



ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

CƠ SỞ HẠ TẦNG CÔNG NGHỆ THÔNG TIN

GV: ThS. Tạ Thu Thủy

CHƯƠNG 3:

Các chủ đề phổ biến trong
công nghệ thông tin

Nội dung

- 1. Giới thiệu**
2. Mạng máy tính
3. Mô hình tham chiếu OSI
4. Đảm bảo và an toàn thông tin
5. Bài tập

1. Giới thiệu



Mạng
máy tính

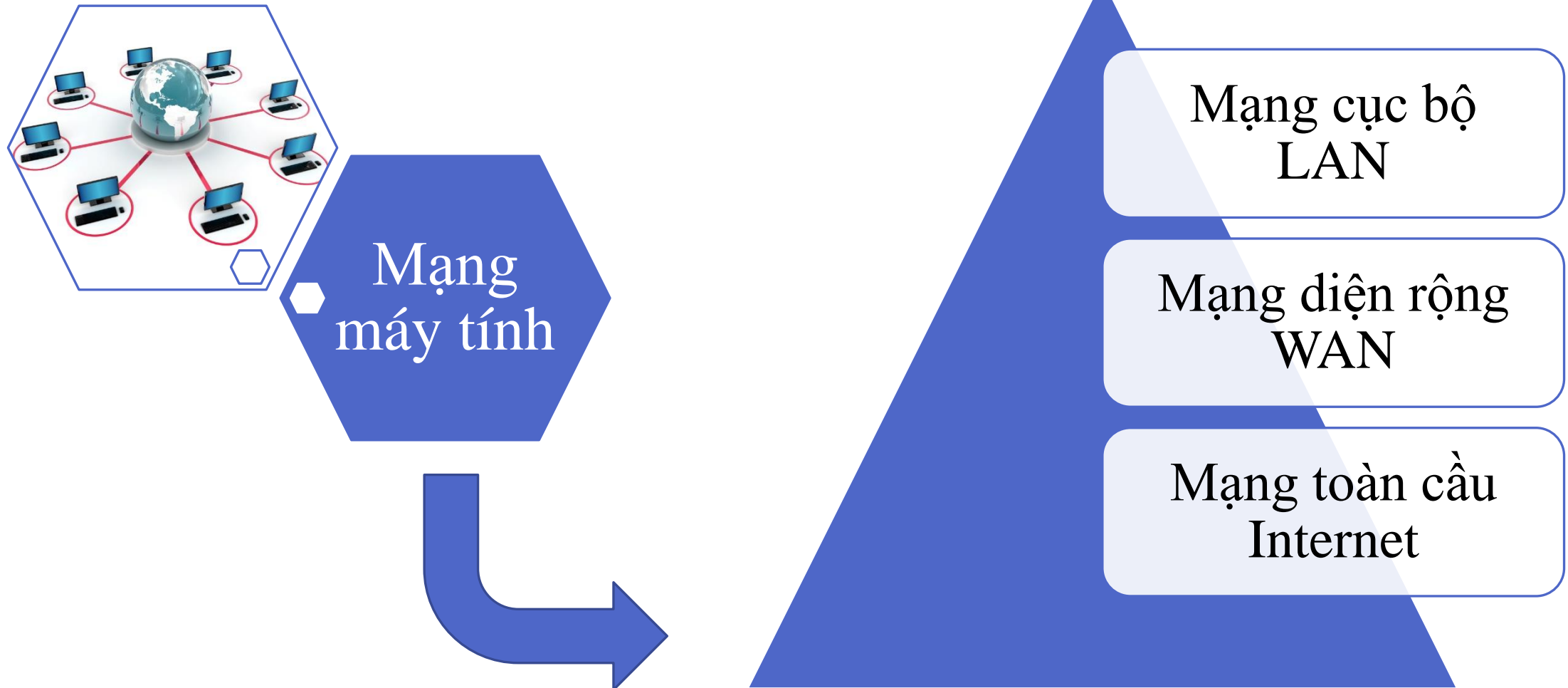
Mô hình
tham
chiếu OSI



Nội dung

1. Giới thiệu
- 2. Mạng máy tính**
3. Mô hình tham chiếu OSI
4. Đảm bảo và an toàn thông tin
5. Bài tập

2. Mạng máy tính



2. Mạng máy tính

2.1 **Mạng cục bộ LAN**

2.2 Mạng diện rộng WAN

2.3 Mạng toàn cầu Internet

2.1 Mạng cục bộ LAN

Mạng cục bộ (*LAN*) là một mạng truyền thông kết nối nhiều thiết bị với nhau và cung cấp một cơ chế trao đổi thông tin giữa các thiết bị.

Phương thức trao đổi thông tin:

- Tại mỗi trạm, thiết bị truyền/nhận làm nhiệm vụ truyền thông qua môi trường truyền được chia sẻ chung.
- Bản tin truyền từ một trạm bất kỳ được quảng bá tới tất cả các trạm còn lại.
- Vì môi trường truyền được chia sẻ chung nên chỉ có 1 trạm được phép truyền dữ liệu tại một thời điểm.
- Dữ liệu được truyền theo các gói.

2. Mạng máy tính

2.1 Mạng cục bộ LAN

2.2 Mạng diện rộng WAN

2.3 Mạng toàn cầu Internet

2.2 Mạng diện rộng WAN

Mạng diện rộng (WAN) là loại mạng có phạm vi trải rộng theo khoảng cách địa lý thường được phát triển dựa trên các hệ thống chuyển mạch công cộng.

Mạng WAN thực hiện truyền thông tin dựa vào một trong hai công nghệ là:

- Chuyển mạch kênh (*circuit switching*)
- Chuyển mạch gói (*packet switching*)

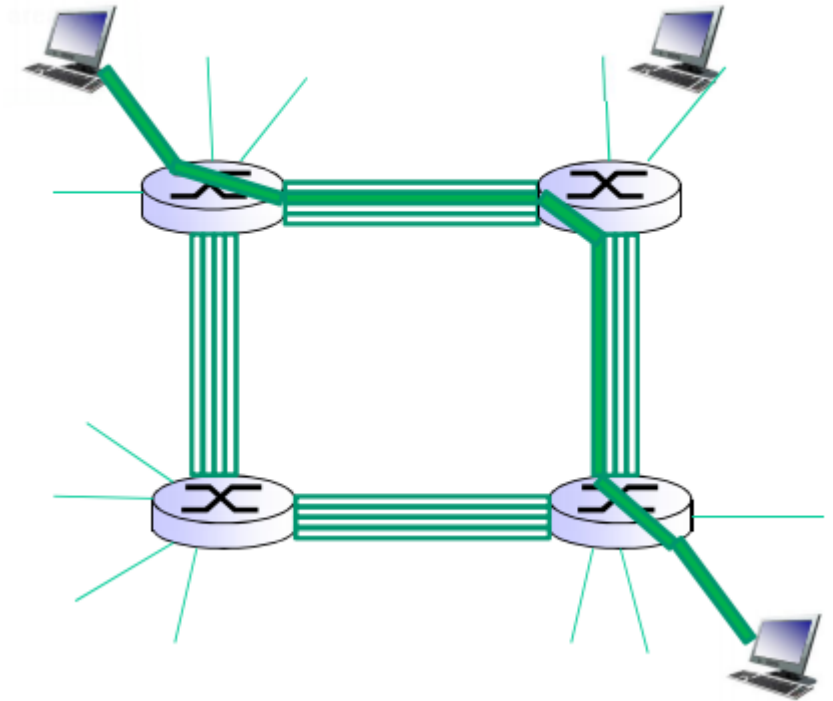
Gần đây, có thêm các công nghệ khác:

- Frame Relay
- ATM

2.2 Mạng điện rộng WAN

➤ Chuyển mạch kênh (*circuit switching*)

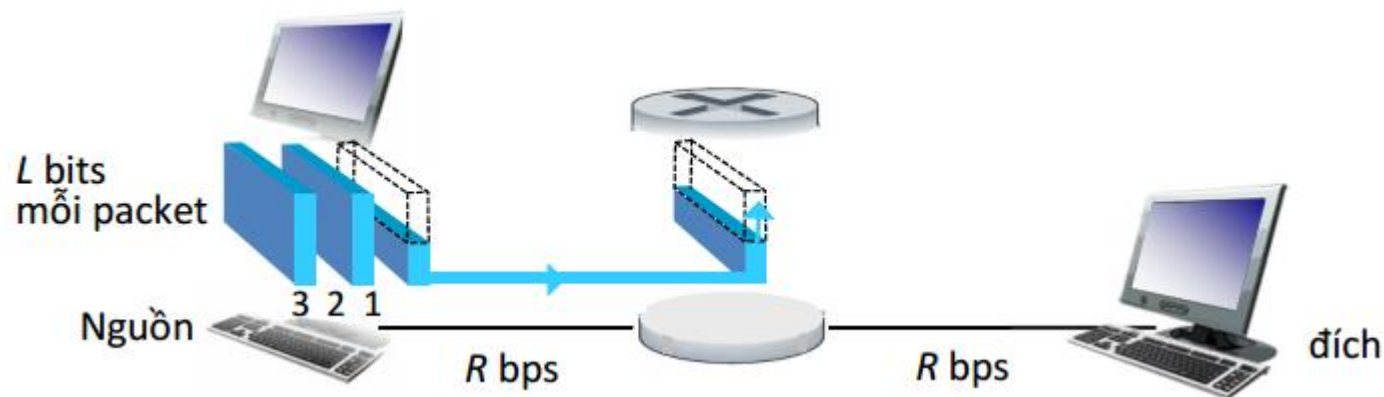
- Một đường truyền thông xác định được thiết lập giữa hai trạm thông qua các nút mạng.
- Con đường này là một thứ tự kết nối các liên kết vật lý giữa các nút.
- Dữ liệu do trạm nguồn sinh ra được truyền dọc theo con đường xác định một cách nhanh nhất có thể.
- Tại mỗi nút, dữ liệu vào được định tuyến hay chuyển mạch vào kênh ra thích hợp mà không có thời gian trễ.



2.2 Mạng diện rộng WAN

➤ Chuyển mạch gói (*packet switching*)

- Không cần phải đề ra trước một dung lượng của đường truyền xác định theo một con đường qua mạng.
- Dữ liệu được gửi đi theo trình tự các gói nhỏ. Mỗi một gói được truyền qua mạng từ nút này đến nút khác theo nhiều con đường dẫn từ trạm nguồn đến trạm đích.
- Tại mỗi nút, khi nhận được toàn bộ gói, sau một khoảng thời gian lưu lại ngắn, gói này sẽ được tiếp tục chuyển tới nút tiếp theo.



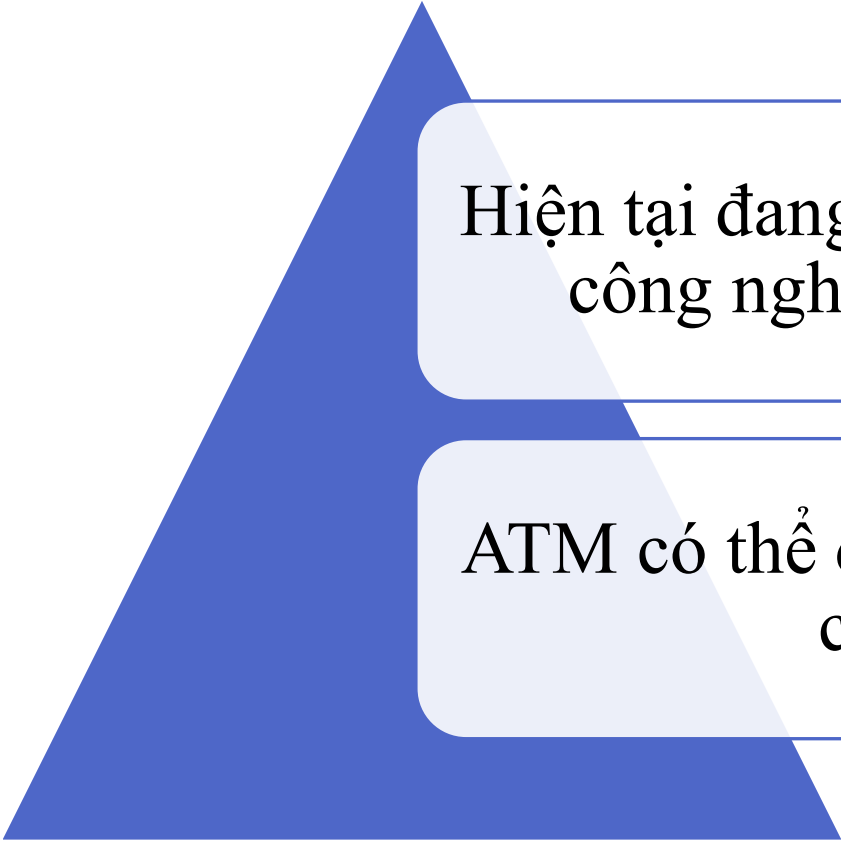
2.2 Mạng diện rộng WAN

➤ Frame Relay

- Chuyển mạch gói được phát triển tại thời điểm công nghệ truyền số trên khoảng cách xa thường có tỷ suất gặp lỗi lớn. Vì thế, tại mỗi gói tin sẽ có thêm phần thông tin nhận định để kiểm soát và điều khiển lỗi.
 - Với các hệ thống truyền thông tốc độ cao hiện nay, phần thông tin kiểm soát lỗi này trở thành không cần thiết và phản tác dụng.
- Công nghệ **Frame Relay** được phát triển để tận dụng ưu điểm của môi trường truyền tốc độ cao và tỷ suất lỗi nhỏ.
 - Nhân tố chính giúp nâng cao tốc độ truyền là loại bỏ phần thông tin thêm vào để kiểm soát lỗi của công nghệ chuyển mạch gói.

2.2 Mạng diện rộng WAN

- **ATM:** Công nghệ phương thức truyền bất đồng bộ (*ATM*) đôi khi còn được gọi là chuyển tiếp tế bào (*cell relay*).



Hiện tại đang là đỉnh cao của cuộc phát triển công nghệ từ công nghệ chuyển mạch kênh và chuyển mạch gói.

ATM có thể được xem là công nghệ tiến hóa từ công nghệ chuyển mạch kênh và frame relay.

2.2 Mạng diện rộng WAN

➤ ATM:

ATM là công nghệ tiến hóa từ công nghệ chuyển mạch kênh

- **Chuyển mạch kênh**: chỉ có duy nhất các kênh truyền với tốc độ truyền cố định.
- **ATM**: cho phép định nghĩa nhiều kênh ảo có tốc độ truyền thay đổi phụ thuộc vào thời điểm tạo ra.

ATM là công nghệ tiến hóa từ công nghệ chuyển mạch gói

- ***ATM*** sử dụng kỹ thuật chuyển mạch gói tương tự như ***Frame Relay*** chỉ khác:
 - **Frame Relay**: sử dụng gói tin kích thước không cố định gọi là *frame*.
 - **ATM**: sử dụng gói tin có kích thước cố định gọi là *cell*.

2.2 Mạng diện rộng WAN

➤ ATM:

ATM là công nghệ tiến hóa từ công nghệ chuyển mạch kênh

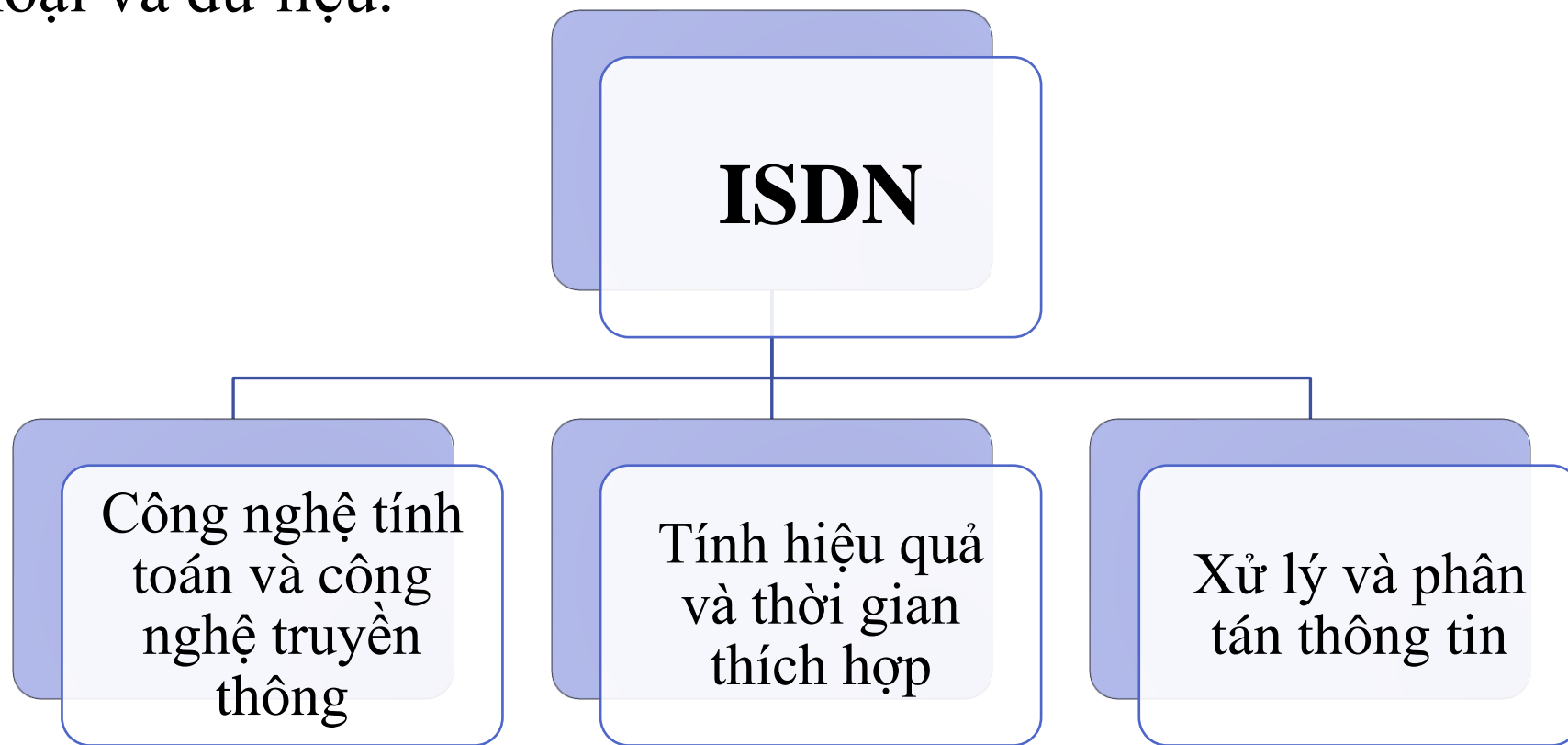
- Cho phép cung cấp một kênh truyền có tốc độ truyền dữ liệu cố định.
- Cho phép thiết lập động bộ tốc độ truyền dữ liệu của nhiều kênh truyền trên cơ sở nhu cầu truyền thông.

ATM là công nghệ tiến hóa từ công nghệ chuyển mạch gói

- Vì sử dụng gói tin có kích thước cố định nên cắt giảm nhiều hơn thông tin thêm vào để kiểm soát và điều khiển lỗi so với Frame Relay.

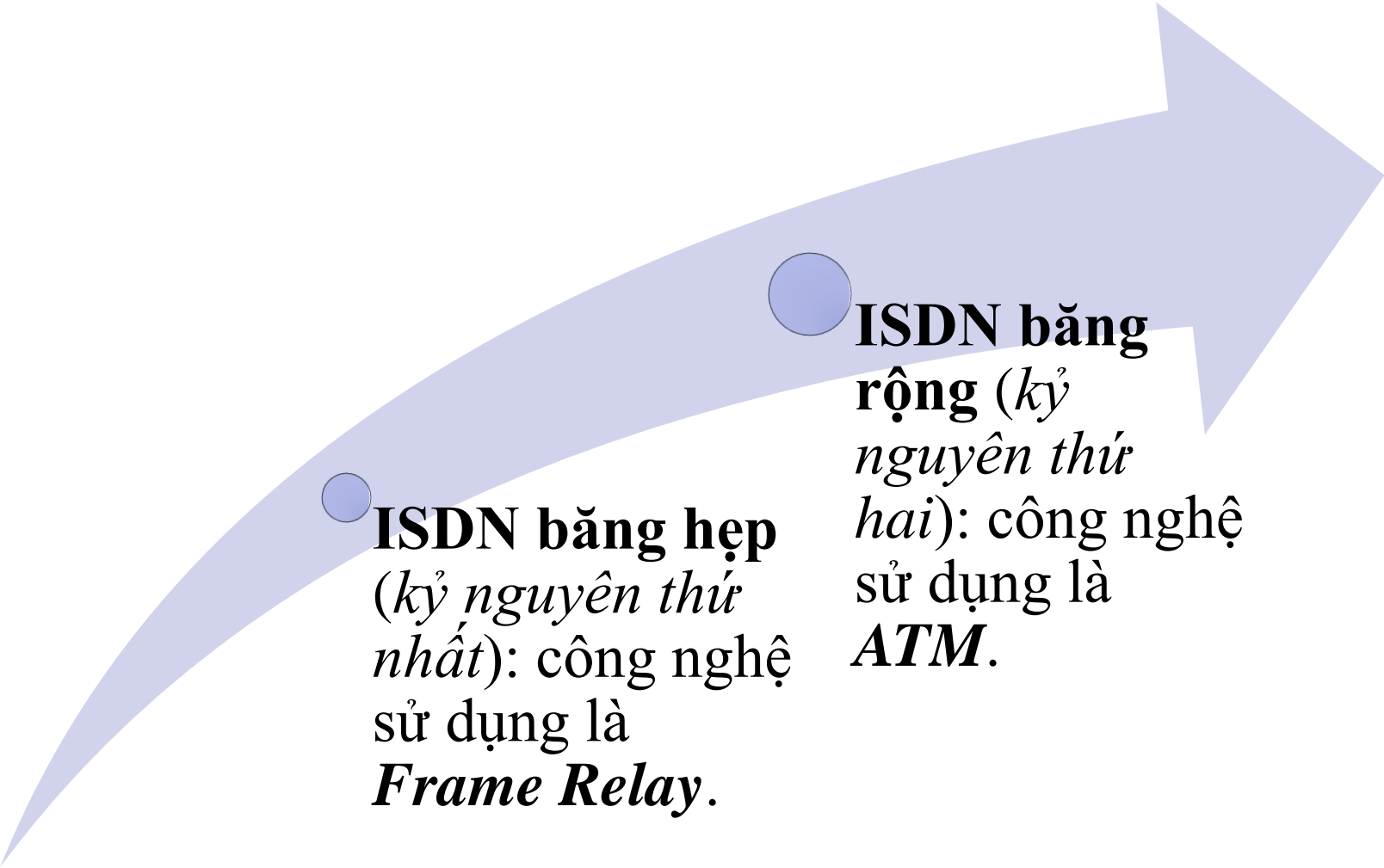
2.2 Mạng diện rộng WAN

- **ISDN:** Dịch vụ tích hợp Mạng kỹ thuật số cung cấp truyền kỹ thuật số các dịch vụ thoại và dữ liệu.



2.2 Mạng diện rộng WAN

➤ ISDN:



ISDN băng hẹp
(*kỹ nguyên thứ nhất*): công nghệ sử dụng là ***Frame Relay***.

ISDN băng rộng (*kỹ nguyên thứ hai*): công nghệ sử dụng là ***ATM***.

2.2 Mạng diện rộng WAN

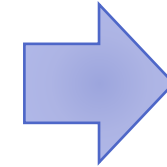
➤ Sự khác nhau giữa mạng WAN và LAN:

WAN

- Phạm vi địa lý lớn (*thành phố, quốc gia*).
- Không chỉ thuộc một tổ chức sở hữu.
- Tốc độ truyền dữ liệu thấp hơn so với mạng LAN.

LAN

- Phạm vi địa lý nhỏ (*tòa nhà hoặc nhóm tòa nhà gần nhau*).
- Thuộc một tổ chức nào đó sở hữu.
- Tốc độ truyền dữ liệu cao hơn nhiều so với mạng WAN.



Vì yếu tố địa lý cũng như tính chất khác nhau nên giải pháp công nghệ giữa mạng **LAN** và **WAN** cũng khác nhau.

2. Mạng máy tính

2.1 Mạng cục bộ LAN

2.2 Mạng diện rộng WAN

2.3 Mạng toàn cầu Internet

2.3 Mạng toàn cầu Internet

Mạng toàn cầu (*Internet*) là một mạng máy tính có phạm vi trải rộng toàn cầu.

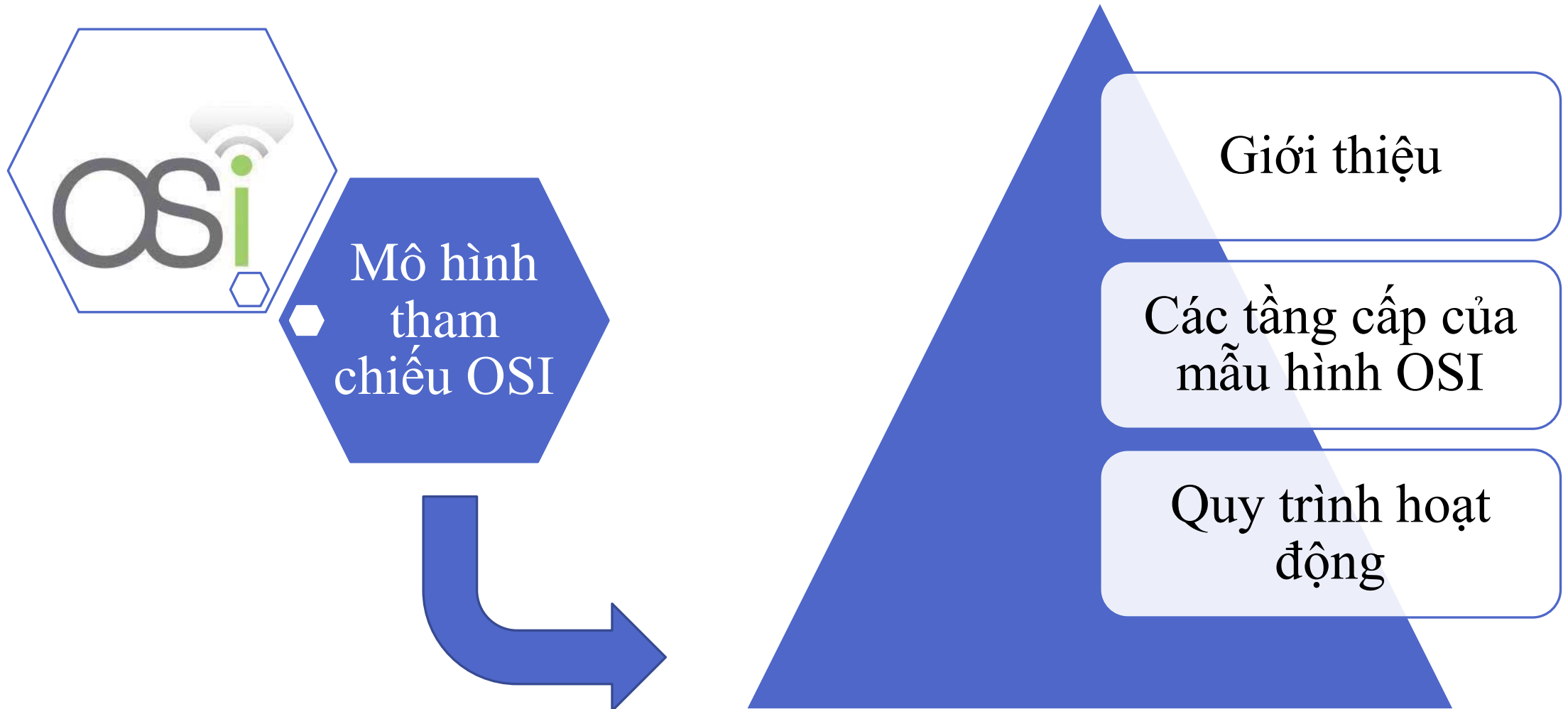
Các ứng dụng chính của mạng Internet:

- Thư điện tử
- Mạng xã hội
- Đăng nhập từ xa
- Truyền tập tin
- Tìm kiếm thông tin
- ...

Nội dung

1. Giới thiệu
2. Mạng máy tính
- 3. Mô hình tham chiếu OSI**
4. Đảm bảo và an toàn thông tin
5. Bài tập

3. Mô hình tham chiếu OSI



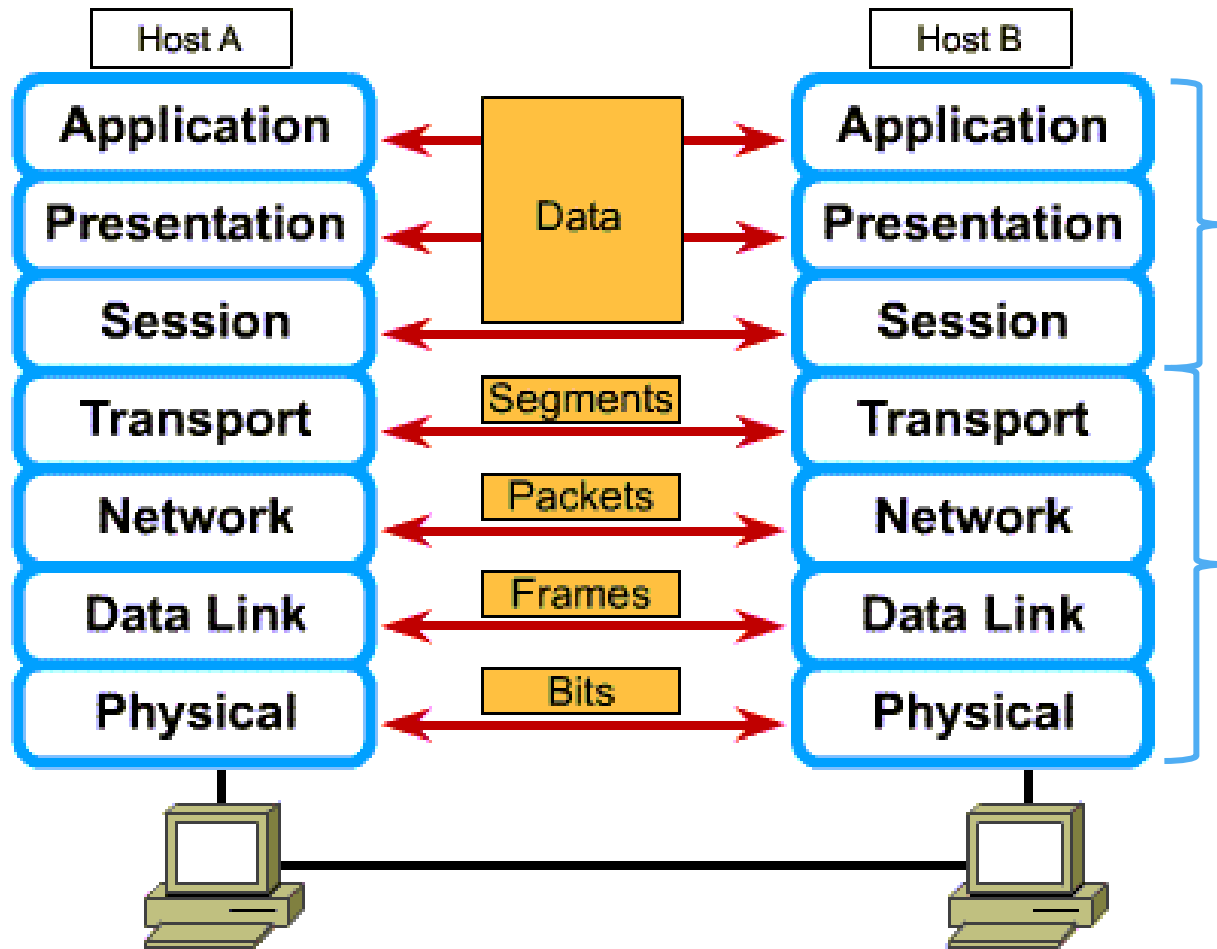
3. Mô hình tham chiếu OSI



Tổ chức tiêu chuẩn quốc tế (*ISO*) đã đưa ra tiêu chuẩn đầu tiên về kiến trúc tổng thể của một hệ thống thông tin hoàn chỉnh gọi là *mô hình tham chiếu OSI*.

Các hệ thống máy tính của các nhà sản xuất khác nhau giao tiếp được với nhau.

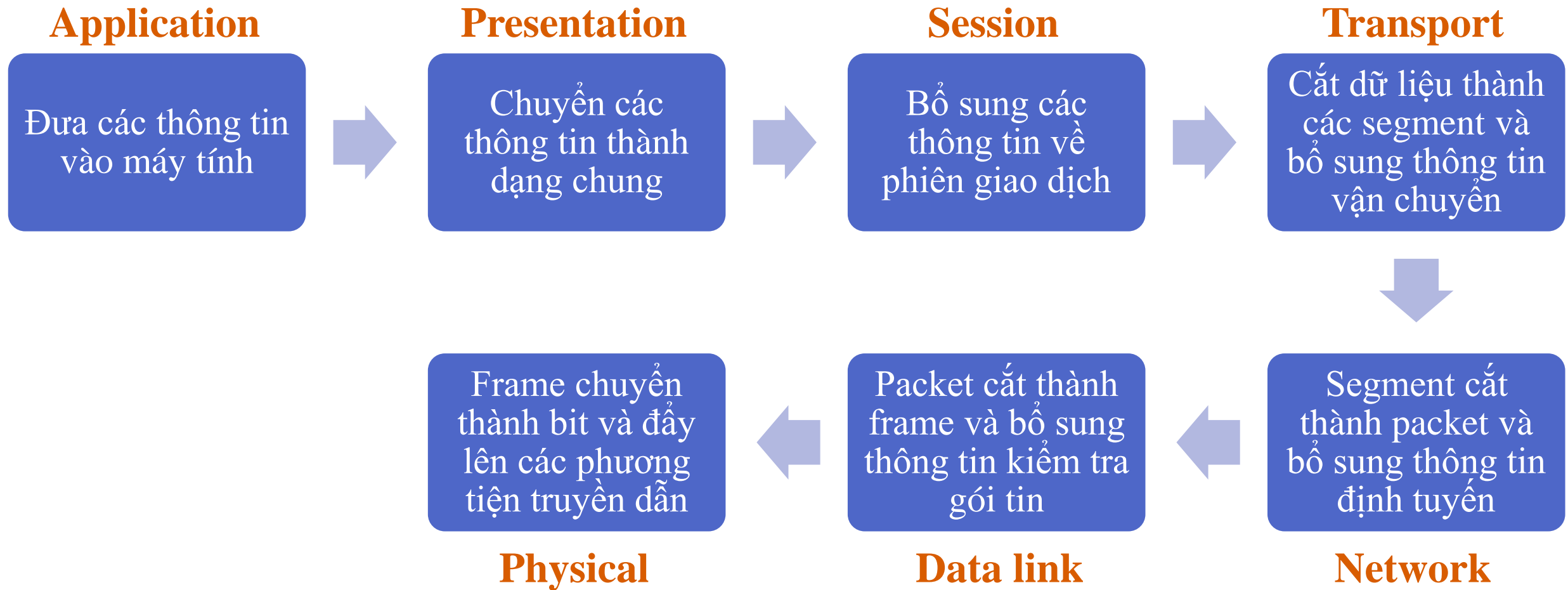
3. Mô hình tham chiếu OSI



3 tầng cao (*phiên, trình diễn và ứng dụng*): đáp ứng các yêu cầu và các ứng dụng của người sử dụng.

4 tầng thấp (*vật lý, liên kết dữ liệu, mạng và giao vận*): quan tâm đến việc truyền dữ liệu giữa các hệ thống cuối qua phương tiện truyền thông.

3. Mô hình tham chiếu OSI



Cách thức truyền gói tin trong Internet



3. Mô hình tham chiếu OSI

Môi trường mạng

Liên quan đến giao thức và các tiêu chuẩn thuộc về các dạng khác nhau của hạ tầng cơ sở mạng truyền số liệu.

Môi trường OSI

Bao gồm môi trường mạng, các giao thức và các tiêu chuẩn hướng ứng dụng để cho phép các hệ thống đầu cuối liên lạc với nhau theo phương thức mở.

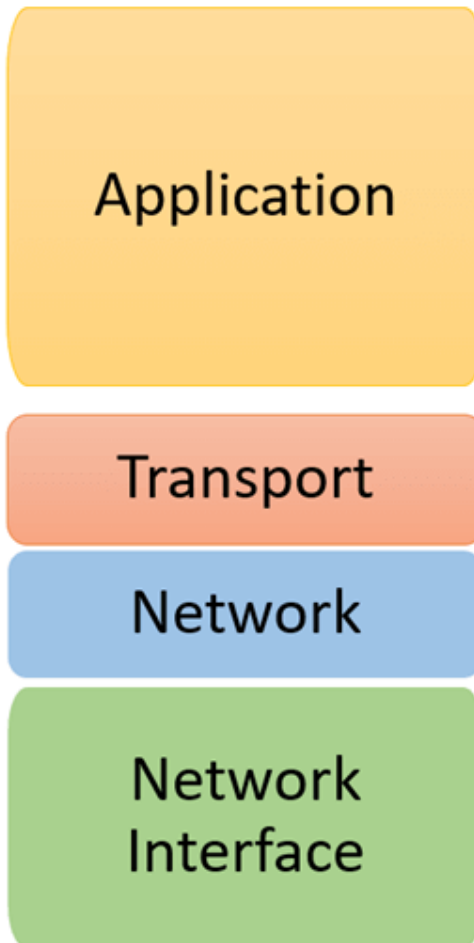
Môi trường hệ thống thực

Xây dựng lên môi trường OSI, liên quan đến các dịch vụ và phần mềm đặc trưng của các nhà chế tạo.

OSI Reference Model



TCP/IP Conceptual Layers

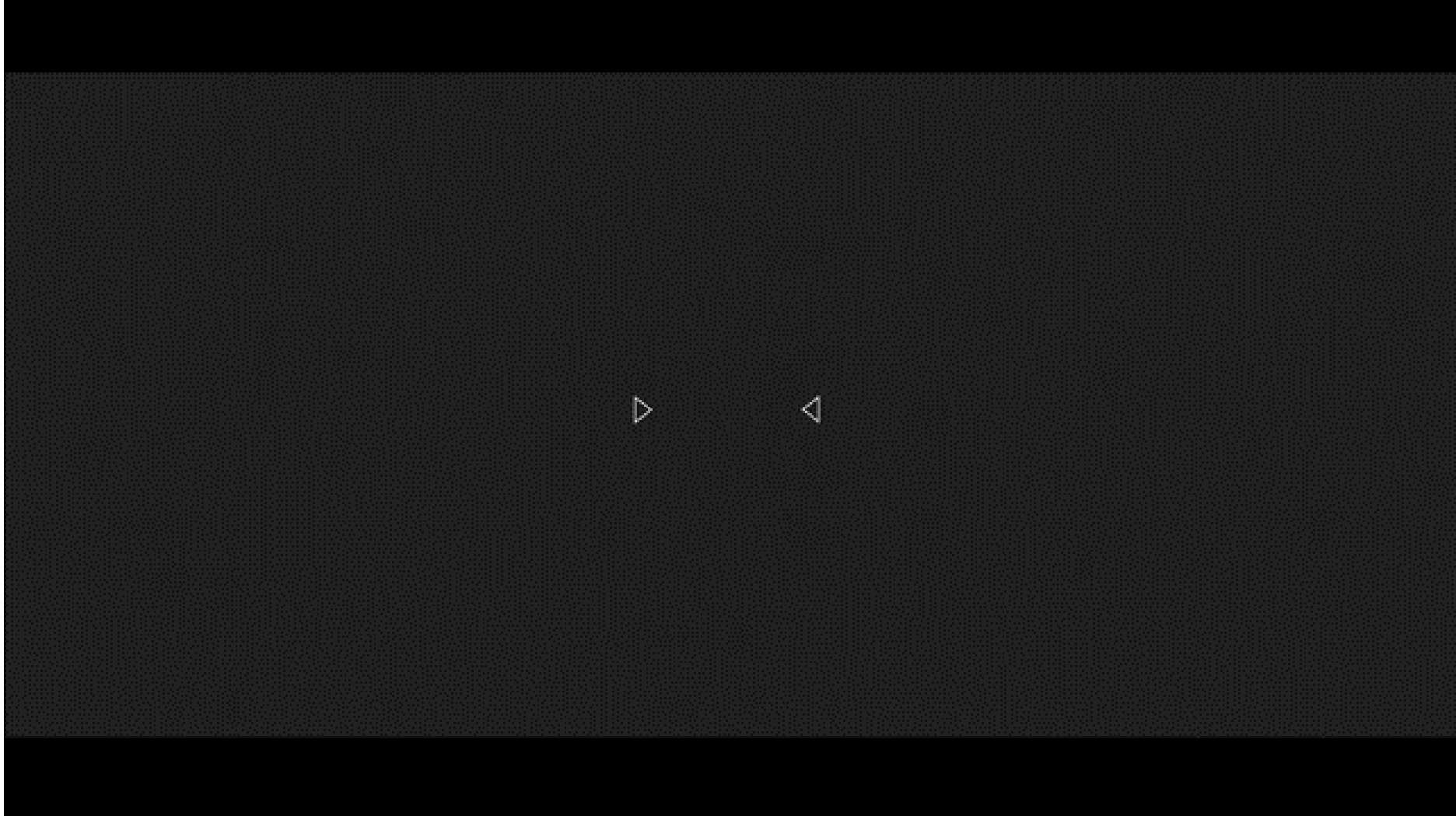


© guru99.com

Mạng toàn cầu Internet

Video minh họa

Mạng toàn cầu Internet



Nội dung

1. Giới thiệu
2. Mạng máy tính
3. Mô hình tham chiếu OSI
- 4. Đảm bảo và an toàn thông tin**
5. Bài tập

4. Đảm bảo và an toàn thông tin

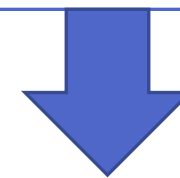
4.1 Giới thiệu

- 4.2 Bảo vệ thông tin trong quá trình truyền thông tin trên mạng
- 4.3 Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

4.1 Giới thiệu



Công nghệ thông tin
và mạng Internet
phát triển ngày càng
mạnh mẽ



Nhiều thông tin
được lưu trữ trên
máy tính và gửi đi
trên Internet

4.1 Giới thiệu

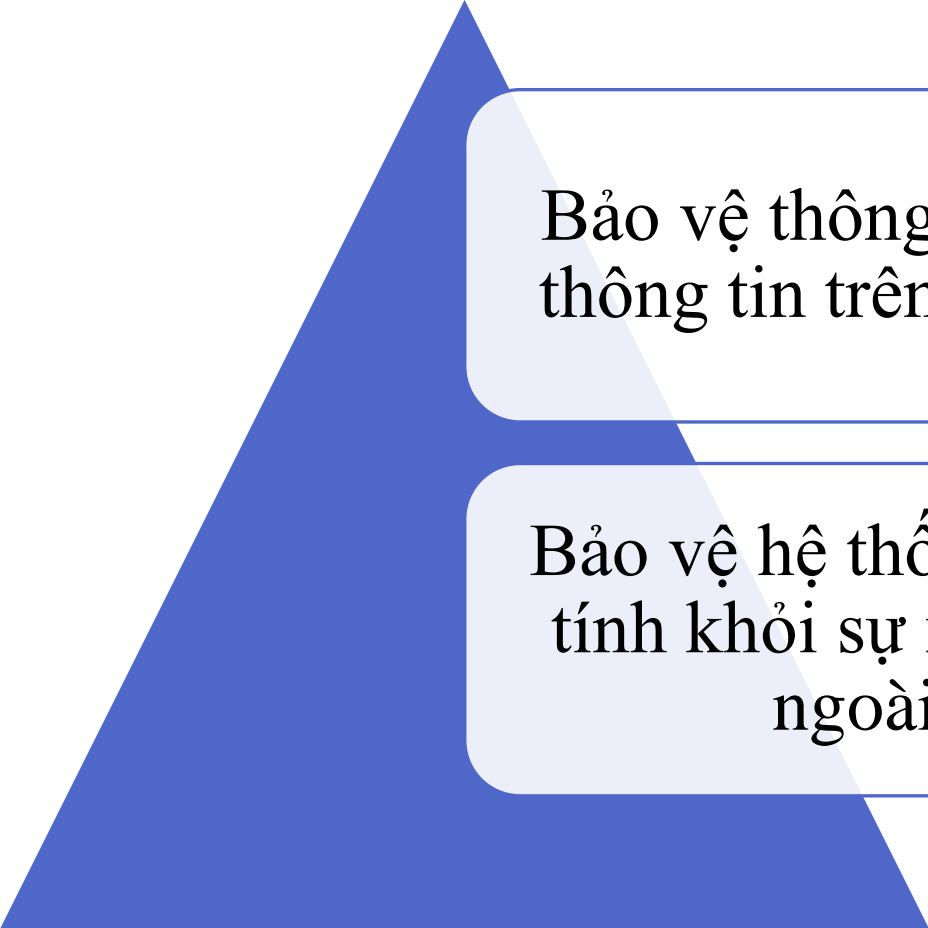


Đảm bảo và an toàn
thông tin ngày càng
trở nên quan trọng



4.1 Giới thiệu

Phân loại mô hình an toàn bảo mật thông tin trên máy tính theo 2 hướng chính:



Bảo vệ thông tin trong quá trình truyền thông tin trên mạng (*Network Security*)

Bảo vệ hệ thống máy tính và mạng máy tính khỏi sự xâm nhập phá hoại từ bên ngoài (*System Security*)

4. Đảm bảo và an toàn thông tin

4.1 Giới thiệu

4.2 Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

4.3 Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

4.2. Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

4.2.1 Các loại hình tấn công

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng

4.2.4 Các giao thức (protocol) thực hiện bảo mật

4.2.1 Các loại hình tấn công

Bối cảnh: Có 3 nhân vật tên là *Alice*, *Bob* và *Trudy*.

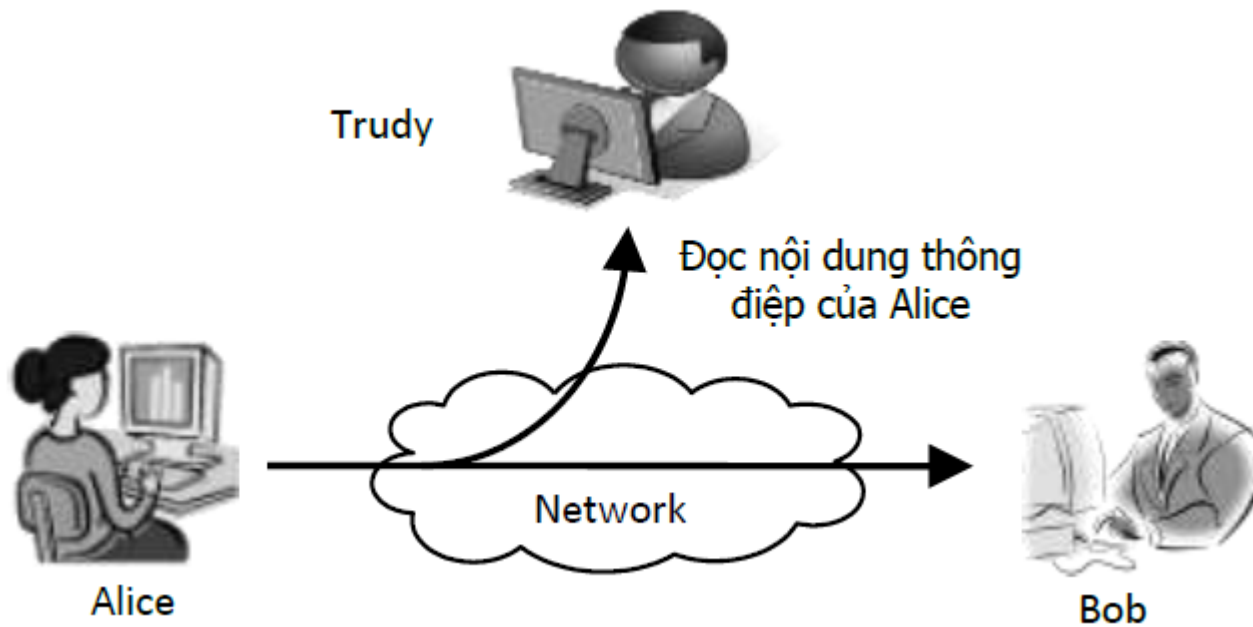
- *Alice* và *Bob* thực hiện trao đổi thông tin với nhau.
- *Trudy* là kẻ xấu, đặt thiết bị can thiệp vào kênh truyền tin giữa *Alice* và *Bob*.



Trudy tấn công quá trình truyền tin của *Alice* và *Bob* như thế nào?

4.2.1 Các loại hình tấn công

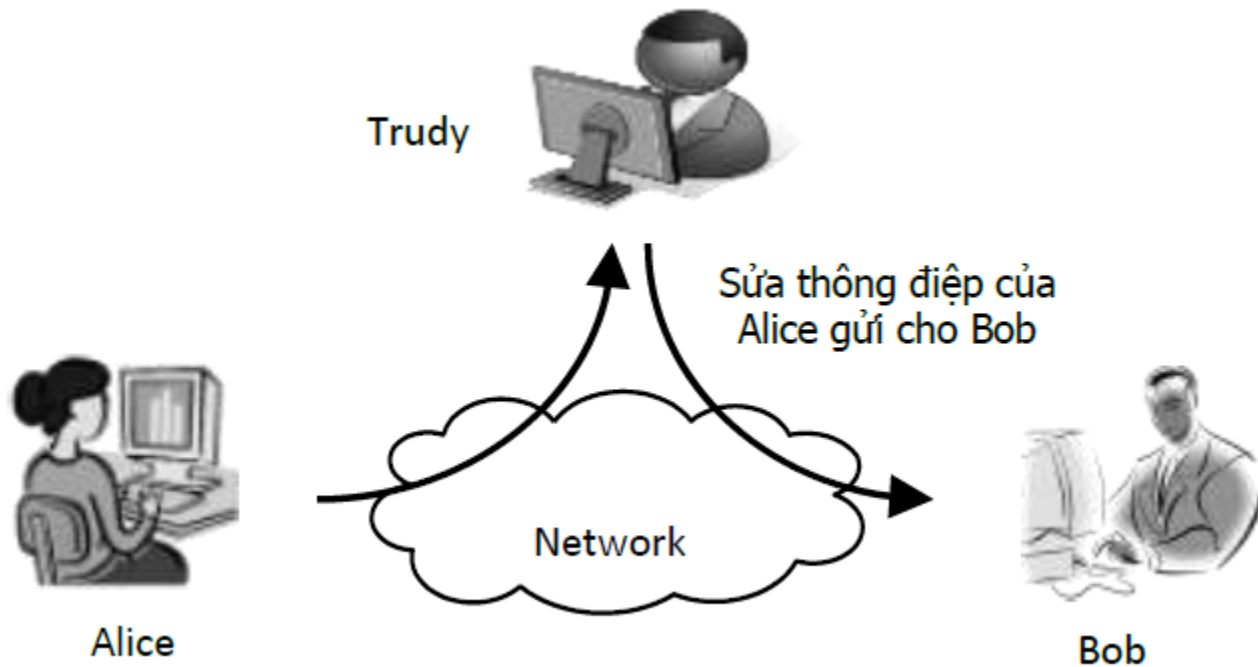
1) Xem trộm thông tin (*Release of Message Content*)



Trudy chặn các thông điệp *Alice* gửi cho *Bob* và xem được nội dung của thông điệp.

4.2.1 Các loại hình tấn công

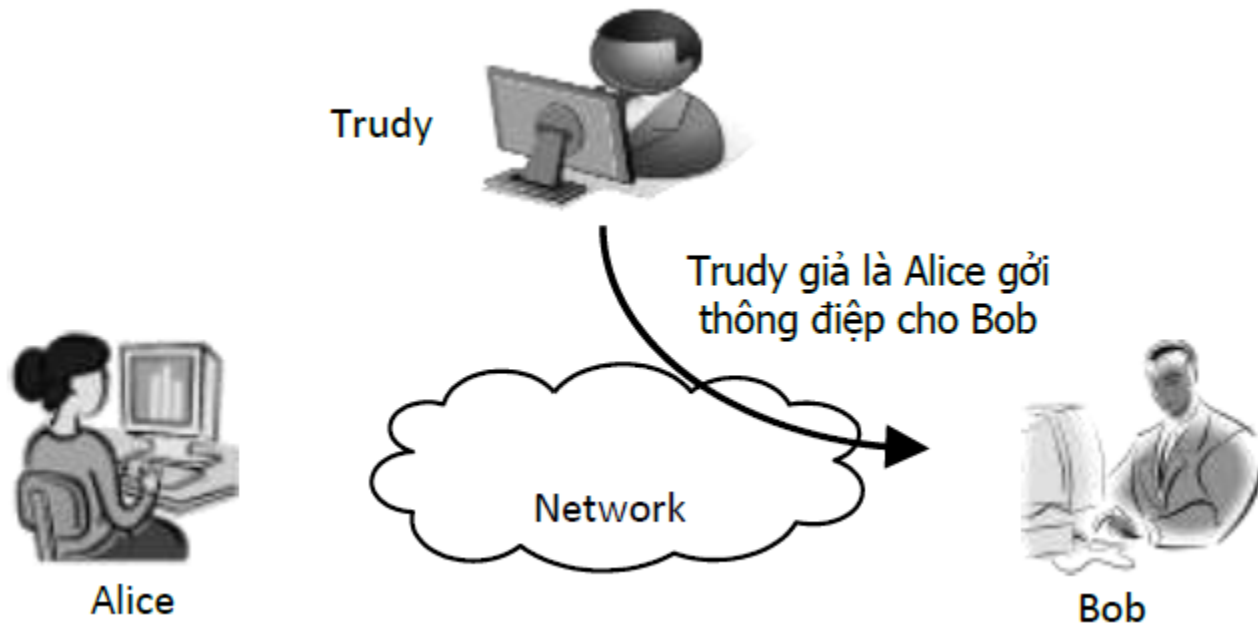
2) Thay đổi thông điệp (*Modification of Message*)



- **Trudy** chặn các thông điệp **Alice** gửi cho **Bob** và ngăn cho các thông điệp này đến đích.
- Sau đó, **Trudy** thay đổi nội dung của thông điệp và gửi tiếp cho **Bob**.

4.2.1 Các loại hình tấn công

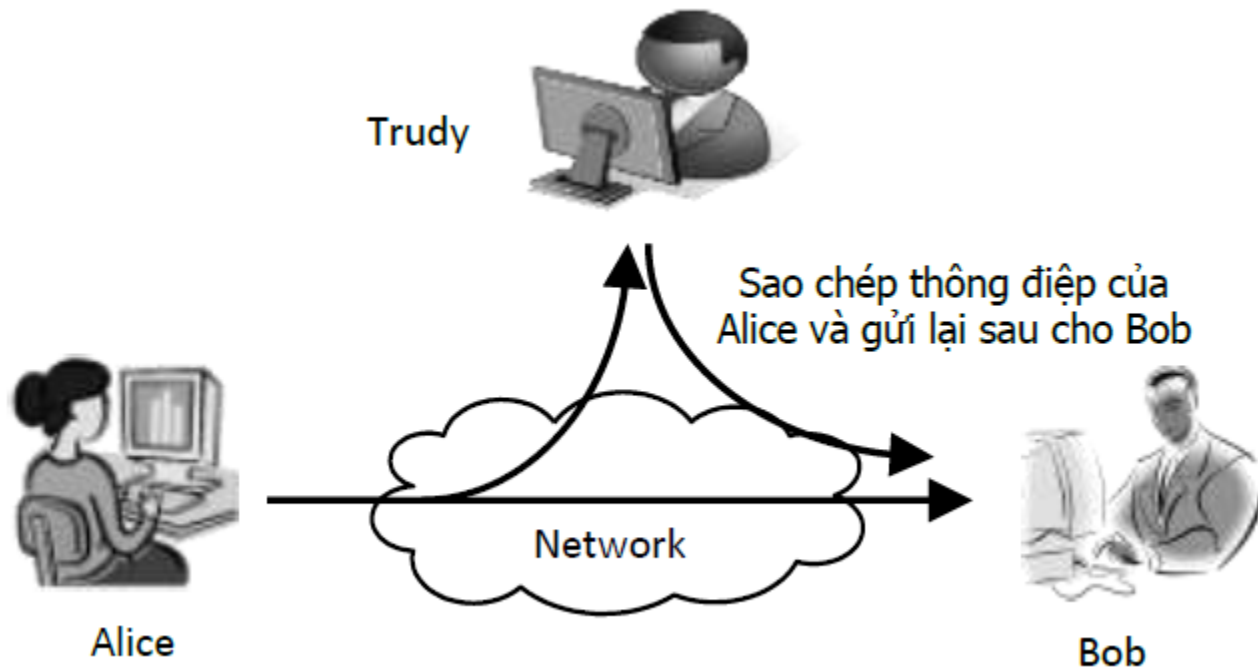
3) Mạo danh (*Masquerade*)



- **Trudy** giả là **Alice** gửi thông điệp cho **Bob**.
- **Bob** không biết điều này và nghĩ rằng thông điệp là của **Alice**.

4.2.1 Các loại hình tấn công

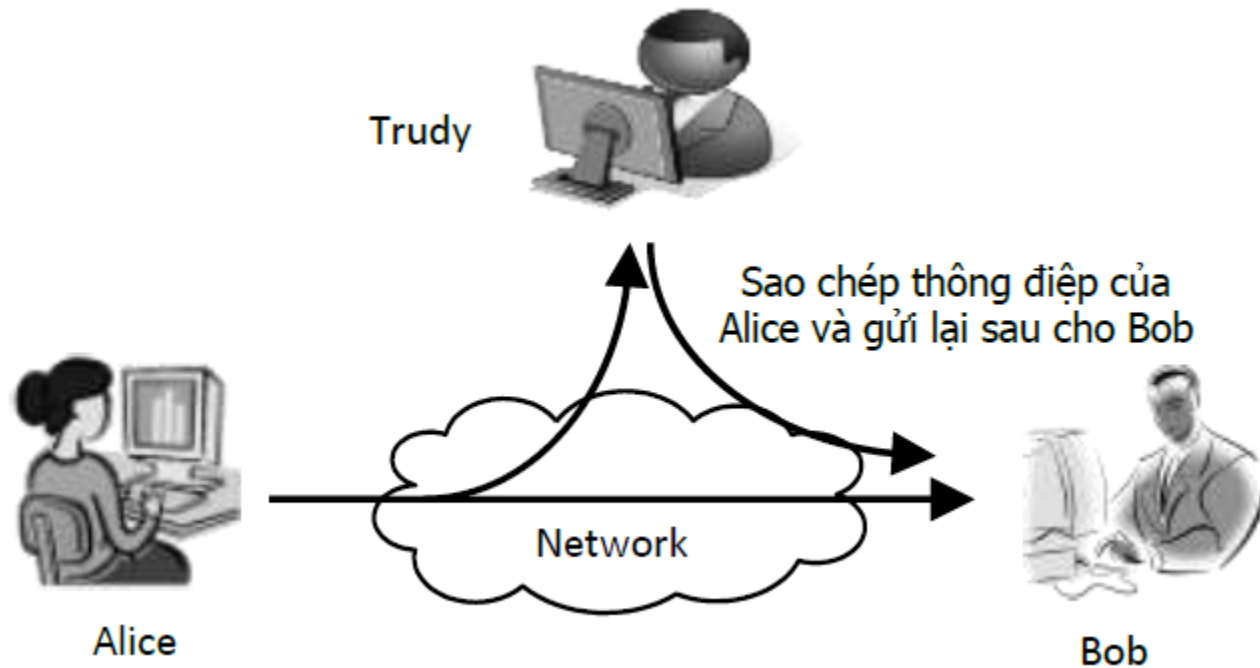
4) Phát lại thông điệp (*Replay*)



- **Trudy** sao chép lại thông điệp **Alice** gửi cho **Bob**.
- Sau một khoảng thời gian, **Trudy** gửi bản sao chép này cho **Bob**.
- **Bob** tin rằng thông điệp thứ 2 vẫn là từ **Alice**, nội dung 2 thông điệp này giống nhau.

4.2.1 Các loại hình tấn công

4) Phát lại thông điệp (*Replay*)



Giả sử:

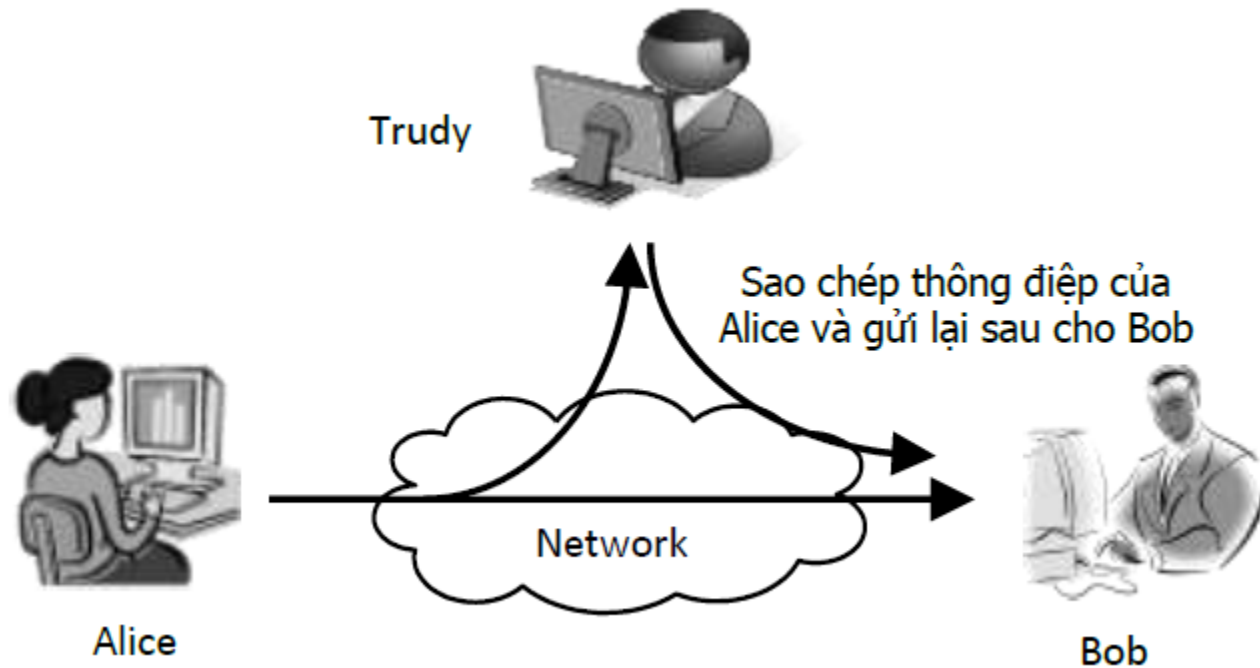
- ***Bob*** là ngân hàng.
- ***Alice*** là khách hàng.

Alice gửi thông điệp đề nghị ***Bob*** chuyển cho ***Trudy*** 1000\$ với biện pháp bảo mật là sử dụng chữ ký điện tử.

Chữ ký điện tử \Rightarrow Tránh việc mạo danh và thay đổi thông điệp.

4.2.1 Các loại hình tấn công

4) Phát lại thông điệp (*Replay*)



Tuy nhiên, nếu *Trudy* sao chép và phát lại thông điệp thì biện pháp bảo vệ này không còn ý nghĩa gì nữa.

Phát lại thông điệp \Rightarrow **Bob** tin rằng **Alice** gửi thông điệp mới và thực hiện giao dịch thêm một lần nữa.

4.2. Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

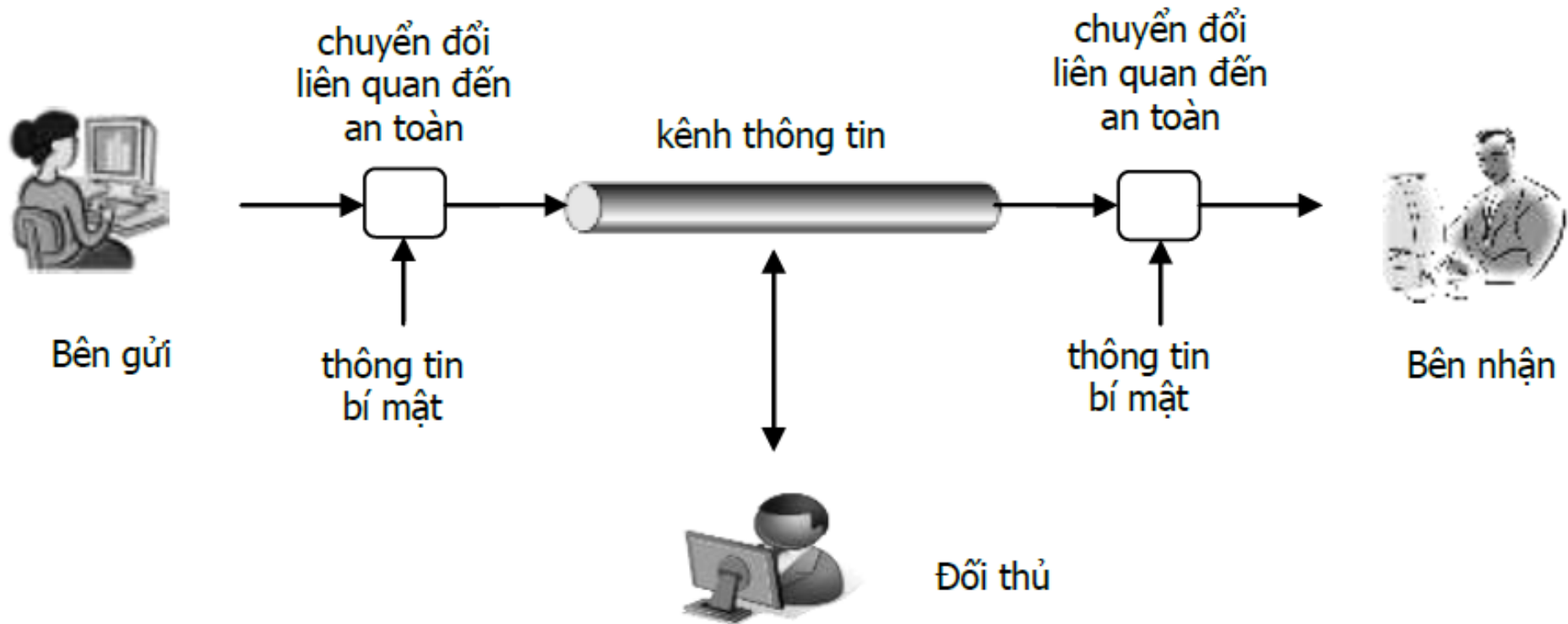
4.2.1 Các loại hình tấn công

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng

4.2.4 Các giao thức (protocol) thực hiện bảo mật

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật



Mô hình bảo mật truyền thông tin trên mạng

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

Tính bảo mật

- Ngăn chặn được vấn đề xem trộm thông điệp.

Tính chứng thực

- Ngăn chặn các hình thức tấn công sửa thông điệp, mạo danh và phát lại thông điệp.

Tính không từ chối

- Xác định người gửi thông điệp và không từ chối trách nhiệm.

4.2. Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

4.2.1 Các loại hình tấn công

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

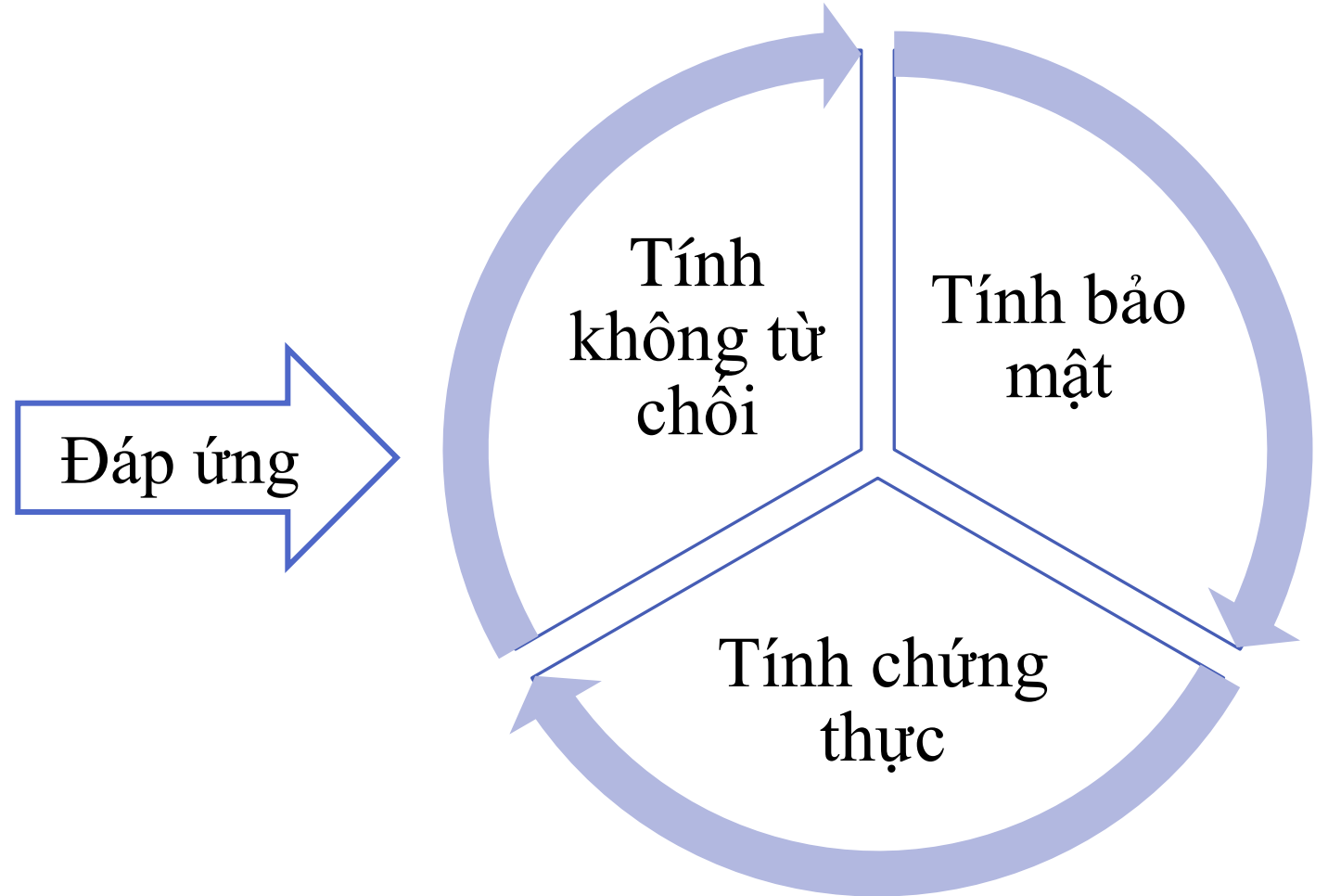
4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng

4.2.4 Các giao thức (protocol) thực hiện bảo mật

4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng



Mật mã hay mã hóa dữ liệu



4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng

- Hệ mật mã là một công cụ cơ bản thiết yếu của bảo mật thông tin.
- Có nhiều cách để phân loại hệ mật mã:

- Mật mã cổ điển (*trước 1970*)
- Mật mã hiện đại (*sau 1970*)

Dựa vào thời gian

- Mã dòng
- Mã khối

Dựa vào cách thức tiến hành mã

- Hệ mật mã đối xứng (*mật mã khóa bí mật*)
- Hệ mật mã bất đối xứng (*mật mã khóa công khai*)

Dựa vào cách truyền khóa

4.2. Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

4.2.1 Các loại hình tấn công

4.2.2 Yêu cầu của một hệ truyền thông tin an toàn và bảo mật

4.2.3 Vai trò của mật mã trong việc bảo mật thông tin trên mạng

4.2.4 Các giao thức (protocol) thực hiện bảo mật

4.2.4 Các giao thức (protocol) thực hiện bảo mật



**Mật mã hay
mã hóa dữ liệu**

Ứng dụng

**Giao thức bảo mật
(protocol)**

Keberos

- Là giao thức dùng để chứng thực dựa trên mã hóa đối xứng.

**Chuẩn chứng
thực X509**

- Dùng trong mã hóa khóa công khai (bất đối xứng).

4.2.4 Các giao thức (protocol) thực hiện bảo mật



**Mật mã hay
mã hóa dữ liệu**

Ứng dụng

**Giao thức bảo mật
(protocol)**

**Secure Socket
Layer (SSL):**

- Là giao thức bảo mật web, được sử dụng phổ biến trong web và thương mại điện tử.

PGP và S/MIME

- Bảo mật thư điện tử email.

4. Đảm bảo và an toàn thông tin

4.1 Giới thiệu

4.2 Bảo vệ thông tin trong quá trình truyền thông tin trên mạng

4.3 Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Thực hiện bảo vệ thông qua việc “*kiểm soát truy cập*” với 2 yếu tố sau:

Chứng thực truy cập (*Authentication*)

- Xác nhận rằng đối tượng (*con người hay chương trình máy tính*) được cấp phép truy cập vào hệ thống.

Phân quyền (*Authorization*)

- Các hành động được phép thực hiện sau khi đã truy cập vào hệ thống.

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Ví dụ:

Chứng thực truy cập (*Authentication*)

- Login vào máy tính bằng *username* & *password*.
- Phương pháp sinh trắc học (*dấu vân tay, mống mắt, ...*)

Phân quyền (*Authorization*)

- Phân quyền cho ***user account*** trong hệ thống (*ví dụ chỉ có quyền đọc file nhưng không có quyền chỉnh sửa file, ...*)

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Với 2 nguyên tắc trên, máy tính và mạng máy tính sẽ được bảo vệ khỏi sự xâm nhập.

Tuy nhiên, các vụ tấn công phá hoại vẫn xảy ra.

- Để thực hiện điều đó, kẻ phá hoại tìm cách phá bỏ 2 cơ chế: *chứng thực truy cập và phân quyền*.

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Các cách thức phá hoại:

➤ Dùng các đoạn mã phá hoại (Malware)

Đoạn mã độc (*virus, worm, Trojan, ...*) lan truyền từ máy tính này sang máy tính khác

Dựa trên sự bất cẩn của người sử dụng hay các lỗi của phần mềm

Lợi dụng các quyền được cấp cho người sử dụng (*chẳng hạn rất nhiều người login vào máy tính với quyền administrator*)

Gửi cho *hacker*, cài đặt các cổng hậu để *hacker* bên ngoài xâm nhập

Các đoạn mã này thực hiện các lệnh phá hoại hoặc dò tìm password của quản trị hệ thống

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài

Các cách thức phá hoại:

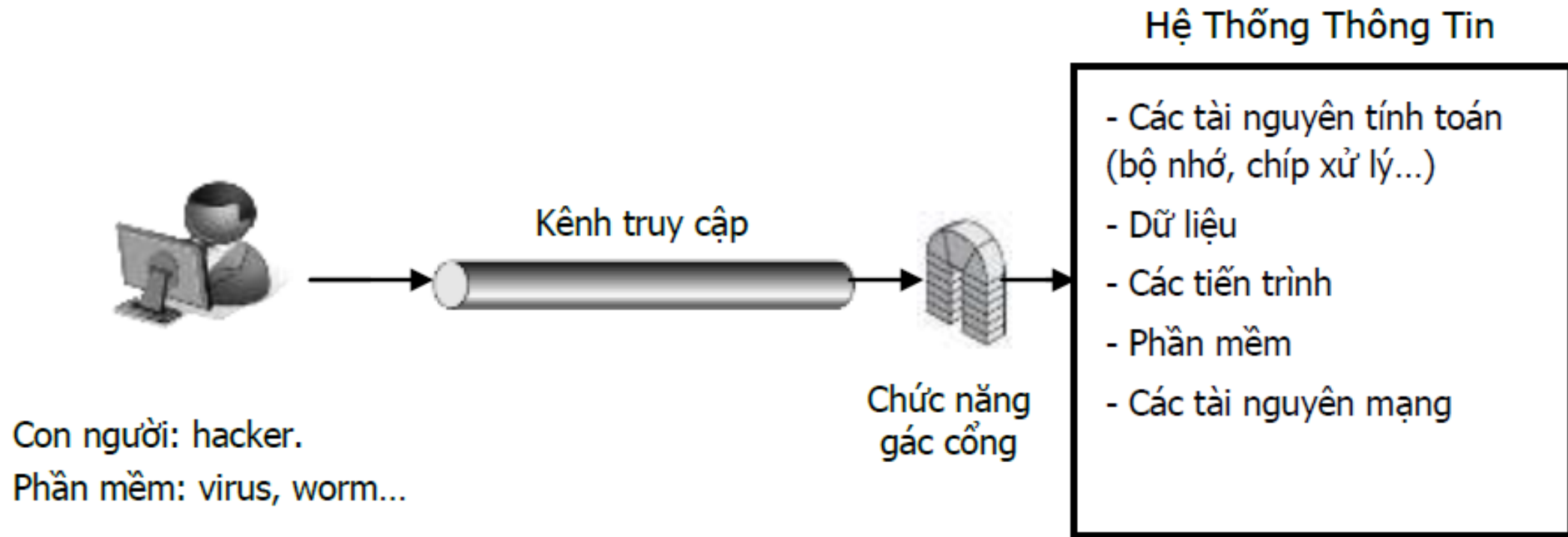
➤ Thực hiện các hành vi xâm phạm (Intrusion)

Việc thiết kế các phần mềm có nhiều lỗ hổng, dẫn đến các *hacker* lợi dụng để thực hiện những lệnh phá hoại

Lỗ hổng phần mềm cho phép thực hiện những lệnh phá hoại mà ngay cả người thiết kế chương trình không ngờ tới

Hacker có thể sử dụng các cổng hậu do các *backdoor* tạo ra để xâm nhập

4.3. Bảo vệ hệ thống khỏi sự xâm nhập phá hoại từ bên ngoài



Chương trình có chức năng gác cổng dò tìm virus hoặc dò tìm các hành vi xâm phạm để ngăn chặn chúng, không cho chúng thực hiện hoặc xâm nhập.

Ví dụ: các chương trình chống virus, chương trình firewall...

Nội dung

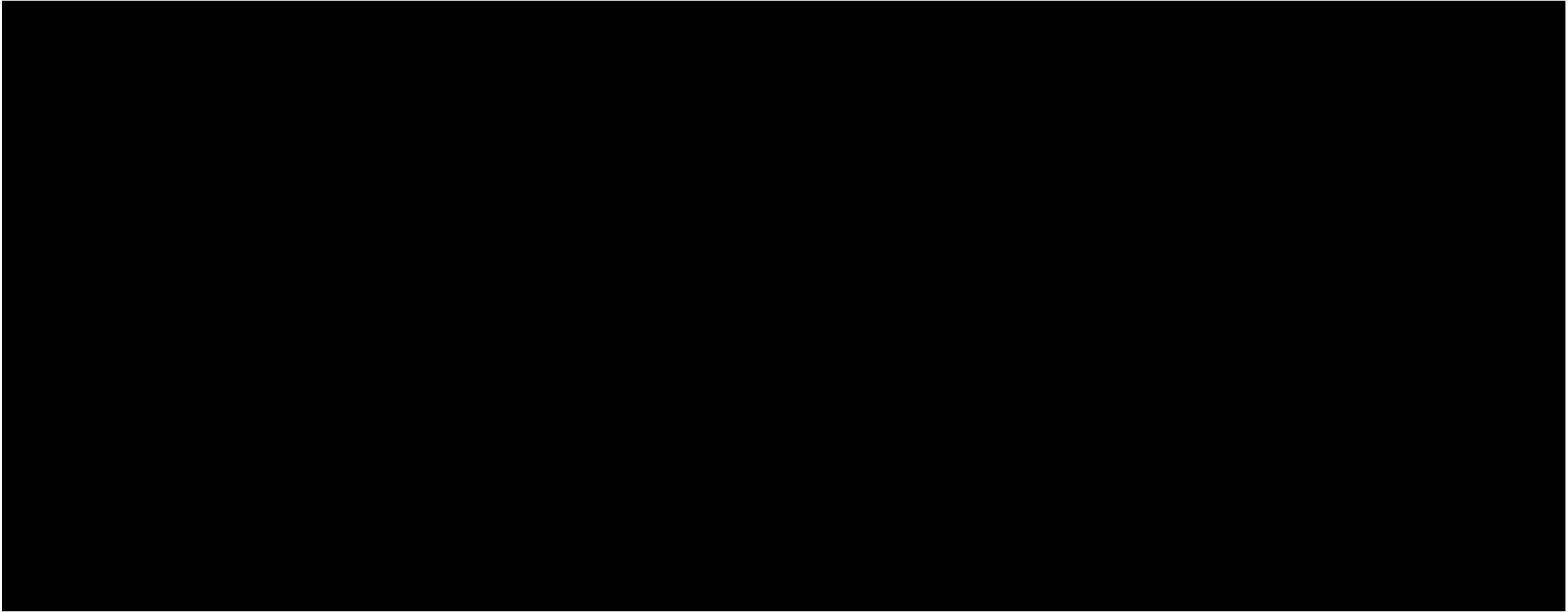
1. Giới thiệu
2. Mạng máy tính
3. Mô hình tham chiếu OSI
4. Đảm bảo và an toàn thông tin
- 5. Bài tập**

5. Bài tập

Tìm hiểu về các công nghệ kỹ thuật số được kỳ vọng phát triển trong tương lai (**Ví dụ công nghệ được minh họa trong video Microsoft: Productivity Future Vision**).

Link tham khảo: <https://www.youtube.com/watch?v=w-tFdreZB94>

5. Bài tập



Question & Answer
