ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN

TRẦN DUY MINH

GIẢI PHÁP AN NINH TRONG KIẾN TRÚC QUẢN TRỊ MẠNG SNMP

Chuyên ngành: Khoa học máy tính

Mã số: 60.48.01

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Người hướng dẫn: PGS.TS Nguyễn Văn Tam

Thái Nguyên, tháng 12/2008

MỤC LỤC

CÁC THUẬT NGỮ VIẾT TẮT

THUẬT NGỮ, VIẾT TẮT	MÔ TẢ Ý NGHĨA
ARP	Address Ressulation Protocol
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
Buffer	Bộ đệm
CA	Certificate Authentication
CHAP	Challenge Handshake Authentication Protocol
Datagram	Đơn vị dữ liệu
DES	Data Encryption Standard
full-duplex	Cơ chế truyền song công
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Message Protocol
ISN	Initial Sequence Number
JNDI	Java Naming Directory Interface
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
MSS	Maximum Segment Size
NAS	Network Access Service
NMS	Network Management System
OID	Object identifier
Packet filtering	Bộ lọc gói tin
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Ressulation Protocol
RAS	Remote Access Service
RFC	Requests for Comments
RMON	Remote Network Monitoring
Segment	Đoạn dữ liệu
SGMP	Simple Gateway Management Protocol
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol

DANH MỤC CÁC HÌNH

ĐẶT VẤN ĐỀ

Công nghệ mạng Internet/Intranet đang phát triển mạnh mẽ và xu hướng tích hợp các mạng không đồng nhất để chia sẻ thông tin cũng xuất hiện ngày càng nhiều. Việc bảo đảm hệ thống mạng phức tạp, có quy mô lớn hoạt động tin cậy, hiệu năng cao, thông tin tin cậy đòi hỏi phải phải có hệ quản trị mạng để thu thập và phân tích một số lượng lớn dữ liệu một cách hiệu quả. Tuy nhiên, thông tin quản trị mạng lại phải truyền trên môi trường Internet, có thể bị thất thoát, thay đổi hay giả mạo cần phải được bảo vệ. Các phiên bản SNMPv1 và SNMPv2 mới chỉ đưa ra giải pháp xác thực yếu dựa trên cộng đồng (community). Chính vì vậy, việc nghiên cứu các giải pháp bảo đảm tính xác thực, tính toàn vẹn, tính mật của các thông điệp quản trị mạng là hết sức cần thiết. Phiên bản SNMPv3 đã ra đời nhằm đáp ứng một phần yêu cầu cấp bách này. Tuy nhiên, việc lựa chọn mô hình thực thi vẫn còn nhiều vấn đề cần giải quyết. Tôi chọn hướng nghiên cứu này mong muốn đóng góp, xây dựng thử nghiệm vào một mô hình cụ thể và qua đó đánh giá khả năng triển khai trong thực tế hệ thống quản trị mạng có độ an ninh cao.

Khuôn khổ luận văn bao gồm 3 chương:

Chương 1: Tổng quan về quản trị và an ninh thông tin trên Internet.

Chương 2: Nghiên cứu giải pháp an ninh mạng SNMP.

Chương 3: *Xây dựng mô hình thử nghiệm.*

Em xin chân thành cảm ơn sự nhiệt tình giúp đỡ của thầy giáo PGS.TS Nguyễn Văn Tam đã giúp em hoàn thành luận văn.

Người thực hiện

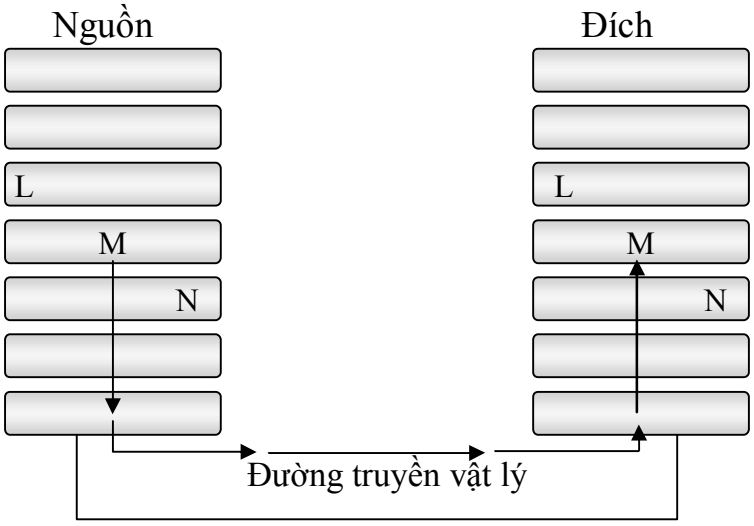
Trần Duy Minh

Chương 1: TỔNG QUAN VỀ QUẢN TRỊ VÀ AN NINH THÔNG TIN TRÊN INTERNET

1.1. Giao thức và dịch vụ Internet

Bộ giao thức là tập hợp các giao thức cho phép sự truyền thông mạng từ một host thông qua mạng đến host khác. Giao thức là một mô tả hình thức của một tập luật và tiêu chuẩn khống chế một khía cạnh đặc biệt trong hoạt động thông tin của các thiết bị trên mạng. Giao thức xác định dạng thức, định thời, tuần tự và kiểm soát lỗi trong hoạt động truyền số liệu. Không có giao thức, máy tính không thể tạo ra hay tái tạo luồng bít đến từ máy tính khác sang dạng ban đầu. Các giao thức điều khiển tất cả các khía cạnh của hoạt động truyền số liệu, bao gồm:

- Mạng vật lý được xây dựng như thế nào.
- Các máy tính được kết nối đến mạng như thế nào.
- Số liệu được định dạng như thế nào để truyền.
- Số liệu được truyền như thế nào.
- Đối phó với lỗi như thế nào.



L, M, N	Các lớp trong mô hình truyền thông
Msource, Mdestination	Các lớp ngang hàng
⟶	Truyền thông ngang hàng
M layer Protocol	Các nguyên tắc thông tin giữa Msource và Mdestination

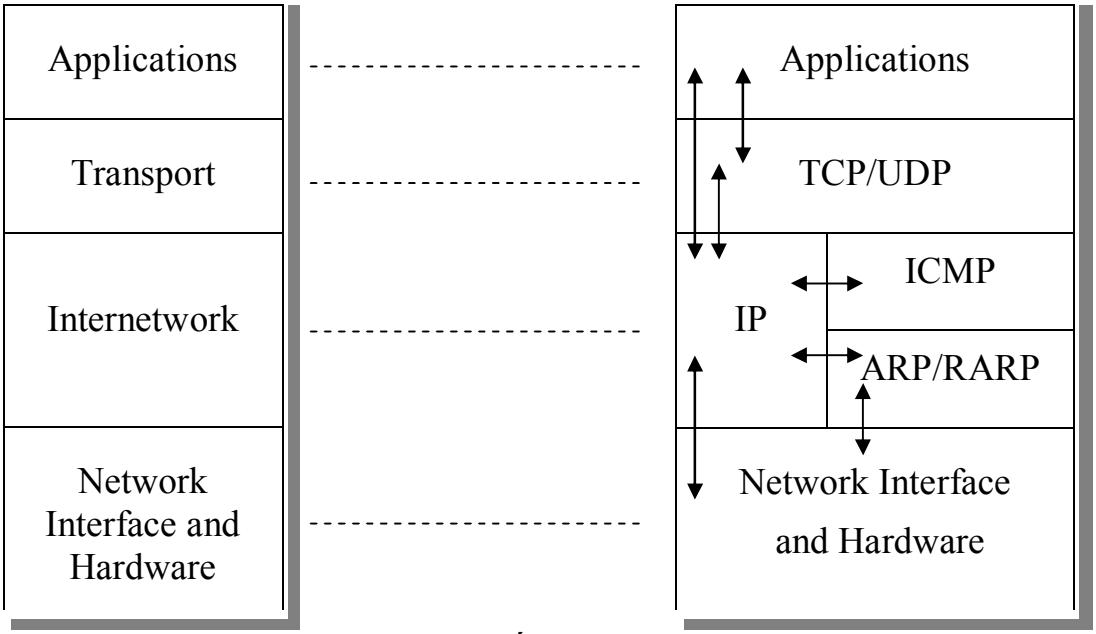
Hình 1.1: Giao thức truyền thông trên máy tính

Các luật mạng này được tạo ra và duy trì bởi nhiều tổ chức và hiệp hội khác nhau. Bao gồm trong các nhóm này là IEEE, ANSI, TIA/EIA và ITU-T (trước đây là CCITT).

1.1.1. Giới thiệu giao thức TCP/IP

Giao thức TCP/IP (Transmission Control Protocol/Internet Protocol) là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên Internet toàn cầu. TCP/IP được xem là giản lược của mô hình tham chiếu OSI với 4 tầng như sau:

+ Tầng liên kết mạng (Network Access Layer)
+ Tầng Internet (Internet Layer)
+ Tầng giao vận (Host-To-Host Transport Layer)
+ Tầng ứng dụng (Application Layer)

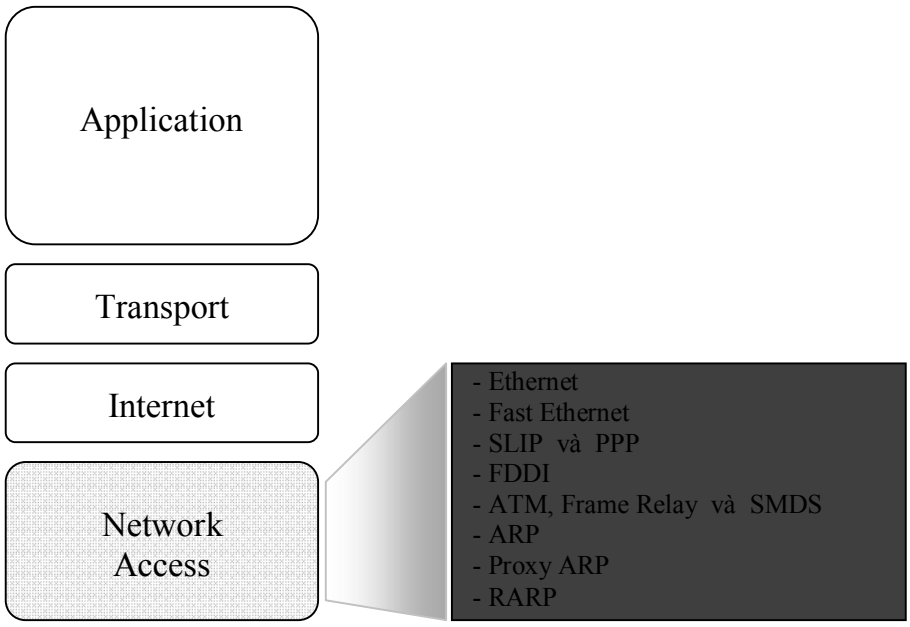


Hình 1.2. Kiến trúc TCP/IP

➢*Tầng liên kết:* Tầng liên kết (còn được gọi là tầng liên kết dữ liệu hay là tầng giao tiếp mạng) là tầng thấp nhất trong mô hình TCP/IP, bao gồm các thiết bị giao tiếp mạng và chương trình cung cấp các thông tin cần thiết để có thể hoạt động, truy nhập đường truyền vật lý qua thiết bị giao tiếp mạng

đó. Nó bao gồm các chi tiết của công nghệ LAN, WAN và tất cả các chi tiết chứa trong lớp vật lý và lớp liên kết số liệu của mô hình OSI.

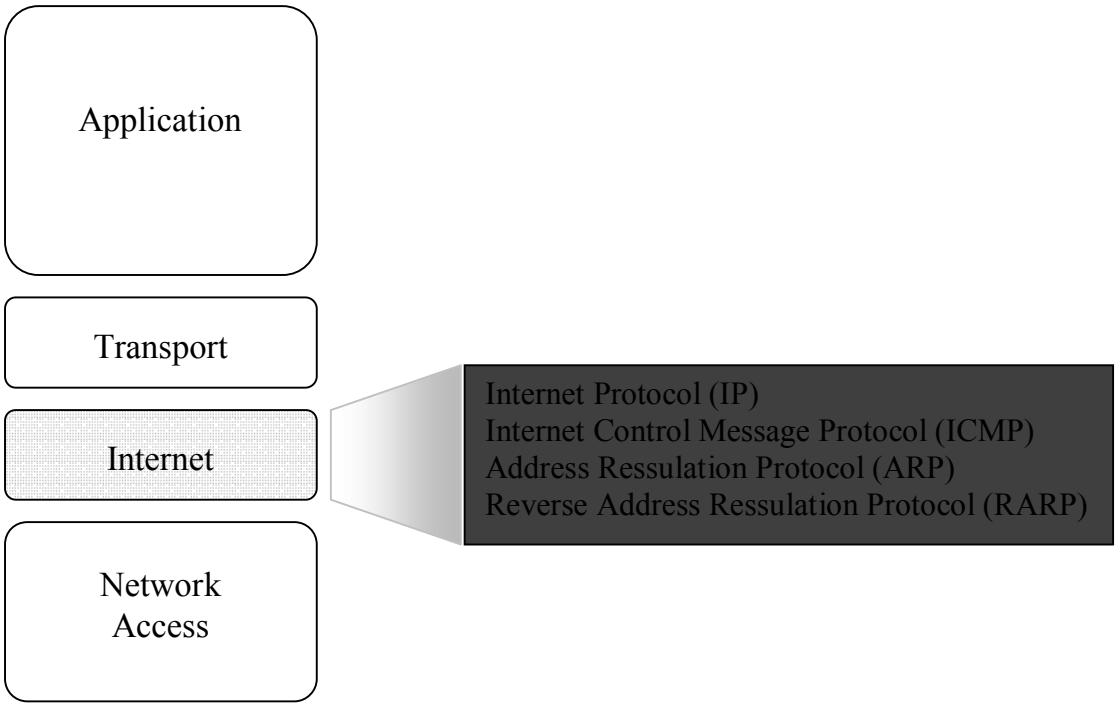
Lớp liên kết định ra các thủ tục để giao tiếp với phần cứng mạng và truy nhập môi trường truyền. Các tiêu chuẩn giao thức modem như SLIP (Serial Line Internet Protocol) và PPP (Point-To-Point Protocol) cung cấp truy xuất mạng thông qua kết nối dùng modem.



Hình 1.3: Các giao thức thuộc lớp Network Access

Chức năng của lớp truy nhập mạng bao gồm ánh xạ địa chỉ IP sang địa chỉ vật lý và đóng gói (encapsulation) các gói IP thành các frame. Căn cứ vào dạng phần cứng và giao tiếp mạng, lớp truy nhập mạng sẽ xác lập kết nối với đường truyền vật lý của mạng.

➢*Tầng Internet*: Tầng Internet (còn gọi là tầng mạng) xử lý qua trình truyền gói tin trên mạng. Các giao thức của tầng này bao gồm: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Message Protocol). Mục đích của lớp Internet là chọn lấy một đường dẫn tốt nhất xuyên qua mạng cho các gói di chuyển tới đích. Giao thức chính hoạt động tại lớp này là Internet Protocol. Sự xác định đường dẫn tốt nhất và mạch chuyển gói diễn ra tại lớp này.



Hình 1.4: Các giao thức tại lớp Internet

- IP cung cấp conectionless, định tuyến chuyển phát gói theo best-effort. IP không quan tâm đến nội dung của các gói nhưng tìm kiếm đường dẫn cho gói tới đích.

- ICMP (Internet Control Message Protocol): đem đến khả năng điều khiển và chuyển thông điệp.

- ARP (Address Ressulation Protocol): xác định địa chỉ lớp liên kết số liệu (MAC address) khi biết trước địa chỉ IP.

- RARP (Reverse Address Ressulation Protocol): xác định các địa chỉ IP khi biết trước địa chỉ MAC.

IP thực hiện các hoạt động sau:

+ Định nghĩa một gói là một lược đồ đánh địa chỉ.

+ Trung chuyển số liệu giữa lớp Internet và lớp truy nhập mạng.

+ Định tuyến chuyển các gói đến host ở xa.

➢*Tầng giao vận*: Tầng giao vận phụ trách luồng giữ liệu giữa hai trạm thực hiện các ứng dụng của tầng trên. Tầng này có hai giao thức chính: TCP (Transmission Protocol), UDP (User Datagram Protocol).