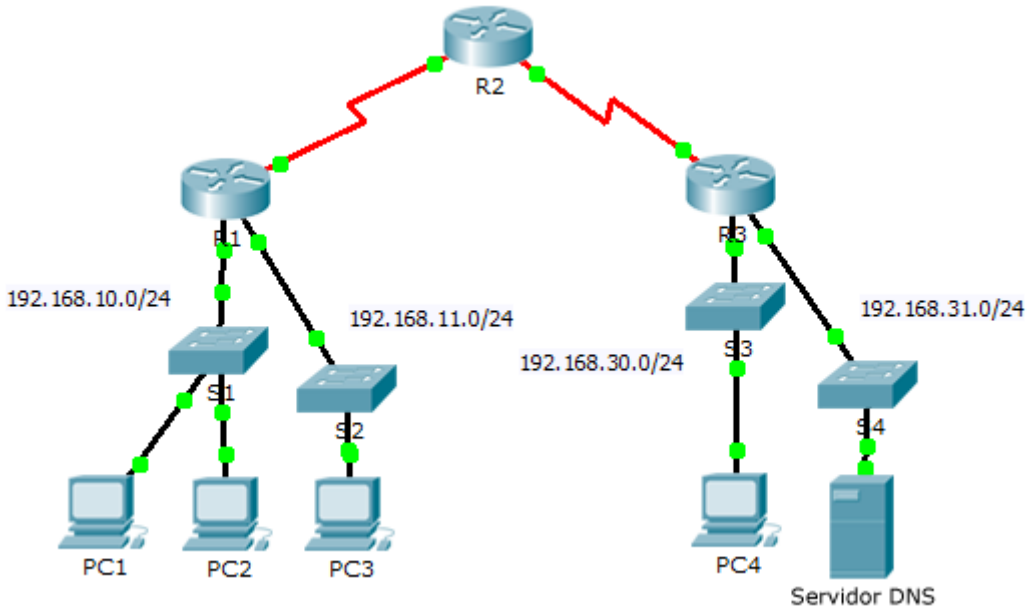
Packet Tracer – Demonstração de lista de controle de acesso

Topologia



Objetivos

Parte 1: Verificar a conectividade local e testar a lista de controle de acesso

Parte 2: Remover a lista de controle de acesso e repetir o teste

Histórico

Nesta atividade, você observará como uma lista de controle de acesso (ACL) pode ser usada para impedir que um ping alcance hosts em redes remotas. Após remover a ACL da configuração, os pings terão êxito.

Parte 1: Verificar a conectividade local e testar a lista de controle de acesso

Etapa 1: Execute o ping nos dispositivos na rede local para verificar a conectividade.

a. Do prompt de comando de **PC1**, execute ping para **PC2**.

b. Do prompt de comando de **PC1**, execute ping para **PC3**.

Os pings tiveram êxito?

PC1 para PC2 - 4 --- PC1 para PC3 - 4

Etapa 2: Execute o ping nos dispositivos em redes remotas para testar a funcionalidade da ACL.

a. Do prompt de comando de **PC1**, execute ping para **PC4**.

b. Do prompt de comando de **PC1**, execute ping para **Servidor DNS**.

Por que o ping falhou? (Dica: use o modo de simulação ou visualize as configurações do roteador para investigar.)

Reply from 192.168.10.1: Destination host unreachable.

Parte 2: Remover a ACL e repetir o teste

Etapa 1: Use comandos show para investigar a configuração de ACL.

a. Use os comandos **show run** e **show access-lists** para exibir as ACLs configuradas atualmente. Para ver rapidamente as ACLs atuais, use **show access-lists**. Insira o comando **show access-lists**, seguido por um espaço e um ponto de interrogação (?) para exibir as opções disponíveis:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Se você souber o número ou o nome da ACL, poderá filtrar ainda mais a saída de **show**. No entanto, **R1** tem somente uma ACL; portanto, o comando **show access-lists** será suficiente.

```
R1# show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

A primeira linha de ACL impede pacotes oriundos da rede **192.168.10.0/24**, que inclui Internet Control Message Protocol (ICMP) echoes (solicitações de ping). A segunda linha da ACL permite todo o tráfego ip restante de qualquer origem para atravessar o roteador.

b. Para uma ACL afetar a operação do roteador, ela deve ser aplicada a uma interface em uma direção específica. Neste cenário, a ACL é usada para filtrar o tráfego em uma interface. Portanto, todo o tráfego saindo da interface de R1 especificada será inspecionado contra ACL 11.

Embora você possa visualizar as informações de IP com o comando **show ip interface**, pode ser mais eficiente em algumas situações, simplesmente usar o comando **show run**.

Usando um ou ambos os comandos, a que interface é aplicada a ACL?

interface Serial0/0/0

Etapa 2: Remova a lista de acesso 11 da configuração.

Você pode remover as ACLs da configuração executando o comando **no access-list** [*number of the ACL*]. O comando **no access-list** exclui todas as ACLs configuradas no roteador. O comando **no access-list** [*number of the ACL*] remove apenas uma ACL específica.

a. Na interface Serial 0/0/0, remova o access-list 11 previamente aplicado à interface como um filtro de **saída**:

```
R1(config)# int se0/0/0
R1(config-if)#no ip access-group 11 out
```

b. No modo de configuração global, remova a ACL inserindo o seguinte comando:

```
R1(config)# no access-list 11
```

c. Verifique se **PC1** agora pode executar ping do **Servidor DNS** e **PC4**.

Rubrica de pontuação sugerida

Etapa da pergunta	Pontos Possíveis	Pontos Obtidos
Parte 1, Etapa 1 b.	50	
Parte 1, Etapa 2 b.	40	
Parte 2, Etapa 2 b.	10	
Pontuação total	**100**	

