

07
Sticky

Transcrição

[00:00] Nós conseguimos configurar essa porta fastEthernet 0/1, pra que ela agora aceite somente o endereço MAC desse meu PC 0. Com isso, se algum outro usuário tentar colocar outro computador nessa porta fastEthernet 0/1, o que vai acontecer? Essa porta vai desabilitar e não vai deixar com que a comunicação seja estabelecida.

[00:18] Só que, tudo bem, aqui somente temos dois computadores, mas imagina um cenário de uma rede corporativa que temos as nossas portas do switch e tem vários equipamentos conectados nessas portas do switch. Imagina termos que ver o endereço MAC de cada um desses dispositivos, ter que voltar no switch, configurar estaticamente cada uma dessas portas pra trabalhar com o endereço MAC? É um pouco trabalhoso demais.

[00:43] Por isso que a Cisco desenvolveu uma forma, uma configuração que vai ajudar a fazermos com que essas portas do meu switch aprendam de forma dinâmica os endereços MAC dos dispositivos com os quais ele está conectado.

[00:57] A ideia nessa porta fastEthernet 0/2, é que eu não precise mais configurar estaticamente, como fizemos anteriormente, o endereço MAC do dispositivo aqui, no caso, o PC 1. A ideia é que essa porta fastEthernet 0/2 consiga aprender de forma dinâmica qual é o endereço MAC desse computador do PC 1, pra que conseguíamos habilitar essa segurança dessa porta pra só aceitar os dados que vierem desse computador PC 1. Vamos fazer essa etapa de configuração agora.

[01:30] No primeiro passo, temos que trabalhar nessa interface fastEthernet 0/2, então temos que subir os níveis pra chegar nessa interface. Colocamos "enable" pra entrar no modo privilegiado, colocamos "configure terminal" pra ele entrar no modo de configuração global, e digitamos agora "interface fastEthernet 0/2", pra entrar no último nível, que seria de configuração da interface.

[01:58] Primeiro passo pra habilitar a segurança nessa porta, temos que falar que essa porta é uma porta que está conectada a um dispositivo final, que na nossa camada do modelo da Cisco, é a chamada camada de acesso da minha rede. Então, eu tenho que vir aqui e falar que essa porta "switchport mode", o modo dela vai ser modo de acesso.

[02:20] E uma vez que eu falei que ela é uma porta que vai trabalhar no modo de acesso, eu posso agora habilitar a segurança nessa porta. Pra eu habilitar a segurança nessa porta tenho que colocar aquele comando "switchport port-security". Pronto. Então essa porta agora está habilitada, está apta pra que configure a segurança que queremos.

[02:42] Agora que já habilitamos vamos dizer como que nós queremos que essa segurança, essa política de segurança seja feita. Então, vamos colocar o comando "switchport port-security", vou colocar de novo o "mac-address" e agora eu vou colocar uma interrogação aqui.

[02:56] Anteriormente nós utilizamos essa primeira opção, onde nós colocamos manualmente, estaticamente, o endereço MAC que queríamos que fosse vinculado a essa porta, pra só aceitar o endereço MAC que configurarmos. Agora o que vamos fazer? Vamos pedir pra essa porta fastEthernet 0/2, pra que ela aprenda de forma dinâmica qual é o computador, o dispositivo que ela está conectada, pra que ela só passe a aceitar esse endereço MAC desse meu computador e não aceite outros endereços MAC no futuro.

[03:27] Eu vou colocar esse comando de baixo, que recebe o nome de sticky. Então, vou colocar aqui agora "sticky". E eu estou falando pra essa porta aprender dinamicamente o endereço MAC do dispositivo com o qual ela está conectada, e partir daí ela só vai aceitar esse endereço MAC. Eu vou colocar agora um Ctrl + Z e somente colocamos esse comando aqui, "switchport port-security mac-address sticky".

[03:54] Vamos fazer o seguinte, eu vou tentar realizar a comunicação desse meu computador do PC 1 com o PC 0. Eu vou vir no PC 1 e vamos tentar realizar a comunicação com o PC 0, afinal, eu falei pra essa porta fastEthernet 0/2 do switch aceitar o endereço MAC do dispositivo com o qual ela está conectada, que nesse nosso caso é o PC 1. Aparentemente está tudo ok, vamos ver se a comunicação com o PC 0 lá da esquerda está sendo feita com sucesso. Faço o ping e a comunicação é feita com sucesso.

[04:26] Vamos ver se agora o meu switch aprendeu o endereço MAC desse meu computador? Eu vou clicar no switch novamente e vou perguntar pro switch quais são os endereços MAC que estão aceitos nessas políticas de segurança.

[04:44] Esperamos que esse meu switch me mostre o endereço MAC da interface fastEthernet 0/1 vinculado a esse PC 0, e esperamos que agora a porta fastEthernet 0/2 aceite o endereço MAC que esteja configurado nesse PC 1. Só que não colocamos estaticamente pro switch aprender o endereço MAC do PC 1, ele deve ter aprendido de forma dinâmica. Vamos perguntar pro switch quais são os endereços MAC que ele aprendeu como sendo endereços MAC aceitos pra políticas aqui de acesso.

[05:18] Vou colocar o comando "show port-security address" e olha só o que ele me fala. Nós temos dois endereços MAC que são aceitos pra realizar a comunicação dessas interfaces. Então, na interface fastEthernet 0/1 tínhamos configurado estaticamente, manualmente, o endereço MAC 0060.2F0B.D1D7, que é o endereço MAC desse meu PC 0. Vamos só confirmar se é ele mesmo? Vamos colocar aqui no "Config", "FastEthernet0". Eu tenho aqui o 0060.2F0B.D1D7.

[06:02] Então, esse daqui tínhamos configurado estaticamente. Ele até fala pra mim "SecureConfigured", ou seja, que foi feita uma configuração segura, manualmente, estaticamente. Nós, usuários, que fomos lá e digitamos esse comando. E aqui embaixo, eu não configurei o endereço MAC estaticamente, olha como ele disse que aprendeu esse endereço MAC, foi daquela forma dinâmica, daquela forma "SecureSticky", que chamamos figurado esse sticky.

[06:28] E vamos só confirmar se esse endereço MAC que está atribuído nessa fastEthernet 0/2, se é o do meu PC 1. Então esse é o endereço MAC, vamos só confirmar se é do PC 1. Vamos colocar o PC 1 pra cá e vamos confirmar se é ele. É ele mesmo, 0003.E405.E978.

[07:00] Com isso conseguimos configurar a segurança dessas portas pra elas aceitarem um endereço MAC, mas estamos somente vinculando pra elas aceitarem o endereço MAC de forma dinâmica. Não precisamos ficar configurando mais estaticamente esses endereços MAC.

[07:15] A partir desse momento, essa porta só vai aceitar esse computador aqui. Se eu tentar conectar outro computador, se eu desconectar essa porta e conectar de novo o nosso funcionário, que vai levar o computador dele que tem os softwares pra fazer teste de vulnerabilidade. Ele traz o notebook dele pra cá e conecta nessa porta, na fastEthernet 0/2, e tentar realizar a comunicação. Vamos só colocar o endereço IP pra ele, 192.168.0.4, vamos só esperar a porta carregar, que ela demora alguns segundos.

[07:52] Então, agora esperamos que essa porta fastEthernet 0/2 não aceite esse computador, o Laptop 5. Porque de forma dinâmica, essa porta fastEthernet 0/2 aprendeu que ela só deve aceitar esse computador PC 1. Então, vamos ver se estamos tendo uma política de segurança.

[08:12] Eu vou clicar nesse meu computador, vamos colocar o comando "ping 192.168.0.1", que é o endereço IP do PC 0, que está lá no lado esquerdo, e vamos ver se a comunicação foi estabelecida. "Request timed out".

[08:29] E olha só o que aconteceu: a porta ficou vermelha, a porta desabilitou. E conseguimos ter uma maior facilidade, de não ter que ficar se preocupando em ver o endereço MAC de cada dispositivo e configurar esses endereços MAC na mão. Através da configuração do sticky, ele consegue pegar o endereço MAC de forma dinâmica do dispositivo que está conectado nessa porta. Vamos seguir.

