Zdalny dostęp do przełącznika.

Wprowadzenie.

Protokół SSH powinien zastąpić Telnet przy zarządzaniu połączeniami. Telnet przesyła dane w postaci niezabezpieczonej - jawnym tekstem. SSH zapewnia bezpieczeństwo zdalnych połączeń szyfrując wszystkie dane transmitowane pomiędzy urządzeniami.

W celu zarządzania przełącznikiem konfigurujemy ustawienia IP. Adres IP nie jest przypisywany do interfejsu fizycznego, lecz wirtualnego w wybranej sieci VLAN (wirtualnej sieci lokalnej). VLAN 1 jest niezalecany przez Cisco ze względów bezpieczeństwa.

interface vlan 100

ip address <adres_IP> <maska_podsieci>

no shutdown

Adres bramy domyślnej podaje się w trybie konfiguracji globalnej.

ip default-gateway <adres_bramy>

Domyślne SSH korzysta z pary kluczy prywatny-publiczny o nazwie będącej połączeniem nazwy i domeny routera.

- Konfiguracja nazwy hosta za pomocą polecenia.

hostname <nazwa>

- Konfiguracja nazwy domeny za pomocą polecenia.

ip domain-name <nazwa_domeny>

SSH korzysta z linii VTY, a logowanie musi odbywać się z wykorzystaniem nazwy użytkownika i hasła:

username <login> secret <hasło>

line vty 0 4

login local

Wygenerowanie pary kluczy RSA za pomocą polecenia (zalecana minimalna długość klucza to 1024 bitów).

crypto key generate rsa

Wyłączenie możliwości logowania się przez telnet:

line vty 0 4

transport input ssh

Ode wersji 12.3(4)T wsparcie dla SSH-2 – należy włączyć (obecnie SSH w wersji 1 nie jest uznawana za bezpieczną)

ip ssh version 2

Do wyświetlania informacji o stanie serwera SSH służą polecenia:

show ip ssh

show ssh

Logowanie się z komputera do urządzenia:

ssh -l <użytkownik> <adres-ip-urządzenia-ssh >

-l (literka l jak login)