HÁLÓZATI ISMERETEK

6. forduló

A kategória támogatója: Deutsche Telekom IT Solutions

RENDELKEZÉSRE ÁLLÓ IDŐ:

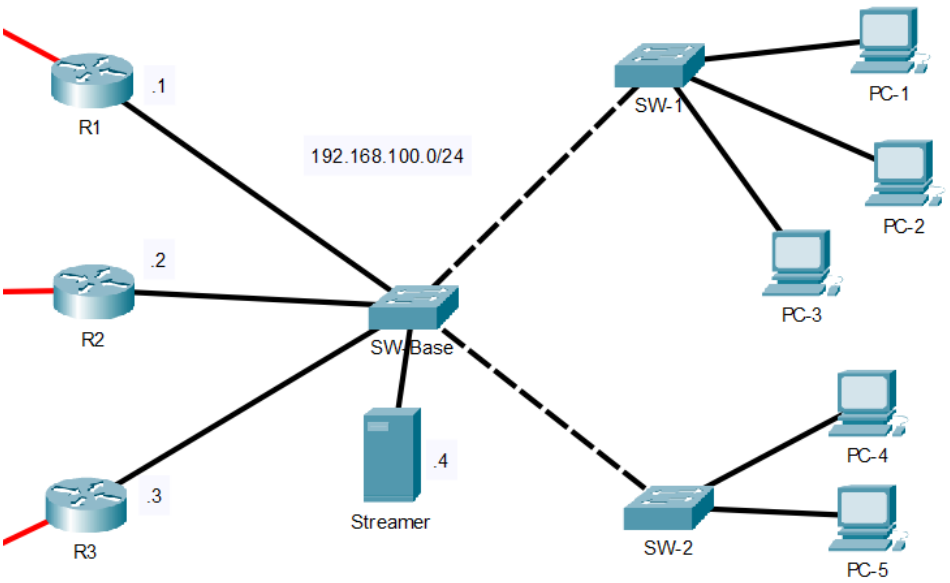
24:00

Ismertető a feladathoz

Felhasznált idő: 02:07/24:00 **Elért pontszám:** 0/40

1. feladat 0/10 pont

Egyik következő projektetek keretein belül egy cég hálózatát kell majd részben átterveznetek. A dokumentáció sajnos eléggé elavult, többnyire csak rajzokból és magyarázat nélküli konfigurációs leírásokból áll. Épp egy ilyen rajzot próbálsz értelmezni.



Az asztaloknál üzleti elemzők ülnek, az egyik monitoron mindenkinél ugyanaz a videostream fut élőben a tőzsdei történésekről. Hogy takarékoskodjanak a sávszélességgel, a tévéadás a Streamer nevű szerverről van egy multicast alapú

szoftverrel továbbstreamelve.

A switchek és a kliensek konfigurációját nem ismerjük, de feltételezhetjük, hogy helyes a konfigurációjuk. Továbbá, a switcheken be van kapcsolva az IGMP snooping szolgáltatás.

R1, R2 és R3 konfigurációja az alábbi:

```
!
hostname R1
!
!
interface GigabitEthernet0/0
 ip address 192.168.100.1 255.255.255.0
 duplex auto
 speed auto
!
end
```

```
!
hostname R2
!
ip multicast-routing
!
interface GigabitEthernet0/0
 ip address 192.168.100.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
end
```

```
!
hostname R3
!
ip multicast-routing
!
interface GigabitEthernet0/0
 ip address 192.168.100.3 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
!
end
```

(A nem releváns részek az átláthatóság kedvéért el lettek távolítva a konfigurációkból.)

A fentiek ismeretében: melyik eszköz tölti be az IGMP querier szerepet a hálózatrészen, ha feltételezhetjük, hogy minden eszköz már legalább 5 perce megbízhatóan üzemel**?**

Válasz

- ○ R1
- ◯ R2
- ○ R3
- ○ R1, R2 és R3
- ○ R1 és R2
- ○ R2 és R3
- ○ R1 és R3
- ○ A Streamer szerver
- ○ Az egyik PC (ennyi információból nem dönthető el, hogy melyik)
- ○ Az egyik switch (ennyi információból nem dönthető el, hogy melyik)
- ○ A többi válaszlehetőség közül egyik sem helyes

Magyarázat

R1-en nincs bekapcsolva semmilyen multicasttal kapcsolatos szolgáltatás, így ő nem lehet IGMP querier. R2-n és R3-on viszont igen, ők mindketten szeretnének querierként viselkedni. Mivel másként nincs definiálva, alapértelmezés szerint IGMPv2-t futtatnak, ott pedig az a szabály, hogy több lehetséges querier közül a kisebb IP-című eszköz lesz a "megválasztott" querier. Mivel R2 IP-címe a kisebb, ő lesz a querier.

Bizonyos switchek szintén tudnak IGMP querierként működni, és létezik olyan szoftver is, amellyel a PC-kből vagy a Streamer szerverből is lehetne IGMP queriert faragni, viszont a fenti szabály mentén ugyanúgy R2 lesz a megválasztott.

(Érdeklődőknek: Cisco - Network Access and Layer 2 Multicast)

2. feladat 0/10 pont

A múlt hónapban nyitott egy új irodát a cég. Ezt követően felmerült az igény, hogy a két telephely belső hálózatát valahogyan össze kellene kötni, hogy el lehessen érni egymás szolgáltatásait, szervereit. Megszületett a döntés, hogy létrehozzatok egy site-to-site VPN kapcsolatot a telephelyek között, már egészen jól halad a tervezés és megvalósítás is.

A két telephely között végig 1 gigabit sávszélességű Ethernet/IP alapú hálózat húzódik, a szokásos 1500 bájtos link-MTU-val (amelybe már bele van számolva a 14 bájtos Ethernet-fejrész, tehát azzal nem kell külön számolni). VPN átjárónak egy olyan eszköz lett kiválasztva, amely IP-csomagokat csomagol be és továbbít egy saját protokoll szerint. Ez a saját protokoll UDP felett működik, és minden továbbított csomaghoz egy 56 bájt hosszú saját fejrészt illeszt. A protokoll titkosítja, hitelesíti és integritásvédi a kiküldött csomagokat, de ez nem változtatja meg azok méretét (minden ehhez szükséges extra információt a saját fejrészben hordoz).

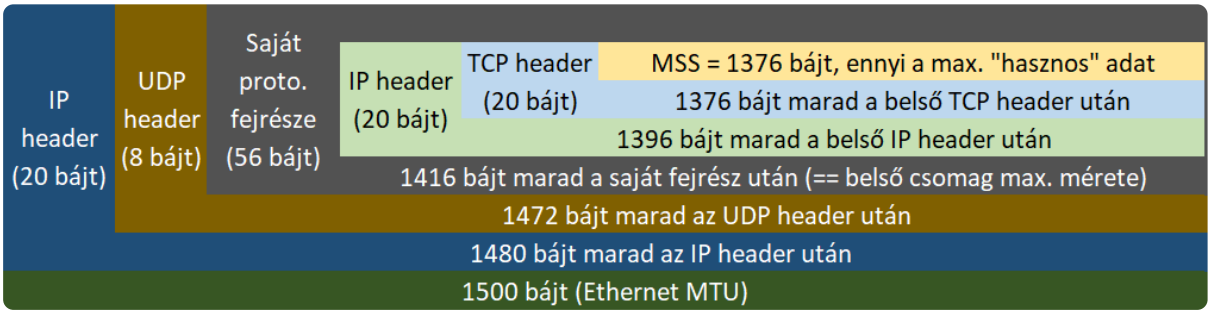
A kérdés: **legfeljebb hány bájt lehet egy ebben az alagútban utazó TCP kapcsolat szegmensmérete (MSS), ha azt szeretnénk, hogy egyik közbülső eszközön se kelljen tördelni a csomagokat?**

Válaszok

A helyes válasz:
1376
ezerháromszázhetvenhat
egyezerháromszázhetvenhat

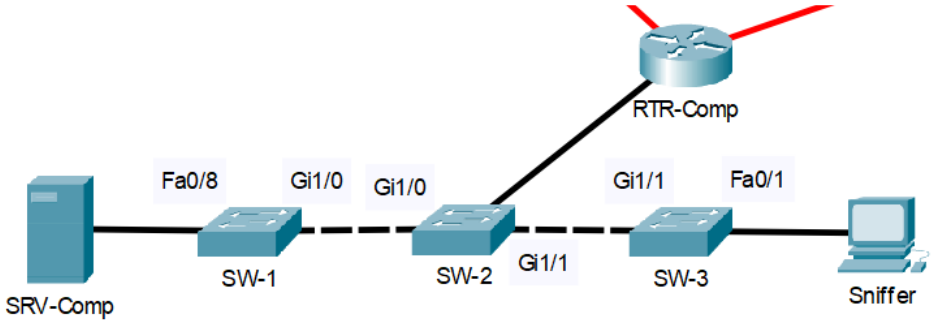
Magyarázat

Induljunk ki az 1500 bájtos MTU-ból. Első körben ebből le kell vonni egy IP és egy UDP header méretét (20 és 8 bájt, ezt illik tudni fejből; UDP, mert a protokoll a leírás szerint UDP felett működik), valamint a VPN megoldás saját protokolljának overheadjét (56 bájt, ezt írja a szöveg). Így marad 1500 - 20 - 8 - 56 = 1416 bájt a belső ("becsomagolt") csomagnak. Mivel a VPN a leírás szerint IP csomagokat továbbít a túloldalra, Ethernet kerettel nem kell számolni ezen a belső csomagon, viszont ennek is lesz egy IP és egy TCP headerje (TCP, mert TCP kapcsolatok szegmensméretére vonatkozik a kérdés), amelyek rendre 20-20 bájtosak. Ezek méretét kivonva az előző 1416 bájtból megkapjuk, hogy a keresett maximális szegmensméret 1376 bájt. (Ezt pedig a megfelelő eszközök megfelelő interfészén kiadott *ip tcp adjust-mss 1376* paranccsal tudjuk kikényszeríteni.)



3. feladat 0/10 pont

Úgy tűnik, ismeretlenek támadják a céges szervert. A biztonsággal foglalkozó csapat kérte, hogy oldjuk meg, hogy élőben láthassák a gép forgalmát.



A szerver az ábra szerint az SW-1-hez van csatlakoztatva, míg a biztonsági csapat szobájához az SW-3 van legközelebb, oda kötötték be a forgalomelemző gépet is. A két switchet az SW-2 köti össze. VTP-t nem használunk, a switchek trunk portjain minden VLAN át van engedve.

Melyik eszközökön és milyen parancsokat kellene kiadni, hogy teljesítsük a biztonsági csapat kérését, anélkül, hogy a normál forgalmat, a hálózat működését akadályoznánk?

Válaszok

- [x]
```
SW-1(config)# vlan 5
SW-1(config-vlan)# remote-span
SW-1(config-vlan)# exit
```

- [x]
```
SW-2(config)# vlan 5
SW-2(config-vlan)# remote-span
SW-2(config-vlan)# exit
```

- [x]
```
SW-3(config)# vlan 5
SW-3(config-vlan)# remote-span
SW-3(config-vlan)# exit
```

- [x]
```
SW-1(config)# monitor session 55 source interface FastEthernet0/8
SW-1(config)# monitor session 55 destination remote vlan 5
```

- [ ]
```
SW-1(config)# monitor session 55 source remote vlan 5
SW-1(config)# monitor session 55 destination interface FastEthernet0/8
```

- [ ]
```
SW-1(config)# monitor session 55 source interface FastEthernet0/8
SW-1(config)# monitor session 55 destination interface GigabitEthernet1/0
```

- [ ]
```
SW-2(config)# monitor session 55 source interface GigabitEthernet1/0
SW-2(config)# monitor session 55 destination interface GigabitEthernet1/1
```

- [ ]
```
SW-2(config)# monitor session 55 source remote vlan 5
SW-2(config)# monitor session 55 destination interface GigabitEthernet1/1
```

- [ ]
```
SW-2(config)# monitor session 55 source interface GigabitEthernet1/0
SW-2(config)# monitor session 55 destination remote vlan 5
```

- [ ]
```
SW-2(config)# monitor session 55 source remote vlan 5
SW-2(config)# monitor session 55 destination remote vlan 5
```

- [x]
```
SW-3(config)# monitor session 55 source remote vlan 5
SW-3(config)# monitor session 55 destination interface FastEthernet0/1
```

- [ ]
```
SW-3(config)# monitor session 55 source interface FastEthernet0/1
SW-3(config)# monitor session 55 destination remote vlan 5
```

- [ ]
```
SW-3(config)# monitor session 55 source interface GigabitEthernet1/1
SW-3(config)# monitor session 55 destination interface FastEthernet0/1
```

Magyarázat

Látható, hogy több switch között kell átvinni a forgalmat, és végig csak switcheink vannak, így a legegyszerűbb az, ha RSPAN-t használunk. Ehhez ki kell jelölni egy csak erre a célra használt VLAN-t, továbbá szükséges, hogy az útvonalon minden eszközön fel legyen véve ez a VLAN, remote-span jelzéssel ellátva. Mivel nem használunk VTP-t, ezt a VLAN-t minden eszközön kézzel kell felvenni és beállítani, és nem kell foglalkozni a pruninggal. Ezen felül biztosítani kell, hogy a VLAN forgalma áthaladhasson a trunk linkeken, de a feladat írta, hogy mindenhol minden VLAN át van engedve, így ezzel nincs külön dolgunk. Végül, SW-1-en be kell állítani, hogy a szerver portján átmenő forgalmat másolja fel az RSPAN VLAN-ra, majd SW-3-on, hogy az ezen a VLAN-on érkező forgalmat tegye ki a megfigyelést végző gép portjára. A többi válasz helytelen, mert fel van cserélve a forrás és a cél, normál portra van kitéve a megfigyelt forgalom (ennek hatására a normál forgalom ott nem fog tudni haladni), vagy normál portról van lemásolva a forgalom (nem csak a megfigyelni kívánt forgalmat fogjuk látni). Egy eszközön belül nem használhatjuk ugyanazt a VLAN-t az RSPAN forrásának és céljának is. SW-2-n jelen esetben nem kell és nem is szabad a VLAN-on kívül semmit sem beállítani (de egyébként olyat lehetne csinálni, hogy SW-2-ről további portok forgalmát is felmásoljuk a VLAN-ra megfigyelésre, vagy épp SW-2-re is lemásoljuk a megfigyelt forgalmat valamelyik portra).

Így tehát a teljes megoldás egyben:

```
SW-1(config)# vlan 5
SW-1(config-vlan)# remote-span
SW-1(config-vlan)# exit

SW-2(config)# vlan 5
SW-2(config-vlan)# remote-span
SW-2(config-vlan)# exit

SW-3(config)# vlan 5
SW-3(config-vlan)# remote-span
SW-3(config-vlan)# exit

SW-1(config)# monitor session 55 source interface FastEthernet0/8
SW-1(config)# monitor session 55 destination remote vlan 5

SW-3(config)# monitor session 55 source remote vlan 5
SW-3(config)# monitor session 55 destination interface FastEthernet0/1
```

(Érdeklődőknek: Cisco - Configuring SPAN and RSPAN)

4. feladat 0/10 pont

Adott az alábbi kimenet egy BGP-t futtató routerről.

```
RTR-Edge-10(config-router)# do show ip bgp
BGP table version is 39, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop    Metric  LocPrf  Weight  Path
* 203.0.113.0/24   10.10.10.1      80      50       0  64522 i
*                  10.10.10.2              50       0  64512 64512 i
*                  10.10.10.3                       0  64511 64511 i
*                  10.10.10.4                       0  64514 64514 64514 i
*>                 10.10.10.5                     200  64515 i
*                  10.10.10.6      90      90       0  64522 i
*                  10.10.10.7     130              0  64527 i
*                  10.10.10.8      70              0  64516 64516 i
*                  10.10.10.9      80              0  64527 i
```

Merre fogja továbbítani az eszköz a 203.0.113.0/24-es hálózatba címzett csomagokat, ha a jelenlegi legjobb útvonal kiesik?

Válasz

- ○ 10.10.10.1
- ○ 10.10.10.2
- ○ 10.10.10.3
- ○ 10.10.10.4
- ○ 10.10.10.5
- ○ 10.10.10.6
- ○ 10.10.10.7
- ○ 10.10.10.8
- ◯ 10.10.10.9

Magyarázat

A feladat megoldásához a BGP útvonalválasztási mechanizmusát, az attribútumok sorrendjét és jelentőségét szükséges ismerni.

Elsőként a weight értékét nézzük, a nagyobb a jobb. Ez egyetlen útvonalnál van megadva, a 10.10.10.5-ön keresztülinél, ahol ez 200 (ahol nincs megadva, ott 0-nak vesszük, az az alapértelmezett érték). Ez a jelenlegi

legjobb útvonal, ezt jelzi a > jel is mellette. A kérdés, hogy mi történik, ha ez kiesik. A válaszért nézzük tovább az attribútumokat. Ezen a ponton szóba jöhet még: .1, .2, .3, .4, .6, .7, .8, .9.

Másodikként a local preference számít, a nagyobb a jobb, az alapértelmezett érték 100. A listában ennél csak kisebbek vannak, ezek kiestek a versenyből, a többinél néznünk kell tovább a többi attribútumot. Ezen a ponton szóba jöhet még: .3, .4, .7, .8, .9.

Harmadikként az számít, hogy magunktól származik-e az útvonal ("locally originated"). Ilyen nincs a listában (ez onnan látszódna, hogy a next hop címe 0.0.0.0), megyünk tovább.

(Ezen a ponton kellene nézni az AIGP-t, de nem írja a feladat, hogy ilyet használnának a hálózatban, és ha igen, akkor milyen paraméterekkel.)

Negyedikként az útvonal (AS path) hossza számít, a rövidebb jobb. Két legrövidebb van, a .7 és a .9, amelyek egy hosszúak. A többi válaszlehetőség kiesett.

Ötödikként az útvonal származása (origin) számít, ami mindkét lehetőségnél egyforma (i betűvel jelölt IGP).

Hatodikként a Multi-Exit Discriminator (MED) számít, a kimeneten Metric néven található meg. Ez a 10.10.10.7 esetében 130, a 10.10.10.9 esetében 80. Itt még egy fontos szempont, hogy alapesetben ez csak akkor számít, ha a két next-hop AS ugyanaz, de ez a feltétel teljesül. A kisebb érték a jobb, tehát 10.10.10.9 felé fog menni a kérdésben szereplő forgalom.