A 12/2013. (III. 29.) NFM rendelet szakmai és vizsgakövetelménye alapján.

Szakképesítés, azonosító száma és megnevezése

54 481 04	**Informatikai rendszergazda**

Tájékoztató

A vizsgázó az első lapra írja fel a nevét!
Ha a vizsgafeladat kidolgozásához több lapot használ fel, a nevét valamennyi lapon fel kell tüntetnie, és a lapokat sorszámmal el kell látnia.

Használható segédeszköz: -

Értékelési skála:

65 – 80 pont	**5 (jeles)**
57 – 64 pont	**4 (jó)**
49 – 56 pont	**3 (közepes)**
41 – 48 pont	**2 (elégséges)**
0 – 40 pont	**1 (elégtelen)**

A javítási-értékelési útmutatótól eltérő helyes megoldásokat is el kell fogadni.

A vizsgafeladat értékelési súlyaránya: 10%.

1. **Melyik az a legkisebb méretű hálózat, ami jellemzően néhány méteres körzetben lévő eszközöket kapcsol össze? 2 pont**

    a. WAN

    b. PAN

    c. LAN

    d. MAN

2. **Tipikusan milyen hardvereszközöket tartalmaz a SOHO „router”? (3 helyes válasz van.) 6 pont**

    a. HUB

    b. Router.

    c. Repeater.

    d. VoIP gateway.

    e. Switch.

    f. Access Point.

    g. Hardveres tűzfal.

3. **Az alábbiak közül melyik átviteli közeg esetében alkalmazzák az érpárok csavarását az áthallás csökkentése érdekében? 2 pont**

    a. STP

    b. Egymódusú optikai szál.

    c. Többmódusú optikai szál.

    d. Koaxiális kábel.

4. Az Ethernet-technológia alkalmaz-e hibajavítást? 2 pont

a. Igen, a CRC mező segítségével.

b. Igen, a szükséges információkat a CRC-ben és az adatmezőben helyezi el.

c. Igen, a típus- és az adatmezőben elhelyezett információk alapján tud a cél hibát javítani.

d. Nem, csak hibadetektálást tesz lehetővé.

5. Az OSI modell melyik rétege kezeli a közeghozzáférés vezérlését? 2 pont

a. Fizikai réteg.

b. Adatkapcsolati réteg.

c. Hálózati réteg.

d. Szállítási réteg.

e. Viszonyréteg.

f. Megjelenítési réteg.

g. Alkalmazási réteg.

6. Az OSI modell melyik rétege gondoskodik az üzenet kódolásáról? 2 pont

a. Fizikai.

b. Adatkapcsolati.

c. Hálózati.

d. Szállítási.

e. Viszony.

f. Megjelenítési.

g. Alkalmazási.

7. Melyik TCP/IP protokoll valósít meg egyszerű, hitelesítés nélküli fájlátvitelt? 2 pont

a. TFTP

b. FTP

c. SFTP

d. SNMP

8. Melyik réteg valósítja meg a cél és a forrás logikai azonosítását a TCP/IP modellben? 2 pont

a. Hálózatelérési réteg.

b. Internetréteg.

c. Szállítási réteg.

d. Alkalmazási réteg.

9. Az alábbiak közül melyik protokoll használható egy hálózati eszköz sávon belüli biztonságos konfigurálására? 2 pont

a. TELNET protokoll.

b. POP3s protokoll.

c. SSH protokoll.

d. DHCP protokoll.

e. ICMP protokoll.

10. Az alábbi címek közül melyek tisztán A, B vagy C osztályú hálózatcímek? (2 helyes válasz van.) 4 pont

a. 172.160.0.0

b. 172.100.100.96

c. 100.100.100.0

d. 200.100.100.0

e. 10.10.10.0

11. Hány bit azonosítja a hálózatot a 192.168.10.125 255.255.255.192-es címben? 2 pont

a. 24

b. 16

c. 8

d. 32

e. 26

f. 30

12. Az ISP-től a 2001:2:2::/48-as IPv6-os címet kaptuk. Maximálisan hány darab alhálózatot hozhatunk létre, ha az EUI64 módszert is alkalmazzuk? 2 pont

a. 1024

b. 4096

c. 8192

d. 16384

e. 65536

13. Adott a 100.200.200.200 255.255.255.192 IP-cím. Számoljuk ki az alábbiakat:

a. Mi a hálózat címe? ……. **2 pont**

b. Mi a hálózat első kioszthatóó címe? ……. **2 pont**

c. Mi a hálózat utolsó kioszthatóó címe? …… **2 pont**

d. Mi a hálózat szórási címe? ……. **2 pont**

14. Milyen tartalmú üzenetet kapunk, ha egy forgalomirányító két interfészén az alábbi címeket állítjuk be: az egyiken 192.168.1.1/24-et; a másikon 192.168.1.254/24-et, és engedélyezzük az interfészek működését? 2 pont

a. Interface is up

b. Line protocol is up

c. 192.168.1.0 overlaps…

d. Semmilyen üzenetet nem kapunk.

15. Mit kell beállítani egy forgalomirányítón ahhoz, hogy az minden unicast csomagot továbbítson, és ismeretlen célhálózat esetén se dobja el azokat (kivéve a TTL=0 esetet)? 2 pont

a. Alapértelmezett IP-címet.

b. Alapértelmezett útvonalat.

c. A szomszédok IP-címeit.

d. Semmit, forgalomirányító alapértelmezetten minden esetben továbbítja a csomagot.

16. Melyik irányítóprotokoll küldi ki hirdetményeit szórásos címre? 2 pont

a. EIGRP

b. OSPF

c. RIP

d. RIPv2

17. Mit kell beállítani az EIGRP esetében, ha nem összefüggő módon helyeztünk el alhálózatokat? 2 pont

a. Osztályos forgalomirányítást, hogy ne küldjék az alhálózati maszkot.

b. Gyakoribb frissítésküldést.

c. Gyakoribb életjelküldést.

d. Ki kell kapcsolni az automatikus útvonal-összefogást.

18. Mit küld ki az OSPF-et futtató forgalomirányító, ha változik egy hálózat állapota? 2 pont

a. HELLO üzenetet.

b. DEAD üzenetet.

c. LSU (benne LSA) üzenetet.

d. DBD üzenetet.

19. Az OSPF esetében hogyan tudjuk megoldani, hogy a kapcsolatállapot-változások ne gerjesszenek túl sok forgalomirányítón újraszámolást? 2 pont

a. Alhálózatokat használunk.

b. Különböző méretű alhálózatokat használunk egy forgalomirányítón belül.

c. Több területre bontjuk az OSPF hálózatot.

d. Nem minden forgalomirányítót kapcsolunk össze egymással.

20. Hogyan oldja meg az OSPF, hogy egy többszörös elérésű hálózatban ne kelljen mindenkivel teljes szomszédsági viszonyt kialakítani? 2 pont

a. Nem minden forgalomirányítón vonja be a közös hálózatot az OSPF folyamatba.

b. Véletlenszerűen küldik a HELLO csomagokat a különböző címzetteknek.

c. Kiválasztanak egy „kijelölt forgalomirányító”-t az információk kezelésére és terjesztésére.

d. Különböző hálózathoz tartozó IP-címet használnak a közös hálózathoz tartozó interfészeken.

21. Hogyan tudjuk megakadályozni, hogy egy kapcsolón egy porton keresztül több hamis kerettel elárasszák és telítsék a MAC címtáblát? 2 pont

a. A kapcsoló minden porthoz csak egy MAC címet rendel, így nincs gond.

b. Maximalizáljuk a megtanulható MAC címek számát minden porton.

c. A kapcsolón előre rögzítjük a csatlakozó PC-k IP-cím MAC cím párosítását.

d. Egyáltalán nem engedünk megtanulni MAC címeket, és kézzel sem állítunk be ilyeneket.

22. A kapcsolók a MAC címtábla alapján hozzák meg továbbítási döntéseiket. Mi történik akkor, ha egy PC-n átírjuk az Ethernet-kártya MAC címét, és be van állítva portbiztonság maximálisan egy címre? 2 pont

a. A kapcsoló lecseréli a régi MAC címet a kapcsolótáblában az újra, és rendben működik tovább.

b. Semmi, mert a kapcsoló az IP-címet látva beazonosítja az új MAC címet, s használja tovább a régit.

c. A kapcsoló leblokkolja a portot.

d. A kapcsoló értesíti a csatlakozó állomásokat a MAC cím változásáról.

23. Mi történik, ha egy topológiában nem a legalkalmasabb kapcsoló lesz a Spanning Tree (feszítőfa) protokoll gyökérponti hídja rosszul beállított prioritás miatt? 2 pont

a. Semmi gondot nem okoz, a hálózat optimálisan működik tovább.

b. Feleslegesen futnak be a keretek nem szükséges útvonalakat.

c. A hálózat korrigálja a hibát, megkeresi az optimális gyökérponti hidat a Spanning Tree protokoll segítségével.

d. A hálózat működése teljesen leáll a hiba kijavításáig.

24. Hogyan gondoskodik a 802.1Q trunk protokoll arról, hogy a különböző VLAN-ok keretei ne keveredjenek? 2 pont

a. Minden trunk vonalon kizárólag csak egy VLAN kereteit továbbítja, és ez előre rögzített, így a VLAN-ok elkülönülnek.

b. Minden keret előtt egy külön értesítést küld, hogy az adott keret melyik VLAN-hoz tartozik.

c. Az Ethernet-keret fejlécében jelzőt helyez el, ami tartalmazza a VLAN-azonosítót.

d. Beágyazza a keretet egy új keretbe, aminek a célcíme az adott VLAN, amelyikhez az eredeti keret tartozik.

25. Okoz-e problémát, ha különböző VLAN-okban ugyanazt az IP-címtartományt használjuk? 2 pont

a. Egyáltalán nem.

b. Csak arra kell ügyelnünk, hogy azonos címek ne legyenek a különböző VLAN-okban, de a hálózatcím lehet azonos.

c. Amíg nem akarunk forgalomirányítást megvalósítani a két VLAN között, addig nem.

d. Igen, egyáltalán nem fog működni egyik VLAN sem.

26. Hogyan nevezzük a háromrétegű hierarchikus tervezési modellnek azt a rétegét, ahol a VLAN-ok közötti forgalomirányítást elvégezzük? 2 pont

a. Hozzáférési réteg.

b. Elosztási réteg.

c. Központi réteg.

d. Bármelyikben megtehetjük.

27. Használ-e kötelezően címzést a PPP protokoll? 2 pont

a. Igen, minden esetben.

b. Nem, soha.

c. Igen, de csupa 1-essel tölti fel, s tömörítéskor el is hagyja.

d. Nem szükséges, mert hitelesítéskor úgyis kiderül, ha nem a jogos felhasználó jelentkezett be.

28. Milyen kapcsolatokat használ leginkább a Frame Relay protokoll? 2 pont

a. VIC

b. PVC

c. SVC

d. FRVC

29. Hogyan teszi lehetővé az SNMP protokoll, hogy váratlan, de veszélyes esemény felléptekor értesüljön erről a rendszergazda? 2 pont

a. Bekapcsol egy riasztó jelzőfényt a meghibásodott eszközön.

b. Eseményvezérelt módon, úgynevezett TRAP üzenetet küld ki.

c. A felügyeleti rendszer a legközelebbi időzített lekérdezéskor értesül a hibáról.

d. Nem tudja megoldani.

30. Miért nem kompatibilis visszafelé a 802.11g szabvány a 802.11a szabvánnyal? 2 pont

a. A 802.11a-t sokkal régebben adták ki.

b. A 802.11g nem használja a CSMA/CA eljárást.

c. Különböző frekvenciasávban dolgoznak.

d. A 802.11g-s szabvány tömörítést használ, a 802.11b pedig nem.

31. A vezeték nélküli kliens hogyan tudja megkeresni az AP-t, ha az nem hirdeti magát? 2 pont

a. Be kell állítani az SSID-t, és a további paramétereket, ennek alapján a kliens aktív keresést hajt végre.

b. Ilyenkor a kliens nem tudja megkeresni az AP-t.

c. A kliens végignézi a teljes frekvenciasávot, és kiolvassa a kommunikációkból az SSID-t.

d. A kliens ilyenkor egy másik klienstől kérdezi le a kapcsolat paramétereit.

32. Hol helyezzük el a hálózatban azokat az ACL-eket, amelyek csak a forráscímet vizsgálják? 2 pont

a. A forráshoz legközelebb.

b. Az útvonal mentén bárhol elhelyezve jól fog működni.

c. Ilyen ACL nem létezik.

d. A célhoz legközelebb.

33. Hogyan működnek az SPI tűzfalak? 2 pont

a. Spionakat („árulókat”) építenek be az üzenetekbe, ezzel nyomon követhetővé teszik azokat.

b. Kifelé haladó üzenetekből feljegyzik annak „állapotát”, és visszafelé ezen információk lapján engedik be a válaszcsomagokat.

c. Azonosítókat helyeznek el az üzenetek fejlécében, és visszafelé ezeket keresik a válaszokban.

d. Befelé érkező csomagok esetén lekérdezik a belső céleszközt, hogy az várja-e az adott üzenetet.

34. Milyen biztonsági funkciót nem tud megvalósítani az IPsec VPN? 2 pont

a. A forrás felhasználó azonosítása.

b. A küldött üzenet sértetlenségének ellenőrzése.

c. Az üzenet tartalmának szűrése.

d. Az üzenet bizalmas jellegének biztosítása.