

# شبکه در لینوکس

فرامین شبکه‌ای در لینوکس

اشاره:

یکی از دغدغه‌های اصلی کاربران علاقه‌مند به لینوکس گنگ‌بودن امکانات این سیستم‌عامل است. سؤالی که اغلب کاربران لینوکس پس از نصب این سیستم‌عامل با آن مواجه می‌شوند این است که چگونه می‌توان شبکه‌ای مطمئن و امن را تنظیم کرد و چگونه می‌توان از امکانات لینوکس بهره‌مند شد. برای انجام تنظیمات سیستمی باید به کدام بخش مراجعه کرد، تنظیمات شبکه در لینوکس به چه شکل است و...

بیشتر کاربران لینوکس نسبت به این موضوع آگاهی دارند که اغلب کارهایی که در ویندوز می‌توان انجام داد در لینوکس نیز انجام پذیر است. اما در روش پیاده‌سازی آن‌ها تفاوت‌هایی وجود دارد که باید به مرور با این تفاوت‌ها آشنا شد. در این مقاله سعی شده که بخشی از همین مبحث مورد بررسی قرار گیرد. چنانچه شما به تنظیمات شبکه‌ای علاقه‌مند باشید، به یقین یکی از جذاب‌ترین و کاربردی‌ترین قسمت‌ها، راه‌اندازی شبکه در محیط لینوکس و تنظیمات شبکه است. از آنجا که کاربران شبکه، کاردر محیط خط‌فرمان را به راهنماهای بصری ترجیح می‌دهند، به طور مستقیم سراغ فرامین شبکه‌ای در لینوکس می‌رویم.

## پینگ در لینوکس

پینگ (Ping) يك دستور رایج در تمام سیستم‌عامل‌ها برای بررسی دسترسی به شبکه است. زمانی که شما در ترمینال يك دستور ping و يك IP آدرس را وارد می‌کنید، در واقع ماشین تلاش می‌کند تا يك سری بسته ICMP را به ماشینی با آدرس IP موردنظر شما ارسال کند. کاربرد اصلی این فرمان مطلع شدن از وضعیت یک هاست در شبکه است، اگر یک هاست در شبکه باشد (و فایروالی جلوی ICMP آن را نبسته باشد) باید به بسته‌های دریافتی پاسخ داده و با نمایش Reply حضور خود را به طرف مقابل اعلام دارد. ضمن آنکه مدت پاسخ‌گویی به هر بسته ارسالی نیز، نشان از وضعیت سلامت مسیر ارتباطی دارد. اما اگر بخواهیم کمی از این فرمان به صورت پیشرفته‌تر استفاده کنیم و با استفاده از آن از وضعیت سیستم‌هایی که در شبکه هستند، مطلع شویم ابتدا باید به محیط ترمینال لینوکس مراجعه کرده و Vim را با دسترسی Root اجرا کرده و خطوط زیر را وارد کنیم.

```
# vim /usr/bin/netup.sh
#/bin/bash
for i in 192.168.1.{1..255};
do
ping -c2 $i > /dev/null;
[ $? -eq 0 ] && echo $i is up.
trap "Exit" SIGINT
done
```

پس از ذخیره کردن فایل در آدرس /usr/bin/netup.sh جهت اجرایی کردن آن دستور زیر را وارد کنید.

```
chmod a+x /usr/bin/netup.sh
```

حال اسکریپت ایجاد شده را اجرا کنید.

```
[slynux@gnuxbox ~]$ netup.sh
192.168.1.1 is up.
192.168.1.3 is up.
192.168.1.4 is up.
```

همانطور که مشاهده می‌کنید آدرس‌های آی‌پی‌ای که در شبکه وجود دارد در این اسکریپت در وضعیت UP قرار می‌گیرند.

### تنظیم یک شبکه

برای راه‌اندازی یک سیستم در شبکه ابتدا باید به آن آدرس IP داده شود، برای انجام این کار هم می‌توانید به صورت دستی آدرس IP را به سیستم معرفی کرده و هم می‌توانید (در صورت وجود DHCP سرور) آن را به صورت خودکار پیاده سازی کنید. برای تنظیم دریافت خودکار IP دستور dhclient را وارد کنید تا تقاضای دریافت نشانی IP را به سرور DHCP منتقل سازید. با این عمل سرور DHCP با توجه به IP‌های موجود نشانی را به سیستم تخصیص خواهد داد. توجه داشته باشید، IP تخصیص داده شده در هر بار وارد کردن دستور فوق می‌تواند متفاوت باشد.

### اطلاع از وضعیت کارت‌های شبکه

اگر می‌خواهید از وضعیت کارت‌های شبکه روی سیستم آگاه شوید یا آدرس IP آن‌ها را بیابید، در ترمینال فرمان `ifconfig -a` را وارد کنید :

```
[slynux@gnuxbox ~]# ifconfig -a
eth0 Link encap:Ethernet HWaddr 00:1C:23:FB:37:22
inet6 addr: fe80::21c:23ff:fe87:25d2/64 Scope:Link
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:9724 errors:0 dropped:0 overruns:0 frame:0
TX packets:2720 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2400589 (2.2 MiB) TX bytes:645396 (630.2 KiB)
Interrupt:17
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:76320 errors:0 dropped:0 overruns:0 frame:0
TX packets:76320 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:87151068 (83.1 MiB) TX bytes:87151068 (83.1 MiB)
wlan0 Link encap:Ethernet HWaddr 00:1C:BF:87:25:D2
inet addr:192.168.1.143 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::21c:bfff:fe87:25d2/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:45302 errors:0 dropped:0 overruns:0 frame:0
TX packets:37510 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:31091293 (29.6 MiB) TX bytes:9734025 (9.2 MiB)
```

در اینجا ما سه کارت شبکه به نامهای eth0 ، lo و wlan0 داریم:  
**eth0** که معادل همان کارت‌های شبکه کابلی است و نشانی IPv6 دارد (fe80::21c:23ff:febf:3722).  
**lo** که معادل حلقه بازگشتی (Loop Back) اشاره به Local Host یا کامپیوتر جاری است (0.0.0.1).  
**wlan0** معادل با یک کارت شبکه LAN بی‌سیم است و نشانی IPv4 دارد (192.168.1.143).

### تخصیص IP به صورت دستی

برای تخصیص IP به صورت دستی دستور زیر را اجرا کنید:  
< ifconfig نام کارت شبکه < IP > نشانی  
به عنوان مثال:

```
ifconfig eth0 192.168.0.2
```

اگر بخواهیم وضعیت کارت شبکه eth0 را ببینیم، دستور ifconfig eth0 را وارد خواهیم کرد.

```
[root@gnubox slynux]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:1C:23:FB:37:22
inet addr:192.168.0.2 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::21c:23ff:febf:3722/64 Scope:Link
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:9724 errors:0 dropped:0 overruns:0 frame:0
TX packets:2720 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2400589 (2.2 MiB) TX bytes:645396 (630.2 KiB)
Interrupt:17
```

برای تغییر Subnet Mask از حالت پیش فرض به حالتی که مدنظرتان است این دستور را وارد کنید:

```
ifconfig eth0 192.168.0.2 netmask 255.255.255.0
```

اگر بخواهیم کارت شبکه‌ای را فعال کنیم، از فرمان ifup و برای غیرفعال کردن آن از ifdown استفاده خواهیم کرد .

```
ifup eth0
ifdown eth0
```

### شبکه‌های بی‌سیم

برای یافتن نام (ESSID) شبکه‌های مجاورتان باید از دستور iwlist استفاده کنید.

```
[root@gnubox~]# iwlist wlan0 scan
wlan0 Scan completed :
Cell 01 - Address: 00:08:5C:52:E9:83
ESSID:"slynux"
```

```
Mode:Master
Channel:11
Frequency:2.462 GHz (Channel 11)
Quality=92/100 Signal level:-39 dBm Noise level=-78 dBm
Encryption key:off
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
24 Mb/s; 36 Mb/s; 54 Mb/s; 6 Mb/s; 9 Mb/s
12 Mb/s; 48 Mb/s
Extra:tsf=00000000fc021187
```

دستورات فوق فهرستی از شبکه‌های مختلف بی‌سیم را که توسط کارت شبکه‌تان قابل شناسایی هستند، نمایش خواهند داد. پس از یافتن نام شبکه، از دستور دیگری به نام iwconfig برای اتصال به یکی از این شبکه‌ها استفاده خواهیم کرد. این دستور شباهت زیادی به ifconfig دارد، با این تفاوت که پارامترهای دیگری را که برای اتصال به شبکه‌های بی‌سیم نیاز دارید نیز در اختیار شما قرار خواهد داد. در این مثال فرض بر این است که نام (ESSID) شبکه بی‌سیم ما slynux است و کلمه عبور (Pass Key) آن 8c140b2037 است.

```
iwconfig wlan0 essid slynux key 8c140b2037
```

پس از اتصال به شبکه موردنظر با اجرای دستور ifconfig یک نشانی IP به کارت شبکه خودتان اختصاص دهید:

```
ifconfig wlan0 192.168.0.5
```

چنانچه نقطه دسترسی (AP) موردنظر امکان تخصیص IP را به صورت خودکار داشته باشد (DHCP)، به جای دستی وارد کردن IP از دستور زیر استفاده کنید:

```
dhclient wlan0
```

تنظیماتی که شما با دستور ifconfig اعمال می‌کنید تنها تا زمانی که سیستم را راه‌اندازی دوباره نکنید، قابل استفاده هستند. به همین دلیل، پس از هر بار راه‌اندازی دوباره، تنظیمات به حالت اولیه باز خواهد گشت. برای اجتناب از این امر کافی است کدهای اسکریپتی را که در ادامه خواهیم گفت، در محل مناسب ذخیره‌سازی کنید. چنانچه شما از سیستم عامل اوبونتو (و یا هر سیستم عامل دیگری که بر پایه دیبیا طراحی شده است) استفاده می‌کنید، کافی است به این مسیر مراجعه کنید `/etc/networks/interfaces`. سپس تغییرات لازم را در آنجا اعمال کنید.

```
auto lo
iface lo inet loopback
```

```
iface eth0 inet static
address 164.164.32.101
netmask 255.255.255.240
gateway 164.164.32.97
```

۱- چنانچه مایل هستید eth0 از DHCP سرور IP دریافت کند، دستورات زیر را به این بخش اضافه کنید:

```
auto eth0
iface eth0 inet dhcp
```

۲- چنانچه تمایل دارید تا IP استاتیک خود را تنظیم کنید، دستورات زیر را وارد کنید.

```
auto eth0
iface eth0 inet static
address <ip_address>
netmask <netmask>
gateway <gateway_ip>
```

۳- چنانچه از شبکه‌های بی سیم استفاده می‌کنید دستورات زیر را به خطوط فرمان قسمت قبلی اضافه کنید.

```
wireless-essid <network_name>
wireless-key <key>
```

حال برای راه‌اندازی دوباره سرویس شبکه، دستور زیر را در شاخه root ترمینال وارد کنید:

```
/etc/init.d/network restart
```

### جعل کردن آدرس MAC

همان‌طور که می‌دانید آدرس MAC یک شناسه یکتا برای هر ابزار شبکه‌ای به شمار می‌آید. این یکتا بودن در بعضی از موارد محدودیت‌هایی را ایجاد می‌کند، به‌عنوان مثال، برخی از سرویس‌دهندگان اینترنتی براساس آدرس MAC مشتریان به آن‌ها سرویس می‌دهند. از این‌رو، فرض کنید قرار باشد یک سیستم جدید وارد شبکه داخلی شما شود (که به یقین آدرس MAC جدید خواهد داشت).

در این سناریو شما مجبور هستید، آدرس MAC جدید را به سرویس‌دهنده اینترنت خود گزارش دهید. امروزه، استفاده از قابلیت فیلتر کردن آدرس MAC یا MAC Filtering در شبکه‌های بی‌سیم بسیار رایج است. مک فیلترینگ در حقیقت این امکان را فراهم می‌سازد که شما به نقطه دسترسی خود دستور دهید فقط آدرس‌های MAC خاصی امکان اتصال به شبکه را داشته باشند. از این‌رو اگر سیستم جدیدی وارد مجموعه شود که در فهرست مک فیلترینگ قرار نگرفته باشد، حتی اگر کلمه عبور شبکه (Pass Key) را هم در اختیار داشته باشد، باز هم قادر به اتصال به شبکه نخواهد بود. برای از میان برداشتن این مسئله شما می‌توانید با چند دستور ساده در لینوکس یک آدرس MAC جدید به دستگاه خود (به‌صورت مجازی) اختصاص

دهید و این محدودیت‌ها را پشت سر بگذارید. آدرس MAC سیستم در خط اول خروجی ifconfig قابل رؤیت است.

```
eth0 Link encap:Ethernet HWaddr 00:1C:23:FB:37:22
```

حال می‌خواهیم دو رقم آخر این آدرس را به ۲۳ تبدیل کنیم.

```
ifconfig eth0 hw ether 00:1C:23:FB:37:23
```

برای ملاحظه خروجی کار دوباره ifconfig را وارد کنید.

```
[root@gnubox slynux]# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:1C:23:FB:37:23
inet addr:192.168.0.2 Bcast:192.168.0.255 Mask:255.255.255.0
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:17
```

### تعیین سرور DNS

ارتباط در دنیای شبکه از طریق IP و آدرس MAC و... سیستم‌ها صورت می‌پذیرد. اما به حافظه سپردن این‌گونه نشانی‌ها برای انسان بسیار مشکل و گاهی امکان ناپذیر خواهد بود. به‌عنوان مثال، فرض کنید می‌خواهید ایمیل‌های خود را در سایت جی‌میل بررسی کنید. برای این کار کافی است در مرورگر اینترنتی خود نشانی جی‌میل ([www.gmail.com](http://www.gmail.com)) را تایپ کنید. اما در حقیقت شبکه چیزی به نام نشانی gmail.com را متوجه نخواهد شد و اگر هزاران بار این اسم را ارسال کنید، جوابی نخواهید یافت.

در حقیقت، زمانی که شما این آدرس را وارد می‌کنید سیستم شما این نشانی را برای سروری که به آن DNS سرور می‌گویند، ارسال کرده و نشانی IP آن را دریافت می‌کند. به‌عنوان مثال، نشانی ۲۰۹،۸۵،۲۲۹،۱۹ جوابی خواهد بود که DNS سرور به سیستم شما خواهد داد. پس از دریافت این نشانی سیستم شما آن را به نخستین روتر (درگاه ورود به اینترنت شبکه داخلی) ارسال خواهد کرد و سپس صفحه جی‌میل در مرورگر شما نمایان خواهد شد.

اگر سیستم شما به‌صورت خودکار (DHCP) نشانی IP دریافت می‌کند، در این شرایط نشانی سرور DNS برای سیستم شما به احتمال قوی از قبل تعریف شده است. اما اگر به‌صورت دستی مایل به وارد کردن نشانی IP هستید، باید نشانی DNS را با اضافه کردن آدرس IP، Subnet Mask و Default Gateway برای سیستم‌تان تعریف کنید، این کار به راحتی با وارد کردن خطوط زیر در فایل `/etc/resolve.conf` امکان‌پذیر است:

```
nameserver 208.67.222.222
```

```
nameserver 208.67.220.220
```

توجه داشته باشید لزومی ندارد که از DNS تعریف شده توسط ISP تان استفاده کنید. برای امنیت بیشتر بهتر است از DNS های باز یا Open DNS ها استفاده کنید. در این باره می توانید به سایت [opendns.org](http://opendns.org) مراجعه کنید.

### ارتباط از راه دور به وسیله SSH

شاید مایل باشید از راه دور به یکی از سیستم های موجود در شبکه تان متصل شوید. این کار به صورت امن و راحت از طریق SSH امکان پذیر است. البته به شرطی که IP و شناسه کاربری و گذرواژه آن سیستم را بدانید.

به عنوان مثال، در این سناریو ما به سیستمی با آدرس IP فرضی ۱۹۲،۱۶۸،۱،۳ متصل خواهیم شد. اگر شناسه کاربری مجازی در سیستم داشته باشید (که در این مثال نام شناسه ما test خواهد بود) می توانید با توجه به میزان دسترسی های شناسه کاربری خود در آن سیستم کارهای مختلفی انجام دهید .

```
[root@gnubox ~]# ssh test@192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA key fingerprint is 9f:61:ae:ac:8f:75:bb:3a:02:4a:f4:6c:7d:b9:0d:07.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.3' (RSA) to the list of known hosts.
test@192.168.1.3's password:
-sh-3.2$ echo I am on 192.168.1.3 Machine
I am on 192.168.1.3 Machine
-sh-3.2$
```

پس از اتصال به سیستم مورد نظر شما قادر خواهید بود کارهای مختلفی (با توجه به سطح دسترسی شناسه کاربریتان) روی آن انجام دهید. به عنوان مثال، سی دی رام آن را باز و بسته کنید، سیستم را دوباره راه اندازی یا حتی خاموش کنید. یکی از ملحقات `setp` ، `ssh` است که به وسیله آن می توانید فایل ها را از یک سیستم به سیستم دیگری منتقل کنید. در `setp` برای دانلود فایل از دستور `get` و برای آپلود از `put` استفاده خواهیم کرد .

```
[root@localhost ~]# sftp test@192.168.1.3
Connecting to 192.168.1.3...
test@192.168.1.3's password:
sftp> ls
Desktop Documents Download Music Pictures Public Templates
Videos a.out test.bin file.cpp t.c
sftp> get t.c
Fetching /home/test/t.c to t.c
/home/test/t.c 100% 239 0.2KB/s 00:00
sftp>
```

در این مثال پس از ورود به سیستم از طریق `sftp` ما فایلی به نام `t.c` را دانلود کردیم. یکی دیگر از ملحقات `ssh` ، `sshfs` نام دارد که به وسیله آن می توان دایرکتوری در سیستم ریموت شده را در سیستم دیگر `Mount` کنید. در مثال زیر ما یک دایرکتوری را از سیستم ۱۹۲،۱۶۸،۱،۳ به سیستم خودمان `Mount` کردیم.

```
root@localhost ~]# sshfs test@192.168.1.3:/home/test /mnt/test
test@192.168.1.3's password:
```

### تنظیمات پراکسی

بسیاری از شبکه‌های اداری، قبل از ورود سیستم‌ها به دنیای اینترنت آنها را از فایروال خود عبور می‌دهند. اینگونه اتصال‌ها اغلب توسط پراکسی انجام می‌شود. به این ترتیب که به عنوان مثال، مرورگر به طور مستقیم درخواست‌های خود را به اینترنت متصل نمی‌کند، بلکه ابتدا به پراکسی سرور (که می‌تواند همان فایروال شبکه هم باشد) ارسال کرده و پس از مجاز شناخته شدن، درخواست سیستم به اینترنت هدایت خواهد شد .

برای تعریف پراکسی برای پروتکل‌های HTTP و FTP دو دستور زیر را وارد کنید .

```
export http_proxy="http://192.168.0.1:3128" ; // HTTP proxy
export ftp_proxy="192.168.0.1:3128" ; //FTP proxy
```

اگر مایل بودید هر بار که به سیستم وارد می‌شوید این دستورها به‌طور خودکار اعمال شوند، آنها را در فایل `~/.bash_profile` وارد کنید.