O que é a Configuração VTY?

VTY significa Virtual Teletype. Em termos simples, são linhas de acesso virtuais que permitem conexões remotas *para dentro* do switch (ou roteador) usando protocolos como Telnet e SSH.

Pense no switch como um servidor que pode aceitar várias sessões de administração remota ao mesmo tempo. Cada sessão aberta por um administrador ocupa uma dessas linhas VTY.

* Virtual: Diferente da console física (porta RJ-45 azul), não existe um conector físico específico para cada sessão VTY.
* Teletype: Um termo histórico que se refere a um terminal de texto.

Em resumo: A VTY é a "porta da frente" para o gerenciamento remoto do seu switch.

Para que serve a Configuração VTY?

A principal finalidade é permitir que um administrador de rede configure, monitore e solucione problemas do switch a partir de um local remoto, sem a necessidade de estar fisicamente conectado à porta de console.

As funções específicas incluem:

1. Habilitar o Acesso Remoto: Sem a configuração VTY, você só pode gerenciar o switch via cabo de console. Configurando as linhas VTY, você ativa a capacidade de o switch aceitar conexões Telnet e/ou SSH pela rede.
2. Gerenciamento Simultâneo: A maioria dos switches Cisco suporta múltiplas linhas VTY (por exemplo, de 0 a 15), permitindo que vários administradores se conectem ao mesmo tempo.
3. Controlar o Método de Acesso: Você pode definir quais protocolos são permitidos (apenas SSH, apenas Telnet ou ambos). É uma prática de segurança altamente recomendável usar apenas SSH, pois o Telnet transmite todas as informações (incluindo senhas) em texto puro.
4. Implementar Segurança: A configuração VTY é onde você aplica medidas de segurança críticas para o acesso remoto:
   * Senha de Login: Define uma senha obrigatória para acessar o modo de execução do usuário.
   * Autenticação Local ou por AAA: Pode usar um nome de usuário e senha configurados localmente no switch ou em um servidor externo (como TACACS+ ou RADIUS) para uma segurança mais robusta.
   * ACLs (Access Control Lists): Restringe quais endereços IP ou redes têm permissão para estabelecer uma sessão VTY com o switch. Isso é vital para impedir que usuários não autorizados tentem acessar o dispositivo.
   * Timeout de Inatividade: Configura um tempo de espera após o qual uma sessão ociosa será automaticamente desconectada.

*Me dê um exemplo de uma configuração de um switch cisco desde sua nomeção até a configuração vty e como entrar de forma remota no*

Vou fornecer um exemplo completo de configuração de um switch Cisco, desde o início até o acesso remoto via SSH.

Conexão Inicial e Configuração Básica

! Conecte-se via cabo de console na porta Console do switch

Switch> enable

Switch# configure terminal

! Configuração básica de identificação

Switch(config)# hostname SW-Office01

SW-Office01(config)# ip domain-name empresa.com

SW-Office01(config)# banner motd #

AVISO: Acesso Autorizado Somente!

#

! Configuração de senhas básicas

SW-Office01(config)# enable secret SenhaEnable123!

SW-Office01(config)# service password-encryption

Configuração de IP Management (VLAN de Gerência)

! Criar VLAN de gerenciamento

SW-Office01(config)# vlan 99

SW-Office01(config-vlan)# name MANAGEMENT

SW-Office01(config-vlan)# exit

! Atribuir IP à VLAN de gerenciamento

SW-Office01(config)# interface vlan 99

SW-Office01(config-if)# ip address 192.168.99.10 255.255.255.0

SW-Office01(config-if)# no shutdown

SW-Office01(config-if)# exit

! Configurar gateway padrão

SW-Office01(config)# ip default-gateway 192.168.99.1

Configuração de Segurança e Usuários

! Criar usuário para acesso remoto

SW-Office01(config)# username admin privilege 15 secret SenhaAdmin123!

SW-Office01(config)# username operador privilege 5 secret SenhaOperador456!

! Configurar logging e timestamp

SW-Office01(config)# logging buffered 8192

SW-Office01(config)# no ip domain-lookup

SW-Office01(config)# line console 0

SW-Office01(config-line)# logging synchronous

SW-Office01(config-line)# exec-timeout 5 0

SW-Office01(config-line)# exit

Configuração VTY para Acesso Remoto SSH

! Gerar chaves RSA para SSH (mínimo 1024 bits, recomendado 2048)

SW-Office01(config)# crypto key generate rsa modulus 2048

! Configurar as linhas VTY

SW-Office01(config)# line vty 0 15

SW-Office01(config-line)# transport input ssh ! Aceita apenas SSH

SW-Office01(config-line)# login local ! Autenticação por usuário local

SW-Office01(config-line)# exec-timeout 10 0 ! Timeout de 10 minutos

SW-Office01(config-line)# logging synchronous

SW-Office01(config-line)# end

Configurações Adicionais de Segurança

SW-Office01# configure terminal

! Configurar SSH mais seguro

SW-Office01(config)# ip ssh version 2

SW-Office01(config)# ip ssh time-out 60

SW-Office01(config)# ip ssh authentication-retries 2

! (OPCIONAL) Criar ACL para restringir acesso por IP

SW-Office01(config)# ip access-list standard ACL-SSH-MGMT

SW-Office01(config-std-nacl)# permit 192.168.99.0 0.0.0.255

SW-Office01(config-std-nacl)# deny any

SW-Office01(config-std-nacl)# exit

! Aplicar ACL nas linhas VTY

SW-Office01(config)# line vty 0 15

SW-Office01(config-line)# access-class ACL-SSH-MGMT in

SW-Office01(config-line)# end

Salvar a Configuração

SW-Office01# copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

SW-Office01#

Continua...

Como Conectar Remotamente no Switch

Método 1: Via SSH (Recomendado)

No Windows (Prompt de Comando ou PowerShell):

ssh [admin@192.168.99.10](mailto:admin@192.168.99.10)

No Linux/macOS (Terminal):

Saída esperada:

Password: (digite "SenhaAdmin123!")

SW-Office01>

Resumo do Processo de Conexão Remota

Fisicamente: Switch conectado na rede com IP 192.168.99.10

Na rede: Cliente precisa estar na rede 192.168.99.0/24 (devido à ACL)

No cliente: Usar comando SSH com IP do switch

Autenticação: Usar usuário e senha configurados

Acesso: Conectado no modo EXEC do switch

Esta configuração fornece um ambiente seguro e funcional para gerenciamento remoto do switch Cisco!