Chương 6

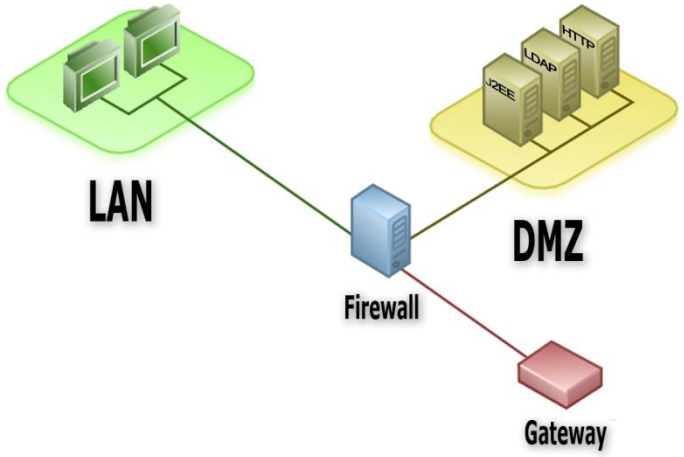
CÁC MÔ HÌNH MẠNG AN TOÀN

Trình bày: Bùi Minh Quân - bmquan@ctu.edu.vn
Khoa MMT&TT – Trường CNTT&TT - ĐHCT

Chương 6

CÁC MÔ HÌNH MẠNG AN TOÀN

- DMZ (vùng phi quân sự)
- VLAN (mạng LAN ảo)
- NAT (dịch địa chỉ)

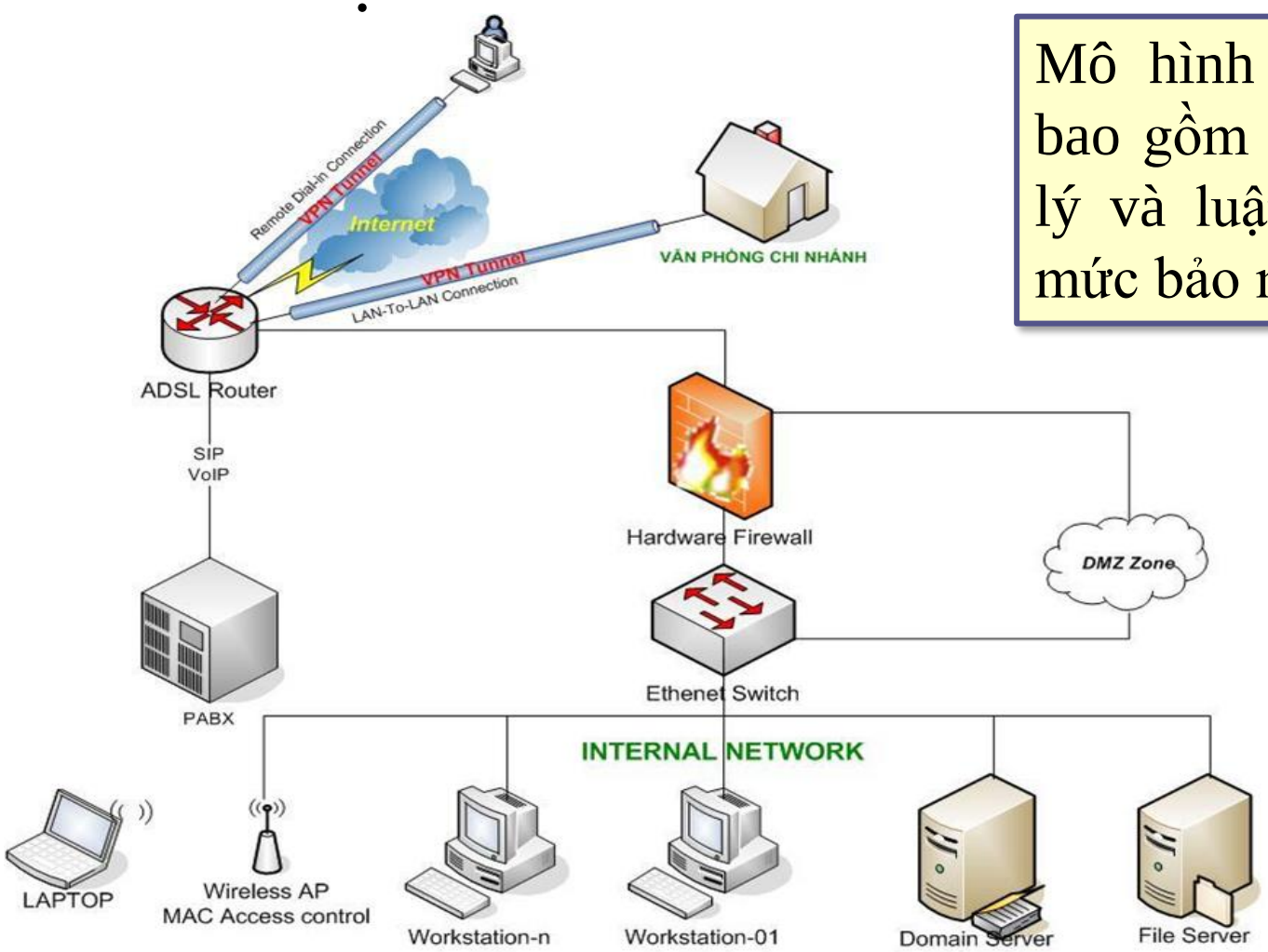


Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về cách thức xây dựng các mô hình mạng an toàn.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Phân biệt được khái niệm về Intranet, Extranet và vùng DMZ.
  - Trình bày mô hình mạng an toàn với vùng DMZ.
  - Hiểu được khái niệm VLAN, ích lợi và kỹ thuật xây dựng mô hình mạng với VLAN.
  - Trình bày được khái niệm NAT-PAT và ứng dụng của NAT-PAT trong việc xây dựng mô hình mạng an toàn.

Mô hình mạng an toàn

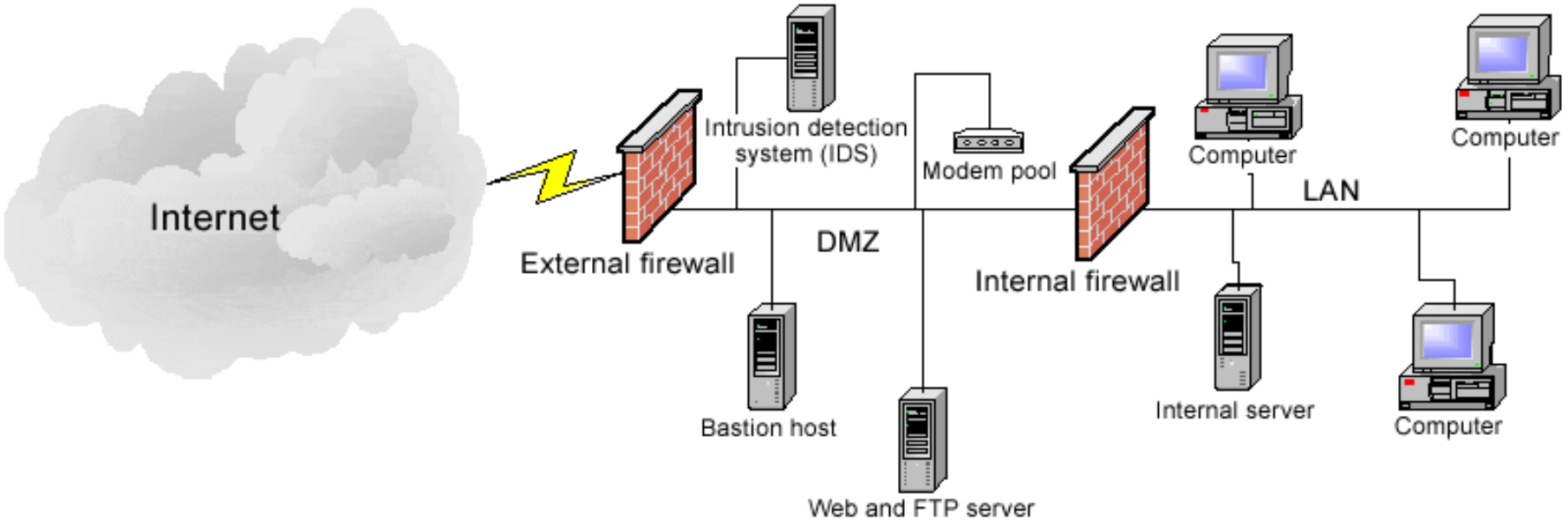
- Khái niệm



Mô hình mạng an toàn bao gồm nhiều vùng vật lý và luận lý với nhiều mức bảo mật khác nhau.

Vùng an ninh

- Khái niệm



Vùng an ninh (**security zone**) là một phần của mạng được định nghĩa chung 1 mức an ninh.

Vùng an ninh thường được chia ra làm 3 loại:

- Intranet
- Extranet
- DMZ

Vùng an ninh

- Intranet

Intranet
• Là một mạng dùng riêng
• Sử dụng các giao thức và dịch vụ thông tin tương tự Internet.
• Cung cấp các dịch vụ như Web, FTP, Email, …

• Tốc độ cao
• Dễ dàng truy xuất các tài nguyên
• Sử dụng các dạng mạng như:
+ Ethernet
+ Fast Ethernet, Gigabit Ethernet
+ Token ring
+ ATM

Vùng an ninh

- Extranet

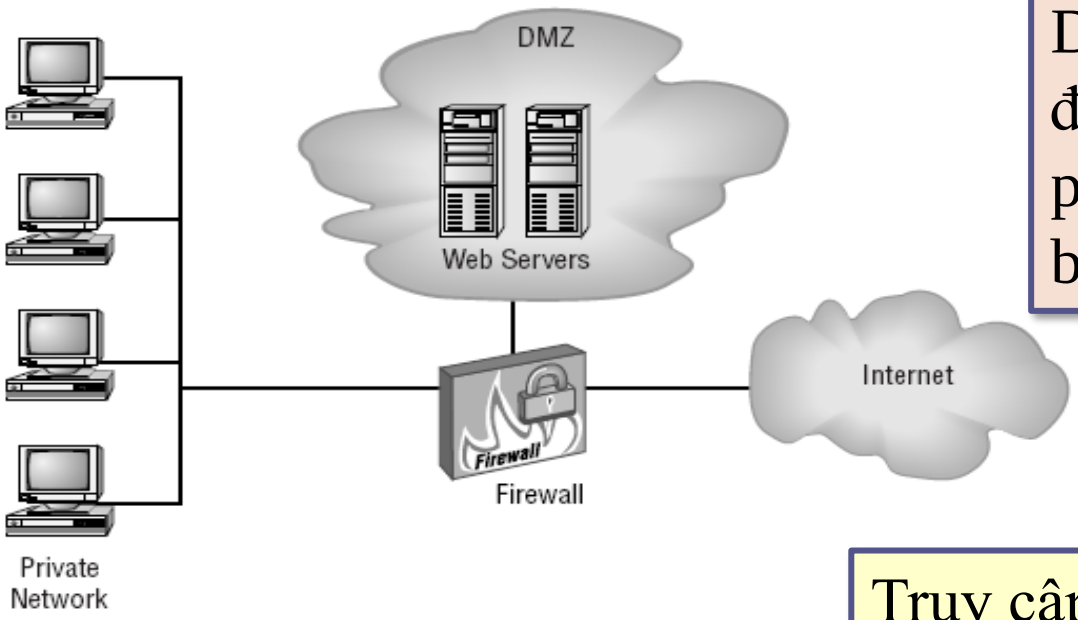
• Yêu cầu tính riêng tư và bảo mật
• Có thể dùng PKI hoặc kỹ thuật VPN để thiết lập nếu cần độ an toàn cao.

Extranet

• Là một Intranet có kết nối với mạng dùng ở ngoài như các khách hàng, đối tác, nhà cung cấp, …
• Sử dụng để trao đổi thông tin, hợp tác hoặc chia sẻ các dữ liệu đặc biệt.
• Có thể nối kết được với Internet.

Vùng an ninh

- DMZ (Demilitarized Zone)



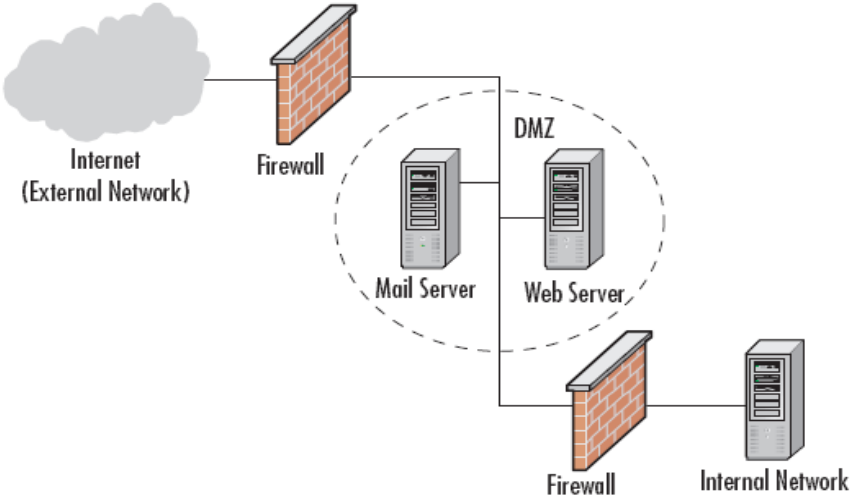
DMZ là 1 vùng của mạng được thiết kế đặc biệt, cho phép những người dùng bên ngoài truy xuất vào.

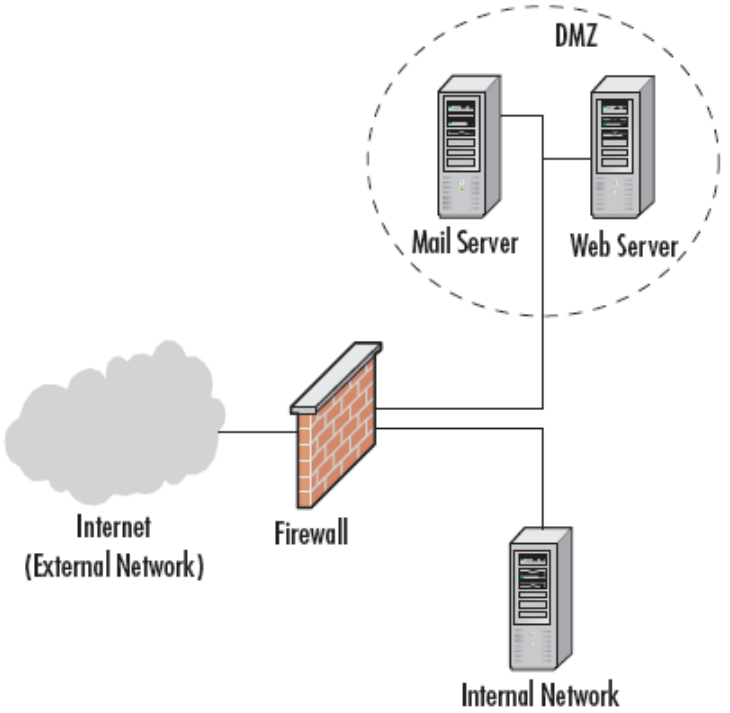
Nếu vùng DMZ bị tấn công và gây hại thì vẫn không ảnh hưởng đến mạng riêng của tổ chức.

Truy cập vào vùng DMZ luôn được điều khiển và giới hạn bởi Firewall và hệ thống Router.

Vùng an ninh

- DMZ - Cách thiết kế





Phân lớp DMZ (Layered DMZ)

• Đặt giữa 2 firewall có các quy định khác nhau.

• Cho phép bên ngoài Internet nối kết vào, nhưng chặn không cho truy cập vào mạng cục bộ bên trong.

Tường lửa nhiều giao diện DMZ (Multiple Interface Firewall DMZ)

• Dùng thiết bị Firewall mạnh có thể quản lý các lưu thông trên nhiều cổng

• Hiện nay, mô hình này được sử dụng nhiều hơn.

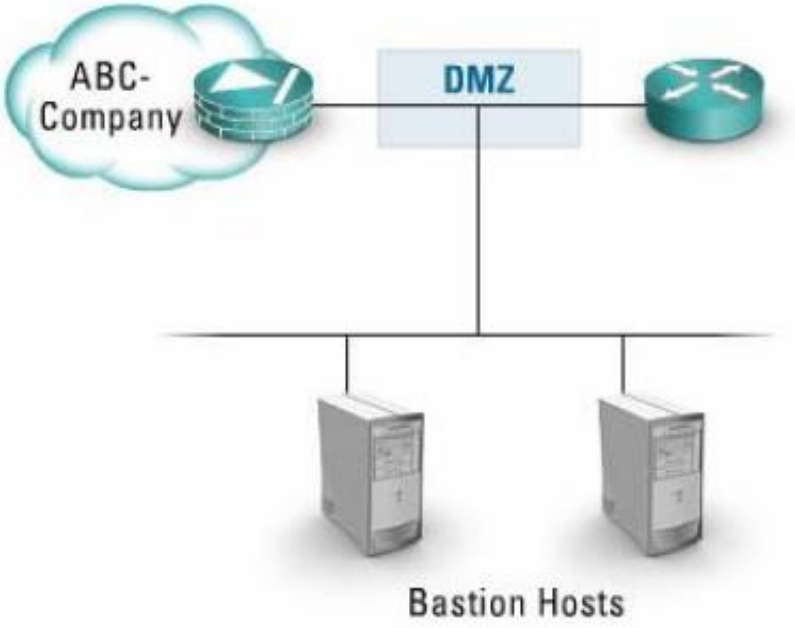
Vùng an ninh

- DMZ - Cách thiết kế

Mạng nội bộ phải được Firewall bảo vệ cả từ mạng bên ngoài (Internet) và cả từ vùng DMZ vì vùng DMZ có khả năng bị tấn công và khai thác.

Phải gia cố hệ thống DMZ, chẳng hạn:

- Gở bỏ các dịch vụ ít sử dụng
- Gở bỏ các thành phần không cần thiết.

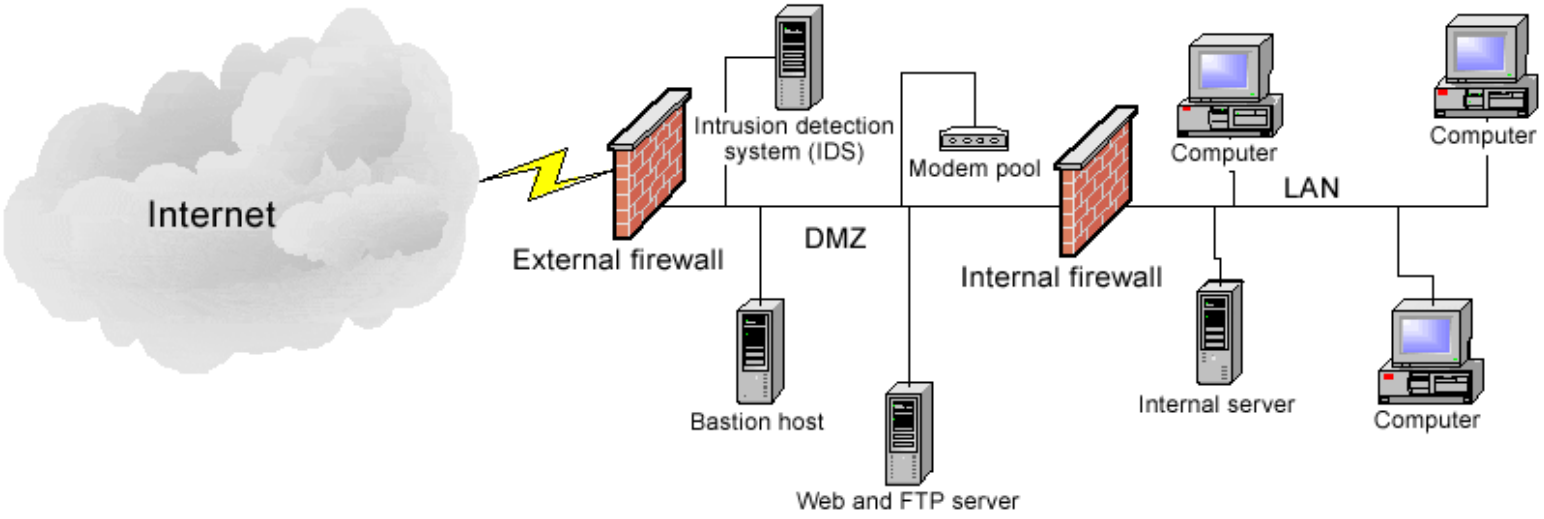


Các máy tính trong vùng DMZ:

- Được gọi là Bastion host.
- Có thể được truy xuất từ mạng nội bộ bên trong và cả mạng bên ngoài.

Vùng an ninh

- DMZ – Các dịch vụ bên trong vùng



Các dịch vụ trong vùng DMZ:

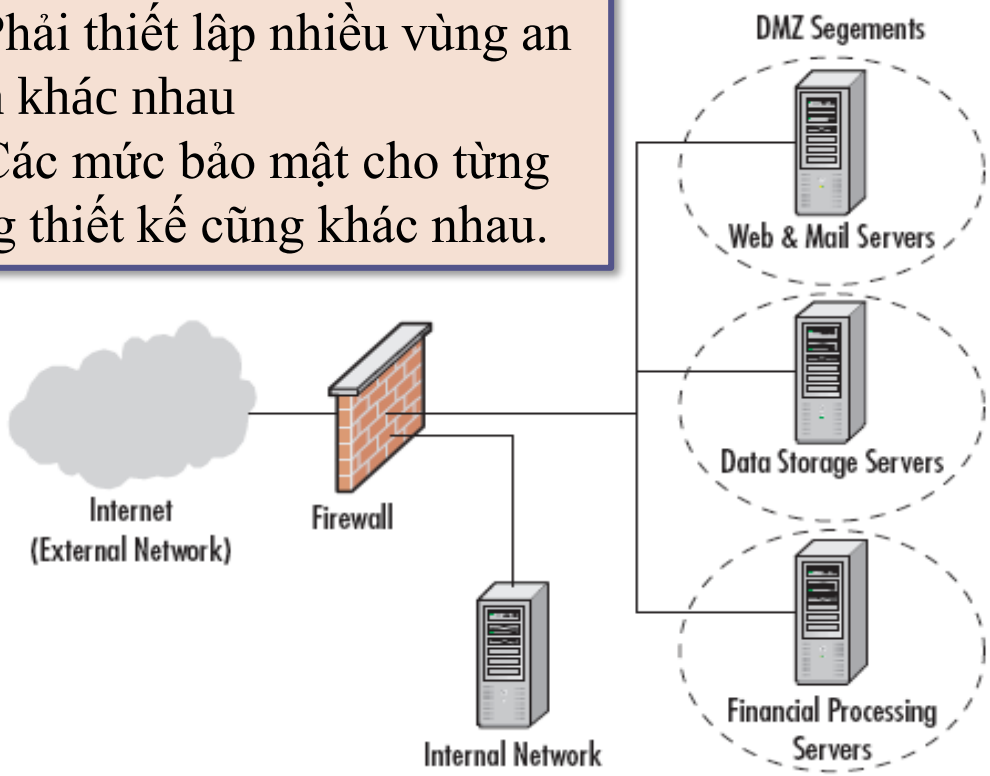
- Web, Email, FTP
- DNS
- IDS (hệ thống phát hiện xâm nhập)

Một số hệ thống yêu cầu phải đảm bảo an toàn cho vùng DMZ bằng cách sử dụng các giao thức bảo mật như SSL, TLS.

Vùng an ninh

- DMZ – Nhiều vùng trong vùng DMZ

Đặc thù yêu cầu của từng hệ thống khác nhau
⇒ Phải thiết lập nhiều vùng an ninh khác nhau
⇒ Các mức bảo mật cho từng vùng thiết kế cũng khác nhau.



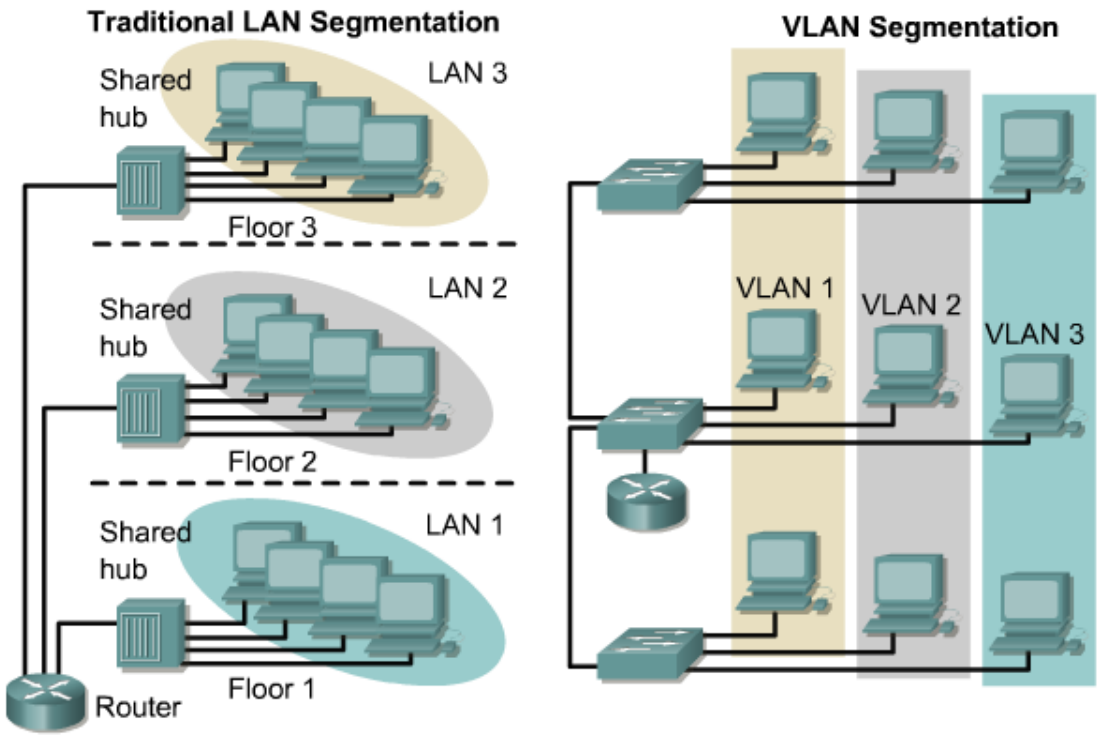
Các vấn đề:
• Phức tạp khi cài đặt, bảo vệ và quản trị.
• Các luật trong Firewall phải lớn => dễ nhầm lẫn.

Giải pháp:
• Dùng chiến thuật **cấm tất cả** (deny all)
• Chỉ cho phép từng dịch vụ riêng biệt có yêu cầu

Một hệ thống E-Commerce hiện đại

VLAN

- Khái niệm

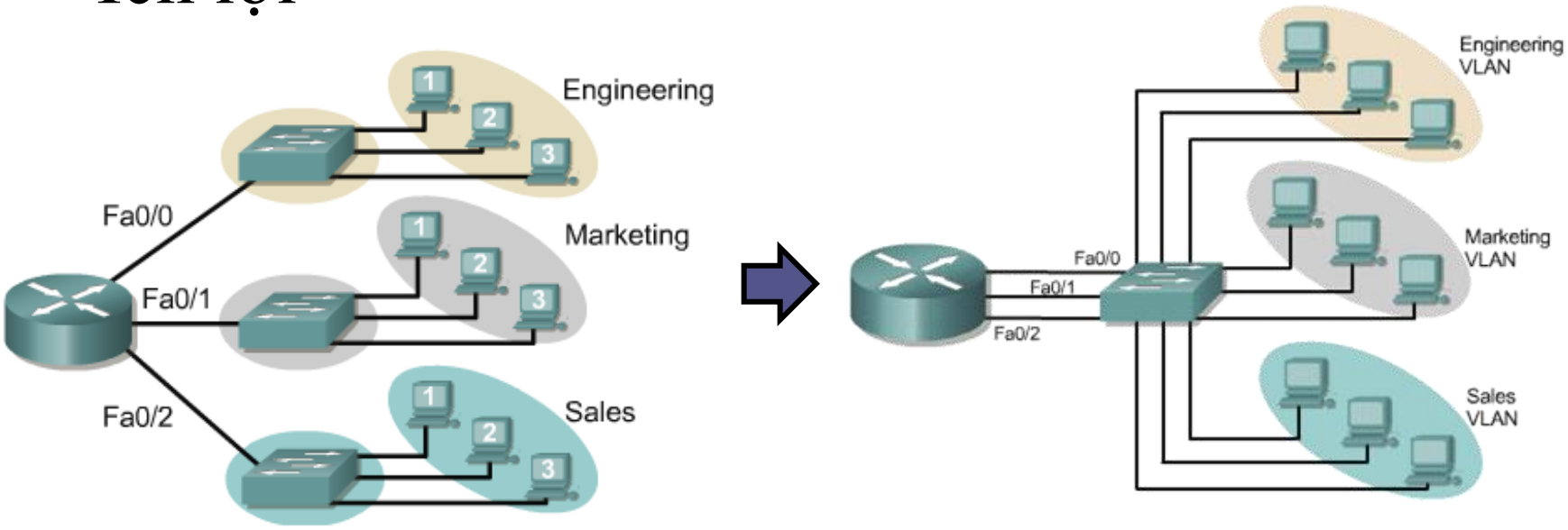


- Phân mạng lớn thành nhiều mạng nhỏ theo chức năng.
- Dùng switch có hỗ trợ tính năng VLAN
- Muốn liên lạc giữa các máy tính trong các VLAN khác nhau phải dùng 1 router.

VLAN là 1 nhóm luận lý các máy tính, thiết bị mạng mà không bị giới hạn vị trí địa lý hay kết nối vật lý giữa chúng.

VLAN

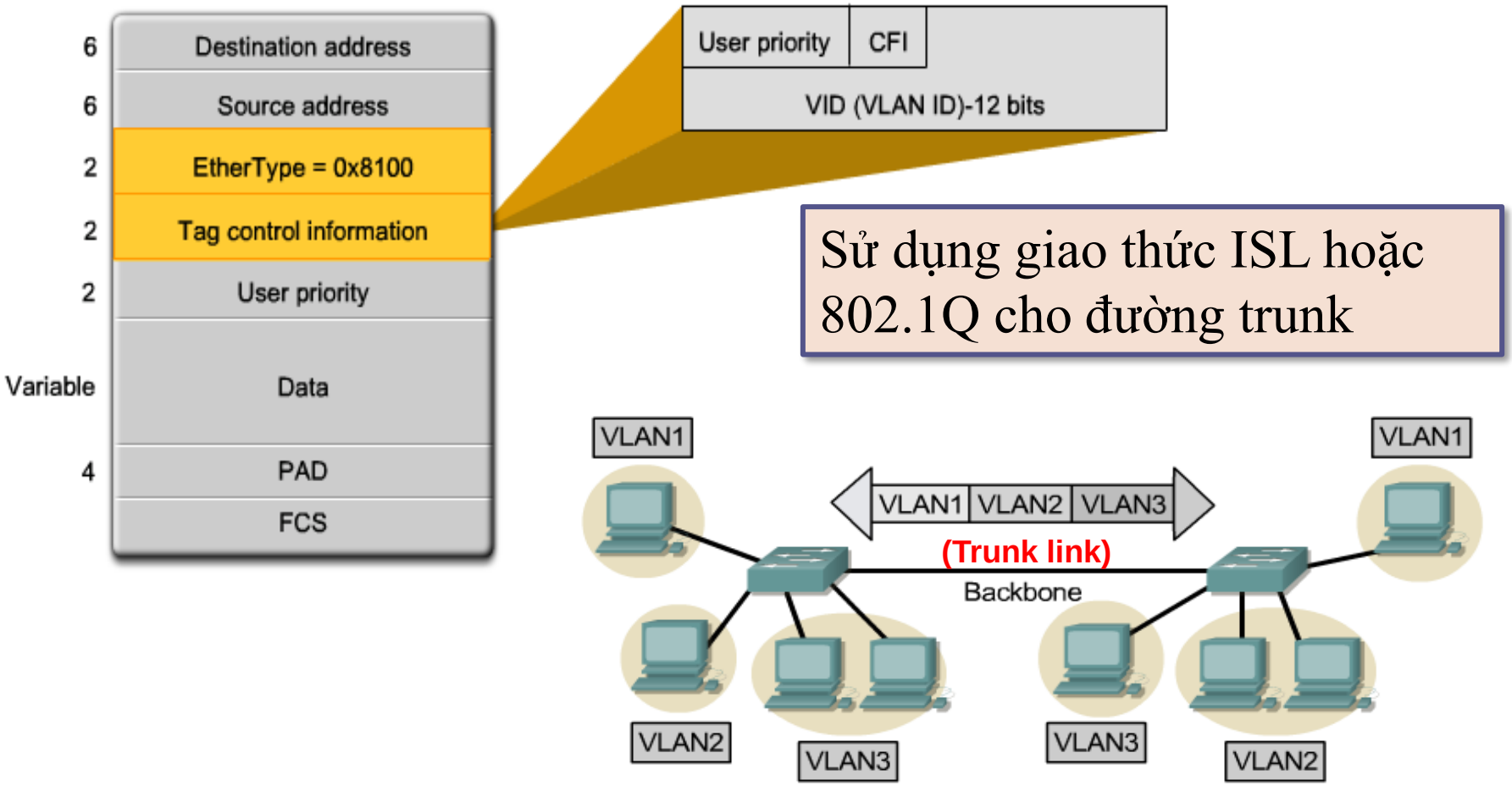
- Ích lợi



- Ngăn broadcast làm tăng hiệu năng mạng
- Tiết kiệm thiết bị switch
- Nâng cao tính bảo mật trong mạng.
- Dễ dàng triển khai và quản lý các nhóm làm việc theo từng VLAN.

VLAN

- Trunk



Switch tự động thêm Tag điều khiển để chỉ rõ Frame thuộc VLAN nào khi Frame đi vào đường trunk.

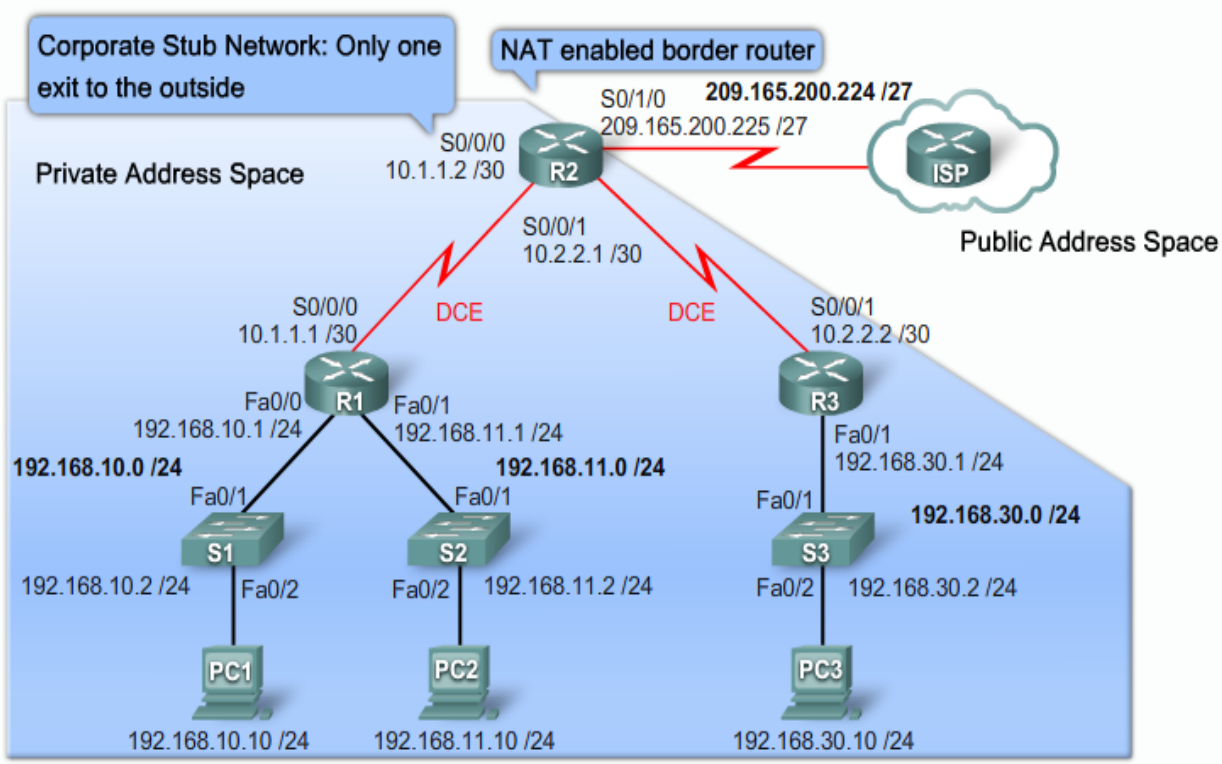
NAT (Network Address Translation)

- Khái niệm

NAT che dấu địa chỉ bên trong mạng cục bộ (địa chỉ private) khi giao tiếp với máy tính ở mạng Internet (public)

Máy tính bên trong mạng LAN có thể nối kết trực tiếp với máy tính ở ngoài, nhưng máy tính ở ngoài không "thấy" được máy tính bên trong LAN.

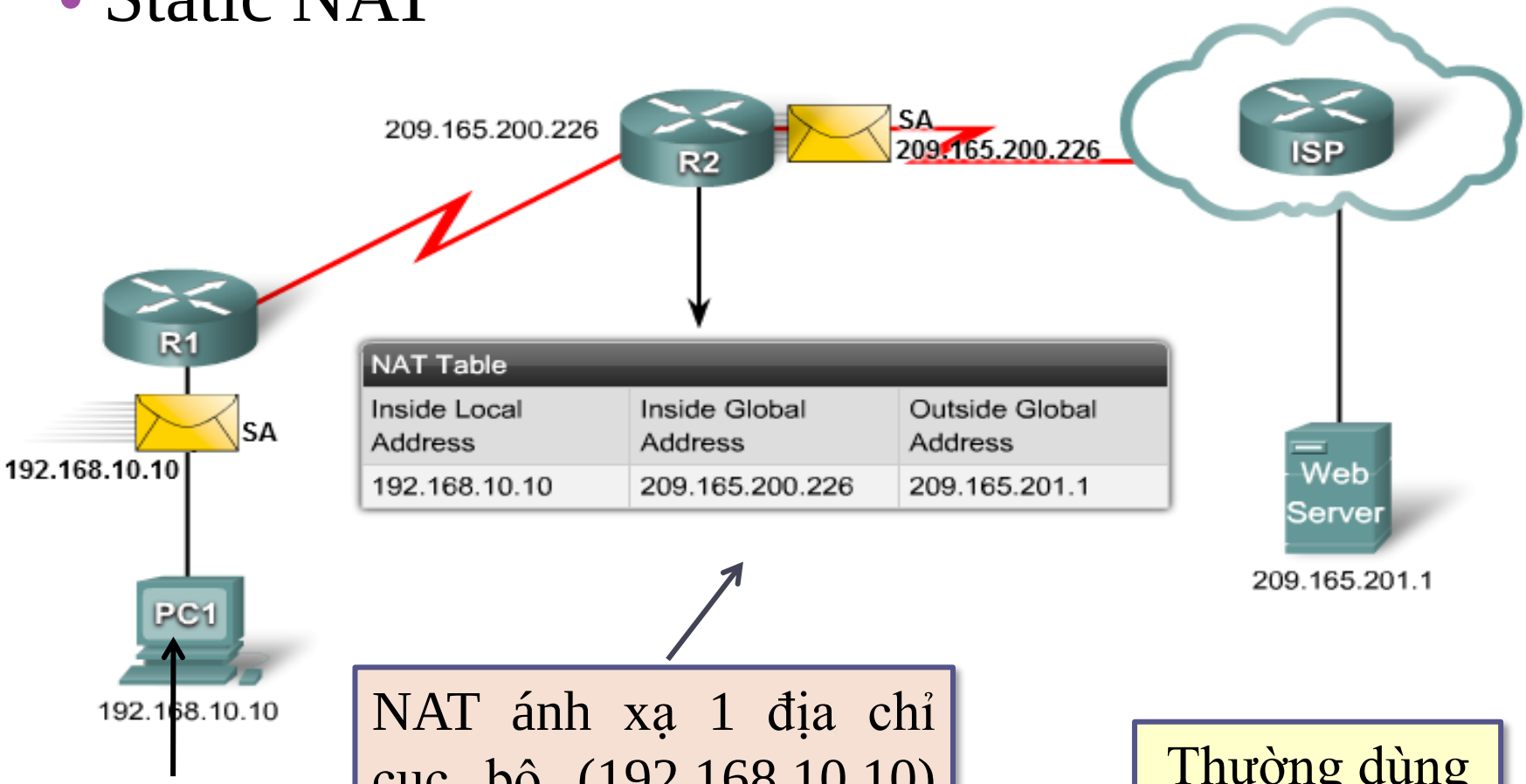
Dãy địa chỉ dùng riêng cho các mạng cục bộ



Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

NAT

- Static NAT

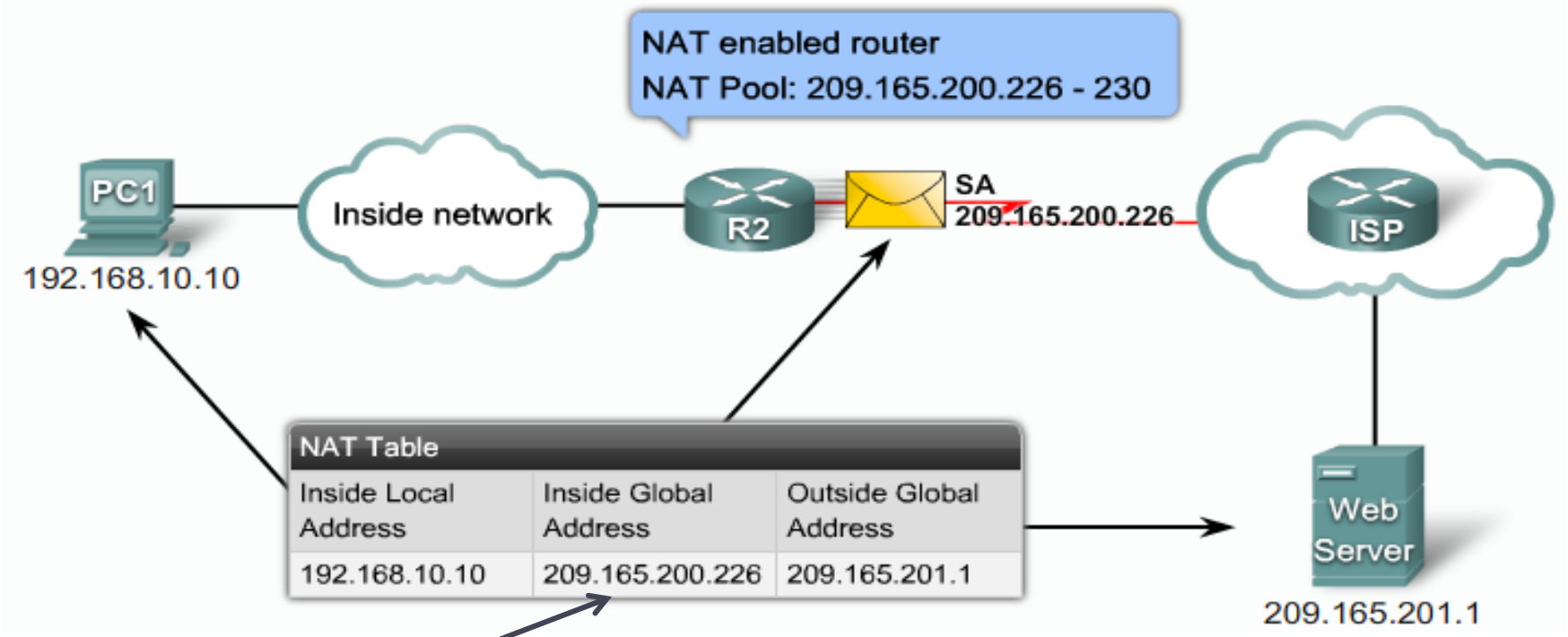


NAT ánh xạ 1 địa chỉ cục bộ (192.168.10.10) sang 1 địa chỉ thực (209.165.200.226)

Thường dùng cho các Server

NAT

- Dynamic NAT



Dynamic NAT tự động ánh xạ 1 địa chỉ priavte (192.168.10.10) sang 1 địa chỉ **trong dãy (pool)** địa chỉ public cho trước (209.165.200.226 - 230)

Dùng khi có được nhiều địa chỉ thực ở ngoài.

NAT - PAT (Port Address Translation)

PAT còn gọi là NAT Overload

PAT ánh xạ **nhiều** địa chỉ cục bộ (192.168.10.11–192.168.10.12) **sang 1 địa chỉ thực** với các **cổng** khác nhau (209.165.200.226 cổng 1444 và 1445)

Thích hợp cho dạng mạng có nhiều máy cục bộ dùng chung đường truyền Internet (như ADSL chẳng hạn)