

INTRODUCTION

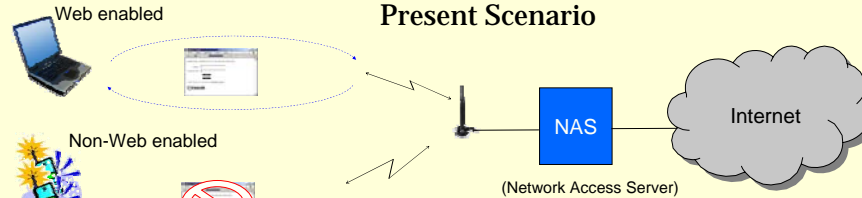
Internet has become an integral part of everyday life. With the advancement in technology and its popularity, there are many open, community-wide Wi-Fi networks available. They provide residents, visitors and businesses with mobile broadband Internet access. But the service providers have to be aware of the misuse of their free service, performing illegal activities on the network, possibly also harming others. For legal and other reasons, a mechanism called a splash screen web page, also called a captive portal, is being implemented. The splash screen displays the acceptable use policy (AUP) and registers those people using the service. The other advantages of a splash page and the registration is that they allow the service providers to pinpoint problems with the Wi-Fi network and also identify if there are any problems within the user devices such as viruses, bad network card interfaces, which could cause outages or slowdowns in the network.

PROBLEM

The implementation of the captive portal to solve legal issues has brought a new set of obstacles for the Wi-Fi service providers. To connect to the Internet a user needs to have a web browser (http, https) in their devices to open the splash page and accept the acceptable use policy (AUP) otherwise they do not get connected.

But there are many devices in the market, such as X-boxes, voice over IP (VoIP) phones, sensor network gateways, that may not support a web browser.

A user may use a file transfer protocol (ftp), simple mail transport protocol (smtp), session initiation protocol (SIP) or many other protocols other than a web browser protocol, which will not allow them to connect.



Present Scenario

SOLUTION

This thesis has a solution to allow non-web browsers enabled client devices to connect to Wi-Fi community networks and retain some security measures.

It looks at SIP as the general connection establishment. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

Some changes on the Network Access Server (NAS) or Wireless Access Point (WAP) is made to see if the device has web browser support by looking at the port request. If a connection request is for a web page at port 80 or 53, then packet is sent to the captive portal. If a non web browser request is received then SIP is used as a general connection establishment by consolidating all connection requests to one (or two) ports and redirect the request to a SIP proxy server.

WORK COMPLETED

A literature research has been done to see if any work has been done for this particular issue.

A private network is created to mimic the real life hotspot scenario, it displays a splash page when a web-enabled devices come within the Wi-Fi range.

Non-web enabled devices like VoIP phones can connect to the private network and they can make calls to devices located in different networks.

WORK IN PROGRESS

Currently code is being completed to account, authenticate, authorize a user in the private network.

Verify and log the information of the connected devices and store it in a secure place.

WORK PLANNED

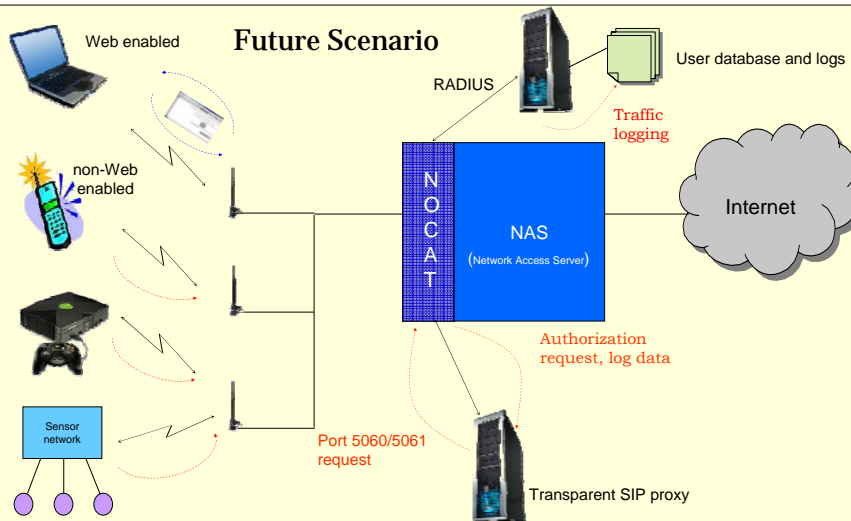
Connect some more devices that do not have web browser that uses SIP protocol for session establishment for example Wi-Fi enabled Black Berry phones, sensor network gateways, gaming devices.

Web enabled



Log Information

user name : Sonam
password : XXXXX
IP address : 192.168.2.101
Port : 80
MAC address :ABCDE:FDG:ERE



Future Scenario

Non Web enabled

Log Information

IP address : 192.168.2.101
Port : 5060
MAC address :ABCDE:FDG:ERE