**Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola**

**Vizsgaremek**

Készítették:

Szikla Benjamin

Kaszás Simon

Möller Milán

**Mohács**

**2025**

**Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola**

Szakma megnevezése: Informatikai rendszer- és alkalmazás-üzemeltető technikus

**Vizsgaremek**

**Link Wave**

Készítették:

Szikla Benjamin

Kaszás Simon

Möller Milán

**Mohács**

**2025**

**Tartalomjegyzék**

Feladat rövid ismertetése

Bevezetés 4

Cél 4

Jövőbeli tervek 5

Használt technológiák 5

Topológia 5

Hálózati eszközök kiválasztása 6

Fejlesztési módszertan 7

Jira 7

Git 8

Packet Tracer 8

Elvégzett tesztek 8

Tesztelési fajták 8

Jelentőség 10

Használt technológiák 10

Hálózat működésének részletes leírása 11

Hálózat részletes leírása 11

Csapatmunka 18

Szerepek 18

Jövőbeli terveink 20

***Feladat rövid ismertetése***

**Bevezetés**

A projekt fő szempontja, hogy a nagyobb hálózatok összetételénél olyan megoldást kínáljon hogy, az költségigényes legyen, hibamentes, és legyen lehetőség akár a bővítésre, fejlődésre. A hálózat amit megterveztünk, képes nagy távon keresztül biztonságosan adatot küldeni és fogadni.

**Cél**

A projekt célja egy olyan modern, skálázható és biztonságos hálózat kiépítése volt, amely teljes mértékben kiszolgálja a vállalat jelenlegi és jövőbeli kommunikációs és adatátviteli igényeit. Az üzleti igények között szerepelt a gyors és megbízható adatátvitel a különböző részlegek között, a biztonságos hozzáférés az üzleti alkalmazásokhoz és adatokhoz, valamint a hálózat rugalmassága, amely lehetővé teszi az egyszerű bővítést és a változó igényekhez való alkalmazkodást. A hálózatnak emellett támogatnia kellett a távoli munkavégzést és a mobil eszközök használatát is. A projekt célja továbbá az volt, hogy a hálózat megfeleljen a legújabb biztonsági szabványoknak és előírásoknak, valamint a lehető legköltséghatékonyabb megoldásokat alkalmazza.

**Jövőbeli tervek**

A jövőbeni tervek között szerepel a projekt továbbfejlesztése olyan kiegészítő funkciókkal, amelyek még teljesebb támogatást nyújtanak a nagyobb vállalatoknak a hálózataik tervezésében és megvalósításában. Azon túlmenően, hogy a jelenlegi tervezett funkciók és modulok implementálására összpontosítunk, számos potenciális irányban is gondolkodunk a bővítés terén.

***Használt technológiák***

**Topológia**

A hálózat **hibrid topológiát** használ, amely több különböző hálózati topológia kombinációja.

1. **Részben hálózatos topológia (Partial Mesh)**
   * A gerinchálózat egyes eszközök között több elérési útvonallal rendelkezik, ami redundanciát biztosít.
   * Az OSPF dinamikus útvonalválasztással működik, amely támogatja a redundanciát és optimalizálja az útvonalakat.
2. **Csillag topológia** 
   * A különböző színes területekben (pl. sárga, lila, zöld, stb.) található hálózatok csillag topológiát használnak, ahol egy központi switch vagy router kapcsolja össze az eszközöket.
3. **Fa topológia (Tree)**
   * A különböző alhálózatok és VLAN-ok hierarchikus szerkezetben épülnek fel, egy-egy központi eszköz irányítja a forgalmat az alsóbb szintekre.

**Használt eszközök kiválasztása**

A hálózat kiépítéséhez és üzemeltetéséhez a következő Cisco eszközöket és szoftvereket használtuk:

Routerek: Cisco ISR (Integrated Services Router) sorozat, amely nagy teljesítményt és biztonságot nyújt a hálózati forgalom irányításához. Az ISR routerek moduláris felépítésűek, így könnyen bővíthetők az igényeknek megfelelően. A routerek támogatják a fejlett routing protokollokat, a biztonsági funkciókat és a QoS (Quality of Service) beállításokat.

Switchek: Cisco Catalyst sorozat, amely intelligens Layer 2 és Layer 3 switching képességeket biztosít a hálózati kapcsolatokhoz. A Catalyst switchek nagy port számmal rendelkeznek, és támogatják a VLAN-okat, a QoS-t és a biztonsági funkciókat. A switchek menedzselhetők Cisco Prime Infrastructure vagy más hálózati menedzsment eszközökkel.

Tűzfalak: Cisco ASA (Adaptive Security Appliance) sorozat, amely átfogó biztonsági védelmet nyújt a hálózatnak a külső támadásokkal szemben. Az ASA tűzfalak hardveres és szoftveres védelemmel rendelkeznek, és támogatják a tűzfal funkciókat, a behatolás érzékelés és -megelőzést (IDS/IPS), a VPN-t és az alkalmazásszintű szűrést.

VPN eszközök: Cisco VPN kliensek és szerverek, amelyek biztonságos távoli hozzáférést biztosítanak a hálózathoz. A Cisco VPN kliensek és szerverek támogatják a különböző VPN protokollokat, mint például az IPsec, az SSL és az L2TP. A VPN kapcsolatok titkosítást és hitelesítést biztosítanak, így védve az adatokat a jogosulatlan hozzáféréstől.

Hálózati operációs rendszer: Cisco IOS (Internetwork Operating System), amely a Cisco eszközökön futó, fejlett hálózati funkciókat biztosító operációs rendszer. A Cisco IOS egy parancssoros interfészt (CLI) és egy grafikus felhasználói felületet (GUI) is kínál a hálózat konfigurálásához és menedzseléséhez.

Hálózati menedzsment szoftver: Cisco Prime Infrastructure, amely átfogó hálózatfelügyeleti és -kezelési képességeket biztosít. A Cisco Prime Infrastructure segítségével monitorozhatjuk a hálózat állapotát, konfigurálhatjuk az eszközöket, hibaelhárítást végezhetünk és jelentéseket készíthetünk.

***Fejlesztési módszertan***

**Jira**

A Jira egy olyan project management eszköz, amely lehetővé teszi a csapatoknak a projektjeik nyomon követését, feladatok kezelését és a fejlesztési folyamatok hatékony szervezését. Az eszköz segíti a feladatok rendszerezését, a prioritások meghatározását és a csapat tagjainak közötti kommunikációt.

**Git**

A Git egy elosztott verziókezelő rendszer, amely segíti a fejlesztőket a hálózat nyomon követésében, változtatások kezelésében és együttműködésben a csapaton belül. Az elosztott jellege lehetővé teszi a párhuzamos fejlesztést, valamint a könnyű visszatérési pontok (commit) készítését és visszaállítását.

**Cisco Packet Tracer**

A Cisco Packet Tracer Lehetővé teszi a felhasználók számára, hogy virtuális környezetben tervezzenek, konfiguráljanak és teszteljenek hálózatokat anélkül, hogy fizikai eszközökre lenne szükségük. A program támogatja a különböző Cisco eszközöket, például routereket, switch-eket és végpontokat, valamint lehetőséget biztosít parancssoros (CLI) és grafikus konfigurációra is.

***Elvégzett tesztek***

**Tesztelési fajták**

A hálózatokon belüli tesztelési fajták különböző célokat szolgálnak, például a teljesítmény, biztonság vagy megbízhatóság ellenőrzését. Mi ezeket a tesztelési fajtákat használtuk:

1. **Funkcionális tesztelés**
   * A funkcionális tesztelés célja annak ellenőrzése, hogy a hálózat alapvető funkciói megfelelően működnek-e. Ide tartozik a kapcsolat tesztelése (ping), a hálózati eszközök elérhetőségének vizsgálata, valamint a DNS-feloldás ellenőrzése. Biztosítja, hogy az adatátvitel, a forgalomirányítás és az autentikáció rendben működjön. Ez a tesztelés segít azonosítani a konfigurációs hibákat és a hálózati eszközök meghibásodását.
2. **Hibakeresési tesztelés**
   * A hibakeresési tesztek célja a hálózati problémák gyors azonosítása és megoldása. Ide tartozik a ping a kapcsolat ellenőrzésére, a traceroute az útvonal elemzésére, és a netstat a hálózati kapcsolatok vizsgálatára. A packet capture (pl. Wireshark) a forgalom részletes elemzésére szolgál. Ezek a tesztek segítenek meghatározni a csomagvesztést, késleltetést és egyéb hálózati hibákat.

**Jelentőség**

1. **Funkcionális tesztelés**
   * A funkcionális tesztelés célja annak ellenőrzése, hogy a hálózat alapvető funkciói megfelelően működnek-e. Ide tartozik a kapcsolat tesztelése (ping), a hálózati eszközök elérhetőségének vizsgálata, valamint a DNS-feloldás ellenőrzése. Biztosítja, hogy az adatátvitel, a forgalomirányítás és az autentikáció rendben működjön. Ez a tesztelés segít azonosítani a konfigurációs hibákat és a hálózati eszközök meghibásodását.
2. **Hibakeresési tesztelés**
   * A hibakeresési tesztek célja a hálózati problémák gyors azonosítása és megoldása. Ide tartozik a ping a kapcsolat ellenőrzésére, a traceroute az útvonal elemzésére, és a netstat a hálózati kapcsolatok vizsgálatára. A packet capture (pl. Wireshark) a forgalom részletes elemzésére szolgál. Ezek a tesztek segítenek meghatározni a csomagvesztést, késleltetést és egyéb hálózati hibákat.

**Használt technológiák**

* Manuális Tesztelés - Packet Tracer
* Hibakeresési Tesztelés - Packet Tracer

***Hálózat működésének részletes leírása***

**Hálózat részletes leírása**

**A hálózatban először az eszközöket választottuk ki amiket az alábbi szempontok alapján gondoltuk át:**

A teljesítményt, a biztonságot, a skálázhatóságot és a költséghatékonyság. A Cisco eszközök megfeleltek ezeknek a követelményeknek, és széles körben elterjedtek a vállalati hálózatokban. Az eszközök kiválasztásakor figyelembe vettük a vállalat specifikus igényeit, például a szükséges portok számát, a támogatott protokollokat és a biztonsági funkciókat.

**Ezután kezdtünk bele a hálózat IP címzésébe:**

A hálózatban privát IP-címeket használtunk az RFC 1918 szabvány szerint. Az IP-címek kiosztása során figyelembe vettük a hálózat logikai felépítését és a különböző részlegek igényeit. Minden részleg külön alhálózatot kapott, amelyhez egyedi IP-címtartományt rendeltünk. Az IP-címek kiosztása dinamikusan történik DHCP szerver segítségével, amely automatikusan osztja ki az IP-címeket az eszközöknek.

A statikus IP-címeket olyan eszközök számára tartottuk fenn, amelyeknek állandó IP-címmel kell rendelkezniük, például a szerverek.

**Majd a szegmentálás következett:**

A hálózat szegmentálása javította a biztonságot és a teljesítményt. A VLAN-ok és az alhálózatok használata is a szegmentálás részét képezte. A szegmentálás lehetővé tette a különböző részlegek forgalmának elkülönítését, megakadályozva ezzel a jogosulatlan hozzáférést és a hálózati problémák terjedését.

**Elértünk a kommunikáció beállításához:**

Dinamikus routing protokollok (OSPF): A hálózatban OSPF (Open Shortest Path First) protokollt használtunk a dinamikus útvonalválasztáshoz. Az OSPF egy link state protokoll, amely automatikusan alkalmazkodik a hálózati változásokhoz és biztosítja a forgalom optimális irányítását. Az OSPF hatékonyan kezeli a változásokat a hálózatban, és gyorsan új útvonalakat talál. Az OSPF támogatja a területeket (areas), amelyek lehetővé teszik a nagyobb hálózatok hierarchikus felépítését. A hálózatban egyetlen OSPF területet használtunk a konfiguráció egyszerűsítése érdekében. Az OSPF konfigurálása magában foglalja a router ID beállítását, az interfészek hozzáadását az OSPF protokollhoz és a szomszédos routerekkel való kapcsolat kialakítását. Az OSPF protokoll használata lehetővé tette a hálózat rugalmas és dinamikus működését, amely alkalmazkodik a változó forgalmi viszonyokhoz és a hálózati hibákhoz.

**A hálózat biztonsága**

ACL-ek és forgalomszűrés konfigurálása: Az ACL-ek (Access Control Lists) segítségével szabályoztuk a hálózati forgalmat, engedélyezve vagy tiltva bizonyos típusú forgalmat bizonyos forrásokból vagy célokba. Az ACL-eket a routereken és switcheken konfiguráltuk, hogy megvédjük a hálózatot a jogosulatlan hozzáféréstől és a rosszindulatú forgalomtól. Az ACL-ek konfigurálása magában foglalja az ACL szabályok létrehozását, az interfészekhez való hozzárendelését és a forgalom irányának megadását.

A VPN (Virtual Private Network) technológia segítségével biztonságos csatornát hoztunk létre a távoli felhasználók és a vállalati hálózat között, valamint a különböző telephelyek közötti összeköttetéshez

Site-to-site VPN: Összekapcsol két vagy több telephelyet egymással, lehetővé téve a biztonságos kommunikációt közöttük. A site-to-site VPN-t Cisco ASA tűzfalakkal valósítottuk meg, amelyek VPN gateway ként működnek a telephelyek között. A site-to-site VPN konfigurációja magában foglalja a VPN alagút beállításait, a hitelesítést és a titkosítási protokollok kiválasztását

**Hálózat felügyelet és karbantartás**

Ping, Traceroute és egyéb diagnosztikai eszközök:

A hálózatfelügyelet és a hibakeresés során számos diagnosztikai eszközt használunk, amelyek segítenek azonosítani és elhárítani a hálózati problémákat. A leggyakrabban használt eszközök a következők:

Ping: A ping parancs segítségével ellenőrizhetjük, hogy egy eszköz elérhető-e a hálózaton. A ping küld egy ICMP (Internet Control Message Protocol) csomagot a cél eszköznek, és ha az eszköz válaszol, akkor az elérhető. A ping parancs hasznos a kapcsolati problémák azonosításához és a hálózati késleltetés méréséhez. A ping parancs használata egyszerű és gyors, és lehetővé teszi a hálózat alapvető működésének ellenőrzését.

Traceroute: A traceroute parancs segítségével nyomon követhetjük a hálózati forgalom útját egy adott célpontig. A traceroute küld egy sor UDP (User Datagram Protocol) csomagot a cél eszköznek, és rögzíti azokat az útvonalakat, amelyeken a csomagok áthaladnak. A traceroute parancs hasznos a routing problémák azonosításához és a hálózati topológia feltérképezéséhez. A traceroute parancs segítségével megtudhatjuk, hogy a forgalom milyen útvonalon halad a hálózaton keresztül, és azonosíthatjuk a problémás pontokat.

Egyéb diagnosztikai eszközök:

ipconfig (Windows) vagy ifconfig (Linux): Megjeleníti az eszköz IP-címét, alhálózati maszkját.

**Tesztelés**

Részletes tesztelési terv és végrehajtás (Folytatás):

A tesztelési tervnek részletesen ki kell térnie a következőkre:

Tesztelési célok: Mi a tesztelés célja? Milyen funkciókat és szolgáltatásokat kell tesztelni? Például a hálózat alapvető működése, az alkalmazások elérhetősége, a biztonsági funkciók működése, a terhelhetőség és a teljesítmény.

Tesztelési módszerek: Milyen tesztelési módszereket kell alkalmazni? Például funkcionális tesztelés, teljesítmény tesztelés, biztonsági tesztelés, terhelési tesztelés. A funkcionális tesztelés során ellenőrizzük, hogy a hálózat megfelelően működik-e és az eszközök kommunikálnak-e egymással. A teljesítmény tesztelés során mérjük a hálózat sebességét és terhelhetőségét. A biztonsági tesztelés során ellenőrizzük a hálózat védelmét a külső és belső támadásokkal szemben. A terhelési tesztelés során szimuláljuk a hálózat nagy terhelését, hogy ellenőrizzük a stabilitást és a terhelhetőséget.

Tesztelési környezet: Milyen hardver és szoftver eszközöket kell használni a teszteléshez? Például teszt szerverek, teszt kliensek, hálózati analizátorok és monitorozó eszközök. A tesztelési környezetnek hasonlónak kell lennie a éles üzemben lévő hálózathoz, hogy a tesztelési eredmények relevánsak legyenek.

Tesztelési ütemterv: Mikor és milyen sorrendben kell elvégezni a teszteket? A tesztelési ütemtervnek tartalmaznia kell a tesztelési fázisokat, a tesztelési időpontokat és a tesztelési felelősöket.

Tesztelési forgatókönyvek: Milyen konkrét teszteket kell elvégezni? Például kapcsolati teszt, adatátviteli teszt, alkalmazás teszt, biztonsági teszt. A tesztelési forgatókönyveknek részletesen le kell írniuk a tesztelési lépéseket, az elvárt eredményeket és a tesztelési környezetet.

Elvárt eredmények: Milyen eredményeket várunk a tesztektől? Például sikeres kapcsolódás, megfelelő adatátviteli sebesség, biztonságos hozzáférés. Az elvárt eredményeknek mérhetőnek és ellenőrizhetőnek kell lenniük.

Tesztelési dokumentáció: Hogyan kell dokumentálni a tesztelési eredményeket? Például tesztjegyzőkönyv, hiba jelentés. A tesztelési dokumentációnak tartalmaznia kell a tesztelési eredményeket, a hibajelentéseket és a tesztelési összefoglalót.

A tesztelés végrehajtása során fontos a tesztelési terv pontos betartása és az eredmények dokumentálása. A tesztelési eredmények alapján értékelni kell a hálózatot, és ha szükséges, javítani kell a hibákat. A tesztelés befejezése után a hálózat üzembe helyezhető.

**Protokollok**

### **1. Hálózati réteg protokolljai (Network Layer – OSI 3. réteg)**

Ezek a protokollok az adatok útvonalválasztásáért és csomagkapcsolásáért felelősek.

* **IP (Internet Protocol)** - Az internet alapja, két verziója van:
  + **IPv4** – 32 bites címzés
  + **IPv6** – 128 bites címzés

**2. Adatkapcsolati réteg protokolljai**

* **STP (Spanning Tree Protocol)** - Hurokellenőrzés kapcsolókon

**3. Alkalmazási réteg protokolljai**

Ezeket a végfelhasználói alkalmazások használják az adatcserére.

* **HTTP/HTTPS (HyperText Transfer Protocol Secure)** - Weboldalak elérése
* **DHCP (Dynamic Host Configuration Protocol)** - IP-címek automatikus kiosztása
* **FTP (File Transfer Protocol)** – Fájlok átvitele
* **DNS (Domain Name System)** – Domainnevek IP-címekké alakítása

**4. Hálózatbiztonsági protokollok**

Ezek a protokollok a biztonságos kommunikációt biztosítják.

* **IPSec (Internet Protocol Security)** – Titkosított VPN-kapcsolatokhoz
* **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** – Weboldalak biztonságos adatátviteléhez (HTTPS)

**5. Irányítóprotokollok**

Ezek a protokollok a hálózatok közötti útvonalválasztást segítik.

* **OSPF (Open Shortest Path First)** – Link-state alapú dinamikus routing protokoll

***Csapatmunka***

**Szerepek**

***Möller Milán vállalt szerepei és felelősségi területei a következők voltak a projekt során:***

***1. Project manager (Projektmenedzser)***

* Feladata a projekt egészének irányítása és felügyelete.
* Koordinálta a csapatmunkát és ütemezte a fejlesztési folyamatokat.
* Hatékony kommunikáció biztosítása a csapattagok között és a projekt érintettjeivel.

***2. Hálózat fejlesztő***

* A hálózat fejlesztése, kialakítása volt az ő feladata
* Problémák, bugok kijavítása

***3. Manuális tesztelő***

* Visszajelzéseket adott a fejlesztő csapatnak a teszteredmények alapján.
* Biztosította, hogy a hálózat megfeleljen a minőségi követelményeknek.

***Kaszás Simon vállalt szerepei és felelősségi területei a következők voltak a projekt során:***

***1. Hálózat fejlesztő***

* A hálózat fejlesztése, kialakítása volt az ő feladata
* Problémák, bugok kijavítása

***2. Projekt prezentációjának a létrehozása***

* A prezentáció létrehozása, ismertetése a csoporttársakkal

***3. Projektmunka dokumentálása***

* Részletes ismertető a projektmunkáról

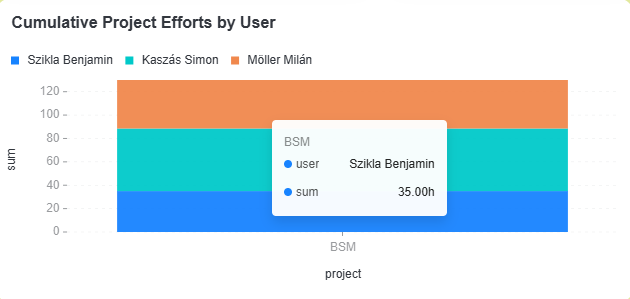
***Szikla Benjamin vállalt szerepei és felelősségi területei a következők voltak a projekt során:***

***1. Hálózat fejlesztő***

* A hálózat fejlesztése, kialakítása volt az ő feladata
* Problémák, bugok kijavítása

***2. Projektmunka dokumentálása***

* Részletes ismertető a projektmunkáról

******

**Jövőbeli terveink**

Az IPv6 címmel rendelkező eszközök listájának bővítése. Ha lehetséges, további eszközökkel való kiegészítés.

A mesterséges intelligencia integrálása a hálózatba, amely automatikusan észleli és megoldja a teljesítményproblémákat.

Az 5G és Wi-Fi 6E technológiák bevezetése a gyorsabb és megbízhatóbb vezeték nélküli kapcsolatok érdekében.

A hálózat logikai szegmentálására VLAN-okat használtunk, amelyekkel elkülönítettük a különböző részlegek forgalmát, javítva ezzel a biztonságot és a teljesítményt. A dinamikus útvonalválasztáshoz OSPF protokollt alkalmaztunk, amely automatikusan alkalmazkodik a hálózati változásokhoz és biztosítja a forgalom optimális irányítását. A hálózat biztonságát tűzfalakkal, ACL-ekkel és VPN kapcsolatokkal erősítettük meg. A hálózatban redundáns kapcsolatokat alakítottunk ki a kiesések elkerülése érdekében. A hálózatot úgy terveztük, hogy az megfeleljen a vállalat növekedési terveinek és a jövőbeli technológiai fejlesztéseknek.

·Használt Cisco eszközök és szoftverek:

A hálózat kiépítéséhez és üzemeltetéséhez a következő Cisco eszközöket és szoftvereket használtuk:

Routerek: Cisco ISR (Integrated Services Router) sorozat, amely nagy teljesítményt és biztonságot nyújt a hálózati forgalom irányításához. Az ISR routerek moduláris felépítésűek, így könnyen bővíthetők az igényeknek megfelelően. A routerek támogatják a fejlett routing protokollokat, a biztonsági funkciókat és a QoS (Quality of Service) beállításokat.

Switchek: Cisco Catalyst sorozat, amely intelligens Layer 2 és Layer 3 switching képességeket biztosít a hálózati kapcsolatokhoz. A Catalyst switchek nagy portszámmal rendelkeznek, és támogatják a VLAN-okat, a QoS-t és a biztonsági funkciókat. A switchek menedzselhetők Cisco Prime Infrastructure vagy más hálózati menedzsment eszközökkel.

Tűzfalak: Cisco ASA (Adaptive Security Appliance) sorozat, amely átfogó biztonsági védelmet nyújt a hálózatnak a külső támadásokkal szemben. Az ASA tűzfalak hardveres és szoftveres védelemmel rendelkeznek, és támogatják a tűzfal funkciókat, a behatolásérzékelést és -megelőzést (IDS/IPS), a VPN-t és az alkalmazásszintű szűrést.

VPN eszközök: Cisco VPN kliensek és szerverek, amelyek biztonságos távoli hozzáférést biztosítanak a hálózathoz. A Cisco VPN kliensek és szerverek támogatják a különböző VPN protokollokat, mint például az IPsec, az SSL és az L2TP. A VPN kapcsolatok titkosítást és hitelesítést biztosítanak, így védve az adatokat a jogosulatlan hozzáféréstől.

Hálózati operációs rendszer: Cisco IOS (Internetwork Operating System), amely a Cisco eszközökön futó, fejlett hálózati funkciókat biztosító operációs rendszer. A Cisco IOS egy parancssoros interfészt (CLI) és egy grafikus felhasználói felületet (GUI) is kínál a hálózat konfigurálásához és menedzseléséhez.

Hálózati menedzsment szoftver: Cisco Prime Infrastructure, amely átfogó hálózatfelügyeleti és -kezelési képességeket biztosít. A Cisco Prime Infrastructure segítségével monitorozhatjuk a hálózat állapotát, konfigurálhatjuk az eszközöket, hibaelhárítást végezhetünk és jelentéseket készíthetünk.

**2. Topológia és hálózati eszközök kiválasztása**

Topológia: A hálózat hierarchikus (csillag) topológiát használ, amely a központi routerekhez csatlakozó switcheken keresztül biztosítja a végfelhasználói eszközök kapcsolatát. Ez a topológia jól skálázható, könnyen kezelhető és lehetővé teszi a forgalom hatékony irányítását. A topológia kialakításakor figyelembe vettük a vállalat méretét, a felhasználók számát és az adatforgalom mennyiségét. A hierarchikus topológia előnyei közé tartozik a redundancia, a hibaelkülönítés és a könnyű bővíthetőség. A topológia kialakításakor figyelembe vettük a hálózat biztonsági követelményeit is.

·Hálózati eszközök: A hálózatban használt eszközök kiválasztásakor a teljesítményt, a biztonságot, a skálázhatóságot és a költséghatékonyságot vettük figyelembe. A Cisco eszközök megfeleltek ezeknek a követelményeknek, és széles körben elterjedtek a vállalati hálózatokban. Az eszközök kiválasztásakor figyelembe vettük a vállalat specifikus igényeit, például a szükséges portok számát, a támogatott protokollokat és a biztonsági funkciókat. Az eszközök kiválasztásakor figyelembe vettük a hálózat jövőbeli bővítésének lehetőségét is. A hálózatban használt eszközök kompatibilisek egymással és a meglévő hálózati infrastruktúrával.

**3. IP-címzés és alhálózatok kialakítása**

IP-címzés: A hálózatban privát IP-címeket használtunk az RFC 1918 szabvány szerint. Az IP-címek kiosztása során figyelembe vettük a hálózat logikai felépítését és a különböző részlegek igényeit. Minden részleg külön alhálózatot kapott, amelyhez egyedi IP-címtartományt rendeltünk. Az IP-címek kiosztása dinamikusan történik DHCP szerver segítségével, amely automatikusan osztja ki az IP-címeket az eszközöknek. A DHCP szerver konfigurálása magában foglalja az IP-címtartományok beállítását, a címkiosztás időtartamának beállítását és az alapértelmezett átjáró és DNS szerverek megadását. A statikus IP-címeket olyan eszközök számára tartottuk fenn, amelyeknek állandó IP-címmel kell rendelkezniük, például a szerverek és a nyomtatók.

·Alhálózatok: A hálózatot alhálózatokra osztottuk a jobb kezelhetőség, a biztonság és a teljesítmény érdekében. Minden alhálózat külön IP-címtartományt használ, és a forgalom az alhálózatok között routereken keresztül irányítódik. Az alhálózatok kialakításakor figyelembe vettük a különböző részlegek igényeit és a hálózat logikai felépítését. Az alhálózatok közötti kommunikációt tűzfalakkal és ACL-ekkel szabályoztuk, hogy biztosítsuk a biztonságos adatátvitelt. Az alhálózatok kialakításakor figyelembe vettük a hálózat jövőbeli bővítésének lehetőségét is. Az alhálózatok címeinek megválasztás

folytathatod

Folytathatjuk a Cisco hálózat dokumentációját és karbantartását a megadott szempontok alapján, részletesebben:

**4. VLAN-ok és szegmentálás**

·Szegmentálás: A hálózat szegmentálása javította a biztonságot és a teljesítményt. A VLAN-ok és az alhálózatok használata is a szegmentálás részét képezte. A szegmentálás lehetővé tette a különböző részlegek forgalmának elkülönítését, megakadályozva ezzel a jogosulatlan hozzáférést és a hálózati problémák terjedését. A szegmentálás emellett javította a hálózat teljesítményét, mivel a forgalom csak a szükséges alhálózatokra korlátozódott. A szegmentálás megvalósításakor figyelembe vettük a vállalat biztonsági szabályzatát és a vonatkozó jogszabályokat. A szegmentálás eredményeként a hálózat jobban védetté vált a külső és belső támadásokkal szemben.

**5. Routing Megoldások**

Dinamikus routing protokollok (OSPF): A hálózatban OSPF (Open Shortest Path First) protokollt használtunk a dinamikus útvonalválasztáshoz. Az OSPF egy link state protokoll, amely automatikusan alkalmazkodik a hálózati változásokhoz és biztosítja a forgalom optimális irányítását. Az OSPF hatékonyan kezeli a változásokat a hálózatban, és gyorsan új útvonalakat talál. Az OSPF támogatja a területeket (areas), amelyek lehetővé teszik a nagyobb hálózatok hierarchikus felépítését. A hálózatban egyetlen OSPF területet használtunk a konfiguráció egyszerűsítése érdekében. Az OSPF konfigurálása magában foglalja a router ID beállítását, az interfészek hozzáadását az OSPF protokollhoz és a szomszédos routerekkel való kapcsolat kialakítását. Az OSPF protokoll használata lehetővé tette a hálózat rugalmas és dinamikus működését, amely alkalmazkodik a változó forgalmi viszonyokhoz és a hálózati hibákhoz.

**6. Hálózatbiztonság és Hozzáférés-vezérlés**

ACL-ek és forgalomszűrés konfigurálása: Az ACL-ek (Access Control Lists) segítségével szabályoztuk a hálózati forgalmat, engedélyezve vagy tiltva bizonyos típusú forgalmat bizonyos forrásokból vagy célokba. Az ACL-eket a routereken és switcheken konfiguráltuk, hogy megvédjük a hálózatot a jogosulatlan hozzáféréstől és a rosszindulatú forgalomtól. Az ACL-ek konfigurálása magában foglalja az ACL szabályok létrehozását, az interfészekhez való hozzárendelését és a forgalom irányának megadását. Az ACL-ek használata lehetővé tette a hálózat részletes szabályozását és a biztonsági szabályzatok érvényesítését. Az ACL-ekkel megvalósított forgalomszűrés hatékony védelmet nyújtott a hálózatnak a DoS (Denial of Service) támadásokkal és más biztonsági fenyegetésekkel szemben.

·VPN beállítás (távoli elérés és site-to-site):

A VPN (Virtual Private Network) technológia segítségével biztonságos csatornát hoztunk létre a távoli felhasználók és a vállalati hálózat között, valamint a különböző telephelyek közötti összeköttetéshez. Kétféle VPN megoldást implementáltunk:

Távoli elérés VPN: Lehetővé teszi a távoli felhasználók számára, hogy biztonságosan csatlakozzanak a vállalati hálózathoz, mintha ott lennének fizikailag. A távoli elérés VPN-t Cisco VPN kliens szoftverrel valósítottuk meg, amelyet a felhasználók telepíthetnek a számítógépükre vagy mobil eszközükre. A VPN kapcsolat titkosítást és hitelesítést biztosít, így védve az adatokat a jogosulatlan hozzáféréstől. A távoli elérés VPN konfigurációja magában foglalja a VPN szerver beállításait, a felhasználói hitelesítést és a titkosítási protokollok kiválasztását. A távoli elérés VPN használata lehetővé tette a vállalat számára, hogy biztonságos hozzáférést biztosítson a távoli munkavállalók számára a vállalati erőforrásokhoz.

Site-to-site VPN: Összekapcsol két vagy több telephelyet egymással, lehetővé téve a biztonságos kommunikációt közöttük. A site-to-site VPN-t Cisco ASA tűzfalakkal valósítottuk meg, amelyek VPN gatewayként működnek a telephelyek között. A site-to-site VPN konfigurációja magában foglalja a VPN alagút beállításait, a hitelesítést és a titkosítási protokollok kiválasztását. A site-to-site VPN lehetővé tette a telephelyek közötti biztonságos adatátvitelt és az erőforrások megosztását. A site-to-site VPN használata csökkentette a telephelyek közötti kommunikáció költségeit és javította a hatékonyságot.

·Cisco tűzfal:

A Cisco ASA tűzfalak központi szerepet játszanak a hálózat biztonságának megőrzésében. A tűzfalak ellenőrzik a bejövő és kimenő forgalmat, és blokkolják a nem kívánt kapcsolatokat. A tűzfalak konfigurációja magában foglalja a biztonsági szabályok beállítását, a forgalom szűrését és a behatolásérzékelést. A tűzfalak emellett védelmet nyújtanak a DoS (Denial of Service) támadásokkal szemben is. A Cisco ASA tűzfalak fejlett biztonsági funkciókat kínálnak, mint például az alkalmazásszintű szűrés, a vírusvédelem és a behatolásmegelőzés (IPS). A tűzfalak naplózási funkciói lehetővé teszik a biztonsági események nyomon követését és a hálózat biztonsági állapotának felmérését. A tűzfalak konfigurálása során figyelembe vettük a vállalat biztonsági szabályzatát és a vonatkozó jogszabályokat. A tűzfalak hatékony védelmet nyújtanak a hálózatnak a külső és belső támadásokkal szemben.

**7. Hálózatfelügyelet és Hibakeresés**

Ping, Traceroute és egyéb diagnosztikai eszközök:

A hálózatfelügyelet és a hibakeresés során számos diagnosztikai eszközt használunk, amelyek segítenek azonosítani és elhárítani a hálózati problémákat. A leggyakrabban használt eszközök a következők:

Ping: A ping parancs segítségével ellenőrizhetjük, hogy egy eszköz elérhető-e a hálózaton. A ping küld egy ICMP (Internet Control Message Protocol) csomagot a cél eszköznek, és ha az eszköz válaszol, akkor az elérhető. A ping parancs hasznos a kapcsolati problémák azonosításához és a hálózati késleltetés méréséhez. A ping parancs használata egyszerű és gyors, és lehetővé teszi a hálózat alapvető működésének ellenőrzését.

Traceroute: A traceroute parancs segítségével nyomon követhetjük a hálózati forgalom útját egy adott célpontig. A traceroute küld egy sor UDP (User Datagram Protocol) csomagot a cél eszköznek, és rögzíti azokat az útvonalakat, amelyeken a csomagok áthaladnak. A traceroute parancs hasznos a routing problémák azonosításához és a hálózati topológia feltérképezéséhez. A traceroute parancs segítségével megtudhatjuk, hogy a forgalom milyen útvonalon halad a hálózaton keresztül, és azonosíthatjuk a problémás pontokat.

Egyéb diagnosztikai eszközök:

ipconfig (Windows) vagy ifconfig (Linux): Megjeleníti az eszköz IP-címét, alhálózati maszkját.

Rendben, nézzük meg a Cisco hálózat dokumentációját és karbantartását a megadott szempontok alapján, részletesebben:

**8. Implementáció és Tesztelés**

Részletes tesztelési terv és végrehajtás (Folytatás):

A tesztelési tervnek részletesen ki kell térnie a következőkre:

Tesztelési célok: Mi a tesztelés célja? Milyen funkciókat és szolgáltatásokat kell tesztelni? Például a hálózat alapvető működése, az alkalmazások elérhetősége, a biztonsági funkciók működése, a terhelhetőség és a teljesítmény.

Tesztelési módszerek: Milyen tesztelési módszereket kell alkalmazni? Például funkcionális tesztelés, teljesítmény tesztelés, biztonsági tesztelés, terhelési tesztelés. A funkcionális tesztelés során ellenőrizzük, hogy a hálózat megfelelően működik-e és az eszközök kommunikálnak-e egymással. A teljesítmény tesztelés során mérjük a hálózat sebességét és terhelhetőségét. A biztonsági tesztelés során ellenőrizzük a hálózat védelmét a külső és belső támadásokkal szemben. A terhelési tesztelés során szimuláljuk a hálózat nagy terhelését, hogy ellenőrizzük a stabilitást és a terhelhetőséget.

Tesztelési környezet: Milyen hardver és szoftver eszközöket kell használni a teszteléshez? Például teszt szerverek, teszt kliensek, hálózati analizátorok és monitorozó eszközök. A tesztelési környezetnek hasonlónak kell lennie a éles üzemben lévő hálózathoz, hogy a tesztelési eredmények relevánsak legyenek.

Tesztelési ütemterv: Mikor és milyen sorrendben kell elvégezni a teszteket? A tesztelési ütemtervnek tartalmaznia kell a tesztelési fázisokat, a tesztelési időpontokat és a tesztelési felelősöket.

Tesztelési forgatókönyvek: Milyen konkrét teszteket kell elvégezni? Például kapcsolati teszt, adatátviteli teszt, alkalmazás teszt, biztonsági teszt. A tesztelési forgatókönyveknek részletesen le kell írniuk a tesztelési lépéseket, az elvárt eredményeket és a tesztelési környezetet.

Elvárt eredmények: Milyen eredményeket várunk a tesztektől? Például sikeres kapcsolódás, megfelelő adatátviteli sebesség, biztonságos hozzáférés. Az elvárt eredményeknek mérhetőnek és ellenőrizhetőnek kell lenniük.

Tesztelési dokumentáció: Hogyan kell dokumentálni a tesztelési eredményeket? Például tesztjegyzőkönyv, hiba jelentés. A tesztelési dokumentációnak tartalmaznia kell a tesztelési eredményeket, a hibajelentéseket és a tesztelési összefoglalót.

A tesztelés végrehajtása során fontos a tesztelési terv pontos betartása és az eredmények dokumentálása. A tesztelési eredmények alapján értékelni kell a hálózatot, és ha szükséges, javítani kell a hibákat. A tesztelés befejezése után a hálózat üzembe helyezhető.

**9. Dokumentáció és Karbantartás**

·Konfigurációs mentések és verziókezelés (Folytatás):

A konfigurációs mentéseket automatizálhatjuk TFTP (Trivial File Transfer Protocol) vagy SFTP (Secure File Transfer Protocol) szerver segítségével. A verziókezeléshez használhatunk olyan eszközöket, mint a Git vagy a Mercurial. A konfigurációs mentések és a verziókezelés lehetővé teszik a hálózat gyors helyreállítását hiba esetén és a konfigurációs változások nyomon követését.

Hibajelentések és naplózás:

A naplózási beállítások konfigurálása magában foglalja a naplózási szint beállítását, a naplózási cél megadását és a naplózási üzenetek formátumának beállítását. A központi naplózási szerverre küldött naplókat elemezhetjük olyan eszközökkel, mint a Syslog vagy az ELK stack (Elasticsearch, Logstash, Kibana). A naplózás lehetővé teszi a hálózat biztonsági eseményeinek nyomon követését, a hibák azonosítását és a hálózat működésének elemzését. A naplók rendszeres áttekintése és elemzése segít a hálózati problémák proaktív azonosításában és a biztonsági incidensek megelőzésében.

·Jövőbeli fejlesztési tervek:

A jövőbeli fejlesztések tervezésekor figyelembe kell venni a hálózat jelenlegi állapotát, a várható növekedést és az új technológiák lehetőségeit. A fejlesztési javaslatok lehetnek például a hálózat sebességének növelése, a biztonság megerősítése, a felhő alapú szolgáltatások bevezetése vagy a mobil eszközök támogatásának javítása. A fejlesztési javaslatoknak tartalmazniuk kell a megvalósítási terveket, az erőforrásigényt és a költségbecslést. A jövőbeli fejlesztések megvalósítása előtt fontos a részletes tervezés és a tesztelés. A fejlesztési javaslatoknak összhangban kell lenniük a vállalat stratégiai céljaival és az üzleti igényekkel. A fejlesztési javaslatok megvalósítása hozzájárulhat a hálózat hatékonyságának, biztonságának és versenyképességének javításához.

**10. Összegzés és Tapasztalatok**

·A projekt eredményeinek értékelése:

A projekt során elért eredmények bizonyítják a tervezési és megvalósítási folyamat helyességét. A hálózat üzembe helyezése után a felhasználók elégedettek voltak a hálózat teljesítményével és megbízhatóságával. A hálózat megfelelően működik és támogatja a vállalat üzleti folyamatait. A projekt sikeresen megvalósította a kitűzött célokat, és egy modern, skálázható és biztonságos hálózatot hozott létre. A projekt során betartottuk a költségvetést és az ütemtervet. A projekt során alkalmazott technológiák és megoldások megfeleltek az elvárásoknak. A projekt sikeres megvalósítása hozzájárult a vállalat hatékonyságának és versenyképességének javításához.

·Tanulságok és fejlesztési lehetőségek:

A projekt során szerzett tapasztalatok alapján a jövőbeli projektek tervezése és megvalósítása hatékonyabb lehet. A projekt során kialakult csapatmunka és kommunikáció sikeresen hozzájárult a projekt sikeréhez. A projekt során felmerült problémák és nehézségek tanulságul szolgálnak a jövőbeli projektekhez. A projekt során szerzett tapasztalatok alapján a jövőbeli projektekben még nagyobb hangsúlyt fektethetünk a részletes tervezésre, a tesztelésre és a biztonságra. A projekt során szerzett tapasztalatok alapján a jövőbeli projektekben hatékonyabban használhatjuk a rendelkezésre álló erőforrásokat és jobban alkalmazkodhatunk a változó körülményekhez. A projekt során szerzett tapasztalatok alapján a jövőbeli projektekben még jobban figyelembe vehetjük a felhasználói igényeket és a legújabb technológiai fejlesztéseket.