**GUIDE 04**

**2.**

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 192.1.1.21:21664 192.168.1.1:21664 192.1.1.45:21664 192.1.1.45:21664

icmp 192.1.1.21:21920 192.168.1.1:21920 192.1.1.45:21920 192.1.1.45:21920

icmp 192.1.1.21:22176 192.168.1.1:22176 192.1.1.45:22176 192.1.1.45:22176

icmp 192.1.1.21:22432 192.168.1.1:22432 192.1.1.45:22432 192.1.1.45:22432

icmp 192.1.1.21:22688 192.168.1.1:22688 192.1.1.45:22688 192.1.1.45:22688

--- 192.1.1.21 192.168.1.1 --- ---

R1#show ip nat statistics

Total active translations: 6 (0 static, 6 dynamic; 5 extended)

Outside interfaces:

FastEthernet0/1

Inside interfaces:

FastEthernet0/0

Hits: 25 Misses: 24

CEF Translated packets: 48, CEF Punted packets: 10

Expired translations: 12

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 2 pool MYNATPOOL refcount 6

pool MYNATPOOL: netmask 255.255.255.0

start 192.1.1.21 end 192.1.1.21

type generic, total addresses 1, allocated 1 (100%), misses 10

Appl doors: 0

Normal doors: 0

Queued Packets: 0

**PC1**

PC1> ping 192.1.1.45

84 bytes from 192.1.1.45 icmp\_seq=1 ttl=63 time=29.880 ms

84 bytes from 192.1.1.45 icmp\_seq=2 ttl=63 time=31.089 ms

84 bytes from 192.1.1.45 icmp\_seq=3 ttl=63 time=30.066 ms

84 bytes from 192.1.1.45 icmp\_seq=4 ttl=63 time=30.983 ms

84 bytes from 192.1.1.45 icmp\_seq=5 ttl=63 time=32.201 ms

**PC2**

PC2> ping 192.1.1.45

\*192.168.1.254 icmp\_seq=1 ttl=255 time=15.988 ms (ICMP type:3, code:1, Destination host unreachable)

\*192.168.1.254 icmp\_seq=2 ttl=255 time=16.528 ms (ICMP type:3, code:1, Destination host unreachable)

\*192.168.1.254 icmp\_seq=3 ttl=255 time=16.152 ms (ICMP type:3, code:1, Destination host unreachable)

\*192.168.1.254 icmp\_seq=4 ttl=255 time=14.768 ms (ICMP type:3, code:1, Destination host unreachable)

\*192.168.1.254 icmp\_seq=5 ttl=255 time=15.708 ms (ICMP type:3, code:1, Destination host unreachable)

A partir desses resultados e da captura no Wireshark, podemos concluir que os pacotes que tiveram os seus endereços IP de origem traduzidos são os enviados pelo PC1. Isso ocorre porque, ao configurar o nat pool do router definimos o pool com apenas um endereço público. Como o PC1 foi o primeiro a executar o comando de ping, ele é quem ocupa e mantém o único endereço público dessa rede privada, e, portanto, o PC2 não consegue comunicar com a rede pública.

**3.**

PC2> ping 192.1.1.45

84 bytes from 192.1.1.45 icmp\_seq=1 ttl=63 time=31.658 ms

84 bytes from 192.1.1.45 icmp\_seq=2 ttl=63 time=31.238 ms

84 bytes from 192.1.1.45 icmp\_seq=3 ttl=63 time=30.988 ms

84 bytes from 192.1.1.45 icmp\_seq=4 ttl=63 time=31.820 ms

84 bytes from 192.1.1.45 icmp\_seq=5 ttl=63 time=30.962 ms

Ao executar o comando clear ip nat translation \* no router, a nat translation table é limpa, liberando o endereço IP público no pool, permitindo que outros dispositivos da rede privada possam usá-lo. O PC2, ao executar o ping primeiro, assumiu o endereço público, garantindo a sua comunicação com a rede pública.

**4.**

Ao configurar o tempo de expiração do NAT para 60 segundos, após 60 segundos de inatividade do PC1, a nat translation table é limpa, podendo então o PC2 assumir o endereço público.

**5.**

As vantagens são que vários endereços internos numa rede privada podem usar o mesmo endereço público, distinguindo cada conexão pelas suas respetivas portas, preservando a segurança e a privacidade.

**6.**

UDP ping:

84 bytes from 192.1.1.40 udp\_seq=1 ttl=63 time=31.026 ms

84 bytes from 192.1.1.40 udp\_seq=2 ttl=63 time=29.272 ms

84 bytes from 192.1.1.40 udp\_seq=3 ttl=63 time=31.077 ms

TCP ping:

Connect 80@192.1.1.40 seq=1 ttl=63 time=46.320 ms

SendData 80@192.1.1.40 seq=1 ttl=63 time=46.193 ms

Close 80@192.1.1.40 seq=1 ttl=63 time=61.321 ms

Connect 80@192.1.1.40 seq=2 ttl=63 time=44.840 ms

SendData 80@192.1.1.40 seq=2 ttl=63 time=46.478 ms

Close 80@192.1.1.40 seq=2 ttl=63 time=56.346 ms

Connect 80@192.1.1.40 seq=3 ttl=63 time=44.554 ms

SendData 80@192.1.1.40 seq=3 ttl=63 time=45.859 ms

Close 80@192.1.1.40 seq=3 ttl=63 time=61.965 ms

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

tcp 192.1.1.21:5449 192.168.1.1:5449 192.1.1.40:80 192.1.1.40:80

tcp 192.1.1.21:8725 192.168.1.1:8725 192.1.1.40:22 192.1.1.40:22

udp 192.1.1.21:12404 192.168.1.1:12404 192.1.1.40:22 192.1.1.40:22

udp 192.1.1.21:28458 192.168.1.1:28458 192.1.1.40:80 192.1.1.40:80

Com isto, podemos concluir que todas as conexões UDP são registradas mesmo que a porta já tenha sido utilizada, mas ao conectar usando TCP através de uma porta já utilizada, a conexão anterior é sobrescrita.

**10.**

**ip dhcp**

Inicialmente, temos um pacote DHCP Discover, usado para verificar se o endereço IP está disponível, solicitando um pacote ARP. Depois disso, temos outro pacote DHCP Discover, desta vez para validar se o endereço está realmente disponível. Em seguida, temos um pacote DHCP Offer que informa ao terminal que ele pode usar o endereço. Depois, temos um pacote DHCP Request do terminal para o router, indicando que ele deseja usar o endereço. Por fim, temos um pacote DHCP ACK (acknowledge) que vai do router para o terminal, confirmando que ele utilizará o endereço.

**ip dhcp -r**

Desta vez, há apenas um pacote DHCP Discover, pois ele vem de um terminal que o serviço DHCP já conhece e tem um endereço IP vinculado a ele. Os outros passos e pacotes são iguais ao comando anterior.

**ip dhcp -x**

O único pacote trocado é o pacote DHCP Release, que informa ao router para liberar o endereço IP que estava sendo utilizado.

**ip dhcp**

O procedimento é o mesmo da primeira execução deste comando, mas agora o endereço IP é incrementado em 1 (de 192.168.1.101 para 192.168.1.102).

**IPV6**

**3.**

O router envia uma mensagem para a máquina virtual, lembrando que o endereço IPv6 foi solicitado no router. Em seguida, uma solicitação é feita pelo router para a máquina virtual referente a esse endereço IPv6 específico. Posteriormente, o roteador envia outra mensagem indicando que o endereço está disponível e pode ser utilizado. Finalmente, a máquina virtual faz um anúncio para o router, confirmando que o endereço IPv6 será utilizado por ela.

**4.**

Uma das desvantagens de usar EUI-64 é que, se um invasor conseguir acesso dentro da rede, ele pode facilmente triangular o endereço IPv6 de alguém e, assim, direcionar ataques a esse terminal específico. Isso pode ser evitado simplesmente randomizando o ID da interface, tornando o endereço IPv6 mais difícil de rastrear/encontrar.

O processo de obtenção de um endereço IPv6 não muda se for feito pelo mesmo endereço MAC, pois o processo é exatamente o mesmo, e é por isso que não é muito seguro utilizá-lo.