ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

GIÁM SÁT MẠNG

Giảng viên: Lê Tự Thanh
Email : ltthanh@vku.udn.vn
Website : www.vku.udn.vn

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

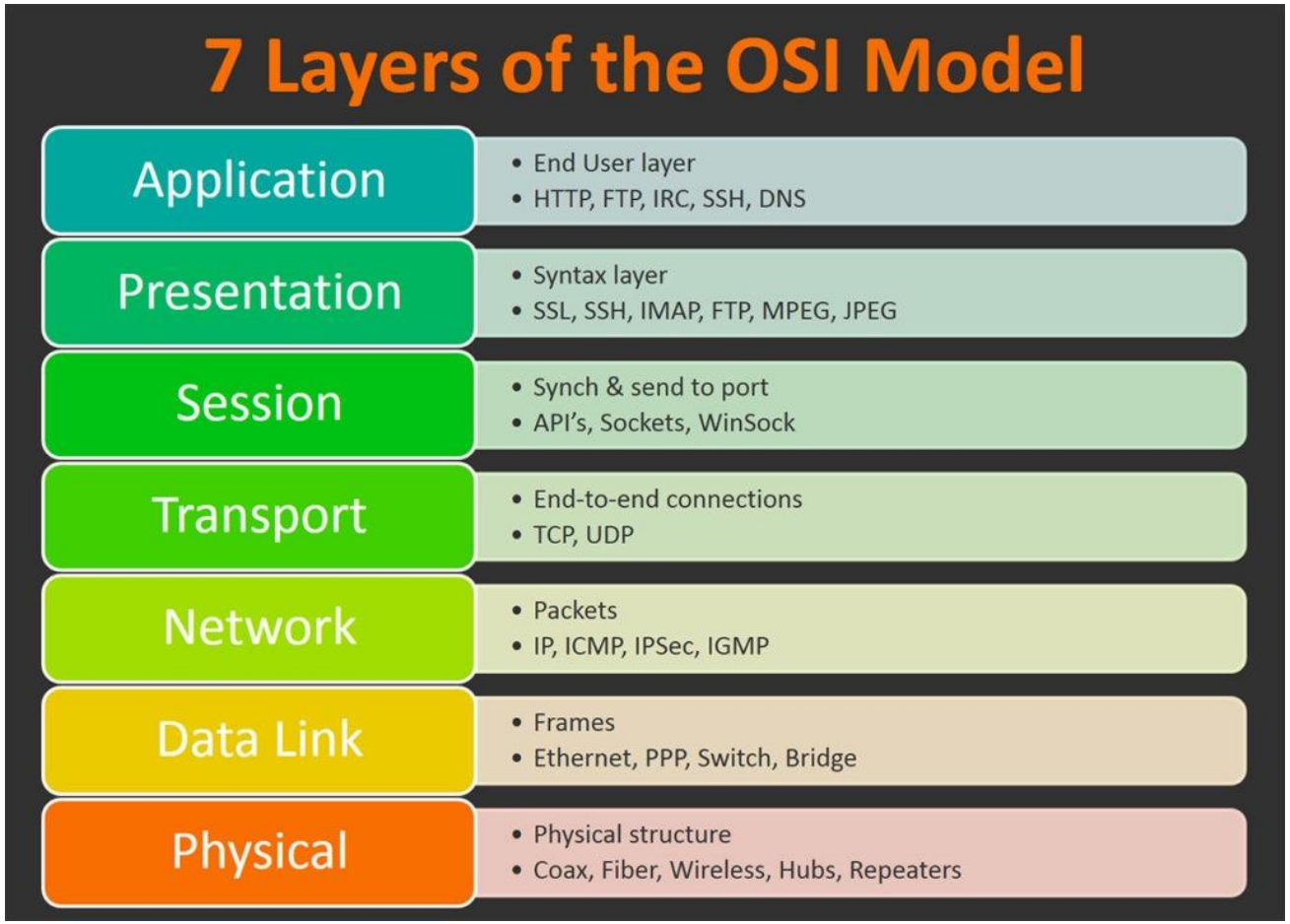
1.1. Khái niệm về giám sát mạng

Giám sát mạng là quá trình giám sát tính khả dụng, thời gian hoạt động, hoạt động và hiệu suất của các hệ thống mạng. Trong đó bao gồm theo dõi và phân tích các thành phần mạng như bộ định tuyến, thiết bị chuyển mạch, tường lửa, các dịch vụ mạng. Điều này cũng liên quan đến việc giám sát các lớp dữ liệu, điểm cuối mạng và liên kết khác nhau. Kiểm tra tình trạng và hiệu suất của giao diện mạng để dò tìm lỗi, giúp chẩn đoán, tối ưu hóa và quản lý các tài nguyên mạng khác nhau cả tại chỗ và từ xa.

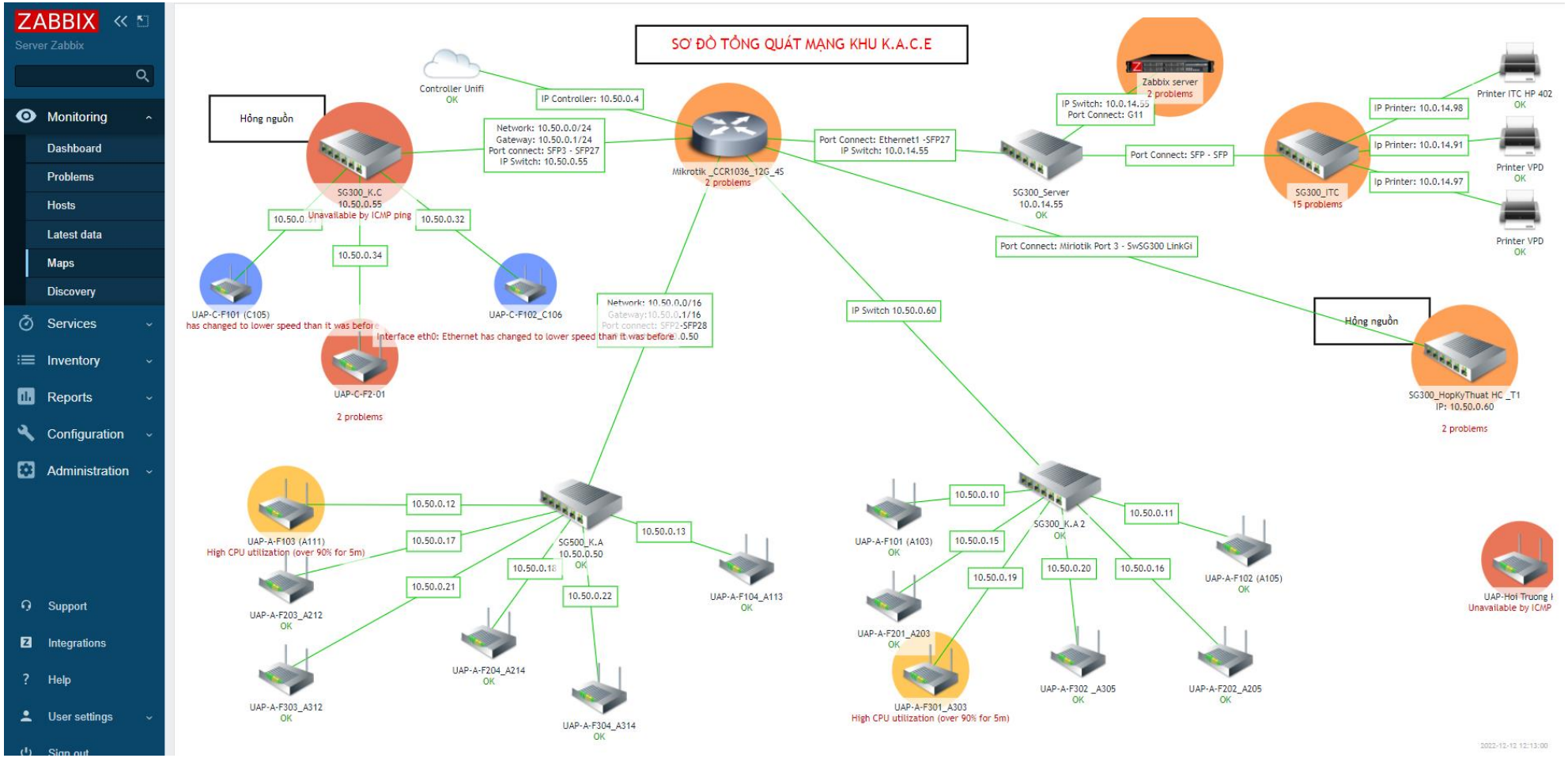
CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

1.2. Các thành phần cơ bản cần giám sát

- Giám sát hạ tầng mạng: Router, Switch, AP,..
- Giám sát dịch vụ mạng: Web server, DHCP Server, DNS Server,..



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Router

Online Status >> Physical Connection

Physical Connection — System Uptime: 18days 3:27:38

IPv4 | IPv6

LAN Status

IP Address	TX Packets	RX Packets	Router Primary DNS:	Router Secondary DNS:
192.168.50.1	1,981,300,116	920,782,632	203.113.131.2	203.113.131.3

WAN 5 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	435:27:21	
IP	GW IP	TX Packets	TX Rate(bps)	RX Packets	RX Rate(bps)
117.3.64.239	27.71.110.4	292,600,646	600.62 K	641,686,112	8.49 M

WAN 6 Status >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	435:27:18	
IP	GW IP	TX Packets	TX Rate(bps)	RX Packets	RX Rate(bps)
113.160.225.171	123.29.8.28	320,086,275	1.01 M	606,723,445	3.33 M

WAN 7 Status >> Drop PPPoE

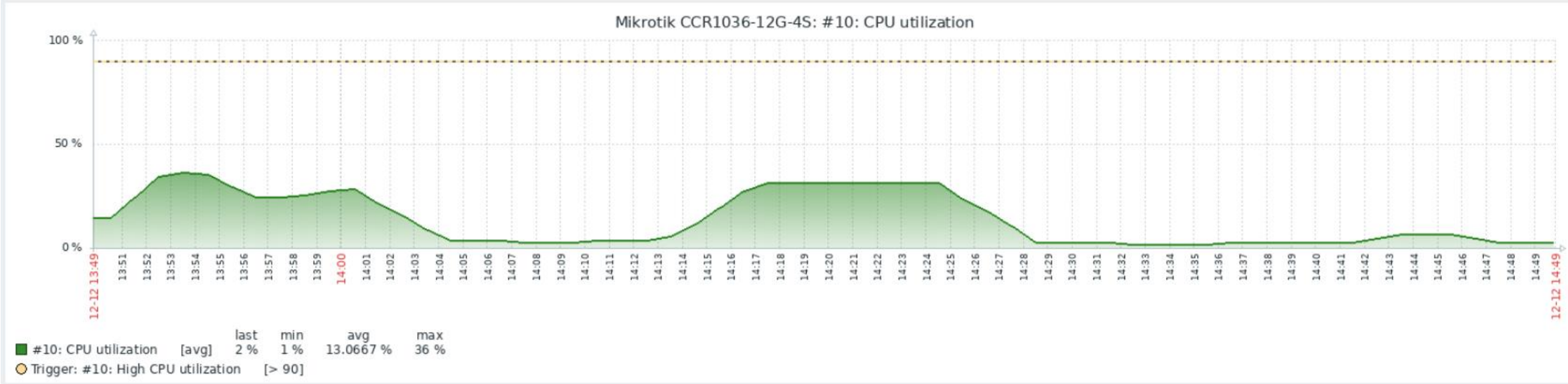
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	256:23:53	
IP	GW IP	TX Packets	TX Rate(bps)	RX Packets	RX Rate(bps)
117.2.155.129	27.71.110.4	281,532,517	553.17 K	652,736,144	8.60 M

WAN 8 Status >> Renew

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	00:00:00	
IP	GW IP	TX Packets	TX Rate(bps)	RX Packets	RX Rate(bps)
---	---	0	0	0	0

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Router

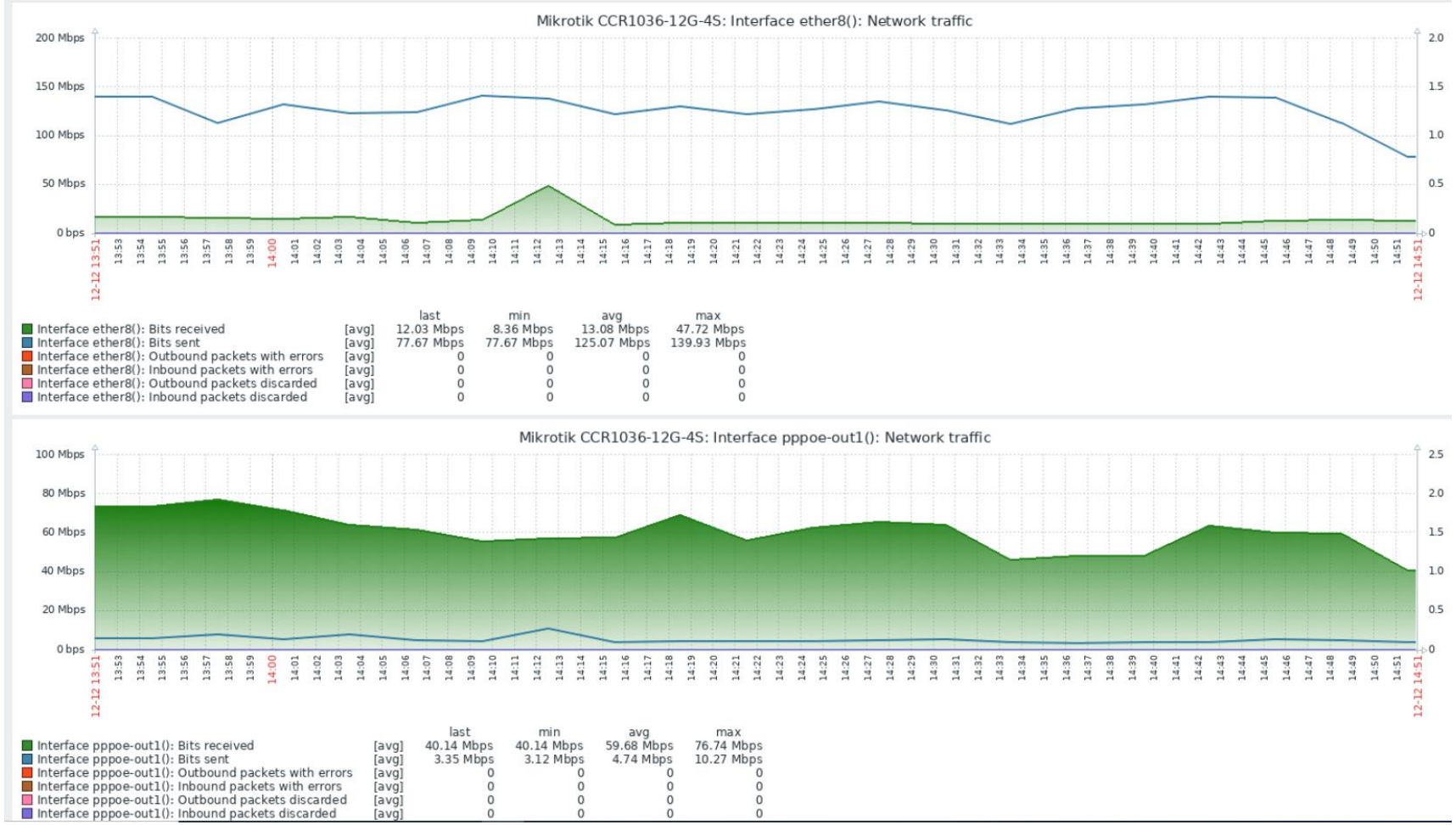


CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Router

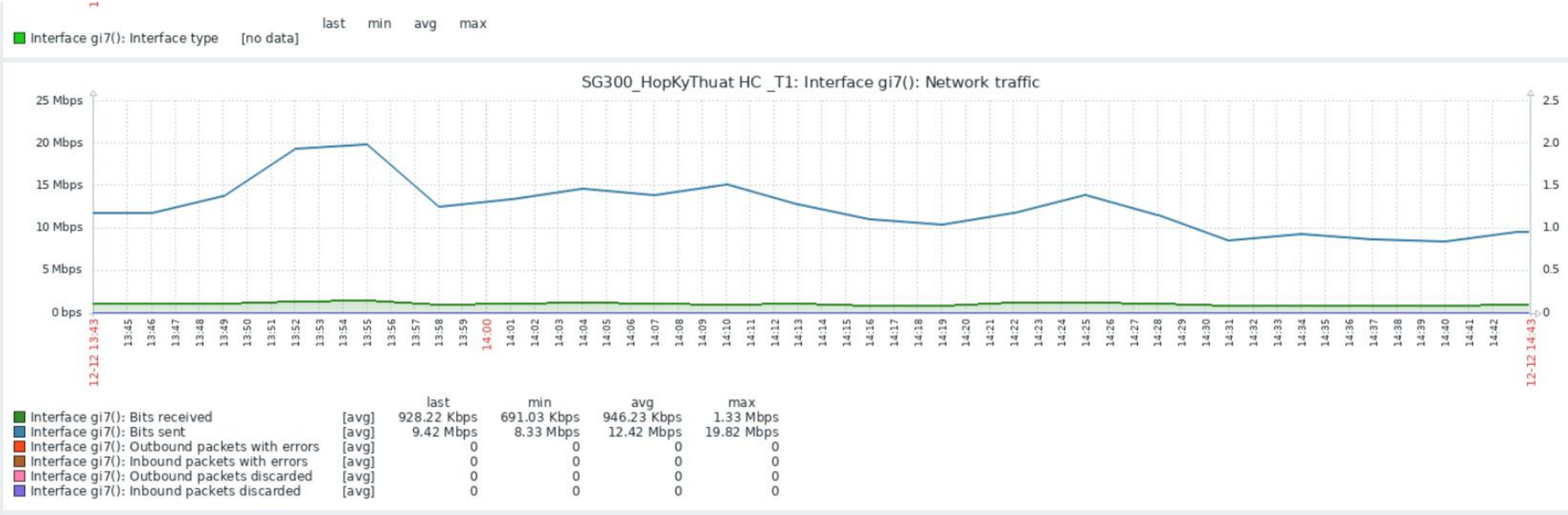
CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Router



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Switch

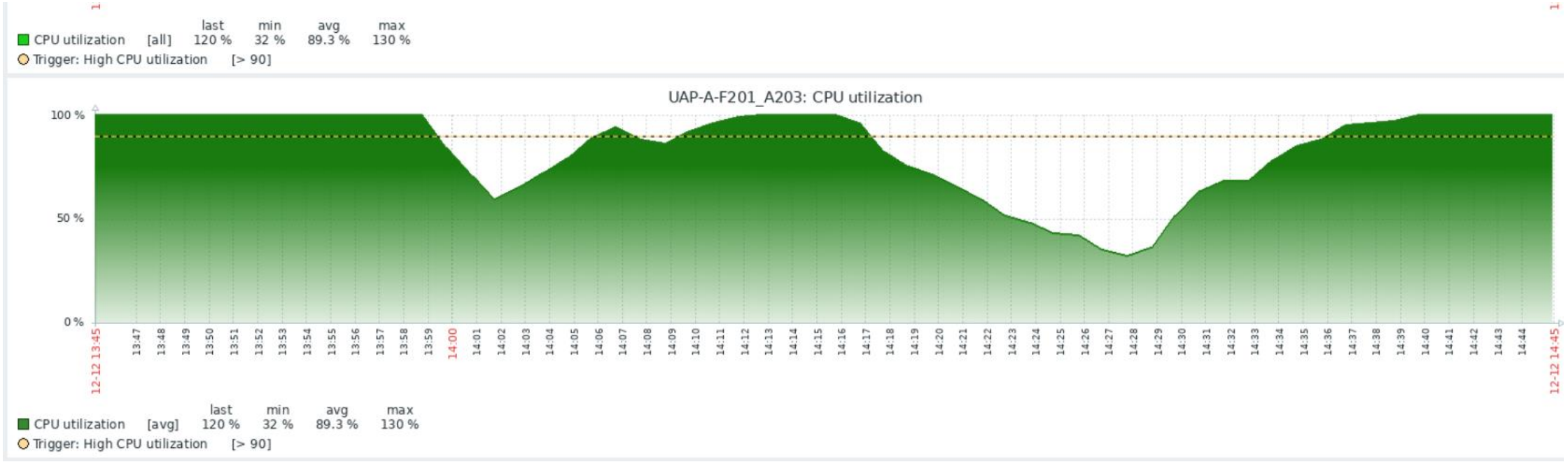


CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Switch

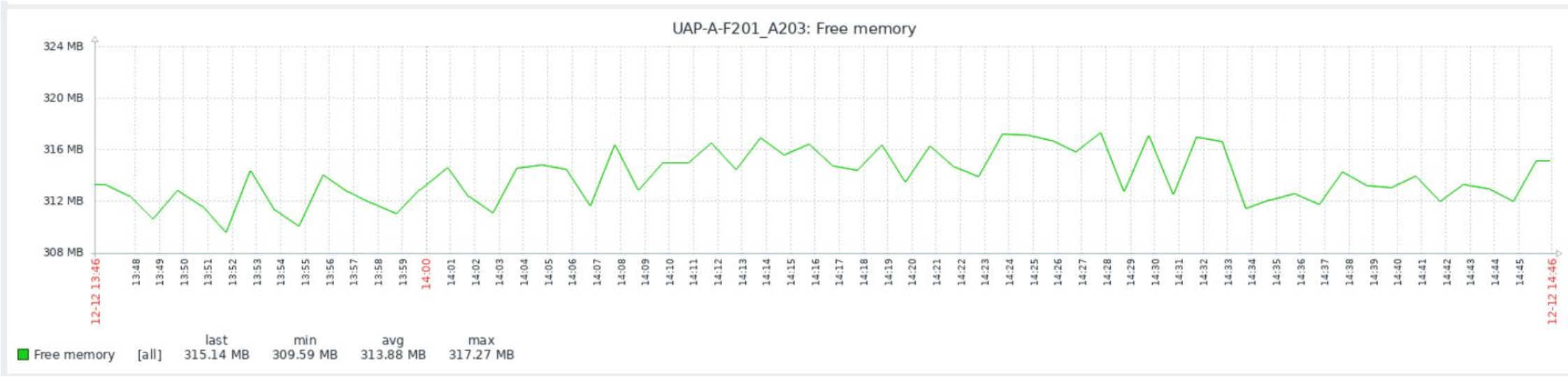
CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Access Point



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Access Point



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Giám sát Access Point

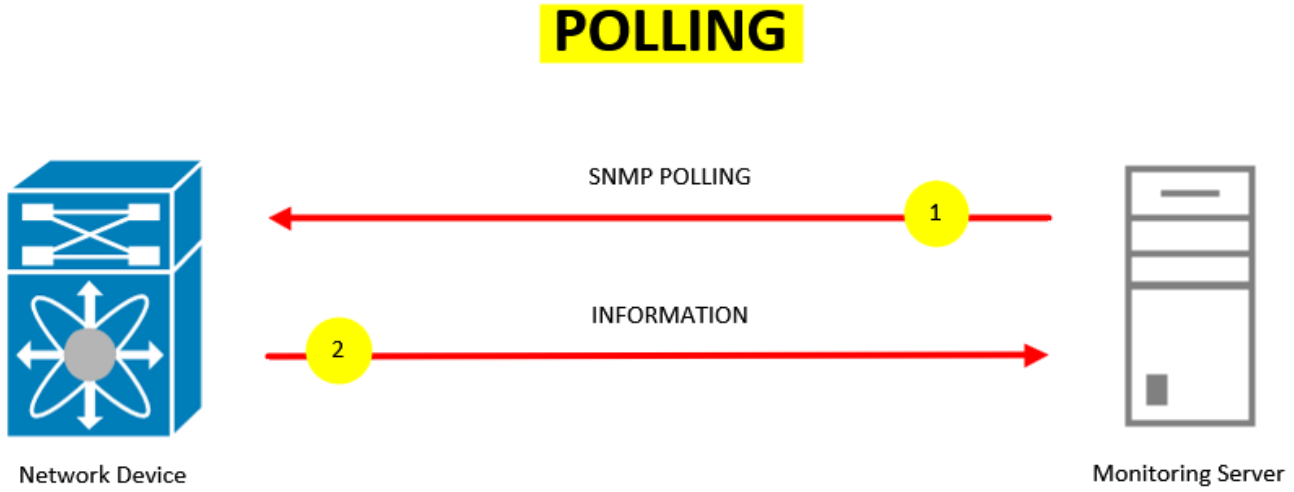
1.3. Các phương thức giám sát mạng

Có 2 phương thức giám sát mạng là **Poll** và **Trap:** Đây là 2 phương thức cơ bản của các kỹ thuật giám sát hệ thống mạng, nhiều phần mềm và giao thức được xây dựng dựa trên 2 phương thức này, trong đó phổ biến là SNMP (Simple Network Management Protocol).

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

Phương thức Poll:

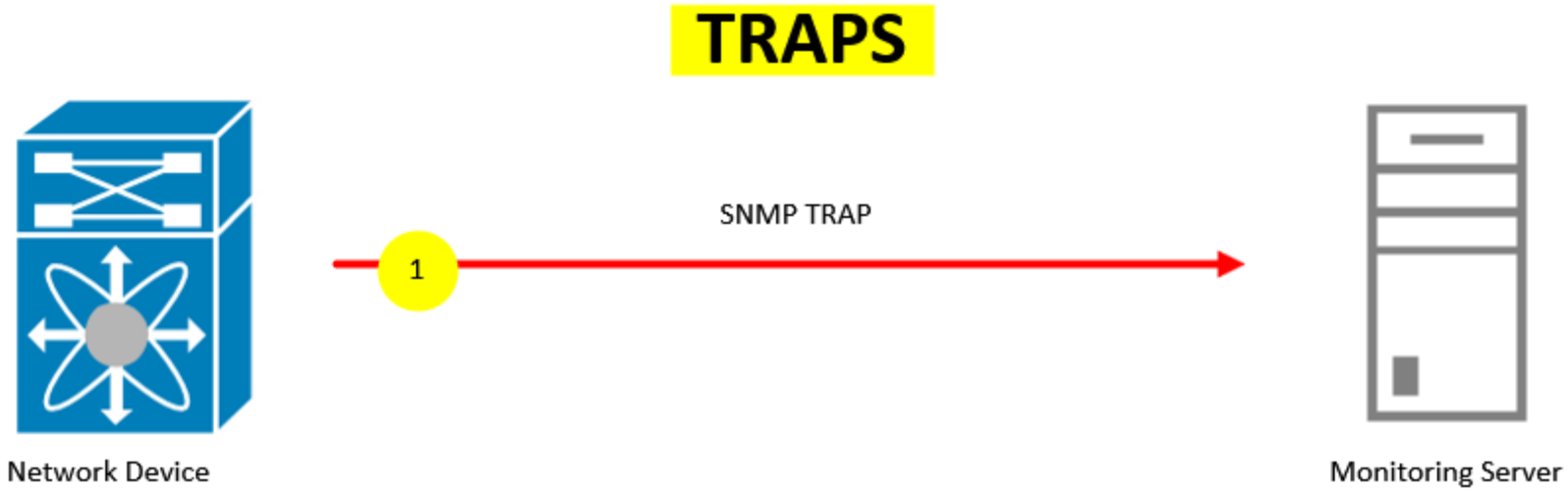
Nguyên tắc hoạt động: Trung tâm giám sát (manager) định kỳ hỏi thông tin của thiết bị cần giám sát (device). Nếu Manager không hỏi thì Device không trả lời, nếu Manager hỏi thì Device phải trả lời. Bằng cách hỏi thường xuyên, Manager sẽ luôn cập nhật được thông tin mới nhất từ Device.



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

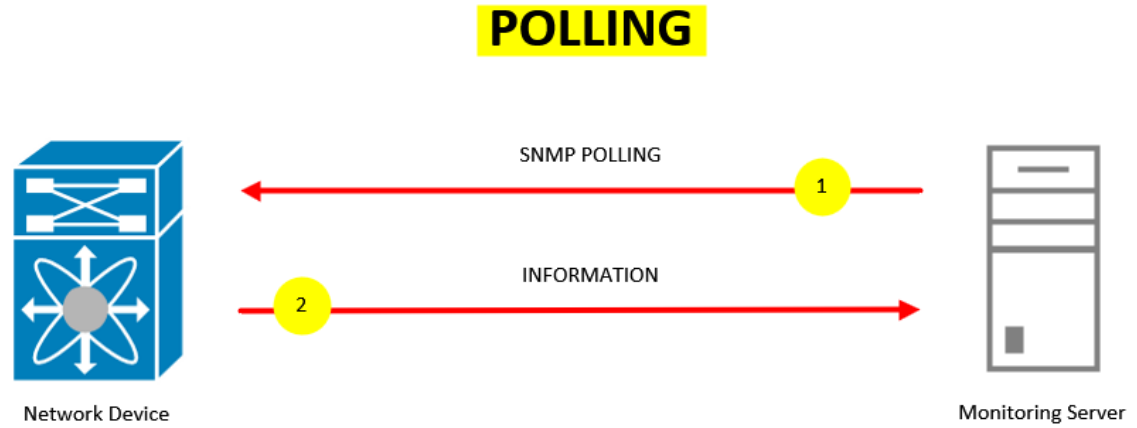
Phương thức Trap:

Nguyên tắc hoạt động : Mỗi khi Device xảy ra một sự kiện (event) nào đó thì Device sẽ tự động gửi thông báo cho Manager, gọi là Trap. Manager không hỏi thông tin định kỳ từ Device.



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

So sánh phương thức Poll và Trap



So sánh phương thức Poll và Trap

Hai phương thức Poll và Trap hoàn toàn khác nhau về cơ chế hoạt động. Một ứng dụng giám sát hệ thống mạng có thể sử dụng Poll hoặc Trap, hoặc cả hai, tùy vào yêu cầu cụ thể trong thực tế. Cụ thể theo bảng sau:

SO SÁNH PHƯƠNG THỨC GIÁM SÁT MẠNG

POLL	TRAP
Chủ động lấy những thông tin cần thiết từ các đối tượng mình quan tâm, không cần lấy những thông tin không cần thiết từ những nguồn không quan tâm.	Tất cả các event xảy ra đều được gửi về Manager. Manager phải có cơ chế lọc các vent cần thiết, hoặc thiết bị phải thiết lập được cơ chế chỉ gửi những event cần thiết.
Có thể lập bảng trạng thái tất cả các thông tin của thiết bị sau khi Poll qua một lượt các thông tin đó.	Nếu không có event gì xảy ra thì Manager không biết được trạng thái của thiết bị.
Nếu đường truyền giữa Manager và thiết bị xảy ra gián đoạn và thiết bị có sự thay đổi, thì Manager sẽ không thể cập nhật. Tuy nhiên khi đường truyền thông suốt trở lại thì Manager sẽ cập nhật được thông tin mới nhất do nó luôn poll định kỳ.	Khi đường truyền gián đoạn và thiết bị có sự thay đổi thì nó vẫn gửi Alert cho Manager, nhưng Trap này sẽ không thể đến được Manager. Sau đó mặc dù đường truyền có thông suốt trở lại thì Manager vẫn không thể biết được những gì đã xảy ra.

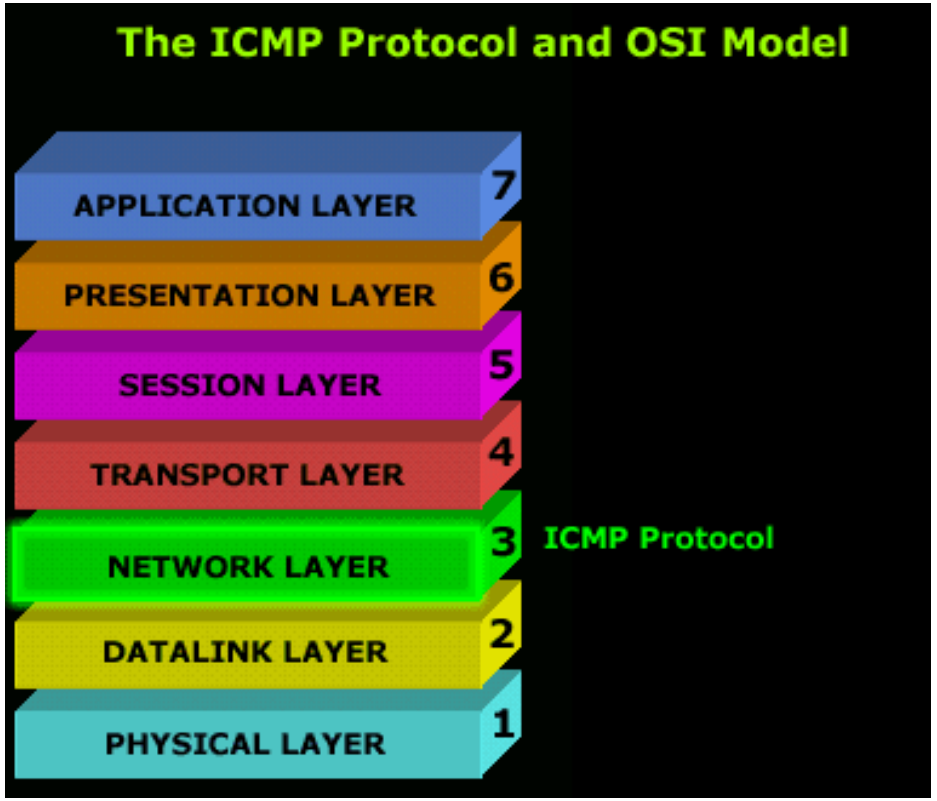
SO SÁNH PHƯƠNG THỨC GIÁM SÁT MẠNG

POLL	TRAP
Chỉ cần cài đặt tại Manager để trỏ đến tất cả các thiết bị. Có thể dễ dàng thay đổi một Manager khác.	Phải cài đặt tại từng thiết bị để trỏ đến Manager. Khi thay đổi Manager thì phải cài đặt lại trên tất cả thiết bị để trỏ về Manager mới.
Nếu tần suất poll thấp, thời gian chờ giữa 2 chu kỳ poll (polling interval) dài sẽ làm Manager chậm cập nhật các thay đổi của thiết bị.	Ngay khi có sự kiện xảy ra thì thiết bị sẽ gửi Trap đến Manager, do đó Manager luôn luôn có thông tin mới nhất tức thời.
Có thể bỏ sót các sự kiện: khi thiết bị có thay đổi, sau đó thay đổi trở lại như ban đầu trước khi đến lượt poll kế tiếp thì Manager sẽ không phát hiện được.	Manager sẽ được thông báo mỗi khi có sự kiện xảy ra ở thiết bị, do đó Manager không bỏ sót bất kỳ sự kiện nào.

1.4. Một số lệnh kiểm tra mạng

- Lệnh Ping

Lệnh PING sử dụng giao thức ICMP, PING cho phép người quản trị mạng xác định được các thiết bị còn hoạt động hay không.

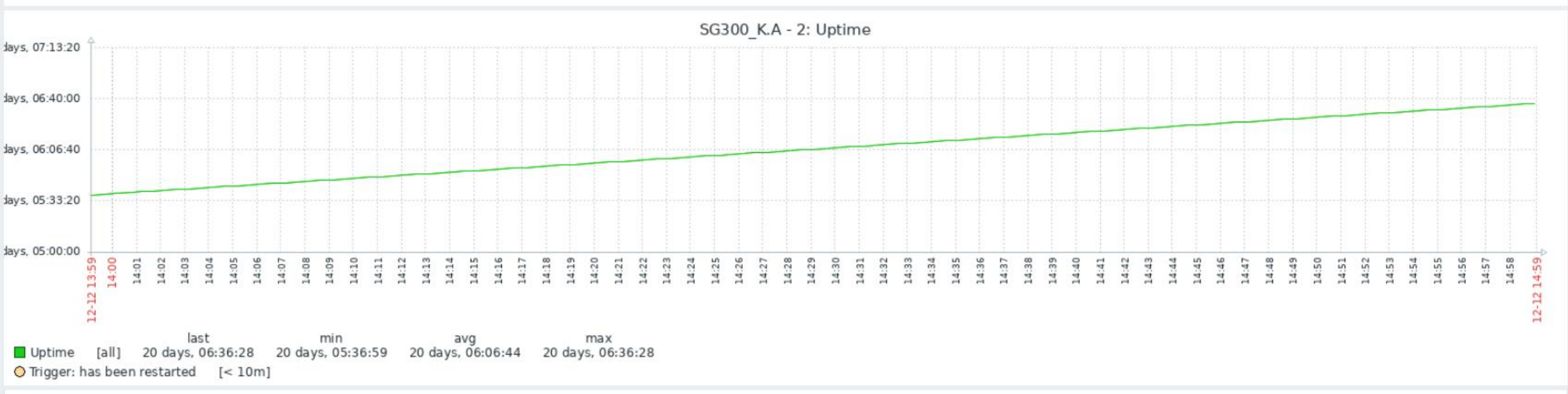


ICMP: Internet Control Message Protocol

- used by hosts, routers, gateways to communication network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG



- Lệnh Tracert

Tracert là công cụ dòng lệnh dùng để xác định đường đi từ nguồn tới đích của một gói Giao thức mạng Internet (IP - Internet Protocol). Tracert tìm đường tới đích bằng cách gửi các thông báo Echo Request (yêu cầu báo hiệu lại) Internet Control Message Protocol (ICMP) tới từng đích. Sau mỗi lần gặp một đích, giá trị Time to Live (TTL), tức thời gian cần để gửi đi sẽ được tăng lên cho tới khi gặp đúng đích cần đến. Thực tế càng qua nhiều trạm thì càng chậm và càng có rủi ro bị time out (mất kết nối).

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

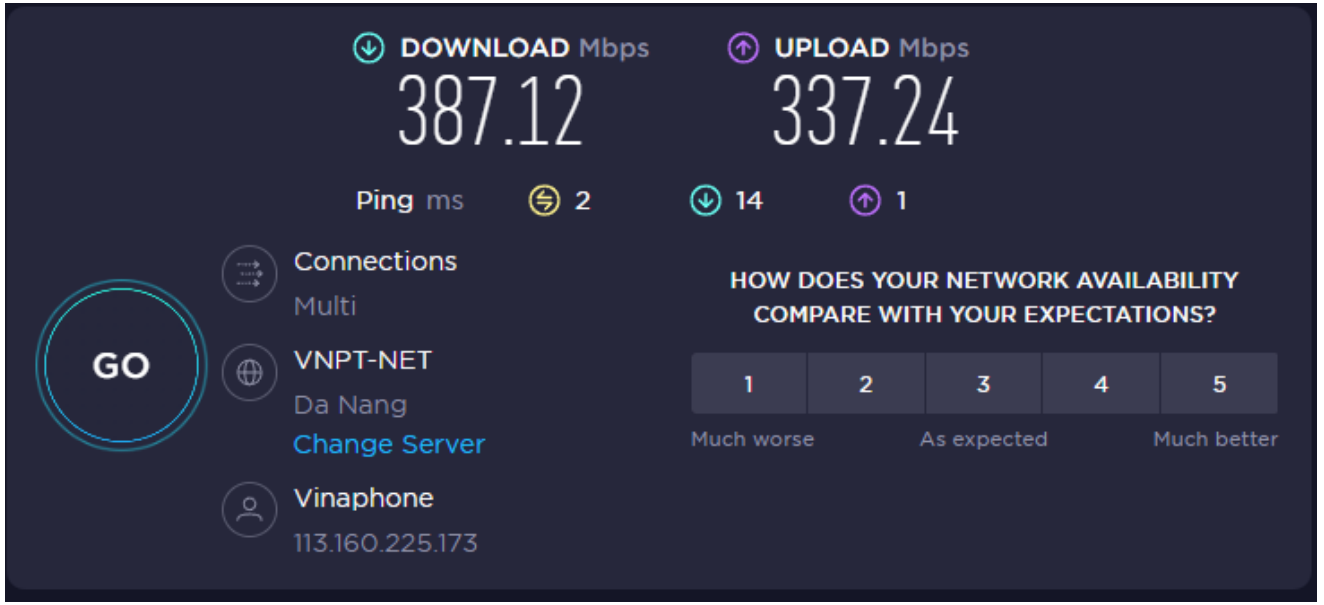
Ví dụ: Tracert Google.com

```
C:\Users\QQ>tracert google.com

Tracing route to google.com [216.58.221.142]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     4 ms     4 ms     2 ms  113.22.4.117
  3    27 ms    27 ms    26 ms  118.69.166.149
  4    24 ms    24 ms    23 ms  118.69.131.170
  5    27 ms    28 ms    28 ms  74.125.50.73
  6    28 ms    32 ms     *     108.170.241.33
  7    25 ms    24 ms    24 ms  108.170.232.255
  8    26 ms    31 ms    27 ms  hkg07s02-in-f14.1e100.net [216.58.221.142]

Trace complete.
```

CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

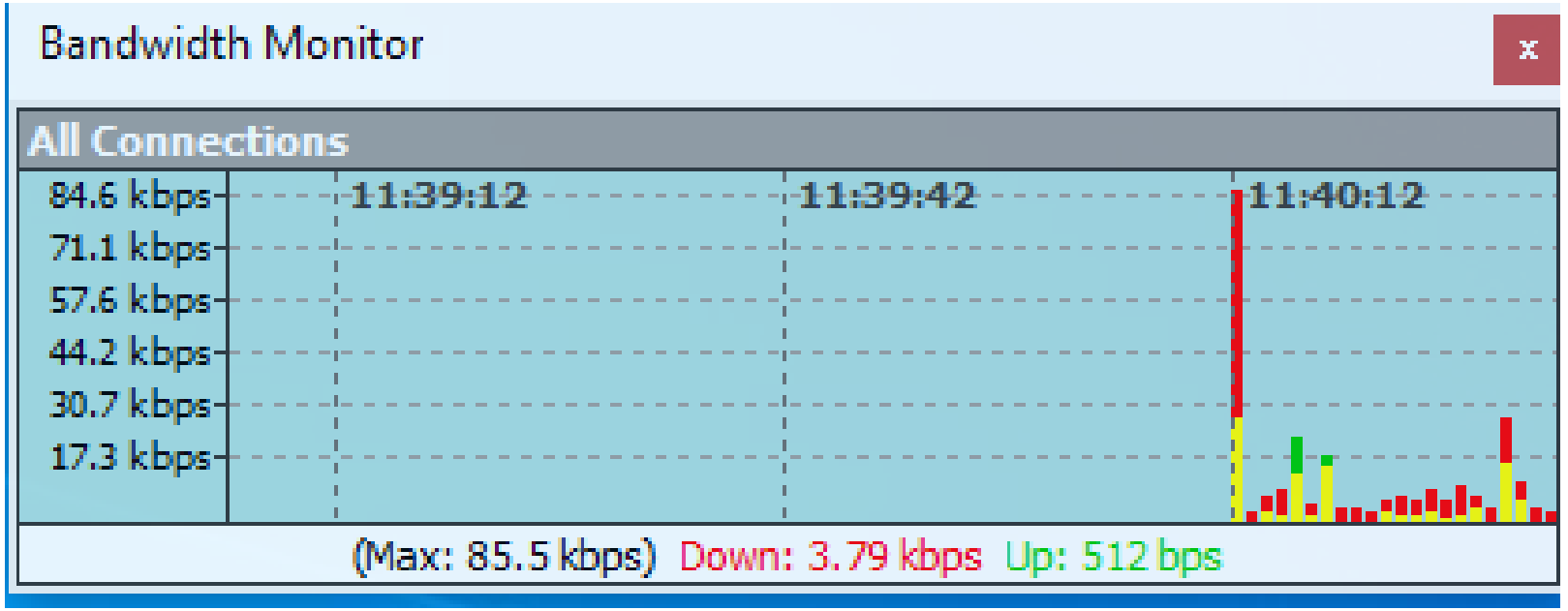
- Kiểm tra băng thông mạng

Có thể sử dụng các ứng dụng hoặc các web site để kiểm tra bang thông của hệ thống mạng



CHƯƠNG 1. CÁC KHÁI NIỆM CƠ BẢN VỀ GIÁM SÁT HỆ THỐNG MẠNG

- Kiểm tra băng thông mạng



CÁC KHÁI NIỆM CƠ BẢN VỀ QUẢN TRỊ MẠNG

Q & A