Atividade PT 5.5.1: Listas de controle de acesso básico

Diagrama de topologia

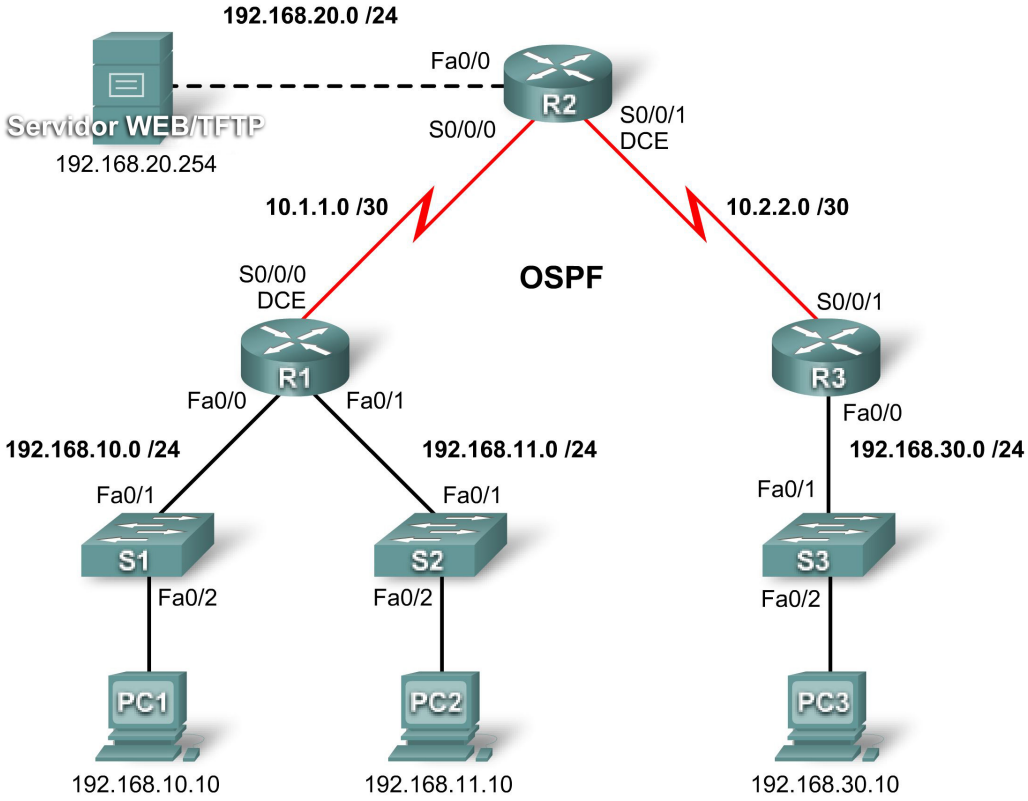

Tabela de endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede	Gateway padrão
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	**Fa0/0**	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	**Fa0/0**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A

Tabela de endereçamento na próxima página

Continuação da tabela de endereçamento

S1	**VLAN 1**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**VLAN 1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**VLAN 1**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**Placa de rede**	192.168.10.10	255.255.255.0	192.168.10.1
PC2	**Placa de rede**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**Placa de rede**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor Web	**Placa de rede**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizagem

- Execute configurações básicas de roteador e de switch.
- Configure uma ACL padrão.
- Configure um tronco estendido.
- Controle o acesso às linhas vty usando uma ACL padrão.
- Solucionar problemas das ACLs.

Introdução

Nesta atividade, você irá criar, aplicar, testar e solucionar problemas nas configurações da lista de acesso.

Tarefa 1: Executar configurações de roteador e de switch básicas

Etapa 1. Configurar os roteadores e os switches.

Configure os roteadores R1, R2, R3, S1, S2 e S3 e os switches de acordo com as seguintes diretrizes:

- Configure nomes de host para corresponder ao diagrama de topologia.
- Desabilite a pesquisa DNS.
- Configure uma senha criptografada **class** em EXEC privilegiado.
- Configure um **banner de mensagem do dia**.
- Configure uma senha **cisco** para as conexões de console.
- Configure uma senha **cisco** para as conexões vty.
- Configure endereços IP e máscaras em todos os dispositivos. Defina o clock rate como **64000**.
- Habilite o OSPF usando o ID de processo 1 em todos os roteadores de todas as redes.
- Configurar uma interface de loopback em R2.
- Configure endereços IP para a interface VLAN 1 em cada switch.
- Configure cada switch usando o gateway padrão apropriado.
- Verificar a conectividade completa do IP usando o comando **ping**.

Etapa 2. Configurar os PCs e o servidor Web/TFTP.

- Utilizando a tabela de endereçamento e o diagrama, configure endereços IP, máscaras de sub-rede e gateways padrão para cada PC por meio da guia **Desktop** > **IP Configuration**.
- Configure o endereço IP, a máscara de sub-rede e o gateway padrão do servidor WEB/TFTP.

Etapa 3. Verifique os resultados.

O percentual de conclusão deve ser 93%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 2: Configurando uma ACL padrão

As ACLs padrão só podem filtrar tráfego com base no endereço IP de origem. Nesta tarefa, você está configurando uma ACL padrão que bloqueia tráfego da rede 192.168.11.0 /24. Esta ACL será aplicada à interface serial do R3. Lembre-se de que toda ACL tem um "deny all" implícito que faz com que todo o tráfego não correspondente a uma instrução na ACL seja bloqueado. Por isso, adicione a instrução **permit any** ao final da ACL.

Etapa 1. Criar a ACL.

No modo de configuração global, crie uma ACL nomeada padrão chamada **std-1**.

```
R3(config)#ip access-list standard std-1
```

No modo de configuração ACL padrão, adicione uma instrução que nega qualquer pacote com um endereço de origem 192.168.11.0/24 e imprime uma mensagem na console de cada pacote correspondido.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255
```

Permita todos os demais tráfegos.

```
R3(config-std-nacl)#permit any
```

Etapa 2. Aplique a ACL.

Aplique a ACL std-1 como um filtro em pacotes que entram em R3 pela interface serial 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group std-1 in
```

Etapa 3. Testar a ACL.

Testar a ACL executando ping do PC2 para o PC3. Como a ACL foi projetada para bloquear tráfego com endereços de origem da rede 192.168.11.0/24, PC2 (192.168.11.10) não deve ser capaz de executar ping em PC3.

No modo EXEC privilegiado em R3, emita o comando **show access-lists**. Você vê a saída de dados semelhante ao seguinte. Cada linha de uma ACL tem um contador associado que mostra quantos pacotes corresponderam à regra.

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 95%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 3: Configurando uma ACL estendida

Quando for exigida uma maior granularidade, você deve utilizar uma ACL estendida. As ACLs estendidas podem filtrar o tráfego com base em mais de um endereço de origem. As ACLs estendidas podem filtrar o protocolo, os endereços IP de origem e de destino, além dos números de porta de origem e de destino.

Uma política adicional desta rede informa que apenas dispositivos da LAN 192.168.10.0/24 têm permissão para alcançar redes internas. Os computadores nesta LAN não podem acessar a Internet.

Portanto, o acesso desses usuários ao endereço IP 209.165.200.225 deve ser bloqueado. Como este requisito precisa ser aplicado na origem e no destino, uma ACL estendida é obrigatória.

Nesta tarefa, você está configurando uma ACL estendida em R1 que impede tráfego com origem em qualquer dispositivo na rede 192.168.10.0/24 de acessar o host 209.165.200.255. Esta ACL será aplicada à saída da interface serial 0/0/0 do R1.

Etapa 1. Configurar uma ACL estendida nomeada.

No modo de configuração global, crie uma ACL estendida padrão chamada **extend-1**.

```
R1(config)#ip access-list extended extend-1
```

Observe que o prompt do roteador é alterado para indicar que agora você está no modo de configuração ACL estendido. Nesse prompt, adicione as instruções necessárias para bloquear o tráfego da rede 192.168.10.0/24 para o host. Use a palavra-chave **host** ao definir o destino.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Lembre-se de que "deny all" implícito bloqueia todos os demais tráfegos sem a instrução **permit** adicional. Adicione a instrução **permit** para garantir que outro tráfego não esteja bloqueado.

```
R1(config-ext-nacl)#permit ip any any
```

Etapa 2. Aplique a ACL.

Com ACLs padrão, a prática recomendada é colocar a ACL o mais perto possível do destino. As ACLs estendidas costumam ser colocadas próximas da origem. A ACL **extend-1** será colocada na interface Serial e filtrará o tráfego de saída

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group extend-1 out
```

Etapa 3. Testar a ACL.

Em PC1 ou qualquer outro dispositivo na rede 192.168.10.0 /24, execute ping na interface de loopback em R2. Deve haver falha nesses pings, pois todo o tráfego da rede 192.168.10.0/24 será filtrado quando o destino for 209.165.200.225. Se o destino for qualquer outro endereço, os pings devem ter êxito. Confirme isso, executando ping em R3 no dispositivo de rede 192.168.10.0/24.

Você pode ainda verificar isto emitindo o comando **show ip access-list** em R1 depois de executar ping.

Você deve ter correspondências para ambas as regras da ACL. Isso porque o ping de PC1 na interface de loopback de R2 foi negado, e o ping em R3 foi permitido.

```
R1#show ip access-list
Lista estendida de acesso IP extend-1
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))
    permit ip any any (4 match(es))
```

Etapa 4. Verifique os resultados.

O percentual de conclusão deve ser 99%. Do contrário, clique em **Check Results** para ver a necessidade de componentes ainda não concluídos.

Tarefa 4: Controlar acesso às linhas vty com uma ACL padrão

É uma prática recomendada restringir o acesso a linhas vty do roteador à administração remota. Uma ACL pode ser se aplicada às linhas vty, o que permite restringir acesso a hosts específicos ou redes. Nesta tarefa, você irá configurar uma ACL padrão para permitir que hosts de duas redes acessem as linhas vty. Todos os demais hosts são negados.

Verifique se você pode enviar um telnet ao R2 do R1 e do R3.

Etapa 1. Configurar os ACL

Configure uma ACL padrão nomeada em R2 que permita tráfego entre 10.2.2.0/30 e 192.168.30.0/24. Negue todos os demais tráfegos. Chame a ACL **Task-4**.

```
R2(config)#ip access-list standard Task-4
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Etapa 2. Aplique a ACL.

Acesse o modo de configuração de linha para o acesso vty.

```
R2(config)#line vty 0 15
```

Use o comando **access-class** para aplicar a ACL às linhas vty na direção de entrada. Observe que ele é diferente do comando que costumava aplicar ACLs a outras interfaces.

```
R2(config-line)#access-class Task-4 in
```

Etapa 3. Testar a ACL.

Telnet de R1 para R2. Observe que R1 não tem endereços IP no intervalo de endereços listado nas instruções de permissão ACL da Tarefa 4. Deve haver falha nas tentativas de conexão.

Em R3, execute telnet em R2 ou em qualquer dispositivo na rede 192.168.30.0 /24. Será apresentado a você um prompt para a senha de linha vty.

Por que as tentativas de conexão de outras redes falham mesmo não estando especificamente listadas na ACL?

_____

_____

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.

Tarefa 5: Identificação e solução de problemas de ACLs

Quando uma ACL é configurada ou aplicada de modo inadequado para a interface errada ou na direção errada, o tráfego da rede pode ser afetado de uma maneira indesejável.

Etapa 1. Testar a ACL.

Em uma tarefa anterior, você criou e aplicou uma ACL padrão nomeada em R3. Use o comando **show running-config** para exibir a ACL e sua localização. Você deve ver que uma ACL chamada **std-1** foi configurada e aplicada na entrada da Serial 0/0/1. Lembre-se de que essa ACL foi criada para impedir todo o tráfego da rede com um endereço de origem da rede 192.168.11.0/24 de acessar a rede local em R3.

Para remover a ACL, vá para o modo de configuração da interface serial 0/0/1 no R3.

```
R3(config)#interface serial 0/0/1
```


Utilize o comando **no ip access-group std-1 in** para remover a ACL da interface.

```
R3(config-if)#no ip access-group std-1 in
```

Utilize o comando **show running-config** para confirmar se a ACL foi removida da Serial 0/0/1

Etapa 2. Aplicar ACL std-1 em S0/0/1 de saída.

Para testar a importância do sentido da filtragem ACL, reaplique a ACL **std-1** à interface Serial 0/0/1. Desta vez, a ACL filtrará o tráfego de saída em vez do tráfego de entrada. Lembre-se de usar a palavra-chave **out** ao aplicar a ACL.

```
R3(config-if)#ip access-group std-1 out
```

Etapa 3. Testar a ACL.

Testar a ACL executando ping do PC2 para o PC3. Como alternativa, use um ping estendido em R1. Observe que ping é executado com êxito desta vez e os contadores ACL não são incrementados. Confirme-a, emitindo o comando **show ip access-list** em R3.

Etapa 4. Restaurar a configuração original da ACL.

Remova a ACL da direção de saída e reaplique-a na direção de entrada.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group std-1 out
R3(config-if)#ip access-group std-1 in
```

Etapa 5. Aplicar a Tarefa 4 à interface de entrada R2 serial 0/0/0.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

Etapa 6. Testar a ACL.

Tente se comunicar com qualquer dispositivo conectado a R2 ou R3 de R1 ou redes conectadas. Observe que toda a comunicação é bloqueada; no entanto, os contadores ACL não são incrementados. Isso ocorre por causa do "negar tudo" implícito no final de cada ACL.

Você deve ver mensagens semelhantes às seguintes impressas nas consoles de R1 e R2 depois que os dead timers do OSPF expirem:

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Remova a ACL da Tarefa 4 da interface.

