Chương 5

An toàn trong truyền thông

- Các giao thức truy cập từ xa: PPP, Telnet, Wireless, VPN, …
- Các giao thức truy cập liên mạng: Email, Web, FTP, File Sharing, Directory, LDAP, …

Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về các giải pháp tạo sự an toàn trong truyền thông.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Trình bày được sự quan trọng của an toàn trong truyền thông.
  - Mô tả được các giao thức sử dụng cho truy cập từ xa như PPP, Telnet, mạng không dây , mạng riêng ảo.
  - Hiểu và vận dụng được một số kỹ thuật nâng cao độ an toàn cho các giao thức truy cập từ xa.
  - Mô tả được các giao thức truy cập liên mạng thông dụng hiện nay như Mail, Web, FTP, File sharing, Directory, LDAP, …
  - Hiểu và vận dụng được một số kỹ thuật nâng cao độ an toàn cho các giao thức truy cập liên mạng .

Phần 1

Các giao thức cho truy cập từ xa

- Khái niệm
- RAS và PPP
- Telnet và SSH
- TACACS+ và RADIUS
- WLAN
- VPN

An toàn trong truyền thông

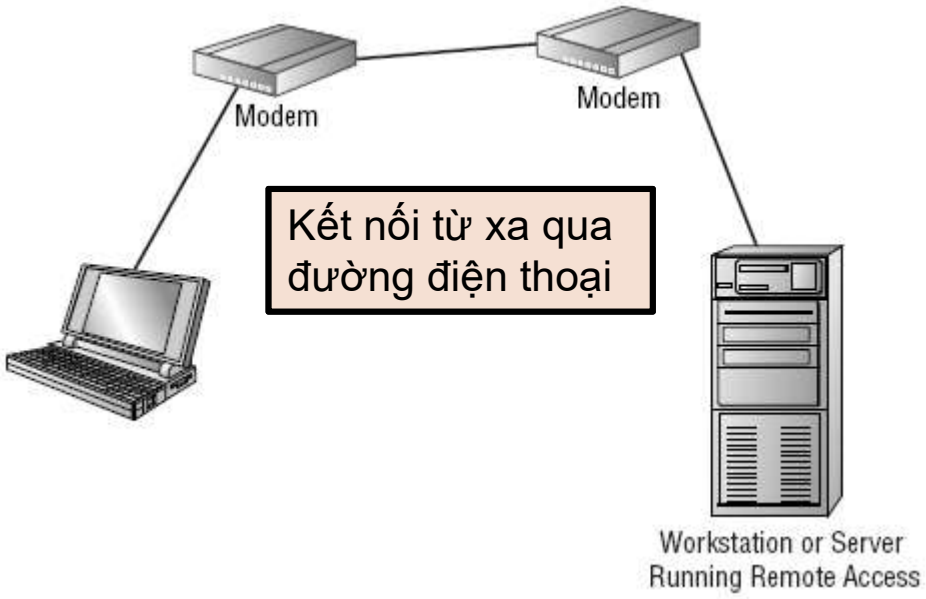
- Sự quan trọng của an toàn trong truyền thông

Với tốc độ của Internet ngày càng nhanh, truyền thông trên mạng, truy cập từ xa, làm việc bằng các thiết bị cầm tay ngày càng trở nên phổ biến.

Đòi hỏi phải có các cơ chế an toàn trên đường truyền, cho các giao thức mạng và các dịch vụ trên mạng.

Truy cập từ xa

- RAS và PPP



Kết nối từ xa qua đường điện thoại

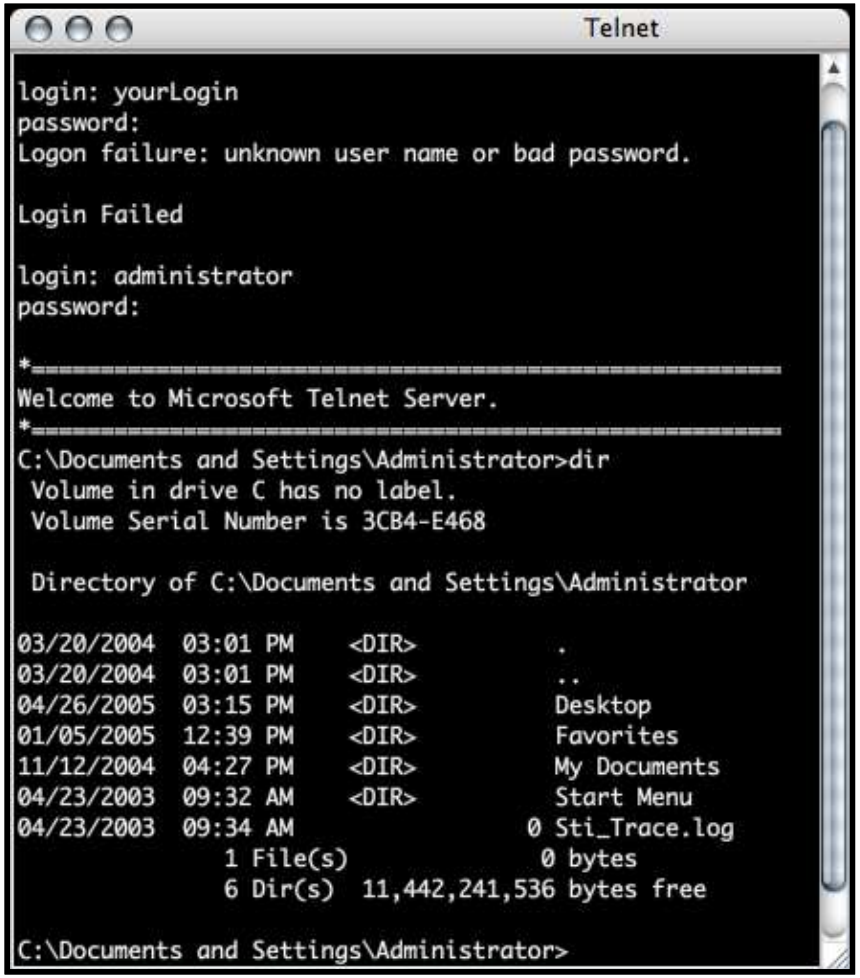
- Dễ sử dụng, tốc độ thấp.
- Kết nối đơn giản.

PPP (Point-to-Point Protocol)

- PPP là giao thức tầng 2
- Cho phép chứng thực:
  - + PAP: không mã hóa
  - + CHAP: có mã hóa
- Có thể dùng cho các dạng mạng IP, IPX, AppleTalk.
- Cho phép cấp địa chỉ IP động
- Cho phép nén dữ liệu và điều khiển chất lượng đường nối kết.

Truy cập từ xa

- Telnet

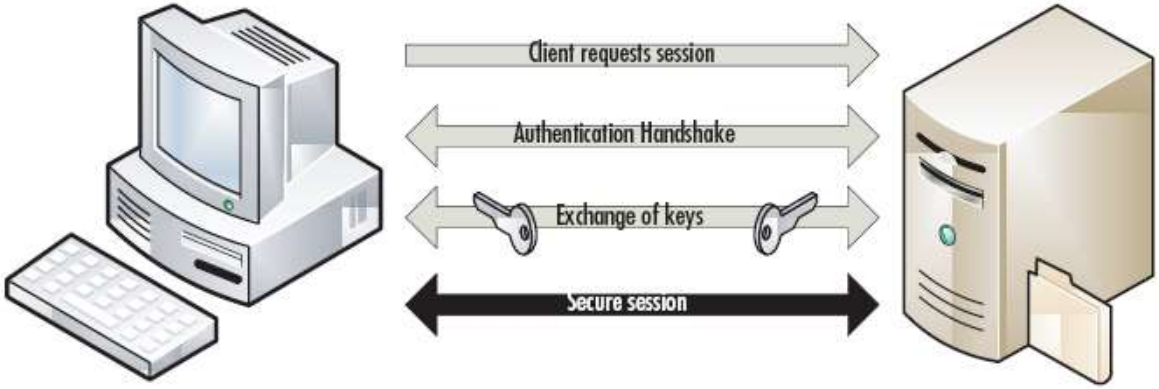


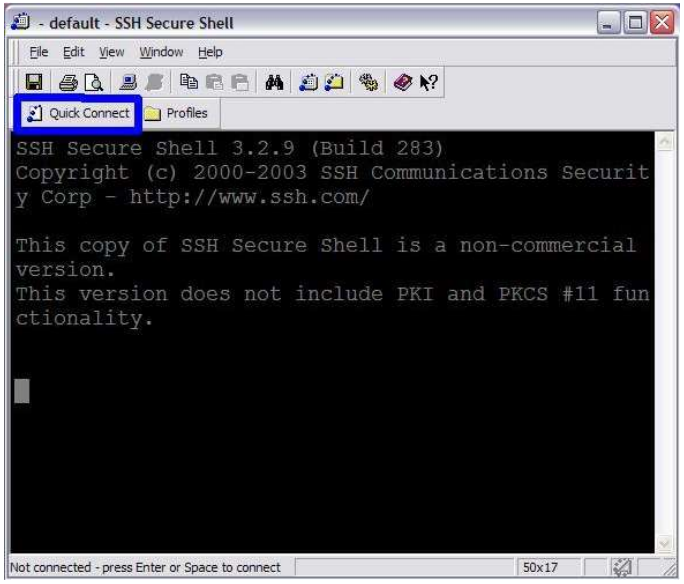
- Đăng nhập và làm việc từ xa
- Dùng cổng 23 TCP
- Cơ chế dòng lệnh
- Là giao thức không an toàn vì dữ liệu truyền đi trên mạng không được mã hóa (plaintext)

- Nên khóa dịch vụ Telnet từ bên ngoài mạng vào.
- Chuyển sang dùng SSH

Truy cập từ xa

- Secure Shell (SSH)

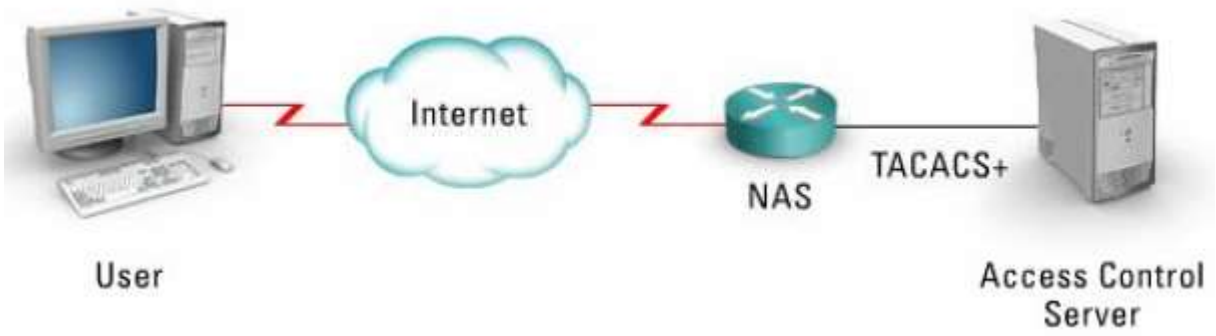




- Thiết lập kết nối mạng 1 cách bảo mật.
- Cổng 22
- Làm việc qua 3 bước:
  + Định danh host: sử dụng cặp khóa công cộng và khóa bí mật.
  + Mã hóa: DES, 3DES, IDEA,Blowfish
  + Chứng thực: RSA, DSA

Truy cập từ xa

- TACACS+



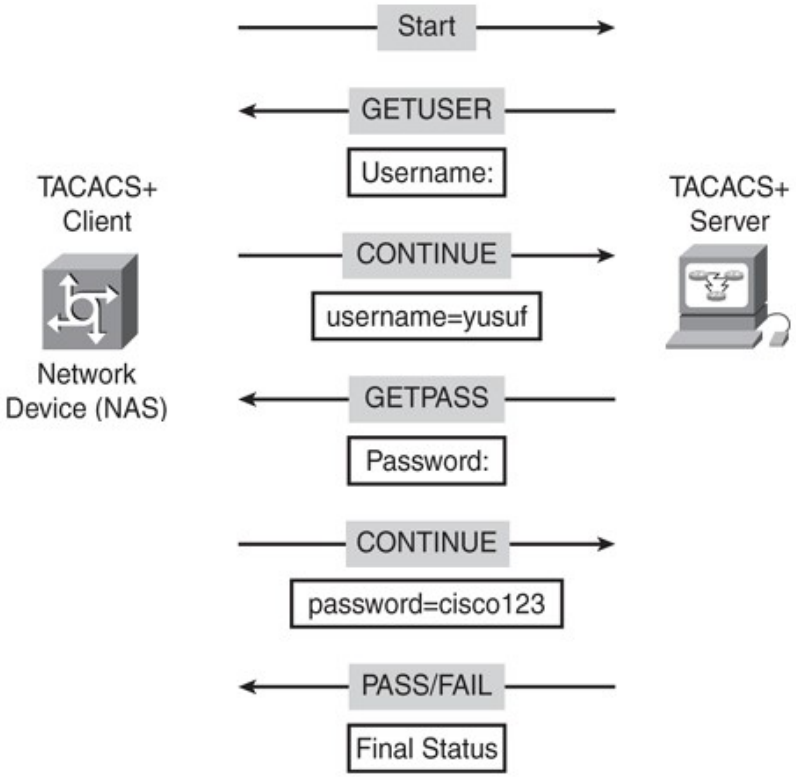
Terminal Access Control Access Control System Plus
- Chứng thực tập trung
- Thích hợp cho các mạng với số lượng người dùng lớn
- Cung cấp riêng rẻ các dịch vụ AAA

- Giao thức riêng của Cisco
- Sử dụng TCP cổng 49
- Hỗ trợ nhiều giao thức tầng 3 như IP, Apple Talk
- Cung cấp khả năng bảo mật trong trao đổi dữ liệu giữa gateway (Router - NAS) và cơ sở dữ liệu trung tâm (ACS).
- **Mã hóa thông tin toàn bộ phiên giao dịch**.
- Dùng 1 khóa bí mật để mã hóa và giải mã trên cả 2 hệ thống.

Điểm yếu
- Có thể bị tấn công vào phần mã hóa vì chỉ dùng 1 khóa bí mật => nên thay đổi thường xuyên.
- Có thể bị tấn công theo dạng Replay.

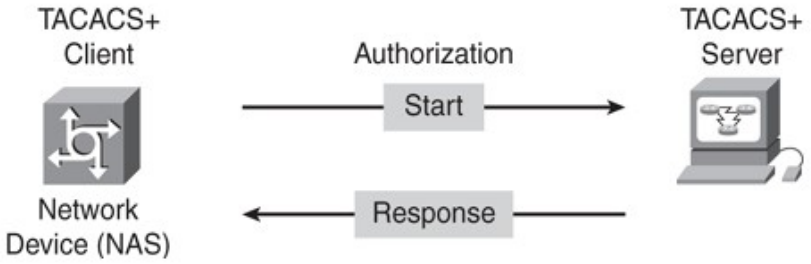
Truy cập từ xa

- TACACS+



Các bước chứng thực (authentication) dùng TACACS+

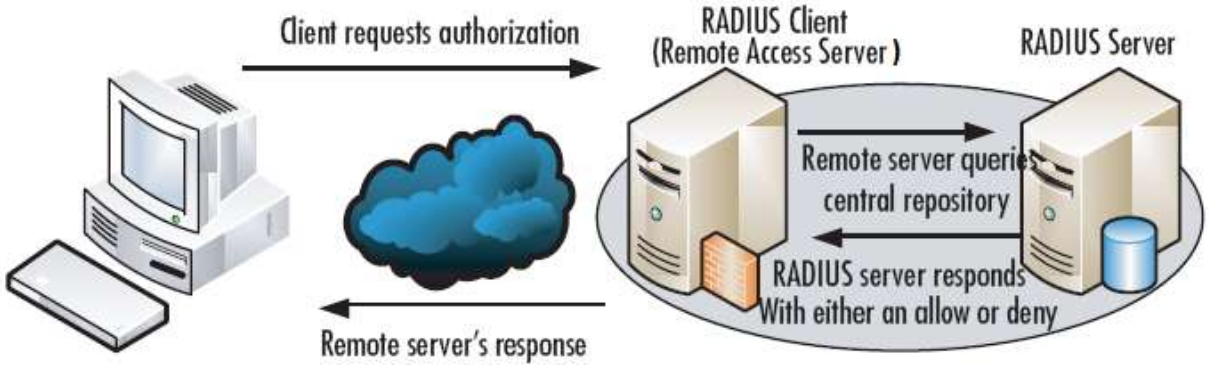
NAS: Router, Switch, PIX/ASA, VPN3000



Quá trình phân quyền (authorization) dùng TACACS+

Truy cập từ xa

- RADIUS

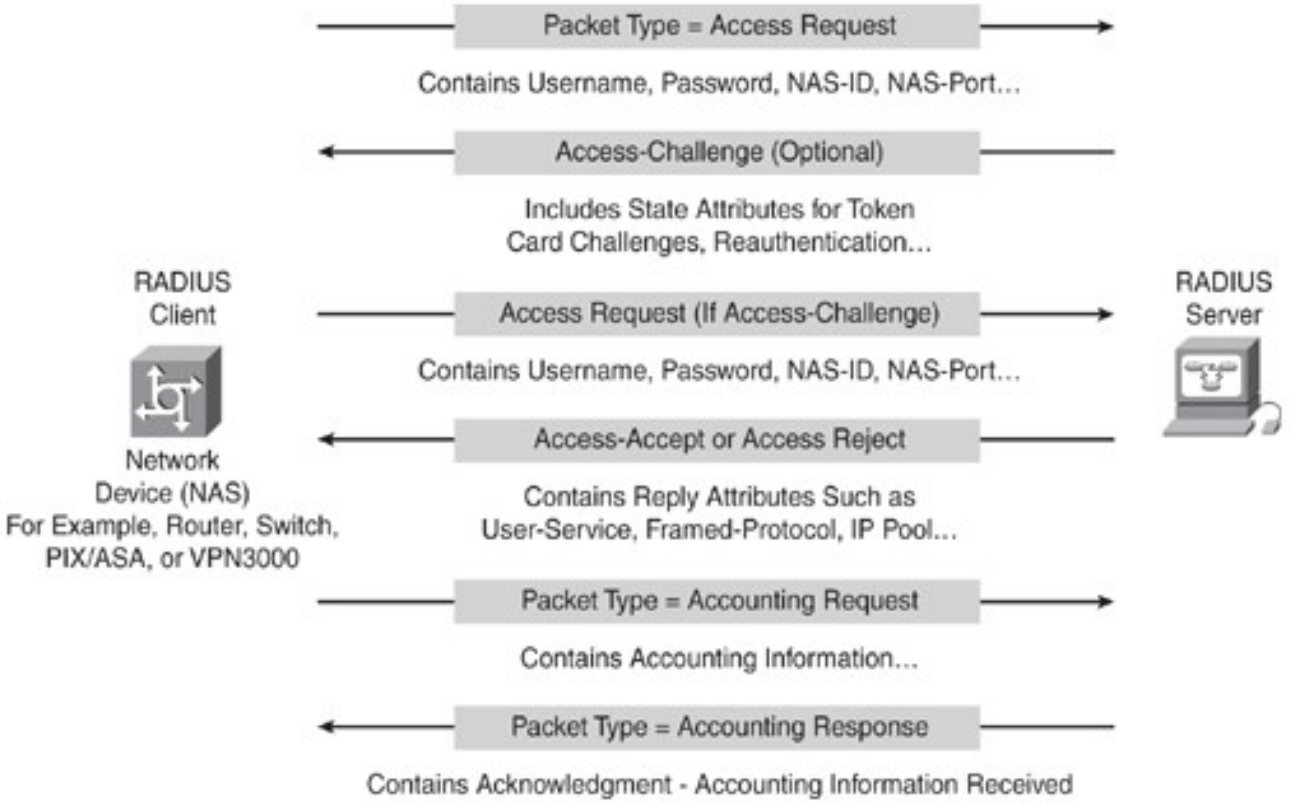


Remote Authentication Dial In User Service
- Tương tự như TACACS+, cung cấp dịch vụ AAA
- Chuẩn mở
- Định nghĩa trong RFC-2865

- Chuẩn chứng thực an toàn của 802.1X
- Sử dụng UDP cổng 1812
- Dùng mô hình Client-Server, trong đó RAS đóng vai trò là RADIUS Client.
- RADIUS **mã hóa mật khẩu và tên người dùng**.
- Hỗ trợ các giao thức: PPP, PAP, CHAP

Truy cập từ xa

- RADIUS



Kết hợp chứng thực và phân quyền dùng RADIUS

Mạng không dây - WLAN

- Khái niệm

• Cung cấp tính tiện lợi trong kết nối mạng: dễ dàng, mềm dẻo, nhanh chóng, tốc độ cao.
• Cung cấp khả năng di động trong mạng LAN
• Sử dụng phương pháp CSMA/CA

Mạng không dây - WLAN

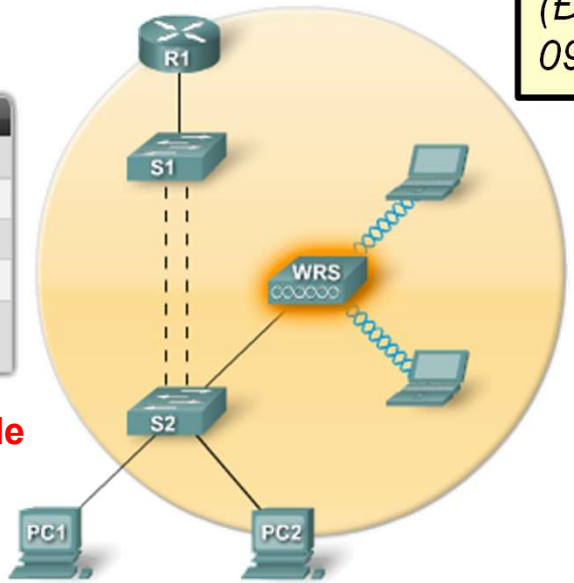
- Các chuẩn

- Chuẩn hóa trong IEEE 802.11
- Gồm các chuẩn mạng :
  + 802.11 A: sử dụng tại Mỹ; 54 Mbps
  + 802.11 B: 11 Mbps
  + 802.11 G: 54 Mbps
  + 802.11 N: ~300 Mbps

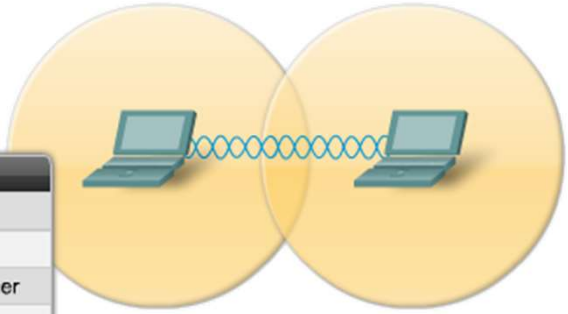
(Đã được công nhận chuẩn quốc tế 09/2009)

APs	One
Topology	BSS
Connection	Client to AP
Mode	Infrastructure
Coverage	Basic Service Area (BSA)

Infrastructure mode



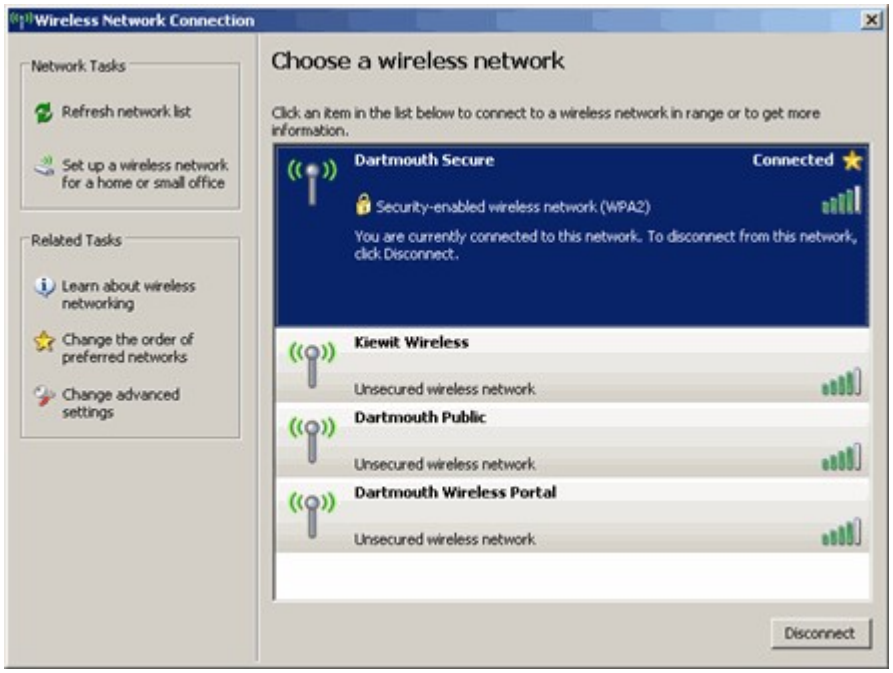
Ad hoc mode

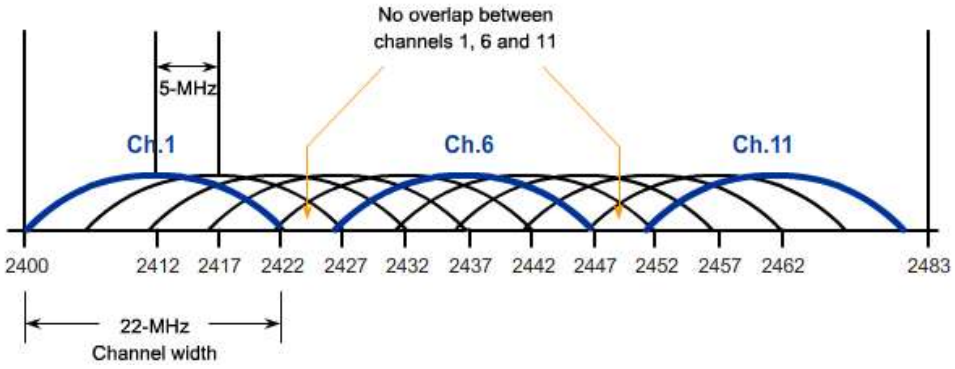


APs	None
Topology	IBSS
Connection	Peer-to-Peer
Mode	Ad hoc
Coverage	Basic Service Area (BSA)

Mạng không dây - WLAN

- Các thông số

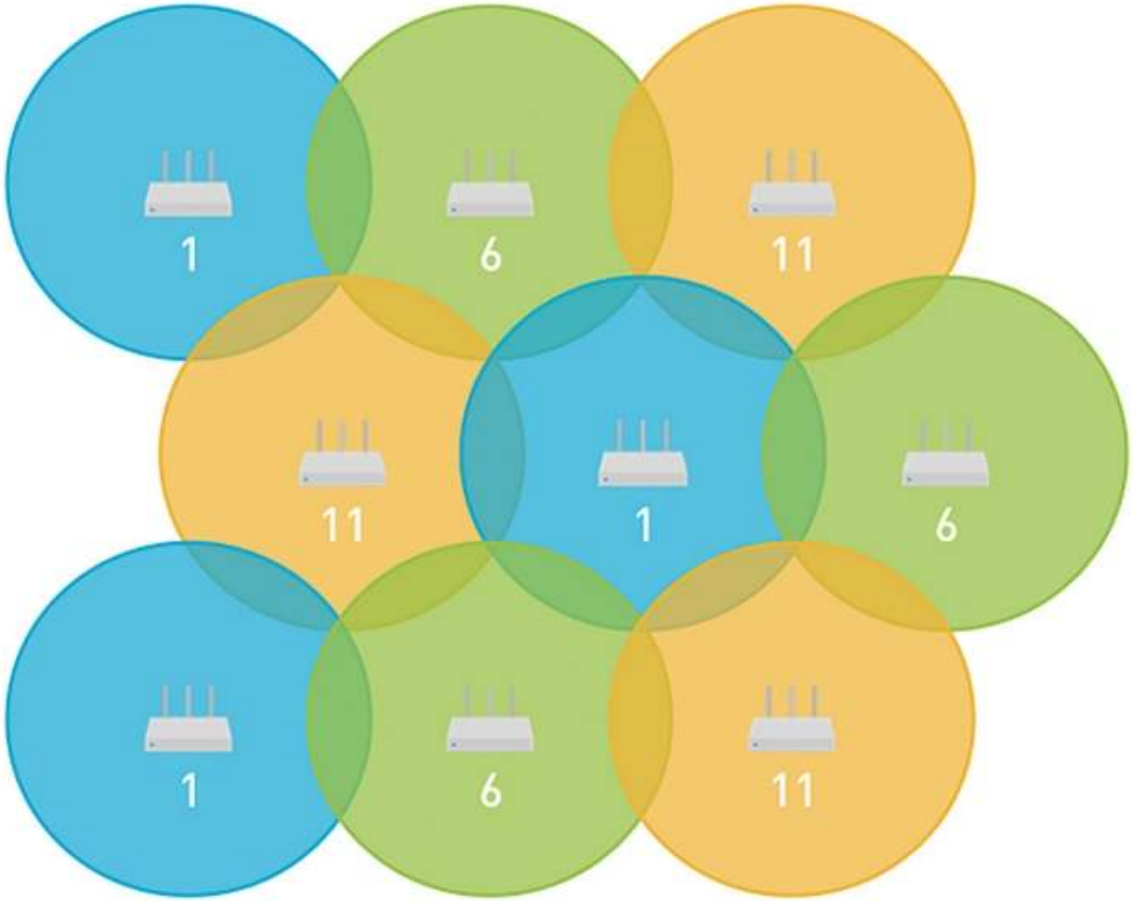




- SSID: định danh của mạng WLAN
- Chiều dài từ 2 – 32 ký tự
- Không đặt trùng nhau trong cùng 1 phạm vi hoạt động

- Chia kênh để không bị nhiễu.
- Mỗi kênh cách nhau 22 MHz
- Bắc Mỹ: chia 11 kênh
- Châu Âu: chia 13 kênh
- Trong cùng phạm vi, nên chọn cách nhau 5 kênh:
  + 3 AP: chọn 1, 6, 11
  + 2 AP: chọn 5, 10 / 4, 9 / 3, 8 / 2, 7

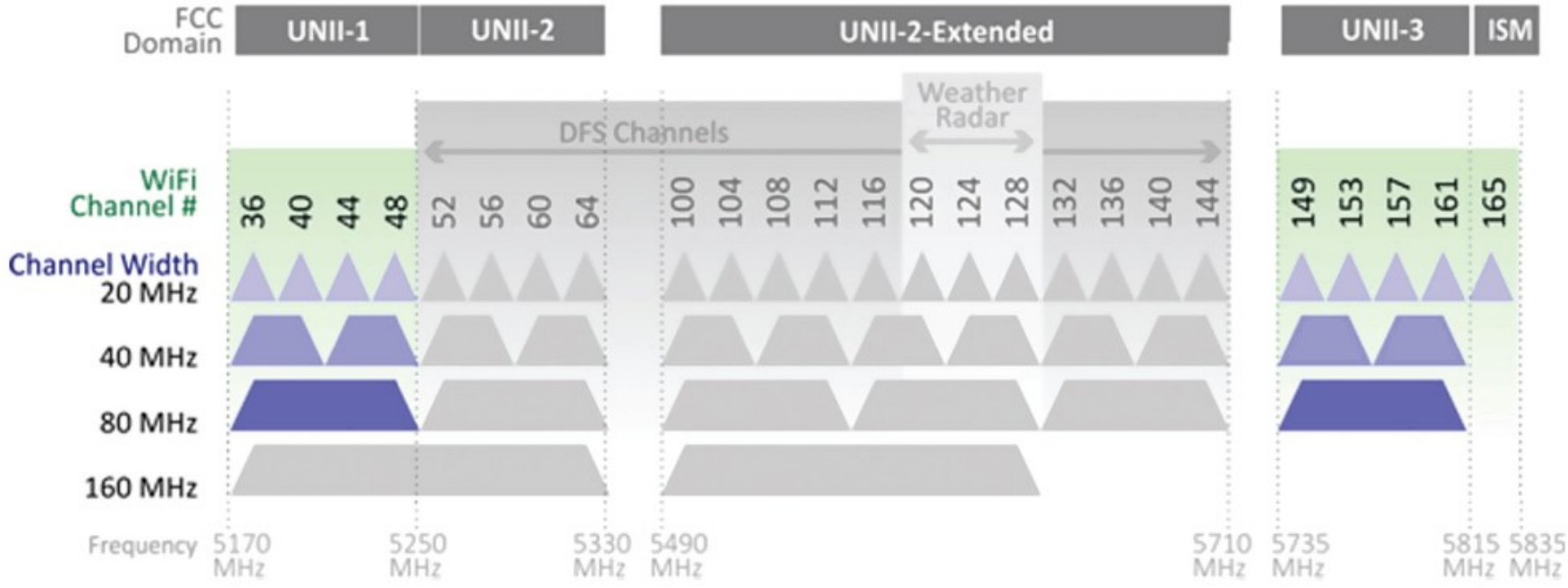
Mạng không dây - WLAN



Nguồn: http://www.pcworld.com.vn

Mạng không dây - WLAN

Phân bố kênh 802.11ac ngoại trừ DFS (khu vực Bắc Mỹ)



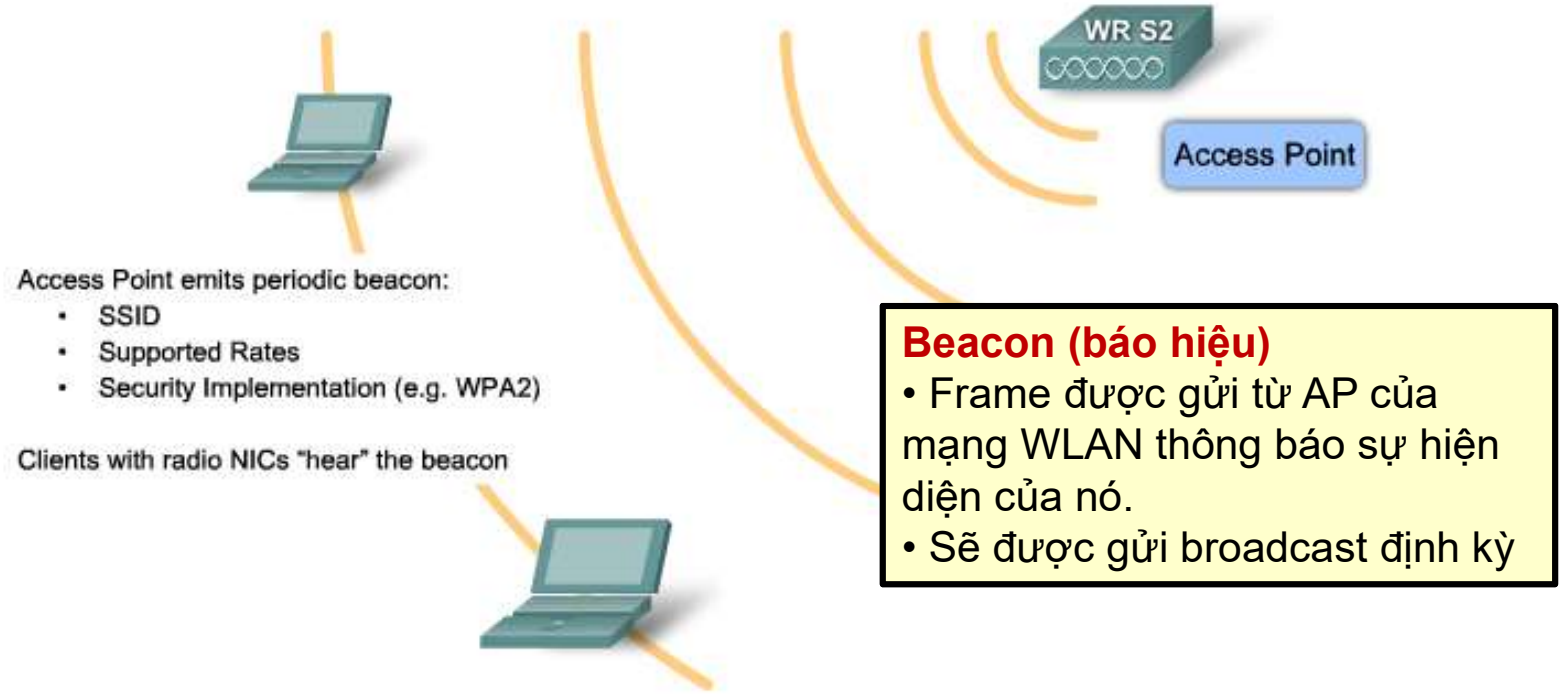
Nguồn: http://www.pcworld.com.vn

- DFS (dynamic frequency selection)

25/02/2017 Bộ môn MMT&TT 16

Mạng không dây - WLAN

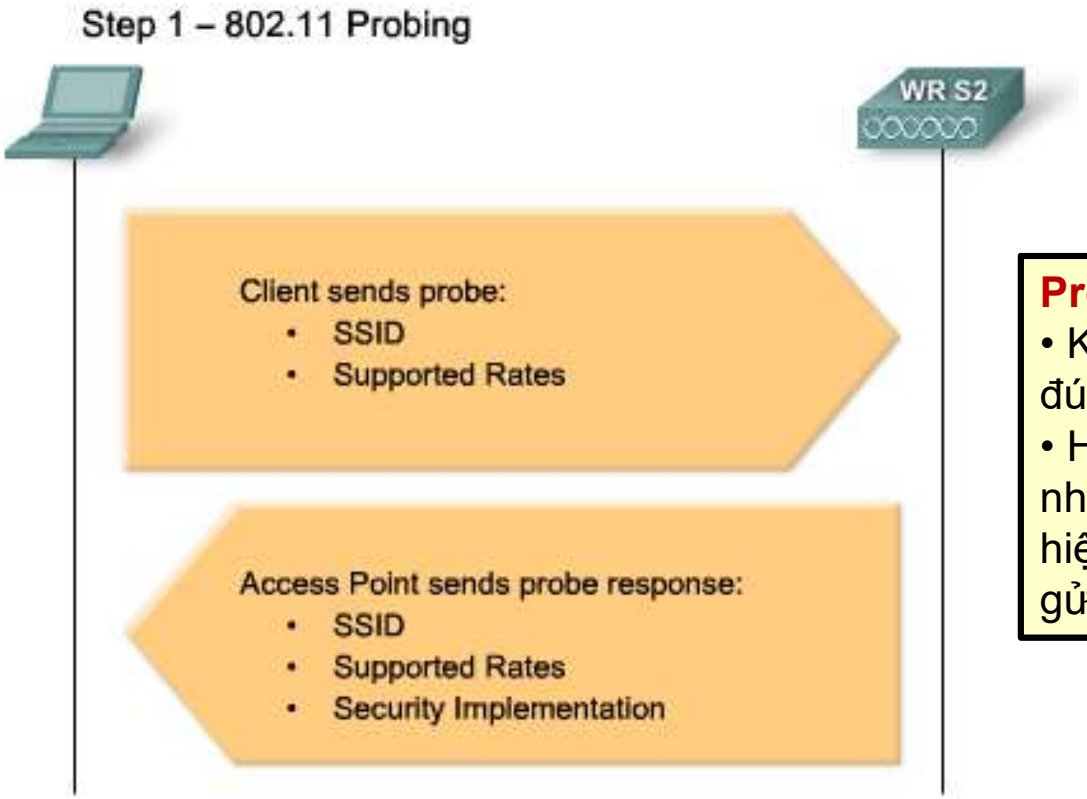
- Hoạt động (1)



Beacon (báo hiệu)
• Frame được gửi từ AP của mạng WLAN thông báo sự hiện diện của nó.
• Sẽ được gửi broadcast định kỳ

Mạng không dây - WLAN

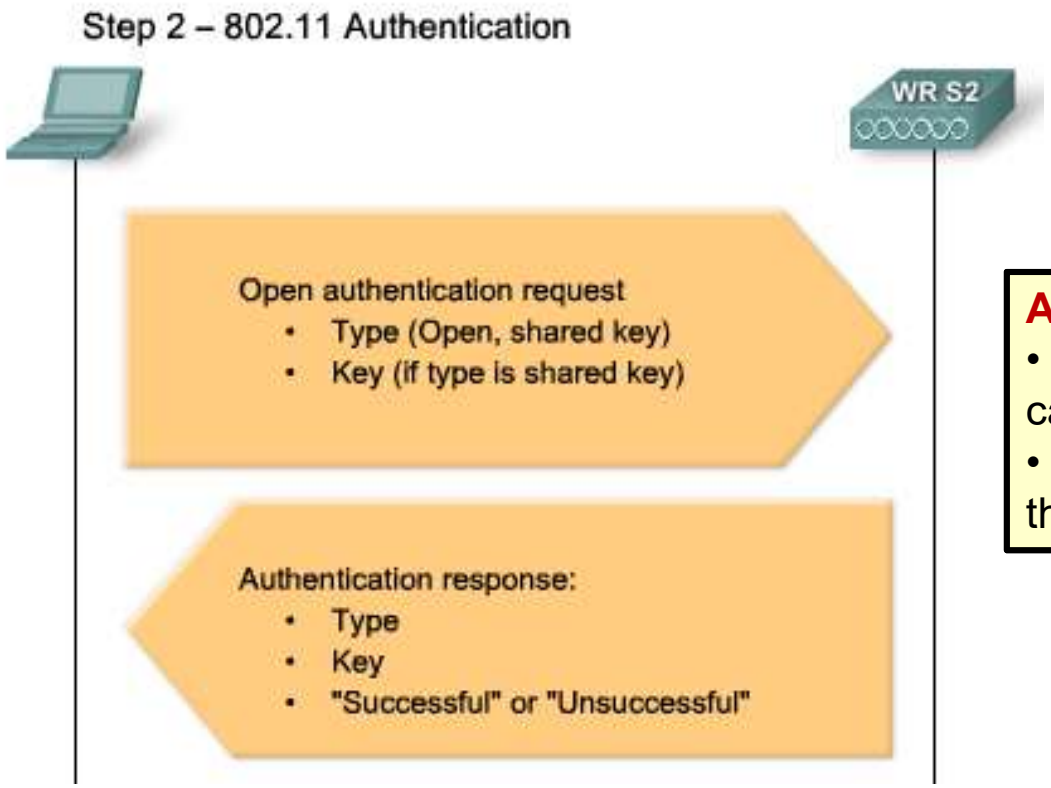
- Hoạt động (2)



Probing (thăm dò)
• Kiểm tra xem có mạng WLAN đúng với SSID cho trước không
• Hoặc dò tìm (liệt kê các SSID) những mạng WLAN nào đang hiện diện trong vùng bằng cách gửi Request không có SSID.

Mạng không dây - WLAN

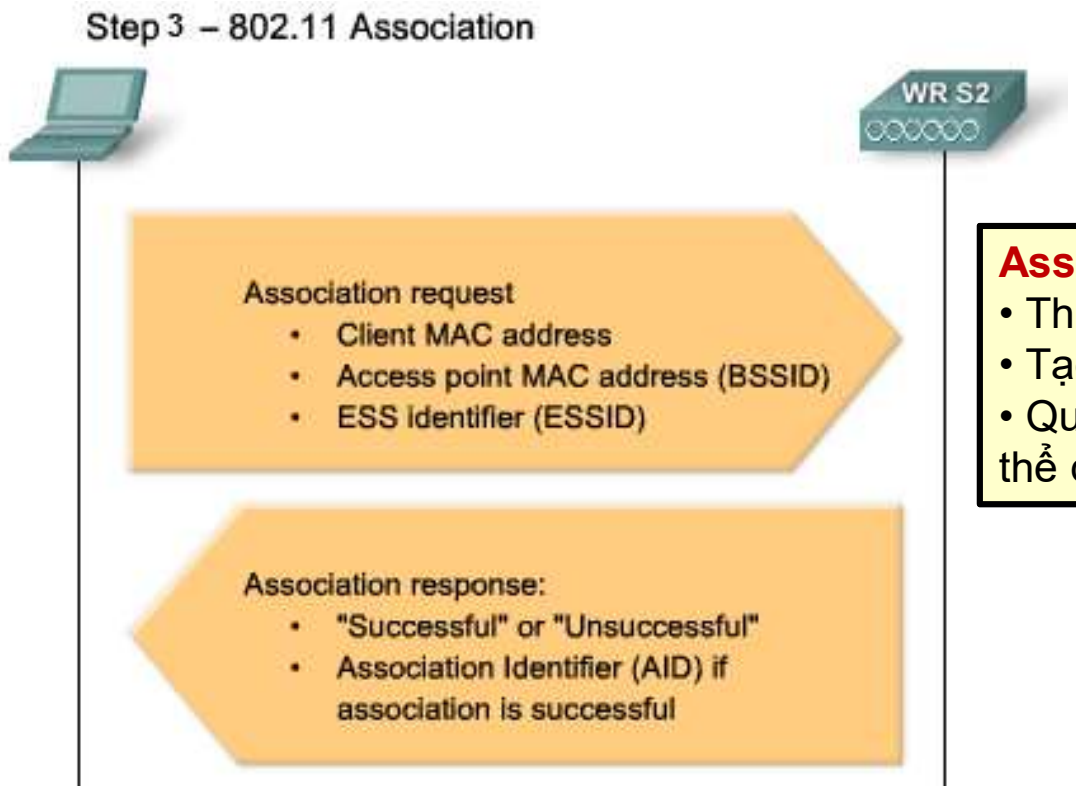
- Hoạt động (3)



Authentication (chứng thực)
• Nếu là dạng mở Open thì không cần key.
• Nếu có mã hóa (chẳng hạn WEP) thì cần Key

Mạng không dây - WLAN

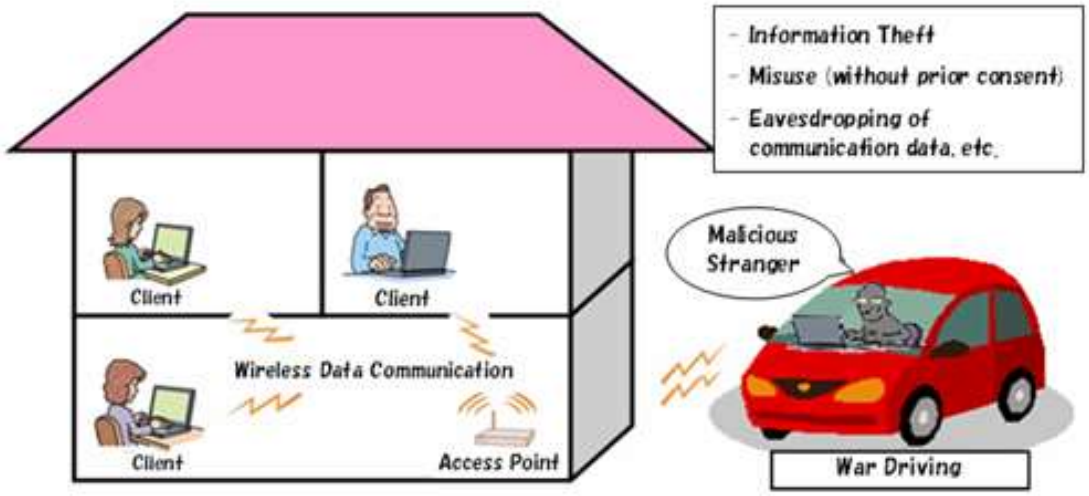
- Hoạt động (4)



Association (kết hợp)
• Thiết lập nối kết ở tầng 2
• Tạo ra 1 port ảo nối kết đến Client
• Quá trình gửi và nhận dữ liệu có thể diễn ra.

Mạng không dây - WLAN

- Nguy cơ từ mạng không dây



War driving
- Dò tìm các mạng WLAN mở (Open)
- Sử dụng Internet miễn phí
- Xâm nhập vào mạng dễ dàng

Hacker
- Tấn công vào các mạng WLAN yếu (cấu hình không cẩn thận, không mã hóa hoặc mã hóa yếu).
- Khai thác mạng không dây để vào mạng LAN của tổ chức.

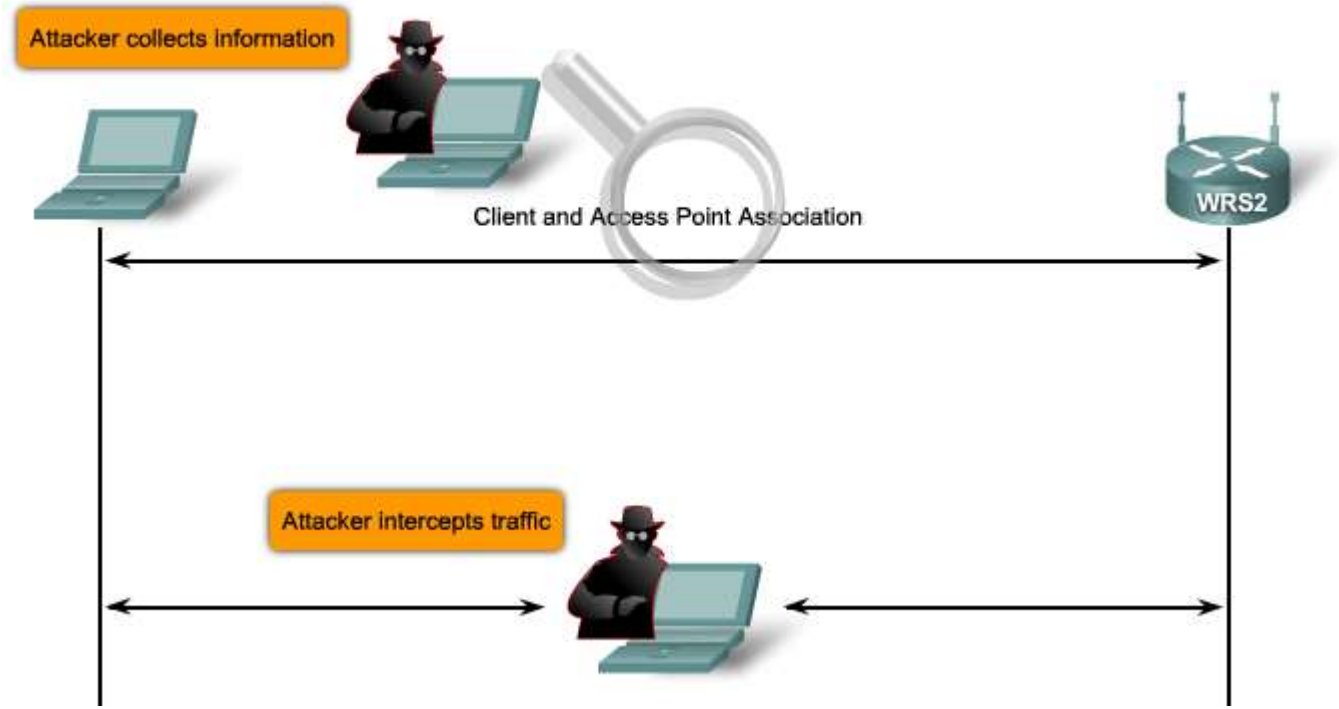
Nhân viên
- Nhân viên tự ý cắm 1 Access Point vào mạng

+ Tạo ra điểm có thể truy cập vào mạng từ bên ngoài.

+ Có thể gây nhiễu với các thiết bị WLAN đã có trong tổ chức.

Mạng không dây - WLAN

- Nguy cơ từ mạng không dây



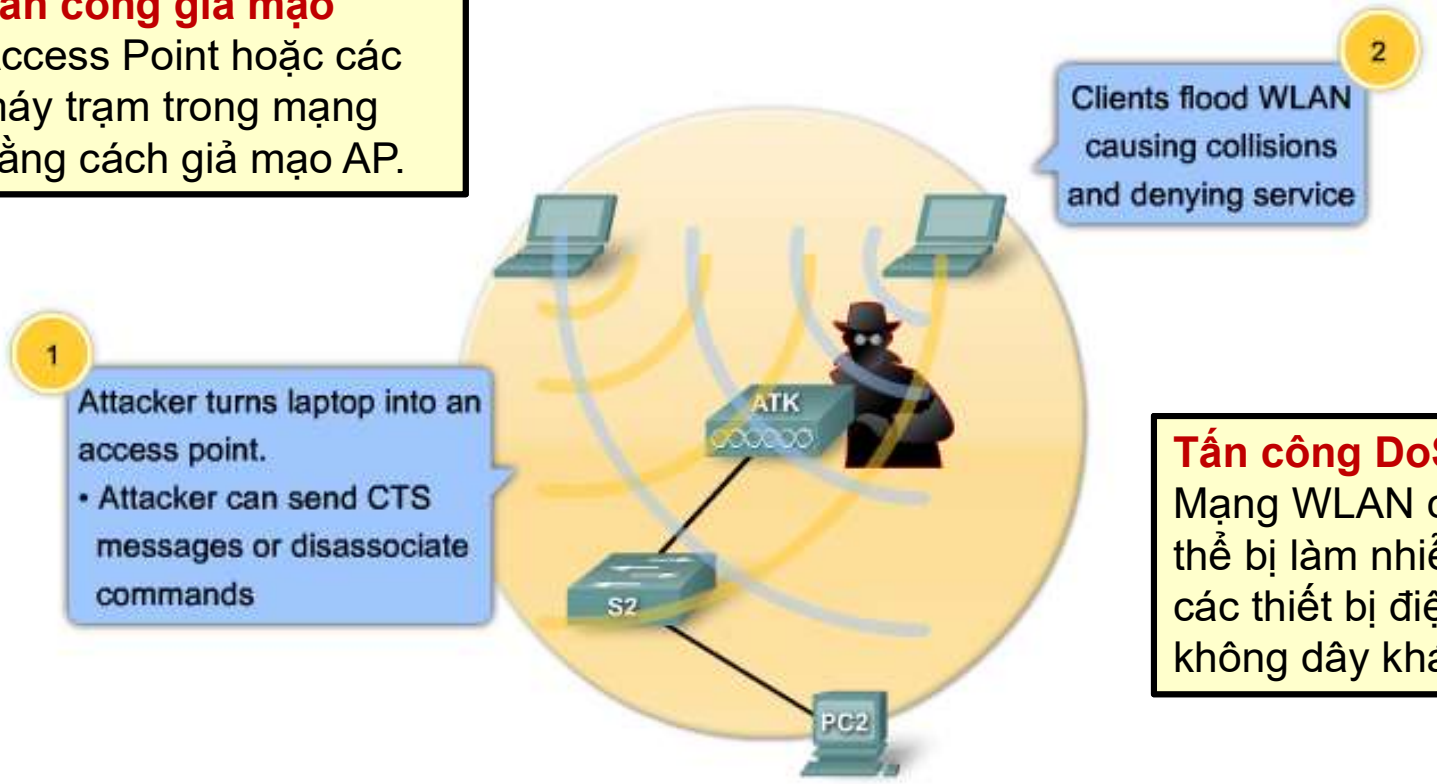
WLAN có nguy cơ bị tấn công dạng "Kẻ đứng giữa" (Man-in-the-middle – MITM) tại giai đoạn Association.

Giải pháp:
Cài đặt hệ thống ngăn chặn xâm nhập (Intrusion prevention system – IPS)

Mạng không dây - WLAN

- Nguy cơ từ mạng không dây

Tấn công giả mạo
Access Point hoặc các máy trạm trong mạng bằng cách giả mạo AP.

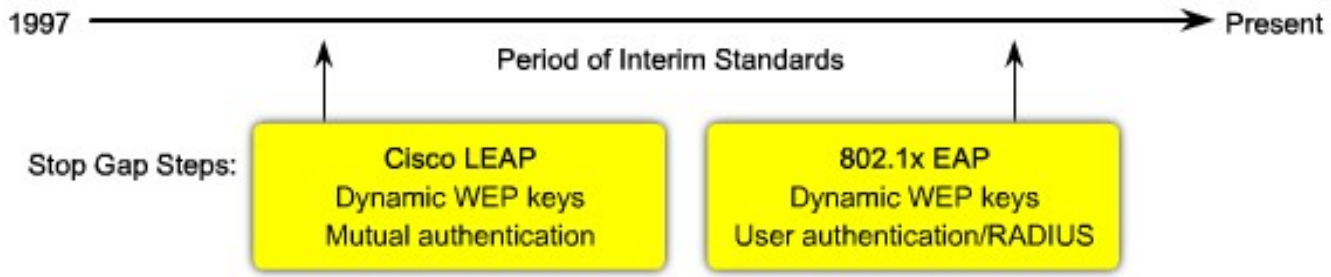


Tấn công DoS
Mạng WLAN cũng có thể bị làm nhiễu bởi các thiết bị điện tử hay không dây khác.

Mạng không dây - WLAN

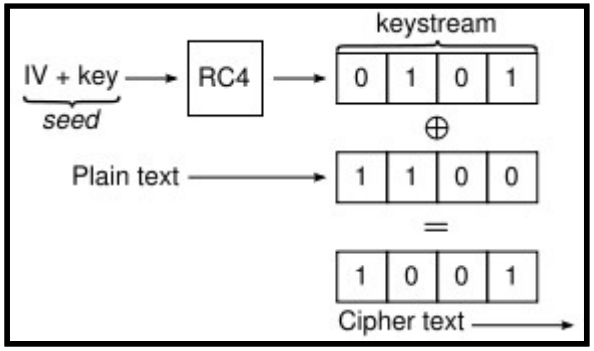
- Các giao thức an toàn cho mạng WLAN

Open	WEP	WPA	WPA2
• Không chứng thực • Không mã hóa • Không có cơ chế an toàn	• Chứng thực yếu • Khóa tĩnh, dễ bị tấn công và phát hiện • Mã hóa dễ bị phá vỡ • Không linh hoạt	• Chuẩn tạm thời • Mã hóa cao • Chứng thực mạnh: LEAP, PEAP, EAP-FAST, …	• Chuẩn hiện tại • 802.11i • Mã hóa AES • Quản lý khóa động



Mạng không dây - WLAN

- WEP (Wired Equivalent Privacy)

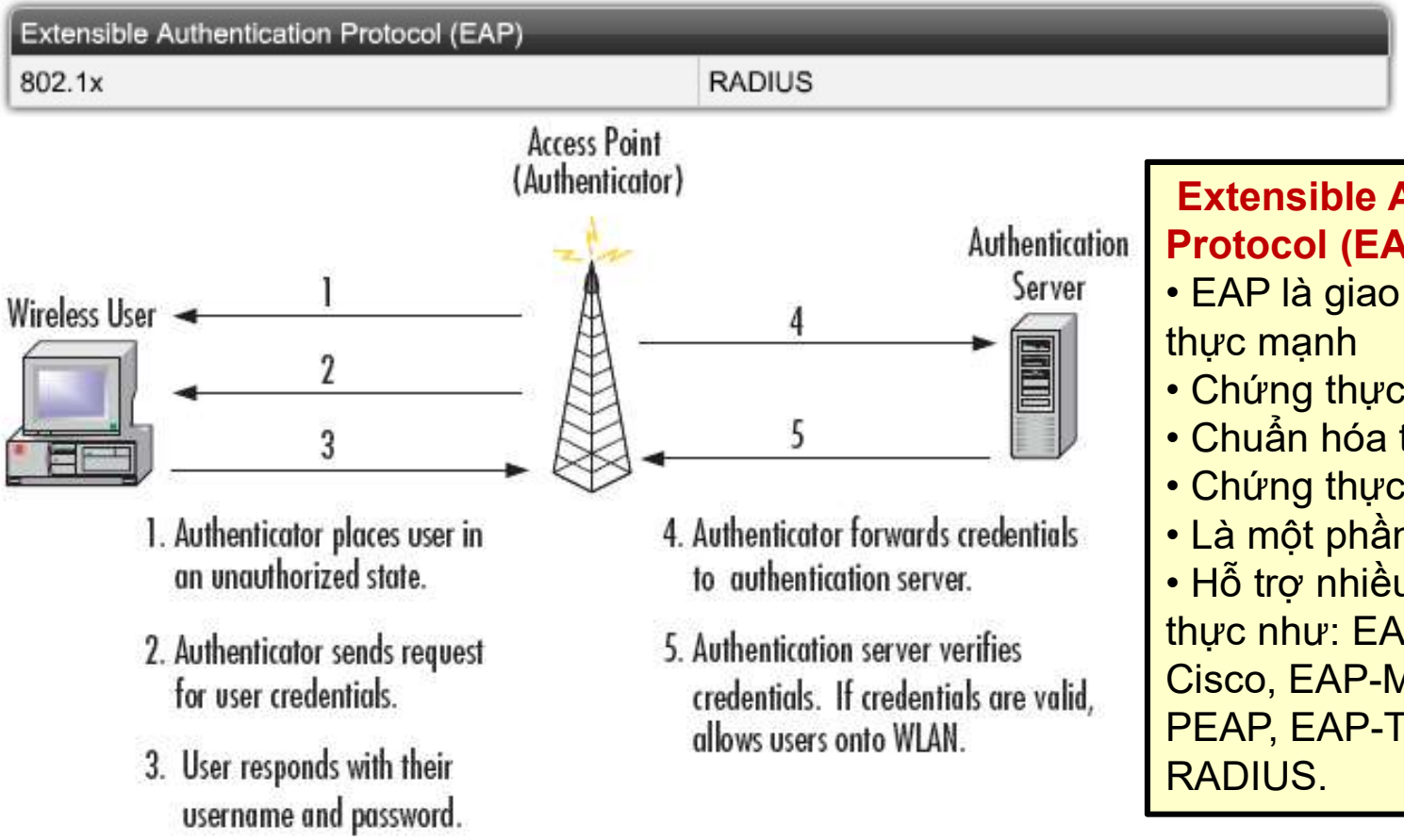


- Sử dụng khóa chia sẻ.
- Thường dùng khóa 64 bits hay 128 bits.
- Mã hóa dùng thuật toán RC4
- WEP có lỗ hổng bảo mật dễ bị khai thác
- Một số công cụ dùng để tấn công WEP như: AirSnort, NetStumbler, WEPCrack, ...

Cài đặt hệ thống phát hiện xâm nhập (IDS) hay hệ thống ngăn chặn xâm nhập (IPS)

Mạng không dây - WLAN

- Các giao thức chứng thực trong mạng WLAN

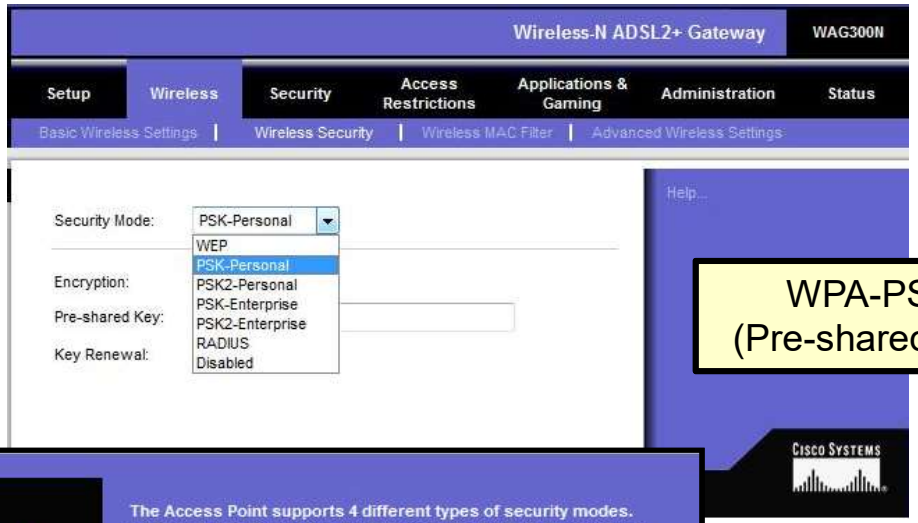


Extensible Authentication Protocol (EAP)

- EAP là giao thức chứng thực mạnh
- Chứng thực qua Server.
- Chuẩn hóa trong RFC 3748
- Chứng thực ở tầng 2
- Là một phần của PPP.
- Hỗ trợ nhiều cơ chế chứng thực như: EAP over IP, LEAP Cisco, EAP-MD5-CHAP, PEAP, EAP-TLS, EAP-TTLS, RADIUS.

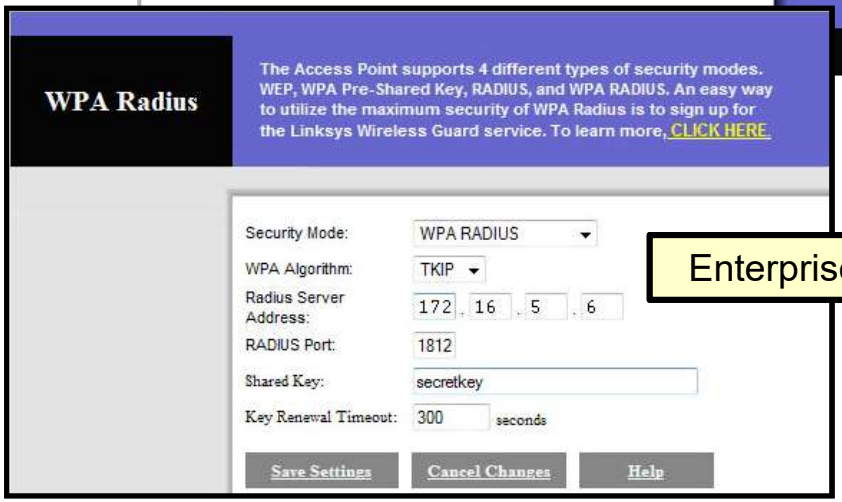
Mạng không dây - WLAN

- WPA và WPA2 (WiFi Protected Access)



WPA-PSK
(Pre-shared key)

- Thay thế cho WEP
- Chứng thực không cần Server
- Passphrase được lưu trên Access Point và trên máy cục bộ



Enterprise mode

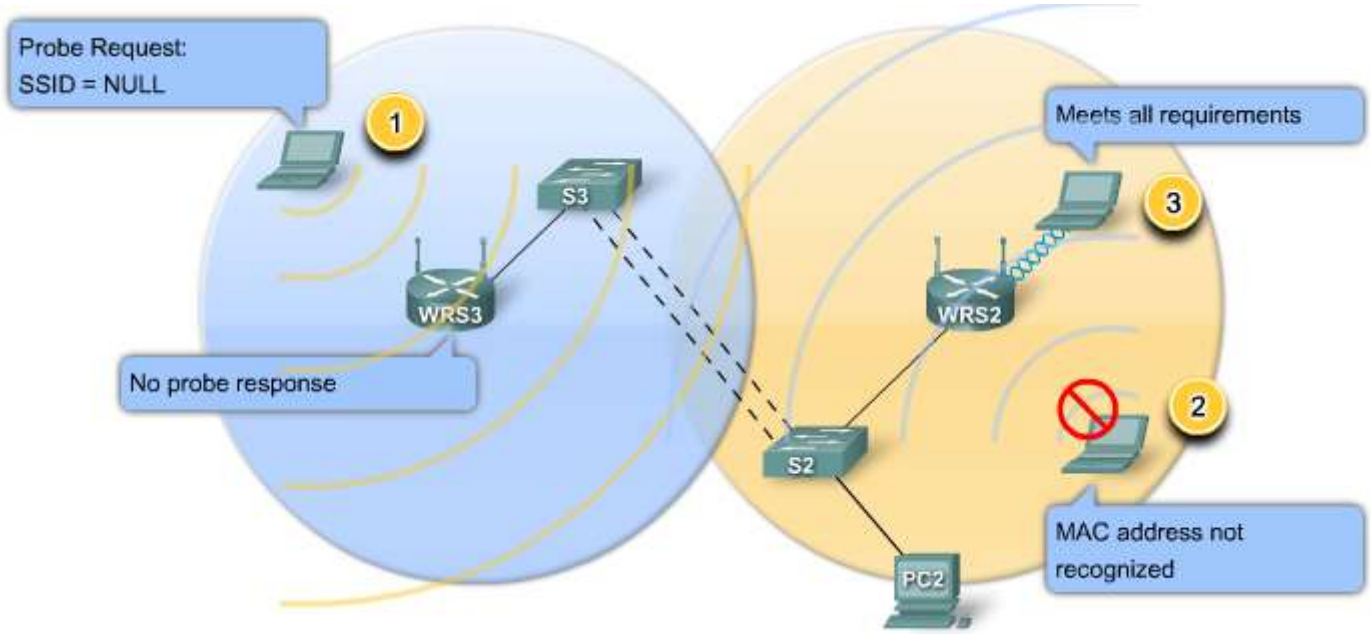
- Chứng thực qua 802.1X Auth. Server
- Mã hóa:

+ TKIP (Temporal Key Integrity Protocol) như WEP nhưng phức tạp hơn.
+ AES (Advanced Encryption Standard) như TKIP nhưng có bổ sung các tính năng để nâng cao tính bảo mật.

- WPA2 dùng mã hóa AES.

Mạng không dây - WLAN

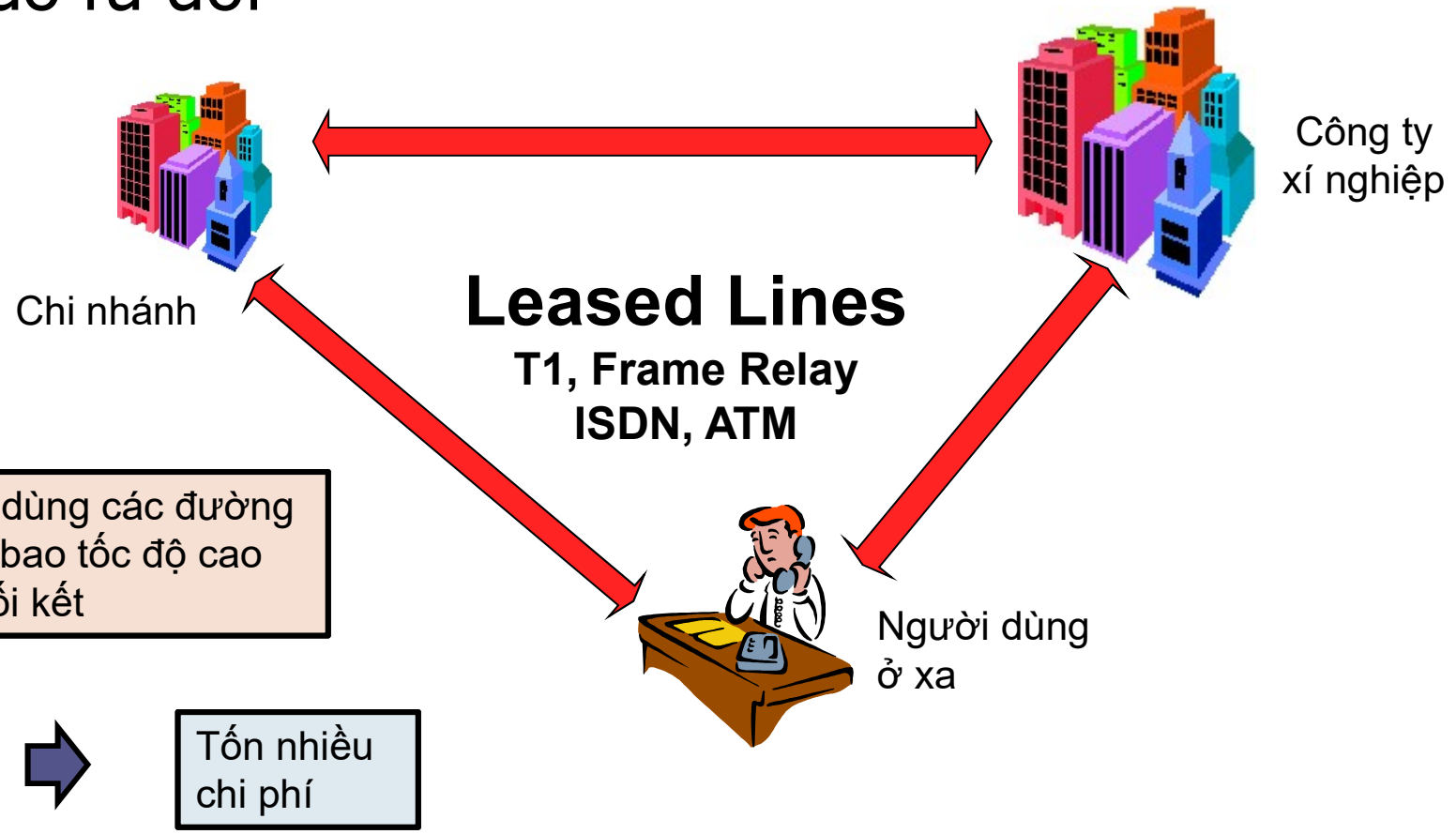
- Nâng cao tính an toàn của mạng WLAN



1. Ẩn (hidden) SSID
2. Chọn WPA hoặc WPA2 cho chứng thực và mã hóa
3. Lọc các máy trạm dựa theo địa chỉ MAC

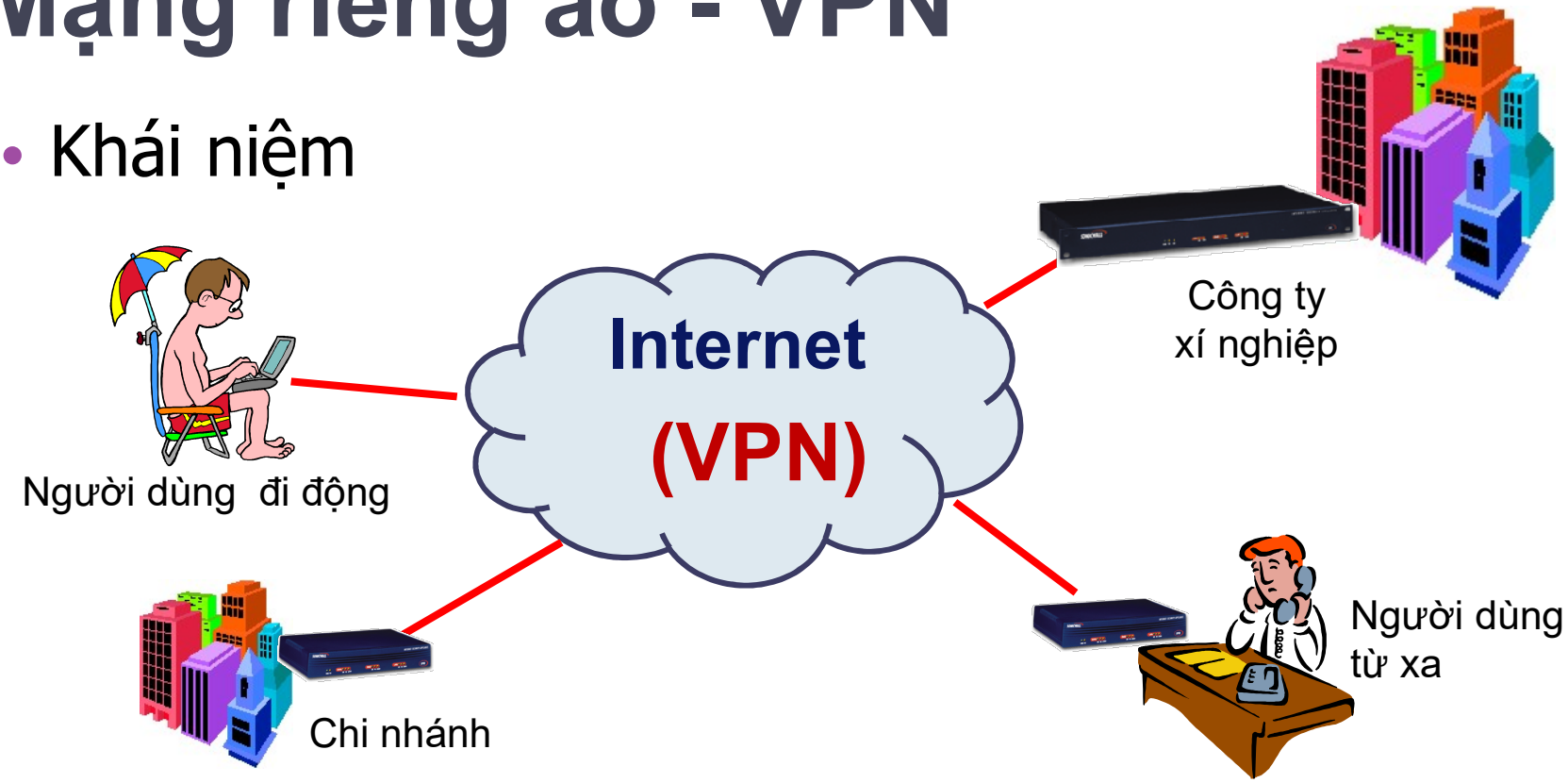
Mạng riêng ảo - VPN

- Lý do ra đời



Mạng riêng ảo - VPN

- Khái niệm

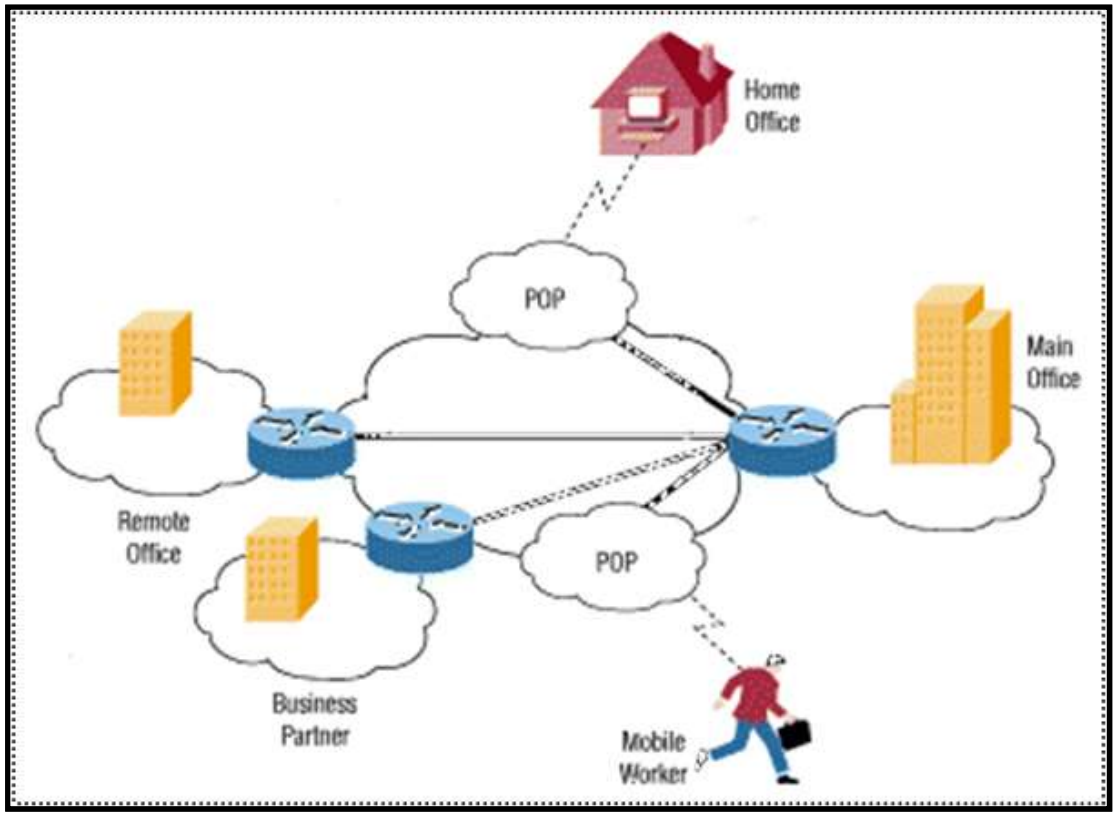


VPN = Virtual Private Network

- **Virtual**: ảo (không có đường nối kết thực giữa 2 thực thể)
- **Private**: riêng (được bảo vệ, không truy xuất được từ bên ngoài)
- **Network**: mạng máy tính (nhóm 2 hoặc nhiều máy tính lại với nhau)

Mạng riêng ảo - VPN

- Ích lợi



Sử dụng đường truyền công cộng không an toàn (Internet) để thực hiện việc trao đổi dữ liệu một cách an toàn.

• Phù hợp với các công ty có nhiều chi nhánh, nhân viên làm việc từ xa hoặc cần có các kết nối mạng an toàn với các đối tác.
• Chi phí thấp.

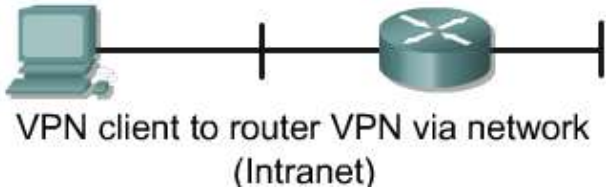
Mạng riêng ảo - VPN

- Phân loại

Site-to-Site VPN
(LAN-to-LAN)

VPN điểm nối điểm có thể được chia làm 2 loại:
• **Intranet VPN**: kết nối các chi nhánh, văn phòng ở xa với công ty, tổ chức.
• **Extranet VPN**: kết nối khách hàng, nhà cung cấp, đối tác với công ty.

Được xây dựng bằng cách sử dụng Router, Security Appliance hoặc VPN Concentrator.



VPN client to router VPN via network
(Intranet)

Router to router VPN gateway
(Extranet)

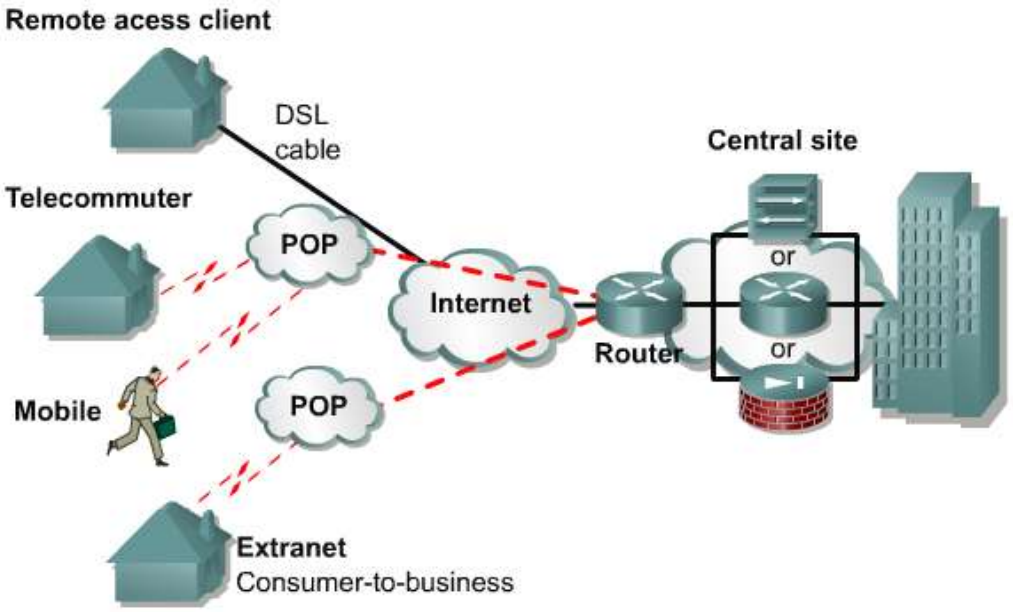
Other vendors to router VPN
Extranet

Router to VPN firewall gateway
(Extranet)

Mạng riêng ảo - VPN

- Phân loại

Remote Access VPN
(VPN truy cập từ xa)



- Còn gọi là Dialup riêng ảo
- Cung cấp cho người dùng ở xa, người dùng di động truy cập vào mạng công ty
- Chia làm 2 loại:

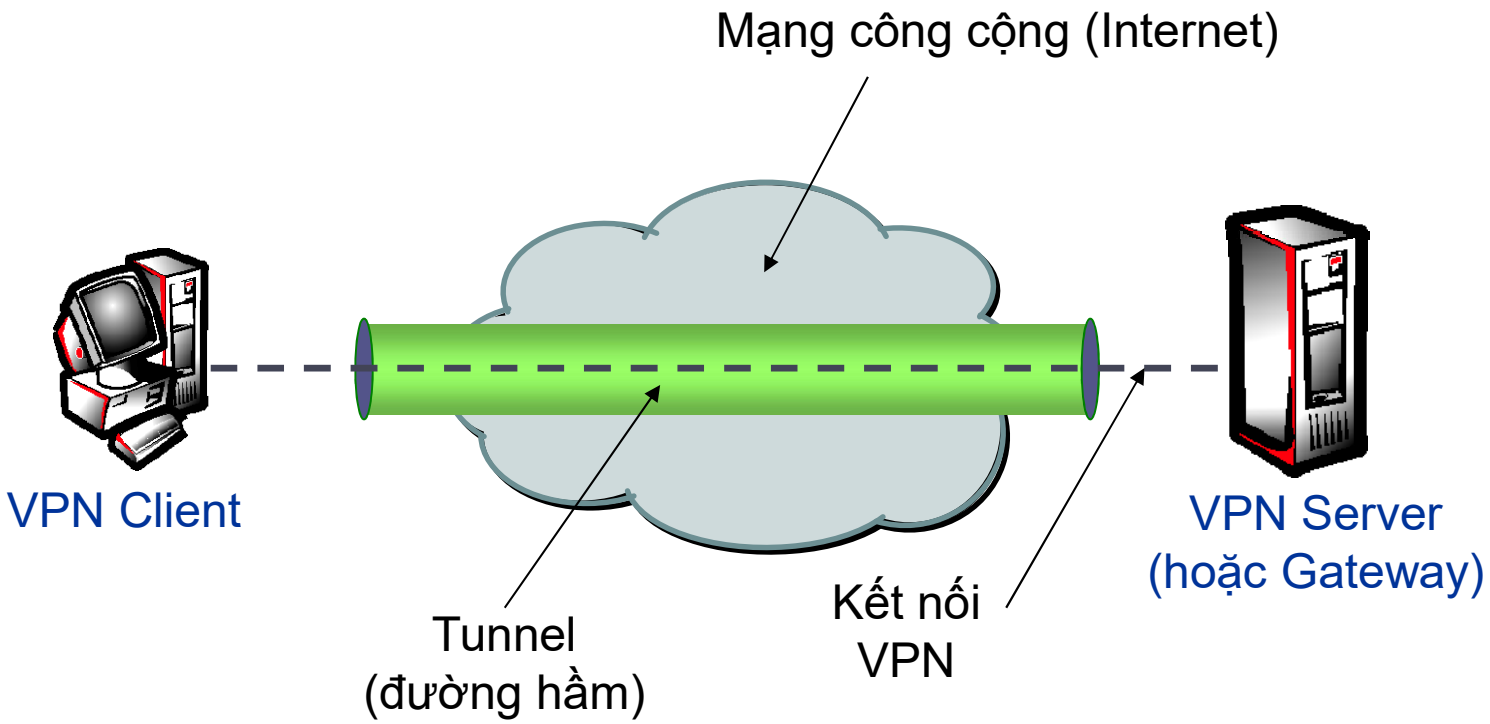
+ **Client-initiated**: người dùng sử dụng VPN Client hoặc trình duyệt Web để thiết lập nối kết.

+ **NAS-initiated**: người dùng dial (gọi) vào mạng của ISP. NAS sẽ thiết lập nối kết.

Client có thể sử dụng router, thiết bị phần cứng VPN hoặc phần mềm VPN.

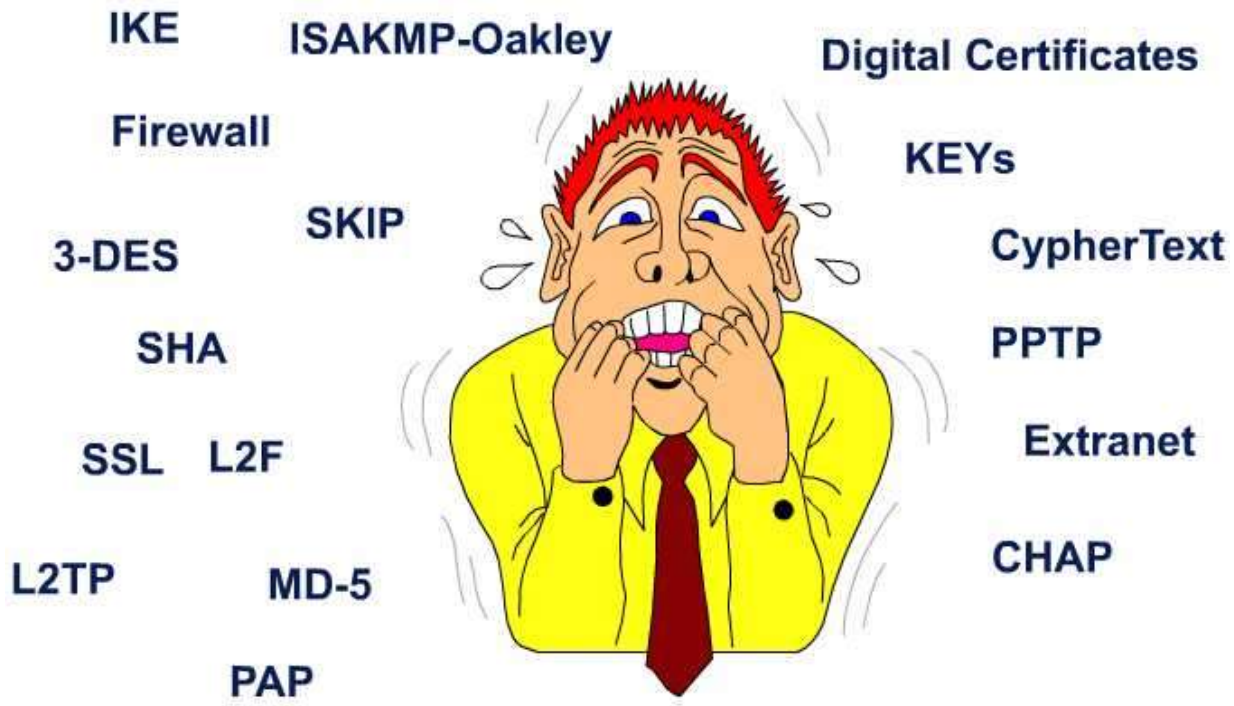
Mạng riêng ảo - VPN

- Các thành phần trong hệ thống VPN



Mạng riêng ảo - VPN

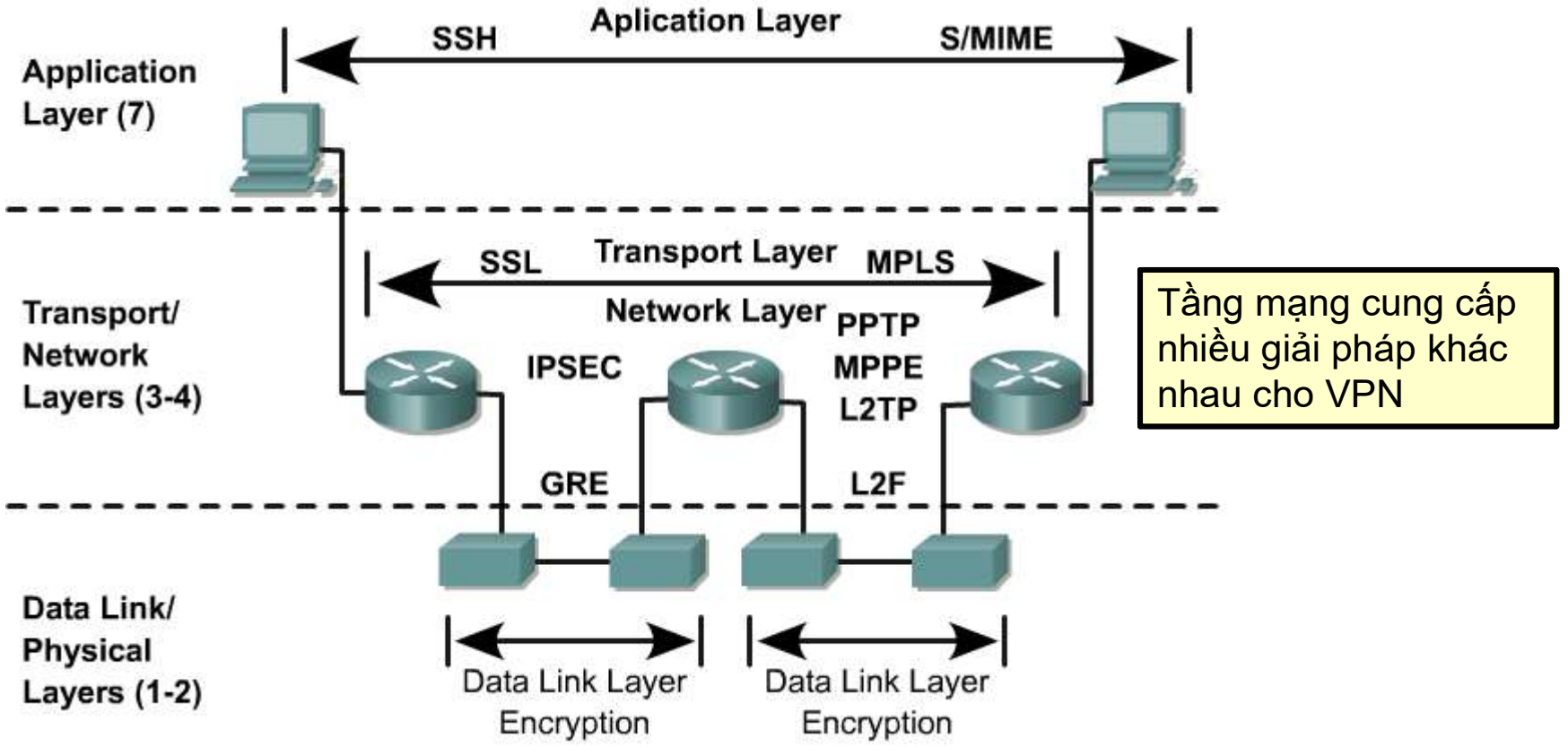
- Công nghệ VPN



Có khá nhiều công nghệ mạng VPN từ nhiều công ty và cài đặt trên nhiều tầng khác nhau.

Mạng riêng ảo - VPN

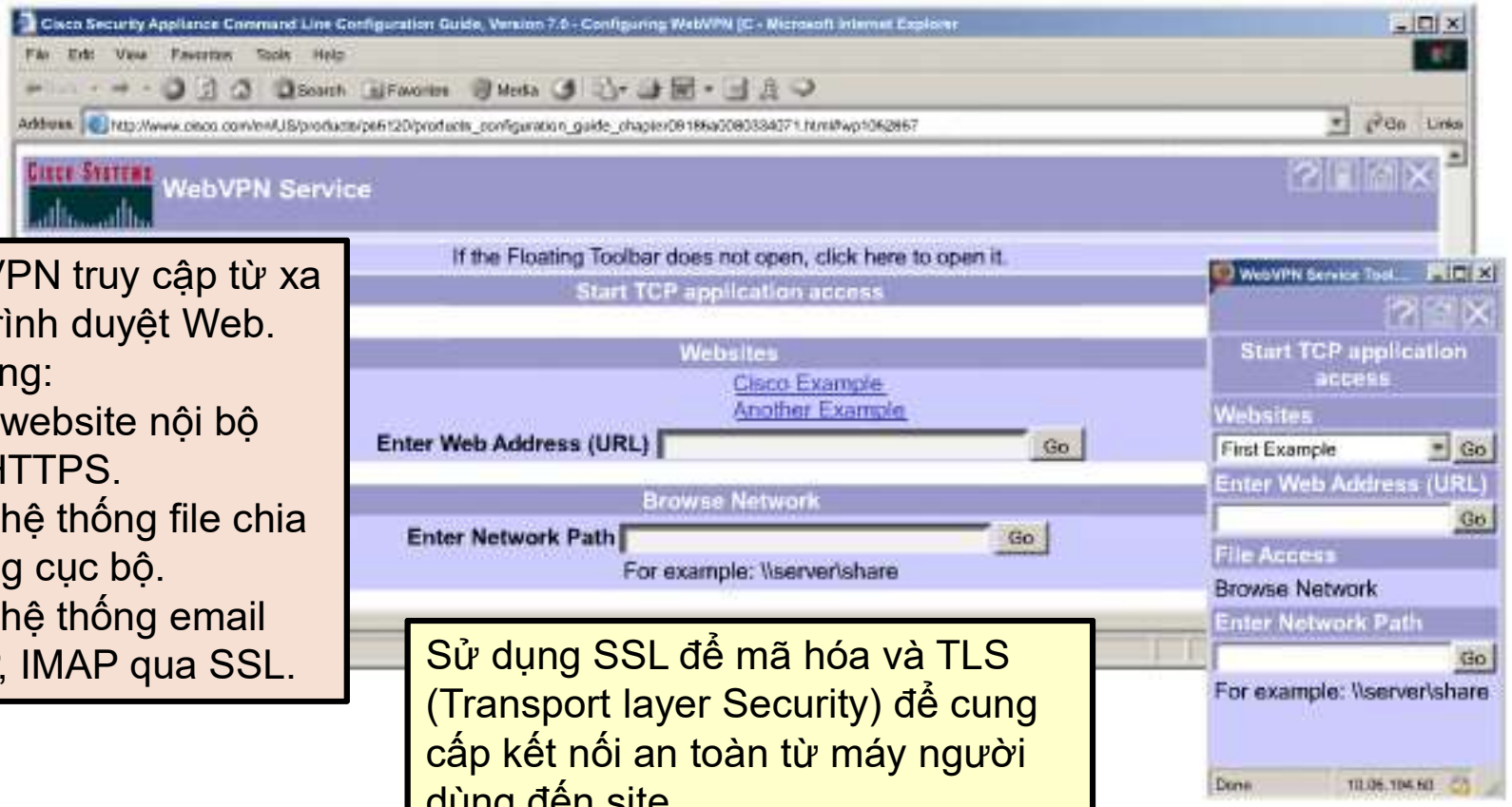
- VPN trên các lớp của mô hình OSI



Mạng riêng ảo - VPN

- Web VPN

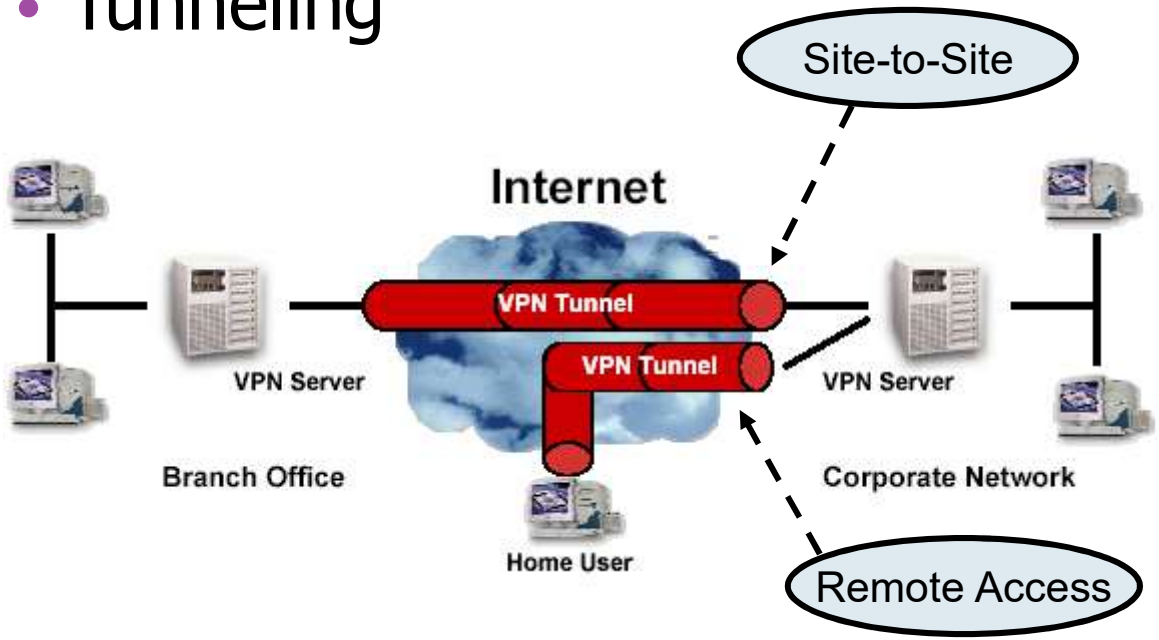
• Thiết lập VPN truy cập từ xa thông qua trình duyệt Web.
• Có khả năng:
+ Truy cập website nội bộ thông qua HTTPS.
+ Truy cập hệ thống file chia sẻ trên mạng cục bộ.
+ Truy cập hệ thống email POP, SMTP, IMAP qua SSL.



Sử dụng SSL để mã hóa và TLS (Transport layer Security) để cung cấp kết nối an toàn từ máy người dùng đến site.

Mạng riêng ảo - VPN

- Tunneling



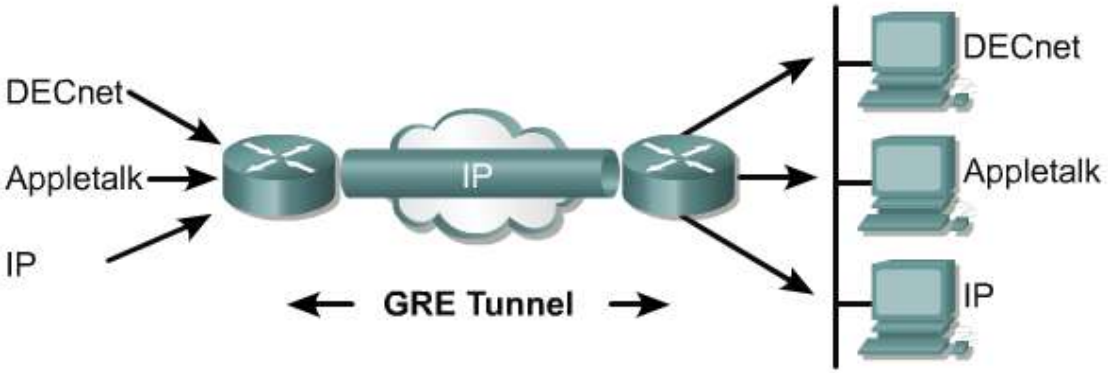
Các giao thức Tunneling (đường hầm) cung cấp tính bảo mật cho dữ liệu gửi và nhận bên trong.

Bao gói dữ liệu gốc vào 1 bên trong gói dữ liệu đã được mã hóa.

Mạng riêng ảo - VPN

- Các giao thức tạo đường hầm (Tunneling)

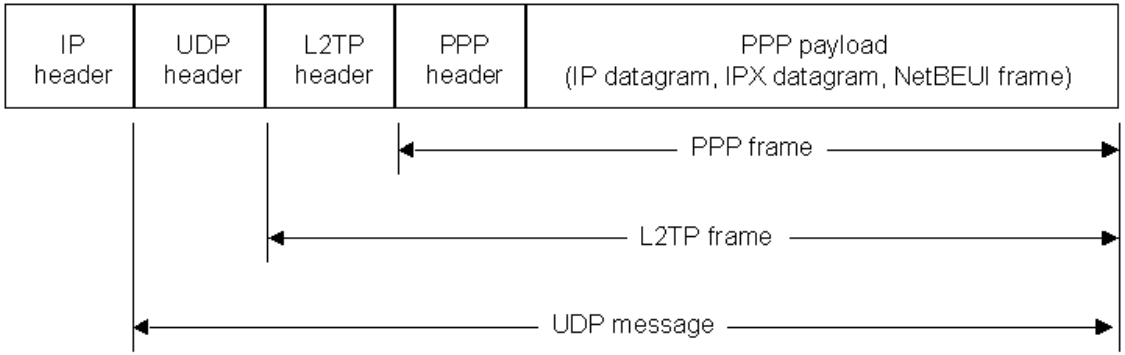
	Description	Standard
GRE	Generic Routing Encapsulation	RFC1701 and 2784
IPSec	Internet Protocol Security	RFC2401
L2F	Layer 2 Forwarding	Cisco
L2TP	Layer 2 Tunneling Protocol	RFC 2661
MPLS	Multiprotocol Label Switching	RFC 2547
PPTP	Point-To-Point Tunneling Protocol	Microsoft



• GRE hỗ trợ nhiều giao thức bên trong IP tunnel
• MPLS thích hợp cho ISP và các doanh nghiệp lớn.

Mạng riêng ảo - VPN

- L2TP/PPTP



L2TP và PPTP đều "bao gói" gói tin PPP truyền đi trong mạng IP.

PPTP
- Được Windows hỗ trợ
- Sử dụng cổng TCP 1723
- Chứng thực dùng MSCHAP-v2 hoặc EAP-TLS.
- Có thể dùng Microsoft Point-to-Point Encryption (MPPE) để mã hóa.
- Chỉ dùng cho giao thức IP

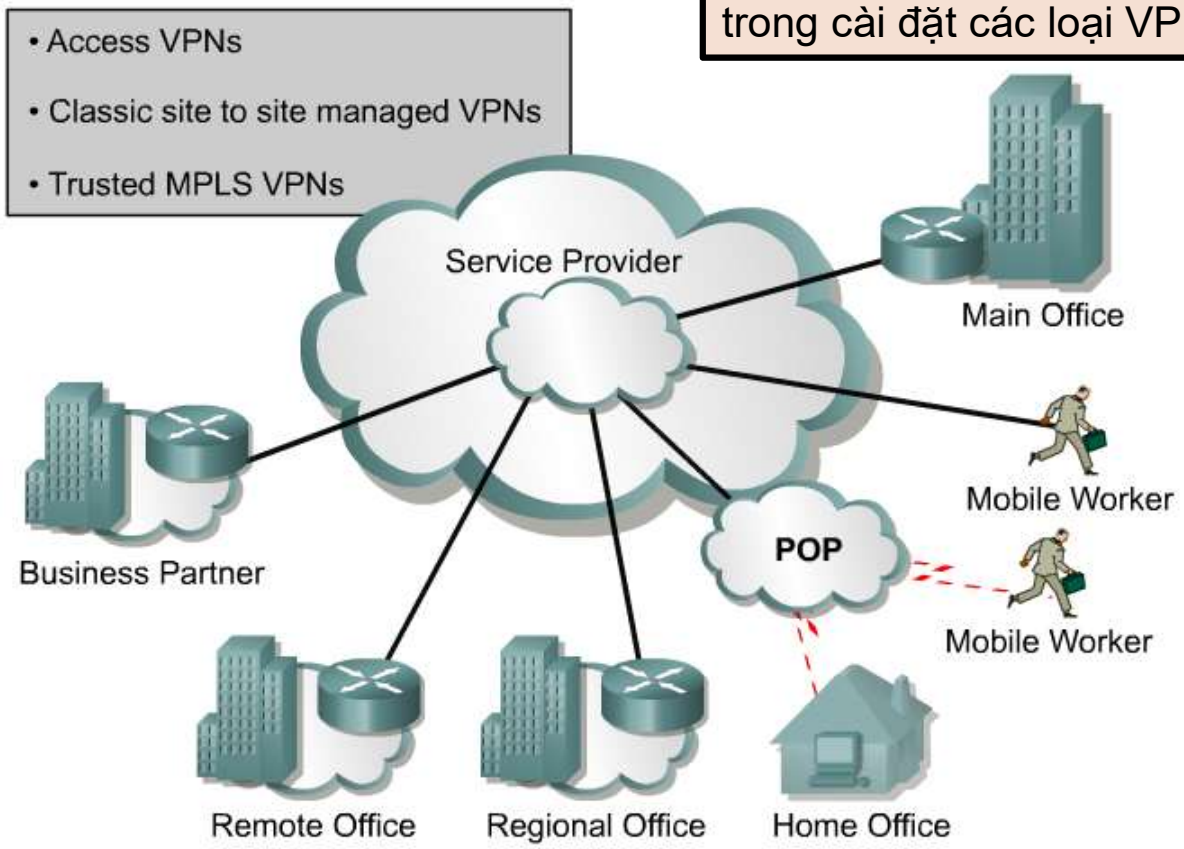
L2TP
- Tương thích ngược với L2F
- Sử dụng cổng UDP 1701
- Có chứng thực, nhưng không mạnh
- Kết hợp với IPSec để mã hóa
- Thường dùng cho dạng VPN truy cập từ xa qua RAS (đường dialup)
- Dùng cho IP, IPX, …

Windows NT/2K/XP/Vista hỗ trợ cả PPTP/L2TP

Mạng riêng ảo - VPN

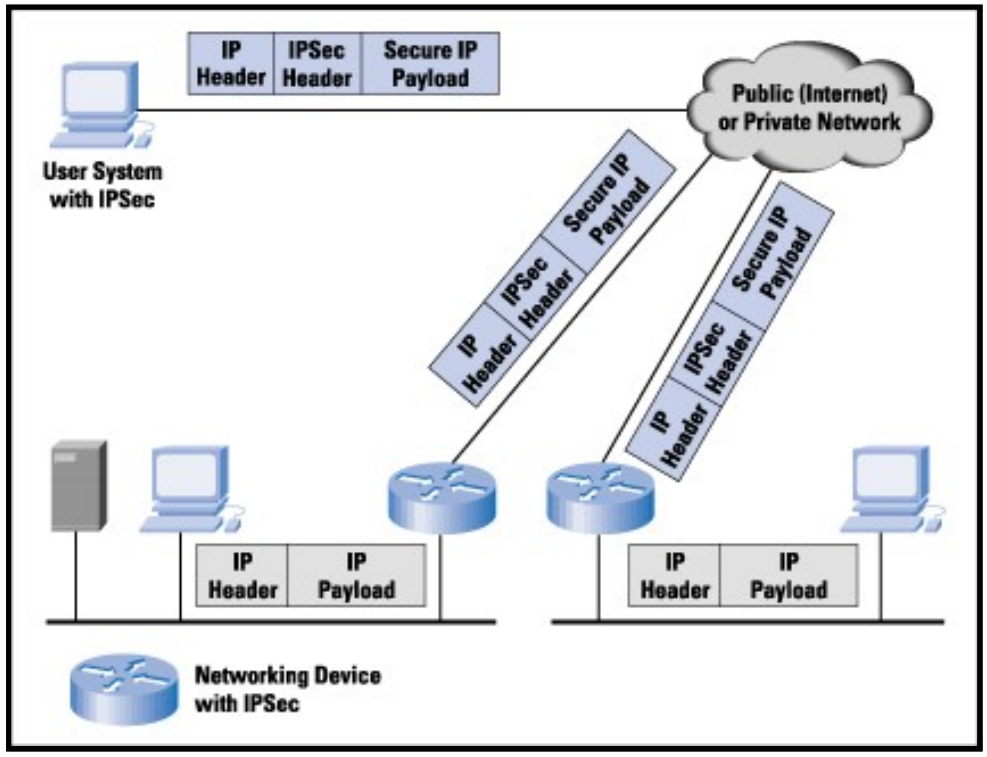
- IPSec – Giới thiệu

IPSec được sử dụng rộng rãi trong cài đặt các loại VPN



Mạng riêng ảo - VPN

- IPSec – Giới thiệu

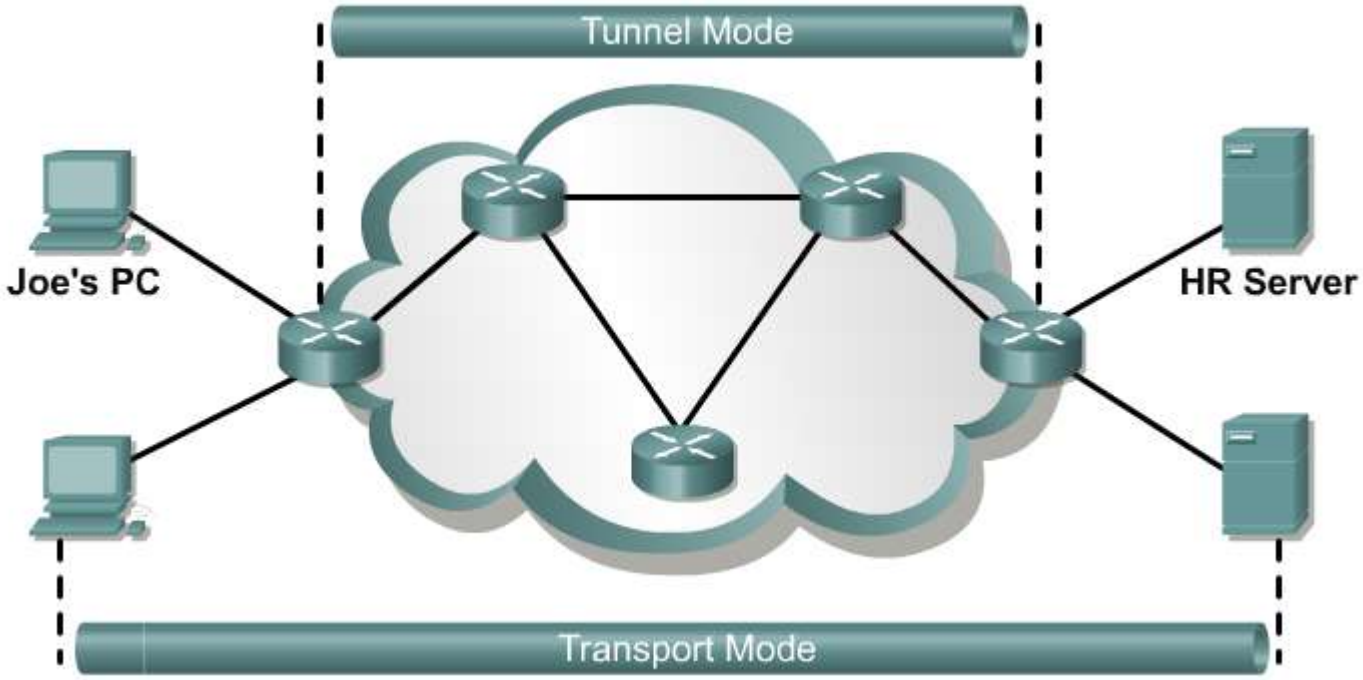


• IPSec là tập các giao thức dùng cho mạng VPN, cung cấp tính bảo mật và toàn vẹn cho gói tin (tầng 3) khi truyền trên mạng IP.
• Sử dụng TCP cổng 50 và 51.

IPSec Framework	Choice 1	Choice 2
IPSec protocol	ESP	ESP +AH
Encryption	DES	3DES
Authentication	MD5	SHA
Diffie-Hellman	DH1	DH2

Mạng riêng ảo - VPN

- IPSec – Các chế độ truyền

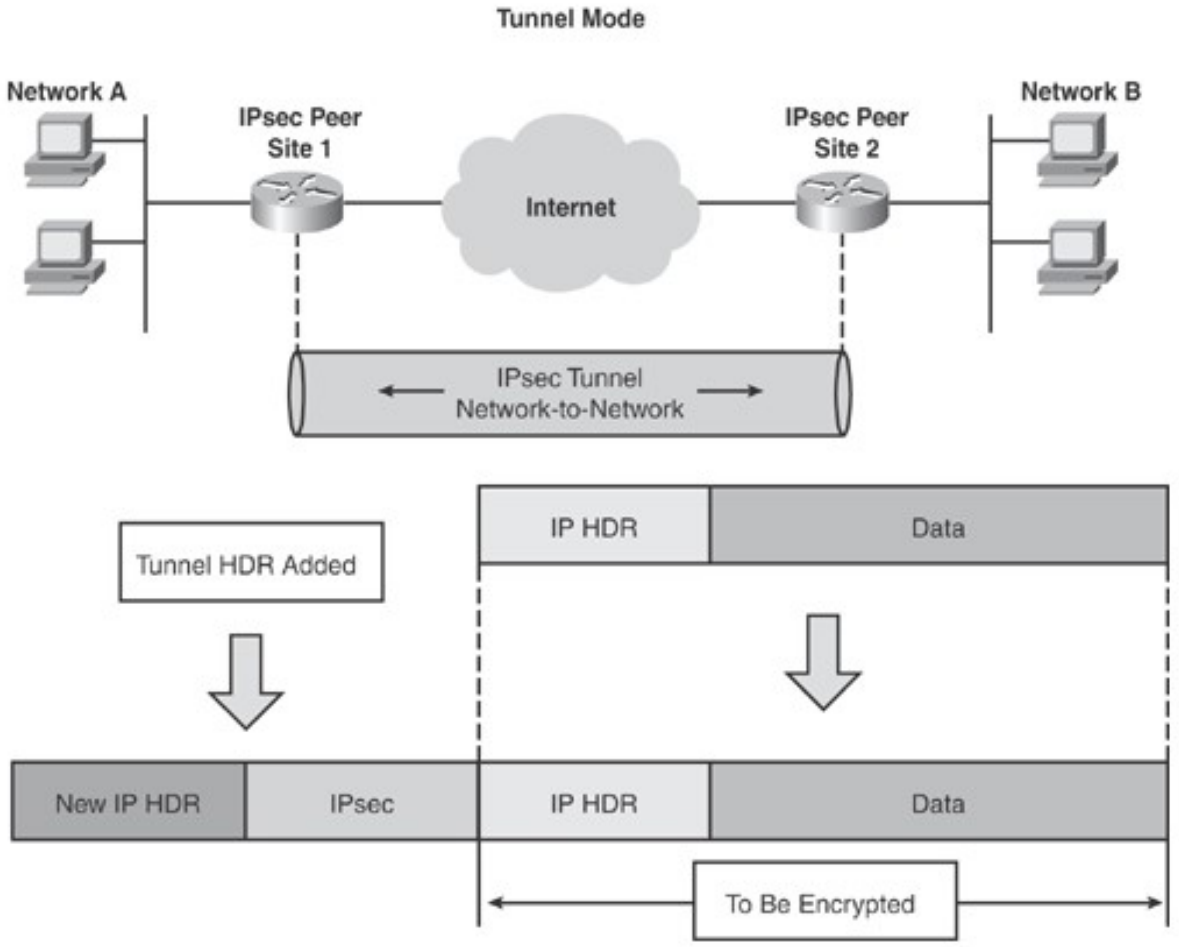


Tunnel mode
- Peer-to-peer
- Sử dụng khi truyền qua đường truyền mạng không tin cậy.
- **Mã hóa cả dữ liệu** (payload) **và phần header.**

Transport mode
- Host-to-host
- Truyền trực tiếp giữa bên gửi và bên nhận.
- **Mã hóa chỉ phần dữ liệu**, **giữ nguyên header**.

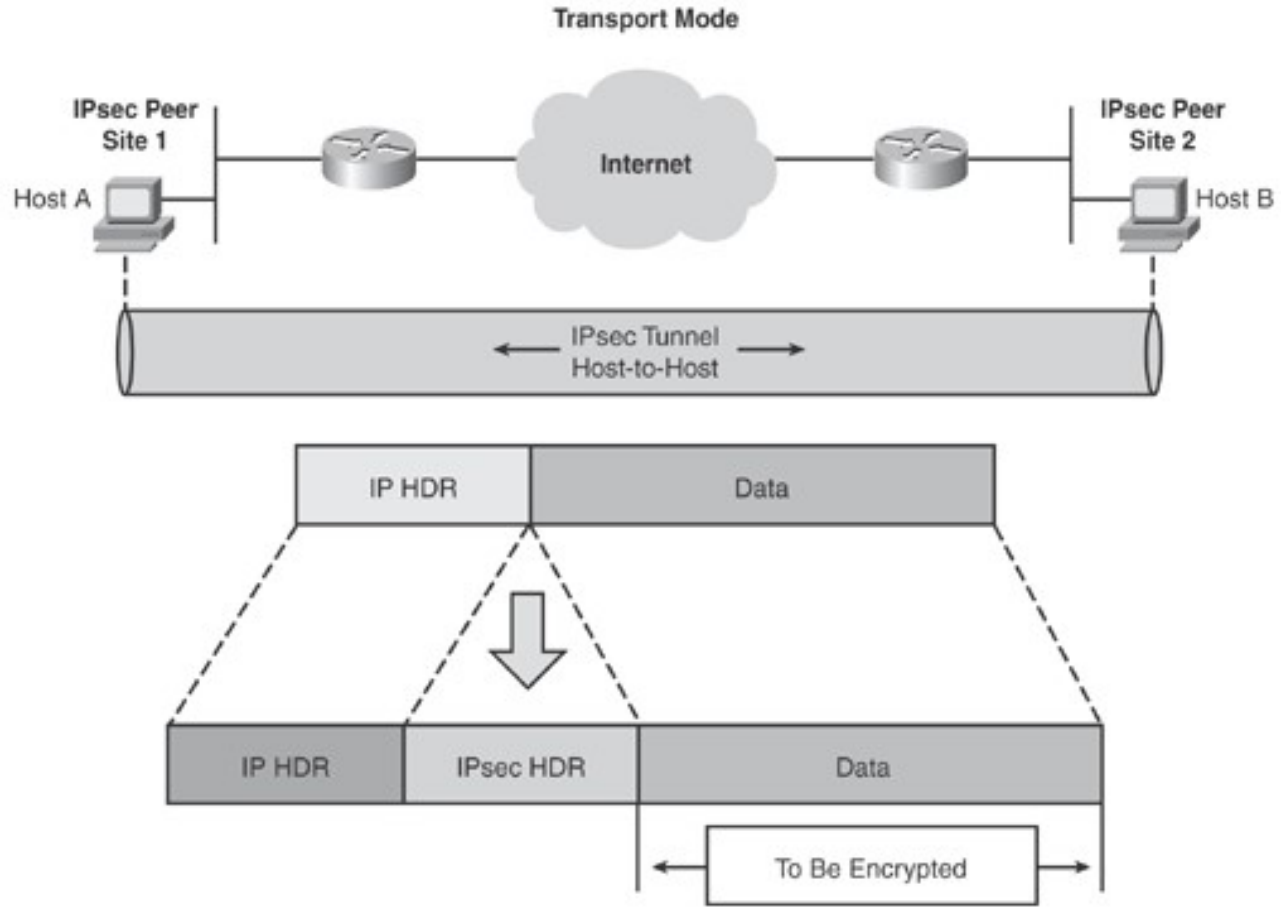
Mạng riêng ảo - VPN

- IPSec – Chế độ truyền Tunnel mode



Mạng riêng ảo - VPN

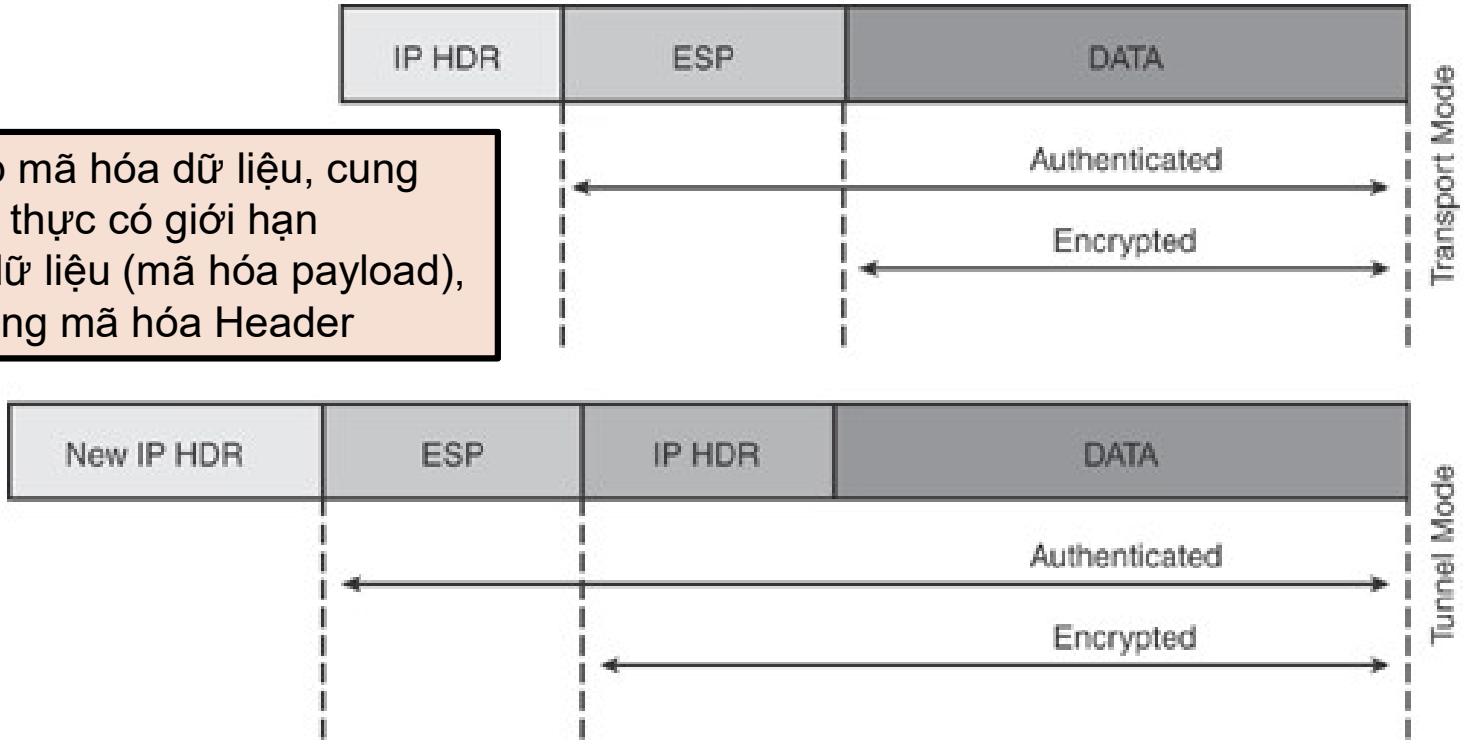
- IPSec – Chế độ truyền Transport mode



Mạng riêng ảo - VPN

- IPSec – Giao thức **Encapsulating Security Payload (ESP)**

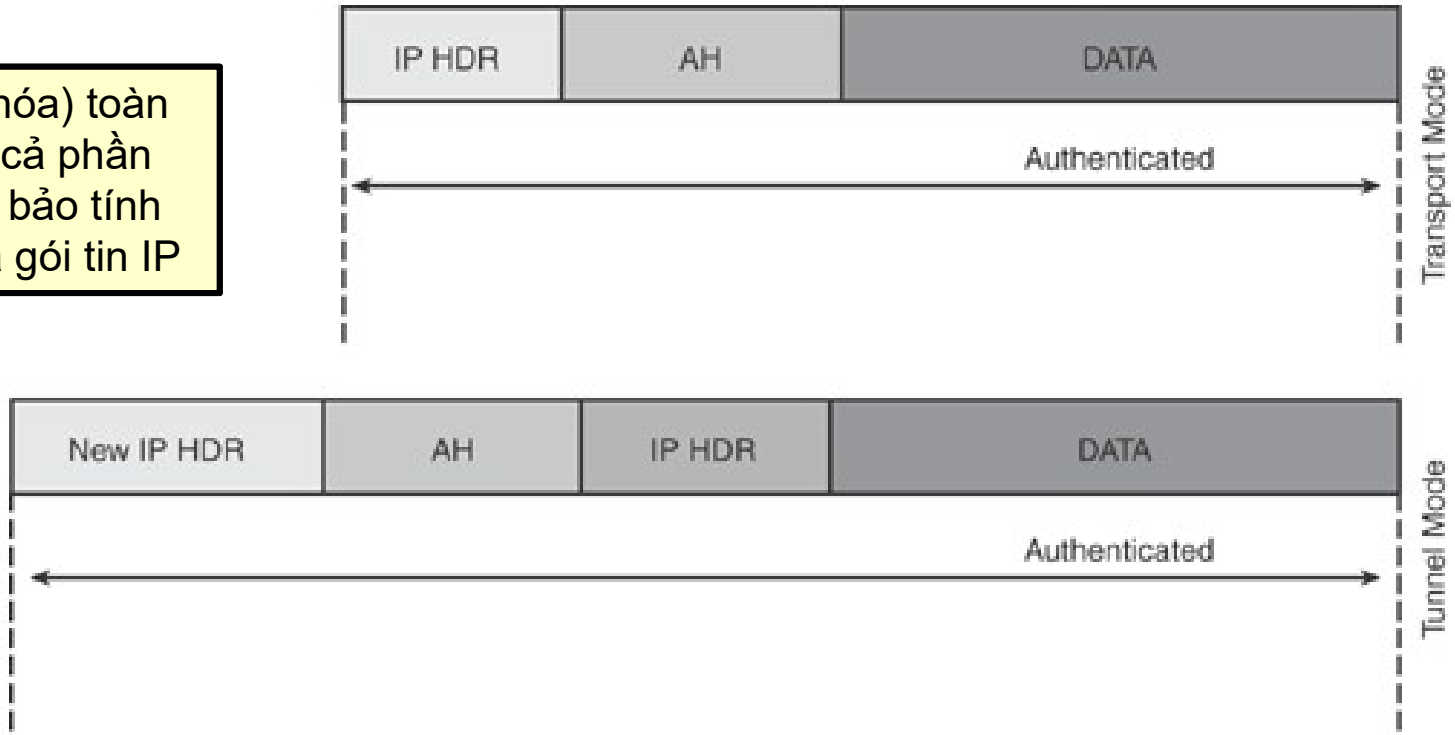
• Cung cấp mã hóa dữ liệu, cung cấp chứng thực có giới hạn
• Bao gói dữ liệu (mã hóa payload), nhưng không mã hóa Header



Mạng riêng ảo - VPN

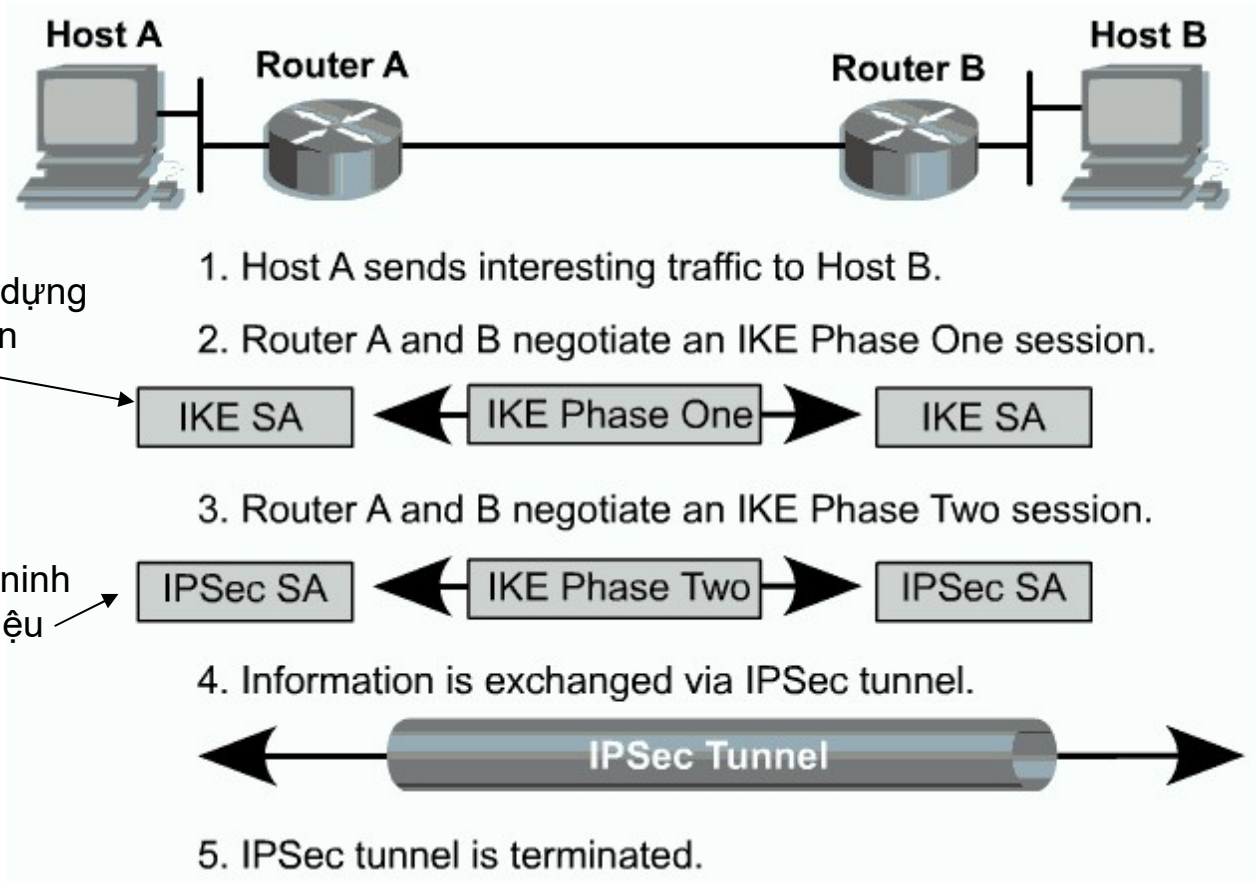
- IPSec – Giao thức **Authentication Header (AH)**

Bảo vệ (mã hóa) toàn bộ gói tin kể cả phần header, đảm bảo tính toàn vẹn của gói tin IP



Mạng riêng ảo - VPN

- IPSec – Hoạt động của IPSec

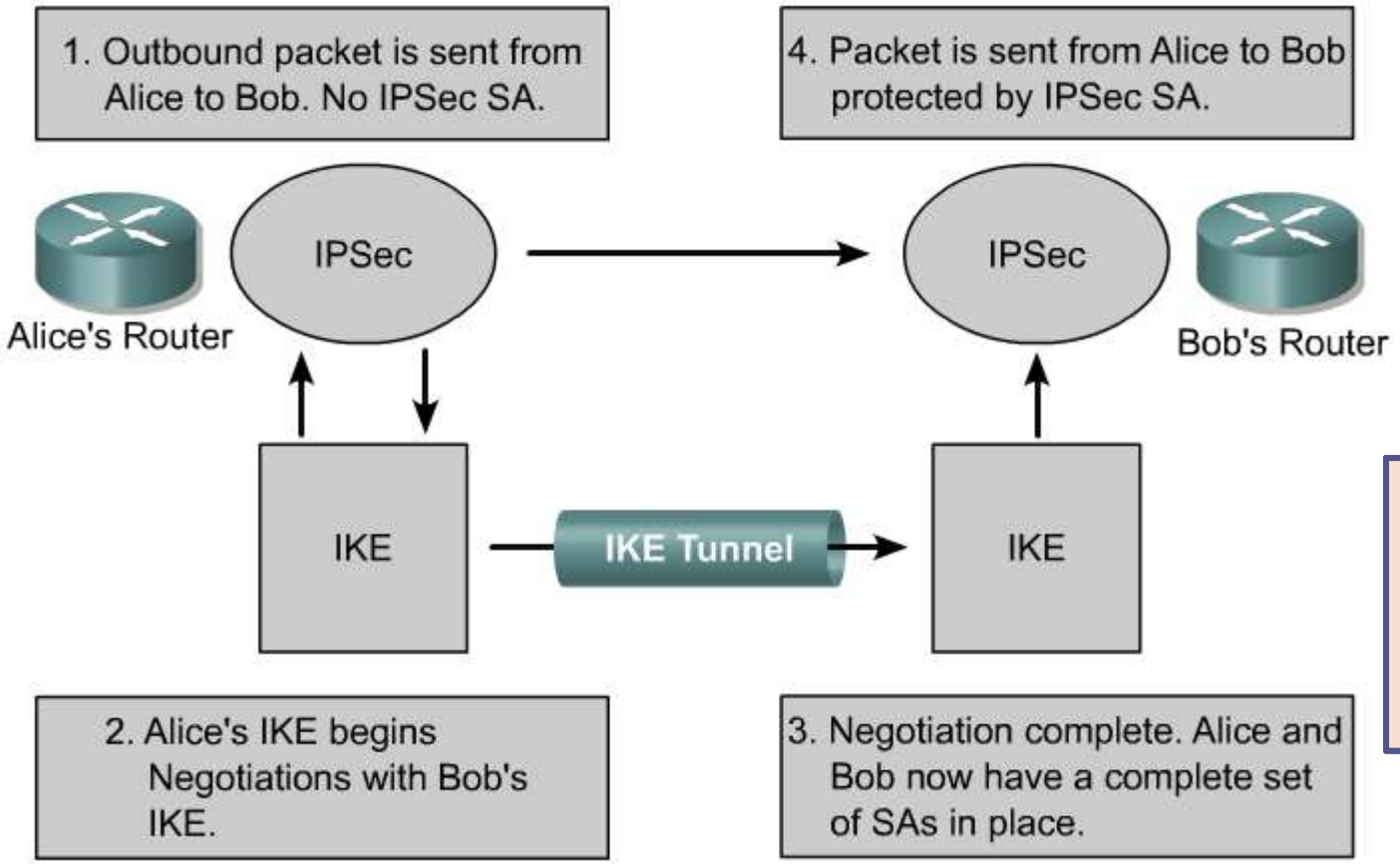


Chính sách xây dựng kênh an toàn

Chính sách an ninh đóng gói dữ liệu

Mạng riêng ảo - VPN

- IPSec – Hoạt động của IPSec



Internet Key Exchange (IKE) đảm bảo tính an toàn khi trao đổi khóa bí mật giữa 2 bên khi thiết lập đường hầm.

Internet Security Association and Key Management Protocol (ISAKMP) được sử dụng để đàm phán và cung cấp chứng thực

Phần 2

Các giao thức truy cập liên mạng

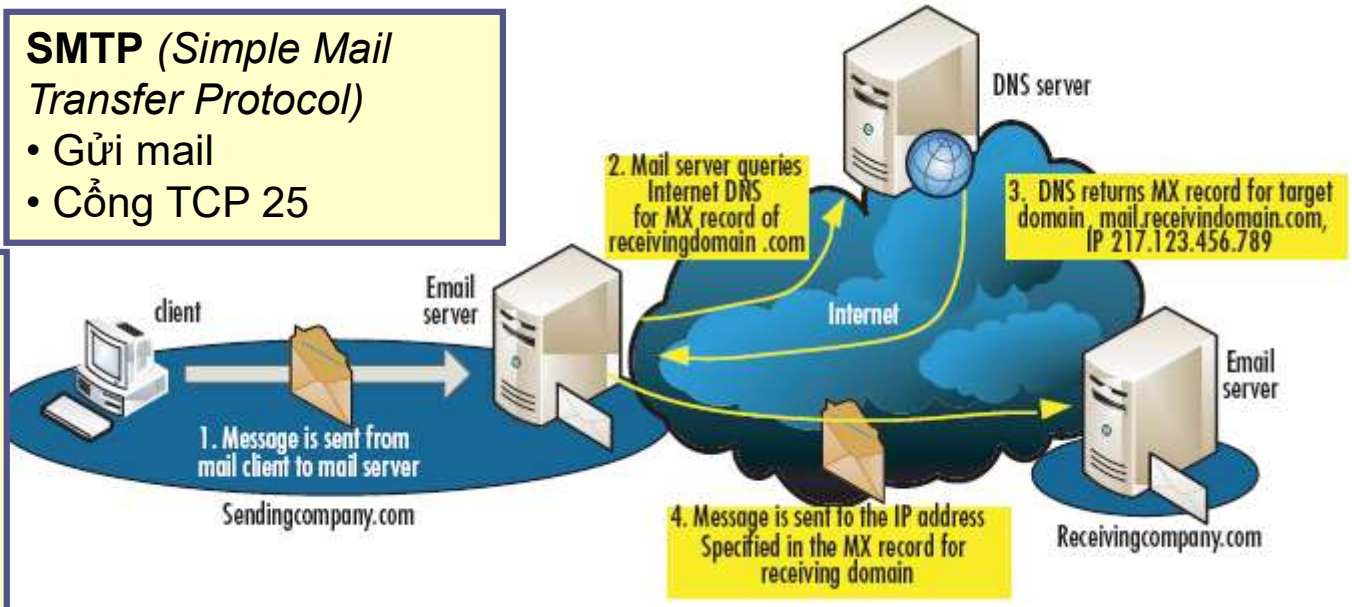
- Email
- Web
- FTP
- File Sharing
- Directory và LDAP, …

Dịch vụ Email

- Các giao thức

SMTP *(Simple Mail Transfer Protocol)*
- Gửi mail
- Cổng TCP 25

POP *(Post Office Protocol)*
/IMAP
(*Internet Message Access Protocol*)
- Nhận mail
- Cổng TCP 110



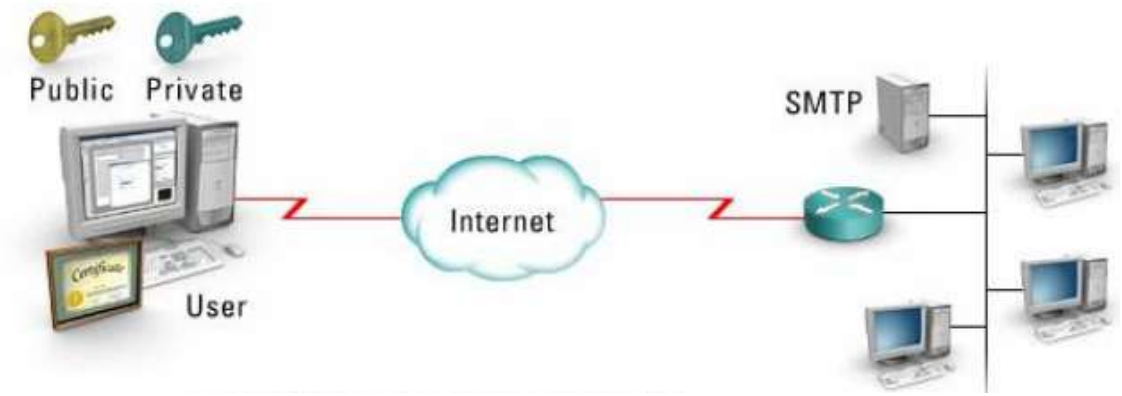
MIME
(Multipurpose Internet Mail Extensions)
- RFC-1512 và 1522
- Hỗ trợ gửi mail có đính kèm file

- Các giao thức chuẩn của email không cung cấp cơ chế an toàn.
- Dịch vụ Email có nhiều điểm yếu có thể dễ dàng bị tấn công và khai thác.

Dịch vụ Email

- S/MIME (Secure MIME)

• S/MIME cung cấp cơ chế bảo mật cho Email.
• Version 2: RFC-2311 và version 3: RFC-2633



S/MIME cung cấp dịch vụ mật mã cho các ứng dụng email:
• Chứng thực
• Tính toàn vẹn và tính không thể phủ nhận (thông qua chữ ký số)
• Bảo mật và riêng tư cho thông điệp (thông qua mã hóa)

• Sử dụng 3 thuật toán mã hóa đối xứng: DES, 3DES, RCC2 trong việc mã hóa thông điệp.
• Dùng giải thuật RSA trong việc trao đổi khóa và chữ ký số.
• Windows Mail (Vista), Outlook Express, Thunderbird hỗ trợ S/MIME.

Dịch vụ Email

- PGP (Pretty Good Privacy)

• Do Philip R. Zimmermann tạo ra vào năm 1991.
•Phần mềm mã hóa và chứng thực.
•PGP là chuẩn đóng thuộc công ty PGP

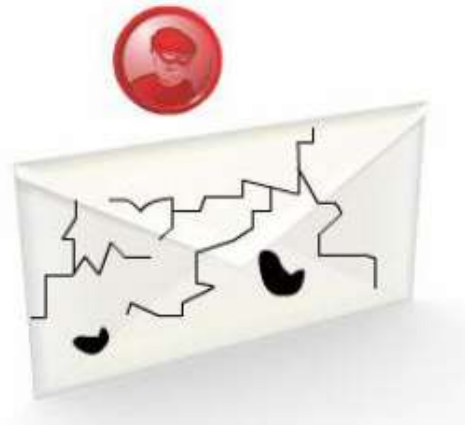
• Sử dụng thuật toán mã hóa bất đối xứng
• Dùng hạ tầng khóa công khai (PKI)
• PGP nén dữ liệu trước khi mã hóa
• Dùng thuật toán RSA hoặc DH

•Open PGP được cung cấp theo chuẩn mở mô tả trong RFC-2440
• Được hỗ trợ trong nhiều phần mềm thương mại và mã nguồn mở.

Một số phần mềm hỗ trợ Open PGP : Authora, WinPT, GnuPG, Enigmail, GPGforWin, PGPFreeware, …

Dịch vụ Email

- Các điểm yếu của Email



SPAM (Mail rác)
• Những mail với nội dung quảng cáo hoặc các thông tin không mong muốn.
• Làm giảm băng thông và hiệu năng của dịch vụ
• Làm đầy hộp thư và tốn thời gian lọc mail của người dùng.

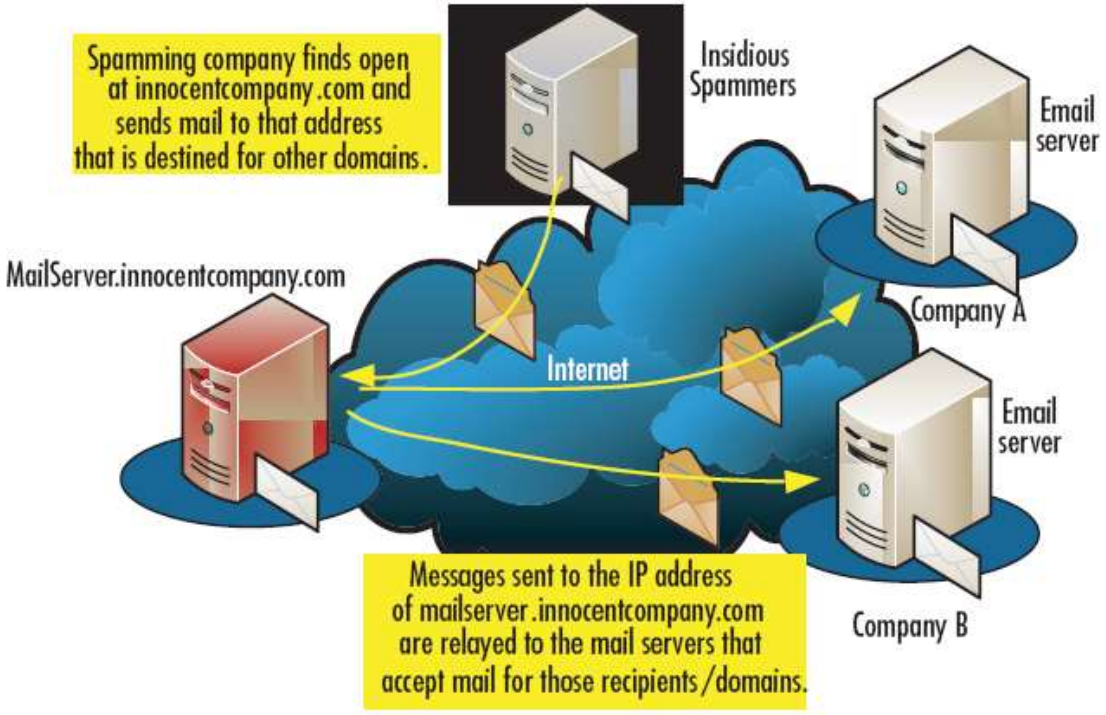
Hoax (Mail đánh lừa)
• Chứa các thông tin không đúng sự thật.
• Lừa người dùng gửi tiếp cho những người khác.

Phishing (lừa đảo)
• Lừa người dùng click vào 1 liên kết dẫn đến 1 URL giả để lấy cắp các thông tin nhậy cảm như tài khoản, số thẻ tín dụng, …
• Các trình duyệt và phần mềm diệt virus mới đều có tính năng chống dạng tấn công phishing này.

Virus, Trojan
• Lừa người dùng mở tập tin đính kèm chứa các mã độc hại như virus, trojan
• Tự động gửi tiếp bản thân nó cho các người dùng khác trong Address Book.

Dịch vụ Email

- SMTP Relay

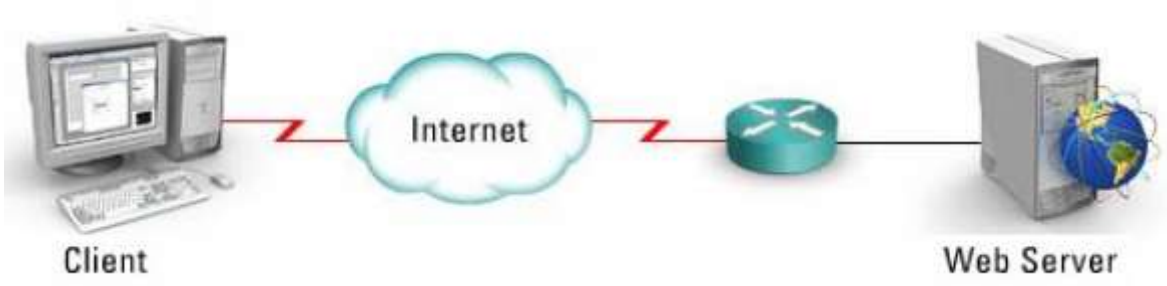


• Lợi dụng Mail Server cấu hình không chính xác gửi email đến các Server khác.
• Thường sử dụng để phát tán SPAM.

Không cho người dùng vô danh từ bên ngoài mạng (chưa chứng thực) gửi mail đi 1 địa chỉ mail bên ngoài.

Dịch vụ Web

- Giao thức



- Dùng giao thức HTTP
- Mô tả trong RFC-2616
- Cổng phục vụ là TCP 80

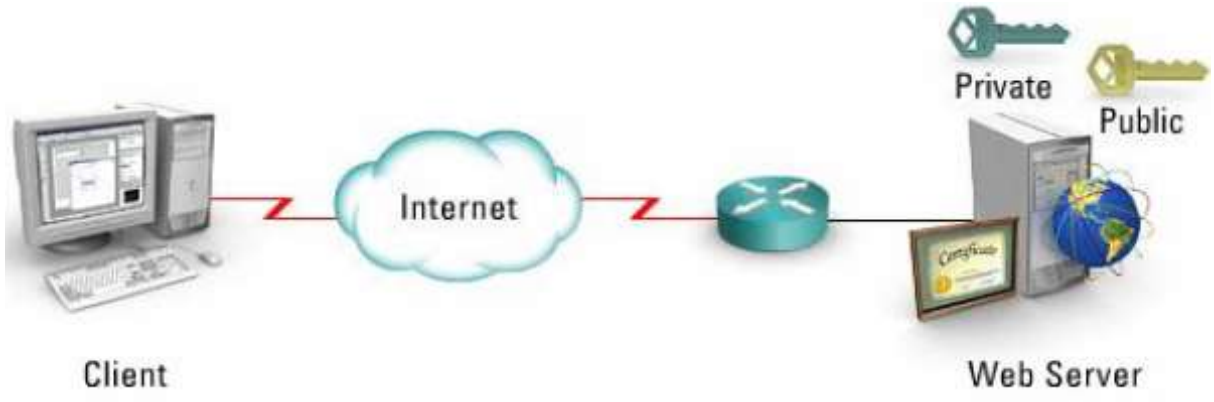
- Ngôn ngữ sử dụng HTML
- Chuyển các file HTML (trang Web) từ Server đến Client.

- HTTP là giao thức không an toàn
- Không chứng thực, không mã hóa

Dịch vụ Web

- HTTPS

Gõ trong trình duyệt **https://**



- **HTTPS** = **HTTP** + **TLS/SSL**
- Cung cấp tính bảo mật cho dịch vụ Web.
- Thích hợp cho các giao dịch an toàn trên Web như: giao dịch ngân hàng, thông tin thẻ tín dụng, mua hàng trực tuyến, …
- Dùng cổng TCP 443
- Sử dụng mật mã khóa công khai: cặp khóa công khai + khóa bí mật và chứng chỉ số X.509.

Dịch vụ Web

- SSL (Secure Sockets Layer) và TLS (Transport Layer Security)

•.Độc lập với giao thức của tầng ứng dụng
• Cung cấp cơ chế bảo mật cho các dịch vụ Web, FTP, Telnet, LDAP, IMAP, …

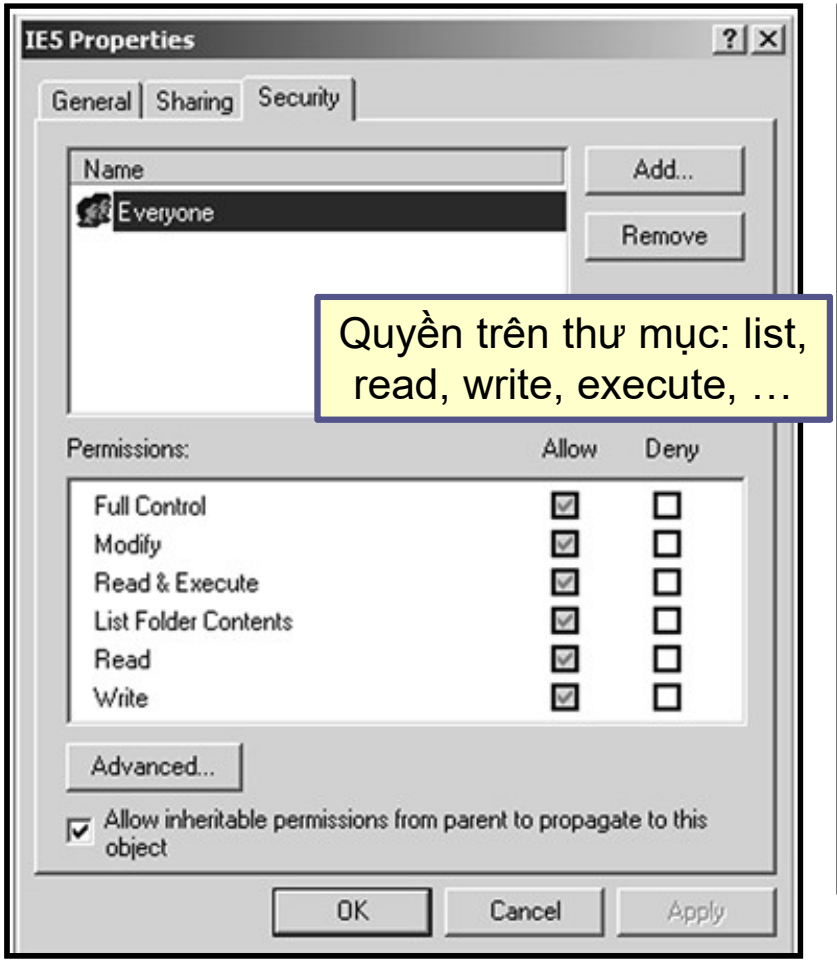
SSL
•.Hoạt động phía trên tầng TCP
• Sử dụng cả khóa công khai và khóa đối xứng cho các phiên giao dịch.
• Sử dụng 3 giao thức:
+ SSL handshake protocol
+ SSL Record protocol
+ SSL Alter protocol

• Kết nối bí mật qua mã hóa đối xứng: DES, RC4, …
• Chứng thực qua mã hóa bất đối xứng: RSA, DSA, …
• Kết nối tin cậy qua kiểm tra tính toàn vẹn bằng các giải thuật băm: SHA, MD5, …

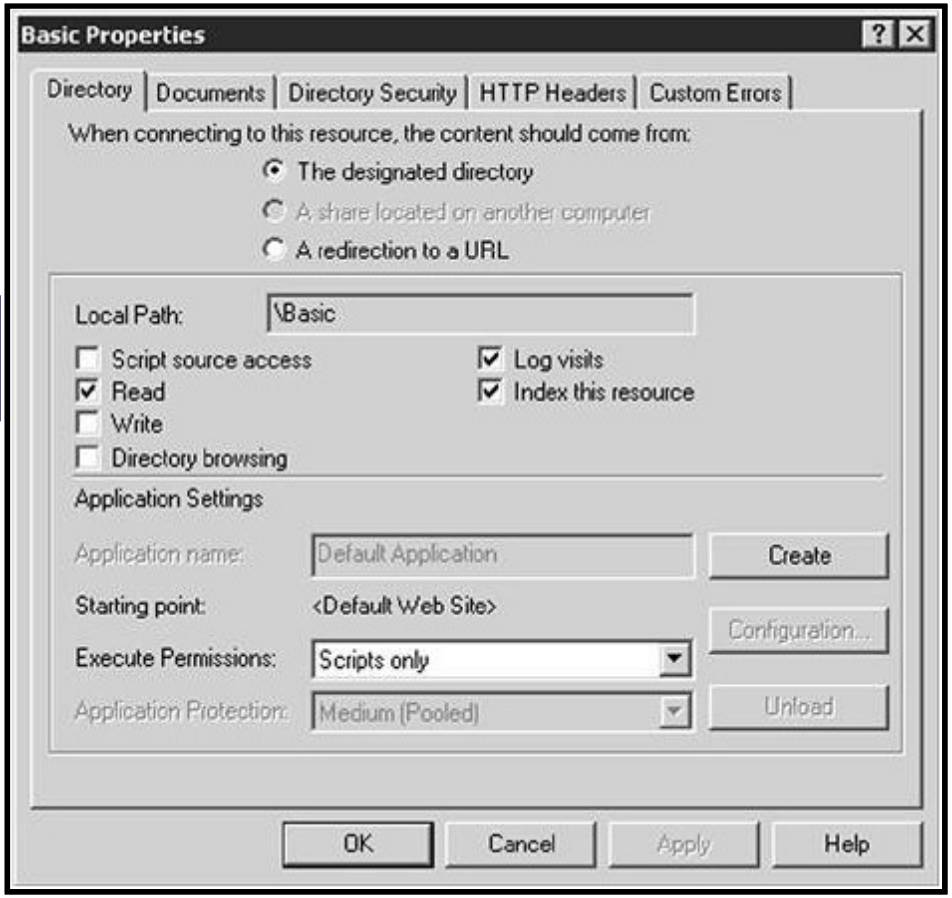
TLS
• Kế thừa từ SSL, nhưng không tương thích với SSL.
• Cung cấp các chức năng bảo mật nâng cao hơn.

Dịch vụ Web

- Một số vấn đề cần quan tâm

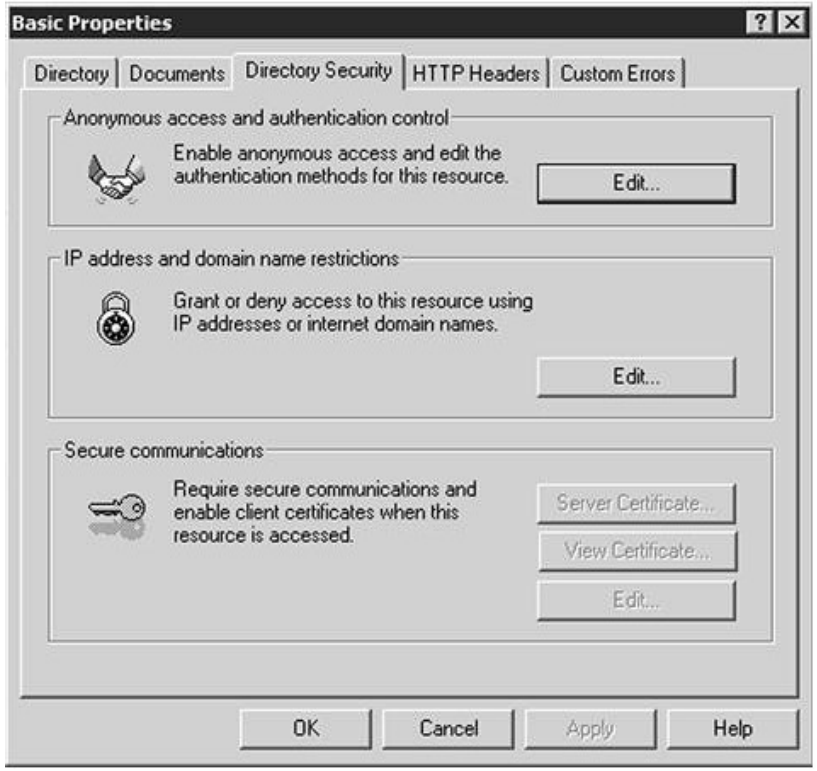


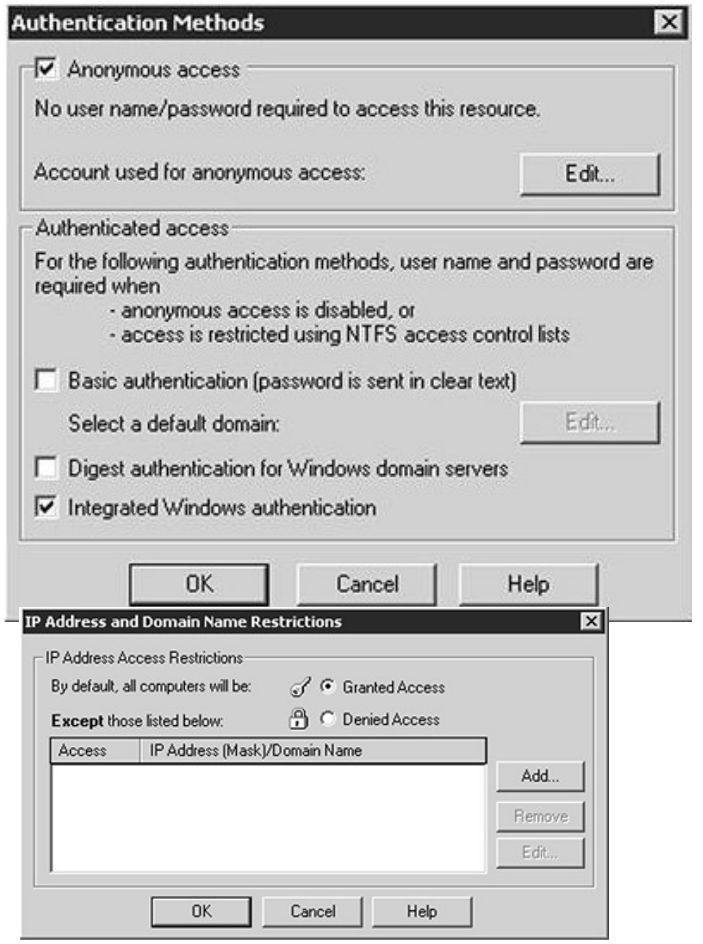
Quyền trên thư mục: list, read, write, execute, …



Dịch vụ Web

- Một số vấn đề cần quan tâm

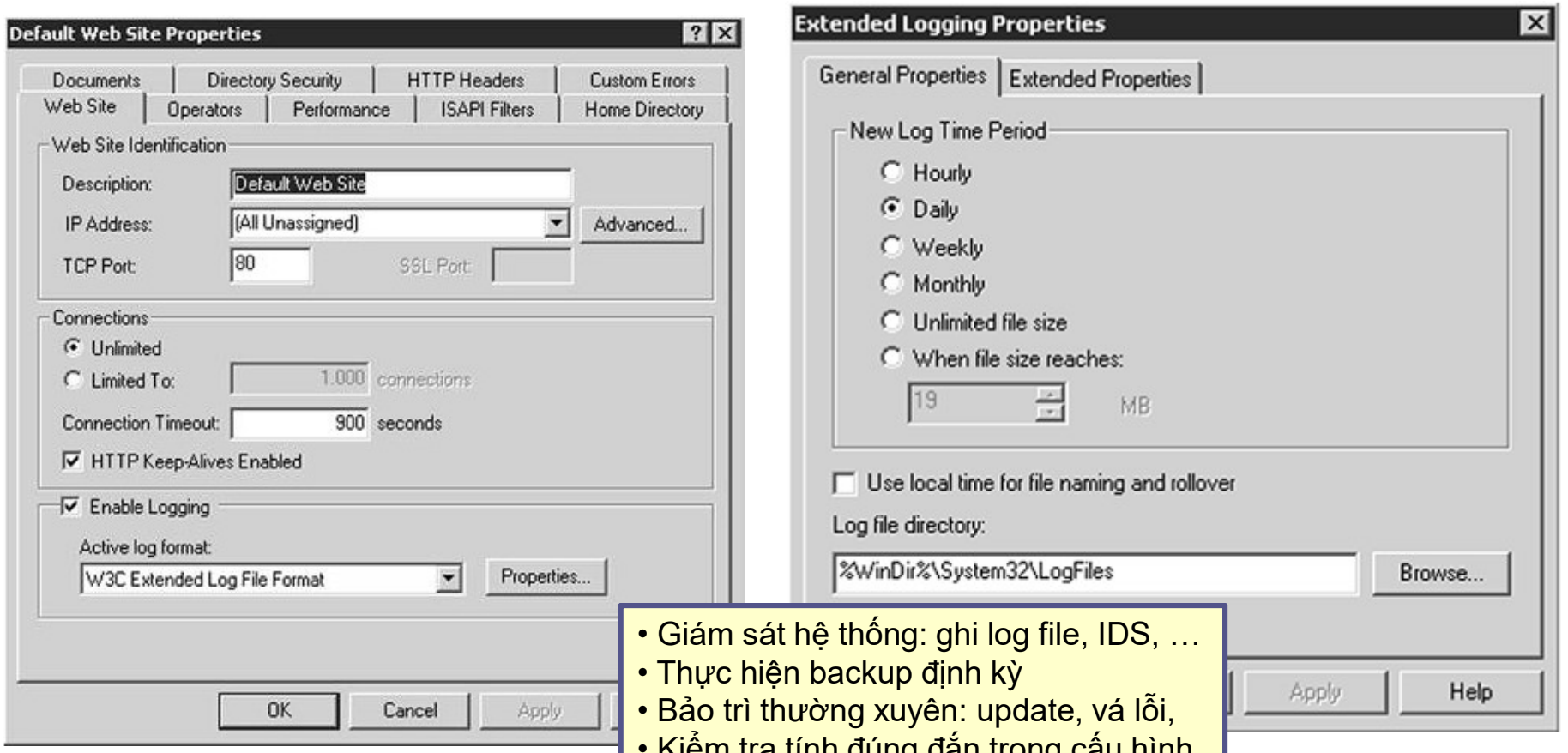




Quản lý điều khiển truy cập: người dùng, địa chỉ cho phép truy cập

Dịch vụ Web

- Một số vấn đề cần quan tâm

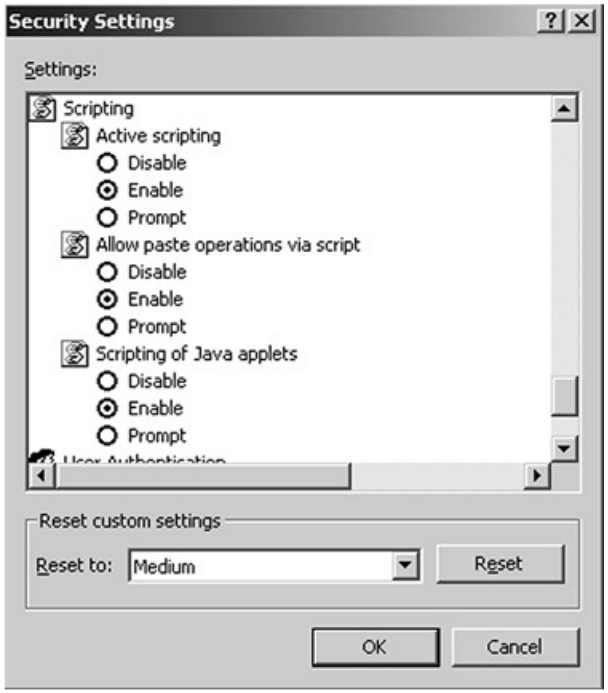


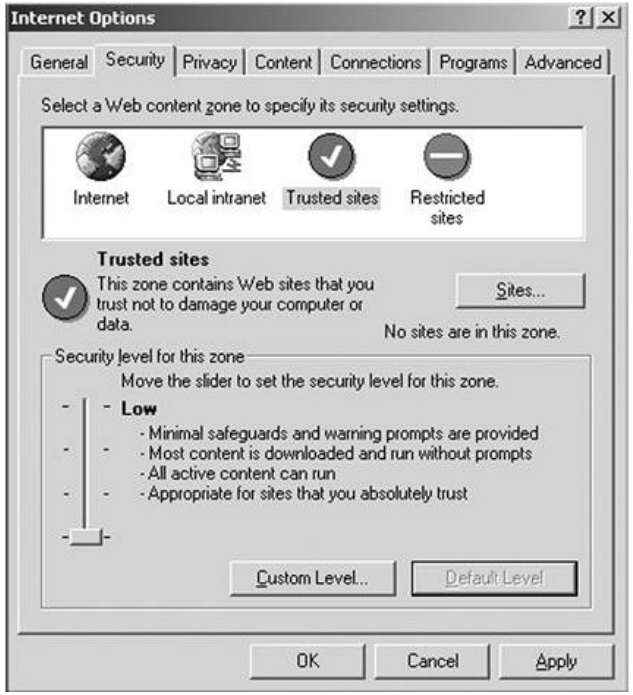
- Giám sát hệ thống: ghi log file, IDS, …
- Thực hiện backup định kỳ
- Bảo trì thường xuyên: update, vá lỗi,
- Kiểm tra tính đúng đắn trong cấu hình Web Server: có thể dùng NMAP.

Dịch vụ Web

- Một số vấn đề cần quan tâm

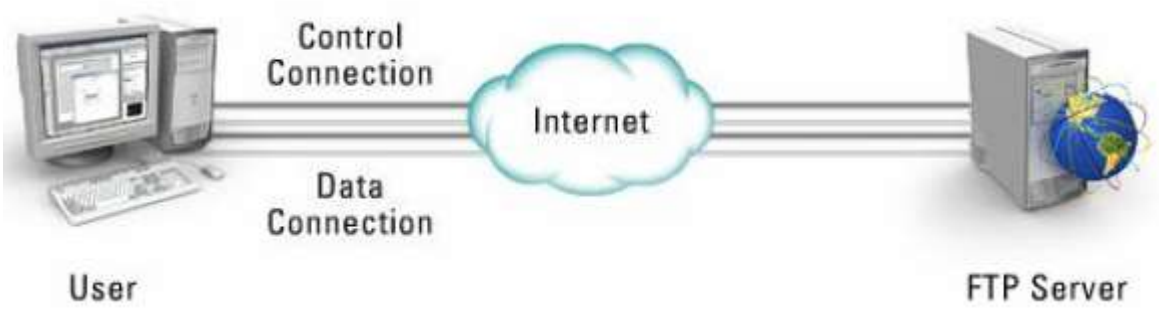
- Đặt mức độ bảo mật cho trình duyệt.
- Giới hạn các script thực thi: VBScript, JavaScript, …
- Cẩn thận khi sử dụng cookie, ActiveX, CGI





Dịch vụ FTP

- Giao thức



• Dùng giao thức FTP
• Mô tả trong RFC-959
• Cổng phục vụ là :
+ TCP 21 cho nối kết
+ TCP 20 cho dữ liệu

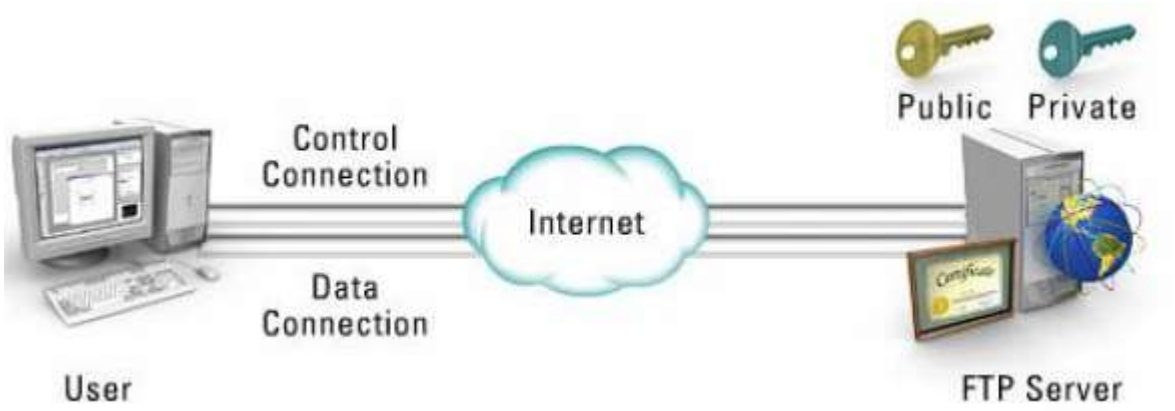
• Có 2 dạng tài khoản người dùng:
+ Tài khoản vô danh (anonymous): đa số chỉ cho download.
+ Người dùng riêng: có thể cho upload vào thư mục riêng.

• FTP là giao thức không an toàn
• Mọi thứ gửi đi trên đường truyền đều không được mã hóa (kể cả password)

• **Standard mode**: có 2 giao dịch
+ Client nối kết đến Server ở cổng 21 để yêu cầu file.
+ Server (dùng cổng 20) nối kết đến Client để upload file đến Client.
• **Passive mode**: có 2 giao dịch
+ Client nối kết đến Server (cổng 21). Server trả lời lại Client giá trị cổng phục vụ.
+ Client nối kết đến Server qua cổng đó để nhận file.

Dịch vụ FTP

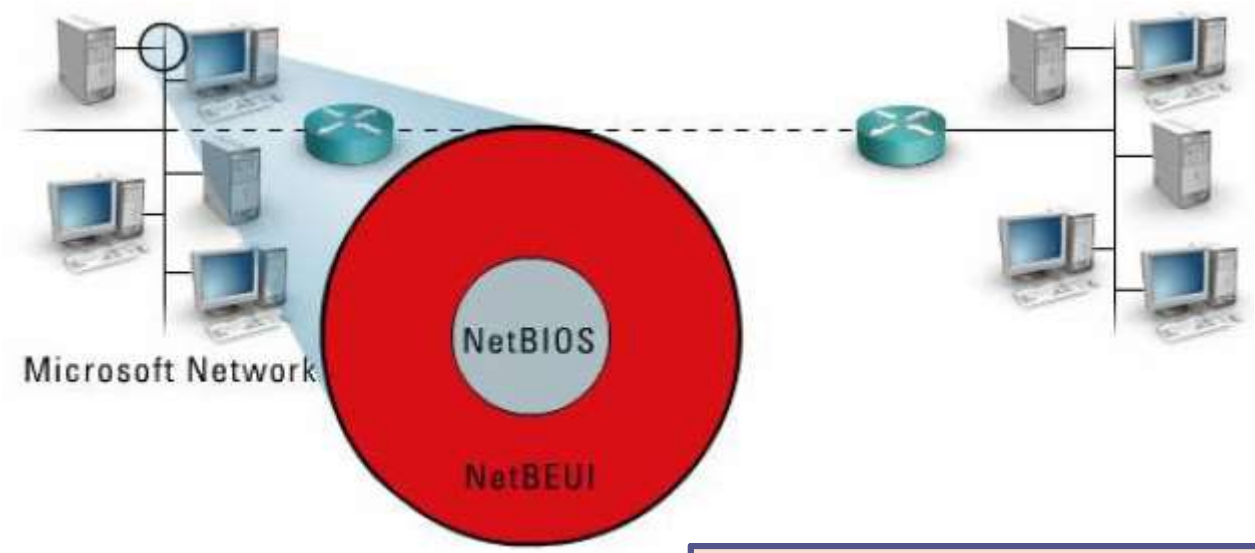
- FTPS



- **FTPS** = **FTP** + **TLS/SSL**
- Cung cấp tính bảo mật cho dịch vụ FTP.
- Thích hợp cho các giao dịch an toàn và bảo mật khi truyền file bằng FTP.
- Dùng cổng TCP 990 cho điều khiển và TCP 898 cho dữ liệu.
- Sử dụng mật mã khóa công khai
- Chữ ký số (chuẩn X.509): dùng RSA, DSA
- Mã hóa dữ liệu dùng khóa bí mật (khóa chia sẻ) : DES, 3DES, AES, …

Dịch vụ chia sẻ file

- File sharing



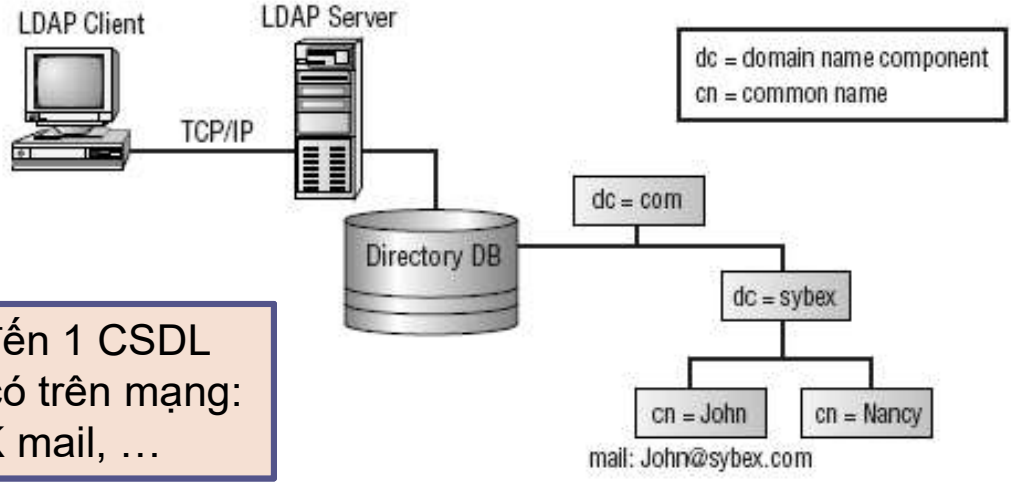
NetBIOS
• Tạo ra bởi IBM, phát triển bởi Microsoft.
• Cung cấp dịch vụ vận chuyển và giao dịch.
• Dùng cổng TCP 137, 138, 139

NetBEUI
• Chuẩn định dạng khung của NetBIOS.
• Giao thức tầng 4 (nhưng không hỗ trợ vạch đường)
NetBIOS trên TCP (NBT)
• Dùng vận chuyển dữ liệu NetBIOS trên các mạng tầng 3 (như IP)

Dịch vụ LDAP

- Lightweight Directory Access Protocol

LDAP là giao thức chuẩn cho phép Client có thể truy cập vào tài nguyên trong dịch vụ thư mục .



Dịch vụ thư mục cung cấp truy cập đến 1 CSDL trung tâm lưu trữ các tài nguyên hiện có trên mạng: tài khoản người dùng, TK máy tính, TK mail, …

- LDAP theo chuẩn X.500
- Sử dụng cổng TCP 389, 636
- LDAP thường dùng để **cung cấp chứng thực** cho các dịch vụ khác trên mạng.

SLDAP (Secure LDAP)
- Dùng SSL/TLS để cung cấp chứng thực và mã hóa.