

HÁLÓZATI ISMERETEK

2. forduló



A kategória támogatója: Deutsche Telekom IT
Solutions

RENDELKEZÉSRE ÁLLÓ IDŐ:

20:00

Ismertető a feladathoz

Fontos információk

Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat

A kérdésekre **mindig van helyes válasz!** Ha csak egy helyes válasz van az adott kérdésre, radio button-os választási lehetőségeket fogsz látni.

Olyan kérdés viszont nincs, amelyre az összes válasz helyes!

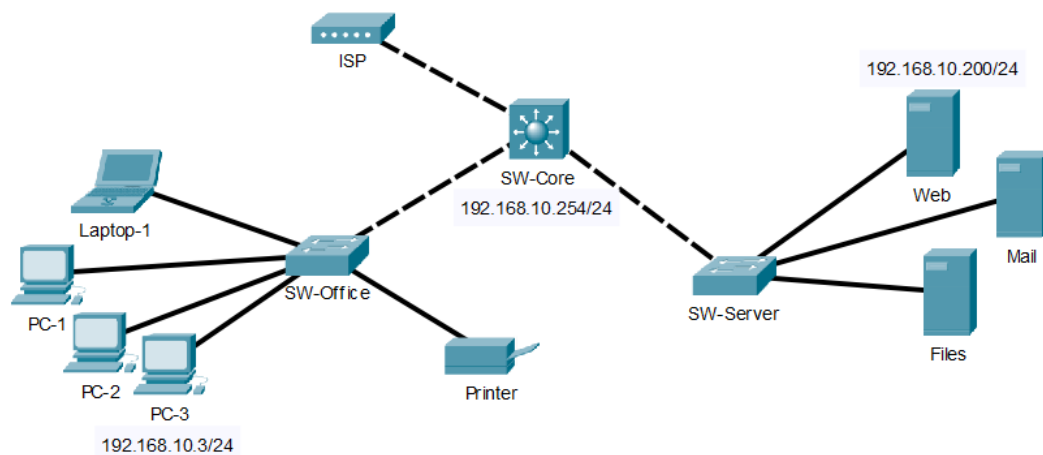
Egyéb információkat a [versenyszabályzatban](#) találsz!

Felhasznált idő: 02:07/20:00

Elért pontszám: 0/20

1. feladat 0/2 pont

Az alábbi irodai hálózatban PC-3 sikeres HTTP kéréseket intéz a Web nevű szerverhez.



A kéréseket tartalmazó csomagok útja során a csomag mely mezőinek tartalma biztosan nem változik?

Válaszok

- ☒ Source MAC address
- ☒ Destination MAC address
- ☒ Source IP address
- ☒ Destination IP address
- ☒ Source port
- ☒ Destination port
- ☒ Time to Live
- ☒ Identification
- ☐ A felsoroltak közül minden mező értéke változni fog.

Magyarázat

Az ábráról leolvasható, hogy a két eszköz egy alhálózaton van (192.168.10.0/24), a csomagok végig switchek között haladnak. SW-Core ugyan routing feladatokat is ellát, ez az alhálózaton belül haladó csomagok útját és tartalmát nem befolyásolja. Így tehát egyik mező tartalma sem fog változni.

2. feladat 0/2 pont

Mi a passzív interfész?

Válasz

- ☐ Egy interfész, amelyet a *shutdown* paranccsal lekapcsoltunk.
- ☐ Egy interfész, amely valamilyen hiba hatására *err-disabled* állapotba került.
- ☐ Egy interfész, amely jelenleg nem áll összeköttetésben semmilyen másik eszközzel.
- ☒ Egy interfész, amely nem küld, csak fogad útválasztással kapcsolatos üzeneteket.
- ☐ Egy interfész, amelyet jelenleg nem használunk, mert vannak jobb útvonalaink.
- ☐ Egy interfész, amelyen keresztül az eszköz nem forgalmaz, hogy ne alakulhasson ki hurok a hálózatban.

Magyarázat

Részletek [itt](#).

3. feladat 0/2 pont

Egy kollégád rendszeresen elgépeli a parancsokat, majd hosszasan mérgelődik, mert néha sokat kell várnia, mire folytathatja azok begépelését. Eközben a konzolon a következőhöz hasonlók láthatók:

```
SW-TEST>enable1
Translating "enable1"...domain server (255.255.255.255)
```

Mit tehet a kollégád -- azon kívül, hogy nem gépeli el a parancsokat --, **hogy ne kelljen ilyenkor hosszasan várakoznia?**

Válaszok

- ☐ Adja ki a *no ip domain-name* parancsot az eszközön globális konfigurációs módban.
- ☒ Adja ki a *no ip domain-lookup* parancsot az eszközön globális konfigurációs módban.
- ☐ Adja ki a *no hostname* parancsot az eszközön globális konfigurációs módban.
- ☐ Adja ki a *terminal ignore mistyped-commands* parancsot az eszközön globális konfigurációs módban.
- ☐ Adja ki a *no ip name-server 255.255.255.255* parancsot az eszközön globális konfigurációs módban.
- ☐ Egy parancs elgépélésekor nyomja le a *Ctrl-C* billentyűkombinációt.
- ☒ Egy parancs elgépélésekor nyomja le a *Ctrl-Shift-6* billentyűkombinációt.
- ☐ Egy parancs elgépélésekor nyomja le a *Ctrl-A* billentyűkombinációt.
- ☐ Egy parancs elgépélésekor nyomja le az *Alt-F4* billentyűkombinációt.
- ☐ Egy parancs elgépélésekor nyomja le a *Ctrl-Shift-Escape* billentyűkombinációt.

Magyarázat

A *no ip domain-lookup* parancs hatására az eszköz nem fogja megpróbálni domainnévként feloldani az elgévelt parancsot, hanem azonnal visszatér hibaüzenettel. Ha ezt nem használjuk, egy elgévelt parancs esetén még mindig megnyomhatjuk a Ctrl-Shift-6 billentyűkombinációt a névfeloldás megszakítására.

A *no ip domain-name* az eszköz azon domainnevét törli, amelyet például SSH kulcsok generálásánál is használ. A *no hostname* az eszköz beállított nevét törli. A *no ip name-server 255.255.255.255* parancs a 255.255.255.255-öt törölné az eszközön beállított névszerverek közül (ha lenne ilyen beállítva). A *terminal ignore mistyped-commands* parancs nem létezik. A Ctrl-A kombináció a sor elejére ugrat vissza, Ctrl-C-vel privileged exec módba tudunk gyorsan visszalépni. A Ctrl-Shift-Escape kombináció Windows operációs rendszeren megnyit egy Task Managert (Feladatkezelő), az Alt-F4 pedig az aktív ablakot zárja be.

4. feladat 0/2 pont

Egy kollégáddal beszélgettek az IPv4 és az IPv6 közötti hasonlóságokról és különbségekről. **Melyek az igaz állítások?**

Válaszok

- ☐ Négyyszer annyi IPv6-os cím létezik mint IPv4-es.
- ☒ IPv6 esetén nincs lehetőség broadcast forgalmat bonyolítani.
- ☐ Az IPv6 egyik nagy előnye, hogy IPv6 alapú hálózatokban nincs szükség útválasztásra.
- ☒ Egy szerveralkalmazás képes lehet egyszerre IPv4-es és IPv6-os kliensek kiszolgálására is.
- ☒ IPv6 esetén a közbenső állomások nem tördelhetik a csomagokat.
- ☐ Az IPv6-os fejléceket egyszerűbb feldolgozni, mert rövidebbek az IPv4-esnél.

Magyarázat

Négyyszer annyi IPv6-os cím létezik mint IPv4-es. Hamis. A címek mérete négyszeres (32 bit helyett 128 bit), de ez azt jelenti, hogy $2^{(128-32)}$ -szer annyi IPv6-os cím van mint IPv4-es.

IPv6 esetén nincs lehetőség broadcast típusú forgalmat bonyolítani. Igaz. Csak unicast, multicast és anycast forgalmak támogatottak. Broadcast címek egyáltalán nincsenek.

Az IPv6 egyik nagy előnye, hogy IPv6 alapú hálózatokban nincs szükség útválasztásra. Hamis. Ugyanúgy szükség van útválasztásra.

Egy szerveralkalmazás képes lehet egyszerre IPv4-es és IPv6-os kliensek kiszolgálására is. Igaz. Ma már számos ilyen szoftver létezik.

IPv6 esetén a közbenső állomások nem tördelhetik a csomagokat. Igaz. Lásd [az RFC-ben](#).

Az IPv6-os fejléceket egyszerűbb feldolgozni, mert rövidebbek az IPv4-esnél. Hamis. Az igaz, hogy az IPv6-os fejléceket egyszerűbb feldolgozni, de nem azért, mert rövidebbek, sőt, nem is rövidebbek. Egy IPv4-es fejléc legkisebb mérete 20 bájt, míg IPv6 esetén ez a méret 40 bájt.

5. feladat 0/2 pont

Egy vélhetően DNS-sel kapcsolatos probléma megoldásán dolgoztok. Egy kollégád kiad egy parancsot a gépén, melynek hatására a névkiszolgáló naplófájljában megjelenik egy kérés:

```
192.144.36.10.in-addr.arpa. IN PTR
```

Milyen parancsot adhatott ki a kollégád?

Válasz

- ☐ nslookup arpa.in.ptr
- ☐ nslookup arpa.ptr.in
- ☒ nslookup 10.36.144.192
- ☐ nslookup srv1.oitm.local
- ☐ nslookup 192.144.36.10
- ☐ nslookup 192.144.36.10.in-addr.arpa
- ☐ nslookup in-addr.arpa

Magyarázat

A kolléga gépe egy PTR (pointer) rekordra kérdezett rá, tehát reverse feloldást kért (azaz egy IP-címhez milyen szimbolikus név tartozik). Erre az *in-addr.arpa* domain használatos, a kérdéses IP-cím oktettjeit fordított sorrendben kell leírni a kérésben ([RFC 1035](#)). A kérdéses IP-cím tehát 10.36.144.192 volt, a kiadott parancs innen *nslookup 10.36.144.192*.

Az *nslookup 192.144.36.10* kivételével az összes többi parancs 'A' rekordra kérdezett volna rá, itt pedig az oktettek sorrendje rossz (nem fordított a sorrend).

6. feladat 0/2 pont

A TCP/IP modell alkalmazási (application) rétege mely réteg(ek)nek feleltethető meg az OSI modellben?

Válaszok

- ☒ Application (alkalmazási)
- ☒ Presentation (megjelenítési)
- ☒ Session (viszony)
- ☐ Transport (szállítási)
- ☐ Network (hálózati)

- ☐ Data Link (adatkapcsolati)
- ☐ Physical (fizikai)

Magyarázat

A TCP/IP modell az OSI modellre hasonlító, egyszerűbb és gyakorlatiasabb modell. Az egyes szakirodalmakban több változata is megtalálható, jellemzően 4-5 réteggel és hasonló rétegnevekkel. Az viszont közös bennük, hogy a legfelső rétegük egy alkalmazási réteg, mely lefedi az OSI modell felső három rétegének funkcióit.

OSI	TCP/IP "internet model" (Cisco)	TCP/IP reference model (Tanenbaum)
Application	Application	Application
Presentation		
Session		
Transport	Transport	Transport
Network	Internetwork	Internet
Data Link	Network interface	Data Link
Physical		Physical

7. feladat 0/2 pont

Egy új kolléga érkezik a céghez. Laptopot használ, vezetékes hálózati csatlakozással, de gyakran járkal a tárgyalóba. Arra panaszodik, hogy valahányszor leül az asztalához és szeretné használni a vezetékes hálózatot, várnia kell jó fél percet, mire "működik bármi is". Elmondása szerint az előző munkahelyén nem volt, illetve a tárgyalóban most sincs ilyen problémája.

Előszeded a dokumentációt, majd ránézel az irodai portjának konfigurációjára:

```
SW-Office-2# sh run | section GigabitEthernet2/18
interface GigabitEthernet2/18
description Room 18, right
switchport access vlan 80
switchport mode access
switchport nonegotiate
no cdp enable
spanning-tree bpduguard enable
storm-control broadcast level 10
```

Hogyan tudnál segíteni a problémáján?

Válasz

- ☐ A konfiguráció rendben van, máshol lesz a gond.
- ☐ A portot át kellene kapcsolni trunk módba (*switchport mode trunk*).
- ☐ A CDP ki van kapcsolva a portra, be kellene kapcsolni (*cdp enable*).
- ☐ A BPDU Guard be van kapcsolva a portra, ki kellene kapcsolni (*spanning-tree bpduguard disable*).
- ☒ A PortFast nincs bekapcsolva a portra, be kellene kapcsolni (*spanning-tree portfast*).

- ☐ A port duplexitását át kellene állítani full duplexre (*duplex full*).
- ☐ A port sebességét be kellene állítani kézzel 1000 Mbit/s-re (*speed 1000*).

Magyarázat

A [PortFast](#), ha be van kapcsolva, egy eszköz csatlakoztatásakor egyből forgalomképes állapotba helyezi a portot, míg egyébként ki kellene várni a 15 + 15 másodpercet, amíg az [STP](#) konvergál.

Az összes többi válasz közül egyik sem oldaná meg a problémát, sőt, pár eset még rontana is a helyzeten.

8. feladat 0/2 pont

Egy kolléga IPSec alapú kapcsolatot szeretne létrehozni két eszköz között. Kiadja az alábbi parancsokat:

```
S2S-Bud(config)# crypto isakmp policy 1
S2S-Bud(config-isakmp)# encryption aes 256
S2S-Bud(config-isakmp)# hash sha384
S2S-Bud(config-isakmp)# authentication pre-share
S2S-Bud(config-isakmp)# group 16
S2S-Bud(config-isakmp)# lifetime 300
S2S-Bud(config-isakmp)# exit
```

Milyen kulcscsere-algortmust fog használni az eszköz, amikor ezt a policyt használja?

Válasz

- ☐ GDOI
- ☒ Diffie-Hellman
- ☐ AES-256
- ☐ SHA-384
- ☐ ISAKMP

Magyarázat

A parancsokat nem is feltétlenül szükséges megnézni, az IPSec hallatán már lehet tudni, hogy Diffie-Hellmanról van szó. A group 16 parancs is megerősíti ezt, amely a 16-os DH-csoportot állítja be. De ha még ezt nem is tudjuk, az AES-256 titkosításra, az SHA-384 hashelésre való, így kizárhatók. Az ISAKMP egy kulcsmenedzsment-keretrendszer, nem konkrét algoritmus. A GDOI ugyan kulcscserére használatos, de csoportok szintjén, itt nem erről van szó.

9. feladat 0/2 pont

Kaptam egy hibajegyet, miszerint az egyik FTP szerverünk nem érhető el a külsőbb hálózatokból. Utánajártam, az egyik tűzfal teljes mértékben blokkolta a forgalmat a szerver és az érintett hálózatrész között. Felvettem egy-egy szabályt a tűzfalakon, amely beengedi a forgalmat az érintett hálózat felől a szerver felé a TCP 21-es portra, valamint kiengedi a szerver válaszüzeneteit erről a portról, majd lezártam a ticketet. A hibajegyet az illető visszanyitotta, miszerint továbbra sem sikerül fájlokat le- és feltöltenie. **Mi lehet a probléma?**

Válasz

- ☐ Nem a 21-es portot kellett volna engedélyeznem.
- ☐ TCP helyett UDP-t kellett volna engedélyeznem.
- ☐ A TCP mellett az UDP-t is engedélyeznem kellett volna.
- ☒ További portokat is engedélyeznem kellett volna.
- ☐ Semmi; visszaírok, hogy a hiba nem nálam van, majd ismét lezárom a hibajegyet.

Magyarázat

Az [FTP](#) egy out-of-band protokoll, a fájlok (és a könyvtárlista) átvitelére egy másik kapcsolatot használ, melynek paramétereit a kontrollcsatornán egyeztetik le. Én csak a kontrollcsatornát (TCP 21) engedtem be a tűzfalon, de ez önmagában kevés. Passzív mód esetén a szerver által használt további portokat is be kellett volna engednem, aktív mód esetén kimenő irányban kellett volna a TCP 20-as portot kinyitnom.

10. feladat 0/2 pont

Az alábbiak közül melyek formailag helyes IPv6-címek? (RFC 4291 szerint, azaz a kevésbé szigorú szabályokat alkalmazva.)

Válaszok

- ☒ 2001:db8:2fe4:184c:55ac:0000:bada:55af
- ☐ 2001:db8:0746:b055:7a2f:c3d4:9b1d:978c:6dce
- ☐ 2001:db8::5b7d::cac7
- ☐ 2001:db8:acc5:e941:fge8:abd0:1c2d:7462
- ☒ fe80::13cd:7cbc:3436:51b0
- ☐ 2001:0db8:0f95:9f31:f526:dfc1:6d02
- ☒ FF02::2
- ☐ 2001:db8:::a740:70f0

Az IPv6-os címek 128 bit hosszúak. A 128 bit 8 csoportra oszlik el, minden csoport 4 szimbólumot tartalmaz, melyek egyenként 4 bitet tesznek ki ($8 * 4 * 4 = 128$). A csoportokat kettősponttal (:) választjuk el. A szimbólumok a 16-os (hexadecimális) számrendszer számai, azaz a hagyományos arab számok 0-tól 9-ig, majd betűk a-tól f-ig (a = 10, b = 11, ...). A csoportok elejéről (és csakis az elejéről!) a nullák elhagyhatók (pl. 00ab -> ab). Egy vagy több csupa nulla csoport helyettesíthető dupla kettősponttal (::, például d:0:0:0:b -> d::b), viszont dupla kettőspont legfeljebb egyszer szerepelhet egy címben (hiszen ellenkező esetben nem mindig lenne egyértelmű a cím). (Részletek: [RFC 4291](#).)

Ezen szabályok mentén:

2001:db8:2fe4:184c:55ac:0000:bada:55af helyes, mert minden szabálynak megfelel.

fe80::13cd:7cbc:3436:51b0 úgyszintén.

2001:db8::5b7d::cac7 helytelen, mert két helyen is szerepel benne ::.

2001:db8:acc5:e941:fge8:abd0:1c2d:7462 helytelen, mert szerepel benne egy 'g' betű.

2001:db8:0746:b055:7a2f:c3d4:9b1d:978c:6dce helytelen, mert 9 csoportból áll.

2001:0db8:0f95:9f31:f526:dfc1:6d02 helytelen, mert 7 csoportból áll (és nem azért, mert rövidítve volna).

FF02::2 helyes, ez egy ismert multicast cím (link-local all routers). Ez az RFC pedig megengedi a nagybetűk használatát is.

2001:db8:::a740:70f0 helytelen, egymás mellett három kettőspont szerepel benne (:::).

Az érdeklődők a szigorúbb (5952-es) RFC szövegét [itt](#) olvashatják.