

# Chương 5 CÔNG CỤ QUẢN TRỊ MẠNG

---

UIT, KHOA MMT-TT

1

## Nội dung

---

Các tác vụ quản trị mạng

SNMP

Công cụ quản trị mạng mã nguồn mở

2

2

## Các tác vụ quản trị mạng (ISO)

---

Fault management – Lỗi

Configuration management – Cấu hình

Accounting management – Tài khoản

Performance management – Hiệu năng

Security management – An toàn

3

3

Các tác vụ quản trị mạng

## Fault management

---

- Phát hiện, cô lập, tìm nguyên nhân và sửa lỗi
- Báo cáo cho người dung và quản lý
- Theo dõi xu hướng liên quan đến các lỗi đã được phát hiện

4

4

Các tác vụ quản trị mạng

## Configuration management

---

Lưu trữ và kiểm soát các phiên bản cấu hình của các thiết bị mạng/dịch vụ mạng

Lưu trữ danh sách tài sản network

Ghi lại các phiên bản của hệ điều hành cũng như các ứng dụng được sử dụng trong hệ thống

5

5

Các tác vụ quản trị mạng

## Accounting management

---

Theo dõi, kiểm soát việc sử dụng mạng của cá nhân hay các phòng ban

Tìm những người sử dụng tài nguyên mạng sai mục đích

6

6

Các tác vụ quản trị mạng

## Performance management

---

Theo dõi hiệu năng mạng

Theo dõi các thành phần riêng biệt như thiết bị, sử dụng băng thông

Kiểm tra kết nối

Đo thời gian phản hồi (response times)

Ghi nhận sự thay đổi của các đường định tuyến

7

7

Các tác vụ quản trị mạng

## Security management

---

Quản lý tập trung và phân phát username/password

Tạo khóa, phân phối và lưu trữ các khóa mã hóa

Phân tích cấu hình các thiết bị như router, switch, và server đối chiếu với các chính sách và quy trình an ninh thông tin

Thu thập, lưu trữ và kiểm tra các security logs

8

8

## Nội dung

Các tác vụ quản trị mạng

**SNMP**

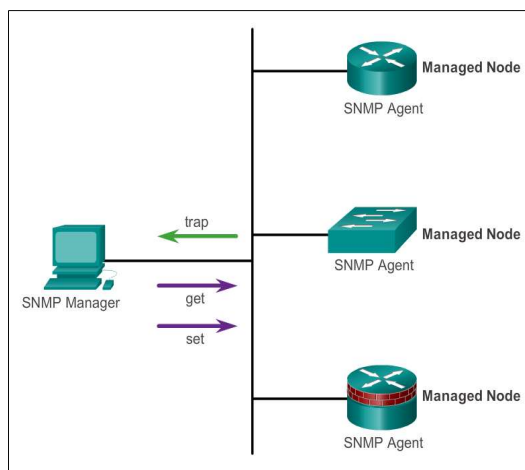
Công cụ quản trị mạng mã nguồn mở

9

9

## Giới thiệu SNMP

SNMP là một giao thức cho phép người quản trị quản lý từ xa các thành phần của thiết bị mạng như servers, PCs, routers, switches.



10

## Các thành phần quản lý mạng

**Managed device** là một thành phần chịu trách nhiệm thu thập và lưu các thông tin quản lý.

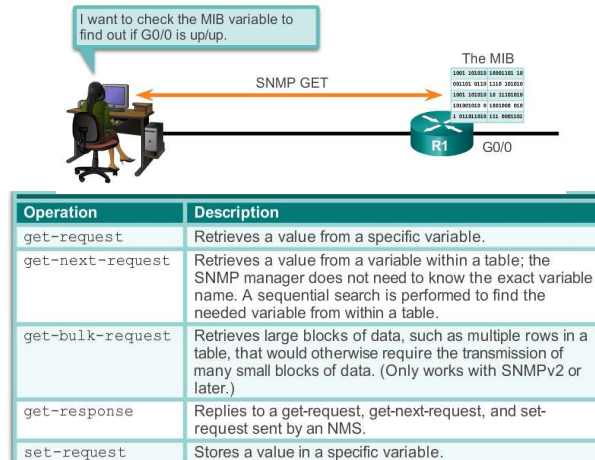
**Agent** là một phần mềm trên managed device

**Network-management system (NMS)** có nhiệm vụ hiển thị các thông tin quản lý, theo dõi và kiểm soát các managed devices, có khả năng liên lạc với các agents

**Management Information Base (MIB)** được sử dụng để lưu và trao đổi các thông tin quản trị

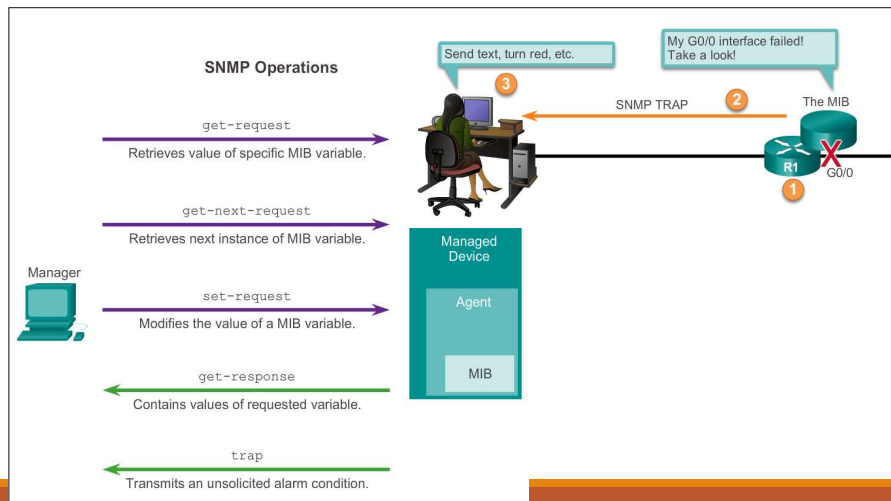
11

## Hoạt động của SNMP



12

## Hoạt động của SNMP (tt.)



13

## Các phiên bản của SNMP

- SNMPv1
- SNMPv2c
- SNMPv3

14

## Community Strings

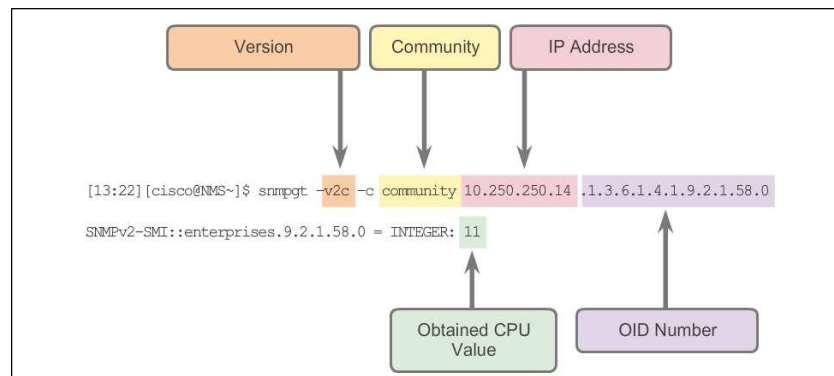
Có 2 loại community String:

**Read-only (ro)** – Cho phép truy cập đến các tham số trên MIB, nhưng không cho phép thay đổi các giá trị trên MIB

**Read-write (rw)** – Cho phép truy cập, đọc và thay đổi tất cả các đối tượng trên MIB

15

## Management Information Base Object ID



16



## Cấu hình SNMP

Step 1. Cấu hình community string **snmp-server community string ro | rw** command.

Step 2. Ghi chú vị trí của SNMP server **snmp-server location text**.

Step 3. Ghi chú người quản trị hệ thống **snmp-server contact text**.

17

## Cấu hình SNMP (tt.)

Step 4. Định nghĩa ACL cho phép các host có thể được truy cập đến SNMP Server **snmp-server community string access-list-number-or-name**.

Step 5. Xác định host được nhận SNMP trap **snmp-server host host-id [version {1 | 2c | 3 [auth | noauth | priv]}}] community-string**.

Step 6. Bật chế độ trap trên SNMP agent **snmp-server enable traps notification-types**.

18

## Kiểm tra cấu hình SNMP

```

R1# show snmp
Chassis: PTX16368482
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
  0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  19 Trap PDUs
SNMP Dispatcher:
  queue 0/75 (current/max), 0 dropped
SNMP Engine:
  queue 0/1000 (current/max), 0 dropped

```

```

R1# show snmp community
Community name: ILMI
Community Index: cisco0
Community SecurityName: ILMI
storage-type: read-only      active

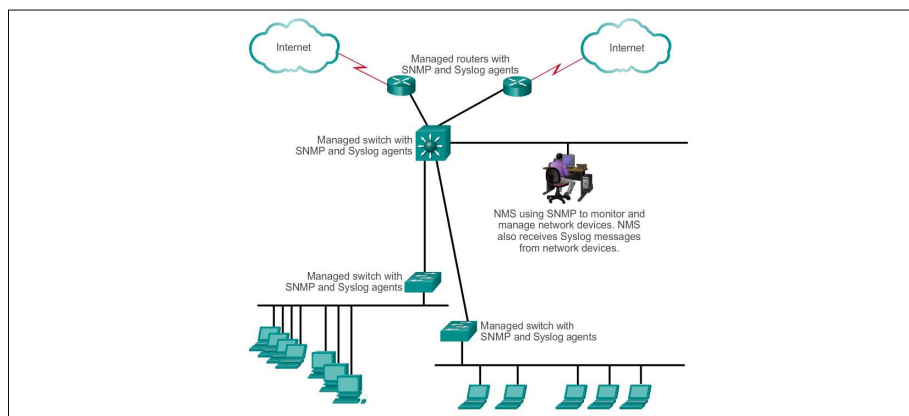
Community name: batonaug
Community Index: cisco7
Community SecurityName: batonaug
storage-type: nonvolatile    active    access-list: SNMP_ACL

Community name: batonaug@1
Community Index: cisco8
Community SecurityName: batonaug@1
storage-type: nonvolatile    active    access-list: SNMP_ACL

```

19

## Mô hình sử dụng SNMP



20

## Nội dung

---

Các tác vụ quản trị mạng

SNMP

Công cụ quản trị mạng mã nguồn mở

21

21

## Công cụ quản trị mạng mã nguồn mở

---

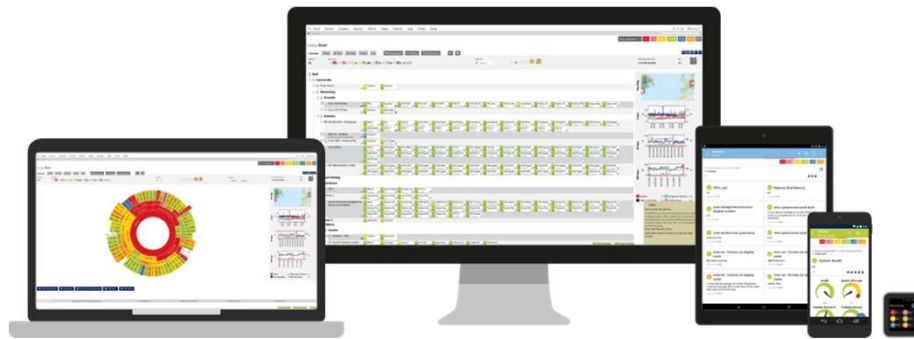
- Paessler PRTG
- Spiceworks
- Zabbix
- Nagios
- OpenNMS

22

22

Công cụ quản trị mạng mã nguồn mở  
Paessler PRTG

<https://www.paessler.com/prtg>

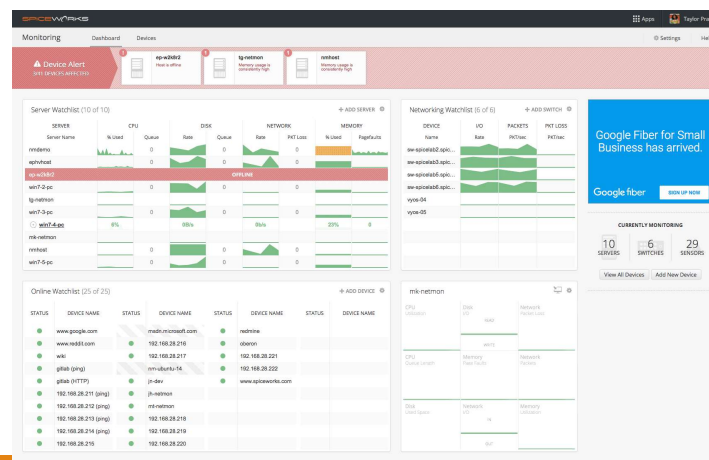


23

23

Công cụ quản trị mạng mã nguồn mở  
Spiceworks

<https://www.spiceworks.com/>



24

24

## Công cụ quản trị mạng mã nguồn mở Zabbix

[www.zabbix.com/](http://www.zabbix.com/)

**ZABBIX** Monitoring Inventory Reports Configuration Administration

Dashboard Problems Overview Web Latest data Triggers Graphs Screens Maps Discovery IT services Central NOC

Problems [Export to CSV](#)

Filter

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
11:59:31 AM	Average		PROBLEM		Linux000	Too many queries per second	1m 23s	Yes 1	Done 1	Datacenter: NY1   Env: Production   Service: HTTP balancer
11:58:55 AM	Average		PROBLEM		Linux002	Too many transactions per second	1m 59s	No	Done 1	Datacenter: FR2   Env: Staging   Service: Oracle
11:00										
10:13:32 AM	High		PROBLEM		Linux009	Service RestAPI stopped	1h 47m 22s	Yes 1		Datacenter: NY1   Env: Staging   Service: RestAPI
10:11:06 AM	High		PROBLEM		Linux005	Service Redis stopped	1h 49m 48s	Yes 1		Datacenter: FR2   Env: Staging   Service: Redis
Today										
09/13/2016 11:01:08 PM	Information		PROBLEM		Linux007	Slow query execution time	12h 59m 46s	No		Datacenter: NY1   Env: Production   Service: AWS Dynam...
09/13/2016 10:48:24 PM	Average		PROBLEM		Linux003	Too many transactions per second	13h 12m 30s	No		Datacenter: FR2   Env: Staging   Service: Oracle
09/13/2016 10:47:27 PM	Average	11:59:19 AM	RESOLVED		Linux000	Too many queries per second	13h 11m 52s	Yes 2		Datacenter: NY1   Env: Production   Service: HTTP balancer
09/13/2016 10:47:04 PM	Average		PROBLEM		Linux009	Too many queries per second	13h 13m 50s	No		Datacenter: NY1   Env: Production   Service: HTTP balancer
Yesterday										
09/07/2016 05:08:38 PM	Information		PROBLEM		Linux008	Low CPU utilization on host machines	6d 16h 51m	Yes 1		Datacenter: FR2   Service: Kubernetes
09/07/2016 09:58:08 AM	Average		PROBLEM		Linux001	Too many transactions per second	7d 2h 2m	Yes 1	Failures 1	Datacenter: FR2   Service: Oracle

0 selected [Bulk acknowledge](#)

Displaying 10 of 10 found

25

25

## Công cụ quản trị mạng mã nguồn mở Nagios

<https://www.nagios.org/>

**Nagios** 3.5.4 System OK: 100% (10/10) logged in as...

Home Views Dashboards Reports Configure Tools Help Admin

My Reports

Linux Servers Hostgroup  
Availability  
Capacity Planning  
Capacity Planning Forecast  
1 min  
Capacity Planning table

Available Reports

Executive Summary  
Availability  
SLA Report  
Status History  
Top Alert Producers  
Alert Histogram  
Notification  
Event Log  
Backend Log  
Capacity Planning  
Network Report  
Network Query

Network Report

Web Server: 192.168.1.120 Source: Sourcegroup localhost [+] Show Column Endpoints

Report to run: Top 5 Talkers By Source IP (Last 24 Hours) Run Report

Report: Top 5 Talkers By Source IP (Last 24 Hours)

Source: localhost on 192.168.1.120 (Showing top 5 based on Source IP and ordered by Bytes)  
Timeframe: Last 24 Hours

Other: 25.0%  
18.4.129.5: 5.4%  
168.3.37: 0.3%  
92.168.5.224: 7.5%  
244.177.131.20: 22.0%

Pie Chart Cloud Diagram (Only + - - - - -) Cloud Diagram (Only + - - - - -) Cloud Diagram (Only + - - - - -) Cloud Diagram (Only + - - - - -)

Start Date	End Date	Duration	Protocol	Source IP	Flows	Flow %	Packets	Packet %	Bytes	Byte %	Packets/sec	Byte/sec	Bits/Sec	Bits/Package
2016-09-13 12:25:36	2016-09-13 12:18:22	9512.057	any	244.177.131.205	2742	9.1	42769	10.6	31.47 MB	31.4	0	3068	768	
2016-09-13 12:27:26	2016-09-13 12:17:22	95882.795	any	192.168.1.134	2432	8.3	20594	9.8	22.68 MB	22.6	0	2226	650	
2016-09-13 12:25:36	2016-09-13 12:18:59	86387.883	any	192.168.1.224	1132	2.7	43657	10.8	7.49 MB	7.5	0	720	179	

26

26

Công cụ quản trị mạng mã nguồn mở

OpenNMS

demo.opennms.org

Horizon

OpenNMS

Nov 27, 2016 11:36 EST

Search Info Status Reports Dashboards Maps demo

Home

Nodes with Pending Problems

search.internal.opennms.com has 1 alarm (33 minutes)

chef.internal.opennms.com has 2 alarms (2 days)

Nodes with Outages

search.internal.opennms.com (33 minutes)

chef.internal.opennms.com (2 days)

demo.opennms.org (4 days)

monity.internal.opennms.com (4 days)

172.20.1.114 (6 days)

modaniels.internal.opennms.com (2 weeks)

mrmakay.internal.opennms.com (2 weeks)

cartman.internal.opennms.com (1 month)

linny.internal.opennms.com (1 month)

biggavai.internal.opennms.com (1 month)

meghesto.internal.opennms.com (2 months)

DJ's Raspberry Pi (4 months)

Business Services with Pending Problems

There are no pending problems.

Applications with Pending Problems

There are no pending problems.

Availability Over the Past 24 Hours

Categories	Outages	Availability
Network Interfaces	19 of 141	93.614%
Web Servers	5 of 55	93.936%
Email Servers	0 of 17	100.000%
DNS and DHCP Servers	5 of 8	75.000%
Database Servers	0 of 9	100.000%
JMX Servers	0 of 0	100.000%
Software Update	5 of 30	86.310%
Other Servers	11 of 79	92.405%
<b>Total</b>		
Overall Service Availability	48 of 379	97.068%

Alarm Heatmap (by Categories)

Production

Unacknowledged

Servers

Probes

Dev

Self

Alarms / Outages Categories / Foreign Sources / Services Normal Warning Minor Major Critical

Notifications

You have no outstanding notices

There are no outstanding notices

On-Call Schedule

Resource Graphs

Search

KSC Reports

Search

Grafana Dashboards

Demo

OSMC

Test

Quick Search

Node ID:

Search

Node label like:

27