A Pentagon hálózati felépítése



Kivitelező: Horribili Kft.

Cég tulajdonosok:

Fülöp Krisztián Szilárd

Móricz Flávió

Tartalomjegyzék

[1. Hálózat leírása 3](#_heading=h.30j0zll)

[1.1 Hálózat tervezése 3](#_heading=h.1fob9te)

[1.2 Hálózat felépítése 3](#_heading=h.3znysh7)

[1. ábra: Hálózat logikai felépítése](about:blank) 4

[2. ábra: Hálózat fizikai felépítése](about:blank) 5

[2. VLAN 6](#_heading=h.2et92p0)

[1. táblázat: Kapcsolókon átengedett VLAN-ok portonként 6](#_heading=h.tyjcwt)

[2. táblázat: VLAN-ok neve és IP tartománya részlegenként 7](#_heading=h.3dy6vkm)

[3. IP-címek 7](#_heading=h.1t3h5sf)

[3. táblázat: Hadosztályba tartozó PC IP-címek 7](#_heading=h.4d34og8)

[4. táblázat: Eszköz IP-címek 8](#_heading=h.2s8eyo1)

[4. Biztonság 8](#_heading=h.17dp8vu)

[4.1 Biztonsági beállítások 8](#_heading=h.3rdcrjn)

[4.2 Jelszavak 9](#_heading=h.26in1rg)

[5. táblázat: Jelszavak 9](#_heading=h.lnxbz9)

[5. Tesztelés 9](#_heading=h.35nkun2)

[5.1 Show parancsok 9](#_heading=h.1ksv4uv)

[3. ábra: SERVER\_SW VLAN-ok](about:blank) 10

[4. ábra: AIRFORCE\_SW VLAN-ok](about:blank) 10

[5. ábra: SPACEFORCE\_SW Fa0/2 portja (show running config részlet)](about:blank) 10

[6. ábra: ARMY\_SW Gig0/1 portja (show interfaces gig0/1 switchport részlet)](about:blank) 11

[5.2 Ping parancsok 11](#_heading=h.44sinio)

[7. ábra: PC10 (172.16.1.3) – SPACEFORCE\_SERVER (172.16.1.2) ping](about:blank) 11

[8. ábra: PC20(2) (172.16.1.37) – NAVY\_SERVER (172.16.1.66) ping](about:blank) 11

[9. ábra: NAVY\_SW (172.16.1.134) – Admin PC (172.16.1.158) ping](about:blank) 12

# 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-al 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)

## 1.2 Hálózat felépítése

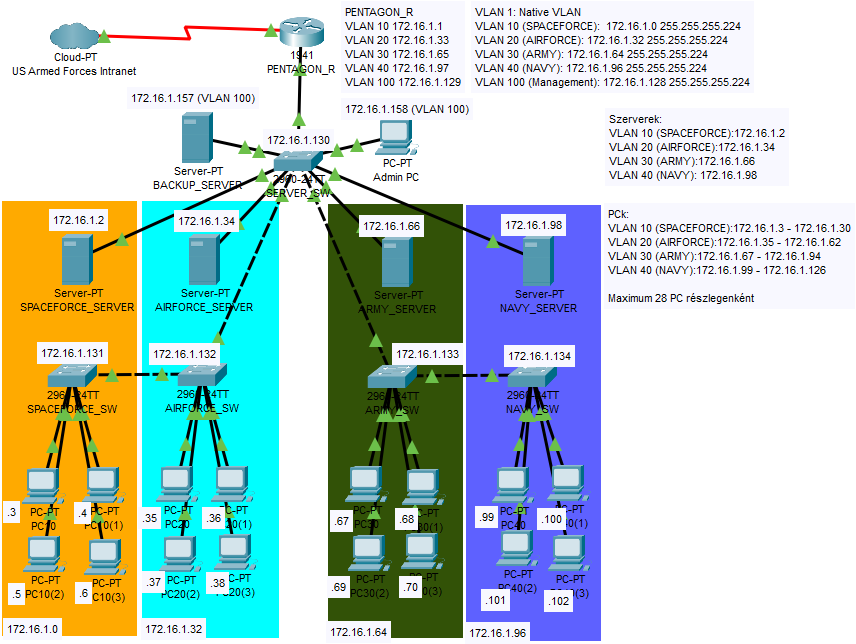
A hálózat összeköt:

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

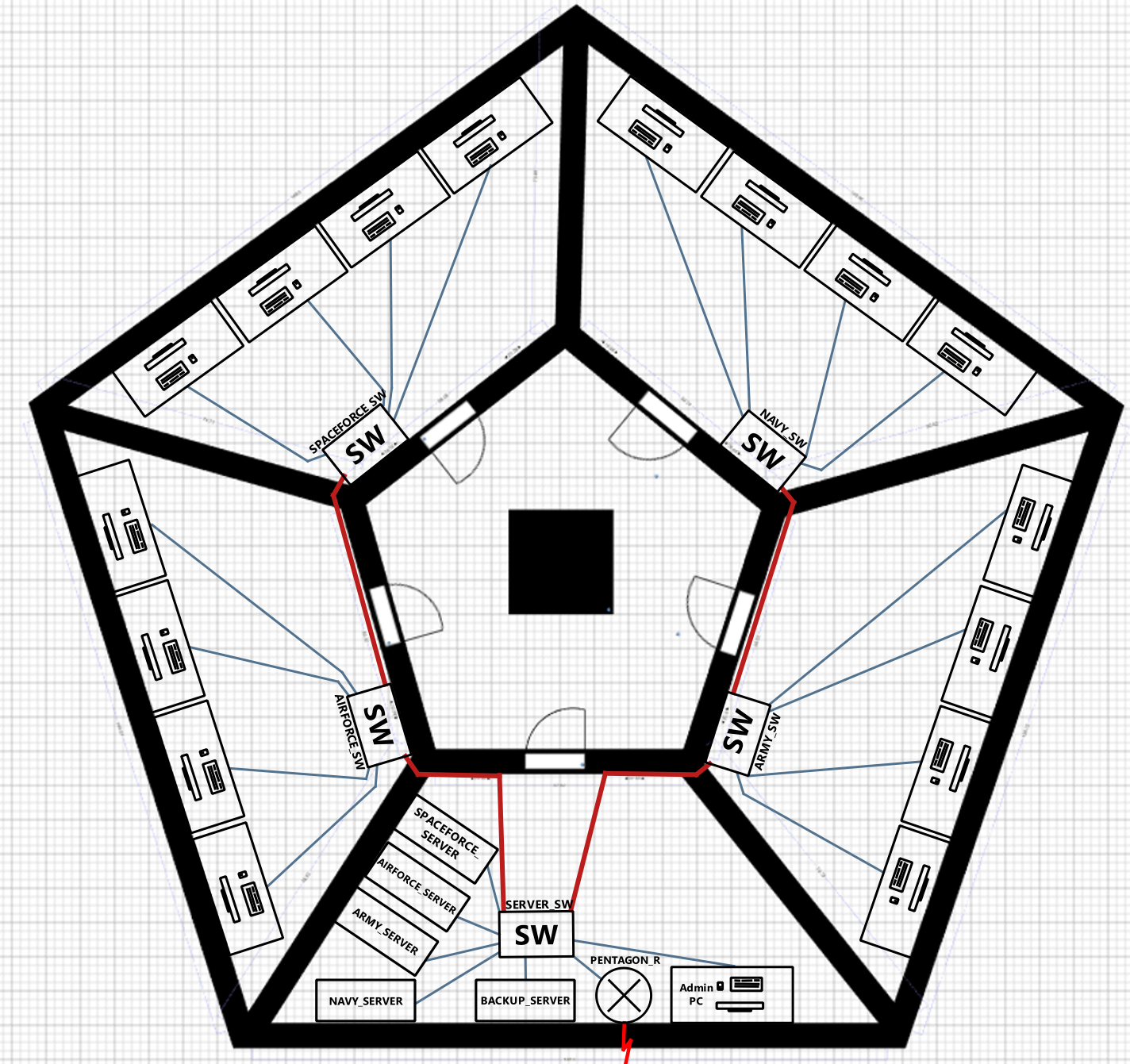
A felhasznált forgalomirányító eszközök:

* 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







# 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 trunkportjain, 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 portonként

| 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 |
| Gig0/1 | 10, 20, 100 |
| Gig0/2 | 30, 40, 100 |
| AIRFORCE\_SW | Gig0/1 | 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 | Gig0/1 | 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 | 255.255.255.0 |

# 3. IP-címek

Minden hadosztálynak és a managementnek van egy saját /27-es alhálózata, ami 30 eszköz csatlakoztatását engedélyezi alhálózatonként. Hadosztályonként maximum 24 PC üzemeltethető a kapcsolók bővítése nélkül, de az épületben jelenleg csak 4 PC van hadosztályonként.

A PC-k és eszközök IP-címei a *3.* és *4. táblázat*ban láthatók:

### 3. táblázat: Hadosztályba tartozó PC IP-címek

| Hadosztály | Interface | IP-cím tartomány | Alhálózati maszk | Alapértelmezett átjáró |
| --- | --- | --- | --- | --- |
| SPACEFORCE | Fa0 | 172.16.1.3 - 172.16.1.6 | 255.255.255.224 | 172.16.1.1 |
| AIRFORCE | 172.16.1.35 - 172.16.1.38 | 172.16.1.33 |
| ARMY | 172.16.1.67 - 172.16.1.70 | 172.16.1.65 |
| NAVY | 172.16.1.99 - 172.16.1.102 | 172.16.1.97 |

### 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 |
| BACKUP\_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 backup serverre is el vannak mentve)

## 4.2 Jelszavak

A biztonsági beállításokon kívül minden eszköz jelszóval van védve. Ezek a *4. táblázat*ban láthatók:

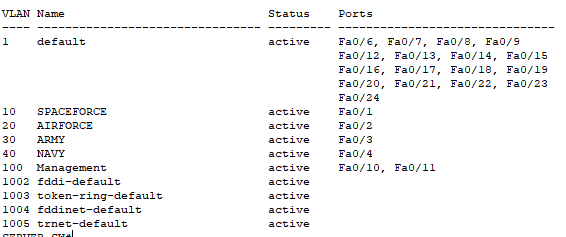
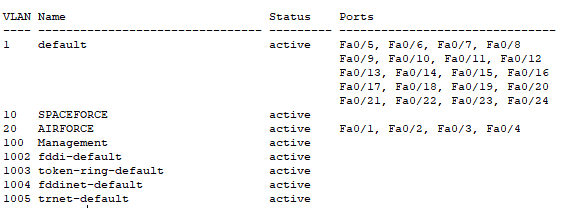
### 5. táblázat: Jelszavak

| 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 |

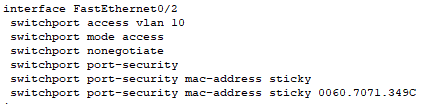
# 5. Tesztelés

## 5.1 Show parancsok

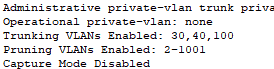
A SERVER\_SW VLAN táblázata, ami minden VLAN-t tartalmaz, és az AIRFORCE\_SW VLAN táblázata, ami csak azt, ami szükséges a működéséhez a *3.* és *4. ábrán látható*:





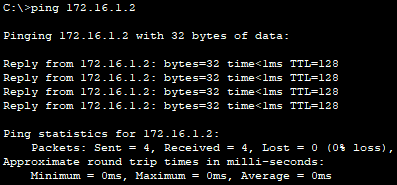
A hozzáférési portok biztonsági konfigurációjára egy példa az *5. ábrán* látható:



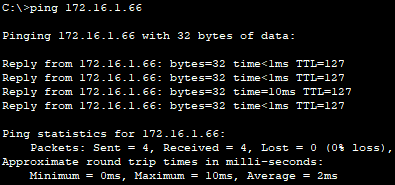
A trunk portok forgalomszabályozására egy példa a *6. ábrán* látható:



## 5.2 Ping parancsok

VLAN-on belüli forgalomirányítás tesztelése egy PC saját hadosztályához tartozó szerverének pingelésével a *7. ábrán* látható:



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

A management VLAN forgalomirányításának tesztelése egy kapcsolóról az Admin PC pingelésével a *9. ábrán* látható: