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](#_Toc196639998)

[Szolgáltatások meg minden (mégse xd) 2](#_Toc196639999)

[Fizikai Tervezet 3](#_Toc196640000)

[Logikai Tervezet 3](#_Toc196640001)

[VLAN-ok 3](#_Toc196640002)

[Vlanok létrehozása 3](#_Toc196640003)

[VTP (VLAN trönk protokoll) 4](#_Toc196640004)

[Inter-VLAN routing 4](#_Toc196640005)

[Második rétegbeli megvalósítások (L2) 4](#_Toc196640006)

[EtherChannel (port összevonás) 4](#_Toc196640007)

[Portbiztonság 5](#_Toc196640008)

[STP (Spanning Tree Protocol) 5](#_Toc196640009)

[HSRP 6](#_Toc196640010)

[Forgalomirányítás 6](#_Toc196640011)

[OSPF 6](#_Toc196640012)

[OSPF Hitelesítés 7](#_Toc196640013)

[NAT 7](#_Toc196640014)

[Access-List 7](#_Toc196640015)

[Port Forward 7](#_Toc196640016)

[Ip telefonok 9](#_Toc196640017)

[WEB-VPN 11](#_Toc196640018)

[BGP 13](#_Toc196640019)

[WLC 13](#_Toc196640020)

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 cégnél mint korábban kiemeltük magas prioritást élvez a redundancia, nem engedhető meg a kiesés. Ezért a következő megoldást javasoltuk nekik két telephelyen is, ez pedig a HSPR protokoll használata.

A HSRP (Hot Standby Router Protokol) nagyon egyszerű. Ugyebár tudjuk, hogy az eszközeinknek egy alapértelmezett árjárót tudunk beállítani. Ezzel az egyértelmű probléma, hogy ha az a kapcsolat megszakad, a hálózatunk nem jut tovább sehova. A HSRP erről úgy gondoskodik, hogy több routernek az interfészei is lehetnek a hálózatban, és az interfészek IP címe helyett az alapértelmezett átjáró egy külön IP cím, ami a virtuális alapértelmezett átjárónk lesz.

A forgalomirányítókon konfiguráljuk a HSRP-t, az egyiket magasabb prioritásra rakjuk, az lesz a fő alapértelmezett átjáró útvonala. Ha az a link megszakad, a másik átveszi a helyét. Ezzel a redundancia megvalósúl, és a hálózatunk zavartalanul tud működni.

Forgalomirányítás

OSPF

A cégen belül a kommunikációt az OSPF forgaloirányító protokollal oldottuk meg. Az OSPF egy kapcsolatállapot alapú dinamikus forgalomirányító protokoll, nagyobb hálózatokhoz kiváló, és más forgalomirányító protokollokkal szemben gyorsabb konvergenciát tesz lehetővé.

Az OSPF remek választás a redundáns megvalósításokhoz, amint egy útvonal kiesik, gyorsan talál új útvonalat az adatoknak. Továbbá hatékony, könnyen skálázható, és biztonságos a megfelelő beállításokkal, például ha hitelesítést állítunk.

OSPF Hitelesítés

Az OSPF biztonságossá tétele érdekében konfiguráltunk OSPF Hitelesítést. Interfész alapú hitelesítést választottunk, ez biztosítja, hogy csak a megbízható eszközök csatlakozhatnak a forgalomirányítók hálózatába. Ezzel gátolja hogy nem megbízható eszköz kommunikáljon, és hamis OSPF üzeneteket küldjön a hálózatunkba.

NAT

Mivel a cég a belső hálózatának megtervezésére kért fel minket egyértelmű, hogy a belső címeket meg kell akadályozni, hogy kimenjenek a belső hálózatból az internetre.

Ugyebár a beső hálózatok lényege, hogy privát címtartománybeli címeket használunk, és ezeket nem engedjük ki az internetre. ebből kifolyólag, akár minden belső hálózatnak lehet ugyan az a privát címe, nem fognak ütközni, mivel nem érik el az internetet ezek a címek. Ugyebár a logikus kérdés, hogy akkor hogyan éri el a hálózat az internetet?

A cég határ forgalomirányítóját beállítottuk, hogy a belső címeket a sajátjaként küldje ki. Ez az interéfsz alapú PAT. Mivel a határ forgalomirányítónak van publikus címe a szolgáltató felé, így megadtuk a routernek egy hozzáférési listában, hogy milyen belső címeink vannak (amiket engedünk hogy kiküldjön), és megmondtuk, hogy azokat a külső címére fordítsa át.

Ez alapján ha egy gép az interneten pingel egy szervert, a külső szerver azt látja, hogy a router pingelte, mivel ő a külső címet látja. Válaszol rá, a router pedíg a port szám alapján tudja, hogy melyik gépnek küldje vissza a választ. Összefoglalva, a privát címeink sosem mennek ki az internetre, csak a forgalomirányító publikus címét használva látják az internetet.

Tűzfalak, hozzáférési listák

A tűzfalak fontos részei egy hálózatnak. Az egyik fő biztonsági elemei a hálózatunknak. Lényegében a tűzfalak hozzáférési listák, amikben megadjuk, hogy egy adott IP című eszköz, vagy egy egész IP tartomány elérhet-e egy adott címet, vagy átmehet-e egy adott irányba, vagy akár csak szolgáltatásokra is tudunk szűrni, hogy semmit nem érhetnek el, csak az adott szolgáltatást amit mi engedünk nekik.

Jelen esetben kezdjük az egyik legfontosabb listával. Az 1-es hozzáférési listába írtuk a hálózatunkban megtalálható belső IP címeket, amiket szeretnénk hogy a PAT által fordítva legyenek a forgalomirányító publikus címére. Majd a PAT konfigurácíónál megadtuk, hogy az 1-es listát használja,a kimevezető interface-n. Ezt a listát nem használtuk más célra.

A következő fontos elemünk a tűzfalak voltak. Természetesen a cég szerette volna, ha a privát adataik privátok is maradnak. Ehez javasoltuk nekik a tűzfalak használatát, amivel specifikusan megszabhatják, kiket szeretnék, hogy elérjék a szervereiket. A cég el is fogadta a javaslatunkat.

A tűzfalakat alapértelmezetten úgy konfiguráltuk, hogy a szervereket a belső hálózatból el lehet érni mindenhonnan, viszont a vezeték nélküli kapcsolaton a Vendégek ne érhessék el a belső szervert.

Port továbbítás

A port továbbítás a cég szempontjából igen fontos volt hiszen több telephellyel is rendelkeznek és csak 1 fő webszerver van ahol a cég weboldala és felülete található, ezért megkértek hogy a többi telephelyről is elérhető legyen a szerver. Ezt egy port átirányítással oldottuk meg, hogy a külső címekről is el lehessen érni a belső webszervert.

Engedélyeztük a külső elérést a 80 as porton és a 443 as porton továbbá átiránytottuk ezeket a kéréseket a Linux szerverünknek ahol egy webszerver üzemel. Ez által a http és a védett https kapcsolaton keresztül is lehet kapcsolódni a szerverhez a beslő hálózaton kívülről is.

Ezt lényegében egy statikus NAT, úgy működik, hogy megadtuk a routernek, hogy amennyiben a külső publikus címének a 80, vagy 443-as portjára érkezik kérés (http, https) azt továbbítsa a belső szervernek az adott portjára, így kívülről hogyha el szeretnénk érni a web szervert, akkor a router publikus címét kell keressük.

Ip telefonok

Mivel a cég egy call center, a legfontosabb része az üzemelésüknek a hívások kezelése. Kiemelt figyelmet szenteltünk a telefonos hálózat kiépítésének, és ebben sikerrel is jártunk.

Egy hívásközpont ugyebár úgy működik, hogy a cégnek egy publikus telefonszáma van, és azt amikor hívják, felveszi egy automatikus telefonos rendszer (Interactive Voice Response) ami üdvözli a hívót, és kérdéseket tesz fel, hogy milyen témában kér segítséget.

Miután ez kiderült, a megfelelő gombnyomás után az ügyfél hívása átirányításra kerül, és a várakozási sorba tolódik, közben a rendszer figyeli mikor lesz szabad ügyintéző az adott területen. Amint lesz szabad ügyintéző a rendszer tárcsázza, és az ügyfél hívását átirányítja oda.

A cégnél viszont a terheltséget, és a nagy mennyiségű hívásokat figyelembe véve a hagyományos telefonokat IP telefonokkal váltottuk fel, így a hívások kezelése olcsóbb, és jobban skálázható lesz.

Mi ennek a rendszernek a kiépítését vállaltuk az ügyfélnek, amivel sikerrel is járunk, azonban sajnálatos módon, ennek a szimulálását nem tudjuk bemutatni, mivel Packet Tracerben nem állnak rendelkezésünkre a megfelelő eszközök, és erőforrások. Amit viszont be tudtunk mutatni, a cégen belüli telefonok konfigurációja, ugyanis sikeresen szimuláltuk, hogy a különböző hálózatban, és részlegen levő emberek fel tudják hívni egymást.

WEB-VPN

A cég értesített minket, hogy van nekik egy már meglevő felhőben elérhető bérelt tárhelyük, ahol a biztonsági mentések mellett a céges programok is fent vannak például a könyvelőprogram. Ezt figyelembe véve, mi a cég számára a következő ajánlatot tettük.

Kiépítünk a cég számára egy Home Office lehetőséget, hogy a könyvelőknek, vagy akinek a munkájának nem kell az irodában történjen, lehessen otthonról dolgozni. Ezt úgy oldjuk meg, hogy a tárhely szolgáltató céggel konzultálva, kiépítünk egy WEB-VPN szolgáltatást a cég részére.

A szolgáltató cég azt az információt adta, hogy egy ASA eszközük védi a szervereket, és a megfelelő informásiók cseréje után ki tudjuk építeni az ASA WEB-VPN szolgáltatást a cégnek.

Ez egy egyszerű szolgáltatás a felhasználók számára, ugyanis nem kell hozzá semmilyen VPN klienst telepíteni, csak egy böngészőre van szükség hozzá, ebből kifolyólag szinte bármilyen eszközről lehet dolgozni. Az oldalra felhasználónévvel és jelszóval lehet belépni, az ASA naploózza a belépéseket, ezeket később lehet ellenőrizni, hogy ki lépett be.

WLC

A cég igényei között szerepelt vezeték nélküli internet elérés mind a dolgozók számára, mind a vendégek számára, akik esetlegesen megfordulnak az irodákban.

Mivel egy nagyobb létesítményről beszélünk, a cégnek ajánlottuk a WLC (Wireless Lan Controller) használatát, amit el is fogadtak. A WLC helyes beállításával a dolgozó bárhova megy az épületben, az elhelyezett Access Pointoknak hála, a lefedettség teljes, és csak egyszer kell a wifire csatlakozni, automatikusan átkerül másik Access Pointra