Automated Network Administration for Large Organizations

Shaikh Shaima'a[1]
Department of Computer Engineering
M.H. Saboo Siddik C.O.E.
Mumbai, India

Shaikh Shifa[2]
Department of Computer Engineering
M.H. Saboo Siddik C.O.E.
Mumbai, India

Zahida Bano[3]
Department of Computer Engineering
M.H. Saboo Siddik C.O.E.
Mumbai, India

Z. A. Usmani[4]
Department of Computer Engineering
M.H. Saboo Siddik C.O.E.
Mumbai, India

Abstract - The network society is a global society having limitless boundaries. Organizations are highly dependent on networks since it forms the foundation for their fundamental growth through device management, sharing data and information that is being accessed. It necessitates for extremely on-demand, fast and user friendly network management application that can be used to monitor and supervise the private networks. Incorporating a network tool used by the administrators to search and trace out IP address information will facilitate real time screening and decision making in any network subnet efficiently and frequently.

The proposed approach is able to allocate IP addresses and IP pool to the designated user in wide-ranging organizations and provides incident reports so that administrators can handle cases frequently.

Although there have been some proposed tools available for the assignment of unique IP addresses, there is a need of proper mechanism through which all information should be traced out in desired manner, is proposed in this paper.

Keywords - Hardware Traceability, fabrication, FCAPS, accounting management.

1. INTRODUCTION

The vitality and complexity of computer network makes them challenging to design and manage. Network management denotes to the events, approaches, trials and various resources that are relevant to the manoeuvre, administration of network system. Information for large network management is composed by means of efficient super visioning and logging of data travelled over the network. The exclusivity of network management is its ability to gain control over a vast network and reducing malicious data and security breaches. But there are some drawbacks such as redundancy in data and is greatly reliant on human manipulation, vulnerable to unauthorized fabrication and its adaptability with today's networking needs. Here, comes the need of a rationalization that can offer a complete IP space management along with the control of automation to reduce processing time and avoid expensive network idle time.

In this paper, we have proposed a system architecture that can be used by any organization for securing and providing their IPs over entire network and that will provide them secure reports for analysis of accidental or unintentional activities over network.

2. NETWORK MANAGEMENT FCAPS MODEL

Automated network administration in large organizations is a means of organization of IPs and supervision of the Internet Protocol address space used in a network [1].The Goal of network management is to ensure that the users of a network receive the information technology services with the quality of service that they expect [3].

FCAPS model is used for network management. FCAPS model is divided into five levels. The five levels are listed as:

2.1. Fault Management

At this level, network faults are found and fixed. Active fault management addresses the problems by actively observing the network traffic.

2.2. Configuration Management

This level deals with monitoring and controlling of operations. Precautionary maintenance can be performed in order to tackle the disputes.

2.3. Accounting Management

It is also called as Billing Management. Here, optimal resource distribution is achieved. Statistics can be used for locating the boundaries.

2.4. Performance Management

Overall performance and throughput of the network is examined by the performance management. Network health is monitored by comparing the past and current performance.

2.5. Security Management

Unauthorized access is prevented to ensure confidentiality of data. Proper authentication and auditing is provided so that sensitive information remain secure.

Our proposed system comprises all five categories of FCAPS model by allocating IPs to verified users only, detecting faults and providing security from unauthorized access.

3. EXISTING SCENARIO

Various organizations are highly dependent on static spreadsheets implemented through excel files which are maintained by hands. Tracking, managing, incident detection, handling and reporting is all manual. These systems have following limitations:

- It has problems regarding redundancy in data and is greatly reliant on human manipulation adding more burden on the network administrator.
- It is notably vulnerable to unauthorized fabrication and interception and thus the security breach.
- The system evidently cannot adapt with today's networking needs
- The System also lacks in automation in hardware traceability, automatic blocking and unblocking, reporting tools, etc.

Because of all above issues, there is a need for developing a system through which these issues can be controlled in well-organized manner.

4. PROPOSED SYSTEM

Here, comes the need to develop a Web application, which will be used to manage the network and associated subnets in the growing organizations. Our proposed system will aim at overcoming the shortcomings of the existing systems. Any network node has a valid public IP and can be traced to an I/O port. This application should serve as a network management tool which will be used by the network administrators to search and trace out IP information about any node. This tool should have provision for the department administrators to draw IPs from a pool and also should have provision to request a new IP pool from the network administrator. This tool should provide an interface to log network incidents and should generate incident reports as may be required. This tool should also generate necessary reports by the network administrators for surveillance and audit of network elements and network. It also has the provision for network admin to take control as a department admin to serve as a proxy in case of his unavailability.

Proposed system consists of four major components: User Profiling, Search and Navigation of IP data, IP Management and Reporting Tool. Fig. 1. shows the block diagram of proposed system.

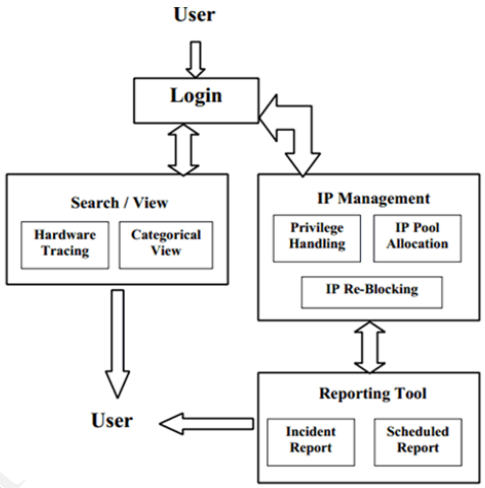

Fig. 1. Block diagram of proposed system

Legitimate users are authenticated and given access to the system. With the help of search and navigation, hardware traceability can be performed to the end node. Various search selection allows the user to search the desired information in various style and conveniently. IP allocation and IP pool allocation are key operations through which department administrator can allocate IP to the user and network administrator can provide IP pool to the requesting department after verifying the request. After performing a scheduled check, free IPs can be reclaimed via the IP Re-Blocking. There is a need to generate Incident reports and scheduled reports for discovering incidents on networks [2].

5. OBJECTIVES

The core objectives for the administration includes the following:-

5.1 IP Pool Allocation and Management

Various Block Administrators can submit the mandatory data with respect to the requirement of the end usage of IPs. Once all vital data has been stored in the system regarding the end use of IPs, this system will begin the unblocking process of IP at firewall and subsequently will release the IP for end use. It will also ensure that relevant computer code which is used to identify each user uniquely in the system would be put in for IPs drawn for personal use and that computer code will be cross linked to the

database for legitimacy verification. If idle, the IP will be reclaimed and re-blocked.

5.2 New IP Pool Allocation

Each Department is given a set of IP addresses in the form of IP Pool. Whenever the Department will be exhausted with the IP's given request will be sent to the Network Administrator to allocate the IP Pool for that particular Block along with that a VLAN will be associated with it.

5.3 Statistical Incident Reporting

Network incident reporting of external as well as internal network are vital to know how exactly the system is working. This system will have the capability to serve out incident related information and generate report with respect to the details of incident ID which is distinctively generated from the system. Users will also have to enter a diminutive description of the incident such as unavailability of the IP, unable to access data after authentication etc. The date and time of the occurred incident and the frequency of incidents will be recorded in the system automatically.

5.4 User Profiling or Role Implementation

Automated Network Administration provides variety of exclusive privileges based on three different profiles namely network administrator, department administrator and subnet administrator which are in essence with the unique roles for the users.

Fig. 2. Shows the login screen with username and password which differs according to the role of administrator. For precise authentication, these parameters needs to be unique in a network.

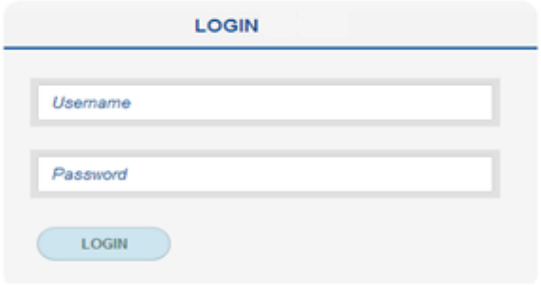

Fig. 2. Login screen

5.4.1 Network Administrator:

Network administrator is in charge for congregating details of the IP and underlying network related data & to smooth the progress of searching the user till the end node in hardware traceability section from the dashboard. The network administrator facilitates automatic check for use of IPs drawn within 48 hours of allocating the IP to ensure that the IP owed is not unutilized in case the IP is not drawn for personal end use. Network administrator has the highest privilege and accessing rights as compared to department or subnet administrators.

Fig. 3. shows the dashboard that will appear on the network administrator's homepage indicating the facilities available to network administrator. Central authority over the features provided to the network administrator.

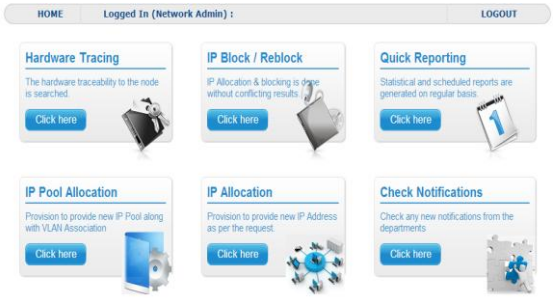

Fig. 3. Homepage of Network Administrator

5.4.2 Subnet Administrator:

For a subnet administrator, who manages one or more subnets, the information served out will include the detail on every IP address [4] in the assigned subnets' range, name of the end users / machines to which it is allocated to and the location Subnet administrator is responsible for managing subnets where there is no qualified department administrator and serve as a proxy.

5.4.3 Department Administrator:

Department administrator is designated to be in-charge of a particular department. She/he facilitates release of IP's upon submission of necessary and mandatory details at the application. Department administrator also provides facility for automatic unblocking of IPs on request with logging and report generation.

5.5 Reporting

The reporting functionality provides quick configuration alerts for related events, unrelenting conditions, and complex combinations of device states.It also assures that the IPs listed as blocked by the system are in reality blocked. Graphs are also generated to depict that there are no floating IPs in the assigned subnet range with scheduled scanning and checking of allocated IPs. Generation of alerts on free IPs for any department hitting a configurable low threshold level is also depicted through statistical graphs to provide ease in comprehension.

5.6 Hardware Traceability

Network trace information to the node is direct dependent on the underlying network architecture. Every IP / IP range is bound to a set of identifiers. The system will be scalable to adopt more network architectures and take in corresponding identifiers if there is a need to do so to represent any other different network scheme. The

hardware traceability to the node for a network will be represented by a corresponding table structure at the system which will give the information about end usage of IPs, which will include information such as department, username, IP address, etc. Figure 4 shows a sample hardware traceability table which indicates the details of all users in a particular department along with a provision to edit or delete the information of the users.

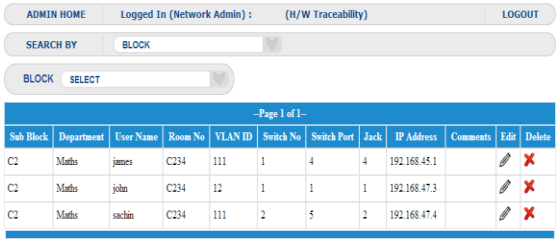

Fig. 4. Hardware Traceability

6. GENERIC APPLICATION FEATURES

The system proposed, encompasses the following features in order to improve the overall performance.

a) The network alerts help administrators recognize and correct issues before users experience performance deprivation or availability issues.

b) Classified information is served out at the interface to the users based on user profiling.

c) Obligatory web application security & IP based Access control is provided. All security considerations exist on the spectrum between convenience and protection.

d) The interface will have proper authentication and authorization to act upon the data made available to them.

e) The login will be through secure sessions and over https protocol. Use of Sessions will take care not to allow access to internal pages and hence data and information bypassing the authentication phase.

f) Automated network device discovery is done to ensure and monitor all the critical equipment used in the network thus saving precious time by eliminating manual database entries.

7. CONCLUSION

IP address space Management is most widespread but commonly ignored in large organizations. A number of studies were reviewed and some common issues in these methods were identified. The proposed system eliminates these issues by dividing the management work in different gears and among different profiles, and thus monitoring and management of network becomes trouble-free.

8. ACKNOWLEDGMENT

We are grateful to M.H.Saboo Siddik College of Engineering for guiding us in preparation of this paper. We are also thankful to our teaching staff and our project guide for their gentle assistance.

9. REFERENCES

1. A.Clemm, A. Network management fundamentals. Indianapolis, Cisco Press, 2007.
2. Parker, J. FCAPS, TMN, & ITIL: Three key ingredients to effective IT Management. 2005.
3. Mark Subramanian, Network Management Principles and Practice, 2nd ed. Pearson Education, 2010.
4. Timothy Rooney, Introduction to IP Address Management, Wiley Publication, 2010.