1. **So sánh mô hình TCP/IP và OSI:**

- được xây dựng cùng 1 lúc và sử dụng như công cụ để triển khai hệ thống mạng tuyền thông dữ liệu.
- Lớp truy cập mạng của TCP/IP tương ứng với 2 lớp vật lý và liên kết dữ liệu của mô hình OSI.
- Lớp Internet của mô hình ICP/IP tương ứng với lớp mạng của mô hình OSI liên quan đến địa chỉ và cách định tuyến giữa 2 thiết bị mạng.
- Lớp vận chuyển của mô hình ICP/IP tương tự OSI, cung cấp phương tiện cho phép nhiều ứng dụng trên máy tính truy cập lớp theo phương thức best-effert hoặc tin cậy.
- Lớp ứng dụng của mô hình ICP/IP bao gồm chức năng của 3 lớp trên cùng của mô hình OSI.
- Điểm giống và khác nhau

Giống nhau:

- được xây dựng cùng 1 lúc và sử dụng như công cụ để triển khai hệ thống mạng tuyền thông dữ liệu.
- Lớp vận chuyển của 2 mô hình đều tương tự nhau, đều là cung cấp phương tiện cho phép nhiều ứng dụng trên máy tính truy cập lớp theo phương thức best-effert hoặc tin cậy.

Khác nhau:

TCP/IP	OSI
Lớp ứng dụng	• Lớp phiên • Lớp trình bày • Lớp ứng dụng
Lớp internet	Lớp mạng
Lớp truy cập mạng	• Lớp vật lý • Lớp liên kết dữ liệu

2. **Phương pháp truyền dữ liệu (phân phối gói tin) từ máy sang máy**

VD: Một ứng dụng trên máy tính 192.168.3.1 muốn gửi dữ liệu qua máy có địa chỉ là 192.168.3.2 .

B1: Lớp vận chuyển chọn TCP để thiết lập truyền thông (session). TCP khởi tạo phiên truyền thông bằng cách chuyển thông tin header TCP với bit SYN và địa chỉ IP đích là 192.168.3.2.

B2: Lớp IP đóng gói dữ liệu SYN của TCP vào gói tin bằng cách gắn thêm vào phía trước dữ liệu TCP địa chỉ lớp 3 của máy gửi sau đó gửi qua lớp 2 để xử lý tiếp.

B3: Lớp 2 đóng gói dữ liệu lớp 3 (IP packet) vào trong Frame lớp 2. Lớp 2 gửi yêu cầu đến ARP để ánh xạ địa chỉ IP – MAC của máy đích.

ARP kiểm tra cache của mình. Nếu máy này chưa bao giờ giao tiếp với máy khác thì lớp 2 sẽ giữ lại gói tin đến khi ánh xạ ARP được tạo ra vì ARP hiện tại đang rỗng

B4: ARP xây dựng gói tin ARP Request và chuyển cho lớp 2, yêu cầu lớp 2 gửi lại thông tin với địa chỉ đích boardcast.

Lớp 2 đóng gói ARP Request trong frame lớp 2 dùng địa chỉ MAC đích là boardcast, và địa chỉ MAC nguồn của máy yêu cầu phân giải.

B5: Khi máy 192.168.3.2 nhận được frame, nó sẽ lưu ý địa chỉ boardcast và thực hiện đóng gói frame lớp 2.

Thông tin ARP Request được chuyển đến cho chương trình ARP

B6: Sử dụng thông tin ARP Request, chương trình ARP cập nhật bảng cache của nó.

Chương trình ARP xây dựng gói tin ARP Reply và gửi cho lớp 2, yêu cầu lớp 2 gửi đến địa chỉ MAC 0800:0222:2222 (IP: 192.168.3.1)

B7: Lớp 2 đóng gói ARP Reply vào frame lớp 2 với địa chỉ MAC đích cung cấp bởi bảng ARP và địa chỉ nguồn máy gửi.

Khi máy 192.168.3.1 nhận được frame, nó lưu ý đến địa chỉ MAC đích của nó. Máy đích sẽ đóng gói frame lớp 2.

B8: hần thông tin ARP reply sẽ được chuyển đến cho chương trình ARP.

ARP thực hiện cập nhật bảng cache ánh xạ IP – MAC tương ứng.

B9: Lớp 2 giờ có thể gửi gói tin treo lúc nãy.

Ở máy 192.168.3.2, frame được chuyển lên cho các lớp phía trên (giải đóng gói dữ liệu). Phần PDU tương ứng còn lại được chuyển cho TCP.

B10: Để trả lời cho SYN, TCP chuyển dữ liệu SYN ACK xuống cho các lớp bên dưới thực hiện việc đóng gói.

B11: Khi quá trình bắt tay 3 bước (three – way handshake), TCP có thể báo cho ứng dụng biết rằng phiên truyền thông (session) đã được thiết lập.
Bây giờ ứng dụng có thể gửi dữ liệu thông qua phiên truyền thông dựa trên TCP để sửa các lỗi nếu có.
B12: Dữ liệu tiếp tục được trao đổi đến khi ứng dụng dừng việc gửi dữ liệu.

3. **Phương pháp truyền dữ liệu (phân phối gói tin) thông qua switch**

B1: Ví dụ host 192.168.3.1 có data muốn chuyển cho host 192.168.3.2. Ứng dụng không cần một liên kết đáng tin cậy. Giao thức UDP-User Datagram Protocol được dung.

B2: Bởi không cần thiết lập phiên làm việc, ứng dụng có thể bắt đầu gửi data. UDP sẽ thêm phần đầu (UDP heacher) và chuyển protocol data unit (PDU) đến IP (Layer 3) với các chỉ thị để gửi thông tin này (PDU) đến 192.168.3.2. IP đóng gói PDU trong Layer 3 và chuyển nó đến Layer 2.

B3: Giao thức Address Resolution Protocol (ARP) không tham gia thành một mục trong bảng.

B4: Host 192.168.3.1 gửi ARP request. Tuy thế trong ví dụ nó sẽ nhấn thông tin từ switch trước khi liên lạc được máy tính ở xa.

B5: Khi switch nhận Frame, nó phải chuyển đến port thích hợp. Tuy nhiên, trong ví dụ này, hoặc địa chỉ nguồn hay địa chỉ đích đang được lưu trong bảng MAC của switch. Switch có thể học việc đồng bộ địa chỉ MAC và port trong Frame do đó switch có thể thêm như sau: 0800:0222:2222 = port 1). Bởi vì địa chỉ đích là địa chỉ quảng bá (broadcast) nên switch sẽ làm tràn gói thông tin nhận ra tất cả các port còn lại. Ghi chú, swith không thay đổi nội dung của Frame.

B6: Máy đích nhận được ARP request từ switch

B7: Máy đích nhận yêu cầu ARP (ARP request) rồi trả lời

B8: Switch đọc được địa chỉ MAC của máy nguồn tương ứng với port trên switch. Ví thế, switch thêm một bản ghi vào bảng MAC 0800:0222:1111 = port 2. Bởi vì máy đích đã được thêm địa chỉ MAC vào bảng MA của switch do đó switch sẽ chuyển tiếp ra port Ghi chú, switch không thay đổi nội dung của Frame

B9: Máy nguồn nhận được ARP reply gửi từ máy đích.

B10: Data được gửi và nhận. Mọi Frames chuyển qua switch không thay đổi nội dung bên trong.

4. **Phương pháp truyền dữ liệu (phân phối gói tin) thông qua router**

B1: Host sẽ gởi bất kỳ một gói dữ liệu nào không nằm trong địa chỉ mạng cục bộ hiện tại ra ngoài default gateway

B2: host 192.168.3.1 có dữ liệu muốn gởi đến host 192.168.4.2. Các ứng dụng không cần quá trình truyền tin cậy bởi đã dụng dịch vụ với giao thức UDP

B3: Bởi vì không cần thiết phải thiết lập các phiên giao dịch, các ứng dụng có thể bắt đầu gởi dữ liệu. UDP chuẩn bị các header và đưa PDU xuống IP (lớp 3) và hướng dẫn cách gởi PDU đến 192.168.4.2. IP đóng gói PDU ở lớp 3 và tiếp tục đưa xuống lớp 2.

B4: Bảng ARP hiện tại không có bất kỳ một thông tin nào.

B5: Bởi vì các host không chạy bất kỳ giao thức định tuyến nào, do vậy nó sẽ không biết các với về đoạn mạng bên kia. Các host sẽ gởi khung dữ liệu đến default gateway, các host này sử dụng tiến trình ARP bình thường để lấy MAC này

B6: User đã được cấu hình địa chỉ 192.168.3.2 như một defualt gateway. Host 192.168.3.1 gởi ra yêu cấu ARP và thông tin này được nhận bởi router.

B7: Router sử lý tiến trình ARP giống như tất cả các host khác

B8: Phản hồi được gởi lại cho thông tin ARP yêu cầu.

B9: Host đích nhận được yêu cầu ARP. Thông tin lớp 2 lúc này được phản hồi. Chú ý rằng ARP gởi về thông tin ánh xạ giữa địa chỉ IP 192.168.4.2 và địa chỉ MAC của default gateway thay vì địa chỉ MAC thực.

5. **Phương thức quản trị tín hiệu truyền trên mạng (CSMA/CD)**

- Tín hiệu Ethernet được phát từ mỗi máy nối vào mạng, dùng một tập các qui tắc đặc biệt để xác định trạm nào đang phát.
- Ethernet quản trị tín hiệu trên mạng bằng phương thức Carrier Sense Multiple Access with Collision Detection (CSMA/CD), hình trên minh họa tiến trình CSMA/CD thực hiện.
- Trong mạng Ethernet, trước khi phát tín hiệu, máy tính phải lắng nghe trên môi trường truyền. Nếu môi trường truyền đang ở trạng thái nghỉ, máy tính sẽ gửi dữ liệu. Sau khi tín hiệu được phát đi, tất cả các máy tính khác trên mạng sẽ cạnh tranh nhau tìm thời

gian nghỉ kế tiếp để gửi frame khác. Quá trình cạnh tranh tìm thời gian nghỉ có nghĩa là không có trạm nào có ưu thế hơn các trạm còn lại.

- Các trạm trên mạng cục bộ CSMA/CD có thể truy cập mạng bất kỳ lúc nào. Trước khi gửi dữ liệu, các trạm CSMA/CD lắng nghe mạng để xác định xem mạng đã được sử dụng hay không. Nếu mạng đang được sử dụng các trạm sẽ phải đợi. Nếu mạng đang rảnh rỗi, các trạm sẽ phát dữ liệu. Đụng độ (collision) xãy ra khi 2 trạm cùng phát dữ liệu một lúc (xem hình). Trong trường hợp đó, cả hai tín hiệu đều bị hỏng, và các trạm phải gửi lại tín hiệu sau đó. Trạm CSMA/CD phải có khả năng phát hiện đụng độ để gửi lại tín hiệu khi cần thiết.
- Khi một trạm phát, tín hiệu được xem như là carrier. Card mạng sẽ nhận biết được carrier và tư kiềm chế việc phát tín hiệu lên mạng. Nếu không có carrier, một trạm đang đợi sẽ biết rằng đã sẵn sàng để phát tín hiệu. Chức năng này được gọi là nhận diện carrier (“carrier sense”). Toàn bộ phần mạng trên đó xảy ra đụng độ được gọi là miền đụng độ (collision domain). Kích thước miền đụng độ ảnh hưởng đến hiệu năng và thông lượng của mạng Ethernet.
- Trong tiến trình CSMA/CD, không có độ ưu tiên cho các trạm, vì thế tất cả các trạm trên mạng đều có quyền truy xuất như nhau, vì thế xuất hiện khả năng cùng truy cập (“multiple access”). Nếu có từ 2 trạm trở lên cố gắng phát dữ liệu cùng lúc đụng độ sẽ xảy ra. Khi xảy ra đụng độ các trạm sẽ thực hiện thuật toán backoff sinh ra thời gian chờ ngẫu nhiên trước khi phát lại tín hiệu. Cách làm này sẽ giúp ngăn chặn các máy tiếp tục cố gắng tín hiệu đồng thời đó là kỹ thuật giải quyết đụng độ “collision detection”.

6. Phương pháp dừng và chờ

Đơn giản nhất,

Kém hiệu quả, chỉ có một khung tin được truyền tại một thời điểm

Truyền một gói tin và chờ báo nhận

- Bên phát truyền một khung tin
- Sau khi nhận được khung tin, bên nhận gửi lại xác nhận
- Bên phát phải đợi đến khi nhận được xác nhận thì mới truyền khung tin tiếp theo

Không hiệu quả

- Bên nhận có thể dừng quá trình truyền bằng cách không gửi khung tin xác nhận
- Tại một thời điểm chỉ có một khung tin trên đường truyền → chậm
- Trường hợp độ rộng của kênh truyền lớn hơn độ rộng của khung tin thì nó tỏ ra cực kỳ kém hiệu quả.

7. **Phương pháp cửa sổ trượt**

Hiệu quả

Cho phép truyền nhiều khung tin cùng một lúc trên kênh truyền

- Cho phép nhiều khung tin được truyền tại một thời điểm => Truyền thông hiệu quả hơn.
- A và B được kết nối trực tiếp song công (full-duplex).
- B có bộ đệm cho n khung tin => B có thể chấp nhận n khung tin, A có thể truyền n khung tin mà không cần đợi xác nhận từ bên B
- Mỗi khung tin được gán nhãn bởi một số thứ tự.
- B xác nhận khung tin đã được nhận bằng cách gửi xác nhận cùng với số thứ tự của khung tin tiếp theo mà nó mong muốn nhận

8. **Bắt tay ba bước**

Ngắn

Bây giờ là các bước thực hiện việc thiết lập kết nối (giả sử A là người gởi và B là người nhận)

- Bước 1. A gởi cho B một SYN segment, trong đó chứa Sequence number của A

- Bước 2. Khi B nhận được B sẽ gởi lại một SYN – ACK Segment, trong đó chứa Sequence number của B và vùng ACK= Sequence number của B + 1

- Bước 3. Khi A nhận được sẽ gởi lại một ACK Segment chứa Sequence number A bằng giá trị vùng ACK của B gởi tới và vùng ACK của A có giá trị bằng Sequence number +1

Sau bước 3, kết nối được thiết lập và sẵn sàng truyền Data. Mục đích là để trao đổi Sequence Number và ACK Number.

Dài

1> SYN: Các chương trình máy con (như web browser, ftp, ...) bắt đầu connection với máy chủ bằng cách gửi 1 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 cho 1 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 Web Server sẽ luôn chờ tín hiệu ở cổng 80 và IE sẽ connect vào cổng 80 của máy chủ .

Ngoài ra trong gói dữ liệu còn có thêm địa chỉ IP của máy con và máy chủ (cả 2)

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 SYN và ACK :

SYN/ACK packet được gửi ngược lại bằng cách đổi 2 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 gủi 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 . Hoặc ICMP cổng khÔng chấp nhận để thông báo cho client rằng yêu cầu đã bị từ chối .

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 nhất 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 giữa connection.

$0_{hex} = 0_{dec} = 0_{oct}$	0	0	0	0
$1_{hex} = 1_{dec} = 1_{oct}$	0	0	0	1
$2_{hex} = 2_{dec} = 2_{oct}$	0	0	1	0
$3_{hex} = 3_{dec} = 3_{oct}$	0	0	1	1
$4_{hex} = 4_{dec} = 4_{oct}$	0	1	0	0
$5_{hex} = 5_{dec} = 5_{oct}$	0	1	0	1
$6_{hex} = 6_{dec} = 6_{oct}$	0	1	1	0
$7_{hex} = 7_{dec} = 7_{oct}$	0	1	1	1
$8_{hex} = 8_{dec} = 10_{oct}$	1	0	0	0
$9_{hex} = 9_{dec} = 11_{oct}$	1	0	0	1
$A_{hex} = 10_{dec} = 12_{oct}$	1	0	1	0
$B_{hex} = 11_{dec} = 13_{oct}$	1	0	1	1
$C_{hex} = 12_{dec} = 14_{oct}$	1	1	0	0
$D_{hex} = 13_{dec} = 15_{oct}$	1	1	0	1
$E_{hex} = 14_{dec} = 16_{oct}$	1	1	1	0
$F_{hex} = 15_{dec} = 17_{oct}$	1	1	1	1