Packet Tracer - Configuração da segurança de switch (Versão do Instrutor)

**Nota do Instrutor**: Cor vermelha da fonte ou realces em cinza indicam o texto que aparece apenas na cópia do instrutor.

# Tabela VLAN

| Switch | Número da VLAN | Nome da VLAN | Associação à Porta | Captura de dados |
| --- | --- | --- | --- | --- |
| SW-1 | 10 | Admin. | F0/1, F0/2 | 192.168.10.0/24 |
| SW-1 | 20 | Vendas | F0/10 | 192.168.20.0/24 |
| SW-1 | 99 | Gerenciamento | F0/24 | 192.168.99.0/24 |
| SW-1 | 100 | Nativo | G0/1, G0/2 | Nenhum |
| SW-1 | 999 | BlackHole | All unused | Nenhum |
| SW-2 | 10 | Admin. | F0/1, F0/22 | 192.168.10.0/24 |
| SW-2 | 20 | Vendas | F0/10 | 192.168.20.0/24 |
| SW-2 | 99 | Gerenciamento | F0/24 | 192.168.99.0/24 |
| SW-2 | 100 | Nativo | Nenhum | Nenhum |
| SW-2 | 999 | BlackHole | All unused | Nenhum |

# Objetivos

Parte 1: Criar um tronco seguro

Parte 2: Switchports não utilizados seguros

Parte 3: Implementar a segurança da porta

Parte 4: Habilitar a espionagem DHCP

Parte 5: Configurar o Rapid PVST PortFast e o BPDU Guard

# Background

Você está aprimorando a segurança em dois comutadores de acesso em uma rede parcialmente configurada. Você implementará a gama de medidas de segurança que foram abordadas neste módulo de acordo com os requisitos abaixo. Observe que roteamento foi configurado nesta rede, portanto, a conectividade entre hosts em VLANs diferentes devem funcionar quando concluídas.

# Instruções

## Criar um tronco seguro

* + - 1. Conecte as portas G0 / 2 dos dois switches da camada de acesso.
      2. Configure as portas G0/1 e G0/2 como troncos estáticos nos dois switches.
      3. Desative a negociação de DTP nos dois lados do link.
      4. Crie a VLAN 100 e atribua a ela o nome Native nos dois switches.
      5. Configure todas as portas de tronco nos dois switches para usar a VLAN 100 como VLAN nativa.

## Proteja Switchports não utilizados.

* + - 1. Encerre todas as portas de switch não utilizadas no SW-1.
      2. No SW-1, crie uma VLAN 999 e chame-a de BlackHole. O nome configurado deve corresponder exatamente ao requisito.
      3. Mova todas as portas de switch não utilizadas para a VLAN do BlackHole.

## Implementar a segurança de porta

* + - 1. Ative a segurança da porta em todas as portas de acesso ativas no switch SW-1.
      2. Configure as portas ativas para permitir que um máximo de 4 endereços MAC sejam aprendidos nas portas.
      3. Para as portas F0 / 1 no SW-1, configure estaticamente o endereço MAC do PC usando a segurança da porta.
      4. Configure cada porta de acesso ativa para adicionar automaticamente os endereços MAC aprendidos na porta à configuração em execução.
      5. Configure o modo de violação de segurança da porta para descartar pacotes de endereços MAC que excedam o máximo, gerar uma entrada Syslog, mas não desativar as portas.

## Configurar o Espionagem de DHCP

* + - 1. Configure as portas de trunk no SW-1 como portas confiáveis.
      2. Limite as portas não confiáveis no SW-1 a cinco pacotes DHCP por segundo.
      3. No SW-2, ative a espionagem de DHCP globalmente e para as VLANs 10, 20 e 99.

**Nota:** A configuração de Espionagem do DHCP pode não ser pontuada corretamente no Packet Tracer.

## Configurar portfast e bpdu guard.

* + - 1. Ative o PortFast em todas as portas de acesso que estão em uso no SW-1.
      2. Ative o BPDU Guard em todas as portas de acesso que estão em uso no SW-1.
      3. Configure o SW-2 para que todas as portas de acesso usem o PortFast por padrão.

Fim do documento

# Configurações SW1

enable

configure terminal

spanning-tree portfast default

interface FastEthernet0/1

ip dhcp snooping limit rate 5

switchport mode access

switchport port-security

switchport port-security maximum 4

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security mac-address 0010.11E8.3CBB

spanning-tree portfast

spanning-tree bpduguard enable

!

interface range FastEthernet0/2, FastEthernet0/10,FastEthernet0/24

ip dhcp snooping limit rate 5

switchport mode access

switchport port-security

switchport port-security maximum 4

switchport port-security mac-address sticky

switchport port-security violation restrict

spanning-tree portfast

spanning-tree bpduguard enable

!

interface range FastEthernet0/3 – 9, FastEthernet0/11 - 23

switchport access vlan 999

shutdown

!

interface range GigabitEthernet0/1 - 2

switchport trunk native vlan 100

ip dhcp snooping trust

switchport mode trunk

switchport nonegotiate

vlan 100

name Native

vlan 999

name BlackHole

# Configuração SW-2

enable

configure terminal

ip dhcp snooping

ip dhcp snooping vlan 10,20,99

spanning-tree portfast default

interface GigabitEthernet0/1

switchport trunk native vlan 100

switchport mode trunk

switchport nonegotiate

!

interface GigabitEthernet0/2

switchport trunk native vlan 100

switchport mode trunk

switchport nonegotiate