**MẠNG CĂN BẢN**

Trong thời đại kỹ thuật số phát triển vượt bậc như ngày nay, kiến thức về mạng đã trở thành một phần không thể thiếu của cuộc sống và công việc chúng ta. Từ việc duyệt web cơ bản cho đến triển khai hạ tầng mạng phức tạp, hiểu biết về mạng máy tính đóng vai trò quan trọng trong việc đảm bảo thông tin liên lạc liên tục và hiệu quả.

Với sự đam mê công nghệ cùng với kinh nghiệm làm việc cho ISP, mình có cơ hội tiếp xúc với nhiều thiết bị mạng, xử lí trên dưới 10.000 ca bảo trì logic. Mình hiểu rõ sự khó khăn và khắc nghiệt mà người mới bắt đầu hoặc những ai chưa có kiến thức đối mặt khi tìm hiểu về mạng máy tính. Đó chính là lý do tại sao mình đã quyết định viết tài liệu này - một tài liệu dành riêng cho những người đang bước đầu tìm hiểu về mạng và cho những anh em mới bước chân vào ngành, mà thậm chí cả kiến thức cơ bản cũng là điều xa lạ. Từ ngữ được đơn giản hóa giúp dễ hiểu hơn.

Nội dung gồm :

1. **MÔ TẢ THUẬT NGỮ**
2. **CHI TIẾT MỘT SỐ GIAO THỨC PHỔ BIẾN**
3. **CÔNG NGHỆ WIFI**
4. **TỐC ĐỘ**
5. **THIẾT BỊ MẠNG**
6. **MẠNG QUANG**
7. **MỘT SỐ MÔ HÌNH TRIỂN KHAI ROUTER – WIFI THAM KHẢO**
8. **Q&A**

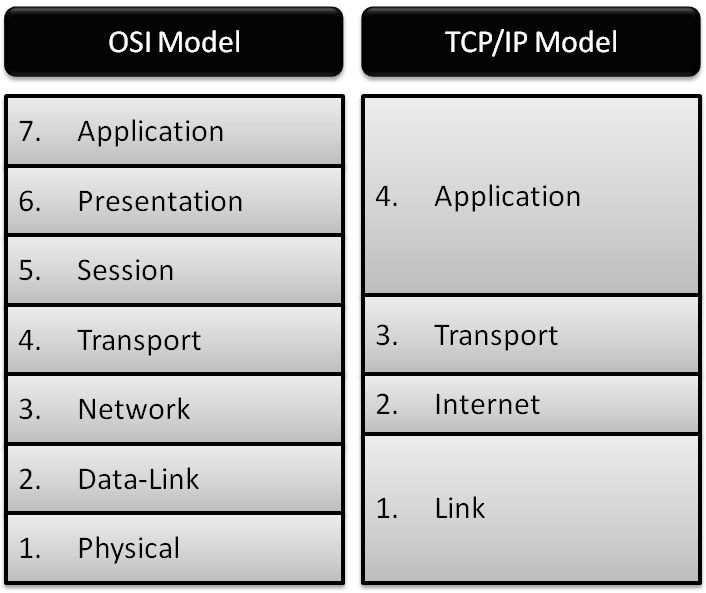
**A.MÔ TẢ CƠ BẢN VỀ MỘT SỐ THUẬT NGỮ THÔNG DỤNG**

| Thuật Ngữ | Mô tả |
| --- | --- |
| IP | IP (Internet Protocol) là một giao thức được sử dụng để định danh địa chỉ các thiết bị trong mạng.  Thời điểm hiện tại có Ipv4 và Ipv6 . |
| Router | Bộ định tuyến. Chức năng chính của router là quyết định cách dữ liệu được truyền đi giữa các mạng, dựa trên địa chỉ IP của các thiết bị mạng.  Một chức năng quan trọng của router là chỉ dẫn đường đi cho gói tin dựa trên địa chỉ IP. |
| Switch | Switch là một thiết bị mạng được sử dụng để kết nối các thiết bị trong mạng cục bộ (LAN - Local Area Network) và chuyển tiếp dữ liệu giữa chúng dựa trên địa chỉ MAC (Media Access Control).  Cách dùng phổ biến : chúng ta có 1 cổng mạng nhưng có 5 máy tính, switch sẽ giúp chia 1 cổng mạng ra 5 cổng. |
| LAN | LAN (Local Area Network) là một mạng máy tính ở phạm vi hẹp, thường bao gồm các thiết bị nằm trong khoảng cách gần nhau vật lý, chẳng hạn như trong một văn phòng, một tòa nhà, hoặc một khu công nghiệp nhỏ. |
| WAN | WAN (Wide Area Network) là một loại mạng máy tính mở rộng ở phạm vi rộng, kết nối các mạng con (LAN hoặc MAN - Metropolitan Area Network) nằm ở các địa điểm khác nhau, thậm chí có thể cách xa hàng trăm hoặc hàng nghìn dặm. WAN được sử dụng để kết nối các địa điểm địa lý khác nhau, cho phép truyền dữ liệu, thoại, và dịch vụ khác giữa các vị trí xa nhau. |
| AP | AP (Access Point) là một thiết bị trong mạng không dây (wireless) được sử dụng để tạo ra một điểm truy cập không dây cho các thiết bị di động như laptop, điện thoại di động, máy tính bảng để kết nối vào mạng LAN hoặc mạng Internet. |
| Beacon | Beacon là một khung tín hiệu phát ra từ các thiết bị không dây như Access Points (APs) để thông báo về sự tồn tại và các thông tin khác về mạng. Client đọc thông tin beacon để biết được thông tin về mạng wifi dù chưa cần kết nối vào.  Nội dung thường có trong beacon là : SSID, các tiêu chuẩn không dây, tốc độ hỗ trợ, mã hóa và các thông số khác.  Beacon interval là khoảng thời gian giữa các lần gửi beacon. |
| DTIM | DTIM (Delivery Traffic Indication Message), là một khung thông báo trong mạng không dây để thông báo cho các thiết bị client đang ở chế độ tiết kiệm năng lượng (sleep mode) về việc gửi dữ liệu multicast hoặc broadcast trong mạng.  Nói đơn giản thế này, để tiết kiệm năng lượng cho các thiết bị sử dụng wifi nên khi vào chế độ ngủ các client sẽ thực hiện ngừng trao đổi dữ liệu, tuy nhiên nó vẫn lắng nghe 1 khung tín hiệu gọi là DTIM, khung này sẽ nói cho client biết khi nào cần thức dậy để nhận dữ liệu, giống như 1 chiếc báo thức.  Ví dụ beacon interval đặt là 100ms thì AP cứ đều đặn mỗi 100ms sẽ gửi beacon đi, tuy nhiên nếu DTIM đặt là 2 thì đến lần thứ 2 beacon gửi đi client mới thức dậy đọc, trong ví dụ ở đây là cứ 200ms client mới đọc beacon 1 lần. |
| Roaming | Là quá trình mà một thiết bị di động di chuyển từ một vùng phủ sóng của một Access Point (AP) sang một vùng phủ sóng khác mà không mất kết nối hoặc trục trặc đáng kể. |
| CSMA/CA | CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) là một phương pháp tránh xung đột trong mạng không dây (wireless network) được sử dụng để điều khiển quy trình truyền và nhận dữ liệu giữa các thiết bị trong môi trường không dây. Phương pháp này giúp tránh xảy ra xung đột dữ liệu khi nhiều thiết bị cố gắng truyền dữ liệu cùng lúc. |
| MAC | Địa chỉ MAC là một địa chỉ duy nhất gắn với mỗi card mạng. |
| Mesh | Là một kiến trúc mạng linh hoạt và phức tạp trong đó các AP trong mạng không chỉ kết nối với AP trung tâm, mà còn kết nối với nhau để tạo thành một mạng phủ sóng liên thông. |
| DHCP | DHCP (Dynamic Host Configuration Protocol) là một giao thức trong mạng máy tính được sử dụng để tự động cấp phát địa chỉ IP và các cài đặt mạng khác cho các thiết bị trong mạng, như máy tính, điện thoại, máy chủ, và thiết bị mạng khác. |
| PPPOE | PPPoE (Point-to-Point Protocol over Ethernet): PPP Là một giao thức liên kết dữ liệu, thường được dùng để thiết lập một kết nối trực tiếp giữa 2 nút mạng. Nó có thể cung cấp kết nối xác thực, mã hóa việc truyền dữ liệu, cho phép nhà cung cấp kiểm soát truy cập thông qua các kết nối PPP. PPPOE là sự kết hợp của PPP và hệ thống mạng có dây Ethernet.    Giao thức này thường được các nhà cung cấp dịch vụ internet (ISP) sử dụng để cung cấp, quản lí dịch vụ đến người dùng đầu cuối. |
| ONT/ONU | ONT viết tắt của "Optical Network Terminal"/”Optical Network Unit” tùy theo tên gọi từ nhà cung cấp, là một thiết bị quang học đầu cuối được sử dụng trong mạng quang để chuyển đổi tín hiệu quang học thành tín hiệu điện tử hoặc tín hiệu mạng có thể sử dụng bởi các thiết bị mạng khác như router, máy tính, điện thoại, và các thiết bị khác. |
| Bridge Mode | Trong chế độ này, thiết bị không thực hiện việc định tuyến (routing) hoặc chuyển gói dữ liệu dựa trên địa chỉ IP, mà chỉ chuyển tiếp dữ liệu theo địa chỉ MAC.  Ví dụ chúng ta không muốn quay PPPOE trên router quang nhà mạng thì sẽ chuyển sang Bridge Mode để quay PPPOE trên router khác. |
| OLT | OLT là viết tắt của "Optical Line Terminal", là một thiết bị quang học chính trong mạng quang, thường đặt phía ISP.  OLT đóng vai trò phân phối tín hiệu quang, quản lý và điều khiển các thiết bị cuối như ONU (Optical Network Unit) hoặc ONT (Optical Network Terminal). |
| Modem | Modem là viết tắt của "Modulator-Demodulator", là một thiết bị trong mạng được sử dụng để chuyển đổi tín hiệu số từ thiết bị điện tử như máy tính thành tín hiệu analog để truyền qua các phương tiện truyền dẫn như dây điện thoại hoặc cáp đồng trục, cáp quang (Fiber modem) và ngược lại. |
| Frequency -Tần số | Trong mạng máy tính, tần số là số lần lặp lại của tín hiệu trong 1 đơn vị thời gian.  Đơn vị là Hz (Hertz). |
| Frequency band – Băng tần | Băng tần đại diện cho khoảng tần số trong đó tín hiệu hoạt động.  Ví dụ, trong mạng Wi-Fi chuẩn 2.4 GHz, băng tần là khoảng từ 2.400 MHz đến 2.4835 MHz. |
| Channel | Trong ngữ cảnh wifi, mỗi băng tần lại được chia thành nhiều khoảng tần số hẹp hơn gọi là kênh.  Mục đích để tăng hiệu quả sử dụng tần số khi nhiều thiết bị cùng sử dụng chung 1 băng tần nhưng hạn chế được xung đột do truyền dẫn ở các kênh khác nhau. |
| Channel width | Độ rộng kênh chính khoảng cách giữa 2 giới hạn của băng tần. |
| Backhaul | Hay còn được xem như mạng xương sống, ám chỉ phần của hạ tầng mạng có nhiệm vụ kết nối các điểm truy cập (APs - Access Points) đến mạng lõi hoặc nguồn cung cấp dịch vụ Internet.  Ví dụ trong 1 mạng mesh có nhiều AP, đường liên kết từ AP vào các AP khác gọi là backhaul, nếu không dây là Wireless Backhaul, còn dùng cáp là Ethernet Backhaul. |
| OFDM | OFDM (Orthogonal Frequency Division Multiplexing) chia một tín hiệu dữ liệu lớn thành nhiều tín hiệu con nhỏ trên các tần số khác nhau.  Ví dụ mỗi kênh trong wifi lại được chia nhỏ thành các tín hiệu có tần số khác nhau.  Mỗi tín hiệu con được gọi là "subcarrier" và chúng được truyền đồng thời qua kênh. |
| Symbol | Trong OFDM sẽ gồm nhiều sóng mang con liên tục, tại 1 khoảng thời gian thì trên mỗi sóng mang sẽ có 1 symbols, tức là có nhiều symbols được truyền cùng lúc.  Symbol thể hiện 1 tổ hợp bit dữ liệu được tạo thành thông qua các phương pháp điều chế. |
| Guard interval | Môi trường Wifi là 1 môi trường phức tạp, dễ bị ảnh hưởng bởi ngoại cảnh, hơn nữa hiệu ứng đa đường trong wifi gây ra tình trạng việc tín hiệu phía đầu nhận có thể không còn sắp xếp đúng hoặc tín hiệu trong quá trình truyền bị va chạm gây lỗi. Từ đó ý tưởng là tạo ra 1 khoảng thời gian giữa các symbol đủ để tránh việc xáo trộn, khoảng thời gian này gọi là khoảng thời gian bảo vệ. |
| Unicast | Unicast là phương thức truyền thông một-đến-một, trong đó một gói tin được gửi từ một nguồn đến một đích duy nhất. |
| Broadcast | Broadcast là phương thức truyền thông một-đến-tất-cả, trong đó một gói tin được gửi từ một nguồn và được nhận bởi tất cả các thiết bị trong mạng. |
| Multicast | Multicast là phương thức truyền thông một-đến-nhiều, trong đó một gói tin được gửi từ một nguồn và được nhận bởi một nhóm thiết bị đích được chỉ định. |
| Client | Máy khách, ví dụ điện thoại, laptop… |
| QAM | Quadrature Amplitude Modulation (QAM) là một kỹ thuật điều chế sử dụng trong mạng Wi-Fi để chuyển đổi tín hiệu số thành tín hiệu analog để truyền qua kênh sóng radio. QAM kết hợp cả biên độ (Amplitude) và pha (Phase) của sóng mang để tạo ra các điểm trong không gian tín hiệu, từ đó cho phép truyền dữ liệu số thông qua sóng analog.  Số bit tương ứng với mỗi Symbol phụ thuộc vào loại QAM đang sử dụng : -16QAM : 4bit  -64QAM : 6 bit  -256QAM : 8 bit  -1024QAM : 10 bit  -4096QAM : 12bit |
| BSS | BSS là viết tắt của "Basic Service Set” là một nhóm các thiết bị không dây (chẳng hạn như điểm truy cập và các thiết bị kết nối đến nó) mà có thể giao tiếp trực tiếp với nhau qua các tần số sóng radio chung và cùng một kênh sóng.  Ví dụ AP và client trong 1 mạng wifi gọi là 1 BSS. |
| WMM | WMM (Wi-Fi Multimedia) là một tập hợp các cải tiến liên quan đến chất lượng dịch vụ (QoS - Quality of Service) trong mạng Wi-Fi, được đưa vào sử dụng để tối ưu hóa việc truyền tải dữ liệu âm thanh, hình ảnh và video trong môi trường không dây.  Nó phân loại dữ liệu và ưu tiên, thông thường thứ tự ưu tiên là Voice, Video, Best Effort, Background.  Ví dụ các dữ liệu dạng Voice cần độ trễ thấp nên sẽ được ưu tiên trong quá trình tranh chấp truyền cũng như thời gian chiếm kênh truyền hơn. |
| Digital Signal | Tín hiệu số là dạng tín hiệu mà thông tin được biểu diễn và truyền tải dưới dạng các giá trị số, thường là các con số nhị phân (0 và 1) trong hệ thống nhị phân.  Tín hiệu số là tín hiệu biểu thị dữ liệu dưới dạng một chuỗi các giá trị rời rạc.  Ví dụ tín hiệu số được biểu diễn thông qua việc sử dụng các mức điện áp khác nhau. Các mức điện áp được đặt theo một số tiêu chuẩn, chẳng hạn như 0V cho bit 0 và +5V cho bit 1. |
| Analog Signal | Tín hiệu Analog là tín hiệu liên tục, đồ thị biểu diễn tín hiệu analog là một đường liên tục (ví dụ sin, cos hoặc đường cong lên xuống bất kỳ).  Ví dụ âm thanh là 1 dạng tín hiệu analog. |
| Half duplex | Half duplex là một chế độ truyền thông trong mạng mà thiết bị có thể truyền dữ liệu theo một hướng tại một thời điểm nhưng không thể truyền và nhận dữ liệu cùng lúc.  Wifi hoạt động theo chế độ half duplex (tính tại thời điểm viết tài liệu này), khi đang gửi dữ liệu nó sẽ không thể nhận dữ liệu mà phải đợi truyền xong mới bắt đầu nhận. |
| Full Duplex | Full duplex, ở chế độ này cho phép gửi và nhận cùng lúc.  Các mạng cáp LAN các bạn sử dụng là full duplex. |
| UDP và TCP | UDP (User Datagram Protocol), giao thức này truyền gói tin với tốc độ nhanh nhưng không tin cậy vì không có cơ chế ACK để phản hồi việc đã nhận gói tin hay chưa. Thường dùng trong hệ thống cần độ trễ thấp, tính thời gian thực như IPTV.  TCP (Transmission Control Protocol): là giao thức truyền tin đáng tin cậy vì có cơ chế truyền lại nếu gói tin nếu phía nhận bị mất, lỗi. |
| Port forwarding | Chuyển tiếp port, là một quá trình chuyển tiếp của một port cụ thể từ hệ thống mạng này sang một mạng khác. |
| Beamforming | Công nghệ xác định vị trí client để tăng hiệu quả truyền dẫn. |

**B. CHI TIẾT MỘT SỐ GIAO THỨC PHỔ BIẾN**

**1. Mô Hình Tham Chiếu :**

Mô hình OSI (Open Systems Interconnection) và TCP/IP (Transmission Control Protocol/Internet Protocol) là hai mô hình tham chiếu được sử dụng trong lĩnh vực mạng máy tính để mô tả cách thức hoạt động và giao tiếp giữa các thiết bị trong mạng.



* Tương ứng với mỗi tầng sẽ có các thiết bị hoặc giao thức tương ứng, ví dụ Switch nằm ở tầng Data Link làm việc với địa chỉ MAC nên thường sẽ gọi là Switch Layer 2. Cũng có 1 số loại switch layer 3 nhưng nội dung bài này sẽ không đề cập đến.
* Trong thực tế mô hình TCP/IP được sử dụng phổ biến, mô hình OSI thường phục vụ cho nghiên cứu, thiết kế, giảng dạy.

**2. IP (Internet Protocol) :**

-**Địa chỉ IP (Internet Protocol Address)** : là một định danh duy nhất được gán cho mỗi thiết bị kết nối vào mạng Internet hoặc mạng nội bộ (intranet).

-Về phiên bản có 2 phiên bản IP hiện tại là IPv4 và IPv6.

-Về mục đích sử dụng có 2 dạng IP là IP Public và IP Private :

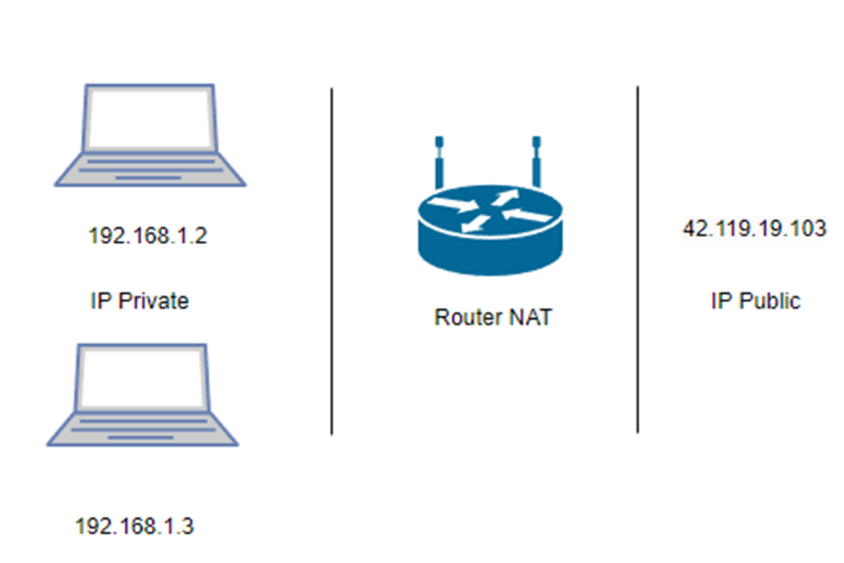
**+ IP Public** : hay còn gọi là IP công cộng, mỗi địa chỉ IP Public là duy nhất trên thế giới, do các nhà cung cấp dịch vụ cấp.

**+ IP Private** : hay còn gọi là IP riêng tư, IP này thường sử dụng cho mạng nội bộ, do máy chủ DHCP Server nội bộ cấp.

***Dải địa chỉ Public và Private :***

*Ipv4 Public :*

Dải A: Từ 1.0.0.0 đến 9.255.255.255

11.0.0.0 -126.255.255.255

Dải B: Từ 128.0.0.0 đến 172.15.255.255

172.32.0.0 - 191.255.255.255

Dải C: Từ 192.0.0.0 đến 192.167.255.255

192.169.0.0 - 223.225.255.255

Dải D: Từ 224.0.0.0 đến 239.255.255.255

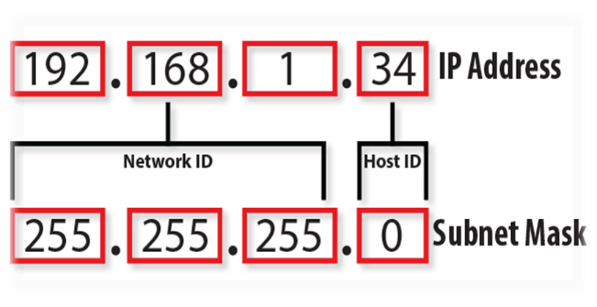
Dải E: Từ 240.0.0.0 đến 255.255.255.255

*Ipv4 Private*

Dải A: Từ 10.0.0.0 đến 10.255.255.255

Dải B: Từ 172.16.0.0 đến 172.31.255.255

Dải C: Từ 192.168.0.0 đến 192.168.255.255



***Cấu Trúc Ipv4 :***

Cấu trúc IPv4 gồm 32 bit chia thành 4 Octet :

Gồm 2 phần là **NetID** : Để định danh mạng.

**HostID**: Để cấp cho client trong mạng.

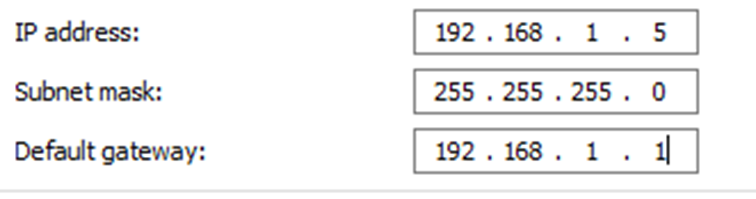
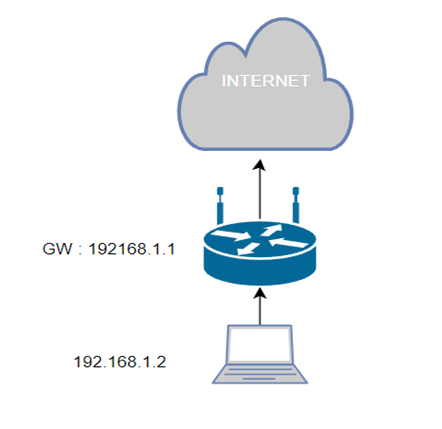
**-Subnet Mask** : Mỗi địa chỉ IP đều đi kèm với một Subnet Mask, để xác định được phần NetID của địa chỉ đó.

Ví dụ subnet mask : 255.255.255.0 (có thể viết ngắn gọn bằng số lượng bit Net của mạng như /24) 192.168.1.0 thì phần NetID là 192.168.1

**-Default gateway** (cổng mặc định) bản chất là một địa chỉ IP và còn được gọi là cổng mặc định của mạng máy tính. Địa chỉ này sẽ được cấu hình cho thiết bị máy tính và máy tính mặc định sẽ gửi gói tin đến địa chỉ này để có thể tiếp tục đi đến mạng khác.

Nói cách khác Default Gateway xem như là cửa ngõ để các thiết bị local có thể đi ra ngoài mạng.

Các thiết bị trong cùng 1 mạng LAN giao tiếp với nhau thì có thể không cần đi qua Gateway.



Hiện tại IPv4 Public đã cạn kiệt nên sự ra đời của IPv6 để giải quyết vấn đề (IPv4 chỉ có khoảng 4 tỷ địa chỉ).

**Địa chỉ IPv6** (Internet Protocol version 6) được biểu diễn dưới dạng một dãy số hexa dài 128-bit, chia thành 8 nhóm, mỗi nhóm gồm 4 chữ số hexa, được phân tách bởi dấu hai chấm.

Ví dụ: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

***Một số giao thức của IPv6 :***

+ *ICMPv6* (Internet Control Message Protocol version 6): ICMPv6 là phiên bản IPv6 của giao thức ICMP trong IPv4.

+ *NDP* (Neighbor Discovery Protocol): NDP được sử dụng trong IPv6 để xác định các địa chỉ IPv6 của các thiết bị trong cùng một mạng LAN.

+ *DHCPv6* (Dynamic Host Configuration Protocol version 6): DHCPv6 là phiên bản IPv6 của giao thức DHCP trong IPv4.

+ *IPv6 over IPv4* tunneling protocols: IPv6 hỗ trợ các giao thức tunneling để vận chuyển gói tin IPv6 qua mạng IPv4.

**+** *Multicast Listener Discovery* (MLD): Giao thức quản lí Multicast, hoạt động trên nền các thông điệp ICMPv6.

**3. NAT (Network Address Translation) :**

- **NAT** (Network Address Translation) là một kỹ thuật được sử dụng trong mạng máy tính để chuyển đổi địa chỉ IP của gói tin trong quá trình truyền thông giữa các mạng.

Thường sẽ chuyển đổi từ IP Private sang IP Public (cũng có thể từ Private sang Private), thông qua cổng WAN.

Khi gói tin gửi đi từ mạng nội bộ (local), router NAT sẽ thay thế IP nguồn và Port của máy local thành IP và Port Public.

Thông tin cặp IP và Port này sẽ được lưu lại vào bảng gọi là NAT Table.

Khi gói tin từ phía ngoài trả về, router sẽ tra bảng NAT để biên dịch và gửi lại về máy local.

Các loại NAT thông thường là Dynamic NAT, Static NAT và NAT Overload :

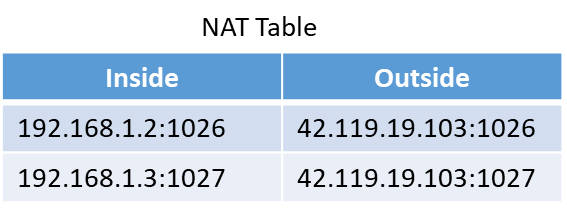
+ 1 IP Private ánh xạ với 1 IP Public.

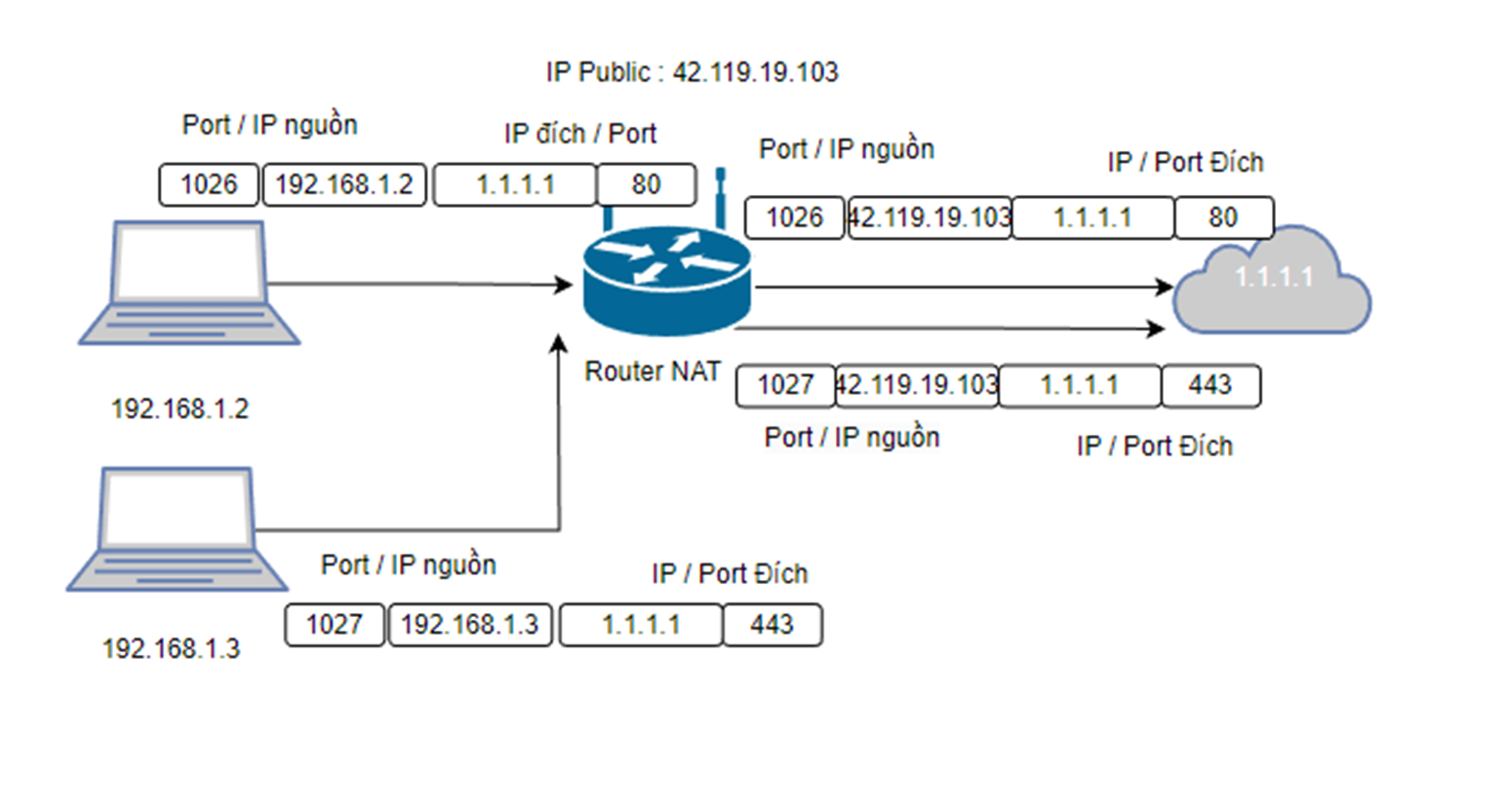
+ Nhiều IP Private ánh xạ với nhiều IP Public.

+ Nhiều IP Private ánh xạ với 1 IP Public.

Hiện nay **NAT Overload** là loại NAT phổ biến, nhiều IP Private có thể NAT với 1 IP Public bằng việc sử dụng các Port khác nhau.

Tóm lại, NAT vốn được sinh ra để giải quyết vấn đề thiếu hụt Ipv4 Public không thể cấp cho toàn bộ thiết bị, ví dụ chúng ta có 5 máy tính nhưng chỉ có 1 IP Public thì phải chia nó ra thành 5 địa chỉ Private để cấp, quá trình đó gọi là NAT Overload.





**4.MAC (Media Access Control)** :

**Địa chỉ MAC** (Media Access Control) là một địa chỉ duy nhất được gán cho mỗi card mạng trong mạng máy tính, mỗi địa chỉ MAC là duy nhất trên toàn cầu. Ví dụ địa chỉ mac 00:1B:44:11:3A:B7

Trên mỗi thiết bị mạng, nếu như IP có thể thay đổi thì địa chỉ MAC lại là cố định với mỗi các mạng.

**5.DHCP (Dynamic Host Configuration Protocol) :**

**- Dynamic Host Configuration Protocol** : Là một giao thức cho phép cấp phát địa chỉ IP một cách tự động cùng với các cấu hình liên quan như subnet mark, gateway và DNS. **Quá trình DHCP như sau** :

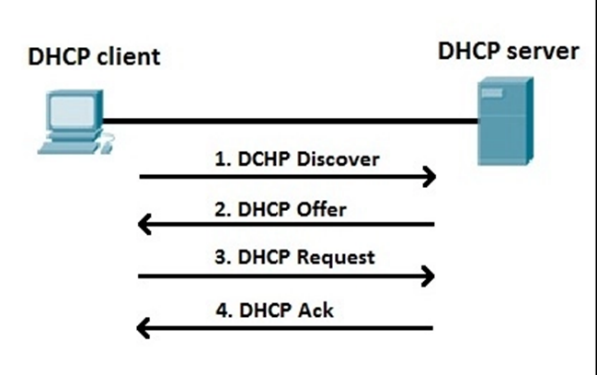
1. Client phát 1 thông báo yêu cầu địa chỉ IP từ các DHCP Server.

2. DHCP Server gửi một địa chỉ IP còn trống đến Client (bao gồm IP Address, Subnet Mask, Lease time, Default Gateway, DNS)

3. Client xác nhận địa chỉ IP vừa nhận được.

4. DHCP Server ghi lại thông tin về địa chỉ IP và máy tính đã sử dụng nó trong bảng quản lý.

5. Sau 50% thời gian leasetime cài đặt client sẽ gửi cho DHCP Server yêu cầu xin gia hạn thời gian thuê IP.

\* Trong trường hợp client không lấy được địa chỉ IP, thông thường client sẽ nhận một địa chỉ IP tự động gán từ dải "169.254.0.0/16".

**6. PPPoE (Point-to-Point Protocol over Ethernet)** :

- **PPP** (Point-to-Point Protocol) là một giao thức liên kết dữ liệu, thường được dùng để thiết lập một kết nối trực tiếp giữa 2 nút mạng. Nó có thể cung cấp kết nối xác thực, mã hóa việc truyền dữ liệu, cho phép nhà cung cấp kiểm soát truy cập thông qua các kết nối PPP. PPPOE là sự kết hợp của PPP và hệ thống mạng có dây Ethernet.

- Quá trình thiết lập của giao thức PPPOE bao gồm :

1. PADI (PPP Active Discovery Initiation): Quá trình bắt đầu bằng việc thiết bị client khởi tạo một gói tin PADI và gửi nó đến địa chỉ đích Broadcast (địa chỉ MAC FF-FF-FF-FF-FF-FF). Gói tin PADI được gửi để tìm kiếm một máy chủ PPP (PPP server) có sẵn.

2. PADO (PPP Active Discovery Offer): Nếu một máy chủ PPP nhận được gói tin PADI, nó sẽ phản hồi bằng một gói tin PADO chứa các thông tin cấu hình và các tùy chọn kết nối có sẵn. Gói tin PADO này được gửi từ máy chủ PPP đến thiết bị client thông qua địa chỉ MAC của thiết bị (địa chỉ unicast).

3. PADR (PPP Active Discovery Request): Sau khi thiết bị client nhận được gói tin PADO, nó sẽ gửi một gói tin PADR đến máy chủ PPP . Gói tin PADR chứa yêu cầu thiết lập kết nối PPP và thông tin cần thiết để xác thực.

4. PADS (PPP Active Discovery Session-confirmation): Máy chủ PPP nhận được gói tin PADR và kiểm tra thông tin xác thực. Nếu thông tin hợp lệ, máy chủ sẽ phản hồi bằng gói tin PADS để xác nhận việc thiết lập phiên (session) PPP, đồng thời cung cấp ID phiên được sử dụng trong suốt quá trình.

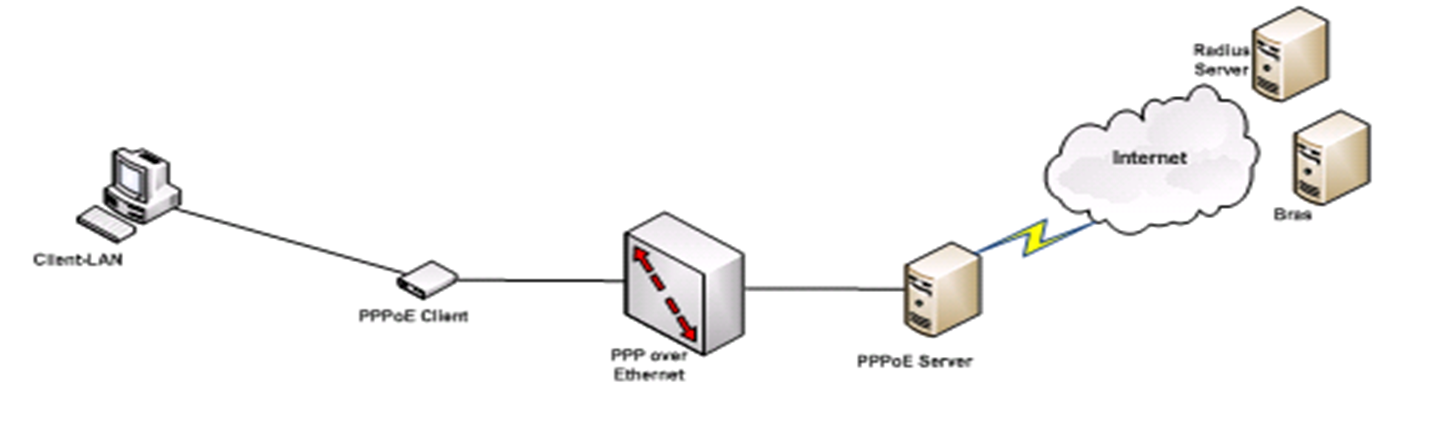
5. LCP/IP (Link Control Protocol/Internet Protocol): Sau khi phiên PPP được thiết lập thông qua các quá trình PADI, PADO, PADR và PADS, quá trình LCP/IP sẽ được thực hiện. Trong quá trình này, LCP sẽ xác nhận và đàm phán các tham số cấu hình PPP như các tùy chọn mã hóa, địa chỉ IP và DNS. Khi các tham số cấu hình đã được đồng ý, PPP session sẽ chính thức được thiết lập và các gói tin IP có thể được truyền qua kết nối PPP.



*Quá trình thực hiện PPPOE tại 1 ISP :*1 .Khách hàng quay pppoe bằng username và password(nhà mạng cung cấp) qua router để kết nối lên hệ thống.

2. Thông tin username/password sẽ được gửi lên Bras, Bras sẽ đẩy thông tin này về Radius Server để xác thực.

3. Nếu đúng thông tin,Bras sẽ tiến hành cấp phát IP đến khách hàng từ các Pool IP đã quy hoạch sẵn.



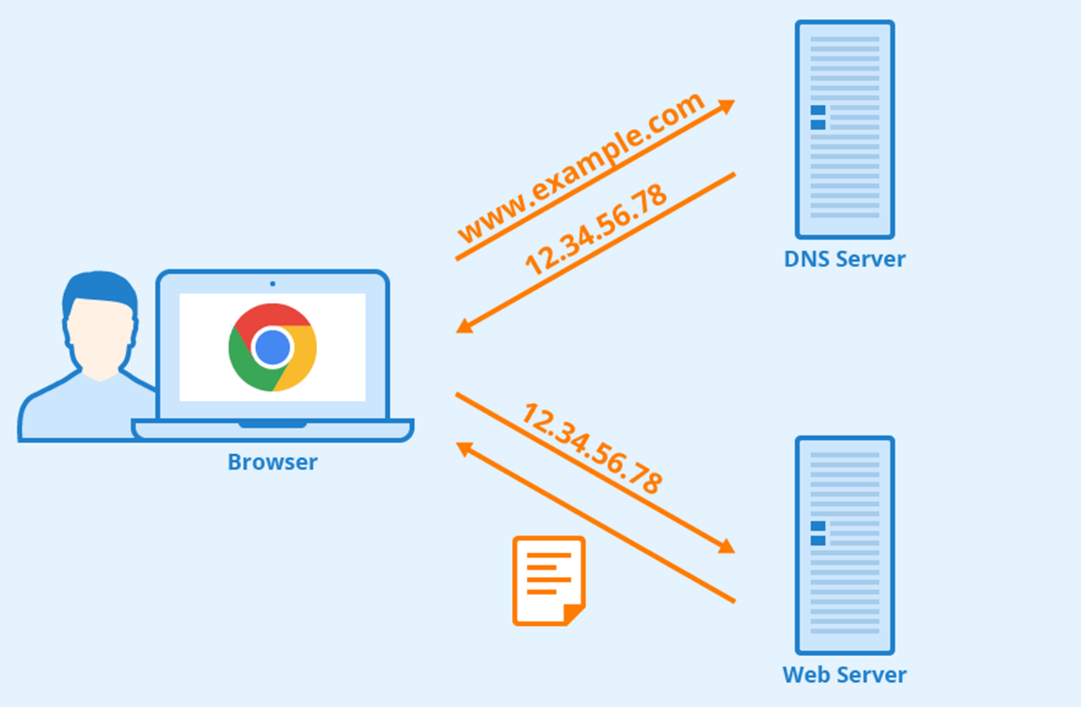
**7. DNS (của Domain Name System) :**

- Nó là một cơ chế quan trọng trong mạng Internet để chuyển đổi tên miền (như xxxxx.com) thành địa chỉ IP (như 192.0.2.1) và ngược lại.

- Mạng Internet hoạt động dựa trên địa chỉ IP, mà mỗi thiết bị trên Internet cần có một địa chỉ IP duy nhất để được xác định và liên lạc với các thiết bị khác. Tuy nhiên, ghi nhớ địa chỉ IP của mọi trang web và dịch vụ trên Internet là khá khó khăn và phiền toái. Đó là lý do tại sao DNS ra đời để cung cấp một cách dễ nhớ và người dùng thân thiện hơn để tìm kiếm các trang web và dịch vụ.

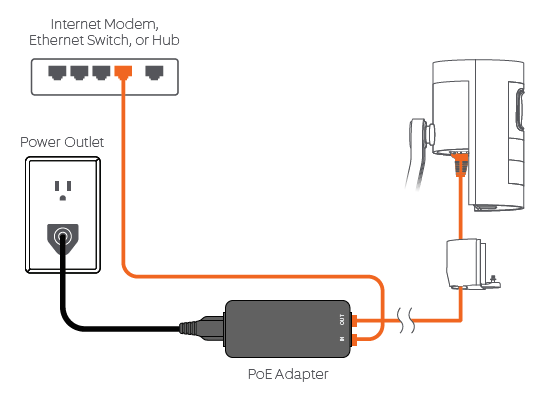
- . Nguyên lí hoạt động :

1. Nhập một tên miền vào trình duyệt web (ví dụ: google.com), trình duyệt sẽ gửi yêu cầu đến máy chủ DNS qua gói tin DNS Query . Máy chủ DNS là một hệ thống phân giải tên miền, nơi chứa thông tin về địa chỉ IP tương ứng của tên miền được yêu cầu.
2. Máy chủ DNS sẽ tìm trong cơ sở dữ liệu của nó để tìm địa chỉ IP của tên miền đó và trả về cho trình duyệt qua gói tin DNS Response . Sau đó, trình duyệt sử dụng địa chỉ IP này để thiết lập kết nối và tải nội dung từ trang web tương ứng.
3. Trong trường hợp máy chủ DNS không tìm thấy địa chỉ IP tương ứng với tên miền được yêu cầu, gói tin DNS Response sẽ chứa thông báo lỗi và mã lỗi tương ứng. Cụ thể, thông điệp lỗi sẽ được gửi trở lại cho trình duyệt để hiển thị cho người dùng hoặc cho ứng dụng cần thực hiện yêu cầu DNS.



**8. Công nghệ POE :**

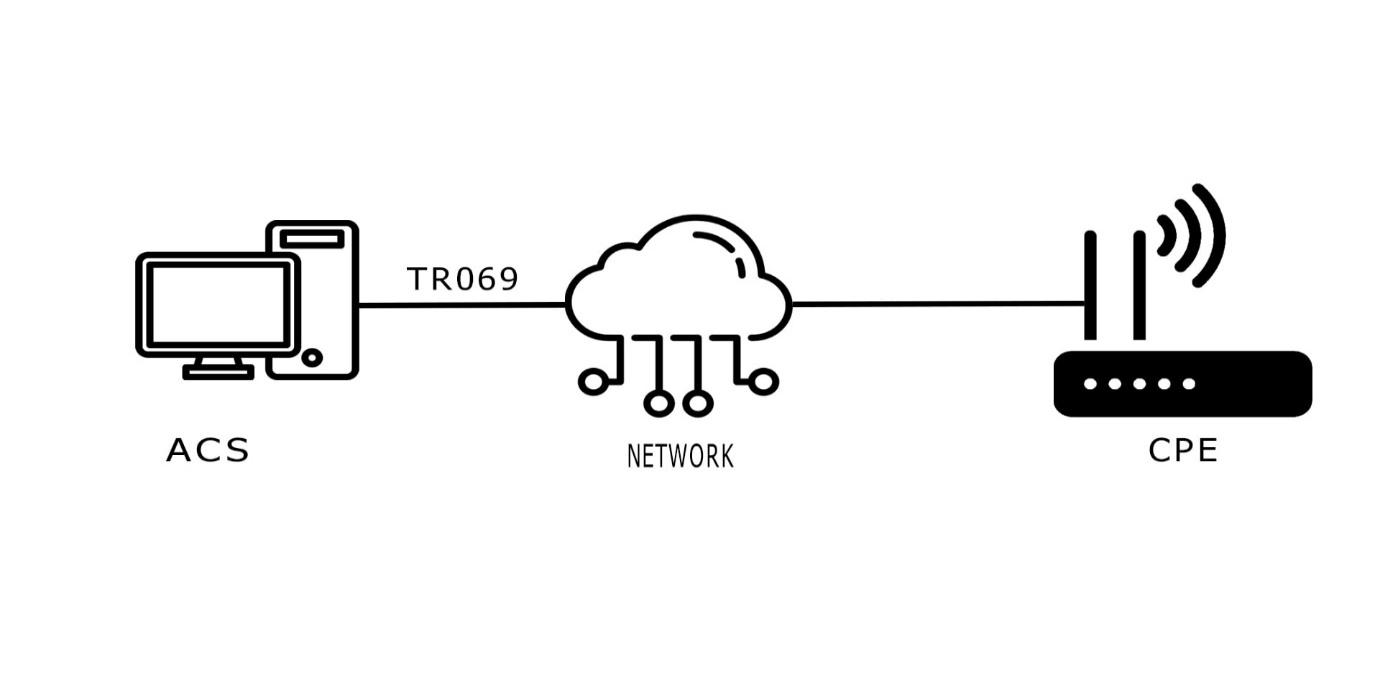
POE viết tắt của "Power over Ethernet," là một công nghệ cho phép truyền điện áp và dữ liệu qua cùng một dây cáp LAN. Công nghệ này giúp cung cấp nguồn điện cho các thiết bị mạng như điểm truy cập (access points), camera an ninh, điện thoại IP và nhiều thiết bị mạng khác mà không cần cấp nguồn điện riêng biệt.



**9. CWMP :**

- CWMP (CPE WAN Management Protocol) là một giao thức được sử dụng để quản lý và cấu hình các thiết bị mạng tại cơ sở khách hàng (CPE - Customer Premises Equipment) thông qua giao diện WAN (Wide Area Network) như internet.

- Nhà mạng thường dùng giao thức này để quản lí thiết bị tại nhà khách hàng. Ví dụ Modem Wifi.



**10. VLAN :**

**VLAN (Virtual Local Area Network)** là một phương pháp để chia nhiều mạng logic độc lập trên cùng một hệ thống vật lý. Kỹ thuật này cho phép bạn tạo ra các mạng ảo mà không cần thay đổi cơ sở hạ tầng vật lý.

Ví dụ : chúng ta có 1 router 4 cổng LAN, chúng ta muốn mỗi cổng 1 lớp mạng khác nhau thì chúng thực hiện chia vlan và gán nó cho từng cổng.

*Ưu điểm của VLAN :*Tách biệt và bảo mật: Bằng cách tạo các VLAN riêng biệt, bạn có thể tách các thiết bị và người dùng khác nhau ra khỏi nhau để đảm bảo tính riêng tư và bảo mật.

Hiệu suất: Các VLAN có thể được cấu hình để ưu tiên lưu lượng trong mạng, giúp cải thiện hiệu suất cho các ứng dụng quan trọng hơn.

Quản lý linh hoạt: Quản trị viên có khả năng quản lý mạng một cách linh hoạt hơn bằng cách chia thành từng phân đoạn nhỏ.

Tối ưu hóa địa chỉ IP: VLAN giúp tối ưu hóa sử dụng địa chỉ IP bằng cách chia mạng thành các mạng nhỏ hơn.

**11. VPN**

**VPN (Virtual Private Network)** là một kỹ thuật cho phép bạn tạo ra một mạng riêng ảo trên mạng công cộng, giúp bảo mật và mã hóa dữ liệu trong quá trình truyền tải. Mục tiêu chính của VPN là tạo ra một kết nối an toàn và riêng tư giữa các thiết bị hoặc mạng, cho phép truyền tải dữ liệu một cách an toàn qua mạng Internet hoặc mạng công cộng khác.

Các đặc điểm quan trọng của VPN bao gồm:

Bảo mật dữ liệu: VPN sử dụng mã hóa để bảo vệ dữ liệu khi nó được truyền qua mạng, đảm bảo rằng người không được phép không thể đọc hoặc xem thông tin.

Ẩn danh: VPN giúp ẩn danh địa chỉ IP thật của bạn, đặc biệt hữu ích khi bạn truy cập Internet từ nơi công cộng hoặc muốn tránh theo dõi trực tuyến.

Truy cập từ xa: VPN cho phép bạn truy cập vào mạng nội bộ của công ty hoặc tổ chức từ xa, giống như bạn đang ở trong mạng nội bộ đó.

Vượt qua các rào cản địa lý: Một số dịch vụ và trang web có thể bị chặn tại một số vị trí địa lý. VPN giúp bạn vượt qua những hạn chế này bằng cách kết nối thông qua một máy chủ nằm ở vị trí khác.

Mở rộng mạng LAN ảo: VPN có thể kết nối nhiều vị trí khác nhau và tạo ra một mạng riêng ảo (VLAN) giữa chúng, cho phép chia sẻ dữ liệu và tài nguyên một cách an toàn.

Ví dụ thực tế về chứ năng cơ bản của VPN, 1 số tài liệu chỉ có thể truy cập bằng mạng công ty mới lấy được và bạn đang ở nhà làm sao lấy được nó. Cách đơn giản là trên router cty bạn tạo 1 VPN server và trên máy tính ở nhà bạn kết nối vào VPN server đó. Như vậy bạn đã có thể truy cập vào mạng nội bộ công ty.

**C. CÔNG NGHỆ WIFI :**

- **Sóng wifi (IEEE 802.11)** : Sóng wifi là dạng sóng điện từ, điện từ hoạt động chủ yếu trên băng tần 2,4Ghz và 5Ghz,

- 1 số thiết bị Wifi 6E có thể hoạt động trên băng tần 6Ghz. Hiện nay phổ biến có 3 chuẩn Wifi N/AC/AX.

**-Một số định nghĩa :**

**+ Kênh truyền** : Tần số của wifi vốn không phải cố định mà chạy trong 1 dải tần số. Ví dụ :  
 Dải tần số 2.4GHz có phạm vi từ khoảng 2.400GHz đến 2.4835GHz, độ rộng kênh 20Mhz :

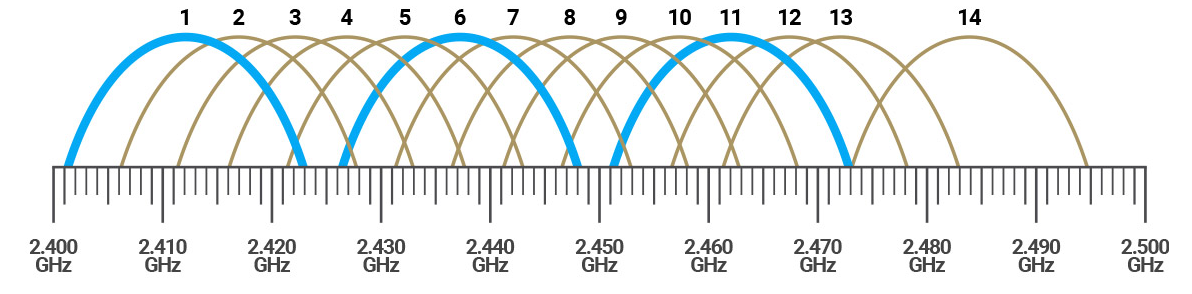
Kênh 1: Từ 2.412GHz đến 2.432GHz

Kênh 2: Từ 2.417GHz đến 2.437GHz

………

Có thể thấy mỗi kênh là 1 dải tần số khác nhau, người ta chia ra nhiều kênh là mục đích : tránh nhiễu, tránh xung đột

khi có nhiều thiết bị hoạt động liền kề. Tăng hiệu quả sử dụng tần số.

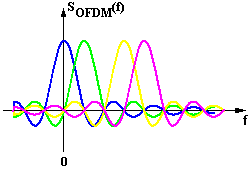


+ **Độ rộng kênh truyền** : trong wifi có 1 thông số là độ rộng kênh truyền. Tùy theo tiêu chuẩn wifi có thể là 20Mhz, 40Mhz ,80Mhz, 160Mhz.

Độ rộng kênh truyền ở đây chính là dải tần số của 1 kênh, ví dụ :

Kênh 1 – 20Mhz: Từ 2.412GHz đến 2.432GHz

Kênh 1 – 40Mhz: Từ 2.412GHz đến 2.452GHz

-Để hiệu quả sử dụng kênh truyền, wifi sử dụng 1 phương pháp trải phổ là OFDM, phương pháp này sẽ chia nhỏ 1 kênh ra các tần số nhỏ hơn gọi là subcarrier (sóng mang con), mỗi sóng mang con này sẽ mang dữ liệu riêng khi truyền, càng nhiều sóng mang con thì sẽ truyền được nhiều dữ liệu cùng lúc giúp tăng tốc độ.

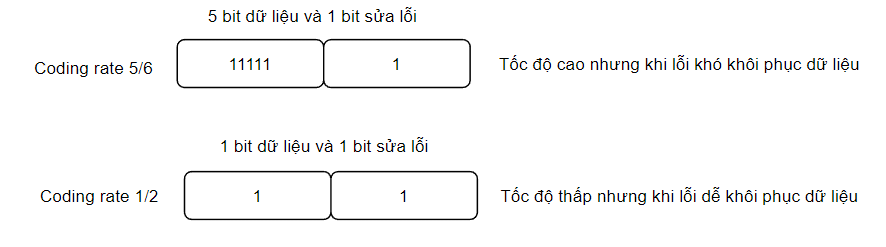
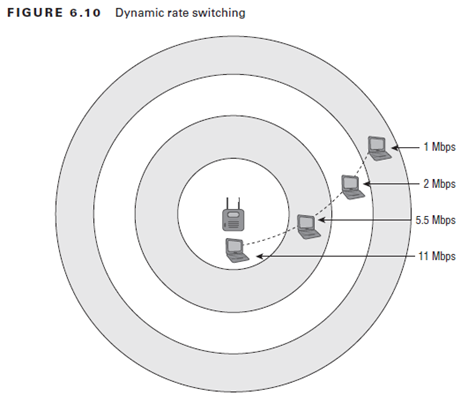
-Từ wifi AC trở về trước mỗi sóng mang con có tần số cách nhau 312.5 kHz, do vậy mỗi kênh 20Mhz sẽ có 64 sóng mang và tương tự  40Mhz sẽ có 128 sóng mang.

**-Tốc độ động (Dynamic Rate Switch)** : Việc client di chuyển ra xa AP hoặc có nhiều vật cản sẽ khiến tốc độ giảm, cả tốc độ liên kết vật lí và tốc độ dữ liệu khi speedtest. Nguyên nhân là do cơ chế chuyển đổi tốc độ của Wifi :

+Dữ liệu được CPU AP/ Client xử lí là dữ liệu số (bit 0 1), còn khi truyền từ AP đến client trong môi trường không dây là dạng sóng điện từ, cách để chuyển từ tín hiệu số sang sóng điện từ gọi là điều chế tín hiệu, ví dụ QAM.

+ Phương thức điều chế dữ liệu bậc cao, tỉ lệ bit dữ liệu / bit sửa lỗi (coding rate) càng lớn thì tốc độ càng nhanh nhưng sẽ đi kèm rủi ro mất hoặc sai dữ liệu trong quá trình truyền ở môi trường không thuận lợi cũng sẽ tăng cao.

=> Do vậy, khi ghi nhận các tham số như RSSI thấp, tỉ lệ lỗi gói, mất gói xảy ra nhiều thì thiết bị wifi sẽ tự động thương lượng 1 tốc độ truyền thấp hơn (tốc độ thấp hơn do đưa về phương thức điều chế tín hiệu bậc thấp đơn giản, tăng bit sửa lỗi và giảm bit dữ liệu).



-**CSMA/CA** : Carrier Sense Multiple Access with Collision Avoidance , phương phức đa truy nhập cảm biến sóng mang phòng chống xung đột.

Cơ chế của phương thức này là trước khi truyền dữ liệu trên kênh thiết bị sẽ lắng nghe kênh truyền, nếu kênh truyền đang bận nó sẽ chờ 1 khoảng thời gian ngẫu nhiên gọi là backoff time, sau đó nếu kênh truyền trống nó sẽ bắt đầu truyền.

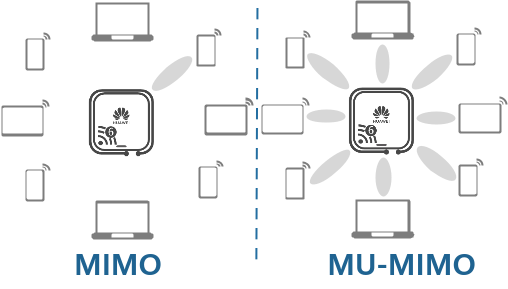
Cũng chính vì nguyên lí phòng chống xung đột này của wifi nên trong 1 mạng wifi có quá nhiều thiết bị hoặc 1 thiết bị liên tục yêu cầu truyền/ nhận dữ liệu sẽ dẫn đến các máy khác bị tăng thời gian chờ làm giảm hiệu suất mạng.

**-MIMO (Multi Input Multi Output)** : Lợi dụng việc AP có nhiều anten và client có nhiều anten, công nghệ MIMO cho phép mỗi cặp anten 1 trên AP và 1 trên Client sẽ gửi 1 luồng dữ liệu riêng (gọi là spatial stream), ví dụ có 2 anten thì sẽ gấp đôi luồng dữ liệu, mục đích tăng băng thông. Nhưng 1 lúc chỉ có thể giao tiếp với 1 thiết bị.

-**MU MIMO (Multi Input Multi Output) :** Tương tự như MIMO nhưng được cải tiến 1 chút là mỗi anten trên AP có thể giao tiếp với 1 client, có 2 anten thì đồng thời có thể giao tiếp với 2 client.

- MU MIMO thường đi kèm Beamforming ( Wifi 5 trở về trước thì chỉ có Tx MU-MIMO, nghĩa là chỉ có 1 hướng từ AP đến client nghệ xác định ví trí client để tăng hiệu quả truyền dẫn).

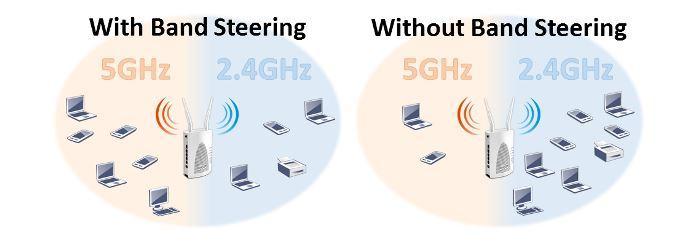
-Với MU MIMO giao thức CSMA/CA được của tiến để có thể cho phép gửi dữ liệu đồng thời đến nhóm MU.



**-Bandsteering** là một kỹ thuật được sử dụng trong mạng Wi-Fi để định hướng các client kết nối đúng dải tần số (band) Wi-Fi phù hợp nhằm tối ưu hiệu suất mạng.

Bandsteering thường được sử dụng khi 2 hoặc 3 băng tần đặt cùng 1 SSID, AP sẽ hướng cho client kết nối đến 1 băng tần nhất định theo thiết lập :  
+ Ưu tiên 5Ghz : Ưu tiên client kết nối vào 5Ghz.

+ Cân bằng : Tính toán dựa trên số lượng kết nối trên mỗi băng tần, chia số lượng cho phù hợp.



**-Roaming** là quá trình mà một thiết bị di động (như điện thoại di động, máy tính bảng hoặc laptop) kết nối và duy trì kết nối mạng liên tục khi di chuyển qua các vùng phủ sóng của các điểm truy cập không dây (access point) khác nhau trong mạng không dây.

Với mạng Wifi thông thường, để roaming cần đặt chung SSID giữa cái AP và AP cũng cần hỗ trợ các công nghệ roaming (802.11r/k/v).

-802.11r : Fast BSS Transition (FT), giúp quá trình xác thực khi client di chuyển giữa các AP trở lên nhanh chóng.

- 802.11k : Radio Resource Measurement (RRM), cho phép các client và AP thu thập thông tin về tình trạng môi trường sóng radio như cường độ tín hiệu, độ tắc nghẽn, nhiễu từ các AP khác và chia sẻ thông tin này với nhau. Các thông tin này có thể giúp client và AP đưa ra quyết định chính xác hơn về việc kết nối với AP tốt nhất trong phạm vi, giúp tối ưu hóa quá trình roaming và tăng cường hiệu suất mạng.

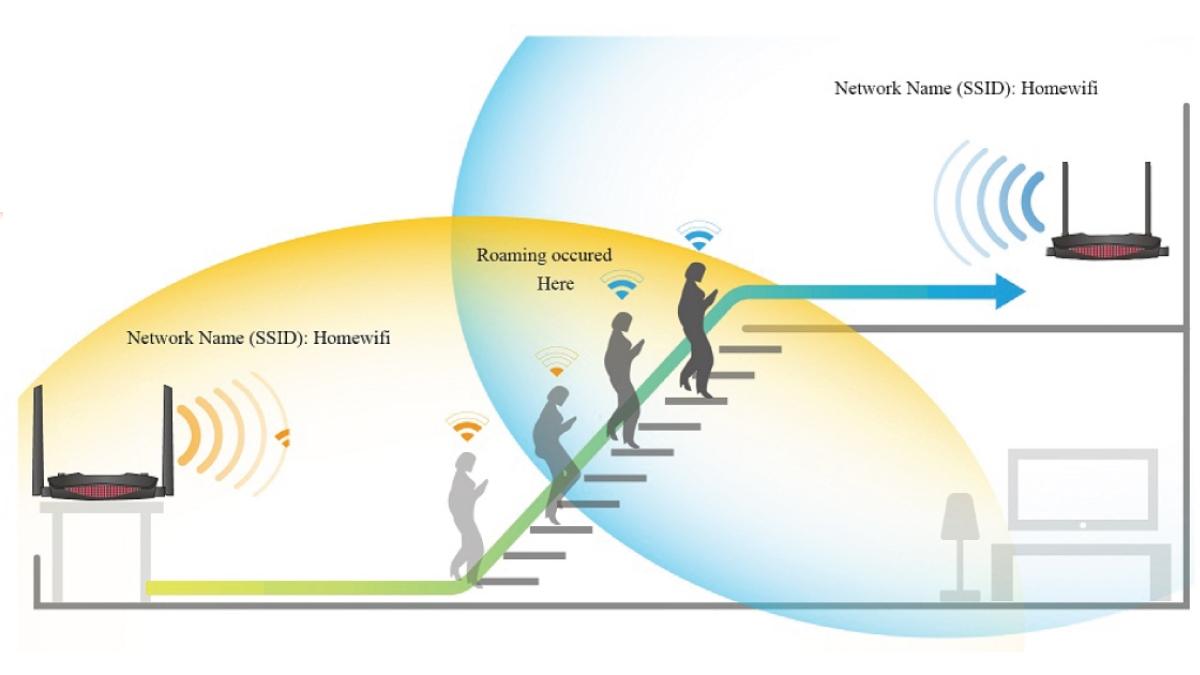
-802.11v : Wireless Network Management. Thông thường, một thiết bị di động giám sát tình trạng liên kết Wi-Fi của nó để chuyển vùng. Tuy nhiên, nó không biết những gì diễn ra bên trong AP được kết nối như cân bằng tải, lịch khởi động lại và số lượng client, v.v. Với sự hỗ trợ của 802.11v, một AP có thể yêu cầu client của mình chuyển vùng sang một AP khác có điều kiện mạng tốt hơn vì nó sẽ nắm được thông tin tình trạng hiện tại của các AP khác.

**Ví dụ về 3 yếu tố kích hoạt chuyển vùng của 1 hãng điện thoại android :**

*Tín hiệu yếu* — Client kích hoạt quét chuyển vùng để tránh truyền lại thường xuyên từ các gói bị mất. Khi giá trị Chỉ báo cường độ tín hiệu nhận được (RSSI) của AP hiện tại yếu (dưới -75dBm), thiết bị sẽ tìm kiếm một AP có tín hiệu mạnh hơn.

*Mất Beacon* — Khi không nhận được các gói beacon từ một AP được kết nối sau 2 giây (6 giây nếu màn hình TẮT), client coi đó là beacon bị mất và kích hoạt quét chuyển vùng.

*Sử dụng kênh (CU - Channel Utilization)* — Khi nhiều client kết nối với cùng một AP, kết nối có thể bị cản trở mặc dù có tín hiệu vô tuyến mạnh do tài nguyên hạn chế (quá tải). Trong trường hợp đó, AP sẽ thông báo cho client về lưu lượng truy cập hiện tại của nó thông qua hệ số CU trong beacon của nó. Sau đó, client sẽ kích hoạt quét chuyển vùng nếu giá trị CU nhận được lớn hơn 70% và giá trị RSSI hiện tại nằm trong khoảng -65dbm đến -75dBm.



**-ANTEN :** Anten chuyển đổi năng lượng điện sang sóng vô tuyến đối với anten phát hay chuyển đổi sóng vô tuyến sang năng lượng điện đối với anten nhận.

*Anten phân loại chính theo tính bức xạ gồm 2 loại :*

Anten định hướng : Tập trung về 1 hướng nhất định.

Anten đẳng hướng : Phát đều về mọi hướng.

Lưu ý : anten là 1 thiết bị thụ động, bản thân nó không tăng được công suất phát, việc tăng độ lợi anten (gain) sẽ liên quan đến góc phát, hay nói cách khác là nó lấy đi năng lượng ở hướng này để chuyển qua hướng khác.



**WIFI 6 :**

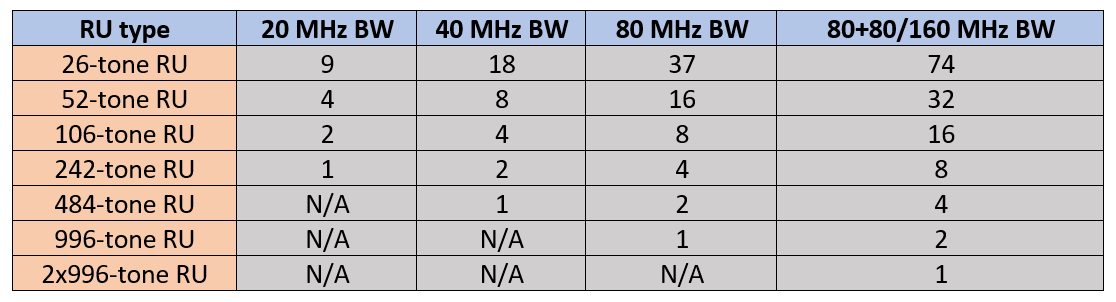
Ở phần trước, chúng ta đã biết về trải phổ OFDM chia 1 kênh truyền thành nhiều sóng mang con, nhưng giới hạn của nó là toàn bộ sóng mang con này 1 thời điểm chỉ truyền đến 1 thiết bị.

Wifi 6 được cải tiến với phương thức đa truy nhập OFDMA, điều này có nghĩa là số lượng sóng mang con sẽ được chia cho nhiều client cùng lúc nhằm truyền dữ liệu đồng thời. Từ đó giảm độ trễ, sử dụng hiệu quả kênh truyền nên Wifi 6 còn được gọi là Hiệu quả cao.

Wifi 6 các sóng mang con có khoảng cách 78.125 KHz, vậy nên mỗi kênh 20Mhz ta có đến 256 sóng mang con, tương tự tăng dần với 40 80 160Mhz.

Các sóng mang này được nhóm lại thành gọi là RU, RU nhỏ nhất có 26 và lớn nhất là 996 sóng mang con (chỉ có ở độ rộng kênh 80Mhz trở lên). Ví dụ như sau :

+ Ở wifi chuẩn N cũ, với kênh 20Mhz thì tại thời điểm chỉ có 1 máy được nhận dữ liệu thì với Wifi 6 cùng độ rộng kênh nhưng có thể cùng gửi dữ liệu đến 9 client (20Mhz có 256 sóng mang con chia cho mỗi người 26 sóng mang = 9).



* *Một số tính năng mới trên wifi 6 :*

-1024QAM : Nhanh hơn 25% so với 256-QAM của wifi 5.

- BSS Coloring : Đánh dấu màu cho các BSS giúp các thiết bị mạng có thể biết được gói tin được gửi ở thiết bị cùng BSS hay từ BSS khác, từ đó đưa ra phương án xử lí việc sử dụng kênh.

- MU-MIMO UL : Hỗ trợ MU-MIMO đường upload.

-TWT : Target Wake Time, tính năng để tối ưu hóa việc sử dụng năng lượng của các client bằng cách thương lượng thời gian ngủ và thức dậy.

**Mạng Lưới (Mesh) :**

**Cấu Trúc Lưới (Mesh)** : Đối với mạng dạng lưới, mỗi một AP sẽ được kết nối với tất cả hoặc 1 phần các AP mạng còn lại. Như trong hình minh họa, các AP đều được kết nói với nhau bằng nhiều đường dẫn.

Chính vì việc các AP liên kết đan xen với nhau như mắt lưới nên mới có tên gọi là cấu trúc mạng lưới (mesh).

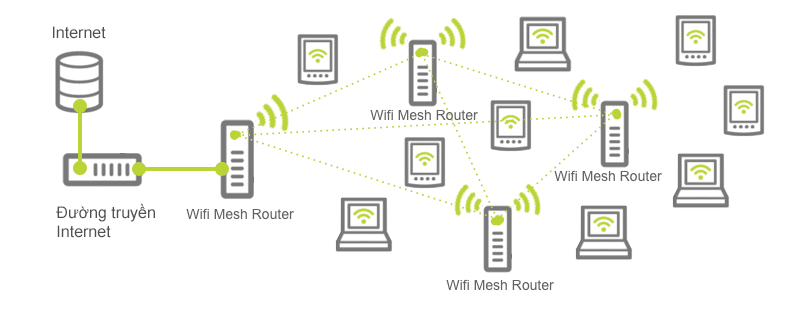
Ưu điểm của cấu trúc mesh :

+Mở rộng mạng: Mạng mesh cho phép mở rộng phạm vi mạng một cách dễ dàng.

+Độ tin cậy cao: Do sự tự động chuyển tiếp dữ liệu và khả năng tự phục hồi, mạng mesh có tính khả năng chịu lỗi cao.

+ Thuận tiện với người dùng cuối : mạng wifi mesh thường cung cấp 1 SSID trên tất cả các AP và tích hợp công nghệ roaming giúp di chuyển liền mạch.

- Có 2 phương thức kết nối giữa các AP mesh là qua mạng cáp LAN (Ethernet backhaul) hoặc Wifi (Wireless backhaul). Ưu tiên sử dụng cáp LAN để bảo tốc độ cũng như độ ổn định.



* Cấu trúc mạng mesh nhỏ dành cho cá nhân, gia đình thường bao gồm :

+ 1 Mesh root có khả năng chịu trách nhiệm quản lý, định tuyến và điều phối lưu lượng mạng trong toàn bộ mạng mesh, đảm bảo topology mạng, máy chủ DHCP Server, NAT, firewall.

+ Và 1 hoặc nhiều mesh agent, Mesh Agent (hoặc còn gọi là Node hoặc Client Node) là các thiết bị AP trong mạng mesh có nhiệm vụ tham gia gửi/nhận dữ liệu trong mạng. Mesh Agent không có khả năng quản lý hoặc định tuyến cho toàn bộ mạng mesh, mà chỉ tham gia truyền tải dữ liệu và thực hiện các chức năng mạng cơ bản.

**D. TỐC ĐỘ**

**1. Dạng tốc độ tối đa mà card mạng hỗ trợ hay còn gọi là tốc độ liên kết (PHY Rate):**

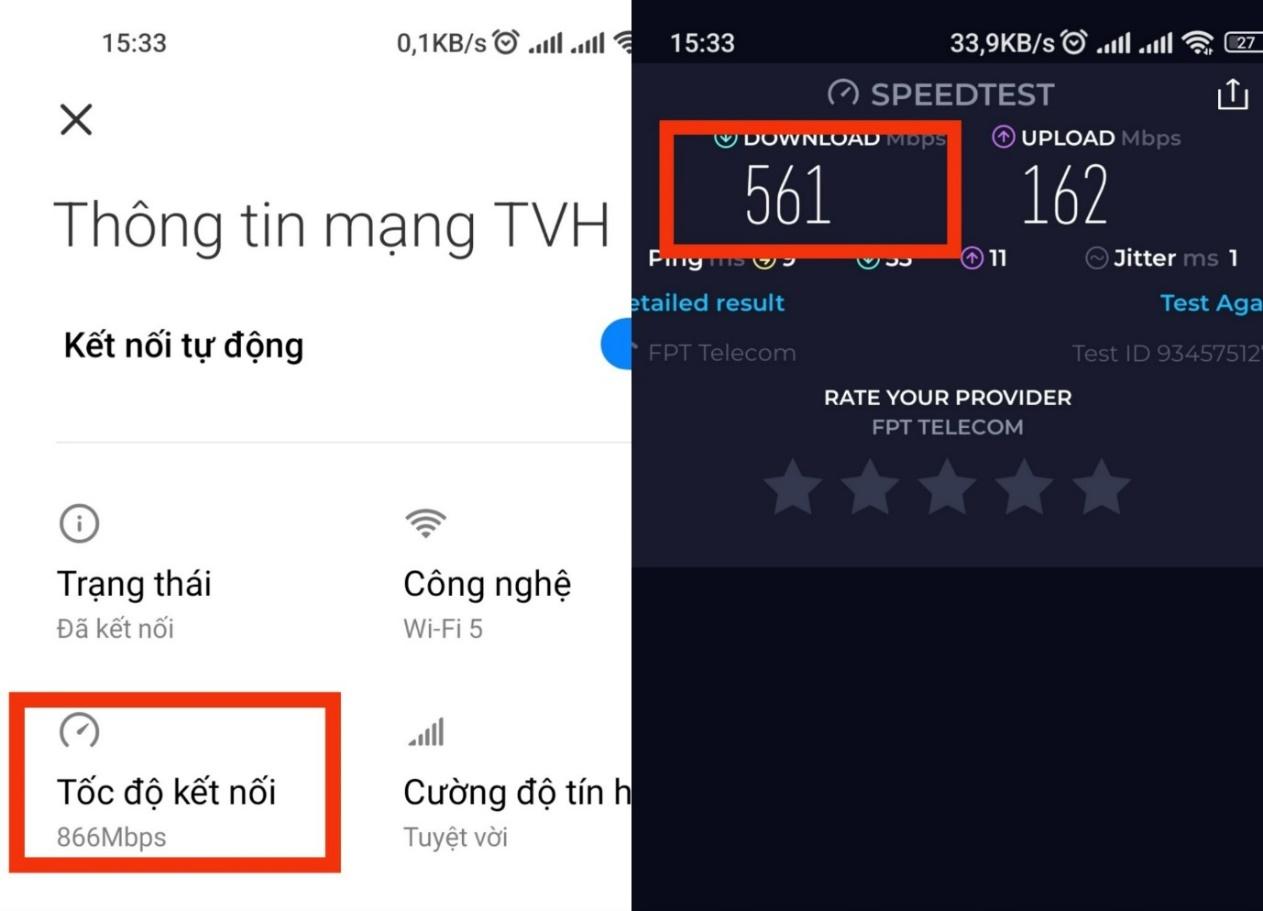
+ Tốc độ này được hình thành bởi 2 card mạng liên kết với nhau (ví dụ card mạng trên AP và card mạng trên điện thoại). Tốc độ này phụ thuộc vào chuẩn công nghệ (wifi 5, wifi 6, LAN), tùy thuộc vào yếu tố tác động khác nhau sẽ có các mức tốc độ cố định khác nhau dựa vào cài đặt của nhà sản xuất.

**2. Dạng tốc độ hiển thị qua các phần mềm đo tốc độ (app speedtest) :**

+ Trước tiên, cần biết rằng 1 gói tin truyền qua 1 card mạng nó không chỉ mang dữ liệu người dùng (payload : nhạc, hình, phim...) mà còn kèm theo nhiều thành phần (địa chỉ MAC, địa chỉ IP, bit sữa lỗi, các thành phần quản lí khác...).

+ Trong khi đó, các phần mềm đo tốc độ chỉ đọc phần dữ liệu người dùng (payload), do đó dù là môi trường tiêu chuẩn thì tốc độ qua phần mềm đo sẽ hiển thị thấp hơn tốc độ card mạng, ngoài ra nó còn phụ thuộc vào gói cước internet sử dụng.

+ Thông thường tốc độ speedtest ở cổng LAN *tối đa là 94%* tốc độ PHY card mạng. Nghĩa là card mạng 1Gbps sẽ speedtest được tối đa 940Mbps điều kiện chuẩn (Công nghệ luôn thay đổi, ở đây tính tại thời điểm viết bài).

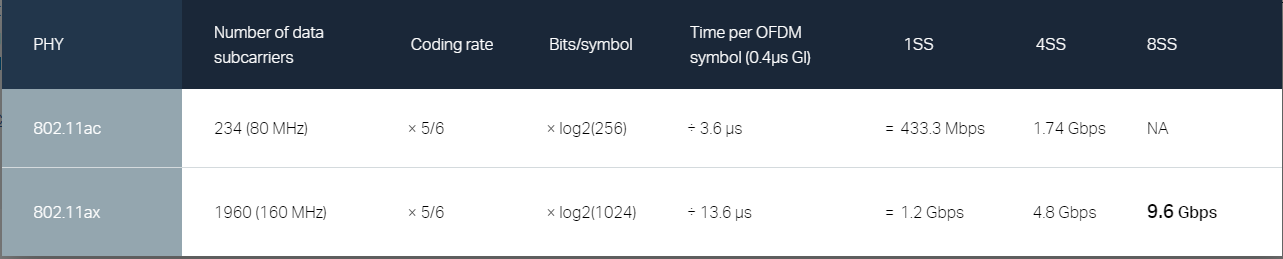
+ Ở Wifi tùy theo tiêu chuẩn và các yếu tố tác động khác, speedtest tối đa nằm trong khoảng 65% tốc độ card mạng. Ví dụ điện thoại card mạng Wifi AC 433Mbps thì speedtest tối đa sẽ khoảng 281 Mbps. 

TỐC ĐỘ LIÊN KẾTCỦA CARD MẠNG TỐC ĐỘ QUA APP SPEEDTEST

* **Ví dụ về cách tính PHY Rate của wifi, ta có công thức :**

PHY Rate = (Số lượng sóng mang con x coding rate x bit/symbol) /Thời gian khoảng Symbol

Ở chuẩn 802.11ac với mô phỏng có (1 anten x 234 sóng mang con (80Mhz độ rộng kênh) x coding rate là 5/6 x điều chế 256QAM ta có 8 bit )/ khoảng thời gian symbol 3,6uS= 433 Mbps.



**E. THIẾT BỊ MẠNG**

1. **Router :**

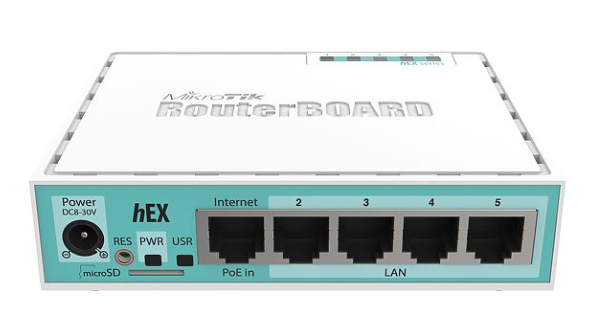
**Router** : bộ định tuyến, là thiết bị mạng máy tính dùng để chuyển các gói dữ liệu qua một liên mạng và đến các đầu cuối, thông qua một tiến trình được gọi là định tuyến.

*Chúng ta có thể nhân hóa nó như 1 bưu cục chuyển phát, nhận gói hàng từ địa chỉ người gửi và gửi đến địa chỉ người nhận.*

Router làm việc với địa chỉ IP, thực hiện chức năng của Lớp 3 trong mô hình mạng OSI.

Một số tính năng tích hợp thường có trên router : DHCP Server, NAT, Routing, Firewall, một số dòng router tích hợp thêm Wifi.





**2.Switch :**

-Là một thiết bị trong hệ thống mạng máy tính dùng để kết nối các thiết bị mạng khác nhau và chuyển tiếp dữ liệu giữa chúng.

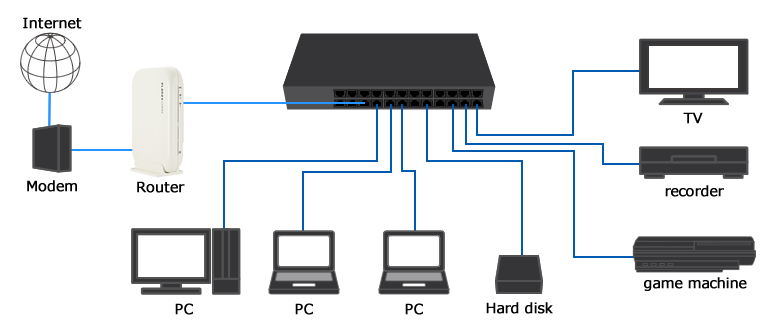
-Switch mạng hoạt động ở tầng 2 (tầng Data Link) và tầng 3 (tầng Network) trong mô hình OSI (Open Systems Interconnection). Ở phạm vi tài liệu này, chúng ta sẽ tìm hiểu về Switch tầng 2 (Layer 2).

-Switch làm việc với địa chỉ MAC, Khi nhận được gói dữ liệu, switch mạng sẽ đọc địa chỉ MAC đích trong gói và xác định cổng kết nối tương ứng trong bảng MAC Table để chuyển tiếp gói đến thiết bị đích.

- Switch mạng cung cấp băng thông riêng biệt cho mỗi cổng kết nối, giúp tránh xung đột và đảm bảo truyền dữ liệu nhanh chóng và hiệu quả.

| **MAC TABLE** | |
| --- | --- |
| MAC | Port |
| AA:AA:AA:AA:AA:AA | 1 |
| BB:BB:BB:BB:BB:BB | 2 |

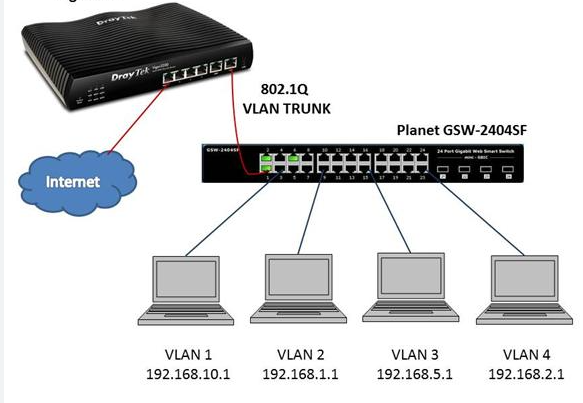
- Đa số nhiệm vụ của switch trong mô hình đơn giản là chia 1 cổng mạng thành nhiều cổng mạng đáp ứng cho số lượng client dùng kết nối có dây. Với những nhu cầu cao cấp hơn người dùng cho thể lựa chọn dòng switch quản lí (Managed switch) có thêm tính năng VLAN, giám sát quản lí, Qos, DHCP Snooping, Spanning Tree Protocol…



*+ VLAN trên Switch gồm 2 loại port chính là*

1.*Trunk Port (Cổng Trunk)* : cổng trunk cho phép nhiều vlan đi qua.

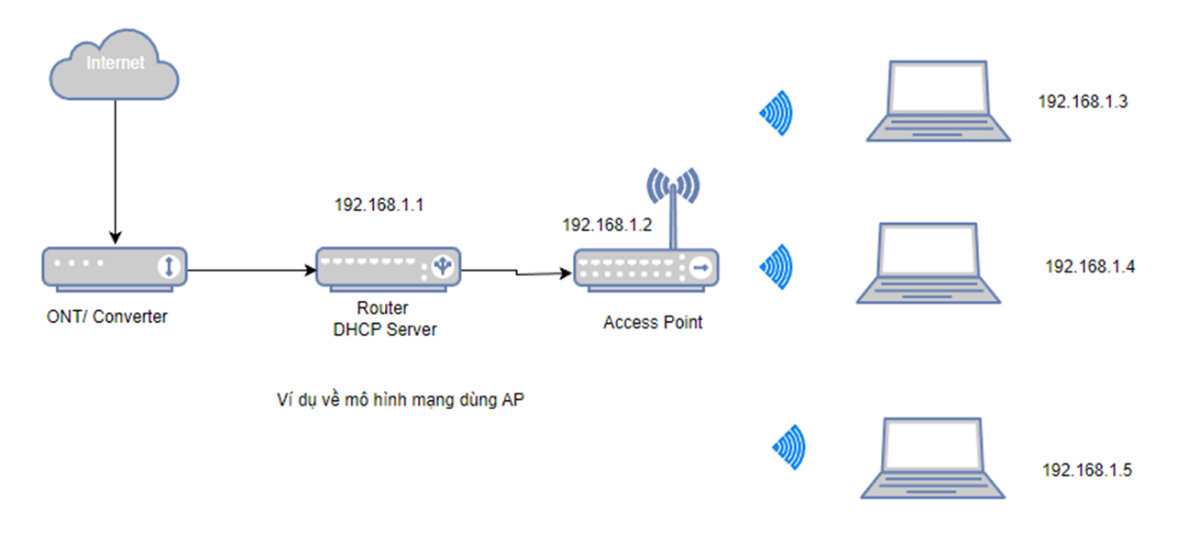
2.*Access Port (Cổng Access):* Access port là cổng trên switch được cấu hình thuộc một VLAN cụ thể.



**3.Access Point :**

**- Access Point (AP)** là một thiết bị mạng không dây (wireless) dùng để kết nối các thiết bị không dây (như máy tính, điện thoại di động, máy tính bảng) vào một mạng có dây (wired network) hoặc mạng không dây lớn hơn.

-Access Point hoạt động như một trạm gốc trong mạng không dây. Nó có thể được kết nối trực tiếp với một router hoặc switch mạng để cung cấp kết nối mạng cho các thiết bị không dây trong phạm vi tương đối gần.

-Access Point thuần túy không cung cấp dịch vụ DHCP (Dynamic Host Configuration Protocol).

**4.Modem, ONT, SFP, Media Converter :**

**- Modem :** Modulator-demodulator là bộ điều chế và giải điều chế, ví dụ phía máy tính A muốn gửi 1 bài hát qua cáp đồng đến máy tính B thì hiệu số đó phải được điều chế sang tín hiệu analog thì mới có thể truyền đi xa trong môi trường truyền dẫn, phía đầu nhận lại giải điều chế tín hiệu analog sang tín hiệu số để máy tính xử lí => Đó là công việc của modem, modem đã tồn tại từ thời điểm cáp đồng ADSL.



**-ONT : (Optical Network Terminal**), là thiết bị đầu cuối mạng quang, thường đặt ở nhà khách hàng. Tính năng của nó tương tự như modem hoạt động với mạng quang. Chuyển đổi tín hiệu quang học sang điện (số) để máy tính, router có thể xử lí.



**-SFP** : Small Form-factor Pluggable (ngữ cảnh bài này nói đến SFP quang) là module nhỏ gắn trực tiếp vào các thiết bị mạng như switch, router, server, hoặc thiết bị mạng khác để chuyển đổi tín hiệu điện (số) sang tín hiệu quang và ngược lại.

Ưu điểm dễ thấy của SFP so với ONT là nhỏ gọn hơn và hầu hết không cần nguồn rời.



-**Optical Media Converter** : Như tên gọi, nó là 1 bộ chuyển đổi quang sang điện (với cổng Ethernet RJ45), có thể tích hợp slot SFP dễ dàng tương thích với các hạ tầng công nghệ khác nhau.

Vậy chứ năng có vẻ tương tự ONT, thật ra xét kĩ hơn Media Converter chỉ phục vụ việc chuyển tín hiệu quang sang điện, với ONT có thể đơn thuần chuyển quang sang điện hoặc có thể nhà sản xuất thêm các tính năng nâng cao như định tuyến, DHCP Server nên tính năng của nó sẽ mở rộng với chỉ 1 tên gọi ONT.

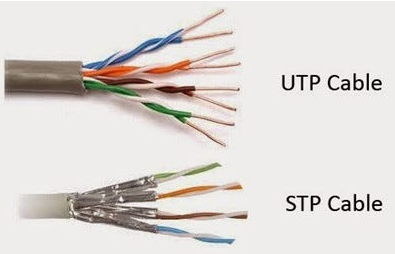
**\*Câu hỏi** : Tại sao lại có nhiều thiết bị như vậy sao nhà mạng chỉ cấp 1 thiết bị modem wifi nhưng tôi vẫn sử dụng được tất cả dịch vụ ?

Trả lời : Vì thiết bị modem wifi nhà mạng cung cấp là thiết bị tích hợp, nó có sẵn module quang – điện, router và bộ phát wifi.

**5.Cáp LAN :** Local Area Network Cable là một loại cáp được sử dụng để kết nối các thiết bị trong mạng cục bộ (LAN) như máy tính, máy in, điểm truy cập, và thiết bị mạng khác. Cáp LAN chủ yếu được sử dụng để truyền tải dữ liệu giữa các thiết bị trong một phạm vi nhỏ, chẳng hạn trong một tòa nhà hoặc một văn phòng.

Trong tài liệu này chúng ta đề cập đến loại cáp kim loại xoắn (Twisted Pair), cáp xoắn phổ biến gồm 2 loại là STP (Shielded Twisted Pair) và UTP (Unshielded Twisted Pair).

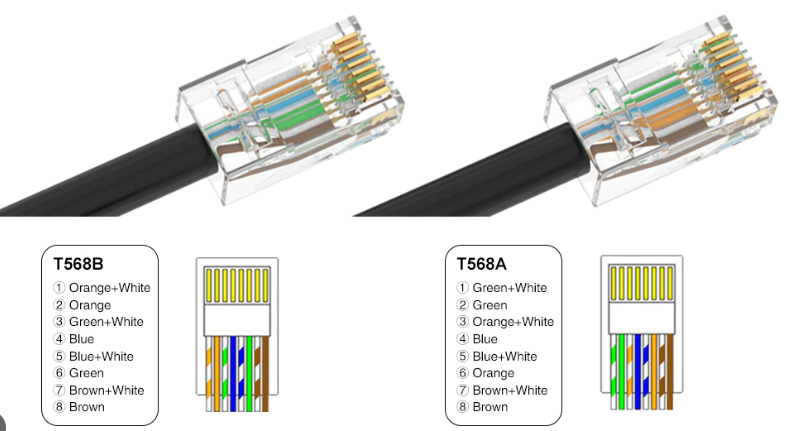
- Cáp STP là loại cáp xoắn đôi mà lõi cáp được bao bọc bởi một lớp nhôm bảo vệ, chống nhiễu điện từ. Trong khi đó cáp UTP là loại cáp không có lớp nhôm chống nhiễu, các cặp cáp xoắn được để trần.



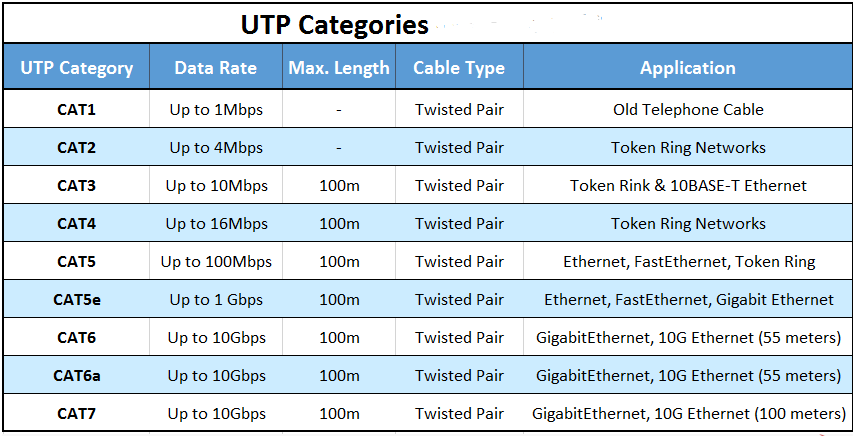
*-Hiện tại có 2 chuẩn bấm dây :*

Chuẩn T568A (chuẩn A) và T568B(chuẩn B) để đấu nối các thiết bị như sau :

| Cáp thẳng 2 đầu đều chuẩn A hoặc B | Cáp chéo 1 đầu chuẩn A và 1 đầu chuẩn B |
| --- | --- |
| Nối switch đến router Nối switch đến PC  Nối hub đến PC | Nối switch đến switch Nối switch đến hub Nối hub đến hub Nối router đến router Nối PC đến PC Nối router đến PC |



*Phân loại cáp LAN theo Cat :*



**-** Với các gói cước tối đa hiện nay là 1Gbps thì cáp UTP Cat5 là đáp ứng tốt cho hầu hết các dịch vụ. Tuy nhiêu về lâu dài hoặc bạn làm việc với các hệ thống tốc độ cao lớn hơn 1Gbps thì Cat6 trở lên là 1 lựa chọn hợp lí.

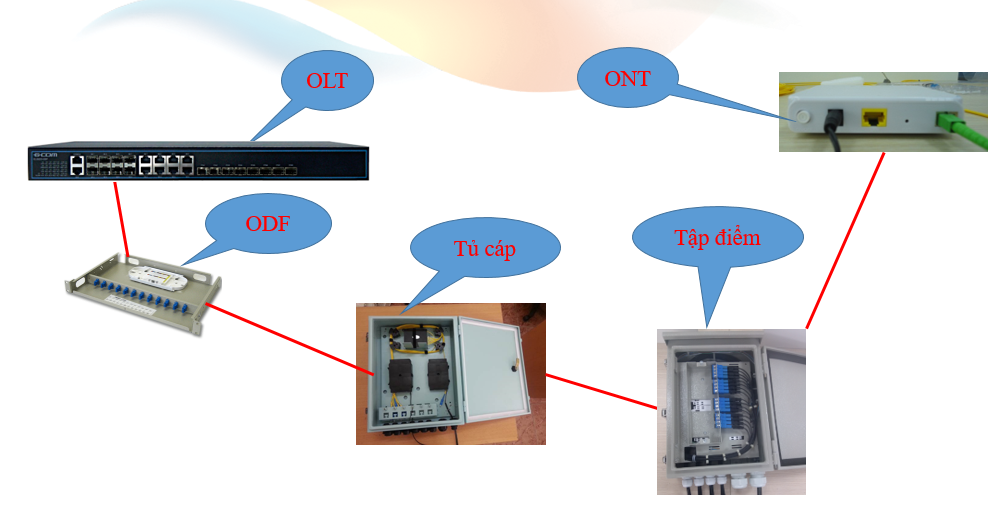
**F. Mạng quang (Optical Network)**

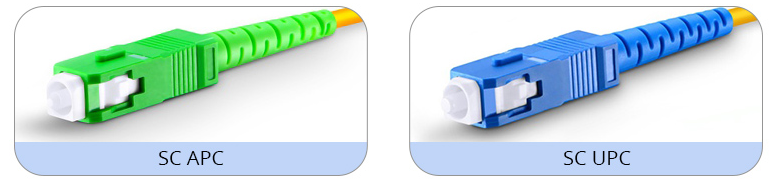
- Là một hệ thống mạng truyền thông sử dụng sợi quang để truyền tải dữ liệu bằng ánh sáng. Cáp quang được sử dụng vì khả năng truyền tải dữ liệu ở tốc độ cao và khoảng cách xa hơn so với các phương tiện truyền thông khác như cáp đồng trục hoặc sóng radio.

Trong tài liệu này chúng ta sẽ tìm hiểu về GPON, là công nghệ có độ phổ biến nhất hiện nay tại Việt Nam.

**GPON (Gigabit Passive Optical Network)** : Là mạng quang thụ động được sử dụng phổ biến hiện nay. Trong mạng GPON, tín hiệu dữ liệu được truyền tải bằng cách sử dụng sợi quang kết nối các điểm đầu và cuối trong mạng. GPON sử dụng phương thức chia sẻ băng thông giữa nhiều thiết bị khách hàng, trong đó một trạm chủ (OLT - Optical Line Terminal) quản lý việc chia sẻ và phân phối dữ liệu tới các ONT (Optical Network Terminal) ở các vị trí khách hàng.

*Sơ đồ cơ bản của 1 mạng GPON :*



* Ở Việt Nam, GPON thường hoạt động ở bước sóng 1490nm hướng từ OLT đến ONT và 1310nm hướng ngược dòng từ ONT về OLT.
* Tiêu chuẩn GPON cung cấp tốc độ tối đa 2.5Gbps download và 1.25Gbps upload.
* Để kết nối tiện lợi giữa các điểm kết nối cáp quang thường dùng 1 thiết bị gọi là Fast Connecter (FC), có nhiều loại FC khác nhau nhưng phổ biến là SC/APC và SC/UPC
* 

**G.MỘT SỐ MÔ HÌNH TRIỂN KHAI ROUTER – WIFI THAM KHẢO**

**I. Mô hình chịu tải cao :**

1.Loại Router : Mô hình này cần Router chịu tải cao, có thể cân bằng tải nhiều đường WAN, tích hợp nhiều chức năng chuyên sâu như giới hạn BW,Session, QoS Protocol, VLAN...

- Quay PPPOE trực tiếp trên router, modem nhà mạng chuyển Bridge hoặc đổi ONT/Converter.

Nên lựa chọn thương hiệu uy tín như Draytek, Mikrotik...

2. Loại AP : Cần sử dụng AP chịu tải cao, roaming tốt, có thể quản lí tập trung, hỗ trợ nhiều công nghệ tối ưu như :

Bandsteering : Cân bằng tải client nhiều băng tần.

Airtime Fairness : Công bằng thời gian phát sóng, hạn chế 1 client chiếm kênh truyền quá lâu.

MU-MIMO : Đa người dùng đồng thời.

PMF : Bảo vệ tránh bị tấn công deauth gây rớt mạng.

.......

Nên lựa chọn thương hiệu uy tín như Unifi, Aruba...

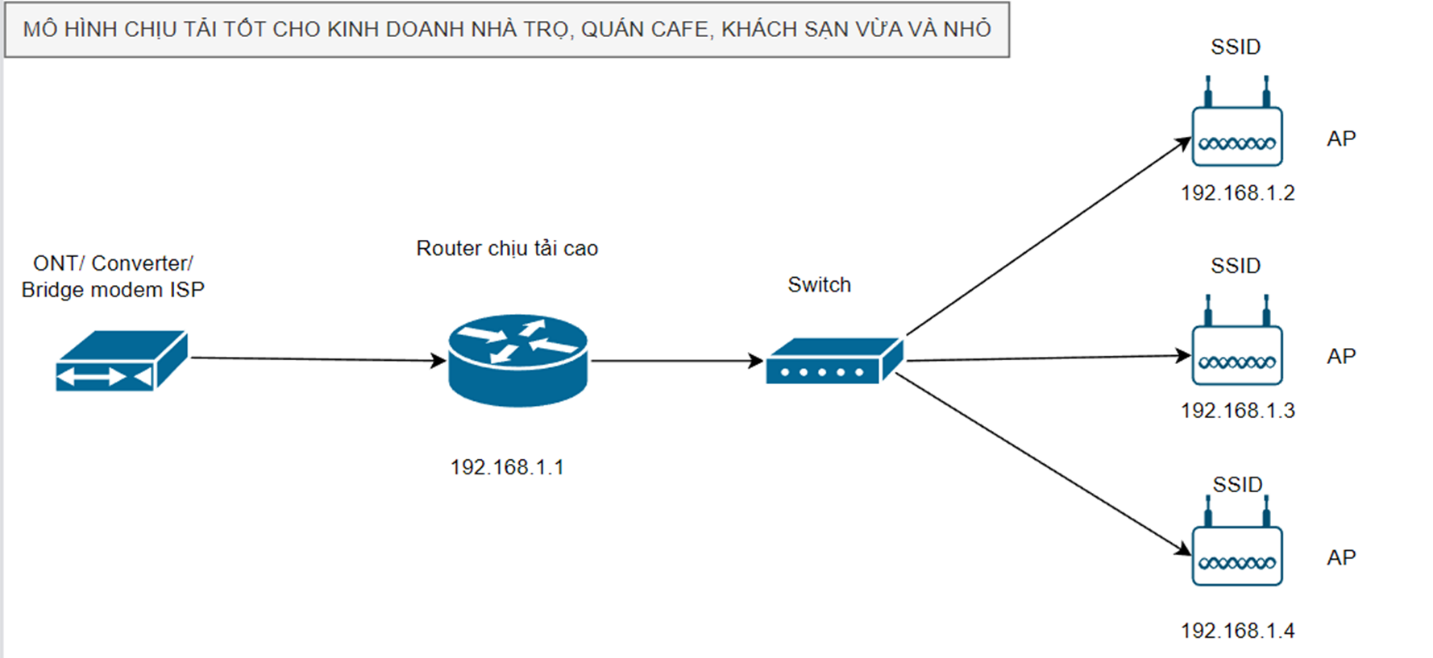
3. Switch : Tùy vào nhu cầu có thể lựa chọn SW L2/L3/Managed/Unmanaged.

Nhưng nếu hệ thống phức tạp nhiều thiết bị nên chọn dòng hỗ trợ tính năng cơ bản :

DHCP Snooping : Tính năng này tránh 1 thiết bị lạ cấp ngược DHCP gây lỗi mạng.

Loop Protection : Bảo vệ tránh loop do cắm nhầm port gây lỗi mạng,cơ chế thường là khóa port loop.

VLAN : Một tính năng cần thiết nếu cần sự riêng tư và khi số lượng client quá lớn thì việc chia VLAN để giảm broadcast cũng là 1 phương án tốt.



**II. Mô hình dùng Mesh :**

1.Loại AP : Sử dụng AP hỗ trợ MESH.

2. Phương thức đấu nối :

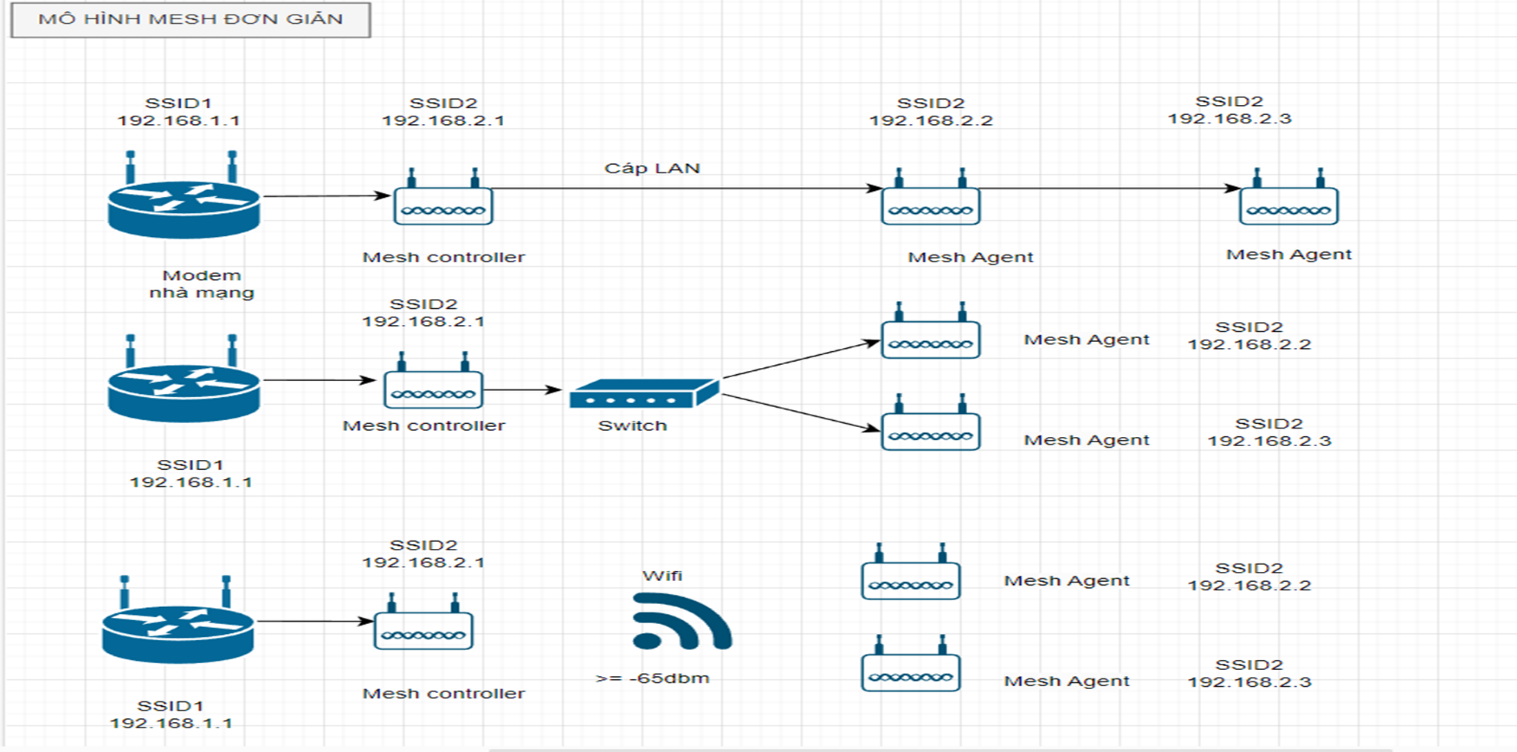
Cách 1 : Sử dụng cáp LAN, nối từ cổng LAN modem nhà mạng sang cổng WAN AP Mesh Controller, các AP còn lại nối tiếp vào AP Mesh Controller.

Cách 2 : Sử dụng cáp LAN, nối từ cổng LAN modem nhà mạng sang cổng WAN AP Mesh Controller, các AP còn lại kết nối AP Mesh controller bằng Wifi ,tuy nhiên cần lưu ý RSSI các AP Mesh Agent cần thu được tối thiểu - 65dbm ở băng tần 5Ghz để hạn chế suy giảm tốc độ.

3.Cấu hình : Hệ thống mesh chạy cùng dải IP modem nhà mạng hoặc khác modem nhà mạng tùy theo trường hợp cụ thể.

Modem nhà mạng có thể Bridge hoặc đổi thành ONT nếu cần thiết.

Tuy nhiên cần lưu ý, các AP Mesh Agent cần cắm sau AP Mesh controller, KHÔNG ĐƯỢC CẮM SONG SONG VÀO MODEM NHÀ MẠNG NẾU MODEM NHÀ MẠNG KHÁC CHỦNG LOẠI SẼ DỄ LÀM LỖI MẠNG.



**III. Mô hình đơn giản giá thành rẻ :**

1.Loại AP : các loại AP cơ bản 1 hoặc 2 băng tần giá rẻ.

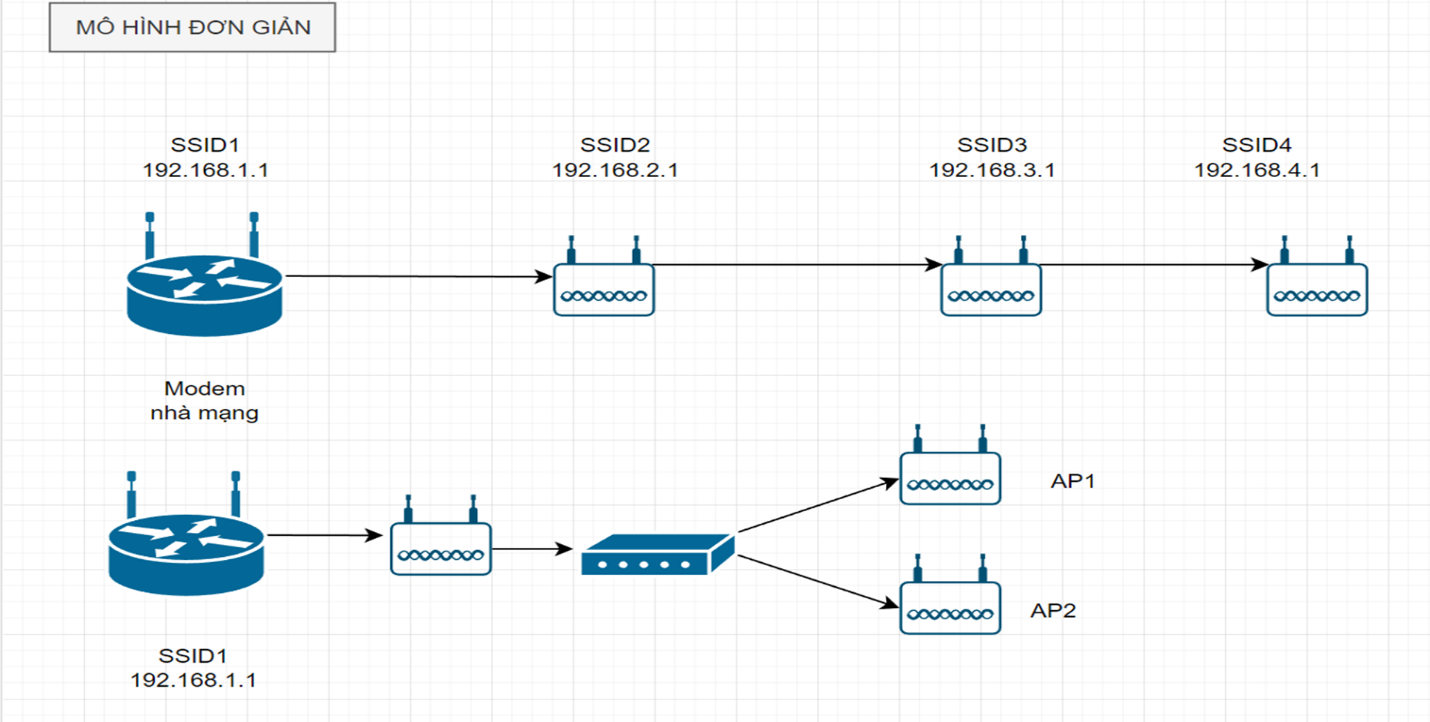
2.Phương thức đấu nối : Sử dụng cáp LAN, nối từ cổng LAN modem nhà mạng sang cổng WAN AP1 và AP2.

3.Cấu hình : Mỗi AP 1 lớp mạng khác nhau và tên Wifi khác nhau.

4.Đây là mô hình đơn giản nhất, chi phí thấp để triển khai cho hộ gia đình ít thiết bị, nhu cầu không cao nhưng diện tích rộng cần mở rộng vùng phủ bằng AP.

5. Ưu điểm : chi phí thấp, thiết kế đơn giản.

6. Nhược điểm : Không hỗ trợ roaming và các tính năng nâng cao, khó quản lí.



**H. Q&A**

**Câu hỏi 1 :** Nên tránh lắp đặt AP wifi tại nhưng vị trí nào ?

Trả lời : Nên tránh lắp AP wifi tại nhưng vị trí khuất như gầm tủ, gầm bàn, gầm cầu thang vì dễ bị chắn sóng. Tránh lắp gần các thiết bị điện tử như sau tivi, nóc tủ lạnh hoặc cạnh lò vi sóng sẽ bị ảnh hưởng.

**Câu hỏi 2 :** Tôi nghe nói về wifi mesh, có thể mở rộng vùng phủ sóng mà không cần phải đi dây mạng rất tiện lợi ? Tôi có nên sử dụng nó ?

Trả lời : Đúng nó rất tiện lợi nếu bạn muốn mở rộng vùng phủ sóng mà không cần phải kéo dây mạng rườm rà. Tuy nhiên nếu yếu tố môi trường không thuận lợi sẽ dễ dẫn đến nhiễu, độ trễ cao, băng thông suy giảm, hơn nữa bản chất của wifi là half duplex nghĩa là trong 1 thời điểm trên 1 băng tần wifi nó chỉ có thể gửi hoặc nhận (ít nhất là cho đến wifi 6) vậy nên việc liên kết các AP bằng wifi thì độ trễ tăng và ảnh hưởng băng thông ít nhiều là điều chắc chắn.

Do vậy, tôi khuyên bạn nên cố gắng liên kết bằng cáp mạng nếu có thể.

**Câu hỏi 3 :** Vậy repeater và Wifi mesh khác gì nhau nếu liên kết giữa các AP bằng Wifi :

Trả lời : Về vật lí phần cứng chúng gần như tương tự nhau, nhận dữ liệu từ 1 mạng wifi và phát lại chúng. Tuy nhiên wifi mesh được nâng cấp thêm các giao thức roaming, tự cấu hình và tìm đường dẫn tốt hơn trong định tuyến gói tin.

**Câu hỏi 4** : Tôi có nghe nhiều người nói rằng nên bridge router nhà mạng cấp để tự mua 1 router khác quay PPPOE, có nên làm vậy không ?

Trả lời : Có và Không, điều đó phụ thuộc vào nhu cầu của bạn.

Router đơn giản là 1 máy tính thu nhỏ, nó bao gồm CPU, RAM, bộ nhớ NAND, chipset Wifi và 1 hệ điều hành (ví dụ linux). Nên cũng giống 1 chiếc máy tính cá nhân, nếu cấu hình của nó không đáp ứng nhu cầu của bạn thì bạn có thể mua 1 chiếc router khác mạnh mẽ hơn và thay thế vào, còn nếu nó vẫn đáp ứng tốt thì việc thay thế là lãng phí.

Việc Bridge router nhà mạng nghĩa là chuyển router nhà mạng về đơn thuần 1 thiết bị chuyển đổi tín hiệu quang điện như ONT/Converter, lúc này bạn thực hiện quay PPPOE, định tuyến, NAT, DHCP… trên 1 thiết bị khác.

**Câu hỏi 5 :** Tại sao tôi đăng kí gói mạng 1Gbps nhưng speedtest qua modem cổng LAN 1Gbps chỉ được 300 400Mbps hoặc cao lắm là 940Mbps ?

Trả lời : Thông lượng thực tế sẽ phụ thuộc vào phần cứng của thiết bị, ví dụ bạn có 1 router cổng LAN 1Gbps nhưng CPU của nó thông lượng tối đa chỉ 300Mbps thì nó sẽ không thể vượt qua tốc độ đó.

Đồng thời với cổng LAN 1Gbps thông thường dữ liệu người dùng sẽ vào khoảng 94%, nghĩa là khoảng 940Mbps, phần còn lại là chi phí cho các phần quản lí.

**Câu hỏi 6** : Tôi thấy AP quảng cáo là 300Mbps nhưng sao điện thoại tôi chỉ hiện kết nối là 65Mbps ?

Trả lời : Ở trong trường hợp này 300Mbps là tốc độ tối đa mà AP hỗ trợ, cùng 1 chuẩn wifi nhưng sẽ có nhiều mức tối độ khác nhau, thậm chí nó còn thay đổi tùy thuộc vào yếu tố môi trường, để client nhận được đủ 300Mbps sẽ còn phụ thuộc vào chuẩn phần cứng của client, ở đây bạn nhận được 65Mbps dù trên AP đã cấu hình mức cao nhất thì nghĩa là card mạng trên client của bạn chỉ hỗ trợ mức tốc độ 65Mbps.

**Câu hỏi 7** : Router cân bằng tải là gì ?

Trả lời : Trước tiên, cân bằng tải (load balancing) là một kỹ thuật trong mạng máy tính để phân phối công việc và tải giữa các thiết bị mạng, máy chủ hoặc đường truyền khác nhau, nhằm đảm bảo sự tối ưu hóa hiệu suất hoạt động của mạng và ngăn chặn tình trạng quá tải.

Cân bằng tải trên mạng LAN: Cân bằng tải có thể thực hiện trên mạng nội bộ để phân phối lưu lượng giữa các thiết bị trong mạng LAN.

Cân bằng tải trên mạng WAN: Cân bằng tải có thể thực hiện trên mạng WAN để phân phối lưu lượng giữa các đường truyền WAN khác nhau.

Router cân bằng tải thường được xem lại 1 router có khả năng chịu tải cao, nhiều tính năng chuyên sâu, hỗ trợ kết nối cùng lúc nhiều đường truyền WAN.

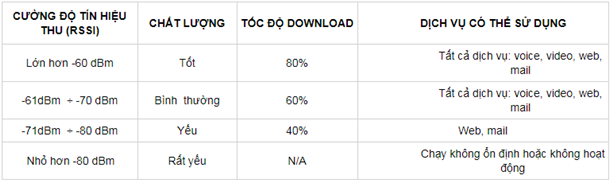
**Câu hỏi 8 :** Tôi có 1 AP 2 băng tần wifi 2.4Ghz và 5Ghz, tôi nên tách tên hay để cùng tên 2 băng tần ?

Trả lời : Tất nhiên sẽ tuy theo trường hợp, nếu bạn thường xuyên di chuyển ra vào giữa 2 vùng phủ sóng 2.4G/5Ghz thì nên đặt cùng tên, vì nếu khác tên tính chất sóng 2.4Ghz thường phát xa hơn 5Ghz khi bạn ra khỏi vùng phủ sóng 5Ghz client sẽ nhảy qua 2.4Ghz nhưng khi quay trở lại vùng có 5Ghz điện thoại vẫn sẽ giữ 2.4Ghz, mà 2.4Ghz tốc độ thấp hơn 5Ghz và nhiễu nhiều hơn nên không tối ưu. Nếu đặt cùng tên thì điện thoại sẽ lựa chọn tối ưu hơn khi di chuyển.

Hoặc nơi phức tạp mật độ cao nên đặt cùng tên để cân bằng tải tránh dồn vào 1 băng tần gây quá tải.

Trường hợp cần tách tên khi bạn muốn luôn luôn sử dụng 1 băng tần nào đó.

**Câu hỏi 9** : Nên khảo sát lắp đặt AP với RSSI như thế nào ?

Trả lời : Nên lắp đặt AP sao cho các vị trí cần sử dụng mạng có RSSI từ -65dbm trở lên để có chất lượng tốt. Hãy tham khảo bảng sau :  


**Câu hỏi 10** : Tôi đang lắp 1 đầu ghi Camera nhưng lại không thể mở port ?

Trả lời : Rất có thể bạn đang nằm trong dải IP CGNAT, do Ipv4 đã cạn kiệt nên các ISP thường dùng phương pháp NAT để có thể có nhiều Ipwan cấp cho router của khách hàng. Nếu bạn đạng trong dải IPNAT thì có thể gây lỗi khi mở port, cách kiểm tra là vào web canyousee xem IP hiển thị có trùng với IP wan trên router không ? Nếu không hãy gọi tổng đài hỗ trợ.

**Câu hỏi 11** : Tại sao 1 số trang web cần phải đổi DNS mới vào được ?

Trả lời : DNS có nhiệm vụ phân giải tên miền sang IP và ngược lại. Nếu tên miền trang web của bạn không có trong cơ sở dữ liệu của DNS thì nó không phân giải được. Vậy nên bạn sẽ cần đổi sang 1 DNS khác.

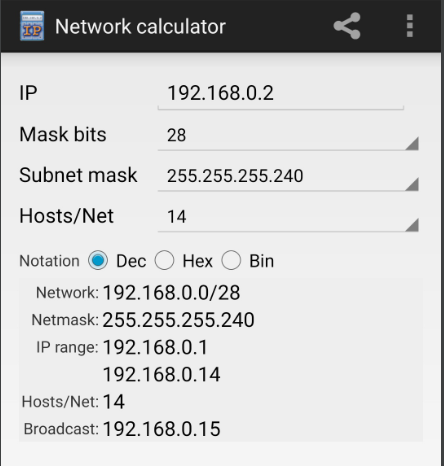


**Câu hỏi 12** : Tôi có 1 mạng 192.168.1.0 –subnet mask 255.255.255.0, nó chỉ có tổng 254 IP cấp cho client, làm sao có thể tăng nó lên ?

Trả lời : Hãy thay đổi subnet mask bạn sẽ có nhiều IP cấp cho client hơn, ví dụ mạng 192.168.1.0 nhưng nếu bạn thay đổi subnet mask thành 255.255.254.0 bạn sẽ có 510 IP.

Hoặc bạn cũng có thể sử dụng 1 dải IP thuộc lớp mạng khác để có IP cấp cho client nhiều hơn. Hãy tham khảo các tài liệu về tính toán IP.

Bạn hoàn toàn có thể sử dụng 1 phần mềm hỗ trợ như Network Calcalutor để hỗ trợ tính toán.



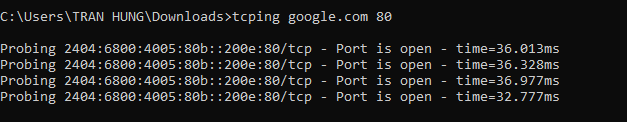
**Câu hỏi 13** : Tôi đăng kí dịch vụ truyền hình IPTV Multicast của 1 nhà mạng, nêu dùng router nhà mạng thì xem tốt, tuy nhiên tôi sử dụng router tự mua thì bị giật xé hình ?

Trả lời : Router nhà mạng cấp đã được tối ưu cho dịch vụ IPTV, thông được đã được QoS sẵn cho dịch vụ IPTV nên khi bạn dùng router tự trang bị không hỗ trợ tốt theo chuẩn của nhà mạng sẽ bị packet loss hoặc tăng độ trễ dẫn đến giật xé hình. Hãy tham khảo nhà cung cấp dịch vụ trước khi lựa chọn router.

**Câu hỏi 14 :** Tôi muốn kiểm tra đầu ghi camera có đang mở port theo yêu cầu hay không thì bằng cách nào ?

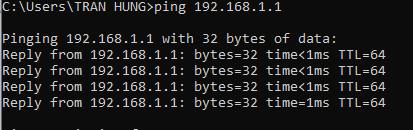
Trả lời : Hãy sử dụng công cụ tcping , thực hiện lệnh với cú pháp

tcping <tênmiềnhoặcipcần kiểm tra> <portcầnkiểmtra> , nếu báo Open nghĩa là mở, còn No response là không nhận được phản hồi là đóng.



**Câu hỏi 15 :** Tôi muốn kiểm tra xem router của mình ổn định không bằng cách nào ?

Trả lời : Cách đơn giản nhất mà bất cứ ai cũng có thể thao tác là dùng lệnh Ping, hãy ping IP của router sẽ có 2 yếu tố :

1. Thông thường lệnh ping đến router nội bộ sẽ khoảng <1ms nếu dùng cáp lan.
2. Từ 1-3ms nếu dùng wifi trên windows, nhỏ hơn 20ms nếu dùng wifi trên hệ điều hành android.

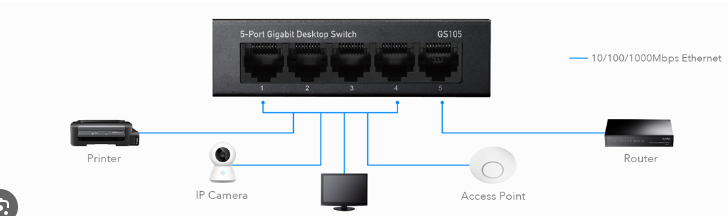
* Nếu vượt qua các chỉ số trên quá nhiều lần và tỉ lệ rớt gói cao, hãy kiểm tra lại router hoặc client của bạn.

**Câu hỏi 16** : Tôi thực hiện Ping đến router kết quả <1ms nhưng truy cập 1 số web rất chậm ?

Trả lời : Lúc này nó sẽ liên quan đến đường truyền mạng của bạn hoặc server web bạn truy cập. Hãy thử ping đến web bạn truy cập xem kết quả thế nào ? Đồng thời liên hệ nhà cung cấp dịch vụ để kiểm tra hỗ trợ.

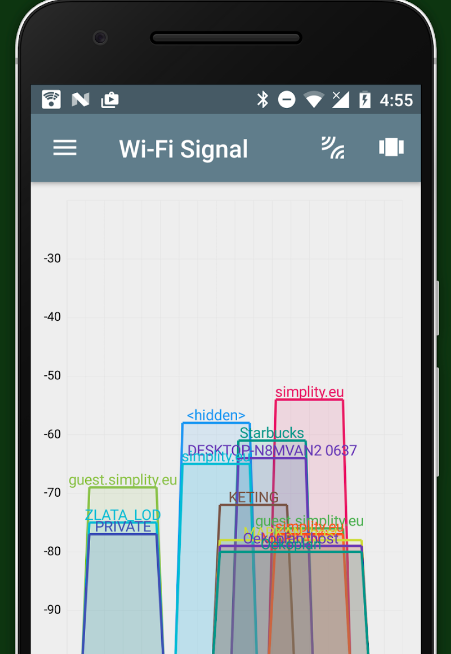
**Câu hỏi 17 :** Router nhà tôi có chỉ 4 cổng nhưng đã dùng hết, giờ muốn thêm cổng thì làm sao ?

Trả lời : Hãy lắp thêm switch, dùng 1 sợi dây mạng cắm từ router qua switch, tại switch sẽ có nhiều cổng để đáp ứng nhu cầu.



**Câu hỏi 18 :** Tôi ở chung cư khu vực sóng wifi mật độ cao cứ đến tôi mọi người về là yếu, tôi dùng AP wifi đời cũ chỉ có 1 sóng 2.4Ghz, máy tính cắm dây mạng vẫn hoạt động bình thường ?

Trả lời : Bạn hãy dùng 1 phần mềm quét các wifi xung quanh (ví dụ Net analyzer) để quét xem khu vực bạn đang ở có bị trùng kênh quá nhiều không ? Nếu bị trùng ở mọi kênh thì bạn có thể cân nhắc đổi sang loại AP wifi có băng tần 5Ghz hoặc 6Ghz (nếu client của bạn hỗ trợ) điều đó sẽ giảm thiểu việc nhiễu do trùng kênh.



**Câu hỏi 19 :** Tại sao tôi chơi game ping cao trong khi coi youtube bình thường ?

Trả lời : Loại bỏ yếu tố đường truyền và server, dịch vụ video yêu cầu băng thông cao nhưng độ trễ trung bình trong khi chơi game online cần độ trễ cực thấp để tương tác với máy chủ.

Do vậy để đáp ứng tốt cho game online nói chung và các dịch vụ yêu cầu độ trễ thấp nên ưu tiên sử dụng các thiết bị AP có sóng 5Ghz và chuẩn 802.11ac trở lên để hạn chế nhiễu và giảm độ trễ, giảm số lượng client trên mỗi AP để giảm tranh chấp kênh truyền.

**Câu hỏi 20 :** Tại sao tôi sao máy tính tôi cổng LAN 1Gbps và cổng LAN Router cũng 1Gbps nhưng tối đo tốc độ chỉ tối đã 94Mbps ?

Bỏ qua yếu tố người dùng bị giới hạn tốc độ trên router thì nguyên nhân thường gặp là do cáp LAN, có thể đã bấm sai chuẩn dây, cũng có thể do cáp chất lượng kém dẫn đến nhiễu buộc thiết bị hạ tốc độ về chuẩn 100Mbps thậm chí 10Mbps.

**Câu hỏi 21 :** Tôi muốn tăng tính bảo mật cho mạng wifi của mình ? Tôi cần cài đặt thế nào ?

Trả lời : Đầu tiên để biết cách thiết lập 1 mạng wifi cá nhân độ bảo mật cao chúng ta sẽ tìm hiểu về các cách thức tấn công wifi :

Brute Force Attack / Dictionary Attack  : Thử nhiều password.

Evil Twin Attack/ Rogue Access Point : Tạo mạng wifi giả hướng người dùng đăng nhập.

Nhưng phương pháp trên thường lợi dụng 1 lỗ hổng WPA/WPA2 để can thiệp quá trình 4-way handshake vì vậy chúng ta nên :

+ Đặt password có kí tự số, kí tự đặc biệt, khi tự hoa.

+ Kích hoạt tính năng Protected management frames (không phải tất cả AP đều có).

+ Sử dụng chuẩn bảo mật WPA3.

Nếu bạn cảm thấy tài liệu này hữu ích với bạn, có thể ủng hộ mình tại :

STK : 0981026159

Mbank

TRẦN VĂN HÙNG

---TRÂN TRỌNG CẢM ƠN---