# The Discovery of Enterprise Network Topology Created in a Virtual Environment with SNMPv3

Musa BALTA[1], İbrahim ÖZÇELİK[2]

[1,2] Computer Engineering Department, Faculty of Computer and Information Science
Sakarya Üniversitesi 54187 Serdivan / SAKARYA / TURKEY
[1]e-mail: mbalta@sakarya.edu.tr, [2]e-mail: ozcelik@sakarya.edu.tr

**Abstract:** To design network management systems in a best way, network topology have to be discovered with every features of network such as connectivity, device type, etc. Our goal is to discover an enterprise network which is created in a virtual environment (GNS3 and VMWARE Workstation) with SNMPv3. An algorithm which is used in previously academic researchs is redesigned according to features of virtual environments which are used in project.

**Key words:** Topology Discovery, Snmpv3, GNS3, VMWARE Workstation

## Introduction

Nowadays enterprise networks have become more complex and wide because of huge number of users and a lot of applications that work in networks (Pandey, Choi, Won and Hong (2011), Siamwalla, Sharma and Keshav (1999), Breitbart, Garofalakis,Jai,Martin,Rastogi and Silberschatz (2004), Lowekamp, O'Hallaron and Gross (2001)). To benefit from this growing enterprise networks more effectively and efficiently, network management concept which means management and maintenance at the highest level has occured. Network management systems have some kind of basic concepts such as security, topology discovery, monitoring, controlling, coordination and schedule. To benefit from these concepts of network management more effectively, first of all, topology discovery and connection of between devices have to be detected in a best way. And then network management system can be designed according to these results.

There are several techniques in network topology discovery such as ping mechanism, trace-route, DNS (Domain Name System) and SNMP (Simple Network Management Protocol) (Pandey and et.al.(2011), Siamwalla and et.al.(1999), Breitbart and et. al. (2004), Lowekamp and et. al. (2001)). But only SNMP can provide better performance than others and also it pulls a lot of queries in completely and a secure way like as name of device, device type or connectivities between devices.

In this paper, an enterprise network topology that has been created in virtual environmet (GNS3 and VMWARE workstation) is going to be discover through an algorithm which uses SNMPv3 that is security version of SNMP. Due to work in virtual environment, the proposed algorithm is going to finish topology discovery more less time than a real environment.

## Snmp

SNMP is a network management protocol for managing IP (Internet Protocol) networks. SNMP has a three structure; agent software which runs on managed devices, SNMP manager which communicates between NMS (Network Management System) and agent, and finally NMS which manages all network operations. SNMP'working mechanism is like as sending request and reply to request and to make these operations, UDP (User Datagram Protocol) is used (Harrington, Presuhn and Wijnen (1999a),Harrington and et. al. (1999b)). By means of SNMP, data can be pulled from device easily and configurations on device can be changed easily. For example, device can be restarted or a configuration file can be send to device. Hereby, we realize that SNMP is more important protocol in network management.

When SNMP pull data from the device, SNMP uses some kind of identifier to pull data. These identifiers are called as MIB (Management Information Base) values and these values are represented with numbers. For instance, 1.3.6.1.2.1.1.5.0 variable means device name (Harrington, Presuhn and Wijnen (1999b), Blumenthal and Wijnen

(1999)). The requested values in MIB are called also OID (Object Identifier) variables. Values of MIB and OID are existed in reference numbered (Levi, Meyer and Stewart (1998)) .

SNMP uses some criterias in for network security. Some more important criterias are given in below (Levi and et. al.(1998));

- Authentication: It provides data integrity and authenticate source of data.
- Community name: It is used for authetication parameter during message transmission between SNMP and managed devices.
- Encryption: It encodes SNMP packages.
- Privacy: It provides to keep content of SNMP packages in network in hidden.
- Security Level: This means an algorithm which is used on every SNMP packages. HMAC, MD5 or SHA are used.
- Data Integrity: It means not divided data situation of a message package.
- SNMP User: This is a user who manage the SNMP system. According to SNMP messages that comes from network management system, user can make any related changes about situation of network.
- Security Model: This is a security strategy that is used by SNMP agent. There are 3 version: SNMPv1, SNMPv2c, SNMPv3.

Unfortunalety, all of SNMP version can't support all these security criterias. There is a comprasion of SNMP version about security in table 1.

**Table 1**: SNMP Security Models and Levels (Levi and et. al. (1998))

| | Model | Level | Authetication | Encryption |
|---|---|---|---|---|
| 1 | v1 | noAuthNoPriv | Community name | No |
| 2 | v2c | noAuthNoPriv | Community name | No |
| 3 | v3 | noAuthNoPriv | User name | No |
| 4 | v3 | authNoPriv | MD5 or SHA | No |
| 5 | v3 | authPriv | MD5 or SHA | DES, AES |

As we see in above, SNMPv3 made SNMP queries are used in secure way with encryption algorithms during data communication because of supporting all security levels. So SNMP packages are encrypted during all communication and network security is ensured.

## Application of Network Topology Discovery

Network topology discovery is very big and comprehensive area and there are also a lot of academic research about it (Pandey and et.al.(2011), Siamwalla and et.al.(1999), Breitbart and et. al. (2004), Lowekamp and et. al. (2001)). In addition, there are a lot of applications about network discovery in both academic and commercial environment (Lyon (1997) NMAP, Paessler AG (2003) PRTG). Most of these studies are made in real environment. In our study, we have referenced to Pandey's (2011) academic research which is made with using SNMPv2c. But in our study, both an enterprise network is created in virtual environment and the topology is discovered with SNMPv3 in securely.

With this goal, in the following sections, firstly information with related to modelling environment is going to be given and then information of algorithm in used will be given.

**Modelling Environment**

To modelling a network topology, we use a well-known program called as GNS3 (Graphical Network Simulator) that is a modelling program for network modelling simulator. Since GNS3 can model Cisco devices exactly, it has been used for this study (Grossmann, Marsili, Alt and Eromenko (2007), GNS3). To run the application codes, at first a virtual machine is created in VMWARE Workstation that is a well-known program in virtulization environment, and then this created virtual machine is attached to network topology that is created in GNS3 program with making related configurations (VMWARE (1995)).

An enterprise network means to connect all isolated departmental or workgroup networks into an intracompany network, with the potential for allowing all computer users in a company to access any data or computing resource. And also it would provide interoperability among autonomous and heterogeneous systems and have the eventual goal of reducing the number of communication protocols in use. In brief, it integrates all the systems within an organization.

Depending on the information given in above, for network topology discovery which is purpose of this study, an enterprise network structure which is created with GNS 3 and Vmware programs, is chosen as a sample model. In this model, part 1 is given a form as backbone of the network and for this part, Cisco 6509 switches are used. In part 2, cloud describes the virtual machine in VMWARE Workstation which we developed our application in. In part 3, 4, 5 and 6, different departments of the enterprise network are shown. One of the main backbones manages DMZ (Demilitarized Zone) which is shown in part 7. DMZ exposes an organization's external seriveces to a larger untrusted network (usually internet). The other one manages VPN (Virtual Private Network) servers which are shown in part 8. VPN provides remote offices or traveling users access to a central organizational network securely. On the other hand, the rest of topology consist of call managers and access points.

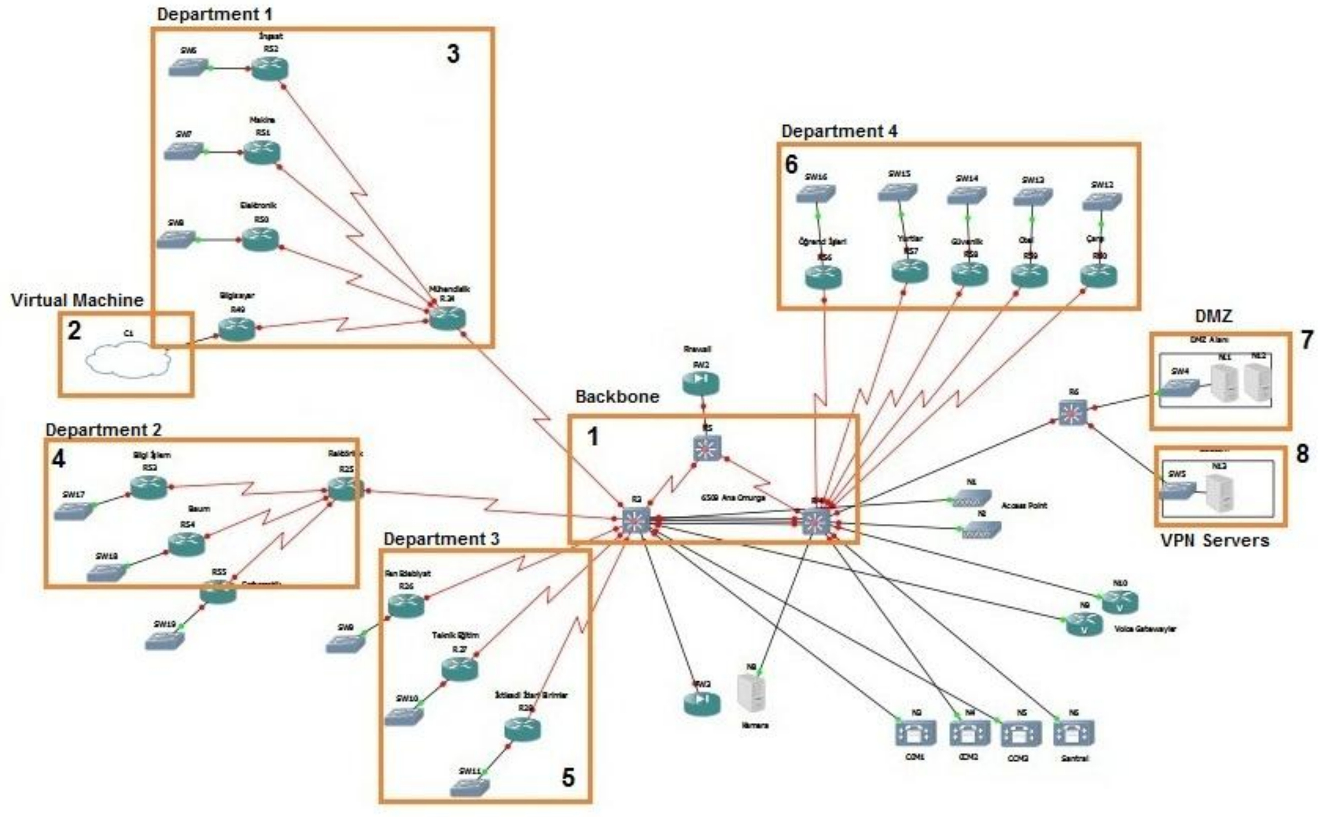


**Figure 1**: An Example of An Enterprise Network Topology

After finishing all required configurations (such as enabling SNMP, router configurations etc.) in GNS3 program, modelling of an enterprise network is completed. The part that application codes and algorithm run in, is created in VMWARE Workstation program and attached to topology as a cloud which is shown in part 2 of Figure 1.

### Configuration

This proposed algorithm consists of a lot of subjects such as device type, connectivity of devices, routing table etc.

Before we start to run the algorithm, we have to check all configuration on devices are ok. To pull out datas from devices, we use SNMPv3 which is shown in row number 5 of Table 1. For enabling SNMP on each device, we have to observe these rules in below (Blumenthal and et. al.(1999), (Levi and et. al.(1998));

- Group is created: The security model and level that is given in row number 5 of Table 1 is selected. “grup1” is created for devices in same area in command line in below. This group is set to “read” feature and security level is selected as “v3”. And then “grup1_oku” is created for “read” feature.

  *snmp-server group grup1 v3 priv read grup1_oku*
- User is created: According to security criterias, users are added to group. For user names, “kullanici” is used. To add security criterias, “md5” algorithm is used for authentication, “aes 256” algorithm is used for encryption. And this security criterias are set to “grup1”.

  *snmp-server  user kullanici grup1 v3 encrypted auth md5 cisco priv aes 256*

- Features is created: “read, write and notify” features can be set to group. Our study’aim is only about topology discovery, “read” feature ise enough for us. And “read” feature is related to “view” command. “izle” is created for “view” feature.

  *snmp-server view izle system included*

### The Used Algorithm and Implementation

After all of the configurations have been completed, the algorithm is ready to start. As we told, SNMP mechanism is send request and reply to the request (Lowekamp (2001)). All values (such as system situation of device, routing table on device, mac address table of device, package that flows over device) are identified by MIB values. So when you want to pull out data from device, you have to add related MIB values to end of the SNMP query.

According to this SNMP MIB value responses from device, the algorithm is created and also in every step of algorithm, related MIB values are used.

The used algorithm for the project is shown in Figure 2. Since GNS3 doesn’t support some features in swithes and logical topologies, this proposed algorithm is the renewed version of the algorithm that is given in academic research (Pandey and et. al. (2011)):

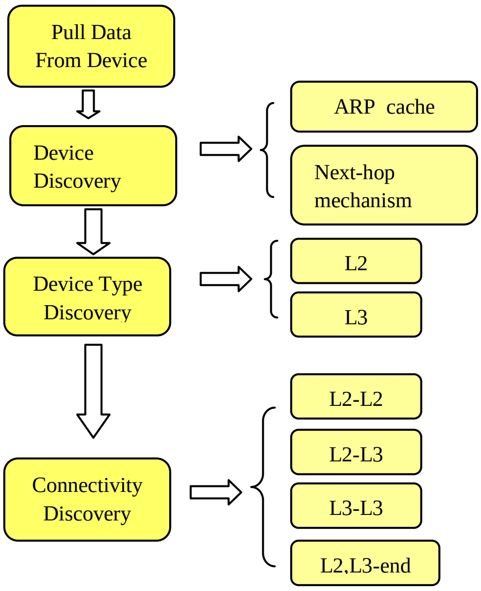
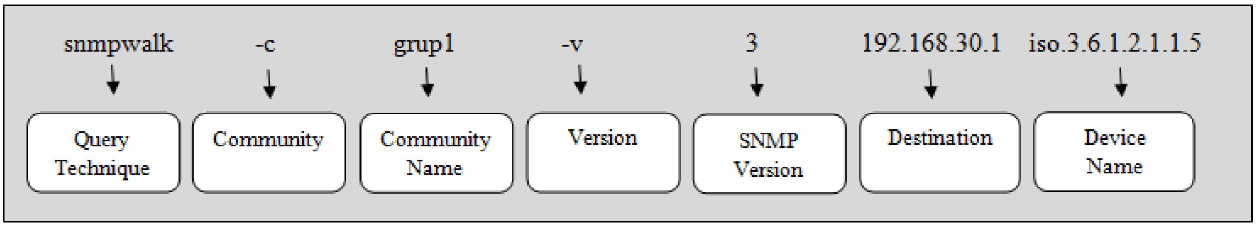


**Figure 2***:* The Used Algorithm

Steps of the algorithm:

- **Pull data from device**: After creating network topology on virtual environment, we configure device and then we can pull datas from devices with SNMP queries. For pulling out data from device, we use "snmpwalk" query technique of "net-snmp" library which includes all SNMP PDU's (Protocol Data Units). For example, to get the name of device name, we have to add this query to our application:



- **Device discovery**:"ipNetToMediaNetAddress" and "ipRouteNextHop" values are pulled out from devices with using ARP caching and Next-hop mechanism (Cisco 2005, Bierman and Jones (2000)). Firstly, we find out our subnet, then we start to ping all the subnet. After pinging all the subnet, we can find all alive devices. And then we send query of "sysServices" to all the alive devices. If the response that comes from device is equal to "78", we realize that device is a router and we look at the routing table of that device with query of "ipRouteNextHop". This tables includes all subnets of the network. Finally we ping again all of the subnets of the network. Hereby, we can find all alive devices. With ARP caching, we can find IPs of layer 2 devices with using query of "ipNetToMediaNetAddress".

- **Device type discovery**: According to "sysServices" value that is pulled from device, system decides that device is L2 or L3 device. After completing the device discovery part of the algorithm, system sends to query of "sysServices" to all of the alive devices. According to response comes from device, we can realize device is a what kind of device.

- **Connectivity discovery**: According to result of matching of ip and mac address that comes from device, we system decide that connectivity between devices is L2 or L3 connectivity. For finding L3-L3 connectivity, we use query of "ipRouteNextHop". According to the result of query, we can check out the routing table. In routing table, we can see only "direct" or "indirect". Direct means that ip is an interface of that router. Indirect means that ip is destination route of that router. For L2-L2 connectivity, we check out AFT (adres forwarding table) of L2 devices. If there is an match of this tables, we can realize these devices are connected to each others. For L2-L3 matching, we check out all the entries of mac tables of switches. If any entry is the same mac of any router's interface, we realize that router is connected to that switch.

Project is coded with C# programing language in Visual Studio. As a database, MySql is chosen for this study. For SNMP libraries, Web SNMP API.Net Edition 4 is used (Zoho, WebNMS). After running the program,we have a network view in Figure 3. In Figure 3, we have run the algorithm only on these parts of Figure 1.

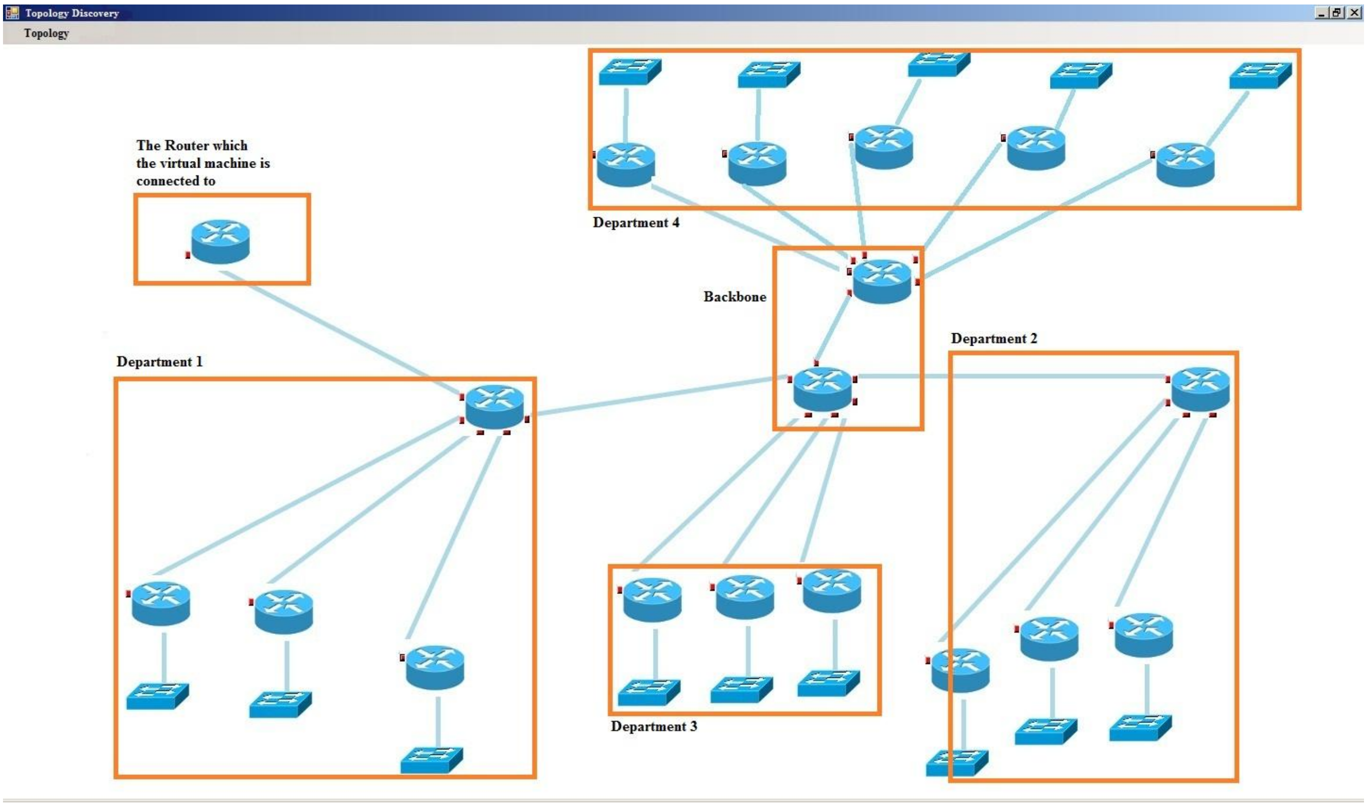


**Figure 3:** Graph View of Network

## Conclusion

In this study, we have chosen a virtual environment instead of real environment in order to not come up some problems in real environment  for network topology. For virtual environments, GNS3 and VMWARE programs are used, related configuration are made on this programs. Because of security features, we have chosen SNMPv3 for network discovery. Since network discovery is made in different virtual environments which communicate with each other, this study can be an example for futureworks.

## Acknowledgement

This project is supported by SAU Committee of Academic Research Projects (Project number: 2011-50-01-072)

## References

Bierman and  Jones (2000). IETF web page, Physical topology MIB. <http://www.ietf.org/rfc/rfc2922.txt> (2011 June 27).

Blumenthal and Wijnen (1999). IETF web page, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). < http://www.ietf.org/rfc/rfc2574.txt> (2011 July 24).

Breitbart, Garofalakis,Jai,Martin,Rastogi and Silberschatz (2004). Topology discovery in heterogeneous IP networks:the NetInventory system. *IEEE/ACM Transactions on Networking* 12(3) 401–414.

Cisco (2005). Cisco web page, SNMP community string indexing.
<http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801576ff.shtml> (2011 June 27)

Grossmann, Marsili, Alt and Eromenko (2007). GNS3 web page, Homepage. <http://www.gns3.net/documentation> (2011 June 25).

Harrington, Presuhn and Wijnen (1999a). IETF web page, A Simple Network Management Protocol (SNMP ). <http://www.ietf.org/rfc/rfc1157.txt> (2011 July 22).

Harrington, Presuhn and Wijnen (1999b). IETF web page, An Architecture for Describing SNMP Management Frameworks. <http://www.ietf.org/rfc/rfc2571.txt> (2011 July 22).

Levi, Meyer and Stewart (1998). IETF web page, SNMPv3 Applications. <http://www.ietf.org/rfc/rfc2273.txt> (2011 July 24).

Lowekamp, O'Hallaron and Gross (2001). Topology discovery for large ethernet networks. *ACM SIGCOMM* August; 237–248.

Lyon (1997). NMAP web page, Homepage. <http://nmap.org/book/man.html> (2011 July 16).

Paessler AG (2003). Paessler web page, PRTG. <http://www.paessler.com/manuals/prtg8/quick_start_guide.htm> (2011 July 16).

Pandey, Choi, Won and Hong (2011). SNMP-based enterprise IP network topology discovery. *International Journal of Network Management* 21 (3) 169-184.

Siamwalla, Sharma and Keshav (1999). *Discovering internet topology*. (Report May). Cornell University.

VMWARE (1995). WMWARE web page, WMRARE Workstation. <http://www.vmware.com/support/pubs/> (2011 June 25).

Zoho. WebNMS web page, WebNMS SNMP API.NET EDITION 4. <http://www.webnms.com/netsnmp/datasheet.html> (2011 August 1).