International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Comprehensive Survey on Network Management System (NMS) by CISCO

Mrityunjaya D. Hatagundi[1], Amruta Navadagi[2], H. V. Kumaraswamy[3]
[1,2]*PG Student, Department of Telecommunication Engineering, RVCE, Bengaluru, India*
[3]*Professor, Department of Telecommunication Engineering, RVCE, Bengaluru, India*

***Abstract*: Network management system (NMS) is important both in ensuring the correct operation of network devices and in maintaining the services that run on them. However, the relentless growth of DSL's users, meaning that IP traffic volumes nearly double every two years, renders real-time monitoring and analysis of every customer's service parameter is a very challenging problem. The most important problem is the bottleneck in centralized NMS which most of services provider use as SNMP-based system. This paper presents a new model which will be able to ease the problem from bandwidth consumption of SNMP-based by two main methods. Firstly, to ease the problem from bandwidth consumption of SNMP-based, this model will use the probabilistic data structure to decrease the number of packets of monitoring network device's parameter. Secondly, to ease the problem from the relentless growth of the number of the network's devices, this model is designed to support distributed network devices' operations in a distributed NMS fashion. Meaning that, the number of NMS's devices can be increased with the number of network's devices if it is necessary. By using both of two methods, customer expectations with bandwidth requirements and reliability requirements can be improved with this model.**

***Keywords*: Network Management System; Probabilistic Data Structure Distributed; Network Services Provider; Bloom Filter; SNMP Protocol.**

1. Introduction

Networks and distributed processing systems are of critical and growing importance in enterprises of all sorts. The trend is toward larger, more complex networks supporting more applications and more users. A large network cannot be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools. The urgency of the need for such tools is increased, and the difficulty of supplying such tools is also increased, if the network includes equipment from multiple vendors. Moreover, the increasing decentralization of network services as exemplified by the increasing importance of workstations and client/server computing makes coherent and coordinated network management increasingly difficult. In such complex information systems, many significant network assets are dispersed far from network management personnel. For either LAN management alone, or for a combined LAN/WAN environment, what is needed is a network management system that includes a comprehensive set of data gathering and control tools and that is integrated with the network hardware and software. We look at the general architecture of a network management system and then examine the most widely used standardized software package for supporting network management: SNMP.

Cloud services prove as a great support to these digitized trends. Earlier these services were only within the reach of established organizations but now small and medium scale companies are also able to access advanced IT services in a rapid and cost effective manner. The network operations are required to become more dynamic in nature and generate more events and data for increasing number of users and applications and thus making them complex. The evolution of the digitization embracing mobile, cloud, Internet of Things (IoT), etc is posing challenges to the enterprise network architectures. The world is moving towards the era of digitization. The acceptance of these digitized technologies could impact the same way as that of Internet and World Wide Web (www) did 20 years ago. To make these digitized applications competitive enough in businesses/enterprises, big data and analytics have been introduced. Big data and analytics provide better real time decision making, automation and efficiencies required to deliver such digitized applications.

Fig. 1. Overview of DNA

Nothing comes without risks and this can be applied to the evolution towards a dynamic, ubiquitous digitalized business [1]. Destructive security risks are associated with provision of universal connectivity. For better management and operation, network issues are to be addressed. All these digitized trends direct towards the need for a significant new architecture for enterprises. Cisco's Digital Network Architecture (DNA) is a network architecture that acts as a blueprint for the digital

organization. This architecture is built to facilitate fast and flexible network services that support digitalized business processes. Cisco's DNA centres on a network infrastructure that is not only fully programmable and open to third–party innovation, but can also fully and seamlessly integrates the cloud as an infrastructure component [1].

The Cisco's DNA controller facilitates simple, automated, and programmatic deployment of network services. It brings the notion of user–and application–aware policies into the foreground of network operations. With DNA, the network can provide continuous feedback to simplify and optimize network operations and to support digitalized applications to become inherently network–aware. It is a move towards Software Defined Networking (SDN) has taken up by Cisco. DNA would comprise of data centre, cloud and IoT infrastructures encompassing the traditional high availability, scalability and performance characteristics as shown in figure 1.

2. Technical background

One of the core Internet protocols in network management and administration, ICMP is used to send error messages. ICMP is a control protocol, meaning that it does not carry application data, but rather information about the status of the network itself. There are many commonly used network utilities based on ICMP messages that will help detect errors in the underlying communications of network applications; availability (up/down status) of remote hosts; network congestion; and latency. One of the common ICMP utilities, Ping sends ICMP echo request packets and tests the reachability or availability of a device or host on a network.

Ping also measures the round-trip time for messages sent between the originating host and the destination. Ping is lightweight (small packets = fast results), low level (Typically handled by the NIC), very flexible, and has a near zero impact on the network. Although the result from a ping command provides information about a network route's latency, this information is exceptionally coarse in its granularity. Latency as defined by a ping response represents little more than the amount of time that occurred between sending the ping request and receiving its reply. As such, its response illuminates little about the actual route taken and behaviours seen through its journey from source to target. A ping response will also report on the number of hops required to complete the travel from source to destination as well as information about the connection's packet loss. Although the specifics of a problem are left to other more granular protocols, this simple command provides a very easy way to gauge a connection's health at the highest level [5]. SNMP goes beyond ICMP's very simple and highly-structured information to enable the gathering of virtually any kind of data from a network device. Due to SNMP's long history and widespread use, virtually every network device—and even many servers and applications—have been made SNMP-aware. "Awareness" in this context means that the device is configured to receive and respond to SNMP requests from a central Network Management Solution (NMS).

SNMP works by polling the MIB (Management Information Base) of an SNMP enabled device to obtain information stored on the target device. An SNMP trap allows a network device to notify a network management system (NMS) [6] of an event through an SNMP message. SNMP traps differ from SNMP queries in that the device initiates the trap while the query is initiated by the NMS.

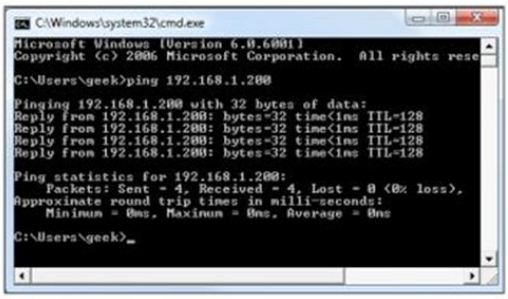

Fig. 2. PING Results

The present network management system, which is based on simple network management protocol (SNMP), comes along with central management approach and lacks of reliability and scalability. It cannot adapt to the new self-organizing network. In addition, relaying monitoring data consumes bandwidth, delays its availability, and might be lost in case of a network failure. Self-organization, however, might be highly helpful on implementing novel distributed network management and control concepts. Furthermore, on the basis of the exact traffic identification, flexible strategies might be introduced to achieve reasonable and effective accounting to provide users with the proper incentives to ensure a desirable allocation of network [3].

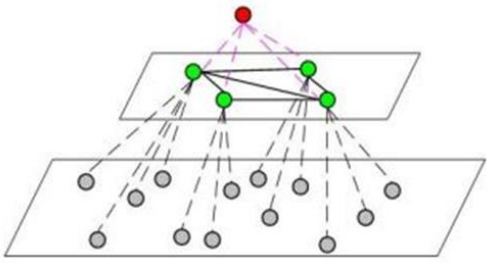

Fig. 3. Self-organizing network [8]

As the core unit of the system, DNA is equipped with modules of monitoring, communication, caching, local MIB and interfaces as shown in Figure 4. The individual DNAs build and maintain a self-organization overlay network. The main purpose of the overlay is to keep DNAs connected in one logical network and enable a single DNA to find another DNA in reasonable time and end-users to communicate with each other independent of their heterogeneous networks and devices. The DNA Controller acts as the central module responsible for

communicating with the NM server and user as well as passing the requests and corresponding parameters [4] by the interfaces respectively. DNA controller also runs for delivering the related queries to functional modules by the function interface to trigger the related monitoring modules, which deal with the arriving packets according to the preset strategies and store the results to local Management Information Database (MIB) [2].

The user can configure the monitoring modules to satisfy his requirements, and the NM server can retrieve the statistic information by collecting from DNAs regularly or requesting when needed. Caching module aims at shortening the response time of queries to decrease search delay. But the consistency problem should be taken into account, and cached data should be refreshed in time. Local MIB [13] is used for storing the analysed and filtered network management data, NM strategies and relevant data from the other peer DNAs [5]. MIB data are shared by communication module. In order to exchange or transfer the messages, it is necessary to change MIB's data format to XML, which is the most prevalent standard data format independent of the language and platform. Thus it facilitates the information transfer and share between the DNA peers and addresses the issue of data sharing between the multiple management agents in the distributed NM.

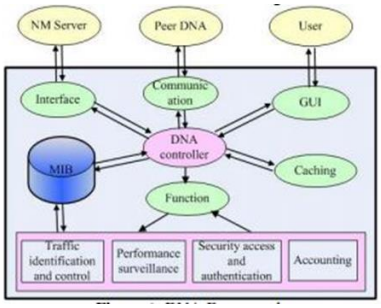

Fig. 4. DNA Framework

3. Network management architectural model (hierarchical approach)

Layering of network management not only allows NMS systems to communicate better, it reduces the amount of alerts seen by network operations support staff. At the lowest layer, it is nearly impossible to keep up with events displayed from each network element reported in the NMS architecture. For example, it is not feasible to have someone watching every syslog event that occurs on the network. Instead, you rely on systems at the Network Management Layer (NML) to filter through all events and show only those events deemed as most important. The Service Management Layer (SML), [15] meanwhile, is used to further summarize events from the NML and tie multiple network management systems together. A good NMS system will also provide deduplication of these network events in order to further reduce the amount of unnecessary messages seen by operations personnel. The hierarchical model in Figure 5 shows the major components that make up a comprehensive NMS system and provides a high-level integration scenario. Cisco Advanced Services encourages the adoption of a layered, hierarchical network management system. This type of architecture involves data flow and integration of multiple NMS tools to be effective. Figure 1 depicts those tool and data relationships. The underlying hierarchical philosophy is to get the organization to a basic level of integrated network management. The foundation for this architecture comes from the Telecommunications Management Network (TMN) (M.3000) model. "TMN provides a framework for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks. To achieve this, TMN defines a set of interface points for elements which perform the actual communications processing (such as a call processing switch) to be accessed by elements, such as management workstations, to monitor and control them. The standard interface allows elements from different manufacturers to be incorporated into a network under a single management control.

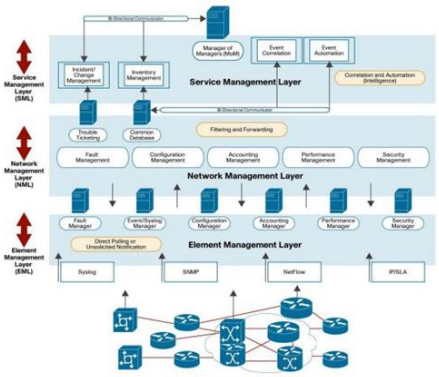

Fig. 5. Hierarchical model

The first level, the Element Management Layer, defines individual network elements used in deployment. In defining this layer, for each anomaly that occurs in the network, potentially multiple devices can be affected by the event and can independently alert network management systems that an event has occurred resulting in multiple instances of the same problem.

In the middle of the diagram is the Network Management Layer. This function takes input from multiple elements (which in reality might be different applications), correlates the information received from the various sources (also referred to as root-cause analysis), and identifies the event that has occurred [16]. The NML provides a level of abstraction above the Element Management Layer in that operations personnel are not "weeding" through potentially hundreds of Unreachable or Node Down alerts but instead are focusing on the actual event such as, "an area-border rou" At the top of the diagram is the Service Management Layer. This layer is responsible for adding intelligence and automation to filtered events, event correlation, and communication between databases and incident management systems. The goal is to move traditional network management environments and the operations personnel from

element management (managing individual alerts) to network management (managing network events) to service management (managing identified problems) [17].

4. Conclusion

The DNA controller centralizes the network control plane of the infrastructure and plays a critical role in automating its operations. It configures policies that govern network access and transport to instantiate the intent of the network services delivered to business applications. Analytics and telemetry offer the feedback mechanisms to support network–enabled applications, providing real–time data to application developers for continuous improvement cycles. The cloud becomes an integral part of the Cisco DNA infrastructure. Network operators are empowered to run applications where it makes sense from a business perspective. They can take full advantage of cloud infrastructure to operate the DNA, or to offer advanced analytics services. Based on these building blocks, Cisco Digital Network Architecture delivers a flexible and innovative environment to deliver transport, security, and digital network services. The architecture consists of several main building blocks. Transport fabrics connect users, applications, and things seamlessly to greatly simplify network operations. Virtualization in DNA allows for the decoupling of network or transport functions from the underlying hardware elements, and offers the flexibility and speed required to instantiate services in the network. Enterprise networks are evolving rapidly to support the requirements arising from digitalizing business processes. The Cisco Digital Network Architecture provides the network infrastructure to support this evolution.

Since most of services providers use SNMP to be the main tool for management their network devices. But IP traffic volumes nearly double every two years, renders real-time monitoring and analysis of every network devices parameter is a very challenging problem. Firstly, bandwidth consumption of SNMP directly depends on the number of monitored parameters. Moreover, generally the number of monitored parameters of services provider is more than ten times of the number of monitored parameter of an enterprise. So, it is not possible to use only a single SNMP system to manage all of provider's network devices. In order to manage a large network, provider needs to separate a large network into a smaller network. But it still takes a lot of bandwidth consumption for monitoring a large number of network devices by only using the SNMP-based.

References

[1] "The Cisco Digital Network Architecture Vision –An Overview", White Paper, pp. 16-20, Cisco, 2017.
[2] Danda B. Rawat, Swetha R. Reddy, "Software Defined Networking Architecture, Security and Energy Efficiency: A Survey", IEEE Communications Surveys & Tutorials, volume 19, no. 1, First Quarter 2017, pp. 13-16, 2017.
[3] Sandra Scott-Hayward, Sriram Natarajan, Sakir Sezer, "A Survey of Security in Software Defined Networks", IEEE Communication Surveys & Tutorials, volume 18, no. 1, First Quarter 2016, pp. 3-5, 2016.
[4] Nishtha, Manu Sood, "A Survey on Issues of Concern in Software Defined Networks", 2015 Third International Conference on Image Infonnation Processing, pp. 2-5, 2015.
[5] Wenfeng Xia, Yonggang Wen, Chuan Heng Foh, Dusit Niyato, Haiyong Xie, "A Survey on Software-Defined Networking", IEEE Communications Surveys & Tutorials, pp. 22-27, 2013.
[6] Fei Hu, Qi Hao, Ke Bao, "A Survey on Software-Defined Network (SDN) and OpenFlow: From Concept to Implementation", IEEE Communications Surveys & Tutorials, pp. 16-19, 2013.
[7] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, Andrei Gurtov, "Security in Software Defined Networks: A Survey", IEEE Communications Surveys & Tutorials, pp. 11-23, 2015.
[8] Diego Kreutz, Fernando M. V. Ramos, "Software-Defined Networking: A Comprehensive Survey", in Proceedings of the IEEE, volume 103, no. 1, pp. 31-38, January 2015.
[9] Tao Chen, Marja Matinmikko, Xianfu Chen, Xuan Zhou, Petri Ahokangas, "Software Defined Mobile Networks: Concept, Survey, and Research Directions", IEEE Communications Magazine, pp. 6-8, November 2015.
[10] Yong Li, Min Chen, "Software-Defined Network Function Virtualization: A Survey", IEEE Access, volume 3, pp. 2-5, 2015.
[11] Deepthi Gopi, Samuel Cheng and Robert Huck, "Comparative Analysis of SDN and Conventional Networks using Routing Protocols", IEEE Access, pp. 8-18, 2017.
[12] Bruno Nunes Astuto, Marc Mendonica, Xuan Nam Nguyen, Katia Obraczka, Thierry Turletti, "A Survey of Software Defined Networking: Past, Present, and Future of Programmable Networks", IEEE Communications Society, pp. 1617-1634, 2014.
[13] P. Goransson and C. Black, "Software Defined Networks: A Comprehensive Approach" Elsevier, 2014.
[14] N. McKeown, "Software-defined networking," INFOCOM Keynote Talk, volume 17, no. 2, pp. 30–32, 2009.
[15] T. Xing, Z. Xiong, D. Huang, and D. Medhi, "SDNIPS: Enabling software-defined networking based intrusion prevention system in clouds," in Proceedings 10th Int. Conf. Network Service Management (CNSM), pp. 308–311, Rio de Janeiro, Brazil, 2014.
[16] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in Recent Advances in Intrusion Detection, pp. 161–180, Heidelberg, Germany: Springer, 2011.
[17] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in Proceedings of IEEE SDN Future Network Services (SDN4FNS), pp. 1–7, Trento, Italy, 2013.
[18] D. B. Rawat and C. Bajracharya, "Software defined networking for reducing energy consumption and carbon emission," in Proceedings of IEEE Southeast Conference, pp. 1–2, Norfolk, VA, USA, 2016.