



A Pentagon hálózati felépítése

Kivitelező: Horribili Kft.

Cég tulajdonosok:

Fülöp Krisztián Szilárd

Móricz Flávió

Tartalomjegyzék

1. Hálózat leírása	4
1.1 Hálózat tervezése.....	4
1.2 Hálózat felépítése	4
1. ábra: Hálózat logikai felépítése.....	5
2. ábra: Hálózat fizikai felépítése.....	6
2. VLAN	7
1. táblázat: Kapcsolókon átengedett VLAN-ok interfacenként.....	7
2. táblázat: VLAN-ok neve és IP tartománya részlegenként.....	8
3. IP-címek	8
3.1 DHCP	8
3. táblázat: IP-cím tartományok a DHCP szolgáltatásban.....	8
3. ábra: DHCP szolgáltatás a DHCP szerveren	9
3.2 Statikus	10
4. táblázat: Eszköz IP-címek.....	10
4. Biztonság	11
4.1 Biztonsági beállítások	11
4.2 Jelszavak.....	11
5. táblázat: Jelszavak.....	11
5. STP	12
4. ábra: SERVER_SW show spanning-tree részlet	12
5. ábra: SPACEFORCE_SW show spanning-tree részlet	12
6. ábra: NAVY_SW show running config részlet	13
6. Etherchannel.....	13
7. ábra: AIRFORCE_SW show interfaces etherchannel	13
6. táblázat: Etherchannel eszközök	14
7. Tesztelés	14

7.1 Show parancsok.....	14
8. ábra: SERVER_SW VLAN-ok.....	14
9. ábra: AIRFORCE_SW VLAN-ok	14
10. ábra: SPACEFORCE_SW Fa0/2 portja (show running config részlet)	15
11. ábra: ARMY_SW Gig0/1 (SERVER_SW felé néző) portja (show interfaces gig0/1 switchport részlet).....	15
7.2 Ping parancsok	15
12. ábra: PC10 (172.16.1.3) – SPACEFORCE_SERVER (172.16.1.2) ping	15
13. ábra: PC20(2) (172.16.1.37) – NAVY_SERVER (172.16.1.66) ping	16
14. ábra: NAVY_SW (172.16.1.134) – Admin PC (172.16.1.158) ping	17

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

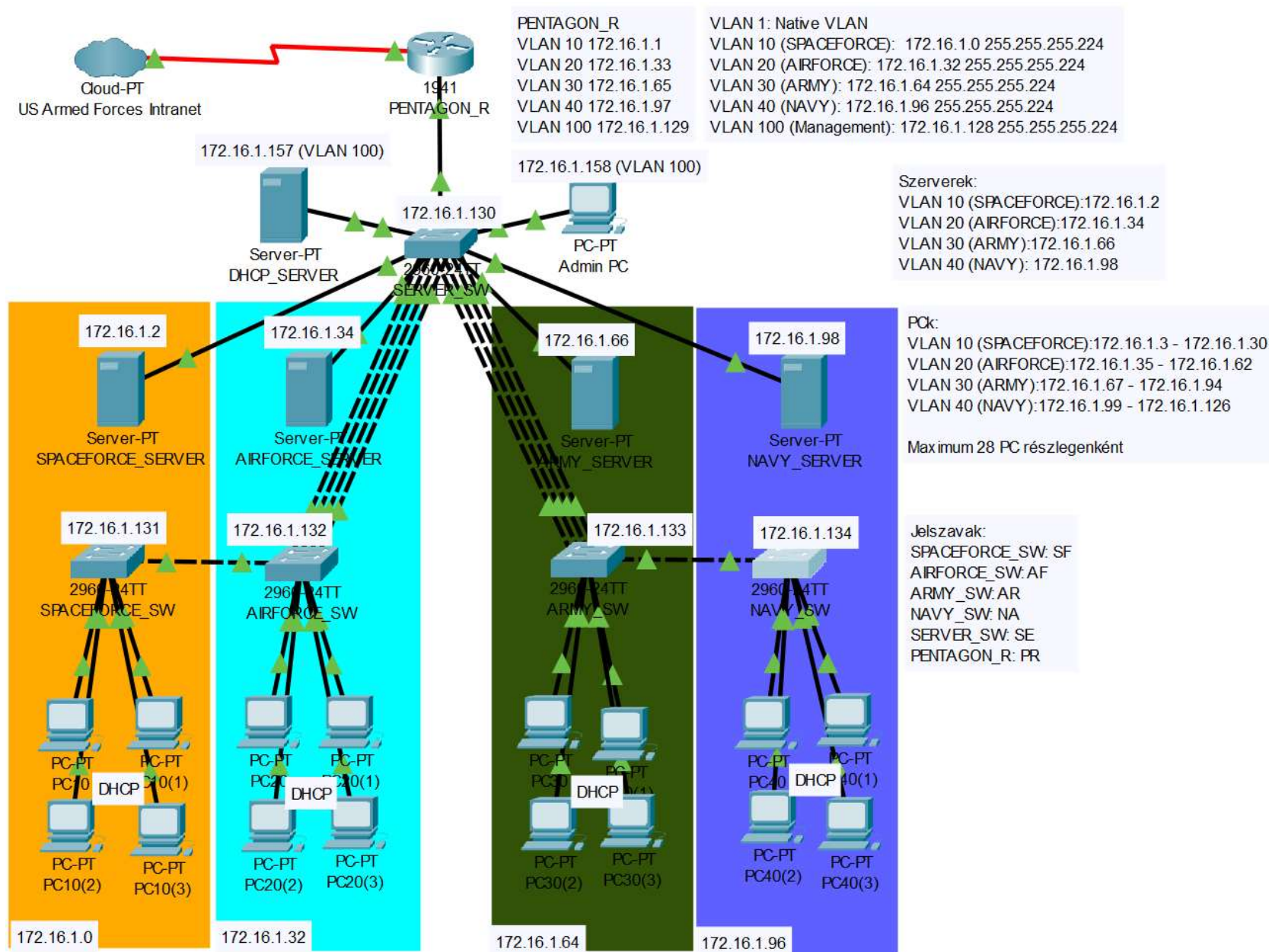
A hálózat összeköt:

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

A felhasznált forgalomirányító eszközök:

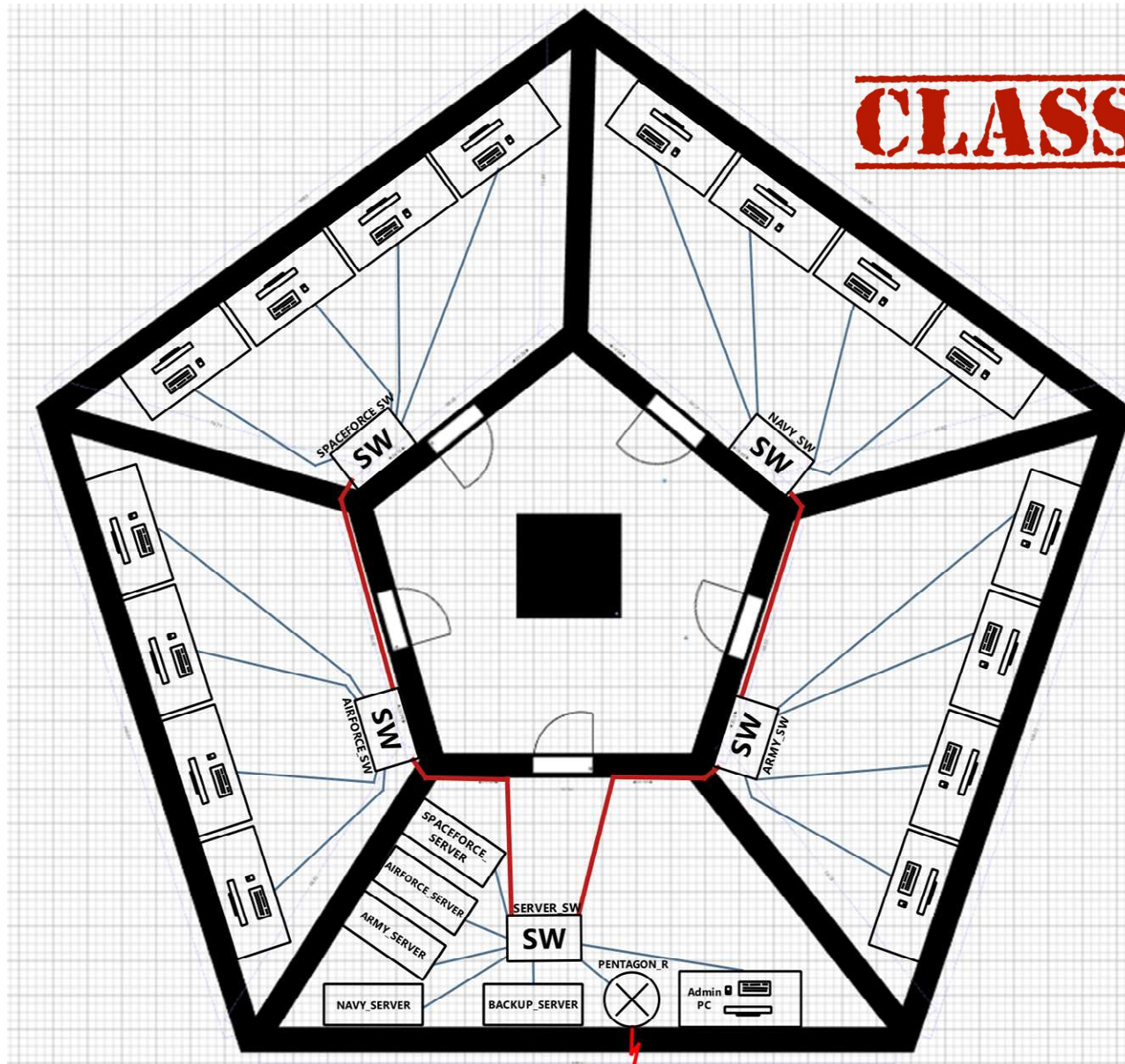
- 5 Cisco 2960-24TT kapcsoló
- 1 Cisco 1941 router (1 db HWIC-2T 2 portos serial bővítőkártyával)

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

CLASSIFIED



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

DHCP

Interface	FastEthernet0			Service	<input checked="" type="radio"/> On	<input type="radio"/> Off
Pool Name	serverPool					
Default Gateway	0.0.0.0					
DNS Server	0.0.0.0					
Start IP Address :	172	16	1	128		
Subnet Mask:	255	255	255	224		
Maximum Number of Users :	31					
TFTP Server:	0.0.0.0					
WLC Address:	0.0.0.0					
Add		Save			Remove	

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
ARMY	172.16.1.65	172.16.1.157	172.16.1.66	255.255.255.224	30	0.0.0.0	0.0.0.0
AIRFORCE	172.16.1.33	172.16.1.157	172.16.1.34	255.255.255.224	30	0.0.0.0	0.0.0.0
SPACEFORCE	172.16.1.1	172.16.1.157	172.16.1.2	255.255.255.224	30	0.0.0.0	0.0.0.0
NAVY	172.16.1.97	172.16.1.157	172.16.1.98	255.255.255.224	30	0.0.0.0	0.0.0.0

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. táblázatban 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. táblázatban láthatók:

5. táblázat: Jelszavak

Eszköz	Jelszótípus	Jelszó
SPACEFORCE_SW	enable console vty	SF
AIRFORCE_SW	enable console vty	AF
ARMY_SW	enable 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.

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    0004.9A40.621B
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24586 (priority 24576 sys-id-ext 10)
           Address    0004.9A40.621B
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  20
```

4. ábra: SERVER_SW show spanning-tree részlet

```
VLAN0010
Spanning tree enabled protocol ieee
Root ID    Priority    24586
           Address    0004.9A40.621B
           Cost        23
           Port        25(GigabitEthernet0/1)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
           Address    0001.C915.E7C4
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  20
```

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. ábrán látható

```
interface FastEthernet0/2
  switchport access vlan 40
  switchport mode access
  switchport nonegotiate
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 000A.F346.1ED9
  spanning-tree portfast
  spanning-tree bpduguard enable
```

6. ábra: NAVY_SW show running config részlet

6. Etherchannel

A nagyobb sávszélesség és megbízhatóság érdekében a SERVER_SW-hez több kábelén keresztül csatlakoznak a kapcsolók. Ezeknek a leírása a 6. táblázatban látható

Az Etherchannel dinamikusan, LACP-vel van konfigurálva, ami a SERVER_SW oldalán aktív, a másik oldalon passzív. Egy Etherchannel jellemzése látható a 7. ábrán

```
Port-channel1:Port-channel1    (Primary aggregator)
Age of the Port-channel    = 00d:00h:48m:23s
Logical slot/port    = 2/1          Number of ports = 4
HotStandBy port = null
Port state            =
Protocol              = 1
Port Security         = Disabled

Ports in the Port-channel:
```

Index	Load	Port	EC state	No of bits
-----+	-----+	-----+	-----	-----+
0	00	Fa0/14	Passive	0
0	00	Fa0/13	Passive	0
0	00	Fa0/12	Passive	0
0	00	Fa0/15	Passive	0

```
Time since last port bundled:    00d:00h:46m:05s    Fa0/15
```

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:

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
10 SPACEFORCE	active	Fa0/1
20 AIRFORCE	active	Fa0/2
30 ARMY	active	Fa0/3
40 NAVY	active	Fa0/4
100 Management	active	Fa0/10, Fa0/11
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

8. ábra: SERVER_SW VLAN-ok

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10 SPACEFORCE	active	
20 AIRFORCE	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
100 Management	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

9. ábra: AIRFORCE_SW VLAN-ok

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

```
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
  switchport nonegotiate
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0060.7071.349C
```

10. ábra: SPACEFORCE_SW Fa0/2 portja (show running config részlet)

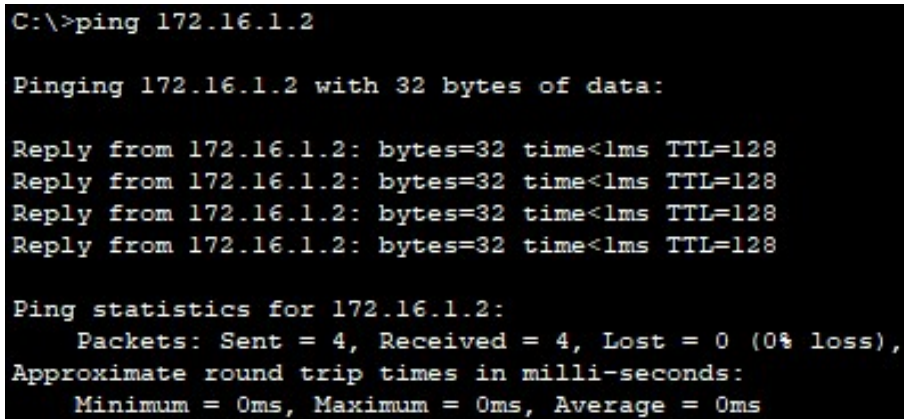
A trunk portok forgalomszabályozására egy példa a 11. ábrán látható:

```
Administrative private-vlan trunk priva
Operational private-vlan: none
Trunking VLANs Enabled: 30,40,100
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

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 szervert pingelésével a 12. ábrán látható:



```
C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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:

```
C:\>ping 172.16.1.66

Pinging 172.16.1.66 with 32 bytes of data:

Reply from 172.16.1.66: bytes=32 time<1ms TTL=127
Reply from 172.16.1.66: bytes=32 time<1ms TTL=127
Reply from 172.16.1.66: bytes=32 time=10ms TTL=127
Reply from 172.16.1.66: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

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:

```
NAVY_SW#ping 172.16.1.158
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.158, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

14. ábra: NAVY_SW (172.16.1.134) – Admin PC (172.16.1.158) ping