1. Sw2: VLAN-ok létrehozása, port hozzárendelés és trunk sz?rés

Kérdés: Hozza létre Sw2 kapcsolón a VLAN?okat a következ? táblázatnak megfelel?en és rendelje hozzá a megfelel? portokat. Állítsa be, hogy Sw1 és Sw2 között csak a táblázatban szerepl? VLAN azonosítóval rendelkez? keretek haladhassanak át!

Válasz és magyarázat: El?ször beállítjuk a privilegizált (enable) mód jelszavát, majd létrehozzuk a két VLAN?t, hozzárendeljük a megadott portokat, és végül konfiguráljuk a trunkot a Sw1 felé, amelyen csak a VLAN 10 és 20 forgalma mehet át.

plaintext

Magyarázat:

A vlan parancsok létrehozzák a szükséges VLAN?okat, és elnevezik ?ket.

Az interface fastEthernetX részben beállítjuk a portokat access módra, és hozzárendeljük a megfelel? VLAN?hoz.

A trunk porton a switchport trunk allowed vlan 10,20 korlátozza, hogy csak ezek a VLAN?ok keretei haladhassanak át, így a két kapcsoló közti forgalom kizárólag a megadott VLAN?okra korlátozódik.

2. Alhálózatok tervezése VLSM alapokon

Kérdés: A Szende-LAN hálózatában, a 172.31.0.0/16 tulajdonosi címtartományon belül, alakítson ki VLSM szabályoknak megfelel? alhálózatokat az alábbiigények alapján:

Töltse ki a címtáblázat rovatait:

Válasz és magyarázat: A 20 hostot igényl? hálózathoz a leghatékonyabb megoldás egy /27 (32 cím, 30 kiosztható), míg a 40 hoszt esetén egy /26 (64 cím, 62 kiosztható) alhálózat.

plaintext

VLAN ID	alhálózat IP-címe	alhálózati maszk	kiosztható címtartomány
10	172.31.0.0	255.255.255.224 (/27)	172.31.0.1 ? 172.31.0.30
20	172.31.0.32	255.255.255.192 (/26)	172.31.0.33 ? 172.31.0.94

Magyarázat:

VLAN 10: A 172.31.0.0/27 tartomány 32 címet tartalmaz; a hálózat címe 172.31.0.0, a broadcast pedig 172.31.0.31, így a hasznos, kiosztható címek 172.31.0.1?172.31.0.30.

VLAN 20: A következ? blokknál a 172.31.0.32/26 tartományot használjuk, mely 64 címet ad, ebb?l 62 kiosztható (172.31.0.33?172.31.0.94), a broadcast címe 172.31.0.95.

3. Router-on-a-stick: Inter-VLAN routing konfigurálása

Kérdés: A Szende-LAN hálózatában a VLAN-ok közti forgalomirányítást router-on-a-stik technikával valósítsa meg úgy, hogy az al-interface azonosítója megegyezik a VLAN ID?vel, és az alinterface címe az adott alhálózat els? kiosztható címe legyen!

Válasz és konfiguráció:

plaintext

Magyarázat: A router alinterface?jeiket úgy konfiguráljuk, hogy mindegyikhez hozzárendelt, dot1Q encapsulation?t alkalmazzuk. A VLAN 10 esetén a 172.31.0.1, míg a VLAN 20 esetén a 172.31.0.33 cím lesz az els? kiosztható cím az adott alhálózatban.

4. Sw2 felügyeleti interfész beállítása (management)

Kérdés: A Sw-2 kapcsoló felügyeleti interfészét a VLAN 10?be kell helyezni, mely az alhálózat harmadik IP címét kapja, valamint állítsa be az alapértelmezett átjárót, hogy távoli hálózatokból is elérhet? legyen!

Válasz és konfiguráció:

plaintext

Magyarázat: A VLAN 10 alhálózat (172.31.0.0/27) els? kiosztható címei: 172.31.0.1, .2, .3; itt a 3-as címet választjuk a menedzsment interfész számára. Az alapértelmezett átjáró (gateway) általában a router alinterface?je (172.31.0.1) lesz, amely az inter-VLAN routingot végzi.

5. Port-biztonság engedélyezése Sw2 minden FastEthernet portján

Kérdés: Az Sw-2 kapcsolón az összes FastEthernet porton engedélyezze a port-biztonságot oly

módon, hogy maximum két darab eszköz kapcsolódhasson a porthoz, és a csatlakozáskor a MAC címet automatikusan rögzítse!

Válasz és konfiguráció:

plaintext

interface range fastEthernet 0/1 - 24

switchport mode access

switchport port-security

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security violation restrict

exit

Magyarázat:

A switchport port-security maximum 2 biztosítja, hogy maximum két MAC cím legyen engedélyezve az interfészen.

A mac-address sticky opció automatikusan beszúrja a tanult MAC címeket a konfigurációba.

A violation restrict pedig a jogosulatlan eszközök forgalmát korlátozza (más variáns például shutdown is lehet).

6. Távoli hozzáférés biztonságos konfigurálása Sw2?n

Kérdés: Az Sw-2 kapcsolón állítsa be, hogy távoli hozzáférés esetén a helyi felhasználót kérje hitelesítésként, valamint kizárólag SSH-n keresztül lehessen bejelentkezni!

Válasz és konfiguráció:

plaintext

line vty 0 4

login local

transport input ssh

exit

Magyarázat:

A login local paranccsal a helyi felhasználói adatbázist használjuk az autentikációhoz.

A transport input ssh kizárólag SSH protokollt engedélyez a távoli bejelentkezéshez.

7. ACL létrehozása a távoli bejelentkezéshez Sw2?n

Kérdés: Az Sw-2 kapcsolón hozzon létre megfelel? ACL-t, hogy kizárólag az Admin VLAN?ból (példaként 172.31.50.0/24) lehessen távoli (SSH) bejelentkezni!

Válasz és konfiguráció:

plaintext

access-list 2 permit ip 172.31.50.0 0.0.0.255 any

!

line vty 0 4

access-class 2 in

exit

Magyarázat: Az ACL (azonosító 2) csak az Admin VLAN alhálózatból (172.31.50.0/24) enged be SSH-on keresztüli hozzáférést, míg minden más forrás le lesz tiltva.

8. R-Szende router ? ACL a PAT (NAT túlterhelés) számára

Kérdés: Az R-Szende routeren hozzon létre 1-es azonosítójú ACL-t, amely engedélyezi a Port túlterheléses NAT?ot a következ? VLAN?okra: Terminal, Iroda, Admin és Szerver. (A címfordítás már konfigurálva van, csak az ACL szükséges!)

Válasz és konfiguráció: Példaként az alábbi IP tartományokat használjuk:

Terminal (VLAN 10): 172.31.0.0/27

Iroda (VLAN 20): 172.31.0.32/26

Admin VLAN: 172.31.1.0/24

Szerver VLAN: 172.31.2.0/24

plaintext

access-list 1 permit ip 172.31.0.0 0.0.0.31

access-list 1 permit ip 172.31.0.32 0.0.0.63

access-list 1 permit ip 172.31.1.0 0.0.0.255

access-list 1 permit ip 172.31.2.0 0.0.0.255

Magyarázat: A wildcard maszkokkal megadjuk az engedélyezett tartományokat, így a router a NAT konfigurációban ezeket az IP blokkokat használja a forgalom fordításához.

9. R-Szende router ? DHCP szolgáltatás az Iroda VLAN részére

Kérdés: Az R-Szende routeren hozzon létre DHCP pool?t az Iroda VLAN számára úgy, hogy az els? 5 kiosztható cím ne kerüljön kiosztásra, és a DNS szerver 8.8.8.8 legyen!

Válasz és konfiguráció: A VLAN 20 alhálózata 172.31.0.32/26 esetén az els? kiosztható cím 172.31.0.33, így az els? 5 cím: 172.31.0.33?172.31.0.37.

plaintext

ip dhcp excluded-address 172.31.0.33 172.31.0.37

ip dhcp pool Iroda_VLAN

network 172.31.0.32 255.255.255.192

default-router 172.31.0.33

dns-server 8.8.8.8

Magyarázat: Az ip dhcp excluded-address paranccsal kizárjuk az els? 5 kiosztható címet a poolból. Ezután a DHCP pool a maradék címeket osztja ki az Iroda eszközei számára, a megadott alapértelmezett átjáróval és DNS?szerversel.

10. Törpe-LAN ? HSRP konfiguráció R-Hapci és R-Vidor routereken

Kérdés: A Törpe-LAN hálózatban, a két VLAN esetében (példaként VLAN 10 és VLAN 20) hozzon létre HSRP csoportokat úgy, hogy: ? A virtuális átjáró címe az adott VLAN harmadik cím legyen ? Az R-Hapci legyen aktív (magasabb prioritással), és preemptáljon, ha helyreáll a kapcsolat ?

Mindkét HSRP csoportban legyen engedélyezve a preempt

Válasz és konfiguráció: Példaként a VLAN 10 és 20 esetében a következ? IP címeket használjuk (egy /24-es példanetwork):

R-Hapci konfigurációja:

plaintext

R-Vidor konfigurációja:

plaintext

Magyarázat:

Az adott VLAN alhálózatban a harmadik kiosztható cím (például 10.10.10.3) lesz a virtuális átjáró.

Az R-Hapci magasabb prioritása (120) miatt lesz az aktív router.

A standby preempt lehet?vé teszi, hogy ha az R-Hapci meghibásodás után helyreáll, visszanyerje az aktív szerepet.

11. R-Vidor router ? OSPFv2 konfiguráció

Kérdés: Az R-Vidor forgalomirányítón konfiguráljon OSPFv2 protokollt a folyamat azonosító 200, terület 0 szerint, hirdesse az összes kapcsolt hálózatát, de ne küldjön hirdetéseket az Admin és Szerver VLAN felé!

Válasz és konfiguráció: Példánkban feltételezzük, hogy az OSPF által hirdetend? hálózatok a VLAN 10 (10.10.10.0/24) és a VLAN 20 (10.10.20.0/24).

plaintext

Magyarázat: Az OSPF konfigurációban a network parancsokkal hirdetjük az adott hálózatokat. A passive-interface paranccsal megakadályozzuk, hogy az Admin és Szerver VLAN interfészein keresztül OSPF üzeneteket küldjön, így azok nem fognak interakcióba lépni a szomszédos routerekkel.

12. R-Tudor router ? Statikus alapértelmezett útvonal konfigurálása

Kérdés: Az R-Tudor forgalomirányítón konfiguráljon statikus alapértelmezett útvonalat az ISP felé a

next-hop címeként 91.0.0.1-et használva!

Válasz és konfiguráció:

plaintext

Magyarázat: Ez a parancs azt jelenti, hogy ha a router nem találja a specifikus célhálózatot a routing táblában, akkor a forgalmat a 91.0.0.1-es next-hop címen keresztül továbbítja az ISP felé.

13. R-Tudor router ? Statikus címfordítás (NAT) Server részére

Kérdés: Az R-Tudor forgalomirányítón konfiguráljon statikus címfordítást a Server eszköz számára úgy, hogy a server bels? IP?címet a publikus 91.0.0.15 címre fordítsa!

Válasz és konfiguráció:

plaintext

ip nat inside source static <Server_Bels?_IP> 91.0.0.15

Magyarázat: Cseréld ki a <Server_Bels?_IP>-t a Server tényleges privát IP?címére. Ez a parancs garantálja, hogy a bels? címen érkez? forgalom a 91.0.0.15 címen érhet? el a külvilágban.

14. R-Tudor router ? WAN PPP beágyazás és CHAP hitelesítés

Kérdés: Az R-Tudor és az ISP közötti WAN kapcsolaton konfiguráljon PPP-t úgy, hogy CHAP hitelesítést alkalmazzon, és a jelszó legyen: wancon314!

Válasz és konfiguráció: MINDKÉT ROUTEREN BE KELL ÁLLÍTANI

plaintext

interface Serial0/0/0

encapsulation ppp

ppp authentication chap

ppp chap hostname R-Tudor (ellentétes router neve)

ppp chap password wancon314 (jelszó ugyanaz kell hogy legyen)

Magyarázat: Ez a konfiguráció biztosítja, hogy a WAN interfész PPP encapsulation alatt m?ködjön, és a CHAP hitelesítés segítségével a kapcsolat biztonságos legyen a megadott jelszóval.

15. R-Szundi router ? Statikus útvonal konfigurálása a Tunnel interfészen

Kérdés: Az R-Szundi forgalomirányítón konfiguráljon statikus útvonalat, hogy a Tudor-LAN hálózat elérhet? legyen a Tunnel interfész irányába!

Válasz és konfiguráció: Tételezzük fel, hogy a Tudor-LAN hálózat tartománya 172.31.3.0/24, és a tunnel interfész neve Tunnel0:

plaintext

ip route 172.31.3.0 255.255.255.0 Tunnel0 (ip cím kell még a tunnel0 helyett)

Magyarázat: Ezzel a statikus útvonallal a router tudja, hogy minden a 172.31.3.0/24 tartományba tartozó forgalmat a Tunnel0 interfészen kell továbbítania.

16. Szundi-LAN: Vezeték nélküli hálózat konfigurálása az SOHO eszközön

Kérdés: A Szundi-LAN hálózatban konfiguráljon vezeték nélküli hálózatot az SOHO eszközön az alábbi paraméterekkel:

SSID: SzundiWLAN

Biztonsági mód: WPA2-PSK/AES

Kulcs: SzW20250403

Ezután csatlakoztassa a Tabletet a vezeték nélküli hálózathoz!

Válasz és konfiguráció: A konfiguráció típusa az eszközt?l függ, de egy Cisco?szer? AP esetén a konfiguráció a következ? lehet:

plaintext

dot11 ssid SzundiWLAN

authentication open

authentication key-management wpa version 2

wpa-psk ascii SzW20250403

exit

interface Dot11Radio0

ssid SzundiWLAN

no shutdown

exit

Magyarázat: Ez a konfiguráció létrehozza a ?SzundiWLAN? SSID?t WPA2-PSK/AES biztonsági módban, a megadott kulccsal. Miután az AP konfigurálva van, a Tablet vezeték nélküli beállításaiban használd az SSID-t és a kulcsot a csatlakozáshoz.

Összegzés

Ezek a részletes kérdések és válaszok ? a konfigurációs parancsokkal és az azt kísér? magyarázatokkal ? segítséget nyújtanak abban, hogy a Szende-LAN, Törpe-LAN, R-Tudor, R-Szundi, R-Hapci és R-Vidor eszközeiden végrehajtsd a megadott feladatokat. Mindig ellen?rizd a konfiguráció m?ködését olyan parancsokkal, mint a show vlan, show ip route, show standby, show ip ospf neighbor, stb., hogy a beállítások hibamentesen m?ködjenek.

Ha bármelyik lépés vagy részletek további magyarázata szükséges, kérlek jelezd ? szívesen kifejtem még az egyes beállítások mögötti koncepciókat és lehet?ségeket!