Tầng Application

Tầng cung cấp các dịch vụ mạng cho end-user.

Port: là địa chỉ phân biệt các p hần mềm với nhau: 0-1023 là các ứng dụng phổ biến, 1024-49151 là port cố định, đăng kí trước, 49152-65535 là port linh động.

Giao thức HTTP (TCP, port 80): giao thức để truyền tải các object (html, video, ảnh...).

Các giao thức email

- SMTP: dùng để đưa mail từ bên gửi lên mail server bên gửi, sau đó gửi sang mail server bên nhận. Port: 25 (không mã hóa), 465 (có mã hóa)
- POP3: dùng để kéo mail từ mail server bên nhận về nhưng không lưu trữ mail trên server. Port: 110 (không mã hóa), 995 (có mã hóa)
- IMAP: dùng để kéo mail header từ mail server về và vẫn lưu trữ mail trên server. Thay đổi ở end-user đều tương tự trên server. Port: 143 (không mã hóa), 993 (có mã hóa)

DNS có tác dụng phân giải tên miền ra địa chỉ IP và ngược lại. Cấu trúc cây DNS bao gồm: Root DNS (nắm quyền tất cả), Top-Level Domain (quốc gia hoặc một số tổ chức), Authoritative (cấp quyền và quản lý tên miền), Local DNS (trường học, cơ quan...).

Phân giải tên miền:

- đệ quy (local-root-TLD-author-TLD-root-local)
- tuần tự (local-root-local-TLD-local-author-local)

DHCP (UDP) cấp phát địa chỉ IP động cho máy. Xin cấp mới: Discover → offer → request → ack (server xác nhận) / nak (server từ chối) || Xin cấp lại: Request → Ack/Nak || Hủy: Release

Tầng Transport

Cung cấp kênh truyền dữ liệu ở mức logic giữa 2 process trên 2 máy, cung cấp kết nối logic giữa các tiến trình

Dồn kênh phía gửi: đóng các dữ liệu từ tầng Application vào các segment, gắn header là port gửi và port nhận tương ứng và gửi xuống tầng Network.

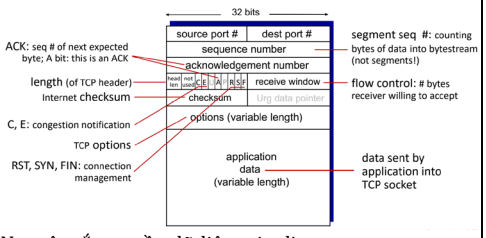
Phân kênh phía nhận: nhận segment đã phân rã ở tầng Network, gửi dữ liệu đến socket tương ứng với port nhận.

Các giao thức: TCP (Transmission Control Protocol) và UDP (User Datagram Protocol).

UDP có đặc điểm: truyền nhanh, header nhỏ, không quan tâm gói tin bị mất, trễ hay sai thứ tự, connectionless, không kiểm soát luồng, không handshaking giữa receiver và sender, các gói tin được xử lý độc lập. Được sử dụng cho các dịch vụ live-streaming hoặc video games. VD: NS, SNMP, TFTP...

TCP có đặc điểm: 1 gửi 1 nhận, đáng tin cậy, dữ liệu đi 2 chiều, có đánh dấu thứ tự ACK, giao thức pipeline, có handshaking.

TCP segment structure



Nguyên tắc truyền dữ liệu: pipeline

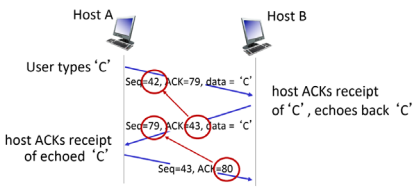
Bên gửi:

1. Nhận dữ liệu từ tầng ứng dụng: tạo các segment, bật đồng hồ, thiết lập thời gian chờ
2. Nhận gói tin ACK: nếu trước đó chưa nhận thì trượt "cửa sổ" và thiết lập lại thời gian của đồng hồ
3. Hết time out: gửi lại dữ liệu còn trong buffer và reset đồng hồ

Bên nhận:

1. Nhận gói tin đúng thứ tự: chấp nhận và gửi ACK về cho bên gửi
2. Nhận gói tin không đúng thứ tự: phát hiện "khoảng trống dữ liệu" và gửi ACK trùng

TCP sequence numbers, ACKs



simple telnet scenario

(seq=x thì ack sau=x+data_size, ack = x thì seq sau=x, vì ack gửi yêu cầu gói tin tiếp theo)

Thiết lập kết nối: A->B: syn, seq=x; B->A: syn, seq=y,ack=x+1; A->B: seq=x+1, ack=y+1.

Ngắt kết nối: A->B: fin; B->A: ack,fin; A->B: ack.

Điều khiển luồng: sử dụng trường window size để kiểm soát lượng dữ liệu đưa vào buffer. Nếu buffer hết chỗ, yêu cầu khóa bên gửi.

Kiểm soát tắc nghẽn: tăng tốc độ gửi đến khi gặp trường hợp bị mất gói hoặc bị lỗi thì giảm tốc độ gửi.

TCP Fast Retransmit: nếu ack của cùng 1 gói gửi về 3 lần thì xem như mất gói đó, gửi lại.

Nguyên tắc truyền dữ liệu đáng tin cậy: Nghi thức truyền dữ liệu đáng tin cậy: RDT1.0/2.0/2.1/2.2/3.0 || Nguyên tắc của RDT: bên gửi gửi gói kèm thông tin kiểm lỗi, dừng và chờ, gửi lại khi có lỗi xảy ra; bên nhận kiểm lỗi, trùng lắp dữ liệu, gởi gói tin phản hồi || giải quyết lỗi bit: bên gửi - gửi kèm thông tin kiểm tra lỗi; sử dụng phương pháp kiểm lỗi (checksum, parity checkbit,...), bên nhận - kiểm lỗi bit; hành động khi xảy ra lỗi bit (báo về bên gửi) || giải quyết mất gói: bên gửi - định nghĩa trường hợp mất gói; chờ nhận tín hiệu báo; hành động khi phát hiện mất gói, bên nhận - gửi tín hiệu báo (ACK, NAK)

Tầng Network

Thiết lập kết nối giữa 2 host để truyền dữ liệu từ host – host, cung cấp kết nối logic giữa các host.

Đóng gói segment từ tầng transport thành các packet, gắn header là IP add. gửi và nhận. Cung cấp 2 loại dịch vụ: hướng kết nối và phi kết nối. Router định tuyến bằng cách: tính địa chỉ đường mạng giữa địa chỉ đích đến và subnet mask của từng record rồi so sánh với destination network. Nếu trùng thì chuyển tiếp theo port tương ứng với des. network. Router tự học để xây dựng bảng định tuyến.

ICMP: host và router trao đổi thông tin ở tầng mạng. Bao gồm: báo lỗi (mạng, host, protocol, port ... không đến được), báo mạng bị nghẽn, báo timeout, echo request/reply (ping).

NAT: chuyển địa chỉ IP private ra public và ngược lại.

Có 4 loại: static (1 local – 1 global), dynamic (n local – m global), overloading (local<IP,port> - global<IP,port>), overlapping (<local IP, port> - <global IP, port>).

Tầng Data Link

Điều khiển truy cập đường truyền và điều khiển liên kết.

Đóng gói packet từ tầng network thành frame, gắn header là MAC add. gửi và nhận. Tại nơi nhận có kiểm tra lỗi frame.

Tầng này có 2 tầng con:

- Logical Link Control (lớp trung gian giữa giao thức tầng Network và các công nghệ mạng của tầng MAC, không để cho 2 thành phần này phụ thuộc nhau), có chức năng: điều khiển luồng, kiểm tra lỗi, báo nhận
- Media Access Control (driver card mạng): truy cập đường truyền

Kiểm lỗi: sử dụng phương pháp checksum:

1. Bên gửi: d bits trong dữ liệu gửi đi được xem như gồm N số có độ dài k bits: x1, x2,...,xN
2. Tính tổng X = x1 + x2 + ... + xN
3. Tính bù 1 của X → giá trị checksum
4. Bên nhận: tính tổng tất cả giá trị nhận được (kể cả checksum)
5. Nếu tất cả các bit là 1 thì dữ liệu đúng, nếu có 1 bit 0 thì dữ liệu sai

CSMA: phương pháp truyền dữ liệu có đụng độ.

Lắng nghe đường truyền trước khi truyền:

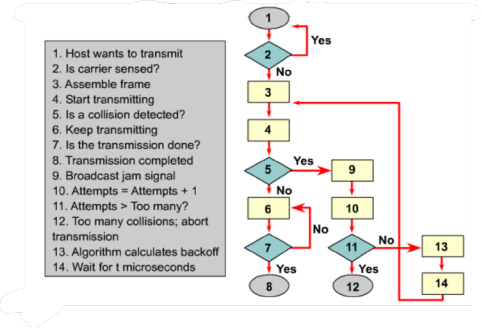
- Đường truyền rảnh: truyền dữ liệu
- Đường truyền bận: chờ

Lắng nghe đường truyền sau khi truyền. Nếu đụng độ xảy ra: dừng truyền, đợi 1 khoảng thời gian và truyền lại.

Đặc điểm: không ưu tiên, chấp nhận được với số lượng node nhỏ.

Cải tiến: CSMA/CD, CSMA/CA

Mô hình CSMA/CD



Luân phiên:

Token passing: dùng 1 token, máy nào cầm token thì được truyền dữ liệu, trả lại hệ thống sau khi sử dụng xong. Dễ dàng thiết lập độ ưu tiên cho các thiết bị và phù hợp để tải nặng; chi phí cao. Sử dụng trong mạng token ring.

Polling: 1 máy chủ thu thập nhu cầu của các máy trong mạng và xếp vào hàng chờ để trao quyền sử dụng. Chi phí cao, máy chủ thu thập là "gót chân Achilles".

ARP: Phân giải IP add. thành MAC add. và ngược lại. Chỉ phân giải trong cùng đường mạng. Có sẵn trong tất cả các thiết bị mạng. ARP table: 1 record bao gồm: IP, MAC, TTL (time to live). Được lưu trên RAM.

Cách hoạt động:

1. Máy nguồn tra trong bảng ARP xem địa chỉ IP được đưa đã có địa chỉ MAC tương ứng hay không.
2. Nếu không, gửi ARP request theo hình thức broadcast. Máy đích nhận được sẽ gửi lại ARP response, trong đó sẽ có địa chỉ MAC của máy đích.
3. Map địa chỉ IP với địa chỉ MAC.

Ethernet là 1 kỹ thuật mạng LAN có dây. Đây là công nghệ mạng LAN đầu tiên trên thế giới.

- Chuẩn 802.3.
- Hoạt động ở tầng Data Link và Physical.
- Tốc độ: 10Mbps - 10Gbps.
- Đồ hình mạng: bus/star.
- Giao thức tầng MAC: CSMA/CD.
- Đơn giản và rẻ hơn mạng Token Ring LAN, ATM.

Các công nghệ mạng LAN: 10Base2, 10Base5, 10BaseT, 100BaseTX, 100BaseFX, Gigabit Ethernet (T: Twisted pair, cáp đồng xoắn đôi, F: Fiber, cáp quang; hậu tố X: sử dụng trong mạng fast ethernet). Base(band): công nghệ truyền dữ liệu dưới dạng digital và chiếm toàn bộ dữ liệu của kênh truyền.

Các thiết bị mạng

Thiết bị tầng 1 (tầng physical)

Modem: chuyển tín hiệu mạng (digital) qua sóng điện thoại (analog) và ngược lại.

Repeater: khuếch đại sóng mạng này và truyền vào mạng kia.

Hub: tập kết tất cả các dây mạng.

Repeater & Hub: Tái sinh tín hiệu mạng và chuyển tín hiệu mạng đến các segments mạng còn lại. Đặc điểm: Không thể liên kết các segment mạng khác nhau (khác đường mạng, khác công nghệ mạng), không thể "nhận dạng" packet, không cho phép giảm tải mạng, cho phép mở rộng mạng dễ dàng.

Thiết bị tầng 2 (tầng data link)

Bridge: kết nối 2 mạng vật lý, chức năng: chuyển có chọn lọc các gói tin đến nhánh mạng chứa trạm

nhận gói tin. Duy trì bảng địa chỉ (MAC-port)
Nếu trạm nhận cùng segment với trạm gửi, hủy gói tin; ngược lại chuyển gói tin đến segment đích.
Switch: 1 bridge nhiều port, hỗ trợ truyền 2 chiều.
Có khả năng tự học địa chỉ MAC:
1. Host A muốn liên lạc với host B nhưng chưa biết địa chỉ MAC của nó. A sẽ sử dụng chức năng ARP để tìm ra được địa chỉ MAC của B.
2. ARP request này sẽ được đưa lên switch và được broadcast trên tất cả các máy trừ A. Trong quá trình đó, switch học được cổng nào dẫn đến địa chỉ MAC của A.
3. B sau khi nhận được ARP request sẽ trả lại ARP response, trong đó có chứa địa chỉ MAC của B. Gói tin này sẽ phải đi qua switch để đến được A, trong quá trình đó switch cũng học được cổng nào dẫn đến địa chỉ MAC của B.
VLAN: nhóm 1 số port thành 1 mạng LAN ảo.
Thiết bị tầng 3 (tầng network)
Router: kết nối các mạng logic khác nhau, sử dụng địa chỉ logic (IP) để xử lý gói tin, định tuyến (chạy các thuật toán định tuyến tạo ra bảng định tuyến), chuyển tiếp (chuyển gói tin từ cổng vào ra cổng ra).
Các thiết bị khác
NIC: card mạng, thiết bị kết nối thiết bị người dùng và phương tiện truyền thông.
Access Point: là thiết bị cho phép thiết bị truy cập mạng không dây, đóng vai trò như 1 hub. Thành phần:
- Bộ thu: thu tín hiệu radio và chuyển thành tín hiệu mạng
- Bộ phát: chuyển tín hiệu mạng thành tín hiệu radio
Một số AP còn tích hợp chức năng của 1 router.
Collision Domain & Broadcast Domain
Collision Domain: là miền dùng chung, hai segment thuộc cùng 1 collision domain nếu chúng gây ra collision khi đồng thời gởi dữ liệu xuống đường truyền.
Broadcast Domain: là 1 tập hợp các collision domain được liên kết với nhau. Collision domain A và B thuộc cùng 1 broadcast domain nếu các node mạng trong collision domain B nhận được gói tin broadcast từ 1 node trong collision domain A.
Thiết bị mở rộng collision domain: repeater, hub.
Thiết bị phân tách collision domain: switch, bridge (bao nhiêu cổng, bấy nhiêu collision domain).
Thiết bị phân tách broadcast domain: switch (VLAN), router (bao nhiêu cổng, bấy nhiêu broadcast domain).
Số broadcast domain = số port của router.
Số collision domain = số port của bridge/switch.
Nguyên nhân gây trễ:
+ trễ do tốc độ truyền (transmission delay) (gây tốn thời gian nhất) (kích thước gói/tốc độ truyền)
+ trễ trên đường truyền (propagation delay)
+ xử lí tại nút (nodal processing) (kiểm lỗi bit, xác định đầu ra)
+ hàng đợi (queuing delay)
Đặc điểm của Virtual Circuit Network:
+ Thiết lập kết nối trước khi truyền dữ liệu
+ Thiết lập, quản lý và duy trì mỗi kết nối khi truyền dữ liệu
+ Thông tin định tuyến: VCID
+ Dữ liệu được gắn thông tin định tuyến khi truyền
Đặc điểm của Datagram Network:
+ Không thiết lập kết nối trước khi truyền dữ liệu
+ Router không cần quản lý trạng thái kết nối
+ Thông tin định tuyến: địa chỉ đích đến
Overloading NAT giải quyết vấn đề gì?
Overloading NAT giúp giải quyết vấn đề cạn kiệt địa chỉ IP bằng cách cho phép nhiều thiết bị trong mạng sử dụng cùng một địa chỉ IP duy nhất để kết nối đến Internet và sử dụng thông tin cổng (port) để phân biệt các kết nối. Vấn đề này thường gặp trong các hộ gia đình, doanh nghiệp nhỏ và mạng WiFi công cộng, nơi số lượng thiết bị cần kết nối tới Internet nhiều hơn số lượng địa chỉ IP có sẵn.
Overlaping NAT giải quyết vấn đề gì?
Overlaping NAT hỗ trợ máy trên Internet truy cập được máy trong mạng nội bộ đang mang địa chỉ private
Nêu ứng dụng của VPN
VPN cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu. Giải pháp VPN (Virtual Private Network) được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên tồn quốc hay tồn cầu). Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn nên tiết kiệm được được chi phí và thời gian. Xác thực nguồn gốc (Origin Authentication): Người nhận có thể xác thực nguồn gốc của gói dữ liệu, đảm bảo và công nhận nguồn thông tin.Tính toàn vẹn dữ liệu (Data Integrity): Người nhận có thể kiểm tra rằng dữ liệu đã được truyền qua mạng Internet mà không có sự thay đổi nào. Sự bảo mật (Confidentiality): Người gửi có thể mã hóa các gói dữ liệu trước khi truyền chúng ngang qua mạng. Bằng cách làm như vậy, không một ai có thể truy nhập thông tin mà không được phép, mà nếu lấy được thông tin cũng không đọc được vì thông tin đã được mã hóa
2 kiểu kết nối non-persistent và persistent của HTTP
- Non-persistent HTTP: mỗi kết nối chỉ truyền tải 1 đối tượng. Muốn truyền tải nhiều đối tượng (object) cần phải thiết lập nhiều kết nối giữa client và server.
- Persistent HTTP: mỗi kết nối cho phép gửi và nhận nhiều đối tượng (object) giữa client và server.
Nguyên lý hoạt động của phương thức CSMA/CD
- Thiết bị lắng nghe đường truyền
- Nếu đường truyền rảnh, thiết bị truyền DL của mình lên đường truyền
- Sau khi truyền, lắng nghe đụng độ?
- Nếu có, thiết bị gởi tín hiệu cảnh báo các thiết bị khác
- Tạm dừng 1 khoảng thời gian ngẫu nhiên rồi gởi DL
- Nếu tiếp tục xảy ra đụng độ, tạm dừng khoảng thời gian gấp đôi.
Cách chống vấn đề nghe lén trên một đoạn mạng (LAN)
- Thay thế thiết bị tập trung Hub bằng Switch, và giám sát chặt chẽ sự thay đổi địa chỉ MAC (Media Access Control) của card mạng
- Áp dụng cơ chế one-time password – thay đổi password liên tục
- Mã hóa dữ liệu truyền dẫn bằng các cơ chế truyền thông dữ liệu an toàn SSL (Secure Sockets Layer), thiết lập IPSec và mạng riêng ảo VNP (Virtual Private Network),… Hạn chế hay thay thế các chương trình không chức năng mã hóa dữ liệu hay mã hóa mật khẩu
- Sử dụng các phần mềm phát hiện sự hoạt động của các chương trình nghe lén trên mạng
Các cách thức để ẩn danh trên Internet
- Sử dụng VPN/Trình duyệt riêng tư/tính năng ẩn danh trong trình duyệt
- Sử dụng tìm kiếm không lưu lịch sử
- Tắt cookies và javascript
- Tích hợp mạng Tor vào ứng dụng
- Sử dụng tài khoản phụ/có thể hủy được
Công dụng của Firewall là gì? Firewall khác với proxy thế nào? Firewall có làm chức năng quét virus không
- Về căn bản firewall là: giải pháp bảo vệ hệ thống mạng ở tầng network - Dựa vào Access Policy để cho phép luồng dữ liệu nào đi vô và chặn luồng dữ liệu nào lại
- Kiểm soát luồng dữ liệu:
+ Từ mạng bên trong đi ra ngoài
+Từ bên ngoài đi vào bên trong
Firewall đóng vai trò người gác cổng người cho phép ra vào thông tin, còn proxy được cài trên firewall đóng vai trò người trung gian lấy thông tin
Nếu access policy được cập nhật có các thông tin về mối nguy (như virus) thì firewall sẽ đóng vai trò chặn mối nguy. Tuy nhiên firewall tường lửa không vô hiệu hóa phần mềm độc hại đã có trên thiết bị như quét virus
Sự khác biệt giữa Hub và Switch

Nguyên tắc chung trong việc cấu hình DNS Server
Nguyên lý: Làm 2 việc:
+ Đưa tên và địa chỉ IP vào DNS Server (tên này thì địa chỉ này A Record, địa chỉ này tên này PTR Record)
+ Dạy DNS Server khi khi bị hỏi một tên mà DNS Server không quản lí thì chuyển câu hỏi đi đâu
Các công nghệ LAN khác nhau thì khác nhau ở tầng nào trong mô hình OSI ?
Tầng physical và tầng datalink
Mô hình screened subnet Firewall (triple-homed setup)
Gồm có 3 thành phần:
+ public interface kết nối đến internet, có thể là router
+ Middle zone hay Demilitary Zone (DMZ), đóng vai trò là bộ đệm
+ Một subnet kết nối đến một Intranet hoặc kiến trúc như Bastion Host. Đóng vai trò là mồi nhử để bảo vệ hệ thống chính và lọc các cuộc tấn công (nếu có)