Giới thiệu về An ninh mạng

Mô hình OSI và TCP/IP

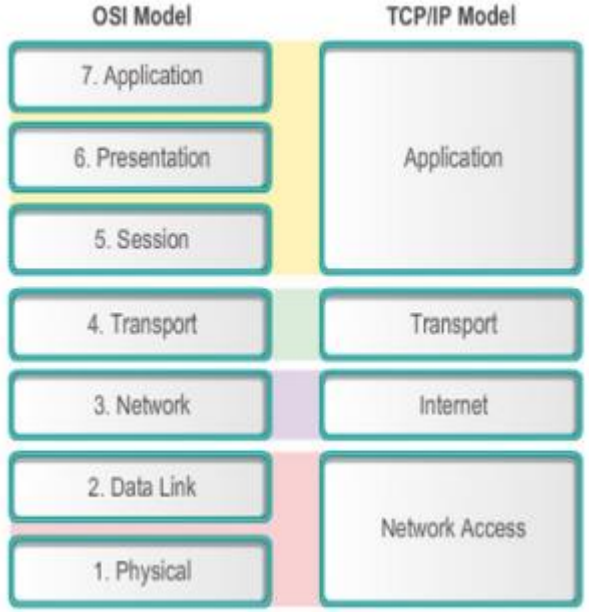
- Mô hình OSI

Application	Giao tiếp cho người dùng truy nhập các thông tin và dữ liệu trên mạng thông qua chương trình ứng dụng
Presentation	Dịch dữ liệu được gửi từ tầng ứng dụng sang như định dạng, nén dữ liệu, mã hóa dữ liệu.
Session	Thiết lập, quản lý và kết thúc các phiên làm việc của các kết nối giữa trình ứng dụng địa phương và ở xa.
Transport	Vận chuyển dữ liệu từ nguồn đến đích. Chia nhỏ dữ liệu bên gửi cho phù hợp với kênh truyền và tái lập ở bên nhận
Network	Định tuyến cho các gói tin; xử lý dữ liệu dạng gói (packet); liên quan đến địa chỉ luận lý
Data Link	Cung cấp phương tiện truyền dữ liệu giữa hai node kết nối trực tiếp với nhau, xử lý các kết nối bị lỗi từ tầng Physical.
Physical	Định nghĩa đặc tả về điện và vật lý cho các thiết bị của hệ thống. Xử lý dữ liệu dạng bit.

Mô hình OSI và TCP/IP

- Các giao thức ở các tầng của mô hình OSI

Layer	Các giao thức
Application Layer	Telnet, SSH, FTP, SMTP, HTTP, NFS, SNMP
Presentation Layer	JPG, PNG, GIF, MPEG, ASCII, CSS, HTML
Session Layer	RPC, SCP, TLS
Transport Layer	TCP, UDP
Network Layer	IPv4, IPv6, ICMP, IPsec
Data Link Layer	MAC, PPP, ATM, HDLC, Frame Relay



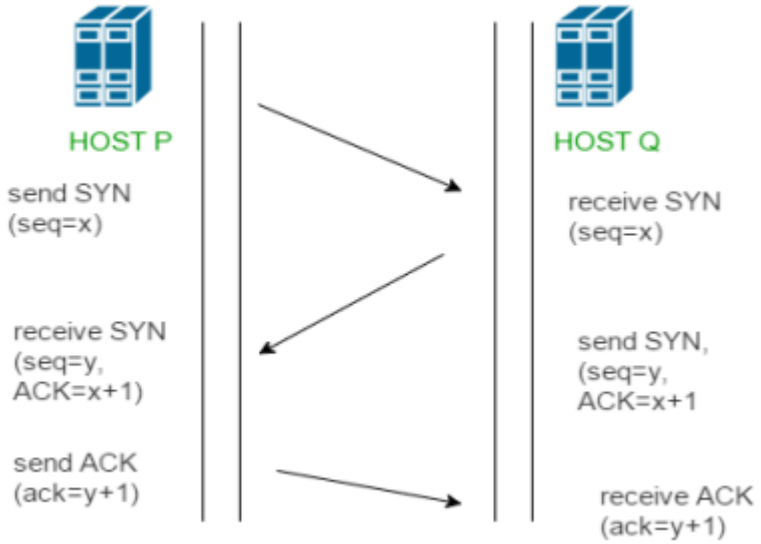
Giao thức TCP và UDP

- So sánh TCP và UDP

TCP là một giao thức hướng kết nối; nghĩa là, một kết nối hợp lệ giữa các hệ thống được thiết lập trước khi dữ liệu được truyền đi.	UDP là một giao thức không hướng kết nối. Không có kết nối trước được thiết lập trước khi bắt đầu truyền dữ liệu.
Các ứng dụng yêu cầu độ tin cậy cao để truyền dữ liệu sử dụng TCP.	Các ứng dụng có độ tin cậy của truyền dữ liệu không phải là sự cân nhắc quan trọng nhất sử dụng UDP.
TCP mất nhiều thời gian hơn để truyền dữ liệu so với UDP.	UDP nhanh hơn TCP vì nó không tiêu tốn thời gian trong việc thiết lập kết nối hoặc sửa lỗi.
FTP, HTTP, HTTPS, Telnet và SMTP là một vài trong số các giao thức sử dụng TCP.	DNS, DHCP, TFTP, SNMP là một vài trong số các giao thức sử dụng UDP.
Kích thước tiêu đề trong TCP là 20 byte - chứa nhiều thông tin hơn.	Kích thước tiêu đề trong UDP là 8 byte.
TCP cung cấp khả năng phát hiện và phục hồi lỗi và do đó đảm bảo dữ liệu đến đích nguyên vẹn.	UDP không cung cấp phục hồi lỗi, nên không đảm bảo dữ liệu đến đích nguyên vẹn.

Thiết lập kết nối trong TCP

- Quá trình bắt tay ba bước trong TCP



No.	Time	Source	Destination	Protocol	Length	Info
12	1.99…	192.168.1.202	104.18.60.128	TCP	66	18987 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK
13	2.02…	104.18.60.128	192.168.1.202	TCP	66	443 → 18987 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
14	2.03…	192.168.1.202	104.18.60.128	TCP	54	18987 → 443 [ACK] Seq=1 Ack=1 Win=17408 Len=0

Giao thức IP/địa chỉ IP/Cổng

- Giao thức IP
  - Hoạt động ở tầng network, làm cho các gói dữ liệu có thể định tuyến đến các mạng khác nhau
  - Chức năng: đánh địa chỉ và định tuyến
  - Public và Private

Giao thức IP/địa chỉ IP/Cổng

- Một số cổng thông dụng

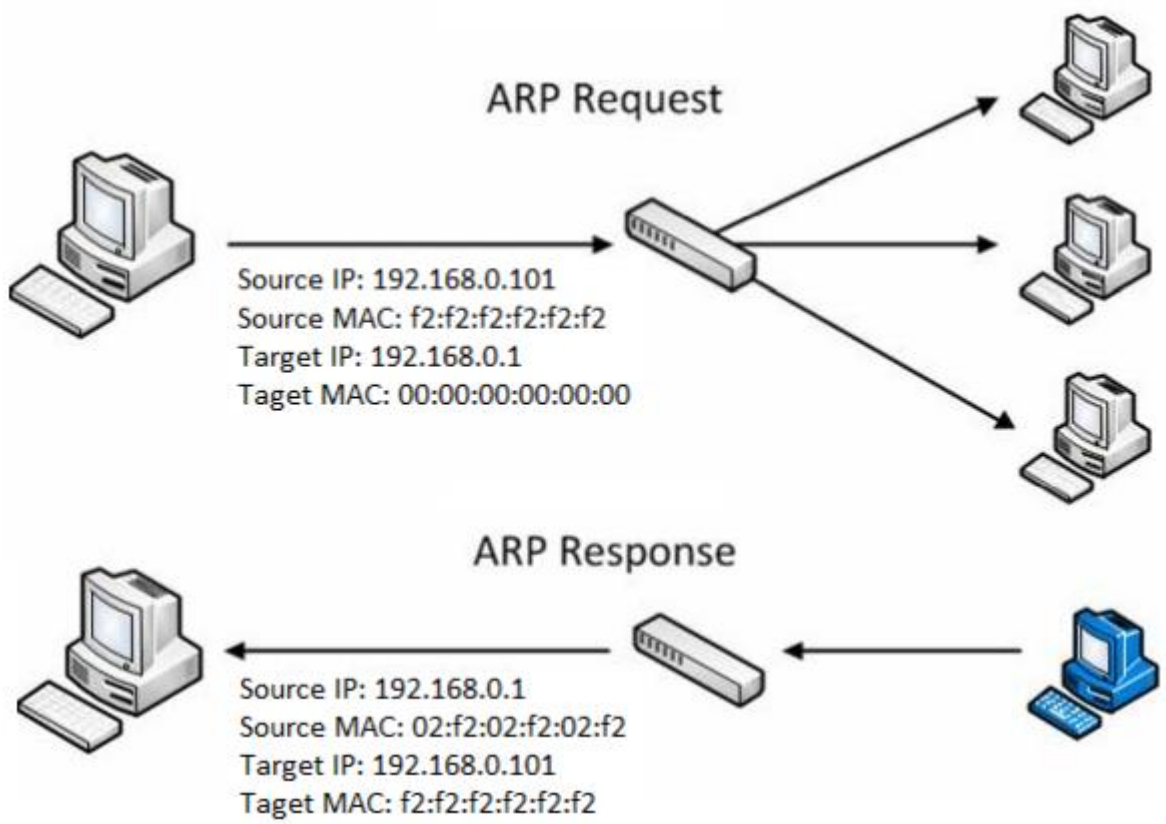
Application	Port Number
FTP	20-21
Telnet	23
SMTP	25
DNS	53
TFTP	69
HTTP	80
POP3	110
NTP	123
Microsoft RPC	135
NetBIOS	137-139
LDAP	389
HTTPS	443

Địa chỉ MAC và giao thức phân giải ARP

- Địa chỉ logic: IP
- Địa chỉ vật lý: MAC (duy nhất, gán bởi nhà sản xuất)
  - Lệnh xem địa chỉ mac: getmac /v
- Giao thức ARP: chuyển đổi địa chỉ MAC và IP
  - Lệnh xem địa chỉ MAC và IP: arp /a
  - ARP chuyển đổi địa chỉ lớp 3 (network) thành địa chỉ lớp 2 (datalink)

Hoạt động của ARP

- Kết nối 2 IP

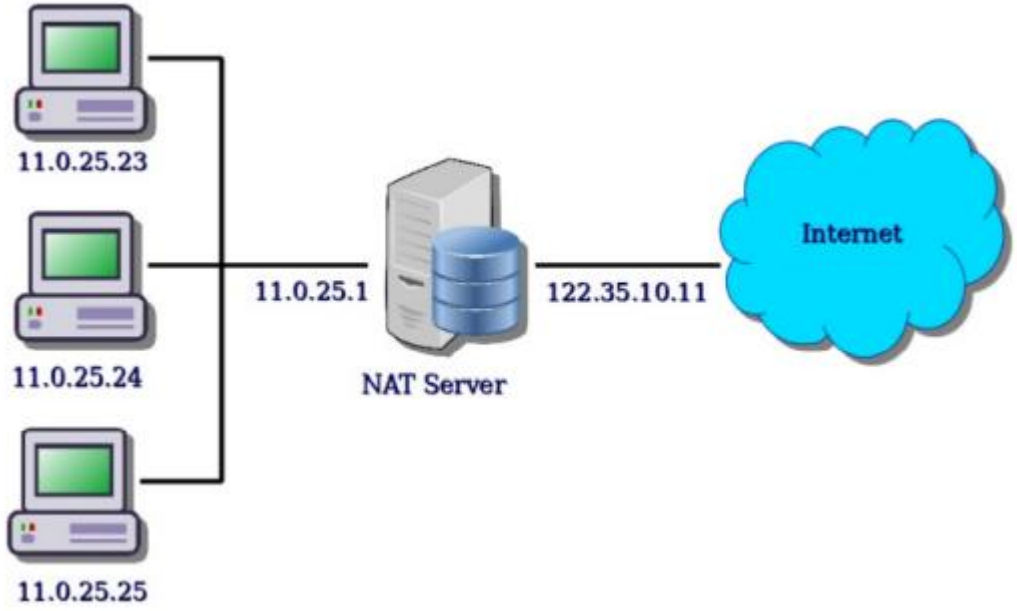


DNS và DHCP

- DNS
  - Chuyển đổi IP sang tên miền
    - Lệnh nslookup tên miền
- DHCP
  - Cấp phát IP tự động cùng các cấu hình liên quan khác như subnet mask, gateway mặc định và DNS

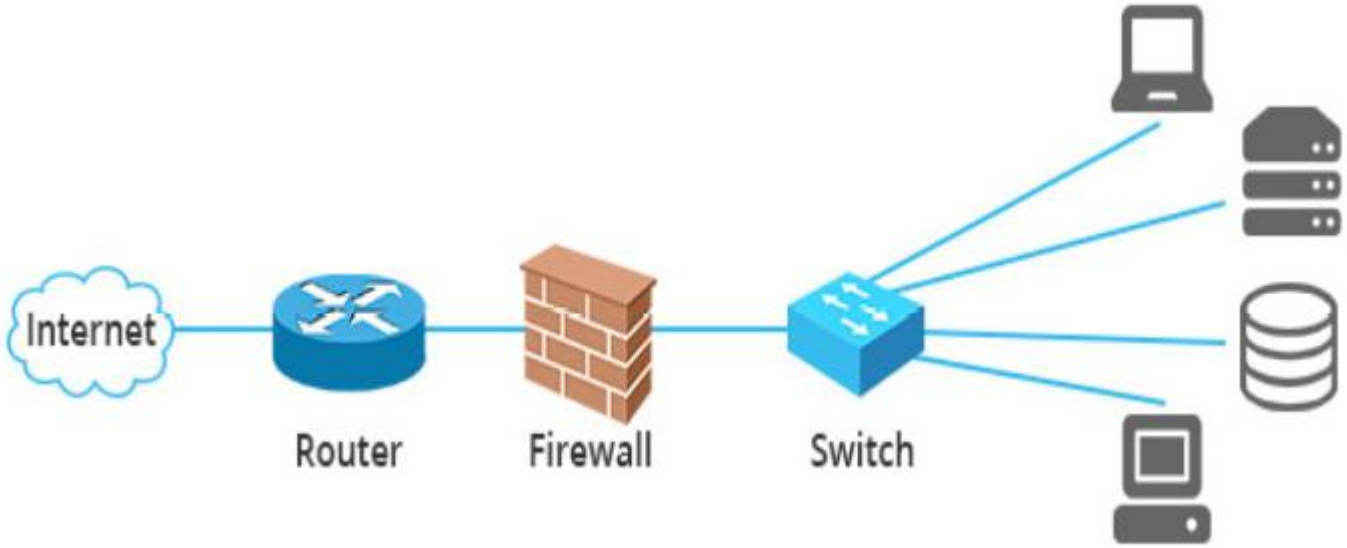
Chuyển dịch địa chỉ NAT

- Cho phép một hay nhiều địa chỉ IP nội miền được ánh xạ với một hay nhiều địa chỉ IP ngoại miền
  - Thay đổi một hoặc cả hai địa chỉ bên trong một gói tin khi đi qua router



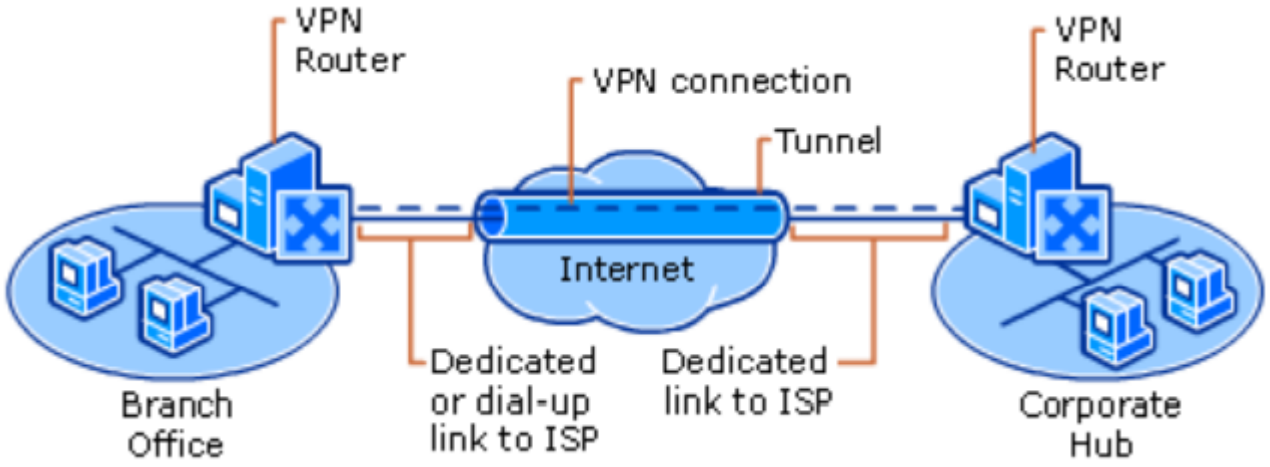
Các thiết bị mạng

- Router
- Switch
- …



Mạng riêng ảo VPN

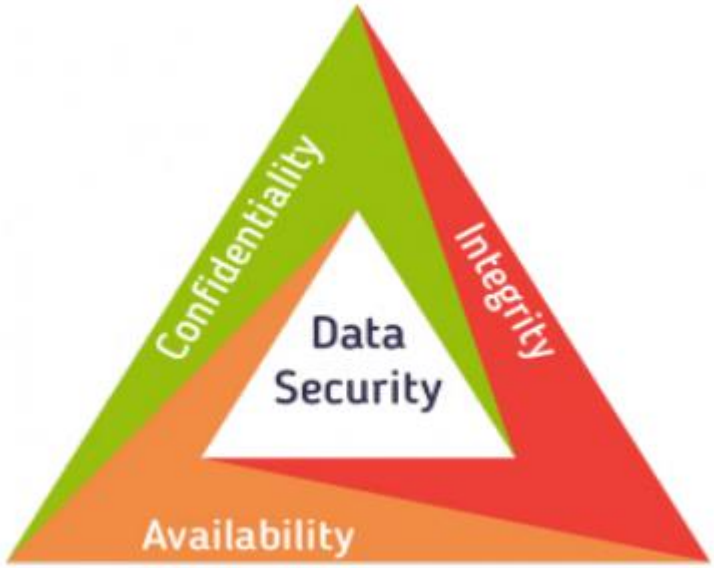
- Tạo kết nối mạng an toàn khi tham gia vào mạng công cộng



  - Remote access VPN
  - Site-to-Site VPN

An toàn thông tin trên mạng

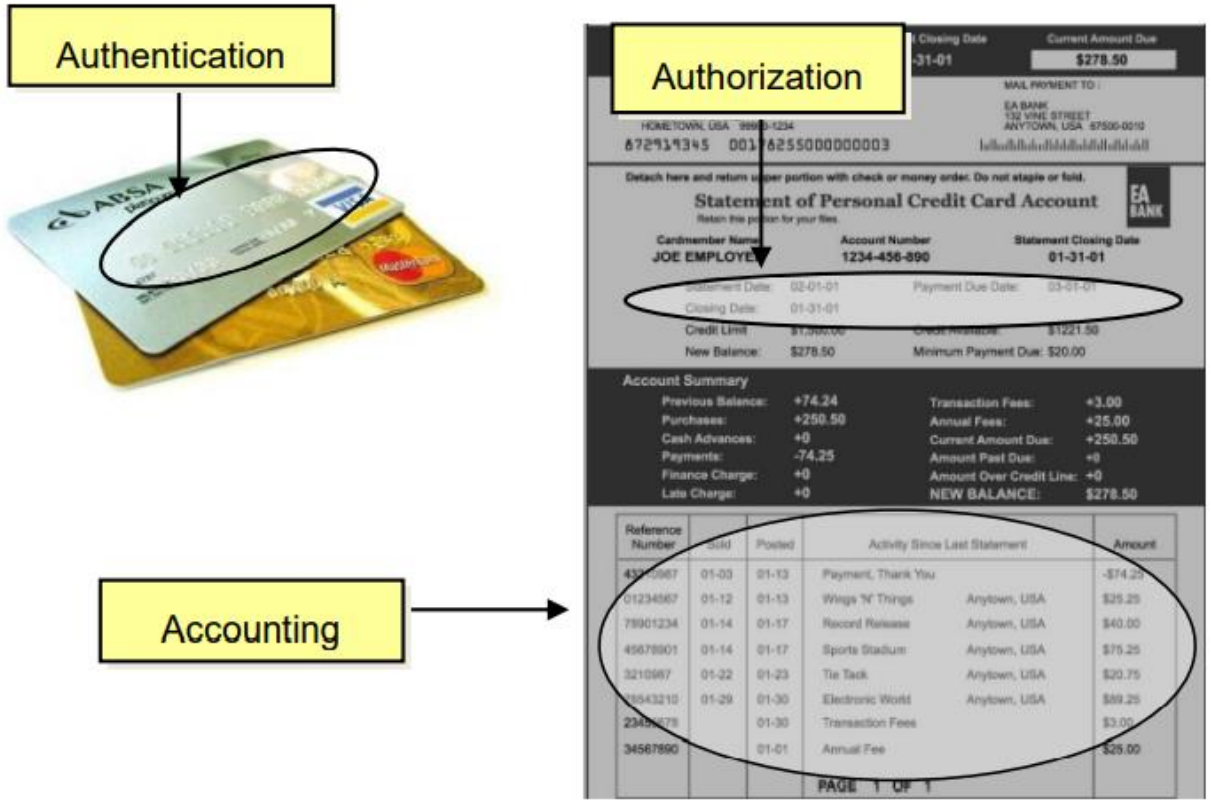
- CIA Triad: bí mật, toàn vẹn và sẵn sàng



Attacks that affect:	Examples
Confidentiality	Packet sniffing, password cracking, dumpster diving, wiretapping, keylogging, phishing
Integrity	Salami attacks, data diddling attacks, session hijacking, man-in-the-middle attack
Availability	DoS and DDoS attacks, SYN flood attacks, physical attacks on server infrastructure

An toàn thông tin trên mạng

- AAA: xác thực, phân quyền và chịu trách nhiệm



Các nguy cơ An toàn thông tin

- Đe dọa tự nhiên, vật lý, con người
- Bảo mật nhiều lớp