**Informatikai rendszer- és alkalmazás-üzemeltető vizsga bemutatási dokumentuma**

Csapatunkkal azt a feladatot kaptuk hogy egy iskolának a hálózatát kell kiépíteni a megadott szempontok alapján amiket ismertetni fogunk,

Hálózati Infrastruktúra Követelmények

A hálózati infrastruktúrának a következő követelményeknek kell megfelelnie:

* Legalább három telephely vagy iroda lefedése
* Legalább egy telephelyen több VLAN kialakítása
* Második és harmadik rétegbeli redundáns megoldások alkalmazása
* IPv4 és IPv6 címzés egyaránt használata
* Vezeték nélküli hálózat biztosítása
* Statisztikus és dinamikus forgalomirányítás megvalósítása
* Statisztikus és dinamikus címfordítás alkalmazása
* WAN-összeköttetések kiépítése
* Virtuális magánhálózati kapcsolat (VPN) megvalósítása
* Programozott hálózatkonfiguráció alkalmazása
* Forgalomirányítón megvalósított biztonsági funkciók, például ACL-ek
* Hardveres tűzfaleszköz alkalmazása
* Minimum egy Linux és egy Windows kiszolgáló, amelyek az alábbi szolgáltatásokat nyújtják:
  + Címtárszolgáltatás (pl. Active Directory)
  + DHCP
  + DNS
  + HTTP/HTTPS
  + Fájl- és nyomtatómegosztás
  + Automatizált mentés
  + Automatizált szoftvertelepítés kliens számítógépekre

Itt látható az elkészült hálózat topológiai ábrázolása.

A képen diagram, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A hálózat kialakításához négy routert használtunk. Az elsődleges routerek közötti kommunikációhoz a RIP (Routing Information Protocol) verzió 2-t alkalmaztuk, mivel a routerek között több alhálózat található. A RIP v2 támogatja a hálózati maszkok küldését, így hatékonyabb, mint az első verzió.

Ezen kívül statikus útválasztást is beállítottunk bizonyos szegmenseknél, hogy optimalizáljuk az adatforgalmat és elkerüljük a dinamikus protokollok esetleges késleltetéseit. Ez biztosítja, hogy a kritikus fontosságú hálózati forgalom előre meghatározott útvonalakon haladjon, növelve a rendszer stabilitását és megbízhatóságát.

**Rendszergazdai szegmens:**

A rendszergazdai szegmensen valósítottuk meg az internetelérést. A hálózat számára biztosítottuk az internetkapcsolatot, amely lehetővé teszi a belső hálózati eszközök számára az internet elérését és az internetes adatforgalom továbbítását.

A hálózatra egy tűzfalat is beállítottunk, amely védi a hálózatot a külső támadásoktól és szabályozza a belső forgalmat. A tűzfal:

* Szűri a bejövő és kimenő forgalmat az előre meghatározott szabályok alapján.
* Megakadályozza az illetéktelen hozzáférést az érzékeny hálózati erőforrásokhoz.
* Segít a hálózati forgalom optimalizálásában és a jogosulatlan kapcsolatok blokkolásában.

Ezek az intézkedések növelik a hálózat megbízhatóságát és biztonságát, biztosítva, hogy a rendszer folyamatosan működőképes maradjon, és védve legyen a potenciális fenyegetésektől.

A rendszergazda gépének **Linux operációs rendszerrel** való konfigurálása számos előnyt biztosít, amelyek kifejezetten fontosak a rendszer stabilitásának, biztonságának és hatékony kezelésének szempontjából. Az alábbiakban összefoglaljuk, miért választottuk a Linuxot a rendszergazda munkájához.

1. **Költséghatékonyság**

A Linux ingyenes és nyílt forráskódú operációs rendszer, így nem kell licencdíjat fizetni a használatáért. Ez lehetővé tette számunkra, hogy költséghatékonyan működtessük a rendszert anélkül, hogy a szoftverekre külön költségeket kellene fordítani.

1. **Stabilitás és megbízhatóság**

A Linux hosszú távú, folyamatos üzemeltetésre lett tervezve. A rendszergazda gépeinek stabilitása és megbízhatósága kiemelkedő fontosságú a napi adminisztráció során, és a Linux kiválóan teljesít ezen a téren. A rendszer ritkán igényel újraindítást, és kevesebb rendszerhiba lép fel, így minimálisra csökkenti az állásidőt.

1. **Biztonság**

A Linux erős beépített biztonsági funkciókkal rendelkezik, mint a felhasználói jogosultságok szigorú kezelése és a fejlett tűzfal konfigurációs lehetőségek. Mivel a rendszergazda gépe kritikus szerepet játszik a hálózati infrastruktúra menedzselésében, elengedhetetlen volt, hogy olyan operációs rendszert válasszunk, amely maximális biztonságot kínál.

1. **Parancssoros Felület és Automatizálás**

A Linux parancssoros eszközei lehetővé tették számunkra, hogy automatizáljuk a rendszergazdai feladatokat, mint a frissítések, monitorozás és karbantartás. A szkriptek és ütemezett feladatok alkalmazása jelentősen csökkentette a manuális beavatkozás szükségességét.

A rendszergazdai szerveren **statikus címfordítást** alkalmaztunk, amely lehetővé teszi, hogy bizonyos belső IP-címekhez mindig ugyanaz a külső IP-cím legyen hozzárendelve. Ez különösen hasznos a hálózati szolgáltatások esetében, mivel biztosítja, hogy a kívülről érkező kapcsolatok mindig ugyanarra a belső eszközre irányuljanak.

Az internet-hozzáférésnél **dinamikus címfordítást** alkalmaztunk, amely lehetővé teszi, hogy a belső hálózat több eszköze egyetlen külső IP-cím mögött kommunikáljon az internettel. Ezzel optimalizáltuk a címhasználatot, miközben fenntartottuk a hálózat biztonságát és hatékonyságát.

A képen szöveg, nyugta, Betűtípus, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A rendszergazdai szervert úgy állítottuk be, hogy a rendszergazda manuálisan el tudja menteni a hálózati eszközök (routerek, switchek) konfigurációit.

Ez biztosítja, hogy egy esetleges meghibásodás vagy beállítási hiba esetén gyorsan visszaállíthatók legyenek a korábbi működőképes konfigurációk, minimalizálva a hálózat leállásának idejét.

A rendszergazda egyetlen paranccsal TFTP-n keresztül el tudja menteni az aktuális konfigurációt a szerverre, így szükség esetén az bármikor visszaállítható.

A képen szöveg, képernyőkép, Betűtípus, fehér látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A rendszergazda SSH (Secure Shell) hozzáférést alkalmazott a rendszer távoli adminisztrációjához, mivel az SSH biztosítja a titkosított, biztonságos kommunikációt a hálózaton keresztüli elérések során. Az SSH lehetővé tette a távoli csatlakozást a rendszerekhez, miközben megakadályozza az adatlopást és a lehallgatást, ami a nem titkosított protokollok, például a Telnet esetében kockázatot jelenthetne.

A használatával biztosítottuk, hogy a rendszergazda biztonságosan végezhesse el a rendszerkarbantartásokat, konfigurálásokat és hibaelhárítást anélkül, hogy érzékeny információk szivárognának ki. Az SSH használata tehát alapvető intézkedés a hálózati biztonság fenntartása érdekében, mivel garantálja az adatvédelem magas szintjét a távoli elérések során.

A megfelelő router IP címének megadása után ezzel a jelszóval tud csatlakozni majd SSH-val.



**Irodai szegmens:**

A DHCP-t az iroda szegmensen állítottuk. Az iroda szegmensben azért állítottunk be DHCP-t, hogy egyszerűsítsük és automatizáljuk az IP-címek kiosztását a hálózatban.

Mivel az irodai környezetben több munkaállomás, laptop és egyéb hálózati eszköz csatlakozik, a DHCP használata lehetővé teszi, hogy ezek az eszközök automatikusan és konfliktusmentesen kapjanak IP-címet, valamint a megfelelő hálózati beállításokat (pl. alhálózati maszk, átjáró, DNS-kiszolgáló).

Ez nemcsak csökkenti az adminisztrációs terhelést, hanem rugalmasságot is biztosít, mivel az új eszközök gyorsan és egyszerűen csatlakoztathatnak a hálózathoz manuális konfiguráció nélkül.

A képen szöveg, Betűtípus, képernyőkép, fehér látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, nyugta látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Itt látható, hogy milyen beállításokat végeztünk a DHCP-n és hogy milyen IP címeket fog kiosztani.

A hálózati biztonság növelése érdekében az irodai szegmensen a **CHAP**-ot alkalmaztuk a felhasználói hitelesítés biztosítására. A CHAP egy titkosított hitelesítési mechanizmus, amelyet a PPP kapcsolatokat használó eszközök között alkalmaznak a biztonságos kapcsolat létrehozása érdekében.

**Termek szegmens**

VLAN-ok és VTP beállítása a termek routerénél lévő switcheken

A termek routeréhez csatlakozó switcheken VLAN-okat állítottunk be a hálózat logikai szegmentálása érdekében. Az alábbi VLAN-ok kerültek létrehozásra:

* **VLAN 10**
* **VLAN 20**
* **VLAN 30**

Ezek a VLAN-ok biztosítják, hogy az egyes hálózati szegmensek elkülönüljenek egymástól, javítva a hálózat biztonságát és hatékonyságát.

Emellett a switcheken **VTP**  került beállításra, amely lehetővé teszi a VLAN-információk központi kezelését és szinkronizálását a hálózat többi kapcsolójával. Ez megkönnyíti a VLAN-ok konfigurálását és biztosítja, hogy a hálózat bővítése vagy módosítása esetén a VLAN-beállítások automatikusan frissüljenek az érintett eszközökön. Van egy fő kapcsolónk, ami a szerver módot kapta és a többi kapcsoló a kliens módba van. Itt látható lesz egy kliens módba lévő kapcsolónak a VTP beállításai.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az FTP szolgáltatás letiltása az Access Control List (ACL) segítségével történt a termékhálózaton, hogy megakadályozzuk a diákok számára az FTP-n keresztüli fájlletöltést és -feltöltést az internetre. Az FTP protokoll titkosítatlan adatátvitelt használ, ami biztonsági kockázatokat jelenthet. Az ACL konfigurálásával blokkoltuk az FTP forgalmat a 21-es porton, így biztosítva, hogy a diákok ne tudjanak fájlokat áthelyezni a hálózaton kívüli rendszerekre. Az intézkedés célja a hálózat védelme és az adatbiztonság növelése volt.



A **Windows Active Directory (AD)** használata a termekben található Windows alapú gépeken lehetővé teszi a központi felhasználó- és eszközkezelést, így biztosítva a hálózat biztonságos és hatékony működését.

**Miért alkalmaztunk Active Directory-t?**

1. **Központi Felügyelet:** Az AD lehetővé teszi a felhasználók, számítógépek és hálózati erőforrások központi kezelését, egyszerűsítve a rendszergazdák munkáját.
2. **Biztonság és Hozzáférés-vezérlés:** Az AD segítségével pontosan szabályozhatjuk, hogy ki férhet hozzá a hálózati erőforrásokhoz, biztosítva ezzel a biztonságot.
3. **Csoportházirendek:** A Windows gépeken a csoportházirendek (Group Policies) segítségével központilag alkalmazhatók a biztonsági beállítások, mint például a jelszóházirendek és tűzfal konfigurációk.
4. **Karbantartás és Frissítések:** Az AD segít központilag frissíteni a Windows gépeket, biztosítva azok naprakész állapotát.

**Könyvtár szegmens:**

A hálózat biztonságának és hatékonyságának növelése érdekében a könyvtár szegmensében található szerver **IPv6 címzést** használ a kommunikációhoz. Az IPv6 (Internet Protocol version 6) az internet új generációs protokollja, amely a címek kimerülésétől való félelmet elkerülve hosszabb és dinamikusan hozzárendelhető IP címeket biztosít. Az IPv6 előnyei különösen fontosak, amikor egyre több eszköz csatlakozik a hálózatra, és biztosítani kell a jövőbeli skálázhatóságot.

**Miért használtunk IPv6-ot a Könyvtár Szegmensen?**

1. **Címkimerülés elkerülése:** Az IPv4 címek kimerülésével a szervezetek kénytelenek voltak új címzési megoldásokat keresni. Az IPv6 globálisan egyedülálló címeket biztosít, így hosszú távú megoldást kínál, mivel gyakorlatilag végtelen számú cím rendelkezésre áll.
2. **Jövőbeli kompatibilitás:** Mivel az IPv6 már egyre inkább elterjedt a világ különböző hálózataiban, a könyvtári szerverek IPv6-os címzése biztosítja, hogy a jövőbeli eszközökkel és szolgáltatásokkal is kompatibilis legyen a rendszer.
3. **Jobb teljesítmény és biztonság:** Az IPv6 előnyei közé tartozik a jobb adatcsomag-kezelés és az integrált biztonsági mechanizmusok, mint az IPsec (Internet Protocol Security), amely biztosítja az adatok védelmét a hálózaton belül.
4. **Továbbfejlesztett hálózati konfiguráció:** Az IPv6 képes automatikusan konfigurálni a címeket, ami lehetővé teszi az egyszerűbb eszközkiválasztást és a dinamikus címzést a könyvtár szegmensen belül, így könnyebbé válik az új eszközök integrálása a hálózatba.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A könyvtár szegmensen egy új **Wi-Fi hálózatot** helyeztünk el, amely biztosítja a vezeték nélküli hozzáférést a helyi eszközök számára. Az új Wi-Fi hálózat segítségével a könyvtár dolgozói és látogatói kényelmesen csatlakozhatnak a hálózatra, miközben biztosítva van a megfelelő biztonság és adatvédelem.

**Wi-Fi Hálózat Konfigurációja**

A Wi-Fi hálózatot a következő beállításokkal konfiguráltuk:

1. **Hálózat neve (SSID):** A Wi-Fi hálózat neve (SSID) **"wifi"**. Ez egy egyszerű, könnyen felismerhető név, amelyet a könyvtár látogatói és dolgozói használhatnak a hálózatra történő csatlakozáshoz.
2. **Biztonsági protokoll:** A Wi-Fi hálózathoz **WPA2 Personal** biztonsági protokollt alkalmaztunk, amely a legjobb választás a helyi, kisebb hálózatok számára. A WPA2 Personal biztosítja a titkosítást és védi a hálózati forgalmat, így az adatkommunikáció biztonságos és védett marad.
3. **Hozzáférési jelszó:** A Wi-Fi hálózatra való csatlakozáshoz szükséges jelszó: **alma1234**. Ez a jelszó biztosítja, hogy csak azok az eszközök férhessenek hozzá a hálózathoz, akik ismerik a megfelelő hitelesítési adatokat.

**Miért WPA2 Personal?**

A **WPA2 Personal** egy olyan biztonsági protokoll, amely titkosítja a Wi-Fi hálózaton keresztül küldött adatokat, így megakadályozza, hogy illetéktelenek hozzáférjenek a hálózati forgalomhoz. A WPA2 Personal ideális választás, mivel könnyen beállítható, és erős titkosítást biztosít a hálózat számára, miközben nem igényel különálló hitelesítési szervert, mint a WPA2 Enterprise.