

ifconfig

يستخدم من اجل تعيين ip address لأحد المنافذ الخاصة بالشبكة او من اجل استعراض معلومات عن المنافذ الموجودة في الشبكة والتحكم بها.

Ifconfig دون اي بارامتر تعرض لنا المنافذ النشطة فقط

ولعرض جميع المنافذ النشطة والغير نشطة نكتب الأمر : **Ifconfig -a**

```
[Fedora@linux ~]$ ifconfig -a
eth2      Link encap:Ethernet  HWaddr 00:0C:29:96:3D:8F
          inet addr:192.168.64.128  Bcast:192.168.64.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe96:3d8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:953 errors:0 dropped:0 overruns:0 frame:0
          TX packets:227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:72166 (70.4 KiB)  TX bytes:29862 (29.1 KiB)
          Interrupt:19 Base address:0x2000

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:86 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:11528 (11.2 KiB)  TX bytes:11528 (11.2 KiB)

pan0      Link encap:Ethernet  HWaddr DE:8B:A7:66:0A:F0
          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:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

virbr0    Link encap:Ethernet  HWaddr AE:E7:81:8C:94:C4
          inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:4381 (4.2 KiB)

[Fedora@linux ~]$
```

لعرض معلومات منفذ معين نكتب:

Ifconfig اسم المنفذ

لإيقاف تفعيل منفذ معين نكتب:

Ifconfig down اسم المنفذ

لتفعيل منفذ معين نكتب:

Ifconfig up اسم المنفذ

إذا اردنا تغيير عنوان ال **ip address** و ال **mask** و ال **Bcast** الخاص بمنفذ ما نكتب :

العناوين الجديدة اسم المنفذ **ifconfig**

مثال : تغيير عنوان المنفذ eth2

```
[root@linux Fedora]# ifconfig eth2 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255
[root@linux Fedora]# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:0C:29:42:E4:5A
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::20c:29ff:fe42:e45a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:88 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11375 (11.1 KiB)  TX bytes:11843 (11.5 KiB)
          Interrupt:19 Base address:0x2000
```

ما هو الأمر ping وكيف يعمل ؟

هو أمر يقوم بفحص الاتصال مع أجهزة الشبكة أو أي موقع على الإنترنت .
يعمل أمر ping على فحص إمكانية الوصول إلى عنوان IP ، مضيف أو خادم انطلاقاً من شبكتك.
يكثر استخدام الأمر للتدقيق في أخطاء الشبكة وتحديد مشاكلها.

المعطى الضروري الوحيد لأمر ping هو اسم المضيف أو عنوان IP المراد فحصه.

ping example.com

example.com اسم المضيف

ping 93.184.216.34

أو من خلال ال IP له

مخرجات الأمر:

PING example.com (93.184.216.34) 56(84) bytes of data.

64 bytes from example.com (93.184.216.34): icmp_seq=1 ttl=42 time=116 ms

64 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=42 time=154 ms

64 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=42 time=163 ms

64 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=42 time=1028 ms

64 bytes from example.com (93.184.216.34): icmp_seq=5 ttl=42 time=768 ms

64 bytes from example.com (93.184.216.34): icmp_seq=6 ttl=42 time=128 ms

لتوقيف تنفيذ الأمر بالضغط على الزرين CTRL و C وإلا فإن الأمر سيستمر في إرسال الحزم.
يظهر ملخص بالإحصاءات بعد توقف الأمر:

^X^C

--- example.com ping statistics ---

24 packets transmitted, 23 received, 4% packet loss, time 23041ms

rtt min/avg/max/mdev = 114.323/307.465/1057.499/296.627 ms, pipe 2

يتضمن الملخص :

Transmitted عدد الحزم المُرسلة

Received عدد الحزم المستلمة

Packet loss نسبة فقدان الحزم

min. الحد الأدنى للمدة الزمنية لوصول الإجابة.

avg. متوسط وصول الإجابة.

max. الحد الأقصى للمدة الزمنية لوصول الإجابة.

عدد مرات تنفيذ الأمر

السلوك المبدئي لأمر ping إن استخدم بدون خيارات هو الاستمرار في إرسال الحزم إلى أن يتدخل أحد لإيقافه، إلا أنه توجد طريقة لتحديد عدد مرات إرسال الحزم.

استخدم الخيار -c متبوعاً بعدد على النحو التالي:

ping -c 5 example.com

الخرج :

PING example.com (93.184.216.34) 56(84) bytes of data.

64 bytes from example.com (93.184.216.34): icmp_seq=1 ttl=43 time=129 ms

64 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=43 time=127 ms

64 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=43 time=126 ms

64 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=43 time=125 ms

64 bytes from example.com (93.184.216.34): icmp_seq=5 ttl=43 time=284 ms

--- example.com ping statistics ---

5 packets transmitted, 5 received, % packet loss, time 9011ms

rtt min/avg/max/mdev = 125.003/149.335/284.433/47.508 ms

تعديل حجم حزمة البيانات :

يُرسل أمر ping مبدئيًا حزمة بحجم ٦٤ بايت على لينكس، و ٣٢ بايت على ويندوز. إن أردت تغيير الحجم المبدئي للحزمة على لينكس فيمكنك ذلك باستخدام الخيار : -s

ping -s 100 -c 4 example.com

الخرج:

PING example.com (93.184.216.34) 100(128) bytes of data.

108 bytes from example.com (93.184.216.34): icmp_seq=2 ttl=51 time=1113 ms

108 bytes from example.com (93.184.216.34): icmp_seq=3 ttl=51 time=253 ms

108 bytes from example.com (93.184.216.34): icmp_seq=4 ttl=51 time=263 ms

--- example.com ping statistics ---

4 packets transmitted, 3 received, 16% packet loss, time 4999ms

rtt min/avg/max/mdev = 253.093/590.201/1113.044/408.995 ms, pipe 2

زيادة المدة الزمنية أو تقليصها:

ينتظر أمر ping مبدئيًا ثانية واحدة قبل إرسال الحزمة الموالية إلى الوجهة. يمكن استخدام الخيار -i من زيادة هذا المجال أو تقليصه.

ping -i 3 example.com

يمكننا بنفس الطريقة التسريع من إرسال الحزم بدل انتظار ثانية في كل مرة:

ping -i 0.2 example.com

عرض إحصاءات ping فقط :

يمكن استخدام الخيار -q الإبقاء على إحصاءات الأمر فقط دون إظهار معلومات الحزم:

ping -c 5 -q example.com

PING example.com (93.184.216.34) 56(84) bytes of data.

--- example.com ping statistics ---

5 packets transmitted, 4 received, 20% packet loss, time 6221ms

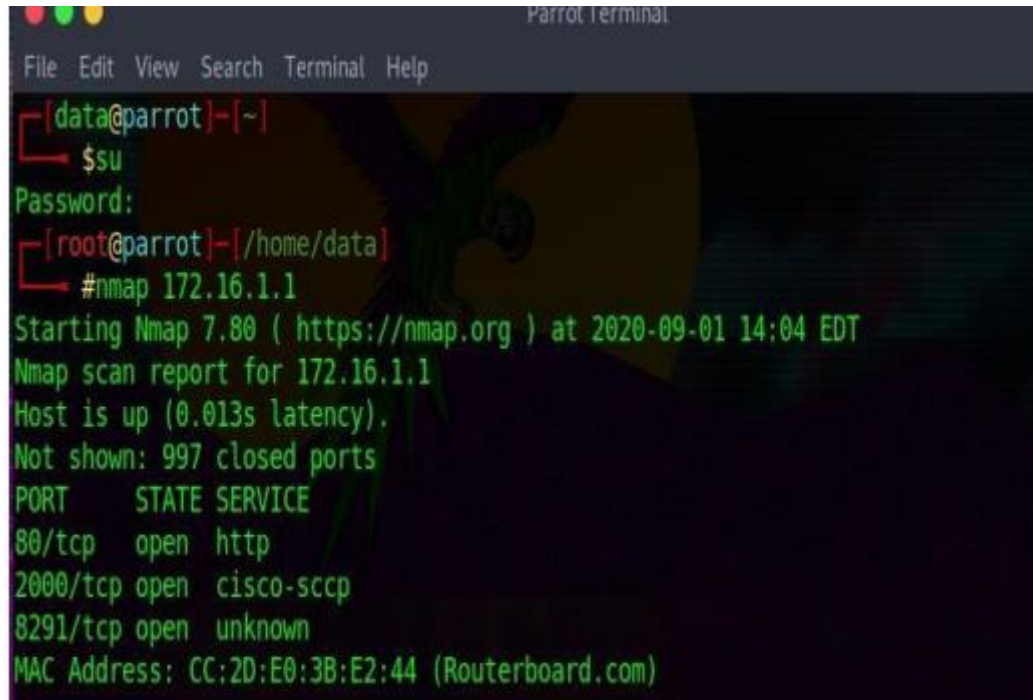
rtt min/avg/max/mdev = 259.175/723.504/1219.311/460.540 ms, pipe 2

يظهر التقرير فقط في مخرجات الأمر أعلاه.

NMAP

(Nmap)، اختصار لـ (Network Mapper) هي أداة مجانية ومفتوحة المصدر تُستخدم لفحص الثغرات الأمنية ومسح المنافذ ورسم خرائط الشبكة.

إذا كنت تريد فقط فحص شبكتك المحلية ومعرفة عدد الأجهزة المتصلة بشبكة Wifi الخاصة بك ، فيمكنك استخدام هذا الأمر. سيعطيك هذا الأمر قائمة بجميع الأجهزة في الشبكة بالإضافة إلى جميع المنافذ المفتوحة لتلك الأجهزة 172.16.1.1 \$ nmap .

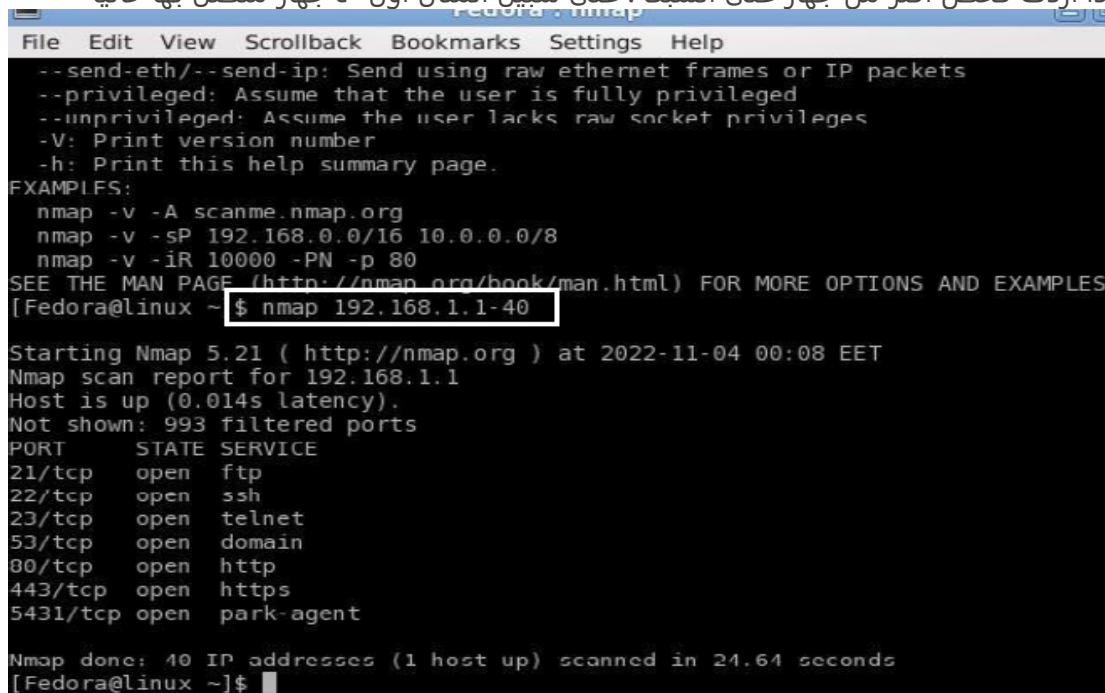


```

Parrot Terminal
File Edit View Search Terminal Help
[data@parrot]~$ su
Password:
[root@parrot]~/home/data# nmap 172.16.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-01 14:04 EDT
Nmap scan report for 172.16.1.1
Host is up (0.013s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
2000/tcp   open  cisco-sccp
8291/tcp   open  unknown
MAC Address: CC:2D:E0:3B:E2:44 (Routerboard.com)

```

إذا أردت فحص أكثر من جهاز على الشبكة، على سبيل المثال أول ٤٠ جهاز متصل بها حالياً



```

Fedora: nmap
File Edit View Scrollback Bookmarks Settings Help
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
[Fedora@linux ~]$ nmap 192.168.1.1-40
Starting Nmap 5.21 ( http://nmap.org ) at 2022-11-04 00:08 EET
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
5431/tcp   open  park-agent
Nmap done: 40 IP addresses (1 host up) scanned in 24.64 seconds
[Fedora@linux ~]$

```

إذا أردت فحص كامل الشبكة استخدم رمز النجمة * الذي يعني الكل All كالتالي.

nmap 192.168.1.1*

إذا أردت فحص آيبيات محددة، ننشئ ملف txt على سطح المكتب و نكتب فيه الآيبيات ، على

سبيل المثال إذا قمت بتسمية الملف targets3.txt إفتح الترمينال و استخدم الأمر -iL كالتالي.

```
[root@parrot]-[/home/data]
#cd Desktop
[root@parrot]-[/home/data/Desktop]
#nmap -iL targets3.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 08:39 EDT
Nmap done: 4 IP addresses (0 hosts up) scanned in 0.62 seconds
[root@parrot]-[/home/data/Desktop]
```

لعمل فحص قوي يسمى فحص عدواني، نستخدم الرمز -A كالتالي مع الإشارة إلى أنه يتطلب وقت أكثر في لإتمام المهمة لأنه يفحص كل شي.

nmap -A 192.168.1.1

لمعرفه نظام تشغيل روتر او سيرفر موقع معين نستخدم الأمر -O كالتالي.

nmap -O 192.168.1.1

لعمل فحص سريع (ضعيف) يعطي بعض المعلومات فقط و هذه اكثر طريقة مستخدمه

لمعرفه بعض المعلومات السطحية عن الهدف نستخدم الأمر -sV كالتالي.

nmap -sV 192.168.1.1

لفحص بورتات محددة مثلاً البورتات 80 و 139 و 443 نستخدم -p

nmap -p 80,139,443 192.168.1.1

لعرض البورتات المفتوحة نستخدم الأمر --open

```
File Edit View Search Terminal Help
#nmap --open harmash.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 08:54 EDT
Nmap scan report for harmash.com (160.153.208.196)
Host is up (0.15s latency).
rDNS record for 160.153.208.196: ip-160-153-208-196.ip.secureserver.net
Not shown: 975 filtered ports, 13 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-rate
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
```

NETSTAT

netstat : هو عبارة عن أمر يستخدم من أجل إظهار معلومات تفصيلية عن الشبكة وعن كيفية اتصال الحاسب مع الأجهزة والشبكات الأخرى.

من المعلومات التي يعرضها الأمر:

- عرض اتصالات الشبكة.
- عرض جداول التوجيه.
- عرض تفاصيل كروت الشبكة.

□ طريقة التثبيت:

yum install net-tools (Fedora) من أجل

apt install net-tools (Debian) من أجل

يتم تثبيت **netstat** فقط في حال كانت توزيعه لينكس غير مثبت عليها **Netstat**.

وسائط netstat:

-i, --interfaces: يستخدم لعرض كافة كروت الشبكة.

-n, --numeric: تعرض عنوان IP بدلا من **hostname**.

--all, -a: تعرض كل الاتصالات الحالية من مختلف البروتوكولات.

-t, --tcp: تستخدم لعرض اتصالات TCP.

-u, --udp: تستخدم لعرض اتصالات UDP.

--program, -p: يستخدم لعرض (process identifier) PID واسم البرنامج الذي قام بتأسيس الاتصال.

- عند تنفيذ الأمر **netstat** من دون أي وسائط يعرض قائمة من المقابس المفتوحة.

```

vibr0
[zina@linux ~]$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State
unix 2      [ ]                 DGRAM                  12403
unix 24     [ ]                 DGRAM                  11441
unix 3      [ ]                 STREAM                 30869
unix 3      [ ]                 STREAM                 30868
unix 3      [ ]                 STREAM                 30861
unix 3      [ ]                 STREAM                 30860
unix 2      [ ]                 DGRAM                  30093
unix 3      [ ]                 STREAM                 28696
unix 3      [ ]                 STREAM                 28695
unix 3      [ ]                 STREAM                 28686
unix 3      [ ]                 STREAM                 28685
unix 3      [ ]                 STREAM                 28684
unix 3      [ ]                 STREAM                 28683
unix 3      [ ]                 STREAM                 28680
unix 3      [ ]                 STREAM                 28679
unix 3      [ ]                 STREAM                 28676
unix 3      [ ]                 STREAM                 28675
unix 3      [ ]                 STREAM                 28635
unix 3      [ ]                 STREAM                 28634
unix 3      [ ]                 STREAM                 28623

```

- من أجل عرض كل الاتصالات الحالية من مختلف البرتوكولات الموجودة نستخدم الوسيط «-a».

```
[root@linux Fedora]# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:sunrpc                *:                      LISTEN
tcp        0      0 192.168.122.1:domain    *:                      LISTEN
tcp        0      0 *:ssh                   *:                      LISTEN
tcp        0      0 linux.fedora:ipp        *:                      LISTEN
tcp        0      0 *:36888                 *:                      LISTEN
tcp        0      0 linux.fedora:smtp       *:                      LISTEN
tcp        0      0 *:sunrpc                *:                      LISTEN
tcp        0      0 *:ssh                   *:                      LISTEN
tcp        0      0 localhost:ipp           *:                      LISTEN
tcp        0      0 *:38683                  *:                      LISTEN
udp        0      0 *:42602                 *:                      LISTEN
udp        0      0 *:sunrpc                *:                      LISTEN
udp        0      0 *:ipp                   *:                      LISTEN
```

- من أجل عرض كل الاتصالات الحالية من البرتوكول TCP نستخدم الوسيط -t
- **ملاحظة:** يمكن دمج عدة وسائط مثل -a و -t يصبحوا على الشكل التالي -at

```
[root@linux Fedora]# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:sunrpc                *:                      LISTEN
tcp        0      0 192.168.122.1:domain    *:                      LISTEN
tcp        0      0 *:ssh                   *:                      LISTEN
tcp        0      0 linux.fedora:ipp        *:                      LISTEN
tcp        0      0 *:36888                 *:                      LISTEN
tcp        0      0 linux.fedora:smtp       *:                      LISTEN
tcp        0      0 *:sunrpc                *:                      LISTEN
tcp        0      0 *:ssh                   *:                      LISTEN
tcp        0      0 localhost:ipp           *:                      LISTEN
tcp        0      0 *:38683                  *:                      LISTEN
```

- من أجل عرض كل الاتصالات الحالية من البرتوكول UDP نستخدم الوسيط -u

```
[root@linux Fedora]# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:42602                 *:                      LISTEN
udp        0      0 *:sunrpc                *:                      LISTEN
udp        0      0 *:ipp                   *:                      LISTEN
udp        0      0 *:mdns                  *:                      LISTEN
udp        0      0 *:netconfsoapbeep       *:                      LISTEN
udp        0      0 *:895                   *:                      LISTEN
udp        0      0 192.168.122.1:domain    *:                      LISTEN
udp        0      0 *:53823                 *:                      LISTEN
udp        0      0 *:bootps                *:                      LISTEN
udp        0      0 *:bootpc                *:                      LISTEN
udp        0      0 *:sunrpc                *:                      LISTEN
udp        0      0 *:43250                 *:                      LISTEN
udp        0      0 *:netconfsoapbeep       *:                      LISTEN
```

Nslookup

تعلیمة تعمل كعمل dns نحصل على اسم الجهاز أو اسم موقع من ip

Nslookup google.com

ipcalc

هناك طريقة تستخدم في العنونة اسمها prefix

192.168.1.0 /24

يكافئ الشبكة التالية

Network 192.168.1.0 mask 255.255.255.0

يستخدم الأمر ipcalc لاستنتاج ال subnet mask و ال Broadcast

مثال نستخدم الأمر ipcalc لحساب ال Prefix

ipcalc -p 192.168.1.0 255.255.255.0

وتكون النتيجة هي 24

مثال معاكس استنتاج القناع وعنوان البث وعنوان الشبكة

ipcalc -m -n -b 192.168.1.0/16

وتكون النتيجة

NETMASK=255.255.0.0 BROADCAST=192.168.255.255

NETWORK=192.168.0.0