Prototyping and Guidelines for Educational demonstrations of Captive Portals Technologies

Author: Lianting Wang

Supervisor: Marcelo Ponce

The Secret of Free Wi-Fi

INTRODUCTION

Captive Portal technology is everywhere, from airports to restaurants, letting us access the Internet by verifying our identity. It seems simple, but it's built on complex network protocols and authentication processes, with automatic pop-ups showing its sophistication.

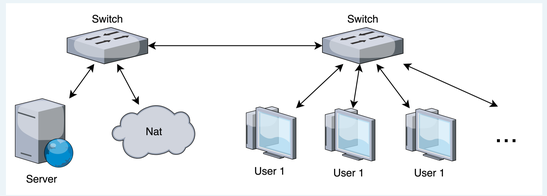
This technology's widespread use is a great chance for learning in computer science, particularly in networking. Most students know how it works on the surface and are ready to learn more. By explaining Captive Portal's basics, we aim to deepen students' understanding of network communication and security, turning everyday tech interactions into valuable learning moments.

OBJECTIVES

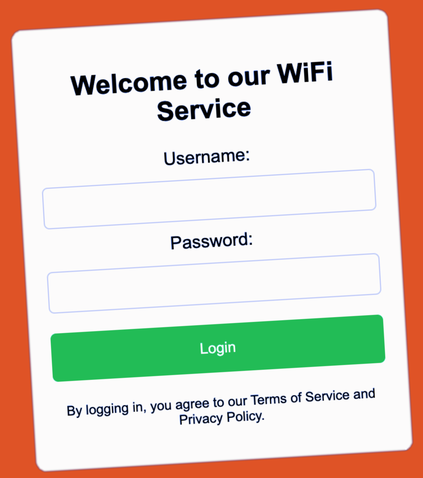
I would like to propose a hands-on educational tool for a deep dive into Captive Portal technology to enhance students' understanding of networking fundamentals. Through practical exercises, students understand networking principles such as MAC addresses, ARP requests, switches, DNS, web servers, and the differences between HTTP and HTTPS. This approach bridges theory with real-world network operations and promotes an intuitive understanding of networking.

This poster shows different ways to build a captive portal, giving instructors flexibility based on the level of difficulty.

METHODS

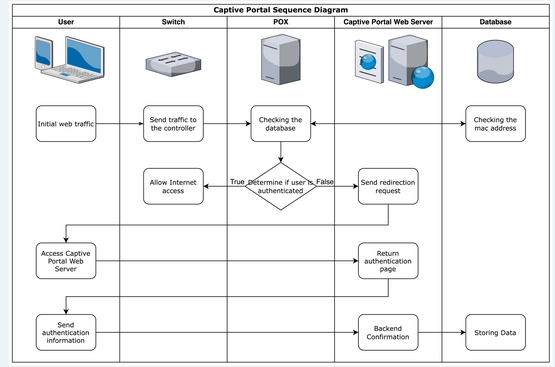


This is the infrastructure of our Captive Portal, where users and servers are connected through two Switches.



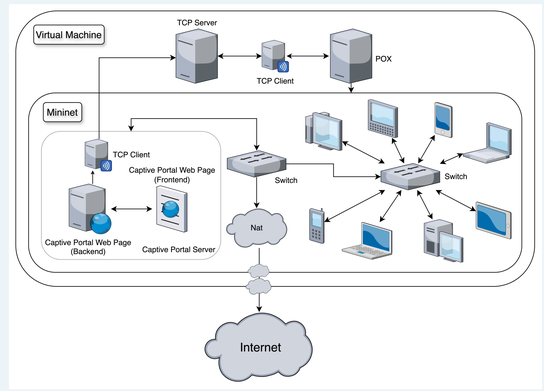
Using SDN technology, we can manage connections at the link layer, directing users with unique MAC addresses either to the Nat or to the Captive Portal Server. However, since the network layer focuses solely on delivering data to the correct IP address without regard to the connection's status, we employ specific techniques to reroute user requests to the appropriate server.

One key method is DNS Spoofing. Here's how it works: when a user tries to access an external website, their device sends out a DNS request to find the website's IP address. Normally, this would lead them to the intended website, but we intervene by using a special DNS server. This server directs all domain name requests to the Captive Portal Server, ensuring the user encounters the authentication page regardless of their intended destination.



Another approach we use is IP Forgery. With this technique, when a user‘s device sends a DNS request, we provide the correct IP address. However, when the user attempts to access the website, we intercept the web request and respond with an HTTP redirect message that redirects the user to the Captive Portal Server’s domain name. The user‘s second connection will connect to the Captive Portal Server.

FINAL STRUCTURE



SECURITY DISCUSSION

Captive Portal helps with login but doesn't secure your data. Using open Wi-Fi can expose your information to others.