Utilizarea plăcii Raspberry Pi 3 ca Access Point WiFi

La momentul actual nu se poate concepe o rețea locală fără componentă de acces fără fir (WiFi). Prețul dispozitivelor Access Point (ce permit accesul WiFi într-o rețea locală (1)) a scăzut destul de mult și există o diversitate foarte mare de astfel de dispozitive acoperind o funcționalitate variată. Totuși, posibilitatea de personalizare a acestor dispozitive se rezumă de cele mai multe ori la o interfață web destul de sărăcăcioasă cu funcții predefinite pentru o utilizare generică. În cazul în care dorim implementarea unor funcționalități specifice (pentru o rețea de dispozitive IoT de exemplu) ce implică filtrarea traficului, cifrarea traficului sau detectarea și prevenirea intruziunilor suntem obligați să achiziționăm dispozitive AP scumpe cu funcționalități avansate de router (2) / firewall (3).

Placa Raspberry Pi 3 oferă posibilitatea implementării facile a funcționalității de Access Point WiFi datorită celor două interfețe de rețea integrate: interfață ethernet și interfață WiFi, permițând implementarea de funcții avansate (VPN (4), IDS/IDPS(5)) și o personalizare completă a funcționării datorită sistemului de operare Linux. În plus, conectivitatea USB a plăcii permite conectarea de dispozitive de tip modem GSM oferind posibilitatea de conectare la Internet a rețelei locale prin intermediul rețelelor mobile de date (6),(7). Pentru implementarea funcționalității de AP WiFi nu este necesară distribuția Raspbian with Pixel (cu interfață grafică), se poate utiliza și Raspbian Lite deoarece toată configurare se va efectua în linie de comandă (în Terminal). Testarea configurației prezentate s-a făcut pe un sistem Raspberry Pi 3 rulând Raspbian 8 Jessie Lite cu kernel 4.9.28-v7+.

Configurarea interfeței de rețea WiFi

Ambele interfețe de rețea ale plăcii Raspberry Pi 3 (ethernet și WiFi) sunt configurate implicit să funcționeze în rețele locale ce oferă configurație dinamică (prin serviciul de DHCP). Primul pas în implementarea funcționalității de AP WiFi este configurarea adresei IP a interfeței WiFi – modificarea configurației din alocare dinamică în alocare statică – trebuie să stabilim adresa IP a interfeței și clasa de adrese IP pentru viitori clienți WiFi.

Primul lucru este dezactivarea serviciului de configurare dinamincă. Se va edita fișierul */etc/dhcpcd.conf* și se va adăuga la sfârșit următoarea linie:

```
denyinterfaces wlan0
```

După dezactivarea achiziției configurației dinamice trebuie să stabilim adresa IP statică a sistemului. Se va edita fișierul */etc/network/interfaces* și pentru interfața wlan0 se va introduce următoarea configurație:

```
allow-hotplug wlan0
iface wlan0 inet static
        address 192.168.99.1
        netmasq 255.255.255.0
        network 192.168.99.0
        broadcast 192.168.99.255
```

unde 192.168.99.1 este adresa locală a sistemului AP și 192.168.99.0/24 este clasa de adrese a viitorilor clienți WiFi. Se poate alege orice altă clasă de adrese IP nerutabile atâta timp cât nu intră în conflict cu clasa de adrese a interfeței ethernet. Pentru ca modificările să-și facă efectul sistemul trebuie repornit. Atenție!!! Interfața ethernet trebuie să fie conectată al o rețea locală cu acces Internet, interfața WiFi a sistemului va avea rolul, de acum încolo, de AP WiFi, nu va mai putea asigura conectivitatea de rețea normală.

Instalarea și configurarea aplicației HostAPD

Aplicația HostAPD (8) implementează partea de autentificare și control al conexiunilor WiFi. Pentru instalarea acestei aplicații vom rula comanda:

```
sudo apt-get install hostapd
```

După instalare vom crea fișierul */etc/hostapd/hostpad.conf* cu următorul conținut:

```
interface=wlan0
```

```
ssid=Pi3-AP
hw_mode=g
channel=6
ieee80211n=1
wmm_enabled=1
ht_capab=[HT40][SHORT-GI-20][DSSS_CCK-40]
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_passphrase=raspberry
rsn_pairwise=CCMP
```

Denumirea AP-ului și parola de acces pot fi stabilite, bineînțeles, după bunul plac. Fișierul de configurare creat trebuie referit în fișierul de inițializare a aplicației hostapd: */etc/default/hostapd*, prin inserarea următoarei linii:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

După repornirea sistemului vom putea să vedem AP-ul generat de placa Raspberry Pi dar acesta nu va funcționa încă corect.

Instalarea și configurarea aplicației DNSMASQ

Funcționalitatea de Access Point implică în mod obligatoriu două servicii de bază fără de care clienții nu pot accesa rețeaua Internet: serviciul de configurare dinamică a informațiilor IP (DHCP (9)) și serviciul de rezolvare a adreselor IP (DNS (10)). Aplicația DNSMASQ (11) oferă ambele servicii pentru rețele de mici dimensiuni cum este o rețea locală formată de un AP. Instalarea aplicației se va face cu ajutorul comenzii:

```
sudo apt-get install dnsmasq
```

După instalarea aplicație vom înlocui fișierul de configurare (*/etc/dnsmasq.conf*)

```
sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
sudo nano /etc/dnsmasq.conf
```

cu următorul conținut:

```
interface=wlan0
listen-address=192.168.99.1
bind-interfaces
server=8.8.8.8
domain-needed
bogus-priv
dhcp-range=192.168.99.2,192.168.99.100,12h
```

Bineînțeles, adresa interfeței WiFi a AP și plaja de adrese pentru clienții WiFi pot fi personalizate în funcție de alegerea clasei de adrese IP făcută anterior. Pentru ca aplicația DNSMASQ să devină funcțională utilizând configurația stabilită trebuie repornit sistemul.

Activarea rutării pachetelor și configurarea regulilor de rutare

Ultimul pas în configurarea sistemului AP este activarea rutării pachetelor între cele două interfețe de rețea a plăcii Raspberry Pi (12), adică pachetele provenite de la clienții WiFi să fie retrimise spre rețeaua plăcii ethernet (spre Internet). Acest lucru necesită editarea fișierului */etc/sysctl.conf* și decomentarea liniei următoare:

```
net.ipv4.ip_forward=1
```

În plus de activarea rutării este necesar să definim reguli suplimentare deoarece clasa de adrese IP oferită clienților WiFi este privată (13). Aceste reguli vor fi impuse cu ajutorul utilitarului iptables (14) specific sistemului de operare Linux. Vom utiliza următoarea succesiune de instrucțiuni pentru definirea regulilor:

```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state
                          RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

Vom salva apoi regulile într-un fișier:

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
```

Pe care îl vom utiliza pentru reinițializare la fiecare repornire a sistemului. Pentru acest lucru vom adăuga în fișierul */etc/rc.local* următoarea linie (chiar înainte de linia *exit 0*):

```
iptables-restore < /etc/iptables.ipv4.nat
```

După repornirea sistemului vom avea un sistem AP complet funcțional.

Posibile funcționalități suplimentare

Configurarea prezentată este cea mai rapidă modalitate de implementare a funcționalității de AP WiFi pe o placă Raspberry Pi 3, în nici un caz nu este singura soluție – puteți vedea mai multe informații consultând (15), (16), (17), (18), (19), (20).

În plus, sistemul AP poate căpăta funcționalități suplimentare specifice sistemelor router avansate, ca de exemplu:

- Server VPN (Virtul Private Network) ce permite realizarea de canale de comunicație complet cifrate între două sisteme Internet sau între un sistem Internet și un server VPN ce deservește o rețea locală. Distribuția Raspbian 8 Jessy include pachetul *openvpn* (21) ce poate fi instalat cu ajutorul comenzii (se poate consulta și materialul (22)):


```
sudo apt-get install openvpn
```

- Server IDS (Intrusion Detection System) – este un sistem ce permite analiza traficului de rețea în vederea detectării activității malițioase și protejarea calculatoarelor din rețeaua locală. Distribuția Raspbian 8 Jessy include pachetul snort (23) ce poate fi instalat cu ajutorul comenzii (se poate consulta și materialul (24)):


```
sudo apt-get install snort
```

- PPPoE gateway – mulți furnizori de Internet oferă serviciile de acces la Internet prin intermediul unei conexiuni de PPPoE (25), conexiune ce necesită de obicei un echipament specializat. Interfața ethernet a plăcii Raspberry Pi poate fi utilizată și în acest scop utilizând pachetul *ppp* (26). Se poate vedea și materialul (27).

- Server proxy – serviciu ce permite accelerarea traficului web într-o rețea cu conexiune la Internet mai lentă. Distribuția Raspbian include pachetul *squid* (28) ce implementează această funcționalitate. Se poate vedea și materialul (29). Suplimentar, combinând funcționalitatea oferită de pachetul squid cu funcționalitatea oferită de sistemul antivirus *clamav* (30) se poate obține un sistem ce poate scana tot traficul web împotriva aplicațiilor malițioase și a programelor de tip virus. În acest sens se pot consulta materialele (31), (32).

Referințe on-line

(1) Wireless access point
https://en.wikipedia.org/wiki/Wireless_access_point

(2) Router
https://en.wikipedia.org/wiki/Router_(computing)

(3) Firewall
https://en.wikipedia.org/wiki/Firewall_(computing)

(4) Virtual private network
https://en.wikipedia.org/wiki/Virtual_private_network

(5) Intrusion detection system
https://en.wikipedia.org/wiki/Intrusion_detection_system

(6) How to fit a Raspberry Pi with mobile M2M connectivity
https://www.emnify.com/2015/06/18/how-to-fit-a-raspberry-pi-with-mobile-connectivity/

(7) Guide How to use Raspberry Pi with 3G USB Stick
http://copyndone.com/2015/06/27/guide-how-to-use-raspberry-pi-with-3g-usb-stick/

(8) hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator
https://w1.fi/hostapd/

(9) Dynamic Host Configuration Protocol
https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

(10) Domain Name System
https://en.wikipedia.org/wiki/Domain_Name_System

(11) Dnsmasq
http://www.thekelleys.org.uk/dnsmasq/doc.html

(12) How to Enable IP Forwarding in Linux
http://www.ducea.com/2006/08/01/how-to-enable-ip-forwarding-in-linux/

(13) Private network
https://en.wikipedia.org/wiki/Private_network

(14) iptables
https://en.wikipedia.org/wiki/Iptables

(15) Using your new Raspberry Pi 3 as a WiFi access point with hostapd
https://frillip.com/using-your-raspberry-pi-3-as-a-wifi-access-point-with-hostapd/

(16) Turn a RaspBerryPi 3 into a WiFi router-hotspot
https://medium.com/@edoardo849/turn-a-raspberrypi-3-into-a-wifi-router-hotspot-41b03500080e

(17) How-To: Turn a Raspberry Pi into a WiFi router
http://raspberrypihq.com/how-to-turn-a-raspberry-pi-into-a-wifi-router/

(18) Setting WiFi up via the command line
https://www.raspberrypi.org/documentation/configuration/wireless/wireless-cli.md

(19) Turn your Raspberry Pi into a WiFi router
http://yannickloriot.com/2016/03/turn-your-raspberry-pi-into-a-wifi-router/

(20) Setting up a Raspberry Pi as a WiFi access point
https://learn.adafruit.com/setting-up-a-raspberry-pi-as-a-wifi-access-point/

(21) OpenVPN - Open Source VPN
https://openvpn.net/

(22) Raspberry Pi VPN Router
https://gist.github.com/superjamie/ac55b6d2c080582a3e64

(23) Snort - Network Intrusion Detection & Prevention System
https://www.snort.org/

(24) Raspberry Pi Firewall and Intrusion Detection System
http://www.instructables.com/id/Raspberry-Pi-Firewall-and-Intrusion-Detection-Syst/

(25) Point-to-point protocol over Ethernet
https://en.wikipedia.org/wiki/Point-to-point_protocol_over_Ethernet

(26) Linux PPP HOWTO
http://www.tldp.org/HOWTO/PPP-HOWTO/

(27) how connect my Pi to Internet through PPPoE connection?
https://raspberrypi.stackexchange.com/questions/50982/how-connect-my-pi-to-internet-through-pppoe-connection

(28) Squid: Optimising Web Delivery
http://www.squid-cache.org/

(29) Using a Raspberry Pi as a Squid proxy cache
https://the-server.ninja/2016/03/26/using-a-raspberry-pi-as-a-squid-proxy-cache/

(30) ClamavNet
https://www.clamav.net/

(31) SquidClamav : Securing Web Delivery (antivirus for Squid)
http://squidclamav.darold.net/

(32) SquidClamav Proxy Scanner on A Raspberry Pi Model B
http://how2itstuff.blogspot.ro/2015/04/squidclamav-proxy-scanner-on-raspberry.html