Journal of Network and Information Security
9 (2) 2021, 09-13
http://www.publishingindia.com/jnis

Network Management Protocols: Analytical Study and Future Research Directions

Samman Tyata[1] and Ayad Barsoum[2*]
[1]St. Mary's University, San Antonio, TX, USA. Email: styata@mail.stmarytx.edu
[2]St. Mary's University, San Antonio, TX, USA. Email: abarsoum@stmarytx.edu
*Corresponding Author

Abstract: A computer network consists of many complex, interacting pieces of hardware and software. Network management is the process of administering, managing, and operating a computer network using a network management system. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security. In this paper, we summarize widely used network management protocols and provide an analytical study based on their architecture and concept. The paper highlights the advantages and disadvantages of different network management protocols. Moreover, we provide some directions for the future research of network management protocols in network automation, network assurance, and network analytics considering Internet of Things (IoT). This paper particularly focuses on two of the management protocols: Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). We describe the architecture of the protocols and their management components. We also study how SNMP can be implemented for monitoring IoT devices.

Keywords: Computer networks, Internet of Things (IoT), Network management, Network protocols.

I. Introduction

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure, or design [1, 11-15]. Network protocols take large-scale processes and break them down into small, specific tasks or functions to provide security, management, and smooth communication.

Network protocols help in the management by defining and describe the various procedures needed to effectively operate a computer network. These protocols affect various devices on a single network — including computers, routers and servers — to ensure each one, and the whole network perform optimally. Some of the widely used network protocols includes SNMP (Simple Network Management Protocol) and CMIP (Common Management Information Protocol). These protocols particularly revolve around the idea of:

- Maintaining stable connection between different devices connected to the same network.
- Identifying the errors affecting a network, evaluating the quality of network connection, and determining how issues can be tackled.
- Combining multiple network connections into a single link between two devices to increase strength and sustain the connection [2, 15].

II. SNMP - Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices [12-15]. It is a part of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite and was developed in the late 1980s to provide a general-purpose internetworking. Its primary goal was to be simple and efficient; however, its simplicity made it vulnerable to numerous other weaknesses as well.

SMTP provides management of Internet Protocol (IP) networks system using a hierarchical database to describe a system called a management information base (MIB) which holds the details about the device, performance, configuration, counters and any other data that give access to SNMP. Moreover, it is a client/server application which allows centralized management and monitoring of the networking requirements. To sum it up, it is one of the widely accepted network protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents must be enabled and configured to communicate with

the network monitoring tools or network management system (NMS) [3].

III. SNMP Architecture

SNMP has a simple architecture based on a client-server model and includes four layers:

- SNMP Network Managers - It is an application in NMS (Network Management Station) that asks for information from masters and displays that information using a GUI. A network can have multiple SNMP network managers.
- Master Agents - A master agent is a software that provides the interface between an SNMP network manager and a sub agent.
- Sub Agents - A subagent is a software program that provides information to a master agent.
- A managed component is hardware or software that provides a subagent. For example, database servers, operating systems, routers, and printers can be managed components if they provide subagents [4].

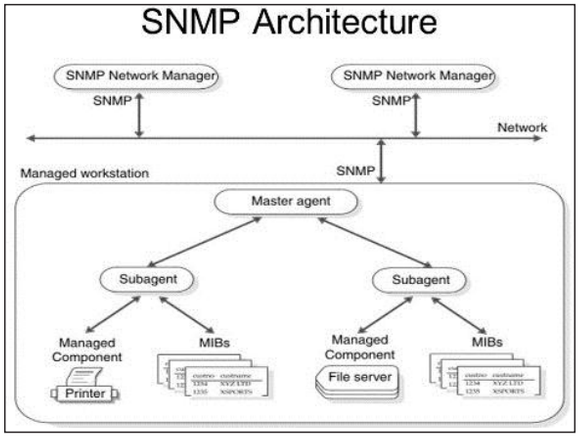

Fig. 1: SNMP Architecture

IV. SNMP Management Components

SNMP also makes the use of two other independent protocols MIB (Management Information Base) and SMI (Structure of Management Information) for effective management.

MIB - A Management Information Base (MIB) is a group of tables that specify the information that a subagent provides to a master agent. Each agent has its own MIB, which is a collection of all the objects that the manager can manage. The database is hierarchical, and each entry is addressed through an object identifier. It is basically categorized into eight groups: system, interface, address translation, IP, ICMP, TCP, UDP and EGP.

SMI - Structure of Management Information is a component used in network management to define the type of data that can be stored in an object and to encode the data for the transmission over a network. SMI is a subset of ASN.1 (Abstract Syntax Notation 1), which adopts an independent method for describing data and rules for transmitting the data [5].

SNMP Protocol - SNMP manager and SNMP agent communicate using the SNMP protocol. The five different types of messages are:

1. GetRequest: The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.
2. GetNextRequest: TheGetNextRequest message is sent from the manager to agent to retrieve the value of a variable. This type of message is used to retrieve the values of the entries in a table. If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. In such situations, GetNextRequest message is used to define an object.
3. GetResponse: The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This message contains the value of a variable requested by the manager.
4. SetRequest: The SetRequest message is sent from a manager to the agent to set a value in a variable.
5. Trap: The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting [6].

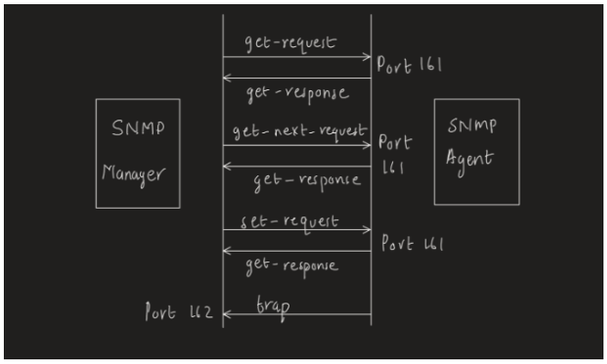

Fig. 2. UDP Connections in a SNMP Protocol

V. SNMP Versions

Three different versions of SNMP has been introduced so far.

- SNMPv1 - This is the first version and offers weak security features. Managers can easily athunticate to the agents without encryption when requesting information. Due to this, it is vulnerable to sniffing tool and can provide access to unauthorized devices. Unfortunately, this version is still in use as some networks has not been updated yet.

- SNMPv2c - This version offered some security enhancements over the first version. This version provided the remote monitoring (ROMN) capibility.
- SNMPv3 - This version started from SNMPv1 instead of SNMPv2c and offered various security enhancements over the previous 2 versions. This version makes the data encryption possible using hash based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version also allows the admins to specify various requirments for authentication and prevents unauthorized access [4].

SNMPv3 also introduces a security algorithm to be performed on the SNMP packes which are:

- noAuthNoPriv - This (no authentication, no privacy) security level uses community string for authentication and no encryption for privacy.
- authNopriv - This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.
- authPriv - This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses DES-56 algorithm [5].

To sum it up, the first version of the SNMP made a bad impression due to its vulnerabilities; however, the second and the third version solved these issues. All three versions are still in practise and provide up-to-date and secure way to monitor the network.

VI. Common Management Information Protocol (CMIP)

CMIP is an OSI (Open Systems Interconnection) model that defines how to create a common network management system. In network management and distributed systems protocols alone cannot provide communication. Therefore, the OSI proposes an object-oriented management model that provides the required standard resource descriptions. It was designed to be better than SNMP by overcoming theweaknesses of SNMP and thus, to become a greater and more comprehensive network manager. Within this network management environment, the agents are capable to initiate more communication between the manager, to define and communicate more complex traps to the manager and to support more devices [5].

While both CMIP and the SNMP define network management standards, CMIP is more complex. In fact, CMIP is only used by some telecommunications service providers for network management since the widespread availability was delayed because of the problems during its implementation. CMIP particularly centers around functions like:

- Monitoring the network usage, detect and fix the faults to tune the network for better performance.
- View and manage the system resources and management information.
- Authenticate users, detect intrusions, and transmit data securely.

The managed objects in the system consists of attributes, behaviors, actions, notifications, packages. These parameters are used by CIMP managers as point of reference while issuing request; moreover, it is based on a client/server model: the managing system is the client, the managed system the server.

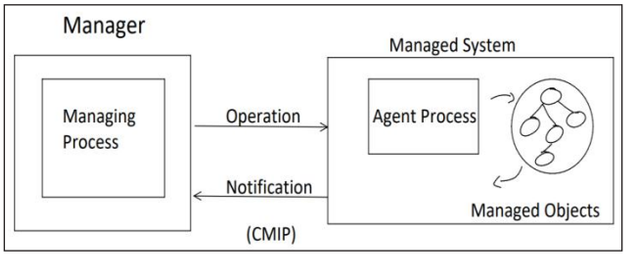

Fig. 3: CMIP Manager to Agent Request

Common Management Information Service Element (CMISE) works together with CMIP by transferring network management information from one system to another. (Scoggins, 416). CMIP then maps every CMISE operation to a remote (CMIP) operation [7].

For instance, let us say you wanted to set a terminal's IP address. In this case you would send out a CMISE service element, and it would call the CMIP operation m-set to set the terminal's information. In all cases, it is CMISE that summons CMIP to set (or get) the desired information. It is thus CMIP, and not CMISE, that releases the PDU's. On the receiving end, it is CMIP that translates the terminal's response and CMISE that reports this to the user [2].

VII. CMIP Protocol Service Elements

CMIP supports 11 service operations which are:

- M-ACTION - requests an object to perform an action of some sort.
- M-CANCEL-GET - cancels the previous M-GET command.
- M-CREATE - creates specified objects.
- M-DELETE - deletes specified objects.
- M-EVENT-REPORT - when an event occurs, allows network agents to announce it.
- M-GET - reads value of an object from MIB and directs the agent to return attribute values from managed objects.

- M-SET - adds, removes, or replaces specified objects.
- M-EVENTREPORT-CONFIRMED - when EventReport needs a confirmation.
- M-SET-CONFIRMED - when the set needs a response.
- M-ACTION-CONFIRMED - when action needs response.
- M-LINKED-REPLY - works in conjunction with M-Get, M-Set, M-Delete, M-Action, for multiple requests [8].

The protocol can manage a large number of agents, which are capable of processing information before they pass it back to the management system. Furthermore, the object-orientation allows sharing and grouping resources in particular classes and subclasses. Inheritance and relationships between specifications of classes make it an efficient management system.

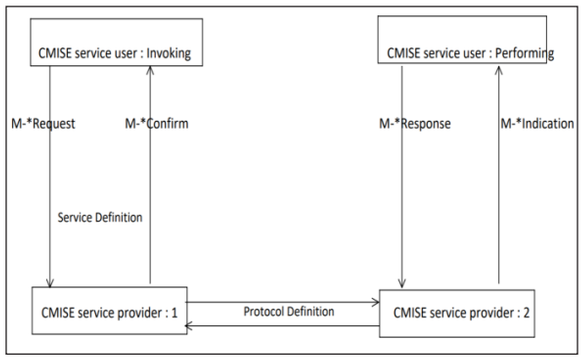

Fig. 5: CIMP Protocol

Table I highlights the main differences between SNMP and CIMP.

TABLE I

	SNMP	CMIP
Architecture	Simple architecture based on a client-server model	More complex
Security	• SNMPv1: weak security • SNMPv2c: some security enhancements • SNMPv3: various security enhancements	Safer system as it has built in security that supports authorization, access control, and security logs.
Components	Master Agents, Sub Agents, and Managed Components	Manager and managed systems

VIII. Use of SNMP for Monitoring IOT

The Internet of Things (IoT) is a network of interconnected, internet-connected devices that can capture and transmit data without the need for human interaction over a wireless network. IoT can mean different things to different people, but few can argue that to fully realize the potential of a smart world based on IoT, one must be able to fully track and monitor all the things that make IoT possible.

Depending upon the support for SNMP, we can divide the IOT devices we want to monitor into three different categories. The first category revolves around the devices that support SNMP and provide needed monitoring data. Second category concerns the devices that support SNMP but do not share needed data directly. Lastly, the third category do not support the SNMP. Simply put, second and third categories make it harder to monitor devices as the required data is not shared directly.

The first group particularly centers around the devices providing network connectivity as they are designed to be remotely managed and monitored by SNMP. Some other examples are physical infrastructures in the cloud environment. The security provided by the 1st and 2nd version of SNMP and reachability issues - like VPN and NAT - are some of the problems; however, this can be solved by using SNMP proxy services.

Generally, there are 4 principal ways to gather data from devices that do not provide them in a suitable form for monitoring:

- Devices that support messaging or event notifications allow us to subscribe to relevant topics and queues or implement listeners and receive the data as generated by the device. This is the best approach as all the data is current and the required resources are minimal, but it is limited by the support of the monitored device.
- Polling (predefined intervals) is a simple, robust and enables us to estimate needed resources in advance. Down sides are possible monitoring of devices that are not required, risk of stale data or higher resource consumption if polling more frequently.
- Proxying data collection as requests is made. It provides minimal resource usage as we are collects only the data needed when it is requested. However, it introduces unknown response delay in the system, as we have to wait for all required devices to respond. This makes estimates about resource usage difficult as we are dealing with random requests (example would be large number of clients) and makes aggregate data calculations almost impossible.
- Proxying with caching extends previous approach by introducing a proxy level cache that can reduce system load at the price of not returning current data to all requests and significantly increasing the complexity of the system.

The methods described can be combined in a variety of ways to produce a hybrid solution that is tailored to one's particular needs, but at the cost of adding to the already high degree of complexity.

Only the 1st of the 4 methods for monitoring devices in an IoT environment allows for meaningful handling and notification generation. In the case of polling, the remaining three methods would either impose a substantial delay or could completely miss the event if there were no requests to track the system. To sum it up, we can process and react to events with minimal delay if a system supports messaging or can produce SNMP alerts [9].

IX. Conclusion: SNMP vs CIMP

The way it stands today, TCP/IP and its network management protocol SNMP are in widespread use today. They have almost total control of the inter-network communication protocol market. With these facts, many people consider using SNMP over CIMP. Moreover, the major advantage of using SNMP is its simplistic design. It is easy to implement on a network since it does not require a long configuration. Moreover, it is easy to update the protocol to meet the needs of future users. It also supports peer to peer topology as the manager talks directly to the agent making the response quicker.

One of the major drawbacks of the SNMP is its security and unreliability. When the data transfer takes place, the only way to check for the authority of the machines involved is by means of a community name string. Once outsiders know the name, it is easy for them to issue the set/get commands maliciously, and gain control of the network. Furthermore, the use of UDP protocol for transferring data makes the SNMP packets vulnerable to being lost, corrupted, deleted, duplicated, or delayed.

CIMP does have several advantages as well: First, it was funded by governments and large corporations. Second, CMIP is superior to SNMP for it can provide greater control over a network. For instance, its security and notification services equal or surpass those available in SNMPv2. The object-orientation gives designers and developers the ability to think of resources in an abstract way which unlocks a lot of powerful capabilities that allow for efficient network management.

References

[1] M. Subramanian et al., *Network Management: Principles and Practices*. Prentice Hall, 2012, [Online]. Available: www.amazon.com/Network-Management-Principles-Mani-Subramanian/dp/0201357429.

[2] A. Leinwand, and K. F. Conroy, *Network Management: A Practical Perspective*. Addison-Wesley, 2001.

[3] T. Kramer, *Network Management Protocols and Tools Study*. Germany, GRIN Publishing, 2002.

[4] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Addison-Wesley, 2009.

[5] S. Feit, *SNMP: A Guide to Network Management*. McGraw-Hill, 1995.

[6] Network Management Protocols and Features > Structuring and Modularizing the Network with Cisco Enterprise Architecture. Cisco Press. [Online]. Available: www.ciscopress.com/articles/article.asp?p=1073230&seqNum=4

[7] S. Scoggins, and A. Tang, *Open Networking with OSI*. Prentice-Hall: Toronto, 1992.

[8] H. Zottmann, *CMIP/CMIS - Object Oriented Network Management*, Aug. 18, 2000. [Online]. Available: www.cellsoft.de/telecom/cmip.htm

[9] M. Savić, "Bridging the SNMP gap: Simple network monitoring the internet of things," *Facta Universitatis Series: Electronics and Energetics*, vol. 29, no. 3, pp. 475-487, 2016, doi: 10.2298/FUEE1603475S.

[10] K. Amirthalingam, and R. Moorhead, "SNMP - An overview of its merits and demerits," *Proceedings of the Twenty-Seventh Southeastern Symposium on System Theory*, 1995, pp. 180-183, doi: 10.1109/SSST.1995.390588.

[11] A. Ben-Artzi, A. Chandna, and U. Warrier, "Network management of TCP/IP networks: Present and future," *IEEE Network*, vol. 4, no. 4, pp. 35-43, 1990.

[12] K. McCloghrie, and M. Rose, "Management information base for network management of TCP/IP-based internets," RFC 1156, Hughes LAN Systems, Performance Systems International, 1990.

[13] C. Hare, *Simple Network Management Protocol (SNMP)*. 2011.

[14] A. King, and R. Hunt, "Protocols and architecture for managing TCP/IP network infrastructures," *Computer Communications*, vol. 23, no. 16, pp. 1558-1572, 2000.

[15] X. Du, M. Shayman, and M. Rozenblit, "Implementation and performance analysis of SNMP on a TLS/TCP base," in *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470)*, pp. 453-466, IEEE, May 2001.