

Network Mapping (NMAP)

List of Content:

1. ARP Ping
2. ICMP Address Mask Ping
3. ICMP Echo Ping
4. ICMP Timestamp Ping
5. Ping Scan
6. TCP ACK Ping
7. TCP SYN Ping
8. UDP Ping

1. ARP: ARP (Address Resolution Protocol) is a network protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) within a local network (LAN).

Works:

Sending ARP Request:

- The ARP Ping tool sends an ARP request to a specific IP address.
- This request asks: "Who has IP 192.168.1.104? Tell me your MAC address."

Receiving ARP Reply:

- If the target device is active, it replies with its MAC address.
- If the target device is offline, there will be no response.

Command for ARP ping

`nmap -PR 192.168.1.104`

where, nmap denotes network mapping

PR denotes **ARP Ping** (Address Resolution Protocol) to check if the target is alive.

192.168.1.104 is the target ip address.

Example:

```
(root@kali) - [~]
# nmap -PR 192.168.1.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 19:30 IST
Nmap scan report for 192.168.1.104
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

→ Target ip address

→ Use for ARP ping

```

512/tcp open  exec
513/tcp open  login
514/tcp open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  cccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:DD:64:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds

```

Result:

No.	Time	Source	Destination	Protocol	Length	Info
21	5.187472234	PCSSystemtec_27:1b::	Broadcast	ARP	42	Who has 192.168.1.104? Tell 192.168.1.102
22	5.188349890	PCSSystemtec_dd:64::	PCSSystemtec_27:1b::	ARP	60	192.168.1.104 is at 08:00:27:dd:64:23
25	5.338113933	PCSSystemtec_27:1b::	Broadcast	ARP	42	Who has 192.168.1.104? Tell 192.168.1.102
26	5.338785996	PCSSystemtec_dd:64::	PCSSystemtec_27:1b::	ARP	60	192.168.1.104 is at 08:00:27:dd:64:23
2057	10.333995511	PCSSystemtec_dd:64::	PCSSystemtec_27:1b::	ARP	60	Who has 192.168.1.102? Tell 192.168.1.104
2058	10.334010727	PCSSystemtec_27:1b::	PCSSystemtec_dd:64::	ARP	42	192.168.1.102 is at 08:00:27:27:1b:c7
2059	10.455701988	PCSSystemtec_27:1b::	MercusysTech_95:c2::	ARP	42	Who has 192.168.1.1? Tell 192.168.1.102
2060	10.459467038	MercusysTech_95:c2::	MercusysTech_95:c2::	ARP	60	192.168.1.1 is at 08:eb:d8:95:c2:d1
2065	18.745768687	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2068	30.733084249	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2069	46.715869682	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2071	58.763559485	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2073	59.727493130	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2100	87.700525608	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2129	120.790733224	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2130	121.712763545	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2136	142.818551671	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2139	154.805566601	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2140	166.792849441	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1
2141	167.817427634	MercusysTech_95:c2::	Broadcast	ARP	60	Who has 192.168.1.100? Tell 192.168.1.1

Send and Receive information

ARP Ping

Hex Code

```

Frame 21: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_27:1b:c7 (08:00:27:27:1b:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: PCSSystemtec_27:1b:c7 (08:00:27:27:1b:c7)
  Sender IP address: 192.168.1.102
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.104

```

2. ICMP Address Mask Ping

ICMP (Internet Control Message Protocol) operates at Layer 3 (Network Layer) of the OSI model and is primarily used for network troubleshooting and communication.

ICMP Address Mask Ping (ICMP Type 17 & 18)

ICMP “Address Mask Request” (Type 17) asks a router for its subnet mask. If allowed, the router replies with “Address Mask Reply” (Type 18) containing the subnet mask.

How it Works?

1 Host sends an ICMP Type 17 request (Address Mask Request).

2 If the router allows it, it replies with ICMP Type 18 (Address Mask Reply) containing the subnet mask (e.g., 255.255.255.0).

Command in Linux:

`nmap -PM 192.168.1.1`

Where, nmap is network mapping.

-PM stands for ICMP Address Mask Ping.

```
(root@kali: ~)
# nmap -PM 192.168.43.238
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 03:03 EST
Nmap scan report for 192.168.43.238
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  domain
80/tcp    open  http
81/tcp    open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
5909/tcp  open  rmiregistry
524/tcp   open  ingreslock
6049/tcp  open  nfs
6121/tcp  open  ccproxy-ftp
6306/tcp  open  mysql
6432/tcp  open  postgresql
6900/tcp  open  vnc
7000/tcp  open  X11
7667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:2B:EE:15 PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=0/0, ttl=64
2	1.000002091	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=256/4, ttl=64
3	2.000552522	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=512/7, ttl=64
4	3.007334423	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=768/3, ttl=64
5	4.008304322	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=1024/4, ttl=64
6	5.009080833	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=1280/5, ttl=64
7	6.011269016	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=1536/6, ttl=64
8	7.012421784	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=1792/7, ttl=64
9	8.013622212	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=2048/8, ttl=64
10	9.015197941	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=2304/9, ttl=64
11	10.016222102	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=2560/10, ttl=64
12	11.017106804	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=2816/11, ttl=64
13	12.018044250	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=3072/12, ttl=64
14	13.019139016	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=3328/13, ttl=64
15	14.021554877	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=3584/14, ttl=64
16	15.022927241	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=3840/15, ttl=64
17	16.023857831	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=4096/16, ttl=64
18	17.027515433	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=4352/17, ttl=64
19	18.028613039	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=4608/18, ttl=64
20	19.027669565	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=4864/19, ttl=64
21	20.028261036	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=5120/20, ttl=64
22	21.029189021	192.168.43.158	192.168.43.238	ICMP	46	Address mask request id=0xaa2, seq=5376/21, ttl=64

Purpose: Checks if a device is online and measures response time.

1 Sender sends ICMP Echo Request (Type 8) to the target.

2Target replies with ICMP Echo Reply (Type 0) if it's reachable.

3Round-Trip Time (RTT) is measured for latency analysis.

Command in Kali Linux:

`nmap -PE 192.168.43.0`

Where, nmap is network mapping.

-PE stands for ICMP echo ping.

192.168.43.0 is a targeted ip address.

```
(root@kali)~[/home/kali]
# nmap -PE 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:33 EST
Nmap scan report for 192.168.43.1
Host is up (0.0020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.00068s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)
Nmap scan report for 192.168.43.238
Host is up (0.0081s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
6099/tcp  open  rmiregistry
6524/tcp  open  ingreslock
8049/tcp  open  nfs
8121/tcp  open  ccproxy-ftp
8306/tcp  open  mysql
8432/tcp  open  postgresql
8900/tcp  open  vnc
9000/tcp  open  X11
9667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.43.158)
Host is up (0.000022s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 256 IP addresses (4 hosts up) scanned in 7.03 seconds
Packets: 6580 - Displayed: 8 (0.1%) - Dropped: 0
```

Result:

The image shows a Wireshark packet capture with several ICMPv6 packets. A red box highlights a series of Neighbor Solicitation and Neighbor Advertisement packets. Below the packet list, a diagram shows the flow of an ICMP Echo Ping, with a red arrow pointing to the 'Hex Code' section. The hex code section shows the raw data of the Neighbor Solicitation packet, with a red box highlighting the destination address field.

No.	Time	Source	Destination	Protocol	Length	Info
6573	7.468207796	fe80::1a02:aeff:fe5...	2409:4042:4d0d:de10...	ICMPv6	80	Neighbor Solicitation for 2409:4042:4d0d:de10:3624:252a:883b:a048 from 18:02:ae:5a:e9:e1
6574	7.468378775	2409:4042:4d0d:de10...	fe80::1a02:aeff:fe5...	ICMPv6	78	Neighbor Advertisement 2409:4042:4d0d:de10:3624:252a:883b:a048 (sol)
6575	7.469393164	fe80::a00:27ff:fe89...	2409:4042:4d0d:de10...	ICMPv6	80	Neighbor Solicitation for 2409:4042:4d0d:de10::66 from 08:00:27:89:49:08
6576	7.470612537	2409:4042:4d0d:de10...	fe80::a00:27ff:fe89...	ICMPv6	78	Neighbor Advertisement 2409:4042:4d0d:de10::66 (rtr, sol)
6577	12.585361378	fe80::a00:27ff:fe89...	fe80::1a02:aeff:fe5...	ICMPv6	80	Neighbor Solicitation for fe80::1a02:aeff:fe5a:e9e1 from 08:00:27:89:49:08
6578	12.588472150	fe80::1a02:aeff:fe5...	fe80::a00:27ff:fe89...	ICMPv6	80	Neighbor Solicitation for fe80::a00:27ff:fe89:4908 from 18:02:ae:5a:e9:e1
6579	12.588529570	fe80::a00:27ff:fe89...	fe80::1a02:aeff:fe5...	ICMPv6	78	Neighbor Advertisement fe80::a00:27ff:fe89:4908 (sol)
6580	12.588861212	fe80::1a02:aeff:fe5...	fe80::a00:27ff:fe89...	ICMPv6	78	Neighbor Advertisement fe80::1a02:aeff:fe5a:e9e1 (rtr, sol)

Frame 6575: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec 89:49:08 (08:00:27:89:49:08), Dst: vivoMobileCo 5a:e9:e1 (18:02:ae:5a:e9:e1)
Internet Protocol Version 6, Src: fe80::a00:27ff:fe89:4908, Dst: 2409:4042:4d0d:de10::66
Internet Control Message Protocol v6

18 02 ae 5a e9 e1 08 00 27 89 49 08 06 dd 66 00 ... Z ... I ...
00 00 00 20 3a ff fe 80 00 00 00 00 00 0a 00 ... I \$ @BM ...
27 ff fe 89 49 08 24 09 40 42 4d 0d de 10 00 00 ... f ga ... \$...
00 00 00 00 06 87 00 07 01 00 00 00 00 24 09 ... @BM ... f ...
40 42 4d 0d de 10 00 00 00 00 00 00 00 01 01 ... ' I ...
08 00 27 89 49 08

4. ICMP Timestamp Ping:

ICMP Timestamp Request (Type 13) asks a device for the current time. If allowed, the device responds with Type 14 (Timestamp Reply) containing the time in milliseconds since midnight UTC.

How it Works?

- 1 Host sends an ICMP Type 13 request (Timestamp Request).
- 2 If the target allows it, it replies with ICMP Type 14 (Timestamp Reply) containing the system timestamp.

Command in Kali Linux:

```
nmap -PP 192.168.43.0
```

where, nmap is network mapping.

-PP stands for Timestamp Ping.

192.168.43.0 is targeted ip address.

Example:

```
--# nmap -PP 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:42 EST
map scan report for 192.168.43.1
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT 80 STATE SERVICE 8080/16, ttl=64
3/tcp open  domain 8080/16, ttl=64
AC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

map scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT 80 STATE SERVICE 8080/16, ttl=64
35/tcp open  msrpc 4864/19, ttl=64
39/tcp open  netbios-ssn 20, ttl=64
45/tcp open  microsoft-ds 20, ttl=64
070/tcp open  realserver 8080/16, ttl=64
AC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

map scan report for 192.168.43.238
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT 80 STATE SERVICE 8080/23, ttl=64
1/tcp open  ftp 6144/24, ttl=64
2/tcp open  ssh 6144/24, ttl=64
3/tcp open  telnet 23, ttl=64
5/tcp open  smtp 6400/25, ttl=64
3/tcp open  domain 8080/16, ttl=64
0/tcp open  http 8080/25, ttl=64
11/tcp open  rpcbind 11, ttl=64
39/tcp open  netbios-ssn 20, ttl=64
45/tcp open  microsoft-ds 20, ttl=64
12/tcp open  exec 0, ttl=64
13/tcp open  login 13, ttl=64
14/tcp open  shell 14, ttl=64
099/tcp open  rmiregistry 99, ttl=64
524/tcp open  ingreslock 524, ttl=64
049/tcp open  nfs 49, ttl=64
121/tcp open  ccproxy-ftp 121, ttl=64
306/tcp open  mysql 306, ttl=64
432/tcp open  postgresql 432, ttl=64
900/tcp open  vnc 900, ttl=64
000/tcp open  X11 0, ttl=64
667/tcp open  irc 667, ttl=64
009/tcp open  ajp13 9, ttl=64
180/tcp open  unknown 180, ttl=64
AC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

map scan report for kali (192.168.43.158)
Host is up (0.000071s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Result:

No.	Time	Source	Destination	Protocol	Length	Info
11	5.009678450	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=3840/15, ttl=64
12	5.012043148	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=3840/15, ttl=64
13	6.010931640	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4096/16, ttl=64
14	6.012732210	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=4096/16, ttl=64
15	7.012085657	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4352/17, ttl=64
16	7.013105895	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=4352/17, ttl=64
17	8.012439748	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4608/18, ttl=64
18	8.014177263	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=4608/18, ttl=64
19	9.014151039	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=4864/19, ttl=64
20	9.015016426	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=4864/19, ttl=64
21	10.014538291	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5120/20, ttl=64
22	10.015317257	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=5120/20, ttl=64
23	11.015607193	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5376/21, ttl=64
24	11.017174227	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=5376/21, ttl=64
25	12.017493199	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5632/22, ttl=64
26	12.018955766	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=5632/22, ttl=64
27	13.018454848	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=5888/23, ttl=64
28	13.020233825	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=5888/23, ttl=64
29	14.019765729	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=6144/24, ttl=64
30	14.023055977	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=6144/24, ttl=64
31	15.020555032	192.168.43.158	192.168.43.238	ICMP	54	Timestamp request id=0x5494, seq=6400/25, ttl=64
32	15.022596316	192.168.43.238	192.168.43.158	ICMP	60	Timestamp reply id=0x5494, seq=6400/25, ttl=64

Frame 31: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_08:00:27:2B:EE:15, Dst: PCSSystemtec_2b:ee:15 (08:00:27:2b:ee:15)
Internet Protocol Version 4, Src: 192.168.43.158, Dst: 192.168.43.238
Internet Control Message Protocol

0000 00 00 27 2b ee 15 08 00 27 89 49 08 08 00 45 00 +...+...I...E...
0010 00 28 92 91 00 00 40 01 0f 67 c0 a8 2b 9e c0 a8 (...@...g...+...
0020 2b ee 0d 0d 25 54 94 19 00 01 ad c6 98 00 00 +...%T...
0030 00 00 00 00 00 00

TCP ACK Ping (-PA) is a technique used by Nmap to detect live hosts by sending TCP ACK packets instead of ICMP Echo Requests.

Works:

- Nmap sends a TCP ACK packet to the target.
- If the target is alive, it responds with TCP RST (Reset) (since no connection exists).
- If no response, the target is either offline or blocking packets.
- Bypasses ICMP filtering, useful when ICMP ping is blocked by firewalls.

Command in Kali Linux:

```
nmap -PA 192.168.43.0/24
```

Where, nmap is network mapping

-PA stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

Example:

```
(root@kali) ~ - [ /home/kali ]
# nmap -PA 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:58 EST
Nmap scan report for 192.168.43.1
Host is up (0.0021s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql

Packets: 6583 - Displayed: 2007 (30.5%) - Dropped: 0 (0.0%)
```


Result:

No.	Time	Source	Destination	Protocol	Length	Info
605	2.609667929	192.168.43.1	192.168.43.158	TCP	60	135 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
606	2.609668194	192.168.43.1	192.168.43.158	TCP	60	111 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
617	2.613084747	192.168.43.238	192.168.43.158	TCP	60	8888 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
619	2.613304090	192.168.43.238	192.168.43.158	TCP	60	89 -> 44683 [SYN, ACK] Seq=0 Ack=1 Win=2560 Len=0 MSS=1460
623	2.620696552	192.168.43.238	192.168.43.158	TCP	60	3389 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
624	2.620696877	192.168.43.238	192.168.43.158	TCP	60	143 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
625	2.620696953	192.168.43.238	192.168.43.158	TCP	60	83 -> 44683 [SYN, ACK] Seq=0 Ack=1 Win=2560 Len=0 MSS=1460
626	2.620696980	192.168.43.1	192.168.43.158	TCP	60	8888 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
627	2.620696916	192.168.43.1	192.168.43.158	TCP	60	80 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
628	2.620697276	192.168.43.1	192.168.43.158	TCP	60	3389 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
629	2.620697588	192.168.43.1	192.168.43.158	TCP	60	143 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
630	2.620697938	192.168.43.1	192.168.43.158	TCP	60	93 -> 44683 [SYN, ACK] Seq=0 Ack=1 Win=5535 Len=0 MSS=1460
639	2.623472760	192.168.43.238	192.168.43.158	TCP	60	110 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
650	2.623473451	192.168.43.1	192.168.43.158	TCP	60	118 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
651	2.623473828	192.168.43.1	192.168.43.158	TCP	60	995 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
652	2.623474175	192.168.43.1	192.168.43.158	TCP	60	25 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
653	2.623474558	192.168.43.238	192.168.43.158	TCP	60	995 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
654	2.623474919	192.168.43.238	192.168.43.158	TCP	60	8925 -> 44683 [SYN, ACK] Seq=0 Ack=1 Win=2560 Len=0 MSS=1460
655	2.623475276	192.168.43.238	192.168.43.158	TCP	60	8080 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
656	2.623475598	192.168.43.238	192.168.43.158	TCP	60	21 -> 44683 [SYN, ACK] Seq=0 Ack=1 Win=2560 Len=0 MSS=1460
659	2.624022221	192.168.43.1	192.168.43.158	TCP	60	8080 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
660	2.624755672	192.168.43.1	192.168.43.158	TCP	60	21 -> 44683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Send & Receive Information

```

Frame 651: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, 0
Ethernet II, Src: vivoMobileCo_Ba:9e:01 (18:02:ae:ba:9e:01), Dst: PCSSystemt_89:49:08 (08:00:27:89:49:08)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.158
Transmission Control Protocol, Src Port: 995, Dst Port: 44683, Seq: 1, Ack: 1, Len: 0
          
```

Hex Code

TCP ACK Ping

Send & Receive
Information

No.	Time	Source	Destination	Protocol	Length	Info
605	2.609967929	192.168.43.1	192.168.43.158	TCP	60	60 135 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
606	2.609968194	192.168.43.1	192.168.43.158	TCP	60	60 111 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
617	2.613084147	192.168.43.238	192.168.43.158	TCP	60	60 8688 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
618	2.613894949	192.168.43.238	192.168.43.158	TCP	60	60 80 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
623	2.620965052	192.168.43.238	192.168.43.158	TCP	60	60 3389 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
624	2.620965077	192.168.43.238	192.168.43.158	TCP	60	60 143 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
625	2.620965023	192.168.43.238	192.168.43.158	TCP	60	60 53 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
626	2.620965058	192.168.43.1	192.168.43.158	TCP	60	60 8888 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
627	2.620965616	192.168.43.1	192.168.43.158	TCP	60	60 80 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
628	2.620967276	192.168.43.1	192.168.43.158	TCP	60	60 3389 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
629	2.620967595	192.168.43.1	192.168.43.158	TCP	60	60 143 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
630	2.620967335	192.168.43.1	192.168.43.158	TCP	60	60 53 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
649	2.623272766	192.168.43.238	192.168.43.158	TCP	60	60 111 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
650	2.623473451	192.168.43.1	192.168.43.158	TCP	60	60 110 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
651	2.623473928	192.168.43.1	192.168.43.158	TCP	60	60 135 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
652	2.623474718	192.168.43.1	192.168.43.158	TCP	60	60 75 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
653	2.623474558	192.168.43.238	192.168.43.158	TCP	60	60 995 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
654	2.623474912	192.168.43.238	192.168.43.158	TCP	60	60 75 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
655	2.623475270	192.168.43.1	192.168.43.158	TCP	60	60 135 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
656	2.623475598	192.168.43.238	192.168.43.158	TCP	60	60 21 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
659	2.624622521	192.168.43.1	192.168.43.158	TCP	60	60 8080 - 44663 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
660	2.624755072	192.168.43.1	192.168.43.158	TCP	60	60 21 - 44663 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

```

Frame 660: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, 10 B
Ethernet II, Src: vmnic1 (18:02:ae:a9:8e:1), Dst: PCSystematic-89:48 (08:00:27:78:9f:49)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.158
Transmission Control Protocol, Src Port: 995, Dst Port: 44663, Seq: 1, Ack: 1, Len: 0
  
```

Hex Code

7. TCP SYN Ping:

TCP SYN Ping (-PS) is a host discovery technique used by Nmap to check if a system is alive by sending TCP SYN packets instead of ICMP pings.

Works:

Works:

Sends a TCP SYN Packet: Nmap sends a SYN packet to a target port.

Receives a Response: SYN-ACK: Indicates the port is open and the host is alive.

RST (Reset): Indicates the port is closed, but the host is still up.

No Response: May mean the host is down or blocking the probe.

Command I Kali Linux:

```
nmap -PS 192.168.43.0
```

Where, nmap is network mapping.

-PS stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

Example:

```
(root@kali)~# nmap -PS 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:48 EST
Nmap scan report for 192.168.43.1
Host is up (0.0025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0010s latency).
Not shown: 996 filtered tcp ports (no-response)
```

```

PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry

Packets: 6620 - Dropped: 0 (0.0%)

```

Result:

4377 2.579761934	192.168.43.238	192.168.43.158	TCP	60 1639 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Send & Receive Information
4378 2.579762044	192.168.43.238	192.168.43.158	TCP	60 2869 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4379 2.579762156	192.168.43.238	192.168.43.158	TCP	60 5910 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4380 2.579921386	192.168.43.238	192.168.43.158	TCP	60 1310 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4381 2.579921587	192.168.43.238	192.168.43.158	TCP	60 7025 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4382 2.580158269	192.168.43.1	192.168.43.158	TCP	60 7200 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4383 2.580158544	192.168.43.1	192.168.43.158	TCP	60 0025 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4384 2.580350430	192.168.43.1	192.168.43.158	TCP	60 1998 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4385 2.580350710	192.168.43.1	192.168.43.158	TCP	60 1839 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4386 2.580952937	192.168.43.1	192.168.43.158	TCP	60 2869 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
4387 2.580953461	192.168.43.1	192.168.43.158	TCP	60 5910 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	TCP ACK Ping
4388 2.581102005	192.168.43.158	192.168.43.238	TCP	58 49088 -- 3027 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4389 2.581101838	192.168.43.158	192.168.43.1	TCP	58 49088 -- 1310 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4390 2.581310315	192.168.43.158	192.168.43.238	TCP	58 49088 -- 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4391 2.581491426	192.168.43.158	192.168.43.1	TCP	58 49088 -- 7025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4392 2.581529659	192.168.43.158	192.168.43.238	TCP	58 49088 -- 42510 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4393 2.581564073	192.168.43.158	192.168.43.1	TCP	58 49088 -- 3827 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4394 2.581585746	192.168.43.158	192.168.43.238	TCP	58 49088 -- 687 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4395 2.581607511	192.168.43.158	192.168.43.1	TCP	58 49088 -- 65129 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4396 2.581701035	192.168.43.158	192.168.43.238	TCP	58 49088 -- 3030 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4397 2.581857967	192.168.43.158	192.168.43.1	TCP	58 49088 -- 42510 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
4398 2.581971795	192.168.43.1	192.168.43.158	TCP	60 1310 -- 49088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

Frame 531: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0

Ethernet II, Src: PCSysmetec_89:49:08 (08:00:27:09:49:08), Dst: Intel_55:da:1b (68:ec:c5:55:da:1b)

Internet Protocol Version 4, Src: 192.168.43.158, Dst: 192.168.43.141

Transmission Control Protocol, Src Port: 49088, Dst Port: 256, Seq: 0, Len: 0

Hex Code

8. UDP Ping:

UDP Ping is a network scanning technique used to determine if a host is online by sending UDP packets to a target port.

Works:

Sends a UDP Packet: A UDP packet is sent to a specific port on the target host.

Response Received: ICMP "Port Unreachable" reply indicates the host is up if the port is closed.

No Response: Could mean the port is open/filtered or the host is down.

Command in Kali Linux:

Nmap -PU 192.168.43.0

Where, nmap is network mapping

-PU stand for UDP Ping.

192.168.43.0 is a target ip address.

Example:

```
(root@kali: ~/nmap/kali)
# nmap -PU 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:08 EST
Nmap scan report for 192.168.43.1
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
13/tcp    open  domain
13/tcp    open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0013s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
35/tcp    open  msrpc
39/tcp    open  netbios-ssn
45/tcp    open  microsoft-ds
670/tcp   open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.00074s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  ftp
2/tcp     open  ssh
3/tcp     open  telnet
5/tcp     open  smtp
3/tcp     open  domain
10/tcp    open  http
11/tcp    open  rpcbind
39/tcp    open  netbios-ssn
45/tcp    open  microsoft-ds
12/tcp    open  exec
13/tcp    open  login
14/tcp    open  shell
1099/tcp  open  rmiregistry
524/tcp   open  ingreslock
1049/tcp  open  nfs
121/tcp   open  ccproxy-ftp
306/tcp   open  mysql
432/tcp   open  postgresql
900/tcp   open  vnc
1000/tcp  open  X11
667/tcp   open  irc
1009/tcp  open  ajp13
180/tcp   open  unknown
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for kali (192.168.43.158)
Host is up (0.000015s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Target ip address

UDP Ping

Result:

No.	Time	Source	Destination	Protocol	Length	Info
519	1.912418813	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	106	Standard query 0xd631 PTR 1.43.168.192.in-addr.arpa
520	1.913845995	192.168.43.158	192.168.43.1	DNS	87	Standard query 0xd632 PTR 141.43.168.192.in-addr.arpa
521	1.914875614	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	107	Standard query 0xd633 PTR 238.43.168.192.in-addr.arpa
522	1.922370922	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	105	Standard query response 0xd631 No such name PTR 1.43.168.192.in-addr.arpa
523	1.922372227	192.168.43.1	192.168.43.158	DNS	116	Standard query response 0xd632 PTR 141.43.168.192.in-addr.arpa PTR DESKTOP-2EUMV42
524	1.922372784	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	107	Standard query response 0xd633 No such name PTR 238.43.168.192.in-addr.arpa
525	1.930842237	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	107	Standard query 0xd634 PTR 158.43.168.192.in-addr.arpa
526	1.941949729	2409:4042:4d0d:de10::	2409:4042:4d0d:de10::	DNS	125	Standard query response 0xd634 PTR 158.43.168.192.in-addr.arpa PTR kali

UDP Ping

Send & Receive Information

Hex Code

Frame 526: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface eth0, id 0

Ethernet II, Src: vivoMobileCo_5a:e9:e1 (18:02:ae:5a:e9:e1), Dst: PCSSystemtec_89:49:08 (08:00:27:89:49:08)

Internet Protocol Version 6, Src: 2409:4042:4d0d:de10::c6, Dst: 2409:4042:4d0d:de10:3624:252a:083b:a048

User Datagram Protocol, Src Port: 53, Dst Port: 33727

Domain Name System (response)

0000

08 00 27 89 49 08 18 02 ae 5a e9 e1 86 dd 00 0d

... I ... Z ...

0010

2d 00 00 47 11 40 24 09 40 42 4d 0d de 10 00 00

... G @ \$ @ B M ...

0020

00 00 00 00 00 00 24 09 40 42 4d 0d de 10 36 24

... f S @ B M ...

0030

25 2a 88 3b a9 48 00 35 83 bf 00 47 fe f3 d6 34

... * ; H 5 ... G 4

0040

85 80 00 01 00 01 00 00 00 00 03 31 35 38 02 34

... 158 4

0050

33 03 31 36 38 03 31 39 32 07 09 6e 2d 61 64 04

3 168 19 2 in-add

0060

72 04 61 72 70 61 00 00 0c 00 01 c9 0c 00 0c 00

r arpa ...

0070

01 00 00 00 00 00 06 04 6b 41 6c 69 00

... kali