NAT and DHCP Support for Wi-Fi Access Point

Chandana J N[1], S Mercy[2]

[1]*Student, M.Tech-Computer Network and Engineering, Department of IS&E, Bangalore Institute of Technology, Bangalore, Karnataka, India*
[2]*Assistant Professor, Department of IS&E, Bangalore Institute of Technology, Bangalore, Karnataka, India*

Abstract - *The project enables Access Point operator to conserve internet routable IPv4 addresses by providing the security for isolation the users with IP's from external network. AP will perform NAPT for clients to which IPv4 address is assigned by the AP. It also provides secured and fast network to the users.*

***Key Words*: Wi-Fi, Access Points, Controller, DHCP, NAT, AAA, WLAN, EMS**

1. INTRODUCTION

With the increasing tendency of wireless devices and the extensive use of internet has created high demand for security and privacy in the communication channels. Wi-Fi networks are important challenges for network administrators. It allows the user to communicate with one other through LAN without wired connections. By describing the behavior of Wi-Fi users and understanding the Wi-Fi network usage model, it is useful for identifying the management problems so that network administrator can manage Wi-Fi network more efficiently. Currently in Wi-Fi architecture Dynamic Host Configuration Protocol (DHCP) will assign the IP address dynamically to each user to access the network.

2. Existing System

In the existing system DHCP network protocol is used on IP network where each host on the network is automatically assigned an IP address and other information by DHCP server so that they can communicate effectively with other endpoints.

In the existing system the WLAN can be in 3 different bearer modes:

i. LBO-Local Break Down
ii. L2GRE/L2TP

In the existing system they are mainly two features to be considered that is LBO and L2GRE/L2TP.In LBO feature IP is assigned by the DHCP and internet to each user. In L2GRE/L2TP feature AP is connected to WAG followed by DHCP server and internet, for each user the IP is assigned by the DHCP server. For monitoring and configuration of the access point the controller is been used.

3. Methodology

The proposed system will provide the users with very good network connectivity. The external DHCP server used in the existing system to assign the IP's to the User Entity(UE) but in the proposed system the AP will act as the NAT server and assign the IP's to the user's based on their MAC address.

3.1 Introduction to Wi-Fi Architecture

Wi-Fi solution provides good services to increase network capacity, imporved cost efficiency and to deliver an enhanced user experience. It facilities Wi-Fi user to use WLAN access networks to access the internet and other services. Wi-Fi software system basically consists of Access Points (AP's) and Controller (cWLC) along with servers such as Accounting Server, Authentication Server, Authorization Server (AAA). Wi-Fi solution provides cellular like authentication and security for Wi-Fi access. It also supports non-SIM devices via Media Access Control (MAC) based on Captive Portal Authentication.

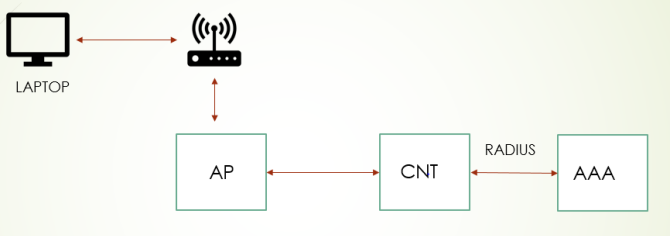

Figure 1: Wi-Fi Solution Architecture

3.2 Controller

The controller is a web based Graphical User Interface (GUI) mainly used for monitoring and configuration of access points It supports Integrated Element Management System(EMS) for monitoring and managing the Wi-Fi system via controller GUI. It also

provides centralized management for large set of Access Points. Wi-Fi controller is a cloud managed, low cost controller that manages up to 10k access points and upto 450k stations. The controller terminated management and control place traffic from the Wi-Fi AP while the bearer traffic is directly sent from Wi-Fi AP to internet.

3.3 Access Points

Access Points (AP's) is basically a LINUX box in which kernel is configures. The Wi-Fi AP portfolio includes AP's which are deployed as stand-alone units and include indoor and outdoor models. Control and management of Access Points is integrated into the cWLC and the bearer is directly routed either through or to the WiFi gateway. Wi-Fi AP is small, light weight and offers high data throughput, it also delivers concurrent operation in both 2.4GHz and 5GHz frequency bands. The Access Points provides Wi-Fi connections to hundered of STA's and are managed and configures via the controller.

4. Implementation

In the proposed system the access point will act as NAT and assign the unique IP address to each user. The access point will receive two IP addresses.IP1 is from the controller, IP2 is the NAT IP then the AP will single IP to user entity. AP will perform NAPT by using AP IPv4 address for client's ingress and egress traffic. AP will act as the NAT in this feature then AP will respond to the user based on their User MAC address. The Proposed system can be implemented in two ways:

i. GRE Tunnel with NAT
ii. NAT

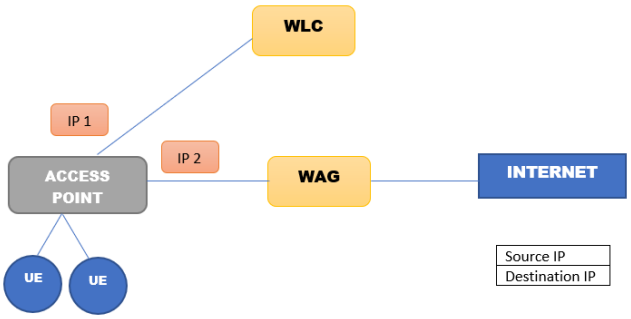

Figure 2: System Design of Proposed Feature

On configuring the AP to act as DHCP server and perform NAT the AP will provide an IPv4 address to the users in private range and won't be accessible from the rest of the network. Since the IPv4 address are private, the AP will have to translate between the IP of all the connected users and the Access Point IP address.

5. Results

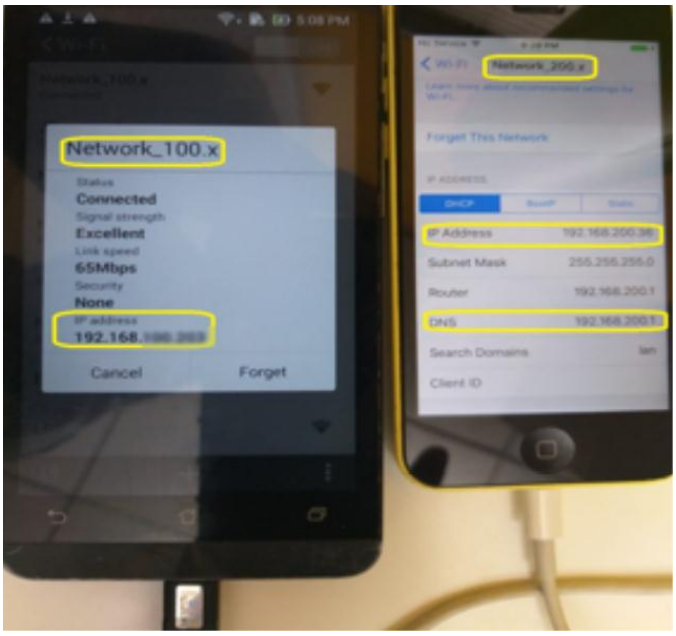

Figure 3: Accessing Network through different WLAN

6. Conclusions

In this feature AP acting as DHCP server to serve IPv4 address for users, DHCPv4 relay functionality is not to be used.

This feature cannot support the following functionalities:

- Unless the user's address is enabled at WLAN level in private IP address set, the data packet can be transmitted.
- When a configured IP address range is in conflict, the response can be dynamic to the user.
- If user address is not within the configured WLAN-level private IP address range , then the data packet must be dropped.

REFERENCES

[1] DHCP Protocol using OTP Based Two Factor Authentication: IEEE Conference in Trends.

[2] The Helping Protocol DHCP: Published in IEEE 16426709

[3] Yan Niu, Jun Li, Lala Li, Information Technology, Research on Authentication Security of Wireless Local Area Network Based on L2TP Protocol

[4] Mingming Hu, Qin Zhao, Minoru Kuramoto, "Implementation of L2TP on carrier network"

[5] Kingsley A. Ogudo "Analyzing Generic Routing Encapsulation (GRE) and IP Security (IPSec) Tunneling Protocols for Secured Communication over Public Networks".