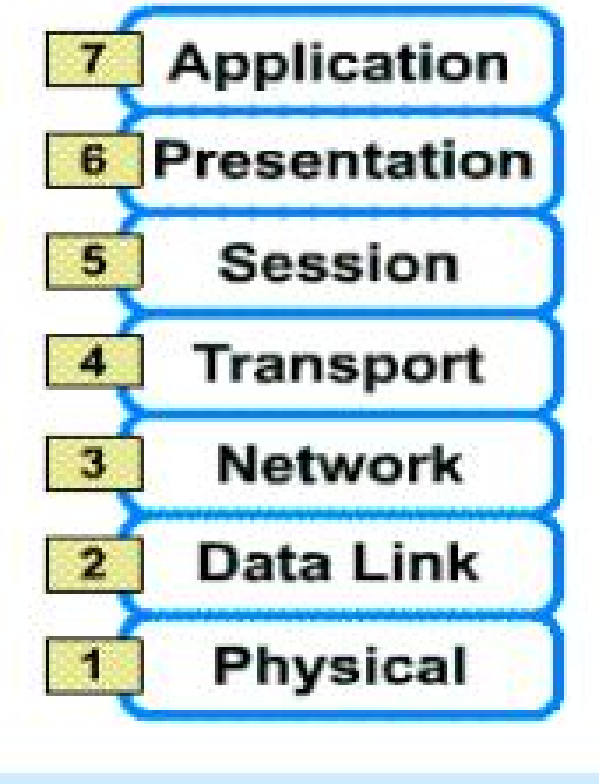
CHƯƠNG 6

AN TOÀN & BẢO MẬT HỆ THỐNG THÔNG TIN TRÊN INTERNET

6.1 Hạ tầng mạng

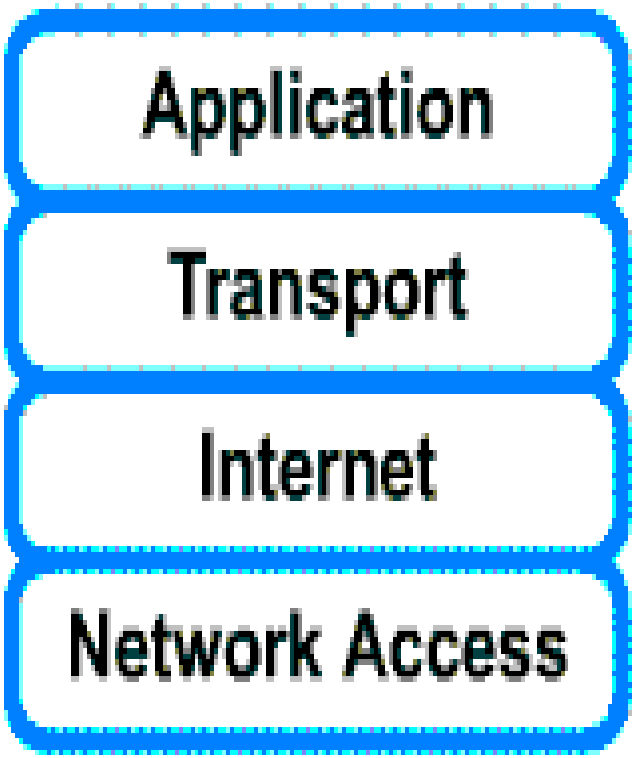
6.1.1 Chuẩn OSI và TCP/IP

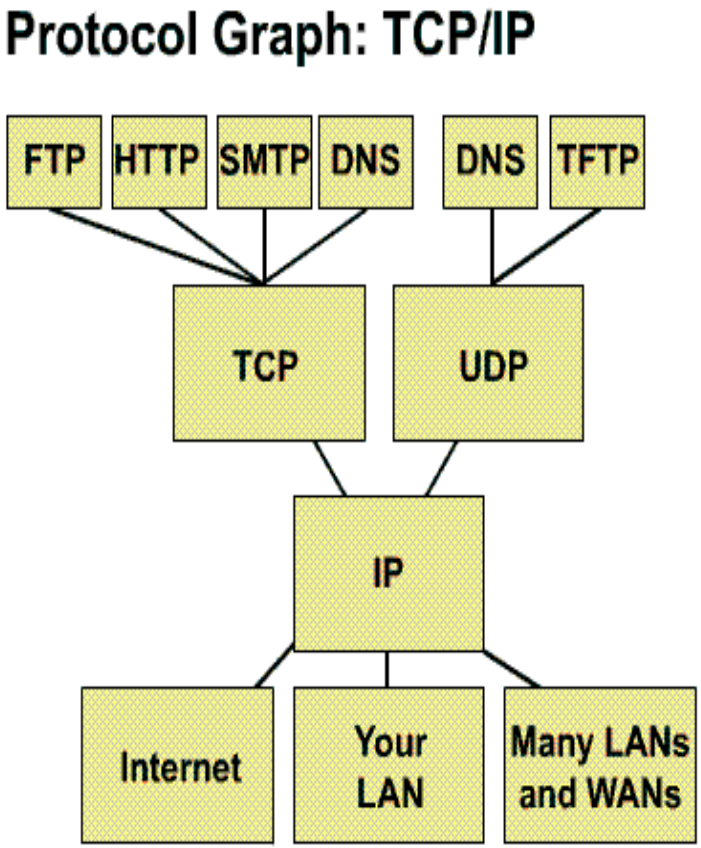


Mô hình phân lớp nhằm

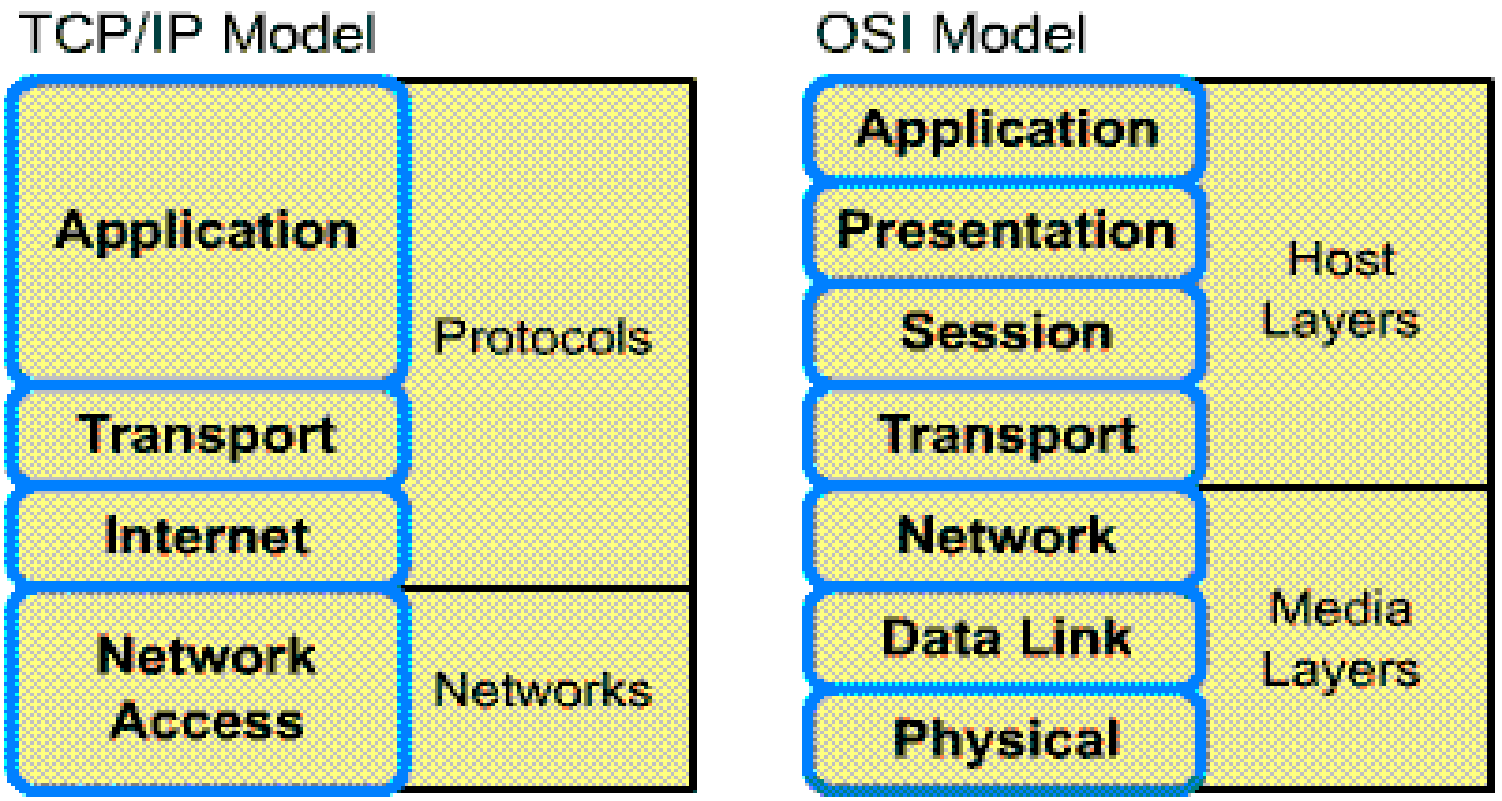
- ✓Giảm độ phức tạp
- ✓Tiêu chuẩn hoá các giao diện
- ✓Module hoá các chi tiết kỹ thuật
- ✓Đảm bảo mềm dẻo quy trình công nghệ
- ✓Thúc đẩy quá trình phát triển
- ✓Dễ dàng trong việc giảng dạy ,huấn luyện

6.1.2. TCP/IP model

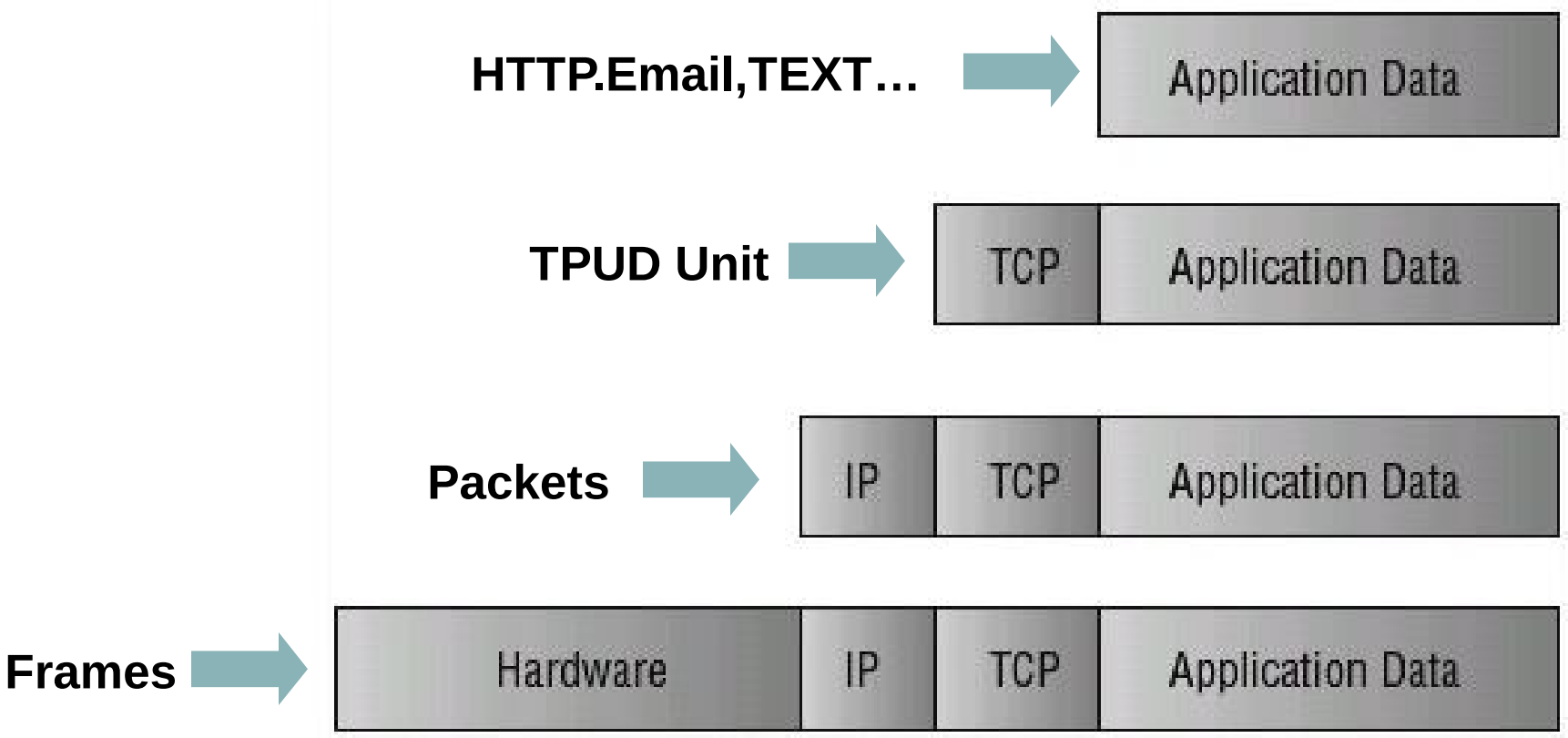




6.1.3 Mô hình OSI và TCP/IP

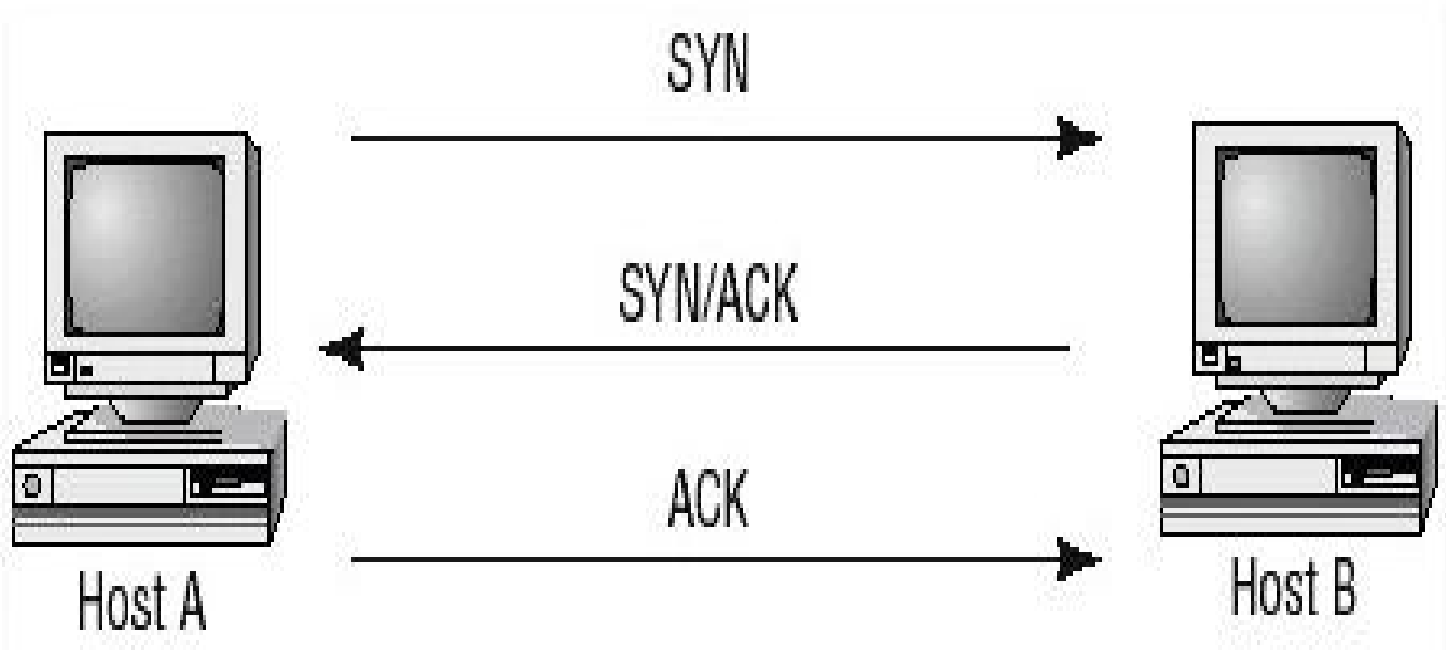


6.1.4. Đóng gói trong TCP/IP

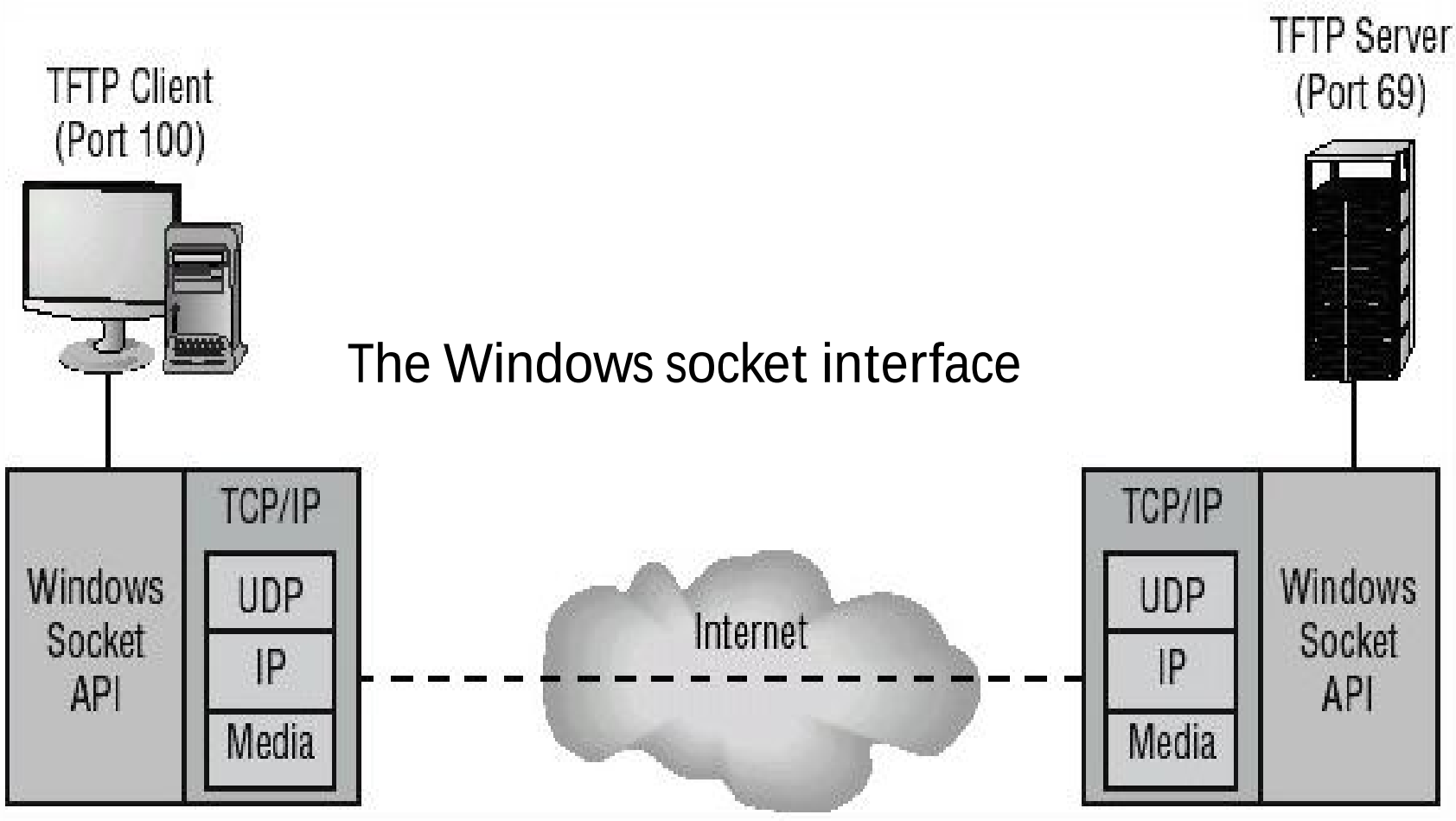


6.1.5. TCP Three - Way – Handshake

Kết nối có định hướng → thực hiện bằng "tree - way handshake"



6.1.6.Application Programming Interfaces (API)



6.2. Các điểm yếu dễ bị khai thác trên mạng

6.2.1.TCP/IP Attacks

- Xảy ra trên lớp IP hay “host –to- host”
- Router /Firewall có thể ngăn chặn một số giao thức lộ liễu trên Internet
- ARP không phải giao thức định tuyến nên không gây tổn thương do tấn công từ bên ngoài
- Các điểm yếu :SMTP & ICMP, TCP, UDP và IP → có thể đi xuyên qua các lớp mạng

Các hình thức TCP/IP attack

- Port Scans : Quét các cổng
- TCP Attacks :

  TCP SYN or TCP ACK Flood Attack,

  TCP Sequence Number Attack,

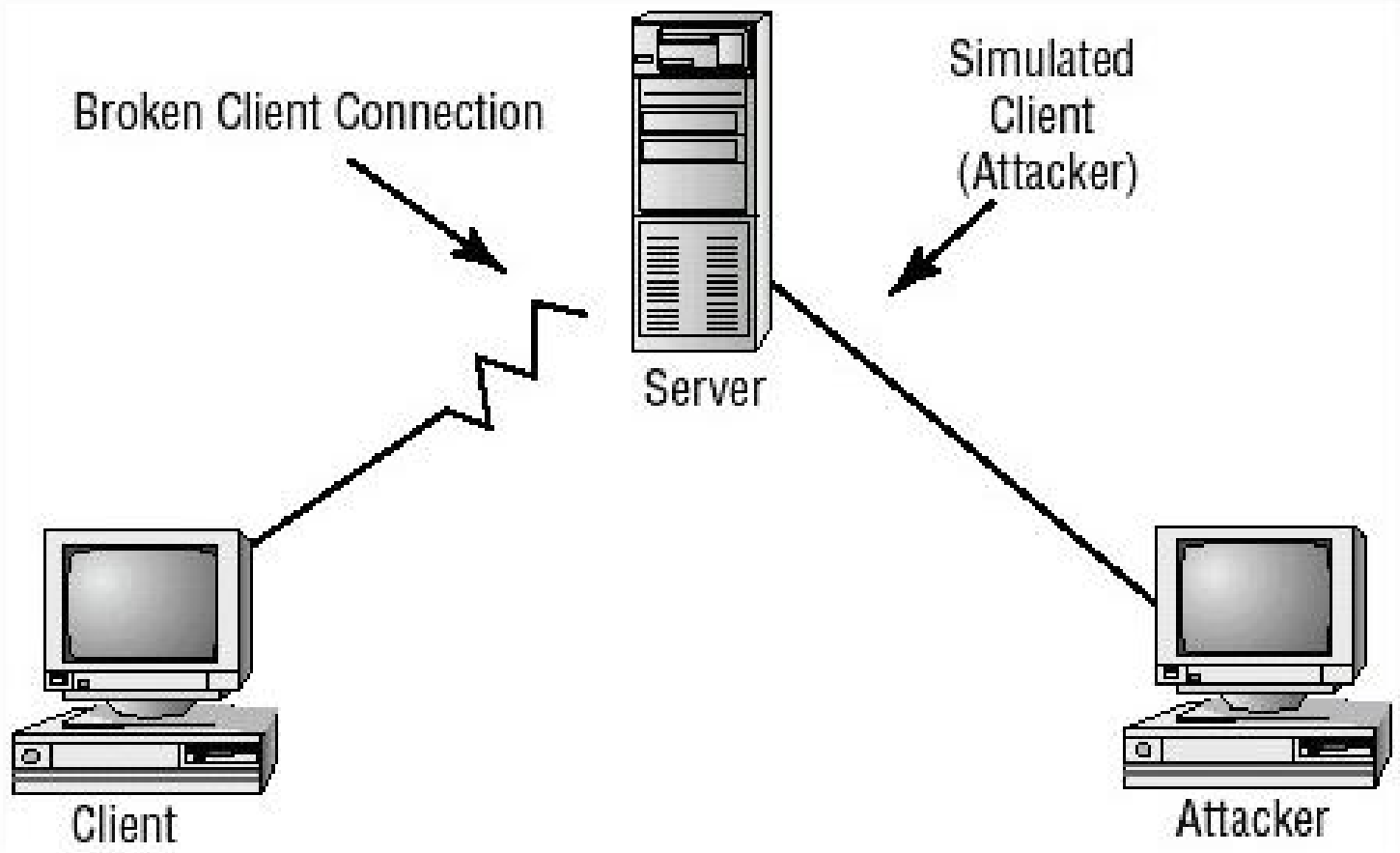
  TCP/IP Hijacking

  Network Sniffers : Bắt giữ và hiển thị các thông báo trên mạng

1. Network Sniffers

- Network sniffer đơn thuần chỉ là thiết bị dùng để bẫy và hiển thị dòng thông tin trên mạng
- Nhiều card NIC có chức năng " Promiscuous mode"→ Cho phép card NIC bắt giữ tất cả các thông tin mà nó thấy trên mạng.
- Các thiết bị như routers, bridges, and switches có thể được sử dụng để phân tách các vùng mạng con trong một mạng lớn .
- Sử dụng sniffer, kẻ tấn công bên trong có thể bắt giữ tất cả mọi thông tin truyền trong mạng.

2. TCP/IP hijacking - active sniffing



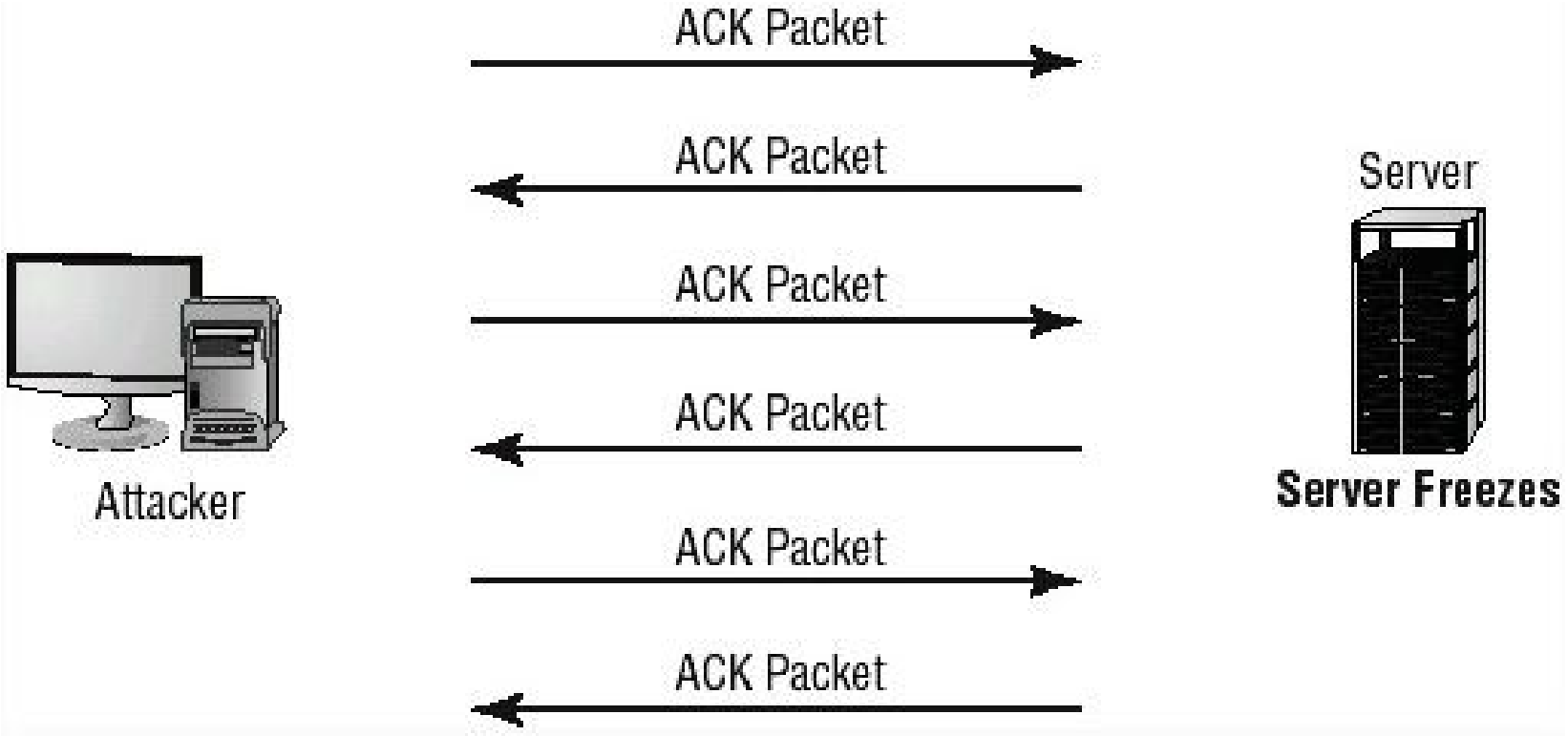
3.Port Scans

- Kể tấn công dò tìm một cách có hệ thống mạng và xác định các cổng cùng viới các dịch vụ đang mở (port scanning), việc quét cổng có thể tiến hành từ bên trong hoặc từ bên ngoài. Nhiều router không được cấu hình đúng đã để tất cả các gói giao thức đi qua.
- Một khi đã biết địa chỉ IP , kẻ tấn công từ bên ngoài có thể kết nối vào mạng với các cổng mở thậm chí sử dụng một giao thức đơn giản như Telnet.
- Quá trình Port Scans được dùng để "in dấu chân (footprint)" một tổ chức .Đây là bước đầu tiên của một cuộc tấn công.

4. TCP Attacks

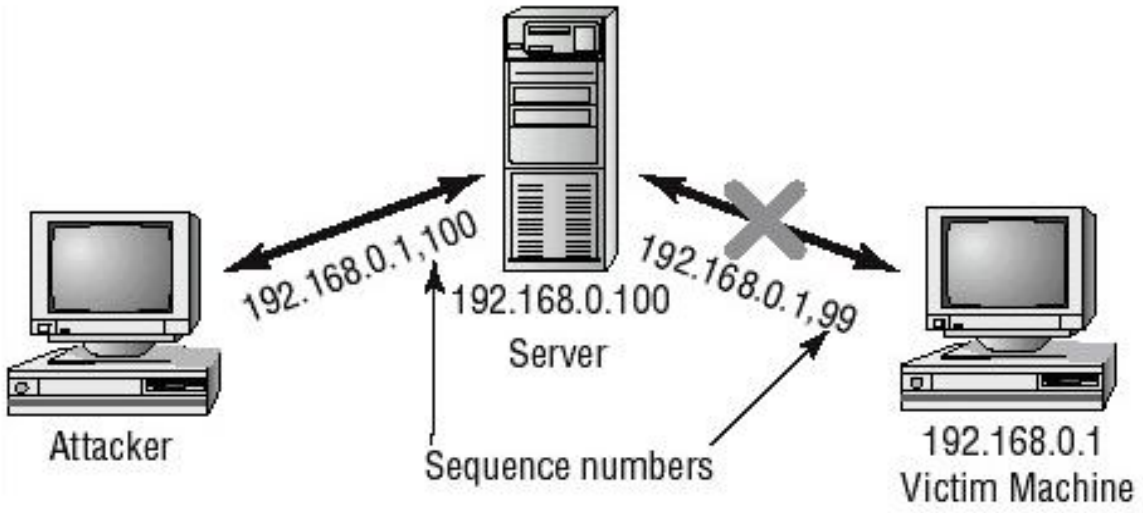
- Đặc điểm : Bắt tay ba chiều " Three Way Handsake "
- Tấn công tràn ngập SYN (TCP SYN hay TCP ACK Flood Attack)
- Máy client và server trao đổi các gói ACK xác nhận kết nối
- Hacker gửi liên tục các ACK packet đến server.
- Máy server nhận được các ACK từ hacker song không thực hiện được bất cứ phiên làm việc nào nào → kết quả là server bị treo → các dịch vụ bị từ chối (DoS).
- Nhiều router mới có khả năng chống lại các cuộc tấn công loại này bằng các giới hạn số lượng các cuộc trao đổi SYN ACK.

Mô tả TCP SYN hay TCP ACK Flood Attack



5.TCP Sequence Number Attack

- *TCP sequence attacks* xảy ra khi attacker nắm quyền kiểm soát một bên nào đó của phiên làm việc TCP .
- Khi truyền một thông điệp TCP ,một "sequence number - SN "được một trong hai phía tạo ra.
- Hacker chiếm SN và thay đổi thành SN của mình.



6. UDP Attack

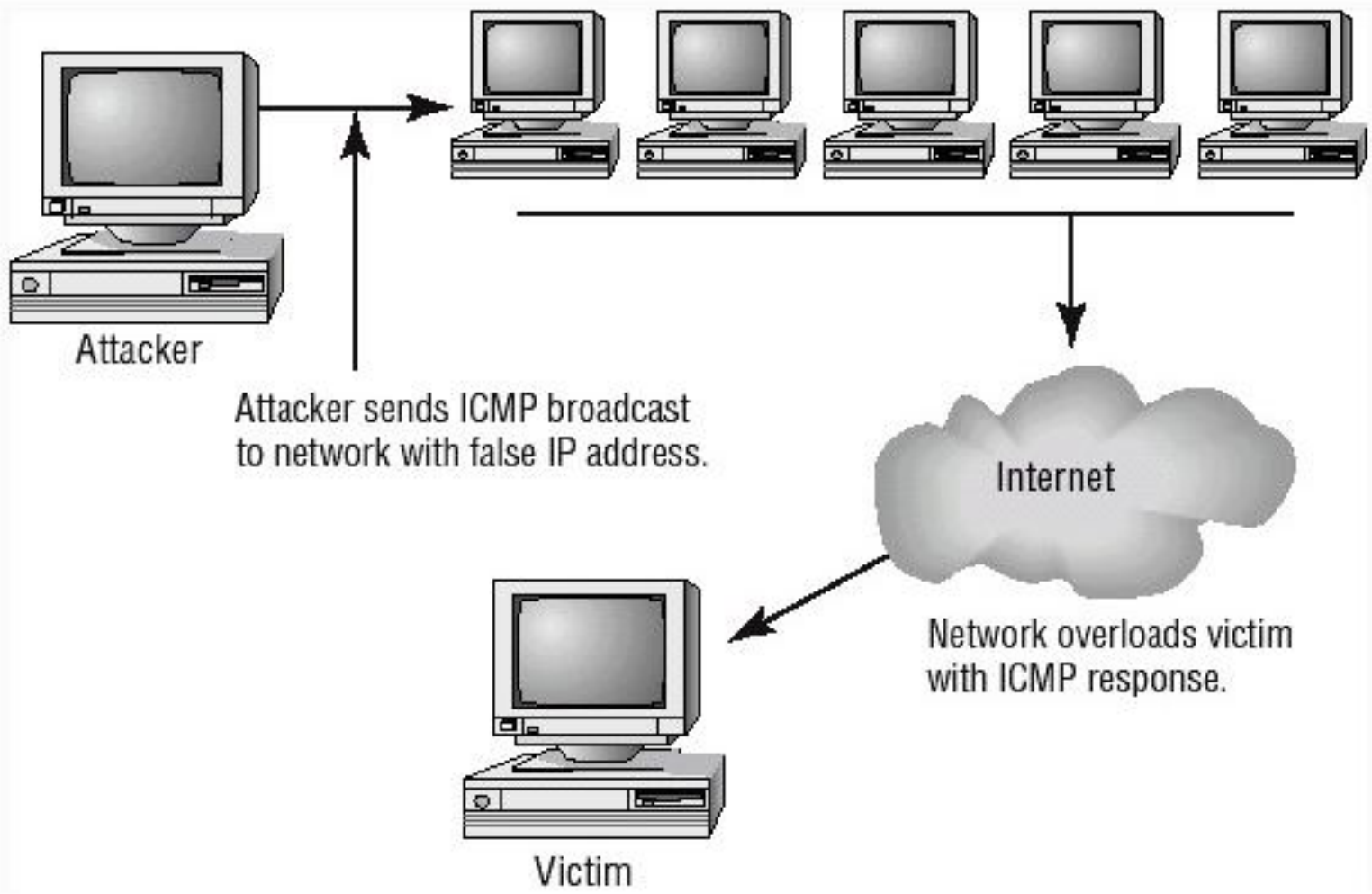
- *UDP attack* sử dụng các giao thức bảo trì hệ thống hoặc dịch vụ UDP để làm quá tải các dịch vụ giống như DoS . UDP attack khai thác các giao thức UDP protocols.
- UDP packet không phải là " connection-oriented" nên không cần "synchronization process – ACK"
- UDP attack - *UDP flooding (Tràn ngập UDP)*
- Tràn ngập UDP gây quá tải băng thông của mạng dẫn đến DoS .

7. ICMP attacks : Smurf và ICMP tunneling

- ICMP sử dụng PING program. Dùng lệnh PING với địa chỉ IP của máy đích
- Gây ra do sự phản hồi các gói ICMP khi có yêu cầu bảo trì mạng.
- Một số dạng thông điệp ICMP

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

a. SMURF ATTACKS



SMURF ATTACKS

- Attacker gửi packet đến network amplifier (router hay thiết bị mạng khác hỗ trợ broadcast), với địa chỉ của nạn nhân. Thông thường là những packet ICMP ECHO REQUEST, các packet này yêu cầu yêu cầu bên nhận phải trả lời bằng một ICMP ECHO REPLY .
- Network amplifier sẽ gửi đến ICMP ECHO REQUEST đến tất cả các hệ thống thuộc địa chỉ broadcast và tất cả các hệ thống này sẽ REPLY packet về địa chỉ IP của mục tiêu tấn công Smuft Attack.

b. Fraggle Attack: tương tự như Smuft attack nhưng thay vì dùng ICMP ECHO REQUEST packet thì sẽ dùng UDP ECHO packet gửi đến mục tiêu.

6.2.2.Tấn công DDOS

Các giai đoạn của một cuộc tấn công kiểu DDoS:

1. Chuẩn bị :

- Là bước quan trọng nhất của cuộc tấn công, Các công cụ DDoS hoạt động theo mô hình client-server.(Xem 10 best tools for DDOS).
- Dùng các kỹ thuật hack khác để nắm trọn quyền một số host trên mạng.
- Cấu hình và thử nghiệm toàn bộ attack-netword (bao gồm các máy đã bị lợi dụng cùng với các software đã được thiết lập trên đó, máy của hacker hoặc một số máy khác đã được thiết lập như điểm phát động tấn công) cũng sẽ được thực hiện trong giai đoạn này.

- Best Tool DDOS 2011

1. Slowloris
2. HTTP POST 3.6
3. DDosim
4. Keep-alive attack
5. Low Orbit Ion Cannon Anonymous
6. r-u-dead
7. Slow Post Newver
8. Smurf 6.0
9. DNSDRDOS
10. Tools Slow dos PURIDDE Goobye ver3.0

2. Giai đoạn xác định mục tiêu và thời điểm:

- Sau khi xác định mục tiêu lấn cuối, hacker sẽ có hoạt động điều chỉnh attack-netword chuyển hướng tấn công về phía mục tiêu.

- Yếu tố thời điểm sẽ quyết định mức độ thiệt hại và tốc độ đáp ứng của mục tiêu đối với cuộc tấn công.

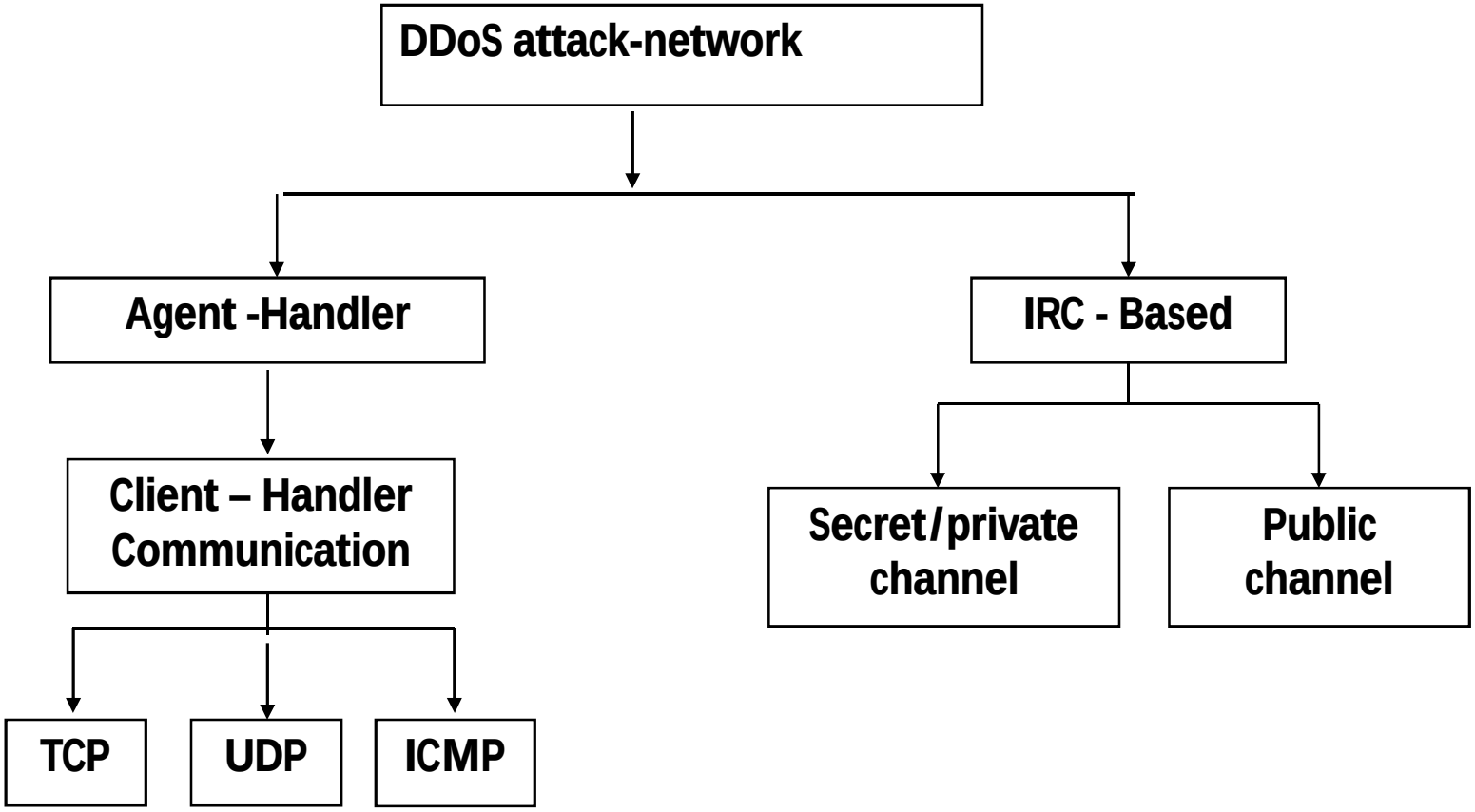
3. Phát động tấn công và xóa dấu vết:

- Đúng thời điểm đã định, hacker phát động tấn công từ máy của mình, lệnh tấn công này có thể đi qua nhiều cấp mói đến host thực sự tấn công. Toàn bộ attack-network (có thể lên đến hàng ngàn máy), sẽ vắt cạn năng lực của server mục tiêu liên tục, ngăn chặn không cho nó hoạt động như thiết kế.
- Sau một khoảng thời gian tấn công thích hợp, hacker tiến hành xóa mọi dấu vết có thể truy ngược đến mình, việc này đòi hỏi trình độ khá cao .

4. Kiến trúc tổng quan của DDoS attack-network:

+ Mô hình Agent – Handler

+ Mô hình IRC – Based

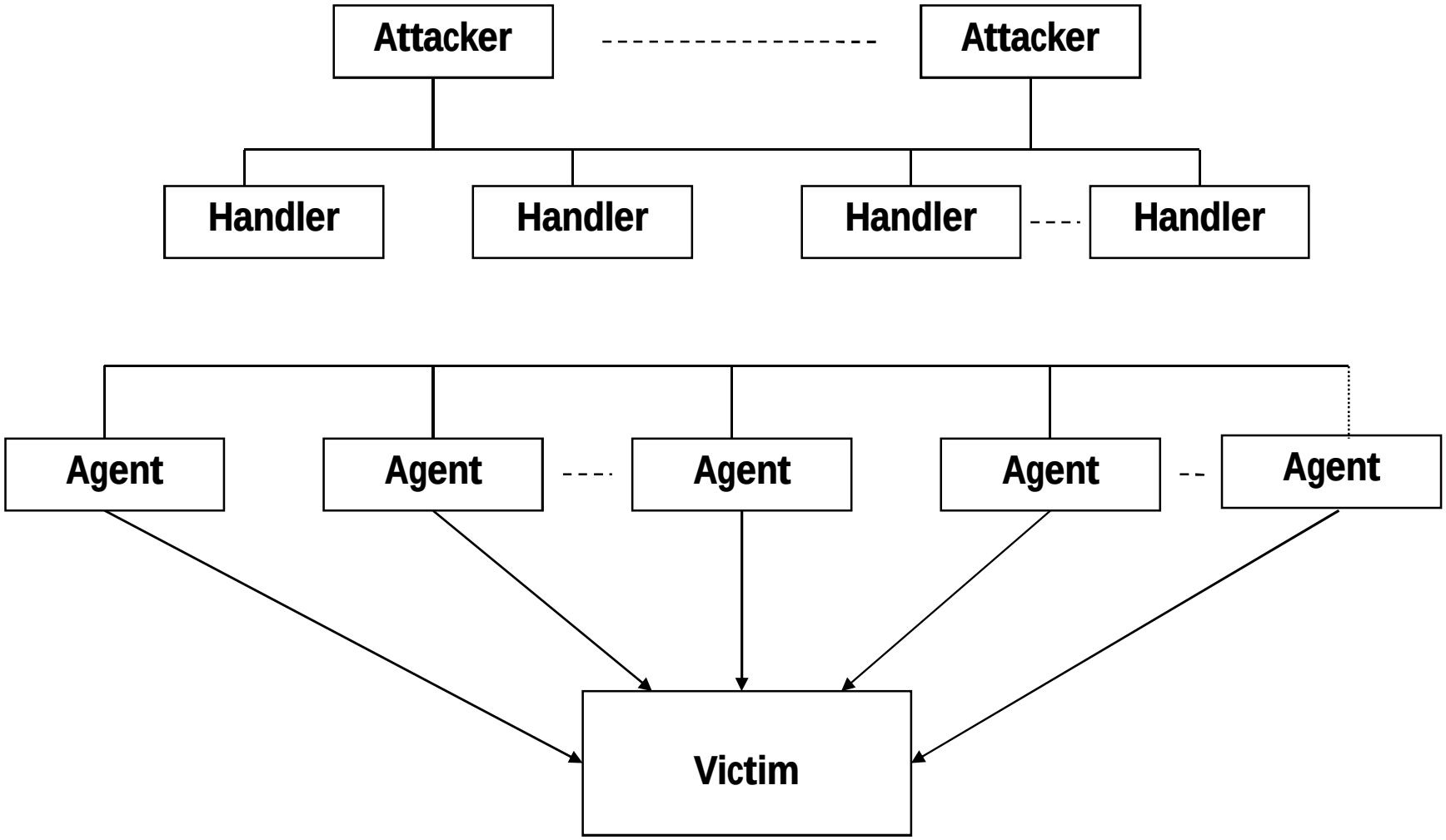


4.a. Mô hình Agent – Handler

Theo mô hình này, attack-network gồm 3 thành phần: Agent, Client và Handler

- ✓ Client : là software cơ sở để hacker điều khiển mọi hoạt động của attack-network
- ✓ Handler : là một thành phần software trung gian giữa Agent và Client
- ✓ Agent : là thành phần software thực hiện sự tấn công mục tiêu, nhận điều khiển từ Client thông qua các Handler

Mô hình Agent-Handler



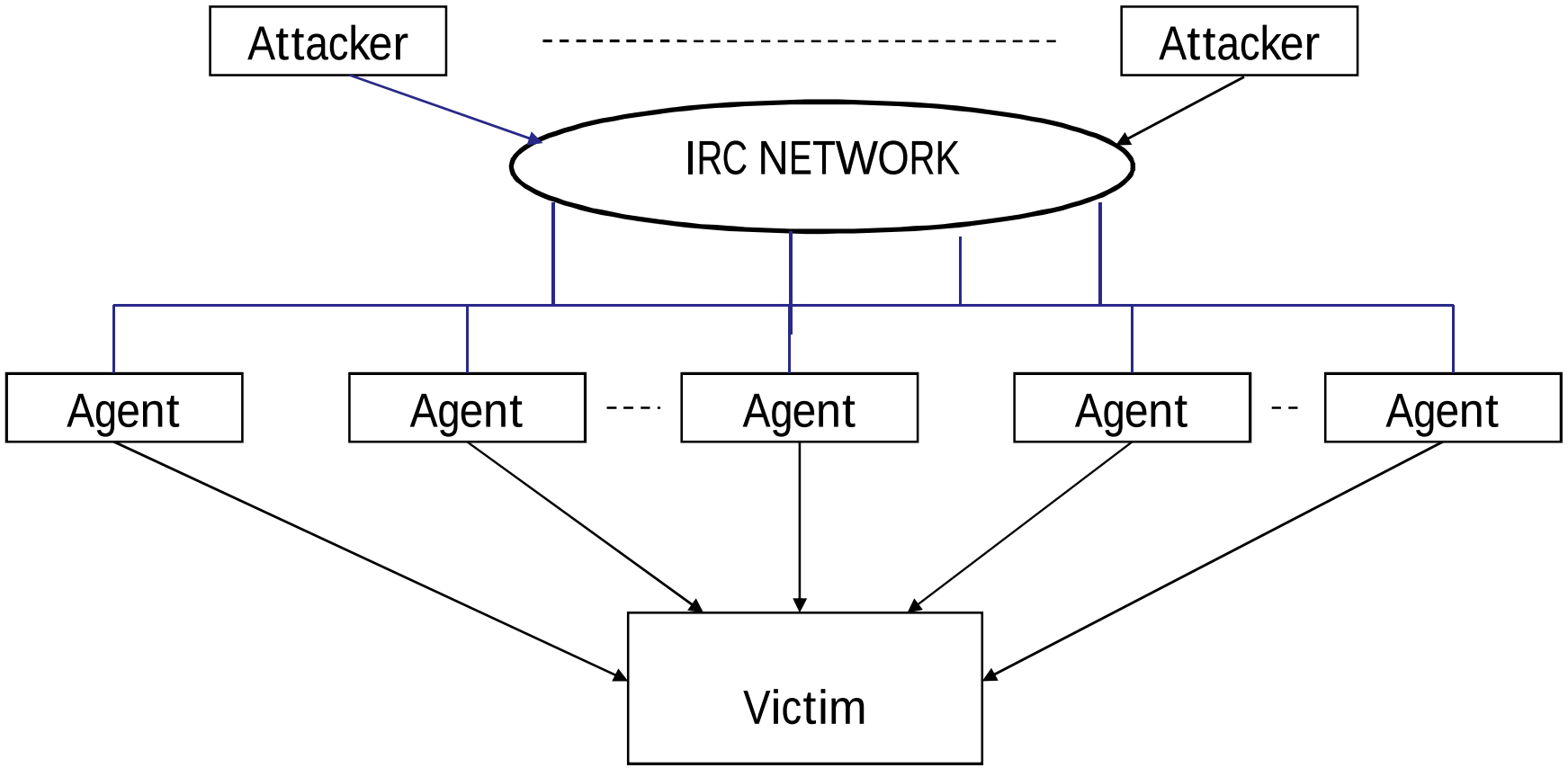
4.b.Mô hình IRC – Based:

- Internet Relay Chat (IRC) là một hệ thống online chat multiuser
- IRC cho phép User tạo một kết nối multipoint đến nhiều user khác và chat thời gian thực.
- Kiến trúc của IRC network bao gồm nhiều IRC server trên khắp internet, giao tiếp với nhau trên nhiều kênh (channel).
- IRC network cho phép user tạo ba loại channel: public, private và serect.

Các kênh IRC

- Public channel: Cho phép user của channel đó thấy IRC name và nhận được message của mọi user khác trên cùng channel
- Private channel: giao tiếp với các đối tượng cho phép. Không cho phép các user không cùng channel thấy IRC name và message trên channel. Tuy nhiên, nếu user ngoài channel dùng một số lệnh channel locator thì có thể biết được sự tồn tại của private channel đó.
- Secrect channel : tương tự private channel nhưng không thể xác định bằng channel locator.

Kiến trúc attack-network của kiểu IRC-Base



5.Một số thế mạnh của mô hình IRC

- Rất khó phát hiện do các giao tiếp dưới dạng chat message.
- IRC traffic có thể di chuyển trên mạng với số lượng lớn mà không bị nghi ngờ
- Không cần phải duy trì danh sách các Agent, hacker chỉ cần logon vào IRC server là đã có thể nhận được report về trạng thái các Agent do các channel gửi về.
- Sau cùng: IRC cũng là một môi trường file sharing tạo điều kiện phát tán các Agent code lên nhiều máy khác.

6.Những kỹ thuật anti-DDOS

Có ba giai đoạn chính trong quá trình Anti-DDoS:

- Giai đoạn ngăn ngừa: tối thiểu hóa lượng Agent, tìm và vô hiệu hóa các Handler
- Giai đoạn đối đầu với cuộc tấn công: Phát hiện và ngăn chặn cuộc tấn công, làm suy giảm và dừng cuộc tấn công, chuyển hướng cuộc tấn công.
- Giai đoạn sau khi cuộc tấn công xảy ra: thu thập chứng cứ và rút kinh nghiệm

Những vấn đề có liên quan đến DDoS

- DDoS là một kiểu tấn công rất đặc biệt , cực kỳ hiểm ác . “DDos đánh vào nhân tố yếu nhất của hệ thống thông tin – con người - mà lại là dùng người chống người”.
- Các yếu điểm:
  - *Thiếu trách nhiệm với cộng đồng*
  - *Sự im lặng*
  - *Tầm nhìn hạn hẹp*

Một số vấn đề cần thực hiện :

- Giám sát chi tiết về luồng dữ liệu ở cấp ISP để cảnh cáo về cuộc tấn công.
- Xúc tiến đưa IPSec và Secure DNS vào sử dụng
- Khẳng định tầm quan trọng của bảo mật trong quá trình nghiên cứu và phát triển của Internet II.
- Nghiên cứu phát triển công cụ tự động sinh ra ACL từ security policy và router và firewall.
- Phát triển hệ điều hành bảo mật hơn.
- Sử dụng các hệ thống tương tự như Intrusion Dectection, hoạt động giám sát hệ thống và đưa ra các cảnh báo.v…v

6.3. Khai thác phần mềm

- **Khai thác Database** Nhiều sản phẩm database gây ra những mối hoài nghi khi truy cập vào môi trường clientt/server .Nếu phiên làm việc bị chiếm hoặc bị giả mạo, attacker có thể truy vấn đến các database không được phép.(SQL injections)
- **Khai thác Application** Macro virus là một ví dụ. Macro virus là một tập các chỉ thị trong một ngôn ngữ lập trình như VB script , chúng ra lệnh cho một ứng dụng tạo ra những chỉ dẫn sai.
- **Sử dụng e-mail** : Tích hợp nhiều công cụ → dễ bi khai thác

6.3.1.Malicious Code – mã độc hại

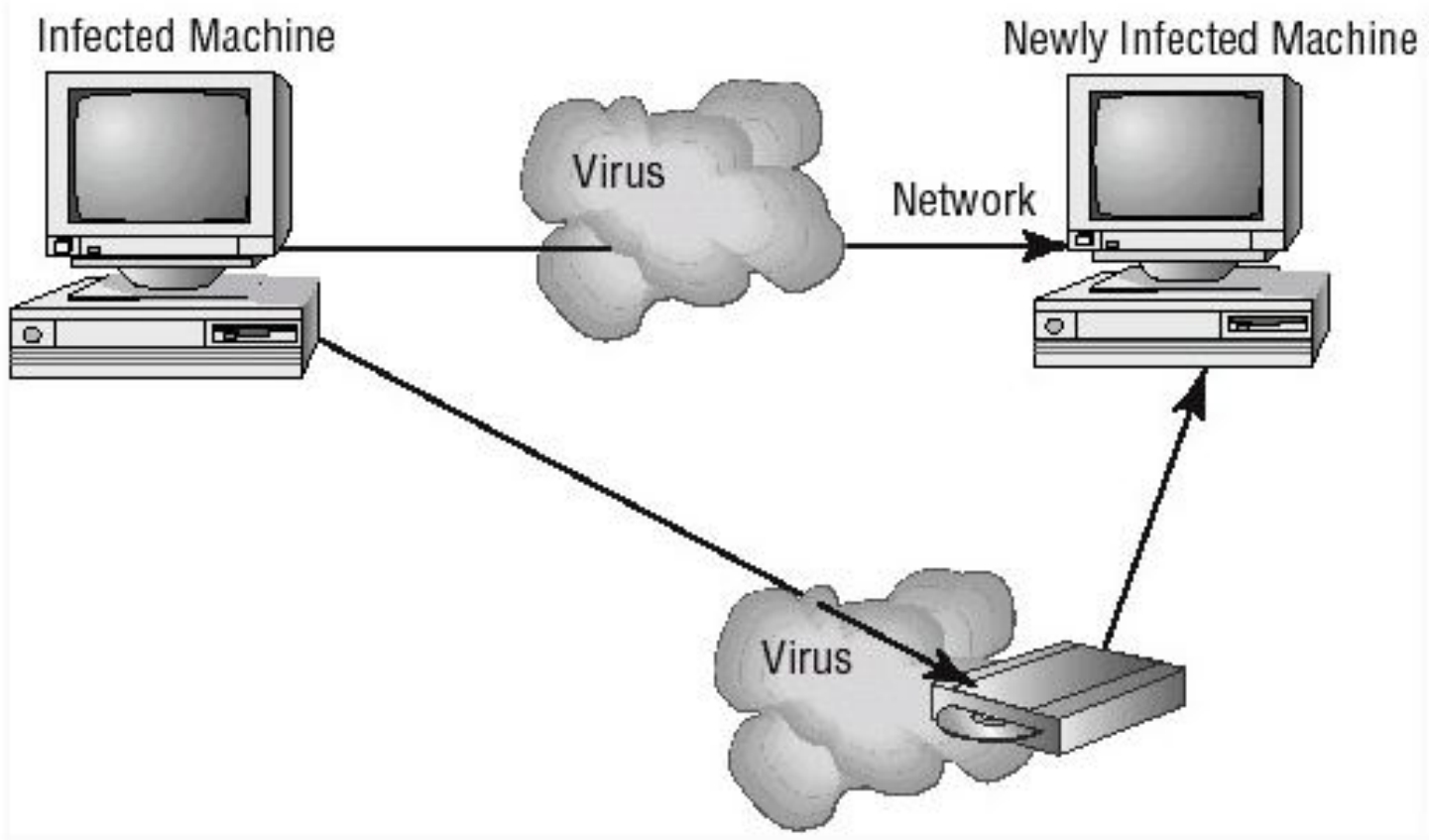
- *Virus* là một phần mềm được thiết kế để thâm nhập vào hệ thống máy tính. Virus làm hỏng dữ liệu trên hard disk, là sụp OS và lây lan sang các hệ thống khác.
- Phương pháp lây lan : Từ floppy hoặc CD-ROM, theo đường e-mail, hoặc một phần của một chương trình khác.

1.Một số dấu hiệu nhiễm virut

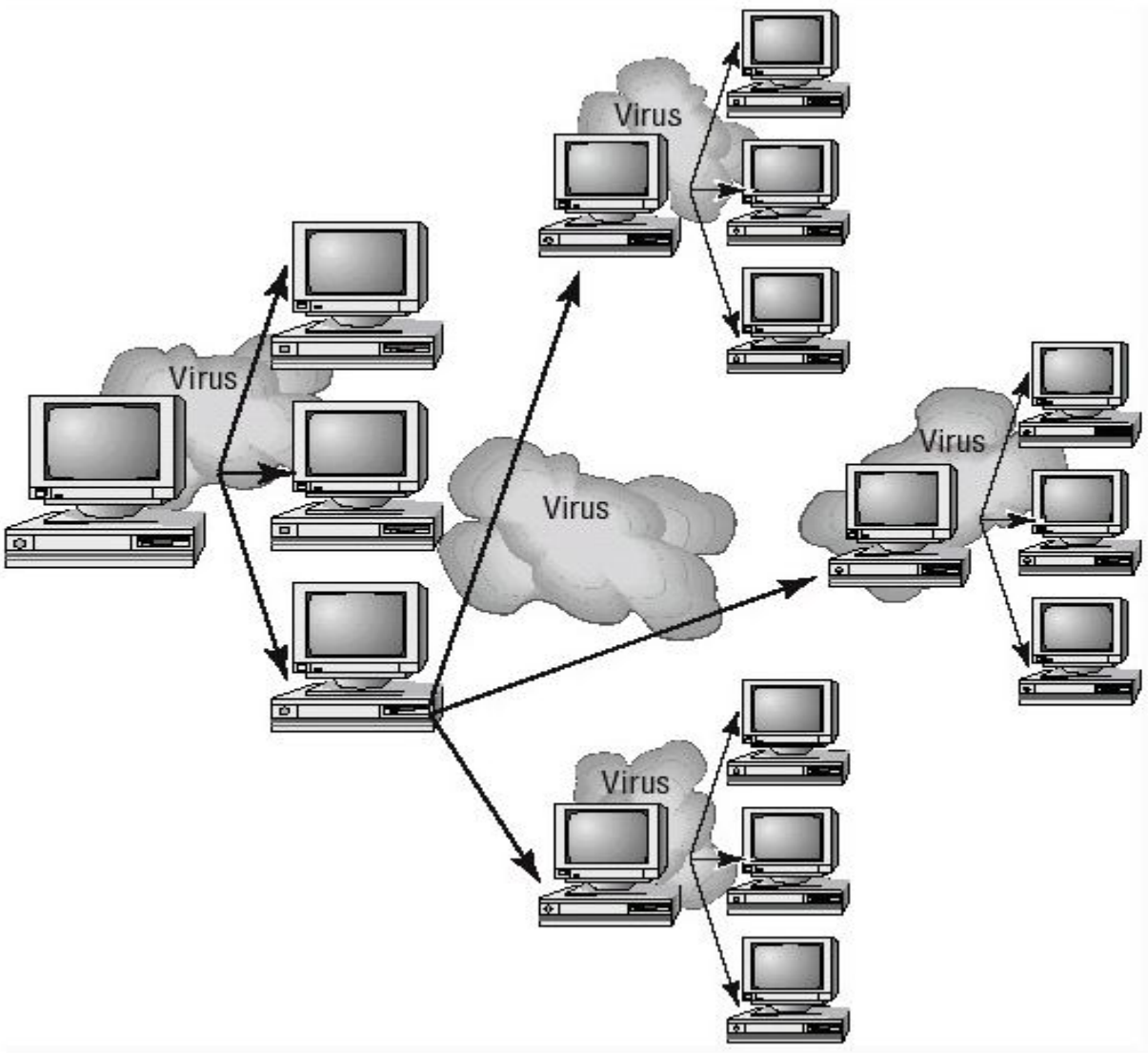
- Khởi động hoặc nạp chương trình chậm.
- Xuất hiện một số file lạ trên HDD hoặc mật một số file khởi động .
- Kích thước một số file bị thay đổi so với nguyên bản .
- Browser, bộ xử lý văn bản hoặc các phần mềm khác bắt đầu bằng những ký tự lạ . Màn hình hoặc menu có thể bị thay đổi (Deface).
- Hệ thống tự tắt hoặc khởi động lại một cách không bình thường.
- Mất truy cập vào các tài nguyên một cách khó hiểu.
- Không khởi động hệ thống.

2.Hoạt động của virut

a.Phá hoại và lây lan



b.Lây nhiễm qua e-mail

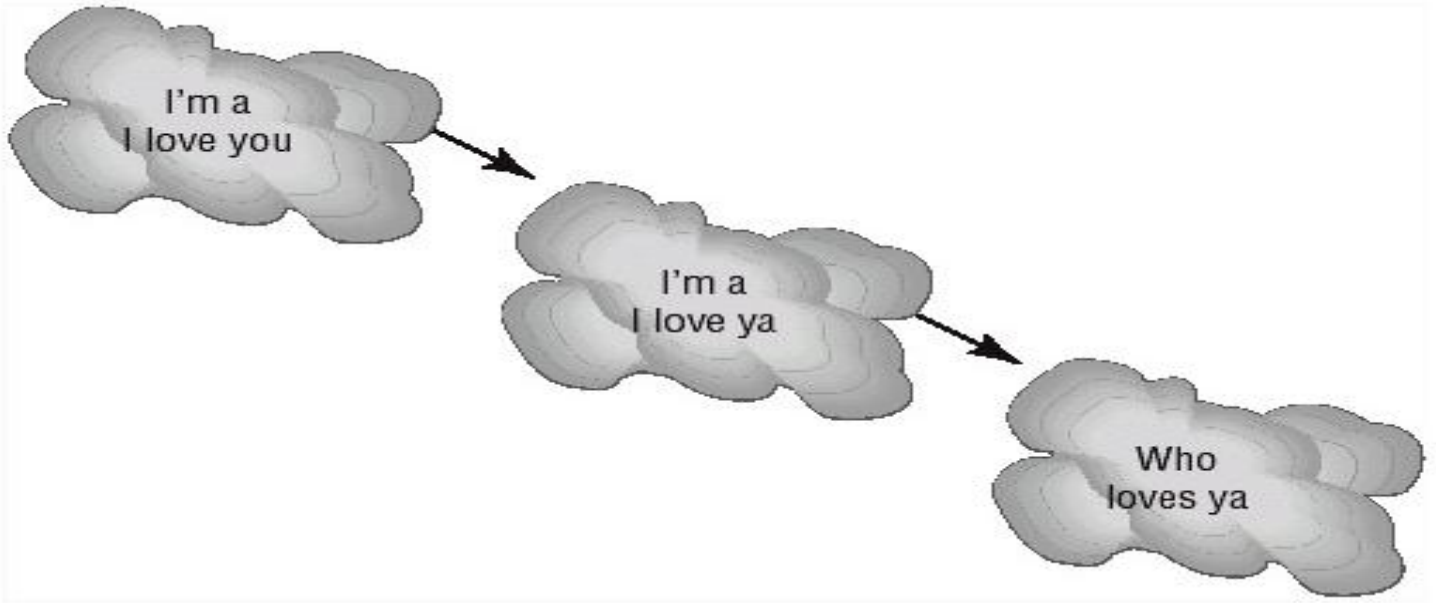


Lây nhiễm qua e-mail (tiếp)

Ví dụ : Virut Melissa lây nhiễm 100,000 user trong một khoảng thời gian rất ngắn vào 5/1999 (CERT). Một site đã nhận được 32,000 bản copy của virut Melissa trong vòng 45 phút.

3. Các loại virut

a. Polymorphic Virus : Virut đa hình → thay đổi hình thể để khó bị phát hiện. Luôn thay đổi ,phá các dữ liệu

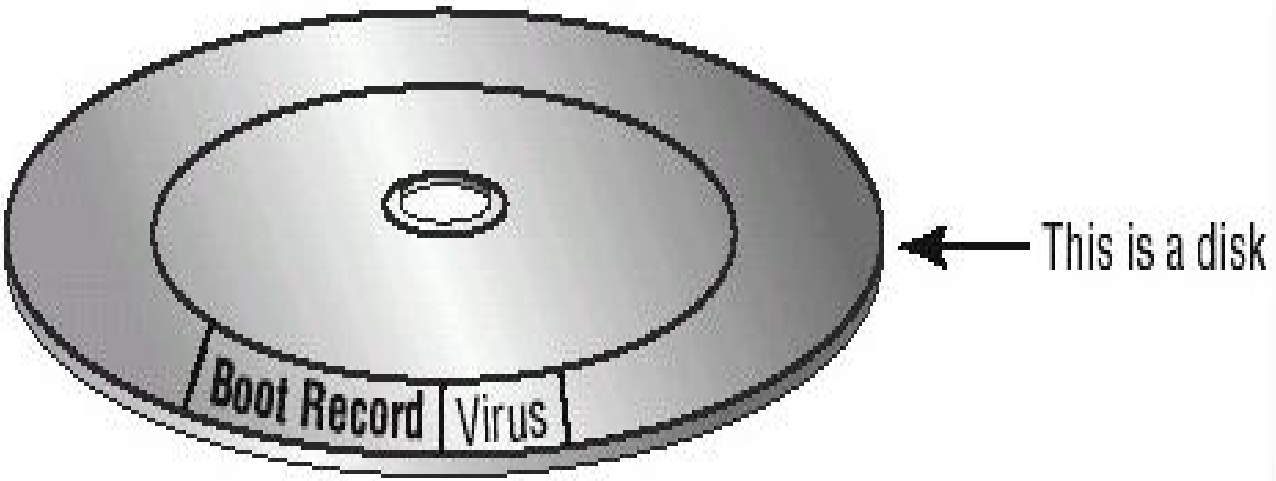


b.Trojan Horse

- Được gửi đính kèm một file nào đó
- “Trojan horse” còn là một phần của e-mail , free game, software, hoặc mộtloại file nào đó.Khi nhiễm ,“Trojan horse” sẽ kích hoạt các tác vụ như xử lý văn bản hoặc các file template . Hậu quả là nhiều file mới không cần thiết được sinh ra .
- “Trojian Horse” còn kích hoạt nhiều tác vụ theo kịch bản của hacker .
- “Trojan horse” rất khó phát hiện vì chúng được che bởi các chương trình hợp lệ .

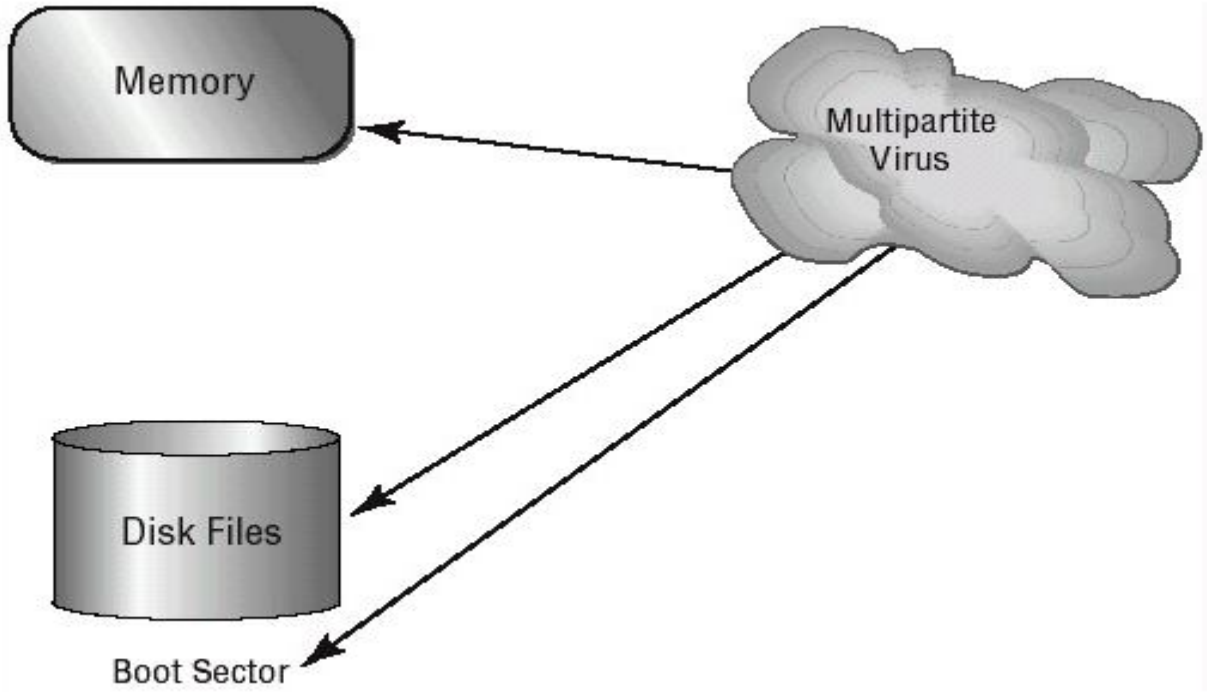
c. Stealth Virus

Stealth virus rất khó bị phát hiện do chúng có khả năng tự che dấu .Virut loại này tấn công vào các "boot sector" trên đĩa cứng.



d.Multipartite Virus

Multipartite virus tấn công vào hệ thống bằng nhiều đường .Chúng thâm nhập vào “boot sector”, các file “executable ”,và phá hoại các file ứng dụng.



e.Companion Virus

- Companion virus tự nó tấn công lên các chương trình hợp pháp và sau đó tạo ra các file có phần mở rộng khác nhau .Chúng trú ngụ tại các thư mục “temporary”.
- Khi người dùng gõ tên một chương trình hợp lệ , “companion virus” thực thi thay cho chương trình gốc . Điều này cho phép chúng tự che dấu một cách hiệu quả khỏi người dùng.

f .Macro Virus

- *Macro virus* thường tác động lên các chương trình ứng dụng .
- Các chương trình như Word , Excel cho phép lập trình viên tăng năng lực của ứng dụng .Ví dụ “Word” hỗ trợ “mini-BASIC programming language” cho phép các file được chế tác một cách tự động .
- Chúng là những “macros”. Macro có thể thông tin cho bộ xử lý văn bản “kiểm tra chính tả- spellcheck” mỗi khi chúng được mở.
- Macro viruses có thể bị nhiễm vào tất cả các văn bản và lây lan đến các hệ thống khác qua e-mail hoặc các phương thức khác.
- Macro viruse phát triển rất nhanh .

g. Phần mềm diệt Virut

- Là công cụ chủ yếu để phát hiện và diệt virut
- Khoảng 60,000 virut , worms, bombs, và các “malicious codes” được xác định.Con số này còn tiếp tục tăng nhanh.
- Biện pháp quan trọng thứ hai là đào tạo ,nâng cao nhận thức về phòng và chống virut .
- Diệt virut “on-line”
- “Trenmicro” , “synmatec” , “Kasparsky” …..

6.4.Social Engineering

- *Social engineering* là quá trình attacker thu lượm thông tin về mạng , hệ thống thông qua những nhân viên trong một tổ chức.”Social engineering” có thể xảy ra trên điện thoại , e-mail hoặc qua các khách thăm viếng.Những thông tin này có thể là thông tin truy cập như user IDs , passwords…
- Biện pháp khắc phục duy nhất : Đào tạo , nâng cao nhận thức , ý thức của nhân viên về ATTT

6.5. Các giao thức bảo mật trên mạng Internet

6.5.1 Bảo mật giao thức PPP (Layer 2)

Giao thức PPP trên layer 2 của mô hình OSI (tương ứng với lớp DATA LINK trên TCP/IP)

1. CHAP (Challenger Handshake Protocol) [RFC 1994] : Đây là cơ chế xác thực (authentication) cho giao thức PPP.CHAP dùng khóa quy ước kết hợp với hàm băm (H).

2. EAP (Extensible Authentication Protocol) [RFC2716].

3. ECP (Encryption Control Protocol) [RFC1968] [RFC2419] quản lý quá trình mã hóa dữ liệu. Sử dụng khóa bí mật và các hệ mật đối xứng (DES).

Bảo mật giao thức PPP (Layer 2) (tiếp)

4. PPTP hỗ trợ việc đóng gói dữ liệu trên môi trường point-to-point .

– PPTP đóng gói và mã hoá các gói PPP . PPTP phù hợp với giao thức mức mạng thấp (low-end protocol).

– Sự thoả thuận giữa hai phía trên kết nối PPTP rất rành mạch.Mỗi lần thoả thuận được thiết lập,kênh truyền sẽ được mã hoá → Điểm yếu của giao thức. Dùng packet-capture device, ví dụ như sniffer, có thể xác định các thông tin "tunnel đang làm việc như thế nào ?".

– PPTP sử dùng cổng 1723 và TCP để kết nối.

Bảo mật giao thức PPP (Layer 2) (tiếp)

5. L2TP

- L2TP là sự thỏa thuận giữa Microsoft và Cisco về việc kết hợp hai giao thức " tunneling " vào một : "Layer Two Tunneling Protocol (L2TP)".
- L2TP là sự lai tạp PPTP và L2F.
- L2TP cơ bản là giao thức "point-to-point"

- L2TP hỗ trợ nhiều giao thức mạng bên ngoài TCP/IP.
- L2TP làm việc trên IPX, SNA, và IP → L2TP có khả năng làm việc như cầu nối giữa các mạng khác kiểu .
- Điểm yếu của L2TP là không được hỗ trợ bảo mật , thông tin khồng được mã hoá như IPSec.
- L2TP sử dụng cổng và TCP để kết nối.

6.5.2.Tunneling Protocols

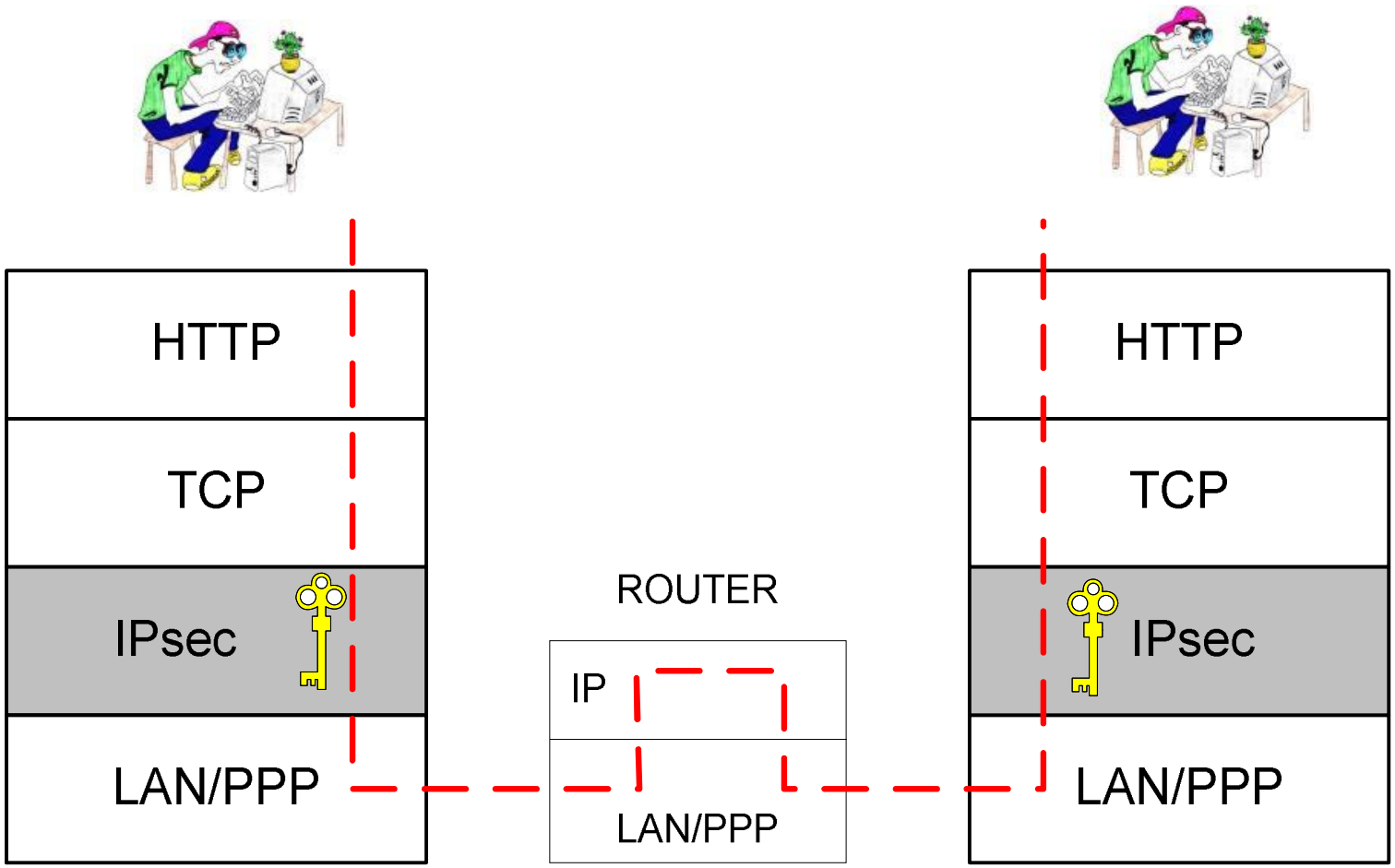
- Tunneling protocols tăng thêm năng lực của mạng. Chúng tạo ra những đường hầm " tunnels" giữa các lớp mạng và làm cho chúng an toàn hơn.Chúng cung cấp một mạng ảo giữa hai hệ thống.
- Các giao thức chính :
  - Point-to-Point Tunneling Protocol (PPTP),
  - Layer 2 Forwarding (L2F),
  - Layer 2 Tunneling Protocol (L2TP),
  - IPSec

6.5.3 IPsec (Layer 3)

6.5.3.1. Mô tả

- **IP Security (IPSec)** là một giao thức hỗ trợ thiết lập các kết nối an toàn dựa trên **IP**.
- Hoạt động ở tầng ba (**Network**)
- **IPSec** cũng là một thành phần quan trọng hỗ trợ giao thức **L2TP** trong công nghệ **VPN (Virtual Private Network).**
- Để sử dụng **IPSec cần có** các qui tắc (**rule**). Qui tắc **IPSec** là sự kết hợp giữa hai thành phần **filter** và **action.**

IPsec (Layer 3) - Mô hình



Ví dụ nội dung của một qui tắc IPSec :

"Hãy mã hóa tất cả những dữ liệu truyền Telnet từ máy có địa chỉ 192.168.0.10", nó gồm hai phần:

- Phần "lọc" là "*qui tắc này chỉ hoạt động khi có dữ liệu được truyền từ máy có địa chỉ 192.168.0.10 thông qua cổng 23*",
- Phần "action" là *"mã hóa dữ liệu"*.

6.5.3.2. Cấu trúc IPsec

Là một bộ giao thức dùng cho lớp 2 – lớp network bao gồm mã hóa dữ liệu và các thủ tục trao đổi khóa (IKE – Internet Key Exchange)

1. Mã hóa dữ liệu
    a. ESP (Encapsulated Security Payload) [RFC2406] cho phép mã hóa và đóng gói lại dữ liệu. Có hai mode làm việc
        - Transport mode
        - Tunnel mode

b. AH (Authentication Header) [RFC 2402] : tạo một bản xác thực phần “Header” sau khi packet được mã hóa , sử dụng ký thuật băm (Hash).

2. IKE Quy định các thủ tục trao đổi , quản lý khóa mã ví dụ như SKIP , Kerberos…

- IPSec hỗ trợ bốn loại tác động (action) bảo mật :

  - *Block transmissons:* ngăn chận những gói dữ liệu được truyền, IPSec ngăn chận dữ liệu truyền từ máy A đến máy B.

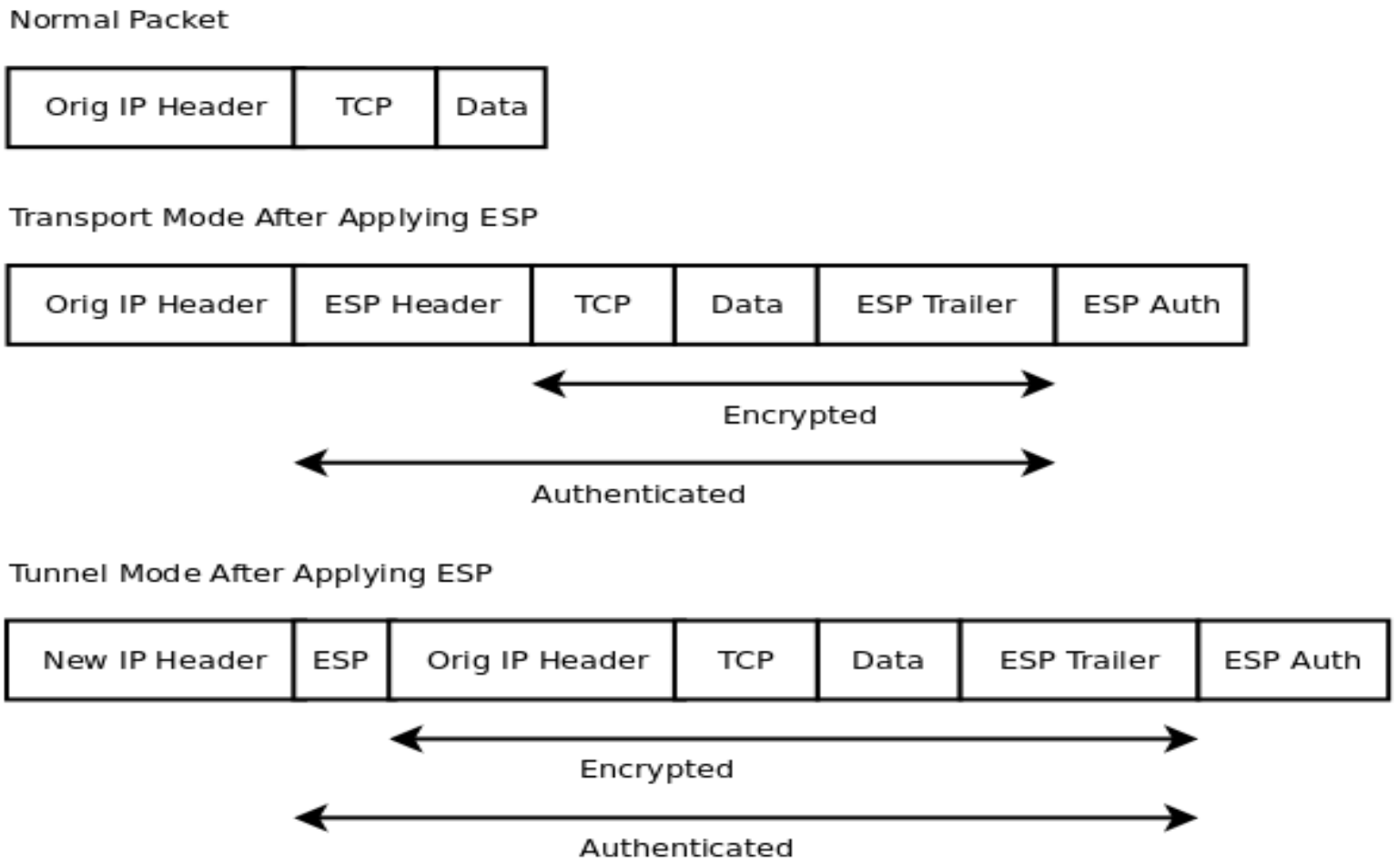
  - *Encrypt transmissions*: mã hóa những gói dữ liệu được truyền, sử dụng giao thức ESP (encapsulating security payload) để mã hóa dữ liệu cần truyền. .

  - *Sign transmissions*: tạo chữ ký số cho các gói dữ liệu , nhằm tránh những kẻ tấn công trên mạng giả mạo , (man-in-the-middle). Sử dụng giao thức authentication header.

  - *Permit transmissions*:cho phép dữ liệu được truyền qua.

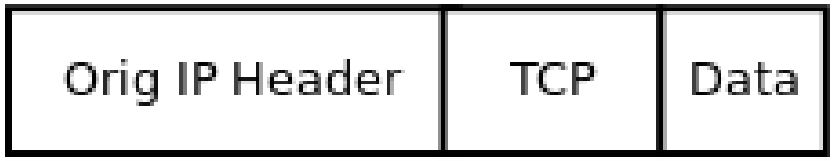
- Những actions này dùng để tạo ra các qui tắc (**rules**) hạn chế một số điều và cho phép làm một số điều khác. Ví dụ một qui tắc dạng này *“Hãy ngăn chặn tất cả những dữ liệu truyền tới, chỉ trừ dữ liệu truyền trên các cổng 80 và 443”.*

6.5.3.3 Các mode làm việc của IPsec
1. RFC-2406 ESP (Encapsulated Security Payload)

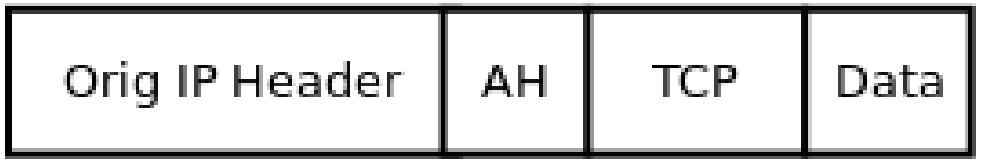


2. RFC 2402- Authentication Header

Normal Packet



Transport Mode After Applying AH



Tunnel Mode After Applying AH

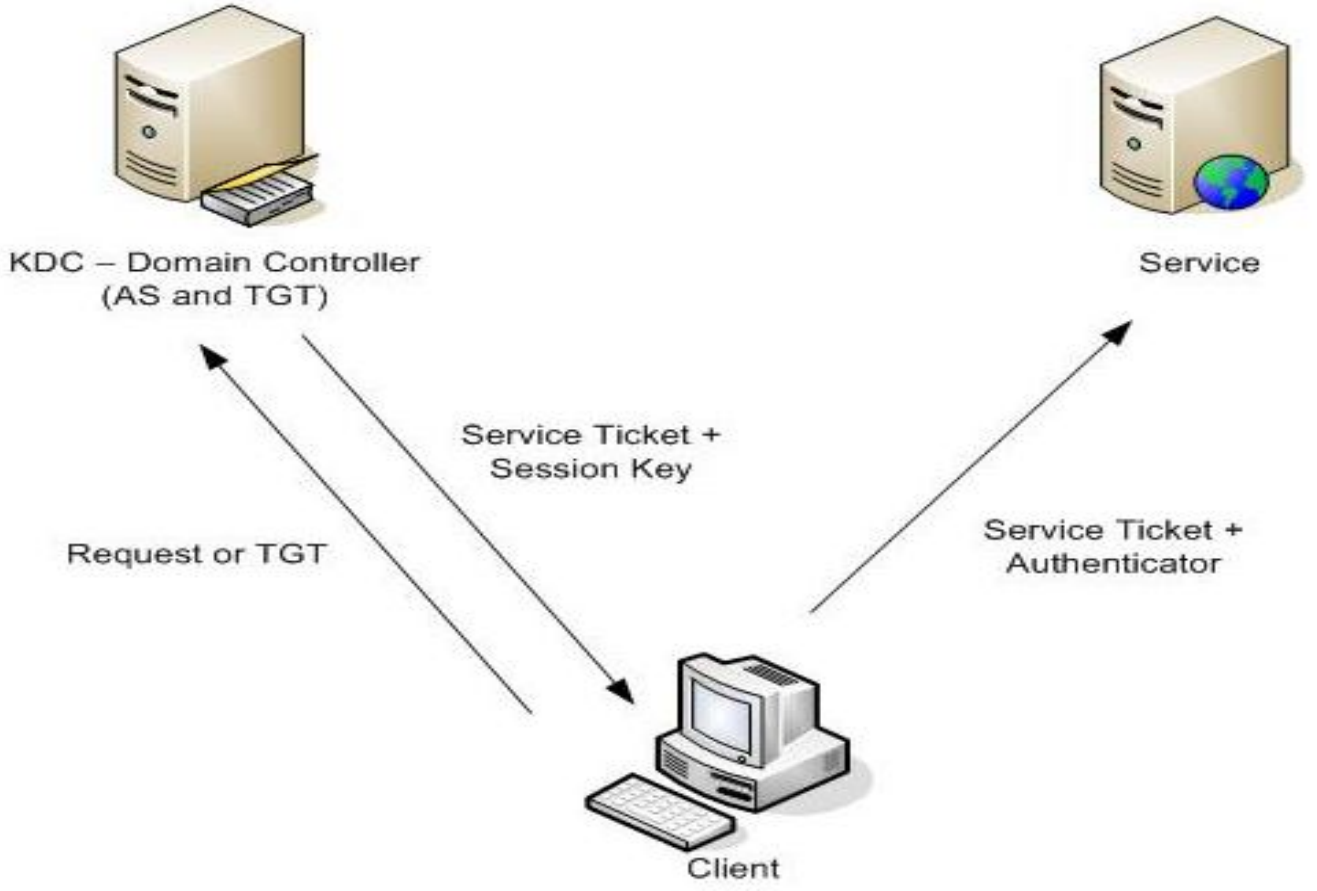
- Đối với hai tác động bảo mật theo phương pháp chứng thực và mã hóa thì hệ thống sẽ yêu cầu **IPSec** dùng phương pháp chứng thực được chọn.
- **Microsoft** hỗ trợ ba phương pháp chứng thực:
  - ✓ **Kerberos**,
  - ✓ Chứng chỉ (**certificate**)
  - ✓ Một khóa dựa trên sự thỏa thuận (**agreed-upon key**).

Phương pháp **Kerberos** chỉ áp dụng được giữa các máy trong cùng một miền **Active Directory** hoặc trong những miền **Active Directory** có ủy quyền cho nhau.

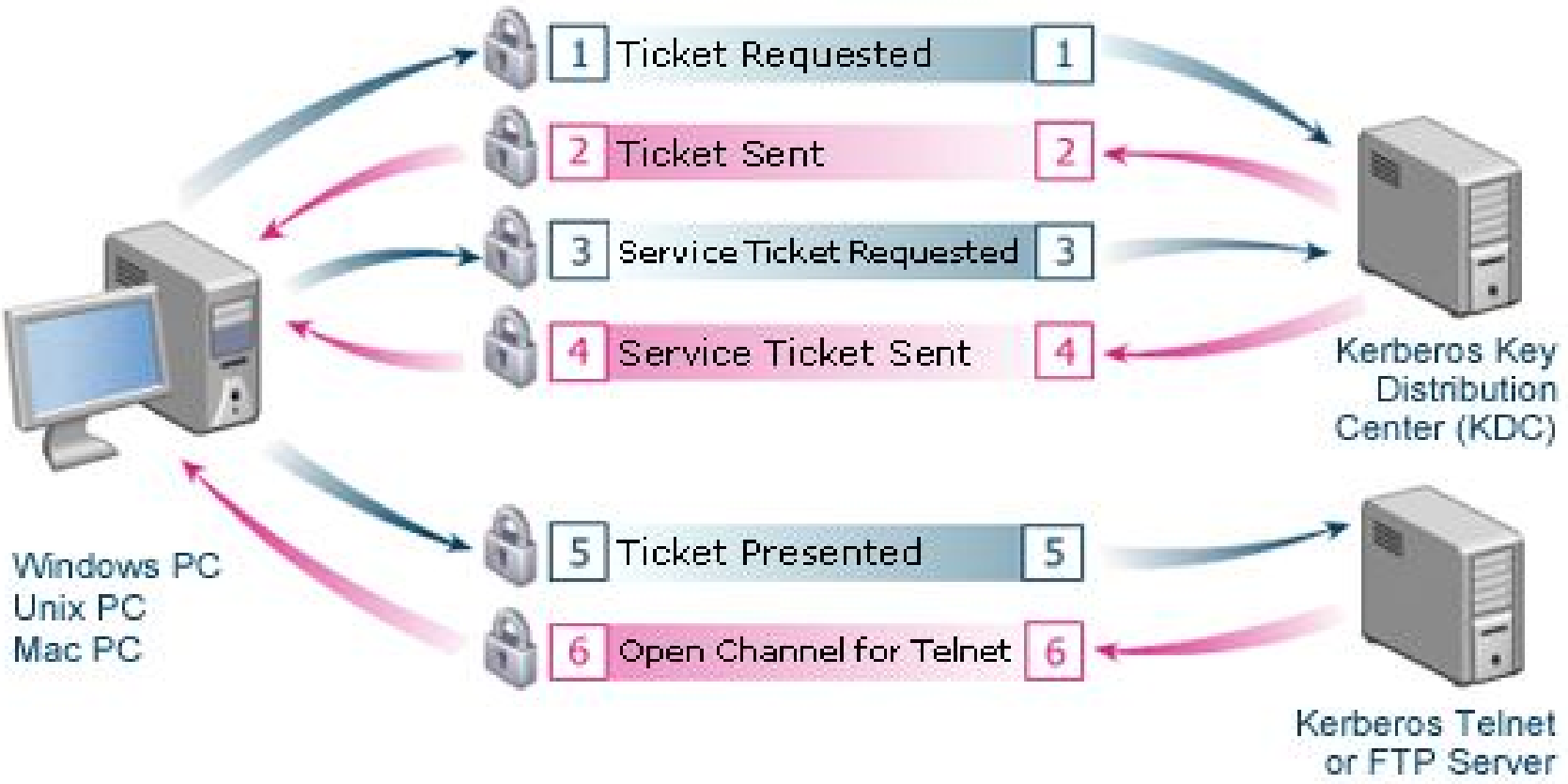
- Phương pháp dùng các chứng chỉ cho phép sử dụng các chứng chỉ **PKI** (**public key infrastructure**) để nhận diện một máy.
- Phương pháp dùng chìa khóa chia sẻ trước (Preshare key) cho phép dùng một chuỗi ký tự văn bản thông thường làm chìa khóa (**key**).

IKE Quy định các thủ tục trao đổi , quản lý khóa mã

Kerberos model



Phân phối khóa theo Kerberos



6.5.3.4.Các bộ lọc IPSec

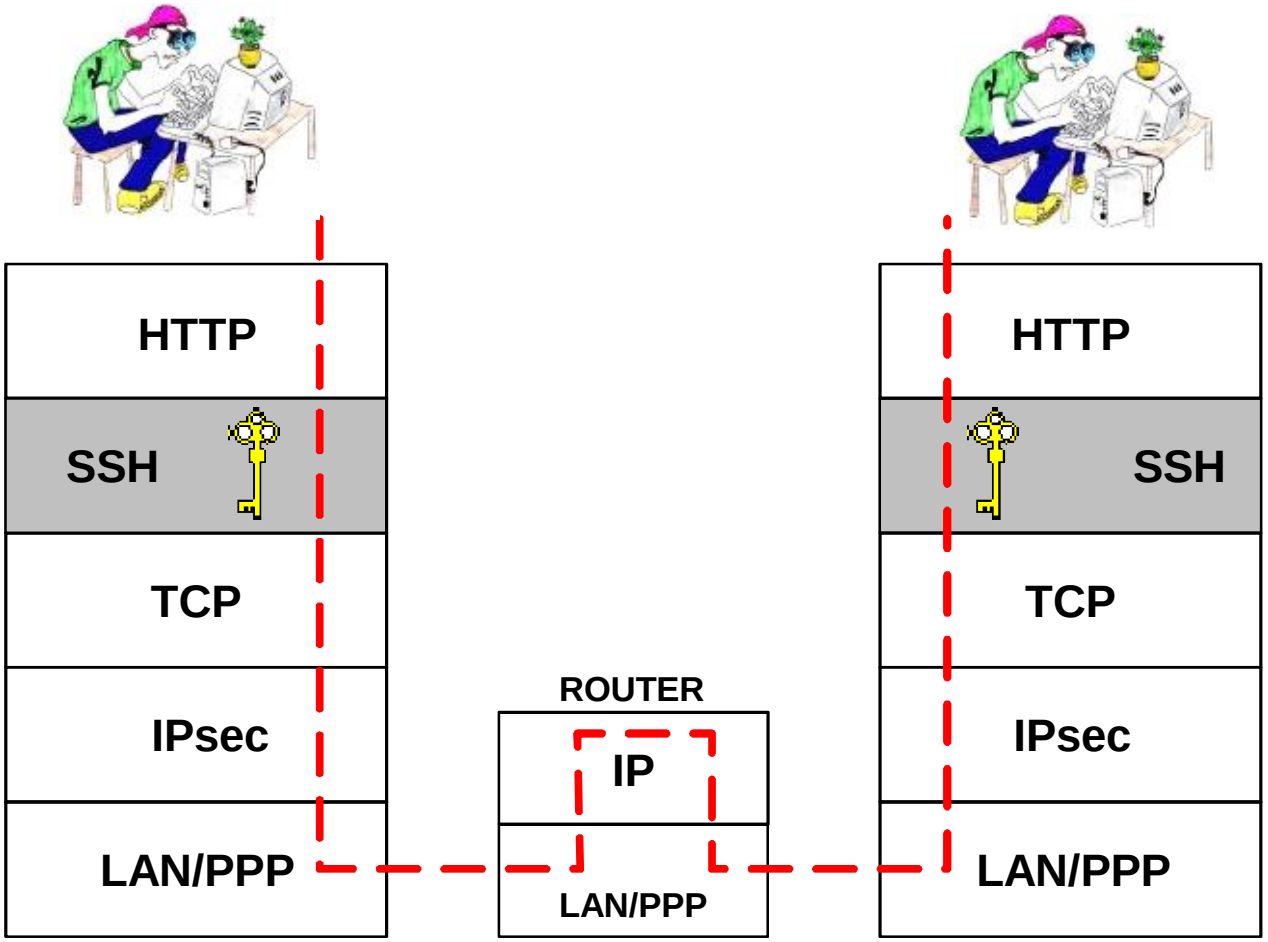
Bộ lọc (**filter**) giúp **IPSec** hoạt động linh hoạt hơn . Bộ lọc có tác dụng thống kê các điều kiện để qui tắc hoạt động. Đồng thời chúng cũng giới hạn tầm tác dụng của các tác động bảo mật trên một phạm vị máy tính nào đó hay một số dịch vụ nào đó. Bộ lọc **IPSec** chủ yếu dự trên các yếu tố sau:

- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy nguồn.
- Địa chỉ **IP**, subnet hoặc tên **DNS** của máy đích.
- Theo số hiệu cổng (**port**) và kiển cổng (**TCP, UDP, ICMP**…)

6.5.4 Secure Shell (SSH) (Layer 4)

- Secure Shell (SSH) là "tunneling protocol" thiết kế riêng cho hệ UNIX .
- SSH sử dụng mật mã để thiết lập kết nối an toàn giữa hai hệ thống.
- SSH cung cấp các chương trình an toàn tương ứng cho Telnet, FTP, và các chương trình "communications-oriented" trên UNIX.
- SSH hiện nay được sử dụng rông rãi trên Windows cho Telnet và các " cleartext-oriented programs" trên môi trường UNIX.
- SSH sử dụng cổng 22 và TCP để kết nối.

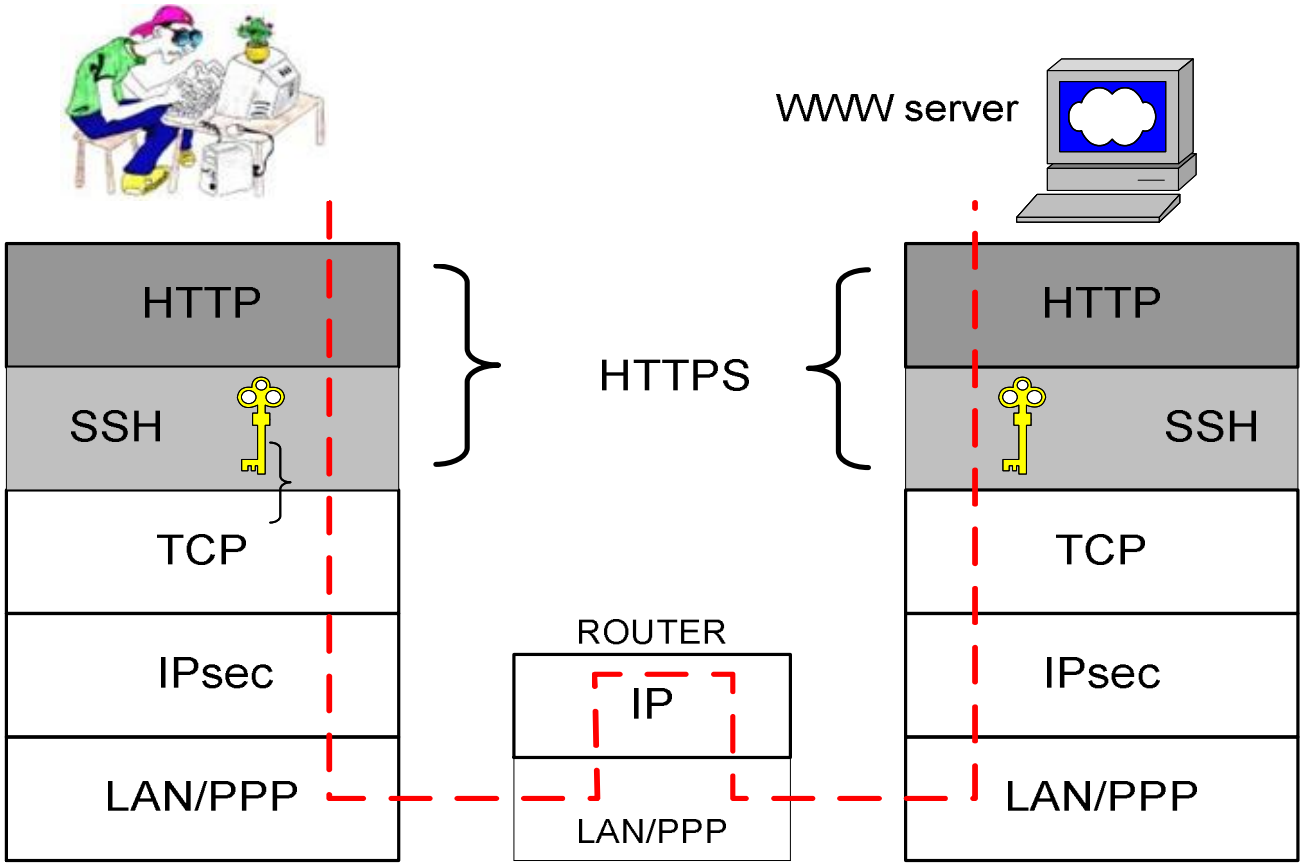
Secure Shell (SSH) (Layer 4)



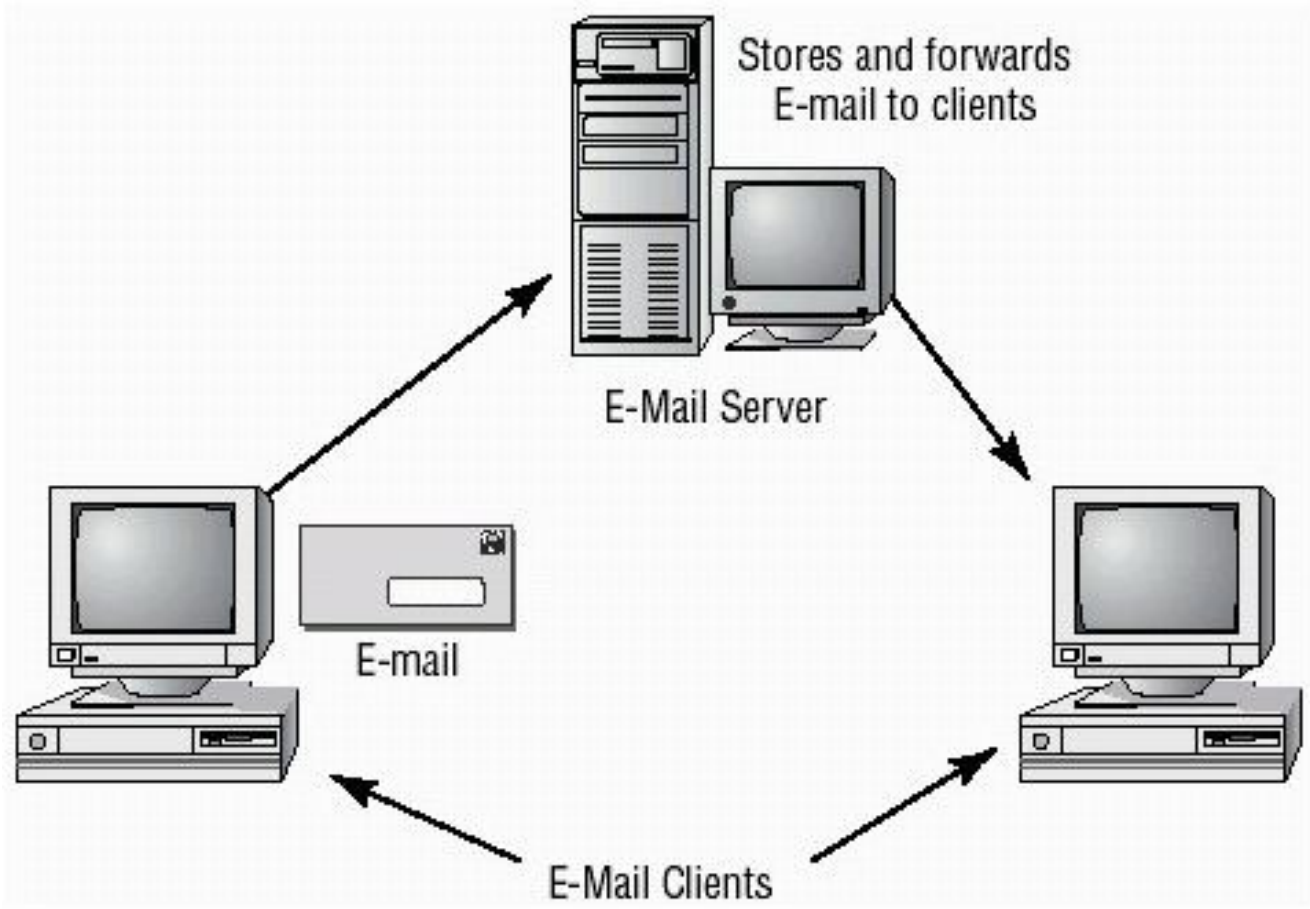
6.5.5. HTTP/S – on top of SSH (Layer 4 ,5)

- **HTTP/S** -HTTP Secure *(RFC 2818)* là giao thức bảo mật kết nối giữa hai hệ thống dùng WEB . HTTP/S bảo vệ kết nối giữa hai hệ thống WEB .Tất cả thông tin giữa hai hệ thống được mã hoá. HTTP/S sử dụng SSL hoặc TLS để kết nối an toàn . HTTP/S sử dụng cổng port 443 và TCP.
- **SSL/TLS** Secure Socket Layer (SSL) và Transport Layer Security (TLS) *(RFC 2246)* sử dụng để truyền thông tin giữa " web client" và " server". SSL sử dụng hệ thống mật mã giữa hai hệ thống.TLS là giao thức mới hơn với mật mã mạnh hơn như "Triple DES". SSL/TLS làm việc trên cổng 443 và kết nối bằng TCP.

HTTPS – on top of SSH



6.5.6 Bảo mật E-Mail (Layer 5)



1. Các giao thức

a.Simple Mail Transport Protocol (SMTP)

b. Post Office Protocol (POP)

c.Internet Message Access Protocol (IMAP)

d.S/MIME [RFC2632 ,2633,2634] của "RSA" .Sử dụng 3-DES để mã hóa dữ liệu kết hợp với DSA và SHA1.

e. PGP

2. Các điểm yếu trên E-Mail

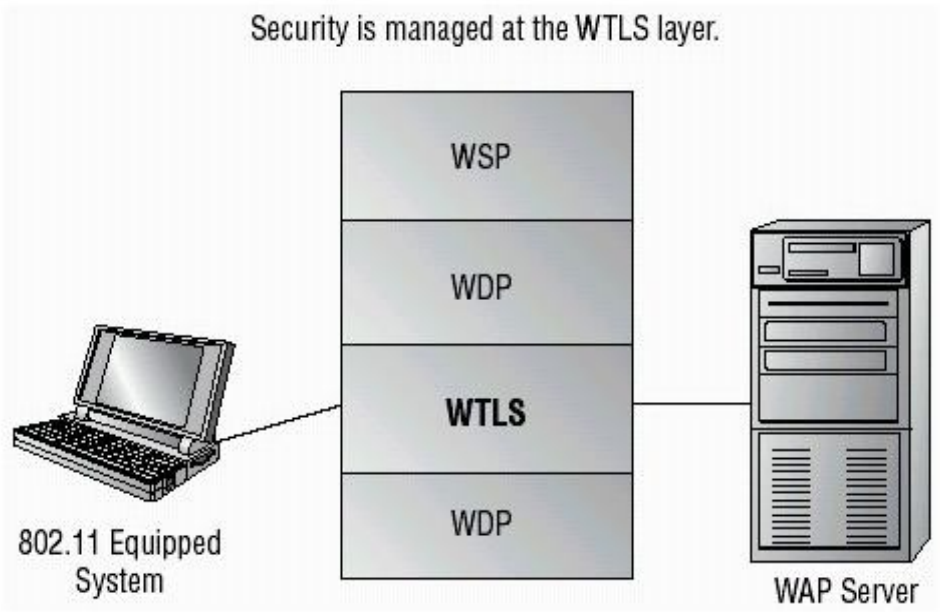
- Spam
- Hoaxes

6.6. Bảo mật Wireless network

6.6.1 Wireless Applications Protocol (WAP).

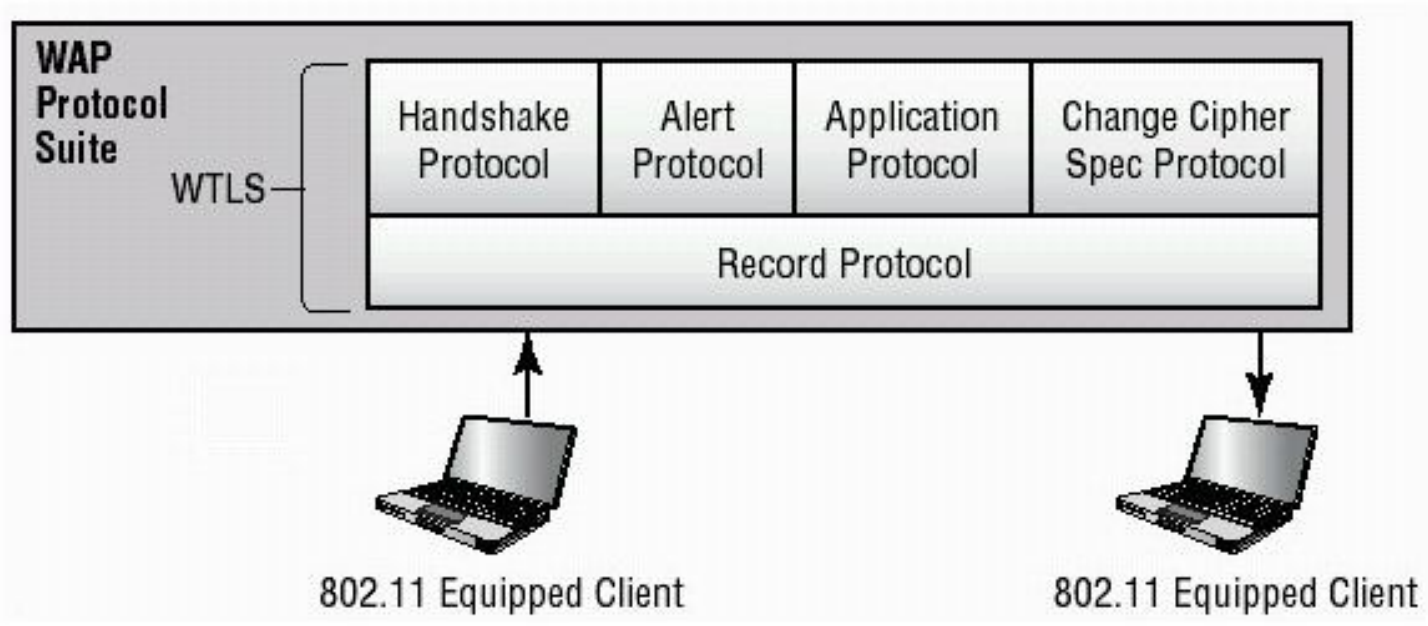
Có ba mức an toàn cho giao thức này :

- Anonymous authentication
- Server authentication
- Two-way (client and server) authentication . Yêu cầu cả hai bên “client và server” xác thực .



6.6.2 Wireless Transport Layer Security (WTLS)

- Là mức bảo mật của Wireless Applications Protocol.
- WTLS cung cấp dịch vụ “authentication”, “encryption”, và “data integrity” cho các thiết bị không dây.
- WTLS là một phần của môi trường WAP .

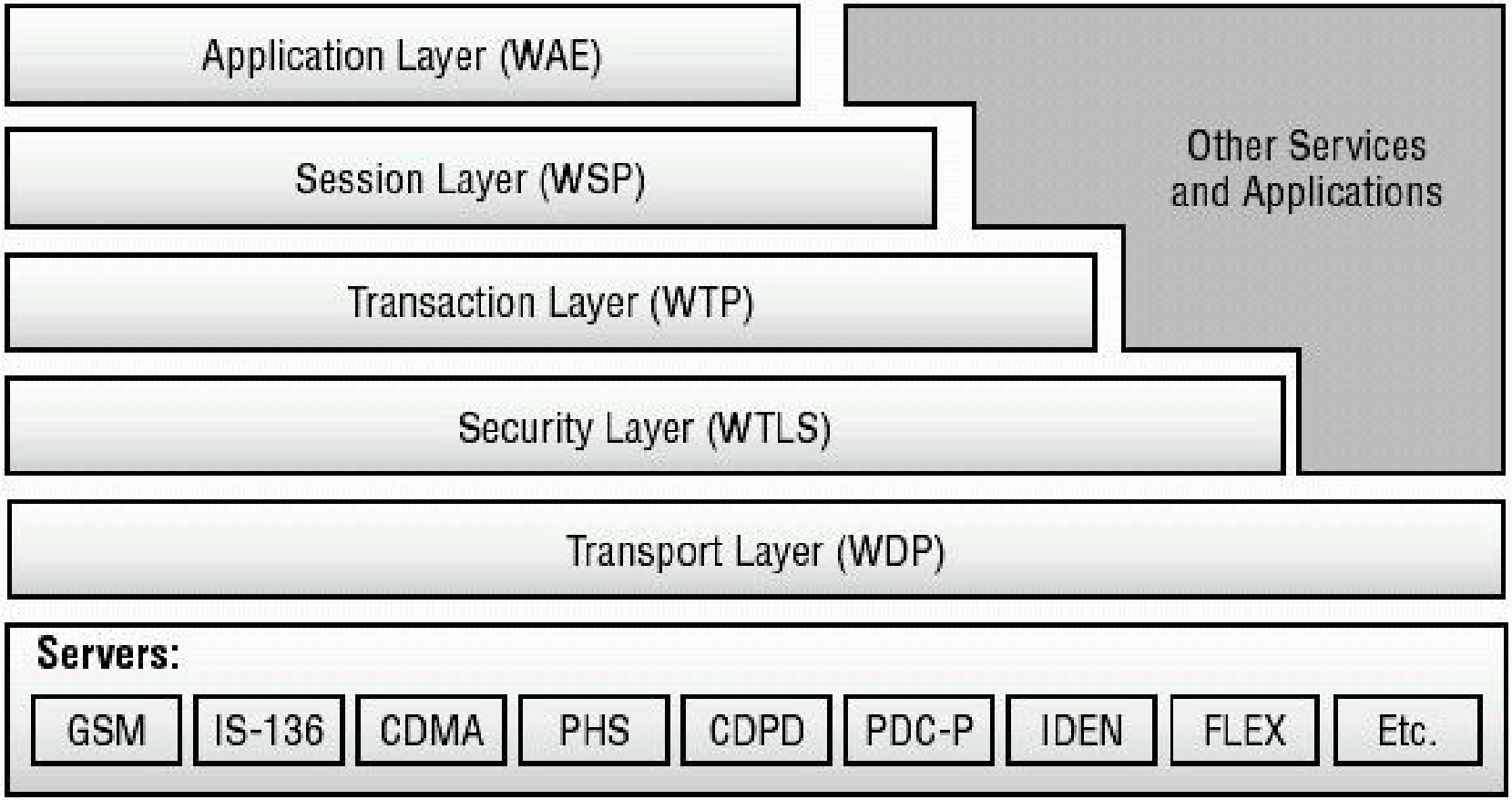


6.6.3 WEP/WAP

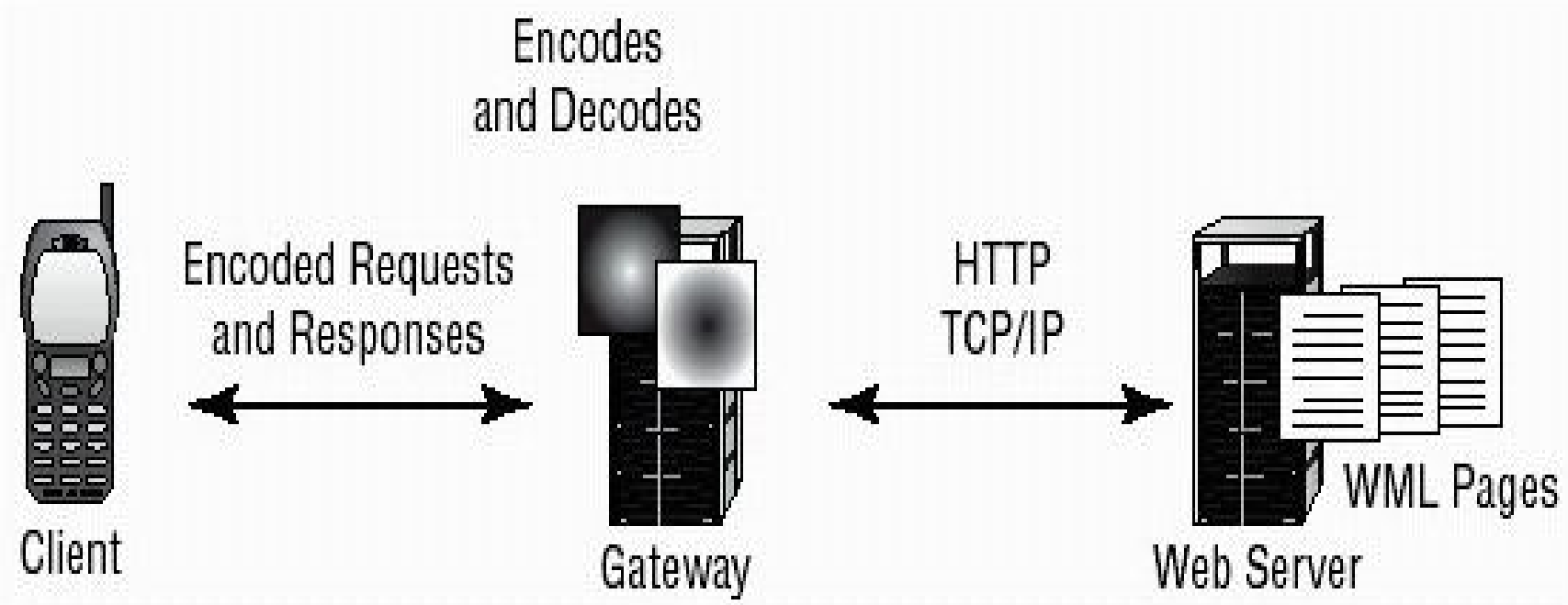
6.6.3.1. WAP :The Wireless Access Protocol (WAP)

- WAP hoạt động tương tự như TCP/IP functions.
- WAP sử dụng phiên bản rút gọn của HTML-*Wireless Markup Language (WML)*,dùng để hiển thị trên Internet .
- WAP- tương tác với môi trường *WMLScript tương tự như* Java .. Notice that the layers of WAP appear to resemble the layering in TCP/IP.

WAP protocol stack



WAP gateway cho phép kết nối đến các thiết bị WAP trên Internet



6.6.3.2. Wired Equivalent Privacy (WEP)

- Là chuẩn security mới cho các thiết bị wireless .
- WEP mã hoá dữ liệu → data security.
- Sử dụng khoá mật mã : 40 (không còn sử dụng) ,64,128 bit key .
- 128 bit kết hợp với lọc địa chỉ MAC → hiệu quả cao
- Từ 8 / 2002 , giao thức không được coi là an toàn do có những điểm yếu trong các thuật toán mã hoá (đặc biệt 40 bit) . Mã hoá có thể bị hack trong vòng 5 giờ.

6.6.4 Các điểm yếu trên Wireless

- ***Bảo mật:*** Đây có thể nói là nhược điểm lớn nhất của mạng WLAN → Truyền sóng vô tuyến
- ***Phạm vi:*** Chuẩn IEEE 802.11n mới nhất hiện → hoạt động ở phạm vi tối đa là 150m, chỉ phù hợp cho một không gian hẹp.
- ***Độ tin cậy:*** Do phương tiện truyền tín hiệu là sóng vô tuyến nên việc bị nhiễu, suy giảm…là điều không thể tránh khỏi. Điều này gây ảnh hưởng đến hiệu quả hoạt động của mạng.
- ***Tốc độ:*** Tốc độ cao nhất hiện nay của WLAN có thể lên đến 600Mbps nhưng vẫn chậm hơn rất nhiều so với các mạng cáp thông thường (có thể lên đến hàng Gbps)

6.6.4. Các điểm yếu trên Wireless(tiếp)

- Tất cả tín hiệu “radio frequency” đễ dàng bị thu lại.
- Để bắt được thông tin theo 802.11 ,chỉ cần một PC với card 802.11 tương thích.
- Một phần mềm đơn giản trên PC có thể giữ lại thông tin trên WAP và sau đó xử lý chúng nhằm giải mã tài khoản và mật khẩu .

6.7. Các hình thức tấn công WLAN

- Rogue Access Point (Giả mạo AP)
- De-authentication Flood Attack (Y/c xác thực lại)
- Fake Access Point
- Tấn công dựa trên sự cảm nhận lớp vật lý
- Disassociation Flood Attack

6.7.1. Rogue Access Point (Giả mạo AP)

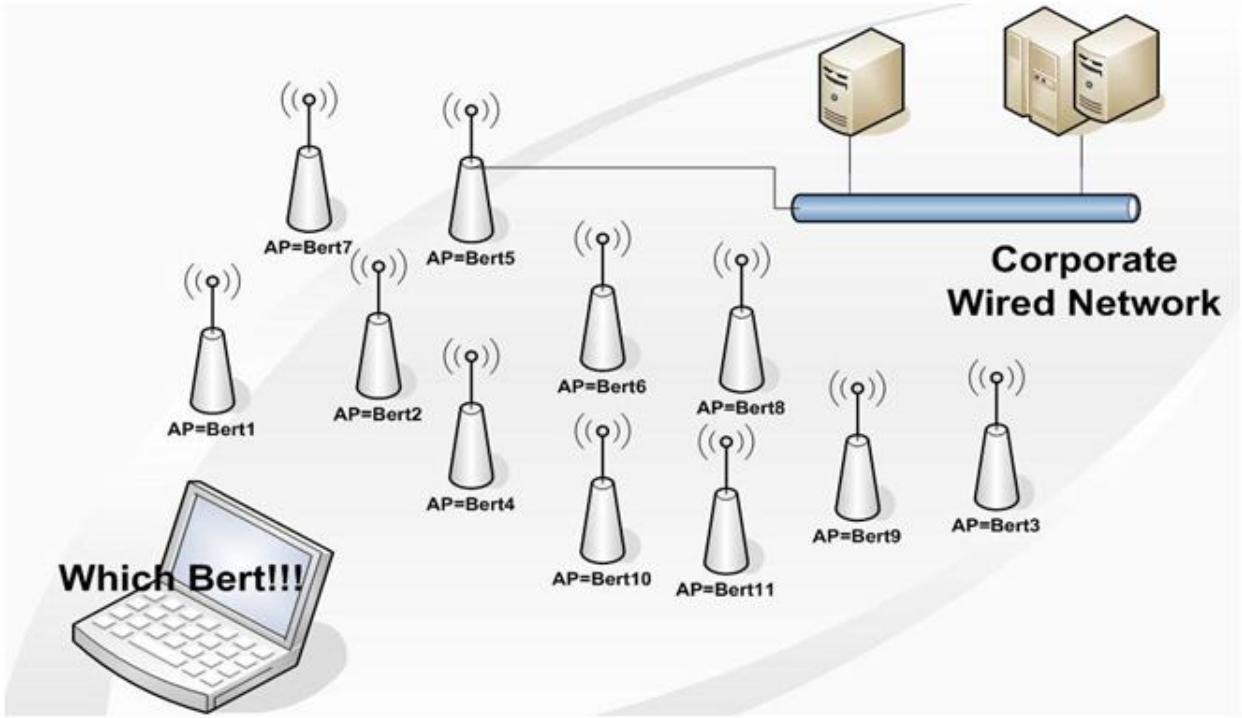
- Access Point được cấu hình không hoàn chỉnh do sai sót trong việc cấu hình
- Access Point giả mạo từ các mạng WLAN lân cận
- Access Point giả mạo do kẻ tấn công tạo ra .Đây là kiểu tấn công *"man in the middle"* cổ điển. Kiểu tấn công này rất hiệu quả so với mạng có dây.
- Access Point giả mạo được thiết lập bởi chính nhân viên của công ty -một số nhân viên của công ty đã tự trang bị Access Point và kết nối chúng vào mạng có dây của công ty

6.7.2. De-authentication Flood Attack (Y/c xác thực lại)

- Xác định mục tiêu tấn công trong mạng wireless và các kết nối của họ.
- Chèn **các frame yêu cầu xác thực lại** bằng cách giả mạo địa chỉ MAC nguồn và đích của Access Point và người dùng.
- User khi nhận được frame “yêu cầu xác thực lại” thì nghĩ rằng chúng do Access Point gửi đến.
- Sau khi ngắt được một người dùng ra khỏi dịch vụ , kẻ tấn công tiếp tục đối với các người dùng còn lại.
- Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công đã nhanh chóng tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng.

6.7.3. Fake Access Point

Sử dụng công cụ có khả năng gửi các gói beacon với địa chỉ vật lý (MAC) giả mạo và SSID giả để tạo ra vô số Access Point giả lập. Làm xáo trộn tất cả các phần mềm điều khiển card mạng không dây của người dùng.



6.7.4. TẤN CÔNG DỰA TRÊN GIAO THỨC CSMA/CD LỚP MAC

- Kẻ tất công lợi dụng giao thức CSMA/CD. Các máy tính khác luôn luôn ở trạng thái chờ đợi việc truyền dữ liệu kết thúc → nghẽn mạng.
- CSMA - Cảm nhận sóng mang
  - ✓Carrier Sense (CS) : Gửi các DATA FRAME khi kênh truyền rảnh
  - ✓Multiple Access (MA) : Nhiều trạm cùng truy nhập trên một kênh truyền
- Tần số sóng mang (CS) là một nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm phụ thuộc vào giao diện của lớp vật lý

6.7.5.TẤN CÔNG NGẮT KẾT NỐI

- Kẻ tấn công xác định mục tiêu (wireless clients) và mối liên kết giữa AP với các clients.
- Kẻ tấn công gửi **disassociation frame** bằng cách giả mạo Source và Destination MAC đến AP và các client tương ứng.
- Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gởi disassociation frame đến AP.
- Sau khi ngắt kết nối của một client, hacker tiếp tục thực hiện tương tự với các client còn lại làm cho các client tự động ngắt kết nối với AP.
- Khi các clients bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức. Kẻ tấn công tiếp tục gởi DSF đến AP và clients.

- So sánh Disassociation flood attack và De-authentication Flood Attack.
  - Giống nhau : Về hình thức tấn ,vừa tấn công Access Point vừa tấn công Clients. Và trên hết, chúng “tấn công" liên tục.
  - Khác nhau:
    - De-authentication Flood Attack: Yêu cầu cả AP và client gởi lại frame xác thực → xác thực failed.
    - Disassociation flood attack : Gởi disassociation frame làm cho AP và client tin tưởng rằng kết nối giữa chúng đã bị ngắt.

6.7.6. Các biện pháp an toàn trên WIRELESS

Để bảo mật mạng WLAN, ta cần thực hiện các bước:
Authentication → Encryption → IDS & IPS.

- Chỉ có những người dùng được xác thực mới có khả năng truy cập vào mạng thông qua các Access Point.
- Xác thực và bảo mật dữ liệu bằng cách mã hoá thông tin truyền trên mạng.
- Cảnh báo nguy cơ bảo mật bằng hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System).

6.8.1 Sử dụng các giao thức bảo mật trên wireless

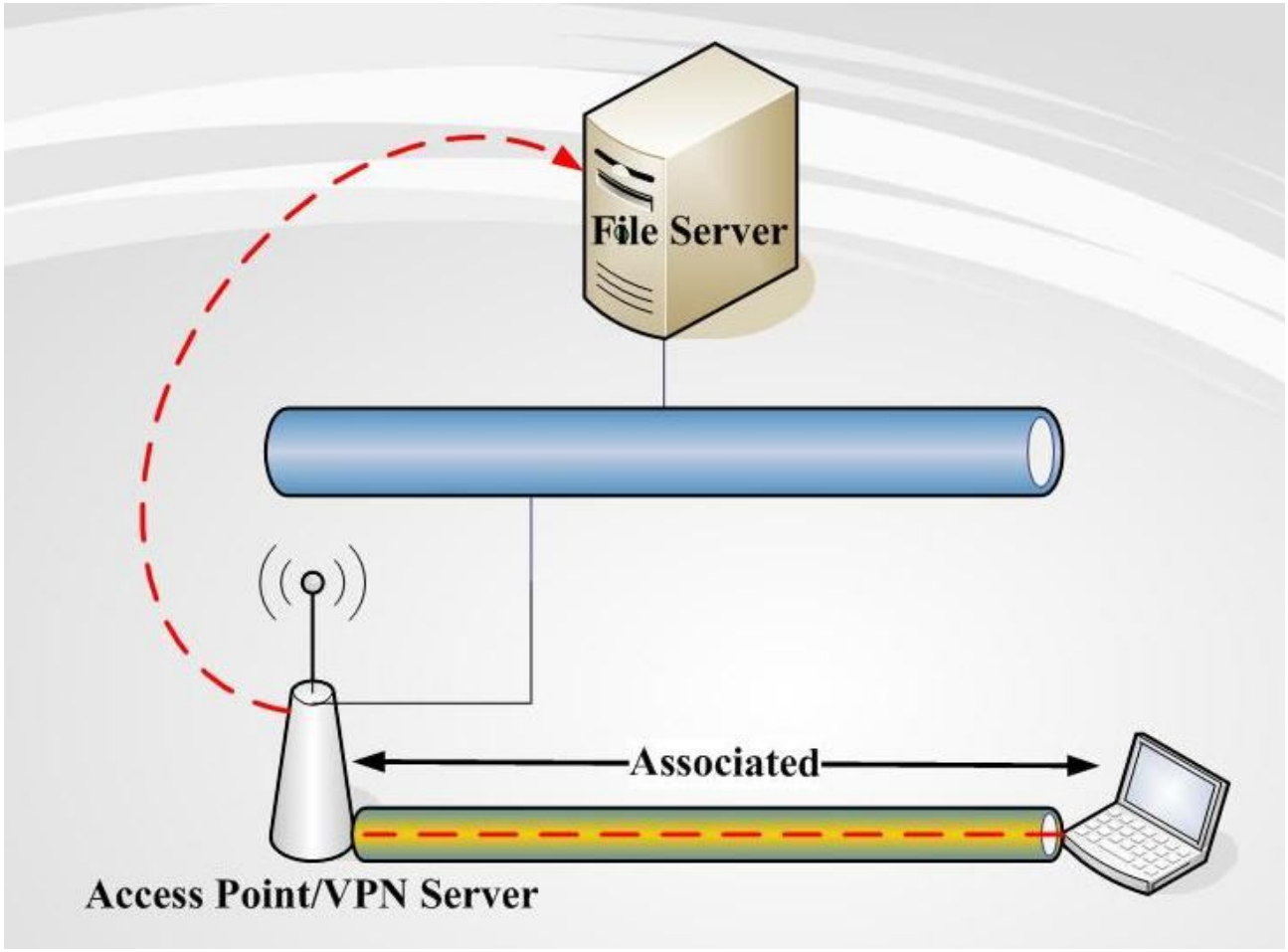
1.WEP (Wired Equivalent Privacy)

WEP sử dụng *một khoá không thay* đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit. →Khóa yếu → Dễ bị bẻ bằng " brute force" hoặc "trial-and-error".

2. WLAN VPN tạo một một kênh tin cậy cao

VPN sử dụng giao thức IPSec . IPSec dùng các thuật toán mạnh như DES và Triple DES (3DES) để mã hóa dữ liệu và dùng các thuật toán khác để xác thực gói dữ liệu (Public Key).

Mô hình WIRELESS VLAN



3. TKIP (TEMPORAL KEY INTEGRITY PROTOCOL)

- Là giải pháp của IEEE được phát triển năm 2004.
- Là một nâng cấp cho WEP nhằm vá những lỗi bảo mật trong cài đặt mã dòng RC4 trong WEP.
- TKIP dùng hàm băm (hashing) IV để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) và đảm bảo tính chính xác của gói tin.
- TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

3. Sử dụng **AES** : đây là một chuẩn mật mã đối xứng thay thế cho DES
4. 802.1X VÀ EAP

   802.1x là chuẩn đặc tả "port-based" được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây.
5. **WPA (WI-FI PROTECTED ACCESS)**

   Công nghệ WPA (Wi-Fi Protected Access) ra đời, nhằm khắc phục các nhược điểm của WEP

6. LỌC (FILTERING)

Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan:

- Lọc SSID
- Lọc địa chỉ MAC
- Lọc giao thức

Kết thúc CH4 bạn phải nắm vững

- Cấu trúc TCP/IP
- Các điểm yếu và các dạng tấn công :
- Attack methods
- Malicious code
- Social engineering
- Các chuẩn và các giao thức bảo mật

HẾT CHƯƠNG 4