

به نام خدا

عنوان پروژه : فیلتر کردن packet های ورودی به کارت شبکه

استاد درس : دکتر ملک زاده

نام ارایه دهنده : ابوالفضل بیات

فهرست

فصل صفر مقدمه

فصل اول کانفیگ کردن سیستم ها

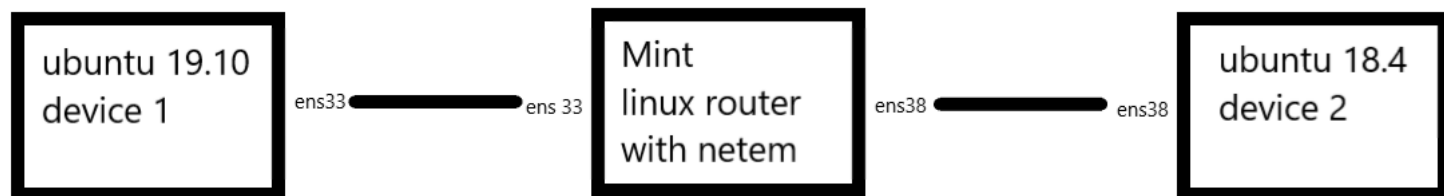
فصل دوم ساخت فیلتر

منابع

در این مطلب قصد دارم روش فیلتر کردن packet های ورودی به کارت شبکه شما رو توضیح بدم , در این مطلب من از سه سیستم لینوکس برای پیاده کردن این روش استفاده کردم که یک سیستم در بین دو سیستم دیگر قرار میگیرد , به نوعی linux router می باشد و packet های ارسالی از سیستم لینوکسی شماره یک به این سیستم ارسال می شود و سپس از این سیستم به سیستم لینوکسی شماره دو فرستاده می شود

فصل اول : کانفیگ کردن سیستم ها

برای کانفیگ کردن سیستم های خود به صورت زیر عمل میکنیم



linux router => mint

Ip addres ens33 : 192.168.88.138

Ip addres ens38 : 192.168.126.203

Netmask : 255.255.255.0

Device 1 => ubuntu 19.10

Ip address : 192.168.88.137

Netmask : 255.255.255.0

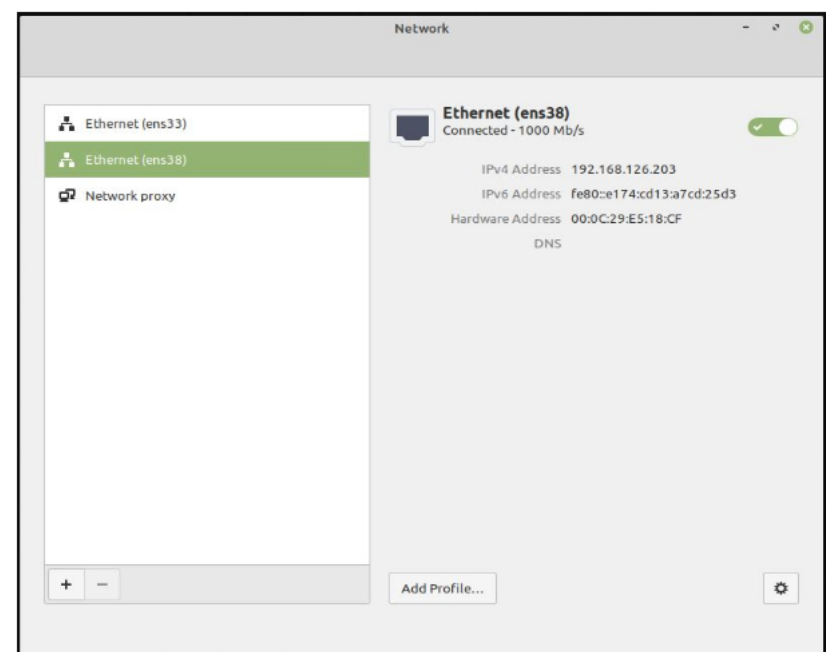
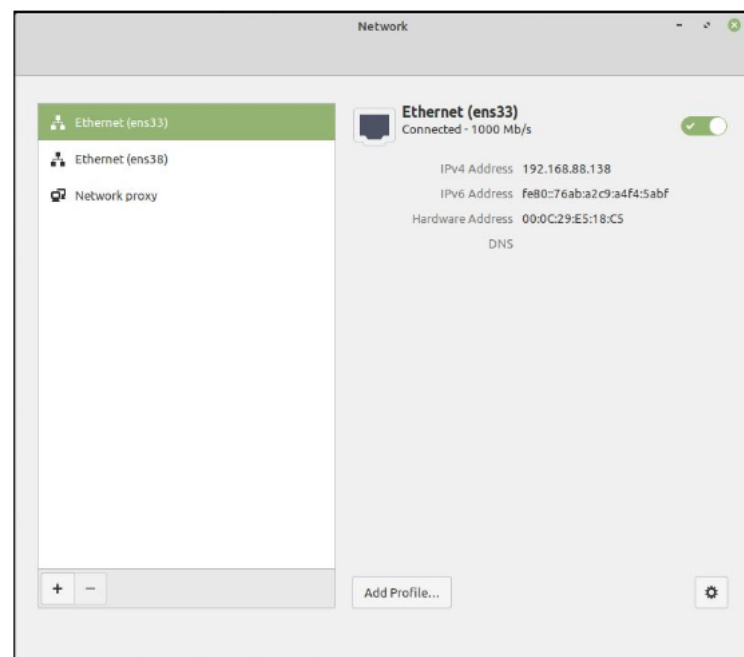
Geteway : 192.168.88.138

Device 2 => ubuntu 18.04

Ip address : 192.168.126.200

Netmask : 255.255.255.0

Gateway : 192.168.126.203



Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

Link speed

1000 Mb/s

IPv4 Address

192.168.88.137

IPv6 Address

fe80::158e:21f1:8746:c3bf

Hardware Address

00:0C:29:89:DB:E7

Default Route

192.168.88.138

DNS

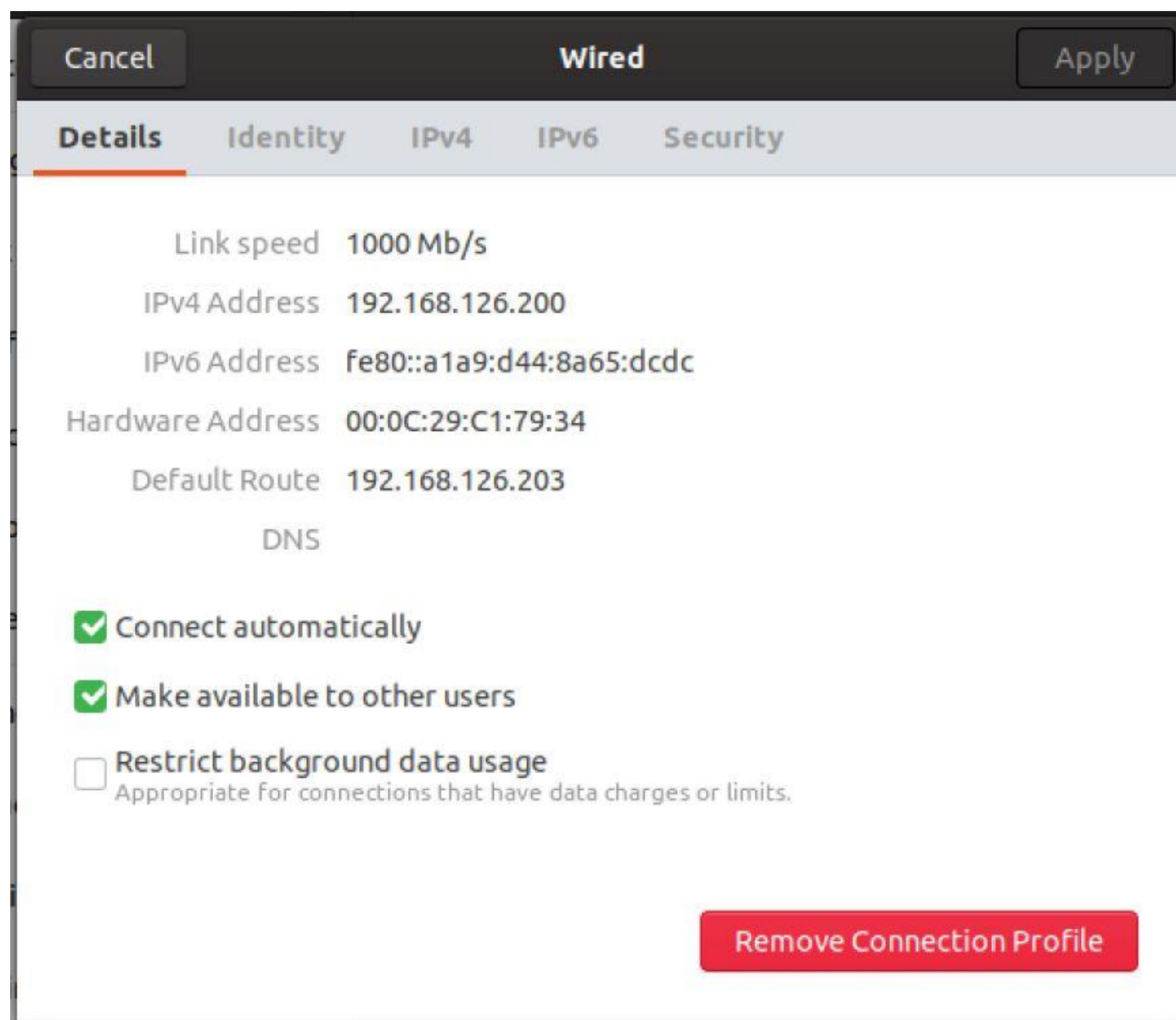
☒ Connect automatically

☒ Make available to other users

☐ Restrict background data usage

Appropriate for connections that have data charges or limits.

Remove Connection Profile



برای کانفیگ کردن ip سیستم ها می توانید از محیط ترمینال نیز استفاده کنید

ست کردن آدرس ip :

```
# ifconfig ens33 192.168.126.200
```

ست کردن netmask :

```
# ifconfig ens33 netmask 255.255.255.0
```

ست کردن gateway :

```
# route add default gw 192.168.126.203
```

و به همین صورت برای سیستم های دیگر هم تنظیم میکنیم ...

فصل دوم : ساخت فیلتر

برای انجام شدن این عملیات routing این دستور را در لینوکس روتر (linux mint) میزنیم

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

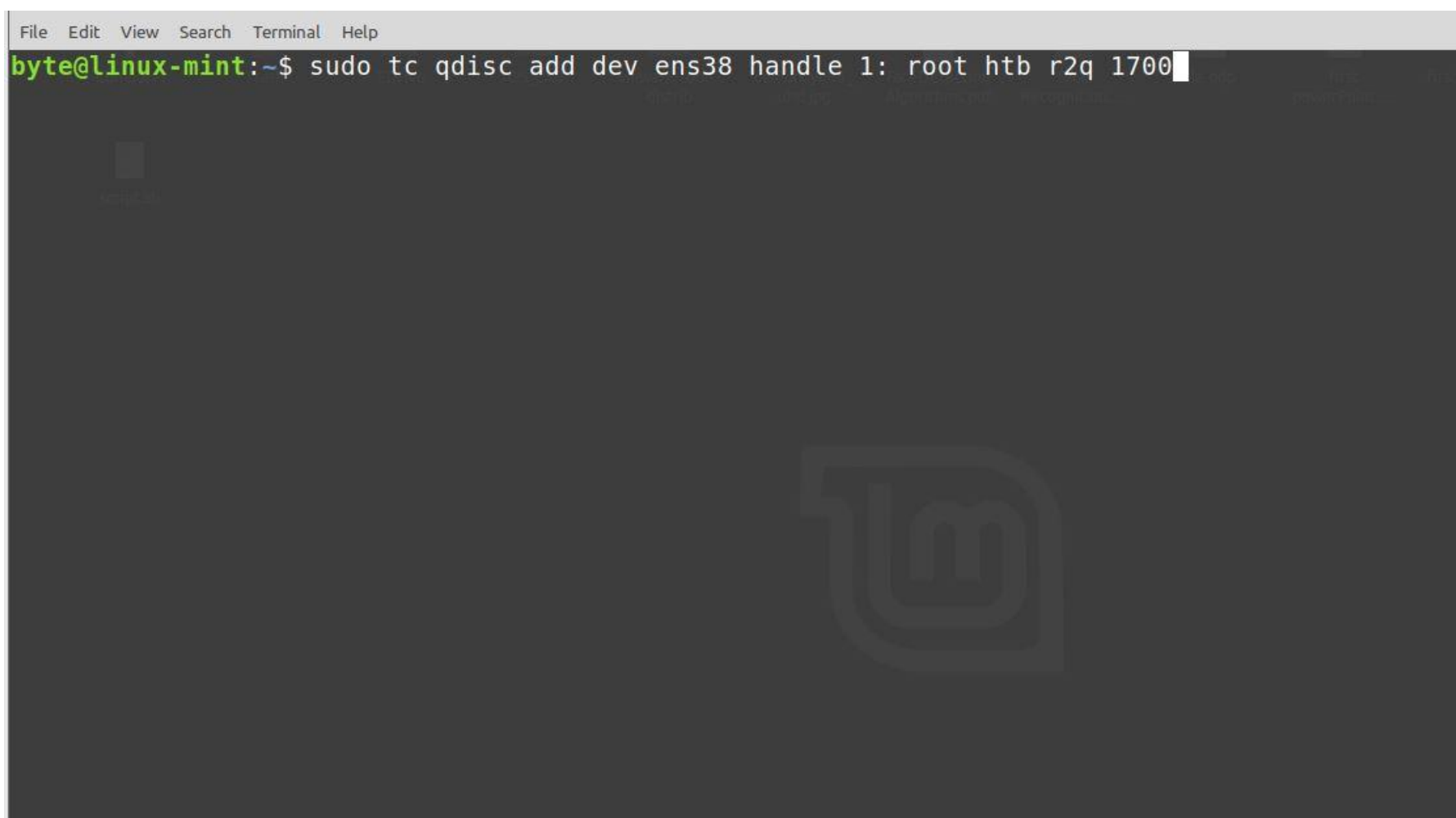
```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
bash: /proc/sys/net/ipv4/ip_forward: Permission denied
byte@linux-mint:~$ sudo su
root@linux-mint:/home/byte# echo 1 > /proc/sys/net/ipv4/ip_forward
root@linux-mint:/home/byte#
```

حالا باید کانفیگ هایی را بر روی کارت شبکه ens38 انجام دهیم تا تمام بسته های tcp را که به 192.168.126.200 و پورت 80 یا 21 , 20 (ترافیک http و ftp) می روند را فیلتر کند

ساخت class و qdisc ها

```
# tc qdisc add dev ens38 handle 1: root htb r2q 1700
```

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc qdisc add dev ens38 handle 1: root htb r2q 1700
```



```
# tc class add dev ens38 parent 1: classid 1:1 htb rate 100Mbps ceil 100Mbps
```

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc class add dev ens38 parent 1: classid 1:1 htb rate 100Mbps ceil 100Mbps
byte@linux-mint:~$
```

Tc class add dev ens38 parent 1:1 classid 1:20 htb rate 100Mbps

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc class add dev ens38 parent 1:1 classid 1:20 htb rate 100Mbps
byte@linux-mint:~$
```

tc qdisc add dev ens38 parent 1:20 handle 12: netem trace test.bin 10

File Edit View Search Terminal Help

```
byte@linux-mint:~$ sudo tc qdisc add dev ens38 parent 1:20 handle 12: netem trace test.bin 0 1
```

What is "trace"?

```
Usage: ... netem [ limit PACKETS ]  
                [ delay TIME [ JITTER [CORRELATION]] ]  
                [ distribution {uniform|normal|pareto|paretonormal} ]  
                [ corrupt PERCENT [CORRELATION]]  
                [ duplicate PERCENT [CORRELATION]]  
                [ loss random PERCENT [CORRELATION]]  
                [ loss state P13 [P31 [P32 [P23 P14]]]]  
                [ loss gemodel PERCENT [R [1-H [1-K]]]]  
                [ ecn ]  
                [ reorder PRECENT [CORRELATION] [ gap DISTANCE ]]  
                [ rate RATE [PACKETOVERHEAD] [CELLSIZE] [CELLOVERHEAD]]
```

```
byte@linux-mint:~$
```

ساختن فیلتر

tc filter add dev ens38 parent 1:0 prio 1 protocol ip u32

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 protocol ip u32
byte@linux-mint:~$
```

tc filter add dev ens38 parent 1:0 prio 1 handle 1: u32 divisor 1

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 handle 1: u32 divisor 1
```

tc filter add dev ens38 parent 1: protocol ip prio 1 u32 ht 800:: match
:u8 0 0 offset at 0 mask 0x0f00 shift 6 link 1

```
File Edit View Search Terminal Help
byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1: protocol ip prio 1 u32 ht 800:: match u8 0 0 offset at 0 ma
sk 0x0f00 shift 6 link 1:
```

```
# tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 80
xffff match ip protocol 6 0xff match ip src 192.168.88.137/24 match ip dst
flowid 1:20 192.168.126.200
```

A terminal window with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (byte@linux-mint). The command prompt shows the execution of a tc filter command: `byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 80 0xffff match ip protocol 6 0xff match ip src 192.168.88.137/24 match ip dst 192.168.126.200 flowid 1:20`. The command is executed successfully, and the prompt returns to the shell.

```
byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 80 0xffff match ip protocol
6 0xff match ip src 192.168.88.137/24 match ip dst 192.168.126.200 flowid 1:20
```

```
# tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 20
xfffe match ip protocol 6 0xff match ip src 192.168.88.137/24 match ip dst
flowid 1:20 192.168.126.200
```

A terminal window with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (byte@linux-mint). The command prompt shows the execution of a tc filter command: `byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 20 0xfffe match ip protocol 6 0xff match ip src 192.168.88.137/24 match ip dst 192.168.126.200 flowid 1:20`. The command is executed successfully, and the prompt returns to the shell.

```
byte@linux-mint:~$ sudo tc filter add dev ens38 parent 1:0 prio 1 u32 ht 1: match tcp dst 20 0xfffe match ip protocol
6 0xff match ip src 192.168.88.137/24 match ip dst 192.168.126.200 flowid 1:20
```

با این روش توانستیم تمام packet های دریافتی به کارت شبکه مورد نظر را فیلتر کنیم

منابع

Linux advanced routing and traffic control howto: <http://lartc.org/howto>

Netem: <http://linux-net.osdl.org/index.php/Netem>

پایان