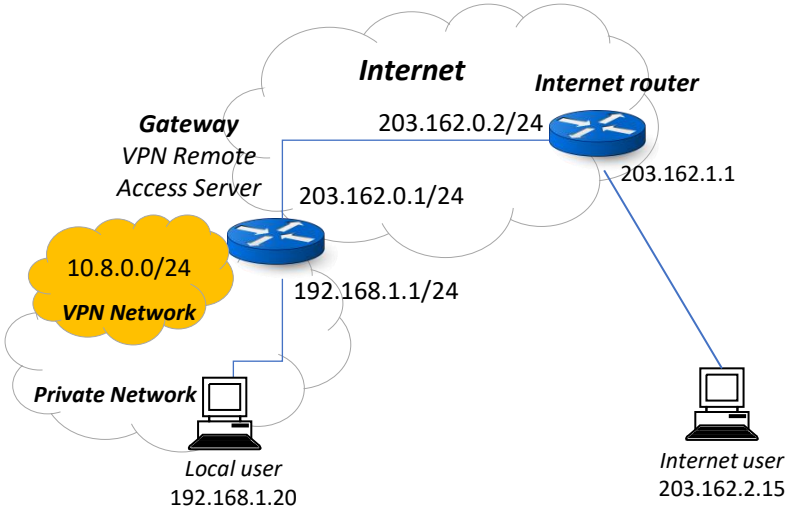
Host-to-net VPN demo (tiếp)

1. Server xử lý yêu cầu của VPN client, gửi kết quả cho client bằng gói tin IP với các địa chỉ IP private
2. Gói tin IP chuyển trong private network từ server và được virtual client nhận xử lý
3. Gói tin này được mã hóa và đưa vào phần data của một gói tin IP khác với địa chỉ nguồn là gateway và đích là remote client
4. Theo cơ chế đường hầm, gói tin bọc bên ngoài được chuyển đến remote client thông qua mạng public Internet
5. Remote client nhận được gói tin từ đường hầm, lấy ra phần data lại thu được gói tin gốc mà server trả lời trong bước 1
6. Remote client lấy phần data của gói tin và chuyển cho ứng dụng đã ra yêu cầu truy nhập tài nguyên của private network. Kịch bản truy nhập tài nguyên của private network từ remote client kết thúc ở đây.



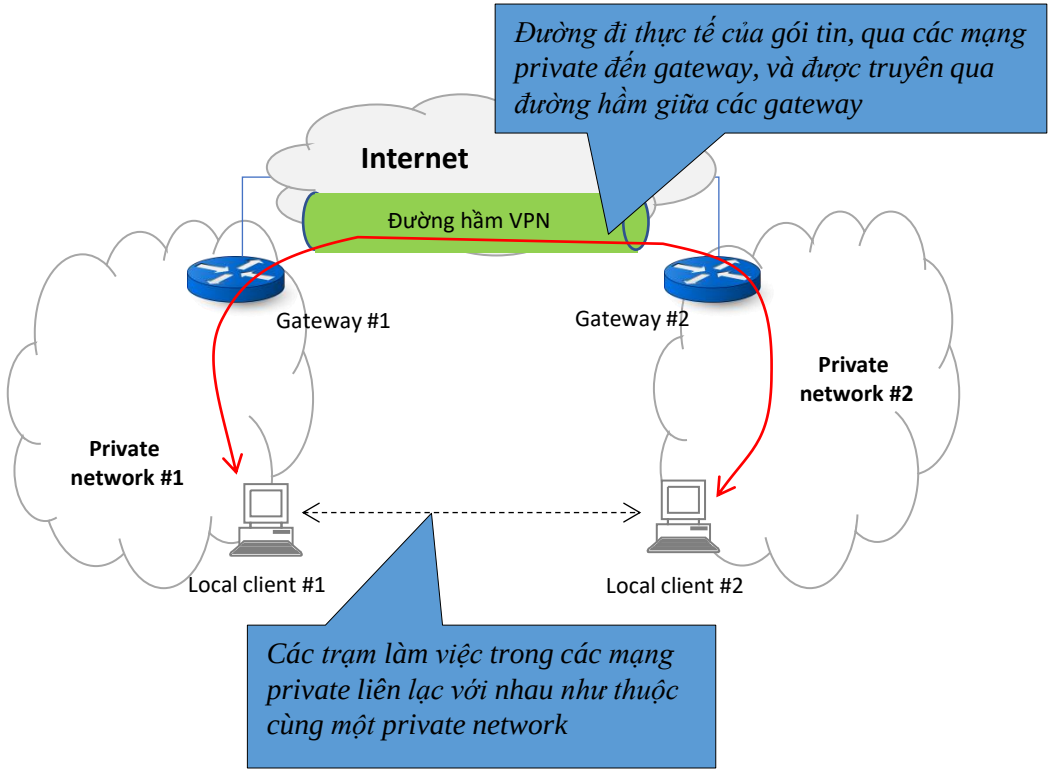
thực hành: host-to-net VPN

- Tham khảo https://users.soict.hust.edu.vn/hoangph/textbook/ch06-5.html
- Tạo mạng Internet và Private Net giả lập với Internet user và Local user
- Cài đặt OpenVPN server trên máy Gateway
- Tạo file xác thực cho Internet user
- Cài đặt OpenVPN client trên máy Internet user
- Kết nối VPN sử dụng file xác thực đã được tạo ra
- Kiểm tra kết nối giữa Internet user với Local user
- Kiểm tra các gói tin đi qua Internet router để hiểu cơ chế đường hầm



Net-to-net VPN

- Mục đích sử dụng của net-to-net VPN là kết nối nhiều mạng private với nhau thông qua mạng public Internet để trở thành một mạng private đồng nhất. Người sử dụng ở các mạng private khác nhau có thể kết nối với nhau giống như trong một mạng private mà không cần cơ chế remote login như mô hình host-to-net
- Mô hình net-to-net thường được triển khai để kết nối chiều chi nhánh của một tổ chức nằm phân tán cách xa nhau mà không cần duy trì một hệ thống mạng riêng để kết nối các chi nhánh này
- Một trong những công nghệ triển khai net-to-net VPN cũng là cơ chế đường hầm IP được thiết lập sẵn giữa các gateway của các private network.



[1] https://en.wikipedia.org/wiki/IP_tunnel

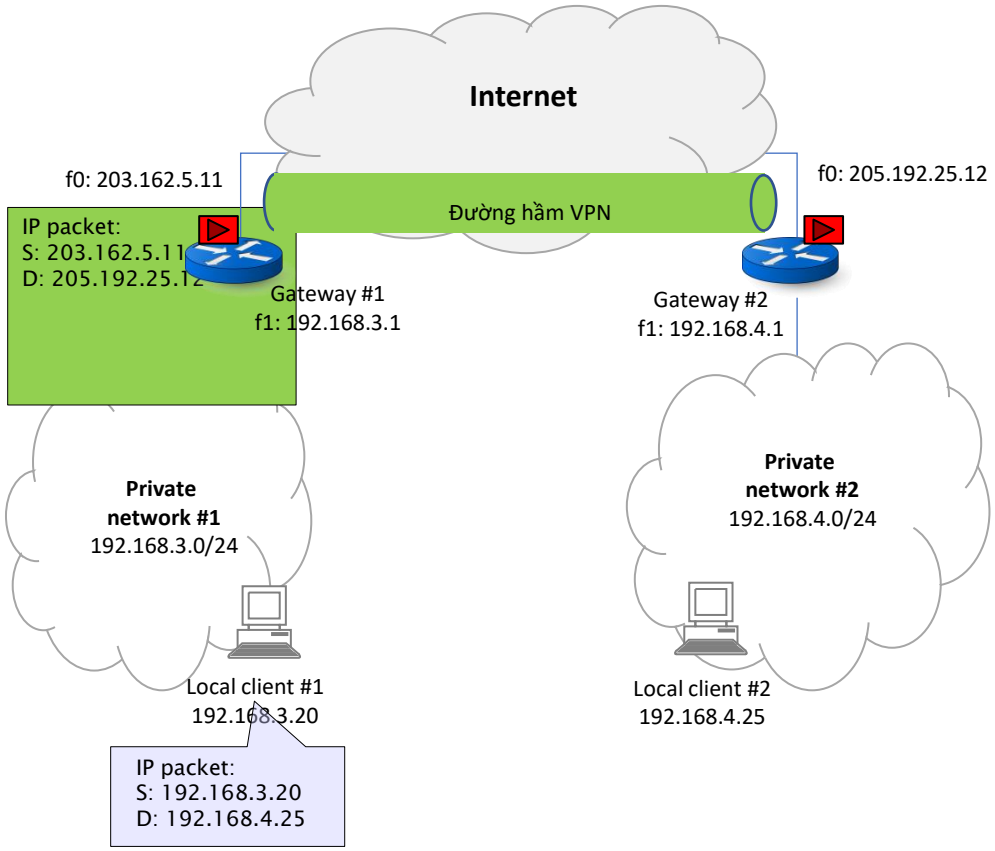
Net-to-net VPM demo

1. Công ty có 2 private net. #1 & #2 sử dụng các dải địa chỉ IP private và kết nối Internet qua các gateway (bằng NAT chẳng hạn). Công ty muốn "gộp" 2 private net. này thành một VPN, để các trạm trên 2 private net có thể liên lạc với nhau bằng các địa chỉ IP private (và như vậy có thể truy nhập đến các tài nguyên private của nhau)
2. Đường hầm IP được thiết lập với 2 đầu là 2 địa chỉ mặt ngoài của các gateway nhằm mục đích chuyên chở các gói tin IP giữa 2 private net
3. Routing table của các gateway có cấu hình đặc biệt: đường đi đến private net ở xa được thiết lập với next hop là "cửa ra" của đường hầm:

```
Gateway #1:
192.168.3.0 → f1 (0.0.0.0)
192.168.4.0 → tunnel (f0)
```

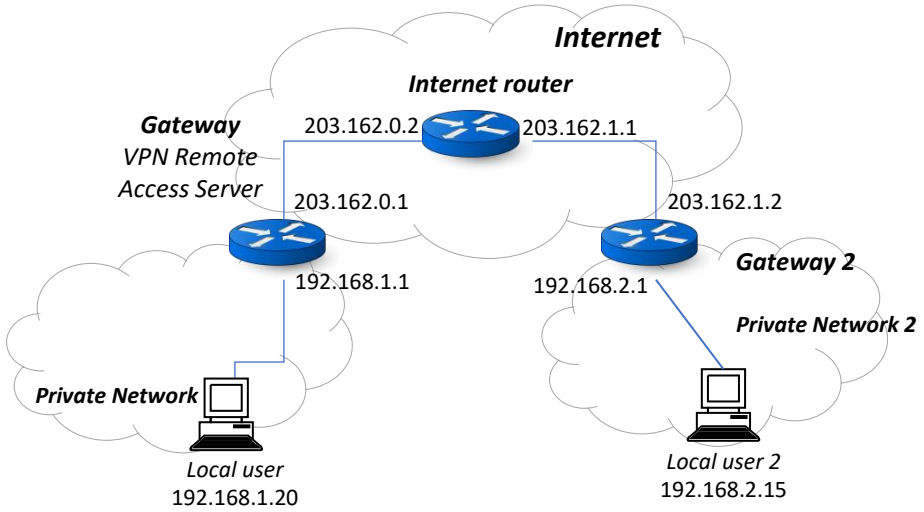
```
Gateway #2:
192.168.4.0 → f1 (0.0.0.0)
192.168.3.0 → tunnel (f0)
```

4. Các gateway được cài đặt thêm các VPN agent để xử lý routing cho trường hợp gói tin cần gửi đến private net ở xa (các agent này thường được cài đặt trong gói phần mềm hỗ trợ VPN)
5. Client #1 yêu gửi gói tin IP đến client #2 nằm trong private net ở xa
6. Gói tin được gửi đến gateway #1. Gateway xử lý theo routing table và chuyển tiếp gói tin vào đường hầm.
7. Ở cửa vào đường hầm, VPN agent nhận gói tin từ client #1 và bọc nó trong một gói tin IP khác rồi chuyển qua đường hầm đến gateway #2
8. VPN agent ở cửa ra đường hầm trên gateway #2 nhận được gói tin gửi qua đường hầm, bóc header để nhận gói tin gốc mà client #1 đã gửi, chuyển gói tin này vào mặt trong của gateway #2 để chuyển đến client #2



thực hành: net-to-net VPN

- Tham khảo https://users.soict.hust.edu.vn/hoangph/textbook/ch06-5.html
- Tạo mạng Internet và Private Net giả lập với Internet user và Local user
- Cài đặt OpenVPN server trên máy Gateway
- Tạo file xác thực cho Internet user
- Cài đặt OpenVPN client trên máy Internet user
- Kết nối VPN sử dụng file xác thực đã được tạo ra
- Kiểm tra kết nối giữa Internet user với Local user
- Kiểm tra các gói tin đi qua Internet router để hiểu cơ chế đường hầm



203.162.1.2$ route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.0.2.2	0.0.0.0	UG	100	0	0	enp0s3
10.9.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	tun0
192.168.1.0	10.9.0.1	255.255.255.0	UG	0	0	0	tun0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s10
203.162.0.0	203.162.1.1	255.255.255.0	UG	0	0	0	enp0s9
203.162.1.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s9

192.168.2.15$ tracepath -n 192.168.1.20

1?: [LOCALHOST]	pmtu 1500
1: 192.168.2.1	0.803ms
1: 192.168.2.1	0.493ms
2: 10.9.0.1	2.695ms
3: 192.168.1.20	3.142ms reached

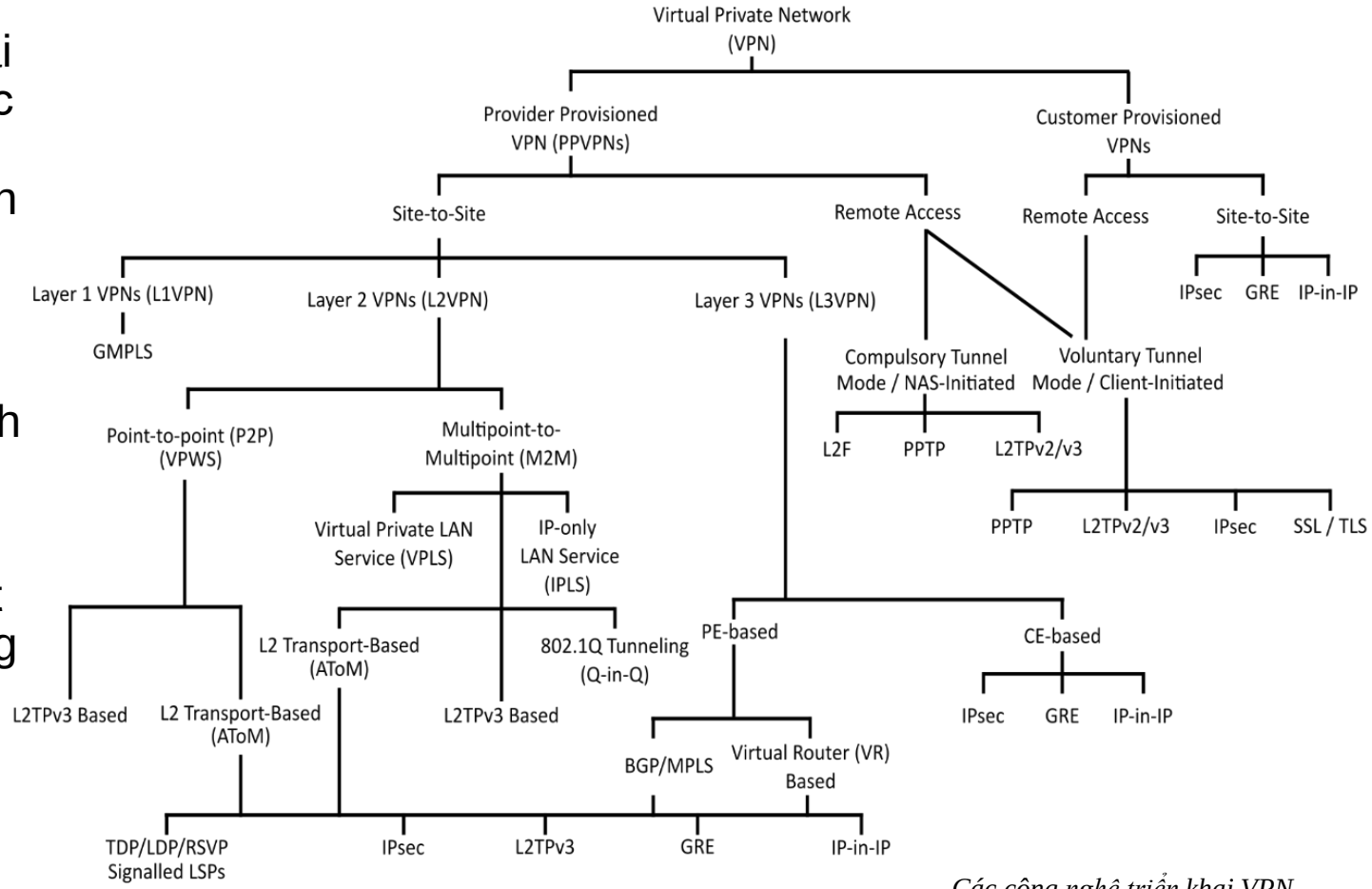
Resume: pmtu 1500 hops 3 back 3

192.168.2.15$ ping 192.168.1.20

PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=62 time=3.46 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=2.99 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=3.19 ms

Các công nghệ triển khai VPN

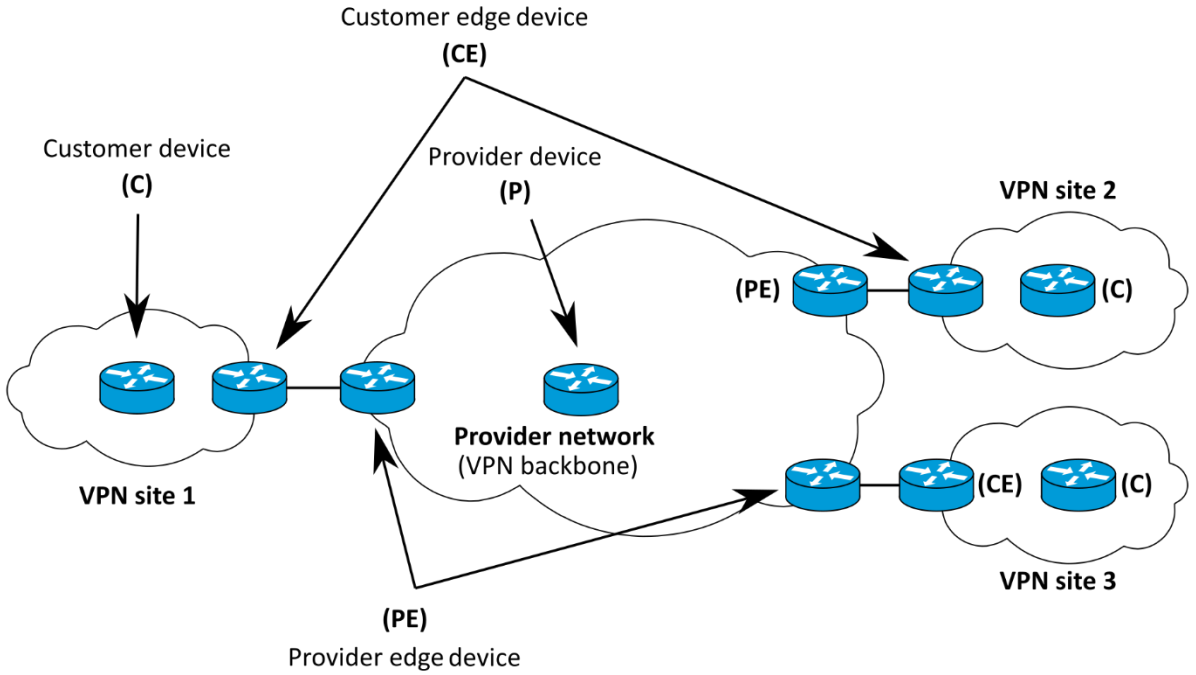
- Công nghệ đường hầm IP để triển khai VPN chỉ là một ví dụ. VPN có thể được triển khai bằng rất nhiều công nghệ khác, và tại các tầng dưới IP hoặc trên IP
- Triển khai VPN phía người dùng (customer provisioned): admin của private network tự thiết lập và vận hành VPN
- Triển khai VPN phía nhà cung cấp (provider provisioned): VPN được thiết lập và vận hành với sự hỗ trợ của công ty cung cấp đường truyền (ví dụ các ISP)



Các công nghệ triển khai VPN
nguồn: Wikipedia

Triển khai VPN phía nhà cung cấp

- Internet phổ cập toàn cầu và nền kinh tế đòi hỏi công ty phải tổ chức phân tán/cộng tác khiến VPN trở nên cần thiết như một hạ tầng kết nối chuẩn ➔ mô hình triển khai VPN được các nhà cung cấp dịch vụ mạng chuẩn hóa để đáp ứng nhanh nhu cầu từ công ty
- Nhà cung cấp VPN xây dựng hệ thống VPN backbone của mình dựa trên nền tảng Internet và bán dịch vụ VPN cho các công ty
- Private network của các công ty kết nối vào VPN backbone tại điểm truy nhập dịch vụ VPN được triển khai bằng cặp thiết bị Provide edge device (PE) và Customer edge device (CE)
- Tại Việt Nam hiện cũng đã có nhiều nhà cùng cấp dịch vụ VPN độc lập với các ISP *(Google: "top VPN provider in Viet Nam")*



Các thành phần kết nối VPN theo mô hình Provider Provisioned nguồn: Wikipedia

Kết nối dịch vụ với Internet

Kết nối tầng giao vận & các dịch vụ

Qui hoạch public server trong mạng private

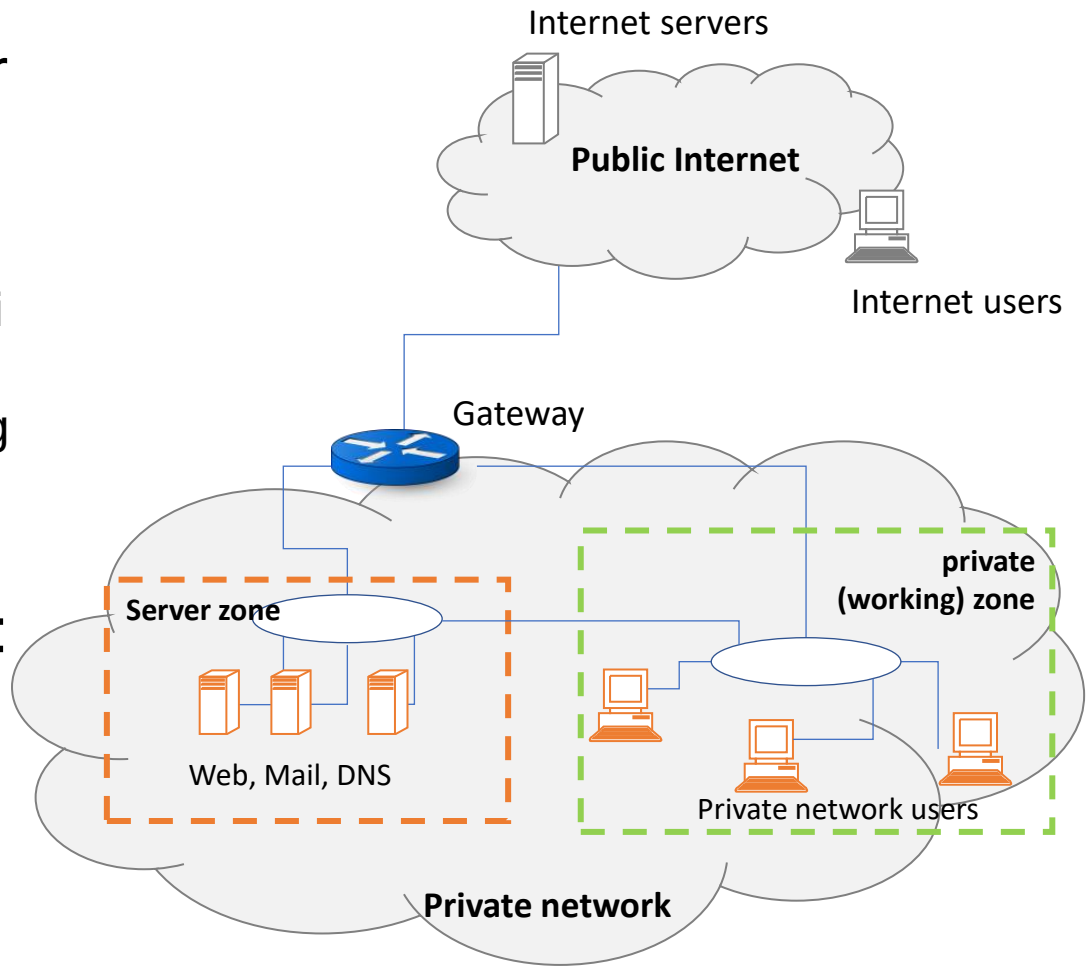
Dịch vụ IP cơ bản: DNS, Mail, FTP

Dịch vụ IP cơ bản và dịch vụ giao vận

Dịch vụ	**Giao thức tầng ứng dụng**	**Giao thức tầng giao vận**
domain name	DNS	UDP
e-mail	SMTP	TCP
remote terminal access	Telnet	TCP
Web	HTTP	TCP
file transfer	FTP	TCP
streaming multimedia	giao thức riêng (e.g. RealNetworks)	TCP or UDP
Internet telephony	giao thức riêng (e.g., Vonage,Dialpad)	thường là UDP

Qui hoạch public server trong mạng private

- Private servers được qui hoạch trong một vùng riêng của mạng private, gọi là server zone
- Truy nhập đến private servers:
  - Từ người dùng trong mạng private (theo đường nội bộ, an toàn, tin cậy)
  - Từ người dùng trên Internet (không an toàn, không tin cậy)
  - Từ các server trên Internet (an toàn, tin cậy)
- Truy nhập đến các public Internet servers:
  - Từ người dùng trong mạng private
  - Từ các server trong mạng private



Nhắc lại khái niệm dịch vụ DNS

- Tên miền: định danh trên tầng ứng dụng cho các nút mạng
  - Trên Internet được quản lý tập trung
  - Quốc tế: ICANN
  - Việt Nam: VNNIC
- DNS (Domain Name System): hệ thống tên miền gồm các máy chủ quản lý thông tin tên miền và cung cấp dịch vụ DNS
- Vấn đề phân giải tên miền sang địa chỉ IP
  - Người sử dụng dùng tên miền để truy cập dịch vụ
  - Máy tính và các thiết bị mạng không sử dụng tên miền mà dùng địa chỉ IP khi trao đổi dữ liệu
- Làm thế nào để chuyển đổi tên miền sang địa chỉ IP?

Chuyển đổi địa chỉ và ví dụ

- Máy tính dùng địa chỉ IP
- NSD dùng tên miền

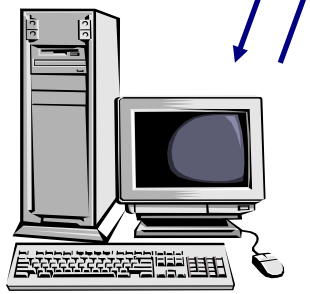
Cần có chuyển đổi địa chỉ

NSD

Tôi muốn vào địa chỉ
www.soict.hust.edu.vn

Mời truy cập vào
202.191.56.65

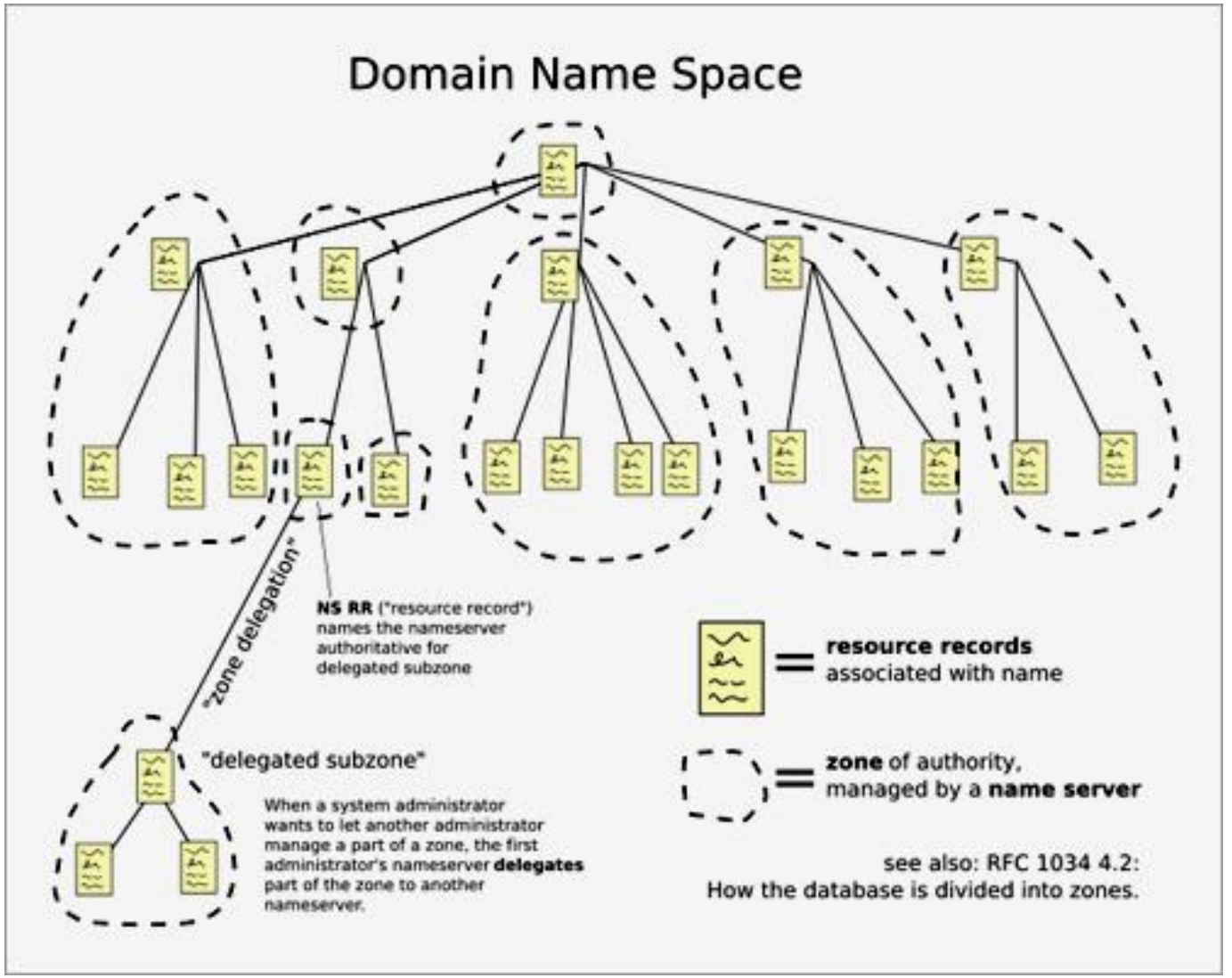
Máy chủ tên miền



Máy chủ web
202.191.56.65

Không gian tên miền

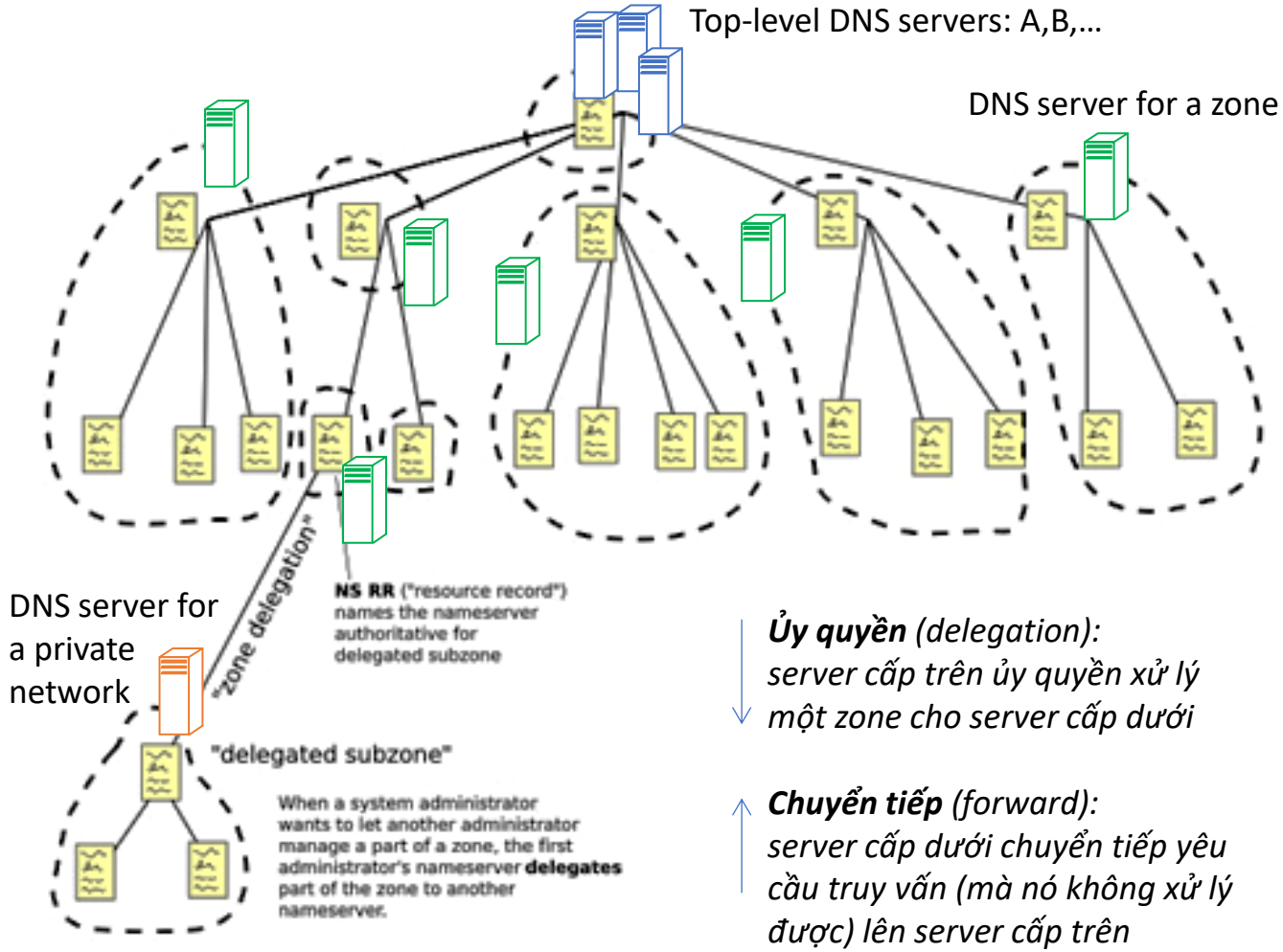
- Kiến trúc : hình cây
  - Root: Nút gốc
  - Chia thành các zone
- Mỗi nút là một tập hợp các bản ghi mô tả tên miền tương ứng với nút đó. Ví dụ:
  - SOA
  - NS
  - A
- Các tên miền “mới”
  - Top level
  - daotao.ai
  - zalo.me



Hình ảnh từ: Wikipedia

Internet DNS servers & private DNS server

- Dịch vụ tên miền Internet đang được cung cấp bởi sự kết hợp của các top-level DNS servers và các DNS servers của các zone
- Mạng nội bộ bổ sung DNS server để xử lý các tên miền nội bộ
- Khai báo “forward” để xử lý truy vấn tên miền Internet (mà server nội bộ không có khả năng)
- Xin “delegate” zone private để server cấp trên ủy quyền dữ liệu zone private này cho server nội bộ
- Cần cơ chế xác thực giữa server private với server cấp trên trực tiếp



Ủy quyền *(delegation): server cấp trên ủy quyền xử lý một zone cho server cấp dưới*

Chuyển tiếp *(forward): server cấp dưới chuyển tiếp yêu cầu truy vấn (mà nó không xử lý được) lên server cấp trên*

Bài thực hành DNS

- https://users.soict.hust.edu.vn/hoangph/textbook/ch04-1.html
- Thiết lập DNS giả lập hệ thống của Internet Việt Nam: có tương tác với top-level DNS servers, phục vụ zone “.vn”
- Thiếp lập 2 DNS cấp dưới phục vụ zone “.edu.vn” và “.com.vn”
- Thiếp lập DNS phục vụ private zone “hust.edu.vn”, kết nối vào server “.edu.vn”
- Khai báo các host nội bộ của zone “.hust.edu.vn”
- Xử lý host public www.hust.edu.vn trong zone nội bộ và public Internet

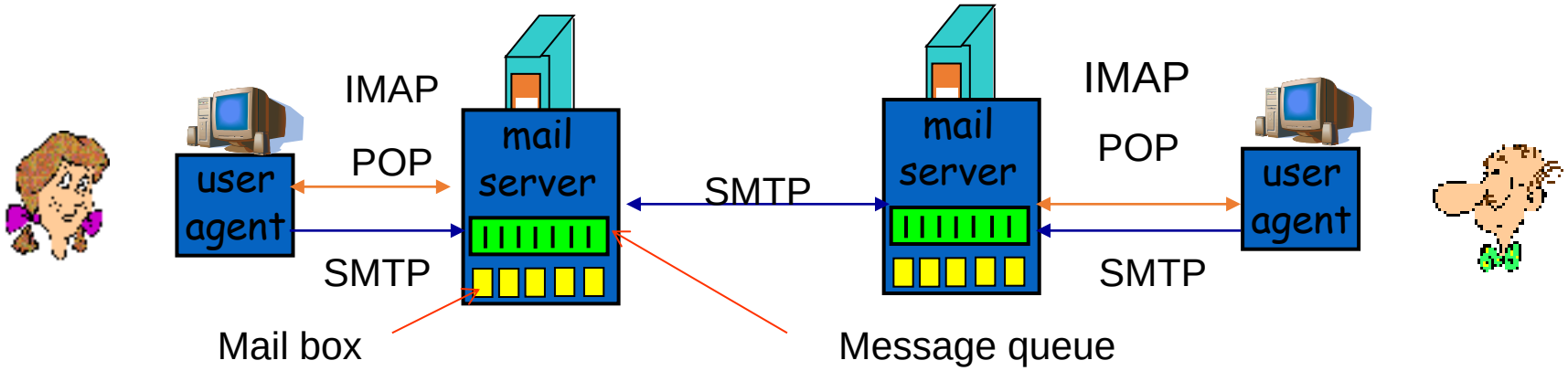
Một số xử lý mở rộng DNS

- Cân bằng tải dựa trên DNS
- Dịch vụ top-level DNS

Dịch vụ thư điện tử (Email)

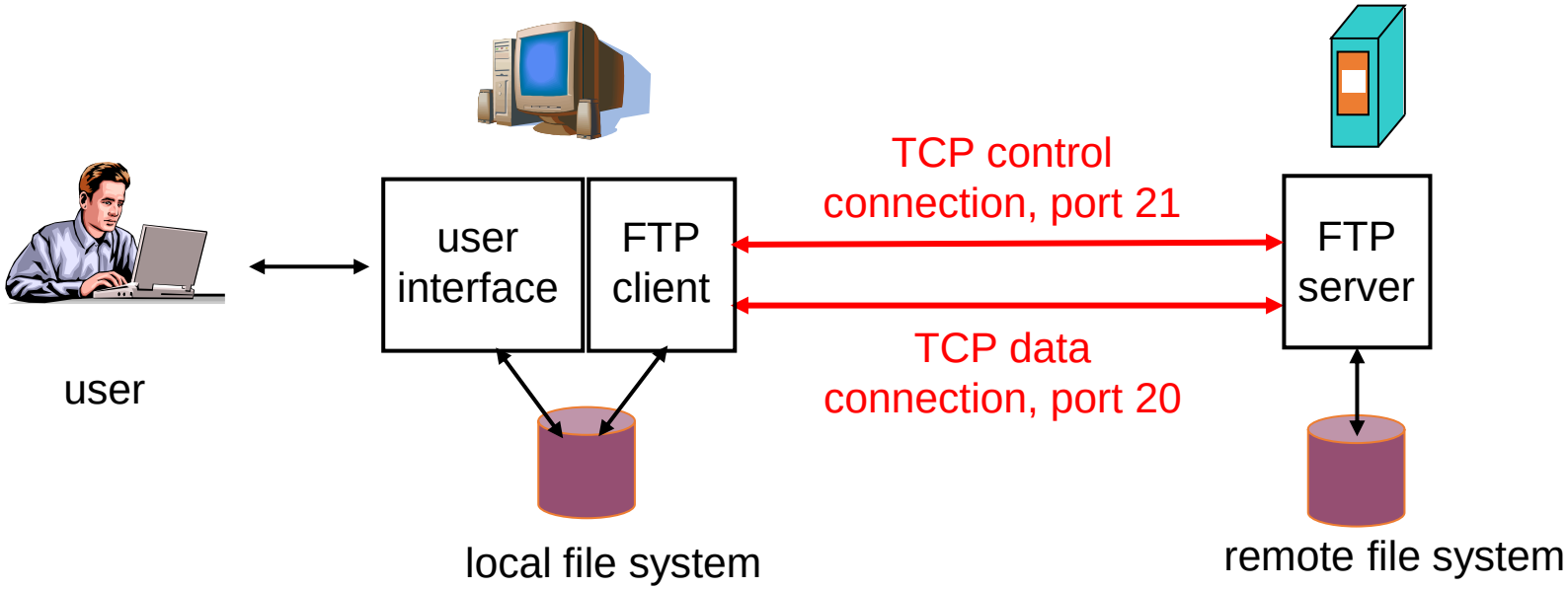
- MUA (Mail User Agent)
  - Lấy thư từ máy chủ
  - Gửi thư đến máy chủ
  - VD: Outlook, Thunderbird…
- MTA (Mail Transfer Agent): :
  - Chứa hộp thư đến của NSD (mail box)
  - Hàng đợi để gửi thư đi
  - VD: Sendmail, MS Exchange…

- Giao thức:
  - Chuyển thư: SMTP-Simple Mail Transfer Protocol
  - Nhận thư
    - POP – Post Office Protocol
    - IMAP – Internet Mail Access Protocol



Triển khai Email trong mạng nội bộ

Dịch vụ truyền file: File Transfer Protocol (FTP)



- Mô hình Client-server
- Trao đổi file giữa các máy
- Sử dụng TCP, cổng dịch vụ 20, 21

- Điều khiển Out-of-band :
  - Lệnh của FTP : cổng 21
  - Dữ liệu: cổng 20
- Người dùng phải đăng nhập trước khi truyền file
- Một số server cho phép người dùng với tên là anonymous

Đảm bảo an toàn mạng nội bộ

Qui hoạch các vùng an toàn trong mạng nội bộ

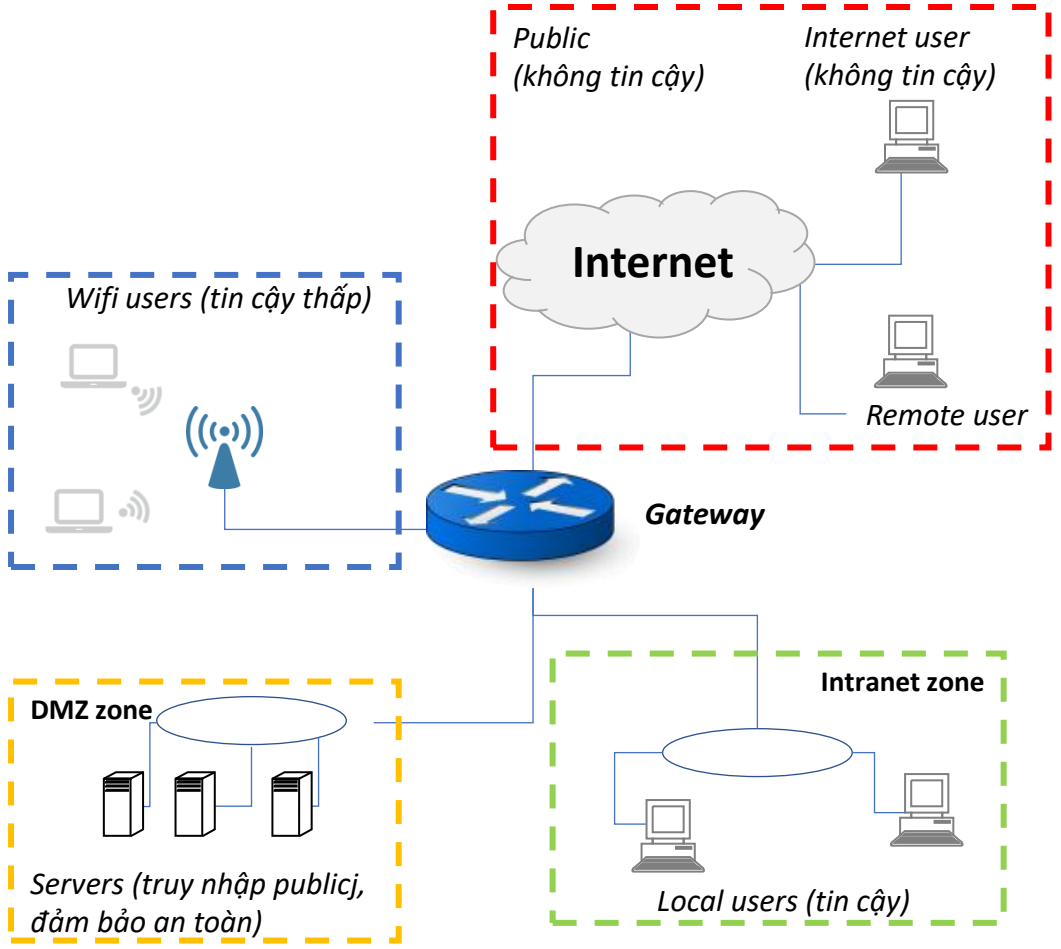
Tường lửa (firewall)

Phát hiện & chống xâm nhập (IDS, IPS)

Qui hoạch các vùng mạng nội bộ

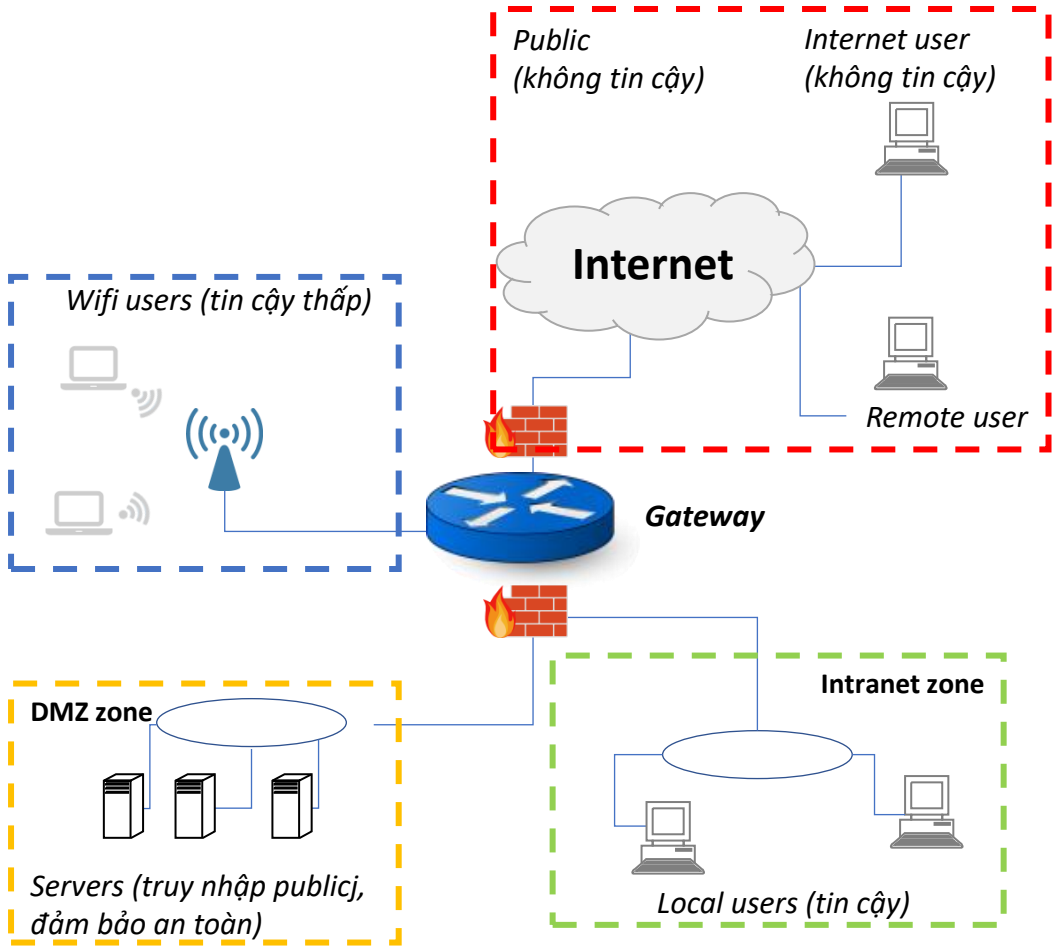
- Mục đích
  - "Nhóm" các trạm làm việc để xử lý đảm bảo an toàn cùng nhau
  - Các trạm làm việc trong cùng nhóm có nguy cơ bảo mật như nhau
  - Nhóm "không dây", nhóm "máy chủ", nhóm "trạm làm việc an toàn", v.v..

- Phương pháp chia nhóm thông thường:
  - "Green": các trạm làm việc tin cậy, kết nối có dây, kiểm soát tối đa (ra/vào mạng, cài đặt phần mềm, virus, v.v..)
  - "Orange": còn gọi là DMZ, vùng truy nhập tranh chấp giữa private và public. Nơi kết nối server
  - "Blue": vùng wifi. Không kiểm soát kết nối mạng vật lý
  - "Red": vùng public, không tin cậy



Tường lửa (Firewall)

- Đặt tại vị trí kiểm soát được kết nối giữa các vùng đã qui hoạch
- Đặc biệt quan tâm đến vùng Green và Red
- Tùy vào thiết kế hình trạng của mạng nội bộ để quyết định vị trí đặt tường lửa
  - Phía ngoài Gateway, kết nối với public Internet
  - Kết nối giữa vùng Green và DMZ
- Nguyên tắc hoạt động
  - Luật kiểm soát giao thông giữa các vùng: cho phép (grant) hoặc cấm (deny)
  - Mặc định cấm + các luật cho phép
  - Mặc định cho phép + các luật cấm

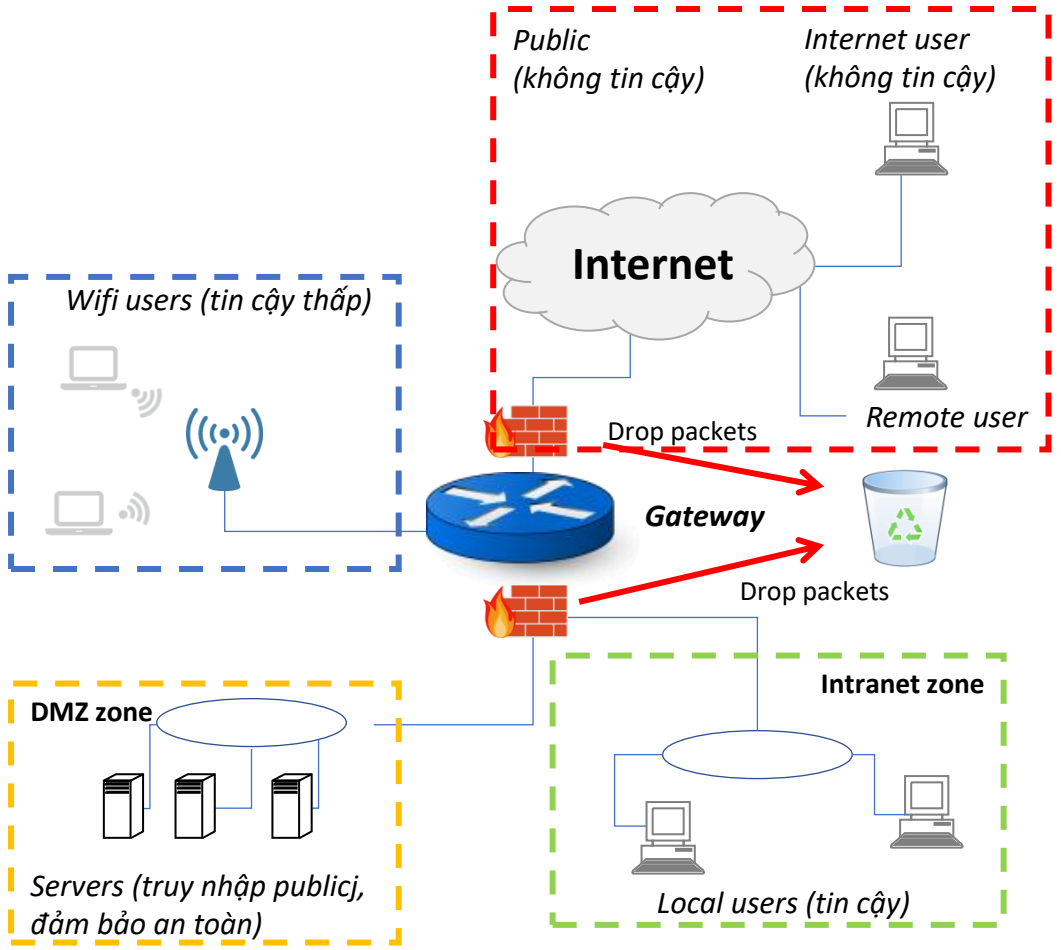


Các loại tường lửa

- Tường lửa kiểu cổng lọc gói tin (packet filtering gateway)
  - Đơn giản nhất nhưng vẫn hiệu quả ➔ phổ biến nhất
  - Luật kiểm soát truy nhập dựa trên các trường dữ liệu của gói tin: địa chỉ (nguồn/đích), loại giao thức, cổng truy nhập, v.v..
  - Đảm bảo hiệu năng ➔ không kiểm tra nội dung gói tin ➔ bài toán lạm dụng giao thức
- Tường lửa dựa trên trạng thái (stateful inspection firewall)
  - Khái niệm trạng thái (state) hay ngữ cảnh (context) của dòng giao thông
  - Bài toán chống quét cổng (trinh sát)
  - Ghi nhớ dòng dữ liệu (gói tin) & phát hiện nghi vấn: gửi đi từ một địa chỉ, tần suất gửi gói tin vượt ngưỡng, kết nối liên tục đến hoàng loạt cổng, v.v..
- Tường lửa kiểu bảo vệ (guard)
  - Hoạt động giống như một proxy ở tầng ứng dụng: nhận gói tin, kiểm soát, tạo gói tin mới, nhận kết quả, tạo gói tin kết quả trả về cho người yêu cầu
  - Kiểm soát chi tiết, loại bỏ hầu như mọi rủi ro
  - Great Firewall of China: https://en.wikipedia.org/wiki/Great_Firewall
- Tường lửa cá nhân (personal firewall)
  - Ứng dụng chạy trên máy trạm cần được bảo vệ
  - Có thể được cung cấp như một cấu phần của hệ điều hành

Tường lửa: Thiết lập luật giữa các vùng

	Direction		Status
Red	→	Firewall	Closed, Use external access
Red	→	Orange	Closed. Use port forwarding
Red	→	Blue	Closed. Use port forwarding or VPN
Red	→	Green	Closed. Use port forwarding or VPN
Orange	→	Firewall	Closed, No DNS nor DHCP for Orange
Orange	→	Red	Open
Orange	→	Blue	Closed, use DMZ pinholes
Orange	→	Green	Closed, use DMZ pinholes
Blue	→	Firewall	Closed, no access for Blue
Blue	→	Red	Closed, no access for Blue
Blue	→	Orange	Closed, no access for Blue
Blue	→	Green	Closed, use DMZ pinholes or VPN
Green	→	Firewall	Open
Green	→	Red	Open
Green	→	Orange	Open
Green	→	Blue	Open



Bài thực hành tường lửa: IPFire

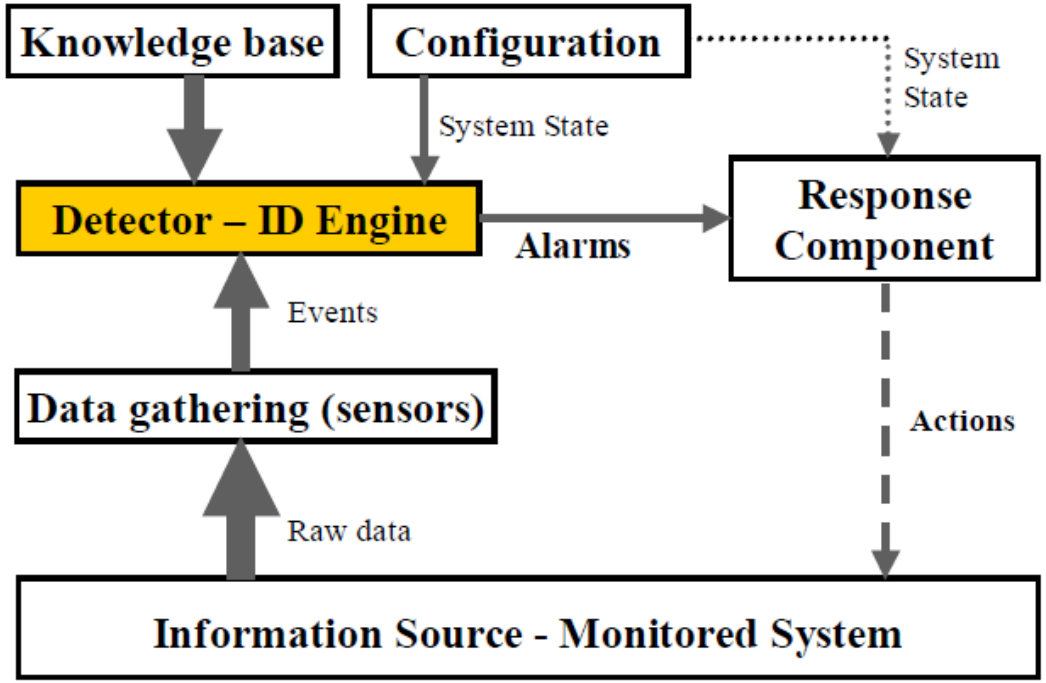
- https://users.soict.hust.edu.vn/hoangph/textbook/ch05-1.html

Hệ thống phát hiện & chống xâm nhập IDS/IPS

- Tại sao cần hệ thống phát hiện xâm nhập?
  - Tường lửa tạo cảm giác yên tâm cho mạng nội bộ nhưng chưa quyết triệt để các vấn đề tấn công mạng.
  - Sự cố bảo mật gây ra bởi các trạm bên trong (vùng Blue & Green)
- Intrusion Detection System (IDS):
  - Theo dõi các hoạt động trên mạng, phát hiện sớm nghi ngờ hoặc các hoạt động có khả năng gây hại (như hệ thống báo khói trong tòa nhà)
  - Xử lý nghi ngờ không nằm trong phạm vi của IDS
- IDS phản ứng nhanh:
  - Tự động chuyển sang chế độ bảo vệ: cách ly thành phần nghi ngờ nhiễm độc, ngăn chặn truy cập tài nguyên, v.v..
  - IDS bổ sung chức năng bảo vệ (Protection) thay vì chỉ phát hiện (Detection) ➔ IPS

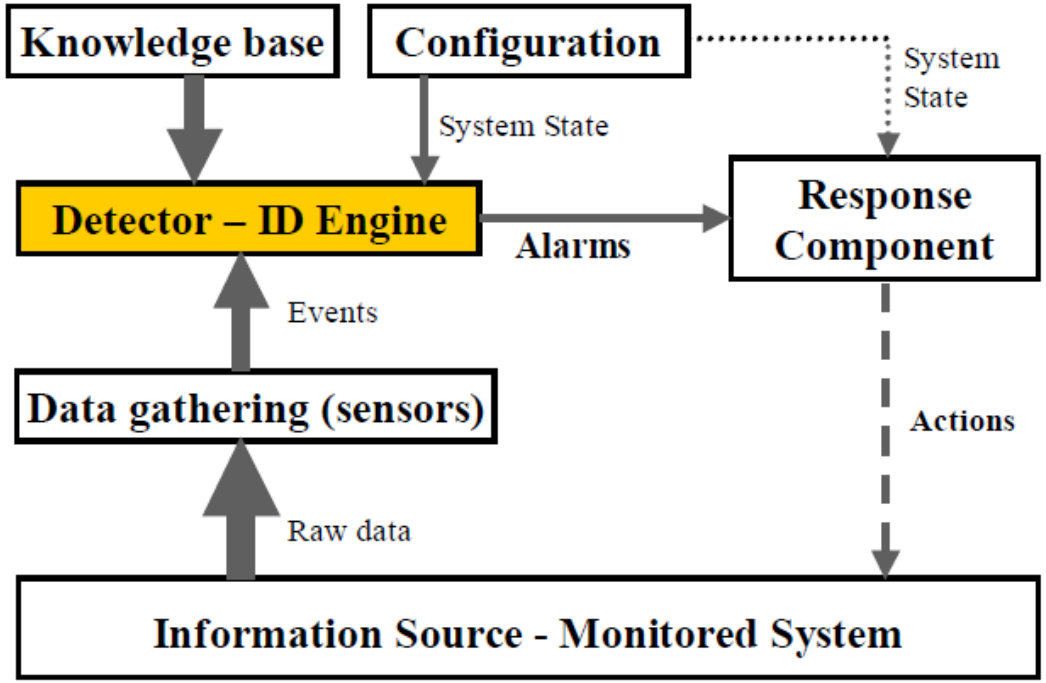
Kiến trúc IDS

- Các thành phần cơ bản của IDS:
  - Data gathering: thu thập thông tin (sensors) từ hệ thống cần giám sát
  - Detector – ID Engine: xử lý dữ liệu từ hệ thống sensor để phát hiện truy nhập khả nghi
  - Response Component: xử lý truy nhập khả nghi, có thể là cảnh báo người quản trị hoặc can thiệp ngay để ngăn chặn (chức năng Protection của IPS)
  - Knowledge base (database): thông tin hỗ trợ Detector xử lý dữ liệu sensor phát hiện truy nhập
  - Configuration: cấu hình cho Detector tùy theo trạng thái hệ thống (system state)
- Cơ chế phát hiện truy nhập
  - Signature-based: dựa trên dấu hiệu nhận biết
  - Abnomal-based: dựa trên hành vi bất thường



Phân loại IDS

- Information source
  - Host based
  - Network based
  - Application Logs
  - Wireless networks
  - Sensor Alerts
- Analysis strategy
  - Anomaly Detection
  - Misuse Detection
- Time Aspects
  - Real-time prediction
  - Off-line prediction
- Architecture
  - Centralized
  - Distributed & heterogeneous
- Response
  - Active response
  - Passive reaction

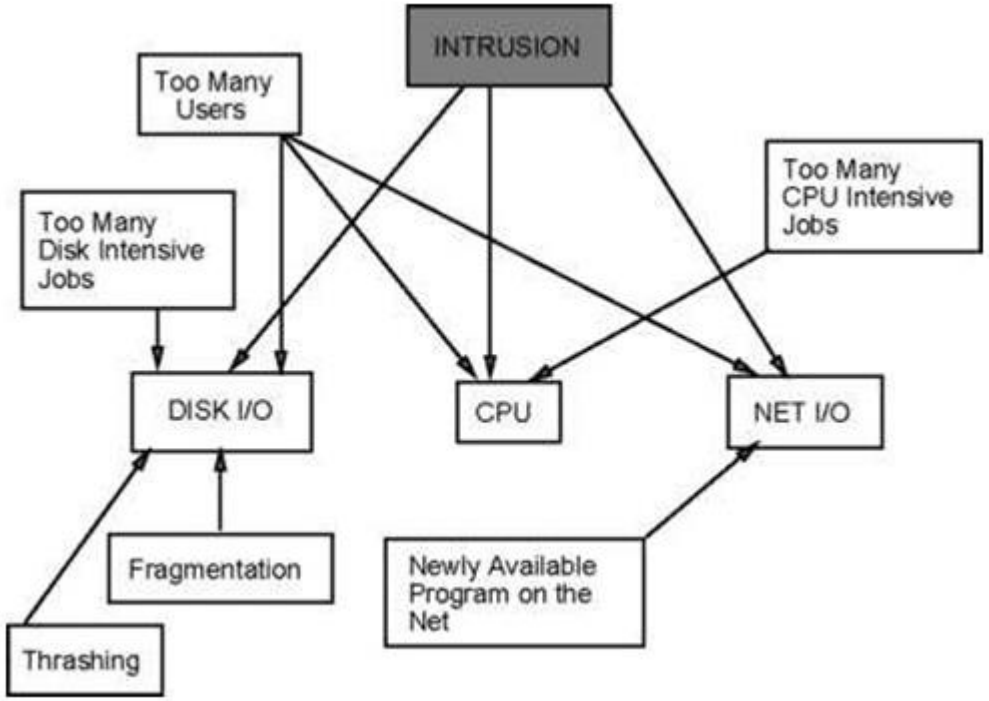


IDS dựa trên dấu hiệu nhận biết

- Chủ yếu dựa trên thông tin các trường header trong gói tin (IP, ICMP, TCP, v.v..). Ví dụ nhận biết có truy nhập ssh từ bên ngoài:
  - alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"incoming SSH connection!"; flags:S; sid:10000;)
- Cũng có thể dựa trên nội dung. Ví dụ nhận biết một trạm thuộc vùng Green truy nhập đến danh sách terrorism:
  - alert tcp $HOME_NET any -> $EXTERNAL_NET 80 (msg:"terrorism contact!"; content:"terrorism"; nocase; sid:10003;)
- Xây dựng các luật nhận biết không đơn giản, có sự tham gia của cộng đồng. Ví dụ sau là một luật nhận biết có truy nhập khai thác lỗ hổng bảo mật ssh đã được cộng đồng phát hiện và chia sẻ luật xử lý:
  - alert tcp $EXTERNAL_NET any -> $HOME_NET $SSH_PORTS (msg:"INDICATOR-SHELLCODE ssh CRC32 overflow filler"; flow:to_server,established; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; fast_pattern:only; metadata:policy max-detect-ips drop, ruleset community; reference:bugtraq,2347; reference:cve,2001-0144; reference:cve,2001-0572; classtype:shellcode-detect; sid:1325; rev:14;)

IDS dựa trên hành vi bất thường

- IDS dựa trên dấu hiệu nhận biết chỉ phát hiện được các tấn công có dấu hiệu đã được khai báo. Kỹ thuật này cũng chỉ áp dụng được với các tấn công dấu hiệu cố định.
- IDS dựa trên hành vi bất thường hướng đến xử lý các tồn tại của IDS dựa trên đấu hiệu nhận biết. Cơ chế là dựa trên mô hình thống kê mô tả trạng thái bình thường và so sánh với dữ liệu ser



Bài thực hành IDS/IPS

- Snort: IDS dựa trên dấu hiệu nhận biết:
  - https://users.soict.hust.edu.vn/hoangph/textbook/ch05-3.html
- IPS: Snort + IPFire:
  - https://users.soict.hust.edu.vn/hoangph/textbook/ch05-4.html