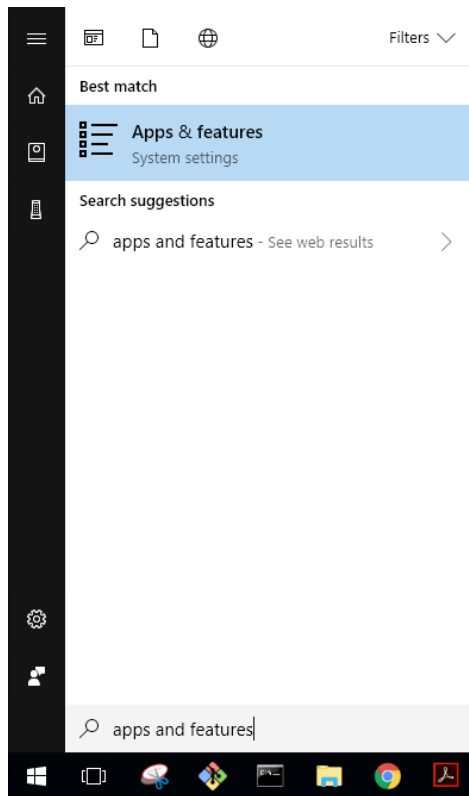


Лабораториска вежба број 3 - Зајакнување на вашите уреди

Зајакнување на безбедноста на лаптоп компјутер (Windows 10)












Апликациите се еден од главните извори на ранливости на компјутерските системи, особено оние кои не се ажурирани. Со цел да ја намалиме површината врз која се воопшто можни напади, се препорачува да се ослободиме од софтверот кој не го користиме.

Во Windows 10, деинсталација на апликации се прави преку **Apps & features**.



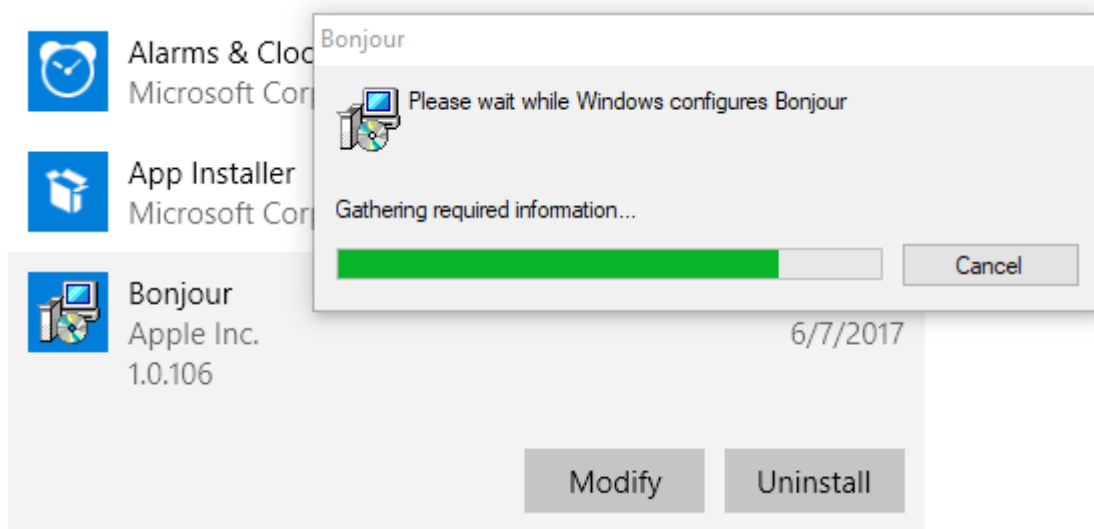
Пристап до Apps & features преку менито

Apps & features

	Adobe Systems Incorporated	2/20/2018
	Adobe Creative Cloud Adobe Systems Incorporated	248 MB 2/28/2018
	Alarms & Clock Microsoft Corporation	16.0 KB 3/1/2018
	App Installer Microsoft Corporation	16.0 KB 11/14/2017
	Bonjour Apple Inc.	6.44 MB 6/7/2017
	Calculator Microsoft Corporation	144 KB 2/28/2018
	Camera Microsoft Corporation	40.0 KB 2/14/2018
	Cisco eReader Cisco Systems	53.4 MB 2/28/2018
	Cisco Packet Tracer 7.0 64Bit Cisco Systems, Inc.	219 MB 7/5/2017
	CodeBlocks The Code::Blocks Team	2/28/2018
	Composer - Php Dependency Manager getcomposer.org	1.43 MB 9/6/2017

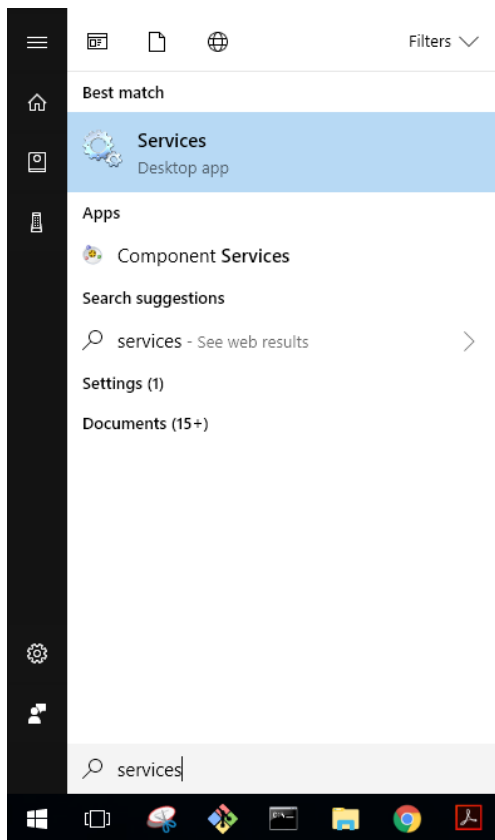
Листа на инсталирани апликации

Од листата на инсталираните апликации ги одбираме оние кои не ги користиме и ги деинсталираме.

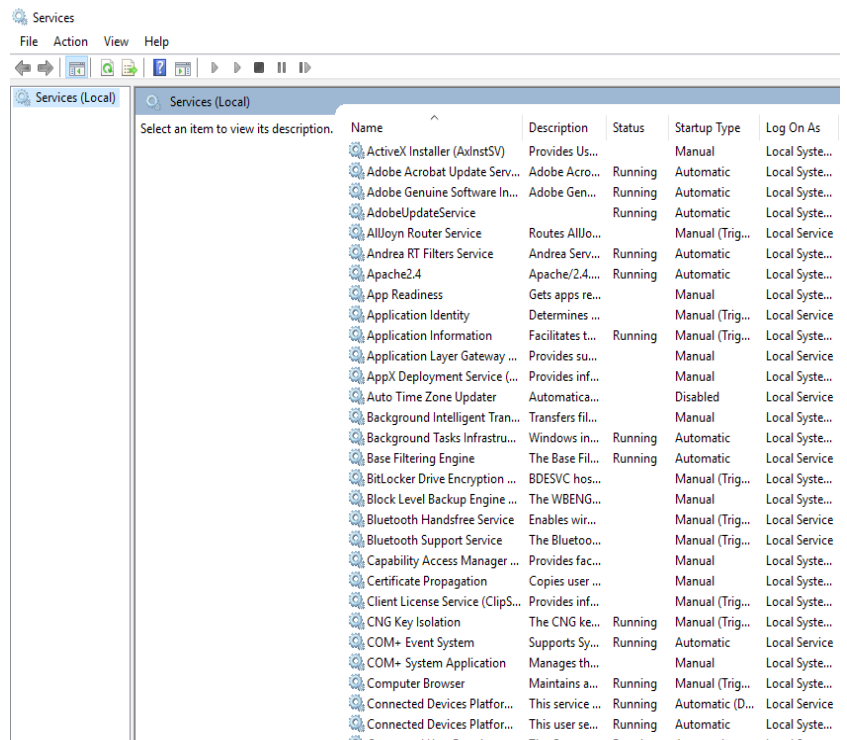


Деинсталација на апликација

Следно нешто што може да го направме е да ги исклучиме сервисите кои не ни се потребни.

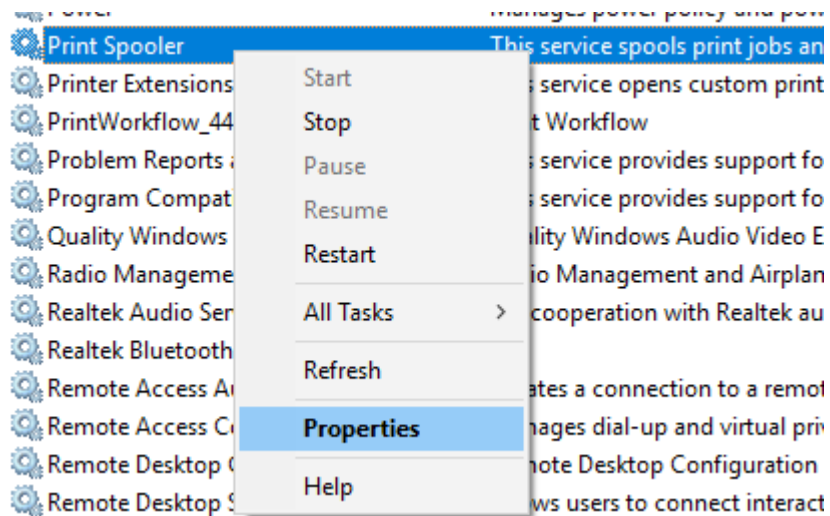


Пристап до Services преку менито

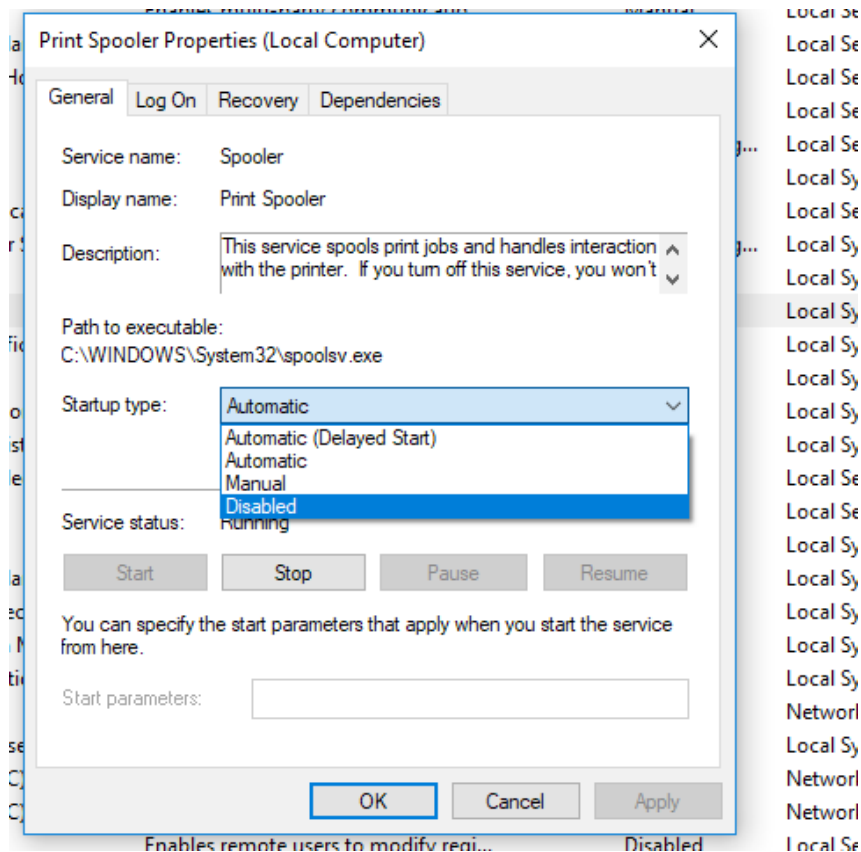


Листа на сервиси

Во колоната Description е даден опис за секој од сервисите, односно пишува за што служи и што ќе биде оневозможено доколку го исклучиме. Бидејќи јас немам принтер, сервисот *Print Spooler* не ми е потребен. Поради тоа можам да го стопирам и онеспособам овој сервис.

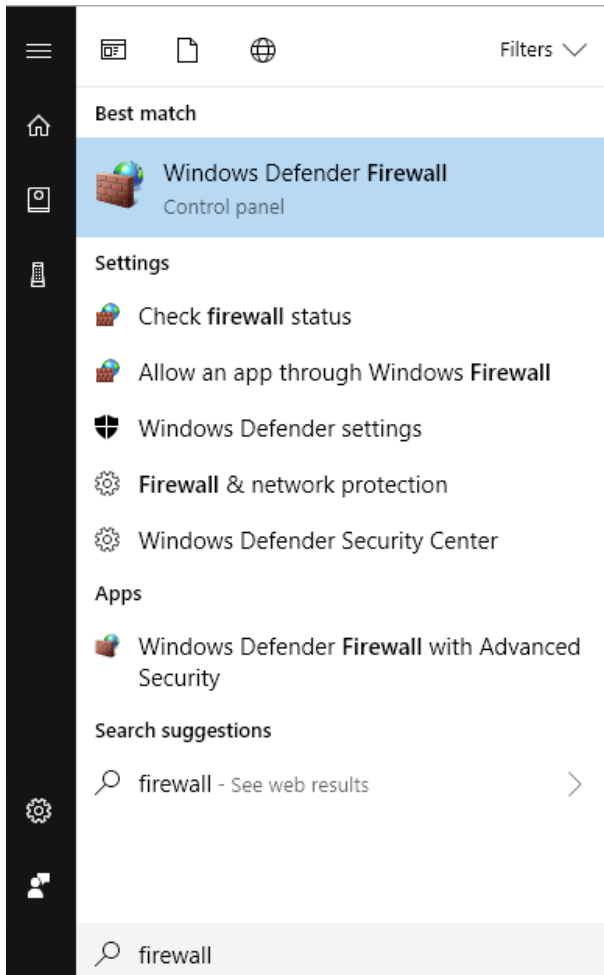


Со десен клик → Properties пристапуваме до прозорецот за подесување на соодветниот сервис

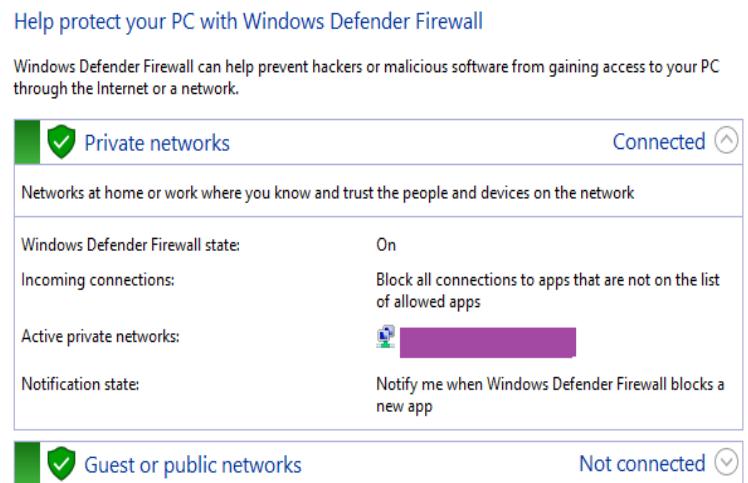


Онеспособување на автоматско вклучување сервисот

Следно нешто што треба да го направиме е да се осигураме дека имаме активен firewall и истиот е соодветно подесен. Во Windows 10 има вграден firewall – **Windows Defender Firewall**



Пристап до Windows Defender Firewall преку менито

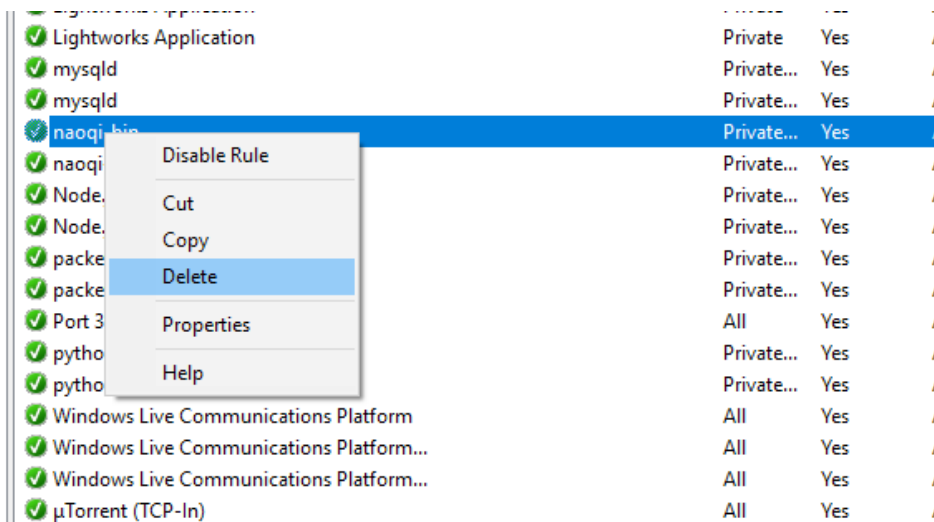


Состојбата на Windows Firewall: активен

Може да извршиме детален преглед на сите правила, да додадеме нови (да блокираме или пропуштиме некоја апликација низ firewall-от), да избришеме постоечки правила, ИТН.

Name	Group	Profile	Enabled	Action	Override	Program
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Program Files\Mozilla Firefox\firefox.e
launch		Private	Yes	Block	No	C:\program files\openshot video editor\
launch		Private	Yes	Block	No	C:\program files\openshot video editor\
Lightworks Application		Private	Yes	Allow	No	C:\Program Files\Lightworks\ntcardvt.ex
Lightworks Application		Private	Yes	Allow	No	C:\Program Files\Lightworks\ntcardvt.ex
mysqld		Private...	Yes	Allow	No	C:\xampp\mysql\bin\mysqld.exe
mysqld		Private...	Yes	Allow	No	C:\xampp\mysql\bin\mysqld.exe
naoqi-bin		Private...	Yes	Allow	No	C:\program files (x86)\aldebaran robotic
naoqi-bin		Private...	Yes	Allow	No	C:\program files (x86)\aldebaran robotic
Node.js: Server-side JavaScript		Private...	Yes	Allow	No	C:\program files\nodejs\node.exe
Node.js: Server-side JavaScript		Private...	Yes	Allow	No	C:\program files\nodejs\node.exe
packettracer7		Private...	Yes	Allow	No	C:\program files\cisco packet tracer 7.0\
packettracer7		Private...	Yes	Allow	No	C:\program files\cisco packet tracer 7.0\
Port 3306		All	Yes	Allow	No	Any
python		Private...	Yes	Allow	No	C:\python27\python.exe
python		Private...	Yes	Allow	No	C:\python27\python.exe
Windows Live Communications Platform		All	Yes	Allow	No	C:\Program Files (x86)\Windows Live\Co
Windows Live Communications Platform...		All	Yes	Allow	No	Any
Windows Live Communications Platform...		All	Yes	Allow	No	Any
µTorrent (TCP-In)		All	Yes	Allow	No	C:\Users\va\AppData\Roaming\utorrent\
µTorrent (UDP-In)		All	Yes	Allow	No	C:\Users\va\AppData\Roaming\utorrent\
@{Microsoft.Windows.CloudExperience...}	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow	No	Any
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
App Installer	App Installer	Domai...	Yes	Allow	No	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%SystemRoot%\system32\svchost.exe
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%SystemRoot%\system32\svchost.exe

Листа на сите inbound правила (во внатрешна насока)



Бришење на правило од листата

Од клучно значење е софтверот на компјутерот секогаш да е ажуриран, особено оперативниот систем. Поради тоа треба да се осигураме дека **Windows Update** е активен и дека Windows ја има најновата верзија.

Windows Update

Update status



Your device is up to date. Last checked: Today, 3:26 AM

Check for updates

[View installed update history](#)

Проверка на статусот на Windows Update

Пожелно е да се подеси автоматска проверка за нови верзии и ажурирање на оперативниот систем со цел секогаш да ја имаме најновата верзија која ги содржи сите мерки против најновите безбедносни закани.

Исто така, многу е важно да инсталираме антивирусен софтвер и истиот да има ажурирани дефиниции. Бидејќи на овој компјутер има Windows 10 со кој доаѓа вграден **Windows Defender**, одлучив да не инсталирам друг.

Your device is being protected.

Last threat scan: 3/2/2018
Last threat definition update: 3/7/2018
Last health scan: 3/7/2018



Virus & threat protection
No action needed.



Device performance & health
No action needed.



Firewall & network protection
No action needed.



App & browser control
No action needed.



Family options
Manage how your family uses their devices.

Дефинициите на Windows Defender се ажурирани. Последното скенирање е пред 5 денови.

Пожелно е Windows Defender да е подесен автоматски да ги ажурира дефинициите и периодично да извршува скенирање на компјутерот.

Last scan

Windows Defender Antivirus automatically scans your device for viruses and other threats to help keep it safe.

Last scan: 3/2/2018 (quick scan)

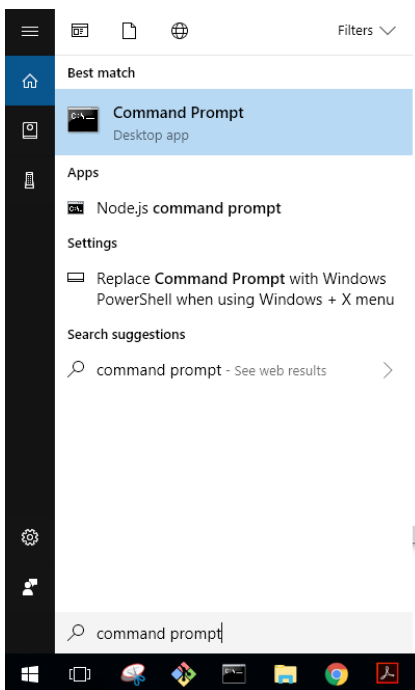
No threats found.

25524 files scanned.

Краток преглед на последното скенирање

Зајакнување на безбедноста на безжична точка на поврзување (wireless access point)

Модерните рутери најчесто имаат web интерфејс за администрирање. До истиот може да се пристапи со локалната IP адреса на рутерот. Доколку не ја знаеме, може да се обидеме со преглед на излезот од командата **ipconfig**, во која може да се види кој е Default Gateway на нашиот компјутер, а тоа е најчесто адресата на рутерот.



Пристап до Command Prompt преку менито

```
C:\Users\v>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

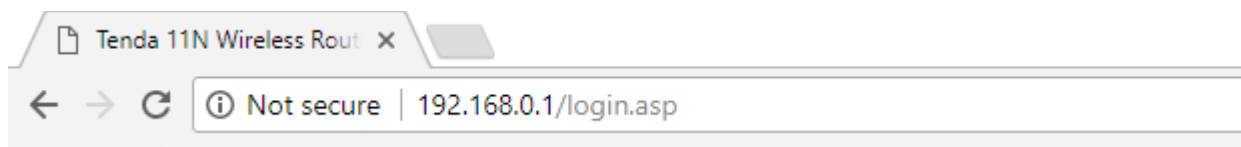
    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\v>
```

Излезот од командата ipconfig



Во мојот случај адресата на рутерот е 192.168.0.1, па преку веб прелистувач пристапим до неговиот интерфејс за конфигурација.

Во зависност од моделот на рутерот, опциите ќе бидат различни но генерално ја следат истата шема. SSID е името на безжичната мрежа. Секогаш е потребно да се промени default вредноста бидејќи најчесто тоа е моделот на рутерот, што за напаѓачите може да биде голема предност ако го знаат (особено ако и лозинката за пристап е оставена на default вредноста). Следно, потребно е да се постави безбедносен режим, односно соодветен безбедносен протокол кој ќе нуди силна енкрипција. Денес, WPA2 е издржан стандард до кој се препорачува да се придржуваме и најбезбедната опција. Бидејќи на мојот рутер беше поставено WPA, го променив во WPA2. Исто така се препорачува да се користи безбедна лозинка, која содржи повеќе од 8 карактери, меѓу кои: големи и мали букви, специјални знаци и броеви.

Wireless Security Setup

Select SSID

Security Mode

WPA Algorithms AES(Recommended) TKIP TKIP&AES

Security Key
Default: 12345678

To configure a wireless security key, disable the WPS below!

WPS Settings Disable Enable

Wireless Security Setup

Select SSID

Security Mode

WPA Algorithms

Security Key

To configure a wireless security key, disable the WPS below!

WPS Settings Disable Enable

Подесување на безбедносен протокол

За потребите на оваа вежба, ја тестирав MAC Filter опцијата на мојот рутер.

Со командата `ipconfig /all` ја дознав MAC адресата на мојот лаптоп, а потоа на рутерот подесив да се оневозможи пристап на сите други MAC адреси освен на таа.

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8723BE 802.11 bgn Wi-Fi Adapter
Physical Address. . . . . :
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.0.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, March 6, 2018 11:02:22 PM
Lease Expires . . . . . : Wednesday, March 14, 2018 2:38:23 AM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DNS Servers . . . . . : 8.8.8.8
                        8.8.4.4
```

Access Control

Select SSID	<input type="text" value=""/>
MAC Address Filter	Permit
MAC Address	Operate
<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	<input type="button" value="Add"/>

Сите останати MAC адреси ќе бидат блокирани

Се обидов да се конектирам на мрежата од мојот смартфон, и мојот обид беше неуспешен поради MAC филтрирањето кое го поставив на рутерот. Единствено беше можно да се пристапи од лаптопот чија MAC адреса е дозволена.

Ги тестирав и следните опции на рутерот:

URL Filter Settings

Filter Mode	Forbid Only
Access Policy	(1)
Policy Name(Optional)	block_fb
Start IP	192.168.0.104
End IP	192.168.0.104
URL Character String	facebook.com
Time	0 : 0 ~ 0 : 0
Day(s)	Sun ~ Sat
Enable	<input checked="" type="checkbox"/> Clear this item: <input type="button" value="Clear"/>

Блокирање пристап до facebook.com на IP адресата соодветна на мојот смартфон

