Different modes of Discovery of Network nodes using SNMP and Reconciliation

[#1]Hemlata Eglambe, [#2]Divyani Vade, [#3]Megha Temgire, [#4]Prof. Radha Shirbhate

[1]4321hema@gmail.com
[2]divyanivade12@gmail.com
[3]meghatemgire1@gmail.com
[4]radha.shirbhate@gmail.com

[#123]Department of Computer Engineering
[#4]Prof. Department of Computer Engineering

JSPM's, Bhivarabai Sawant College of Engineering & Research, Pune,India.

ABSTRACT

Designing of a proficient discovery module is a key challenge in a spread out network. It is necessary to keep records of every device in network for the company by which it can keep the details about the devices recorded in the network as per the condition of presence or failure of that device. Discovery of Network Elements (NEs) in the network is achieved through two modes of detection that are through IP range specification i.e. range based discovery, device based discovery and individual discovery. In range based discovery they have to give the range of IP addresses which are already present in the database, this will find out existing network elements and maintained their information. Network consists of dissimilar devices like switches, hubs, routers etc. This is reason that to keep record of all these devices. Network is the collection of links and devices in a network and the interconnections among the devices. Network devices finding can also be portioned the local area network (LAN) or an organizational-level network discovery or any network. An new network administrator joining an organization faces many difficulties due to the unavailability of a discovery tool, which otherwise would show the device categorization and layout of the networks. Even for the experienced administrator, keeping trail of devices and their connectivity details, without having a proper method of visually representing them becomes a difficult task. A network element is usually defined as a manageable logical entity combining one or more physical devices.

Keyword: SNMP, NMS, Network Elements, Node Discovery, Reconciliation.

ARTICLE INFO

I. INTRODUCTION

Designing of an efficient discovery module is a key challenge in a spread out network. Discovery of Network Elements (NEs) in the network is achieved through two modes of discovery that are through IP Range Specification i.e. Range Based Discovery. In Range Based Discovery we have to give the range of IP addresses which are already present in the database, this will discover existing network elements and maintained their information. If we specify whole IP range of company network then it will scan all the devices present in the network as well as subnets in the networks. "Discovery of NEs & Reconciliation using SNMP" is used to scan the devices connected in the network. keep track of all the devices in the network because functioning of every device & to check whether they are alive is very important purpose. In case of existing system it is possible to run discovery but Reconciliation was not their & it was given to third party. This software gives facility to discover the nodes [2] as well as after completing discovery we can reconcile it. This will become very helpful for company &

easier because no need of third party. Authorized person can perform the Discovery &Reconciliation very easily.

II. RELATED WORK

SNMP

Simple Network Management Protocol (SNMP) is an "Internet- standard protocol for managing devices on IP networks. Devices that typically support SNMP [4][5] include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network - attached devices for conditions that warrant administrative attention.SNMPis a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management' data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

NMS

A network management system (NMS) [1] is a combination of hardware and software used to monitor and administer a computer network. Individual network elements (NEs) in a network are managed by an element management system. An NMS manages the network elements, also called managed devices. Device management includes faults, accounting, configuration, performance, and security (FCAPS) management. Management tasks include discovering network inventory, monitoring device health and status, providing alerts to conditions that impact system performance, and identification of problems, their source(s) and possible solutions [3].

EMS

An element management system (EMS) consists of system and applications for managing network elements (NE) on the network element management layer (NEL) of the Telecommunications Management Network (TMN) model. As recommended by International Telecommunication Union -Telecommunication Standardization Sector (ITU-T), the element management system's key functionality is divided into five key areas - fault, configuration, accounting, performance and security (FCAPS). Portions of each of the FCAPS functionality fit into the TMN models. An element management system manages one or more of a specific type of telecommunications network element. Network Element A network element is usually defined as a manageable logical entity uniting one or more physical devices. This allows distributed devices to be managed in a unified way using one management system. According to Telecommunications Act of 1996, the term `network element' means a facility or equipment used in the provision of a telecommunications service. Such term also includes features, functions, and capabilities that are provided by means of such facility or equipment, including subscriber numbers, databases, signaling systems, and information sufficient for billing and collection or used in the transmission, routing, or other provision of a telecommunications service.

III.PROBLEM STATEMENT

Discovery of NEs using SNMP & Reconciliation" is based on concept of discovering nodes in network which can include switches, routers, hubs etc. Aim to get information about all those devices in network & keep records of each & every element. This is helpful for company to identify if any fault occurs in the process afterwards. Using SNMP i.e. Simple Network Management Protocol we will perform discovery of Network Elements.

IV.PROPOSED SYSTEM

In system they are providing Range based discovery, Individual discovery Device based discovery of network elements from which Device Based Discovery is absent-minded in existing system. This main advantage is any new device has been added will get invention at the time of Range Based Discovery and gets added in the main database &save the lot of time then improve the efficiency of the system by reducing the efforts of manual entry. Our system also provides the Individual Device Discovery by which the user can search any one particular standalone device by its IP address. Discovery and Reconciliation helps create an exact opinion of your network so that you can harness all your resources to make service fulfillment reactive and cost-effective. Consider Discovery and Reconciliation for data integrity management if you want to:

•   **Cut costs:**
Remove costly data cleansing procedures with an automated discovery and reconciliation process, coupled with checks and balances to ensure and keep the integrity across your OSS/BSS.

•   **Get exceptional data accuracy:**
Rise data accuracy to 90% or better to decrease provisioning fallout and time to repair, and to increase the overall effectiveness of process automation struggles to further reduce operating expenses.

•   **Use all your resources:**
Improve stranded and missing assets to minimize network overbuilding and thus reduce capital expenses.

•   **Reduce revenue leakage:**
Make sure all your services are being billed for properly.

•   **Take a non-intrusive approach:**
Reconcile discovered data without distracting your existing OSS/BSS.

•   **Speed time to market:**
Quickly enhance your data integrity management to maintenance new services or systems with flexible customization tools.

Benefits:

•   Open interfaces with established integration with 3rd party systems such as Ericsson (Telcorida/Granite), Amdocs (Cramer), Oracle (MetaSolv), and many more.

- Springy, programmable business rules to enable workflow automation and automatic reconciliation.
- Minimize manual interposition, growth flow-through provisioning success rates.
- Improve effectiveness of field operations and processes with integrated Record Browser supporting powerful search engines.
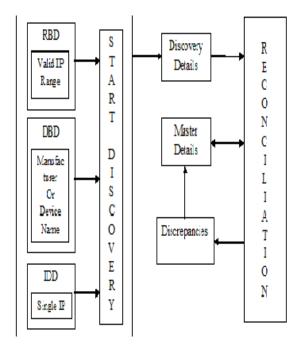
V.SYSTEM ARCHITECTURE
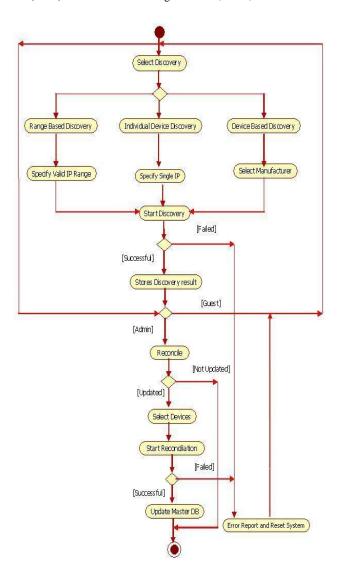

Fig1.SystemArchitecture

Fig 2.Workflow Diagram

V.IMPORTANCE DISCOVERY

This will be used by the company for management of the networks as well as keeping the track of the devices used in network. As our system also allows dynamic discovery of NEs, this will be helpful in error detection & recovery. The reconciliation module implement in our system is for the handling of the database perfectly. System gives the facility to view newly updated, added or old deleted nodes before the changes are reflected to the database. User can also check for the information after the discovery gets completed and he can either do the updating automatically or manual.

VI.ADVANTAGES AND APPLICATION

Advantages:

1) Complete Approach for Discovery.
2) Reconciliation Module.
3) Automatic identification of Network Element.

Application:

1) Organization.

2) Educational Sector.
3) Research Center.

VII.CONCLUSION

The proposed system overcomes the limitation of existing system. It will improve the performance of system and keeping information off all the devices which is present in network as well as performs fault detection and management. By using this system time of network administrator saved because authorized person can perform the Discovery & Reconciliation very easily. Avoid duplication of data by using reconciliation module & achieve central point recovery by using this system.

REFERENCE

[1] "Network Management –Principles and Practices" by Mani Subramanian.

[2] Kishori M. Konwara, Dariusz Kowalski , Alexander A. Shvartsman , "Node discovery in networks", 2008.

[3]Y. Bejerano, Y. Breitbart, M. Garofalakis, and R. Rastogi, "Physical topology discovery for large multi-subnet networks," in Proc. IEEE INFOCOM, 2003, pp. 342–352.

[4] M. Shoaib Yousaf ,Ahmed Mattin ,Ahsan Raza Sattar , "Real Time Network Monitoring System in LAN Environment", IJRIME Volume1Issue5 ISSN-2249-1619,2011.

[5]Suman Pandey, Mi-Jung Choi, Sung- Joo Lee, James W. Hong "IP Network Topology Discovery Using SNMP".

[6] C. Perkins and E. Royer, "Ad-Hoc On-Demand Distance VectorRouting,"Proc. IEEE Second Workshop Mobile Systems and Applications,1999.

[7] S. Podlipnig and L. Boszormenyi, "A Survey of Web CacheReplacement Strategies," ACM Computing Surveys, vol. 35, pp. 374-398, 2003.