DESIGN PROPOSAL OF HOTSPOT SETUP

TITLE :

Design proposal of hotspot setup for coffee shop

INTRODUCTION :

- ❑ The main scope of this project is to set up a hotspot in a coffee shop , which can be accessed by customers and staff .

- ❑ This wifi will have multiple access points because customers and staff will be able to access only certain pages whereas admin can access all the pages without any restriction .

ABSTRACT :

- ❑ A coffee shop needs to set up a hotspot, where users can access ADSL(Asymmetric digital subscriber line) internet .

- ❑ The users will be able to get access to the wireless network with a prepaid card.
- ❑ We introduce virtual prepaid tokens (VPTs), a novel billing scheme that allows users to obtain access at WiFi hotspots without having an account with a hotspot provider or a physical prepaid token (PPT). Upon arrival at a hotspot, a user buys a VPT online, using a third-party payment server with which the user already has an account. Experiments show that users can buy a VPT and gain full Internet connectivity in less than 15 seconds, i.e. much less time than it would take to create another account or to buy and activate a PPT.
- ❑ VPTs can be used in hotspots that use a captive portal or 802.1x for user authentication. The latter alternative enables better security. We also contribute a novel technique that allows a single access point to authenticate users by either method. Hotspots can use this solution for migrating to 802.1x without disrupting legacy captive-portal users. Wi-Fi hotspots are expected to have an important role in future provisioning of “anywhere, anytime”connectivity. They are quickly being deployed at locations that tend to attract nomadic users, such as cafes, airports, hotels, and conference centers. Although hotspots have limited range, they offer lower installation costs and higher bandwidth than do competing alternatives, such as 3G wireless. However, many hotspots have low utilization and are unprofitable. This low utilization is not due to incompatibility (many users’ notebook computers and PDAs have a Wi-Fi interface) or other technologies’ dominance (3G deployment has been

slow in most markets). The observed unprofitability could limit growth in the deployment of Wi-Fi hotspots.

- ❑ The customers will be able to access the network using Virtual prepaid Token bought at the coffee shop and staff will be able to access networks without any password .
- ❑ Network setup is demonstrated using Cisco Packet Tracer
.

OBJECTIVE :

People are busy. They need to access things on the move ,whether that's checking in for a flight, accessing their banking details, or replying to important emails, there is no need to be static to tick off your to-do list.

So, if you're a café owner, and you don't offer your guests WiFi, not only could you be angering impatient millennials who want to refresh their Twitter, but you could be alienating a whole sector of cabin-fever stricken freelancers, ready to swap their four walls for a flat white.

There are plenty of cafés that pride themselves on being a hotspot for flexi-workers, offering large workspaces, plugs, and a reliable WiFi connection. But even if you're more of a traditional café, you don't want to lose custom by not offering guests access to basic WiFi and a plug socket.

NETWORK REQUIREMENTS :

HARDWARE:

- ❑ WIRELESS ROUTER
- ❑ NETWORK CABLES
- ❑ SWITCHES

❑ HUB

❑ MODEM

❑ HIGH SPEED BROADBAND CONNECTION

NETWORK REQUIREMENTS ANALYSIS :

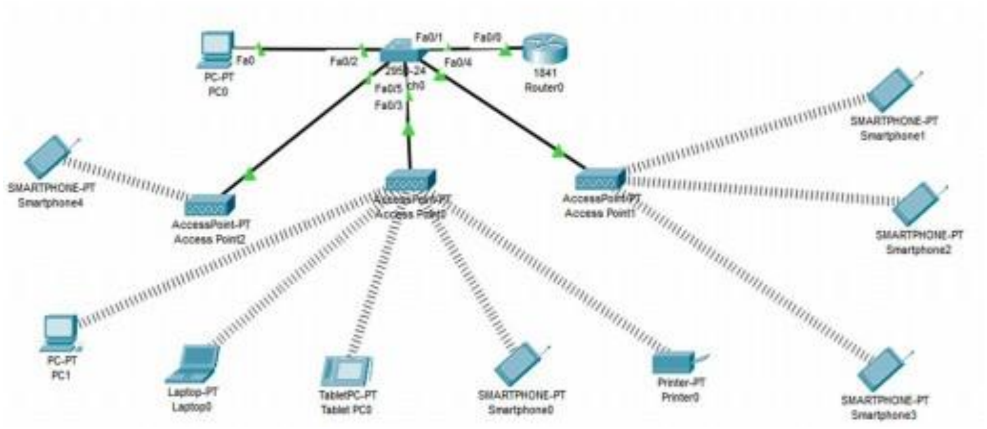
❑ Network speed and reliability is ultimately dependent on the equipment we choose. In the most basic form, you’ll need to purchase a modem and wireless router. However, in order to create a separate WiFi signal that allows for public access, you’ll need to invest in a premium model router.

❑ Some models provide us with a captive portal , meaning users need to agree to your terms and conditions before they can access your WiFi.

❑ This can be ideal when it comes to coffee shop WiFi management, because not only will it provide your business with legal protection; it also allows you to filter adult content (e.g. gambling), whilst managing and limiting how much bandwidth your guests can use – putting a stop to frustrating video streaming.

Billing is often cited as a problem area that contributes to low hotspot utilization,Existing billing methods have drawbacks that turn away many potential users. Three of the most common methods are subscription, pay-per-use account, and prepaid token. Subscriptions give to the provider a steady revenue stream and to the user the convenience of a fixed price and single monthly payment. However, subscriptions are nontrivial commitments. Several concerns may militate against such a commitment, including user doubts about whether he or she will need access in a covered area often enough to justify the cost of a subscription. Users can also be concerned about provider reliability.Instead of a subscription, users may set up a pay-peruse account with a provider. Pay-per-use accounts typically draw funds automatically from one of the user’s bank or credit card accounts, when the user gains access. Pay-per-use accounts can be less wasteful than are subscriptions to sporadic users. However, many users hesitate to open such an account with a provider that is not perceived as reliable and well-established in areas frequented by the user. Many providers are startups that do not meet such criteria. Moreover, a user may occasionally need access in places that are not served (directly or by agreement) by any of the providers that serve areas more frequently visited by the user. In the latter cases, users may prefer prepaid tokens (PPTs). PPTs contain an id and password that are typically revealed by scratching a card and are activated after first use for a limited time. A user does not need to set up any account to buy such a token; payment maybe, e.g., by cash or credit card. Prepaid tokens offer little risk to users. However, such tokens can complicate access because they need to be physically obtained from a vendor. In many cases (e.g., at an airport), vendor location may be inconvenient or not obvious. Moreover, a vendor location may be closed when a token is needed. Users can buy a VPT from a provider without any relationship between them before or after a specific access session. Users buy VPTs at the point and time of access, using a third-party online payment server. Users can employ the same server also for making or receiving many other types of payment. Therefore, such an account is more flexible than is a conventional pay-per-use account, which can be used only to purchase access from a specific provider or set of providers. Like physical prepaid tokens, VPTs do not require users to maintain a possibly wasteful subscription with the access provider. However, because VPTs are bought online, they have several advantages relative to PPTs, including saved time and no need of staffing outlets for selling them. The main difficulty in VPT implementation is that most current hotspot architectures authenticate a user before authorizing any Internet access by the user. VPT purchases require, however, that unauthorized users communicate with payment servers on the Internet. The VPT architecture accommodates such communication while blocking all other Internet access by unauthorized users. Communication between user and payment server is secured end-to-end by SSL. The payment server authenticates the user, debits the user’s credit or bank account for the price of access, and credits that amount to the provider. After verifying payment, the provider authorizes full Internet access by the user.VPTs involve more steps than do the password-based authentication schemes typically used for subscriptions and pay-per-use accounts. Although the VPT architecture is secured end-to-end by SSL, 802.1x can provide a valuable additional line of defense at the link layer.

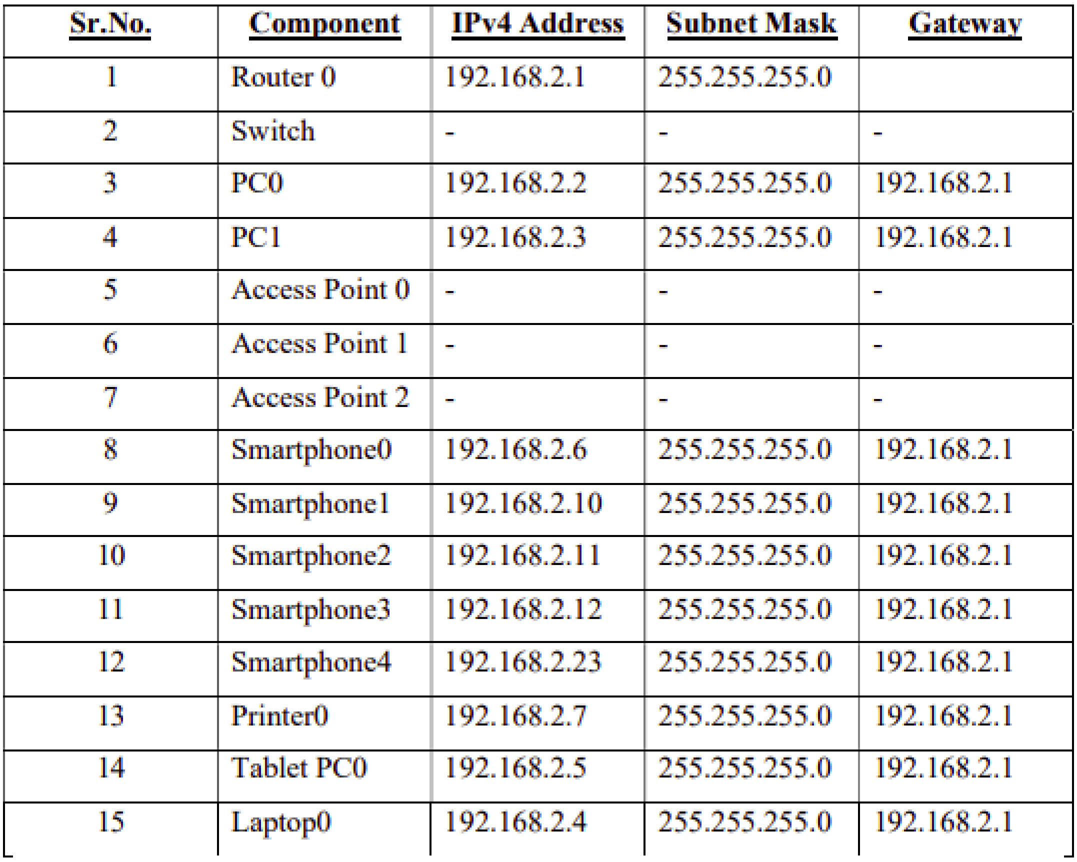
NETWORK DIAGRAM



The above is a basic diagram of how the topology will look,Multiple access points can be used, we have used two for example. The devices will connect wirelessly to the access points

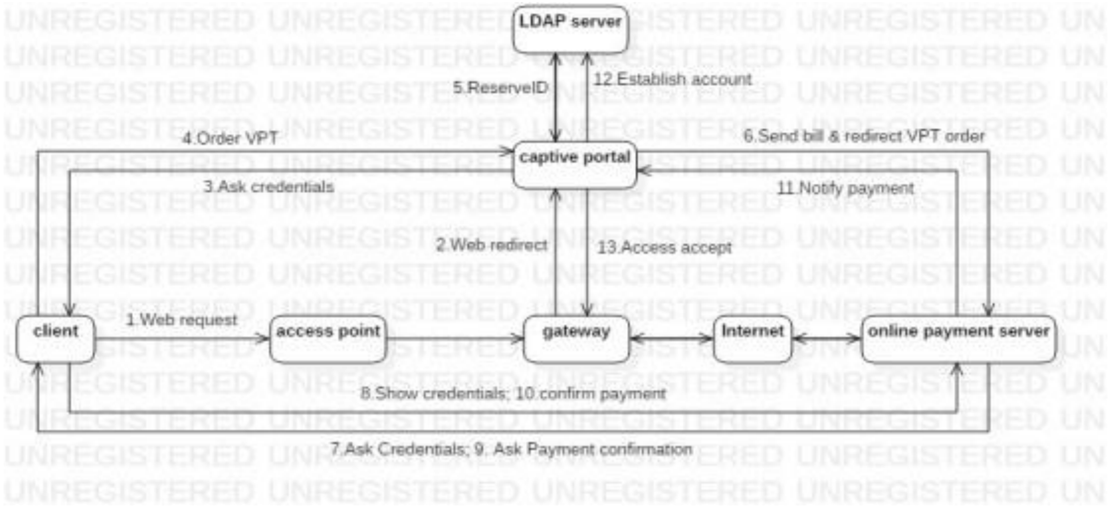
(Point 1 & 0) and log into the network using the credentials which will be provided after a payment to access the service. However the employees will be provided a separate Access point(AP-PT0) from which the can access the internet without paying, number of access points and routers can be decided with the size of the establishment , for example for an establishment with occupancy of 20-30, three access point (1 employee dedicated and 2 customers oriented). The employee access point doesn't need a VPT, so it can be encrypted used a simple WEP or WPA-PSK keys to allow them to directly connect to the net. IP

IP Network Design table for users and components



Sr.No.	Component	IPv4 Address	Subnet Mask	Gateway
1	Router 0	192.168.2.1	255.255.255.0	
2	Switch	-	-	-
3	PC0	192.168.2.2	255.255.255.0	192.168.2.1
4	PC1	192.168.2.3	255.255.255.0	192.168.2.1
5	Access Point 0	-	-	-
6	Access Point 1	-	-	-
7	Access Point 2	-	-	-
8	Smartphone0	192.168.2.6	255.255.255.0	192.168.2.1
9	Smartphone1	192.168.2.10	255.255.255.0	192.168.2.1
10	Smartphone2	192.168.2.11	255.255.255.0	192.168.2.1
11	Smartphone3	192.168.2.12	255.255.255.0	192.168.2.1
12	Smartphone4	192.168.2.23	255.255.255.0	192.168.2.1
13	Printer0	192.168.2.7	255.255.255.0	192.168.2.1
14	Tablet PC0	192.168.2.5	255.255.255.0	192.168.2.1
15	Laptop0	192.168.2.4	255.255.255.0	192.168.2.1

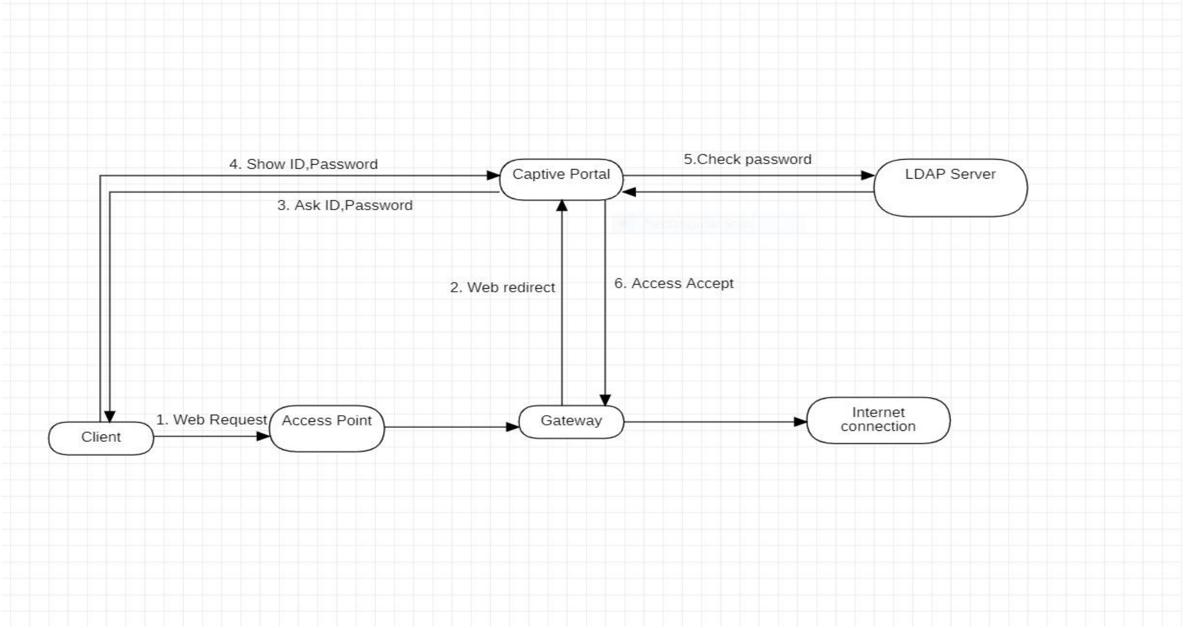
HOW THE BILLING SETUP CAN BE ACHIEVED?



The above diagram shows the steps and processes that the customer/client needs to follow in order to buy their token and access the internet. Hotspots usually employ captive portals for user authentication. Captive portals were first proposed in Stanford’s SPINACH project and are illustrated in the above diagram. Captive portals do not require special configuration of user computers. A special gateway between the hotspot’s LAN and the Internet enables only authorized users to communicate with the Internet. The gateway distinguishes authorized and unauthorized users by their MAC and IP addresses. The gateway allows unauthorized users’ DHCP, ARP, and DNS query packets. Unauthorized users use DHCP to obtain networking configuration parameters. They are then expected to open a Web browser and send a Web request. The gateway redirects any Web requests from unauthorized users to a captive portal, and drops any other unauthorized packets. The captive portal returns to the user an SSL-secured login page that requests the user’s id and password. The captive portal verifies the latter and, in case of success, sends the user’s MAC and IP addresses to the gateway for authorizing the user’s Internet access. The captive portal usually also sends the user a session management page with a button for logging off, on a small popup window that is not used for browsing. Finally, the captive portal redirects the user to the Webpage that the user initially requested (note that the initial redirection by the gateway makes it unnecessary for the user to know the captive portal's URL). Captive portals typically communicate with a remote account database for authenticating user passwords. Any of several protocols may be 8 | Page used for such communication, e.g., RADIUS, LDAP, or Kerberos. In the case of physical prepaid tokens, the database would have been previously populated with temporary accounts containing user ids and passwords that match those on the tokens.

Upon first authentication of such an account's user, the database manager calculates and updates the respective account's expiration time. The SSL-secured login page that the captive portal sends to the user is modified so that it contains an area where users who do not have a valid password can order a VPT. In the latter case, the user enters the respective user id and password and selects an expiration time and online payment server (OPS), possibly from among several alternatives displayed as buttons. The captive portal reserves in the account database the entered user id. In case of success, the captive portal sends the bill to the selected OPS and redirects the user to the OPS. The gateway is modified so that it allows unauthorized users to communicate with the supported OPSs. The selected OPS authenticates the user and asks the user to confirm payment of the provider's bill. After user confirmation, the OPS debits the bill's amount from the user's account and credits the same amount, minus OPS fees, to the provider's account. If the user's account does not carry enough balance, the OPS withdraws the bill's amount from the user's credit card or bank account. After crediting the provider, the OPS notifies the provider's captive portal. The captive portal establishes the user's account in the database and sends the user's MAC and IP addresses to the gateway for authorizing the user's Internet access.

Below is the illustration to access the user's account once the account is established in the server.



ARCHITECTURE DIAGRAM :

The most suitable topology for this type of network will be **HYBRID TOPOLOGY**.

Hybrid topology is an integration of two or more different **topologies** to form a resultant **topology** which has many advantages (as well as disadvantages) of all the constituent basic **topologies** rather than having characteristics of one specific **topology**.

REASON FOR CHOOSING HYBRID TOPOLOGY :

- ❑ We can get the correct network diagram only using hybrid topology as we need to combine two topologies to make the network .

HARDWARE REQUIREMENTS :

- Choose a business-class router, which allows you to set up different access points (APs)
- Ask if the router offers more than one Service Set Identifier (SSID), so you can create different WiFi IDs
- Purchase a router with a Virtual Local Area Network (VLAN) which works alongside your SSIDs to configure different security protocols for each different ID
- If you think you'll want to create a hotspot for your WiFi, check your router is compatible with the relevant software.