

# nmap ?????

??????

### Scan a single ip address ###

```
nmap 192.168.1.1
```

## Scan a host name ###

```
nmap server1.cyberciti.biz
```

## Scan a host name with more info###

```
nmap -v server1.cyberciti.biz
```

??????

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3
```

## works with same subnet i.e. 192.168.1.0/24

```
nmap 192.168.1.1,2,3
```

## You can scan a range of IP address too:

```
nmap 192.168.1.1-20
```

## You can scan a range of IP address using a wildcard:

```
nmap 192.168.1.*
```

## you scan an entire subnet:

```
nmap 192.168.1.0/24
```

# Ping scan subnet

```
nmap -sP 10.15.9.0/24 | grep -E '\b(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?\.)\{3\}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)'
```

```
nmap -sP 10.15.9.0/24 | sed -n '/^.*[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*p' | sed 's/^.*\([0-9]*\.[0-9]*\.[0-9]*\.[0-9]*\)\.*/\1/g'
```

????? IP ??

```
nmap -iL /tmp/ip.txt
```

## ?? IP ???

```
nmap 192.168.1.0/24 --exclude 192.168.1.5  
nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254  
nmap -iL /tmp/scanlist.txt --excludefile /tmp/exclude.txt
```

## ????????????

```
nmap -A 192.168.1.254  
nmap -v -A 192.168.1.1  
nmap -A -iL /tmp/scanlist.txt
```

## ????????????

```
nmap -A 192.168.1.254  
nmap -v -A 192.168.1.1  
nmap -A -iL /tmp/scanlist.txt
```

## ????(????????)

```
nmap -PN 192.168.1.1  
nmap -PN server1.cyberciti.biz
```

## ?? IPv6 ??

```
nmap -6 IPv6-Address-Here  
nmap -6 server1.cyberciti.biz  
nmap -6 2607:f0d0:1002:51::4  
nmap -v A -6 2607:f0d0:1002:51::4
```

## ????????????/??

```
nmap -sP 192.168.1.0/24
```

## ??????

```
nmap -F 192.168.1.1
```

## ????????(Reason)

```
nmap --reason 192.168.1.1
```

## ????????

```
nmap --open 192.168.1.1
```

## ????/????

```
nmap --packet-trace 192.168.1.1
```

## ????????????

```
nmap --iflist
```

## ??????

```
nmap -p [port] hostName
```

```
## Scan port 80
```

```
nmap -p 80 192.168.1.1
```

```
## Scan TCP port 80
```

```
nmap -p T:80 192.168.1.1
```

```
## Scan UDP port 53
```

```
nmap -p U:53 192.168.1.1
```

```
## Scan two ports ##
```

```
nmap -p 80,443 192.168.1.1
```

```
## Scan port ranges ##
```

```
nmap -p 80-200 192.168.1.1
```

```
## Combine all options ##
```

```
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
```

```
nmap -p U:53,111,137,T:21-25,80,139,8080 server1.cyberciti.biz
```

```
nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.254
```

## Scan all ports with \* wildcard ##

```
nmap -p "*" 192.168.1.1
```

## Scan top ports i.e. scan \$number most common ports ##

```
nmap --top-ports 5 192.168.1.1
```

```
nmap --top-ports 10 192.168.1.1
```

????????????????/??

```
nmap -T5 192.168.1.0/24
```

## Cheat Sheet

### Nmap Cheat Sheet

#### Target Specification

| Switch    | Example                      | Description              |
|-----------|------------------------------|--------------------------|
|           | nmap 192.168.1.1             | Scan a single IP         |
|           | nmap 192.168.1.1 192.168.2.1 | Scan specific IPs        |
|           | nmap 192.168.1.1-254         | Scan a range             |
|           | nmap scanme.nmap.org         | Scan a domain            |
|           | nmap 192.168.1.0/24          | Scan using CIDR notation |
| -iL       | nmap -iL targets.txt         | Scan targets from a file |
| -iR       | nmap -iR 100                 | Scan 100 random hosts    |
| --exclude | nmap --exclude 192.168.1.1   | Exclude listed hosts     |

#### Scan Techniques

| Switch | Example              | Description  |
|--------|----------------------|--|
| -sS    | nmap 192.168.1.1 -sS | TCP SYN port scan (Default)                            |
| -sT    | nmap 192.168.1.1 -sT | TCP connect port scan (Default without root privilege) |
| -sU    | nmap 192.168.1.1 -sU | UDP port scan  |
| -sA    | nmap 192.168.1.1 -sA | TCP ACK port scan                                      |
| -sW    | nmap 192.168.1.1 -sW | TCP Window port scan                                   |
| -sM    | nmap 192.168.1.1 -sM | TCP Maimon port scan                                   |

#### Host Discovery

| Switch | Example                        | Description                                     |
|--------|--------------------------------|---|
| -sL    | nmap 192.168.1.1-3 -sL         | No Scan. List targets only                      |
| -sn    | nmap 192.168.1.1/24 -sn        | Disable port scanning                           |
| -Pn    | nmap 192.168.1.1-5 -Pn         | Disable host discovery. Port scan only          |
| -PS    | nmap 192.168.1.1-5 -PS22-25,80 | TCP SYN discovery on port x. Port 80 by default |
| -PA    | nmap 192.168.1.1-5 -PA22-25,80 | TCP ACK discovery on port x. Port 80 by default |
| -PU    | nmap 192.168.1.1-5 -PU53       | UDP discovery on port x. Port 40125 by default  |
| -PR    | nmap 192.168.1.1-1/24 -PR      | ARP discovery on local network                  |
| -n     | nmap 192.168.1.1 -n            | Never do DNS resolution                         |

#### Port Specification

| Switch      | Example                             | Description   |
|-------------|-------------------------------------|---|
| -p          | nmap 192.168.1.1 -p 21              | Port scan for port x  |
| -p          | nmap 192.168.1.1 -p 21-100          | Port range  |
| -p          | nmap 192.168.1.1 -p U:53,T:21-25,80 | Port scan multiple TCP and UDP ports                                  |
| -p-         | nmap 192.168.1.1 -p-                | Port scan all ports   |
| -p          | nmap 192.168.1.1 -p http,https      | Port scan from service name   |
| -F          | nmap 192.168.1.1 -F                 | Fast port scan (100 ports)  |
| --top-ports | nmap 192.168.1.1 --top-ports 2000   | Port scan the top x ports   |
| -p-65535    | nmap 192.168.1.1 -p-65535           | Leaving off initial port in range makes the scan start at port 1      |
| -p0-        | nmap 192.168.1.1 -p0-               | Leaving off end port in range makes the scan go through to port 65535 |

[www.stationx.net/nmap-cheat-sheet/](http://www.stationx.net/nmap-cheat-sheet/)

