Vizsgaremek Dokumentáció

Ismertető leírás

Külkereskedelmi Technikum

Informatikai rendszer- és alkalmazás-üzemeltető technikus

Tartalomjegyzék

[Bevezetés 2](#_Toc127538521)

[Telephelyek 3](#_Toc127538522)

[The Marathon: 3](#_Toc127538523)

[The Blesston: 7](#_Toc127538524)

[The Coleton 9](#_Toc127538525)

# Bevezetés

Ebben a dokumentációban összegzésre kerül Kádár Kristóf, Zachar András és Buzsák Norman által készített vizsgaremeknek teljes körű leírása. Ez a dokumentáció segítséget nyújt a vizsgaremekben szereplő minden hálózati szolgáltatás és működési sajátosság megértéséhez. Azonban mielőtt az egész vizsgaremeket megismernénk felületesen felvázolnám miről is lesz szó.

Elsőkörben a telephellyel kapcsolatos tudnivalókat fogom leírni. Itt kitérek minden olyan információra, amely elengedhetetlen az épületek ismerete érdekében, mint például az alapterület, helységek mérete, a belmagasság, a falvastagság, a feladatkör és egyéb építési sajátosságok.

Ezt követően szót ejtek a hálózatot megvalósító alkotóelemekről és a fizikai, illetve logikai topológiáról. A hálózatban alkalmazandó eszközöket, illetve fizikai átviteli közegeket és operációs rendszereket a mai modern elvárásoknak megfelelően választottuk ki. Az elvárásoknak megfelelve igyekeztünk mindent a lehető legjobban átgondolni és megvalósítani és ezeket tesztelni. A biztonság és tökéletes működés érdekében számos óvintézkedéseket hajtottunk végre. Igyekezetünk kitartott amellett is, hogy igényes átlátható és könnyen megérthető legyen mindenki számára a hálózat felépítése és működése. A továbbiakban ismertetve lesz minden olyan létfontosságú információ, amely segíti hálózat megértését.

A teszteléskor igyekeztünk elvonatkoztatni az emulátor programok használatától és inkább a szimulátorok felé vettük az irányt, hogy minél inkább valósághűbb környezetben érezhessük magunkat nem beszélve a sokkalta több funkció és lehetőség tárházáról. Azonban ehhez szükségünk volt erőforrásokra is. Sok idő és utánajárás árán sikerült is megvalósítani a megfelelő tesztkörnyezetet, amely lehetőséget adott arra, hogy tesztelhessük azt, hogy elképzelésünk megállná-e a helyét valós környezetben vagy sem. Azonban ennek köszönhetően megbizonyosodtunk róla, hogy működne a hálózatunk, ha megvalósítanánk élőben is. A későbbiekben a tesztelésről is szó esik hogyan sikerült megvalósítani, miféle problémákba ütköztünk és ezek után mely mérföldköveket sikerült elérnünk. A tesztelésről a **tesztelési leírásban** lesz szó.

Végezetül a feladat megoldásához alkalmazott összes alkalmazásra, szolgáltatásra és segítségre is kitérünk. Ezek nélkül sokkal bonyolultabb és átláthatatlan lett volna a munkánk haladásának nyomon követése.

Hálózati terv és működése

Hosszas tanácskozást követően három helyileg különböző, de országosan egy, azonban elhelyezkedésileg több száz kilométeres távolságban tartózkodó irodai (a továbbiakban telephely) épületekre esett a választásunk. Ezen irodák újságírói feladatkört látnak el egy hírlap számára. A három telephely közül egy nagyobb, illetve kettő kisebb területű épületekről beszélhetünk. A telephelyek számára elengedhetetlen az internetelérés mivel a fő tevékenység ott jelenik meg az olvasók számára. (Bevezetés)

Az eszközök közötti hatékony kommunikáció érdekében a hálózati topológia kulcsfontosságú szempont hálózatunk tervezésében. Több útválasztó és kapcsoló kombinációját vezettük be, hogy biztonságos és megbízható infrastruktúrát hozzunk létre. A hálózat elrendezését gondosan megterveztük, hogy optimális összeköttetést biztosítsanak a három irodaház között, és úgy terveztük, hogy méretezhető és alkalmazkodó legyen a szervezet változó igényeihez. Kialakítása stabilitást és hatékonyságot biztosít a szervezet kommunikációs igényeinek kielégítésében. (Hálózat kialakítása)

Hálózati infrastruktúránk kiterjesztett fa topológiából áll, és mindhárom telephely külön forgalomirányítóval van felszerelve. Ez a tervezési megközelítés számos előnnyel jár, beleértve a megnövelt hálózati teljesítményt és jobb hálózati rugalmasságot. Mivel minden útválasztó felelős a saját telephelyén belüli forgalom kezeléséért, a teljes hálózati terhelés megoszlik, csökkentve az egyetlen központi útválasztóra nehezedő terhelést. Ez hatékonyabb és stabilabb hálózatot eredményez, csökkentett állásidővel és nagyobb megbízhatósággal. Ezenkívül a kiterjesztett fa topológia nagyobb testreszabási lehetőséget kínál, lehetővé téve az egyes telephelyek egyedi követelményeinek megfelelő specifikus konfigurációját, ezáltal növelve a hálózat hatékonyságát. (Topológia)

Az eszközszám meghatározásának folyamata kulcsfontosságú volt, mivel ez alapozta meg a hálózati infrastruktúra tervezését és megvalósítását. A hálózatban használt eszközök számát a hálózati követelmények és használati szokások alapján határoztuk meg. A három telephelyet külön-külön elemeztük, hogy meghatározzuk a szükséges eszközök optimális számát. A helyiségek közül kettő egy darab forgalomirányítóval és legalább három darab kapcsolóval, legalább egy szerverrel és legalább két hozzáférési ponttal.(Eszközszám)

Az útválasztók hálózati topológiánk alapvető összetevői. Ők felelősek az eszközök és az internet közötti forgalom irányításáért. Mindhárman teljes adminisztrátori hozzáféréssel rendelkezünk az útválasztókhoz, és bármilyen konfigurációs vagy felügyeleti feladatot elvégezhetünk. Hálózatunk biztonsága érdekében az útválasztókat MD5 hash algoritmussal titkosított jelszavakkal védjük. Ez megnehezíti az illetéktelen felhasználók hozzáférését az eszközhöz, mivel a jelszavak rögzített hosszúságú hash-értékként tárolódnak és nem pedig egyszerű szövegként. (Router: password)

Hálózatunk biztonsága iránti elkötelezettségünk részeként egyéb különféle biztonsági funkciókat is használunk, mint például a Virtual Private Network (VPN) és a Secure Shell (SSH).

A virtuális magánhálózat (VPN) segítségével biztonságos kapcsolatot biztosítunk titkosítással, hogy megvédjük az érzékeny információkat az illetéktelen hozzáféréstől. A VPN-ek számos előnyt kínálnak, beleértve a távoli hozzáférést azoknak a dolgozóknak, akiknek az irodán kívül kell hozzáférniük a vállalati erőforrásokhoz, miközben megőrzik a biztonságot. Ezenkívül a VPN-ek felhasználhatók a webhelyekre és online szolgáltatásokra vonatkozó földrajzi korlátozások megkerülésére, így a felhasználók hozzáférést biztosítanak a régiójukban blokkolt vagy korlátozott tartalmakhoz. Ezenkívül a VPN-ek költségmegtakarítást kínálnak az utazási és egyéb költségek csökkentésével, mivel a távoli dolgozók bárhonnan hozzáférhetnek a vállalati erőforrásokhoz internetkapcsolattal, így pénzt takarítanak meg a drága bérelt vonalakon és egyéb hálózati infrastruktúrákon. (Router: VPN)

Az SSH vagy a Secure Shell számos előnnyel rendelkezik. Először is, az SSH biztonságos távoli hozzáférést tesz lehetővé az eszközökhöz és szerverekhez az interneten keresztül, lehetővé téve a rendszerek kezelését és konfigurálását a világ bármely pontjáról. Ezenkívül az SSH-kliensek és a szerverek között továbbított összes adat titkosított, így védelmet nyújt a lehallgatás és más biztonsági fenyegetések ellen. Az SSH Secure File Transfer Protocol (SFTP) segítségével a rendszergazdák biztonságosan továbbíthatnak fájlokat az eszközök és a szerverek között. Ezenkívül, erős hitelesítési módszereket biztosít, beleértve a nyilvános kulcsú hitelesítést is, hogy csak az arra jogosult felhasználók férhessenek hozzá a rendszerekhez. Ez a funkció segít megelőzni az illetéktelen hozzáférést, és biztosítja, hogy csak azok férhessenek hozzá, akiknek a rendszerhez hozzá kell férniük. Végül az SSH használható biztonságos alagutak létrehozására az eszközök között, lehetővé téve a forgalom biztonságos áthaladását közöttük. Ez a funkció különösen hasznos az internetről közvetlenül nem elérhető források eléréséhez. (Router: SSH)

Összességében mind a VPN, mind az SSH kulcsfontosságú eszközök a hálózatok védelmében és az érzékeny adatok védelmében. E technológiák használatával a szervezetünk magas szintű biztonságot tarthat fenn, és biztosak lehetünk abban, hogy adataink biztonságban maradnak a kíváncsi szemek elől.

A virtuális terminálvonalak konfigurálása az útválasztókon fontos feladat az eszközök hálózaton keresztüli távoli eléréséhez. Ezek segítségével a jogosult felhasználók távolról hozzáférhetnek az eszközhöz és konfigurálhatják annak beállításait. A hitelesítés helyi felhasználónevekkel és jelszavakkal létesíthető, a távoli hozzáférés pedig SSH protokollal engedélyezhető.(Router: vty line)

Forgalomirányítóink számos alapvető funkciót képesek ellátni, mint például a hálózati címfordítás (NAT) és az IP-útválasztás. Ők irányíthatják a forgalmat a különböző hálózatok között.

A Network Address Translation (NAT) egy olyan technológia, amely számos előnnyel jár a számítógépes hálózatokban. A NAT hálózati infrastruktúránk kritikus összetevője, amely lehetővé teszi több eszköz számára, hogy megosszák egyetlen nyilvános IP-címet. Ez a funkció megőrzi a nyilvános IP-címeket, ami különösen hasznos olyan helyzetekben, amikor az elérhető nyilvános IP-címek száma korlátozott. NAT nélkül hálózatunknak sokkal nagyobb számú nyilvános IP-címre lenne szüksége, ami költséges és nehezen kezelhető lenne. Ezért a NAT kulcsfontosságú szerepet játszik hálózatunk hatékony és eredményes működésében.

Ezenkívül a NAT tűzfalként működik az internet és a privát hálózatunk között, és bizonyos szintű biztonságot nyújt azáltal, hogy elrejti a magánhálózaton lévő eszközök IP-címét. A NAT úgy is konfigurálható, hogy blokkolja a bejövő forgalmat a magánhálózat bizonyos portjaira, szükség esetén tovább növelve a hálózat biztonságát.

A NAT rugalmasságot biztosít a hálózattervezésben is, ugyanis lehetővé teszi a magánhálózat eszközei számára, hogy olyan privát IP -címeket használjanak, amelyek nem nyilvánosan mozgathatók. Így akár kibővíthetjük vagy újrakonfigurálhatjuk a magánhálózatunkat a nyilvános IP -címek megváltoztatása nélkül, így a NAT növeli hálózatunk kialakításának rugalmasságát.

A terheléselosztás olyan kritikus tulajdonság, amelyet a NAT biztosít a hálózati teljesítmény és a rendelkezésre állás javítása érdekében. A hálózati forgalom több nyilvános IP -címen történő elosztásával a NAT hatékonyan képes kezelni a hálózati forgalom áramlását, megakadályozva a szűk keresztmetszeteket és biztosítva az erőforrások hatékony felhasználását. Ez különösen hasznos a nagy forgalmú környezetben, ahol a hálózati teljesítmény kritikus. Ezenkívül a NAT -val történő terheléselosztása elősegítheti annak biztosítását, hogy a hálózati erőforrások mindig rendelkezésre álljanak, még meghibásodás vagy leállás esetén is. (Router: NAT)

Az IP útválasztás a modern számítógépes hálózat kritikus eleme, és számos fontos előnyt nyújt. Ezen előnyök egyike a hálózati erőforrások hatékony felhasználása, mivel az IP -útválasztás biztosítja, hogy az adatcsomagjaink a lehető legrövidebb úton keresztül kerüljenek át, ami csökkenti a hálózatunk torlódását és javítja az általános hatékonyságot.

Ezenkívül az IP útválasztási protokollok redundanciát és hibatoleranciát biztosítanak, a hálózati hibák észlelése és a forgalom automatikus átirányítását az alternatív utakra, biztosítva, hogy a hálózatunk működőképes maradjon. Végül, az IP útválasztás lehetővé teszi a skálázhatóságot azáltal, hogy lehetővé teszi a hálózatnuk kisebb alhálózatokra történő felosztását, amelyek függetlenül kezelhetők és konfigurálhatók, nagyobb rugalmasságot biztosítva a hálózati tervezésben és a nagyobb hálózatok befogadására akár több ezer eszközzel. (Router: Ip routing)

Ezeken a biztonsági szolgáltatásokon túlmenően hozzáférés-vezérlési listákat (ACL) írtunk az útválasztóknak, hogy további biztonságot nyújtsunk. Az ACL-ek konfigurálásával szabályozzuk, hogy mely eszközök kommunikálhatnak a hálózattal, és korlátozzuk a hozzáférést az érzékeny információkhoz.

Kibővített ACL-eket használtunk a hálózati forgalom szűrésére különféle kritériumok alapján, például forrás- és cél IP-címek, protokollok és portok alapján. Ezek a szabályok használhatók a VPN-kapcsolat különböző hálózatai közötti forgalom szabályozására. Az ACL engedélyezi vagy tiltja a forgalmat a szabályokban meghatározott feltételek alapján, ami segíthet a hálózat biztonságában, és biztosítja, hogy csak engedélyezett forgalom haladjon át.(Router: ACL)

Összességében az útválasztók kulcsfontosságúak hálózatunk biztonságának és funkcionalitásának fenntartásához. Különféle biztonsági funkciók megvalósításával és az útválasztók képességeinek kihasználásával biztosíthatjuk hálózatunk biztonságosságát. (Router)

UA kapcsolók több kapcsolat létrehozására szolgálnak a hálózaton belül, lehetővé téve az eszközök egymás közötti kommunikációját.

A kapcsolók a hálózati infrastruktúra szerves részét képezik, lehetővé téve az eszközök számára, hogy egy hálózaton belül több kapcsolat létrehozásával kommunikáljanak egymással. A kapcsolóknak két fő típusa van: a 2. rétegű és a 3. rétegű kapcsolók.

A 2. rétegbeli kapcsolók az adatkapcsolati rétegben működnek, lehetővé téve virtuális LAN-ok (VLAN) létrehozását, és gyorsabb és hatékonyabb kommunikációt biztosítanak az eszközök között. Különösen hasznosak kis és közepes méretű hálózatokban, ahol VLAN-szegmentációra van szükség a hálózat biztonságának javítása és a forgalmi torlódások csökkentése érdekében.

A 3. rétegbeli kapcsolók a hálózati rétegben működnek, és rendelkeznek a 2. réteg kapcsolóinak összes funkciójával, de hozzáadott útválasztási képességekkel. IP-útválasztást hajtanak végre, és támogatják az olyan protokollokat, mint az OSPF, EIGRP és BGP, így ideálisak nagyobb hálózatokhoz, ahol hatékony útválasztásra van szükség.

Összességében a kapcsolók használata számos előnnyel jár, beleértve a jobb hálózati teljesítményt, a méretezhetőséget és a rugalmasságot.

Az egyes telephelyeken lévő végberendezések, például számítógépek és nyomtatók összekapcsolására kapcsolók szolgálnak.

U

UA tűzfalak alapvető fontosságúak hálózati topológiánkban, mivel további biztonsági réteget és védelmet nyújtanak a külső fenyegetésekkel szemben.

Az Adaptive Security Appliance (ASA) tűzfal a Cisco Systems által kifejlesztett hálózati biztonsági eszköz. A hálózatok védelmére szolgál a biztonsági fenyegetésekkel, például az illetéktelen hozzáféréssel, vírusokkal és más típusú rosszindulatú forgalommal szemben.

Az ASA tűzfal olyan funkciókat biztosít, mint az állapotalapú csomagellenőrzés, a hozzáférés-vezérlés és a VPN-kapcsolat. A tűzfal számos biztonsági házirenddel és szabállyal konfigurálható a hálózatok közötti forgalom szabályozására és a biztonsági szabályzatok érvényesítésére.

Az ASA tűzfal az OSI modell 4. rétegében (szállítási réteg) és 7. rétegében (alkalmazási réteg) is működhet, és minőségi szolgáltatást (QoS) is képes biztosítani a hálózati forgalom számára. Ez egy sokoldalú és hatékony eszköz a hálózatbiztonsághoz, és széles körben használják a vállalati hálózatokban.U

Szerver: NTP pl, domain name + name server

Acces point

UVLAN-okat használtunk a hálózat szegmentálására, ami fokozott biztonságot és jobb erőforrás-kihasználást tesz lehetővé.

A modern hálózati infrastruktúrában fontos a virtuális helyi hálózatok (VLAN) megvalósítása a hálózat jobb szegmentálása érdekében. A VLAN-ok lehetőséget biztosítanak a hálózati forgalom logikai csoportosítások alapján történő elkülönítésére, és különféle célokra használhatók, például biztonságra, hálózatoptimalizálásra és méretezhetőségre. Ebben az összefüggésben a VLAN-ok megvalósítása hozzájárult a biztonság növeléséhez és a hálózati erőforrások jobb kihasználásához.

A VLAN-ok egyik előnye a fokozott biztonság, mivel a forgalom funkciójuk vagy elhelyezkedésük alapján elkülöníthető az eszközök különböző csoportjai között. Ez azt jelenti, hogy ha a VLAN egyik eszköze veszélybe kerül, az nem tud könnyen átterjedni a többi VLAN-ban lévő eszközre. Ezenkívül a VLAN-ok jobb erőforrás-kihasználást biztosítanak azáltal, hogy lehetővé teszik a hálózati adminisztrátorok számára, hogy az igényeik alapján hálózati erőforrásokat rendeljenek hozzá adott VLAN-okhoz. Például a nagy sávszélességű eszközök, például a szerverek saját VLAN-ba, míg a kis sávszélességű eszközök, például a nyomtatók külön VLAN-ba helyezhetők.

A bemutatott hálózati topológiában a VLAN-okat különböző célokra használták, mint például felügyelet, iroda, Wi-Fi, nyomtató, szerver és üres. Ezek a VLAN-ok különböző alhálózati tartományokkal rendelkeznek, és a hálózati forgalom logikai elkülönítésére szolgálnak. Ezenkívül a natív VLAN név "NASA" rövidítésének használata kreatív és emlékezetes módja a VLAN elnevezésének, megkönnyítve a hálózati rendszergazdák számára a hálózat kezelését és karbantartását. Összességében a VLAN-ok megvalósítása javította a hálózat biztonságát, teljesítményét és méretezhetőségét, így fontos szempont a modern hálózattervezésben és adminisztrációban.

Mind a 3 telephelyen létre lett hozva az összes említett vlan.U

NORMAN KÉRTE:

Míg a „NASA” általában a National Aeronautics and Space Administration rövidítése, számos okból jó választás lehet natív VLAN névként egy hálózati rendszerben:

Könnyen megjegyezhető: A „NASA” jól ismert rövidítése a hálózati rendszergazdák és a felhasználók számára könnyen megjegyezhető, ami segíthet csökkenteni a hibákat és leegyszerűsíteni a hálózatkezelést.

Egyedi és megkülönböztethető: A „NASA” natív VLAN-névként való használata segíthet megkülönböztetni a hálózat többi VLAN-jától, így könnyebben azonosítható és kezelhető.

Inspiráló és motiváló: A „NASA” névhez a felfedezés, a felfedezés és az innováció kapcsolódik, ami kreatív gondolkodásra ösztönözheti és motiválhatja a hálózat használóit, és feszegetheti a hálózati rendszerrel lehetséges lehetőségek határait. ezt ki lehet törölni

Egy hálózati diagram készült, amely vizuálisan ábrázolja a hálózat kialakítását és elrendezését.

A topológia célja, hogy minimalizálja az eszközök közötti ugrások számát, ami csökkenti a késleltetést és javítja az általános hálózati teljesítményt.

A hálózatban használt eszközök számát úgy optimalizálták, hogy egyensúlyt biztosítsanak a költségek és a funkcionalitás között.

A hálózat kialakítása redundáns összetevőket tartalmaz, amelyek biztosítják a hálózat működőképességét, még akkor is, ha egy eszköz meghibásodik.

A hálózatban használt eszközöket a megbízhatóságuk és a hálózati tervezéssel való kompatibilitásuk miatt választották ki.

A hálózati topológia célja, hogy könnyű hozzáférést biztosítson az internethez, ami elengedhetetlen az oldalak fő tevékenységéhez.

Hálózati kialakításunk lehetővé teszi az összes eszköz közötti hatékony kommunikációt, még akkor is, ha azok különböző épületekben találhatók.

A hálózati topológia robusztus és skálázható megoldást biztosít, amely alkalmas a jövőbeli növekedésre.

A hálózati topológia kialakításakor figyelembe vettük az egyes irodaházak elhelyezkedését és a többi telephelyhez való közelségét.

A hálózat kialakítása megfelelő intézkedéseket tartalmaz a hálózathoz és eszközeihez való jogosulatlan hozzáférés megakadályozására.

Hálózati topológiánk egyszerű hibaelhárítást tesz lehetővé, ha bármilyen probléma merülne fel, világos útvonalakat biztosítva az adatok áramlásához.

A hálózati topológia célja, hogy a három irodaház hatékonyan tudjon kommunikálni, még nagy távolság mellett is.

IP-címzési séma: definialas a hálózatban használt IP-címsémát, és azt, hogy ez hogyan teszi lehetővé az eszközök egymás közötti kommunikációját.

Az IP-címzési séma hálózatunk kulcsfontosságú eleme, amely lehetővé teszi az eszközök kommunikációját és adatcseréjét.

Hálózatunk minden egyes eszközhöz egyedi IP-címet használ, lehetővé téve azok azonosítását és megcímzését a hálózaton.

Az IP-címzési séma magán és nyilvános IP-címek kombinációját tartalmazza, biztosítva a biztonságot és a hatékony kommunikációt.

Az IP-címek kiosztása alhálózati technikával történik, amely lehetővé teszi a hálózat hatékony szervezését és kezelését.

IP-címzési rendszerünk támogatja mind az IPv4, mind az IPv6 protokollokat, biztosítva a kompatibilitást eszközök és technológiák széles skálájával.

A statikus IP-cím-hozzárendelés használata biztosítja, hogy az eszközök újraindítás után is megőrizzék ugyanazt az IP-címet.

Az IP-címzési séma lehetővé teszi a hálózati forgalom hatékony irányítását, biztosítva az adatok hatékony továbbítását az eszközök között.

Az IP-címzési séma a távoli hozzáférést is támogatja, lehetővé téve az eszközök távoli kezelését és karbantartását.

Az IP-címzési sémát rendszeresen felülvizsgálják és frissítik annak biztosítása érdekében, hogy továbbra is hatékony, biztonságos és alkalmazkodó legyen a változó hálózati követelményekhez.

Az IP-címzési séma hálózatunk alapvető eleme, és döntő szerepet játszik az eszközök közötti hatékony kommunikáció és adatcsere biztosításában.

Útválasztási protokoll: definialasa hálózatban használt útválasztási protokollt és azt, hogy az hogyan teszi lehetővé az eszközök közötti hatékony kommunikációt.

Biztonsági intézkedések: definialas a biztonsági intézkedéseket, amelyek megvédik a hálózatot a külső fenyegetésektől, például tűzfalaktól, hozzáférés-vezérlési listáktól (ACL-ek) és virtuális magánhálózatoktól (VPN).

Hálózatfigyelés: definialas, hogyan figyeli a hálózatot a rendelkezésre állás és a teljesítmény biztosítása érdekében, beleértve a hálózatfigyeléshez használt eszközöket és módszereket.

Biztonsági mentés és katasztrófa utáni helyreállítás: Beszélje meg a biztonsági mentési és katasztrófa-helyreállítási terveket, amelyek megvédik a hálózati hibákat, és biztosítják, hogy a hálózat gyorsan helyreálljon katasztrófa esetén.

Karbantartás és frissítések: Ismertesse a hálózat karbantartásának és frissítésének eljárásait és ütemezését, beleértve a hardver- és szoftverfrissítéseket.

A „HÁLÓZATI TERV ÉS MŰKÖDÉSE” részben ezekre a témákra kiterjedően átfogó áttekintést nyújt a hálózatáról, valamint arról, hogyan kezelik azt a rendelkezésre állás, a teljesítmény és a biztonság biztosítása érdekében.

Windows

Azért esett a választásunk a Windows szerverekre, mert széles körben használják a vállalati környezetekben, és számos szolgáltatást nyújtanak, például fájl- és nyomtatásmegosztást, címtárszolgáltatásokat, webszolgáltatásokat és adatbázis-kezelést. Ezen túlmenően a Windows-kiszolgálók a biztonsági funkciók és felügyeleti eszközök robusztus készletét kínálják, így ideális választást jelentenek számunkra a szerver-infrastruktúra hatékony karbantartásához és kezeléséhez.

A DNS vagy a tartománynévrendszer minden hálózati infrastruktúra kulcsfontosságú összetevője, mivel az ember által olvasható tartományneveket IP-címekké fordítja, amelyek szükségesek az eszközök internethez való csatlakozásához. A DNS-kiszolgálókat megfelelően konfigurálni kell a DNS-sel kapcsolatos problémák vagy biztonsági fenyegetések elkerülése érdekében.

A Syslog egy szabványos protokoll, amely rendszernapló- vagy eseményüzenetek küldésére szolgál a naplózószervernek. A rendszergazda a Syslog segítségével figyelheti és háríthatja el a hálózati problémákat, a biztonsági fenyegetéseket és a teljesítménnyel kapcsolatos problémákat.

Az Active Directory a Microsoft által kifejlesztett címtárszolgáltatás, amely lehetővé teszi a rendszergazdák számára a hálózat erőforrásainak kezelését és rendszerezését. Központi helyet biztosít a hálózati felhasználók és erőforrások számára, lehetővé téve a rendszergazdának az engedélyek és a hozzáférés-szabályozás hatékonyabb kezelését. Az Active Directory kritikus fontosságú a hálózat biztonsága és teljesítménye szempontjából, és az optimális működés érdekében megfelelően be kell állítani.

Linux

A Linux egy rendkívül rugalmas operációs rendszer, amely testreszabható az üzleti igényeknek megfelelően. Robusztus biztonsági funkcióiról is ismert, így kevésbé sebezhető a vírusokkal és rosszindulatú programokkal szemben, mint más operációs rendszerek. Megbízható, sok munkát elbír, megfizethető és nyílt forráskódú, ami azt jelenti, hogy a különböző igényeknek megfelelően alakítható.

A DHCP vagy Dynamic Host Configuration Protocol egy módja annak, hogy az eszközök automatikusan kapjanak IP-címet, amikor hálózathoz csatlakoznak. Segít csökkenteni a hálózat beállításához szükséges munkát azáltal, hogy kiküszöböli az IP-címek manuális hozzárendelését az egyes eszközökhöz. A DHCP-kiszolgáló más fontos hálózati beállításokat is hozzárendelhet, például alhálózati maszkot, átjárót és DNS-kiszolgáló IP-címét, ami hatékonyabbá teszi a hálózatkezelést.

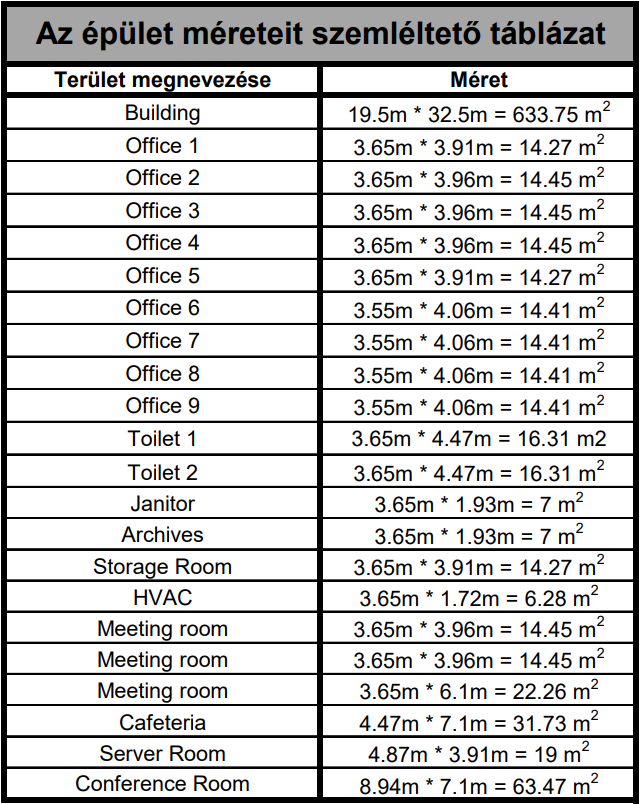
A webszolgáltatás egy olyan szoftverrendszer, amely lehetővé teszi, hogy a gépek szabványosított módon kommunikáljanak egymással a hálózaton keresztül. Segít integrálni a különböző alkalmazásokat, adatbázisokat és rendszereket különböző platformokon és technológiákon keresztül. Rendszergazdaként alapvető fontosságú, hogy figyelemmel kísérje a webszolgáltatások teljesítményét és biztonságát, hogy a végfelhasználók gond nélkül hozzáférhessenek hozzájuk.

tlcsh pinget ne felejtsuk el megirni

# Telephelyek

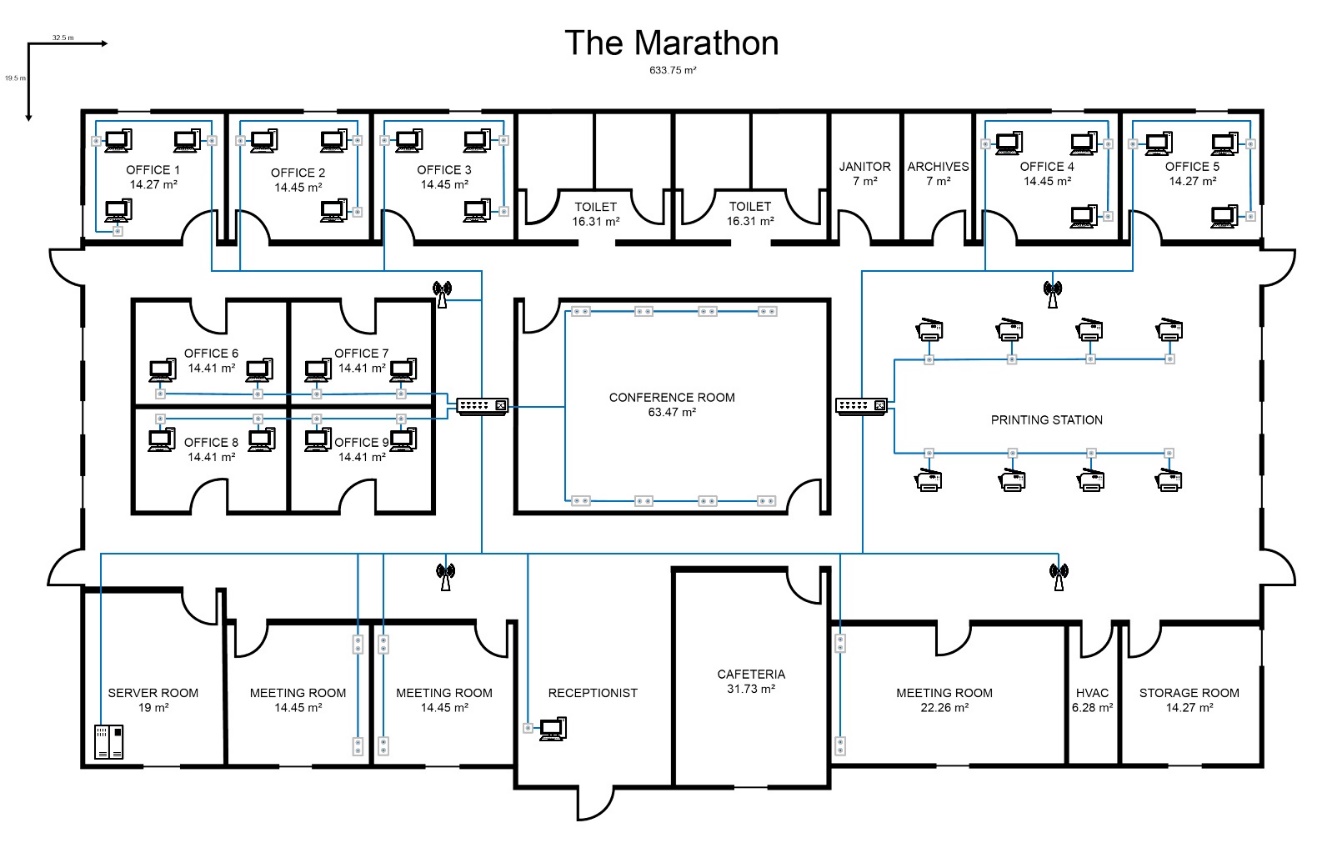
## The Marathon:

Ez a telephely a legnagyobb mindhárom közül és itt valósul meg több olyan elvárás, amelynek eleget kellett tennünk, mint például a redundáns megoldások. Bonyolultságát tekintve ez a telephely a legösszetettebb. Ez az iroda Budapesten helyezkedik el. Ez az épület a modern építészeti jellemzőket tudhatja magának. Az épület függőleges, illetve vízszintes falai 40 cm-esek. A Belmagasság: 4.8 m + 1.2 m álmennyezet. A falak vastagsága változó: az irodák között lévő függőleges válaszfal 10 cm-es és típusa gipszkarton. A vízszintes falak közül a vastagabb válaszfal 20 cm-es míg a vékonyabb szintén 10 cm és gipszkarton. A további méreteket egy táblázat szemlélteti:



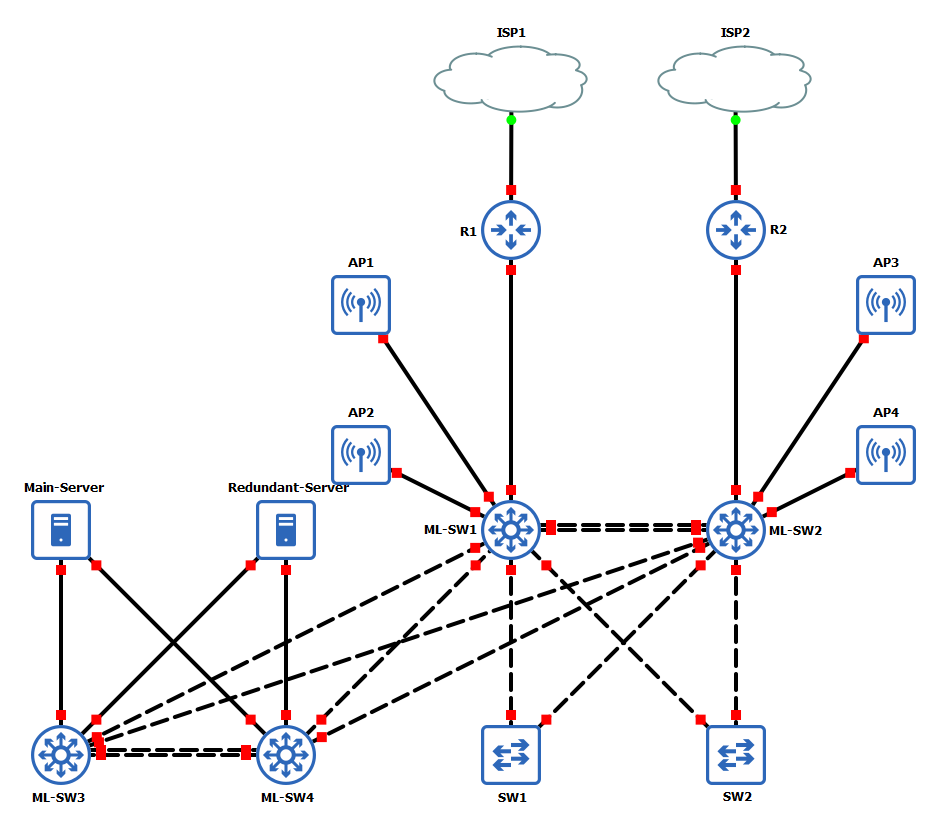
Mint ahogy említettem az épület álmennyezettel is rendelkezik ennek köszönhetően például a kötések megvalósítása egyszerűbb feladatnak bizonyult. A kötés a következő képen látható:

Kötésirajz:



Ezen látható, hogy a szerver szóbából (Server Room ) irányul ki minden összeköttetés az épületben. Az átviteli közegnek a mai viszonylatban modernek számító CAT6a UTP kábelt alkalmaztuk. A képen látható kettő kapcsoló () (SW1 és SW2) végzi el a végfelhasználó eszközök (,) összeköttetését a szerver szobához. A négy csatlakozási pont ( ) (AP1, AP2, AP3, AP4) a szerver szobában lévő kapcsoló (ML\_SW1 és ML\_SW2) kapcsolódik. A négyzetek () és téglalapok () az aljzatokat szimbolizálják. A négyzet alakú csatlakozóaljzat egy míg a téglalap alakú pedig két csatlakozási lehetőséget nyújt. Ehhez a telephelyhez a következő topológia tartozik:

Topológia:



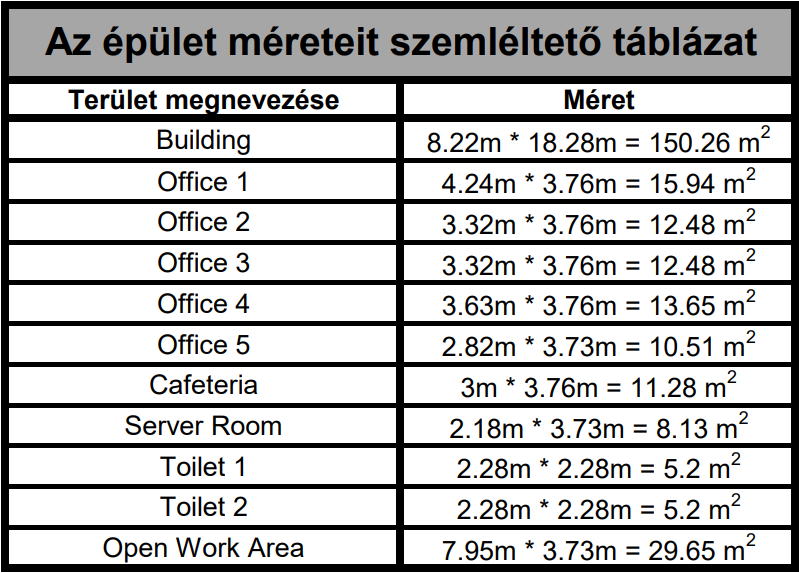
A hálózat működésének leírása:

Fentről lefelé haladva elsőnek az R1 és R2 forgalomirányítókkal találkozunk. A kettő forgalomirányító összeköttetésben áll az ISP-vel (Internet Service Provider) optikai közegen keresztül. A két forgalomirányítóra a redundáns megoldások miatt volt szükség. A két eszköz hasonló konfigurációval rendelkezik. Annyiban különböznek egymástól, hogy míg az R1 VPN kapcsolatot valósít meg a harmadik telephellyel addig az R2 a második telephellyel IPv6-os ún. tunnel kapcsolatot és ezen keresztül dinamikus forgalomirányítást is végrehajt. A forgalomirányítók számos feladatkört látnak el, mint például: címfordítás, VPN összeköttetés, WAN összeköttetés, IPv6 tunnel és dinamikus forgalomirányítás, stb… A forgalomirányítók ezt követően a kettő Multilayer kapcsolóval vannak összeköttetésben. Ez a két kapcsoló (ML-SW1 és ML-SW2) layer 3-as lehetőségét kihasználva a forgalomirányítást ez a két eszköz végzi. A hálózatban vlan-ok kerültek alkalmazásra, melyek segítségével több hálózat megvalósítását teszi lehetővé. A két kapcsoló egymással is össze van kötve port-channel segítségével a nagyobb hálózati sávszélesség megvalósítása érdekében. Ezek a kapcsolók végzik a hálózatban történő forgalom teljes körű irányítását. A kettő kapcsolóra azért volt szükség, mivel ki kell szolgálni a két forgalomirányító által használt HSRP redundáns protokollt. Ezen protokoll az ML-SW1 és ML-SW2 kapcsolón is megtalálható a vlan interfészeken. A kapcsolók feladata ennyiben nem merül ki, mivel a forgalom szűrése is a feladatuk közé tartozik ACL (Access Control List) segítségével. A kapcsolók minden olyan csomagot, amely az intraneten kívülre szándékozunk irányítani ezeket alapértelmezettként a forgalomirányítók (R1 és R2) számára továbbítja tovább. Ezekkel a kapcsolókkal ál összeköttetésben a négy csatlakozási pont (AP1, AP2, AP3, AP4) melyek a vezetéknélküli hálózat megvalósítása érdekében szerepelnek a hálózatban. Az ML-SW1 és ML-SW2 összeköttetésben áll az ML-SW3 és ML-SW4, illetve az SW1 és SW2 kapcsolókkal. Az ML-SW3 és ML-SW4 kapcsoló feladata a két szervert (Main Server és Redundant Server) kiszolgálni a redundáns megoldások érdekében. Ezen két kapcsoló szintén tartalmaz egy port-channel összeköttetést szintén a nagyobb sávszélesség érdekében. Ezek a szerverszámítógépek nyújtanak számos szolgáltatást. Ezek a szervereken egy hardveren két operációs rendszer fut. A két operációs rendszer a Windows Server 2019 és a Debian 11. A fő szerver (Main-Server) az elsődleges szervereket foglalja magába. A másodlagos (Redundant-Server) a fő szerver számára nyújt redundáns megoldást. Ezen operációs rendszerek a VMware ESXI hypervisor-on futnak. A Main-Server-en egy Windows Server 2019 és egy Debian 11 rendszer fut. A Redundant-Server-en ugyanezen rendszerek futnak annak érdekében, hogy megvalósuljon a redundancia. Utoljára maradt az SW1 és SW2 kapcsolók, melyek a végfelhasználói eszközök számára nyújtanak összeköttetést, mint például: a számítógépek és nyomtatók.

## The Blesston:

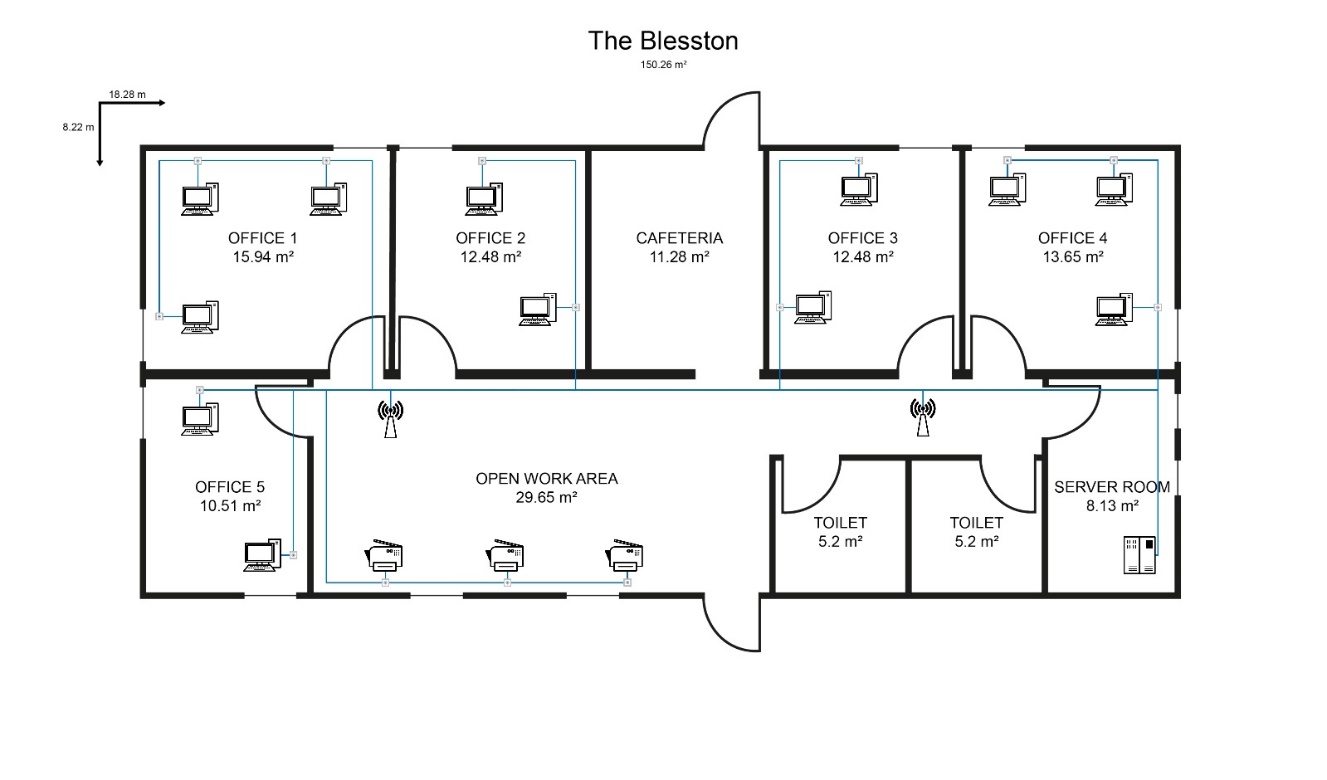
Ez a telephely az egyik a kettő kisebb közül, amelyet egyszerűbb hálózat struktúra jellemez. Ez az iroda Szegeden helyezkedik el. Itt nem volt szükség bonyolult hálózat kiépítésére mivel egy ilyen kisméretű iroda számára felesleges. Ez az telephely kiegészítő munkát végez a fő iroda számára. Ez az épület is a modern építészeti jellemzőket tudhatja magának. Az épület függőleges, illetve vízszintes falai 40 cm-esek. A belmagasság: 3.8 m + 1.2 m álmennyezet. A falak vastagsága változó: az irodák között lévő függőleges válaszfal 10 cm-es és típusa gipszkarton. Az irodaépület közepén elhúzódó vastag válaszfal 50 cm-es téglafal. A további méreteket egy táblázat szemlélteti:

Mérettáblázat:



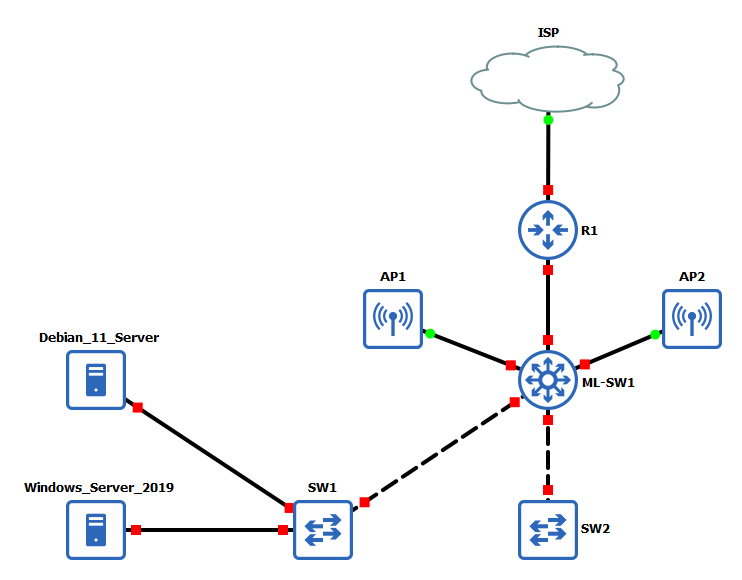
Ahogy említettem az épület rendelkezik álmennyezettel aminek segítségével egyszerűbben sikerült a kötések megvalósítása. A következő képen ez látható:

Kötésirajz:



Ezen látható, hogy a szerver szóbából (Server Room ) irányul ki minden összeköttetés csakúgy, mint az első telephelyen. Az átviteli közegnek a mai viszonylatban modernek számító CAT6a UTP kábelt alkalmaztuk. A végfelhasználói eszközök (,) kiszolgálását az SW2 kapcsoló látja el a szerver szóbából. Nem tartottuk fontosnak kivenni onnan mivel az épület alapterülete nem indokolja ezt. A kettő csatlakozási pont ( ) (AP1, AP2) a szerver szobában lévő kapcsoló (ML\_SW1 és ML\_SW2) kapcsolódik. A négyzetek () az aljzatokat szimbolizálják. A négyzet alakú csatlakozóaljzat egy csatlakozási lehetőséget nyújt. Ehhez a telephelyhez a következő topológia tartozik:

Topológia:

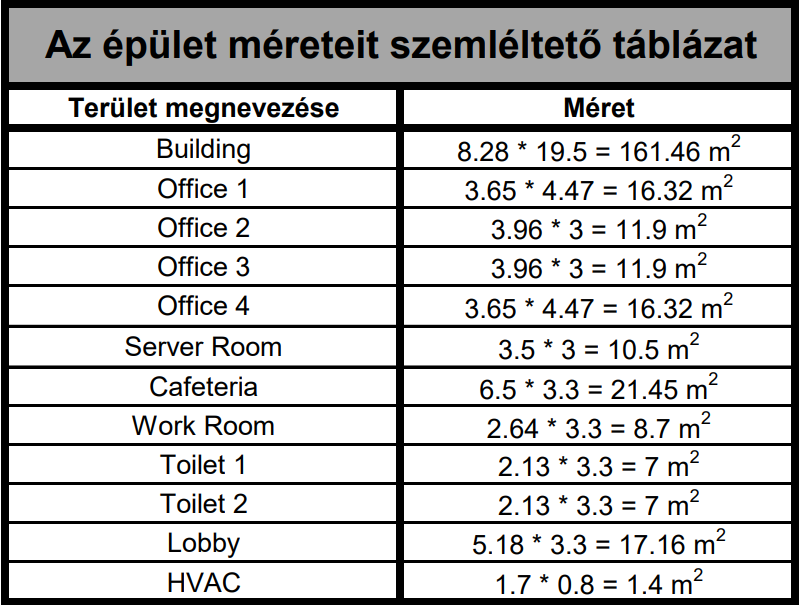


A hálózat működésének leírása:

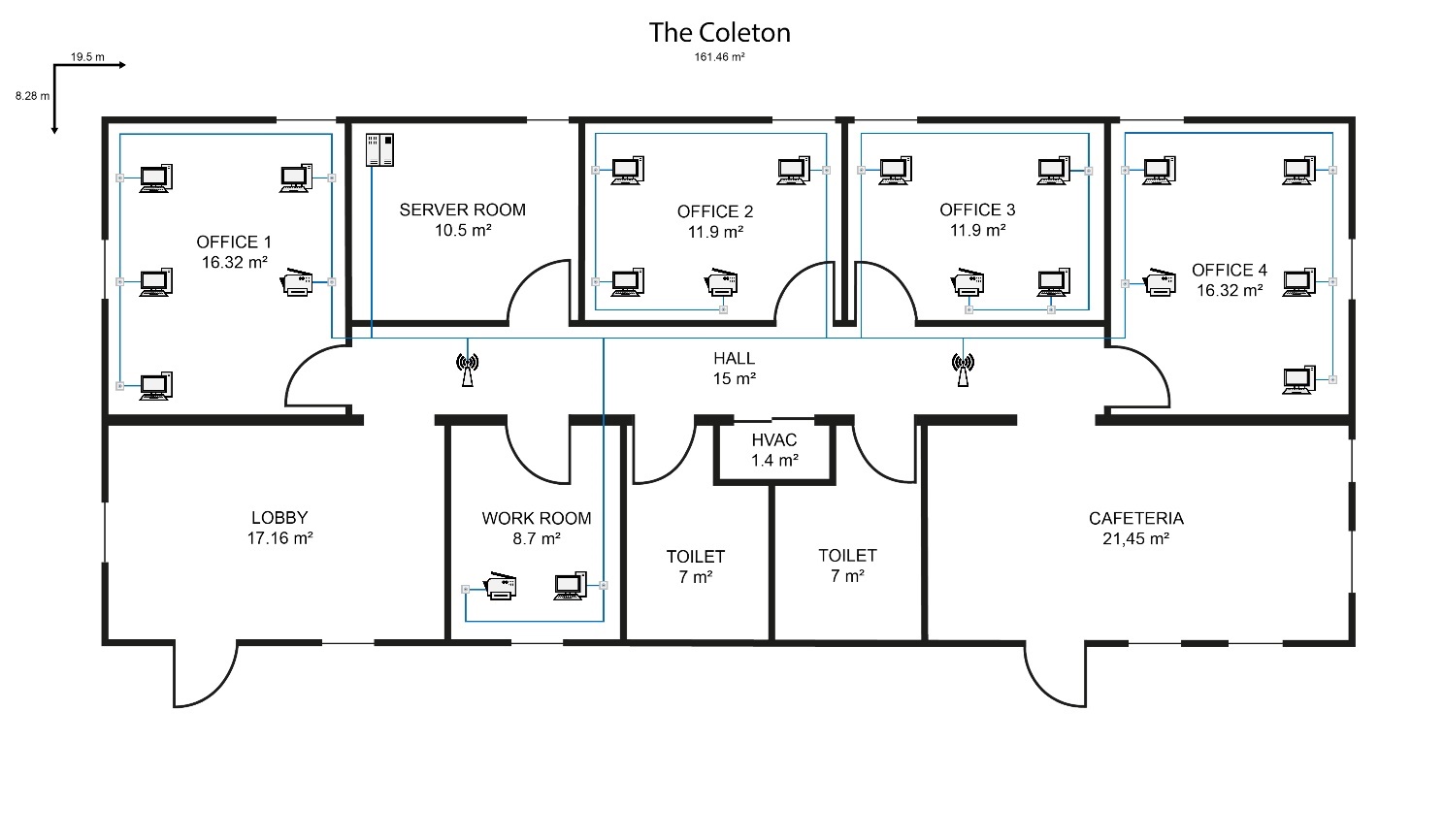
## The Coleton

Az utolsó telephely, amely szinte megegyező hálózati struktúrán osztozik az előző telephellyel.

Mérettáblázat:



Kötésirajz:



Topológia:

A hálózat működésének leírása:

Szerverek:

AlKalmazások

*A rendszeradminisztrációs projektünkben használt programok és alkalmazások áttekintése*

Hálózatépítés projektünk során különféle programokat és használtakat használtunk munkánk alkalmazására. A Packet Tracerben, amely egy hálózati szimulációs eszköz, létrehozhattuk hálózatunk vizuális megjelenítését, és konfiguráltuk az eszközöket, például útválasztókat, kapcsolókat és hozzáférési pontokat. Különböző hálózati forgatókönyvek szimulálására és konfigurációink tesztelésére is használtuk. Ez lehetővé tette számunkra, hogy azonosítsuk a lehetséges problémákat, és módosításokat hajtsunk végre a tényleges hálózaton történő változtatások végrehajtása előtt.

A GNS3 is egy hálózati szimulációs szoftver, amely fejlettebb hálózati szimulátor, mint a Packet Tracer, mivel lehetővé teszi valódi hálózati eszközök és szoftverek használatát. Ennek felhasználásával összetettebb hálózati topológiákat tudtunk felépíteni és valós hálózati környezeteket szimulálni. GNS3-at használtunk virtuális hálózatok létrehozására és különböző hálózati protokollok, például OSPF tesztelésére. Ez lehetővé tette számunkra, hogy mélyebben megértsük, hogyan működnek ezek a protokollok, és hogyan valósíthatók meg egy valós hálózatban.

A Packet Tracer és a GNS3 egyaránt felbecsülhetetlen értékű eszköz volt rendszeradminisztrációs projektünkben. Lehetővé tették számunkra, hogy biztonságos és ellenőrzött környezetben tervezzük, szimuláljuk és teszteljük hálózati topológiánkat. Ez segített minimalizálni az állásidőt, és elkerülni a potenciális problémákat, amikor változtatásokat hajtunk végre a tényleges hálózaton. Összességében ezekkel a programokkal kapcsolatos tapasztalataink rendkívül pozitívak, és bátran ajánljuk más rendszergazdáknak.

Emellett az Oracle VM VirtualBoxot és a VMware Workstation Pro-t használtuk a virtuális gépek létrehozására és kezelésére, lehetővé téve több operációs rendszer futtatását egyetlen fizikai gépen. Ez lehetővé tette a hálózati konfigurációk tesztelését különböző környezetekben anélkül, hogy további hardverre lett volna szükség.

Különféle célokra hoztunk létre virtuális gépeket, például szerverkonfigurációk, kliensgépek és hálózati eszközök tesztelésére. A VirtualBox és a VMware lehetővé tette a virtuális gépek egyszerű klónozását, pillanatfelvételét és visszaállítását tesztelés és kísérletezés céljából. Ezenkívül a VirtualBox és a VMware olyan funkciókat is biztosított, mint a hálózati áthidalás és a NAT-konfigurációk, amelyek lehetővé teszik a virtuális gépek és a fizikai hálózat közötti kommunikációt. Összességében ezek az eszközök kulcsfontosságúak voltak abban, hogy rugalmas és méretezhető tesztelési környezetet hozzunk létre rendszeradminisztrációs projektünk számára.

A Microsoft Visio nélkülözhetetlen eszköze volt a hálózati topológiánk diagramjainak és vizuális megjelenítésének létrehozásához, megkönnyítve a tervünk megértését. Ebben a programban különféle típusú diagramokat hoztunk létre, például hálózati topológiát, folyamatábrákat és folyamatdiagramokat, amelyek bemutatják projektünk különböző aspektusait. A diagramok segítettek bennünket hálózatunk elrendezésének vizualizálásában és a jövőbeli bővítések megtervezésében. Olyan részleteket tudtunk megadni, mint a használt eszközök típusa, elhelyezkedése és csatlakozási lehetősége. Ez lehetővé tette számunkra, hogy korán felismerjük a lehetséges problémákat, és megoldásokat találjunk, mielőtt azok problémává válnának.

A Trellót projektmenedzsmentre használtuk, így nyomon követhettük az előrehaladást, kiosztottuk a feladatokat, és hatékonyan együttműködhettünk egymással. A projekt különböző aspektusaihoz, például tervezéshez, megvalósításhoz és teszteléshez táblákat készítettünk. Minden táblán belül kártyákat készítettünk az egyes feladatokhoz, amelyeket teljesíteni kellett. Konkrét csapattagokhoz tudtunk feladatokat kijelölni, és határidőket szabtunk a teljesítésre. Ez segített abban, hogy lépést tartsunk a projektünk ütemtervével, és biztosította, hogy mindenki tisztában legyen a felelősségével. Ezenkívül megjegyzéseket is hagyhattunk, és fájlokat csatolhattunk a kártyákhoz, így könnyebbé vált az együttműködés és az információk megosztása.

A verziókezeléshez és az együttműködéshez a GitHubot használtuk, egy webalapú platformot, amely lehetővé tette a kódunk kezelését, a változások nyomon követését és a projektünkben való egyszerű együttműködést. A GitHubban létrehoztunk egy repository-t projektünk számára, és fiókokat hoztunk létre a különböző szolgáltatásokhoz és fejlesztési szakaszokhoz, ami segített nekünk a kódütközések kezelésében és az egyértelmű fejlesztési munkafolyamat fenntartásában. Ez lehetővé tette számunkra, hogy a változtatásokat alaposan átnézzük és teszteljük, mielőtt beépítjük őket a projektbe.

Végül a Discord nevű kommunikációs platformot használtuk rendszeres találkozókra, megbeszélésekre és ötletcserére, megkönnyítve a kapcsolattartást és a távoli együttműködést. A Discordban különböző csatornákat hoztunk létre különböző témákhoz és célokhoz, például projektfrissítésekhez, technikai megbeszélésekhez és közösségi interakciókhoz. Összességében a Discord használata segített abban, hogy kapcsolatban maradjunk egymással, annak ellenére, hogy távolról és különböző időben dolgoztunk.