A Pentagon hálózati felépítése



Kivitelező: Horribili Kft.

Cég tulajdonosok:

Fülöp Krisztián Szilárd

Móricz Flávió

Tartalomjegyzék

[1. Hálózat leírása 4](#_Toc131171526)

[1.1 Hálózat tervezése 4](#_Toc131171527)

[1.2 Hálózat felépítése 4](#_Toc131171528)

[1. ábra: Hálózat logikai felépítése 5](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171529)

[2. ábra: Hálózat fizikai felépítése 6](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171530)

[2. VLAN 7](#_Toc131171531)

[1. táblázat: Kapcsolókon átengedett VLAN-ok interfacenként 7](#_Toc131171532)

[2. táblázat: VLAN-ok neve és IP tartománya részlegenként 8](#_Toc131171533)

[3. IP-címek 8](#_Toc131171534)

[3.1 DHCP 8](#_Toc131171535)

[3. táblázat: IP-cím tartományok a DHCP szolgáltatásban 8](#_Toc131171536)

[3. ábra: DHCP szolgáltatás a DHCP szerveren 9](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171537)

[3.2 Statikus 10](#_Toc131171538)

[4. táblázat: Eszköz IP-címek 10](#_Toc131171539)

[4. Biztonság 11](#_Toc131171540)

[4.1 Biztonsági beállítások 11](#_Toc131171541)

[4.2 Jelszavak 11](#_Toc131171542)

[5. táblázat: Jelszavak 11](#_Toc131171543)

[5. STP 12](#_Toc131171544)

[4. ábra: SERVER\_SW show spanning-tree részlet 12](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171545)

[5. ábra: SPACEFORCE\_SW show spanning-tree részlet 12](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171546)

[6. ábra: NAVY\_SW show running config részlet 13](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171547)

[6. Etherchannel 13](#_Toc131171548)

[7. ábra: AIRFORCE\_SW show interfaces etherchannel 13](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171549)

[6. táblázat: Etherchannel eszközök 14](#_Toc131171550)

[7. Tesztelés 14](#_Toc131171551)

[7.1 Show parancsok 14](#_Toc131171552)

[8. ábra: SERVER\_SW VLAN-ok 14](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171553)

[9. ábra: AIRFORCE\_SW VLAN-ok 14](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171554)

[10. ábra: SPACEFORCE\_SW Fa0/2 portja (show running config részlet) 15](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171555)

[11. ábra: ARMY\_SW Gig0/1 (SERVER\_SW felé néző) portja (show interfaces gig0/1 switchport részlet) 15](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171556)

[7.2 Ping parancsok 15](#_Toc131171557)

[12. ábra: PC10 (172.16.1.3) – SPACEFORCE\_SERVER (172.16.1.2) ping 15](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171558)

[13. ábra: PC20(2) (172.16.1.37) – NAVY\_SERVER (172.16.1.66) ping 16](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171559)

[14. ábra: NAVY\_SW (172.16.1.134) – Admin PC (172.16.1.158) ping 17](file:///C:\Users\Krissssz\Desktop\Horribili%20Pentagon%20hálózati%20felépítése.docx#_Toc131171560)

# 1. Hálózat leírása

## 1.1 Hálózat tervezése

A Horribili céget megkérte az Amerikai Egyesült Államok hadügyminisztere, hogy a Pentagon hálózatát korszerűsítsük, ugyanis az újonnan felmerülő orosz, és indiai hackerek támadásától tartanak.

A terv az, hogy a különböző hadosztályokat saját szerverrel és VLAN-nal szereljük fel, így csak felügyelettel férnek hozzá egymás szigorúan titkos adataihoz.

Négy hadosztályt különítünk el:

* Űrhadosztály (Space Force, SPACEFORCE)
* Légierő (Air Force, AIRFORCE)
* Szárazföldi erő (Army, ARMY)
* Tengerészgyalogság (Navy, NAVY)

*A hálózatot 2023 márciusában a Horribili Kft. további biztonságot és redundanciát elősegítő fejlesztésekkel bővítette, a dokumentációt kellően frissítette.*

## 1.2 Hálózat felépítése

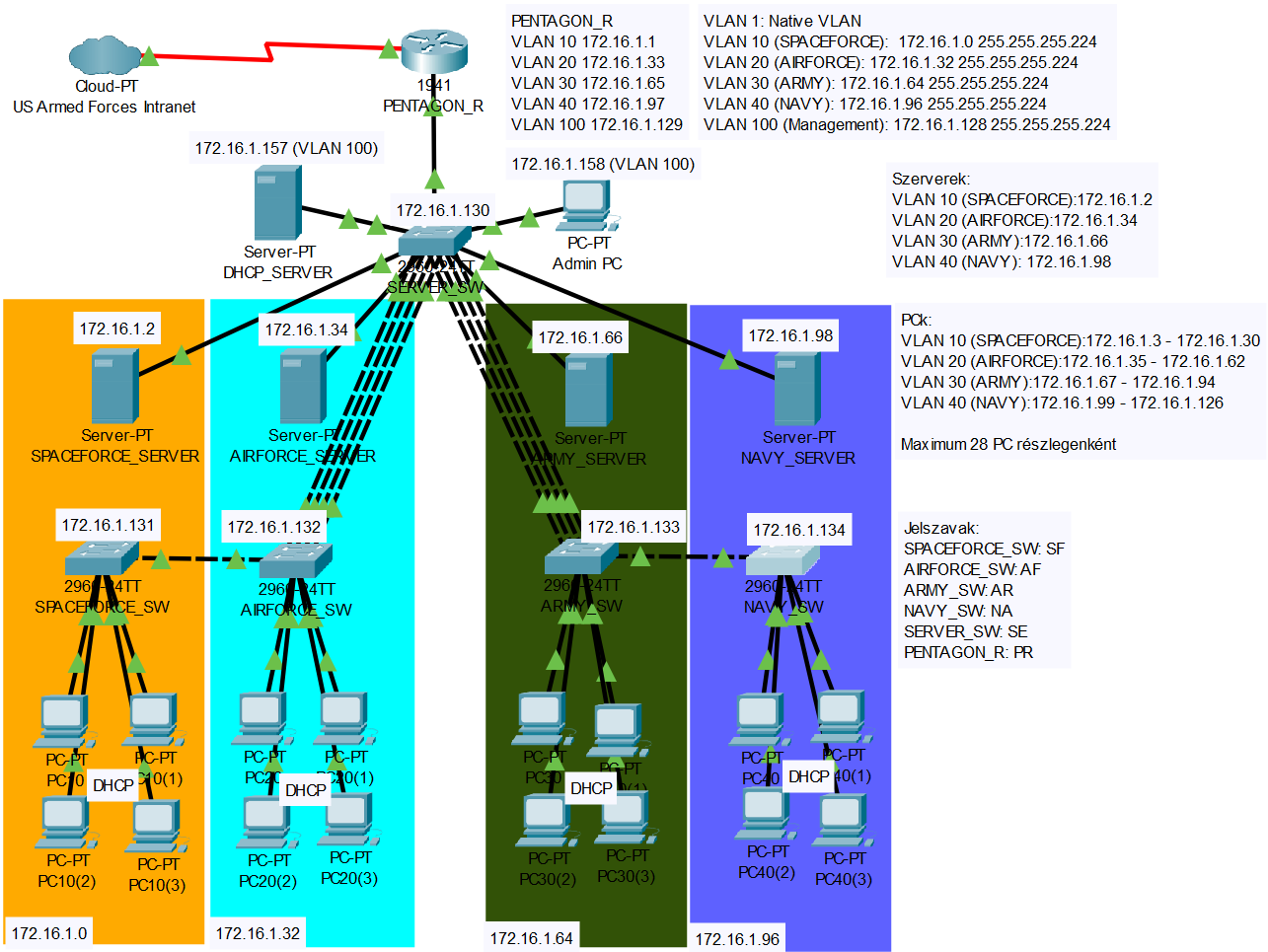
A hálózat összeköt:

* 17 számítógépet (részlegenként 4 PC, 1 Admin PC)
* 5 szervert (részlegenként 1 szerver, 1 DHCP server)

A felhasznált forgalomirányító eszközök:

* 5 Cisco 2960-24TT kapcsoló
* 1 Cisco 1941 router (1 db HWIC-2T 2 portos serial bővítőkártyával)

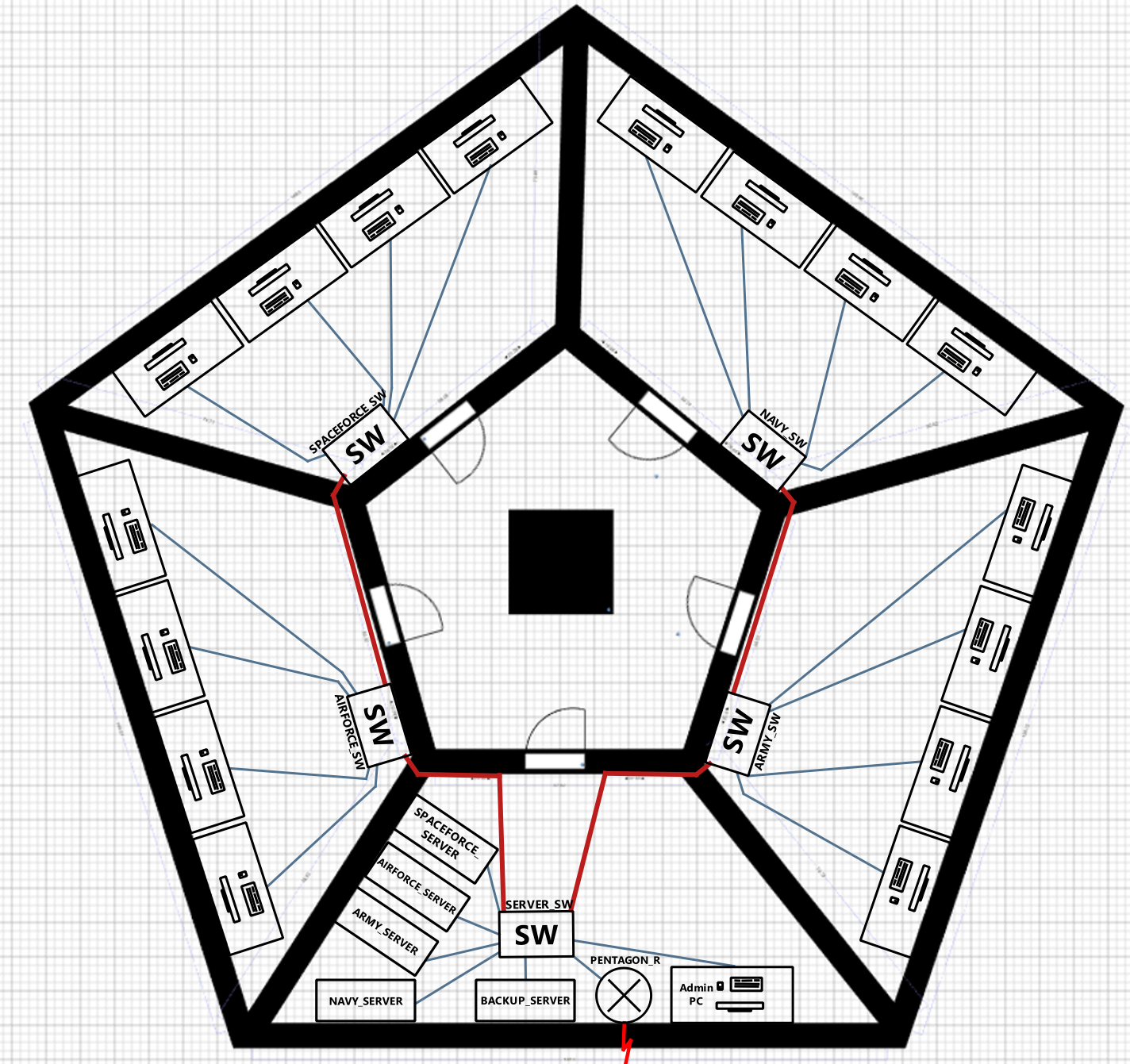
A hálózat 5 alhálózatból áll, ebből 4 a hadosztályoknak fenntarott, 1 pedig a managementnek. A hálózat logikai és fizikai felépítése a *1.* és a *2. ábrán* láthatók



### 1. ábra: Hálózat logikai felépítése



### 2. ábra: Hálózat fizikai felépítése



# 2. VLAN

A VLAN-ok arra szolgálnak, hogy a hadosztályokat elszigeteljék egymástól. A hadosztályok saját szerverüket gyorsabban, router nélkül is elérik, de más szervert lassabban és csak a router felügyeletén keresztül érik el. A VLAN-ok nevei és IP tartománya a *2. táblázatban* láthatók

Minden kapcsoló csak olyan VLAN forgalmát engedi át a trunk portjain, ami szükséges a hálózat működéséhez, ezzel csökkentve az egész hálózat terhelését. Az engedélyezett forgalmat mutatja a *1. táblázat*

Ezen felül a kapcsolók nem ismerik azokat a VLAN-okat, amikre működésük közben nincs szükségül

### 1. táblázat: Kapcsolókon átengedett VLAN-ok interfacenként

|  |  |  |  |
| --- | --- | --- | --- |
| Eszköz | Interface | Port típusa | Átengedett VLAN |
| SERVER\_SW | Fa0/1 | Access | 10 |
| Fa0/2 | 20 |
| Fa0/3 | 30 |
| Fa0/4 | 40 |
| Fa0/10 | 100 |
| Fa0/11 |
| Fa0/5 | Trunk | All |
| Port-channel1 | 10, 20, 100 |
| Port-channel2 | 30, 40, 100 |
| AIRFORCE\_SW | Port-channel1 | 10, 20, 100 |
| Gig0/2 | 10, 100 |
| Fa0/1 – Fa0/4 | Access | 20 |
| SPACEFORCE\_SW | Gig0/1 | Trunk | 10, 100 |
| Fa0/1 – Fa0/4 | Access | 10 |
| ARMY\_SW | Port-channel2 | Trunk | 30, 40, 100 |
| Gig0/2 | 40, 100 |
| Fa0/1 – Fa0/4 | Access | 30 |
| NAVY\_SW | Gig0/1 | Trunk | 40. 100 |
| Fa0/1 – Fa0/4 | Access | 30 |

### 2. táblázat: VLAN-ok neve és IP tartománya részlegenként

|  |  |  |  |
| --- | --- | --- | --- |
| Részleg | VLAN | IP-cím | Alhálózati maszk |
| SPACEFORCE | VLAN 10 | 172.16.1.0 | 255.255.255.224 |
| AIRFORCE | VLAN 20 | 172.16.1.32 | 255.255.255.224 |
| ARMY | VLAN 30 | 172.16.1.64 | 255.255.255.224 |
| NAVY | VLAN 40 | 172.16.1.92 | 255.255.255.224 |
| Management | VLAN 100 | 172.16.1.128 | 255.255.255.224 |

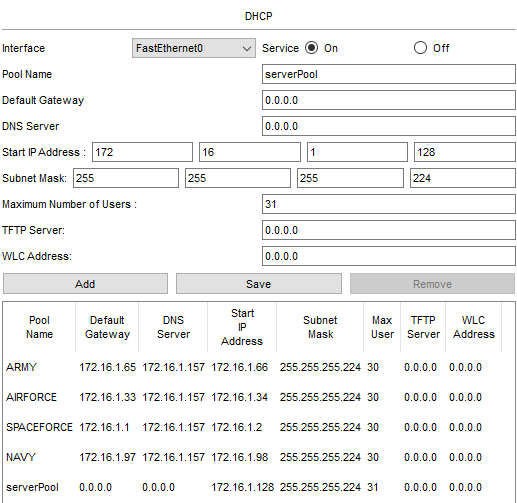
# 3. IP-címek

## 3.1 DHCP

A Pentagon elsőszámú szerverén van DHCP szolgáltatás. Minden részlegnek van saját pool-ja, mindegyik maximum 30 szabad IP-címmel. Az IP-cím tartományok a *3. táblázatban* látható. A szerveren látható szolgáltatást pedig a *3. ábrán* látható.

### 3. táblázat: IP-cím tartományok a DHCP szolgáltatásban

|  |  |  |  |
| --- | --- | --- | --- |
| Hadosztály | IP-cím tartomány | Alhálózati maszk | Alapértelmezett átjáró |
| SPACEFORCE | 172.16.1.0 | 255.255.255.224 | 172.16.1.1 |
| AIRFORCE | 172.16.1.32 | 172.16.1.33 |
| ARMY | 172.16.1.64 | 172.16.1.65 |
| NAVY | 172.16.1.96 | 172.16.1.97 |



### 3. ábra: DHCP szolgáltatás a DHCP szerveren

## 3.2 Statikus

Minden kapcsoló, szerver, router és az Admin PC statikus IP címet kapott. Ezek a *4. táblázat*ban láthatók

### 4. táblázat: Eszköz IP-címek

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Eszköz | Interface | IP-cím | Alhálózati maszk | Alapértelmezett átjáró |
| PENTAGON\_R | Gig0/0.10 | 172.16.1.1 | 255.255.255.224 | \_\_\_ |
| Gig0/0.20 | 172.16.1.33 |
| Gig0/0.30 | 172.16.1.65 |
| Gig0/0.40 | 172.16.1.97 |
| Gig0/0.100 | 172.16.1.129 |
| SERVER\_SW | VLAN 100 | 172.16.1.130 | 172.16.1.129 |
| SPACEFORCE\_SW | 172.16.1.131 |
| AIRFORCE\_SW | 172.16.1.132 |
| ARMY\_SW | 172.16.1.133 |
| NAVY\_SW | 172.16.1.134 |
| SPACEFORCE\_SERVER | Fa0 | 172.16.1.2 | 172.16.1.1 |
| ARIFORCE\_SERVER | 172.16.1.34 | 172.16.1.33 |
| ARMY\_SERVER | 172.16.1.66 | 172.16.1.65 |
| NAVY\_SERVER | 172.16.1.98 | 172.16.1.97 |
| DHCP\_SERVER | 172.16.1.157 | 172.16.1.129 |
| Admin PC | 172.16.1.158 |

# 4. Biztonság

## 4.1 Biztonsági beállítások

* Az összes nem használt port le lett kapcsolva a kapcsolókon és a routeren.
* A kapcsolók hozzáférési portonként csak egy MAC-címet tanulnak meg, és ezt automatikusan a ragadós portbiztonsági módszer miatt.
* Távolról a telnettel szemben csak a biztonságosabb version 2 SSH-n keresztül konfigurálhatók az eszközök.
* Minden kapcsolóporton ki van kapcsolva a DTP.
* A jelszavak titkosítva vannak.
* Minden eszköz beállításai el vannak mentve induló konfigurációként, így áramszünet után sincs biztonsági rés a hálózaton (Esetleges meghibásodás esetén a konfigurációk a DHCP serverre is el vannak mentve)
* BPDU Guard minden access porton

## 4.2 Jelszavak

A biztonsági beállításokon kívül minden eszköz jelszóval van védve. Ezek a *5. táblázat*ban láthatók:

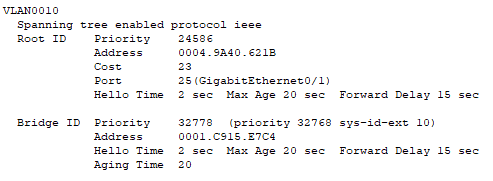
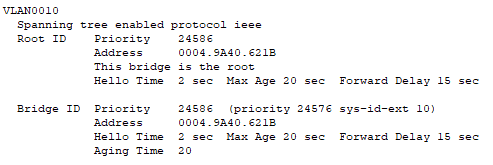
### 5. táblázat: Jelszavak

|  |  |  |
| --- | --- | --- |
| Eszköz | Jelszótípus | Jelszó |
| SPACEFORCE\_SW | enable  console  vty | SF |
| AIRFORCE\_SW | enable  console  vty | AF |
| ARMY\_SW | enbale  console  vty | AR |
| NAVY\_SW | enable  console  vty | NA |
| SERVER\_SW | enable  console  vty | SE |
| PENTAGON\_R | enable  console  vty | PR |

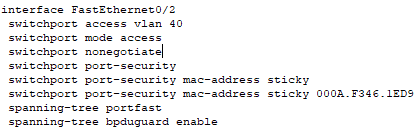
# 5. STP

Minden kapcsolón PVST+ (Per VLAN spanning tree) fut, minden VLAN primary root-ja a SERVER\_SW. Sikeres STP root híd kiválasztás a *4-5. ábrán* látható.

### 4. ábra: SERVER\_SW show spanning-tree részlet



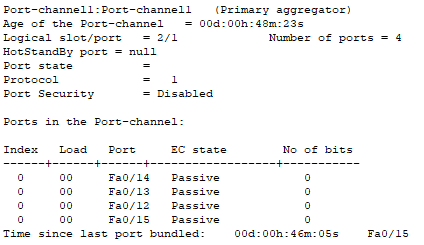
### 5. ábra: SPACEFORCE\_SW show spanning-tree részlet

Az access portok PortFast módban vannak, így nem vesznek részt az STP folyamatban. Ezeken a portokon BPDU Guard is üzemel. Példa ezek beállításaira a *6. ábrá*n látható

### 6. ábra: NAVY\_SW show running config részlet

# 6. Etherchannel

A nagyobb sávszélesség és megbízhatóság érdekében a SERVER\_SW-hez több kábelen keresztül csatlakoznak a kapcsolók. Ezeknek a leírása a *6. táblázat*ban látható

 Az Etherchannel dinamikusan, LACP-vel van konfigurálva, ami a SERVER\_SW oldalán aktív, a másik oldalon passzív. Egy Etherchannel jellemzése látható a *7. ábrá*n

### 7. ábra: AIRFORCE\_SW show interfaces etherchannel

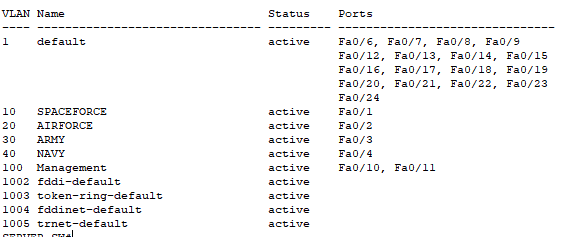
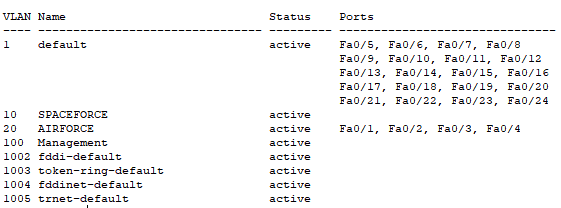
### 6. táblázat: Etherchannel eszközök

|  |  |  |  |
| --- | --- | --- | --- |
| Etherchannel eszközök | Kiinduló portok | Csatlakozó portok | Portok száma kapcsolónként |
| SERVER\_SW (aktív) - AIRFORCE\_SW (passzív) | fa0/12-15 | fa0/12-15 | 4 |
| SERVER\_SW (aktív) - ARMY\_SW (passzív) | fa0/16-19 | fa0/16-19 | 4 |

# 7. Tesztelés

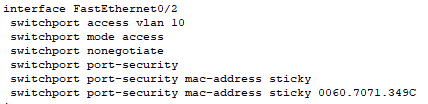
## 7.1 Show parancsok

A SERVER\_SW VLAN táblázata, ami minden VLAN-t tartalmaz, és az AIRFORCE\_SW VLAN táblázata, ami csak azt, ami szükséges a működéséhez a *8.* és *9. ábrán látható*:

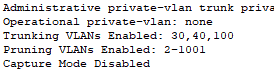


### 8. ábra: SERVER\_SW VLAN-ok

### 9. ábra: AIRFORCE\_SW VLAN-ok

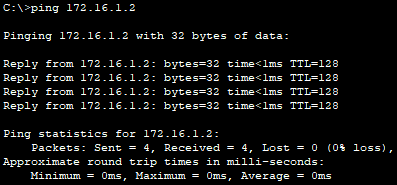
A hozzáférési portok biztonsági konfigurációjára egy példa az *10. ábrán* látható:

### 10. ábra: SPACEFORCE\_SW Fa0/2 portja (show running config részlet)

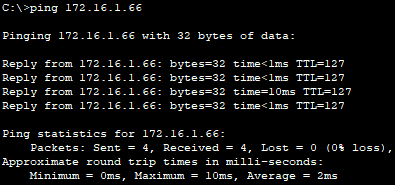
A trunk portok forgalomszabályozására egy példa a *11. ábrán* látható:

### 11. ábra: ARMY\_SW Gig0/1 (SERVER\_SW felé néző) portja (show interfaces gig0/1 switchport részlet)

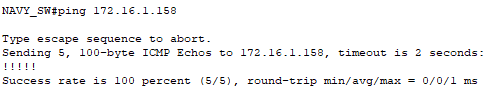
## 7.2 Ping parancsok

VLAN-on belüli forgalomirányítás tesztelése egy PC saját hadosztályához tartozó szerverének pingelésével a *12. ábrán* látható:

### 12. ábra: PC10 (172.16.1.3) – SPACEFORCE\_SERVER (172.16.1.2) ping

VLAN közti forgalomirányítás tesztelése egy PC hadosztályán kívül lévő szerver pingelésével a   
*13. ábrán* látható:

### 13. ábra: PC20(2) (172.16.1.37) – NAVY\_SERVER (172.16.1.66) ping

A management VLAN forgalomirányításának tesztelése egy kapcsolóról az Admin PC pingelésével a *14. ábrán* látható:

### 14. ábra: NAVY\_SW (172.16.1.134) – Admin PC (172.16.1.158) ping