Chương 2

An toàn cho các thiết bị mạng

- Các điểm truy nhập trên tầng 1
- Các điểm truy nhập trên tầng 2
- Các điểm truy nhập trên tầng 3
- Các điểm truy nhập trên tầng 4 trở lên

Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về cách thức để đảm bảo an toàn cho các thiết bị mạng hoạt động trên các tầng khác nhau của mô hình OSI.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Xác định được các điểm truy nhập của hệ thống mạng.
  - Hiểu được các điểm yếu của đường truyền mạng.
  - Mô tả được các điểm yếu của switch, bridge và access point;
  - Trình bày được các điểm yếu của router, Server truy cập từ xa và tường lửa trên tầng 3.
  - Phân biệt được các điểm yếu của proxy server, máy trạm, máy chủ và thiết bị lưu trữ ngoài.
  - Trình bày được những cách thức để bảo vệ được các thiết bị trên.

Phần 1

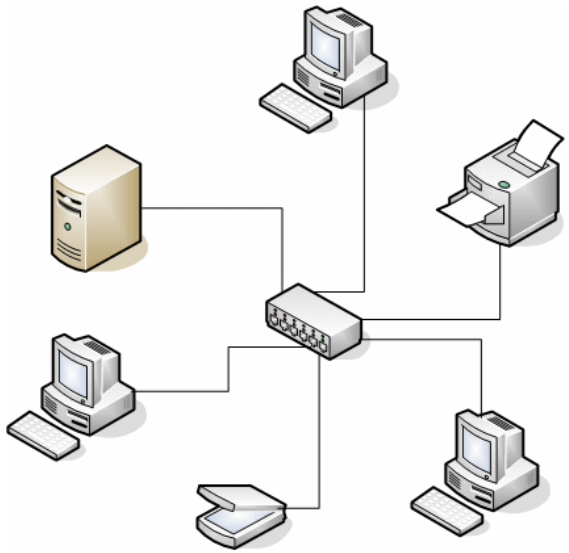
Các điểm truy cập trên tầng 1

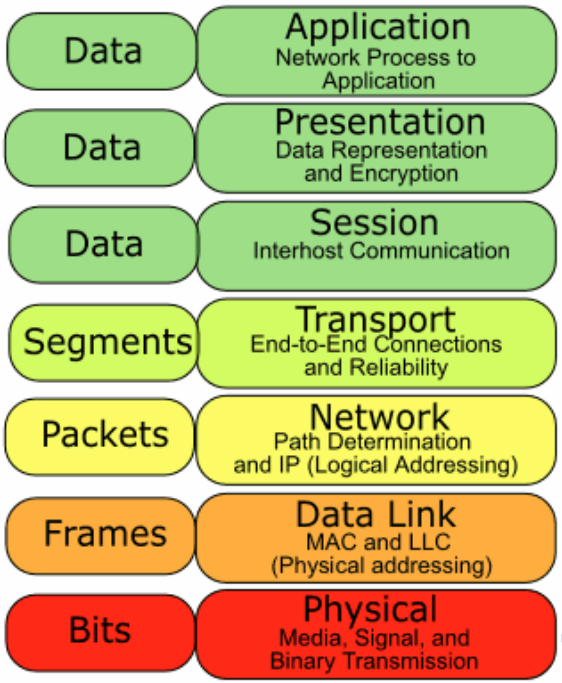
- Khái niệm
- Cáp đồng: cáp đồng trục, cáp xoắn
- Cáp quang
- Mạng không dây
- Modem

Các điểm truy cập trên tầng 1

- Khái niệm

Các điểm truy nhập (access points) là nơi người dùng hợp lệ và cả không hợp lệ truy cập vào mạng để truy xuất các tài nguyên trên mạng.





Những vấn đề an toàn trên tầng vật lý:
- Các loại cáp
- Mạng không dây
- Modem

Các điểm truy cập trên tầng 1

- Cáp đồng trục

Cách 1
Gắn trực tiếp 1 **T-connector** vào đâu đó trên cáp, sau đó đặt thiết bị nghe lén vào

Dễ bị phát hiện vì khi lắp thiết bị sẽ làm gián đoạn hoạt động của mạng

Cách 2
Dùng vòi quỉ (**vampire tab**) gắn trực tiếp vào đường cáp, xuyên qua các vỏ bọc và tiếp xúc đến đường trục chính của cáp

Khó phát hiện nhưng vẫn có thể dò tìm ra

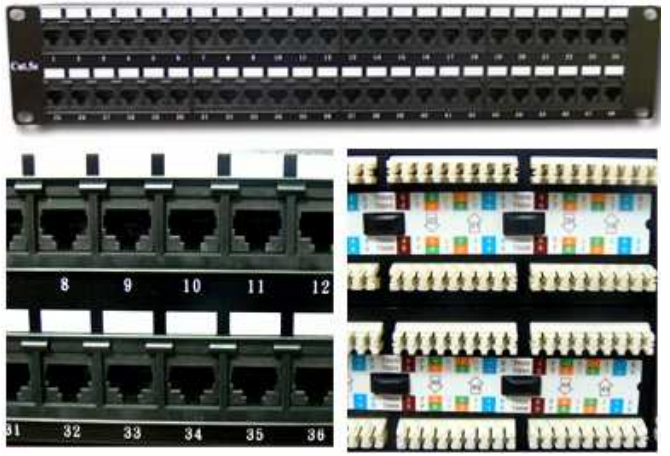
Cách 3
Dùng 1 **thiết bị cảm ứng** bao xung quanh đường cáp, thu nhận và khuyếch đại các tín hiệu ít ỏi nhận được khi tín hiệu di chuyển bên trong.

Không phát hiện được

Cách bảo vệ
- Cô lập đường cáp
- Không cho tiếp xúc trực tiếp với cáp.

Các điểm truy cập trên tầng 1

- Cáp xoắn đôi (UTP – STP)

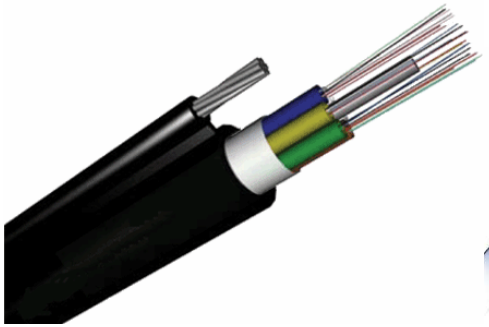


Cách thâm nhập vào cũng chỉ là gắn trực tiếp vào các switch hoặc qua các patch-panel

Cô lập các đường kết nối chính đến hệ thống cáp:
- Tách riêng các switch trung tâm vào phòng quản trị mạng
- Gắn các tủ có khóa để bảo vệ các switch và các patch-panel

Các điểm truy cập trên tầng 1

- Cáp quang



Khó bị xâm nhập bằng cách gắn trộm các thiết bị nghe lén trực tiếp vào đường cáp.

• Điểm yếu của hệ thống cáp quang là các đầu nối (connector)
• Có thể chèn vào mối nối 1 bộ chia (splitter) và nghe lén các tín hiệu tại đây.

Vì phải đi kèm với các bộ thu phát tín hiệu nên dễ dàng bị để phát hiện

Các điểm truy cập trên tầng 1

- Mạng không dây – Hồng ngoại

Giới hạn của hồng ngoại chính là bắt buộc 2 thiết bị phải "nhìn thấy nhau" (line of sigh) và khoảng cách giữa 2 thiết bị cũng phải gần nhau

xâm nhập hay nghe lén sẽ rất khó khăn

Các điểm truy cập trên tầng 1

- Mạng không dây – Sóng radio

• Wireless LAN hiện đang được dùng rộng rãi trong cuộc sống.

• Mạng không dây dùng sóng radio (RF) này **rất không an toàn** vì trong phạm vi phủ sóng, ai cũng có thể nhận được tín hiệu.

Cài đặt cơ chế bảo mật cho mạng không dây:

• Cài khóa (key) theo 2 cách chính là WEP và WPA để mã hóa dữ liệu.

Các điểm truy cập trên tầng 1

- Modem

Các hệ thống phục vụ cho kết nối bằng Modem (RAS – Remote Acces Service) thông thường được cấu hình khá an toàn

Nguy cơ: lắp Modem vào 1 hệ thống máy tính đặt tại cơ quan. Dùng 1 chương trình gọi là War Dialer để kết nối (gọi đến) Modem này và xâm nhập vào máy tính đang gắn trực tiếp vào Modem.

- Giới hạn sử dụng Modem
- Cấu hình Modem chỉ cho phép hướng gọi đi

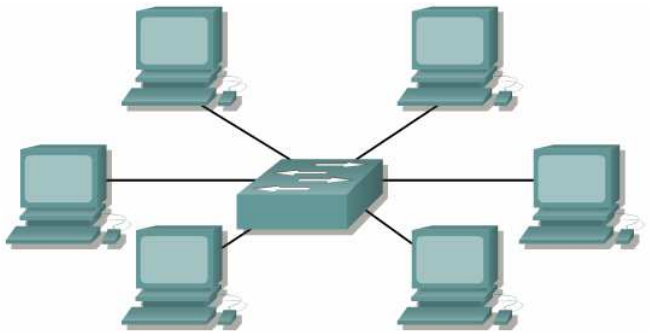
Phần 2

Các điểm truy cập trên tầng 2

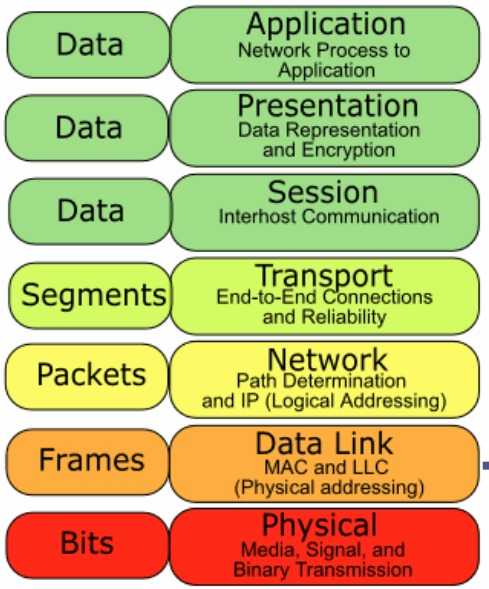
- Khái niệm
- Bridge và switch
- Wireless Access Point

Các điểm truy cập trên tầng 2

- Khái niệm



Các thiết bị trên tầng 2 bắt đầu đã có 1 mức độ "thông minh" nhất định như chúng có thể **ghi nhận** được địa chỉ vật lý của thiết bị mạng và **chuyển dữ liệu** đi dựa trên các địa chỉ vật lý này (**MAC address**).

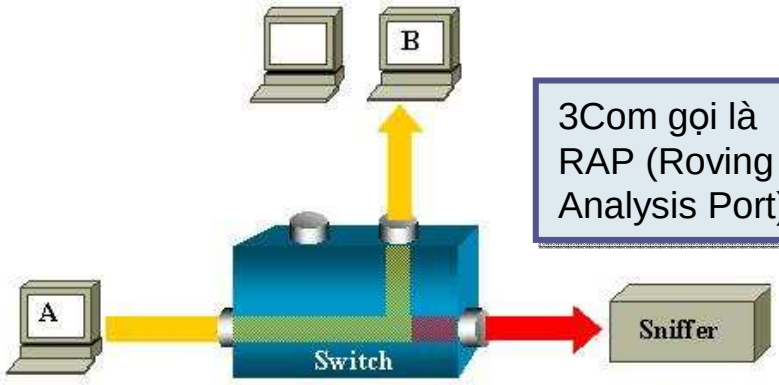


Những vấn đề an toàn trên tầng 2 bao gồm:
- Bridge và Switch
- Wireless Access Point

Các điểm truy cập trên tầng 2

- Cầu nối (Bridge) và bộ chuyển mạch (switch)

• Switch là một thiết bị mạng an toàn hơn Hub
• Mỗi cổng của switch chỉ có thể nhận được đúng thông tin của riêng mình và thông tin quảng bá



Khai thác tính năng SPAN

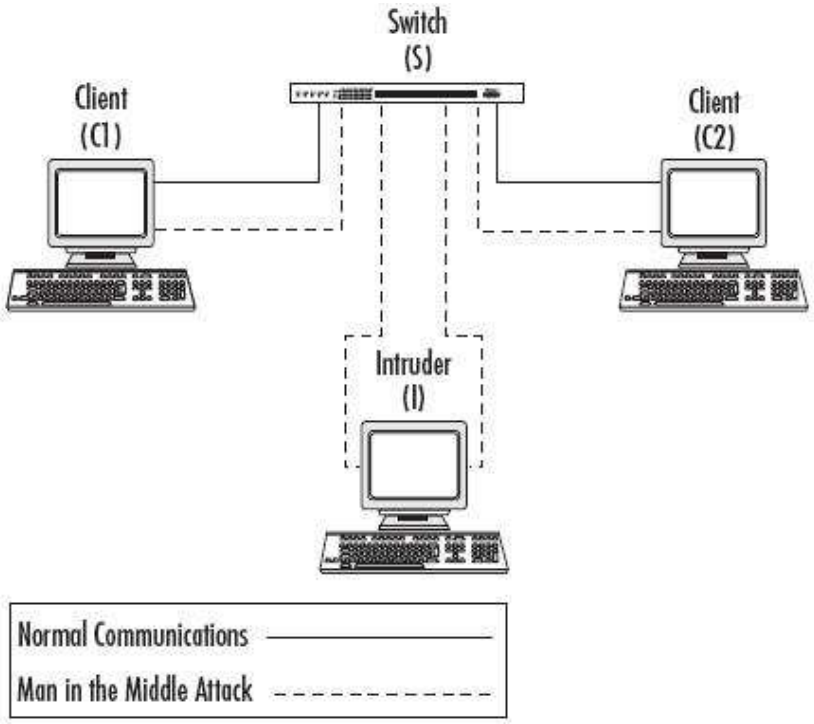
3Com gọi là RAP (Roving Analysis Port)

SPAN (Switched Port Analyzer)
• Là 1 tính năng được người quản trị mạng dùng trong khắc phục sự cố.
• Copy tất cả các gói đi vào và đi ra 1 hoặc nhiều cổng gửi đến 1 cổng đặc biệt nào đó.

Nếu có được tài khoản quản trị switch, hacker có thể lợi dụng tính năng SPAN để nghe lén trên mạng switch.

Các điểm truy cập trên tầng 2

- Cầu nối (Bridge) và bộ chuyển mạch (switch)



Tấn công switch bằng cách giả mạo ARP

- Kẻ xâm nhập sẽ gửi gói ARP đến Client1 với địa chỉ nguồn là địa chỉ IP của Client2 nhưng với địa chỉ MAC của mình (Intruder).
- Tương tự, kẻ xâm nhập cũng sẽ gửi gói ARP đến Client2 với địa chỉ nguồn là địa chỉ IP của Client1 nhưng với địa chỉ MAC của mình.
- Khi đó, Client1 và Client2 đều lưu trữ trong ARP Cache của mình IP của nhau nhưng với MAC của kẻ xâm nhập.
- Do đó, khi Client1 và Client2 gửi dữ liệu cho nhau đều đi qua máy của kẻ xâm nhập mà không hề hay biết.

Các điểm truy cập trên tầng 2

- Wireless Access Point

Hacker có thể dò tìm và kết nối vào 1 Access Point để gia nhập vào 1 mạng WLAN không được mã hóa mà không cần phải có bất kỳ tài khoản nào.

Cài đặt khóa có độ dài lớn (chẳng hạn 128 bits) và thường xuyên thay đổi khóa để tránh bị tấn công.

Cấu hình các cơ chế bảo mật tại Access Point

- Ẩn đi định danh của mạng (hide SSID).
- Cài đặt khóa (key) cho mạng.
- Tạo bộ lọc MAC (filter) chỉ cho phép các thiết bị trong danh sách cho trước tham gia vào mạng.

Phần 3

Các điểm truy cập trên tầng 3

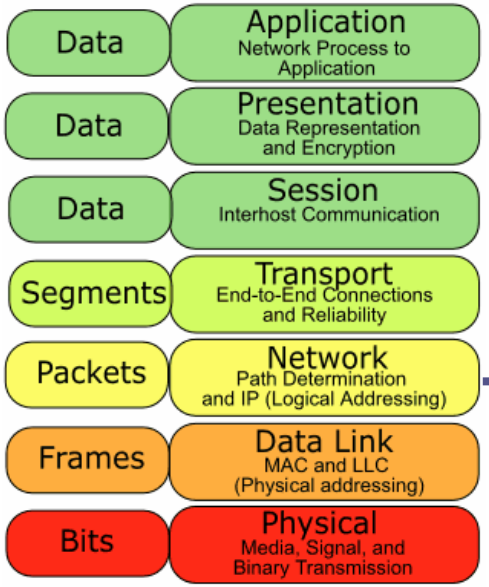
- Khái niệm
- Router
- Remote Access Server
- Layer 3 Firewall

Các điểm truy cập trên tầng 3

- Khái niệm

Các thiết bị trên tầng 3

- Vạch đường cho các gói tin
- Sử dụng địa chỉ luận lý
- Có nhiều các cơ chế bảo mật để chứng thực người dùng và điều khiển lưu thông trên mạng

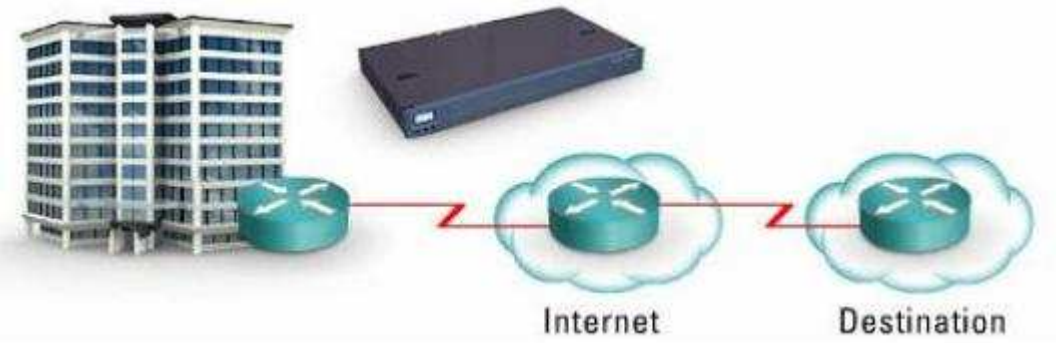


Những vấn đề an toàn trên tầng 3 bao gồm:

- Bộ định tuyến (Router)
- Máy chủ phục vụ từ xa (Remote Access Server)
- Tường lửa trên tầng 3 (Layer 3 firewall)

Các điểm truy cập trên tầng 3

- Router



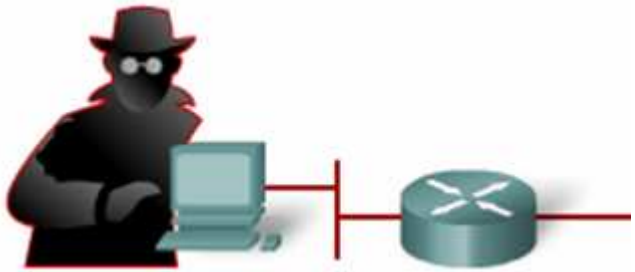
Router dùng để tìm đường đi tốt nhất cho các gói tin, có khả năng ngăn được broadcast.

Router cung cấp một số tính năng bảo mật:

- Danh sách điều khiển truy cập (ACL): cho phép chặn gói tin dựa theo địa chỉ, loại dịch vụ (cổng).
- Lọc gói tin dựa theo loại gói hay nội dung gói.
- Quality of Service (QoS): điều khiển lưu thông trên mạng dựa theo độ ưu tiên của dịch vụ.

Các điểm truy cập trên tầng 3

- Router



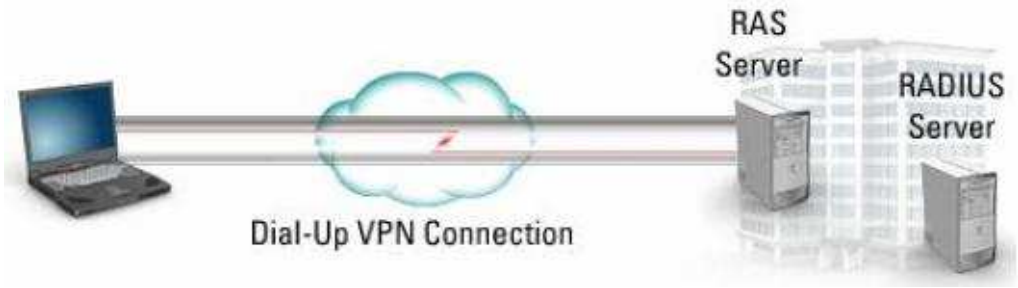
Router có thể bị **tấn công** thông qua đường **Telnet** (dùng để cấu hình thiết bị từ xa qua cổng 23) vì mật khẩu không được mã hóa.

Tấn công tính năng **vạch đường động** (dynamic routing)
- Giả mạo địa chỉ của 1 router trong mạng
- Gửi các thông tin vạch đường cho router mục tiêu

Cách ngăn ngừa
- Dùng giao thức vạch đường có mã hóa
- Cài đặt chứng thực trong giao thức vạch đường

Các điểm truy cập trên tầng 3

- Server truy cập từ xa (RAS)



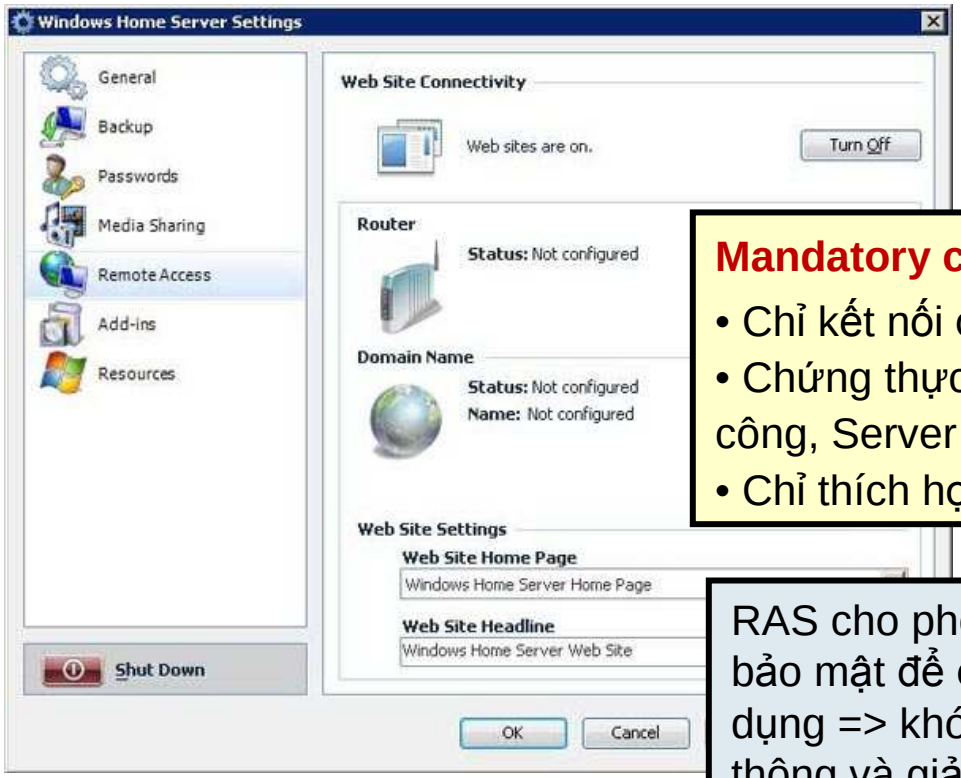
Cung cấp kết nối cho những người dùng ở xa thông qua đường điện thoại (dial-up) hay VPN.

Những cách chứng thực thông dụng là:

- **PAP** (Password Authentication Protocol)
  - o Truyền mật khẩu dạng Plain-Text trên đường truyền => không an toàn
- **SPAP** (Shiva hay Secure PAP): an toàn hơn PAP vì có sử dụng mã hóa.
- **CHAP** (Challenge Handshake Authentication Protocol) và **MS-CHAP** (Microsoft CHAP)
  - o An toàn hơn vì có mã hóa và không truyền mật khẩu trên đường truyền.
- **EAP** (Extensible Authentication Protocol)
  - o Kết hợp với phương pháp chứng thực thứ 3 như smartcard, sinh trắc học.
- Chứng thực tập trung (qua **RADIUS**): an toàn và hiệu quả hơn.

Các điểm truy cập trên tầng 3

- Server truy cập từ xa (RAS)



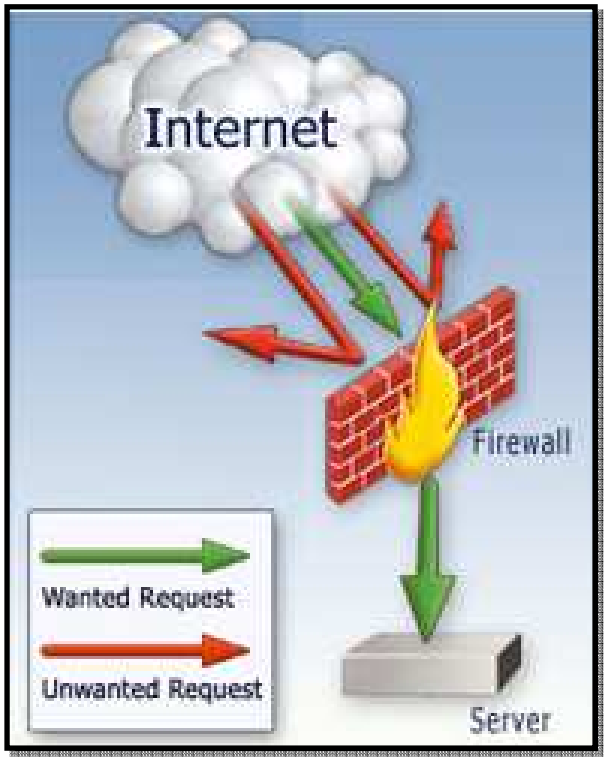
Mandatory callback

- Chỉ kết nối đến Server từ 1 số điện thoại cho trước.
- Chứng thực 2 chiều: sau khi chứng thực thành công, Server sẽ kết nối ngược lại Client.
- Chỉ thích hợp với người dùng cố định.

RAS cho phép người quản trị cài đặt các tính năng bảo mật để điều khiển đúng loại giao thức đang sử dụng => khóa các giao thức khác để giảm băng thông và giảm nguy cơ tấn công.

Các điểm truy cập trên tầng 3

- Tường lửa (Firewall)



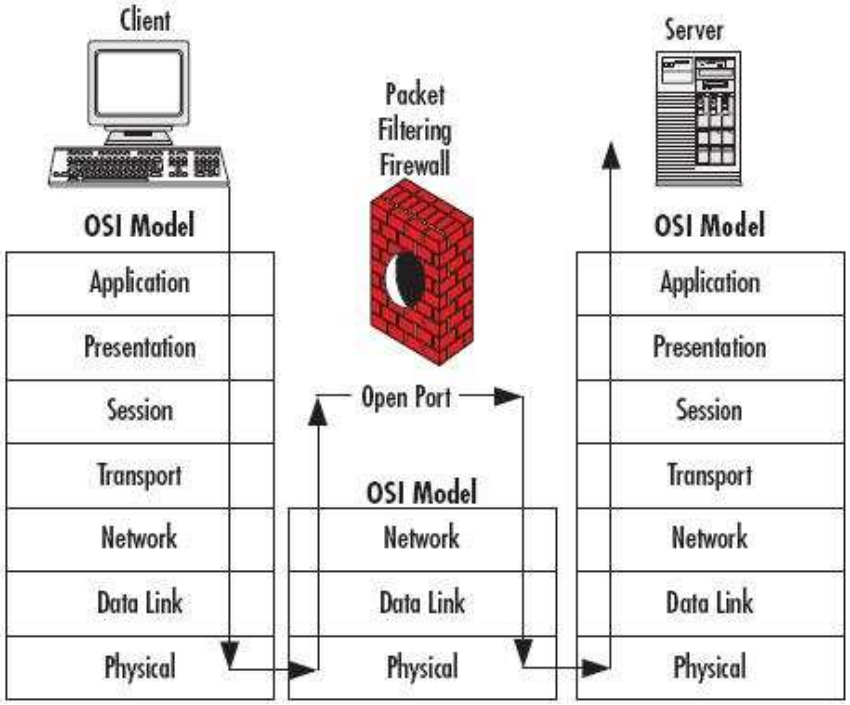
Firewall sẽ ngăn chặn truy cập trái phép từ bên ngoài vào bên trong mạng và khóa người dùng bên trong mạng truy cập các tài nguyên nguy hại bên ngoài mạng.

Firewall được chia thành 3 dạng chính:

- Lọc gói: hoạt động trên tầng 3
- Lọc nội dung: hoạt động trên tầng ứng dụng
- Duyệt tất cả trạng thái: hoạt động trên tất cả các tầng

Các điểm truy cập trên tầng 3

- Firewall trên tầng 3



Firewall lọc gói được cấu hình để từ chối hay cho phép truy cập từ (hoặc đến) 1 **địa chỉ IP** xác định hoặc **1 cổng** cho trước

2 cơ chế thực hiện:
- Mặc nhiên cho phép (allow by default)
- Mặc nhiên cấm (deny by default)

Mặc nhiên cấm là chính sách bảo mật tốt hơn

Các điểm truy cập trên tầng 3

- Firewall trên tầng 3

Các router mạnh hiện nay gần như đều có tùy chọn hỗ trợ loại firewall lọc gói

Những ưu điểm của Firewall trên tầng 3

- Tốc độ nhanh: vì chỉ cần kiểm tra header của gói
- Dễ sử dụng: các rule định nghĩa rõ ràng.
- Trong suốt (Transparency) với các thiết bị mạng và người dùng

Những hạn chế của Firewall trên tầng 3

- Khó mở riêng 1 cổng cho 1 ứng dụng.
- Không quan tâm đến nội dung gói: bỏ sót gói độc hại

Phần 4

Các điểm truy cập trên tầng 4 và cao hơn

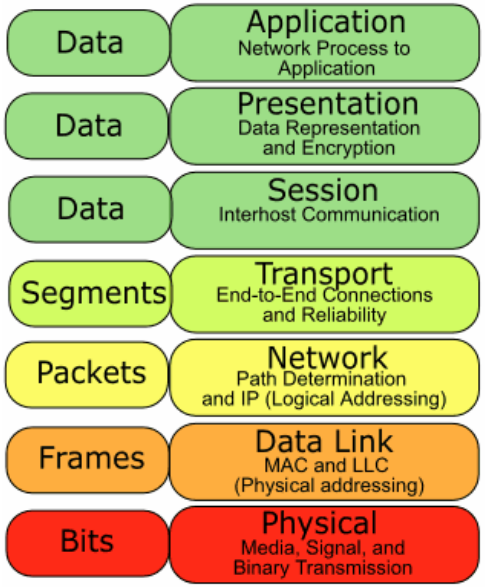
- Khái niệm
- Proxy Server
- Máy trạm
- Máy chủ

Các điểm truy cập trên tầng 4

- Khái niệm

Tầng 4 và các tầng cao hơn là nơi mà hệ điều hành và ứng dụng hiện diện

cần phải có các tính năng bảo mật để cung cấp cho từng hệ điều hành và ứng dụng riêng biệt

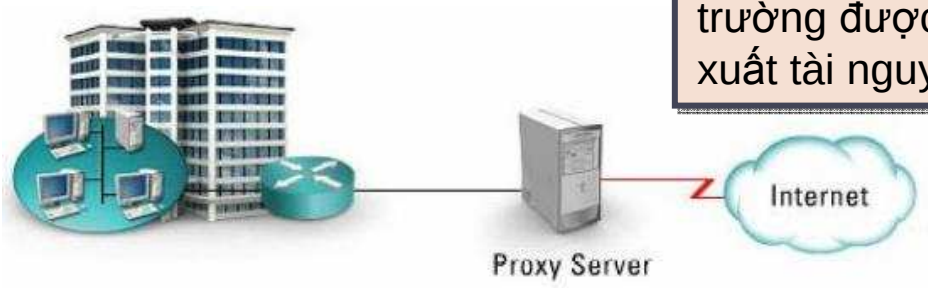


Những vấn đề an toàn trên tầng 4 và cao hơn gồm:
- Proxy Server
- Máy trạm (Workstation)
- Máy chủ (Server)

Các điểm truy cập trên tầng 4

- Proxy Server

cho phép hệ thống bên trong môi trường được bảo vệ có thể truy xuất tài nguyên ở bên ngoài



Đặc điểm
- Làm tăng tốc độ truy xuất Web: do đã lưu cache
- Giám sát các lưu thông trên mạng: lưu log file các truy cập
- Lọc thông tin: dựa theo giao thức, theo địa chỉ, …
- Ngăn chặn hiệu quả sự xâm nhập không mong muốn vào hệ thống mạng

Proxy Server có điểm yếu nếu ta dùng server đó với các chức năng khác có thể sẽ tạo ra các lỗ hổng.

Sử dụng 1 Server chuyên dùng chỉ với chức năng Firewall và Proxy.

Các điểm truy cập trên tầng 4

- Máy trạm (Workstation)

Chúng rất kém an toàn hơn so với Server và thường dễ bị tấn công vì ít quan tâm đến vấn đề bảo mật.

Các điểm yếu thường bị khai thác
- Giao thức TCP/IP là giao thức không an toàn
- Dịch vụ chia sẻ file trên hệ điều hành Windows

Người dùng thường tự mình tạo ra các lỗ hổng:
- Không thường xuyên thay đổi mật khẩu
- Không cập nhật các bản diệt virus mới nhất
- Cài đặt các phần mềm không đáng tin cậy
- Mở các file đính kèm không rõ nguồn gốc trong email

- Gỡ bỏ tất cả các dịch vụ không cần thiết
- Không cài đặt các phần mềm chưa rõ nguồn gốc
- Cập nhật các bản vá lỗi và anti-virus.
- Cài đặt 1 tường lửa
- Có chính sách sử dụng riêng cho từng đối tượng

Các điểm truy cập trên tầng 4

- Máy chủ (Server)

Server thường là đối tượng bị tấn công vì nó chứa các thông tin quan trọng mà các hacker muốn có.

• Server càng có nhiều chức năng càng có nhiều nguy cơ tấn công từ chính các dịch vụ mà nó cung cấp
• Server cũng có thể có các điểm yếu đáng quan tâm như máy trạm nếu người quản trị không cẩn thận.

• Đặt Server phía sau 1 hay nhiều Firewall
• Có lớp bảo vệ (vật lý) giữa những server này và môi trường bên ngoài.
• Luôn cập nhật hệ điều hành, ứng dụng và các chương trình diệt virus.