Analysis on Different Approaches of Network Configuration Management System

Basundhara Dey, University Of Central Florida, PID b3661281

Abstract- *Network Configuration Management (NCM) is the procedure of arranging and keeping up data about every one of the parts of a Computer Network. It is not just a day by day and crucial necessity in Computer Network frameworks however it likewise structures a portion of a boundless field of innovative work. Numerous operational issues confronting system directors today come about because of an absence of configuration management capabilities.*

While trying to comprehend existing frameworks set up and flow innovative work identifying with Network Configuration Management, studies identifying with comparative applications have been did and ideas have been dismembered to assess their conceivable commitments into the improvement of a Network Configuration Management System. With the fast advancement of Artificial Neural Network (ANN), wise substances are additionally created to bolster the basic appropriation of Network Configuration Management System.

In the flow of this paper, we will go through evolution of network configuration management system to understand the key factors and peer review of some referenced prototype. We will discuss some of the integrated and intelligent network management modules introduced till date, i.e., Web Based, CMDB, and CAMM. The paper can be further extended to address network monitoring tool and Network fault management system for advanced discussion on Network management System.

Index Terms - CMDB (Configuration Management Database), Network Management, Network Performance, CAMM, Network Monitor, We-based network configuration, MIB, SNMP

I. INTRODUCTION

Computer systems always in need of configuration. Whether it is first time using your brand new computer/laptop or while you setting up a network system at home/office. To provide better network services, the more complex network devices and technologies evolve, network configuration become more critical to manage. To monitor such complex network, researchers need to keep inventing more reliable and intelligent network management system for continuous monitoring.

Network management is a large area classified into five different functional fields, i.e. Configuration management, Accounting management, Performance management, Fault management and Security management. As OSI defined the functionality of network configuration management, it should be able to collect any data from any supervised object under its control and can pass on the collected information to its respected network manager. In simple words, network configuration management should be able to modify the configuration of any attached network resource to it i.e. Can add or remove attached network devices in any network; initiate, close down or restart any network resource. It should also has the ability to check on The MIB (Management information system) stored in the controlled network resource and help the associate network manager to manage the “enterprise network”.

Due to the rapid grow of modern communication system, Network configuration management has become a great preoccupation now a days for network providers as well as to users. Due to continuous changes in the field of computer network, the approaches to configure the network management system in more secure and reliable

way keep on evolving. Over the year, Network Managers' responsibility have moved from troubling and monotonous monitoring and configuring to less human-more automate mediation for configuration and monitoring. So, in the scope of this paper, I have discussed over conventional approach to recent automated approach for Network configuration management system.

For the conventional one, this paper has analyzed a Wed-based network management (WebNM) model that uses the World Wide Web (WWW) technologies to manage network systems with the benefit of platform-independence, uniform management interface and reduced costs [1]. The lead of this model is the network admin can monitor the network at any preferred check point of the network system.

In next phase, this paper discussed on a better version of more automated and intelligent network management workflow (system) that functions with collecting a large data set and produce meaningful information by filtering, aggregating and visualizing the data and make it handy to network users [2]. In order to discuss, I present a configuration management database (CMDB) and prototype of configuration management system (CMS) developed in the referenced paper. This can be generalized as a semi-automated approach.

For the elevation of scope in work area for Network Managers, the complexity of higher level interaction with network components are mostly handled by Artificial Intelligence (AI) now a days. In implementation of AI, there are two kind of classification of techniques can be seen: expert systems and neural networks. When the problems in network configuration is dealing with "knowledge-based" and "rule-based" – expert system is widely accepted over there to create an automated, intelligent network management system. But when problem revels in application level, it becomes very hard to define any well-structured model for any significant part of the problem. This leads to neural network to solve issues in such a complex domain. So when there is network that has links and communications between its components such as the biological neuron system, it is then called "artificial neural network" To analyze this technique, this paper use the reference of the Connectionist Associative memory model (CAMM) that is used to analyze corrupted network management information as it uses simple set operations leading to minimal computation and furthermore it is memory efficient due to its self-organizing and dynamic structure [3].

This paper analyze the evolution of the techniques with some referenced prototypes [1] [2] [3]. With the inspection result, the paper pulls out the some still existing loopholes and further advancement suggestion.

For future scope, this paper ca be extended to infer few more intelligent techniques to apply in different network management, i.e. Network monitoring, Network Fault management etc.

II. NETWORK MANAGEMENT SYSTEM

Before going into any details of different approaches, first let's have an idea about basic network management system and key terms.

A. What is Network management System?

"A virtual management system for a network facility, such as a data center, or any facility having a plurality of components which can be organized as objects for presentation in a virtualized environment, is disclosed. The system includes a management topology presenting devices, facilities, subscribers, log servers, and services as objects to an administrative interface; and a configuration manager implementing changes to objects in the topology responsive to configuration input from an administrator via the administrative interface. [4]"

The network management model declared by International Organization for Standardization (ISO) has five functional areas of network management which are listed below:

- *Fault Management* – component responsible to detect, isolate and resolve problems in network.
- *Configuration Management* – component responsible for configuring file, software, inventory management.
- *Performance Management* – component responsible to monitor and measure the overall

performance of network and detect any poor performance issue/cause.

- *Security Management* - component responsible for providing access to authorized resources and devices in the network.
- *Accounting Management* – component responsible to provide Utilization data of system assets.

Now when two network devices are communicating, there should have been some protocol present. The interesting fact about Network management protocols is, they work parallel with those protocol that helps to transfer data and application access.

The two fundamental protocols of network management are Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP). ICMP mostly known as 'ping' command; ensure the network connectivity by creating a low level request between to network endpoint. For his paper, we will mostly concentrate on SNMP.

B. 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. It is a part of Transmission Control Protocol / Internet Protocol (TCP/IP) protocol suite. [6]"

SNMP mostly been used when a single network management system (NMS) is accessing a large heterogeneous network. There are three components of this protocol-

- Managed devices or network elements
- SNMP agents - software/footprint packaged inside of the above devices
- NMS (Network Management Station) - a centralized system that manages all the network elements throughout the network.

Fig. 1[7] represents the basic principle of SNMP communication with all its elements shown.

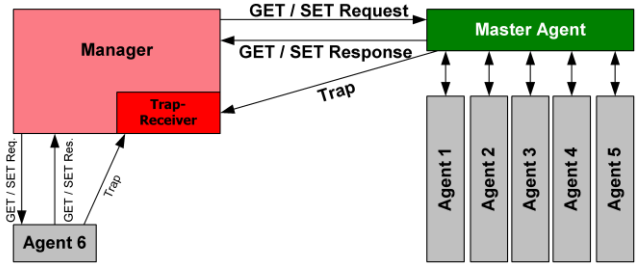

Fig. 1. Principle of SNMP Communication [7]

C. MIB (Management Information database or Management Information Base):

It is a database of Object identifiers of the network elements. NMS use this database to communicate with all the managed devices resides within the network through SNMP. Every SNMP agent should have a MIB that matches the Network Station's MIB.

Typically these MIB contains standard plan of accurate and control qualities portrayed for hardware center points on a framework. SNMP furthermore allows the growth of these standard qualities with qualities specific to a particular pros through the usage of private MIBs.

D. Object Identifier (OID):

Now we know MIB is a set of data that manages the network element. Each MIB is made of unique Object Identifiers (OID). Managed device return information based on which OID the MNS has requested for.

MIB has a hierarchical organization for OIDs, with individual variable identifier.

Now as we are well aware of the basic terminology use in Network Management, we can move forward to discuss about Network Configuration Management and different approaches, from generic to intelligent level.

III. NETWORK CONFIGURATION MANAGEMENT

Configuration management is the inventory collection of device software and hardware and also it is responsible to manage, detect configuration change and implement the changed configuration for device software and hardware.

For this paper, I have examined several different research works and publications and have seen that there are numerous different approaches to

overcome the shortcomings and strengthen the configuration management system. With time, Data Networks grow in size and complexity and give more challenges to network management. Also, with the modernization of science, manual monitoring and troubleshooting over network management with conventional approach almost become impossible. To cop up with the rapid blooming of intuitive networks, intelligent automation start to invade in network management.

To show the transition of approaches with time, this paper has chosen three techniques, starting with mainstream practice, going through semi-automated means and ending with intelligent practice. Below are the basic names of the approaches-

A. Web-based Network Configuration Management system [1]

B. Using CMDB (Configuration Management Database) [2]

C. Using Artificial Neural Network [3]

IV. WEB-BASED NETWORK CONFIGURATION MANAGEMENT SYSTEM

Web-based network Configuration management system (WebNCMS) gives the advantage to remotely manage the entire network through the web browser. It uses HTTP to transfer management information among network objects and managers.

A. Functional Overview:

The main functionality of proposed WebNCMS includes:

- Manage network remotely (i.e. start, restart, shutdown, monitor, reconfigure)
- Retrieve the status report of network

Fig. 2 [1] shows the structure of general functionality of the proposed module.

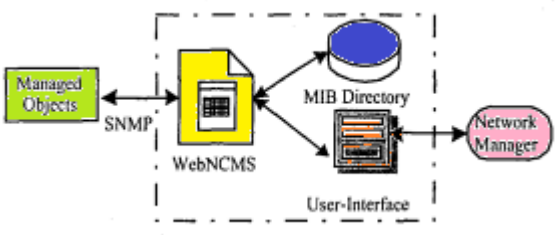

Fig. 2. General Functionality of WebNCMS [1]

WebNCMS basically load and capture configuration information of all Managed Objects in the network into the MIB. Using the WebNCMS, network managers can manage the configuration of network devices from any location using the web browser.

B. Architectural Overview:

In the architecture level of this module, it comprises of three layers (from below to top):

1) NECMS (Network Element Configuration Management System) – responsible to carry forward the detailed information about managed object to the upper layer.

2) NDCMS (Network Domain Configuration Management System) – responsible to manage a network domain configuration and provide information to the enterprise network about it.

3) ENCMS (Enterprise Network Configuration Management System) – after cumulate all the NDCM's information, responsible to provide the network manager a service access point.

C. Management System Overview:

Through the layers of the architecture have different architecture, they have the same management system in order to prove better software quality, flexibility in the model and reduce development time.

Fig. 3 [1] shows the structure of general model of the Management system.

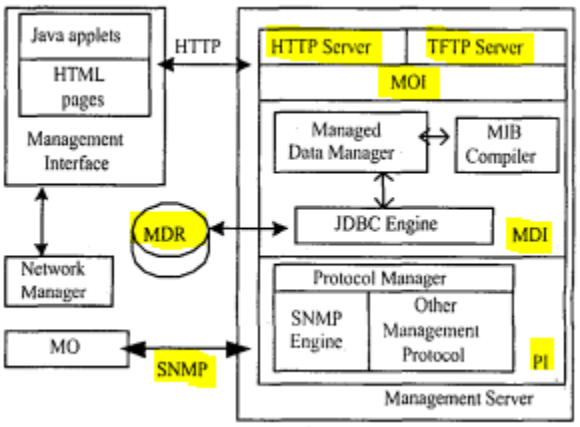

Fig. 3.System Model for the Management Server [1]

This management server actually manages the network object in order to provide the user interface to the network manager. HTTP server is used here

for communication purpose, SNMP to get/set attribute values of related network element and TFTP server to restore/retrieve configuration data of network elements in case of network failure occur and restore/recovery in need.

- *MOI (Managed Object Interface):* works as kernel with the responsibilities of initialize, get-set parameter, operation rollback, list and close down the managed objects in the network.
- *MDI (Managed Data Interface):* When Network manager request a network information via HTTP to MOI, it forward it to MDI. MDI translate it to SNMP and search in the MDR for the request. If found send it back to MOI, else forward to PI asking for the same.
- *MDR (Managed Data Repository):* It is the Data Hub that maintains a relational database and a file store.
- *PI (Protocol Interface):* Build with a SNMP engine, Po is responsible to communicate with MO and MDI.

V. Network Configuration Management Database System

With advancement in network science, this traditional approaches are becoming less effective for network configuration management. In order to generate more intelligent and automated system, researchers try to improvise the configuration management database (CMDB).

CMDB comprises the information of small components of network called Configuration Items (CI). A CMDB must be aware of availability, running status, utilization, specification of CI's.

Before going into any further technical details, let us first jotted down the main functionalities expected from a CMDB. Because upon knowing this only, we can understand why the architecture of the proposed Configuration Management system (CMS) developed like that only as it looks after the functionalities of the CMDB.

A. *Functional Overview:*

1) Trusted Source: Considering all CIs, i.e. routers. Firewall, switches, servers over the network, CMDB should have detailed information about all of them in the network. Because the data stored into the CMDB is analyzed to render the performance of the network and thus network resource capacity design is build.
So CMDB should have access over all elements in the network and update itself frequently.

2) Configuration Repository: To determine the best workflow or to troubleshoot any process over the network, the network manager should have proper knowledge to examine. The CMDB should work as the relational database repository where the manager can run its queries in order to gain sufficient and up to date information.

3) Change Management: CMDB should maintain a table of history where all the new configuration and old configuration should be stored. For performance evaluation, this tables are mostly pulled up by network manager.

4) Best Availability of Data: The latest implemented and current running structure should be considered as baseline model and this should be available to other network management systems too.

5) Asset Management Process: Not only the device or elements information, but CMDB also stored functional information like location, email, and name, contact etc.

6) Visualization: Information stored in CMDB should be visualisable. It helps the network manager to understand the network status way too better.

Now keeping an eye on this features, proposed model has been developed in the referenced paper [2].

B. *Architectural Overview:*

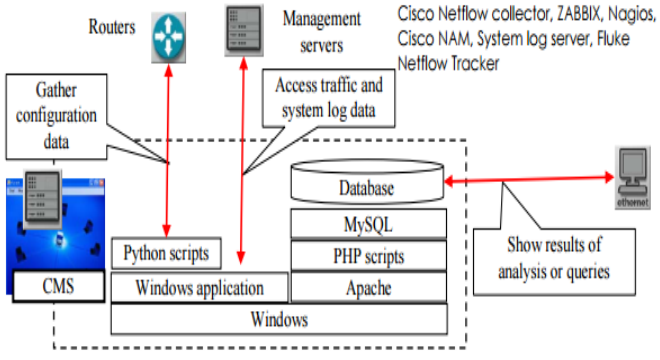

Fig. 4. General Functionality of WebNCMS [2]

To briefly describe the developed CMS, we can say, it gives us freedom to download both netflow data and system log data, in the corresponding Cisco Netflow Collector and System log server. Now we need to gather this configuration information from there in order to access routers in the network. Using Microsoft visual Studio, they have developed a windows application to access the router after obtaining the required data.

There are several management tools to choose from for web interface, i.e. Cisco NAM, Cisco Netflow Collector, ZABBIX etc.

Now for rational database part, where the pulled configurations files will be stored, is based on MYSQL and APACHE and PHP as the Web Interface of it, in order to access the queries and database.

C. Technical Approach:

So how this prototype actually relates the functionalities of CMDB? Well, first, to access configuration commands and routers over the network, this model includes a Python script in it. That is first basic functionality of CMDB.

Next, the cumulative information regarding network elements get stored as a .txt file in CMS server. Then all gathered text files can be exported to OPNET network planner where we can analyze the network performance a, sustainability and many more things. This is also a required functionality of the CMDB.

For the visualization part, using the query result and KML template, it generates KML files that can be opened using google earth software. Thus you can visualize the network architecture.

The configuration files get stored based on date, into different directories. So basically you have access to both old and new configuration of the network.

VI. NETWORK CONFIGURATION MANAGEMENT SYSTEM USING ARTIFICIAL NEURAL NETWORK

To reduce the workload of manual monitoring and troubleshooting, over the time researchers start to think about intelligent approaches for network configuration management. Like in biological data, we know the presence of overlapping subsequence in protein and DNA sequence, we can impose the same knowledge in computer network science as we already aware of OID and MIB that has the same features like them. The tree structure of MIB with branching sequence of unique OIDs has much similarity with the neural science. Thus this connects to neural network.

A. Functional Overview:

CAMM (Connectionist Associative Memory Model): For proper performance management and analyze the entire network and services, the proposed model in this reference [3] has incorporated CAMM instead of expert system.

This model comprises of two phase learning method:

- In the initial phase it involves the strategy maker where a flexible framework will be generated by using lateral links and will help in solving discrete applications. The reason behind this approach is to develop a cognitive model that can deal with OIDs.
- In the next part, new algorithms are generated to learn for the memory model of that existing connectionist. His results into formulating a dynamic database that will the information hub where all the different formats of OIDs will be stored that can be use in future for sequence recognition.

Using this method, in the end of the proposed model in the reference, a network topology has been created and different network component in the topology relates to the same database and thus managing the topology become easier by knowing the overall structure of it.

B. Architectural Overview:

For the proposed model, they applied Pattern recognition technique. It looks like a hierarchical model comprises of CAMM and Neural networks.

Fig 5 [3] and Fig 6 [3] is simple representation of the architecture and topology.

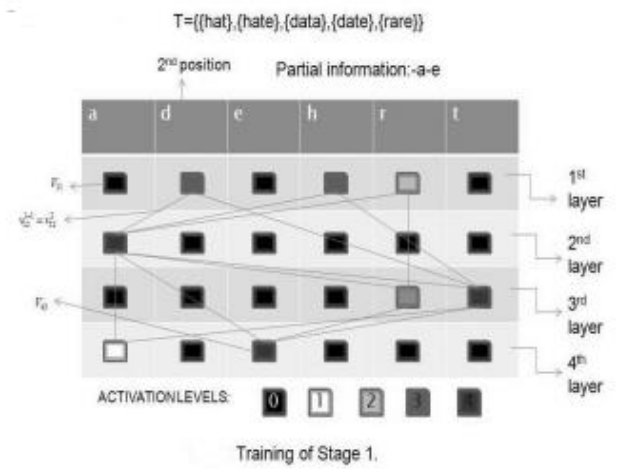

Fig 5. Architecture for stage 1 for 5 strings [3]

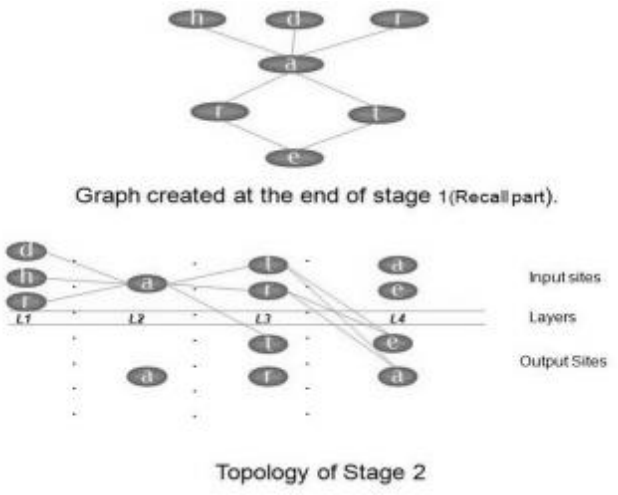

Fig 6. End topology at stage 2 [3]

So at the beginning, there is topology T that is actually an encapsulated input string consists of set of substrings which are partially dependent. Now the connection sets, known as v-sets, responsible to gather the sequence internal relations and also represents the link between nodes of two consecutive layers, formed by the elements in the input string.

So in the end a partially linked graph created where the sub stings are sharing the same storage space.

Now in next part, by using "gradient descent technique [3]", a network topology created with the activated nodes in the training sage 1.

C. *Technical Modification:*

Now in the referenced paper, they modified this CAMM algorithm to some extent, in order to improving the fault message resolving part. To improvise the database, "Microsoft Office Access database" has been used too.

If an input sequence has larger dimension, it provides better results while testing through difficult testing procedures. So as an end result the authors have been expected was to generate different formats for the OID's in the database that can produce improvised size of sequence.

In order to do that, OID's are converted to hex format from string. Then the repetitive pattern in the hex sequence replaced randomly to ensure a larger unique dimension. Below I have given an example [3] to show the change.

.1.3.6.1.2.1.25.6.3.1.1

↓

2e312e332e362e312e322e312e252e362e332e312e31

↓

ek31wx33mc36eu31be32mn31fh25pa36ps33fx31gm31

For the modified CAMM, we consider a fault sequence as an input [3].Now the test results of the improved CAMM will show the probability of components and represent the result in color. There will a key table provided that help us decide the probability level of the colors. Using the database table and the key we can resolve the levels of missing component in the faulty string.

VII. TECHNICAL OVERVIEW

For the technical overview part I would mention technical summery of the three different approaches I have mentioned in this paper so far. Also if there is any more technical points that could be discussed briefly in order to extend the idea of the paper, I will include that too.

A. Web based NCMS:

This paper has mentioned a distributed multilayer architecture that is platform independent. This module is based on SNMP protocol and Web Services. Beside of this, this distributed hierarchical module also involves several different internet technologies like HTTP, TFTP, HTML, Java Applets. The best part of it – it can remotely access the network.

This module allows a network device to integrate in the Network management by producing simple Java Applets.

B. *CMDB System:*

Using database system approach is better than the traditional web based approach as it takes less human involvement and mostly automated. The developed CMS is accruing all the basic functionalities of CDMA, that overcomes the manual effort and security loophole part of traditional web based method.

For database part, the proposed system involve a SQL database and for automated part it uses python scripting language and web services. Various management tools also helps in the automation part.

Nonetheless, involvement of OPNET network planner in the model makes performance evaluation of the network much easier and reliable.

C. *Expert system vs Neural Networks:*

The reason because they choose CAMM over expert system because when concerns about upper layer problems, it is hard to understand due to absence of significant model of the problem, independent applications and very distinct from one other. When complexity grows in the network, getting some pattern or any certain model give a better chance to prepare a more reliable management system.

Even sometime some network display some not so certain behavior of network using any finite state machine model.

For this intelligent technique, they have used pattern recognize and Hebbian based learning in order to develop the model. Then for the advancement of the model, they initiate fault management in OID's of MIB.

VIII. DISCUSSION

After going through all three primary papers and doing some related research for additional knowledge, I understand how the evolution happened with time in the network Configuration management. For the web based approach, that time platform independent and remote controlling privilege was hugely admired. But it compromise the security of the network hugely for any deployment. So to improve the model, deploying SSL will be a good approach as web service is already there.

Using database is a real better approach after that. It makes the thing automated and give more security on the system. Even with the scope of flexible database change, if any router suddenly change the network functioning, using the database the network can adopt that too. But this is only possible in low model designs. There was no scope of fault management. It either can deploy or rollback. Under time crunch this could have been a serious crisis.

To improvise that part, neural intelligence occurred. But it has also some certain drawback too. This model would be unable to capture multiple association of networks. Also the CMDB model considering the netflow in case of dynamic network. But in this AI approach, I am sure if that is quite possible, at least for this module.

Also in this AI module, there is nothing mentioned related to network security part. Security is the biggest threat for the date. I consider the input pattern and missing pattern in the input and concentrate on the fault management. But if any intruder alter the database or send some mischief input, there is no scope of firewall in that case.

In my point, there should be some kind of Hybrid technique. Intelligent technique mostly reduce the manual hassle part in managing the network, at least till now the papers I have been through , I only found the same. It makes failure detection prompt. But security should be the primary focus.

IX. CONCLUSION

In this paper, in order to show the evolution of the network configuration management system, reviewed three primary papers that includes the most traditional one to recent intelligent one.

For organizational security, configuration management is really crucial. For a better configuration management system, we need to have a clear idea on what configuration should be like, what could be important parameters of this and aplenty of knowledge regarding the network and its element.

In future, using this approaches we can go further for network monitoring as well as the other functional areas of networks.

REFERENCES

[1] Siu, João Buptista, and Zhen Sheng Guo. "Web-based network configuration management system." *Communication Technology Proceedings, 2000. WCC-ICCT 2000. International Conference on*. Vol. 1. IEEE, 2000.

[2] Yamada, Hiroshi, Takeshi Yada, and Hiroto Nomura. "Developing network configuration management database system and its application—data federation for network management." *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International*. IEEE, 2010.

[3] Ramiah, R., E. Gemikonakli, and O. Gemikonakli. "Development of a Network Configuration Management System Using Artificial Neural Networks."

[4] Hasan, Taqi, et al. "Network management system." U.S. Patent No. 7,082,464. 25 Jul. 2006.

[5] Network Management System: Best Practices White Paper http://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html#configmanagement

[6] SNMP tutorial https://www.manageengine.com/network-monitoring/what-is-snmp.html

[7] Wiki: Simple Network Management Protocol https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

[8] Network Configuration Management http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.html

[9] Nuansri, Nittida, Tharam S. Dillon, and Samar Singh. "An application of neural network and rule-based system for network management: application level problems." *System Sciences, 1997, Proceedings of the Thirtieth Hawaii International Conference on*. Vol. 5. IEEE, 1997.

[10] Gemikonakli, E., O. Gemikonakli, and S. Bavan. "Intelligent Network Monitoring Using a Connectionist Inference Model." (2008).