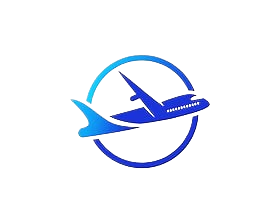


FlyWithMe

****

***Dokumentáció***

Lőrik Levente & Deák Máté

[Bevezetés 3](#_Toc160606445)

[Las Vegas Szerverterem 3](#_Toc160606446)

[HSRP 3](#_Toc160606447)

[NAT 3](#_Toc160606448)

[HTTP 4](#_Toc160606449)

[NTP 4](#_Toc160606450)

[Email 4](#_Toc160606451)

[Syslog 4](#_Toc160606452)

[DNS 5](#_Toc160606453)

[TFTP 5](#_Toc160606454)

[FTP 5](#_Toc160606455)

[AAA 5](#_Toc160606456)

[Budapest székhely 6](#_Toc160606457)

[SSH 6](#_Toc160606458)

[VPN 6](#_Toc160606459)

[Views 6](#_Toc160606460)

[ASA 6](#_Toc160606461)

[London Iroda 6](#_Toc160606462)

[VLAN 6](#_Toc160606463)

[Subinterface 6](#_Toc160606464)

[EtherChannel 6](#_Toc160606465)

[Wi-Fi 7](#_Toc160606466)

[Dhaka Gyár 7](#_Toc160606467)

[IPv6 7](#_Toc160606468)

[DHCPv6 7](#_Toc160606469)

[STP 7](#_Toc160606470)

[Szerver és felhőszolgáltatások 7](#_Toc160606471)

[Frontend 7](#_Toc160606472)

[Backend 7](#_Toc160606473)

[Munka Folyamatok Eloszlása és Beállított Szolgáltatások 9](#_Toc160606474)

Bevezetés

A FlyWithMe egy kitalált vállalat, amely repülőgépek követésével és a jelenleg levegőben repülő gépek adataival foglalkozik. A cég folyamatos fejlesztést és modernizálást hajt végre, hogy biztosítani tudja a felhasználóknak a folyamatos elérést és rendelkezésre állást. A FlyWithMe egy multinacionális vállalat és jelenleg 4 telephellyel rendelkezik. A cégnek van egy szerverterme Las Vegas-ban, egy irodája London-ban és egy gyára a Bangladesben lévő Dhaka-ban. Emellett a cég székhelye Budapesten található.

A telephelyek között EIGRP forgalomirányítást használ a cég. Az ISP-vel való kommunikáció pedig a BGP protokoll segítségével működik. Hajrá Dodder ez egy oldal.

Kép az egész hálózatról

Las VegasSzerverterem

A FlyWithMe a költségek csökkentésé érdekében a helyi szerverek mellett használja a Cloud-ot is. Az AWS Las Vegas-i szerver központjában számos szolgáltatás fut, ami a többi telephelyét szolgálja ki. Az első szerver (192.168.10.10) a fő szerver. Ezen fut a szolgáltatások nagy része. A másik szerver (192.168.10.20) inkább fájltárolásra van használva, valamint ezen a szerveren fut az AAA (Authentication, Authorization, and Accounting) Radius szolgáltatás. Ezen a szerveren található meg az FTP és a TFTP szerver is.

HSRP

A szerverterem a belső forgalomirányítást az EIGRP protokoll segítségével hajtja végre. A router után 2 router is található, ezek között a HSRP (Hot Standby Router Protocol) protokoll lett beállítva, így, ha az egyik router-el bármi technikai probléma történik a másik router veszi át a forgalom irányítását. Ezáltal a hálózatban a harmadik rétegű redundancia biztosítva van, ami azt jelenti, hogy a hálózati szolgáltatások folyamatosan elérhetőek maradnak anélkül, hogy szünet lenne a működésben. A HSRP konfigurálása során a két routeren azonos HSRP csoportot kell létrehozni, amelyek ugyanazon LAN-on vannak. Meg kell határozni a HSRP feladó és átvételi IP-címet, amelyet a hálózati eszközök használnak alapértelmezett átjáróként. Emellett be kell állítani a HSRP prioritást annak érdekében, hogy meghatározzuk, melyik router lesz az aktív és melyik lesz a passzív állapotban. Általában a magasabb prioritású router lesz az aktív.

NAT

A szerverek elött NAT (Network Address Translation) lett beállítva. A hálózati címfordításnak köszönhetően a belső szerverei képesek kommunikálni az interneten lévő szerverekkel úgy, hogy azok csak a NAT által megadott nyilvános IP-címeket látják. Ebben a folyamatban a NAT szerver az adatcsomagok fejlécét módosítja, hogy a belső címek helyett a NAT által használt nyilvános IP-címek legyenek láthatóak a külvilág felé. Ez lehetővé teszi a belső hálózat számára, hogy biztonságosan használja az internetes erőforrásokat, miközben megvédi azokat a külvilág általi támadásoktól, mivel a hálózat belső struktúrája nem ismert. A 192.168.11.0/24 hálózat kívülről a 192.168.10.0/24 hálózat. A fájlok tárolására használt szerver (FTP, TFTP) IP címe: 192.168.10.20, az egyéb funkciókat ellátó szerver (HTTP, NTP, SYSL, DNS) IP címe: 192.168.10.10.

Kép

HTTP

A HTTP szolgáltatás egy belső weboldalt szolgál ki. Ez a belső weboldalon egyfajta admin panelként funkcionál. Egy bejelentkezés után elérhetőek a FlyWithMe belső oldalai. Ez a weboldal elérhető minden telephelyről, kivéve a budapesti vendég Wi-Fi hálózatról. A HTTP szolgáltatás elérhető HTTPS címen is, mivel TLS 1.3 is konfigurálva lett. A weboldal a [www.flywithme.hu](http://www.flywithme.hu) címen érhető el a PC webböngészőjéből.

NTP

Ugyan ezen a szerveren megtalálható egy NTP (Network Time Protocol) szolgáltatás is. Az NTP protokoll segítségével tudjuk beállítani a pontos időt a hálózati eszközök között. Az NTP szerverek pontos időt szolgáltatnak az eszközöknek, ami kritikus fontosságú lehet olyan alkalmazásoknál, amelyek szinkronizált időre támaszkodnak, például hálózati logokhoz, biztonsági tanúsítványokhoz (SSL/TLS) vagy időbélyegekhez. A hálózati eszközök időnként kérést küldenek az NTP szervereknek a pontos idő lekérdezésére. Az NTP szerverek rendelkeznek pontos időreferenciával, amely lehetővé teszi számukra, hogy kiszolgálják ezeket a kéréseket és pontos időinformációt küldjenek vissza a klienseknek. Az NTP protokoll rugalmas és késleltetett hálózatokban is hatékonyan működik, lehetővé téve a pontosság és a stabilitás fenntartását. A routeren megadtuk az NTP szerver IP címét, az NTP titkos kulcsát és beállítottuk, hogy az MD5 hash-t használja.

Email

A szerveren továbbá beállításra került egy levelező szerver, amin a szerver belső kommunikációja zajlik. A szerveren bekapcsoltuk az SMTP és a POP3 szolgáltatást is. Az SMTP (Simple Mail Transfer Protocol) és a POP3 (Post Office Protocol verzió 3) két különböző e-mail protokoll, amelyek kulcsfontosságú szerepet játszanak az elektronikus levelezésben. Az SMTP a levelek küldésére szolgál, míg a POP3 a levelek letöltését és fogadását teszi lehetővé a levelezőszerverről a kliens számítógépére. Az SMTP általában a 25-ös port-on működik, míg a POP3 a 110-es port-ot használja. Ezek a protokollok lehetővé teszik a felhasználók számára, hogy könnyen és hatékonyan kommunikáljanak e-mail üzenetek segítségével a világhálón keresztül. A szerveren továbbá be kell állítani a domain nevet (flywithme.hu) és fel kell venni a felhasználóneveket és jelszavakat. Esetünkben van egy admin és egy IT felhasználó, akik a PC-n tudnak kommunikálni az email kliens segítségével.

Syslog

A SYSLOG (System Logging Protocol) egy olyan protokoll, amelyet a hálózati események rögzítésére és továbbítására használnak a számítógépes hálózatokban. Ennek az a lényege, hogy lehetővé tegye a rendszeradminisztrátorok számára, hogy centralizált módon monitorozhassák és naplózhassák a hálózati eszközökön, szervereken és alkalmazásokon belül bekövetkező eseményeket. A SYSLOG üzeneteket általában szöveges formátumban rögzítik, amely tartalmazza az esemény időpontját, forrását és egyéb fontos információkat. Az események fontosságát különböző prioritási szintekkel látják el, így könnyen azonosíthatók és kezelhetők. Az eszközök SYSLOG funkciójának bekapcsolásával lehetőség nyílik az események monitorozására és azokról értesítések küldésére, például hibák vagy figyelmeztetések esetén. A SYSLOG naplózási szintek lehetővé teszik a felhasználók számára, hogy szűrjék és prioritizálják az eseményeket azok fontosságának megfelelően. A SYSLOG üzeneteket továbbíthatják más eszközökre vagy szerverekre a hálózaton keresztül UDP segítségével általában az 514 porton keresztül. Ezek a naplók jelentős szerepet játszanak a hálózati rendszerek hibakeresésében, a biztonsági események rögzítésében és az általános rendszermonitorozásban. Emellett lehetővé teszik az események időbeli sorrendjének rekonstruálását és a rendszerbiztonság javítását. A SYSLOG általánosan alkalmazott eszköz a hálózatokban a teljesítmény optimalizálására és a rendszerstabilitás fenntartására.

DNS

A szerveren még beállításra került egy DNS kiszolgáló is, ami mind a 4 telephelynek nyújtja a DNS szolgáltatást. A DNS (Domain Name System) egy elosztott adatbázisrendszer, amelyet a világhálón használnak a domain nevek (pl. flywithme.hu) és az ehhez tartozó IP-cím (pl. 192.168.10.10) közötti fordításra. A DNS segítségével a felhasználók könnyen megjegyezhető domain neveket használhatnak a hálózaton, miközben a háttérben a számítógépek IP-címeket használnak a kommunikációhoz. A DNS hierarchikus struktúrában működik, több különböző típusú DNS szerverrel, amelyek közötti átváltás és lekérdezések révén történik az adatok megfelelő elérése. A korábban beállított HTTP szervernek az IP címe van megadva A rekord-ként, ez a 192.168.10.10-es IP cím. Minden DHCP kliens ezt a DNS címet használja, így elérhető a weboldal minden belső számítógépről.

TFTP

A TFTP (Trivial File Transfer Protocol) egy egyszerű, UDP alapú protokoll, amelyet a fájlok egyszerű átvitelére használnak a hálózaton keresztül. A TFTP különösen hasznos olyan helyzetekben, ahol egyszerű, gyors és megbízható fájlátvitelre van szükség, például szoftverfrissítések során a hálózati eszközökön vagy a hálózati eszköz konfigurációjának lementésekor. A protokoll az UDP-t használja és alapértelmezetten a 69-es port-ot.

FTP

Az FTP (File Transfer Protocol) segítségével fájlokat tudunk megosztani egy TCP kapcsolaton keresztül. Titkosítása is lehetséges SSH segítségével (SFTP). A tradicionális kliens-szerver kapcsolat miatt már elavultnak számít és lassúnak. Egy P2P kapcsolat vagy a HTTP is nagyobb teljesítményre képes. Ma már a böngészők se támogatják az ftp:// linkek megnyitását. A FlyWithMe főleg régi fájlok tárolására használja még az FTP-t, amik még nem lettek egy modernebb objektum alapú fájlkiszolgálóra átköltöztetve (AWS S3).

AAA

AAA, radius dodder

Budapestszékhely

A FlyWithMe székhelye Budapesten található.

SSH

Dodder

VPN

A budapesti és londoni iroda között egy VPN tunnel lett kialakítva, így a cég két telephelye között titkosított a kapcsolat. A GRE (Generic Routing Encapsulation) protokollt választottuk a titkosított kapcsolat kialakítására. A GRE a Cisco álltal 1994-ben kifejlesztett tunnel protokoll. A GRE tunnel egy logikai csatornát képez két távoli hálózat között. A GRE protokoll becsomagolja az eredeti IP csomagokat egy új IP csomagba, így biztonságos és titkosított a kapcsolatot a végpontok között. Az IP csomagok GRE fejléccel bővülnek, hogy azokat a túloldali végpont ki tudja bontani. A GRE tunnel létrehozásához azonos konfigurációra van szükség mindkét végponton. Az overhead költség (csomagok becsomagolása) minimális, ami hatékony adatátvitelt biztosít. A GRE tunnel lehetővé teszi a távoli hálózatok közötti összeköttetést, mintha azok helyben lennének. A GRE tunnel alkalmazása növeli a hálózati biztonságot, mivel az adatok titkosítva vannak átvitel közben. A VPN GRE tunnel segítségével a távoli hálózatok közötti kommunikáció biztonságosabbá és megbízhatóbbá válik. A VPN GRE tunnel rugalmas megoldást kínál a távoli hálózatok közötti kapcsolat létrehozására, például vállalati irodák vagy adatközpontok között. A GRE tunnel támogatja a multicast és broadcast forgalmat is, így széles körű alkalmazhatóságot biztosít.

Views

A cégnél több hálózati informatikus is dolgozik, így a view-k segítségével több biztonsági szint is ki lett alakítva. Dodder

ASA

Dodder

LondonIroda

A cég főként itt végzi a szoftver és hardver tervezését és tesztelését. A hálózat hálom VLAN-ra lett felosztva három alinterfész segítségével.

VLAN

A londoni iroda 3 VLAN-ra lett felosztva. dodder

Subinterface

A router GigabitEthernet0/0 portja három alinterfacere lett felosztva: 0.10, 0.20, 0.30. Mindegyik alinterface-hez egy VLAN tartozik. dodder

EtherChannel

Az EtherChannel egy olyan technológia a hálózati infrastruktúrában, amely lehetővé teszi több fizikai interfész csoportosítását egy logikai csatornában. Ez azért fontos, mert növeli a sávszélességet és javítja a hálózati rendszerek teljesítményét. A legtöbb Ethernet hálózati eszköz támogatja az EtherChannel létrehozását és konfigurálását, beleértve a switcheket és a routereket is. Az EtherChannel konfigurációja általában a link-aggregáció elvén alapul, ahol több interfészt egyetlen logikai csoportba sorolnak össze. Ez lehetővé teszi a forgalom terheléselosztását az egyes interfészek között, így kiegyensúlyozva a terhelést a hálózaton. Emellett az EtherChannel redundanciát is biztosít, mivel, ha egy interfész meghibásodik, a többi interfész még mindig képes továbbítani a forgalmat. A leggyakoribb konfiguráció az LACP (Link Aggregation Control Protocol) vagy a PAgP (Port Aggregation Protocol) használata, amely lehetővé teszi az interfészek dinamikus csoportosítását. Az EtherChannel létrehozása előnyös lehet olyan helyzetekben, ahol magas sávszélességre és megbízhatóságra van szükség, például adatközpontokban vagy nagyobb hálózati szegmensekben. Az EtherChannel használata jelentős előnyökkel jár a hálózati teljesítmény és stabilitás szempontjából, különösen nagy forgalmú környezetekben. Az interfészek csoportosítása egyetlen logikai egységbe segít optimalizálni a hálózati erőforrásokat és minimalizálni a hibák kockázatát.

Wi-Fi

Dodder

DhakaGyár

A FlyWithMe az olcsó munkaerő és a régió fejlesztése miatt a Banglades-ben található Dhaka-ban létesített gyárat. Itt történik az ADS-B[[1]](#endnote-1) és MLAT[[2]](#endnote-2) vevők összeszerelése. Két gyártósor került kialakításra, az egyiken az ADS-B, még a másikon az MLAT és a hozzájuk tartozó komponensek gyártása történik. Mivel a gyár egy teljesen új ipari parkban épült így a hálózat is nulláról lett felépítve. A FlyWithMe informatikai csapata ezért az IPv6 címzés beállítása mellet döntött.

IPv6

A dhakai gyár egy teljesen új ipari parkban épült. Ezért a FlyWithMe informatikai csapata egyből a modernebb IPv6 címzés mellet döntött, így később nem kell majd modernizálni a hálózatot. Az IPv6-nak több előnye is van az IPv4-el szemben. 128-bites címeket használ az IPv6, míg az IPv4 32 bites címeket használ, így több IP cím osztható ki egy hálózaton belül. A nagyobb címek miatt NAT használatára sincs szükség. Mivel IPv4-es címből csak 232 számú cím osztható csak ki ezért egyre fontosabb, hogy IPv6-ra álljunk át, mivel itt 2128 számú IP cím osztható ki, így nincs szükség NAT-ra, mivel minden eszköznek jut saját IP cím. Már egy ideje fogyóban vannak az IPv4-es címek, sok helyen alapból már fizetni kell az IPv4-es címekért, míg az IPv6-os címek ingyen vannak, de a kompatibilitás is sokkal rosszabb, mivel sok ISP még mindig nem támogatja az IPv6-os címeket.

DHCPv6

Az összes hálózati eszköz a DHCPv6 (Dynamic Host Configuration Protocol version 6) segítségével kap IP címet. Két féle módon kaphat egy eszköz IPv6-os címet: SLAAC és állapottartó. A SLAAC (Stateless Address Autoconfiguration) segítségével minden eszköz saját magának állít IP címet, és ezt mind egy központi szerver használata nélkül. Segítségével az eszközök automatikusan kaphatnak IPv6 címet, alhálózati információkat, végpont címeit és más hálózati beállításokat. A DHCPv6 célja a hálózati konfiguráció automatizálása és egyszerűsítése, különösen olyan környezetekben, ahol sok eszköz csatlakozik a hálózathoz. A SLAAC-al szemben az az előnye, hogy minden egy központi szerverről érkezik és nem csak IP címek oszthatók ki, hanem más információk is, például Domain vagy DNS név.

STP

A gyár gördülékeny működése miatt 2 switch között STP (Spanning Tree Protocol) protokoll lett beállítva. Így, ha az egyik switch tönkremegy a másikon keresztül gördülékenyül folyik a hálózati kommunikáció. Így biztosítva van a 2. réteg béli redundancia. Az STP-n belül az újabb RSTP (Rapid Spanning Tree Protocol) lett beállítva. Az RSTP gyorsabban reagál a hálózaton belüli változásokra. dodder

Szerver és felhőszolgáltatások

FlyWithMe már teljesen Cloud Native, minden ügyfélnek (B2C) és cégnek (B2B) kínált szolgáltatást a felhőben futtatunk.

Frontend

A weboldal a Node.js keretrendszeren fut, és a React.js-t használja Frontend-ként. Az oldal TailwindCSS és BoorstrapCSS használ az oldal formázáshoz. A kliens oldali navigáláshoz pedig React Router-t. Az weboldal két oldalból áll: Kezdőlap, itt egy rövid bemutatkozás található a cégről és a kínált szolgáltatásokról. A másik oldal pedig a térkép, ahol élőben lehet követni a járatokat.

Backend

A backend PHP-ben lett írva és az Apache webszerver alatt fut. A backend feladata, hogy a repterek közelébe elhelyezett ADS-Bi és MLATii vevők adatait feldolgozza és adatbázisban tárolja el. Az eltárolt adatokat pedig JSON formátumban szolgáltatja a frontend felé. A webszerven a CORS[[3]](#endnote-3) miatt minden válaszban az *Access-Control-Allow-Origin*-t és a *Content-Type: application/json*-t is küldjük a fejlécben, az előbbit azért, hogy minden URL-ről elérhető legyen a webszerver, az utóbbit pedig a JSON enkódolás miatt.

Munka Folyamatok Eloszlása és Beállított Szolgáltatások

|  |  |  |
| --- | --- | --- |
| *Beállított Szolgáltatások* | *Lőrik Levente* | *Deák Máté* |
| IPv4 Címzés |  | X |
| IPv6 Címzés | X |  |
| DHCP Címzés |  | X |
| DHCPv6 Címzés | X |  |
| NAT Címfordítás | X | X |
| EIGRP Útvonalválasztás |  | X |
| BGP Útvonalválasztás |  | X |
| HSRP | X |  |
| PPP | X | X |
| Statikus Útvonal | X |  |
| PAT | X |  |
| EMAIL Kiszolgáló |  | X |
| Pontos Idő (NTP Szerver) |  | X |
| SYSLOG |  | X |
| Távoli Elérés (FTP) | X | X |
| TFTP | X |  |
| HTTP |  | X |
| SSH | X | X |
| VPN | X |  |
| Szerver alapú AAA | - | - |
| Redisztribúció (EIGRP-BGP) |  | X |
| STP | X |  |
| Tűzfal |  | X |
| DNS |  | X |
| Vezeték Nélküli Hálózat | - | - |
| ACL | X |  |
| EtherChannel |  | X |
| SNMP | - | - |
| Programozott Konfiguráció |  |  |
| Alinterfészek | X | X |
| VLAN | X |  |
| Tunnel Interface Kialakítása | X |  |
| Radius Szerver | - | - |
| Switch Port Biztonság | - | - |
| Szerveren Beállított Szolgáltatások | | |
| DHCP |  |  |
| DNS |  |  |
| NAT |  |  |
| Active Directory |  |  |
| Apache |  |  |
| Fájl- és Nyomtatómegosztás  Adatbázis |  |  |
| Adatbázis kezelő szoftver |  |  |
| Frontend | X |  |
| Backend | X | X |

1. Automatic Dependent Surveillance–Broadcast [↑](#endnote-ref-1)
2. Multilateration [↑](#endnote-ref-2)
3. Cross-origin resource sharing [↑](#endnote-ref-3)