

14/08/2016 GNU-LINUX DEBİAN TERMİNAL KOMUTLARI 3 FOR YAPISI

```
#!/bin/bash
for degisken in d1 d2 d3
do
    komutlar
done
```

```
#!/bin/bash
```

```
for bilgisayar in cpu ram gpu
do
    echo $bilgisayar
done
```

```
mehmet@mehmet-Casper-Nirvana-Notebook:~$ bash ornek.sh
cpu
ram
gpu
```

```
#!/bin/bash
if [ $# = 1 ]
then
    ps aux | grep -i $1
else
    echo "bir program girilmedi"
fi
```

/usr/local/bin/ → kullanıcıların kendisi yazdığı bash dosyalarını bu dizine atması daha uygundur
sudo cp pid /usr/local/bin/

```
mehmet@m:~$ pid firefox
mehmet  5592  0.0  0.0 21024 3272 pts/11  S+  12:18  0:00 /bin/bash /usr/local/bin/pid firefox
mehmet  5594  0.0  0.0 22700  928 pts/11  S+  12:18  0:00 grep -i firefox
```

internet → inter networks ; ağlar arası ağlar
internet otonom çalışır. Gayri merkezidir.

Ip → internet protokol ; ağ işlemlerinin gerçekleştirildiği katman anlamına gelir

ağ cihazlara ip paketlerini istenilen adreslere yönlendirilmesini sağlar
ip ile uygulamalar arasında protokolü sağlayan ;

1-tcp → transmission control protokol; tcpip → ağ üzerinden veri aktarımını sağlar, paket iletimlerinde hata kontrolü yapar, hataları düzeltir

2-udp → user datagram protokol, paketlerin iletiminde hata kontrolü gerektirmeyen işlemlerde kullanılır; genelde akış verileri, ses, görüntü, video işlemlerinde kullanılır

telnet → veriler şifrelenmez ; Internet ağı üzerindeki çok kullanıcı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir.

ssh → secure shell ;güvenli veri iletimi için kriptografik ağ protokolüdür.

Http 80 ; https 443 portunu kullanılır

http → "Hyper Text Transfer Protocol" (Hiper Metin Transferi Protokolü) kelimelerinin baş harflerinden oluşan bir kısaltmadır.

Https → HyperText Transfer Protocol Secure kelimelerinin baş harflerinden oluşan bir kısaltmadır. Hypertext terimi, bir web sitesinin kod veya eklenti gerektirmeyen, metin, tablo veya resim gibi içeriklerini açıklar.

/etc/services --> Bir gbu/linux sistemde portlara ait bilgiler /etc/services dosyasının içerisinde bulunur.

/etc/network → ağ ayarlarının bulunduğu dizin

systemd; init'in yeni halidir

networking → sistemde ağ var mı yokmu onu bulur

hostname → sistemimizin adını belirler

gateway → _Ağ geçidi farklı ağ iletişim kurallarını kullanan iki bilgisayar ağı arasında veri çerçevelerinin iletimini sağlayan ağ donanımdır. Bir başka deyişle aynı dili konuşamayan iki ağ arasında tercüman vazifesi görür.

sudo ifconfig → ethernet ip adres bilgilerini öğrenmemizi sağlar

iss → isp -internet service provider; internet servis sağlayıcı

dns → domain name surver ;/etc/resolv.conf/ dns ayarları

dns değiştirmek için **nano /etc/resolv.conf** dosyasına girilir.

bcast → Gönderilen paketin ağ üzerinde bulunan herkese ulaşmasını sağlar

sudo ifconfig içerisindeki internet bağlantısı ayarlarından iptal etmek istenilen kablolu ya da kablosuz ağın kodu yazılır;

sudo ifconfig wlp2s0f0 down → interneti kapatır

sudo ifconfig wlp2s0f0 up → interneti açar11

ifconfig eth0 makinanınipsi networkipsi up → mevcut ip adresimizi sabitleyebilmek için kullanılır... örneğin ; **ifconfig eth0 10.47.150.9 255.255.0.0 up**

route → mevcut yönlendirme tablosu

sudo route add default gw ipadres → gateway değiştirir

15.08.2016 Monday Linux Yaz Kampı 2016 by MEHMET KILIÇ
GNU/LINUX DEBİAN TERMİNAL KOMUTLARI 4

DHCP(Dynamic Host Configuration Protocol) Internet Protokolüne (IP) bağlı çalışan ağlardaki hostlar (yani ağa bağlanan cihazlar) için bir ağ yapılandırma protokolüdür. İster yerel ağdaki bir bilgisayar, ister bir yazıcı ya da başka bir cihaz olsun, ağa bağlanan her cihazın bir [IP adresi](#) olmak zorundadır. IP ağlarına bağlanan cihazların, diğer hostlarla (yani ağa bağlı diğer cihazlarla) iletişim kurabilmeleri için yapılandırılmaları gerekir. Bu yapılandırmada ihtiyaç duyulan temel bilgi IP adresidir. DHCP, ağa bağlanmaya çalışan cihazlara otomatik olarak bir IP adres tahsisi yapar (dinamik IP adresi). Dhcp sunucusunu hayata geçiren servisin adı isc-dhcp-server'dır.

Public IP Address Classes range

| Class | 1st Octet DEC range | 1st Octet BIN | Start address | Finish address | 1st Octet High order Bits | Network/ Host | Default Subnet Mask |
|----------|---------------------|-------------------|---------------|-----------------|---------------------------|---------------|---------------------|
| A | 1-126 | 00000001-01111110 | 0.0.0.0 | 126.255.255.255 | 0 | N.H.H.H | 255.0.0.0 |
| B | 128-191 | 10000000-10111111 | 128.0.0.0 | 191.255.255.255 | 10 | N.N.H.H | 255.255.0.0 |
| C | 192-223 | 11000000-11011111 | 192.0.0.0 | 223.255.255.255 | 110 | N.N.N.H | 255.255.255.0 |
| D | 224-239 | 11100000-11101111 | 224.0.0.0 | 239.255.255.255 | 1110 | | |
| E | 240-255 | 11110000-11111111 | 240.0.0.0 | 254.255.255.255 | 11110 | | |

Note: Class A address **127.0.0.0 - 127.255.255.255** cannot be used and is for **LOOPBACK** and diagnostic

Private IP Address Classes range

| Class | 1st Octet DEC range | 1st Octet BIN | Start address | Finish address | 1st Octet High order Bits | Network/ Host | Default Subnet Mask |
|----------|---------------------|---------------|---------------|-----------------|---------------------------|---------------|---------------------|
| A | 10 | 00001010 | 10.0.0.0 | 10.255.255.255 | 0 | N.H.H.H | 255.0.0.0 |
| B | 172 | 10101100 | 172.16.0.0 | 172.31.255.255 | 10 | N.N.H.H | 255.255.0.0 |
| C | 192 | 11000000 | 192.168.0.0 | 192.168.255.255 | 110 | N.N.N.H | 255.255.255.0 |

www.ic.ims.hr

public ip →

1-126 → a class ip bloğu

128-191 → b class ip bloğu

192-223 → c class ip bloğu

224-239 → d class ip bloğu

240-255 → e class ip bloğu

not : d ve e class ip ler genellikle bilimsel araştırmalar ve deneyler için kullanılır

private ip →

a block: 10.0.0.0.

b block :172.168.0.0.

c block: 192.168.0.0

bu iplerin internette bir karşılığı yoktur. Bulunduğu network için geçerlidir.

127.0.0.1/8 → internette kullanılan böyle bir ip yoktur. Bu bilgisayarın local ip sidir.

Lan → local area networking

van → lan'lar bir araya gelerek van ağını oluşturur

Verilen ip ile netmask ipsi end (çarpım) işleminden geçirildiğinde network içinde dağıtılabilecek ip numaraları bulunabilir.. örneğin;

```
Address: 192.168.56.0          11000000.10101000.00111000. 00000000
Netmask: 255.255.255.0 = 24    11111111.11111111.11111111. 00000000
```

24 ün anlamı; netmask'teki ilk, ikinci ve üçüncü bitlerin 8 bit olması; $3*8=24$. bu buradan elde edilir.

Yani 192.168.56.0 dan 192.168.56.255 e kadar network içinde dağıtılabilecek ip lerdir. Network'un ilk ip'si network'un kendisini ifade eder. Bir istemciye yada bir kişiye bu ip tahsis edilemez. Örneğin 192.168.56.0 yukarıdaki network'un kendisini ifade eder. 192.168.56.255 yukarıdaki örneğin (networkun son ip si olduğu için) network'un broadcast ip sidir. Bilgisayarlar birbirleriyle haberleşmesi için broadcast/yayın yapmak zorundalardır. Bu ip de bir istemciye yada bir kişiye bu ip tahsis edilemez.

Yani yukarıdaki örnekte kullanılabilecek ip'ler 192.168.56.1 dan 192.168.56.254 kadar olanlardır.

Gateway → (gateway bir router yada bilgisayar olabilir.)ağ geçidi, o networkle aynı networkde bulunmalıdır. Ağa bağlanmamızı sağlar. Gateway'lere genellikle (kural olmamakla birlikte) o network un verilebilir ilk ip si hangisi ise o verilir. Bazen ise verilebilen son ip gateway cihazına verilir. Yukarıdaki örnekte gateway 192.168.56.254 ip adresine verilmiştir.

**linux tabanlı işletim sistemleri router olarak tanımlanabilir.

ipcalc ipnumarası → girilen ip numarasına ait netmask, network, broadcast numaralarını gösterir

Soru: 139.179.179.0 ip numarası verilmiştir. Bu ip yi ikiye bölüm iki ayrı network oluşturulması isteniyor...

139.179.179.0 'dan 139.179.179.127 ip numarasına kadar kullanılabilen ip leri hesaplamamızı sağlar:

```
mehmet@casper:~$ ipcalc 139.179.179.0/25
Address: 139.179.179.0          10001011.10110011.10110011.0 00000000
Netmask: 255.255.255.128 = 25  11111111.11111111.11111111.1 00000000
Network: 139.179.179.0/25      10001011.10110011.10110011.0 00000000
Broadcast: 139.179.179.127     10001011.10110011.10110011.0 11111111
Hosts/Net: 126                  Class B
```

139.179.179.128/25 →

139.179.179.128 'dan 139.179.179.155 ip numarasına kadar kullanılabilen ip leri hesaplamamızı sağlar:

```
mehmet@casper:~$ ipcalc 139.179.179.128/25
Address: 139.179.179.128       10001011.10110011.10110011.1 00000000
Netmask: 255.255.255.128 = 25  11111111.11111111.11111111.1 00000000
Network: 139.179.179.128/25    10001011.10110011.10110011.1 00000000
Broadcast: 139.179.179.255     10001011.10110011.10110011.1 11111111
Hosts/Net: 126                  Class B
```

route -nv → ağ geçidine ait ip numaralarını öğrenmemizi sağlar

```
mehmet@casper:~$ route -nv
```

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-----------|-----------------|-------|--------|-----|-----|----------|
| 0.0.0.0 | 10.47.1.1 | 0.0.0.0 | UG | 600 | 0 | 0 | wlp2s0f0 |
| 10.11.0.20 | 10.47.1.1 | 255.255.255.255 | UGH | 600 | 0 | 0 | wlp2s0f0 |
| 10.47.0.0 | 0.0.0.0 | 255.255.0.0 | U | 600 | 0 | 0 | wlp2s0f0 |
| 169.254.0.0 | 0.0.0.0 | 255.255.0.0 | U | 1000 | 0 | 0 | wlp2s0f0 |

Not: gateway’da 0.0.0.0 ip adresi görünmesinin anlamı; aynı network’te bulunan birisinin kullanılan makineye ulaşabileceği anlamına gelir.

ping ipadresi → girilen ip adresine ping atar

netstat → bilgisayarda açık olan portları gösterir

```
mehmet@ubuntu:~$ sudo netstat -ntlp
```

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program name |
|-------|--------|--------|---------------|-----------------|--------|------------------|
| tcp | 0 | 0 | 127.0.1.1:53 | 0.0.0.0:* | LISTEN | 1537/dnsmasq |
| tcp | 0 | 0 | 0.0.0.0:25 | 0.0.0.0:* | LISTEN | 1062/master |
| tcp6 | 0 | 0 | :::25 | :::* | LISTEN | 1062/master |

Ağa Bağlama

→ dhcp bir ip atar... örneğin 192.168.56.0/24

→ isc-dhcp-server kurulur

→ gateway (ağ geçidi)

→ range (aralık) ; ip aralık dağıtımı ... örneğin 192.168.56.101 ile 192.168.56.255 e kadar kullanım aralığı belirlensin

cat /etc/services | grep ssh → ssh’a ait port numarasını öğrenmemizi sağlar

```
mehmet@ubuntu:~$ cat /etc/services | grep ssh
```

ssh 22/tcp

SSH Remote Login Protocol

ssh 22/udp

Sanal Makina ile Net’e Bağlanma

1- Use Bridged Networking : ilk network tipimiz olan use bridged networking seçeneği fiziksel makinemizde bulunan interface kartımızla bridge (köprü) vazifesi görerek bizi sanal makinelerimizle yahut internete çıkmamıza olanak sağlar. Bridgeleme yönteminde sanal makinalarımız (sanal interfacemiz) bir gerçek makine gibi davranarak bizi sanal makinalarımızla ve dış dünyayla iletişime geçirir. Sanal makinelerimiz üzerinde oluşturulan sanal NIC lerin kendine özgü MAC adresleri ve İP adresleri mevcuttur. MAC adreslerinin dünya üzerinde aynısı bulunamaz.

2- Use Network Address Translation (NAT) : NAT kavramını açıklayarak başlayalım. Örneğin işyerimizde 1 adet modem olduğunu ve 10 adette client (istemci) bilgisayar olduğunu düşünelim. Bu bilgisayarlarımız bir switch bağlı switch te direk modeme tüm clientlerimiz bu modem üzerinden internete çıkarlar ve tek bir ip adresi kullanırlar hangi makine çıkarsa çıksın global ip adresleri aynıdır. Local ip adresleri modemden veya içeride bir DHCP sunucu üzerinde

tanımladığımız 192.168.2.2 şeklinde gibi işte 10 clientin aynı anda internete çıkmaları ve bir adet global ip kullanmaları bir NAT işlemidir. Oluşturduğumuz sanal makinada aynısını yapar. Direk NAT yaparak gerçek makineye bağlanır. Sebebi ise sanal makinenin ip adresi farklıdır. Örneğin 192.168.78.18 gibi farklı bir IP bloğu üzerindedir. Özetleyecek olursak sanal makinamız NAT yaparak dış dünyaya açılabilir.

3- Use Host-Only Networking : Üçüncü seçeneğimiz olan use host-only networking seçeneği özel bir ağ gibi davranır. Aynı switch üzerinde olan gerçek makinelerin birbiriyle konuşması gibi düşünebiliriz. İnternete çıkamaz sanal makineler birbiriyle konuşabilir. Ağ içerisinde bulunan fiziksel makine ilede konuşabilir. Fakat dış dünyayla iletişime geçemez.

4- Do Not Use a Network Connection : Son seçeneğimiz olan do not use a network connection kavramı sanal makine oluştururken Network Type olarak en son seçebileceğimiz bir seçenektir. Eğer sanal makinamızın özel veya başka bir ağa dahil olmasını istemiyorsak. Do not use a network connection seçeneğini seçebiliriz. Sanal makinamız sadece fişe takılan ve hiçbir makine ile iletişimi olmayan bir fiziksel makine olarak ta düşünebiliriz.

dhclient -v ağarayüzü → bir DHCP sunucusundan manual olarak ip almamızı sağlar

mehmet@ubuntu : ifconfig → burada çıkan bilgilerde sol köşede bulunan ethernet ya da wifi ağ arayüzü adı yukarıdaki portadı kısmına yazılır...örneğin
mehmet@ubuntu:~\$ dhclient -v wlp20f0

STATIC IP

ifconfig ağarayüzüadı ipadress netmaskipadress up → manual olarak anlık ip adresi sabitlemeye yarar. Sistem boot edildiğinde bu ip sabit kalmaz.

sudo nano /etc/network/interfaces → ağ arayüzlerinin yönetildiği dosyayı terminalde metin editörü olarak açmamızı sağlar

/etc/network/interfaces içerisinde **static ip belirlemek için** aşağıdaki gibi static yazılarak adresler girilir.

```
#the primary network interfaces
auto wlp20f0 → ağ arayüzü adı
iface wlp20f0 inet static
    address      192.168.57.254
    netmask      255.255.255.0
    gateway      192.168.57.1
```

Not: Bu işlem yapılırsa; sistem boot edilse dahi aynı ip adresini verir. Yani ip her durumda static kalır.

service networking restart → ip yapılandırılması değiştirildikten sonra bu işlem yapılır ve ip resetlenir

ifconfig ayarüzadı down & ifconfig arayüzadı up → wifi'ı kapayıp açmamıza yarar