HÁLÓZATI ISMERETEK

4. forduló

A kategória támogatója: Deutsche Telekom IT Solutions

RENDELKEZÉSRE ÁLLÓ IDŐ:

20:00

Ismertető a feladathoz

Fontos információk

A forduló után a megoldások publikálásával együtt iránymutatásként elérhetőek lesznek a **helyezéssel kapcsolatos információk**, látni fogod, hogy a kategóriában a játékosok 20%, 40% vagy 60%-a közé tartozol-e épp.

Felhívjuk figyelmedet, hogy a következő, **5. fordulótól az egyes kategóriák csak a kijelölt napokon lesznek megoldhatóak 7-22 óra között**, érdemes letöltened a naptárat a Kategóriáim menüpontban.

Felhasznált idő: 02:06/20:00 **Elért pontszám:** 0/20

1. feladat 0/5 pont

Két hete mesélted egyik kollégádnak, hogy a virtualizációs szerver portján egyszerre 6 MAC-címet is láttál. Neki rögtön eszébe jutott, hogy az ilyen esetek felderítésére és akár kivédésére is lehetne port securityt használni, majd ezt rögtön fel is konfigurálta az összes olyan portra, amely dolgozói számítógép vagy laptop felé néz.

A mai napon kiderült, hogy az egyik dolgozó behozott otthonról egy SOHO wifi AP-t, kihúzta a gépét a fali portból, az AP-t bedugta a fali portba, majd a gépét bedugta az AP-ba. Később a mobiltelefonját is csatlakoztatta az így beüzemelt wifi hálózathoz.

A switch logjaiban mindebből semmi nem jelenik meg. Az érintett port konfigurációja:

```
interface GigabitEthernet0/12
 description Office 12
 switchport access vlan 20
 switchport mode access
 switchport nonegotiate
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security aging time 1440
 no cdp enable
 spanning-tree portfast
 storm-control broadcast level 20
```

Mi(k) lehet(nek) a probléma oka(i)?

Válaszok

- [ ] A port úgy van beállítva, hogy a feltételek megsértése esetén ne keletkezzen naplóbejegyzés.
- [ ] A CDP ki van kapcsolva a porton.
- [ ] A port access módban van.
- [x] A dolgozó által csatlakoztatott eszközök száma nem lépi túl a megengedett MAC-címek számát.
- [x] Az AP router módban üzemel.
- [x] A port security funkció nem aktív.
- [ ] Nem lett megadva egy engedélyezett MAC-cím sem.

Magyarázat

Helyes válaszok:

A port security funkció nem aktív. Lemaradt a *switchport port-security* parancs, így maga a funkció nem aktív, hiába szerepel a többi kapcsolódó sor a konfigban.

A dolgozó által csatlakoztatott eszközök száma nem lépi túl a megengedett MAC-címek számát. A beállított érték 3, viszont a leírás alapján csak 2 eszköz csatlakozik az AP-hoz. Így még ha az belebeszél a hálózatba a saját MAC-címével is, akkor sem sérül a hármas limit.

Az AP router módban üzemel. Ha az AP router módban üzemel, kifelé egy eszköznek látszik, egy MAC-címmel, így nem fogja kiváltani a védelmi intézkedéseket.

Helytelen válaszok:

A CDP ki van kapcsolva a porton. Az állítás igaz, de ez nincs hatással a port security működésére.

A port access módban van. Ez is igaz állítás, de pont ilyenkor a leghasznosabb a port security, ez nem okoz problémát.

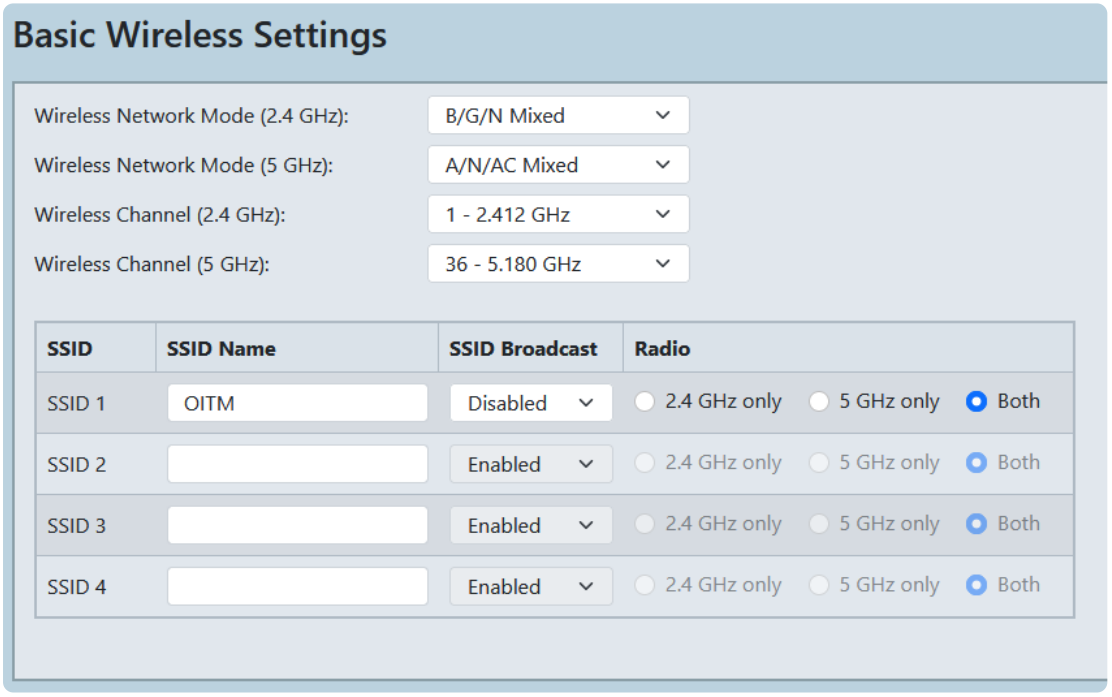
A port úgy van beállítva, hogy a feltételek megsértése esetén ne keletkezzen naplóbejegyzés. Hamis. A beállított violation action *restrict*, amely a feltételek megsértése esetén eldobja a sértést okozó kereteket naplóbejegyzés generálása mellett. *protect* esetén nem keletkezne naplóbejegyzés.

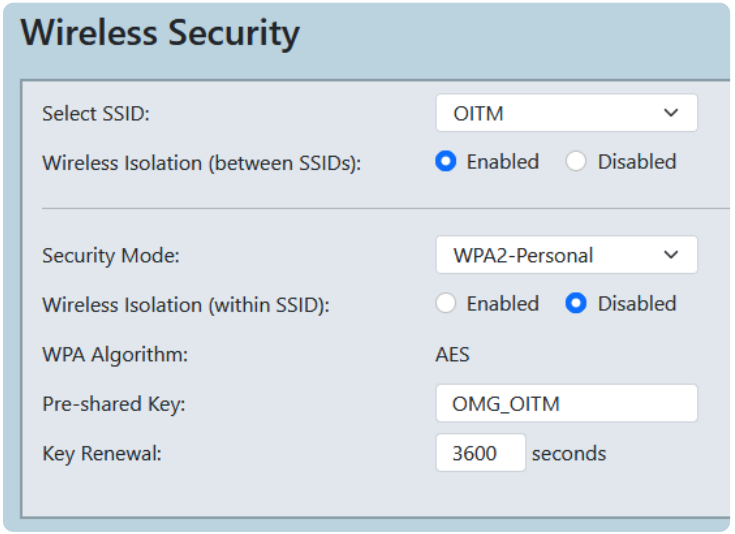
Nem lett megadva egy engedélyezett MAC-cím sem. Ez nem probléma, mert be van kapcsolva a sticky learning.

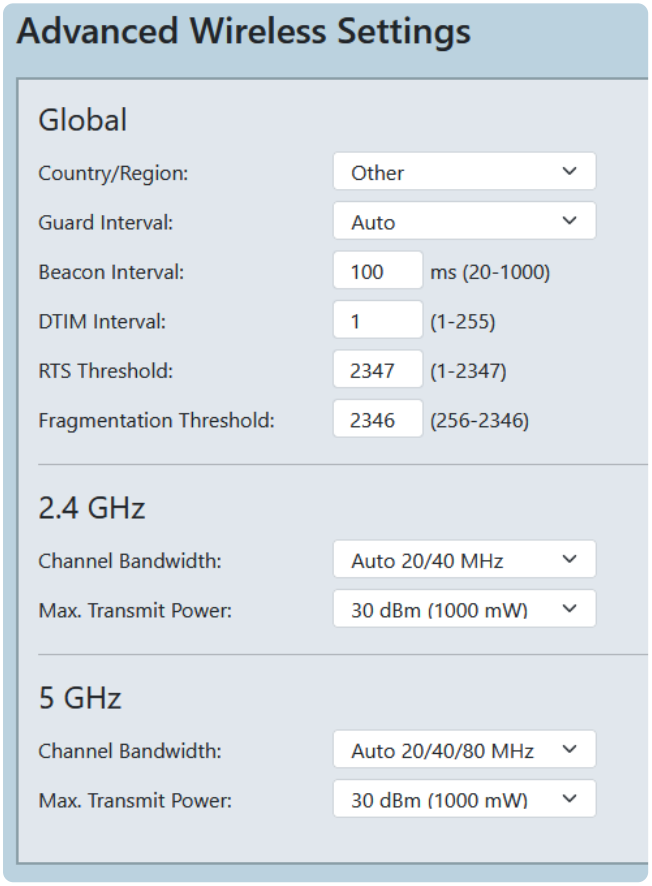
2. feladat 0/5 pont

Új kolléga érkezik a céghez. A kolléga a saját laptopját szeretné behozni, hogy azon dolgozzon, erre kap is engedélyt a biztonsági osztályról. Az íróasztalához leülve azt tapasztalja, hogy nem tud csatlakozni a céges wifihez. Reggel még több más közeli hálózatot felkínált neki az operációs rendszer, csak a cégeset nem. Most viszont már egyetlen vezeték nélküli hálózatot sem látni a laptopról. Eközben neked az íróasztal másik oldalán (kb. 1 méterre) minden rendben működik, meg is nézed, csatlakozva vagy, és látod a szomszédos cégek és épületek hálózatait is. A probléma megoldásával téged bíznak meg.

A céges WAP (Wireless Access Point) beállításai a következők:







A kollégád laptopját megnézve megállapítottad, hogy Intel Dual Band Wireless-N 7260-as modul található benne. Ennek adatlapja a következő:

Intel® Dual Band Wireless-N 7260 Technical Specifications

General

Dimensions (H x W x D)	HMC: 26.80 mm x 30.00 mm x 2.4 mm Max (Top Side) / 1.35 mm Max (Bottom Side) Single Sided M.2: 22 mm x 30.00 mm x 2.4 mm [1.5mm Max (Top Side)/ 0.1mm Max (Bottom Side)]
Weight	TBD
Diversity	Supported
Radio ON/OFF Control	Supported in both hardware and software
Connector interface	HMC: PCIe, USB M.2: PCIe, USB
LED Output	On/Off
Operating Temperature (Adapter Shield)	0º to +80° C
Humidity Non-Operating	50% to 90% RH non-condensing (at temperatures of 25°C to 35°C)
Operating Systems	Microsoft Windows 7*, Microsoft Windows 8*, Linux* (most features not available on Linux)
Wi-Fi Alliance	Wi-Fi CERTIFIED* a/b/g, Wi-Fi CERTIFIED* n, WMM*, WPA*, WPA2*, and WPS, WPS 2.0, Protected Management Frames, Wi-Fi Direct* for peer to peer device connections
IEEE WLAN Standard	IEEE 802.11abgn, 802.11d, 802.11e, 802.11i, 802.11h, 802.11w
Architecture	Infrastructure and SoftAP; Supports simultaneous Client and SoftAP modes
Roaming[9]	Supports seamless roaming between respective access points (802.11b, 802.11g, 802.11a/b/g, 802.11a/b/g/n)
Bluetooth*	Dual Mode Bluetooth* 2.1, 2.1+EDR, 3.0, 3.0+HS, 4.0 (BLE)

Security[10]

Authentication	WPA and WPA2, 802.1X (EAP-TLS, TTLS, PEAP, LEAP, EAP-FAST), EAP-SIM, EAP-AKA
Authentication Protocols	PAP, CHAP, TLS, GTC, MS-CHAP*, MS-CHAPv2
Encryption	64-bit and 128-bit WEP, AES-CCMP, TKIP
Wi-Fi Direct* Encryption and Authentication	WPA2, AES-CCMP
Product Safety	UL, C-UL, CB (IEC 60950-1)
Management Frame Protection	802.11w (WFA- Protected Management Frames)

Compliance

Government	FIPS[11], FISMA
Retail (Credit Card Processing)	PCI, CISP

(Nagyobb változatért kattints ide vagy a képre!)

A fenti információk ismeretében mi okozza vagy mik okozhatják a problémát jelen esetben?

Válaszok

- [ ] Az access point adóteljesítménye túl kicsire van állítva.
- [x] A céges vezeték nélküli hálózat rejtettnek van beállítva.
- [ ] Az access pointon a csatornakiosztás nem automatikusra van beállítva.
- [ ] A laptop WiFi modulja nem támogatja az AP-n beállított hitelesítési módszert.
- [ ] A hitelesítéshez használt RADIUS szervert nem éri el az AP.
- [x] A laptopon be lett kapcsolva a repülő üzemmód (Airplane Mode).
- [ ] A laptop nem támogatja az AP-n beállított egyik WiFi-szabványt (generációt) sem.

Magyarázat

Az alapvető beállítások oldalán látható, hogy az *SSID Broadcast* beállítás *Disabled* értékre van állítva, azaz a laptopon fel kellene venni a céges hálózatot rejtett hálózatként, hogy lehessen csatlakozni. A *reggel még láttam hálózatokat, de most már semmit sem* jellegű esetek pedig általában arra vezethetők vissza, hogy a felhasználó (véletlenül) bekapcsolta a repülő üzemmódot.

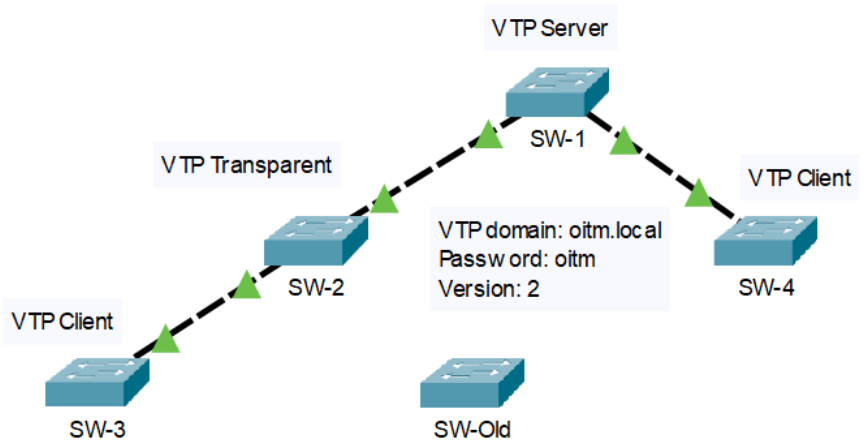
Helytelen válaszok:

> *A laptop nem támogatja az AP-n beállított egyik WiFi-szabványt (generációt) sem.* Hamis. A termék adatlapja alapján a 802.11{a,b,g,n} szabványokat támogatja, amelyek engedélyezve vannak az access pointon is, tehát van bőven közös nevező.
>
> *Az access point adóteljesítménye túl kicsire van állítva.* Hamis. A haladó beállítások oldalon látszik, hogy az adóteljesítmény 1000 mW-ra van állítva, mind 2.4 GHz, mind 5 GHz esetén. 2.4 GHz esetén ez az EU-ban megengedett teljesítmény tízszerese, Amerikában pedig a maximális megengedett érték. 5 GHz esetén mindkét esetben a megengedett érték felett van. (Pontos értékek országonként, érdeklődőknek erre.)
>
> *Az access pointon a csatornakiosztás nem automatikusra van beállítva.* Maga az állítás igaz, de ez nem jelenthet (ilyen szintű) problémát. Bár vannak olyan csatornák, melyek támogatottsága országonként eltérhet, a beállított csatornák nem ilyenek.
>
> *A hitelesítéshez használt RADIUS szervert nem éri el az AP.* Hitelesítési módszernek WPA2-Personal van beállítva, itt nincs is szükség RADIUS szerverre.
>
> *A laptop WiFi modulja nem támogatja az AP-n beállított hitelesítési módszert.* De, támogatja. WPA2 van beállítva, ez szerepel is az adatlapon.

3. feladat 0/5 pont

Az előző héten segítettél megoldani egy VTP-s rejtélyt, de a történet itt nem ért véget. A cég azóta felvett több új dolgozót is, akik részére sajnos nincs elég szabad kapacitás a switchportok tekintetében. Szerencsére találtatok a raktárban egy régi switchet (SW-Old), a terv pedig az, hogy őt bekötitek SW-2-be, a új dolgozókat pedig az SW-Old eszközbe. **Mi fog történni ezek után?**

Pár eszköz mostani állapota, konfigurációja:




```
SW-1# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active
2    Mgmt                 active    Gi0/23
30   Office               active    Gi0/1, Gi0/2, ... [törölve]
40   Servers              active    Gi0/21, Gi0/22
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

```
SW-1# show vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : oitm.local
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCE 0xD4 0x61 0xD0 ... [törölve]
Configuration last modified by 0.0.0.0 at 10-9-21 01:37:30
Local updater ID is 0.0.0.0 (no valid interface found)
```

```
SW-Old# show vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------
1    default              active    Fa0/18, Fa0/19, ... [törölve]
10   Prod                 active    Fa0/1, Fa0/2, ... [törölve]
20   Testing              active    Fa0/15, Fa0/16, Fa0/17
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active
```

```
SW-Old# show vtp status
VTP Version                     : 2
Configuration Revision          : 11
Maximum VLANs supported locally : 255
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : oitm.local
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x85 0x7B 0x78 0xF4 ... [törölve]
Configuration last modified by 0.0.0.0 at 6-8-05 21:01:48
Local updater ID is 0.0.0.0 (no valid interface found)
```

```
SW-Old# show vtp password
VTP Password: oitm
```

Válaszok

- [ ] SW-Old eszközről törlődik a 10-es és a 20-as VLAN.
- [ ] SW-Old eszközre felkerülnek a 2-es, 30-as és 40-es VLAN-ok.
- [x] SW-1 eszközre felkerül a 10-es és 20-as VLAN.
- [x] SW-1 eszközről törlődnek a 2-es, 30-as és 40-es VLAN-ok.
- [ ] SW-2 eszközre felkerül a 10-es VLAN.
- [ ] SW-2 eszközről törlődnek a 2-es, 20-as, 30-as és 99-es VLAN-ok.
- [x] SW-3 eszközre felkerül a 10-es és 20-as VLAN.
- [x] SW-3 eszközről törlődnek a 2-es, 30-as és 40-es VLAN-ok.
- [x] SW-4 eszközre felkerül a 10-es és 20-as VLAN.
- [x] SW-4 eszközről törlődnek a 2-es, 30-as és 40-es VLAN-ok.
- [ ] Semmi nem történik, mert a VTP paraméterei nem egyeznek.

Magyarázat

Mivel a VTP paraméterei (jelszó, domain) egyeznek, az eszközök fognak tudni szinkronizálni egymáshoz. Az SW-Old adatbázisának verziószáma (revision 11) nagyobb mint a jelenlegi eszközökön lévő (revision 8), így mindenki hozzá fog szinkronizálni (annak ellenére is, hogy SW-Old Client módban van!). Mivel rajta nem létezik 2-es, 30-as és 40-es VLAN, ezek törlődni fognak minden eszközről (SW-2-t kivéve), továbbá mindenhová felkerül a 10-es és 20-as VLAN (SW-2-t kivéve). SW-2-n nem változik semmi, mert Transparent módban van továbbra is. Röviden összefoglalva: ezzel a manőverrel sikerült tönkrevágni a VLAN-okat az egész VTP domainben. Ezért fontos ilyenkor előbb átírni a VTP domaint egy garantáltan nem létezőre. Ezzel az adatbázis verziószáma is nullázódik, utána pedig át lehet tenni az eszközt a tényleges domainbe.

4. feladat 0/5 pont

Az alábbiak közül melyek érvényes DHCP-üzenetsorozatok (az RFC 2131 szerint)**?**

Válaszok

- [x] DHCPREQUEST -> DHCPACK
- [ ] DHCPINFORM -> DHCPDECLINE
- [ ] DHCPRENEW -> DHCPNAK
- [x] DHCPREQUEST -> DHCPNAK
- [x] DHCPDISCOVER -> DHCPOFFER -> DHCPREQUEST -> DHCPACK
- [ ] DHCPRELEASE -> DHCPNAK

Magyarázat

Az RFC szövege. A helyes megoldások a szöveg megfelelő részeit elolvasva és értelmezve vagy a 34. oldal 5. ábráját végigkövetve is levezethetők:

DHCPDISCOVER -> DHCPOFFER -> DHCPREQUEST -> DHCPACK Helyes. Az egyik leggyakoribb üzenetsorozat, amelyen keresztül egy kliens a semmiből kiindulva IP-címet szerez magának. DHCP kiszolgálókat keres (DISCOVER), tőlük ajánlatot kap (OFFER), választ és kér egy IP-címet (REQUEST), majd a kérést a választott szerver pozitívan nyugtázza (ACK).

DHCPREQUEST -> DHCPACK Helyes. A másik leggyakoribb üzenetsorozat. A kliens egy már korábban megkapott címbérletet szeretne meghosszabbítani, ezt a szerver nyugtázza.

DHCPRENEW -> DHCPNAK Helytelen. DHCPRENEW üzenettípus nem létezik. Címbérlet megújítására az előző pontban említett üzenetsorozat használatos.

DHCPREQUEST -> DHCPNAK Helyes. A kliens (hosszabbítási) kérését a szerver valamilyen okból negatív nyugtával (NAK) elutasítja (például változott a hálózat, a kliens vagy a szerver beállításai).

DHCPINFORM -> DHCPDECLINE Helytelen. Információkérésre (INFORM) a szerver mindig pozitív nyugtával válaszol. DHCPDECLINE üzenetet a szerver nem is küldhet, azt a kliens küldi a szervernek, ha a címszerzési folyamat során kiderül, hogy a szóban forgó címet más eszköz használja a hálózaton.

DHCPRELEASE -> DHCPNAK Helytelen. Az egy érvényes címbérletről való lemondást jelző (RELEASE) üzenetre nem küld választ a szerver, negatív nyugtát nem is igazán lenne értelme küldenie.

© 2022 Human Priority Kft.