Análise Técnica da Configuração do Switch Cisco

Comandos de Modo de Execução e Sistema

* **enable**: Transfere o operador do modo EXEC usuário para o modo EXEC privilegiado, permitindo acesso a comandos de configuração e diagnóstico.
* **clock set 20:20:00 10 October 2025**: Define o relógio interno do sistema com data e hora específicas para precisão em registros de log e certificados.
* **configure terminal**: Acessa o modo de configuração global, permitindo modificações na configuração do sistema.

Comandos de Identificação e Logging

* hostname sw-02: Estabelece o identificador do dispositivo na rede como "sw-02".
* service password-encryption: Aplica criptografia básica a todas as senhas em texto simples no arquivo de configuração.
* service timestamps log datetime msec: Configura os registros de log para incluir data, hora e milissegundos em cada entrada.
* logging buffered 4096: Aloca um buffer de 4096 bytes na memória para armazenamento temporário de mensagens de log.
* no ip domain-lookup: Desativa a funcionalidade de resolução DNS para termos digitados incorretamente no CLI.

Comandos de Segurança e Autenticação

* banner motd #Vivian Coimbra LGPD#: Define um banner de aviso legal que é exibido antes do login, referenciando a Lei Geral de Proteção de Dados.
* enable secret 123@senac: Configura uma senha criptografada para acesso ao modo EXEC privilegiado.
* username senac secret 123@senac: Cria um usuário "senac" com senha criptografada usando o algoritmo SHA-256.
* username tatuape password 123@senac: Cria um usuário "tatuape" com senha em texto simples (será criptografada pelo serviço password-encryption).
* username admin privilege 15 secret 123@senac: Define um usuário administrativo com privilégio máximo (nível 15) e senha criptografada.

Comandos de Segurança de Rede

* no cdp run: Desativa globalmente o Cisco Discovery Protocol, prevenindo troca de informações com dispositivos vizinhos.
* no lldp run: Desativa globalmente o Link Layer Discovery Protocol, adicionalmente prevenindo descoberta por dispositivos vizinhos.

Configuração de Linhas de Acesso

* line console 0: Acessa o modo de configuração para a porta console física.
  + login local: Habilita autenticação usando o banco de usuários locais.
  + password 123@senac: Define senha específica para acesso via console.
  + logging synchronous: Sincroniza a exibição de mensagens de log para não interferir na digitação.
  + exec-timeout 5 30: Configura timeout de 5 minutos e 30 segundos para sessões ociosas.
* line vty 0 4: Configura as cinco primeiras linhas virtuis para acesso remoto.
  + login local: Requer autenticação via banco de usuários local.
  + password 123@senac: Define senha para acesso VTY.
  + exec-timeout 5 30: Estabelece timeout de inatividade para sessões remotas.
  + transport input ssh: Restringe acesso apenas ao protocolo SSH, bloqueando Telnet.
  + logging synchronous: Mantém a interface de usuário sincronizada durante sessões remotas.

Configuração de Interface de Rede

* ip default-gateway 192.168.1.254: Define o gateway padrão para dispositivos de camada 2.
* interface vlan 1: Acessa a configuração da interface virtual da VLAN 1.
  + description Interface de SVI: Adiciona descrição textual para documentação.
  + ip address 192.168.1.251 255.255.255.0: Atribui endereço IPv4 e máscara de sub-rede.
  + no shutdown: Administrativamente ativa a interface.

Configuração do Serviço SSH

* ip domain-name [senac.br](https://senac.br/): Define o domínio FQDN para o dispositivo, necessário para geração de chaves criptográficas.
* crypto key generate rsa general-keys modulus 1024: Gera par de chaves RSA com módulo de 1024 bits para criptografia SSH.
* ip ssh version 2: Força a utilização exclusiva da versão 2 do protocolo SSH.
* ip ssh time-out 60: Define o tempo máximo de inatividade permitido para sessões SSH.
* ip ssh authentication-retries 2: Limita para duas tentativas de autenticação por sessão SSH.

Comandos Finais de Sistema

* end: Sai do modo de configuração e retorna ao modo EXEC privilegiado.
* write: Salva a configuração atual na memória não volátil (NVRAM), garantindo persistência após reinicialização.

Esta configuração estabelece um ambiente operacional seguro com autenticação local, acesso remoto criptografado via SSH, e políticas básicas de segurança implementadas. O switch estará acessível remotamente através do endereço IP 192.168.1.251 na VLAN 1, com controle de acesso baseado em usuários locais e timeout de sessão configurado.