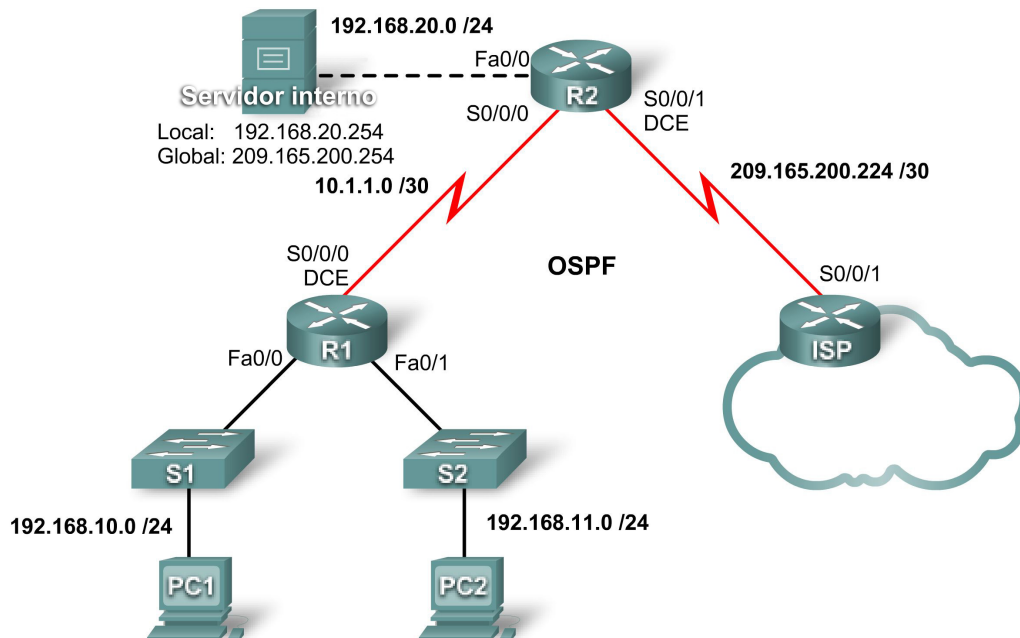


## Laboratório 7.4.1: Configuração básica DHCP e NAT

### Diagrama de topologia



### Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

### Objetivos de aprendizagem

Após concluir este laboratório, você será capaz de:

- Prepare a rede.
- Execute as configurações básicas de roteador.
- Configure um servidor DHCP do Cisco IOS.
- Configurar roteamentos estático e padrão
- Configure a NAT estática.
- Configure NAT dinâmica usando um conjunto de endereços.

- Configure sobrecarga NAT.

## Cenário

Neste laboratório, você irá configurar os serviços DHCP e NAT IP. Um roteador é o servidor DHCP. O outro roteador encaminha solicitações de DHCP ao servidor. Você também definirá as configurações de NAT estáticas e dinâmicas, inclusive sobrecarga de NAT. Quando você concluir as configurações, verifique a conectividade entre os endereços internos e externos.

## Tarefa 1: Preparar a rede

### **Etapas 1: Cabear uma rede de maneira semelhante à presente no diagrama de topologia.**

Você pode utilizar qualquer roteador atual em seu laboratório contanto que ele tenha as interfaces exigidas mostradas na topologia.

Nota: se você utilizar um roteador das séries 1700, 2500 ou 2600, as saídas do comando do roteador e as descrições de interface poderão ser diferentes. Em roteadores mais antigos, alguns comandos podem ser diferentes, ou não existem.

### **Etapas 2: Apagar todas as configurações existentes nos roteadores.**

## Tarefa 2: Executar configurações básicas do roteador

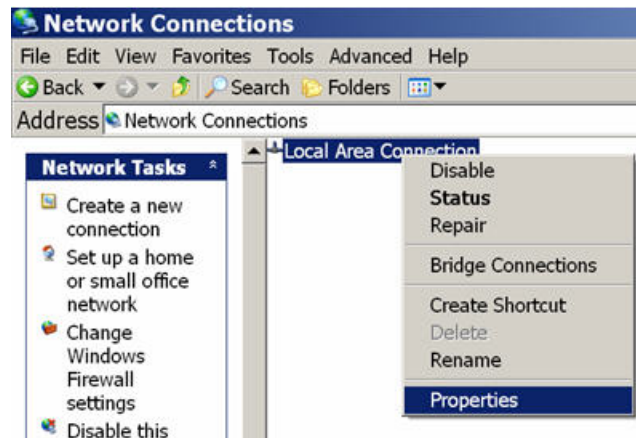
Configure os roteadores R1, R2 e ISP de acordo com as seguintes diretrizes:

- Configure o nome de host do dispositivo.
- Desabilite a pesquisa DNS.
- Configure uma senha no modo EXEC privilegiado.
- Configure um banner de mensagem do dia.
- Configure uma senha para as conexões de console.
- Configure uma senha para todas as conexões vty.
- Configure endereços IP em todos os roteadores. Os PCs recebem endereçamento IP de DHCP posteriormente no laboratório.
- Habilite o OSPF com o ID de processo 1 em R1 e R2. Não anuncie a rede 209.165.200.224/27.

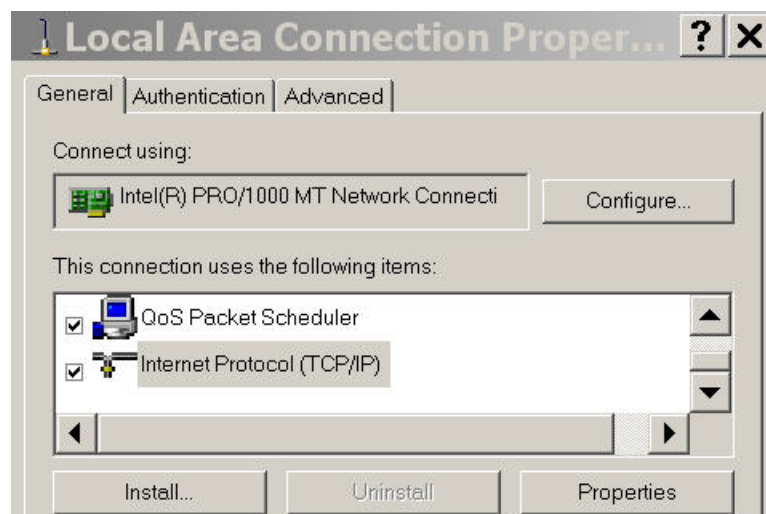
Nota: em vez de anexar um servidor a R2, você pode configurar uma interface de loopback em R2 para utilizar o endereço IP 192.168.20.254/24. Se fizer isso, você não precisará configurar a interface Fast Ethernet.

## Tarefa 3: Configurar PC1 e PC2 para receber um endereço IP por meio de DHCP

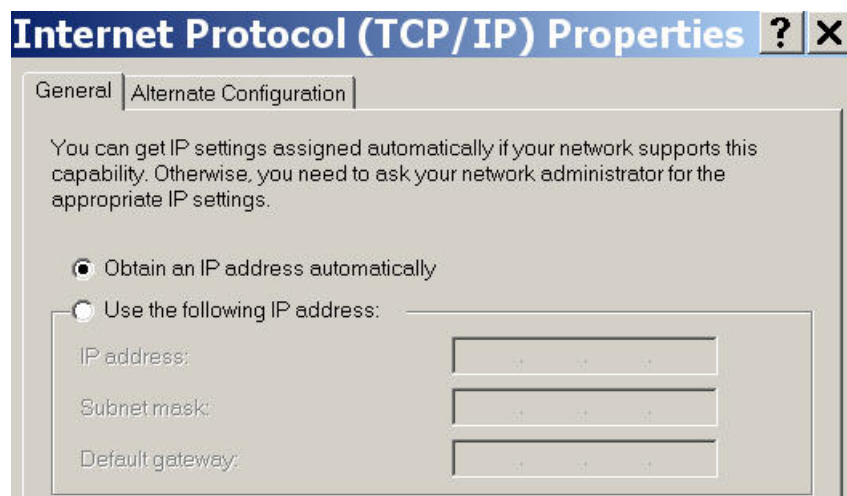
Em um PC com Windows, vá até **Start -> Control Panel -> Network Connections -> Local Area Connection**. Clique com o botão direito do mouse em **Local Area Connection** e selecione **Properties**.



Role para baixo e realce **Internet Protocol (TCP/IP)**. Clique no botão **Properties**.



Verifique se o botão está selecionado informando **Obtain an IP address automatically**.



Quando isso for feito em PC1 e PC2, eles estarão prontos para receber um endereço IP de um servidor DHCP.

#### Tarefa 4: Configurar um servidor DHCP do IOS Cisco

O software IOS Cisco dá suporte a uma configuração de servidor DHCP chamada Easy IP. A meta deste laboratório é ter dispositivos nas redes 192.168.10.0/24 e 192.168.11.0/24 solicitando endereços IP via DHCP de R2.

##### Etapa 1: Excluir endereços atribuídos estaticamente.

O servidor DHCP presume que todos os endereços IP de uma sub-rede de conjunto de endereços DHCP estejam disponíveis para serem atribuídos a clientes DHCP. Você deve especificar os endereços IP que o servidor DHCP não deve atribuir aos clientes. Esses endereços IP são endereços estáticos normalmente reservados para a interface do roteador, endereço IP de gerenciamento de switch, servidores e impressora em rede local. O comando **ip dhcp excluded-address** impede o roteador de atribuir endereços IP dentro do intervalo configurado. Os comandos a seguir excluem os primeiros 10 endereços IP de cada conjunto para as redes locais conectadas ao R1. Esses endereços não serão atribuídos a nenhum cliente DHCP.

```
R2 (config) #ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2 (config) #ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

##### Etapa 2: Configurar o conjunto.

Crie o conjunto DHCP que usa o comando **ip dhcp pool** comando e nomeie como **R1Fa0**.

```
R2 (config) #ip dhcp pool R1Fa0
```

Especifique a sub-rede a ser usada ao atribuir endereços IP. Os conjuntos DHCP são associados automaticamente a uma interface com base na instrução da rede. Agora, o roteador age como um servidor DHCP, entregando endereços na sub-rede 192.168.10.0/24, começando por 192.168.10.1.

```
R2 (dhcp-config) #network 192.168.10.0 255.255.255.0
```

Configure o roteador padrão e o servidor de nome de domínio da rede. Os clientes recebem essas configurações por DHCP, além de um endereço IP.

```
R2 (dhcp-config) #dns-server 192.168.11.5
R2 (dhcp-config) #default-router 192.168.10.1
```

Nota: não há nenhum servidor DNS em 192.168.11.5. Você está configurando o comando somente para prática.

Como dispositivos da rede 192.168.11.0/24 também solicitam endereços de R2, um conjunto separado deve ser criado para atender a dispositivos nessa rede. Os comandos são semelhantes aos comandos mostrados acima:

```
R2 (config) #ip dhcp pool R1Fa1
R2 (dhcp-config) #network 192.168.11.0 255.255.255.0
R2 (dhcp-config) #dns-server 192.168.11.5
R2 (dhcp-config) #default-router 192.168.11.1
```

##### Etapa 3: Testar DHCP

Em PC1 e PC2, teste se cada um recebeu um endereço IP automaticamente. Em cada PC, vá até **Start -> Run -> cmd -> ipconfig**



Quais são os resultados do teste? \_\_\_\_\_

Por que são esses os resultados? \_\_\_\_\_

#### Etapa 4: Configurar um endereço auxiliar.

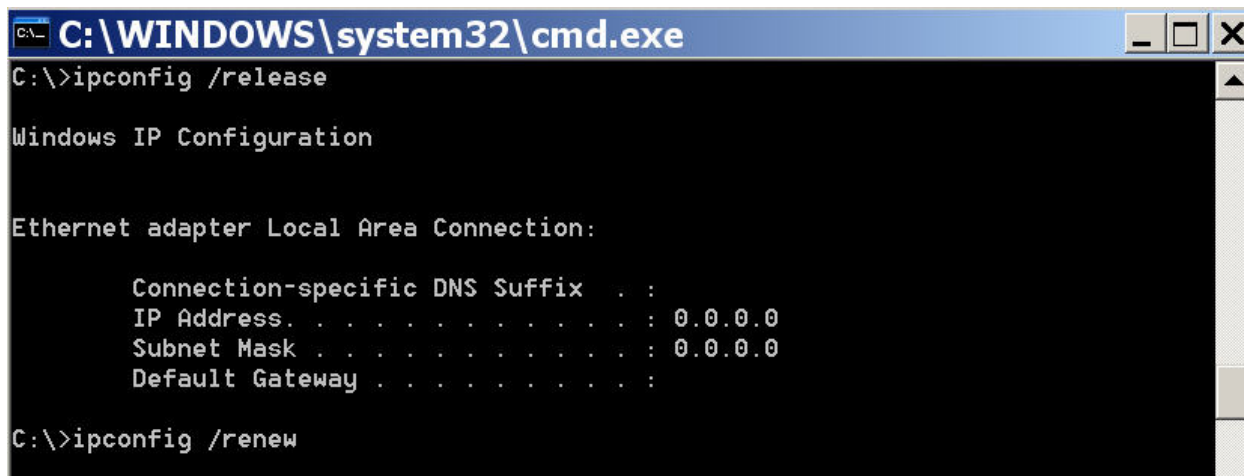
Os serviços de rede, como DHCP, dependem de broadcasts da Camada 2 para funcionar. Quando estão em uma sub-rede diferente dos clientes, os dispositivos que fornecem esses serviços não podem receber os pacotes de broadcast. Como o servidor DHCP e os clientes DHCP não estão na mesma sub-rede, configure R1 para encaminhar broadcasts DHCP para R2, que é o servidor DHCP, utilizando o comando de configuração da interface **ip helper-address**.

Observe que **ip helper-address** deve ser configurado em todas as interfaces envolvidas.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

#### Etapa 5: Liberar e renovar os endereços IP em PC1 e PC2.

Dependendo dos PCs terem sido utilizados em um laboratório diferente, ou conectado à Internet, eles talvez já tenham aprendido um endereço IP automaticamente de um servidor DHCP diferente. Precisamos limpar esse endereço IP, utilizando os comandos **ipconfig /release** e **ipconfig /renew**.



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 0.0.0.0
    Subnet Mask . . . . .             : 0.0.0.0
    Default Gateway . . . . .         : 

C:\>ipconfig /renew
```

#### Etapa 6: Verificar a configuração DHCP.

Você pode verificar a configuração do servidor DHCP de vários modos diferentes. Emita o comando **ipconfig** em PC1 e PC2 para verificar se agora eles receberam um endereço IP dinamicamente. Você pode emitir então os comandos no roteador para obter mais informações. O comando **show ip dhcp binding** fornece informações sobre todos os endereços DHCP atualmente atribuídos. Por exemplo, a saída a seguir mostra que o endereço IP 192.168.10.11 foi designado para o endereço MAC 3031.632e.3537.6563. O aluguel do IP expira no dia 14 de setembro de 2007 às 19h33.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration        Type
                Hardware address/
                User name
192.168.10.11   0063.6973.636f.2d30.  Sep 14 2007 07:33 PM    Automatic
```

```
3031.632e.3537.6563.
2e30.3634.302d.566c.
31
```

O comando **show ip dhcp pool** exibe informações sobre todas as ferramentas DHCP configuradas atualmente no roteador. Nesta saída do comando, o conjunto **R1Fa0** é configurado em R1. Um endereço foi alugado desse conjunto. O próximo cliente a solicitar um endereço receberá 192.168.10.12.

R2#**show ip dhcp pool**

```
Pool R1Fa0 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 0 / 0
  Total addresses                   : 254
  Leased addresses                  : 1
  Pending event                     : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  192.168.10.12      192.168.10.1 - 192.168.10.254  1
```

O comando **debug ip dhcp server events** pode ser extremamente útil durante a identificação e solução de problemas de aluguéis DHCP com um servidor DHCP IOS Cisco. Esta é a saída do comando de depuração em R1 após a conexão com um host. Observe que a porção realçada mostra DHCP informando ao cliente um endereço 192.168.10.12 e uma máscara 255.255.255.0

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072: DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072: DHCPD: remote id 020a0000c0a80b0101000000000000
*Sep 13 21:04:18.072: DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072: DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072: DHCPD: remote id 020a0000c0a80b0101000000000000
*Sep 13 21:04:18.072: DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072: DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072: DHCPD: remote id 020a0000c0a80a0100000000000000
*Sep 13 21:04:18.072: DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072: DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072: DHCPD: remote id 020a0000c0a80a0100000000000000
*Sep 13 21:04:18.072: DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072: DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072: DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072: DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076: DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076: DHCPD: htype 1 chaddr 001c.57ec.0640
```

\*Sep 13 21:04:20.076: DHCPD: lease time remaining (secs) = 86400

## Tarefa 5: Configurar roteamentos estático e padrão

ISP usa roteamento estático para alcançar todas as redes além de R2. No entanto, R2 traduz endereços particulares em endereços públicos antes de enviar tráfego para ISP. Portanto, o ISP deve ser configurado com os endereços públicos que fazem parte da configuração de NAT no R2. Insira a seguinte rota estática em ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Esta rota estática inclui todos os endereços atribuídos ao R2 para uso público.

Configure uma rota padrão em R2 e propague a rota em OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

```
R2(config)#router ospf 1
```

```
R2(config-router)#default-information originate
```

Aguarde alguns segundos até que R1 aprenda a rota padrão de R2 e, em seguida, verifique a tabela de roteamento R1. Você pode limpar a tabela de roteamento com o comando **clear ip route \***. Uma rota padrão apontando para R2 deve ser exibida na tabela de roteamento R1. Observe que a rota estática configurada no ISP só roteia para os endereços públicos que os hosts de R1 utilizarão depois que o NAT for configurada em R2. Até o NAT ser configurada, a rota estática levará a uma rede desconhecida, causando falha nos pings de R1.

## Tarefa 6: Configurar NAT estático

### Etapa 1: Mapear estaticamente um endereço IP público para um endereço IP privado.

O servidor interno conectado ao R2 pode ser acessado através de hosts externos além do ISP. Atribua estaticamente o endereço IP público 209.165.200.254 como o endereço NAT a ser usado para mapear pacotes para o endereço IP privado do servidor interior em 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

### Etapa 2: Especificar interfaces NAT internas e externas.

Para que o NAT possa funcionar, você deve especificar quais interfaces estão dentro e quais estão fora.

```
R2(config)#interface serial 0/0/1
```

```
R2(config-if)#ip nat outside
```

```
R2(config-if)#interface fa0/0
```

```
R2(config-if)#ip nat inside
```

Nota: se estiver utilizando um servidor interno simulado, atribua o comando **ip nat inside** à interface de loopback.

### Etapa 3: Verificar a configuração NAT estático.

Em ISP, execute ping no endereço IP público 209.165.200.254.

## Tarefa 7: Configurar NAT dinâmica com um conjunto de endereços

Embora o NAT estático forneça um mapeamento permanente entre um endereço interno e um endereço público específico, o NAT dinâmico mapeia endereços IP privados para endereços públicos. Esses endereços IP públicos vêm de um conjunto de NAT.



### Etapa 1: Definir um conjunto de endereços globais.

Crie um conjunto de endereços para os quais os endereços de origem correspondentes são traduzidos. O comando a seguir cria um conjunto chamado MY-NAT-POOL que traduz endereços comparados em um endereço IP disponível no intervalo 209.165.200.241 a 209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
```

### Etapa 2: Criar uma lista de controle de acesso estendida para identificar quais endereços são traduzidos.

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

### Etapa 3: Estabelecer tradução da origem dinâmica, vinculando o conjunto à lista de controle de acesso.

Um roteador pode ter mais de um conjunto NAT e mais de uma ACL. O comando a seguir informa ao roteador qual conjunto de endereços ele deverá usar para traduzir os hosts permitidos pela ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

### Etapa 4: Especificar interfaces NAT internas e externas.

Você já especificou as interfaces interna e externa para sua configuração de NAT estático. Agora adicione a interface serial vinculada a R1 como uma interface interior.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

### Etapa 5: Verificar a configuração.

Ping ISP entre PC1 ou a interface Fast Ethernet em R1 usando **ping** estendido. Em seguida, use os comandos **show ip nat translations** e **show ip nat statistics** no R2 para verificar o NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local           Outside local          Outside global
icmp 209.165.200.241:4  192.168.10.1:4         209.165.200.226:4     209.165.200.226:4
--- 209.165.200.241    192.168.10.1          ---                   ---
--- 209.165.200.254    192.168.20.254        ---                   ---
```

```
R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23 Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
  [Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
  pool MY-NAT-POOL: netmask 255.255.255.248
    start 209.165.200.241 end 209.165.200.246
    type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```



Para identificar e solucionar problemas com NAT, você pode utilizar o comando **debug ip nat**. Ative a depuração NAT e repita o ping de PC1.

```
R2#debug ip nat
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

## Tarefa 8: Configurar sobrecarga NAT

No exemplo anterior, o que aconteceria se você precisasse de mais que os seis endereços IP públicos que o conjunto permite?

Como os números de porta são monitorados, a sobrecarga NAT permite a vários usuários internos reutilizarem um endereço IP público.

Nesta tarefa, você irá remover o conjunto e a instrução de mapeamento configurada na tarefa anterior. Em seguida, você configurará a sobrecarga de NAT no R2 para que todos os endereços IP internos sejam traduzidos para o endereço R2 S0/0/1 ao conectarem-se a qualquer dispositivo de origem externa.

### Etapa 1: Remover o conjunto NAT e a instrução de mapeamento.

Use os comandos a seguir para remover o conjunto de NAT e o mapa para a ACL de NAT.

```
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Se você receber a mensagem a seguir, limpe as suas traduções NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

### Etapa 2: Configurar PAT em R2 utilizando o endereço IP público de interface 0/0/1 serial.

A configuração é semelhante ao NAT dinâmico. A diferença é que, em vez de um conjunto de endereços, a palavra-chave **interface** é usada para identificar o endereço IP externo. Portanto, nenhum conjunto de NAT foi definido. A palavra-chave **overload** permite adicionar o número da porta à tradução.

Como já configurou uma ACL para identificar quais endereços IP devem ser traduzidos, bem como quais interfaces estão dentro e fora, você só precisa configurar o seguinte:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

### Etapa 3: Verificar a configuração.

Ping ISP entre PC1 ou a interface Fast Ethernet em R1 usando **ping** estendido. Em seguida, use os comandos **show ip nat translations** e **show ip nat statistics** no R2 para verificar o NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6   209.165.200.226:6 209.165.200.226:6
--- 209.165.200.254    192.168.20.254   ---                ---
```

```
R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48 Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
  [Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

Nota: na tarefa anterior, você poderia ter adicionado a palavra-chave **overload** ao comando **ip nat inside source list NAT pool MY-NAT-POOL** para permitir mais de seis usuários simultâneos.

### Tarefa 9: Documentar a rede

Em cada roteador, emita o comando **show run** e capture as configurações.

```
R1#show run
<saída do comando omitida>
!
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
ip helper-address 10.1.1.2
no shutdown
!
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip helper-address 10.1.1.2
no shutdown
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 125000
!
interface Serial0/0/1
no ip address
shutdown
```

```
!  
router ospf 1  
 network 10.1.1.0 0.0.0.3 area 0  
 network 192.168.10.0 0.0.0.255 area 0  
 network 192.168.11.0 0.0.0.255 area 0  
!  
!  
banner motd ^C  
*****  
!!!AUTHORIZED ACCESS ONLY!!!  
*****  
^C  
!  
line con 0  
 exec-timeout 0 0  
 password cisco  
 logging synchronous  
 login  
line aux 0  
 exec-timeout 0 0  
 password cisco  
 logging synchronous  
 login  
line vty 0 4  
 exec-timeout 0 0  
 password cisco  
 logging synchronous  
 login  
!  
end  
  
R2#show run  
!  
hostname R2  
!  
!  
enable secret class  
!  
no ip dhcp use vrf connected  
ip dhcp excluded-address 192.168.10.1 192.168.10.10  
ip dhcp excluded-address 192.168.11.1 192.168.11.10  
!  
ip dhcp pool R1Fa0  
 network 192.168.10.0 255.255.255.0  
 default-router 192.168.10.1  
 dns-server 192.168.11.5  
!  
ip dhcp pool R1Fa1  
 network 192.168.11.0 255.255.255.0  
 dns-server 192.168.11.5  
 default-router 192.168.11.1  
!  
no ip domain lookup  
!  
interface Loopback0  
 ip address 192.168.20.254 255.255.255.0
```

```
ip nat inside
ip virtual-reassembly
!
!
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
ip nat inside
ip virtual-reassembly
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
ip nat outside
ip virtual-reassembly
clock rate 125000
!
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
network 192.168.20.0 0.0.0.255 area 0
default-information originate
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Serial0/0/1 overload
ip nat inside source static 192.168.20.254 209.165.200.254
!
ip access-list extended NAT
permit ip 192.168.10.0 0.0.0.255 any
permit ip 192.168.11.0 0.0.0.255 any
!
!
banner motd ^C
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
^C
!
line con 0
exec-timeout 0 0
password cisco
logging synchronous
login
line aux 0
exec-timeout 0 0
password cisco
logging synchronous
login
line vty 0 4
exec-timeout 0 0
password cisco
logging synchronous
login
!
```

end

```
ISP#show run
<saída de comando omitida>
!
hostname ISP
!
enable secret class
!
no ip domain lookup
!
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shutdown
!
!
!
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
banner motd ^C
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

## Tarefa 10: Limpar

Apague as configurações e recarregue os roteadores. Desconecte e guarde o cabeamento. Para PCs normalmente conectados a outras redes, como a LAN escolar ou a Internet), reconecte o cabeamento apropriado e restaure as configurações TCP/IP.