ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Survey Paper on Protocol Based Network Management System

Guduru Madhuri
M.Tech Student
Department of Information Technology,
Gokaraju Rangaraju Institute of Engineering & Technology,
Hyderabad, India.

Dr. Y. Vijayalata
Professor & HoD,
Department of Information Technology,
Gokaraju Rangaraju Institute of Engineering & Technology,
Hyderabad, India.

Abstract
Network Management System is a one of the main concern for every network administrator. Implementing network is a big deal for every organization but maintaining it also very important task for organization as well as Administrator. There are number of services working on network to provide required resources to customers and users. If any one of the service down, then it effects to network operations. Admin must know about fall of time and then only they can provide some backup for management. This article is going to explore some basic concepts in network, protocols used in network and protocols or services for monitoring network management.

Keywords: SNMP[2], Wireshark[4], TCP, IP[1].

Introduction
One of the main concerns for any organization would be 100% network up time. If that's not achieved then the organization would lose faith in its clients and may experience loss in the business. It's the responsibility of the IT department to take care of the network. The only goal of the IT department is to maintain 100% up time with maximum throughput. As network deals with various physical devices, it's hard to identify which devices are faulty or experiencing troubles. So, there should be an alternative to keep the network up and running. It can be done by closely monitoring the networking devices. But, as it's not possible to keep an eye on the devices performance, the vendors uses robust material inside and outside of a device, it's a rare event for a networking device to go down.

Study was conducted on how a network outage could occur, what would be the impact of network outage on an organization. This paper discusses the ways to prevent the network outageand to minimize the impact of a network outage in case of any. There might be different reasons for a network outage to occur; they include misconfigurations, faulty cables, hardware failures…etc. The efficient way to monitor the network is to have network monitoring tool in the network. By implementing network monitoring tools IT department can monitor the health of the network (network contains all the networking devices including printers, PCs, networking devices, switches, routers, wireless access points…etc.), flaws in the network and bandwidth utilization in the network. One more advantage with these networking tools is that the administrator can get email alerts direct to his inbox when something wrong goes in the network.

Introduction to Networks
Network: A group of objects/things/people that can interact within that group is called as a network. It can also define as Interconnection two or more computers. Ex: A group of computers – computer network, a group of people – Human network.

In IT (Information technology) world a group of computers connected in a way so that they can all communicate with each other. There are many advantages exists of Networks. One of the main advantage is "resource sharing". So, what exactly is resource sharing? In any organization there would be need of printers, scanners, and storage devices. Based on the employees, every organization purchases those devices and they won't purchase those many as

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

employees. Limitedly organization purchases them. When an employee wants to access them then they should manually connect their PC to that device and access it. Let's consider printing a paper everyone has to go to the printer and connect it to their PC and should take the print out. Otherwise they need to get the printer to their cabinet to get prints. If they have any removable storage device like pen drives or any Optical media then they can use to copy their data and connect them to the printer connected system and get prints. But these all are time and work consuming processes. But, with a properly implemented network everyone in the same network can access any network enabled device right from their cabin, and any number of users can use it simultaneously all tasks will queued and server according to priority. By resource sharing the cost of such devices which will be needed by everyone, would be gradually reduced as a single resource can be shared multiple users.

IP[1] (Internet Protocol):

In a network environment the whole communication takes place with a medium called "IP address". An IP address is a logical address assigned to each network enabled device. An IP address is of 32 bit address separated into 4 parts (octets), 8 bits each. In a network all computers IP addresses are identified with a same network prefix. That network prefix is used to identify network of that device. Subnet mask is term which is used to calculate the network ID and broadcast ID of a network. In any network of IPs the first and last IPs are reserved for network ID and broadcast IDs respectively. Here subnet mask is used for identifying network id and broadcast id of a network. Except Network ID and Broadcast ID all other IP addresses are known as usable or free IPs that can be assigned to hosts in the network. All the hosts within that range are said to be in same network, and can communicate to each other through their IP address.

Each IP address contains two portions one is Network Portion and other is Host Portion. Here network portion is used to identify to which network that computer is belongs to and host portion is used to identify that particular computer in that network. Network Portion must be same for all computers in same network and Host Portion must be unique in all computers in same network. This network and Host portions are identified using Subnet Mask.

While configuring an IP address to any device 3 fields are mandatory they are IP address, subnet mask and default gateway.
Example of 3 fields of IP address:
IP address : 192.168.1.1
Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.100

In the above example the IP address is the actual address (logical name) of a device which is used to uniquely identify it in a network. Subnet mask is used to find out the additional information of network like Network ID, Broadcast ID and usable IPs in that network. Subnet mask is decimal notation of binary digits. Default Gateway is used to identify other networks entry point from this network. It means if a computer wants to communicate with other computer then it will communicate with that directly if destination computer is in same network. If it is presented in other network then through Default Gateway they will communicate.

__ __ __ __ __ __ __ __ . __ __ __ __ __ __ __ __ .
__ __ __ __ __ __ __ __ . __ __ __ __ __ __ __ __
8 bit fields separated by 4 octets
Each octet will be ranging from 0 – 255
7 6 5 4 3 2 1 0 ➔ 12864 32 16 84 2 1
Binary digits decimal numbers

Any digit can be filled up with 0's and 1's.
1 1 1 1 1 1 1 1 ➔ 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 ➔ 255
0 0 0 0 0 0 0 0 ➔ 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 ➔ 0

When a field in subnet mask contains 1s then it's said to be a network portion, and other portion is host portion. So, in the example above first 3 octets are completely filled by all 1's that means they are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

network bits and last octet is with all 0's which means it's for hosts bits. To determine how many IP addresses available in that network calculate the total number of hosts in that network. To calculate the number of hosts in a network we can use the formula 2^h (2 to the power of h) where 'h' is the number of host bits. So in our above example 8 bits from the last octet are used for host bits then, no. of hosts will be 2 to the power 8 that is 256 (0 to 255). Usable IP addresses are only 254 because first and last IP addresses are reserved for Network ID and Broadcast ID.

Manual IP address fields must not be changed where the octets are completely filled. That means the first 3 octets are completely filled so they will remain same throughout the network. Hence, the no. of hosts will from 192.168.1.0 – 192.168.1.255, where 192.168.1.0 is network ID and 192.168.1.255 is broadcast IDs of the network. The network ID is used to identify a network where the broadcast is used to send out broadcast messages in the network.

Protocols

Protocol is a set of rules and regulations for communication in the network. Every computer has to follow some protocols for performing network operations. In TCP / IP Protocol suite they have defined number of protocols. Below is the brief description about major protocols in that suite.

TCP: Transmission Control Protocol is a transport layer or Host to Host layer protocol used for ensuring data delivery. It maintains logical connection between sender and receiver till the transaction completes.

IP: Internet Protocol defines the logical addressing in the network to enable communication between computers in the network.

SMTP [5]: Simple Mail Transfer Protocol is used for sending mails between authenticated users.

POP3 [6]: Post Office Protocol version3 is used to receive mails to any client application of mail server.

ICMP [7]: Internet Control Messaging Protocol is for sending and receiving controlling messages between computers in the network (ping [13]).

FTP [8]: File Transfer Protocol is used to transfer files between computers in network.

HTTP [9]: Hyper Text Transfer Protocol is a web based protocol for transferring hypertext markup pages between server and client.

DHCP [10]: Dynamic Host Configuration Protocol is used to assign IP addresses to computers automatically in the network.

DNS [11]: Domain Name System is for resolving fully qualified domain names to IP addresses and vice versa.

Addressing

For identifying a particular device in the network we need to have a proper addressing method. In computer networks there are 3 addresses for identifying computer, network and service. Those are

- IP Address
- MAC Address
- Port Number

IP [1] Address: It is a logical address used to identify a network of a computer as well as computer in that network.

MAC Address: Media Access Code or Control is a physical unique address which is assigned to each and every LAN Card (Ethernet Adapter) in the computer. It is a 48 bit binary number converted to 12 digit hex decimal. The following is the example for the MAC Address
00-1C-26-E8-79-B3

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

It is like IMEI number of our phone. It was written by Manufacturer of the LAN card and cannot be modified physically

To check our MAC Address use the following commands from command prompt
Windows: getmac
Linux : ifconfig

Port Number: Port number or address is used to identify a service in our computer. In Networks every computer can host more than one service. To identify those services individually we need to use this address. These port numbers are defined and reserved by Internet Authorities in world. The following are some of the port numbers.

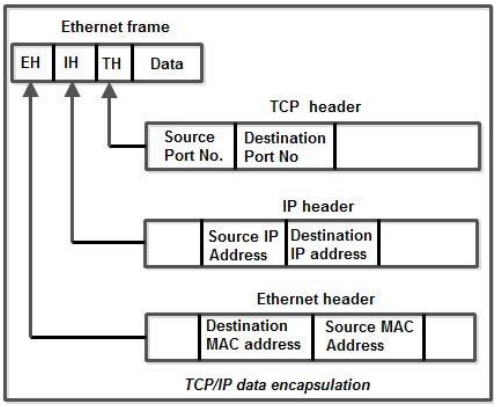
Total Port Numbers: 655536 and Reserved Port Numbers are 0 to 1023.

Service Name	Port Number
HTTP	80
HTTPS	443
SMTP[5]	25
Telnet	23
FTP [8]	20,21
DHCP [10]	67,68
DNS [11]	53
POP3 [6]	110

When network resources are in usage, all of these three addresses are used to locate computer and service in the network.

For Example www.google.com, if you type this in browser then our computer thinks you need http[9] service so the packet is destination was 80 and Using DNS [11] it resolves the IP address which is used to locate Google network. MAC address is resolved by ARP protocol to identify a computer in network.

The following image shows Ethernet Frame with TCP, IP, and Ethernet Headers.



SNMP[2] (Simple Network Management Protocol)

A large part of being a system administrator is collecting accurate information about your servers and infrastructure. There are a number of tools and options for gathering and processing this type of information. Many of them are built upon a technology called **SNMP**.

SNMP[2] stands for simple network management protocol. It is a way that servers can share information about their current state, and also a channel through which an administrator can modify pre-defined values. While the protocol itself is very simple, the structure of programs that implement SNMP can be very complex.

This paper, introduces the basics of the SNMP protocol. Functionality will be same as the way that the protocol is typically used in a network, the differences in its protocol versions, and more.

Basic Concepts

SNMP is a protocol that is implemented on the application layer of the networking stack (click here to learn about networking layers). The protocol was created as a way of gathering information from very different systems in a consistent manner. Although it can be used in connection to a diverse array of systems, the method of querying information and the paths to the relevant information are standardized.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There are multiple versions of the SNMP protocol, and many networked hardware devices implement some form of SNMP access. The most widely used version is SNMPv1, but it is insecure in many ways. Its popularity largely stems from its ubiquity and long time in the wild. Unless you have a strong reason not to, it is recommended to use SNMPv3, which provides more advanced security features.

In general, a network being profiled by SNMP will mainly consist of devices containing SNMP **agents**. An agent is a program that can gather information about a piece of hardware, organize it into predefined entries, and respond to queries using the SNMP protocol.

The component of this model that queries agents for information is called an SNMP **manager**. These machines generally have data about all of the SNMP-enabled devices in their network and can issue requests to gather information and set certain properties.

SNMP[2] Managers

An SNMP manager is a computer that is configured to poll SNMP agent for information. The management component, when only discussing its core functionality, is actually a lot less complex than the client configuration, because the management component simply requests data.

The manager can be any machine that can send query requests to SNMP agents with the correct credentials. Sometimes, this is implemented as part of a monitoring suite, while other times this is an administrator using some simple utilities to craft a quick request.

Almost all of the commands defined in the SNMP protocol (we will go over these in detail later) are designed to be *sent* by a manager component. These include GetRequest, GetNextRequest,GetBulkRequest, SetRequest, InformRequest, and Response. In addition to these, a manager is also designed to *respond to* Trap, and Response messages.

SNMP Agents

SNMP agents do the bulk of the work. They are responsible for gathering information about the local system and storing them in a format that can be queried. Updating a database called the "management information base", or **MIB**.

The MIB is a hierarchical, pre-defined structure that stores information that can be queried or set. This is available to well-formed SNMP requests originating from a host that has authenticated with the correct credentials (an SNMP manager).

The agent computer configures which managers should have access to its information. It can also act as an intermediary to report information on devices it can connect to that are not configured for SNMP traffic. This provides a lot of flexibility in getting your components online and SNMP accessible.

SNMP agents respond to most of the commands defined by the protocol. These include GetRequest,GetNextRequest, GetBulkRequest, SetRequest and InformRequest. In addition, an agent is designed to send Trap messages.

Understanding the Management Information Base

The most difficult part of the SNMP system to understand is probably the **MIB**, or management information base. The MIB is a database that follows a standard that the manager and agents adhere to. It is a hierarchical structure that, in many areas, is globally standardized, but also flexible enough to allow vendor-specific additions.

The MIB structure is best understood as a top-down hierarchical tree. Each branch that forks off is labeled with both an identifying number (starting with 1) and an identifying string that are unique for that level of the hierarchy. You can use the strings and numbers interchangeably.

To refer to a specific node of the tree, you must trace the path from the unnamed root of the tree to the node

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

in question. The lineage of its parent IDs (numbers or strings) are strung together, starting with the most general, to form an address. Each junction in the hierarchy is represented by a dot in this notation, so that the address ends up being a series of ID strings or numbers separated by dots. This entire address is known as an object identifier, or **OID**.

Hardware vendors that embed SNMP agents in their devices sometimes implement custom branches with their own fields and data points. However, there are standard MIB branches that are well defined and can be used by any device.

Standard branches discussed in this paper will be under same parent branch structure.

This branch defines information that adheres to the MIB-2 specification, which is a revised standard for compliant devices.

The base path to this branch is:
1.3.6.1.2.1

This can also be represented in strings like:
iso.org.dod.internet.mgmt.mib-2

The section 1.3.6.1 or iso.org.dod.internet is the OID that defines internet resources. The 2 ormgmtthat follows in our base path is for a management subcategory. The 1 or mib-2 under that defines the MIB-2 specification.

This is a great resource for familiarizing yourself with the MIB tree. This particular page represents the connecting nodes at the junction those are discussed in the paper. You can check what is further up and down the tree by checking out the "superior" and "subsidiary" references respectively.

Another similar tool is a SNMP Object Navigator provided by Cisco. This can be used to drill down into the hierarchy to find information you need. A similar tree is provided by Solar Winds.

Basically, if we want to query our devices for information, most of the paths will begin with 1.3.6.1.2.1. You can browse the tree interfaces to learn what kind of information is available to query and set.

SNMP Protocol Commands

One of the reasons that SNMP has seen such heavy adoption is the simplicity of the commands available. There are very few operations to implement or remember, but they are flexible enough to address the utility requirements of the protocol.

The following PDUs, or protocol data units, describe the exact messaging types that are allowed by the protocol:

Get: A Get message is sent by a manager to an agent to request the value of a specific OID. This request is answered with a Response message that is sent back to the manager with the data.

GetNext: A GetNext message allows a manager to request the next sequential object in the MIB. This is a way that you can traverse the structure of the MIB without worrying about what OIDs to query.

Set: A Set message is sent by a manager to an agent in order to change the value held by a variable on the agent. This can be used to control configuration information or otherwise modify the state of remote hosts. This is the only write operation defined by the protocol.

GetBulk: This manager to agent request functions as if multiple GetNext requests were made. The reply back to the manager will contain as much data as possible (within the constraints set by the request) as the packet allows.

Response: This message, sent by an agent, is used to send any requested information back to the manager. It serves as both a transport for the data requested, as well as an acknowledgement of receipt of the request. If the requested data cannot be returned, the response

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

contains error fields that can be set with further information. A response message must be returned for any of the above requests, as well as Inform messages.

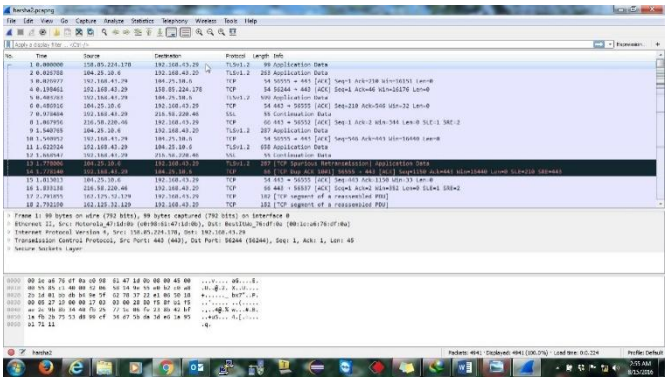
Trap: A trap message is generally sent by an agent to a manager. Traps are asynchronous notifications in that they are unsolicited by the manager receiving them. They are mainly used by agents to inform managers of events that are happening on their managed devices.

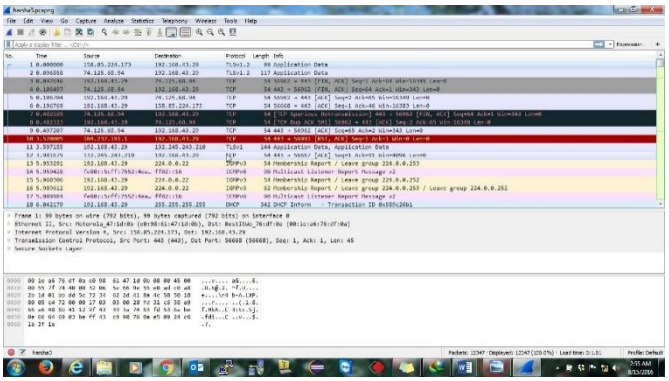
Inform: To confirm the receipt of a trap, a manager sends an Inform message back to the agent. If the agent does not receive this message, it may continue to resend the trap message.

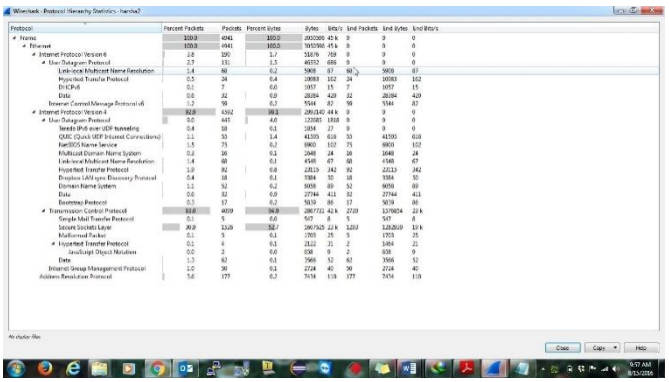
With these seven data unit types, SNMP is capable of querying for and sending information about your networked devices.

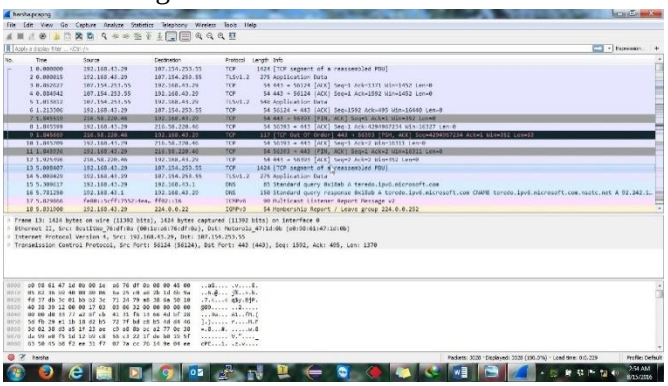
Network Monitoring using Wireshark[4]

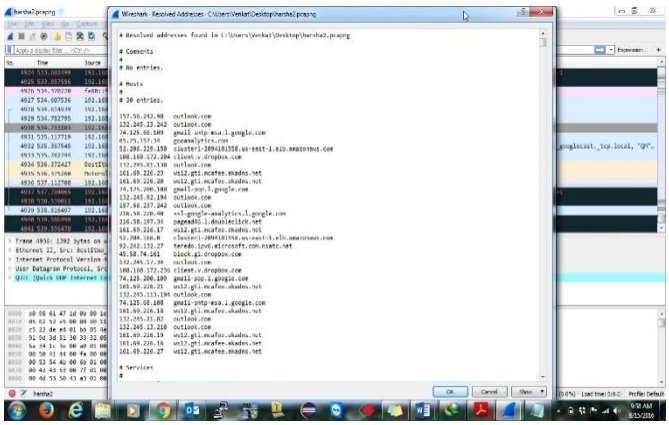
The following images show how we can monitor our network using Wireshark Tool.



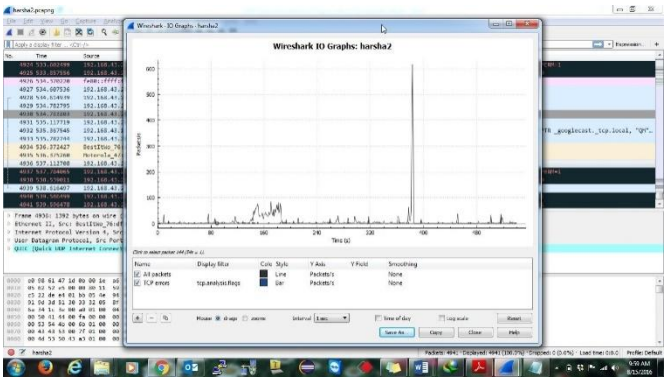








ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



The following are the different types of protocols existed in traffic which I have captured.

HTTP: Hyper Text Transfer Protocol is used for transferring markup pages (Web pages) from server to client. It will be done with 80 / 443 Protocol numbers.

FTP: File Transfer Protocol is used to transfer files from server to clients with 20 and 21 default port numbers.

DNS: Domain Naming System is a protocol used for resolving fully qualified domain names to IP addresses with 53 port number.

TCP: Transmission Control Protocol is a transport layer protocol used for transferring data from source to destination with reliability.

ICMP: Internet Control Messaging Protocol used to transfer ping echo requests and replies.

DHCP: Dynamic Host Configuration Protocol is used assign IP addresses from a pool in the server to client. DHCP uses 67 and 68 Port numbers.

UDP: User Datagram Protocol is used for connection less transmissions in the network. It is also a transport layer protocol.

ARP: Address Resolution Protocol is used to resolve MAC addresses from known IP addresses.

SMTP: Simple Mail Transfer Protocol is used for transferring mails from one user to another.

TLS / SSL: Socket Secure Layer used for transferring data securely using encryption.

Conclusion

Every System Engineer or Network Engineers goal is to protect the network from all kinds of issues. SNMP is the one of very useful protocol to monitor network. It monitors the network devices or services using different protocols or methods. Wireshark is also one of very useful protocol for network administrators which will monitor protocol traffic in the system or network. Nagios, OTRS, and SolarWinds Network Monitor tool, all these are free services which are used to monitor and report network status of any large network.

References

[1] V. Beal, "What is an IP address? Webopedia definition," [Online]. Available: http://www.webopedia.com/TERM/I/IP_address.html. Accessed: Oct. 13, 2016.

[2] IncDigitalOcean™, "An introduction to SNMP (simple network management protocol)," DigitalOcean, 2014. [Online]. Available: https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol. Accessed: Oct. 14, 2016.

[3] Microsoft, "What is SNMP?," 2016. [Online]. Available: https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx. Accessed: Oct. 14, 2016.

[4] T. Wilson, "How to use Wireshark to capture, filter and inspect packets," 2014. [Online]. Available: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/. Accessed: Oct. 14, 2016.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] [Online]. Available: https://www.ietf.org/rfc/rfc0821.txt. Accessed: Oct. 14, 2016.

[6] Microsoft, "POP3," 2016. [Online]. Available: http://windows.microsoft.com/en-in/windows-vista/pop3-smtp-and-other-e-mail-server-types. Accessed: Oct. 14, 2016.

[7] Microsoft, "ICMP," 2016. [Online]. Available: https://support.microsoft.com/en-us/kb/170292. Accessed: Oct. 14, 2016.

[8] V. Beal, "What is FTP - file transfer protocol? Webopedia definition,". [Online]. Available: http://www.webopedia.com/TERM/F/ftp.html. Accessed: Oct. 14, 2016.

[9] "HTTP - Hypertext transfer protocol overview," 1996. [Online]. Available: https://www.w3.org/Protocols/. Accessed: Oct. 14, 2016.

[10] Microsoft, "What is DHCP?," 2016. [Online]. Available: https://technet.microsoft.com/en-us/library/dd145320(v=ws.10).aspx. Accessed: Oct. 14, 2016.

[11] M. Brain and S. Crawford, "How domain name servers work," HowStuffWorks, 2000. [Online]. Available: http://computer.howstuffworks.com/dns.htm. Accessed: Oct. 14, 2016.