1. **Mô hình tham chiếu OSI 7 lớp ( Open systems Interconnection)**

Mô hình này là cơ sở cho việc kết nối các hệ thống mở phục vụ cho các ứng dụng và di chuyển thong tin trong mạng .

|  |
| --- |
| Application  (Lớp ứng dụng ) |
| Presentation  (Lớp thể hiện ) |
| Session  (Lớp phiên) |
| Transport  (lớp vận chuyển) |
| Network  (Lớp Mạng) |
| Data link  (Lớp lien kết dữ liệu) |
| Physical  (Lớp vật lý ) |

* Mô hình tham chiếu OSI –

1. **Ưu điểm của OSI :**

* Giảm độ tạp
* Chuẩn hóa các sản phẩm
* Tương thích với thiết bị
* Thúc đẩy công nghệ mạng
* Dễ tìm hiểu và học tập

1. **Chức năng các lớp**

**2.1.Physical ( Lớp vật lý )**

* Đảm bảo các kết nối vật lý
* Truyền tin dạng bit qua kênh vật lý

**2.2.Data link (Lớp lien kết dữ liệu)**

Lớp này đảm bảo việc biến đổi các tin dạng bit từ lớp vật lý sang khung số liệu và đảm bảo thong tin truyền lên lớp 3 không bị lỗi . Đảm bảo quản lý các thong tin số liệu và các thong tin trạng thái .

**2.3.Network ( Lớp mạng )**

Đảm bảo việc chuyển chính xác số liệu giữa thiết bị cuối trong mạng . Để làm được việc đó phải có chiến lược đánh địa chỉ thống nhất trong toàn mạng . Lớp mạng bảo đảm việc tìm đường tối ưu cho các gói dữ liệu bằng các giao thức dựa trên thiết bị router. Ngoài ra lớp mạng còn điều khiển dữ liệu lưu lượng trong mạng để trách tắc ngẽn.

**2.4. Transport ( Lớp vận chuyển )**

Lớp này nhận thong tin từ lớp session chia thành các gói tin nhỏ và chuyền xuống lớp dưới hoặc nhận thong tin từ lớp dưới và chuyển lên lớp session .Nhiệm vụ quan trọng là đảm bảo chuyển số liệu chính xác giữa 2 thực thể thuộc lớp phiên (session) và điều khiển lưu lượng trách tắc nghẽn ở lớp mạng .

**2.5 Session ( Lớp phiên )**

Liên kết giữa 2 thực thể có nhu cầu trao đổi dữ liệu . chức năng quan trong của lớp phiên là đảm bảo đồng bộ số liệu bằng cách thực hiện điểm kiểm tra . tại các điểm kiểm tra này toàn bộ dữ liệu và trạng thái được lưu lại bộ nhớ đệm . Khi có sự cố sẽ khởi tạo lại phiên làm việc từ điểm kiểm tra cuối cùng

**2.6. Presentation( Lớp thể hiện )**

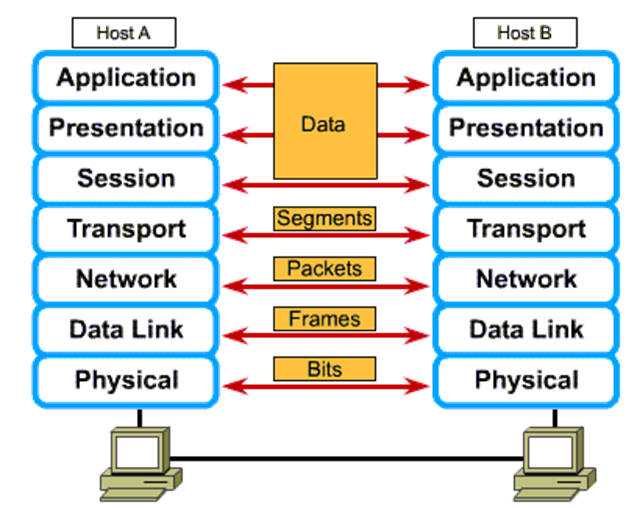
Nhiệm vụ là thích ứng các cấu trúc dữ liệu khác nhau của người dùng với cấu trúc dữ liệu thông nhất sử dụng trong mạng , nén và mã hóa ở lớp Presentation để chuyển xuống lớp dưới . Ngoài ra còn chứ các yêu của người dùng , thư viện tiện ích …

**2.7 Application (Lớp ứng dụng )**

Là lớp người dùng tương tác với môi trường OSI , đông thời cung cấp các dịch vụ và thông tin phân tán .

1. **Các quá trình đồng cấp**

Quá trình để mỗi thiết bị thông tin với nhau tại một lớp được gọi là quá trình đồng cấp (peer to peer processes). Thông tin giữa các máy là quá trình đồng cấp dùng giao thức thích hợp cho lớp này.



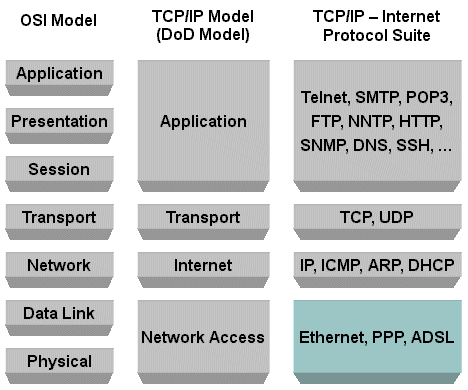
1. **Quá trình chuyển dữ liệu**

**Host A Host B**



Dữ liệu người dùng host A từ tầng 7 được đóng gói qua các tầng và chuyển xuống các tầng 1 . Tầng 1 chuyển các gói dữ liệu thành các bit nhị phân và truyền trên đường vật lý . Ở host B quá trình thực hiện ngược lại quá trình ở A , các gói được bóc tách và chuyển lên tầng 7 .

1. **Mô hình TCP/IP**



Đây là bộ giao thức được sử dụng rộng rãi nhất vì tính mở của nó . Chúng đã nhanh chóng được phát triển qua các phiên bản . TCP/IP có 4 lớp nó giản hơn mô hình tham chiếu OSI . So sánh giữa mô hình OSI và TCP

* **Giống nhau** 
  + Đều phân lớp chức năng
  + Đều có lớp vận chuyển và lớp mạng.
  + Chuyển gói là hiển nhiên.
  + Đều có mối quan hệ trên dưới, ngang hàng.
* **Khác nhau** 
  + TCP/IP gộp lớp trình bày và lớp phiên vào lớp ứng dụng.
  + TCP/IP gộp lớp vật lý và lớp liên kết dữ liệu vào lớptruy nhập mạng.
  + TCP/IP đơn giản vì có ít lớp hơn. OSI không có khái niệm chuyển phát thiếu tin cậy ở lớp 4 như UDP của

**1.Chức năng của các lớp**

**1.1.Network access**

Định ra các trường kết nối phần cứng để truyền dữ liệu vật lý .Có nhiều giao thức hoạt động tại lớp này như: Ethernet, FDDI,ATM….Dữ liệutừ lớp internet được gửi xuống các interface network hoặc ngược lại trong quá trình chuyền và nhận dữ liệu . Hiện nay các máy tính đều có kết nối Ethernet. Ethernet có ba lớp Logic Link Control (LLC), Media Access Control (MAC) và Physical. Lớp này tương tự lớp Data link và Physical ở mô hình OSI.

**1.2.Internet**

Mục đích của lớp Internet là chọn đường đi tốt nhất xuyên qua mạng cho các gói dữ liệu di chuyển tới đích . Giao thức chính của lớp này là Internet Protocol (IP) IP không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích . Phân mảnh và hợp nhất gói liệu IP

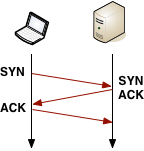
**1.3.Transport**

**-** Có trách nhiệm thiết lập phiên truyền thông giữa 2 máy tính và quy định cách truyền dữ liệu . có 2 cánh truyền thông chính là :

* UDP: là cách truyền thông stream , dữ liệu được đẩy toàn bộ lên và không bảo đảm truyền dữ liệu 1 cách tin cậy , cấu trúc gói tin đơn giản
* TCP : là cách truyền tin cậy , đảm bảo xác thực đã nhận và gửi gói tin .

- Tiến trình bắt tay 3 bước

1. SYN: các chương trình máy con (ví dụ yêu cầu từ browser, ftp client) bắt đầu connection với máy chủ bằng cách gửi một packet với cờ "SYN" đến máy chủ.  
SYN packet này thường được gửi từ các cổng cao (1024 - 65535) của máy con đến những cổng trong vùng thấp (1 - 1023) của máy chủ. Chương trình trên máy con sẽ hỏi hệ điều hành cung cấp cho một cổng để mở connection với máy chủ. Những cổng trong vùng này được gọi là "cổng máy con" (client port range). Tương tự như vậy, máy chủ sẽ hỏi HĐH để nhận được quyền chờ tín hiệu trong máy chủ, vùng cổng 1 - 1023. Vùng cổng này được gọi là "vùng cổng dịch vụ" (service port).  
Ví dụ (mặc định):  
  
- Web Server sẽ luôn chờ tín hiệu ở cổng 80 và Web browser sẽ connect vào cổng 80 của máy chủ.  
- FTP Server sẽ lắng ở port 21.  
  
Ngoài ra trong gói dữ liệu còn có thêm địa chỉ IP của cả máy con và máy chủ.  
  
2. SYN/ACK: khi yêu cầu mở connection được máy chủ nhận được tại cổng đang mở, server sẽ gửi lại packet chấp nhận với 2 bit cờ là SYN và ACK.  
SYN/ACK packet được gửi ngược lại bằng cách đổi hai IP của server và client, client IP sẽ thành IP đích và server IP sẽ thành IP bắt đầu. Tương tự như vậy, cổng cũng sẽ thay đổi, server nhận được packet ở cổng nào thì cũng sẽ dùng cổng đó để gửi lại packet vào cổng mà client đã gửi.  
Server gửi lại packet này để thông báo là server đã nhận được tín hiệu và chấp nhận connection, trong trường hợp server không chấp nhận connection, thay vì SYN/ACK bits được bật, server sẽ bật bit RST/ACK (Reset Acknowledgement) và gởi ngược lại RST/ACK packet.  
Server bắt buộc phải gửi thông báo lại bởi vì TCP là chuẩn tin cậy nên nếu client không nhận được thông báo thì sẽ nghĩ rằng packet đã bị lạc và gửi lại thông báo mới.  
  
3. ACK: khi client nhận được SYN/ACK packet thì sẽ trả lời bằng ACK packet. Packet này được gởi với mục đích duy báo cho máy chủ biết rằng client đã nhận được SYN/ACK packet và lúc này connection đã được thiết lập và dữ liệu sẽ bắt đầu lưu thông tự do.Đây là tiến trình bắt buộc phải thực hiện khi client muốn trao đổi dữ liệu với server thông qua giao thức TCP. Một số thủ thuật dựa vào đặc điểm này của TCP để tấn công máy chủ (ví dụ DOS).



**1.4.Application**

Gồm nhiều giao thức cung cấp ứng dụng để trao đổi thông tin với người dùng . Lớp ứng dụng của mô hình TCP/IP kiểm soát các giao thức lớp cao, các chủ đề về trình bày, biểu diễn thông tin, mã hóa và điều khiển hội thoại. Bộ giao thức TCP/IP tổ hợp tất cả các ứng dụng liên quan đến các chủ đề vào trong một lớp và đảm bảo số liệu này được đóng gói thích hợp trước khi chuyển nó đến lớp kế tiếp. TCP/IP không chỉ chứa các đặc tả về lớp Internet và lớp vận chuyển, như IP và TCP, mà còn đặc tả cho các ứng dụng phổ biến. TCP/IP có các giao thức để hỗ trợ truyền file, e-mail và remote login, thêm vào các ứng dụng sau đây:

* File Transfer Protocol (FTP): FTP là một dịch vụ có tạo cầu nối (connection-oriented) tin cậy, nó sử dụng TCP để truyền các tập tin giữa các hệ thống có hỗ trợ FTP. Nó hỗ trợ truyền file nhị phân hai chiều và tải các file ASCII.
* Trivial File Transfer Protocol (TFTP): TFTP là một dịch vụ không tạo cầu nối (connectionless) dùng UDP (User Datagram Protocol). TFTP được dùng trên router để truyền các file cấu hình và các Cisco IOS image và để truyền các file giữa các hệ thống hỗ trợ TFTP. Nó hữu dụng trong một vài LAN bởi nó hoạt động nhanh hơn FTP trong một môi trường ổn định.
* Network File System (NFS): NFS là một bộ giao thức hệ thống file phân tán được phát triển bởi Sun Microsystems cho phép truy xuất file đến các thiết bị lưu trữ ở xa như một đĩa cứng qua mạng.
* Simple Mail Transfer Protocol (SMTP): SMTP quản lý hoạt động truyền e-mail qua mạng máy tính. Nó không hỗ trợ truyền dạng số liệu nào khác hơn là plaintext.
* Terminal emulation (Telnet): Telnet cung cấp khả năng truy nhập từ xa vào máy tính khác. Nó cho phép một user đăng nhập vào một Internet host và thực thi các lệnh. Một Telnet client được xem như một host cục bộ. Một Telnet server được xem như một host ở xa.
* Simple Network Management Protocol (SNMP): SNMP là một giao thức cung cấp một phương pháp để giám sát và điều khiển các thiết bị mạng và để quản lý các cấu hình, thu thập thống kê, hiệu suất và bảo mật.
* Domain Name System (DNS): DNS là một hệ thống được dùng trên Internet để thông dịch tên của các miền (domain) và các node mạng được quảng cáo công khai sang các địa chỉ IP.