Packet Tracer – Zadanie integrujące umiejętności

Topologia

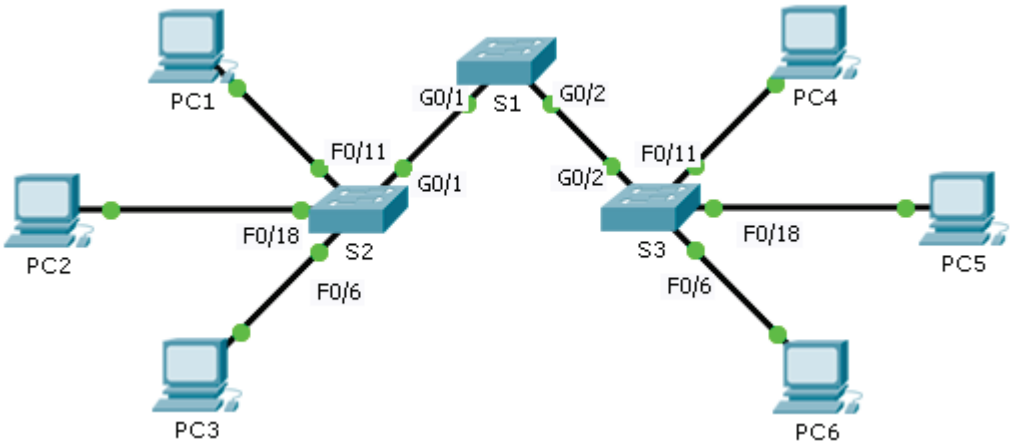

Tabela adresowania

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
S1	VLAN 88	172.31.88.2	255.255.255.0	172.31.88.1
S2	VLAN 88	172.31.88.3	255.255.255.0	172.31.88.1
S3	VLAN 88	172.31.88.4	255.255.255.0	172.31.88.1
PC1	Karta sieciowa	172.31.10.21	255.255.255.0	172.31.10.1
PC2	Karta sieciowa	172.31.20.22	255.255.255.0	172.31.20.1
PC3	Karta sieciowa	172.31.30.23	255.255.255.0	172.31.30.1
PC4	Karta sieciowa	172.31.10.24	255.255.255.0	172.31.10.1
PC5	Karta sieciowa	172.31.20.25	255.255.255.0	172.31.20.1
PC6	Karta sieciowa	172.31.30.26	255.255.255.0	172.31.30.1

Tabela przyporządkowania sieci wirtualnych VLAN i portów

Porty	Przyporządkowanie	Sieć
F0/7 - 12	VLAN 10 - Sprzedaż	172.31.10.0/24
F0/13 - 20	VLAN 20 - Produkcja	172.31.20.0/24
F0/1 - 6	VLAN 30 - Marketing	172.31.30.0/24
Interfejs sieci VLAN 88	VLAN 88 - Zarządzanie	172.31.88.0/24
Łącza trunk	VLAN 99 - Native	Nie dotyczy

Scenariusz

W tym zadaniu dwa przełączniki są już skonfigurowane. Na trzecim przełączniku należy przydzielić adres IP dla wirtualnego interfejsu przełącznika, skonfigurować sieci VLAN, przypisać sieci VLAN do interfejsów, skonfigurować trunk oraz wykonać podstawowe czynności zabezpieczające przełącznik.

Wymagania

S1 i **S2** są już skonfigurowane. Nie masz dostępu do tych przełączników. Odpowiadasz za skonfigurowanie **S3,** które obejmuje następujące wymagania:

- Adresację IP i bramę domyślną skonfiguruj zgodnie z **Tabelą adresowania**.
- Utwórz sieci VLAN, nazwij je i przyporządkuj zgodnie z **Tabelą przyporządkowania sieci wirtualnych VLAN i portów**.
- Przypisz natywną sieć VLAN 99 do portu trunkowego i wyłącz DTP.
- Ogranicz port trunkowy tylko do sieci VLAN 10, 20, 30, 88 i 99.
- Użyj sieci VLAN 99 jako natywnej sieci VLAN na porcie trunkowym.
- Skonfiguruj podstawowe zabezpieczenie przełącznika S3:
  - Zastosuj szyfrowane hasło **itasecret**
  - Zastosuj hasło konsolowe **letmein**
  - Zastosuj hasło do VTY **c1$c0** (0 jest cyfrą)
  - Zaszyfruj wszystkie jawne hasła.
  - Skonfiguruj, jako baner powitalny MOTD (message-of-the-day), komunikat **Authorized Access Only!!**.
  - Wyłącz nieużywane porty.
- Skonfiguruj zabezpieczenia dla portu **F0/6**:
  - Tylko dwa konkretne urządzenia mogą mieć dostęp do tego portu.
  - Poznane adresy MAC zostaną dodane do konfiguracji bieżącej.
  - Zabezpiecz interfejs tak, aby było wysłane powiadomienie o tym, że nastąpiło naruszenie bezpieczeństwa, lecz port pozostaje włączony.
- Sprawdź, czy komputery w tej samej sieci VLAN mogą wysyłać polecenia ping, które zakończą się sukcesem.