SET UP A HOTSPOT IN COFFEE SHOP

Submitted by

SHREEYA CHAUHAN [RA2111026010276]

Under the Guidance of

Dr. S. VELLIANGIRI

Assistant Professor, Department of Computational Intelligence

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with specialization in Artificial Intelligence & Machine Learning

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603203

May 2023

SRM INSTITUTION OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this Course Project Report titled **"SET UP A HOTSPOT IN A COFFEE SHOP"** is the bonafide work done by **SHREEYA CHAUHAN [RA2111026010276]** who conducted under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE
Faculty In-Charge
Dr. S. Velliangiri
Assistant Professor
Department of Computational Intelligence
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai

HEAD OF THE DEPARTMENT
Dr. R Annie Uthra
Professor and Head,
Department of Computational Intelligence,
SRM Institute of Science and Technology
Kattankulathur Campus, Chennai

TABLE OF CONTENTS

CHAPTER NO.	CONTENTS	PAGE NO.
1.	**ABSTRACT**	
2.	**INTRODUCTION**	
3.	**REQUIREMENT ANALYSIS**	
4.	**ARCHITECTURE & DESIGN**	
5.	**IMPLEMENTATION**	
6.	**CODE**	
7.	**EXPERIMENT RESULTS & OUTPUT**	
8.	**CONCLUSION & FUTURE ENHANCEMENT**	
9.	**REFERENCES**	

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 Wi-Fi hotspots without having an account witha 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 thanit 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 contributea 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 anypassword.

Network setup is demonstrated using Cisco Packet Tracer

Objective of the Project

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 Wi-Fi, 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 Wi-Fi 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 Wi-Fi and a plug socket.

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 Wi-Fi will have multiple access points because customers and staff willbe able to access only certain pages whereas admin can access all the pages without any restriction.

Modules of the Project:

- General ward
- Private ward
- Clinical Area
- IT Department
- Entrance Reception
- Lobby and Parking

General Ward: General ward is a common unit where patients who are admitted share the same room. The ward is equipped with health monitoring systems with one-to-one care assistance for patients as required. Facilities are catered as per patient's diagnosis, age, comfort and other essential factors.

Private Ward: Private ward is specifically designed for patients wanting privacy during their time of treatment. Private wards are separate and silent than the normal wards and hence, they provide an excellent atmosphere to recuperate after undergoing extensive surgeries and treatments.

Clinical Area: Clinical Area means an area of a health facility, including related corridors, equipment rooms, ancillary service and support areas that house medical equipment, patient rooms, patient beds, diagnostic, operating, therapy, or treatment rooms or other accommodations related to the diagnosis, treatment, or rehabilitation of individuals receiving services from the health facility**.**

IT Department: Hospital IT departments have an essential role to play in assisting hospital staff to manage and care for patients. These systems are so essential and ingrained into modern-day hospitals that it can literally be a matter of life or death if they stop working effectively. The IT department of a hospital is not only responsible for managing clinical software and the other processes that help administrative staff to keep patient records and admissions systems ticking along, they also have an important role to play in ensuring medical wards, operating rooms, labor and delivery suites and emergency departments run smoothly

Entry Reception: The reception module handles various enquiries about the patient's admission and discharge details, bed census, and the patient's movements within the hospital. The system can also handle fixed-cost package deals for patients as well as Doctor Consultation and Scheduling, Doctor Consultancy Fees and Time Allocation.

Lobby and Parking: The parking system ensures the regulation of entries to and exits from the hospital area and the collection of parking fees in the hospital car park. The parking system allows the operator to select out of many tariffs or to allocate the authorization to enter to individual users (clients, employees, suppliers, etc.).

Aim:

To design proposal of hotspot setup

Components required:

a. WIRELESS ROUTER

b. NETWORK CABLES

c. SWITCHES

d. HUB

e. MODEM

f. HIGH SPEED BROADBAND CONNECTION

NETWORKREQUIREMENTSANALYSIS:

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

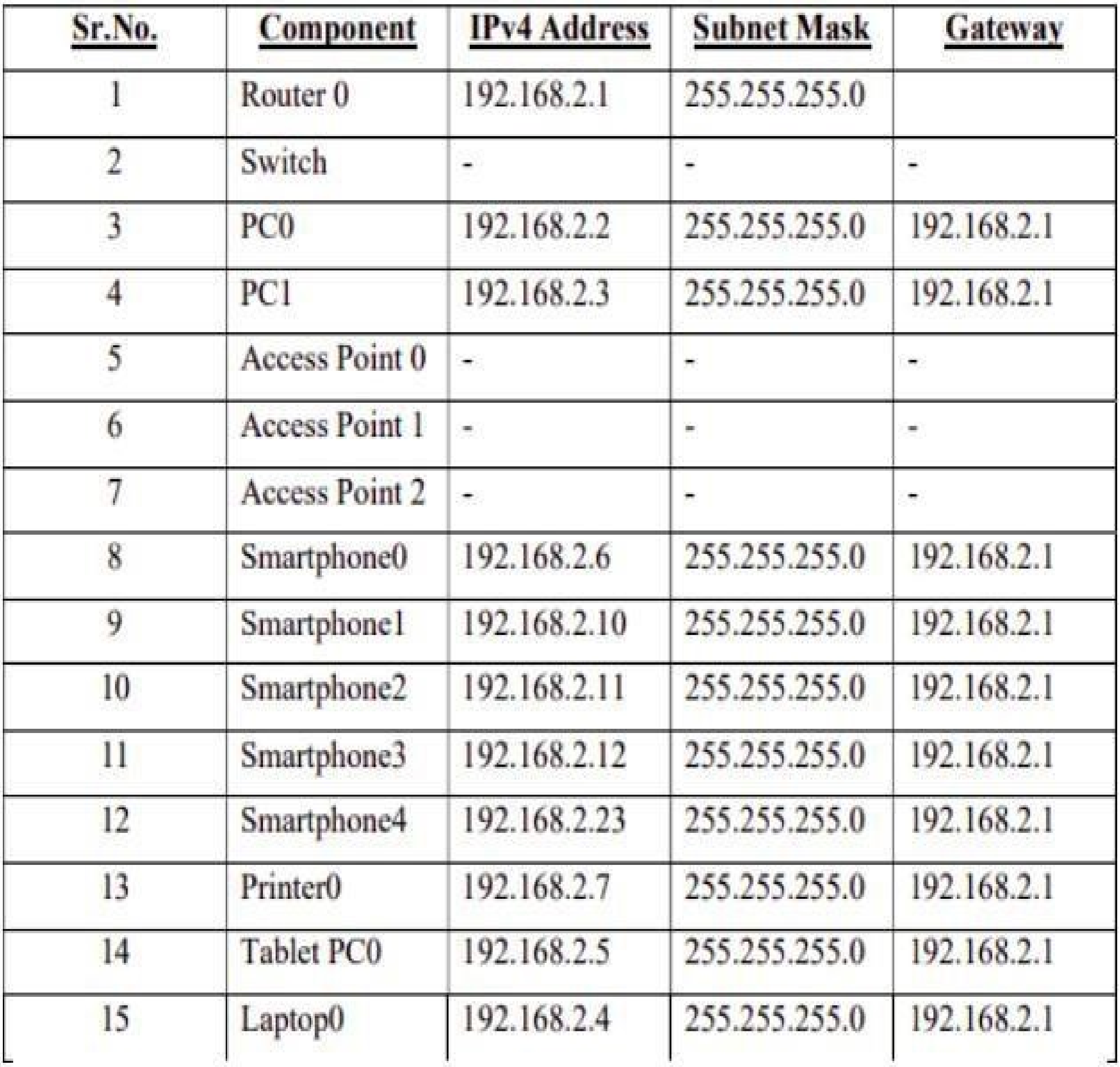
Some models provide us with a captive portal, meaning users need to agree to your terms and conditions before they can access your Wi-Fi.

This can be ideal when it comes to coffee shop Wi-Fi management, because not only willit 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 paper- 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.

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

Network configuration tips: -

1. **Pick the correct network: -**

Have you ever tried to connect to public Wi-Fi and seen multiple network names that are similar but not the same? EricsCoffeeHaus versus EriksCoffeeHaus, or Hilton Guest versus Hilton Guests, for example. This is a tried-and-true man-in-the-middle attack used by hackers—dubbed Wi Phishing (Opens in a new window)—which tries to trick you into logging into the wrong network to get to your info. Most people don't take the time to check, and jump on the strongest, open signal they see. But you should always check that you pick the legitimate network. Just ask someone who works there for the proper network name if it's not posted.

2. Pick a secure Network: -

When you want to pick a Wi-Fi hotspot to log into, try and find one that's got you locked out. You read that right. Usually, if you see the lock icon, it means you can't get access. Networks with zero security don't have a lock icon next to them, or the word "secured," which shows on a Windows laptop. On an iPhone, if you click an unsecured network—even if it's your own at home—you'll get a warning that reads Security Recommendation.

Of course, this isn't a hard and fast rule. Some hotspots don't show the lock because they have what's called "walled garden" security: you have to log in via a browser to get access to the internet. The login usually is provided by the hotspot—you may get it from the front desk at a hotel, for example, while checking in. It's best to stick to hotspots where the provider—be it a conference, hotel, or coffee shop—provides you with a clear network to choose from, plus a password to grant access. Then you know at least you're on the network you're meant to be using.

3. Ask to Connect: -

You can set most devices to ask for your permission before they connect to a network, rather than just automatically connecting to the strongest open network around, or a network they've connected to before. That's a good idea. Never assume the network you used in one place is as safe as one with the same name in another place. Anyone with the right tools could spoof a Wi-Fi network's broadcast name (called the SSID).

If the device asks first, you've got a chance to make a decision about whether it's safe to connect or not. On iOS for example, go to Settings > Wi-Fi, and check off Ask to Join Networks. On Android (Opens in a new window), the exact path will vary, but look for Wi- Fi preferences in Settings.

4. Be Your Own Hotspot:-

Rather than risk everyone in a group using iffy Wi-Fi, one person could designate their own device as the hotspot. Almost all laptops and phones make it easy to become your own hotspot for others. It won't be fast, but it will be more secure.

In Windows 10, turn it on at Settings > Network & Internet > Mobile Hotspot. Pick the kind of internet connection used (if there is more than one option; this is best if you've got an Ethernet connection), and copy the name of the network to hand out to people (or change it), as well as the network password they need for access (or change it—it must be eight characters at least). On macOS (Opens in a new window), go to Apple Menu > System Preferences > Sharing and click the Internet Sharing box. Pick a connection type to share, how you plan to share it (Wi-Fi, duh), then click Wi-Fi options to name your Mac hotspot and give it a password.

On iOS, go to Settings > Personal Hotspot to toggle on Allow Others to Join. You can also reset the password here to one that's a minimum of eight characters. Android users, look for a under Settings > Network & internet > Hotspot & tethering.

5. Take a Hotspot With You:-

Public access Wi-Fi is great, but you could just carry your hotspot with you. Cellular modem hotspots have their own battery, use cellular backhaul for an internet connection, and provide multiple people with Wi-Fi access. Sure, it costs more, but it might be worth it if you've got a lot of traveling ahead. Our top pick depends on your carrier (see our roundup of the Best Mobile Hotspots) or if you're going abroad, consider the Sky roam Solis Lite.

Overall, this is a lot more secure than using publicly provided Wi-Fi. It'll just cost you more, either in money or data (or both).

6. Subscribe to Hotspots:-

Services like Bingo (Opens in a new window)—which partners with others to provide access to over 1 million hotspots around the globe—or Gogo (Opens in a new window), which provides hotspots specifically for planes in flight, are two of the big names in subscription Wi-Fi services. Pay them a monthly fee—which can get pricey—and you know when you find their certified hotspots, they're a lot less likely to be run by the bad guys. (Not impossible, but pretty unlikely.)

7. Use Hotspot 2.0:-

Never heard of 802.11u? How about Wi-Fi Certified Pass point (Opens in a new window)? They're all the same thing: a method to help people not only securely get on a hotspot, but roam from supported hotspot to hotspot, cell-tower style. That means you enter credentials to sign in once, which get reused at hotspots all over the place, logging you in instantly and securely. The major operating systems like Windows 10, macOS, iOS, and Android support Hotspot 2.0. In Windows, go to Settings > Network & Internet > Wi-Fi and flip the switch under Hotspot 2.0 networks to turn it on. In Android, search for it in Settings. You can find it in locations with consistent ISP providers like Optimum or Spectrum, or from paid hotspot providers like Bingo. If it's an option for you, use it.

8. Avoid Personal Data in Hotspots:-

This is less a technical tip than a behavioral one: if at all possible, avoid doing serious tasks like bill paying, accessing your bank account, or even using your credit card when connected to public Wi-Fi. And filing your taxes at a hotspot? No way. Save those transactions for when you're connected safely to your home network, where you're a lot less likely to get targeted by snoops, since you already keep that one secure, right? If you absolutely must do the above, read on.

9. Avoid Using Your Passwords:-

There are a lot of passwords to remember, and you probably have to enter a few even while you're on public Wi-Fi. But if you've been compromised—say some hacker is sniffing the airwaves and pulling down data—anything you type and send to the internet could be equally compromised. That's one of the many reasons you should use a password manager. They store passwords for you and keep them encrypted, even on mobile apps. If you do use passwords, try to make sure they're on sites where you have two-factor authentication set up.

10. Check for a Secure Connection: -

Most websites use the HTTPS protocol to support SSL (Secure Sockets Layer) to make your connection to them more secure. Browsers like Chrome warn you if you visit a site without it. You can tell if the site you're on uses HTTPS even if you can't see it listed in the URL (that would be the first part, as seen in "https://www.pcmag.com"). For example, a lock icon and the word "Secure" appear at the start of the address bar in the Chrome browser on the desktop (the lock appears on most smartphone browsers). There are also extensions, like the Electronic Frontier Foundation's HTTPS Everywhere extension (Opens in a new window) for Chrome, Firefox, or Opera, that try to force every site connection you make to the secure option, if available.

11. Use a VPN:-

This should go without saying by now: you need a virtual private network (VPN) when you're on a public network. While this was moderately good advice the first time we wrote this story almost a decade ago, we live in a surveillance/hacker state today that rivals that of Orwell's 1984.

A VPN creates a private tunnel between your laptop or smartphone and the VPN server on the other end, encrypting your traffic from snoops—even your ISP or the operator of the hotspot itself. To find the one that's right for you, read our roundup of the Best VPN Services. Put it on all your devices that use public Wi-Fi of any sort. Even on your home Wi-Fi. You'll be glad you did. (For complete anonymity, use the Tor network.)11. Use a VPN

This should go without saying by now: you need a virtual private network (VPN) when you're on a public network. While this was moderately good advice the

first time we wrote this story almost a decade ago, we live in a surveillance/hacker state today that rivals that of Orwell's 1984. A VPN creates a private tunnel between your laptop or smartphone and the VPN server on the other end, encrypting your traffic from snoops—even your ISP or the operator of the hotspot itself. To find the one that's right for you, read our roundup of the Best VPN Services. Put it on all your devices that use public Wi-Fi of any sort. Even on your home Wi-Fi. You'll be glad you did. (For complete anonymity, use the Tor network.)

12. Turn Off Sharing:-

When you connect to a network with a PC, be it a Windows or Mac, the goal is typically to share some services—at the very least files and printing ability. If you leave that sharing option open at a hotspot and connect to the wrong thing, you're giving bad guys easy access. Disable it before you go out. In Windows 10, go to Settings > Network and Internet > Wi-Fi

> Change Advanced Sharing Options (on the right) and look for Guest or Public—click the down caret to open that section. Click the radio buttons next to Turn off network discovery so your PC isn't seen, and turn off file and printer sharing to avoid sharing.

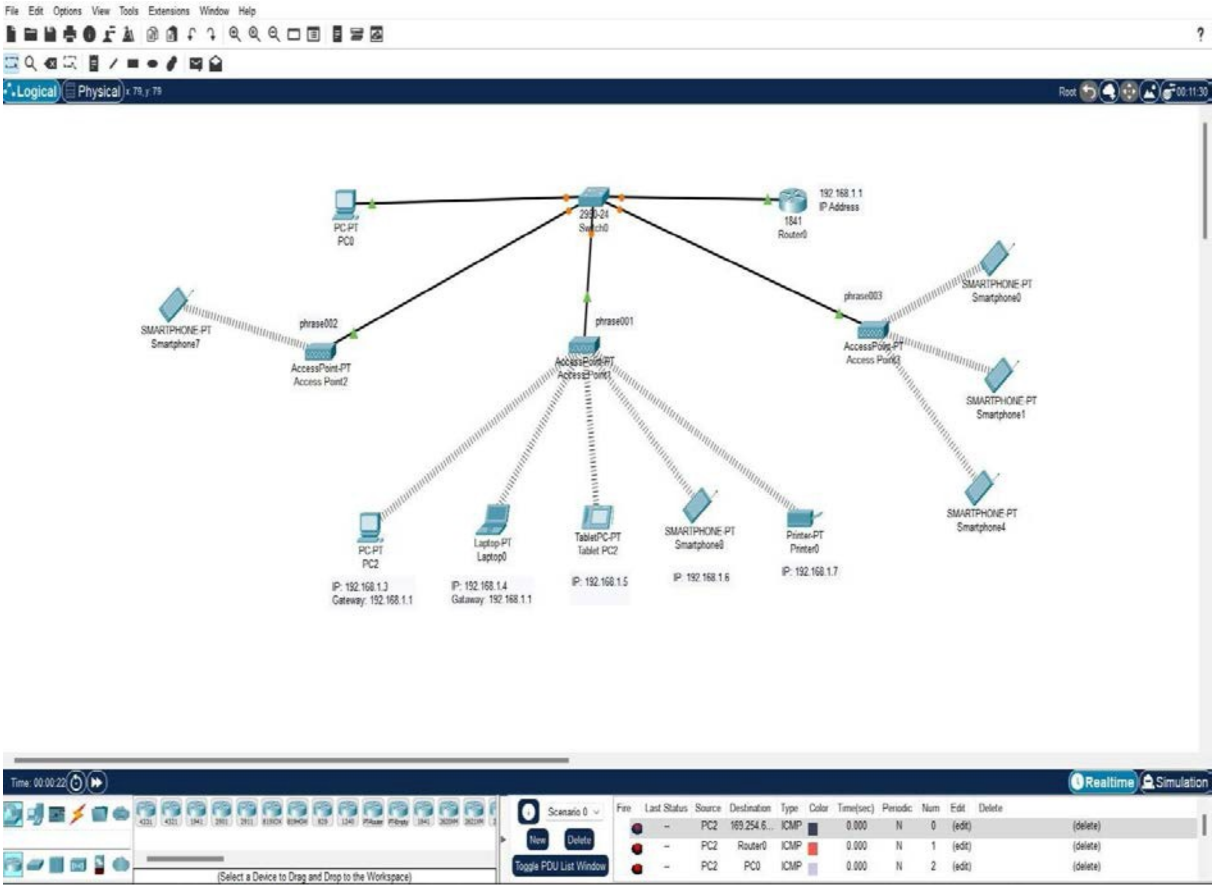
13. Keep Your OS and Apps Updated:-

Operating system (OS) updates are an annoying yet necessary evil. Don't be lulled into a false sense of security because you're a Mac or iPhone user. OS updates are serious business; they often fix serious security holes. Once an update is available, everyone in the world knows about the holes in the previous iteration—if you haven't patched it, your device becomes low- hanging fruit ready to be plucked by an opportunistic hacker.

Don't forget mobile apps either. App updates also fix serious security holes.

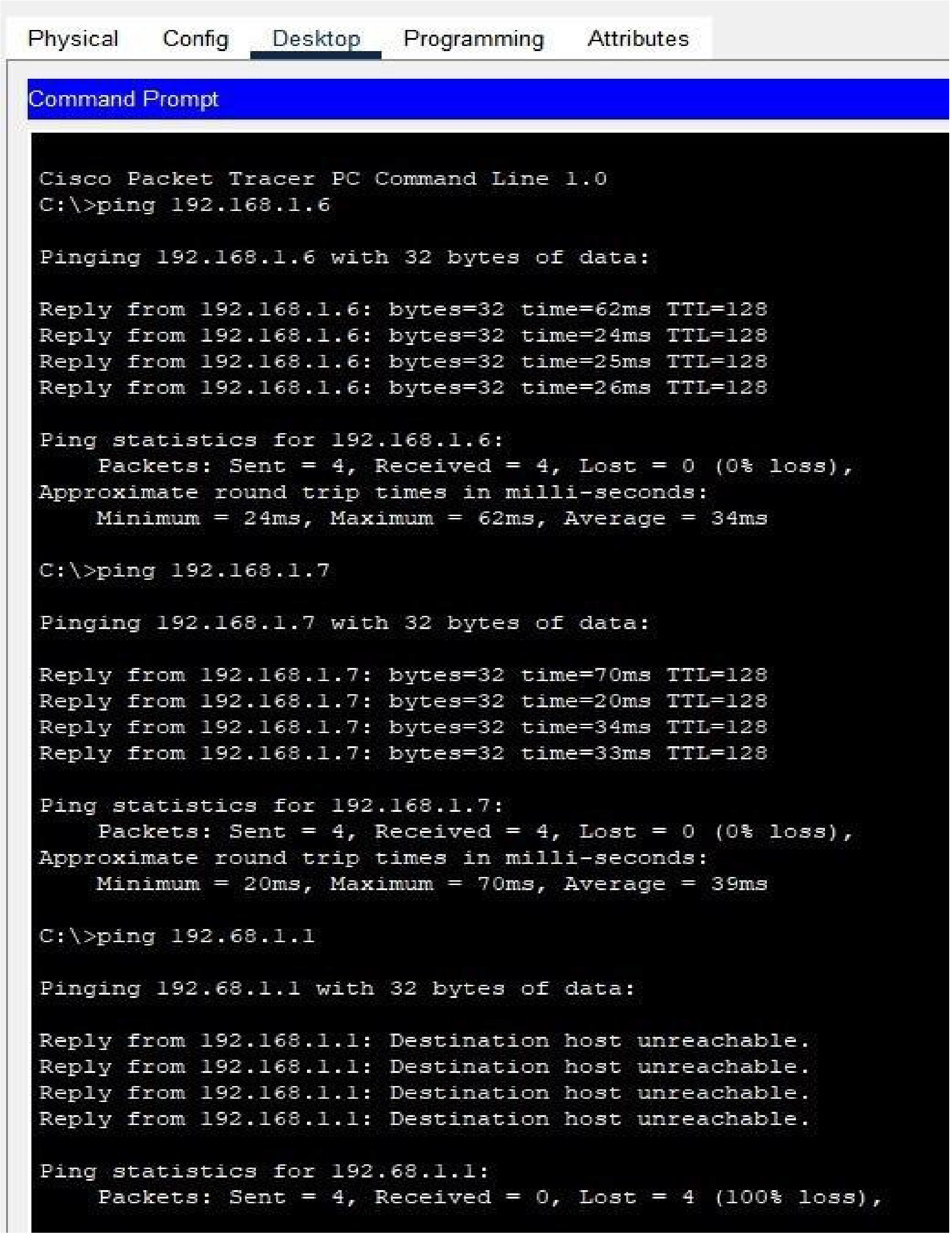
Especially the browser apps, but anything that goes online could be vulnerable. On iOS, go to Settings > App Store > App Updates, and toggle it on so apps update themselves. On Android devices you can do the same with Google Play > Settings > Auto-update apps, and choose whether you want auto-updates to happen over any network (such as your mobile connection) or just when you're on Wi-Fi.

Screenshot of Model:

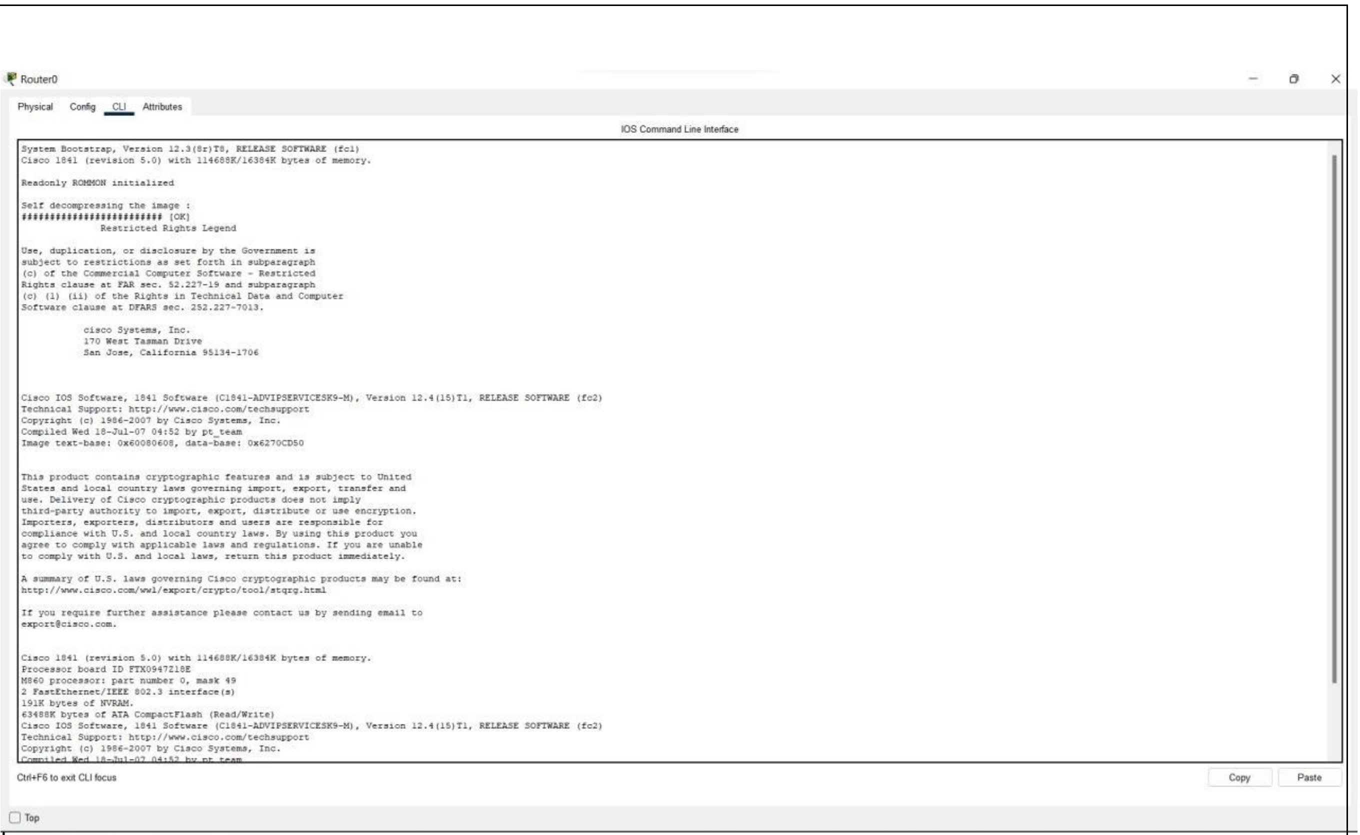


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	--	PC2	169.254.6...	ICMP	■	0.000	N	0	(edit)	(delete)
●	--	PC2	Router0	ICMP	🟥	0.000	N	1	(edit)	(delete)
●	--	PC2	PC0	ICMP	■	0.000	N	2	(edit)	(delete)

SHOW COMMANDS:

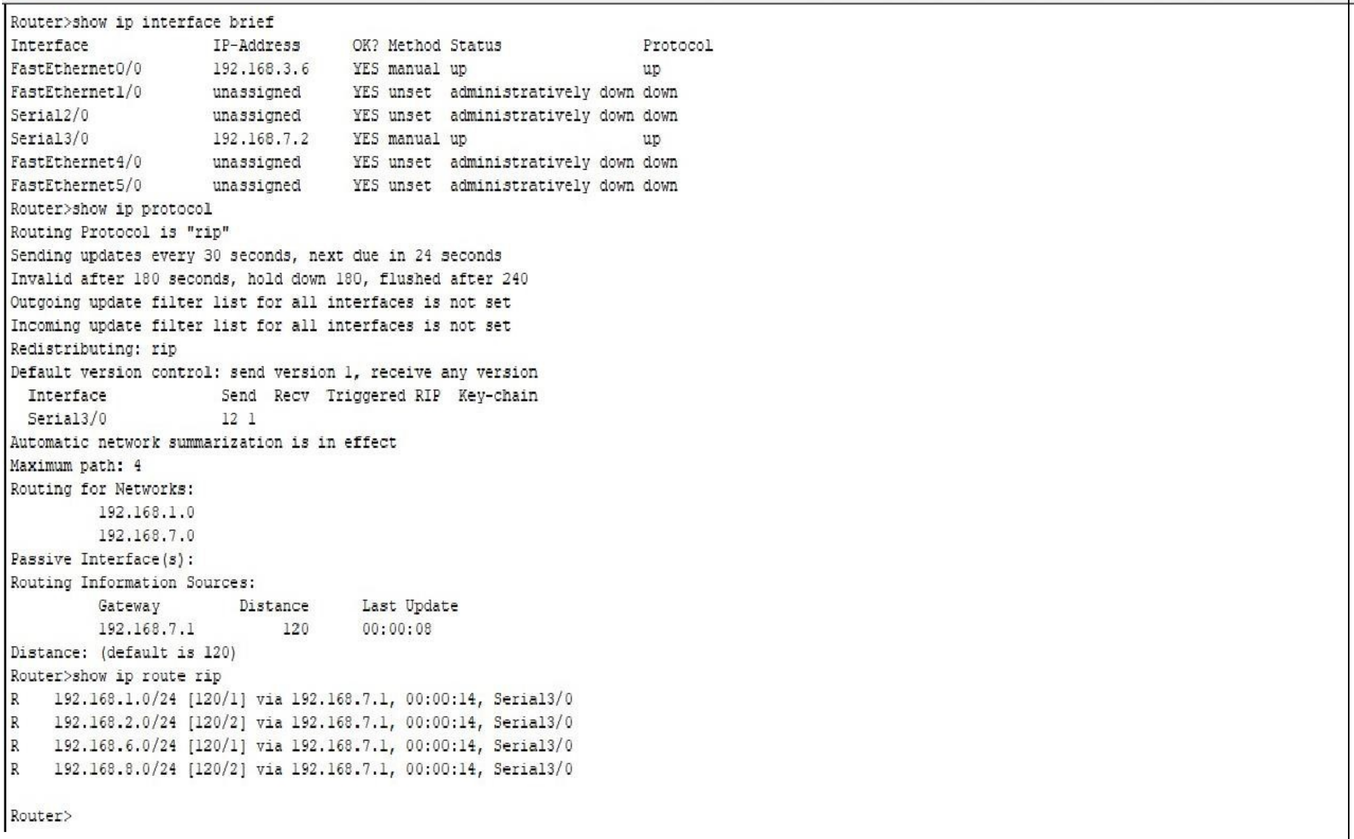


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=62ms TTL=128
Reply from 192.168.1.6: bytes=32 time=24ms TTL=128
Reply from 192.168.1.6: bytes=32 time=25ms TTL=128
Reply from 192.168.1.6: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 62ms, Average = 34ms

C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time=70ms TTL=128
Reply from 192.168.1.7: bytes=32 time=20ms TTL=128
Reply from 192.168.1.7: bytes=32 time=34ms TTL=128
Reply from 192.168.1.7: bytes=32 time=33ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 70ms, Average = 39ms

C:\>ping 192.68.1.1

Pinging 192.68.1.1 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.68.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



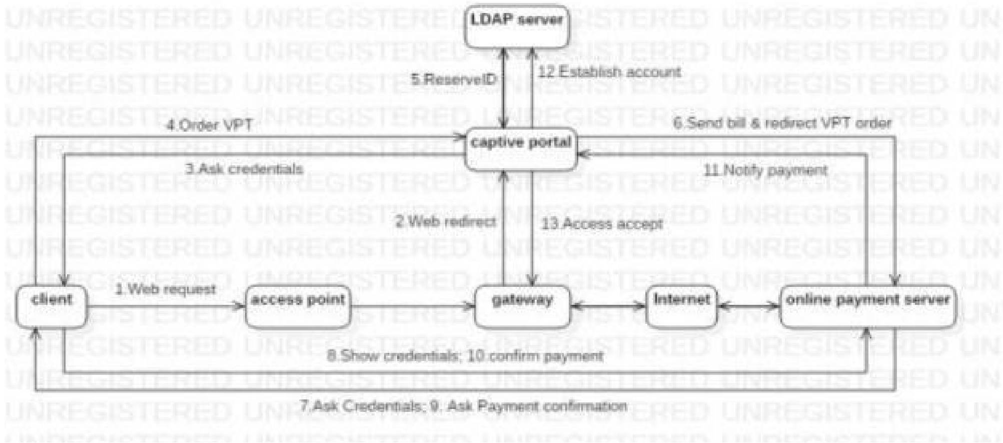
```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Readonly ROMMON initialized

Self decompressing the image :
######################## [OK]
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Image text-base: 0x60080608, data-base: 0x6270CD50


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
```

Ctrl+F6 to exit CLI focus



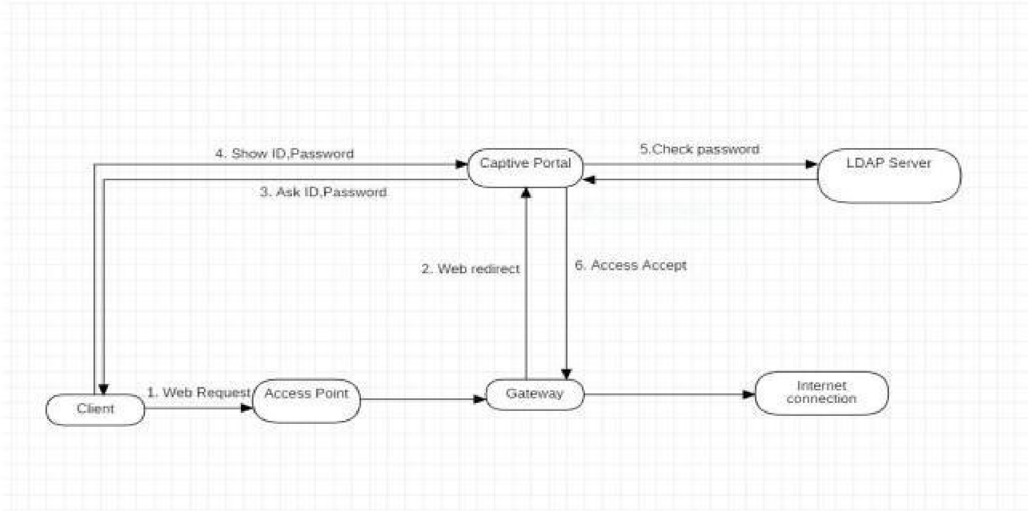
```
Router>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.3.6     YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              unassigned      YES unset  administratively down down
Serial3/0              192.168.7.2     YES manual up                    up
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Router>show ip protocol
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 24 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  Serial3/0             12 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
          192.168.1.0
          192.168.7.0
Passive Interface(s):
Routing Information Sources:
          Gateway         Distance      Last Update
          192.168.7.1          120      00:00:08
Distance: (default is 120)
Router>show ip route rip
R    192.168.1.0/24 [120/1] via 192.168.7.1, 00:00:14, Serial3/0
R    192.168.2.0/24 [120/2] via 192.168.7.1, 00:00:14, Serial3/0
R    192.168.6.0/24 [120/1] via 192.168.7.1, 00:00:14, Serial3/0
R    192.168.8.0/24 [120/2] via 192.168.7.1, 00:00:14, Serial3/0

Router>
```

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 | P a g e 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 Wi-Fi 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 Wi-Fi, check your router is compatible with the relevant software.

Inference:

Owing to the impracticalities described above in the Discussion section, the initial research aims of testing if the presence of Wi-Fi in cafes had helped increased their business was discarded and focus was shifted on the current café culture and people's opinions and attitude towards Wi-Fi in café. It was argued in the literature review section that the café culture in Finland is not as conservative as in some parts of Europe, for instance France. The data obtained from the customer survey concurs with this point. 61% of the respondents use café Wi-Fi and 89% are happy with the presence of café Wi-Fi regardless of whether they use it or not. However, eating and drinking is still the primary activity people do in cafes, followed by socializing and using Wi-Fi. From what has been discussed above, especially from the opinions of café managers, it is quite clear that having Wi-Fis in cafes has not really helped increase the sales in cafes. Wi-Fi in cafes is rather a trendy thing and, in some cases, a taken for granted part of the café environment. People would anyways visit a cafe for some refreshment, irrespective of whether it has Wi-Fi or not. However, for the active users of internet, for example students or tourists, café Wi-Fi can be an important factor in choosing which café they visit, provided that there are several cafes nearby to choose from. As revealed from the chi-test for independence, the occupation "student" and age group "10-29" are active users of café Wi-Fi. To avoid the problem of cafes overcrowding due to laptop users sitting at tables for hours on end, options like offering student discounts (which would also include most of the 10-29 age group) are worth considering. Also changing the café layout to better accommodate both the users and non-users of Wi-Fi can help create a favorable café environment for the customers. The presence of Wi-Fi can also influence the amount of time people (specially Wi-Fi users) spend in cafes. But according to the study, the number of people spending many hours using café Wi-Fi is relatively low, so other people not getting place to sit due to café Wi-Fi users occupying a table for many hours should not be that big of a problem. Nevertheless, it depends on the location of the cafes as well. For instance, the managers of cafes located in the city center like mbar and Café X shared their experiences of facing such problems during busy hours.

Reference:

Acohido, Byron (2007) “Public Wi-Fi use raises hacking risk”. USA TODAY. Gannett Co. Inc. Accessed from:

http://www.usatoday.com/tech/wireless/2007-08-06-wifi-hot-spots_N.htm

https://www.youtube.com/watch?v=AGLfnJkF-mc