

Configuração de Switches

Configuração de switches (comutadores) para redes locais de computadores.

Prof. Fred Sauer

1. Itens iniciais

Propósito

Switches são elementos fundamentais em um projeto de Redes de Computadores. De uma forma geral, pouca (ou nenhuma) configuração é necessária para colocá-los em funcionamento, porém há demandas básicas e avançadas que mudam completamente sua capacidade de operar com desempenho satisfatório e segurança.

Preparação

Antes de iniciar seu estudo, é importante ter o software *Packet Tracer* versão 8.1.0 ou superior.

Objetivos

- Identificar os recursos de cada tipo de switch.
- Aplicar configurações básicas em switches.
- Aplicar configurações de segurança em switches.

Introdução

Switches são equipamentos muito importantes em projetos de redes locais. Eles segregam domínios de colisão por cada porta, evitando que ruídos e quadros corrompidos poluam a rede. Além disso, como são equipamentos de camada de enlace, têm capacidade de usar os endereços físicos das estações e de outros equipamentos de conectividade para as decisões de encaminhamento dos quadros, aumentando assim o *throughput* nominal por equipamento, e consequentemente, de toda a rede local.

Os mais conhecidos são os switches não gerenciáveis. Amplamente usados na maioria das residências onde se compartilha um link de Internet de operadora, são equipamentos *plug-and-play*, ou seja, basta conectar os cabos e alimentar eletricamente que ele já cumpre o seu papel.

Imediatamente, ao ser ligado, inicia um processo de escuta e aprendizado de endereços físicos (*Mac Addresses*), onde são inseridos em tabelas, correlacionados às portas por onde foram recebidos – *Cam Table* – para que a comutação dos quadros seja feita apenas para a porta onde esteja o destinatário.

No entanto, em redes corporativas, com demandas de alta disponibilidade, essa característica de simplicidade dos switches não gerenciáveis pode se tornar um problema. Há inúmeras possibilidades de atividades maliciosas, como, por exemplo, por meio de ataques de negação de serviço. Isso demanda a configuração de recursos mitigatórios que dependem de uma estratégia voltada para cada ambiente, não sendo algo passível de configuração automática.

Além disso, outras possibilidades de melhorar as competências dos switches foram surgindo, como a agregação de links, segregação da rede em VLANs, roteamento entre VLANs e vários outros recursos que dependem de configurações apropriadas, feitas em switches gerenciáveis.

Por essa razão, este conteúdo foi elaborado com ensinamentos práticos, porém, com a abordagem teórica necessária para não apenas justificar, mas também permitir a escolha do equipamento ideal para cada projeto.

Vamos começar?

Acompanhe no vídeo o assunto que vamos estudar.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Atualmente, há switches disponíveis para projetos desde uma rede doméstica até um ambiente de altíssima disponibilidade, como *datacenters*. Este tópico vai tratar dos tipos de switches e suas características.

Switches não gerenciáveis e gerenciáveis

Projetos de redes variam de tamanho e de dependência de recursos específicos para atender a demandas de projeto. Em um ambiente doméstico, tipicamente há limitações de custo, e flexibilidade nos requisitos. Já para ambientes corporativos, demandas de disponibilidade, segurança e qualidade de serviço exigem equipamentos com mais recursos. Este tópico vai apresentar a primeira e mais básica classificação ente switches: **ser gerenciável ou não**.

Switches não gerenciáveis

Em ambiente doméstico, de uma forma geral, é requisito que os equipamentos não demandem conhecimento técnico aprofundado dos usuários. Quanto mais prontos para uso, mais adequados para a maioria dos usuários.

> Switches não gerenciáveis não permitem configurações por parte do usuário, logo, não possuem uma interface de configuração nem de monitoramento.

Apesar disso, há modelos de mesa ou de *rack*, com variações no número de portas e taxa de operação variável. Questões como taxas discrepantes de transmissão, conexão *straight-thru* ou *crossover*, bem como modo de operação *Half* ou *full duplex*, são resolvidas por autonegociação. Em um switch não gerenciável, não é possível criar VLANs, logo, todas as portas permanecem em uma única VLAN – a VLAN padrão.

A seguir, ilustramos alguns modelos populares de switches não gerenciáveis:

DLINK DGS-1008a Switch Gigabit 8 portas

Este equipamento é projetado para pequenos ambientes, sem exigências de recursos dependentes de configuração. Tipicamente usado acima de mesas ou até dentro de gabinetes improvisados.



Cisco Business CBS110-24PP

Este equipamento é mais robusto, oferecendo recursos como PoE em 12 de suas portas, funcionalidades de QoS básicas e detecção de loops, porém automáticas e sem possibilidade de configuração ou ajustes. Esse modelo pode ser instalado em racks de 19 polegadas.
A recomendação do próprio fabricante (CISCO, 2022), apesar deste ser um dos modelos mais robustos não gerenciáveis, é que seja usado em ambientes com poucas estações (small business).



Switches gerenciáveis

Switches gerenciáveis são aqueles que **possuem uma interface para gerenciamento e funcionalidades configuráveis**. Estas funcionalidades variam entre os vários modelos, desde as mais básicas, como colocar um nome e uma senha no equipamento, até recursos avançados de priorização de tráfego e segurança em várias camadas.

Alguns recursos possíveis deste tipo de switch são:

CLI/Web
Uma interface para configuração e diagnóstico.

VLANs
Organização, segregação de tráfego, QoS.

VLAN Routing
Redução do tráfego na rede local.

SNMP/RMON
Monitoramento operacional em tempo real.

STP
Detecção/eliminação de loops.

Link Aggregation
Aumento do throughput de uplinks.

Stacking
Empilhamento de switches para aumento da densidade de portas.

QoS
Mecanismos para priorização de tráfego.

Port Security
Controle das estações conectadas.

Naturalmente, em virtude das suas várias funcionalidades adicionais, switches gerenciáveis são mais caros e demandam conhecimento técnico para sua configuração e monitoramento. É muito importante que durante o projeto de rede sejam especificadas as competências desejadas para a escolha do equipamento mais adequado.

Switches Multicamadas

Acompanhe no vídeo o assunto que vamos estudar.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

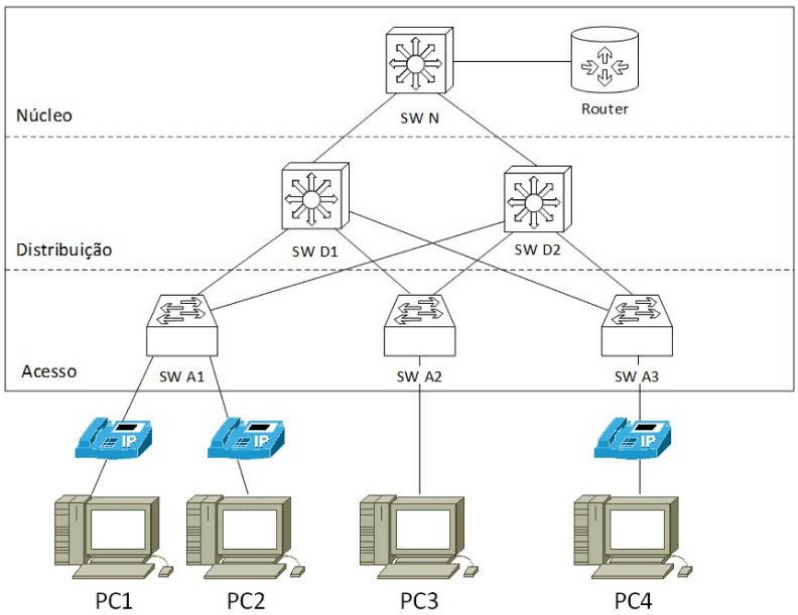
Switches L3

O Switch é um equipamento que opera na camada de enlace (L2), encaminhando os quadros após a verificação da integridade via CRC e consulta à tabela CAM (*Content Addressable Memory*), que contém os MAC *Addresses* "aprendidos" ao longo de sua operação. Com a introdução do conceito de VLAN, as redes passaram a poder ser segregadas em domínios de *broadcasts* diferentes, como sub-redes da rede local.

Comentário

No início, a comunicação entre estações de VLANs diferentes da mesma rede local demandava a utilização de roteadores, provocando muitas vezes um longo trajeto do quadro entre a origem e o destino – grande diâmetro da rede. Com a utilização de técnicas para a implementação de redes escalares e de alta disponibilidade, por meio do design hierárquico, surgiram os switches L3.

A figura a seguir ilustra o modelo hierárquico:



Modelo hierárquico de rede

Nessa figura, podemos observar que a rede está organizada em três camadas: a camada de núcleo se destina ao acesso a outras redes, a de distribuição implementa o roteamento entre as VLANs, entre outras funções, e a camada de acesso oferece a conectividade aos dispositivos finais. Com isso, reduz-se o diâmetro da rede e isola-se o tráfego interno destinado a outras redes, roteado na camada de núcleo.

Nesse cenário ilustrado, enquanto SW A1, A2 e A3 representam switches gerenciáveis L2, os switches SW D1 e D2 seriam switches gerenciáveis L3, em virtude de sua capacidade de rotear entre VLANs.

Supondo que SW A1 tem suas portas agregadas à VLAN 10 e o switch SW A2 implementa o ambiente da VLAN 20, caso PC1 envie um quadro ou faça uma ligação telefônica IP para PC 3, o trajeto seria:

> PC1 → SW A1 → SW D1 ou D2 → SW A2 → PC3, evitando a necessidade de comutação até o roteador na camada de núcleo.

Se os switches SW D1, D2 e N fossem L2, o trajeto seria:

> PC1 → SW A1 → SW D1 → SW N → Router → SW N → SW D1 ou D2 → SW A2 → PC3, ou seja, de 4 hops (saltos) passaríamos a ter o dobro, 8.

Switches para redes metropolitanas

Switches Metro Ethernet

Até agora discutimos apenas soluções no ambiente de redes locais. No passado, a conectividade entre essas redes era basicamente feita por meio de operadoras de telecomunicações, com as LPCD (Linhas Privativas de Comunicação de Dados), explorando a agregação de canais TDM (*Time Division Multiplexing*) de 56Kbps (modelo americano) ou 64Kbps (modelo europeu) em uma hierarquia digital.

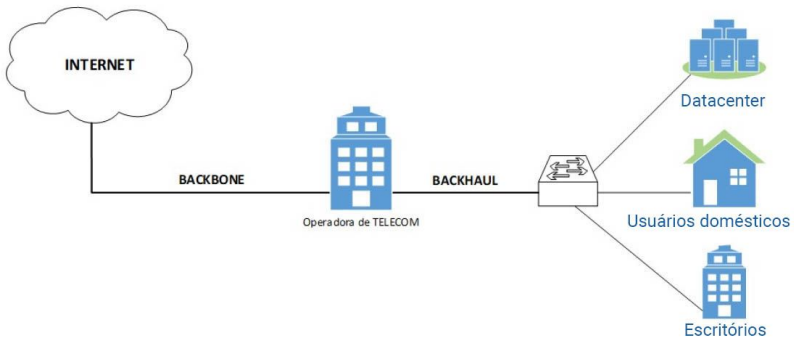
Com o aumento da demanda de conectividade global, surgiram as primeiras soluções de MAN (redes metropolitanas), e entre elas a *metro ethernet*. A ideia foi prover conectividade de última milha a empresas e

assinantes com o mesmo padrão de protocolos das redes locais, oferecendo simplicidade e flexibilidade, com baixo custo.

De acordo com fornecedores de soluções *metro ethernet* (JUNIPER, 2022), as principais aplicações endereçadas são:

- Interconectar escritórios ou *datacenters*, pontoa ponto, ponto a multiponto ou multiponto a multiponto.
- Fornecer conectividade a assinantes residenciais ou empresas, bem como *datacenters* públicos ou privados.
- Fornecer entrega *multicast* para clientes empresariais (para videoconferência) e para assinantes residenciais (para IPTV e outras aplicações de vídeo).
- Fornecer serviços de *backhaul. Backhaul* é a interligação de redes e *backbones.*

Veja na figura a seguir a ilustração de *backhaul*:



Backhaul Metro Ethernet

Uma das principais funcionalidades indicadas pelos provedores de *Metro Ethernet* é a disponibilidade de transporte MPLS (*Multiprotocol Label Switching*). Esta técnica possibilita a implementação de qualidade de serviço por meio de classificação, marcação, policiamento, enfileiramento e agendamento de pacotes. Com isso, políticas podem ser implementadas, adequando a rede às demandas de tráfego dos usuários.

Além disso, uma óbvia e visível vantagem é a simplicidade pela inexistência de conversão de formatos de dados, uma vez que a rede MAN usa o mesmo padrão que a rede local (Ethernet). Há no mercado vários modelos com capacidades variáveis, desde aqueles mais simples com funcionalidades L2 até versões mais robustas com implementação L3, suportando vários protocolos de roteamento e opções para segurança e QoS.

Por se tratar de uma infraestrutura compartilhada, uma importante funcionalidade é a segurança para permitir o isolamento entre os assinantes. Dentre os recursos tipicamente suportados, podemos destacar:

Port Security
Apenas MAC *Addresses* autorizados podem ser conectados.

VLANs e ACLs
Com filtragens por MAC *Address*, IP *Address* e cabeçalho TCP/UDP.

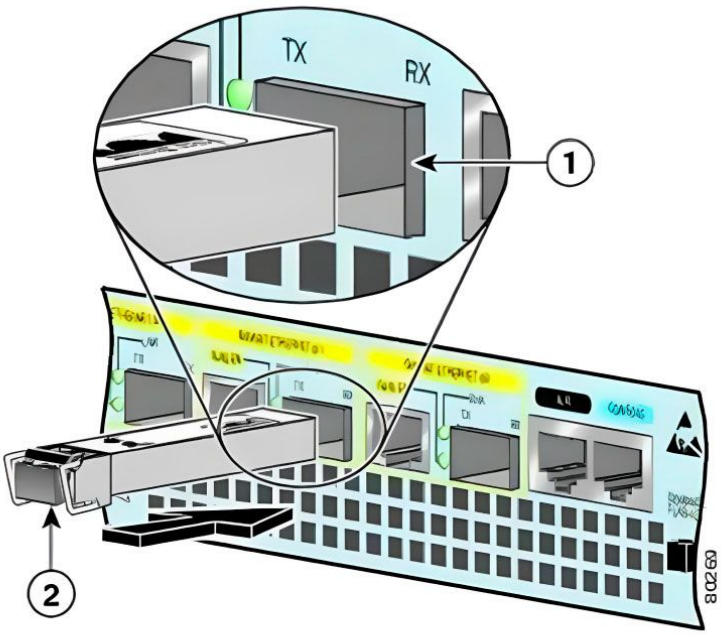
802.1x
Autenticação, autorização e *accounting* de acessos.

VPNs L3
Tunelamento de tráfego.

Switches modulares

A maioria dos switches que conhecemos é de configuração fixa, ou seja, tem pouca ou nenhuma flexibilidade para agregar um recurso redundante ou fazer um *"upgrade"* de porta para aumentar a sua taxa. Com o passar do tempo e a evolução das taxas do padrão ethernet, surgiram as "portas combo", que, na verdade, são *slots* para módulos SFP (*Small Form Pluggable*), que podem variar no tipo de cabo e na taxa de transmissão.

A figura a seguir ilustra essa solução:



Slot e módulo SFP

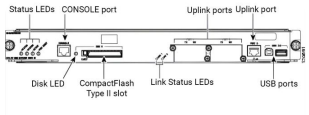
Na figura, é possível observar o *slot* no equipamento, identificado pelo numeral 1, e o elemento 2, um módulo para fibra ótica.

Se, para as soluções de camada de acesso, os switches de configuração fixa são os mais comuns, na camada de núcleo, em alguns projetos com demanda de escalabilidade e incertezas sobre o futuro da rede, o uso de switches modulares pode ser uma opção mais interessante.

Switches modulares são comercializados a partir de um chassi, onde são instalados os módulos, de acordo com o projeto de rede. Módulos típicos são:

Módulo *Supervisor Engine*

É o módulo que controla a operação de todo o switch. Tipicamente, é integrado a este módulo o *switch fabric*, que permite a comunicação entre os módulos simultaneamente sem consumo de banda para os usuários, por meio de uma matriz de comunicação.



Alguns switches modulares permitem a instalação de um módulo supervisor redundante. A figura a seguir ilustra um exemplo de módulo supervisor. Pode-se destacar a porta de console, usada para configuração do módulo, slots para módulos de *uplink* e para carga de software (*Flash Memory* e USB).

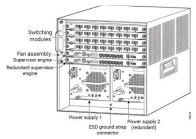
Módulos com portas ethernet par trançado e fibra *(line cards)*

É um módulo com grande variedade de número de portas e taxas de transmissão.

Módulos de fonte de alimentação

É um módulo que pode ser configurado redundantemente de três formas diferentes:

1. Modo N + N – suporta a falha de N fontes;
2. Modo N + 1 – suporta a falha de uma fonte; ou
3. Modo Combinado – A rigor, não representa uma redundância, uma vez que as fontes instaladas “somam” a energia fornecida para alimentar os módulos do switch. Nesse modo, caso uma fonte falhe, módulos tendem a ser desligados para manter os demais operando.



Módulos especializados

Módulos especializados implementam serviços de segurança, como por exemplo o FWSM - Cisco Firewall Service Module e o Cisco WebVPN.

Aqui conhecemos os tipos de switches, destacando a importância do gerenciamento para funções avançadas e customização do serviço de comutação e monitoramento da operação. Entendemos que os switches podem incorporar funcionalidades de outras camadas além da L2, responsável pela comutação em si. Também discutimos a utilização de switches *metro ethernet* em áreas metropolitanas, e suas vantagens em relação a outras opções.

Por fim, aprendemos que os switches podem ser de característica fixa ou modular, permitindo que projetos de redes sejam feitos com a indicação pontual dos equipamentos necessários, mas também suportar escalabilidade e resiliência em caso de falhas.

A seguir, vamos conhecer e acompanhar a configuração básica de switches.

Montando uma topologia de rede em ambiente de simulação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Switches são equipamentos essenciais em um projeto de redes. Caso um projeto demande a criação de VLANs para segregação de tráfego, qual recurso é minimamente necessário para esse propósito?

A

Configuração fixa

B

Configuração modular

C

Ser L2 não gerenciável

D

Ser L2 gerenciável

E

Ser L3

A alternativa D está correta.

A criação e a configuração de VLANs **exige** o uso de uma interface de configuração, apenas disponível em switches **gerenciáveis**. Não é preciso que seja L3, recurso vital para o roteamento entre as VLANs criadas sem a necessidade de um roteador.

Questão 2

Um switch modular possui recursos mais flexíveis do que os de configuração fixa, decorrente da inserção de módulos de acordo com as demandas de projeto. No uso de fontes redundantes, em qual modelo, em caso de falha de uma fonte, módulos podem ser desativados para manter o equipamento em operação?

A

Modo N + N

B

Modo N + 1

C

Modo 1 + 1

D

Modo redundante

E

Modo combinado

A alternativa E está correta.

No modo N + N, a falha de mais de uma fonte pode ser suportada; no N + 1, apenas a falha de uma fonte é suportada, sendo a alimentação da fonte em falha substituída pela de outra fonte; o Modo 1 + 1 não existe, nem o modo redundante.

No modo combinado, cálculos são necessários para que o somatório da energia fornecida pelo *pool* de fontes seja capaz de alimentar os módulos, e, em caso de falha de uma ou mais fontes, a operacionalidade do conjunto como um todo dependerá da demanda de energia. Caso seja insuficiente, módulos serão desativados sequencialmente, visando manter o máximo de módulos operacionais.

Acessando um switch

Acompanhe no vídeo o assunto que vamos estudar.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

O processo de configuração de switches é dependente das funcionalidades, mas há um ciclo básico de configuração que deve ser realizado em qualquer switch gerenciável. Questões de nomeação e segurança são básicas e devem ser feitas antes de qualquer configuração mais complexa. Vamos apresentar estas configurações, que podem ser reproduzidas no ambiente Cisco *Packet Tracer*.

É importante ressaltar que **fabricantes diferentes usam recursos sintáticos diferentes** na maioria dos casos; porém, todas as operações são fundamentadas nos padrões do IEEE, bastando buscar a correspondência sintática dos comandos utilizados pelo fabricante do equipamento a configurar.

Acesso à interface de configuração

Switches gerenciáveis podem ser configurados **local ou remotamente**. Para a configuração remota, apesar de o switch ser um equipamento de camada 2, é necessária a configuração de um endereço IP para que ele possa ser identificado univocamente em uma rede. Para isso, os switches possuem uma interface virtual chamada SVI (*Switch Virtual Interface*), que não é vinculada a nenhuma porta física, mas sim ao switch como um todo.

Dessa forma, sem que alguma configuração já tivesse sido feita ou viesse de fábrica, será necessário realizar o acesso local por meio da porta de console do equipamento. Para isso, é preciso usar um cabo de console conectado a um computador e uma aplicação para acesso ao IOS do equipamento, como o Putty.

A figura a seguir ilustra um cabo console, também chamado *rollover cable*.



Cabo Console

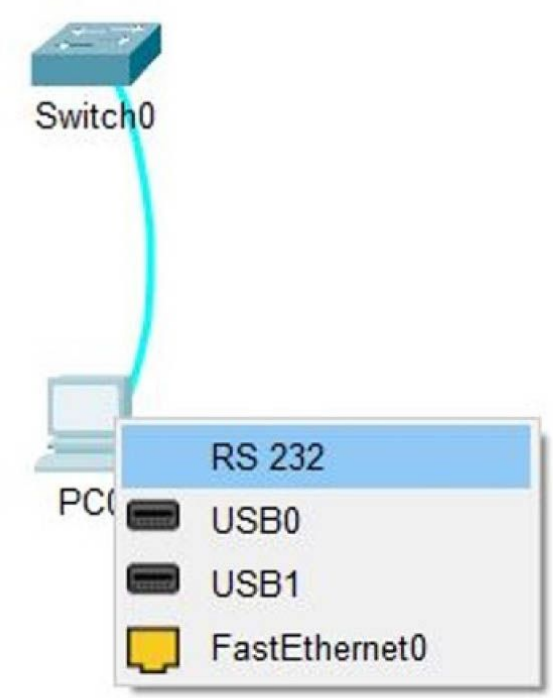
Cabos de console possuem uma extremidade **conectorizada com RJ-45** para conexão à porta **console**, e a outra pode usar conectores seriais ou USB, de acordo com a disponibilidade de interfaces na estação de trabalho usada para configurar o equipamento. A porta console pode estar localizada na frente ou na traseira do equipamento, mas tipicamente tem uma identificação visível como porta de console.

Comentário

Alguns equipamentos mais novos vêm oferecendo a porta console em padrão USB-C. O uso de adaptadores para USB envolve a necessidade de instalação de driver e descoberta da porta serial emulada, mas é um procedimento simples e com farta documentação disponível. O uso da aplicação Putty ou TERA Term para emulação de terminal também é bastante popular, com muitos tutoriais disponíveis.

Como vamos usar o ambiente de simulação do *Packet Tracer*, após selecionar o Switch desejado e um "dispositivo final" para configurá-lo, basta ir em "*connections*", no canto inferior esquerdo, clicar no cabo console e, depois, no computador escolhido, indicando a interface serial RS232 como conexão desejada, e, em seguida, selecionar a porta console no switch.

A figura a seguir ilustra o momento da seleção da interface serial no PC:



Seleção da Interface para console

Ao clicar no PC0, na aba *"desktop"* há várias opções, entre elas a "terminal". Quando clicamos nela, são apresentados os dados de configuração da porta serial (bps, *data bits, parity, stop bits* e *flow control*). Clicando em OK, já entramos na CLI (*Command Line Interface*) do equipamento, e podemos iniciar as configurações.

Iniciando as configurações

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

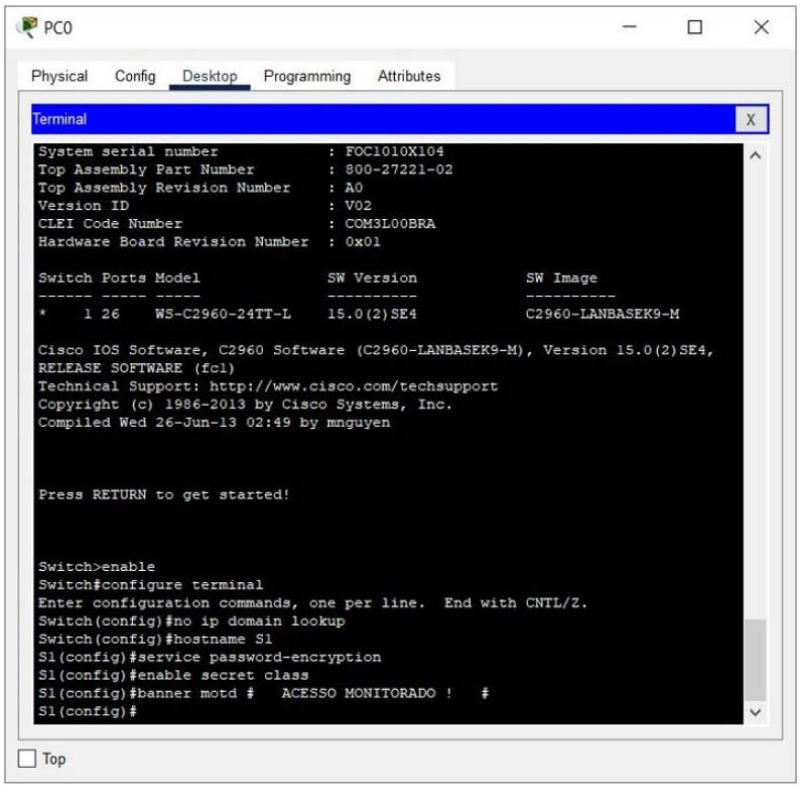
Configurações Básicas

Antes de preparar o equipamento para acesso remoto e outras configurações específicas, como VLANs e outros, é importante seguir um roteiro de personalização. Além da nomeação e endereçamento básico, alguns requisitos de segurança precisam ser cumpridos. Senhas, por exemplo, não podem ficar sem criptografia, uma vez que ficariam visíveis no arquivo de configuração.

Também é considerada boa prática trocar a VLAN nativa para o gerenciamento, uma vez que, caso isso não seja feito, este tráfego usará a VLAN padrão (VLAN 1), facilitando a captura de informações por agentes mal-intencionados.

Personalização inicial

Na CLI do equipamento, precisamos entrar em modo exec privilegiado e, em seguida, modo de configuração global. A figura a seguir ilustra o processo:



Personalização Inicial

Estes comandos e suas respectivas ações são as seguintes:

Switch>enable
Entra em modo privilegiado e muda o prompt para #.

Switch#configure terminal
Entra em modo de configuração global e muda o prompt para (config) #.

Switch (config) #no ip domain lookup
Evita que comandos digitados não reconhecidos sejam enviados para resolução DNS.

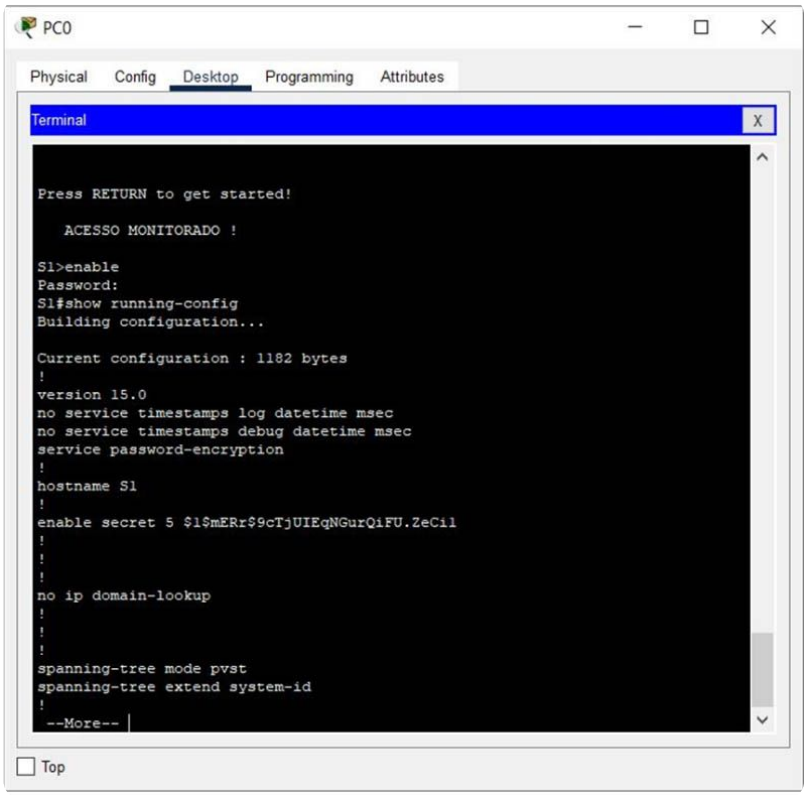
Switch (config) #hostname S1
Alteramos o nome do switch para “S1”.

S1 (config) #service password-encryption
Aplica criptografia às senhas no arquivo de configuração *(running-config* e *startup-config).*

S1 (config) #enable secret class
Introduz uma senha criptografada (class) para acesso ao modo EXEC privilegiado.

S1 (config) #banner motd
Introduz um banner de aviso sempre que a CLI do equipamento é acessada.

Após essa personalização inicial, podemos verificar as alterações no comportamento do switch e no arquivo de configuração em execução (*running-config*), conforme ilustrado a seguir:



Personalização inicial aplicada

Logo no início, podemos ver o *banner* criado, e o pedido de digitação de senha para entrada no modo EXEC privilegiado. No arquivo de configuração em execução, podemos ver a senha protegida por *hash*.

Atenção

Ao fazer configurações no equipamento, não esqueça de salvá-las por meio do comando S1# copy running-config startup-config. Ao ser inicializado, o arquivo usado para carregar as configurações é o startup-config.

A seguir, vamos preparar o switch para receber acesso remoto.

Acesso Remoto ao Switch

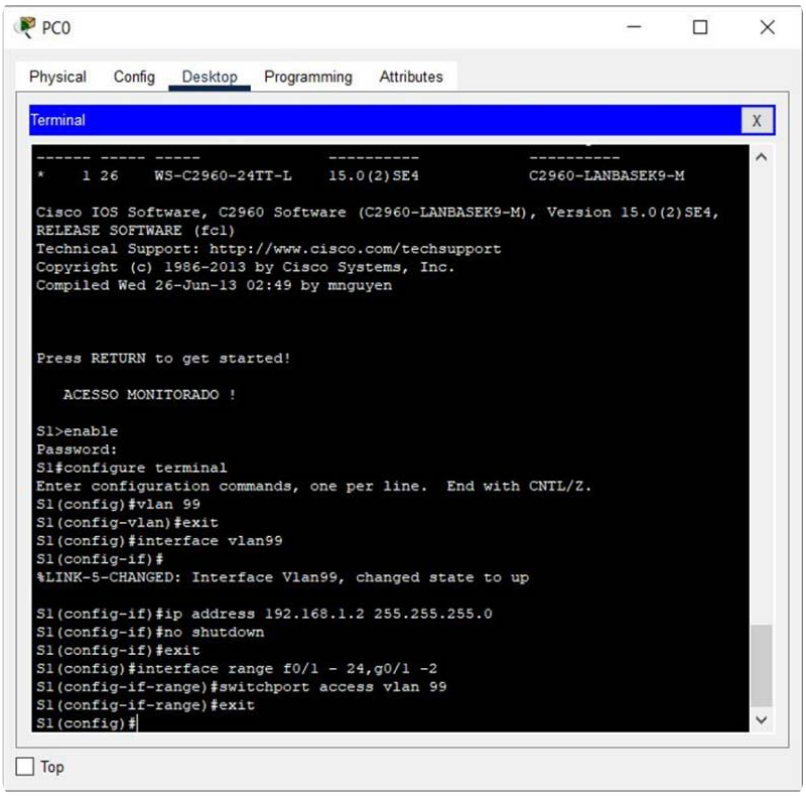
Acompanhe no vídeo o assunto que vamos estudar.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Configuração Básica do Acesso Remoto

Como já dito anteriormente, vamos seguir as recomendações da Cisco e criar uma VLAN para gerenciamento remoto do equipamento. Isso será feito por meio da VLAN 99. A figura a seguir mostra a execução dessa configuração:



Criação da SVI

Os comandos utilizados foram os seguintes:

S1 (config) #vlan 99
Cria a VLAN 99.

S1 (config) #interface vlan99
Entra em modo de configuração de interface.

S1 (config-if) #ip address 192.168.1.2 255.255.255.0
Configura o IP 192.168.1.2/24 na SVI do switch

S1 (config-if) #no shutdown
Coloca a interface em modo operacional.

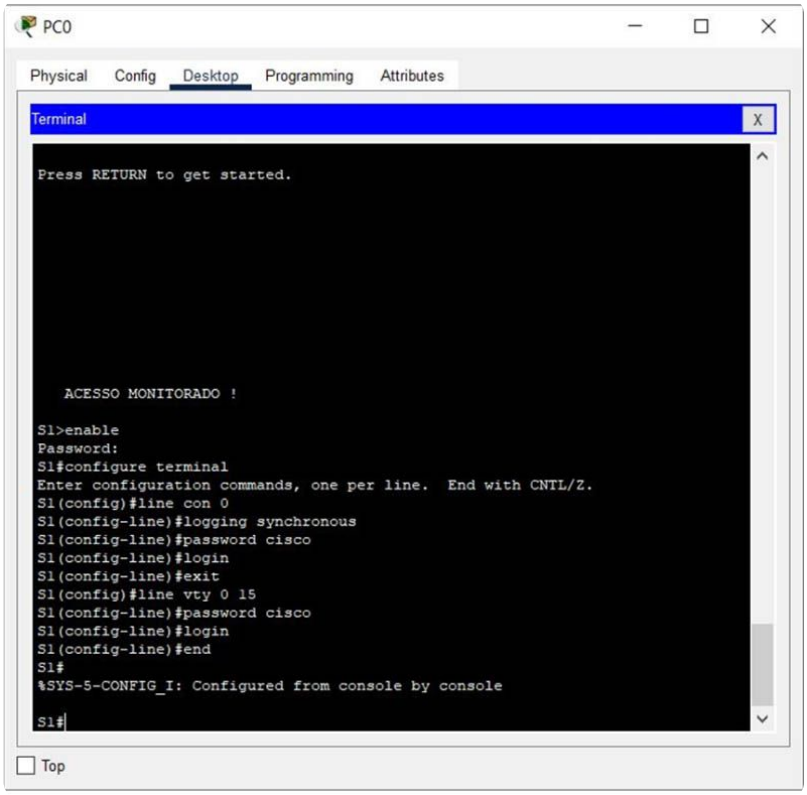
S1 (config-if) #interface range f0/1 - 24,g0/1 -2
Seleciona todas as interfaces do switch para configurar.

S1 (config-if-range) #switchport access vlan 99
Coloca todas as interfaces na VLAN nativa.

Para que o equipamento possa ser remotamente monitorado e acessado, é preciso configurar o endereço do gateway da rede em que ele está instalado. Supondo ser 192.168.1.1, isso é feito por meio do comando abaixo:

S1 (config) #ip default-gateway 192.168.1.1

Agora, precisamos proteger as interfaces de console e vty (*virtual terminal*, usadas com TELNET) com senha. Os passos dessa configuração são os seguintes:



Proteção do acesso via Console e VTY

Os comandos utilizados e seus significados são:

S1 (config) #line con 0
Seleciona a console.

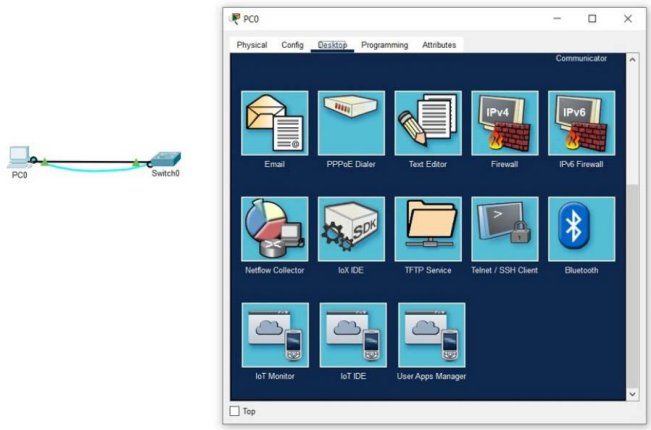
S1 (config-line) #logging synchronous
Impede que mensagens de console interrompam a digitação de comandos.

S1 (config-line) #password cisco
Atribui a *string* "cisco" como senha do acesso via console.

S1 (config-line) #login local
Importante comando! Sem ele, não aparecerá o prompt para digitação de senha.

S1 (config) #line vty 0 15
Seleciona as 16 interfaces vty para configuração.

Com essa configuração, já é possível testar o acesso telnet. Para isso, podemos usar o emulador de cliente Telnet/SSH do *packet tracer*, na aba *"desktop"* do PC. Obviamente, para funcionar, é preciso antes configurar no PC um IP pertencente a mesma rede que o switch, como 192.168.1.10, e ligar um cabo direto (*straight-through*) em uma das interfaces do switch. A figura a seguir ilustra esse cenário:

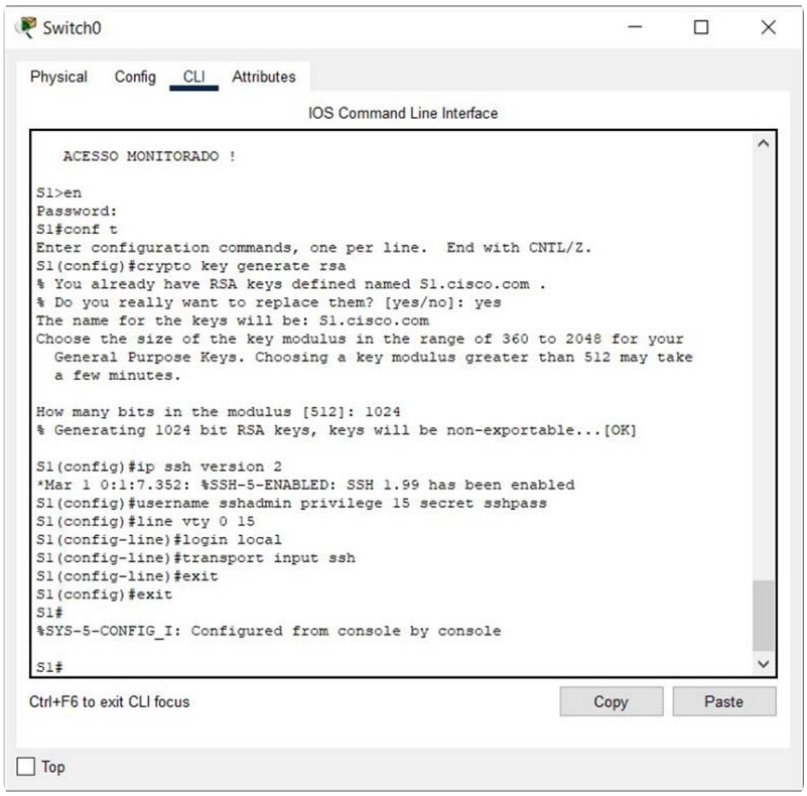


Teste do Acesso Telnet

Ao selecionar o cliente telnet/SSL, basta selecionar o tipo de conexão "Telnet", digitar o IP da SVI do switch, 192.168.1.2, e clicar em *connect*. Será apresentado o prompt para digitação da senha e, caso digitada corretamente, o switch estará conectado ao PC.

Configuração do Acesso SSH e WEB

A configuração do acesso SSH (*Secure Shell*) demanda maior detalhe, uma vez que são necessárias chaves criptológicas assimétricas (RSA). A figura a seguir ilustra o processo:



Configuração do acesso SSH

Antes dessa configuração, é necessário definir o domínio a qual o equipamento pertence. Essa ação é necessária porque as chaves são vinculadas a um equipamento, que é identificado univocamente por meio de um nome de domínio. Ao definir “cisco.com” como domínio, o equipamento passa a ser denominado “s1.cisco.com”.

S1 (config) #ip domain name cisco.com

Os comandos emitidos e suas respectivas ações são:

S1 (config) #crypto key generate rsa
Gerar as chaves RSA. Ao emitir esse comando, o IOS pede o tamanho desejado.

S1 (config) #ip ssh version 2
Uma boa prática é habilitar o ssh 2, mais robusto e versátil.

S1 (config) #username sshadmin privilege 15 secret sshpass
Cria o usuário sshadmin com privilégios de leitura e escrita e senha sshpass encriptada.

S1 (config) #line vty 0 15
Seleciona as interfaces VTY para configurar.

S1 (config-line) #login local
Configura o VTY para autenticação com os dados locais, user sshadmin e senha sshpass.

S1 (config-line) #transport input ssh
Habilita os VTY a permitir o acesso remoto APENAS via SSH.

Com essas configurações, já é possível usar o cliente Telnet/SSH do PC para testar a conexão.

O acesso web é um recurso que não está presente em todos os IOS. As imagens de equipamentos no *Packet Tracer*, no momento da redação deste material, não suportam as opções de configurações necessárias. É importante frisar que isso também pode acontecer com equipamentos reais, demandando atualização do IOS ou a aquisição de módulos de software adicionais.

A configuração do acesso web exige a instalação de um *web server* no switch. Isso é feito por meio dos seguintes passos, em modo de configuração global:

S1 (config) #ip http server
Habilita o servidor web no switch.

S1 (config) #ip http authentication local
Habilita a autenticação por meio das credenciais criadas no switch (usernames e senhas). Outras opções seriam aaa, com o uso do RADIUS ou similar, e ainda enable, que é o método default, usando a senha para acesso EXEC privilegiado.

S1 (config) #ip http port
Definir a porta do servidor (ex.: S1 (config) #ip http port 8080).

Há vários comandos opcionais não ilustrados nessa lista que são dependentes das opções de projeto escolhidas. De uma forma geral, recomenda-se que, por uma questão de segurança, caso se deseje oferecer esta interface para acesso e configuração de equipamentos, isso seja feito de forma protegida, com o uso do https e SSL.

É inegável a importância da preparação dos equipamentos de conectividade com configurações básicas que facilitem a manutenção e a gerência da rede. No próximo módulo, entraremos com mais detalhe nas opções de segurança em switches.

Verificando o aprendizado

Questão 1

Durante a configuração de switches, convém desabilitar a resolução automática de comandos digitados não reconhecidos pelo IOS. Por entender que a *string* digitada pode ser um *hostname*, o switch busca a sua resolução para um endereço IP, bloqueando a interface da CLI para a digitação de novos comandos por alguns segundos. Qual comando podemos usar para desabilitar essa resolução?

A

no ip domain lookup.

B

no domain lookup.

C

no ip lookup.

D

no dns lookup.

E

no lookup.

A alternativa A está correta.

O uso do "no" na frente dos comandos indica a negação do que vem a seguir. As configurações são organizadas em grupos hierárquicos, e a resolução de nomes está dentro do grupo "ip", no grupo "domain".

Questão 2

2. É uma boa prática de segurança restringir o acesso das configurações de equipamentos pertencentes a infraestruturas críticas apenas a usuários autorizados, bem como garantir que o tráfego de gerenciamento seja criptografado e autenticado. Dentre as opções a seguir, qual representa a solução que permite atender a essas boas práticas?

A

TELNET

B

HTTP

C

SSH

D

FTP

E

TFTP

A alternativa C está correta.

O TELNET é uma aplicação insegura por não demandar o uso de senhas nem criptografar o tráfego. O HTTP básico, sem o uso da proteção SSL/TLS, também não protege o tráfego. FTP e TFTP são protocolos de transferência de arquivos, não sendo adequados à atividade ilustrada no enunciado.

O SSH (Secure Shell), por sua vez, por meio da criptografia, protege o tráfego quanto à sua confidencialidade e autenticidade, além de permitir o estabelecimento de métricas para a robustez das senhas de cada usuário autorizado.

Acessando switches de forma segura

Acompanhe no vídeo o assunto que vamos estudar.

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

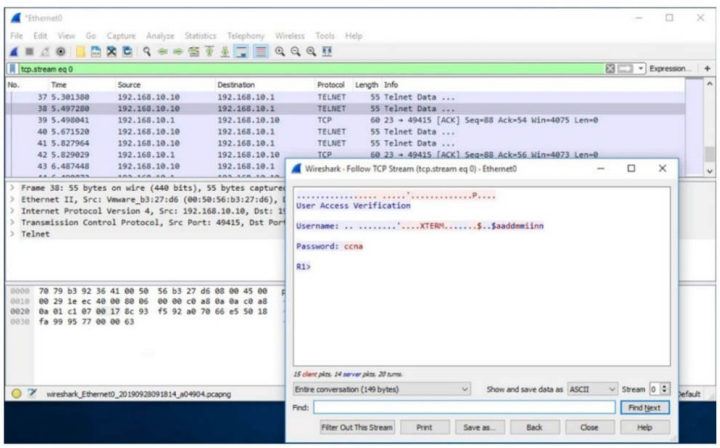
O acesso não autorizado a equipamentos de conectividade pode ser devastador para uma organização. Como todo o tráfego entre as estações e servidores passa por estes equipamentos, a possibilidade de obter o acesso permite, por exemplo, o espelhamento de portas e a consequente captura de toda a informação sensível, além de outras formas do ataque *man-in-the-middle*.

A seguir, vamos descrever importantes ações de *hardening* de switches.

TELNET x SSH

A aplicação TELNET é uma das mais antigas da arquitetura TCP/IP. Quando a segurança ainda não era uma preocupação visível, grande parte do esforço de configuração e gerenciamento remoto de equipamentos era feito por meio da porta TCP 23. Com a evolução das redes e a migração de negócios para a internet, agentes mal-intencionados passaram a explorar as vulnerabilidades dos protocolos e aplicações em uso, e o TELNET passou a ser evitado.

A razão disso é que o TELNET não encripta o tráfego, e para autenticação usa *strings* passadas em claro para conferência no servidor. A figura a seguir ilustra uma captura de uma conexão TELNET:

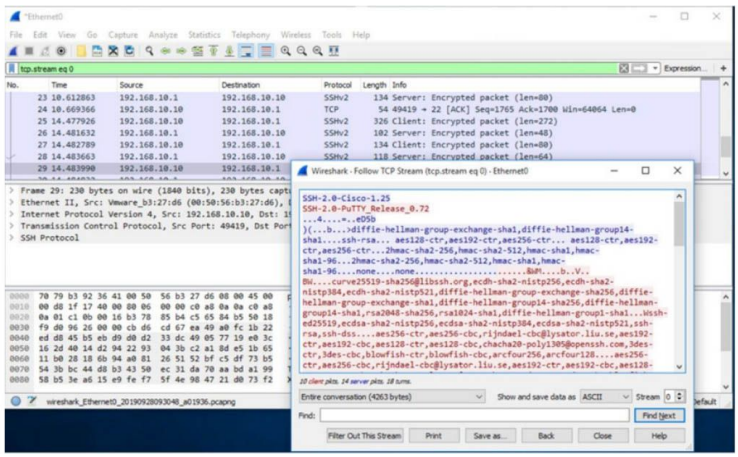


Conexão TELNET capturada

A inspeção da mensagem TCP de login foi capturada, e podemos ver o *username* (admin) e a senha (ccna).

O SSH é um substituto para o TELNET, com a resolução de suas lacunas: a criptografia do tráfego e a autenticidade para as mensagens, bem como a autenticação no acesso com base em chaves RSA. Com isso, todas as mensagens trocadas entre um cliente e um servidor SSH instalado em um switch estarão criptografadas e autenticadas.

A figura a seguir ilustra a captura de um acesso SSH:



Conexão SSH capturada

É possível perceber que, na captura do tráfego SSH, não é possível ler nada além dos cabeçalhos, que não tornam a comunicação insegura. Todo o conteúdo das mensagens, que inclui logins e senhas, está encriptado.

A Cisco recomenda a substituição do TELNET pelo SSH, desabilitando a possibilidade de acessos TELNET. Os comandos para a configuração dos tipos de acesso remoto permitidos são os seguintes, sempre em EXEC privilegiado e do modo de configuração global:

S1 (config) #line vty 0 15
Entra no modo de configuração de VTY.

S1 (config-line) #transport input all
Permite TELNET e SSH.

S1 (config-line) #transport input none
Não permite nenhum.

S1 (config-line) #transport input telnet
Apenas permite TELNET.

S1 (config-line) #transport input ssh
Apenas permite SSH (opção recomendada).

S1 (config-line) #login local
Apresenta prompt para digitação de usuário e senha.

A implementação de **recursos de segurança em equipamentos de conectividade é de extrema importância**, principalmente por serem dispositivos de rede não monitorados com a mesma atenção que servidores e estações. No próximo tópico, vamos nos aprofundar mais no uso da VLAN de gerência.

Acesso WEB seguro

Conforme já descrito anteriormente, o acesso web não é o mais utilizado para gerência e configuração de equipamentos, principalmente pela demanda de módulos de software, nem sempre disponíveis nos equipamentos. Caso seja um requisito de projeto, é importante se assegurar que:

- O serviço HTTP esteja desabilitado, permitindo apenas https.
- O método de autenticação escolhido esteja compatível com os requisitos de projeto (aaa, enable ou local).
- Que esteja em uso o módulo SSL 3.0.

Também é importante seguir as instruções de configuração próprias de cada fabricante/modelo, já que há diferenças entre as implementações.

Configurações de segurança costumam ser deixadas por último, e tipicamente não fazem parte do projeto de rede. Convém integrar as demandas de segurança básicas e específicas de cada negócio ao projeto, de forma a alcançar equilíbrio entre desempenho e segurança. Conhecer os recursos disponíveis é parte fundamental no processo de criação de ambientes estáveis, escaláveis e seguros.

Criando uma VLAN de gerência

Acompanhe no vídeo o assunto que vamos estudar.



Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Switches são equipamentos de camada de enlace em que se pode usar o importante recurso de segregação de domínios de *broadcast*, chamado VLAN (*Virtual Lan*). Por meio do uso de uma TAG 802.1Q - padrão IEEE ou ISL (Proprietária Cisco), os quadros ethernet passam a ser identificados como “pertencentes” a uma determinada VLAN, restringindo o alcance desse quadro para encaminhamento L2 apenas às portas pertencentes à mesma VLAN.

> Caso o destino do quadro pertença a outra VLAN, será necessário um processo de nível de rede (L3), envolvendo um switch L3 ou um roteador.

Quando a rede não está organizada em VLANs, todas as portas pertencem nativamente à VLAN padrão, a VLAN 1. Os quadros desta VLAN não recebem TAGs, de forma que, em um equipamento não gerenciável, todos os quadros possam trafegar por todas as interfaces. A rigor, não há um risco intrínseco em haver uma VLAN 1, mas sim em possibilitar que portas de acesso pertençam a esta VLAN.

Dispositivos podem ser conectados a essas portas e, caso a porta esteja disposta a formar tronco automaticamente - situação DEFAULT em switches Cisco -, pode ser a “brecha” para um ataque. Obviamente, em switches em que todas as estações estão na VLAN 1, não há segregação, e qualquer quadro pode ser capturado com o uso de técnicas de ataque apropriadas.

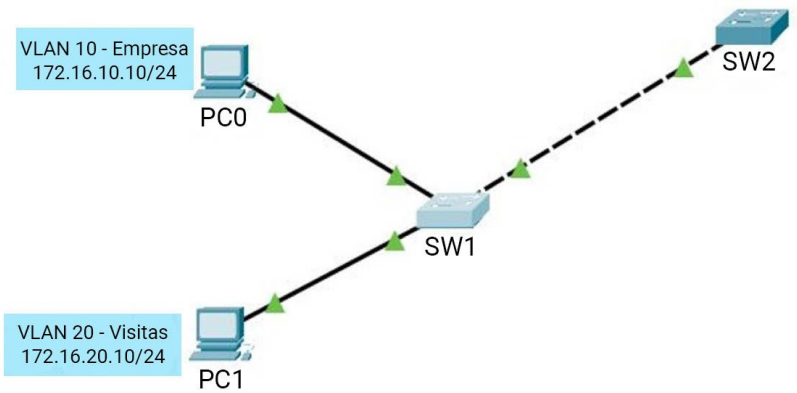
Comentário

Equipamentos de conectividade não pertencem a nenhuma VLAN, mas geram tráfego importante, como, por exemplo, do protocolo STP, importante para evitar loops nas redes. Em switches Cisco, outros protocolos importantes como VTP, DTP, CDP e outros também usam esta VLAN para a troca de mensagens.

Ataques de negação de serviço automatizados podem paralisar rapidamente redes Cisco, direcionando tráfego à VLAN nativa. A captura de tráfego desta VLAN também pode permitir a obtenção de informações importantes para um ataque direcionado (*Fingerprint Hacking*).

Por conta disso, uma primeira e importante ação é criar outra VLAN para suportar este tráfego como VLAN nativa, bem como configurar as portas cujas estações possam vir a ser conectadas em modo de acesso. A VLAN nativa será usada exclusivamente para o tráfego de gerenciamento, e as demais VLANs para o tráfego de dados entre as estações.

Para ilustrar, vamos acompanhar a implementação da VLAN de gerência no cenário a seguir:



Implementação de VLAN Nativa

Este cenário está segregado em duas VLANs, mas ainda usa a VLAN padrão (VLAN 1), conforme pode ser visto na saída do comando a seguir, emitido para a interface tronco do SW1 (g0/1):

SWI# show interface g0/1 switchport

```
SW1#sh interface g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

VLAN nativa default (VLAN 1)

Para substituir a VLAN nativa por outra, é importante observar que isso deverá ser feito em toda a topologia, evitando erros do tipo Native VLAN mismatch.

Em cada Switch, a SVI receberá um IP da VLAN escolhida. No nosso exemplo, VLAN 99, dentro do *range* 172.16.99.0/24. Adicionalmente, vamos alterar a VLAN nativa nos troncos.

Em SW1

SW1 (config) #vlan 99

SW1 (config-vlan) #name Gerencia

SW1 (config-vlan) #interface vlan 99

SW1 (config-if) #ip address 172.16.99.1 255.255.255.0

SW1 (config-if) #no shutdown

SW1 (config-if) #interface g0/1

SW1 (config-if) #switchport trunk native vlan 99.

Em SW2

SW2 (config) #vlan 99

SW2 (config-vlan) #name Gerencia

SW2 (config-vlan) #interface vlan 99

SW2 (config-if) #ip address 172.16.99.2 255.255.255.0

SW2 (config-if) #no shutdown

SW2 (config-if) #interface g0/1

SW2 (config-if) #switchport trunk native vlan 99

Com estes comandos em ambos os switches, criamos uma VLAN atípica (VLAN 99) para o gerenciamento da rede. A figura a seguir mostra a VLAN 99 como nativa para o tronco:

```
SW1#sh int g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Gerencia)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

VLAN de Gerência Alterada para VLAN 99

Outra importante medida de segurança, além das já discutidas, é a proteção das portas, que será apresentada no próximo tópico.

Controle de acesso às portas físicas

Acompanhe no vídeo o assunto que vamos estudar.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Proteção de Portas

É fato que ataques a equipamentos de camada 2, como switches, podem ser difíceis de serem garantidamente evitados, bem como que seus efeitos na rede podem ser devastadores. Além de serem ataques relativamente simples, estes equipamentos são fisicamente acessíveis para o pessoal de suporte, convindo, portanto, ações de natureza lógica para sua proteção.

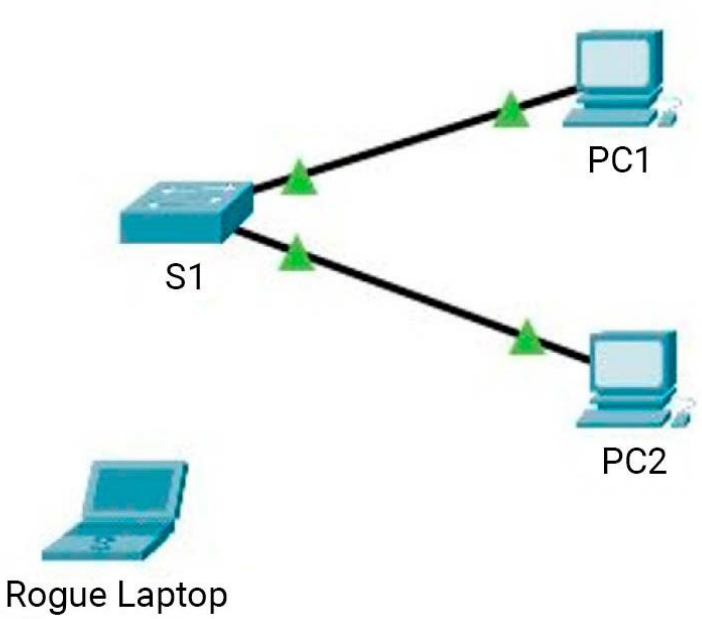
Uma ação muito simples, mas pouco adotada, é a **desativação de portas que não estejam em uso**. A reversão desta ação depende de acesso privilegiado ao equipamento, representando assim uma camada de segurança e, consequentemente, um obstáculo a mais para os agentes mal-intencionados.

> Um ataque amplamente documentado é a inundação da tabela CAM *(Content Addressable Memory)* com endereços MAC fictícios. Se o switch não consegue "aprender" os endereços MAC das estações da rede, comutará os quadros para todas as suas demais portas, representando um risco real de comprometimento do desempenho da rede e possibilitando a captura de tráfego de todas as estações.

A ideia do mecanismo de segurança de portas é definir quais MAC *Addresses* podem se conectar a portas de switch, restringindo a superfície de ataque apenas a máquinas conhecidas.

Conforme já dito, técnicas de ataque adicionais podem ser usadas para a descoberta de endereços autorizados, e técnicas de *spoofing* podem falsificar quadros com o uso destes endereços, mas a camada adicional de segurança e a maior complexidade do ataque para obter sucesso em um ambiente protegido pela segurança de portas tornam o mecanismo uma boa prática inegável.

Para ilustrar, vamos usar o cenário a seguir. Duas estações de trabalho legítimas (PC1 e PC2) estão conectadas por meio de S1, e um *laptop* mal-intencionado (*Rogue Laptop*) será usado para demonstrar a proteção.



Cenário para Port-Security

Após receber os primeiros quadros de PC1 e PC2, S1 aprende os respectivos MAC Addresses e os associa às portas onde estão conectados. Caso não haja segurança de portas, bastaria conectar fisicamente o dispositivo malicioso ao switch.

A figura a seguir ilustra a tabela CAM de S1:

```
S1#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.647c.697e    DYNAMIC      Fa0/2
   1    00e0.b027.2245    DYNAMIC      Fa0/1
```

CAM Table de S1

Para proteção das portas, o primeiro passo é ativar o *port-security* onde desejado, e definir as opções.

```
S1(config)#int range f0/1 - 2
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
  <cr>
```

Configuração de Port-Security

A seguir, é necessário parametrizar a segurança desejada. As opções são as listadas a seguir:

aging – tempo de duração da associação entre MAC *address* e porta.

Usa o seguinte formato:
S1 (config-if-range) #switchport port-security aging {static | time | type {absolute | inactivity}}

Os parâmetros da opção **aging** possuem o seguinte significado:

- *Static* – habilita um prazo de duração para endereços configurados estaticamente na porta;
- *Time* – tempo de duração da associação, de 0 a 1440 minutos. O "0" (zero) indica que não há prazo de vencimento estabelecido;
- *Type* – Pode ser de dois tipos:
  - *absolute* – o tempo de vencimento é contado desde a sua concessão; ou
  - *inactivity* – o tempo é contado apenas em estado de inatividade da porta, só expirando se o tempo de inatividade alcançar o valor especificado no parâmetro time.

Mac *address* – Há três formas possíveis de aprendizado do mac *address* pela *port-security:*

- Dinamicamente aprendida – quando o port security é configurado em uma porta, automaticamente ele "aprende" o mac address já conectado a ela;
- Dinamicamente aprendida – sticky – a porta fica preparada para "aprender" o mac address da estação conectada a ela, tornando-o como estático para a porta após a gravação da configuração em execução;
- Manualmente configurada, por meio da digitação do mac address da estação autorizada para a porta.

Maximum – define o número máximo de mac *addresses* que podem ser configurados para uma porta. O default é "1".

Violation – define a ação a tomar em caso de violação. Configurado por meio do comando a seguir:

S1 (config-if-range) #switchport port-security violation {protect | restrict | shutdown}

O efeito destas opções são os seguintes (CISCO, 2021):

- *Shutdown* – A porta passa imediatamente para o estado desabilitado por erro, desativa o LED da porta e envia um alerta ao syslog. Incrementa o contador de violação. Para reabilitar a porta, o administrador precisa usar os comandos *shutdown/no shutdown*;
- *Restrict* – A porta descarta pacotes com endereços de origem MAC desconhecidos até que o número máximo de endereços MAC seja atendido. Esse modo incrementa-se do contador de violações e gera uma mensagem no syslog;
- *Protect* – A porta descarta pacotes com endereços de origem MAC desconhecidos da mesma forma que o modo *restrict*, porém não registra nada no contador nem no syslog.

Em resumo, as principais diferenças entre estas opções são (CISCO, 2021):

Modo	Descarta tráfego	Registro SYSLOG	Registro Contador	Bloqueia porta
Protect	SIM	NÃO	NÃO	NÃO
Restrict	SIM	SIM	SIM	NÃO
Shutdown	SIM	SIM	SIM	SIM

Opções de configuração de política de Port-security
Cisco, 2021

Dando continuidade ao exemplo, vamos configurar as duas portas como *sticky*, no máximo um mac *address* por porta, e política de violação que não desabilita as portas em caso de ataque, mas será gerada uma notificação de ocorrência, e os quadros, descartados – modo RESTRICT.

```
S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/1 - 2
S1(config-if-range)#switchport port
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#switchport port-security mac-address sticky
S1(config-if-range)#switchport port-security violation restrict
```

Configuração do Port-Security

Além disso, como boa prática complementar, convém desabilitar as portas que não estejam em uso.

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

S1 (config-if-range) #shutdown

Para testar as opções configuradas, primeiro vamos observar a configuração em memória volátil:

```
S1#show run | begin interface
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
```

Print de um trecho do arquivo de configuração em execução ainda sem os MACs

É possível observar as configurações em ambas as interfaces, aguardando o aprendizado dos endereços MAC das estações. Para isso, fazemos um “ping” de uma estação para a outra, e logo a seguir, ao verificar o conteúdo da running-config, temos o seguinte:

```
S1#show run | begin interface
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.B027.2245
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.647C.697E
```

Print de um trecho do arquivo de configuração em execução com os MACs

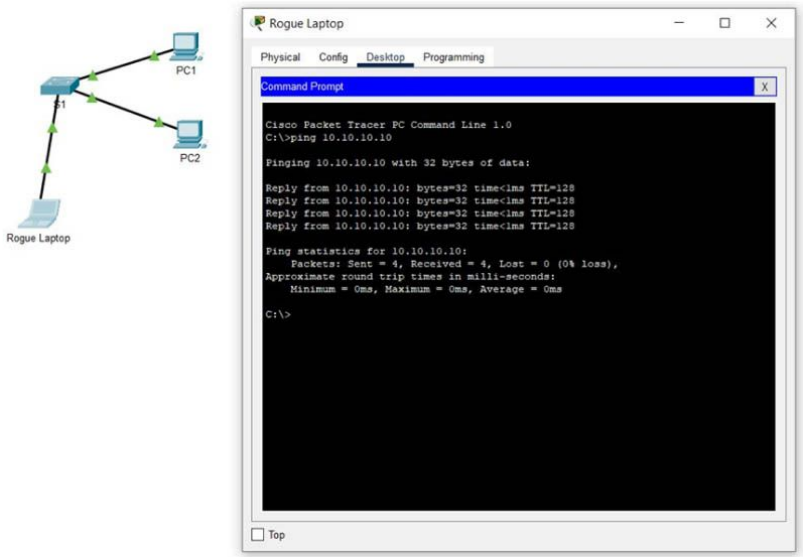
Ou seja, os endereços MAC foram aprendidos e associados às respectivas interfaces. Para assumir estes endereços como estáticos, basta gravar o conteúdo da running-config na startup-config – memória NVRAM, não volátil.

Os comandos a seguir permitem observar mais detalhes da proteção:

```
S1#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
------------------------------------------------------------------------
        Fa0/1        1          1                0         Restrict
        Fa0/2        1          1                0         Restrict
------------------------------------------------------------------------
S1#show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    00E0.B027.2245    SecureSticky                  Fa0/1        -
   1    0001.647C.697E    SecureSticky                  Fa0/2        -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

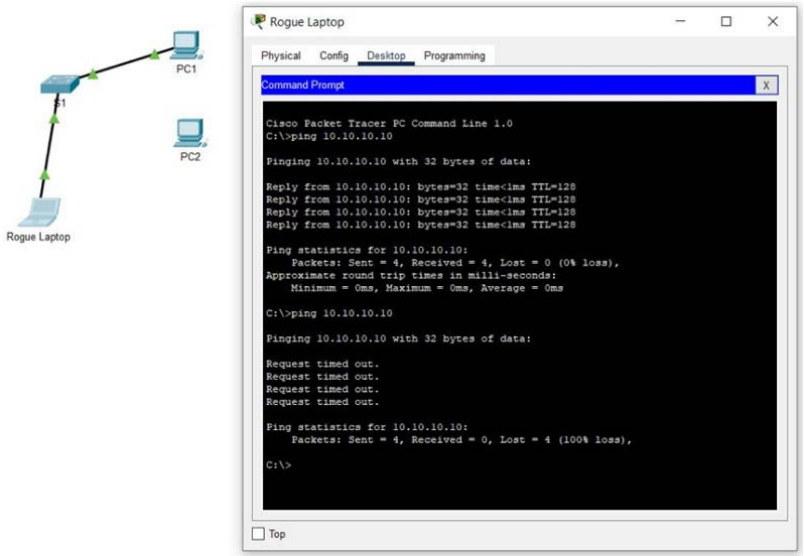
Print das configurações de Port-Security em execução

Agora vamos testar a proteção. A conexão física, seguida da reabilitação da porta onde ele foi conectado, permite acesso normal.



Teste de PING

Agora, vamos conectar o *Rogue Laptop* à porta de PC2, e tentar “pingar” PC1.



Teste de PING

Com as configurações realizadas, o ping foi malsucedido, tendo sido geradas contagens de violação, uma para cada requisição ping (4 ao todo), além de ultrapassar o número máximo de endereços por interface (1).

Também pode ser visto o endereço MAC da estação que descumpriu a política na entrada *Last Source Address*.

```
S1#show port-security interface f0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0002.4A42.C51C:1
Security Violation Count   : 5
```

Print do status do Port-Security

Como se pode ver na prática, a segurança de porta é um recurso simples e útil, porém pouco utilizado em projetos de redes.

Ação do Port Security em um cenário de rede

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Durante a configuração de Switches, um erro comum é o esquecimento de comandos vitais para o funcionamento desejado. Qual é o comando que, caso seja esquecido, impedirá a apresentação de um prompt no acesso remoto via console, telnet ou ssh?

A

Login

B

Show

C

Display

D

Prompt

E

Enable

A alternativa A está correta.

O comando **login** é usado para controlar o acesso ao equipamento. No caso de VTY, podem ser usadas as seguintes opções sem o uso de AAA:

• no login (console ou VTY) – Não é requisitada senha para o acesso Console ou VTY;

• login e password xxx (console ou VTY) – Essa senha deve ser digitada para o acesso (apenas);

• login local (console ou VTY), username xxx e password yyy (nas configurações globais) – O nome de usuário e uma senha serão requisitados no acesso; ou

• login **tacacs** (console ou VTY) e tacacs-server host x.x.x.x (nas configurações globais) – um servidor tacacs usado para autenticação.

Sem a digitação do comando **login**, não aparecerá prompt para digitação de login e/ou senha, apesar da mesma ser necessária. Os demais comandos possuem outras funções, como o show e o enable, ou não existem nesse contexto – **display** e **prompt**.

Questão 2

O Port-Security é um importante recurso para proteção dos equipamentos de conectividade quanto à anexação de dispositivos não-autorizados. Caso a política de violação seja configurada como RESTRICT, como o sistema vai se comportar, respectivamente, quanto às seguintes ações?

I – Bloqueia porta (sim/não)

II – Registra SYSLOG (sim/não)

III – Registra contador (sim/não)

IV – Descarta tráfego (sim/não)

A

I – sim, II – sim, III – sim, IV - não

B

I – não, II – sim, III – sim, IV - sim

C

I – sim, II – não, III – sim, IV - não

D

I – sim, II – sim, III – não, IV - não

E

I – não, II – sim, III – sim, IV - não

A alternativa B está correta.

No modo RESTRICT, a porta descarta pacotes com endereços de origem MAC desconhecidos até que o número máximo de endereços MAC seja atendido, mas sem bloquear a porta. Esse modo incrementa do contador de violações e gera uma mensagem no syslog.

Considerações finais

A dependência crescente dos recursos computacionais nos processos produtivos traz consigo a demanda de redes seguras, escaláveis e com alta disponibilidade. A tomada de decisão nas empresas tipicamente depende do acesso rápido a informações, e as redes possuem papel fundamental nisso.

Para projetistas de redes, o uso de técnicas que garantam maior segurança e gerenciabilidade não é um opcional, e sim um requisito alcançado com o uso de boas práticas. Conhecer e aplicar técnicas de segurança são de inegável importância.

Nesse contexto, apresentamos técnicas de configuração de switches, especialmente recursos de segurança, descrevendo suas características e ilustrando com exemplos.

Podcast

Para encerrar, ouça mais sobre a importância de se adotar boas práticas na configuração de switches.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Para exercitar a configuração básica de switches, acesse o ambiente virtual do Packet Tracer da Cisco e procure reproduzir as experiências demonstradas neste material.

Referências

CISCO SYSTEMS. **CCNA Routing, Switching and Wireless Essentials 7.02**. Consultado na Internet em: 15 dez. 2021.

JUNIPER NETWORKS. **O que é a metro ethernet**. Consultado na Internet em: 19 abr. 2022.