# Network Monitoring Tool

Shanmugam Veeramani, Lenin Gopal
Department of Electrical/Communication Engineering /Computing
Curtin University of Technology
Miri, Malaysia
Phone: +60 85 443826
E-mail: s.veeramani@curtin.edu.my

**Abstract: Computer Network monitoring tool has been used to study different functions, planning, configuration, and future growth and to manage the networks. Local area networks and wide area networks administrators use different vendor's tools to monitor behavior and their performance. This paper presents Network discovery tool which has been designed to monitor the proposed design. The discovery tool had tested in the real time environment and it works as per expectation, it could able to discover number live host in the design as well as retrieving information about each device. This tool could be used in small size networks.**

***Keywords: Network tools, LAN, Wan, switch, routers and Ip address***

## I. INTRODUCTION

Computer Network discovery is referred to as gathering and extracting relevant information about a computer network being investigated. The computer network consists of various types of network devices such as workstation, routers and switches. The useful information would include the topology of the network and the information of each device in the network. This information is very useful for the network administration as well as planning the configuration of the network when expansion is needed. Besides, the information can be used to aid in discovering network devices that involve in the network problems.

It is impossible, tedious and time-consuming for a network administrator to retrieve this network information manually by checking the network devices one by one or by referring to the network configuration files, as the number of network devices would be large. Therefore the desirability of developing a tool for network discovery is increased.

This paper presents a solution for developing a network discovery tool.

Computer network considered in the paper in Internet Protocol (IP) network and the tool develop is to be used in Local Area Network (LAN).The tool is used to discovery a single subnet in a LAN and has the ability to scan, retrieve and analyze the information obtained from the discovered devices. Hence it makes it easy to discover, map and report on the entire investigated network.

The network discovery tool is required to run under Linux or UNIX operating system and executed in command-line. The tool has been written by using C language. As the tool will be incorporated into a main Graphical User Interface (GUI), it will be able to cooperate with the GUI, receiving input from it and output the relevant information in XML format.

The paper consists of the design and algorithm that had been used in developing the network discovery tool. Flowchart had been used to illustrate in the design. The design tool consists of four parts including subnet calculating based on the input form the users, getting relevant information from the investigated network, topology discovery and output format for the information gathered. Moreover, the paper will discuss and compare between different approaches that can be used to develop the tool.

## II. BACKGROUND

Internet Protocol version 4 (IPv4) address formats. IPv4 consist of 32 bits for source and destination with dotted decimal notation. Four decimal numbers are used in place of 32-bit binary string the binary value of an 8- bit byte is expressed as a decimal numbers between 0 and 255.

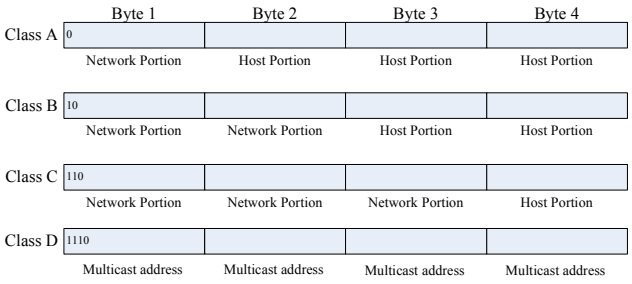


Figure 1. IPV4 Address Format [1]

### A. *Sub netting and the subnet Mask*

Sub netting is a mechanism to share a single network address among two or more networks, sub netting represents an extension of the network and portion of class A,B or C address internally to an organization. Through the use of subnet, the two-level IPV4 address hierarchies of class A, B and C addresses are turned in to three –level hierarchies [1].

To better represent the creation of a subnet by the extension of the network address to determine the host portion of an address.

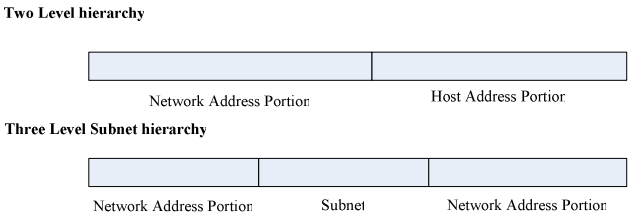


Figure 2. IPV4 Address Format

In computer networks, every subnet has one network address and one broadcast address. Network address is used to identify a network whereas a broadcast address is for broadcasting purposes. Network discovery involving those two addresses as ordinary hosts is not desirable. It is because more than one host residing in the same subnet will respond the network address and it does the broadcast, which is worse than replies from subnet address.

### *B. Utilities for Network Discovery*

**Ping** stands for Packet Internet work Groper, which will invokes a series of internet Control Message Protocol(ICMP) echo message to determine if a device is powered on and operating a TCP/IP protocol stack[1] It is usually used to check if the network device is up and running and also to measure the round trip delay[2]. The device when pinged will respond with an ICMP echo reply, enabling the round trip delay to be determined between the source and the destination devices [1]. Ping done twice on device to prevent getting lost and it has a low overhead. However, pings to dead or non-existence host are expensive, as it will timeout after an interval of 20 seconds [3].

**Trace route**: Traceroute is used to find all the network nodes, which are used for routing from one node to other, which is usually called the source to the destination. It also gives the round trip delay from the source to any node in between the path [2]. It will transmit packets with small TTL (Time to Live) values. TTL is designed to prevent packets from running in loops. Every router that handles a packet subtracts one from the packet's TLL. If the TLL reaches zero, the packet has expired and it's discarded. The trace route utility is normally used to trace a path a packet takes to reach the destination. The advantage of the utility is clearly illustrates the interconnection between source and destination; however it suffers drawback that it will suffer long delays when the destination node doesn't exist.

**Nmap:** Nmap is an open source tool for network exploration and security auditing. It can rapidly scan large networks by using raw IP packets in novel ways to determine available host on the network, operating system fingerprinting on the network as well a dozen of other characteristics [6].

### *C. Algorithms for Network Discovery:*

There are four algorithms appeared in [3], a discovery algorithm generates a topology consists of hosts, routers and subnets. Each item may be associated with additional information such as host name and number of interface at each route [3]. First algorithm uses SNMP and the assumption is that every node in the network implements SNMP. It can retrieve device information quickly and complete if the device is SNMP capable, drawbacks is it fails to discovery nodes that don't support SNMP.

The second algorithm uses DNS (Domain Name System) zone transfer with broadcast ping to get a list of all network devices in the network then it pings to verify that these network devices exist and uses the algorithm for subnet guessing [3]. A DNS is a database that contains of records of the network devices that are having same suffix domain but this algorithm fails to discover a network if broadcast ping and zone transfer is not permitted. The third algorithm uses the DNS zone transfer with addition of trace route, which replaces expensive subnet guessing technique. This algorithm is faster and more efficient than algorithm 2, but it has problem of correctness where the subnet mask determined in the algorithm might not be correct when all the machines in a subnet use IP address at the high end of the subnet's address space. The discovered mask would be longer than the actual one as the common initial bit string is longer [3]. The fourth algorithm uses only traceroute and ping to determine topology. It can be used practically in any network. However, it involves guessing valid addresses in a domain, which subsequently slow down the algorithm.

## III. NETWORK DISCOVERY TOOL DESIGN SPECIFICATION

In this design method uses an open-source tool, named Nmap, for discovering the information of the devices such as MAC address, vendor type, underlying operating system, device type and protocol used. However, SNMP is used for topology discovery this provide valuable information such as retrieving device's ARP table. This proposed topology discovery will only be executed if there is managed switch present in the list of discovered host. Unmanaged switch would be transparent a plug and play device that will not be assigned IP address. A managed switch is a switch that has been assigned the IP address. The proposed design flowchart illustrates various functions performed by system in sequence.

### *A. Function Subnet Calculator*

The functions of the design are subnet calculator, host discovery, topology and reporting function, which will output in XML format. The first function will be implemented when the GUI is executing the computer network discovery tool is the subnet calculator functions shown in Figure –III-2. The input to the function will be the user inputs that are sent by the GUI, which are IP address and subnet mask. The GUI will only check if the inputs are numeric, hence the validation needs to be done in the function to ensure that the user inputs are valid. In addition to validation process the function ensure the numeric value is within a valid range which is form 0 to 255 only, invalid inputs will trigger the function to send warning message to GUI and stop the tool immediately until the GUI sends next available inputs.

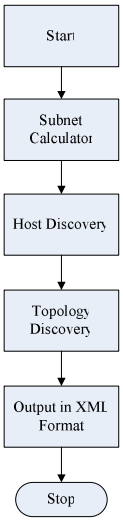


Figure 3. Proposed Design Flowchart

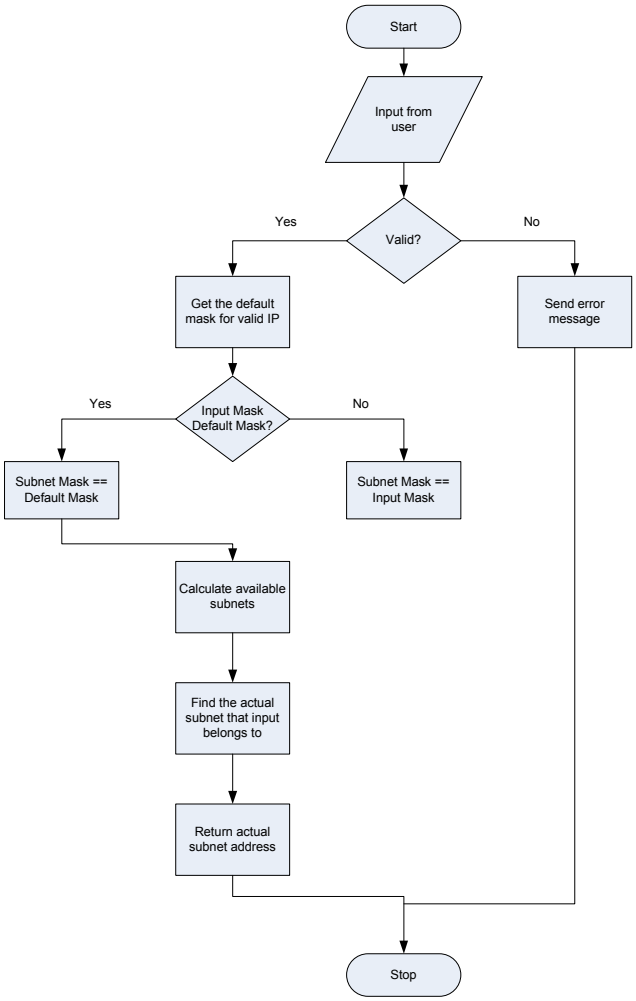


Figure 4. Subnet Calculator Function Flowchart

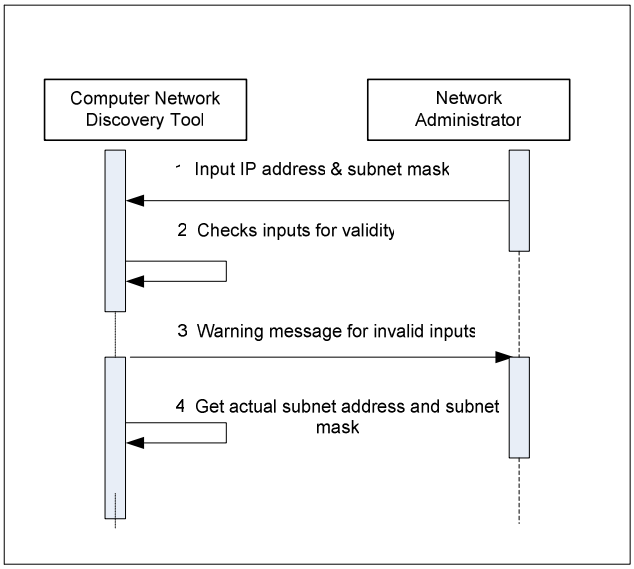


Figure 5. Sequence Diagram for Subnet Calculator

### B. *Host Discovery Function*

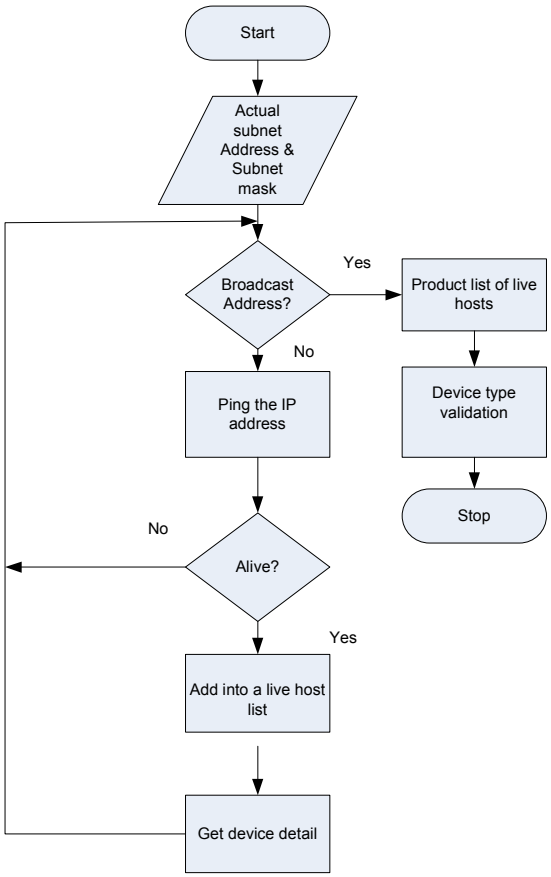


Figure 6. Host Discovery function flowchart

Using the subnet address and subnet bits for the subnet calculator functions, the host discovery function is then being executed. This function basically tests connectivity of all available hosts in the subnet address. Nevertheless, the function will not treat the network address and the broadcast address as live host even if there are replies from those addresses. Figure III-4shows the flowchart of the host discovery function. This function will keep on looping until the broadcast address is encountered. A text file with subnet address as well as a list of lived-host's IP address is produced for the link-quality-testing tool. Before the function stop, the function will check if all hosts have device identity as shown.

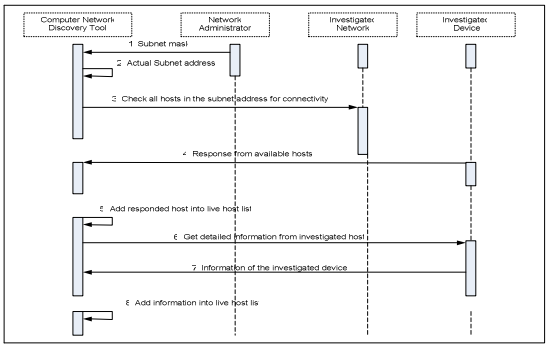


Figure 7. Sequence Diagram of Host Discovery function

During the looping, each available host address is tested for its connectivity by using Nmap utility, a open –source utility that is available on Linux platform, with the option –sp and –n provide subnet address and subnet bits as the arguments. –n option is basically disable DNS resolution on the active IP address that responds to the scan. –sp option is used to perform ping scan, which an ICMP echo request and a TCP packet are sent to port 80 by default. When unprivileged user execute the tool, only SYN packet being sent using connect () call. Therefore, the MAC address of a device will not be retrieved .MAC address will only be retrieved if the tool is executed by privileged user such as network administrator.

### C. *Function Topology Discovery*

Topology discovery function is a process finding interconnection between a managed switch with all the clients. Figure-III-6, clearly illustrates the flowchart of the function. The function, however does not perform if there is no managed switch discovered in the live-host list. The reason is the network being investigated is a single-subnet. All the devices that are sitting on the same line and the sequence are arranged by the IP address of each host, except for managed switch.

The reporting function will take the live-host list as well as switch live-host, if any, to produce output in XML format to the GUI. The output will be aware of the existence of switch live-host list as the syntax for producing output for switch live-host list will be different from the live-host list.

## IV. IMPLEMENTATION

The computer network discovery tool is implemented using C language on Linux platform. There are many other programming languages available such as java and perl.C language had been chosen because of its ease to use, compile,

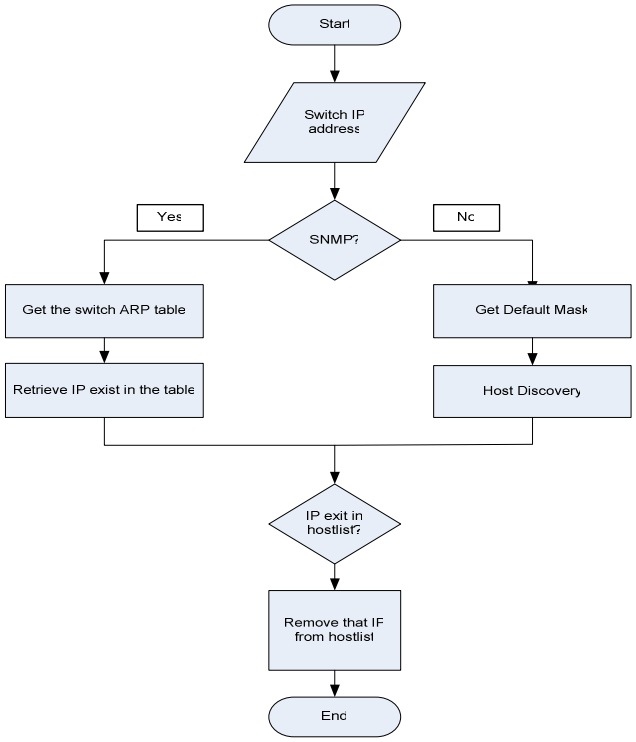


Figure 8. Topology Discovery Function flowchart

debug and program. The tool runs from the command-line, which will be issued by the GUI, where two arguments must be specified.

Topology<IP address> <subnet mask>

The tool will execute exactly as the design specification. Actual subnet where the IP address belongs will be calculated based on the subnet mask. Host discovery function will be performed by sending ICMP echo request to all the hosts in the subnet except for the network address and broadcast address. For each host discovered, detailed information is gathered by using the Namp utility. Topology discovery function will be performed if there is a managed switch present during host discovery function to find the interconnection between the hosts with the managed switch. Finally, the result from both discovery functions will be used to produce out put in XML format to GUI, where the file named network.xml will be placed in the path /usr/.

## V. CONCLUSIONS

The computer Network discovery tool had been successfully designed and implemented with the following characteristics such as fast, accurate, complete and efficient. The tool can able to detect the existence of live hosts in the network and retrieve information about the devices. Output is produced in the XML format, for the GUI and the purpose is to map and display. There are many existing approaches are available, however, each having its pros and cons. This tool could be used in a small networking environment to gather, various information about the network devices and topology. The tool will be extremely useful for the network administrator.

## REFERENCE:

[1] Gilbert Held, Managing TCP/IP Networks, John Wiley & Sons LTD, United Kingdom.

[2] Christos Gkhantsidis. Experiment and Learn to Discover Network Topology. From http://www.cs.cornell.edu

[3] R.Siam Walla, R.Sharma, S.Keshav. Discovering Internet Topology

[4] From http://www.cs.cornell.edu/skeshav/papers/discovery.pdf

[5] David T. Stot.Layer-2 Path Discovery Using Spanning Tree MIBs, Avaya Labs Research,Avaya Inc, Basking Ridge, Nj 2002.

[6] Yuri Breitbart, Minos Garofalskis, Cliff Marin, Rajeev Rastogi, S.Seshadri, Avi Silberschatz. Toplology Discovery in Heterogenious IP Networks.

[7] Insecure.org. http://www.insecure.org/nmap/data/nmap_manage.html

[8] ICMP ,Retrieved http://www.freesoft.org/CIE/Topics/81.htm