NIS TEAM **NISP04**

TRAVEL ROUTER USING RASPBERRY PIE

190030468	Gandluru Sai Chinmayi
190031023	M Maneeshwar
190031134	Pavan Radha Krishna
190031225	P Swarnalekha
190031256	P V S Sumanth

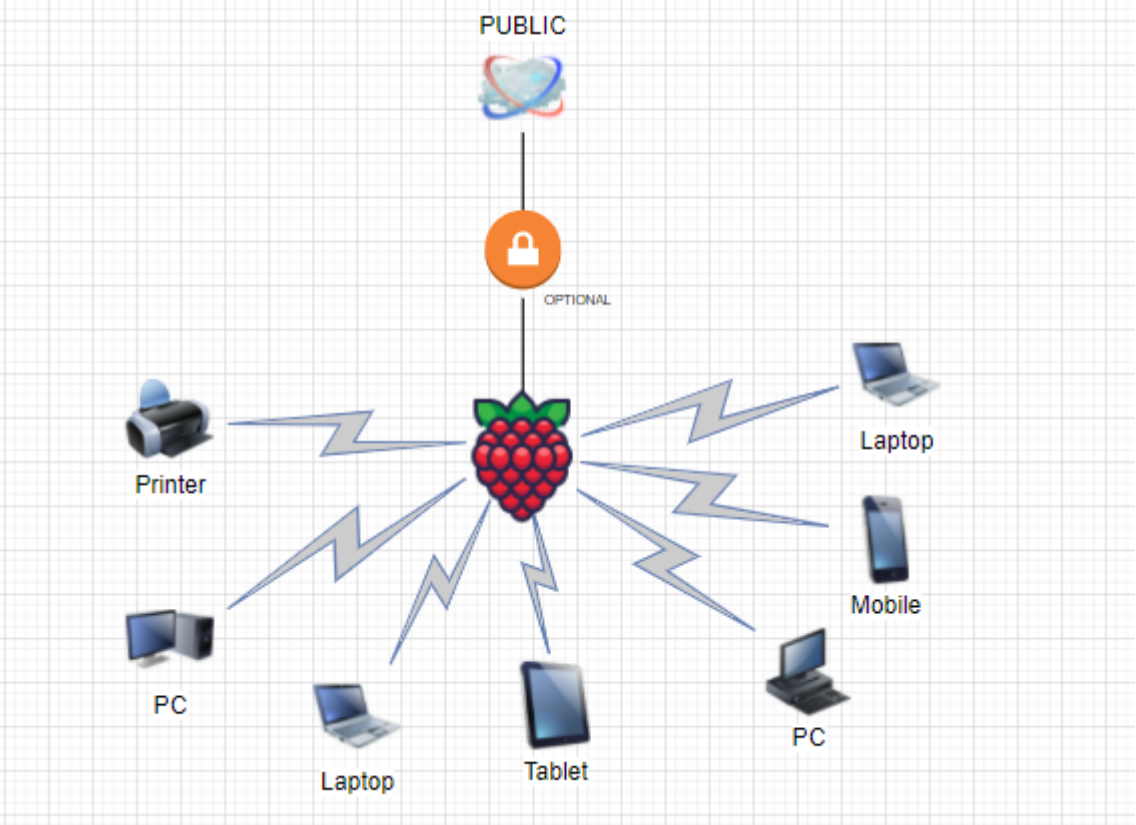
CASE STUDY:

Sumanth and his family planning for a trip in Dubai. He found out that the place he'll be going to check in has free public WIFI. Being an IT engineer Sumanth doesn't want to take any chance to expose his and his family devices to that public Wi-Fi. So, he came up with an idea to build a device which connects to public Wi-Fi and his family will be connecting to that device.

Requirements:

- Raspberry pie
- OpenWRT image file
- Sd card,
- SD card reader,
- USB wireless adapter,
- ETHERNET cable.

Illustration Of Project:



Procedure Of Project:

Config of Raspberry Pi:

- Download the OpenWrt image for the respective raspberry pi that you are working on.
- Download the Balena-etcher (image flashing software).
- Plug in the SD card in the card reader and burn the image into it.

Changes to default:

- Plug SD into the raspberry pie.
- By default, you can have address as 192.168.1.1
- Connect it over SSH, with command
  `ssh root@192.168.1.1`
- Navigate to config directory using
  cd /etc/config
- Create backup for network, firewall and wireless files.
  `cp network network.bk` (similarly to firewall and wireless)

```
cp firewall firewall.bk
cp network network.bk
cp wireless wireless.bk
```

- Change the network configuration to following

From this

```
config interface 'loopback'
        option device 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fde9:bb89:c742::/48'

config device
        option name 'br-lan'
        option type 'bridge'
        list ports 'eth0'

config interface 'lan'
        option device 'br-lan'
        option proto 'static'
        option ipaddr '192.168.1.1'
        option netmask '255.255.255.0'
        option ip6assign '60'
```

To this

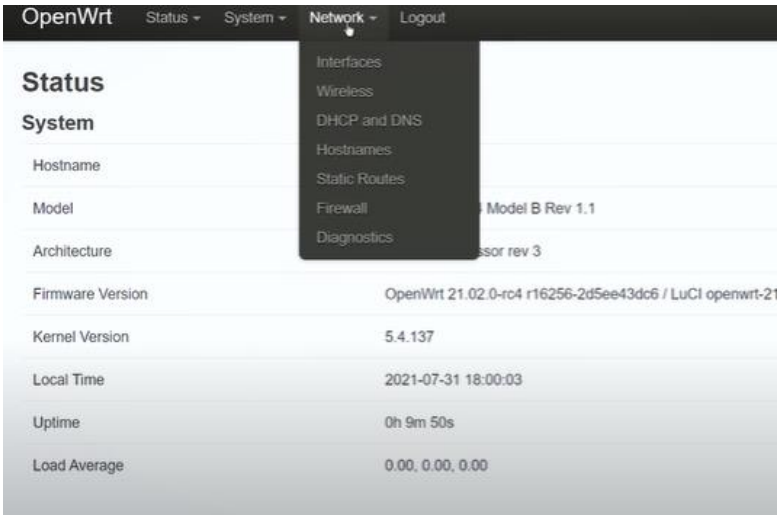
```
config globals 'globals'
        option ula_prefix 'fde9:bb89:c742::/48'

config device
        option name 'br-lan'
        option type 'bridge'
        list ports 'eth0'

config interface 'lan'
        option device 'br-lan'
        option proto 'static'
        option ipaddr '10.71.71.1'
        option netmask '255.255.255.0'
        option ip6assign '60'
        option force_link '1'

config interface 'wwan'
        option proto 'dhcp'
        option peerdns '0'
        option dns '1.1.1.1 8.8.8.8'

config interface 'vpnclient'
        option ifname 'tun0'
        option proto 'none'
```

- We have changed default Ip to 10.71.71.1 which is quite uncommon for attacker to guess since the default Ip is 192.168.1.1

- For firewall we must change the input option of zone to ACCEPT from REJECT.

```
config zone
        option name             lan
        list   network          'lan'
        option input            ACCEPT
        option output           ACCEPT
        option forward          ACCEPT
```

- For the USB Wireless adapter, we need to have drivers pre-installed in the system.
- For that reboot the device.
- Connect it over the WIFI (public) to build in wlan0. Via OpenWrt Portal on 10.71.71.1 (type it in the browser).
- In networks connect to the wi-fi visible which is accessible to work with.



- Now check internet status

  `ping google.com`

- When internet status is up, you can download the drivers you need for OpenWrt Portal.

This is how it looks when it's all done

```
root@OpenWrt:~# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux 5.4.137 xhci-hcd xHCI Host Controller
Bus 001 Device 002: ID 2109:3431  USB2.0 Hub
Bus 001 Device 001: ID 1d6b:0002 Linux 5.4.137 xhci-hcd xHCI Host Controller
root@OpenWrt:~# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux 5.4.137 xhci-hcd xHCI Host Controller
Bus 001 Device 003: ID 148f:5370 Ralink 802.11 n WLAN
Bus 001 Device 002: ID 2109:3431  USB2.0 Hub
Bus 001 Device 001: ID 1d6b:0002 Linux 5.4.137 xhci-hcd xHCI Host Controller
```

Conclusion:

Finally, the family connects to the network which is from the raspberry-Pi they can have a secure. And safe environment when we have a dedicated VPN server, we can have extra measures to save ourselves via private tunnelling of VPN.

Future Work: -

We can be using this to detect intrusion to our network by sending information via mail or telephone medium with

- mailsend
- mailsend-nossl
- mstmp
- features of OpenWrt.

```
#!/bin/sh

# script to detect new dhcp lease

# this will be called by dnsmasq everytime a new device is connected
# with the following arguments
# $1 = add | old
# $2 = mac address
# $3 = ip address
# $4 = device name

known_mac_addr="/etc/known_mac_addr"
notification_email="1234567890@txt.att.net"

# check if the mac is in known devices list
grep -q "$2" "$known_mac_addr"
unknown_mac_addr=$?

if [ "$1" == "add" ] && [ "$unknown_mac_addr" -ne 0 ]; then
  msg="New    device    on    `uci    get    system.@system[0].hostname`.`uci    get
dhcp.@dnsmasq[0].domain` $*"
  echo `date` $msg >> /tmp/dhcpmasq.log

  # encode colon (:) and send email
  echo $msg | sed s/:/-/g | sendmail "$notification_email"
fi
```

Appendix and literature survey: -

- ***Working of WIFI***

a computer's wireless adapter translates data into a radio signal and easily transmits it using an antenna. After that, a wireless router receives the signal and decodes it. The router is there also to send information to the internet using a wired Ethernet connection

- ***Working of VPN***

A VPN works by routing your device's internet connection through your chosen VPN's private server rather than your internet service provider (ISP) so that when your data is transmitted to the internet, it comes from the VPN rather than your computer. The VPN acts as an intermediary of sorts as you connect to the internet, thereby hiding your IP address – the string of numbers your ISP assigns your device – and protecting your identity. Furthermore, if your data is somehow intercepted, it will be unreadable until it reaches its destination.

A VPN creates a private "tunnel" from your device to the internet and hides your vital data through something that is known as encryption.

- ***Strategies to hide ourselves***

First, you can use a virtual private network (VPN). For most intents and purposes, a VPN obscures your IP address, and a proxy does the same — and in some cases, even better. A VPN is a private, encrypted network that "tunnels" through a public network (usually the internet) to connect remote sites or users

- ***Use of raspberry pie***

One of the easiest and most practical uses of the Raspberry Pi is as a low-cost web server, which you can use to host simple websites. Cloud-based hosting is arguably easier and more practical, but setting up a basic server is an excellent way to get to grips with server and networking technology