Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**Gandhi egy szál se**

**Tervezési dokumentáció**

Dombi-Hejcser Bence, Necek Dániel Milán, Veres Kolos  
13IRAÜ1

Budapest, 2025.

TARTALOMJEGYZÉK

[TARTALOMJEGYZÉK 2](#_Toc196346385)

[Szolgáltatások meg minden (mégse xd) 2](#_Toc196346386)

[VLAN-ok 3](#_Toc196346387)

[Vlanok létrehozása 3](#_Toc196346388)

[VTP (VLAN trönk protokoll) 3](#_Toc196346389)

[Inter-VLAN routing 4](#_Toc196346390)

[Második rétegbeli megvalósítások (L2) 5](#_Toc196346391)

[EtherChannel (port összevonás) 5](#_Toc196346392)

[Portbiztonság 6](#_Toc196346393)

[STP (Spanning Tree Protocol) 8](#_Toc196346394)

[HSRP 9](#_Toc196346395)

[OSPF 12](#_Toc196346396)

[OSPF Auth 13](#_Toc196346397)

[NAT 14](#_Toc196346398)

[Access-List 15](#_Toc196346399)

[Port Forward 16](#_Toc196346400)

[Ip telefonok 17](#_Toc196346401)

[WEB-VPN 19](#_Toc196346402)

[BGP 22](#_Toc196346403)

[WLC 22](#_Toc196346404)

Szolgáltatások meg minden (mégse xd)

Fizikai Tervezet

Logikai Tervezet

VLAN-ok

Vlanok létrehozása

Az igényfelmérés során a cég arra kért minket, hogy a különböző szektoroknak (vezetőség, dolgozók, vendégek), elkülönítve legyenek a hálózaton, a forgalmaik véletlenül se follyanak össze. Erre megoldásnak mi a VLAN-ok használatát javasoltuk, amit a cég el is fogadott.

Mint a cégnek is elmondtuk, a VLAN-ok virtuális, ha úgy vesszük a hálózaton belüli hálózatok, különböző VLAN-ok nem kommunikálhatnak egymással, csak ha irányítjuk köztük a forgalmat. A cég legfontosabb kérése az volt, hogy a vendégként csatlakozó eszközök a cég szervereit ne érhessék el.

A feltételeknek eleget téve a következő VLAN tervvel álltunk elő a cég számára:

|  |  |  |  |
| --- | --- | --- | --- |
| **VLAN** | **Telephely 1 (G1SS1)** | **Telephely 2 (G1SS2)** | **Telephely 3 (G1SS3)** |
| **10** | Dolgozok\_Data | Dolgozok\_Data | Dolgozok\_Data |
| **20** | Vezetoseg\_Data | - | Management |
| **30** | Management | Management | VOICE |
| **40** | VOICE | VOICE | Wireless |
| **50** | Wireless | Wireless | - |
| **70** | - | Teszt helyiség | - |
| **80** | - | Teszt Helyiség Wireless | - |
| **99** | Black Hole | Black Hole | Black Hole |

A táblázat alapján a VLAN 10 és 20 szeparálja a Dolgozókat és a vezetőket az első telephelyen. A management a 30-as VLAN-t kapta, a rendszergazdák ezen a vlanon belüli címeken érik el az eszközöket (3. Telephelyen VLAN 20). A Voice VLAN az IP telefonok működése érdekében a 40-es VLAN-t kapta (3. Telephelyen VLAN 30). A Wireless VLAN a vezeték nélküli kapcsolatok elkülönítésére lett kialakítva, nem szeretnénk, hogy a vendégek elérhessék a cég belső szervereit. A 70 és 80-as VLAN a 2. Telephelyen levő javító helyiség igényeit szolgálja ki. A 99-es Black Hole VLAN pedig a biztonság miatt lett létrehozva, a VLAN-hoz rendeltük a kapcsoló nem használt portjait, lekapcsoltuk őket, majd töröltük a VLAN-t.

VTP (VLAN trönk protokoll)

Folytatva a Vlanok létrehozását, mivel a 2. Telephelyen három kapcsolónk is egymáshoz kapcsolódik, a Vlanok létrehozását a VTP protokoll biztosítja. A cégnek javasoltuk ezt a szolgáltatást, mivel egyszerűsíti a Vlanok kezelését, illetve idő és erőforrás megtakarító megdoldás.

A kapcsolók szerepe illetve a konfiguráció pareméterei a következők:

|  |  |  |  |
| --- | --- | --- | --- |
| Kapcsoló | VTP szerep | Domain név | VTP Jelszó |
| G1SS2-SW1 | Szerver | gandhiegyszalse.net | G1SSPASS |
| G1SS2-SW2 | Kliens | gandhiegyszalse.net | G1SSPASS |
| G1SS2-SW3 | Kliens | gandhiegyszalse.net | G1SSPASS |

Inter-VLAN routing

Ahogy a Vlanoknál említettem, a különböző virtuális hálózatok nem tudnak egymással kommunikálni, csak hogyha a forgalmat irányítjuk köztük. Az igényfelmérés folyamán amikor a Vlanokat mutattuk be a megbízó cégnek, ezt a megoldást javasoltuk a Vlanok forgalmának irányítására. A koncepció végtelenül egyszerű, a virtuális hálózatokat összekötő routeren a VLAN számával (VLAN Tag) megegyező alinterfészeket hozunk létre (PL.: FastEthernet0/0.10). Ezeken az alinterfészeken mindegyik Vlanhoz tartozó IP tartomány alapértelmezett átjáróként választott címét állítjuk be IP címnek, és ez után mivel ezek a hálózatok a forgalomirányítónak kapcsolt hálózatai, innentől egyéb beállítás nélkül elvégzi a forgalomirányítást.

Második rétegbeli megvalósítások (L2)

EtherChannel (port összevonás)

A cég kiemelte, hogy náluk priorítás, hogy a hálózat egy bizonyos szintig hibatűrő legyen, a legkisebb meghibásodás ne vezessen kimaradáshoz az egész irodában. Erre mi a lehető legtöbb redundáns megoldást javasoltuk, az egyik példa erre a port összevonás. Ez a megoldás nem csak redundanciát biztosít, de két másik előnye a terhelésmegosztás, és a megnövekedett sávszélesség.

Az EtherChannel egy olyan technológia, ami több fizikai interfészt kapcsol össze egy logikai csatornába. Ezeknek az összekapcsolt interfészeknek a sávszélessége összeadódik (PL.: két darab 100 Mbps interfész ether channelben 200 Mbps), és a forgalmat egyenlően osztja el az összefogott linkek között, nem pedig egy lesz túlterhelve.

A hálózatban két ilyen port összevonást is csináltunk, hogy biztos ne legyen gond, ha egy vezeték meghibásodik. A port összevonások paraméterei a következők:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Channel | „A” oldal kapcsoló | Kapcsoló portjai | „B” oldal kapcsoló | Kapcsoló portjai |
| Po1 | G1SS2-SW1 | Fa 0/21-22 | G1SS2-SW2 | Fa 0/21-22 |
| Po2 | G1SS2-SW1 | Fa 0/18-19 | G1SS2-SW3 | Fa 0/23-24 |

Portbiztonság

A tervezés során kiemelt figyelmet kaptak a portbiztonsági beállítások (Port Security) és a hurokmentes hálózat kialakítása a Rapid-PVST+ protokoll segítségével. A port security egy fontos hálózatbiztonsági funkció, amely lehetővé teszi, hogy a switch portokon csak meghatározott MAC-címekől érkező forgalmat engedjünk be. Az összes switchen alkalmaztuk ezt védelmet továbbá a nem használt portokat letiltottuk és lekapcsoltuk továbbá fizikálisan RJ45 Port Lockerrel lezártuk hogy senki se férhessen hozzájuk.

|  |  |  |  |
| --- | --- | --- | --- |
| Kapcsoló | Port | Maximum Mac cím | Violation |
| G1SS1-SW1 | fa0/1-4 | 2 | Shutdown |
| fa0/5 | 1 | Shutdown |
| G1SS1-SW2 | fa0/1-4 | 2 | Shutdown |
| fa0/21-22 | 1 | Shutdown |
| G1SS1-SW3 | fa0/1-2 | 2 | Shutdown |
| fa0/4 | 1 | Shutdown |
| G1SS2-SW1 | fa0/1 | 1 | Shutdown |
| fa0/20 | 1 | Shutdown |
| G1SS2-SW2 | fa0/1-5 | 2 | Shutdown |
| fa0/6-7 | 1 | Shutdown |
| G1SS2-SW3 | fa0/1-5 | 2 | Shutdown |
| fa0/6-7 | 1 | Shutdown |
| G1SS3-SW1 | fa0/1-3 | 2 | Shutdown |
| fa0/4-6 | 1 | Shutdown |
| fa0/23 | 1 | Shutdown |

Biztonsági alapbeállítások:

- BPDU Guard: aktiválva minden felhasználói porton  
- Sticky MAC: automatikusan elmentett MAC-címek a portokhoz rendelve  
- Szabályszegés esetén: A port automatikusan lekapcsolt (Shutdown) állapotba kerül

STP (Spanning Tree Protocol)

A Spanning Tree Protocol megakadályozza a hurok kialakulását a redundáns kapcsolatokkal rendelkező Layer 2 kapcsolók által kialakított hálózatban. Egy vállalati környezetben, ahol a megbízhatóság és a folyamatos elérhetőség kulcsfontosságú, az STP biztonságot nyújt azzal, hogy automatikusan blokkolja a hurkot okozó kapcsolatokat, miközben lehetővé teszi a redundanciát.

Beállítások:

* spanning-tree mode rapid-pvst: Az STP rövidített konvergencia idejű, VLAN-onkénti verzióját engedélyezi.
* spanning-tree portfast default: Minden access port gyorsabb konvergenciára van állítva, nem várja meg a teljes STP tanulási és hallgatózó állapotait. Ez kritikus a végfogyasztói eszközök (PC, nyomtató) gyors csatlakoztatásához.
* spanning-tree portfast bpduguard default: Ez az opció biztonsági funkciót ad a portfast mellé: ha egy port BPDU-t (Bridge Protocol Data Unit) kap, akkor azonnal letiltódik (shutdown). Ez megelőzi, hogy valaki egy switchet kössön a hálózathoz és esetleg root bridge legyen.
* spanning-tree bpduguard enable: Porton egyénileg is bekapcsolja a BPDU Guard funkciót, amely szintén a fenti védelmet biztosítja.

HSRP

A HSRP tesztelésénél először bemutatjuk a hálózati szegmenst ahol a kiesést szimuláljuk, bemutatjuk az HSRP állapotát, végrehajtjuk a meghibásodást, aztán pedig ellenőrizzük, hogy sikeresen átvette-e az R3 az R1 től az active szerepet.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen látható a HSRP állapota az R1 -n. Látszik hogy az R1 az active router.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen látható a HSRP állapota az R2 -n. Látszik hogy R2 a standby router.

A képen képernyőkép, szöveg látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A hálózat egyik gépéről küldünk egy pinget a belső szervernek, mint látszik a tracert parancsnak ksözönhetően a csomag az R1 (192.168.1.1) felé távozott.

A képen szöveg, sor, képernyőkép, diagram látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az R1 router-t lekapcsolt állapotba tesszük és megismételjük az előző folyamatot.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az előzőekben hasznát gépről küldünk egy pinget a belső szervernek, mint látszik a a csomag az R3 (192.168.1.2) felé távozott és az R3 átvette az R1 től az active szerpet.

OSPF

A forgalomirányítók között OSPF protokollt használtunk, hogy az üzenetek mindig a leggyorsabb útvonalon jussanak célba. A protokoll mellett szól az is, hogy dinamikusan tanítják meg egymásnak a betanult hálózatokat, ezzel skálázhatóvá teszi az egész hálózatot.

A forgalomirányítók konfigurálása után kialakultak a szomszédsági kapcsolatok minden nem passzív interfészen.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A forgalomirányítók miután egyeztették az interfészeken a szomszédokat „Hello” üzenetekkel, elkezdték hirdetni a kapcsolt hálózataikat, majd megtanulni a másik által osztottat.

Minden határforgalomirányítón statikusan állítottuk be az útvonalat az Internet felé. Ezt is hirdetik a többi felé, hogy tudják, ha ki akarnak menni az ISP felé, akkor rajtuk át vezet az út.

A képen szöveg, Betűtípus, képernyőkép, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

OSPF Auth

Hitelesítéssel védjük az OSPF által használt hirdető interfészeket, hogy a jelszavakat kódolva lássa a hálózatba illetéktelenül behatoló. Az alábbi show parancsok utolsó sorai írják, hogy a hitelesítés be van kapcsolva és jelszó kell hozzá.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

NAT

A NAT tesztelésénél először bemutatjuk a router alap NAT statisztikáit, ahol a tesztet szimuláljuk, bemutatjuk az HSRP állapotát, végrehajtjuk a csomagküldést, aztán pedig ellenőrizzük, hogy sikeresen lett e a címfordítás.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, Betűtípus, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képeken látható a G1SS1-R3 router-nek a routing táblája illetve a NAT statisztikái

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Küldünk egy ping csomagot egy külső címre, az egyik eszközünkről.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Újra megnézzük a NAT statisztikákat és láthatjuk hogy a csomag sikeresen átment és a Router átfordította a belső címet külső címmé

Access-List

(work in progress)

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Port Forward

A Port forward tesztelésénél egy külső hálózatból (G1SS3) megpróbáljuk elérni a belső hálózat (G1SS1) webszerverét a G1SS1-R3 külsű címének lekérdezésével.

A képen képernyőkép, diagram, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Először a külső siteon bejelentkezünk a PC-be és belemegyünk a web browserbe

A képen szöveg, elektronika, képernyőkép, képernyő látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Utána beírjuk a G1SS1-R3 külső címet jelen esetben a 22.22.22.1 -es címet és megjelenik az 1-es siton lévő webszerver weboldala.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Lekérdezzük a fordítótábláját a G1SS1-R3 -nak és láthatjuk, hogy a beérkező kérést továbbította a router a szervernek.

Ip telefonok

(work in progress)

A képen Elektronikus eszköz, telefon, elektronika látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen telefon, Elektronikus eszköz, elektronika, kütyü látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

konfiguráció után, a telefonok különböző hálózatban elérik egymást

A képen szöveg, diagram, sor, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, diagram, sor, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, diagram, sor, térkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

WEB-VPN

(work in progress)

A képen szöveg, szoftver, Betűtípus, Weblap látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, szoftver, számítógép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen diagram, sor, kör, szöveg látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

BGP

(work in progress)

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

bgp szomszédos routerek ip címe

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

bgp táblák, melyik hálózat, következő ugrás stb

WLC

(work in progress)