Atividade PT 7.4.1: Configuração básica DHCP e NAT

Diagrama de topologia

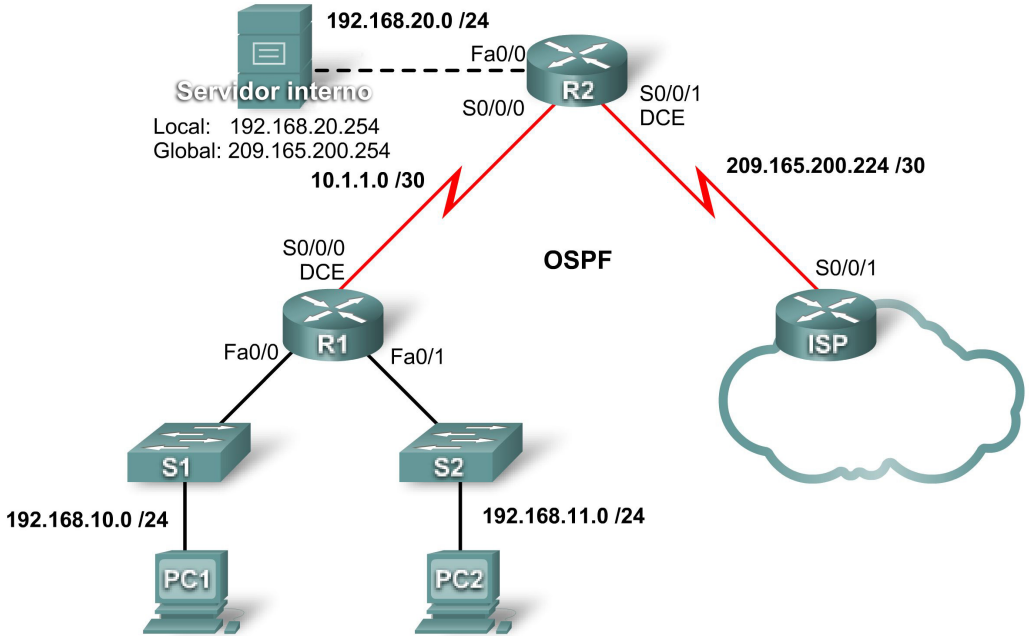

Tabela de endereçamento

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:

- Preparar a rede.
- Executar as configurações básicas de roteador.
- Configurar um servidor DHCP do Cisco IOS.
- Configurar roteamentos estático e padrão
- Configurar a NAT estática.

- Configurar NAT dinâmica usando um conjunto de endereços.
- Configurar 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: Executar configurações básicas do roteador

Etapa 1: Configurar os roteadores.

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 através DHCP posteriormente na atividade.
- Habilite o OSPF com o ID de processo 1 em R1 e R2. Não anuncie a rede 209.165.200.224/27.

Etapa 2. Verifique os resultados.

O percentual de conclusão deve ser 58%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar um servidor DHCP no IOS Cisco

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.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Etapa 2: Configurar o pool.

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

```
R1(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.


```
R1(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.

```
R1(dhcp-config)#dns-server 192.168.11.5
R1(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.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

Etapa 3: Verificar a configuração DHCP.

Você pode verificar a configuração do servidor DHCP de vários modos diferentes. A maneira mais básica é configurar um host na sub-rede para receber um endereço IP via DHCP. 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
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA – Automatic
```

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 75%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurar roteamentos estático e padrão

Etapa 1. Configurar rotas estática 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. Em R1, execute ping na interface serial 0/0/1 em R2 (209.165.200.225). Os pings devem ter êxito. Solucionar problemas se os pings falharem.

Etapa 2. Verifique os resultados.

O percentual de conclusão deve ser 83%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: 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 a 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
```

Etapa 3: Verificar a configuração NAT estático.

Em ISP, execute ping no endereço IP público 209.165.200.254.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 92%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 5: 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 que coincidirem com a ACL 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 padrão para identificar quais endereços serão traduzidos.

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

Etapa 3: Estabelecer tradução da origem dinâmica, vinculando o pool 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 e PC2. Em seguida, use o comando **show ip nat translations** no R2 para verificar o NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.241   192.168.10.11      ---                ---
---  209.165.200.242   192.168.11.11      ---                ---
---  209.165.200.254   192.168.20.254     ---                ---
```

Etapa 6. Verifique os resultados.

O percentual de conclusão deve ser 97%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 6: 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 pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

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 e PC2. Em seguida, use o comando **show ip nat translations** no R2 para verificar o NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.11:3    209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024192.168.11.11:3    209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                ---
```

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.

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 100%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

