05

VLAN Nativa

Transcrição

[00:00] Fizemos a configuração dessas portas fastEthernet 0/3 pra que elas atuassem no modo Trunk, sendo capazes de transportar dados de diferentes VLANs, da VLAN 2 e da VLAN 3 do nosso setor do administrativo e do financeiro.

[00:15] Lembrando, inicialmente colocamos essa porta fastEthernet 0/3 desse switch da esquerda, entramos nela e colocamos aquele comando "switchport mode trunk". E isso fez com que essa porta entrasse naquele modo chamado de on.

[00:32] Quando tem essa porta nesse modo on significa que ela vai tentar já ajudar um pouco a vida do usuário final e vai tentar realizar uma negociação com a porta com qual ela está conectada, que no nosso caso é essa porta aqui, fastEthernet 0/3 desse switch, pra que essa porta fastEthernet 0/3 desse switch da direita também passe a atuar em modo Trunk.

[00:56] Aí o usuário não tem que vir nesse outro switch, entrar na configuração da porta e habilitar essa porta pra trabalhar em modo Trunk. Os switches já conseguem fazer essa automatização para facilitando a vida do usuário final.

[01:13] Só que, o que acontece? Tem essa comunicação entre os switches, então está ocorrendo essa comunicação do protocolo 802.1q, que é responsável por essa negociação das portas Trunk. Só que essa porta fastEthernet 0/3 está passando dados de diferentes VLANs, tem lá a VLAN 2 do administrativo, a VLAN 3 do financeiro.

[01:39] Como que eu consigo separar essa VLAN pra poder referenciar esses dados de gerenciamento que estão sendo passados para os switches, esses protocolos de comunicação que estão sendo passados pelo switch? Vamos dar uma olhadinha nisso agora.

[01:54] Vamos voltar naquela análise que fizemos anteriormente, perguntando para o switch quais são as portas Trunk que ele tem configuradas. Eu vou clicar nesse switch da direita e vou apagar os dados que tinha feito anteriormente. Já estamos no modo privilegiado e vamos colocar de novo aquele comando "show interfaces trunk", porque eu quero perguntar pra esse meu switch as portas Trunk que ele tem configuradas.

[02:22] Nesse caso, tem a porta fastEthernet 0/3 configurada e essa porta fastEthernet 0/3 do switch da direita tinha recebido o comando daquela porta do switch da esquerda, que estava em modo on, que colocamos "switchport mode trunk". E esse switch da direita, pelo fato de estar configurado em auto, ele pegou esse comando que estava com o comando on e já autoconfigurou essa porta, pra ela atuar em modo Trunk.

[02:51] Só que falamos que tem esses protocolos de comunicação que estão acontecendo entre os switches. Então, esses protocolos de gerenciamento vão estar nessa chamada VLAN nativa. E por padrão a VLAN nativa, quando não se faz nenhuma configuração, ela vai ser igual a VLAN default, que é a VLAN número 1.

[03:15] Mas, não é considerado boa prática deixar essa VLAN nativa igual a VLAN número 1. Por que não? Porque essa VLAN nativa vai estar passando esses dados de gerenciamento entre os switches. O que pode acontecer? Se essa VLAN nativa for igual a VLAN número 1, um usuário um pouco mais esperto pode conectar o computador dele em uma interface do switch, que vai também pertencer a VLAN nativa, que é a VLAN número 1, e ele consegue ver alguns protocolos de gerenciamento entre os switches.

[03:51] Pode representar uma vulnerabilidade de segurança manter essa VLAN nativa, que eu uso pra fazer essa passagem de protocolo de gerenciamento dos switches, e deixá-la na mesma VLAN que é a VLAN default número 1.

[04:07] O ideal é deixar essa VLAN nativa somente pra que ocorra a comunicação entre os switches, pra que nenhum usuário curioso faça uma conexão no computador com essas portas que estão trabalhando lá na VLAN default, que é a VLAN número 1, pra que ele não faça uma conexão e use softwares, como o Kali Linux, pra poder manipular esses protocolos e ver esses protocolos de gerenciamento dos switches.

[04:37] Como boa prática, como medida de segurança é sempre bom deixar essa VLAN nativa como um número diferente da VLAN default. Porque mesmo que alguém vá na interface do meu switch e plugue um computador nessa interface desse meu switch, se ela estiver na VLAN default, na VLAN 1, não vai interferir em nada.

[04:56] Mesmo que ele coloque um software pra fazer algumas análises, ele não vai conseguir pegar esses dados de gerenciamento que estão passando pela VLAN nativa, porque a VLAN nativa agora vai estar em outra VLAN. Se dados estão em VLANs diferentes, é como se eu realmente estivesse realizando toda essa segmentação.

[05:13] Para fazer essa troca, precisa fazer o seguinte comando: colocar "configure terminal", temos que ir até a configuração dessa interface que está trabalhando em modo Trunk, que no caso é a fastEthernet 0/3. Então, tem que entrar nela, "fastEthernet 0/3", e aí eu tenho que falar que eu quero que essa porta não trabalhe com a VLAN nativa número 1.

[05:38] Eu escolho como boa prática uma VLAN que não esteja sendo usada para nada, ela vai ser usada somente pra esse transporte dos protocolos de gerenciamento entre os switches. Vou colocar aqui, por exemplo, o comando "switchport trunk" e eu tenho que colocar o comando "native vlan" agora, vai ser uma VLAN que não está associada com nenhuma interface, não está sendo usada pra nada, ela vai ser usada só pra esse gerenciamento. Eu vou colocar aqui, por exemplo, uma vlan 999.

[06:06] Quando eu coloco essa "switchport trunk vlan 999", eu estou alterando essa VLAN nativa pra que ela trabalhe com uma VLAN diferente da VLAN default, eu estou colocando agora uma VLAN 999. Se eu colocar um Ctrl + Z e digitar o comando de novo "show interfaces trunk" perceba que a minha VLAN nativa passou a ser 999.

[06:33] Agora, vamos ver o resultado que teve do switch da esquerda. Então, vou fechar aqui e vou clicar esse switch na esquerda. E olha só a mensagem que tem aqui: teve um problema de compatibilidade da native VLAN. Por quê?

[06:52] Porque a native VLAN é a VLAN nativa onde vai passar esses dados, esses protocolos de gerenciamento entre os switches. Então, os switches têm que concordar em qual vai ser a VLAN nativa que eles têm que adotar. Tem que ser o mesmo número, eles têm que pertencer ao mesmo grupo, à mesma VLAN. Porque se um acha que tem que passar os dados de gerenciamento na VLAN 999 e esse continua achando que é na 1, não vai dar muito certo. Temos que fazer o quê? Temos que trazer os dois pra trabalhar na mesma VLAN.

[07:24] Não podemos deixar, por exemplo, um switch com uma VLAN nativa e o outro switch com uma VLAN nativa diferente. Os dois têm que ter a mesma VLAN nativa, senão tem erros aqui na nossa rede.

[07:39] Se manter assim até o final pode ter o vazamento dessa informação desses protocolos pra outra VLAN. Porque está ocorrendo esse mismatch, está incompatibilidade de VLAN. E o tráfego, como o switch vai se comportar, acaba sendo um pouco imprevisível. Ele pode mandar esses dados desses protocolos de gerenciamento pra outra VLAN, por exemplo, pra VLAN 2 do administrativo, a VLAN 3 do financeiro. O comportamento vai se tornar imprevisível.

[08:04] É sempre bom trocar essa VLAN nativa pra uma VLAN diferente, que não esteja usada pra nenhum outro lugar na minha rede. E tem que lembrar que todas as VLANs nativas de todos os switches têm que ser iguais.

[08:16] Ele fica sempre mandando essa mensagem relembrando: "você tem que trocar a VLAN nativa", porque o que eu detectei na minha ponta remota do switch da direita, a VLAN nativa está diferente do que eu tenho aqui, eu tenho que trocar aqui também.

[08:27] Pra eu trocar aqui vem aqui, coloca o comando "enable" pra entrar no modo privilegiado, e eu tenho que subir o nível até a interface fastEthernet 0/3. Eu coloco "configure terminal", "interface fastEthernet 0/3" e coloco o mesmo comando, "switchport trunk native vlan" e o número que eu quero, que tem que ser igual, 999. Vamos colocar o Ctrl + Z e vamos colocar o comando "show interfaces trunk".

[09:00] Agora, esse switch da esquerda também está configurada a VLAN nativa igual a 999. A VLAN nativa dos dois dispositivos está agora configurada corretamente com o mesmo valor. Vamos lá.