Packet Tracer - Implementar Segurança de Porta (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 de Endereçamento

| Dispositivo | Interface | Endereço IP | Máscara de sub-rede |
| --- | --- | --- | --- |
| S1 | VLAN 1 | 10.10.10.2 | 255.255.255.0 |
| PC1 | NIC | 10.10.10.10 | 255.255.255.0 |
| PC2 | NIC | 10.10.10.11 | 255.255.255.0 |
| Laptop Invasor | Placa de rede | 10.10.10.12 | 255.255.255.0 |

# Objetivo

Parte 1: Configurar a segurança de portas

Parte 2: Verificar a segurança de portas

# Histórico

Nesta atividade, você irá configurar e verificar a segurança de porta em um switch. A segurança de porta permite restringir o tráfego de ingresso em uma porta por meio da limitação de endereços MAC autorizados a encaminhar o tráfego para a porta.

## Configurar a segurança da porta

* + 1. Acesse a linha de comando para **S1** e ative a segurança de portas nas portas Fast Ethernet 0/1 e 0/2.

Abrir a janela de configuração de IP

S1(config)# **interface range fa0/1 - 2**

S1(config-if-range)# **switchport port-security**

* + 1. Defina o máximo de modo que somente um dispositivo possa acessar as portas Fast Ethernet 0/1 e 0/2.

S1(config-if-range)# **switchport port-security maximum 1**

* + 1. Proteja as portas para que o endereço MAC de um dispositivo seja dinamicamente reconhecido e adicionado à configuração em execução.

S1(config-if-range)# **switchport port-security mac-address sticky**

* + 1. Defina o modo de violação para que as portas Fast Ethernet 0/1 e 0/2 não sejam desativadas quando ocorrer uma violação, mas uma notificação da violação de segurança será gerada e os pacotes da fonte desconhecida serão descartados.

S1(config-if-range)# **switchport port-security violation restrict**

* + 1. Desabilite todas as portas não utilizadas. Use a palavra-chave **range** para aplicar esta configuração a todas as portas simultaneamente.

S1(config-if-range)# **interface range f0/3 - 24 , g0/1 - 2**

S1(config-if-range)# **shutdown**

## Verifique a segurança de portas

* + 1. Do **PC1**, faça ping para o **PC2**.
    2. Verifique se segurança de portas está ativada e se o endereço MAC de **PC1** e **PC2** foi adicionado à configuração em execução.

S1# **show run | begin interface**

* + 1. Use os comandos port-security show para exibir informações de configuração.

S1# **show port-security**

S1# **show port-security address**

* + 1. Conecte o **Laptop Invasor** a qualquer porta de switch não usada e observe que as luzes de link estão vermelhas.
    2. Ative a porta e verifique se o **Laptop Invasor** pode fazer ping no **PC1** e **PC2**. Após a verificação, desligue a porta conectada ao **Laptop Invasor.**
    3. Desconecte o **PC2** e conecte **laptop não autorizado** a F0/2, que é a porta à qual o PC2 foi originalmente conectado. Verifique se o **Laptop Invasor** não consegue executar ping para **PC1**.
    4. Exiba as violações de segurança da porta à qual o **Laptop não autorizado**está conectado.

S1# **show port-security interface f0/2**

Fechar janela de configuração

### Pergunta:

Quantas violações ocorreram?

Digite suas respostas aqui.

Deve haver uma contagem de violações de pelo menos quatro, uma para cada solicitação de ping.

* + 1. Desconecte o **Laptop Invasor** e reconecte **PC2**. Verifique se **PC2** pode executar ping para **PC1**.

### Pergunta:

Por que **PC2** pode executar ping para **PC1**, mas o **Laptop Invasor** não pode?

Digite suas respostas aqui.

A segurança da porta que foi habilitada na porta permitiu que apenas o dispositivo, cujo MAC foi aprendido primeiro, acessasse a porta enquanto impedia que outros dispositivos acessassem.

Fim do documento