SNMP MANAGEMENT

Simple Network Management Protocol – SNMP

Trình bày: Bùi Minh Quân
Email: bmquan@cit.ctu.edu.vn

NỘI DUNG

- Tổng quan quản lý SNMP
- Kiến trúc quản lý SNMP
- Các phiên bản SNMP

Tổng quan

- SNMP là giao thức quản lý mạng phổ biến nhất
- Giao thức được sử dụng trong mô hình quản lý Internet
- Mô hình quản lý SNMP :
  - Organization Model
    - Relationship between network element, agent, and manager
    - Hierarchical architecture
  - Information Model
    - Uses ASN.1 syntax
    - SMI (Structure of Management Information)
    - MIB (Management Information Base)
  - Communication Model
    - SNMP over TCP/IP
    - Communication services addressed by messages
    - Security framework community-based model

Functional Model

- Fault
- Performance
- Configuration
- Accounting
- Security

Giao thức SNMP

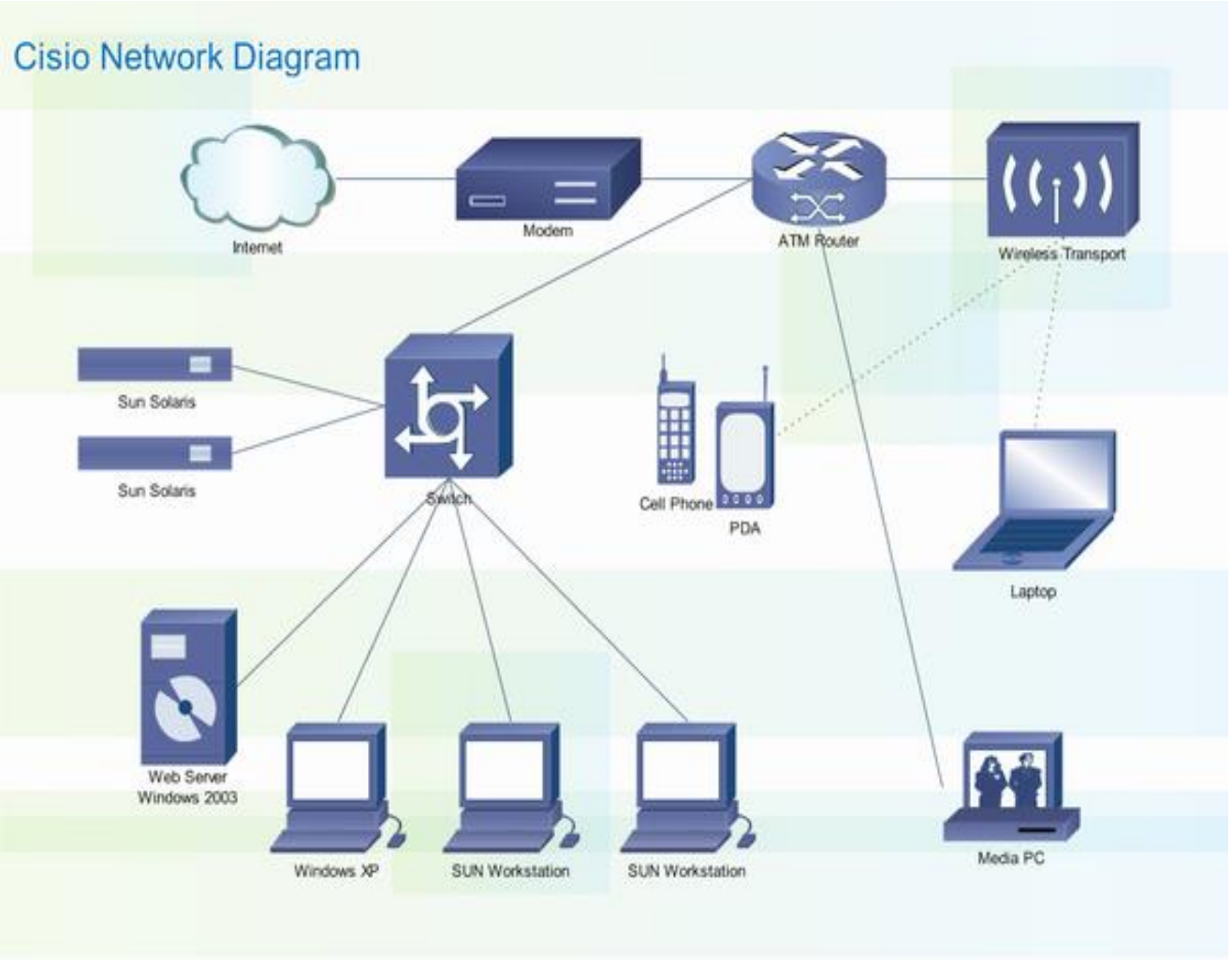
- SNMP là một giao thức lớp ứng dụng được sử dụng để quản lý tài nguyên mạng
  - Giới thiệu lần đầu năm 1988
  - Thiết kế đơn giản – chạy trên nền TCP/IP
  - Được định nghĩa bởi IETF

Giới thiệu SNMP

- Khả năng của SNMP :
  - Giám sát lưu lượng, băng thông mạng
  - Giám sát mức độ sử dụng: HDD, Ram, CPU
  - Giám sát trạng thái và mức độ sử dụng dịch vụ
  - Giám sát nhiệt độ của thiết bị
  - Cảnh báo khi switch, router có một port bị down.
  - Điều khiển tắt/mở các port trên switch, .v.v

Giới thiệu SNMP

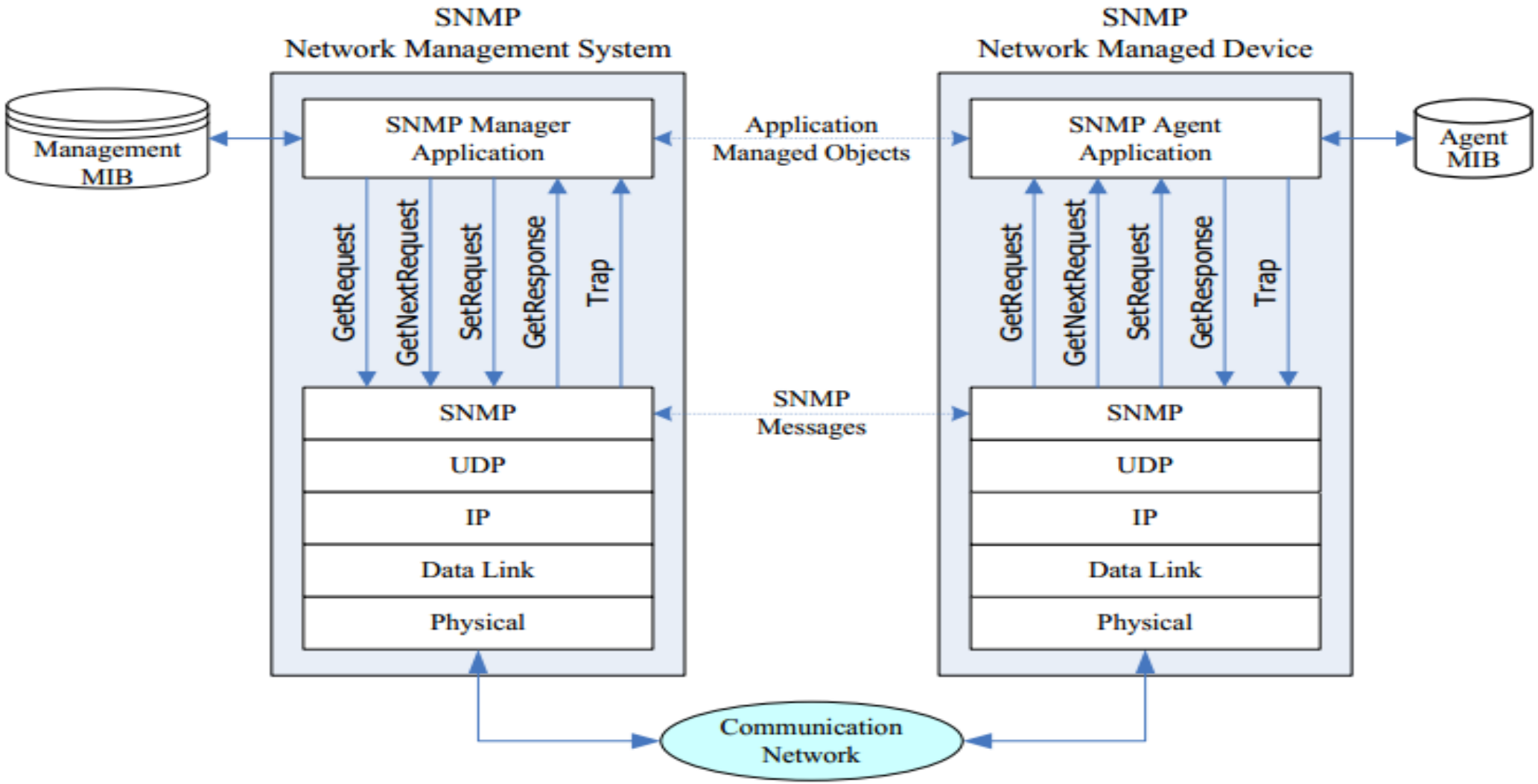
- Đối tưởng quản lý:
  - ✓ Servers
  - ✓ Workstations
  - ✓ Routers
  - ✓ Switches
  - ✓ Printers
  - ✓ . v . v .



Kiến trúc quản lý SNMP

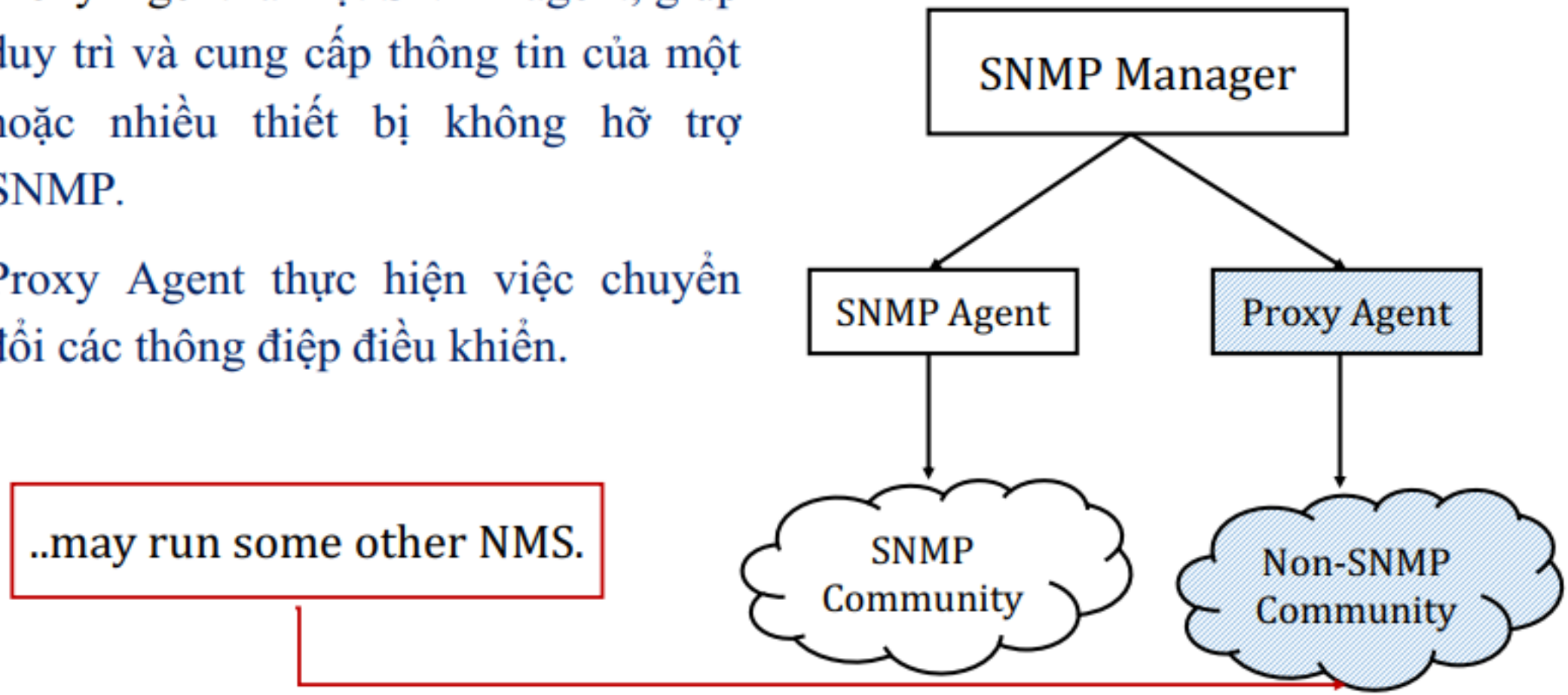
- Các thành phần chính:
  - **Management Station:** là một máy tính chạy phần mềm quản lý SNMP (Management application)
  - **Management Agent:** là một tiến trình chạy trên Network element, cung cấp thông tin quản lý cho Management Station.
  - **Management information base**: định nghĩa thông tin có thể được thu thập và kiểm soát bởi ứng dụng quản lý.
  - **Network management protocol**: giao thức liên kết giữa Manage và Agent (giao thức quản trị mạng TCP/IP là SNMP)

Kiến trúc quản lý mạng SNMP

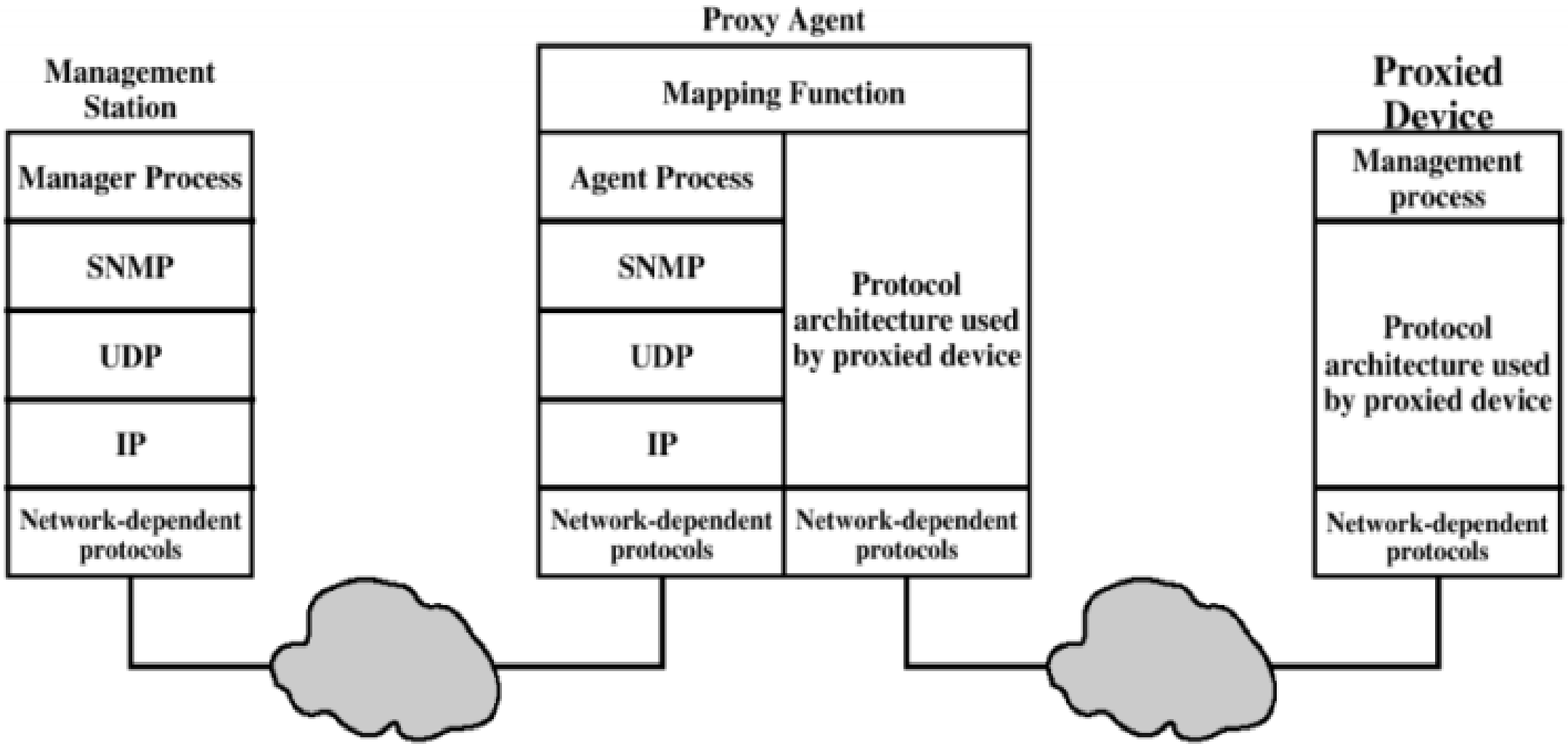


Mô hình triển khai

- Proxy Agent là một SNMP agent, giúp duy trì và cung cấp thông tin của một hoặc nhiều thiết bị không hỗ trợ SNMP.
- Proxy Agent thực hiện việc chuyển đổi các thông điệp điều khiển.



Proxy configuration



Các phương thức của SNMP

Bản tin/phương thức	Mô tả tác dụng
GetRequest	Manager gửi GetRequest cho agent để yêu cầu agent cung cấp thông tin nào đó dựa vào ObjectID (GetRequest có chứa OID)
GetNextRequest	Manager gửi GetNextRequest chứa một ObjectID cho agent để yêu cầu cung cấp thông tin nằm kế tiếp ObjectID đó trong MIB.
SetRequest	Manager gửi SetRequest cho agent để đặt giá trị cho đối tượng của agent dựa vào ObjectID.
GetResponse	Agent gửi GetResponse cho Manager để trả lời khi nhận được GetRequest/GetNextRequest
Trap	Agent tự động gửi thông báo cho Manager khi có một sự kiện xảy ra trong agent (line down, nhiệt độ trên ngưỡng, ...)

Các cơ chế bảo mật cho SNMP - CS

- **Community string:** đóng vai trò như mật khẩu khi trao đổi dữ liệu.
  - Được cài đặt giống nhau trên Manager và Agent
  - Khi Agent nhận yêu cầu từ Manage: **community string** tương ứng sẽ được dùng so sánh
  - Có 3 loại:
    - Read-Community: khi sử dụng phương thức Get
    - Write-Community: khi sử dụng phương thức Set
    - Trap-Community: khi sử dụng phương thức Trap

Các cơ chế bảo mật cho SNMP - View

- Manager có read-community thì có thể đọc toàn bộ thông tin (OID) của Agent.
- Agent có thể qui định chỉ cho phép xem một phần thông tin liên quan bằng cách tạo các View
  - Trên Agent định nghĩa nhiều View
  - Một view phải gắn liền với một community string
  - Có nhiều hệ thống không hỗ trợ tính năng view.

Các cơ chế bảo mật cho SNMP - ACL

- **SNMP access control list:** khi community string bị lộ, để ngăn chặn các SNMP manager không được phép mà gửi yêu cầu giám sát, người quản trị có thể dùng đến SNMP access control list
- **SNMP ACL** là một danh sách các địa chỉ IP được phép quản lý/giám sát agent, nó chỉ áp dụng riêng cho giao thức SNMP và được cài trên agent.
- Đa số các thiết bị đều cho phép thiết lập SNMP ACL.

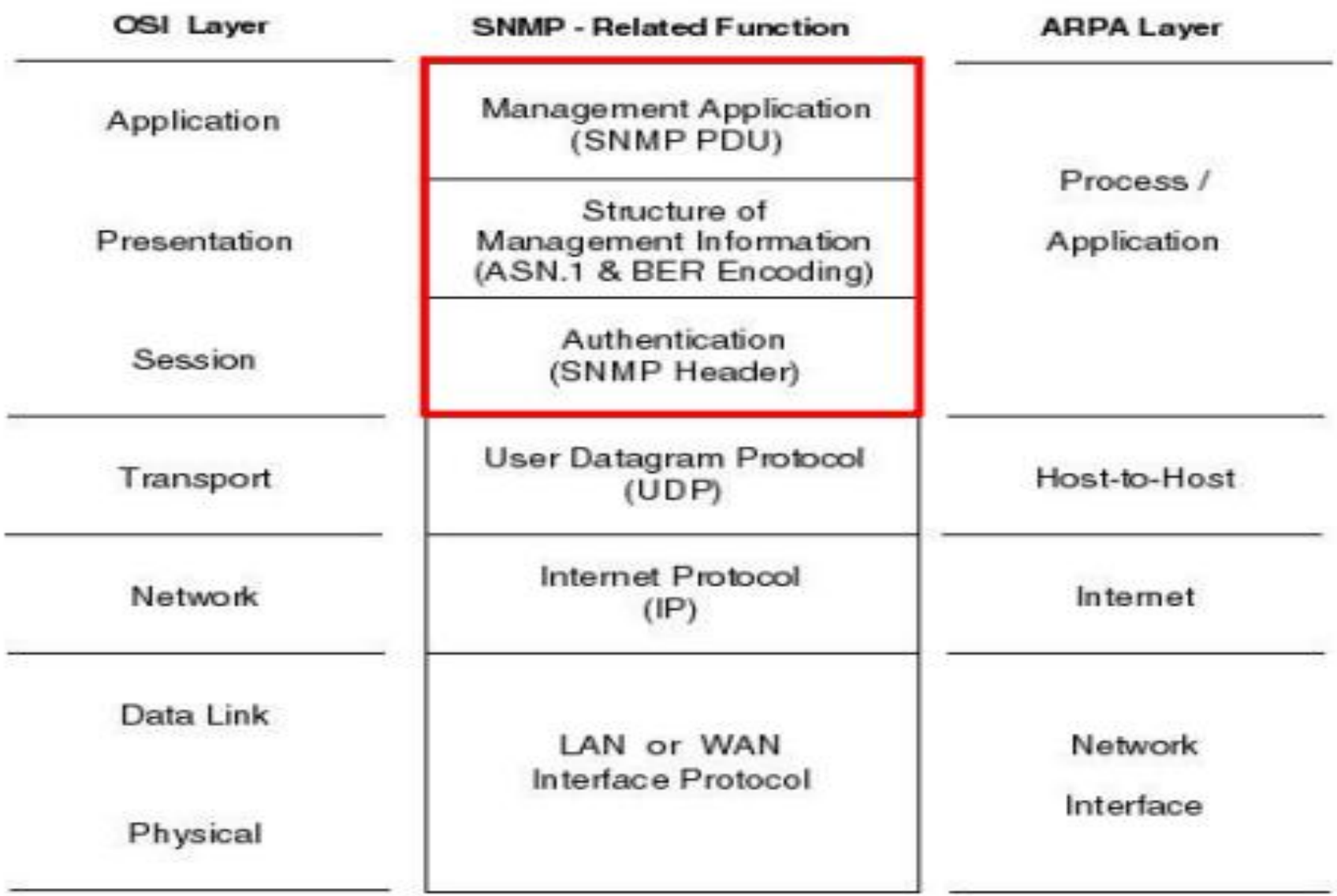
Các phiên bản SNMP

- Có 3 phiên bản:
  - SNMPv1 (1990): (RFC1065, RFC1066, RFC1067)
    - Có 5 phương thức: Get, GetNext, Set, Response, Trap
  - SNMPv2 (1996): v2u, v2c (RFC1441, RFC1452)
    - Có 8 phương thức: thêm GetBulk, Inform, Report
    - SNMPv2c và SNMPv1 có cơ chế xác thực bằng community string
    - SNMPv2u: sử dụng cơ chế chứng thực bằng băm và mã hóa đối xứng
  - SNMPv3 (2002)

Các phiên bản SNMP

- **Phiên bản SNMP khác nhau những gì?**
  - Số lượng phương thức
  - Cấu trúc bản tin SNMP (message format)
- Sử dụng giao thức vận chuyển UDP:
  - Port 161: polling
  - Port 162: trapping

SNMP trong mô hình TCP/IP



Cấu trúc bản tin SNMP

Version	Community Name	SNMP PDU

(a) SNMP message

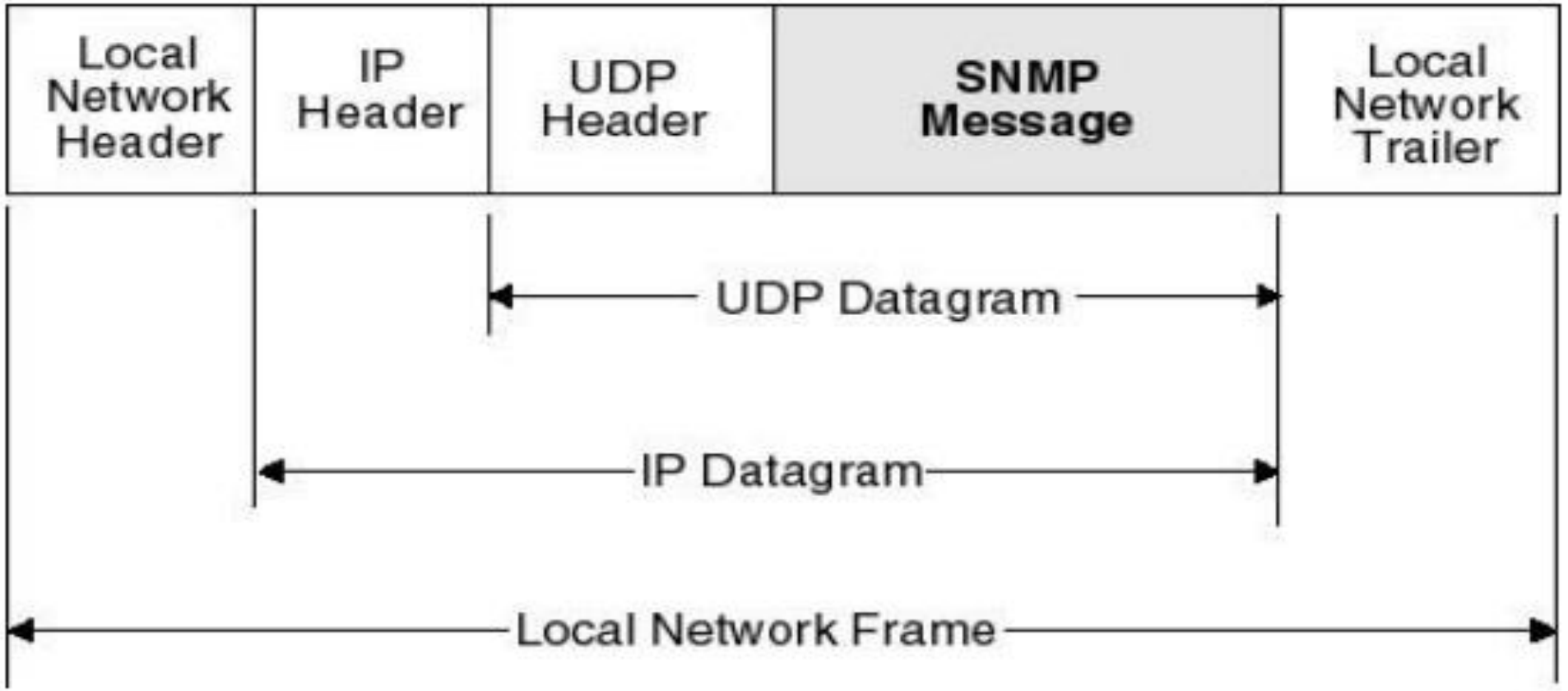
PDU Type	RequestID	ErrorStatus	ErrorIndex	VariableBindings				
				Name 1	Value 1	...	Name N	Value N

(b) `Get/Set` Type of PDUs

PDU Type	Enterprise	Agent-Address	Generic-Trap	Specific-Trap	Timestamp	VariableBindings				
						Name 1	Value 1	...	Name N	Value N

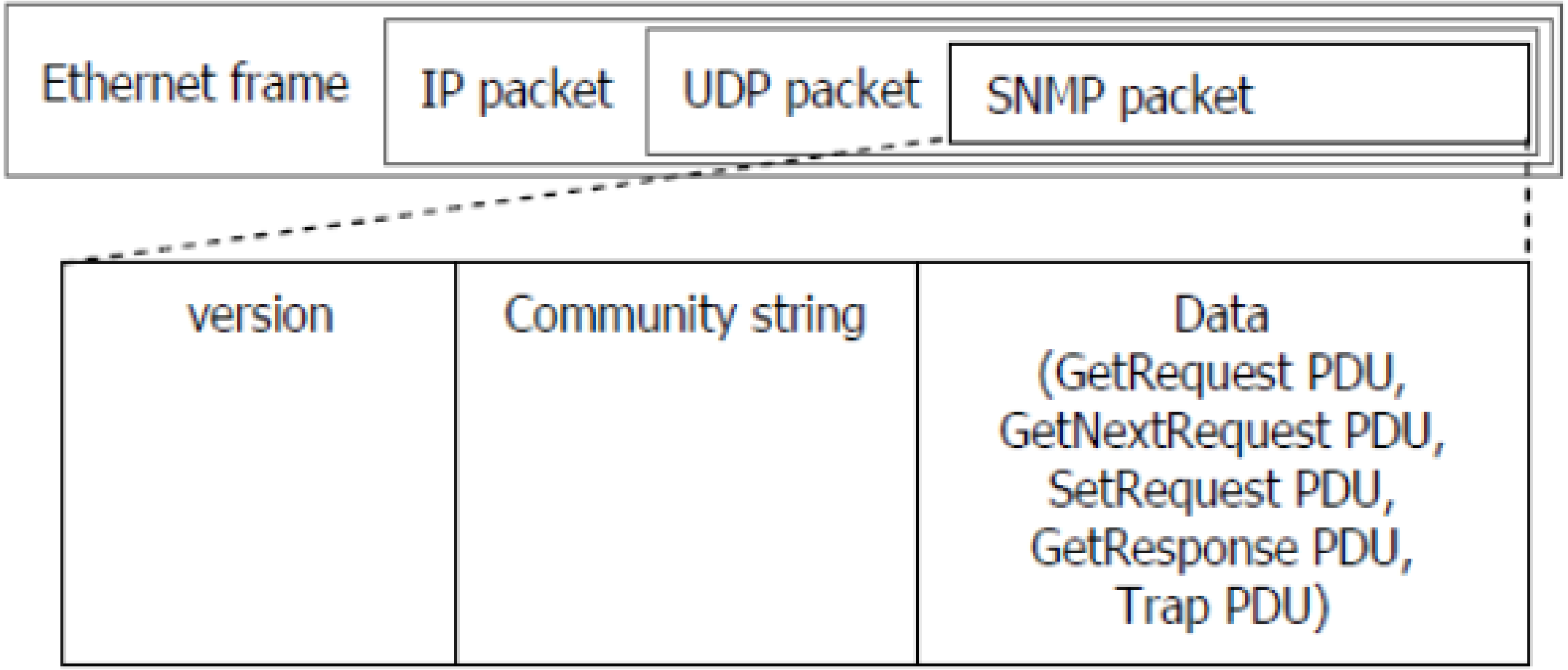
(c) `Trap` PDUs

Cấu trúc bản tin SNMP

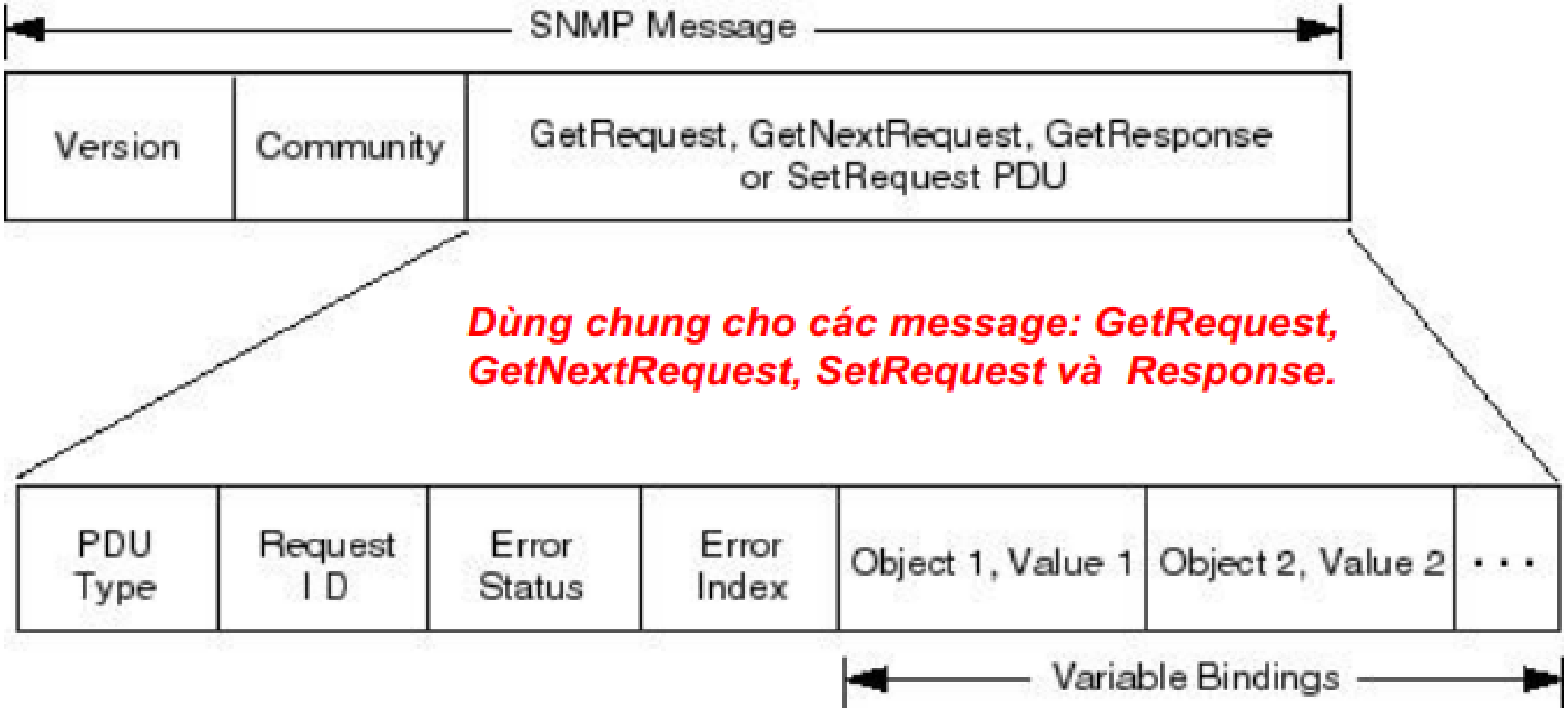


SNMP message được gói trong UDP-IP-Link header

Cấu trúc bản tin SNMP



Cấu trúc SNMP message



SNMP message = Version + Community string + SNMP PDU

SNMPv3

Parameter	Command Line Flag	snmp.conf token
securityName	-u *NAME*	defSecurityName NAME
authProtocol	-a *(MD5|SHA)*	defAuthType (MD5|SHA)
privProtocol	-x *(AES|DES)*	defPrivType DES
authKey	-A *PASSPHRASE*	defAuthPassphrase PASSPHRASE
privKey	-X *PASSPHRASE*	defPrivPassphrase PASSPHRASE
securityLevel	-l *(noAuthNoPriv|authNoPriv|authPriv)*	defSecurityLevel (noAuthNoPriv|authNoPriv|authPriv)
context	-n *CONTEXTNAME*	defContext CONTEXTNAME

- securityName: tên người dùng
- authProtocol: kiểu xác thực
- privProtocol: kiểu bảo mật, mã hóa
- authKeys: Khóa xác thực, ít nhất 8 ký tự
- privKey: khóa bảo mật, ít nhất 8 ký tự
- context: contextName được sử dụng để đặt tên cho một ngữ cảnh. Mỗi contextName phải là duy nhất trong một thực thể SNMP (mô hình proxy)

SNMP Security

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES AES-128	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. By default, the switch provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. The switch also provides an option to use a 128-bit AES algorithm for privacy.

SNMPv3

- RFC3411, RFC3412, RFC3413, RFC3414, RFC3415.
- Mục tiêu: tăng cường bảo mật cho giao thức SNMP
  - Xác thực user (user authentication): giao thức MD5,SHA
  - Mã hóa thông tin (message encryption): ngăn ngừa xem trái xem, sử dụng giao thức DES hoặc AES

SNMPv3

- SNMPv3 rất phức tạp và cồng kềnh
- Là sự lựa chọn tốt nhất cho vấn đề bảo mật của mạng
- Chiếm một phần băng thông đường truyền do đó làm tăng phí tổn mạng
- Vẫn đang được nghiên cứu và hoàn thiện

Một quản trị viên hệ thống cần phải biết?

- Một quản trị viên hệ thống cần phải biết:
  - Sự khác biệt giữa các phiên bản SNMP
  - Thiết bị hỗ trợ các version SNMP nào?
  - Phần mềm SNMP manager mà bạn sở hữu có hỗ trợ version SNMP tương ứng hay không?

Tài liệu tham khảo

1. Network Management, Jian Ren and Tongtong Li, *Michigan State University*, Chapter 12: Network Management
2. https://tools.ietf.org/html/rfc3414
3. https://docs.oracle.com/cd/E19077-01/n1k.switch/819-3047-11/xdoc/switchservices_snmp_user_show.html