Wstępna konfiguracja urządzeń teleinformatycznych.
Konfiguracja aspektów bezpieczeństwa urządzeń teleinformatycznych.

1. Sprawdź bieżącą konfigurację przełącznika
2. Sprawdź startową konfigurację przełącznika zapisaną w pamięci NVRAM.
3. Sprawdź właściwości interfejsu SVI dla VLAN 1.
4. Sprawdź właściwości IP interfejsu SVI VLAN 1.
5. Sprawdź wersję systemu ISO na przełączniku.
6. Sprawdź domyślne ustawienia interfejsu ethernetowego, do którego podłączony jest PC-A.
7. Sprawdź domyślne ustawienia VLAN na przełączniku.
8. Sprawdź pamięć flash.
9. Ustaw nazwę przełącznika.
10. Ustaw szyfrowanie haseł.
11. Ustaw nazwisko jako tajne hasło do trybu EXEC.
12. Wyłącz niepożądane zapytania DNS.
13. Ustaw baner MOTD.
14. Zweryfikuj prawa dostępu przechodząc pomiędzy trybami przełącznika.
15. Stwórz nowy VLAN nr_z_dziennika na przełączniku Następnie przypisz mu adres IP 192.168.nr_z_dziennika.2 z maską 255.255.255.0 na wewnętrznym wirtualnym interfejsie VLAN nr_z_dziennika.
16. Przypisz wszystkie porty do VLAN nr_z_dziennika.
17. Użyj komendy show vlan brief w celu weryfikacji, że wszystkie porty są teraz przypisane do VLAN nr_z_dziennika.
18. Ustaw adres IP bramy domyślnej na S1.
19. Aby zabezpieczyć wiadomości wysyłane przez połączenie konsolowe przed błędami połączenia użyj komendy logging synchronous.
20. Ustaw możliwość połączenia przy użyciu protokołu Telnet poprzez linie wirtualne przełącznika vty.
21. Konfiguracja adresu IP 192.168.nr_z_dziennika.10 na PC-A.
22. Wyświetlanie konfiguracji przełącznika.
23. Zweryfikuj ustawienia interfejsu VLAN nr_z_dziennika.
24. Testowanie łączności w sieci.
25. Testowanie zdalnego zarządzania przełącznikiem S1.
26. Zapis bieżącej konfiguracji przełącznika.
27. Odczyt adresu MAC komputera.
28. Określenie adresu MAC, którego uczy się przełącznik.
29. Użyj komendy show mac address-table dynamic w celu wyświetlenia adresów poznanych dynamicznie.
30. Wyczyść tablicę adresów MAC.
31. Sprawdź czy tablica została wyczyszczona.
32. Wyświetl ponownie tablicę adresów MAC.
33. Ustaw statyczny adres MAC.
34. Sprawdź wpisy w tabeli adresów MAC.
35. Usuń statyczny adres MAC z tablicy. Wejdź do trybu globalnej konfiguracji i użyj tej samej komendy co w punkcie g, tylko z przedrostkiem no na początku.
36. Sprawdź czy statyczny adres MAC został usunięty.

Do przemyślenia

1. Dlaczego powinno konfigurować się linie vty na przełączniku?

2. Dlaczego zmienia się domyślny VLAN 1 na inny?

3. Jak można zapobiec wysyłaniu haseł jawnym tekstem?

4. Dlaczego konfiguruje się statyczny adres MAC na portach przełącznika?

37. Użyj komendy erase startup-config w celu usunięcia startowej konfiguracji z pamięci NVRAM.
38. Użyj komendy reload w celu usunięcia starych konfiguracji z pamięci. Gdy pojawi się komunikat “Czy kontynuować?” wciśnij enter.
39. Użyj komendy show flash w celu określenia czy na przełączniku został stworzony jakiś VLAN.
40. Jeżeli plik vlan.dat jest obecny w pamięci, skasuj go.
41. Użyj komendy erase startup-config w celu usunięcia startowej konfiguracji z pamięci NVRAM.
42. Użyj komendy reload w celu usunięcia starych konfiguracji z pamięci. Gdy pojawi się komunikat “Czy kontunuować?” wciśnij enter.

ćw.2.

1. Włączenie SSH na S1. W trybie globalnej konfiguracji utwórz domenę Lab-4Ti-nazwisko.com.
2. twórz lokalnego użytkownika dla połączeń SSH. Użytkownik powinien mieć uprawnienia administratora.
3. Dla interfejsu wirtualnego zezwól tylko na połączenia SSH i ustaw używanie lokalnej bazy danych podczas autentyfikacji użytkownika.
4. Wygeneruj klucz RSA o długości 1024 btów.
5. Zweryfikuj konfigurację SSH i odpowiedz na pytania.

    Jaka jest wersja SSH używana przez przełącznik?
    Ile jest dozwolonych prób logowania?
    aki jest domyślny czas nieaktywności (timeout) dla SSH?

6. Zmodyfikuj domyślną konfigurację SSH.
7. Jaki jest czas nieaktywności (timeout) dla SSH?
8. Używając klienta SSH na komputerze PC-A, zestaw połączenie SSH do S1. Jeżeli otworzy się okno dotyczące klucza, zaakceptuj je. Zaloguj się używając nazwy admin oraz hasła (które ustawiłeś wcześniej)

    Czy połączenie powiodło się?
    Co zostało wyświetlone na przełączniku S1?

9. Wpisz exit i zamknij sesję SSH na S1.
10. Zapisz adres MAC interfejsu G0/1 routera R1. Użyj komendy show interface g0/1 na routerze R1.
11. Na przełączniku S1 w trybie uprzywilejowanym użyj komendy show mac address-table. Znajdź dynamiczne wpisy dla portów F0/5 i F0/6. Wypisz je poniżej.
12. konfiguruj podstawowe bezpieczeństwo portów.

13. Skonfiguruj statyczny wpis adresu MAC interfejsu G0/1 routera R1.
14. Zweryfikuj bezpieczeństwo portu F0/5 na przełączniku S1 używając komendy show port-security interface.
15. Na routerze R1 użyj polecenia ping na adres komputera PC-A.
16. Sprawdź bezpieczeństwo przełącznika, zmieniając adres MAC interfejsu G0/1 routera R1. Wejdź do trybu konfiguracji interfejsu G0/1 i wyłącz go.
17. Skonfiguruj nowy adres MAC interfejsu. Użyj adresu aaaa.2 x nr_z_dziennika.cccc
18. Jeżeli możliwe otwórz jednocześnie połączenie konsolowe do przełącznika S1. Zobaczysz różne wiadomości pojawiające się na przełączniku związane z naruszeniem bezpieczeństwa. Włącz interfejs G0/1 na routerze R1.
19. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Czy wynik był pozytywny? Dlaczego tak lub dlaczego nie?
20. Na przełączniku zweryfikuj bezpieczeństwo portu.
21. Wyłącz interfejs G0/1 na routerze R1, usuń wpisany adres MAC i ponownie włącz interfejs.
22. Na routerze R1 użyj polecenia ping na adres komputera PC-A. Czy wynik był pozytywny?
23. Na przełączniku użyj komendy show interface f0/5 w celu wykrycia przyczyny braku odpowiedzi polecenia ping. Zapisz znalezioną przyczynę.
24. Wyczyść błąd statusu portu F0/5 na przełączniku S1.
25. Wydaj komendę show interface f0/5 na S1 w celu weryfikacji czy port F0/5 nie jest dłużej w błędnym trybie wyłączenia.