

Ping Sweep (ICMP Sweep) Fping | Nmap

[8 de julho de 2015](#) / [maximoz](#)

Introdução

Para entender o *ping sweep*, é preciso, antes de tudo, entender alguns conceitos para que, ao decorrer da explicação, você não se depare com algum termo desconhecido. Tais conceitos a serem entendidos são os de **ping** e **ICMP**. Depois disso, você estará mais familiarizado com o assunto e será mais fácil compreender.

Ping

Ping é um programa de internet básico que permite um usuário verificar se um endereço de IP particular existe e pode aceitar requisições.

O ping é usado diagnosticamente para garantir se um host (computador) que o usuário está tentando se conectar está realmente operando. Ele funciona enviando uma requisição *Echo* do protocolo ICMP (Internet Control Message Protocol) para uma interface específica em uma rede e esperando por uma resposta. Ele pode ser usado para solucionar problemas, para testar a conectividade de um host e determinar o tempo de resposta.

Como um verbo, ping significa “chamar a atenção de” ou “verificar a presença de” outra parte da rede. o acrônimo (para Packet Internet ou Inter-Network Groper) foi planejado para coincidir com o termo de marinheiros para o som de um pulso sonar retornado.

ICMP

ICMP (Internet Control Message Protocol) é um protocolo relator de mensagens que dispositivos de rede como roteadores usam para gerar mensagens de erro para o endereço de IP de origem quando problemas de rede impedem a distribuição de pacotes IP. O ICMP cria e envia mensagens para o endereço IP de origem indicando que um gateway para a internet que um roteador, serviço ou host não pode ser alcançado para a entrega de pacote. Qualquer IP de um dispositivo da rede tem a capacidade de enviar, receber ou processar ICMP mensagens.

ICMP **não é** um protocolo de transporte que envia dados entre sistemas.

Embora ICMP não usado regularmente em aplicações para o usuário final, é usado pelos administradores de rede para solucionar problemas de conexões de internet em utilitário de diagnóstico, incluindo *ping* e o *traceroute*.

Como um dos principais protocolos de internet, ICMP é usado por roteadores, dispositivos intermediários ou hosts para comunicar erros, informações ou atualizações para outros roteadores, dispositivos intermediários ou hosts. O amplamente utilizado IPv4 (Internet Protocol version 4) e o mais novo IPv6 usam versões similares do protocolo ICMP (ICMPv4 e ICMPv6, respectivamente).

Mensagens ICMP são transmitidas como datagramas e consistem de um cabeçalho de IP que encapsula os dados ICMP. Pacotes ICMP são pacotes IP com ICMP na parte de dados IP. Mensagens ICMP também contém um cabeçalho IP inteiro da mensagem original, então o sistema final sabe qual pacote falhou.

O cabeçalho ICMP aparece depois do cabeçalho do pacote IPv4 ou IPv6 e é identificado como um protocolo IP número 1. O protocolo complexo consiste em três campos:

- O maior tipo que identifica a mensagem ICMP;
- O menor código que contém mais informação sobre o tipo de campo;
- O checksum que ajuda a detectar erros introduzidos durante a transmissão.

Seguindo os três campos, são os dados ICMP e o IP original cabeçalho IP para identificar quais pacotes realmente falharam.

ICMP foi usado para executar ataques de negação de serviço (DoS) enviando pacotes IP maiores que o número de bytes permitidos pelo protocolo IP.

Ping Sweep

Esse não é um assunto muito extenso, mas de qualquer forma eu acho importante aprender sobre qualquer tópicos partindo dos seus princípios, por isso quis que vocês entendessem sobre **ping** e **ICMP**, mesmo que a explicação deles tenha ficado maior que a explicação do principal assunto em

questão.

Um *ping sweep* (também conhecido como um ICMP sweep) é uma técnica básica de **network scanning** (escaneamento de rede) usada para determinar, em um intervalo de endereços (range), quais hosts estão ativos (computadores). Enquanto que um único ping irá dizer para você se um host específico existe na rede, um ping sweep consiste em requisições *ECHO ICMP* (Internet Control Message Protocol) enviadas a vários hosts. Se um dado endereço está ativo, irá retornar um *ICMP ECHO reply*. Os ping sweeps estão entre os métodos mais antigos e lentos usados para fazer a varredura de uma rede.

Há uma série de ferramentas que podem ser usadas para fazer um ping sweep, como [fping](#), [gping](#) e [nmap](#) para sistemas UNIX, e [Ping Sweep](#) para sistemas windows no qual envia vários pacotes ao mesmo tempo e permite o usuário descobrir os hosts e salvar o output para um arquivo.

Ping Sweep com fping

Definição do [site oficial](#):

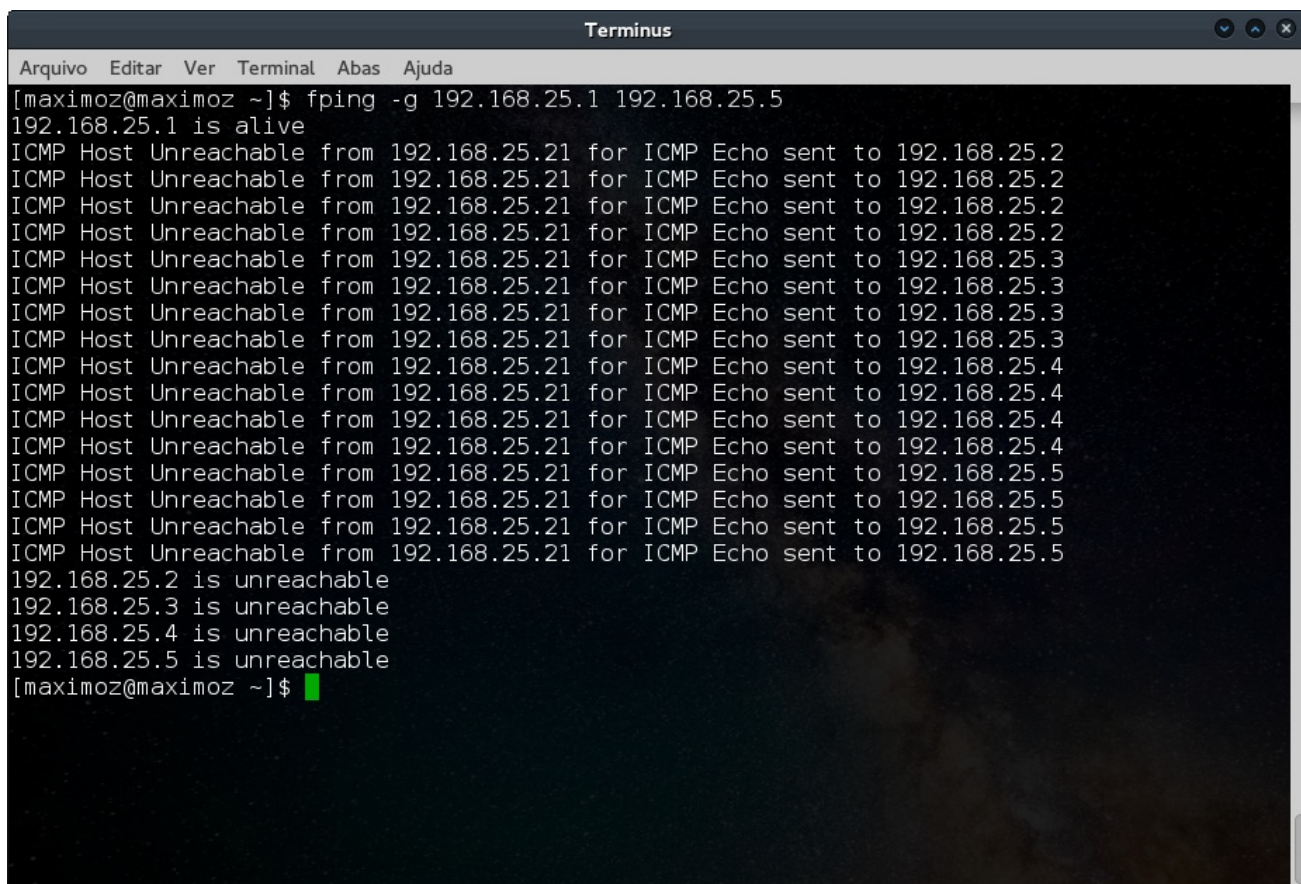
“fping é um programa que envia requisições ICMP echo à hosts de rede, semelhante ao ping, mas muito melhor em caso de múltiplos hosts. O fping tem uma longa história: Roland Schemers publicou uma primeira versão dela em 1992 e ela se estabeleceu por si própria desde então como uma ferramenta padrão para diagnósticos e estatísticas de rede.”

Você pode baixá-la pelo [link](#) direto ou pelo [github](#).

Mas antes verifique se o repositório da sua distro linux já o contém. Dessa forma, facilitando a instalação.

Existem algumas maneiras diferentes para escanear múltiplos hosts. A primeira é usando a flag **-g** **<range>** para indicar que será usado um range de IP. O comando fica o seguinte:

```
fping -g 192.168.25.1 192.168.25.5
```



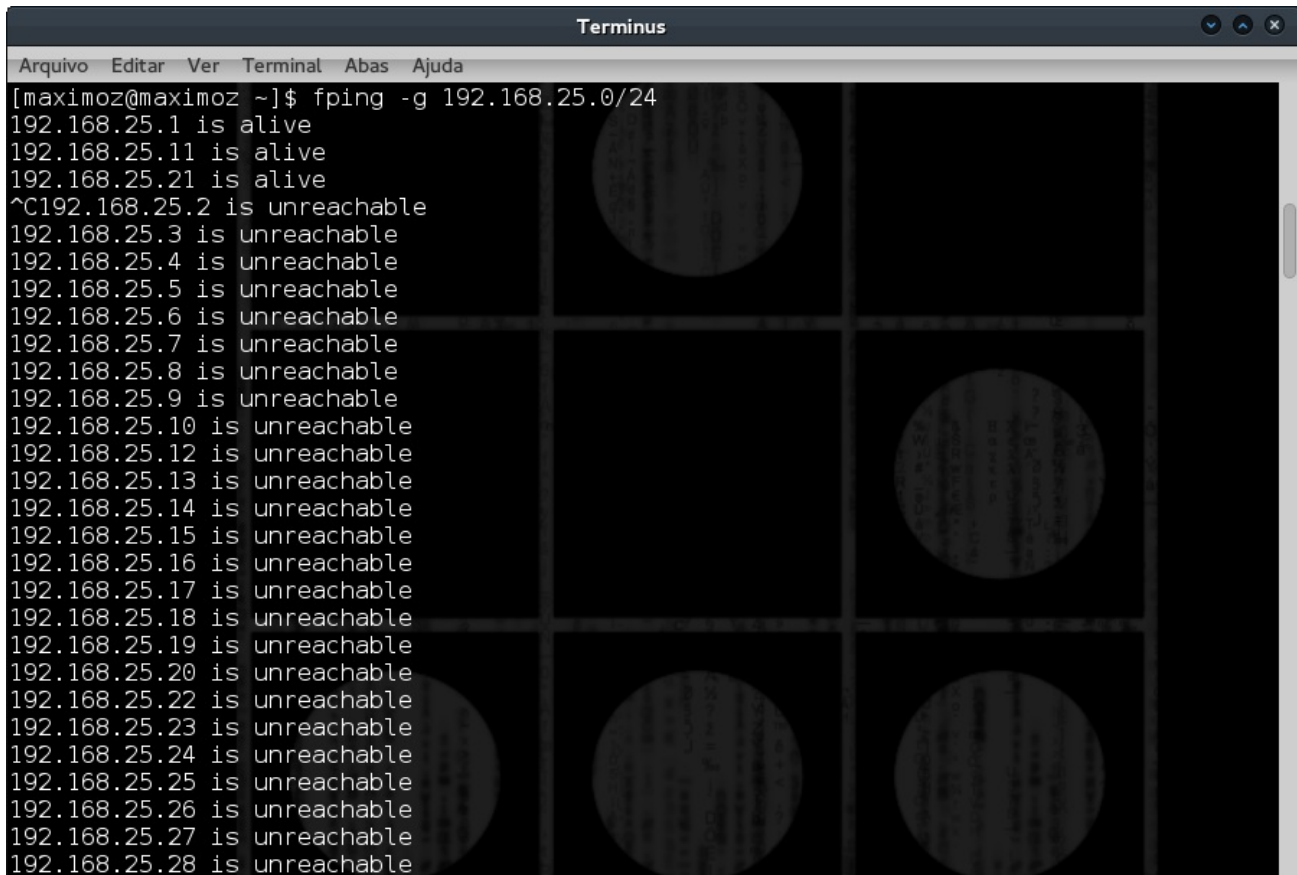
```
Terminus
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[maximoz@maximoz ~]$ fping -g 192.168.25.1 192.168.25.5
192.168.25.1 is alive
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.2
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.2
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.2
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.2
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.3
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.3
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.3
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.3
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.4
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.4
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.4
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.4
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.5
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.5
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.5
ICMP Host Unreachable from 192.168.25.21 for ICMP Echo sent to 192.168.25.5
192.168.25.2 is unreachable
192.168.25.3 is unreachable
192.168.25.4 is unreachable
192.168.25.5 is unreachable
[maximoz@maximoz ~]$
```

Aqui vemos que ele testou cinco hosts e notificou que o 192.168.25.1 está ativo enquanto que os outros estão ‘fora do alcance’, ou seja, não estão ativos. Poderíamos ter colocado para verificar todos os hosts da rede como:

```
fping -g 192.168.25.1 192.168.25.255
```

Você pode colocar o intervalo que quiser se você for fazer entre um intervalo de endereços específicos, mas para uma rede interna toda recomendo usar o seguinte comando:

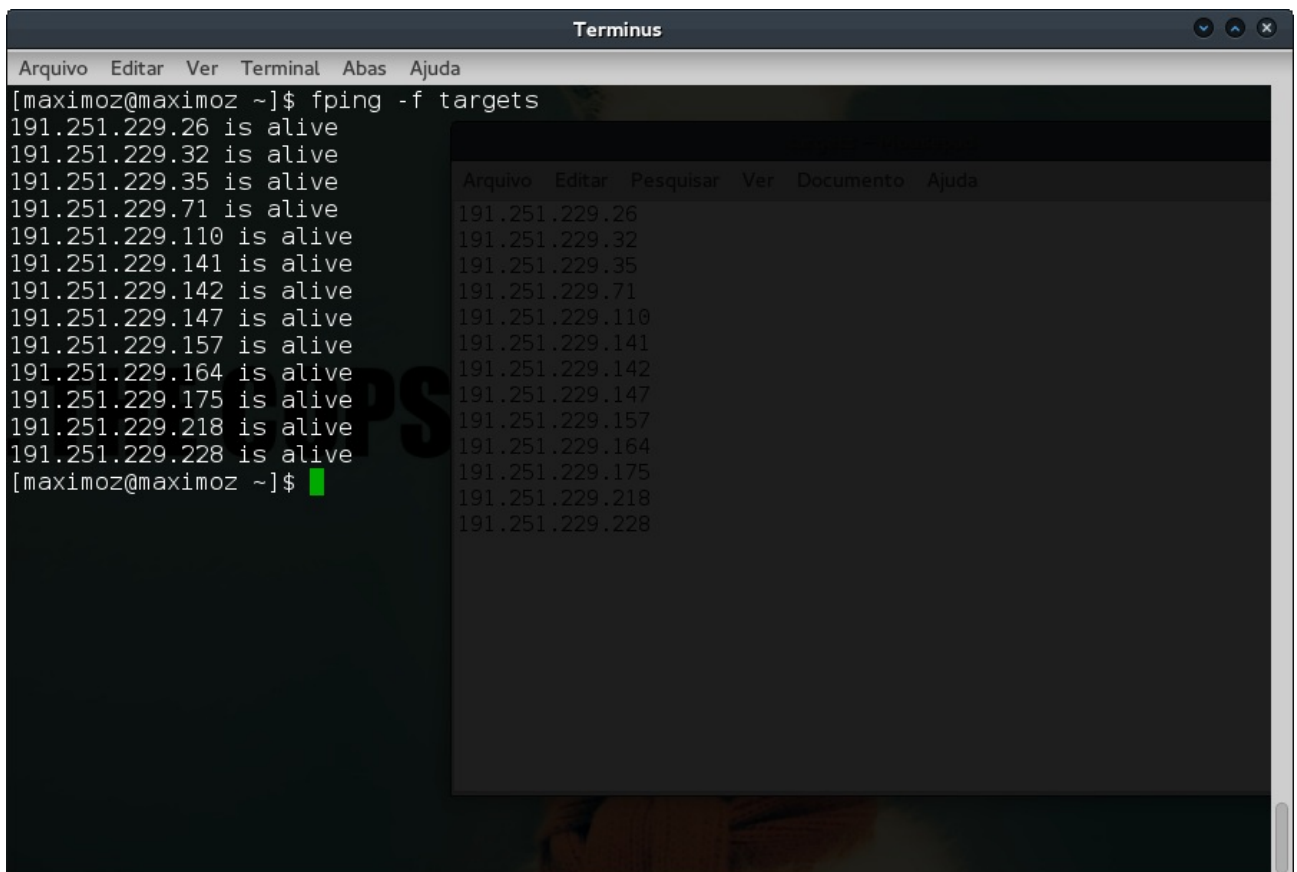
```
fping -g 192.168.25.0/24
```



```
Terminus
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[maximoz@maximoz ~]$ fping -g 192.168.25.0/24
192.168.25.1 is alive
192.168.25.11 is alive
192.168.25.21 is alive
^C192.168.25.2 is unreachable
192.168.25.3 is unreachable
192.168.25.4 is unreachable
192.168.25.5 is unreachable
192.168.25.6 is unreachable
192.168.25.7 is unreachable
192.168.25.8 is unreachable
192.168.25.9 is unreachable
192.168.25.10 is unreachable
192.168.25.12 is unreachable
192.168.25.13 is unreachable
192.168.25.14 is unreachable
192.168.25.15 is unreachable
192.168.25.16 is unreachable
192.168.25.17 is unreachable
192.168.25.18 is unreachable
192.168.25.19 is unreachable
192.168.25.20 is unreachable
192.168.25.22 is unreachable
192.168.25.23 is unreachable
192.168.25.24 is unreachable
192.168.25.25 is unreachable
192.168.25.26 is unreachable
192.168.25.27 is unreachable
192.168.25.28 is unreachable
```

Ele irá fazer o scan de toda a rede da mesma forma. Agora se você tem uma lista de endereços que quer testar, você pode colocá-los em um arquivo de texto e usar a flag **-f** <nome do arquivo>. Veja o exemplo.

```
fping -f targets
```



```
Terminus
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[maximoz@maximoz ~]$ fping -f targets
191.251.229.26 is alive
191.251.229.32 is alive
191.251.229.35 is alive
191.251.229.71 is alive
191.251.229.110 is alive
191.251.229.141 is alive
191.251.229.142 is alive
191.251.229.147 is alive
191.251.229.157 is alive
191.251.229.164 is alive
191.251.229.175 is alive
191.251.229.218 is alive
191.251.229.228 is alive
[maximoz@maximoz ~]$
```

Arquivo Editar Pesquisar Ver Documento Ajuda

```
191.251.229.26
191.251.229.32
191.251.229.35
191.251.229.71
191.251.229.110
191.251.229.141
191.251.229.142
191.251.229.147
191.251.229.157
191.251.229.164
191.251.229.175
191.251.229.218
191.251.229.228
```

Enfim, é só usar o help do fping que terá outras opções que você pode explorar.

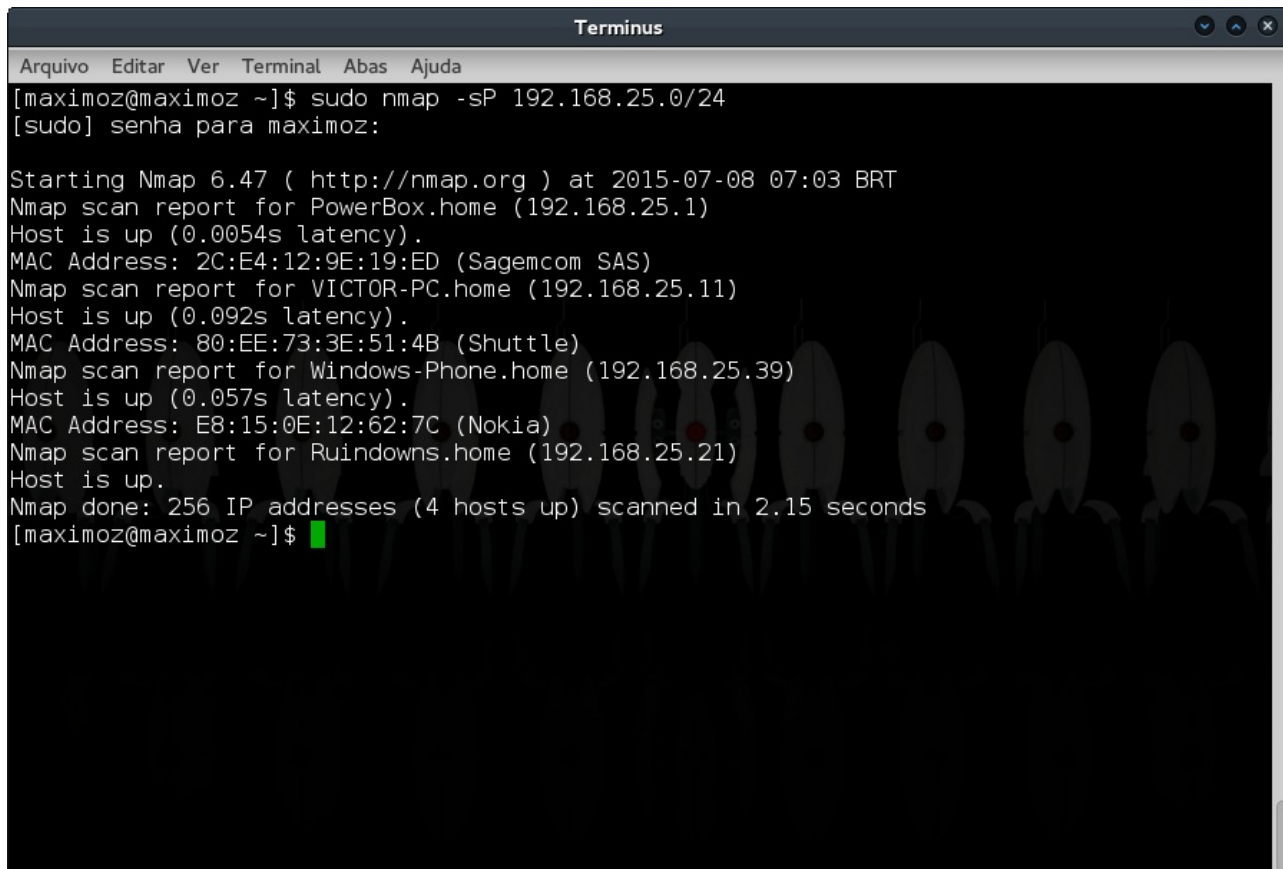
Ping Sweep com Nmap

Agora é a vez da nossa conhecida ferramenta. Uma vez que todos conhecemos ela, não é necessário nenhuma apresentação e explicação para definir o quão poderosa é ela. O nmap tem uma função similar que testa se um host está ativo e é a flag **-sP**. Aqui podemos usufruir de intervalos de endereços também. Se você for usar uma quantidade específica de hosts a serem escaneados, basta fazer o seguinte:

```
nmap -sP 192.168.25.0-56
```

Mas se você quiser escanear toda a rede, é só usar a mesma lógica que foi mostrado no fping, dessa forma:

```
nmap -sP 192.168.25.0/24
```



```
Terminus
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
[maximoz@maximoz ~]$ sudo nmap -sP 192.168.25.0/24
[sudo] senha para maximoz:

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-08 07:03 BRT
Nmap scan report for PowerBox.home (192.168.25.1)
Host is up (0.0054s latency).
MAC Address: 2C:E4:12:9E:19:ED (Sagemcom SAS)
Nmap scan report for VICTOR-PC.home (192.168.25.11)
Host is up (0.092s latency).
MAC Address: 80:EE:73:3E:51:4B (Shuttle)
Nmap scan report for Windows-Phone.home (192.168.25.39)
Host is up (0.057s latency).
MAC Address: E8:15:0E:12:62:7C (Nokia)
Nmap scan report for Ruindowns.home (192.168.25.21)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.15 seconds
[maximoz@maximoz ~]$
```

Esse tipo de scan do nmap nos informa quais hosts estão ativos entre o range que informamos em vez de informar se uma porta está aberta ou não. O nmap envia um pacote ICMP ECHO REQUEST e espera por um ICMP ECHO REPLY. Se ele receber essa resposta, significa que o host está online e que os pacotes não foram bloqueados. Se o nmap não receber uma resposta, ele vai tentar outro método chamado *TCP Ping* no qual vai verificar se o pacote foi bloqueado ou se o host realmente não está ativo.

Um *TCP Ping* envia ou um pacote SYN ou um ACK para qualquer porta (por padrão, é a porta 80) ao sistema alvo. Se um pacote RST ou SYN/ACK é retornado, então o sistema alvo está ativo. Se o sistema alvo não responder, ou ele está offline ou o estado da porta escolhida está como *filtered* e, logo, não responde a nada.

Quando você executa o *Ping Scan* no nmap com o usuário root, o padrão é usar os métodos ICMP e ACK. Enquanto usuários comuns irão usar o método *connect()* no qual tenta se conectar a uma máquina, esperando por uma resposta e derrubando a conexão assim que ela é estabelecida (semelhante ao método SYN/ACK para usuários root mas nesse caso é estabelecido uma conexão TCP completa). O scan ICMP pode ser desabilitado usando **-P0**.

Tip: Você pode usar essa técnica para saber quais IPs da sua região estão ativos. Basta você pegar seu IP externo usando um site como <http://whatismyipaddress.com> e mudar o último elemento depois do ponto para 0/24, ficando assim xxx.yyy.zzz.0/24, ele irá verificar todos os IPs entre 0 e 255.

Referências bibliográficas:

[Ping Sweep](#)

[Ping](#)

[ICMP](#)

<https://nmap.org/bennieston-tutorial/>