


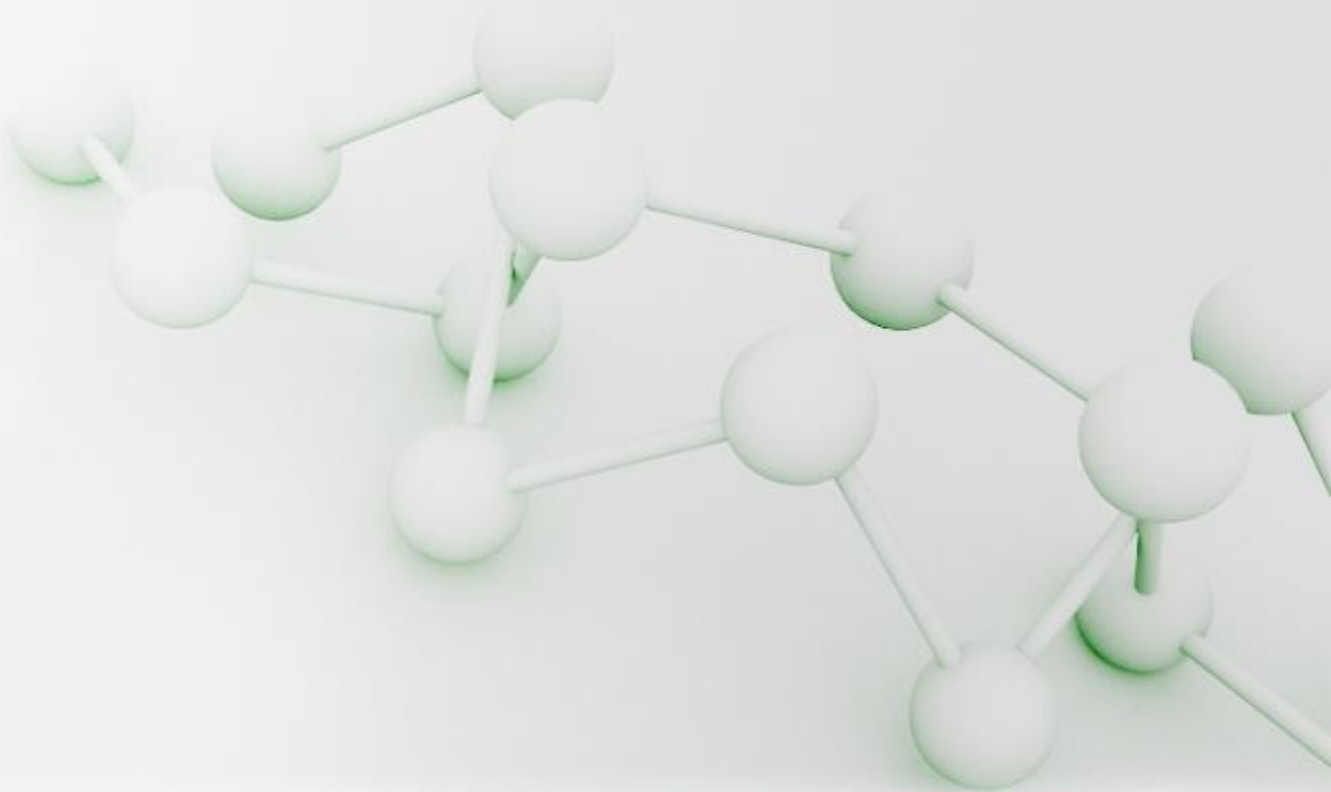
Quản trị Mạng

RMON



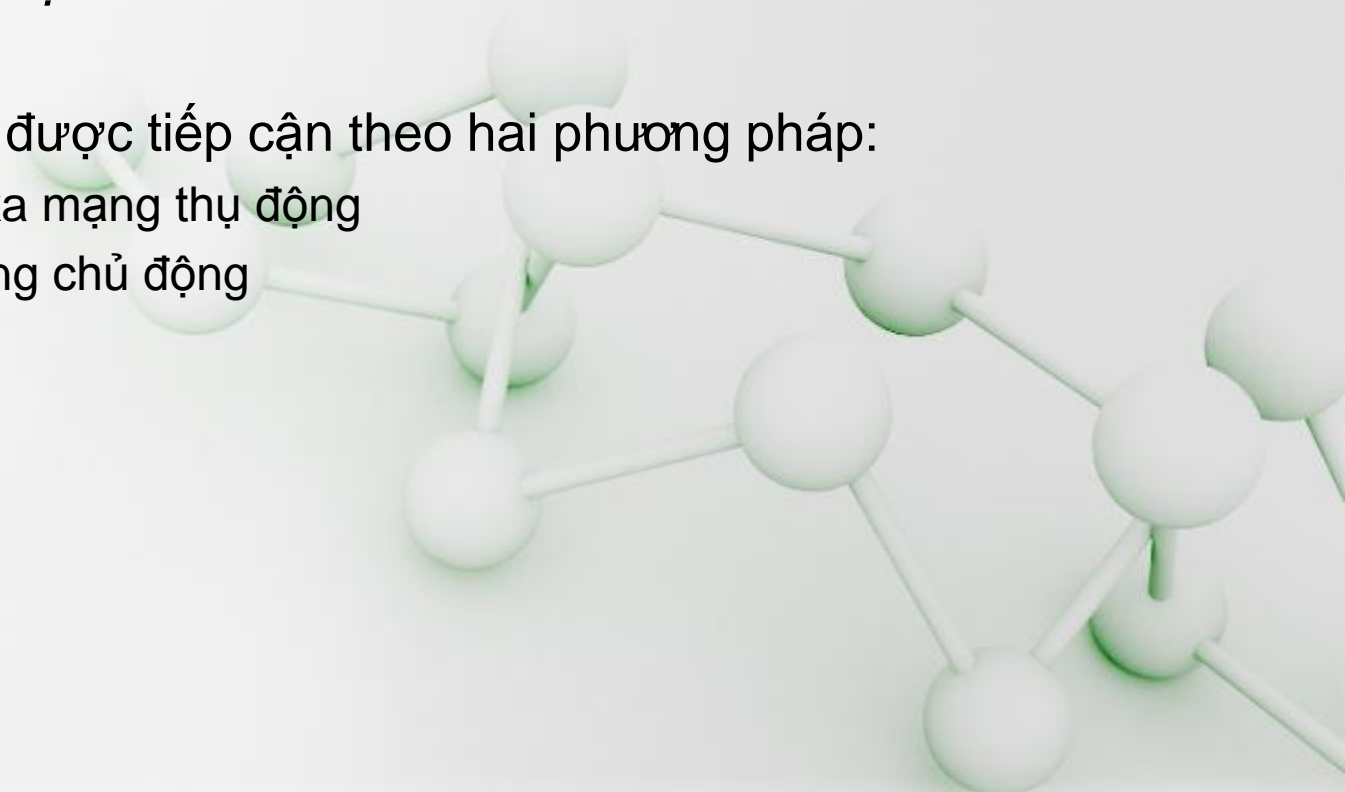
TS. Tran Hoang Hai
Bộ môn Mạng thông tin & Truyền thông
Viện Công nghệ thông tin

- Giới thiệu chung về giám sát mạng
- RMON
- Kết luận



Giám sát mạng

- ◆ **Nguyên lý chung:** *Mục tiêu giám sát nhằm kiểm tra và giám sát hiệu năng thực tế của dịch vụ mạng với các thỏa thuận cung cấp chất lượng dịch vụ.*
- ◆ Giám sát mạng được tiếp cận theo hai phương pháp:
 - ✓ Giám sát từ xa mạng thụ động
 - ✓ Giám sát mạng chủ động

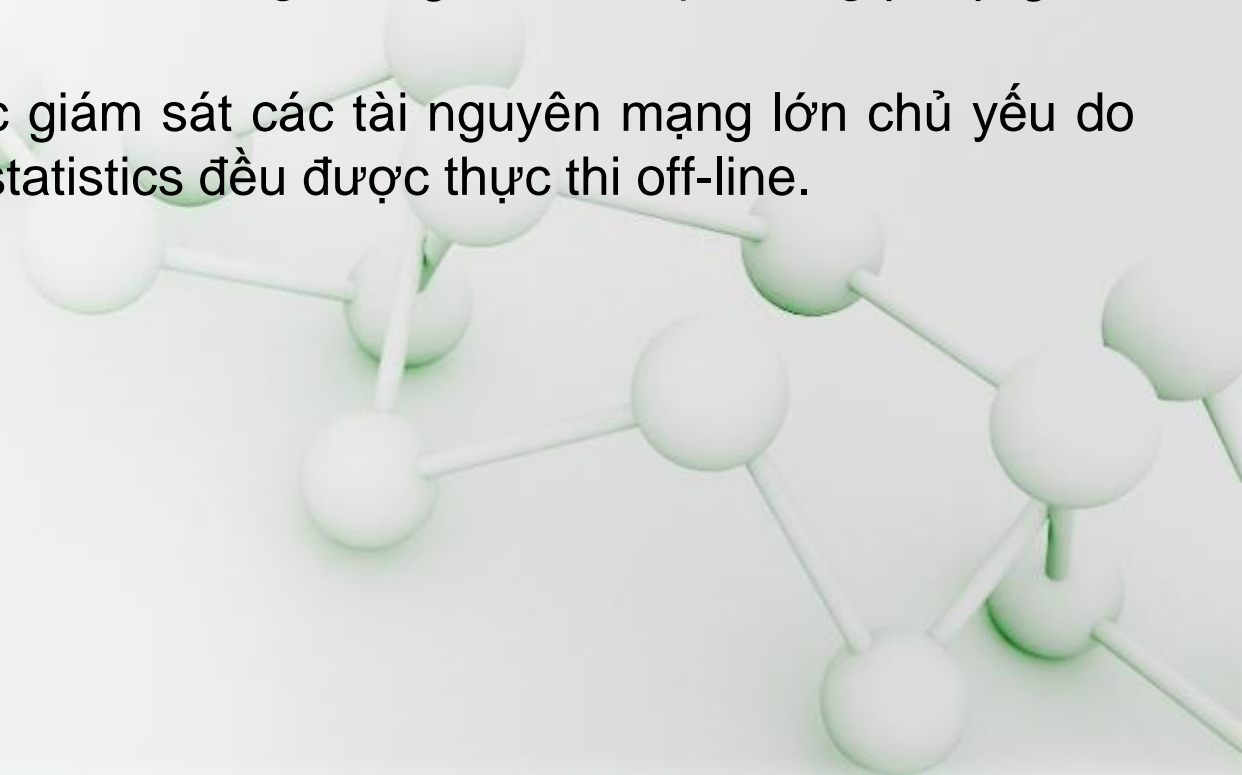


Giám sát mạng bị động

- ◆ Các thiết bị mạng ghi lại các trạng thái lưu lượng mạng để cung cấp các thông tin của một phần tử mạng thực tế.
- ◆ Các bản tin thăm dò (polling) định kỳ được sử dụng để thu thập thông tin dữ liệu cho báo cáo và phân tích.
- ◆ Thông tin trạng thái mạng có thể được suy luận từ tập các phép đo từ các phần tử mạng trên.
- ◆ Giám sát thụ động không yêu cầu bất cứ một lưu lượng phụ nào để sử dụng cho các mục đích đo

Giám sát mạng bị động

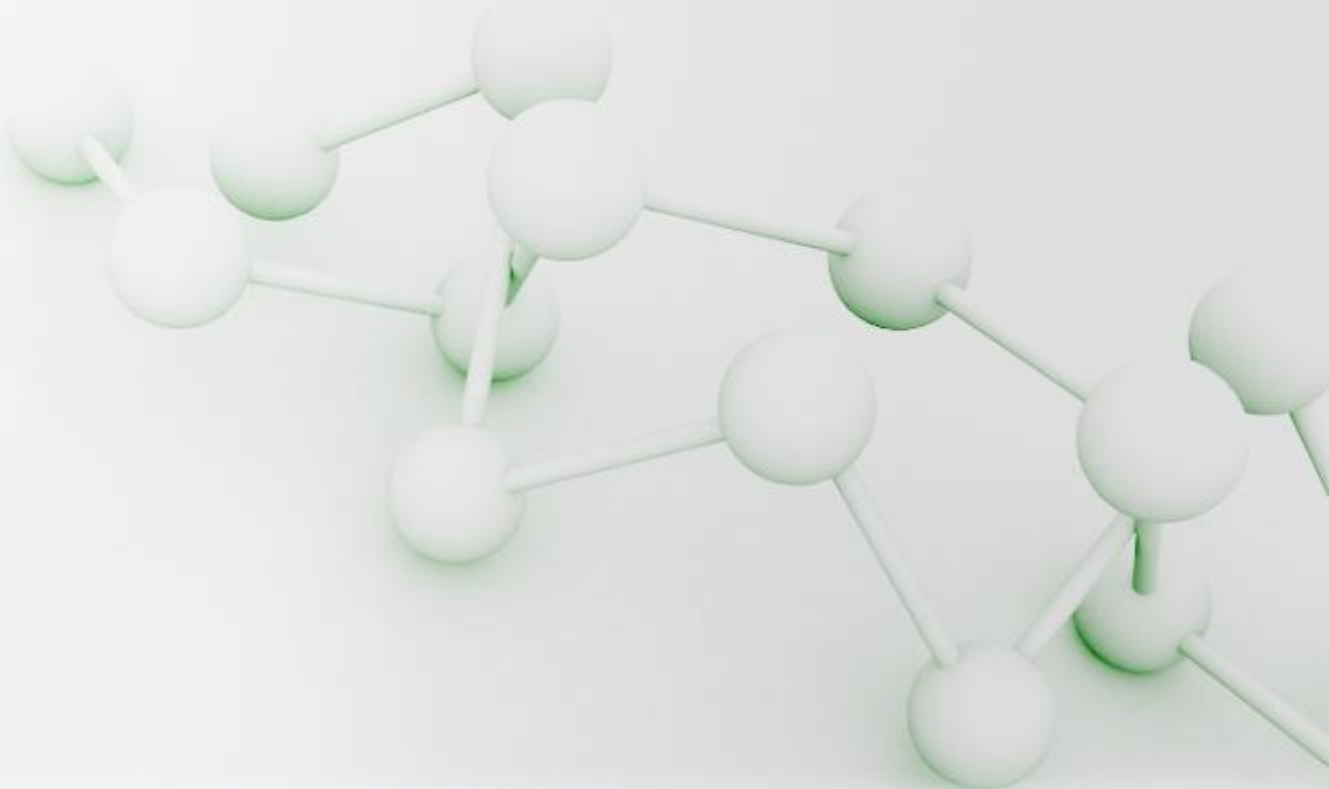
- ◆ Giám sát mạng bị động có thể được thực thi thông qua bất cứ một chương trình nghe lén (sniffer program).
- ◆ Đơn giản, không tốn nhiều băng thông như các phương pháp giám sát chủ động.
- ◆ Khó khăn trong việc giám sát các tài nguyên mạng lớn chủ yếu do thông tin thống kê/ statistics đều được thực thi off-line.



Giám sát mạng bị động

◆ Một số công cụ passive packet sniffer:

- ✓ Wireshark
- ✓ Tcpdump
- ✓ Kismet
- ✓ Ettercap
- ✓ Nétumbler



Giám sát mạng bị động

◆ Wireshark

The image shows the Wireshark network traffic capture interface. The main window is titled "eth0: Capturing - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter bar with a "Filter:" input field and buttons for "Expression...", "Clear", and "Apply".

The packet list pane displays a table of captured packets:

No.	Time	Source	Destination	Protocol	Info
46	139.931187	Wistron_07:07:ee	Broadcast	ARP	Who has 192.168.1.254? Tell 192.168.1.68
47	139.931463	ThomsonT_08:35:4f	Wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
48	139.931466	192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
49	139.975406	192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
50	139.976811	192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51	140.079578	66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52	140.079583	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53	140.080278	192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
54	140.086765	192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55	140.086921	192.168.1.68	66.102.9.99	TCP	62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56	140.197484	66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57	140.197777	66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58	140.197811	192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
59	140.218210	66.102.9.99	192.168.1.68	TCP	http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

The packet details pane shows the structure of the selected packet (Frame 1):

- Frame 1 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

The packet bytes pane displays the raw data in hexadecimal and ASCII:

```
0000  ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01  ....8.....
0010  08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80  ....8....9.
0020  00 00 00 00 00 00 c0 a8 39 02  ....9.
```

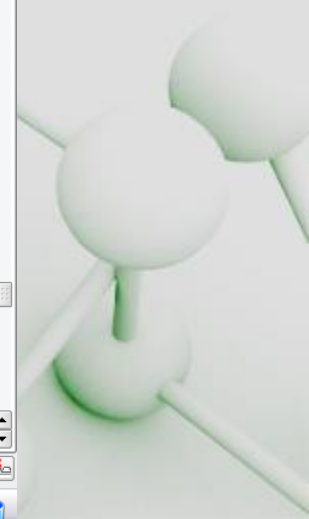
The status bar at the bottom indicates: "eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default".

Giám sát mạng bị động

◆ TCPDump

```
root@ciec: ~ - Shell No. 4 - Konsole
Session Edit View Bookmarks Settings Help

[root@ciec ~]$ tcpdump -XXX
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
01:39:00.239963 arp who-has 10-1-119-90.int.sds.uw.edu.pl tell 10-1-232-251.int.sds.uw.edu.pl
0x0000: ffff ffff ffff 0010 5ae6 d045 0806 0001 .....Z..E....
0x0010: 0800 0604 0001 0010 5ae6 d045 0a01 e8fb .....Z..E....
0x0020: 0000 0000 0000 0a01 775a 0000 0000 0000 .....wZ.....
0x0030: 0000 0000 0000 0000 0000 0000 .....
01:39:00.240803 IP 10-1-225-220.int.sds.uw.edu.pl.32786 > 10-1-254-254.int.sds.uw.edu.pl.domain: 2
680+ PTR? 90.119.1.10.in-addr.arpa. (42)
0x0000: 0030 4884 5ef6 000f ea39 d0e0 0800 4500 ..0H.^...9...E.
0x0010: 0046 1a89 4000 4011 2b41 0a01 e1dc 0a01 ..F..@.@.+A.....
0x0020: fefe 8012 0035 0032 f520 0a78 0100 0001 .....5.2...x....
0x0030: 0000 0000 0000 0239 3003 3131 3901 3102 .....90.119.1.
0x0040: 3130 0769 6e2d 6164 6472 0461 7270 6100 10.in-addr.arpa.
0x0050: 000c 0001 .....
01:39:00.253666 IP 10-1-254-254.int.sds.uw.edu.pl.domain > 10-1-225-220.int.sds.uw.edu.pl.32786: 2
680 1/0/0 PTR[|domain]
0x0000: 000f ea39 d0e0 0030 4884 5ef6 0800 4500 ...9...0H.^...E.
0x0010: 0071 0000 4000 4011 459f 0a01 fefe 0a01 ..q..@.@.E.....
0x0020: e1dc 0035 8012 005d 334c 0a78 8180 0001 ...5...]3L.x....
0x0030: 0001 0000 0000 0239 3003 3131 3901 3102 .....90.119.1.
0x0040: 3130 0769 6e2d 6164 6472 0461 7270 6100 10.in-addr.arpa.
0x0050: 000c 0001 c00c 000c 0001 0001 4a78 001f .....Jx..
01:39:00.255938 IP 10-1-225-220.int.sds.uw.edu.pl.32786 > 10-1-254-254.int.sds.uw.edu.pl.domain: 6
932+ PTR? 251.232.1.10.in-addr.arpa. (43)
0x0000: 0030 4884 5ef6 000f ea39 d0e0 0800 4500 ..0H.^...9...E.
0x0010: 0047 1a8d 4000 4011 2b3c 0a01 e1dc 0a01 ..G..@.@.+<.....
0x0020: fefe 8012 0035 0033 f521 1b14 0100 0001 .....5.3.!.....
0x0030: 0000 0000 0000 0332 3531 0332 3332 0131 .....251.232.1
```

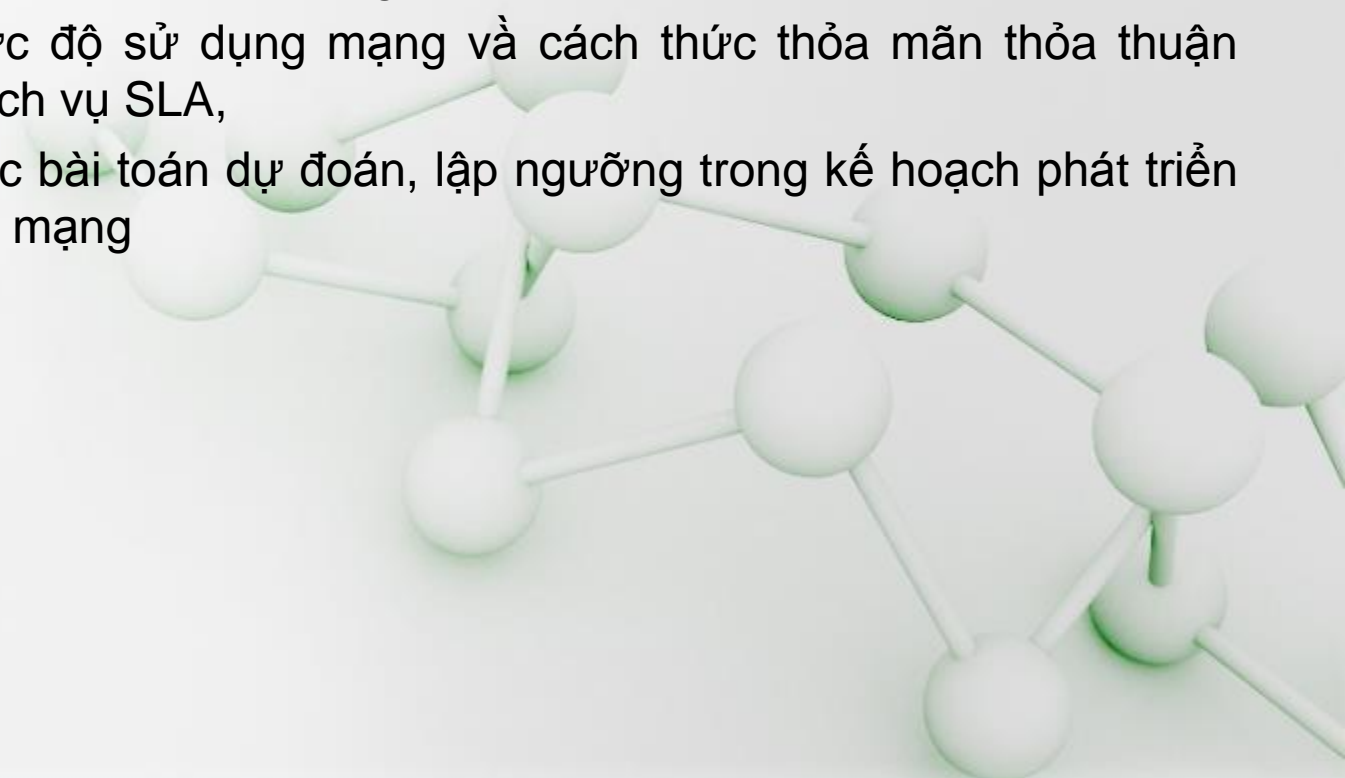


Giám sát mạng chủ động

- ◆ Phương pháp giám sát mạng chủ động gửi các thông tin giám sát vào mạng quản lý.
- ◆ Các luồng dữ liệu tổng hợp gồm các gói tin thăm dò được gửi vào mạng nhằm giám sát hiệu năng mạng.
- ◆ Các nhà phân tích thu thập các luồng dữ liệu để phân tích và đánh giá hiệu năng mạng.
- ◆ Phương pháp giám sát mạng chủ động cung cấp bài đo mạng tính tổng thể qua một loạt các phần tử mạng trong hệ thống.

Giám sát mạng

- ◆ Các hệ thống giám sát bị động hoặc chủ động được phát triển do một số lý do sau:
 - ✓ Giám sát và báo cáo chất lượng dịch vụ,
 - ✓ Đánh giá mức độ sử dụng mạng và cách thức thỏa mãn thỏa thuận chất lượng dịch vụ SLA,
 - ✓ cơ sở cho các bài toán dự đoán, lập ngưỡng trong kế hoạch phát triển và quy hoạch mạng



RMON

- ◆ Giám sát từ xa RMON (Remote MONitoring) là một cơ sở thông tin quản lý tiêu chuẩn khác với giao thức quản lý mạng đơn giản.
- ◆ Các thông tin quản lý , tập hợp và phân tích nội bộ, có thể truyền đến trạm quản lý từ xa và được giám sát.
- ◆ Giám sát từ xa RMON là một tiêu chuẩn mở được định nghĩa bởi IETF (RFC-1757) và gồm hai phiên bản:
 - ✓ RMONv1 (RFC 2819)
 - ✓ RMONv2 (RFC 2021).

RMON

- ◆ RMONv1 cung cấp các trạm quản lý mạng NMS với trạng thái mức gói của toàn bộ mạng LAN, MAN hoặc WAN.
- ◆ RMONv2 cải thiện RMONv1 trên cơ sở bổ sung, cung cấp trạng thái mức mạng và ứng dụng.
- ◆ RMON cung cấp các thông tin tiêu chuẩn cho người quản trị mạng có thể sử dụng để giám sát, phân tích và sửa lỗi cho một nhóm mạng cục bộ phân tán và kết nối T1/E1, T2/E3 tới các trạm trung tâm.
- ◆ RMON định nghĩa các thông tin đặc tả cho các kiểu hệ thống giám sát mạng.

RMON

◆ Sự khác biệt của RMON và SNMP:

- ✓ RMON dựa trên thiết bị, trong đó sử dụng các phần cứng đặc biệt để điều hành.
- ✓ RMON gửi thông tin theo phương pháp chủ động nhằm sử dụng tối ưu băng thông và các sự kiện mạng.
- ✓ RMON có khả năng thu thập dữ liệu chi tiết.
- ✓ Thiết bị RMON cung cấp một hệ thống giám sát mạnh mẽ với chi phí thấp, các thăm dò RMON thường được cài đặt trong các liên kết đường trục và máy chủ.
- ✓ Hệ thống RMON có thể cấu hình để cung cấp dữ liệu như :
 - Các thông tin liên quan tới hiệu suất mạng;
 - Các thông tin thống kê cho phân tích trạng thái và chiến lược mạng;
 - Thông tin mô tả truyền thông giữa các hệ thống và lượng dữ liệu trao đổi.

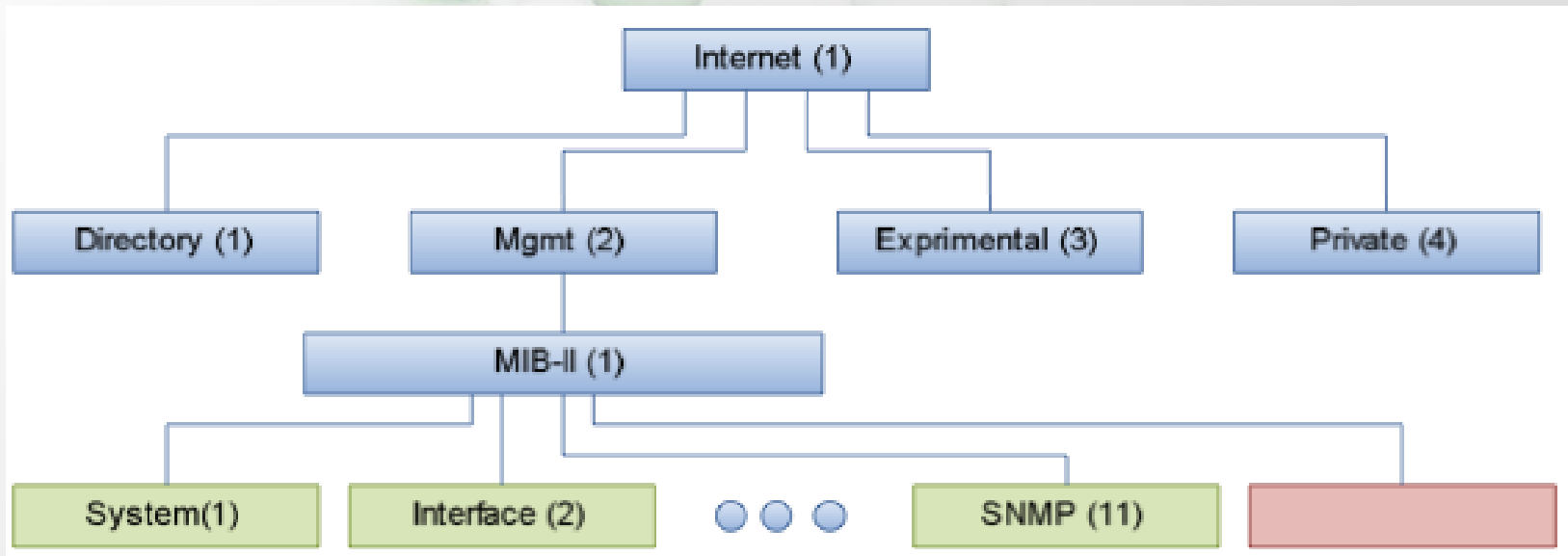
RMON

◆ Đặc điểm RMON:

- ✓ Các phần tử thăm dò RMON thay thế các thiết bị phân tích mạng đắt tiền được gắn vào các vùng trọng yếu trong mạng.
- ✓ Các phần tử thăm dò RMON có nhiều dạng khác nhau phụ thuộc vào kích thước và kiểu thiết bị giám sát
- ✓ Nhúng RMON MIB trên chính thiết bị chịu sự giám sát, card rời, thiết bị hoặc máy tính ngoài.
- ✓ Trong đó, các phần cứng đặc biệt gắn với các thiết bị chịu sự giám sát có ưu điểm:
 - Thu thập được các tham số đo chi tiết hơn agent SNMP và hoạt động như một bộ xử lý thời gian thực cho quá trình thu thập thông tin gửi tới NMS

RMON

- ◆ Trong hệ thống truyền thông của thông tin quản lý mạng, tiêu chuẩn chung cho RMON được định nghĩa tại RFC.1757 trên cơ sở cú pháp ASN.1.
- ◆ Các nhóm của RMON (RMONv1 và RMONv2) thuộc vào nút 16 của cây cơ sở thông tin quản lý MIB-II



RMON

◆ RMONv1 MIB gồm 10 nhóm:

1. *Statistics: real-time LAN statistics e.g. utilization, collisions, CRC errors*
2. *History: history of selected statistics*
3. *Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds*
4. *Hosts: host specific LAN statistics e.g. bytes sent/received, frames sent/received*
5. *Hosts top N: record of N most active connections over a given time period*
6. *Matrix: the sent-received traffic matrix between systems*
7. *Filter: defines packet data patterns of interest e.g. MAC address or TCP port*
8. *Capture: collect and forward packets matching the Filter*
9. *Event: send alerts (SNMP traps) for the Alarm group*
10. *Token Ring: extensions specific to Token Ring*

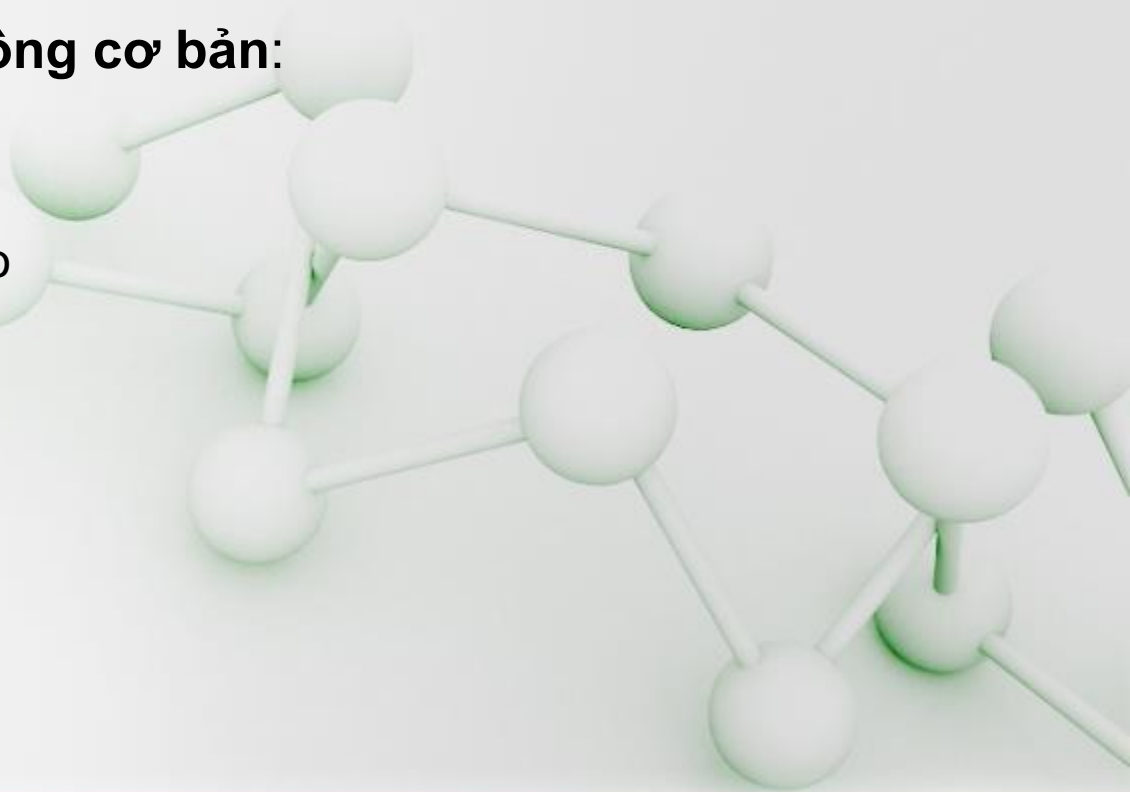
RMON

◆ RMONv2 MIB bổ sung 10 nhóm:

1. *Protocol Directory: list of protocols the probe can monitor*
2. *Protocol Distribution: traffic statistics for each protocol*
3. *Address Map: maps network-layer (IP) to MAC-layer addresses*
4. *Network-Layer Host: layer 3 traffic statistics, per each host*
5. *Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts*
6. *Application-Layer Host: traffic statistics by application protocol, per host*
7. *Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts*
8. *User History: periodic samples of user-specified variables*
9. *Probe Configuration: remote configure of probes*
10. *RMON Conformance: requirements for RMON2 MIB conformance*

RMON

- ◆ RMONv1 định nghĩa các hoạt động tại lớp liên kết dữ liệu của mô hình OSI, trong khi đó RMONv2 mở rộng hoạt động tới các lớp cao hơn.
- ◆ **Một số đặc tính hoạt động cơ bản:**
 - ✓ Điều hành ngoại tuyến,
 - ✓ Giám sát chủ động,
 - ✓ Phát hiện lỗi và báo cáo
 - ✓ Dữ liệu gia tăng giá trị
 - ✓ Đa quản lý



RMON

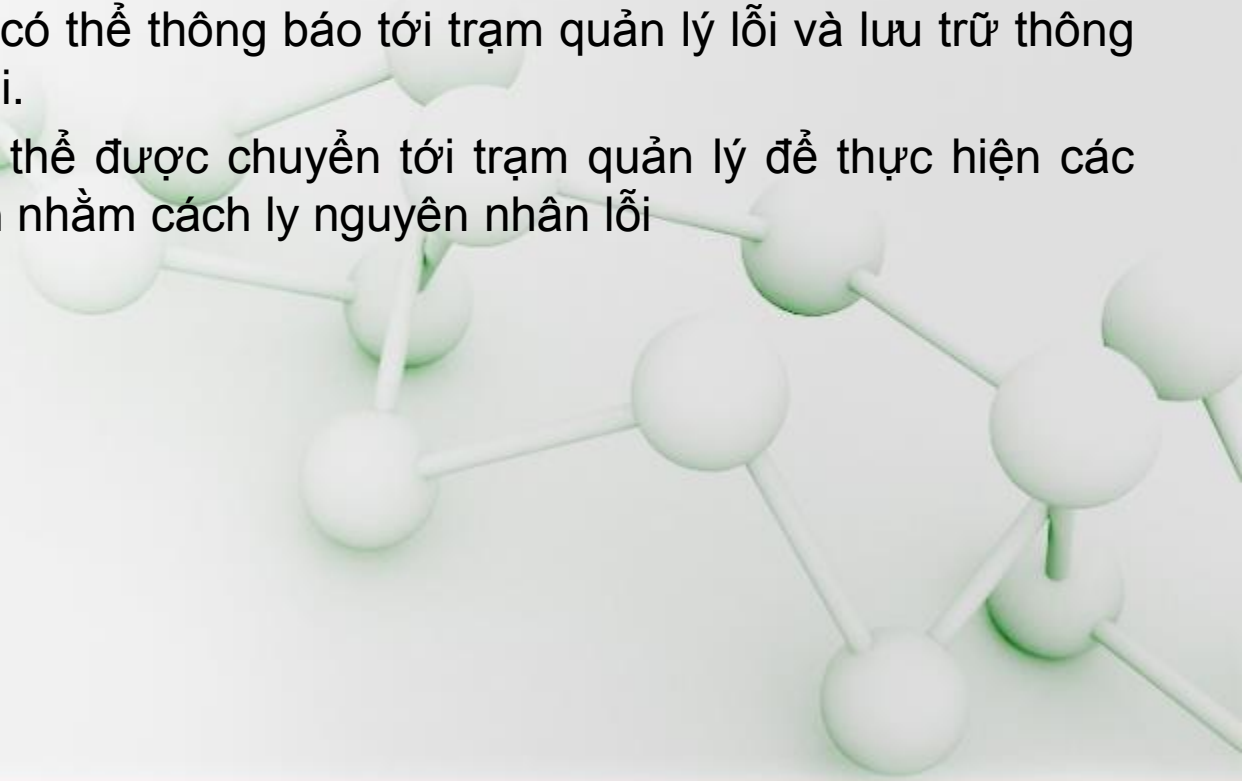
◆ Điều hành ngoại tuyến:

- ✓ RMON cho phép một phần tử thăm dò thực hiện các công tác chẩn đoán và thu thập thông tin liên tục ngay cả khi truyền thông với trạm quản lý không kết nối.
- ✓ Phần tử thăm dò cố gắng thông báo với trạm quản lý khi có các điều kiện bất thường xảy ra.
- ✓ Tuy nhiên, khi xảy ra lỗi truyền thông, phần tử thăm dò lưu trữ thông tin và truyền lại trạm quản lý khi kết nối được khôi phục

RMON

◆ Giám sát chủ động:

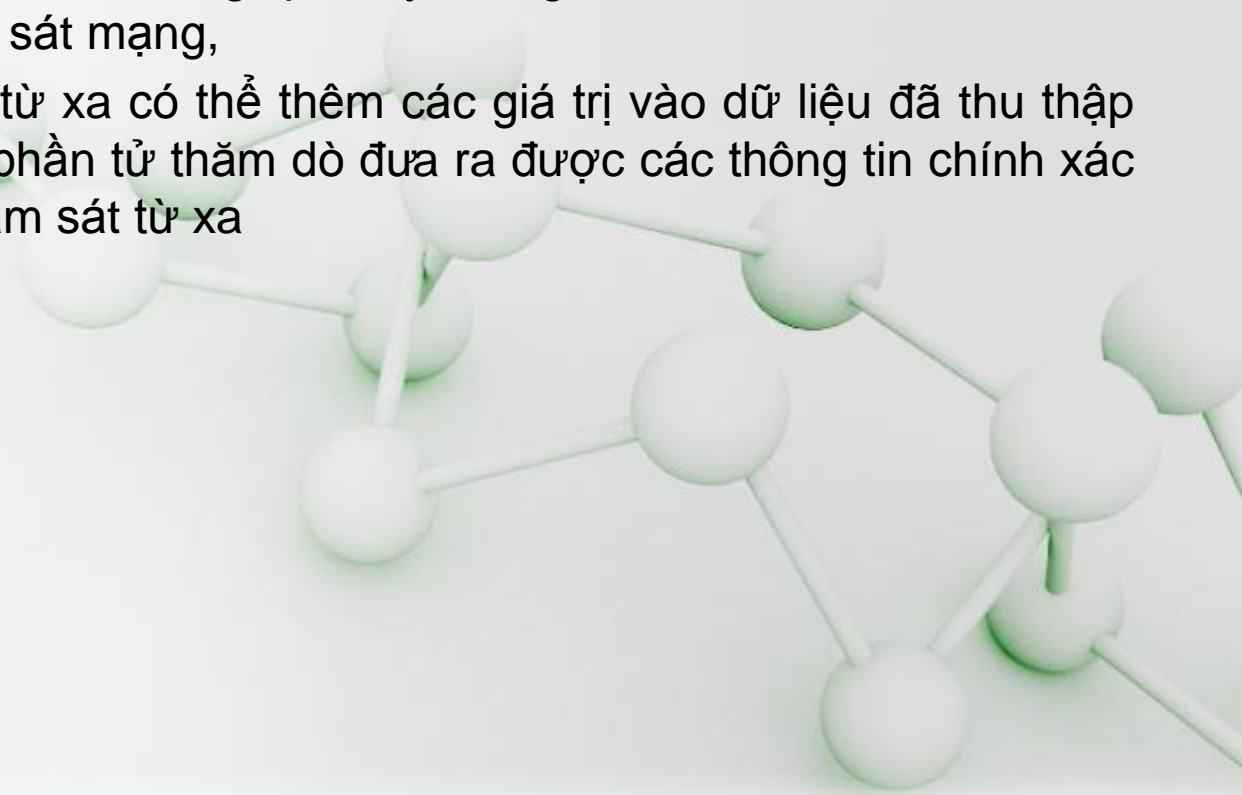
- ✓ Với RMON, thiết bị giám sát từ xa (phần tử thăm dò) có một nguồn tài nguyên để thực hiện chẩn đoán và lưu giữ thông tin hiệu năng mạng.
- ✓ Phần tử thăm dò có thể thông báo tới trạm quản lý lỗi và lưu trữ thông tin trạng thái về lỗi.
- ✓ Thông tin này có thể được chuyển tới trạm quản lý để thực hiện các chẩn đoán xa hơn nhằm cách ly nguyên nhân lỗi



RMON

◆ Dữ liệu gia tăng giá trị:

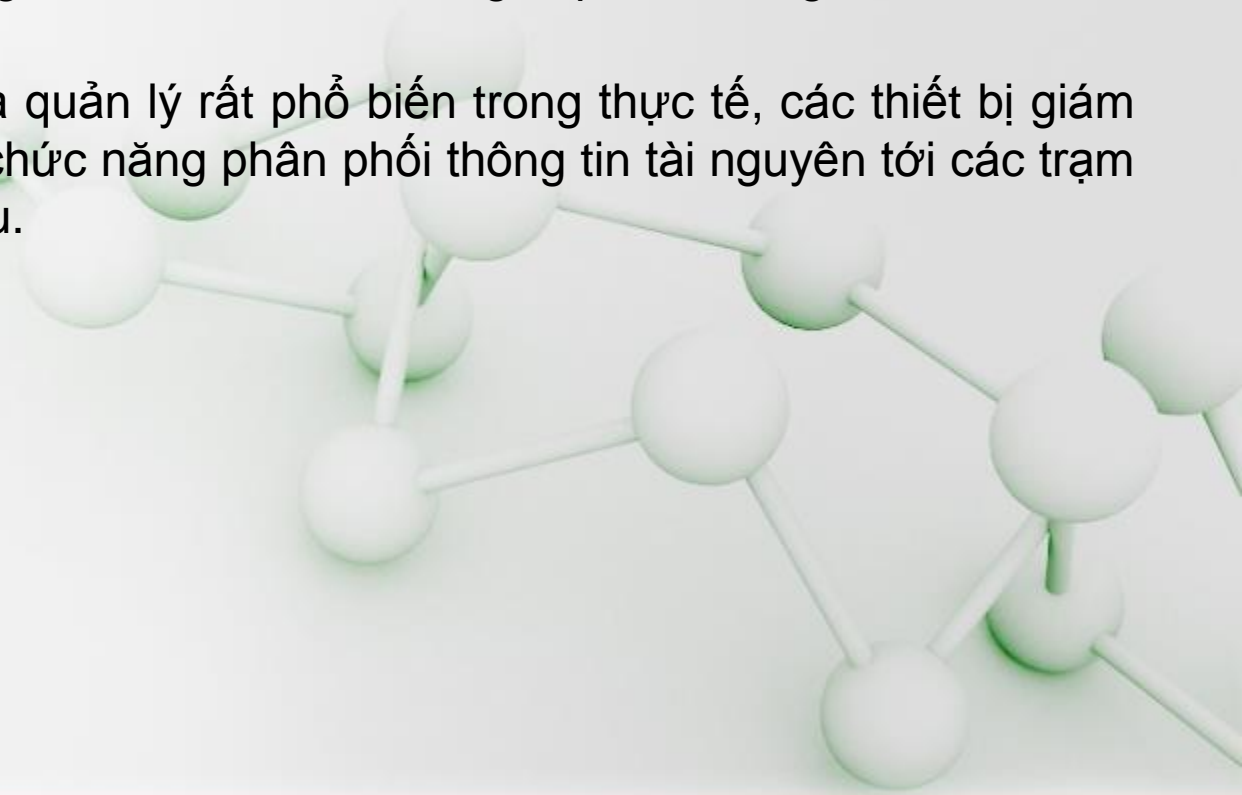
- ✓ Một khi thiết bị giám sát từ xa thể hiện một nguồn tài nguyên mạng khác biệt với các chức năng quản lý mạng vì nó được xác định trực tiếp từ phần giám sát mạng,
- ✓ Thiết bị giám sát từ xa có thể thêm các giá trị vào dữ liệu đã thu thập nhằm hỗ trợ các phần tử thăm dò đưa ra được các thông tin chính xác hơn tới thiết bị giám sát từ xa



RMON

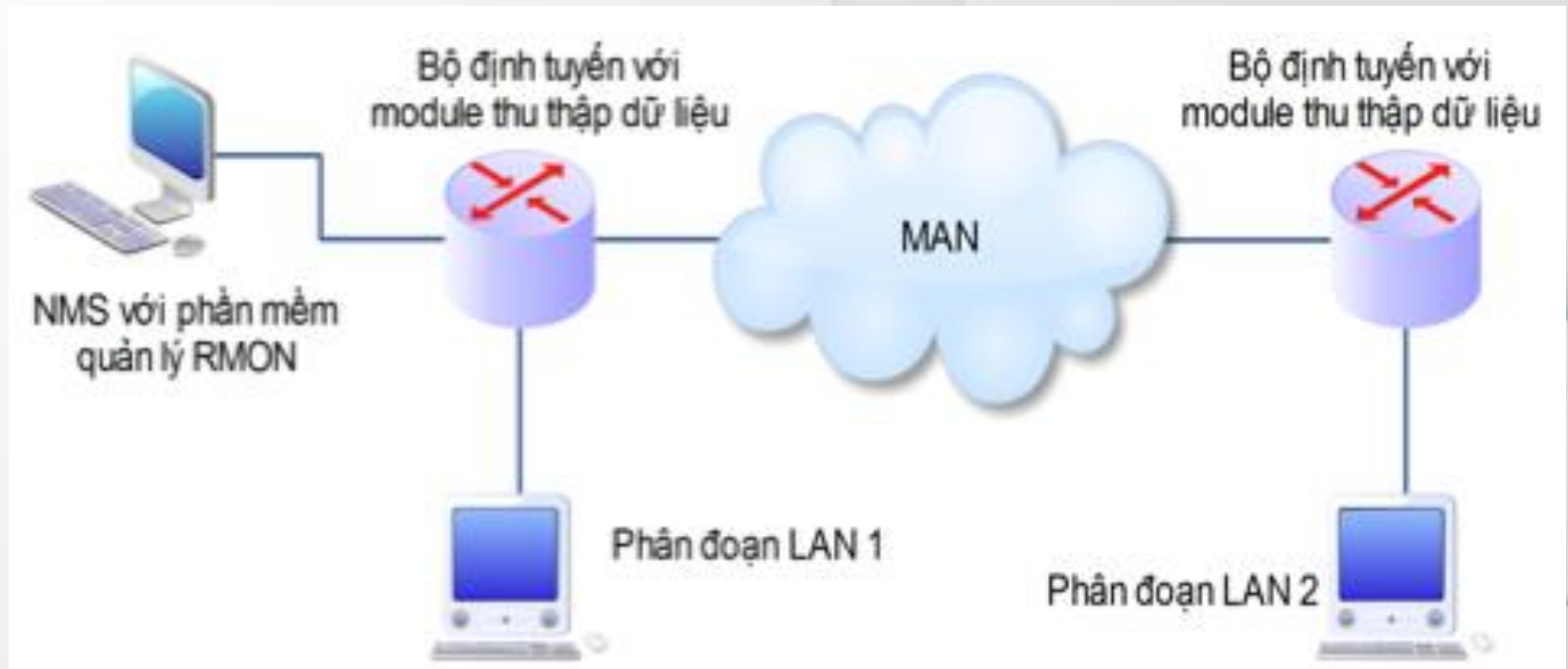
◆ Đa quản lý:

- ✓ Một tổ chức có thể có nhiều trạm quản lý cho các đơn vị của tổ chức với các chức năng khác nhau nhằm cung cấp các thông tin tốt nhất để khôi phục lỗi.
- ✓ Do môi trường đa quản lý rất phổ biến trong thực tế, các thiết bị giám sát từ xa cần có chức năng phân phối thông tin tài nguyên tới các trạm quản lý khác nhau.



RMON

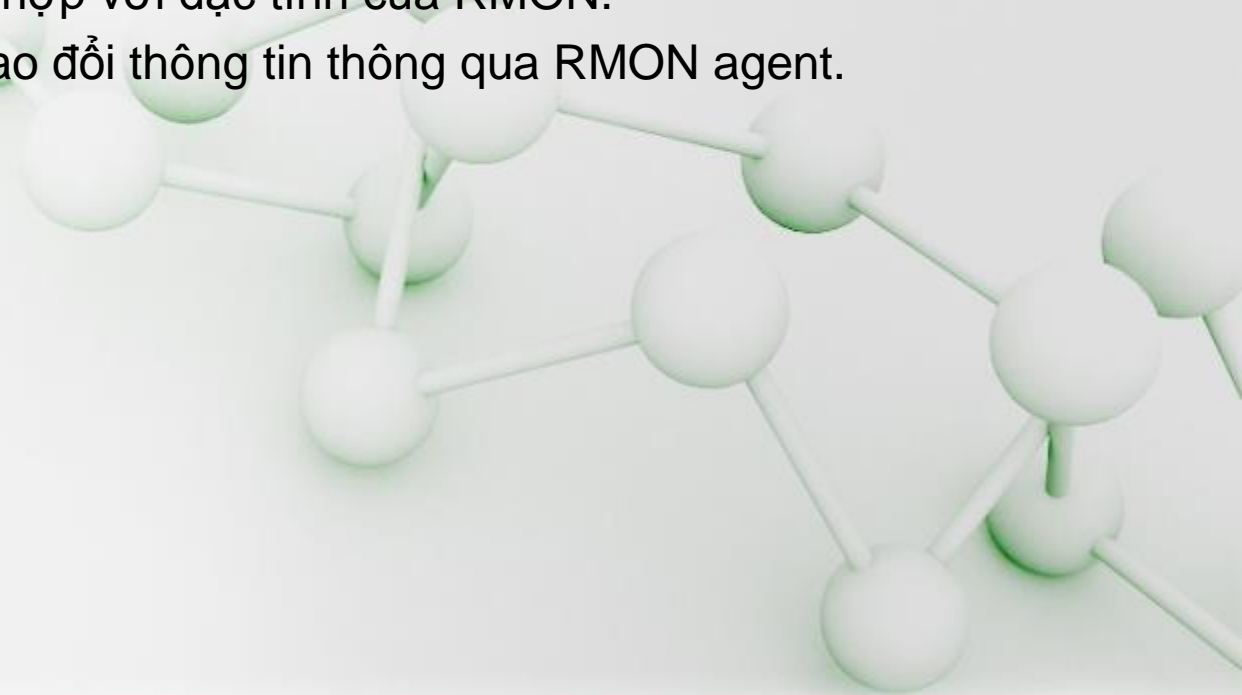
- ◆ **Các thành phần của RMON:** tương tự SNMP, một kiểu cấu hình RMON gồm một trung tâm quản lý mạng NMS và một thiết bị giám sát từ xa RMON.



RMON

◆ Các thành phần của RMON:

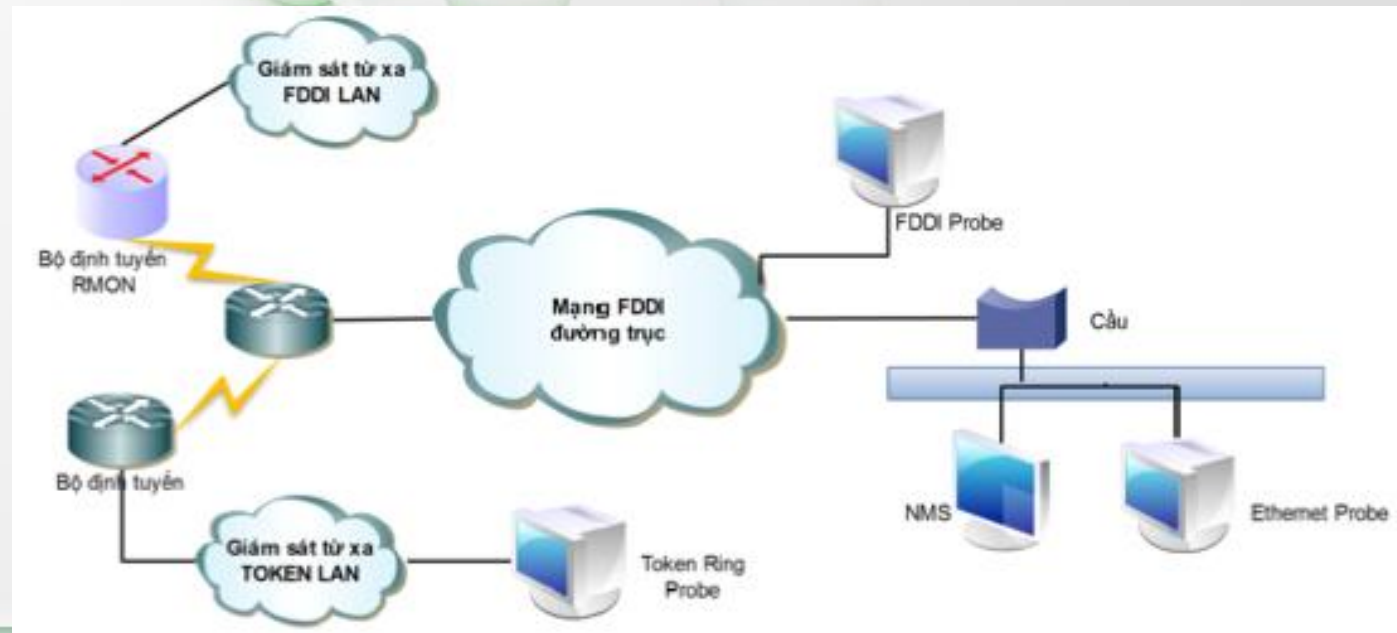
- ✓ NMS có thể hoạt động trên các máy chủ windows, unix hoặc máy PC chạy các ứng dụng quản lý mạng nhằm thực hiện các nhiệm vụ tập hợp trạng thái qua việc giám sát các gói tin dữ liệu trên mạng, lưu trữ các thông tin phù hợp với đặc tính của RMON.
- ✓ NMS thực hiện trao đổi thông tin thông qua RMON agent.



RMON

◆ Ví dụ RMON:

- ✓ Mạng được xây dựng dựa trên mạng đường trục FDDI và kết nối tới mạng LAN thông qua thiết bị cầu. Các bộ định tuyến chứa phần mềm giám sát RMON nhằm giám sát các thành phần trong các phân đoạn mạng. Khi xuất hiện các sự kiện bất bình thường trong các phân đoạn mạng quản lý, RMON gửi thông tin tới hệ thống giám sát mạng từ xa để báo cáo.



RMON

◆ Ví dụ RMON – Nhận xét:

- ✓ Ưu điểm của sử dụng RMON khi các agent không nhất thiết phải tồn tại trong toàn bộ thời gian quản lý hệ thống mạng.
- ✓ Một số cơ chế xác nhận lỗi trong mạng IP như gói tin ICMP ping có thể bị tổn thất trong các đường truyền thông có khoảng cách lớn. Nhất là khi có hiện tượng tắc nghẽn lưu lượng.
- ✓ Các gói tin thăm dò RMON được thực hiện trong từng mạng nội bộ và giám sát liên tục làm tăng độ tin cậy của bài toán giám sát.

RMON

◆ Điều khiển thiết bị RMON:

- ✓ Do tính phức tạp của các hàm chức năng trong các thiết bị, các chức năng điều khiển thường yêu cầu cấu hình từ phía người sử dụng.
- ✓ Trong nhiều trường hợp, chức năng này yêu cầu các tham số để thiết lập các điều hành thu thập dữ liệu và các điều hành chỉ có thể thực hiện khi các tham số được thiết lập đầy đủ.
- ✓ Nhiều nhóm chức năng trong cơ sở thông tin quản lý MIB có một vài bảng để thiết lập tham số điều khiển hoặc sử dụng để lưu kết quả của hoạt động điều hành.

RMON

◆ Điều khiển thiết bị RMON:

- ✓ Một số đối tượng trong MIB cung cấp một cơ chế thực hiện các hoạt động của thiết bị giám sát từ xa.
- ✓ Các đối tượng này có thể thực hiện các hoạt động khi có sự thay đổi trạng thái của đối tượng.



RMON

- ◆ Điều khiển thiết bị RMON – Chia sẻ tài nguyên giữa trạm quản lý:
 - ✓ Một số vấn đề tranh chấp tài nguyên thường xảy ra gồm:
 - Hai trạm quản lý cùng muốn sử dụng nguồn tài nguyên vượt quá khả năng của thiết bị.
 - Một trạm quản lý sử dụng một lượng tài nguyên nhất định trong một khoảng thời gian dài.
 - Một trạm quản lý sử dụng các tài nguyên và không giải phóng sau khi sử dụng.
 - Một cơ chế được cung cấp cho mỗi trạm quản lý tại MIB nhằm tránh các xung đột và giải quyết khi xung đột xảy ra.

RMON

- ◆ Điều khiển thiết bị RMON – Chia sẻ tài nguyên giữa trạm quản lý:
 - ✓ Mỗi một hàm chức năng có một nhãn nhận dạng khởi tạo.
 - ✓ Nhãn này được đặt bởi bộ khởi tạo nhằm tương thích các khả năng sau:
 - Một trạm quản lý có thể xác định rõ nguồn tài nguyên và yêu cầu sử dụng của nó.
 - Người điều hành mạng có thể tìm thấy các trạm chiếm giữ tài nguyên và thỏa thuận để giải phóng tài nguyên.
 - Người điều hành mạng có thể quyết định đơn phương giải phóng tài nguyên với các nhà điều hành mạng khác.
 - Ngay sau khi khởi tạo, một trạm quản lý có thể nhận dạng các nguồn tài nguyên đã được sử dụng trước đó và có thể giải phóng khi không được sử dụng..

RMON

- ◆ Điều khiển thiết bị RMON – Chia sẻ tài nguyên giữa trạm quản lý:
 - ✓ Các trạm quản lý và các phần tử thăm dò cần phải hỗ trợ tất cả định dạng của chuỗi đưa ra bởi các vùng mạng.
 - ✓ Thông tin chứa một hoặc một vài tên sau:
 - Địa chỉ IP, tên trạm quản lý , tên các nhà quản lý mạng, khu vực hoặc số điện thoại.
 - ✓ Các thông tin này sẽ giúp người sử dụng chia sẻ tài nguyên hiệu quả.

RMON

- ◆ Điều khiển thiết bị RMON – Chia sẻ tài nguyên giữa trạm quản lý:
 - ✓ Các trạm quản lý và các phần tử thăm dò cần phải hỗ trợ tất cả định dạng của chuỗi đưa ra bởi các vùng mạng.
 - ✓ Thông tin chứa một hoặc một vài tên sau:
 - Địa chỉ IP, tên trạm quản lý , tên các nhà quản lý mạng, khu vực hoặc số điện thoại.
 - ✓ Các thông tin này sẽ giúp người sử dụng chia sẻ tài nguyên hiệu quả.