Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

Szakképesítés neve: Informatikai rendszer- és alkalmazás-üzemeltető technikus

száma: 5-0612-12-02

VIZSGAREMEK

Gandhiegyszálse

Tervezési dokumentáció

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

Budapest, 2025.

TARTALOMJEGYZÉK

Cégünk bemutatása

Szerény cégünk a VVVa. A név a www.-ból jött, hiszen ahogy a World Wide Web az egész világot köti össze, úgy mi is hasonló módon szeretnénk összekötni az embereket az irodai közegekben, rendezvényeken.

Vállalkozásunk jó néhány éve foglalkozik már a különböző hálózatok kialakításával, életre keltésével. Fontos kiemeljük, hogy cégünk az évek alatt szerzett kapcsolatoknak köszönhetően bekerült a Cisco partner programjába, ami annyit jelent, hogy kizárólag Cisco eszközöket használunk hálózataink felépítéséhez.

Tisztában vagyunk vele, hogy ezek az eszközök drágábbak, mint egy olyan eszköz, ami az egyszerű feladatot ugyan úgy elvégzi, viszont hiszünk abban, hogy a pénzért amit a Cisco eszközeibe fektetnek a vásárók, minőséget is kapnak.

Ezeken felül olyan előnyökkel jár, mint az újítások, fejlesztésekhez való korábbi hozzáférés, így csak a legújabb, legjobb technológiát nyújtjuk a megbízóinknak. Ezen felül a Cisco ügyfélszolgálata is rendelkezésre áll tekintve a Magyarországon fellelhető Cisco együttműködéseket.

Megbízó cég bemutatása

A cég amely megkeresett minket a Gandhiegyszálse. A cég egy elektroniai eszközökkel foglalkozó telefonos segítség nyújtó ügyfélszolgálat.

Azzal a kéréssel fordultak hozzánk, hogy szeretnék a szolgáltatási köreiket bővíteni más országok felé, és itt Magyarországon vásároltak három irodát. Miután az interneten láttak hirdetéseket cégünkről, és az online értékeléseink is kiemelkedőek voltak, megekresetek minket, hogy építsük ki nekik az irodáik hálózatát.

Mivel látták a partnerségünket beleegyeztek, hogy a drágább Cisco eszközöket használjuk, azonban kikötötték, hogy cserébe magas színvonalú munkát várnak el.
Az adategyeztetések után egyeztettünk két időpontot, az egyiket igényfelmérésre, a másikat az irodák megtekintésére.

Igényfelmérés

Helyzetfelmérés

A két irodai közeg az egyikben a vezetőség és a dolgozók egy térségben helyezkednek el, ebből kifolyólag felosztjuk az embereket a beosztásuk szerint külön csoportoba, hogy egymás forgalmát ne akadályozzák, illetve ne lássanak bele. Emellett a rendszergazdáknak és a telefonoknak is lesz külön csoportjuk. Ezt a csoportbesoztást vlan-onként fogjuk megoldani mindkettő irodai közegben.

A könyvelői viszont nem járnak be a hét minden napján, ezáltal ki kell nekik is alakítani egy home office környezetet, amivel hozzá tudnak férni a felhőben levő bérelt tárhelyhez.

A rendszergazákkal szemben a dolgozók nem férhetnek hozzá mindenhez, nem rakhatják saját gépeiket a kapcsolókba, forgalomirányítókba, ezért biztonsági lépéseket is meg kell tennünk, mint például a portbiztonság és a nem használt portok letiltását vagy fizikailag hozzáférés ellehetetlenítése zárakkal. Viszont vannak a cégnek olyan pontjai, helyei, ahol elkerülhetetlen lesz, hogy idegen gépet kelljen felcsatlakoztatni a rendszerre, itt fizikailag elérhetőek lesznek a portok és a logikai biztonsággal fogjuk ellensúlyozni.

A cég kért egy web szolgáltatást is, hogy a meglévő és a leendő ügyfelek meg tudják őket találni interneten keresztül is. Ezt egy saját web szerverrel tervezzük megvalósítani, amelyhez egy DNS szolgáltatást is rakunk, hogy a weboldal IP címét össze tudjuk kötni egy URL-el. A web mellett a cég egy saját fájlmegosztó szolgáltatást is szeretne, szóval egy saját FTP szervert is rakunk bele, hogy a cégen belül legyen egy fájl tároló egység, ahol el tudják érni a céges adatokat.

A vállalat 0-24-es szolgáltatást szeretne nyújtani, ennek érdekében figyelnünk kell a redundanciára, hogy esetleges fizikai kapcsolat megszakadás se állítsa le a forgalmat és akadálymentesen működjön minden továbbra is. A tervezésben közben erre figyeltünk, hogy minden közegben legyen redundancia.

Az egész helyen szeretnék, hogy legyen vezeték nélküli hálózat a dolgozók és főképp a rendszergazda számára, hogy tudjon csatlakozni tudjon az internethez a laptopjával vagy telefonjával. Ezt számításba véve több LAP-t is rakunk le a teljes lefedettség miatt.

Szolgáltatás katalógus

Harmadik Rétegbeli Szolgáltatások

Megnevezés	Feladat
OSPF	A forgalomirányítók megosztják egymással a saját általuk ismert hálózatokat és kiszámolja a legrövidebb utakat egyes célokhoz.
HSRP	Redundánssá teszi a forgalomirányítókat esetleges kapcsolatmegszakadás esetén.
SSH	A rendszergazda számára bekonfigurált biztonságos távoli elérési módszer.
Port továbbítás	Lehetővé teszi külső kérések számára, hogy elérjék a belső hálózat szerverét a forgalomirányítón keresztül.
NAT	A határ forgalomirányítókon címfordítást alkalmaztunk, hogy ne a belső címekkel kerüljenek ki a csomagok az internetre, hiszen ez nem megengedett, emiatt használtunk a port lapú natolást (PAT), amely biztosítja a belső címek lefordítását a forgalomirányító külső (internethez csatlakozó) portjának ip címére.
Tűzfal	A tűzfal nagyon fontos része a biztonságos infrastruktúra kialakításának, gondoskodtunk róla, hogy kívülről ne lehessen elérni a belső hálózatot. Továbbá a telephelyeken a 'guest' wireless hálózatban a belső szervereket elérhetetlenné tettük a cég adatainak biztonsága érdekében.

Második Rétegbeli Szolgáltatások

Megnevezés	Feladat
VTP	Az egyes hálózatokban kijelölt kapcsolók megtanítják a többi kapcsolónak az ő konfigurált vlan-jait.
STP	A kapcsolókat redundánssá alakítjuk ezzel, ahol minden vlan-nak kiadunk egy vezető kapcsolót, amely annak a vlan-nak a forgalmával fog foglalkozni.
Etherchannel	A további redundancia érdekében néhány kapcsolót duplán kötöttük össze, hogy az egyik kábel esetleges megsérülése után, a másik akadálymentesen tudja továbbítani a forgalmat.
Ip helper	Mivel nem lesz miden helyen DHCP szerver, ezért a legtöbb forgalomirányítóra ki kell adni, hogy melyik útvonalon éri el a DHCP szervert.
Portbiztonság	Mivel a hálózat biztonsága nagyon fontos és kiemelt szerepet élvez, ezért nagy hangsúlyt fektettünk az infrastruktúra védelmére. Ennek eredményeképpen a nem használt portokat lekapcsoltuk és fizikailag lezártuk. A használt portokat pedig az eszközök Mac-címéhez rendeltük, ezért, ha új eszközt csatlakoztatnának a kapcsolóhoz egyből shutdown (lekapcsolt) állapotba kerül az a port.

Egyéb rendszerszolgáltatások

Megnevezés	Feladat
DHCP	Dinamikusan oszt IP címeket a dolgozóknak és eszközöknek.
WLC	A vezeték nélküli hálózatok összefogó alakja, amivel külön szegmensekre tudjuk bontani a hálózatra kapcsoltakat.

Üzleti szolgáltatások

Megnevezés	Feladat
Mail	Egy szolgáltatás, amellyel saját domain névvel tudnak levelezni.
FTP	Cégen belüli fájlmegosztás megvalósítója.
DNS	Egy névfeloldó szolgáltatás, hogy ne IP címeket kelljen beírni a weboldal helyett.
Nyomtató	Dolgozók számára nyújtott nyomtatók.
IP telefon	Minden dolgozónak adott telefon, ahol tud hangalapon kommunikálni a többiekkel.
Web	A cég saját irodájukban futatott szerver, ami megtekinthetővé teszi a világ számára.

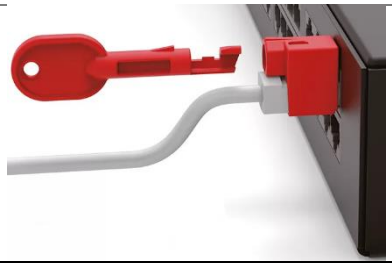
Az üzleti szolgáltatások az év minden napján 0-24-ben működőképes, elérhető állapotban lesznek.

Biztonsági intézkedések

Minden kapcsolón konfigurálunk port biztonságot, amivel megjegyzi az általunk bedugott gép MAC címét, ezzel megakadályozva a jövőbeli idegen gépek használatát.

Emellett minden nem használt portra fizikailag ráillesztünk egy port dugót, amit kulccsal lehet csak leszedni.

Ezt a módszert alkalmazzuk a használt portokra is, ahol egy hasonló zárat rakunk a kábel csatlakozójára, ami által nem lehet kihúzni azt a kábelt.

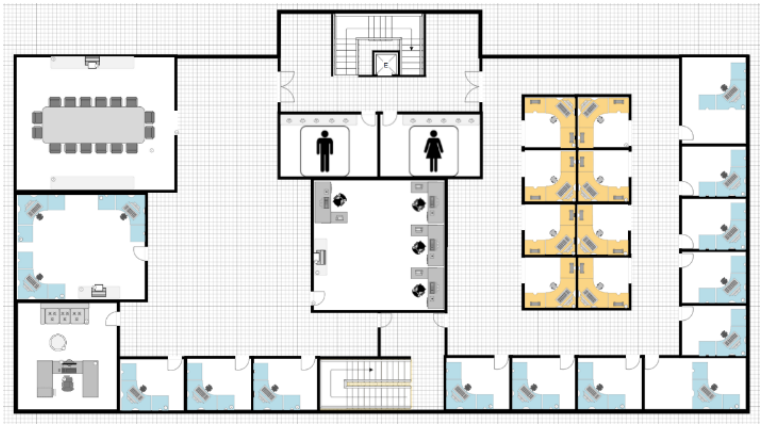


Fizikai Tervezet

Ebben a bekezdésben szeretnénk az iroda fizikai tervezetét bemutatni, amit a megbízó cég számára készítettünk el. Mivel az iroda felújítás alatt áll, szabad kezet kaptunk, amit ki is használtunk.

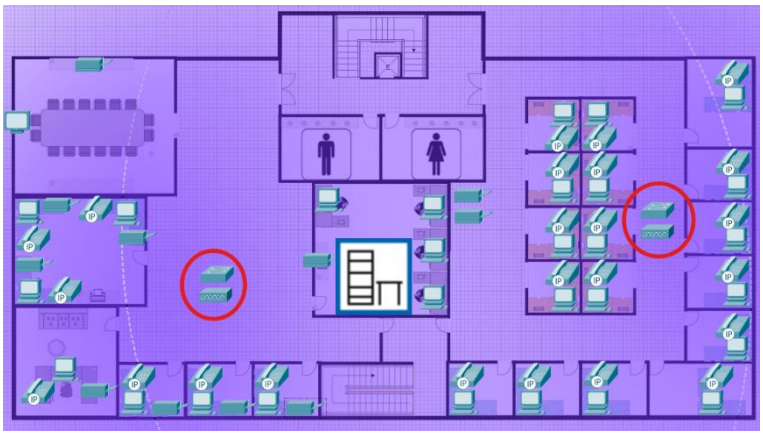
Első Telephely

Először hadd mutassam be az iroda fizikai tervét. Ez az első telephely terve. Itt két osztály található, az egyik a Dolgozók jobb oldalon, mindegyikük saját fülkében, asztallal és géppel. Bal oldalon a Vezetőség található. Az iroda közepén levő helyiségben található a rendszergazdai szoba. Ide helyezzük el a hálózati eszközeinket, és itt lesz a rendszergazda személyzet megtalálható.



A kábelek elrendezése és vezetése nagyon fontos, ezért alapos átgondolás után arra jutottunk, hogy álpadlót választunk az irodába. Ez a megoldás nagyban megkönnyíti a kábelezést, mivel mindent tudunk a padló alatt vinni a képen látható módon. Fontos volt számunkra, hogy ne végezzünk olyan munkát, ami később nem könnyen hozzáférhető, mint például a falakban történő kábel vezetés. Ez a megoldás elegáns mivel semmi sem látszik a kábelekből, mégis könnyen hozzáférhető probléma esetén. Az asztalok alá a képen látható RJ45-ös foglalatot telepítünk, hogy a számítóképek és telefonok telepítésekor, csak egy méretre szabott hálózati kábelt kelljen csatlakozóba dugni.

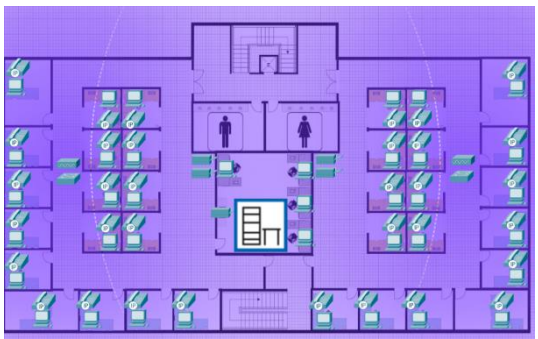
A telephelyen a képen látható módon helyeztünk eszközöket. Mindegyik asztalra került egy telefon és egy PC. A vezetőségnél továbbá minden asztalra került nyomtató is. A dolgozók részlegén két hálózati nyomtatót helyeztünk el. A pirossal karikázott eszközök feltűnően a szobák közepén vannak, ez azért van, mert a részlegek közepére 1-1 AP-t, és kapcsolót helyeztünk a megfelelő lefedettség, és kapcsolat érdekében. Az eszközöket az álpadlózatban helyeztük el, hogy ne lehessen hozzáférni bárkinek.

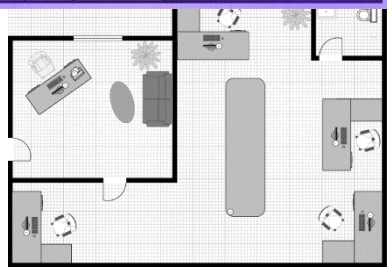


Második Telephely

A második telephelyen irodák találhatóak. Itt a dolgozók helyezkednek el, nekik 34 iroda lett kialakítva. továbbá az iroda közepén a rendszergazdai szoba terül el, ahol a rendszer gazda csapat dolgozik, nekik 4 munkaállomás lett kialakítva. Ezen a telephelyen található még egy kisebb javító részleg, ami egy külön emeleten helyezkedik el és 5 embert foglalkoztat. Egy recepciót, aki felveszi a javításra szánt árukat továbbá 4 szerelőt.

Felszereltségüket tekintve hasonló eszközökkel dolgoznak, mint az első telephelyükön. Minden dolgozó munkaállomásán található egy számítógép és ip telefon. Az iroda közepén mindkét oldalon található 2 hálózati nyomtató. A rendszergazdai szobában mindenkinek saját számítógép lett elhelyezve, illetve egy nyomtatót is telepítettünk. A javító részlegen laptopokkal dolgoznak továbbá a recepciósnak számítógép és nyomtató lett kihelyezve. Az AP-k, illetve kapcsolók ezen a telephelyen is az álpadlózatba lesznek elhelyezve hálózatbiztonsági szempontból.





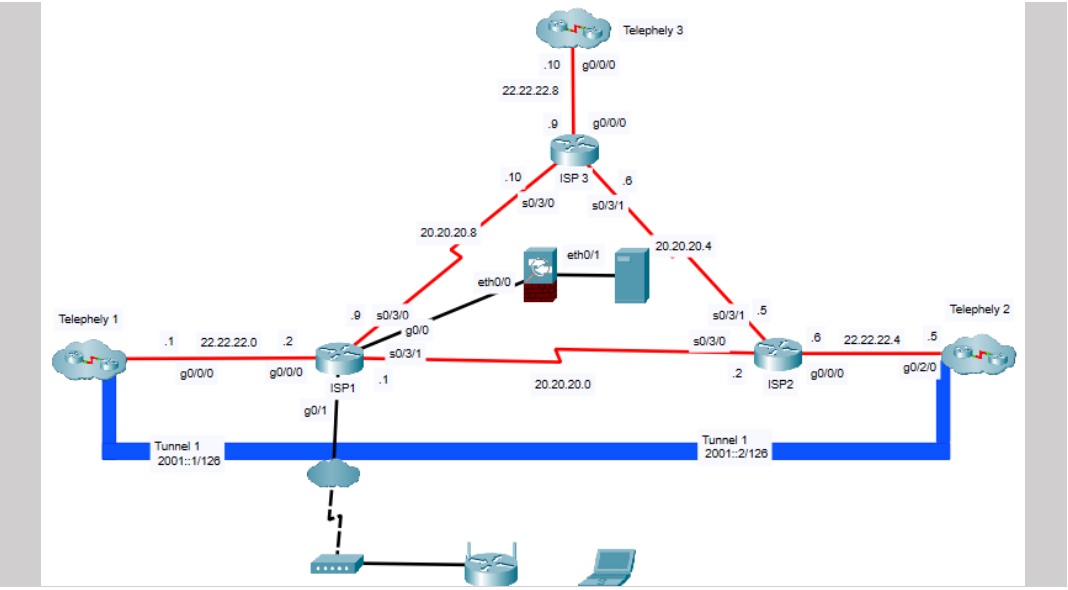
Harmadik telephely

A harmadik telephely egy kisebb üzlethelység, ahol a dolgozók az ügyfeleket fogadják. Összesen négy munkaállomás lesz kiépítve mind a négy dolgozó fel lesz szerelve számítógéppel, IP telefonnal és saját nyomtatóval is. Az üzlethelységben egy AP lesz kihelyezve. Az üzlethelységből továbbá nyílik egy raktár, ahová a kapcsoló és a forgalomirányító, továbbá a saját szerver lesz kihelyezve.

Logikai Tervezet

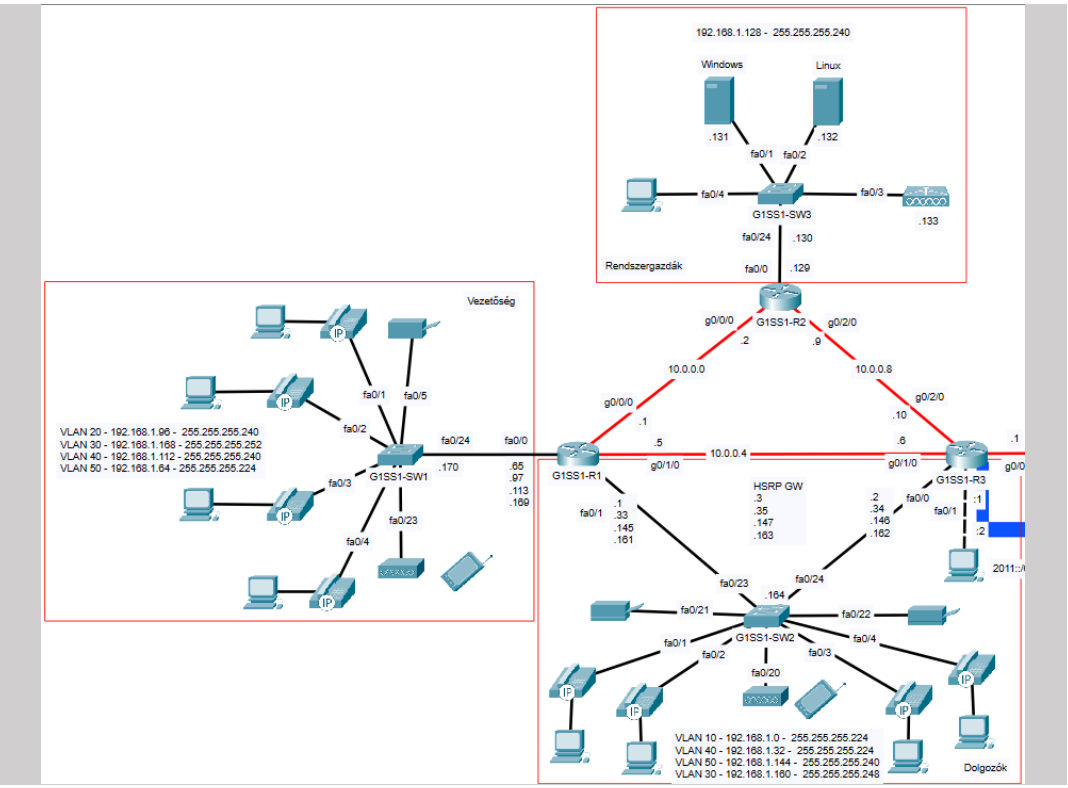
Az alábbi képen lesz látható a három telephely, illetve a gerinchálózat logikai tervezete, az eszközök összeköttetései, a használt interfészek, portok,vlanok és IP címek. Az eszközök fizikai elhelyezése a fentebbi fizikai tervezetben jelenik meg.

Gerinchálózat

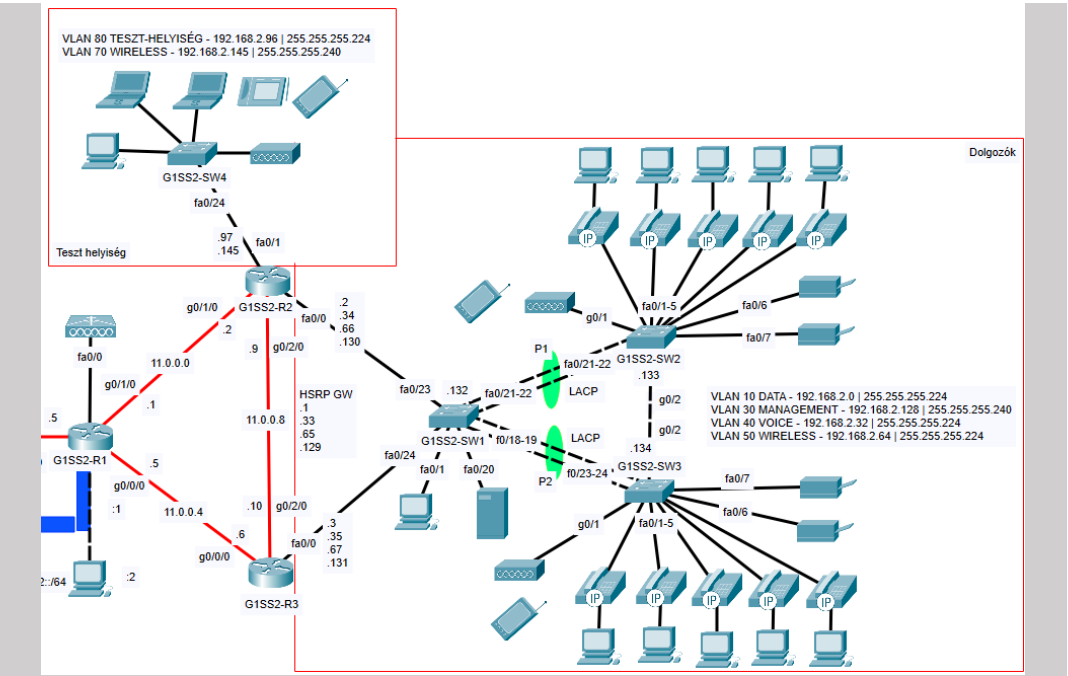


A fentebbi képen látszik az internet szimulálása, amely összeköti a három telephelyet. Az internetet BGP forgalomirányító protokollal szimuláltuk, illetve a Home Office dolgozó is az internetre csatlakozik fel otthonról, és éri el a felhőben levő bérelt tárhelyet. Ugyebár ez a szolgáltató hálózata, rengeteg forgalomirányítóból áll, azonban azt a hármat használjuk ennek szimulálására, amelyre a hálózataink határ forgalomirányítói csatlakoznak.

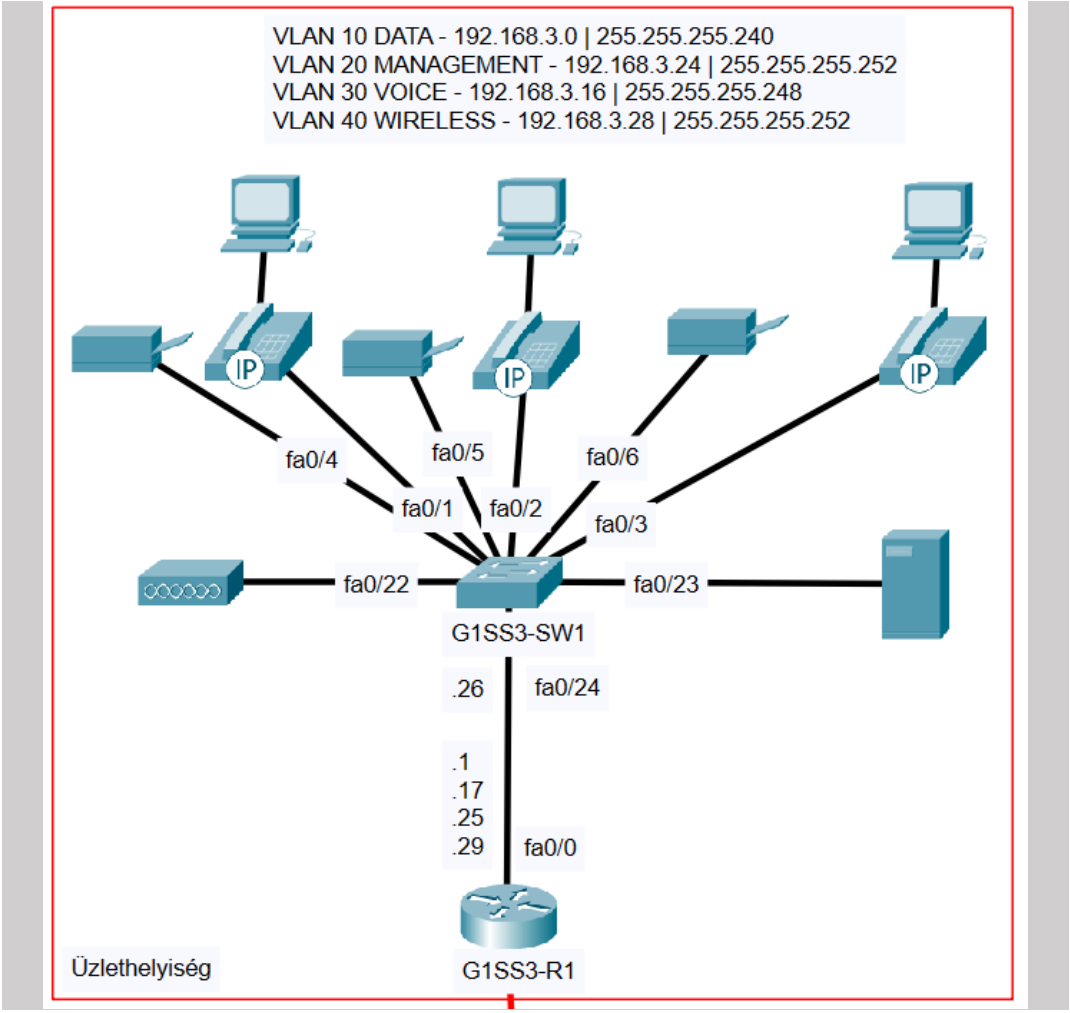
Első Telephely



Második Telephely



Harmadik Telephely



IP címzési terv

Az alábbi táblázatban lesz hátható telephelyekre szétbontva a hálózati eszközök interfészeinek IP címe, a dinamikusan IP-t kapó eszközök nem kerülnek bele a táblázatba.

Első telephely		
Eszköz	Interfész	IP cím
G1SS1-R1	FastEthernet0/0.20	192.168.1.97
	FastEthernet0/0.30	192.168.1.169
	FastEthernet0/0.40	192.168.1.113
	FastEthernet0/0.50	192.168.1.65
	FastEthernet0/1.10	192.168.1.1
	FastEthernet0/1.30	192.168.1.161
	FastEthernet0/1.40	192.168.1.33
G1SS1-R1	FastEthernet0/1.50	192.168.1.145
	GigabitEthernet0/0/0	10.0.0.1
	GigabitEthernet0/1/0	10.0.0.5
G1SS1-R2	FastEthernet0/0.30	192.168.1.129
	GigabitEthernet0/0/0	10.0.0.2
	GigabitEthernet0/2/0	10.0.0.9
G1SS1-R3	FastEthernet0/0.10	192.168.1.2
	FastEthernet0/0.30	192.168.1.162
	FastEthernet0/0.40	192.168.1.34
	FastEthernet0/0.50	192.168.1.146
	FastEthernet0/1	2011::1/64
	GigabitEthernet0/0/0	22.22.22.1
	GigabitEthernet0/1/0	10.0.0.6
	GigabitEthernet0/2/0	10.0.0.10
	Tunnel 1	2001::1
G1SS1-SW1	VLAN 30	192.168.1.170
G1SS1-SW2	VLAN 30	192.168.1.164
G1SS1-SW3	VLAN 30	192.168.1.130
WLC	Management	192.168.1.133
Windows szerver	FastEthernet0/0	192.168.1.131
Linux szerver	FastEthernet0/0	192.168.1.132
Második telephely		
Eszköz	Interfész	IP cím
G1SS2-R1	FastEthernet0/1	2012::1/64
	GigabitEthernet0/0/0	11.0.0.5
	GigabitEthernet0/1/0	11.0.0.1
	GigabitEthernet0/2/0	22.22.22.5
	Tunnel 1	2001::2
G1SS2-R2	FastEthernet0/0.10	192.168.2.2
	FastEthernet0/0.30	192.168.2.130
	FastEthernet0/0.40	192.168.2.34

	FastEthernet0/0.50	192.168.2.66
	FastEthernet0/1.70	192.168.2.145
	FastEthernet0/1.80	192.168.2.97
	GigabitEthernet0/1/0	11.0.0.2
	GigabitEthernet0/2/0	11.0.0.9
G1SS2-R3	FastEthernet0/0.10	192.168.2.3
	FastEthernet0/0.30	192.168.2.131
	FastEthernet0/0.40	192.168.2.35
	FastEthernet0/0.50	192.168.2.67
	GigabitEthernet0/0/0	11.0.0.6
	GigabitEthernet0/2/0	11.0.0.10
G1SS2-SW1	VLAN 30	192.168.2.132
G1SS2-SW2	VLAN 30	192.168.2.133
G1SS2-SW3	VLAN 30	192.168.2.134
G1SS2-SW4	VLAN 70	192.168.2.98
Helyi szerver	FastEthernet0/0	192.168.2.135

Harmadik telephely

Eszköz	Interfész	IP cím
G1SS3-R1	FastEthernet0/0.10	192.168.3.1
	FastEthernet0/0.20	192.168.3.25
	FastEthernet0/0.30	192.168.3.17
	FastEthernet0/0.40	192.168.3.29
	GigabitEthernet0/0/0	22.22.22.10
G1SS3-SW1	VLAN 30	192.168.3.26
Helyi szerver	FastEthernet0/0	192.168.3.2

Jelszókatalógus

A következő táblázatban a keszókatalógus látható, amelyben az összes használt hálózati eszköznek a jelszavát foglaltuk össze. Ezek a jelszavak természetesen nem fix-ek és a biztonságos hálózat érdekében kötelező ezeket megváltosztani a cég jelszószabályai szerint.

TELEPHELY	ESZKÖZ	JELSZÓ
SITE 1	G1SS1-R1	G1SS1-R1PWD
	G1SS1-R2	G1SS1-R2PWD
	G1SS1-R3	G1SS1-R3PWD
	G1SS1-SW1	G1SS1-SW1PWD
	G1SS1-SW2	G1SS1-SW2PWD
	G1SS1-SW3	G1SS1-SW3PWD
	G1SS1-WLC	Cisco1234
SITE 2	G1SS2-R1	G1SS2-R1PWD
	G1SS2-R2	G1SS2-R2PWD
	G1SS2-R3	G1SS2-R3PWD
	G1SS2-SW1	G1SS2-SW1PWD
	G1SS2-SW2	G1SS2-SW2PWD
	G1SS2-SW3	G1SS2-SW3PWD
	G1SS2-SW4	G1SS2-SW4PWD
	G1SS2-WLC	Cisco1234
SITE 3	G1SS3-R1	G1SS3-R1PWD
	G1SS3-SW1	G1SS3-SW1PWD

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
10	Wireless_Dolgozok	Wireless_Dolgozok	-
20	Wireless_Vezetoseg	Wireless_Vezetoseg	-
30	Wireless_Management	Wireless_Management	-
40	Wireless_Guest	Wireless_Guest	-
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 említettük, 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 forgalomirányítón 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)

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 kapcsoló portokon csak meghatározott MAC-címekől érkező forgalmat engedjünk be. Az összes kapcsolón 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

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

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 várakozási folyamatot. Ez a végberendezések számára a legfontosabb (PC, nyomtató), hiszen biztosítja a gyors csatlakoztatást.

- BPDU Guard: Ez egy biztonsági funkció a portfast mellé. Ha a kapcsoló egy BPDU (Bridge Protocol Data Unit) üzenetet kap a guard funkciót használó portól, akkor azonnal lekapcsolódik (Shutdown). Ez akkor történhet meg, ha valaki egy ismeretlen kapcsolót köt a hálózathoz és megpróbálja átvenni a root bridge -től az irányítást.

Harmadik Rétegbeli megvalósítások

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 forgalomirányítónak 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 forgalomirányítónak 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 forgalomirányító pingelte, mivel ő a külső címet látja. Válaszol rá, a forgalomirányító 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 konfigurációnál 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 átirányítottuk 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 forgalomirányítónak, 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 forgalomirányító publikus címét kell keressük.

SSH (Secure Shell Protokoll)

A hálózati eszközök sávon kívüli elérése érdekében a kapcsolókon és forgalomirányítókon konfiguráltunk SSH-t, ami lehetővé teszi a rendszergazdák számára, hogy távolról kapcsolódjanak az eszközökhöz.

Ez a protokoll biztonságot nyújt a távoli elérés közben, ugyanis az adatokat titkosítva küldi. Kettes verziójú SSH-t választottunk, ugyanis támogatja az erősebb titkosítási algoritmusokat, több féle hitelesítési módot is támogat, és több párhuzamos csatornát lehet vele létrehozni egyidejűleg.

A konfiguráció paraméterei a következők voltak:

Telephely	Domain név	Kulcs bit-ek száma	Bejelentkezés
G1SS1	gandhiegyszálse.net	1024	admin/G1SS1<R/S>
G1SS2	gandhiegyszálse.net	1024	admin/G1SS2<R/S>
G1SS3	gandhiegyszálse.net	1024	admin/G1SS3<R/S>

Tunnel

Az alagutat azért hoztuk létre, hogy a két telephely között két IPv6-alapú belső hálózat kommunikációját biztosítsa, egy IPv4 hálózaton keresztül megvalósított GRE (Generic Routing Encapsulation) alagút segítségével. Ez lehetővé teszi IPv6-csomagok átvitelét egy IPv4 infrastruktúrán. Így a két IPv6 -os hálózat tud kommunikálni egymással.

Eszköz	Alagút interfész	IPv6 cím	IPv4 Forrás	IPv4 Cél
G1SS1-R3	Tunnel 1	2001::1/126	22.22.22.1	22.22.22.5
G1SS2-R1	Tunnel 1	2001::2/126	22.22.22.5	22.22.22.1

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.

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 ha attól erősebb jelet vesz a készülék mint a másiktól.

A vezeték nélküli hálózatba négy WLAN-t terveztünk, a következő táblázat mutatja őket.

Első telephely		
SSID	Hálózat	Jelszó
Dolgozók	192.168.1.64/28	DolgozokPWD4321!
Vezetőség	192.168.1.80/28	Vezetoseg@PWD123
Management	192.168.1.128/28	MGMT@246!
Vendég	192.168.1.144/28	vendeg1234

A fenti tábla mutatja az első telephelyen létrehozott vezeték nélküli hálózatok adatait és belépéseit, a másik irodában és üzletben hasonlóképpen elkészítettük ezeket a hálózatokat, a vezetőség kivételével, mivel az csak az egyes telephelyen van.

A kapcsolódó eszközök a DHCP szervertől kapnak IP címet, ezeket a kéréseket a WLC továbbítja. A vendég hálózatra csatlakozók kapnak címet, viszont ezen kívül nem érhetik el a szervert az adatok védelmének érdekében. A WLC eszközt szintén nem érhetik el, csakis a Management hálózatból, ugyanis a 30-as VLAN taget állítottuk a WLC eszköz felügyeleti VLAN-jának.

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 információk 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.

Windows szerver

Active Directory

A cégnek létrehoztunk egy saját tartományt, illetve a kezelőjét konfiguráltuk. A döntés a Windows Active Directory Domain Services szolgáltatásra jutott, hiszen ezzel könnyen központilag tudunk létrehozni csoportokat, felhasználókat, akiket különböző csoportokba rakhatunk, mind ezeknek meghatározni az egyéni jogosultságukat, akár egyesével, akár összefogva. A jogosultságok mellett be lehet állítani egy helyről a gépek használatát (háttérkép, frissítések, biztonsági szabályok).

Emellett a felhasználók könnyen beléphetnek akárhonnan a hálózaton belül egy fiók használatával.

A rendszer rendkívül jól skálázható felhasználó mennyiségtől függetlenül. Több tartományt, illetve kezelőt is lehet beállítani.
A szolgáltatás ezen kívül rengeteg vállalati alkalmazás támogatottja, lehet őket használni.

```
PS C:\Users\Administrator> Get-ADForest


ApplicationPartitions : {DC=DomainDnsZones,DC=gandhiegyszalse,DC=net, DC=ForestDnsZones,DC=gandhiegyszalse,DC=net}
CrossForestReferences : {}
DomainNamingMaster    : G1SS1-WS.gandhiegyszalse.net
Domains               : {gandhiegyszalse.net}
ForestMode            : Windows2016Forest
GlobalCatalogs        : {G1SS1-WS.gandhiegyszalse.net}
Name                  : gandhiegyszalse.net
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=gandhiegyszalse,DC=net
RootDomain            : gandhiegyszalse.net
SchemaMaster          : G1SS1-WS.gandhiegyszalse.net
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

A fő tartományvezérlőnek az első telephelyen helyezkedő Windows szervert választottuk. A tartomány neve megegyezik a cégével, „gandhiegyszalse.net” és a 192.168.1.131/28-as IP cím alatt működik.

Létrehoztunk felhasználókat, hozzájuk csoportokat megfelelően, amikbe beraktuk őket, mindezt egyelőre példajelleggel, bemutatási érdekekből, amit természetesen kibővítünk majd, amint megkapjuk a tényleges dolgozói adatbázist az álláspontjukkal.

A jelenlegi felhasználók, akikkel dolgoztunk:

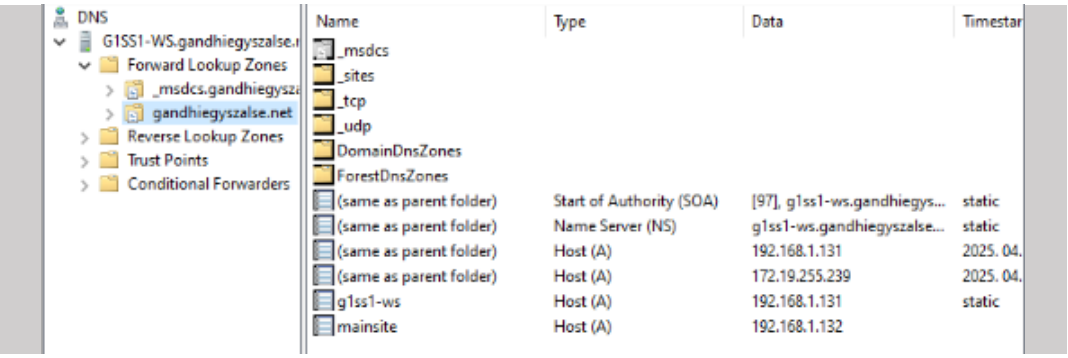
- Munka Misi – Dolgozó
- Olda Gábor – Admin
- Gaz Géza – Vezető

Csoportoknak és pozíciójuknak megfelelően állítottunk be jogosultságokat nekik, az Admin csoportban lévőknek a legmagasabb hozzáférésű jogokat, hiszen neki mindent be kell látnia, mindenbe bele kell látnia.

DNS

A Windows szervert raktuk be DNS szolgáltatónak, így az összes gép hozzá fog fordulni fordítás céljából. Így a gépek a szervert keresik fel a kommunikációhoz, aki megmondja hol található a szerver, amely mögött ott van az oldal, amit felkerestek. A szerver lefordítja a kérést IP címre, hogy az Interneten belül megtalálható legyen az oldal, amit kerestek.

A szolgáltatásba bekerült az Active Domain címe automatikusan, emellett felvettük a Linux szerveren üzemeltett webszervert „mainsite” néven, így akik keresik az oldalt, nem kell tudniuk az IP címet, ami a szerverhez tartozik, elég a weboldal nevét begépelniük.

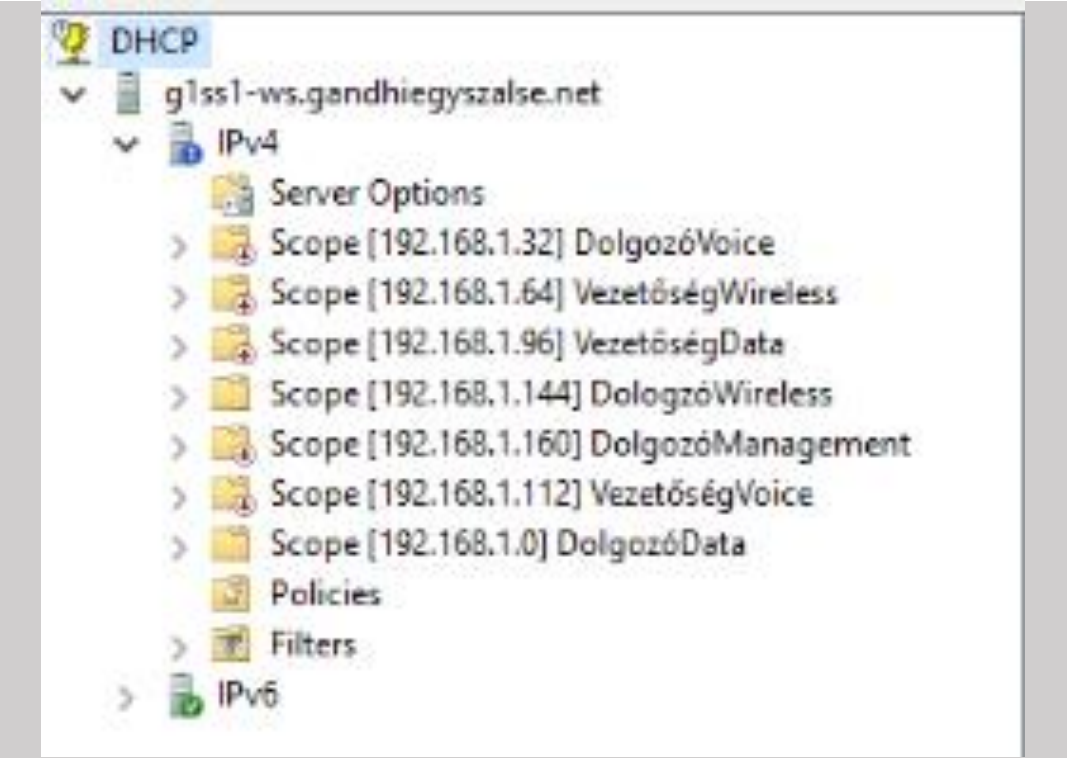


DHCP

A packet tracer és az IP tervezési tábla alapján feltettünk egy DHCP szolgáltatást is a Windows szerverükbe, amelyik jelen esetben az 1. irodának oszt címeket.

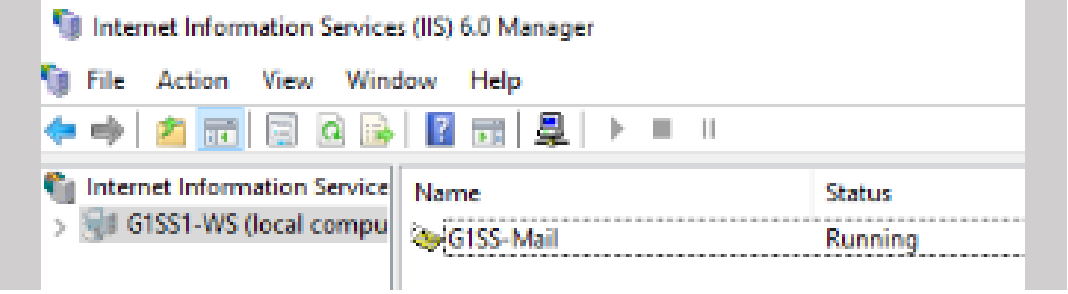
A hálózatban való címzést a Cisco Packet Tracer alkalmazás által nyújtott DHCP szerver által oldottuk meg ténylegesen, ahol Vlan-okra leosztva minden gépnek osztott egyéni címeket.

A szolgáltatás ellenére adtunk ki néhány statikus címet is ki, de a többi gép esetében az Active Directory bejelentkezése miatt nem kell aggódnunk, amiatt, hogy mindig más címet kapnak a gépek, hiszen felhasználóhoz és nem IP-hez vannak kötve a jogosultságok.



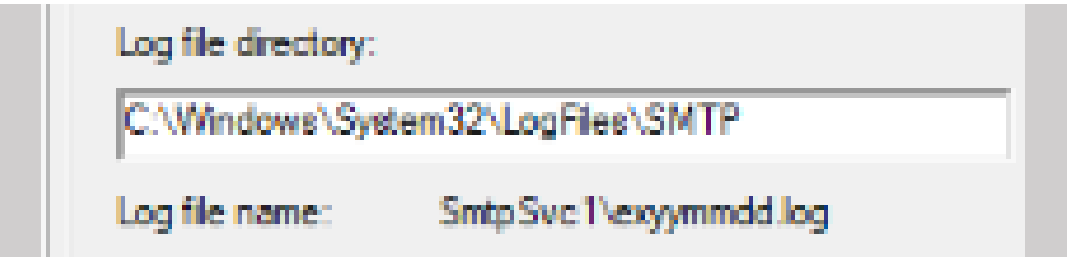
Mail

A cég kikötései és körülményeinek megfelelően konfiguráltunk egy mail szervert az SMTP szolgáltatással. A vállalat nem akart függeni különböző levelező szolgáltatóktól és nem akarják, hogy belső levelezéseik kikerüljenek a külső szerverekre, ezért is kérték a saját mail szervert. A szolgáltatással járó folyamatos figyelmet, kezelést tudják vállalni.



Kérésükre megfigyelhetővé tettük a levelek figyelését, erre külön mappát hoztunk létre, amibe az SMTP küldi a log-okat, azaz mikor küldtek üzenetet, kiment-e az üzenet, illetve, hogy az sikeresen megérkezett-e az.

Ez a szolgálatás hitelességet is nyújt a kliensek, vevők felé, hiszen látják, hogy a saját nevükben, saját szerverükről küldték a levelet. Emellett hosszú távon sokkal jobban megéri a cégnek pénz szempontjából, hiszen nincs szükség így havi licenszdíjakra költeni.



Nyomtató

A nyomtató elérését szintúgy a Windows szerveren valósítottuk meg, ahol elérhetővé tettük a nyilvánosság számára is, amit el tudnak érni a gépekről.

A nyomtatókat megkülönböztettük a hálózatban szereplő Vlan-ok nevei alapján, úgy, hogy egyértelmű legyen az alkalmazottak számára.

Printer Name	Queue Status	Jobs In ...	Server Name	Driver Name
Data nyomtató	Ready	0	G1SS1-WS (loc...	Generic / Text Only
Management nyomtató	Ready	0	G1SS1-WS (loc...	Generic / Text Only
Vezetőségi nyomtató	Ready	0	G1SS1-WS (loc...	Generic / Text Only

Linux szerver

Csatlakoztatás

A két különböző operációs rendszer alapú szerver csatlakozását a samba és a realm protokoll segítségével csatlakoztattuk fel a Windows szerveren futatott tartományba, így elérhetővé válik a Linux szerveren futatott szolgáltatások a tartományban lévő gépek számára is egyszerűen.

```
root@G1SSLinux:~# realm list
gandhiegyszalse.net
  type: kerberos
  realm-name: GANDHIEGYSZALSE.NET
  domain-name: gandhiegyszalse.net
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@gandhiegyszalse.net
  login-policy: allow-realm-logins
```

Webszerver

A szerveren telepítettük az Apache HTTP Server csomagot. Letöltés után létrehoztunk egy külön mappát, amibe elhelyeztük a weboldal fő oldalának jelenleg vázlatos szkriptjét, amit a megállapodások alapján a cég fogja kitölteni, szerkeszteni kedvük szerint a megfelelő tartalomra, ehhez megadtuk a rendszergazdának és a weboldaltervezőknek a hozzáférési utat az oldalhoz. Ezek után módosítottuk az alapértelmezett webtartalmat rejtő mappát, hogy a mi általunk létrehozott HTML állományra mutasson.
Végső teendőként biztosítottuk, hogy a webszerver a megfelelő néven és a hozzátartozó IP címmel legyen megtekinthető, ezt a Windows szerveren található DNS szolgálatáson belül egy új rekord létrehozásával értük el.

FTP

Mivel a cégen belül meglehetősen sok adat folyik át, illetve a web oldalt is fejleszteniük is kell, ezért letöltöttünk egy FTP szolgáltatást, így a Windows gépekről fel és le tudják tölteni az állományokat.

A szervert úgy állítottuk be, hogy az összes felhasználónak legyen egy saját mappája, amihez csak ő tud a felhasználónevével és jelszójával hozzáférni.

Az FTP használatához letöltjük a Windows kliensekre a FileZilla alkalmazást, mivel ez egy grafikus program, így megkönnyíti a dolgozók munkáját, hiszen így nem igényel parancssors tudást, ahhoz, hogy hozzáférjenek a fájlokhoz, ami a szerveren lelhető.

RSYNC

Mivel a Windows szerveren fog futni a legtöbb adat és mivel nem szeretnénk, hogy bármi módon is eltűnjenek, ezért a Debian szerverre feltelepítettük az rsync programot, ami lemásolja és szinkronizálja az eszközöket.

Ezzel a megoldással egész könyvtárakat tudunk másolni át egyik szerverről a másikra. Ezt a folyamatot be tudjuk állítani, hogy milyen időközönként szeretnénk, hogy átmásolja a Debian-ra.

Az egész procedúrához mindkét gépre le kellett töltenem az SSH protokollt is, hiszen az rsync SSH-n keresztül, titkosítva küldi át a változtatott állományokat tömörítve.

A Windows-os gépen telepítettük emellé a DeltaCopy programot is, amely lehetővé teszi számunkra, hogy grafikusan és egyszerűen hozzáférjünk a másik gépen futatott rsync szolgáltatáshoz.

Hálózat Programozás

Programoztunk egy szkriptet, a netmiko-val, amivel át tudjuk írni a forgalomirányítók adatait tetszésünk szerint esetleges utólagos konfiguráció esetében, ha nem férünk hozzá a forgalomirányítóhoz.

A netmiko egy python kiegészítés, ami leegyszerűsíti a CLI csatlakozást több gyártó általi specifikus eszközhöz. A célja, hogy széleskörön belül automatizálja a hálózatokat show parancsokból, miközben változtathatjuk a konfigurációt.