International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 3, Issue 2, February 2014 ISSN 2319 - 4847

IP Address Conflict Resolution and Configuration Theft Management

Mr. Kapil Morey[1], Prof. Sachin Jadhav[2]

[1] M.E.Student, Computer Engineering
Padmashri Dr.V.B. Kolte College of Engineering, Malkapur

[2]Assistant Professor , Computer Science and Engineering
Padmashri Dr.V.B. Kolte College of Engineering, Malkapur

Abstract

IP conflict occurs when two different devices in local network are using the same IP address. The main aim is to resolve the IP address conflicts and ensure consistent network functionality with the aid of the IP Address Manager and basically eliminating the need to maintain large spreadsheets that were used till date to manage the IP addresses. Instead, we should make use of a centralized IP address management solution that scans the network for IP address changes and maintains a static list of IP addresses, ensuring that one can get rid of the downtime caused by the IP address conflicts. It undoubtedly enhances the record-keeping (configuration) feature. By making sure that the IP address conflicts are drastically reduced, it improves the network performance by letting the devices continue the normal execution without losing network connection by reducing the obvious downtime. It tracks the users having changed the IP address and easily identifies non-responsive IP addresses to optimize your IP space. It also has an additional feature of theft management of various configurations on the system. The filtration technique retrieves requested configuration of particular client machine by using its IP address.

Keywords: IP Address, DHCP Server, Configuration Management, IPv6.

1. INTRODUCTION

Unpredictable and generally undesirable things tend to happen when multiple devices attempt to use the same IP address [1]. An address conflict scenario might go like this device A starts up and uses IP address 10.88.80.10 Other devices establish and carry on communications with Device A. Device B has incorrectly been configured to also use 10.88.80.10 Device B starts up Existing communications to Device A may be disrupted and re established with Device B (though not necessarily). New communications initiated by other devices could go to Device A or Device B (or may be established and disrupted again).In such situations, it can be difficult to determine that there even is an address conflict situation, and where the offending device is located. To further complicate the problem, there is no universally implemented mechanism for detecting IP address conflicts. A Windows PC typically displays a pop-up message if it hears a response to gratuitous ARPs sent at start up. Some embedded devices follow the Windows behavior, but in general there is no common behavior for embedded devices. It is desirable to have a common IP address conflict detection mechanism for Ethernet / IP devices. A common mechanism will enable consistent behavior for Ethernet / IP devices, and help the user in diagnosing address conflict conditions.

2. LITERATURE SURVEY

2.1 How IP Address Conflicts Cause Problems

IP address conflicts do not have a major impact on layer 3 or layer 7 communications (where most TCP/IP communications take place), but on the lower layer 2 protocols that layer 3 and above depend on[4][1]. Once packets arrive to their destination network, or the subnet that the target system resides on, an ARP request is generated asking which system has the target IP address. If a routing or switching device that stores ARP information has this information cached in its ARP cache, that data is automatically used for decision making. If not, the first system responding to the request stating that it has the target IP address is added to the cache, and then packets are then forwarded to that host using its MAC (Media Access Control) address. Depending on system and network states or utilization, different systems may win the ARP response race, causing packets to be sent to one system at one time, and the other system other times. For IP communications this kind of reliability issue is unacceptable.

2.2 Static IP Address

A static IP address is an IP address that was manually configured for a device, verses one that was assigned via a DHCP server [8]. A static IP address is called static because it does not change. The public IP address assigned to the routers of most home and business users are a dynamic IP address. Larger companies usually do not connect to the Internet via dynamic IP addresses and instead have static IP addresses assigned to them which do not change. In a local network like in your home or place of business, where you use a private IP address, most devices are probably configured for DHCP and thus use dynamic IP addresses. However, if DHCP is not enabled and you've configured your own network information, you're using a static IP address

3. SYSTEM DESIGN

The Design architecture depicts the project design model. The server shows two Modules - IP address management and system configuration to process the data received from client. The database part comprises of the two databases of IP and Configuration which have a communication interface of Data Abstraction Layer.

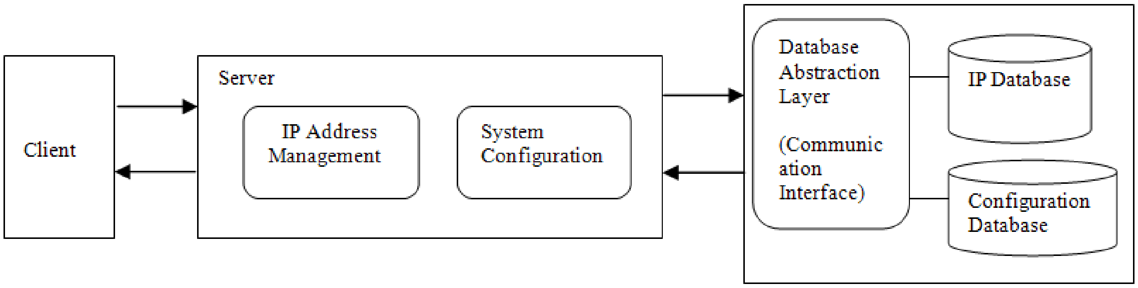

Figure 1 Design Architecture

4. MATHEMATICAL MODEL

4.1 Set Theory

Problem Description**:**

Let S be the Server set.

Let C be the set of clients such that

C = {C1, C2, C3,…Cn}

Where,

C1 represents the client machine 1.

C2 represents the client machine 2. .

Cn represents the client machine n

Let I be the set of IP address assigned to the client

4.2 Graphical Model

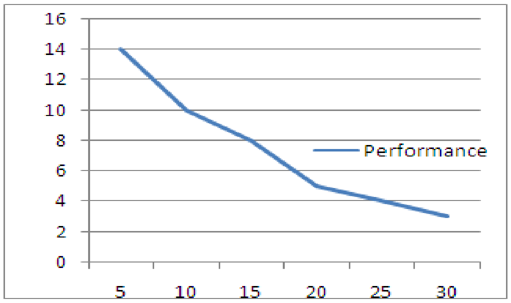

Figure 2 Performance Degradation

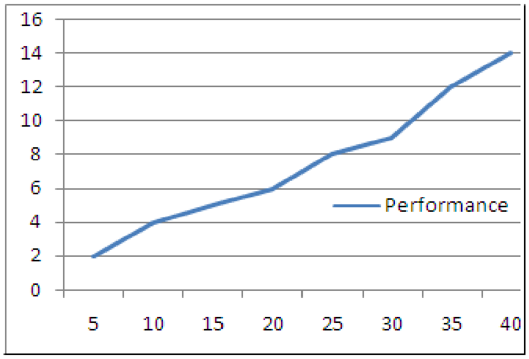

Figure 2 Performance Upgradation

Let N be the set of no. of client machines in the system.

- Let P be the degree of Performance depending on no. of clients.

- In traditional IP conflict management, as the no. of clients in the network goes on increasing then the degradation of performance is seen.
- In our project environment as the no. of client machines goes on increasing the scope of performance of the system also goes on increasing.
- Application on server side for validating the IP Address and Configuration.
- SQL Database for maintaining the IP Address and Configuration.
- Database Abstraction Layer for communication.
- The main aim is to minimize the IP address conflicts and ensure consistent network functionality with the aid of the IP Address Manager and basically eliminating the need to maintain large spreadsheets that were used till date to manage the IP addresses.
- The project aims at developing an application which manages the IP Addresses and system configurations and detects any conflict in assignment of IP Address and any changes or updating in the system configuration.
- The changes in the configuration of the computer system are detected instantly by the application and thus ensure theft management.
- We can also find the configuration of particular computer system by using its IP Address details.
- If the user on client machine assigns an IP address then it is sent to server for checking any conflict in the database.
- If conflict occurs then server/administrator will assign a feasible IP address to the client machine or display a warning message to client.

5. ADVANTAGES, LIMITATIONS AND APPLICATION

5.1 Advantages

- The interruption of the internet in the system network is avoided
- Useful in large client system.
- Manages the configuration of client machines.

5.2 Limitations

- Cannot be used in IPv6.

5.3 Applications

- IP Management in large business firms.
- Theft management of configuration in the network system of private firms.
- Useful for tracing the configuration of the system by using its IP address.
- Multinational Companies can use this in their network system.
- Researchers and academics use this technology for network analysis.

6. CONCLUSION

Although there are more advantages to DHCP & Dynamic IP addresses, there are still applications where they need to have Static IP. Large infrastructures usually not connect to internet via Dynamic IP addresses and instead have Static IP addresses assigned to the systems. By doing this the organization can keep track of log-info and can also handle theft management.

References

[1] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol. RFC-2401, IETF, NOV.2003.
[2] E. Horowitz, S. Sahni : Fundamentals of Computer Algorithms, Computer Science.
[3] “IP Addressing and Services”, Cisco IOS IP configuration Guide, Release 12.3.
[4] E.C. Lupu, M. Sloman : Conflict Analysis for Management Policies. Proc. 5th IFIP/IEEE.
[5] J. Jason : IPSec Configuration Policy Model, Internet Draft, March 2006.
[6] R. Pereira, P. Bhattacharya : IPSec Policy Data Model. Internet Draft, Feb 2007.
[7] M. Gen, R. Cheng: Genetic Algorithms and Engineering Optimization. Wiley- Interscience, 2000. –
[8] Computer Networks – Andrew S. Tanenbaum
[9] http://ipwatchd.sourceforge.net/
[10] http://www.geatbx.com/index.html/