**Lý thuyết chi tiết về các giao thức mạng (SNMP, ICMP, ARP)**

**1. SNMP (Simple Network Management Protocol)**

**Định nghĩa và lịch sử phát triển:**

**SNMP, hay còn gọi là Giao thức Quản lý Mạng Đơn giản, là một giao thức thuộc tầng ứng dụng (Application Layer) trong mô hình TCP/IP, được thiết kế để hỗ trợ việc quản lý và giám sát các thiết bị trong mạng. SNMP được phát triển bởi Internet Engineering Task Force (IETF) vào cuối những năm 1980, với phiên bản đầu tiên (SNMPv1) được chuẩn hóa vào năm 1990 qua RFC 1157. Sau đó, giao thức này được cải tiến qua các phiên bản SNMPv2c (cải thiện hiệu suất) và SNMPv3 (tăng cường bảo mật). Mục tiêu chính của SNMP là cung cấp một phương pháp chuẩn hóa để các nhà quản trị mạng có thể thu thập thông tin, giám sát trạng thái, và điều khiển các thiết bị mạng như router, switch, máy chủ, máy trạm, máy in, và thậm chí cả các thiết bị IoT.**

**Cấu trúc và cách hoạt động:**

**SNMP hoạt động dựa trên mô hình client-server, trong đó có ba thành phần chính:**

**- Manager (Hệ thống quản lý): Đây là phần mềm hoặc hệ thống được sử dụng bởi quản trị viên để gửi yêu cầu và nhận thông tin từ các thiết bị. Manager có thể là một ứng dụng giám sát mạng (như hệ thống mà nhóm các bạn đang phát triển) hoặc các phần mềm chuyên dụng như SolarWinds, Nagios.**

**- Agent (Tác nhân): Là phần mềm chạy trên thiết bị được quản lý (như router, switch, máy chủ). Agent thu thập thông tin từ thiết bị và gửi về Manager khi nhận được yêu cầu. Agent cũng có thể tự động gửi thông báo (TRAP) khi phát hiện sự kiện bất thường, ví dụ: một giao diện mạng bị ngắt kết nối.**

**- MIB (Management Information Base): Là cơ sở dữ liệu chứa các thông số của thiết bị, được tổ chức theo cấu trúc cây (tree structure). Mỗi thông số được truy cập thông qua một OID (Object Identifier), là một chuỗi số phân cấp, ví dụ: `1.3.6.1.2.1.1.3.0` đại diện cho thời gian hoạt động của thiết bị (sysUpTime), hoặc `1.3.6.1.2.1.25.3.3.1.2` để lấy thông số CPU usage.**

**SNMP sử dụng giao thức UDP (User Datagram Protocol) để truyền dữ liệu, với port 161 cho các yêu cầu (GET, SET) và port 162 cho các thông báo TRAP. Việc sử dụng UDP giúp giảm tải cho hệ thống, nhưng cũng có nhược điểm là không đảm bảo độ tin cậy (do UDP không có cơ chế kiểm tra lỗi như TCP).**

**SNMP hỗ trợ các lệnh chính sau:**

**- GET: Manager gửi yêu cầu để lấy thông tin từ Agent (ví dụ: lấy CPU usage).**

**- SET: Manager gửi lệnh để thay đổi cấu hình trên thiết bị (ví dụ: bật/tắt một giao diện).**

**- TRAP: Agent tự động gửi thông báo đến Manager khi có sự kiện xảy ra (ví dụ: thiết bị khởi động lại).**

**- GETNEXT và GETBULK (từ SNMPv2): Dùng để lấy nhiều thông số cùng lúc, giúp tăng hiệu quả.**

**Ứng dụng trong thực tế:**

**SNMP được sử dụng rộng rãi trong quản lý mạng, đặc biệt trong các hệ thống giám sát lớn. Ví dụ, một công ty có thể dùng SNMP để theo dõi trạng thái của hàng trăm router và switch trong hệ thống, phát hiện các sự cố như CPU usage quá cao, băng thông vượt ngưỡng, hoặc thiết bị bị ngắt kết nối. SNMP cũng được tích hợp vào các phần mềm quản lý mạng để tạo dashboard trực quan, giúp quản trị viên dễ dàng theo dõi và xử lý sự cố.**

**Ứng dụng trong dự án:**

**Trong dự án "Phát triển hệ thống quản lý mạng nội bộ để giám sát, cảnh báo kết nối trái phép và phát hiện lỗi nghiêm trọng," SNMP được sử dụng để:**

**- Giám sát thiết bị: Thu thập các thông số quan trọng như CPU usage, memory usage, và băng thông (tốc độ mạng) từ các thiết bị trong mạng nội bộ. Ví dụ, nhóm sử dụng OID `1.3.6.1.2.1.25.3.3.1.2` để lấy CPU usage và OID `1.3.6.1.2.1.2.2.1.10` (ifInOctets) cùng `1.3.6.1.2.1.2.2.1.16` (ifOutOctets) để lấy băng thông vào/ra.**

**- Tính tốc độ mạng: Dựa trên sự thay đổi của băng thông vào/ra theo thời gian, nhóm tính toán tốc độ mạng (network speed) và hiển thị trên dashboard Power BI để quản trị viên có thể theo dõi hiệu suất mạng.**

**- Phát hiện lỗi nghiêm trọng: Phân tích các thông số thu thập được để phát hiện các sự cố, ví dụ: nếu CPU usage vượt quá 90% hoặc một giao diện mạng bị down, hệ thống sẽ gửi cảnh báo qua email, push notification, hoặc Telegram.**

**Ưu và nhược điểm:**

**- Ưu điểm:**

**- SNMP là một giao thức chuẩn hóa, được hỗ trợ bởi hầu hết các thiết bị mạng, giúp dễ dàng tích hợp vào các hệ thống giám sát.**

**- Cung cấp khả năng thu thập thông tin chi tiết từ thiết bị, hỗ trợ cả giám sát và cấu hình.**

**- Hỗ trợ thông báo tự động (TRAP), giúp phát hiện sự cố nhanh chóng.**

**- Nhược điểm:**

**- Phiên bản SNMPv1 và SNMPv2c có bảo mật yếu, vì chỉ sử dụng community string (một dạng mật khẩu dạng plain text) để xác thực, dễ bị tấn công như sniffing hoặc giả mạo.**

**- SNMPv3 cải thiện bảo mật (hỗ trợ mã hóa và xác thực người dùng), nhưng cấu hình phức tạp hơn, đòi hỏi nhiều thời gian và kiến thức.**

**- Việc sử dụng UDP khiến SNMP không đảm bảo độ tin cậy, có thể mất dữ liệu trong môi trường mạng không ổn định.**

**---**

**2. ICMP (Internet Control Message Protocol)**

**Định nghĩa và lịch sử phát triển:**

**ICMP, hay Giao thức Thông điệp Kiểm soát Internet, là một giao thức thuộc tầng mạng (Network Layer) trong mô hình TCP/IP, được thiết kế để hỗ trợ các chức năng chẩn đoán và báo lỗi trong mạng. ICMP được chuẩn hóa lần đầu tiên vào năm 1981 qua RFC 792 và là một phần không thể thiếu của giao thức IP. ICMP không được sử dụng để truyền dữ liệu người dùng (như TCP hoặc UDP), mà chủ yếu phục vụ cho việc gửi các thông điệp kiểm tra và thông báo lỗi giữa các thiết bị trong mạng. Một ví dụ điển hình về ứng dụng của ICMP là lệnh `ping`, được sử dụng để kiểm tra khả năng kết nối giữa hai thiết bị.**

**Cấu trúc và cách hoạt động:**

**ICMP hoạt động dựa trên các gói tin (ICMP messages) được đóng gói trong các gói IP. Mỗi gói tin ICMP bao gồm một Type (loại thông điệp) và một Code (mã chi tiết) để xác định ý nghĩa của thông điệp. Một số loại thông điệp ICMP phổ biến bao gồm:**

**- Type 8 (Echo Request) và Type 0 (Echo Reply): Đây là cặp thông điệp được sử dụng trong lệnh `ping`. Echo Request được gửi từ một thiết bị để kiểm tra xem thiết bị đích có phản hồi hay không, và Echo Reply là phản hồi từ thiết bị đích nếu nó đang hoạt động.**

**- Type 3 (Destination Unreachable): Thông báo rằng không thể kết nối đến thiết bị đích, ví dụ: do địa chỉ IP không tồn tại hoặc bị chặn bởi tường lửa.**

**- Type 11 (Time Exceeded): Thông báo rằng gói tin đã hết thời gian sống (TTL - Time To Live), thường được sử dụng trong lệnh `traceroute` để xác định đường đi của gói tin.**

**- Type 5 (Redirect): Yêu cầu thiết bị gửi dữ liệu qua một đường dẫn khác để tối ưu hóa định tuyến.**

**ICMP không sử dụng cổng (port) như TCP/UDP, mà hoạt động trực tiếp trên giao thức IP. Khi một thiết bị gửi gói ICMP Echo Request (ví dụ: `ping 192.168.1.1`), thiết bị đích nếu đang hoạt động sẽ trả về gói ICMP Echo Reply. Nếu không nhận được phản hồi trong thời gian chờ (timeout), thiết bị đích được coi là không hoạt động (offline).**

**Ứng dụng trong thực tế:**

**ICMP được sử dụng rộng rãi trong các công cụ chẩn đoán mạng. Ví dụ:**

**- Lệnh `ping` giúp kiểm tra xem một máy chủ (như google.com) có đang hoạt động hay không, đồng thời đo độ trễ (latency) của kết nối.**

**- Lệnh `traceroute` (hoặc `tracert` trên Windows) sử dụng ICMP để xác định đường đi của gói tin từ nguồn đến đích, giúp phát hiện các điểm nghẽn trong mạng.**

**- Các hệ thống giám sát mạng dùng ICMP để kiểm tra trạng thái của thiết bị, đảm bảo rằng các máy chủ hoặc thiết bị quan trọng luôn sẵn sàng.**

**Ứng dụng trong dự án:**

**Trong dự án, ICMP được sử dụng để:**

**- Kiểm tra trạng thái online/offline: Hệ thống gửi gói ICMP Echo Request đến từng thiết bị trong mạng nội bộ (dải IP 192.168.1.0/24). Nếu nhận được Echo Reply, thiết bị được đánh dấu là "online"; nếu không, thiết bị được coi là "offline".**

**- Đếm số lượng thiết bị online/offline: Dựa trên kết quả kiểm tra trạng thái, hệ thống tính toán số lượng thiết bị đang hoạt động và không hoạt động, sau đó hiển thị trên dashboard Power BI dưới dạng thẻ (Card) để quản trị viên dễ dàng theo dõi tình trạng mạng.**

**- Hỗ trợ giám sát: Trước khi lấy thông số chi tiết từ thiết bị (bằng SNMP), hệ thống dùng ICMP để xác định xem thiết bị có đang hoạt động hay không, tránh lãng phí tài nguyên khi cố gắng lấy dữ liệu từ thiết bị offline.**

**Ưu và nhược điểm:**

**- Ưu điểm:**

**- ICMP là một giao thức đơn giản, dễ triển khai, và được hỗ trợ bởi hầu hết các thiết bị mạng, từ máy tính cá nhân đến router chuyên dụng.**

**- Cung cấp khả năng chẩn đoán nhanh chóng, giúp quản trị viên xác định trạng thái thiết bị mà không cần cấu hình phức tạp.**

**- Tiêu tốn ít tài nguyên, phù hợp cho việc kiểm tra trạng thái trong các hệ thống giám sát lớn.**

**- Nhược điểm:**

**- Một số thiết bị hoặc tường lửa có thể chặn ICMP (ví dụ: chặn lệnh `ping`) để tăng cường bảo mật, dẫn đến kết quả không chính xác (thiết bị có thể đang hoạt động nhưng bị đánh dấu là offline).**

**- ICMP chỉ cung cấp thông tin cơ bản (online/offline), không thể lấy được các thông số chi tiết như CPU usage hay băng thông.**

**- Dễ bị lạm dụng trong các cuộc tấn công mạng, ví dụ: tấn công DDoS bằng cách gửi hàng loạt gói ICMP (Ping Flood).**

**---**

**3. ARP (Address Resolution Protocol)**

**Định nghĩa và lịch sử phát triển:**

**ARP, hay Giao thức Phân giải Địa chỉ, là một giao thức thuộc tầng liên kết dữ liệu (Data Link Layer) trong mô hình TCP/IP, được thiết kế để ánh xạ địa chỉ IP (tầng mạng) sang địa chỉ MAC (tầng liên kết dữ liệu) trong cùng một mạng nội bộ (LAN). ARP được chuẩn hóa vào năm 1982 qua RFC 826 và là một phần quan trọng trong quá trình giao tiếp mạng, vì các thiết bị trong cùng một mạng nội bộ cần biết địa chỉ MAC của nhau để gửi dữ liệu trực tiếp qua Ethernet. ARP thường được sử dụng trong các mạng Ethernet, nhưng cũng có thể áp dụng cho các công nghệ mạng khác như Wi-Fi.**

**Cấu trúc và cách hoạt động:**

**ARP hoạt động dựa trên cơ chế yêu cầu và phản hồi:**

**- ARP Request: Khi một thiết bị (gọi là nguồn) muốn gửi dữ liệu đến một địa chỉ IP trong cùng mạng nội bộ nhưng chưa biết địa chỉ MAC tương ứng, nó sẽ gửi một gói ARP Request dạng broadcast (gửi đến tất cả thiết bị trong mạng). Gói ARP Request chứa địa chỉ IP đích và hỏi: "Thiết bị nào có địa chỉ IP này? Hãy cho tôi biết địa chỉ MAC của bạn."**

**- ARP Reply: Thiết bị có địa chỉ IP trùng với IP đích sẽ trả về một gói ARP Reply, cung cấp địa chỉ MAC của mình. Gói ARP Reply được gửi trực tiếp (unicast) đến thiết bị nguồn.**

**- ARP Cache: Sau khi nhận được ARP Reply, thiết bị nguồn lưu thông tin (IP-MAC mapping) vào bảng ARP cache để sử dụng cho các lần giao tiếp sau, giảm số lượng ARP Request cần gửi.**

**Ví dụ: Thiết bị A (IP: 192.168.1.2, MAC: AA:BB:CC:DD:EE:FF) muốn gửi dữ liệu đến thiết bị B (IP: 192.168.1.3). A không biết MAC của B, nên gửi ARP Request broadcast với nội dung: "Ai có IP 192.168.1.3?" Thiết bị B nhận được và trả về ARP Reply: "Tôi có IP 192.168.1.3, MAC của tôi là 11:22:33:44:55:66." A lưu thông tin này vào ARP cache và bắt đầu gửi dữ liệu đến B qua địa chỉ MAC 11:22:33:44:55:66.**

**Ứng dụng trong thực tế:**

**ARP là một giao thức nền tảng trong các mạng nội bộ, đảm bảo các thiết bị có thể giao tiếp với nhau qua Ethernet. Ngoài ra, ARP còn được sử dụng trong các công cụ quét mạng:**

**- Các phần mềm như Nmap hoặc Angry IP Scanner dùng ARP để phát hiện thiết bị trong mạng nội bộ, thu thập danh sách IP và MAC.**

**- ARP cũng được dùng trong các hệ thống phát hiện xâm nhập (IDS) để nhận diện các thiết bị mới hoặc không được phép trong mạng.**

**Ứng dụng trong dự án:**

**Trong dự án, ARP được sử dụng để:**

**- Quét mạng nội bộ: Hệ thống gửi ARP Request đến toàn bộ dải IP trong mạng (ví dụ: 192.168.1.0/24) để phát hiện tất cả thiết bị đang hoạt động. Kết quả trả về là danh sách các cặp IP-MAC, được lưu vào cơ sở dữ liệu SQLite để xử lý tiếp.**

**- Phát hiện kết nối trái phép: Hệ thống so sánh danh sách IP/MAC thu thập được với danh sách thiết bị được phép (được lưu sẵn). Nếu phát hiện một địa chỉ IP hoặc MAC mới không có trong danh sách, hệ thống sẽ đánh dấu đó là thiết bị lạ và gửi cảnh báo qua email, push notification, hoặc Telegram.**

**- Hỗ trợ giám sát: Danh sách thiết bị thu thập được từ ARP sẽ được sử dụng để kiểm tra trạng thái online/offline (bằng ICMP) và lấy thông số chi tiết (bằng SNMP), đảm bảo hệ thống có cái nhìn toàn diện về mạng nội bộ.**

**Ưu và nhược điểm:**

**- Ưu điểm:**

**- ARP là một giao thức đơn giản, không yêu cầu cấu hình phức tạp, và được hỗ trợ bởi tất cả các thiết bị trong mạng nội bộ.**

**- Hiệu quả trong việc phát hiện thiết bị, đặc biệt trong các mạng nhỏ (LAN), vì ARP Request broadcast đảm bảo tất cả thiết bị trong mạng đều nhận được yêu cầu.**

**- Tiêu tốn ít tài nguyên, phù hợp cho các hệ thống quét mạng nhẹ.**

**- Nhược điểm:**

**- ARP chỉ hoạt động trong cùng một mạng nội bộ (LAN), không thể quét thiết bị qua router (khác subnet). Để quét các mạng khác, cần sử dụng các giao thức khác như ICMP hoặc SNMP.**

**- ARP dễ bị tấn công bởi các kỹ thuật như ARP spoofing, trong đó kẻ tấn công giả mạo địa chỉ MAC để đánh lừa hệ thống, dẫn đến các vấn đề bảo mật như đánh cắp dữ liệu hoặc tấn công man-in-the-middle.**

**- ARP cache có thể bị lỗi nếu thiết bị thay đổi địa chỉ MAC (ví dụ: do thay card mạng), dẫn đến thông tin không chính xác.**

**---**

**4. Tổng hợp ứng dụng trong dự án và sự kết hợp giữa các giao thức**

**Sự kết hợp giữa SNMP, ICMP, và ARP:**

**Trong dự án "Phát triển hệ thống quản lý mạng nội bộ để giám sát, cảnh báo kết nối trái phép và phát hiện lỗi nghiêm trọng," ba giao thức SNMP, ICMP, và ARP được sử dụng kết hợp để xây dựng một hệ thống giám sát toàn diện:**

**- ARP: Được sử dụng ở bước đầu tiên để quét mạng nội bộ, thu thập danh sách các thiết bị đang hoạt động (IP và MAC). Danh sách này là cơ sở để hệ thống xác định các thiết bị cần giám sát và so sánh với danh sách thiết bị được phép để phát hiện kết nối trái phép.**

**- ICMP: Sau khi có danh sách thiết bị từ ARP, hệ thống dùng ICMP để kiểm tra trạng thái online/offline của từng thiết bị. Kết quả này được sử dụng để tính toán số lượng thiết bị đang hoạt động và không hoạt động, cung cấp thông tin tổng quan về mạng.**

**- SNMP: Với các thiết bị được xác định là online (qua ICMP), hệ thống dùng SNMP để lấy thông số chi tiết như CPU usage, memory usage, và băng thông. Các thông số này được phân tích để phát hiện lỗi nghiêm trọng (ví dụ: CPU usage vượt ngưỡng) và tính toán tốc độ mạng (dựa trên băng thông vào/ra).**

**Quy trình hoạt động của hệ thống:**

**1. Hệ thống quét mạng bằng ARP để thu thập danh sách thiết bị (IP, MAC).**

**2. So sánh danh sách này với danh sách thiết bị được phép để phát hiện thiết bị lạ. Nếu phát hiện thiết bị lạ, hệ thống lưu thông tin vào cơ sở dữ liệu và gửi cảnh báo qua email, push notification, hoặc Telegram.**

**3. Dùng ICMP để kiểm tra trạng thái online/offline của từng thiết bị, đếm số lượng thiết bị online/offline.**

**4. Với các thiết bị online, dùng SNMP để lấy thông số CPU, memory, băng thông, và tính tốc độ mạng.**

**5. Lưu tất cả dữ liệu (danh sách thiết bị, trạng thái, thông số, thiết bị lạ) vào cơ sở dữ liệu SQLite.**

**6. Power BI kết nối với SQLite để hiển thị dữ liệu dưới dạng dashboard, bao gồm: danh sách thiết bị, số lượng thiết bị online/offline, tốc độ mạng, và danh sách thiết bị lạ.**

**Lợi ích của sự kết hợp:**

**- Toàn diện: ARP cung cấp danh sách thiết bị, ICMP xác định trạng thái, và SNMP lấy thông số chi tiết, đảm bảo hệ thống có cái nhìn đầy đủ về mạng nội bộ.**

**- Hiệu quả: Việc kiểm tra trạng thái bằng ICMP trước khi lấy thông số bằng SNMP giúp tiết kiệm tài nguyên, tránh lãng phí khi cố gắng lấy dữ liệu từ thiết bị offline.**

**- Kịp thời: Phát hiện thiết bị lạ (ARP) và lỗi nghiêm trọng (SNMP) được thực hiện liên tục, với các cảnh báo được gửi ngay lập tức qua nhiều kênh (email, push, Telegram).**