Atividade PT 7.2.8: Dimensionando redes com NAT

Diagrama de topologia

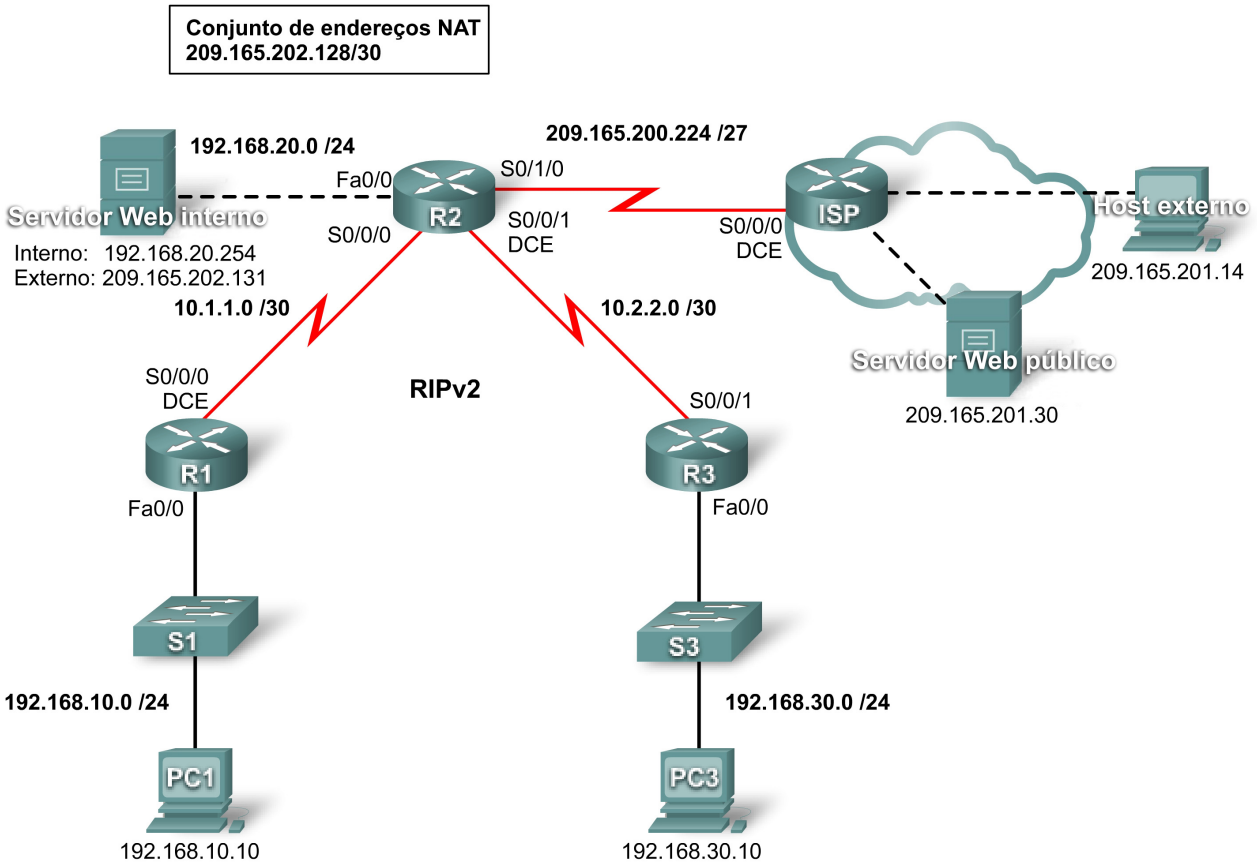

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
R1	**Fa0/0**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**Fa0/0**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/0**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252

Continuação da tabela de endereçamento na próxima página

Continuação da tabela de endereçamento

Servidor Web interno	**Placa de rede**	Local: 192.168.20.254	255.255.255.252
	Placa de rede	Global: 209.165.202.131	255.255.255.252
PC1	**Placa de rede**	192.168.10.10	255.255.255.0
PC3	**Placa de rede**	192.168.30.10	255.255.255.0
Host externo	**Placa de rede**	209.165.201.14	255.255.255.240
Servidor Web público	**Placa de rede**	209.265.201.30	255.255.255.240

Objetivos de aprendizagem

- Configure uma ACL para permitir NAT.
- Configure a NAT estática.
- Configure sobrecarga NAT dinâmica.
- Configure o roteador ISP usando uma rota estática.
- Testar conectividade.

Introdução

A NAT traduz endereços privados, não roteáveis e internos em endereços públicos, roteáveis. A NAT tem um benefício adicional de proporcionar um nível de privacidade e segurança para uma rede porque ela oculta endereços IP internos de redes externas. Nesta atividade, você irá configurar o NAT dinâmico e estático. A senha no modo EXEC do usuário é **cisco** e a senha no modo EXEC privilegiado é **class**.

Tarefa 1: Configurar uma ACL para permitir NAT

Etapa 1. Criar uma ACL padrão nomeada.

Para definir os endereços internos que são traduzidos para endereços públicos no processo de NAT, crie uma ACL de nomenclatura padrão chamada R2NAT. Esta lista é usada nas etapas da configuração NAT a seguir.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

Etapa 2. Verifique os resultados.

O percentual de conclusão deve ser 11%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurar NAT estático

Etapa 1. Configurar NAT estático para um servidor Web interno.

O servidor Web interno precisa ter um endereço IP público que jamais seja alterado para que possa ser acessado fora da rede. Configurar um endereço NAT estático permite ao servidor Web ser configurado com um endereço interno privado. Em seguida, o processo NAT sempre mapeia pacotes utilizando o endereço público do servidor para o endereço privado.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```


Etapa 2. Verifique os resultados.

O percentual de conclusão deve ser 22%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurar sobrecarga NAT dinâmica

Além do endereço IP público atribuído ao servidor Web interno, o ISP atribuiu três endereços públicos para utilização. Esses endereços são mapeados para todos os outros hosts internos que acessam a Internet.

Para permitir a mais de três hosts internos acessar a Internet ao mesmo tempo, configure NAT com sobrecarga (overload) para acomodar os hosts adicionais. A sobrecarga NAT, também chamada de Tradução de Endereço de Porta (PAT – Port Address Translation), utiliza números de porta para distinguir pacotes de hosts diferentes atribuídos ao mesmo endereço IP público.

Etapa 1. Definir o conjunto de endereços e configurar NAT dinâmico.

Digite os comandos a seguir para configurar o conjunto de endereços públicos mapeados dinamicamente para os hosts internos.

O primeiro comando define o conjunto de três endereços públicos mapeados para endereços internos.

O segundo comando instrui o processo NAT a mapear os endereços no conjunto para os endereços definidos na lista de acesso criada na Tarefa 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask
255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

Etapa 2. Configurar as interfaces em R2 para aplicar NAT.

No modo de configuração da interface em R2, configure todas as interfaces utilizando o comando **ip nat** {**inside** | **outside**}. Como os endereços internos estão em redes conectadas às interfaces Fa0/0, Serial 0/0/0 e Serial0/0/1, utilize o comando **ip nat inside** na configuração dessas interfaces. Como a Internet é conectada a Serial0/1/0, utilize o comando **ip nat outside** nessa interface.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 89%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Configurar o ISP com uma rota estática

Etapa 1. Configurar ISP com uma rota estática para R2.

ISP precisa de uma rota estática para os endereços públicos de R2. Use o comando a seguir para configurar essa rota.

```
ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

Etapa 2. 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.

Tarefa 5: Testar conectividade

Você deve poder agora executar ping de qualquer host interno para host externo ou servidor Web público.

Para ver os efeitos de NAT em um pacote específico, entre no modo Simulação e observe o pacote com origem em PC1.

Clique na caixa de informações colorida associada ao pacote passado de R1 para R2. Clicando em **Inbound PDU Details**, você deve ver que o endereço de origem é 192.168.10.10. Clicando em **Outbound PDU Details**, você deve ver que o endereço de origem foi traduzido como um endereço 209.165.x.x.

