Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**Vizsgaremek címe**

Harkányi Dániel 13.B, Kármán Szabolcs 13.A

Budapest, 2025.

[A NetWorkers vállalat előtörténete 3](#_Toc196324710)

[A kezdetek: 3](#_Toc196324711)

[Növekedés és bővülés: 3](#_Toc196324712)

[A jelen és jövőkép: 3](#_Toc196324713)

[A vállalat szolgáltatásai 3](#_Toc196324714)

[Hálózattervezés és kivitelezés: 3](#_Toc196324715)

[Felhőalapú szolgáltatások: 4](#_Toc196324716)

[Biztonságtechnikai megoldások: 4](#_Toc196324717)

[Projektek és referenciák 4](#_Toc196324718)

[Belföldi projektek: 4](#_Toc196324719)

[Nemzetközi partnerek: 4](#_Toc196324720)

[Fogalomtár(Hálózat) 5](#_Toc196324721)

[Fogalomtár(Szerverek) 7](#_Toc196324722)

[Logikai Topológia 8](#_Toc196324723)

[Vizsgaremek Megoldásaink: 8](#_Toc196324724)

[(3 db telephely): 8](#_Toc196324725)

[VLAN + VTP 9](#_Toc196324726)

[HSRP(3.rétegbeli redundáns megoldás): 12](#_Toc196324727)

[Etherchannel(2.rétegbeli redundáns megoldás): 13](#_Toc196324728)

[IVP6- IPV4: 15](#_Toc196324729)

[SOHO router(wireless hálózat): 16](#_Toc196324730)

[Statikus route pl: 18](#_Toc196324731)

[Dinamikus route(OSPF) pl: 18](#_Toc196324732)

[GRE+IPSEC+ACL: 19](#_Toc196324734)

[PAT: 21](#_Toc196324735)

[NAT(elérjük az FTP-szervert): 21](#_Toc196324736)

[Tüzfal(webszerver védelme): 22](#_Toc196324737)

[Hálózat Prog: 23](#_Toc196324738)

[Szerverek (packet tracerben): 24](#_Toc196324739)

[DHCP & ADDS & DNS & FTP: 24](#_Toc196324740)

[Szerverek 25](#_Toc196324741)

A NetWorkers vállalat előtörténete

### A kezdetek:

* A NetWorkers vállalat története 2013-ra nyúlik vissza, amikor két fiatal informatikus – egyetemi éveik alatt megismerkedve – úgy döntöttek, hogy saját céget alapítanak a hálózati rendszerek fejlesztésére és üzemeltetésére. Az alapítókat a gyorsan fejlődő informatikai piac és az egyre növekvő igények inspirálták, különösen a kis- és középvállalkozások hálózati infrastruktúráinak fejlesztése terén.
* Kezdetben egy garázsban működtek Budapesten, ahol kisebb projekteket vállaltak el, például otthoni és irodai hálózatok tervezését és telepítését. A cég alapfilozófiája már akkor is az volt, hogy ügyfeleik számára megbízható, skálázható és biztonságos hálózati megoldásokat nyújtsanak.

### Növekedés és bővülés:

* A vállalat első áttörése 2013-ban következett be, amikor egy nemzetközi kereskedelmi cég őket bízta meg egy több telephelyes VPN-hálózat kiépítésével. Ez a projekt nemcsak anyagi sikert hozott, hanem hírnevet is, amely újabb megrendeléseket eredményezett.
* 2015-től kezdve a NetWorkers tevékenységi köre kibővült felhőalapú hálózati megoldásokkal és adatközponti szolgáltatásokkal is. A cég ekkor már több mint húsz főt foglalkoztatott, és saját irodával rendelkezett Budapest belvárosában. A vállalat külön részleget hozott létre kutatás-fejlesztés céljára, amely az új generációs hálózati protokollok és biztonsági megoldások fejlesztésére fókuszált.

### A jelen és jövőkép:

* Ma a NetWorkers az egyik vezető magyarországi hálózatépítéssel és üzemeltetéssel foglalkozó vállalat, amely hazai és nemzetközi ügyfelek számára kínál testreszabott megoldásokat. Szolgáltatásaik közé tartozik a hálózattervezés, eszközbeszerzés, implementáció, folyamatos karbantartás, valamint a hálózati biztonsági auditok végrehajtása.
* A cég jövőbeli célja, hogy a mesterséges intelligencia és automatizált hálózatmenedzsment területén is élen járjon, miközben megőrzi ügyfélközpontúságát és magas színvonalú szolgáltatásait.

A vállalat szolgáltatásai

### Hálózattervezés és kivitelezés:

* A NetWorkers fő tevékenységi területe a hálózattervezés, amely során az ügyfél igényeihez igazítva készítenek részletes topológiákat, eszközlistákat, valamint kivitelezési tervet. Ezt követi a hálózat fizikai kiépítése, beleértve a kábelezést, aktív eszközök telepítését és konfigurálását.

### Felhőalapú szolgáltatások:

* A cég hibrid és teljesen felhőalapú megoldásokat is kínál, például vállalati szintű VPN-eket, távoli hozzáférési rendszereket, vagy privát felhő-infrastruktúrákat. Kiemelt figyelmet fordítanak a skálázhatóságra és a redundáns, biztonságos működésre.

### Biztonságtechnikai megoldások:

* A NetWorkers szakemberei komplex IT-biztonsági vizsgálatokat végeznek, valamint behatolásmegelőző és behatolásészlelő rendszereket telepítenek. Ezenkívül tűzfalakat, végpontvédelmet és titkosítási megoldásokat is kínálnak, különösen érzékeny adatokat kezelő szervezetek számára.

Projektek és referenciák

### Belföldi projektek:

* Hazai szinten a cég több nagy volumenű projektet is végrehajtott, például oktatási intézmények hálózatainak kiépítését, városi Wi-Fi rendszerek telepítését, valamint állami intézmények informatikai infrastruktúrájának korszerűsítését.

### Nemzetközi partnerek:

* Nemzetközi szinten a NetWorkers együttműködött osztrák, német és lengyel partnerekkel, főként adatközponti rendszerek építésében és nemzetközi WAN-hálózatok kialakításában

Fogalomtár(Hálózat)

**• VLAN (Virtual Local Area Network):**

A VLAN egy logikai hálózat, amely lehetővé teszi, hogy ugyanazon fizikai hálózaton belül különálló hálózati csoportokat hozzunk létre. Például egy cégen belül a pénzügy és az IT osztály külön VLAN-ban lehet, így jobban elkülöníthetőek és biztonságosabbá válik a hálózati kommunikáció.

**• HSRP (Hot Standby Router Protocol):**

Ez a Cisco által kifejlesztett protokoll lehetővé teszi, hogy két vagy több router együttműködjön, és ha az elsődleges router meghibásodik, automatikusan egy másik átvegye a forgalmat. Így a hálózat folyamatosan működőképes marad.

**• EtherChannel:**

Ez a technológia több fizikai hálózati kapcsolatot kombinál egyetlen logikai kapcsolattá. Ezzel növelhető a hálózati sávszélesség, és ha egy kábel meghibásodik, a többi továbbra is működik – így megbízhatóbbá válik az adatátvitel.

**• IPv6 (Internet Protocol version 6):**

A legújabb internetprotokoll-verzió, amely sokkal nagyobb számú IP-címet tud kezelni, mint az IPv4. Erre azért van szükség, mert az internetre csatlakozó eszközök száma folyamatosan nő, és az IPv4-es címek lassan elfogynak.

**• IPv4 (Internet Protocol version 4):**

Ez a legelterjedtebb protokoll, amelyet az eszközök azonosítására és az internetes adatforgalom irányítására használnak. 32 bites címeket használ (például: 192.168.0.1), de a címkészlete korlátozott, ezért vezették be az IPv6-ot.

**• Wireless hálózat (Wi-Fi):**

Vezeték nélküli hálózat, amely rádióhullámokat használ az eszközök közötti adatátvitelhez. Leggyakrabban otthonokban és irodákban használják, mert nem kell kábeleket húzni, és könnyen bővíthető.

**• Statikus útvonal (Static Route):**

Ez egy kézzel beállított útvonal a hálózaton belül. A rendszergazda pontosan megmondja, hogy egy adott címre merre kell mennie az adatnak. Egyszerű és megbízható, de nagy hálózatokban nehézkes kezelni.

**• Dinamikus útvonal (Dynamic Route):**

Ezzel a módszerrel a hálózati eszközök automatikusan megtanulják az optimális útvonalakat a forgalom számára, különböző protokollok (pl. OSPF, EIGRP) segítségével. Rugalmasabb és könnyebben kezelhető, mint a statikus útvonal.

**• NAT (Network Address Translation):**

Ez a technológia lehetővé teszi, hogy egyetlen nyilvános IP-cím mögött több belső eszköz is elérje az internetet. Elrejti a belső hálózat IP-címeit, így biztonságosabbá teszi a kommunikációt.

**• PAT (Port Address Translation):**

A NAT egyik speciális típusa, amely nemcsak az IP-címet, hanem a portszámokat is figyelembe veszi. Így még több eszköz tud egyszerre csatlakozni az internetre egyetlen IP-cím használatával.

**• Hálózatprogramozás (Network Programming):**

Ez azt jelenti, hogy szoftveresen irányítjuk a hálózat működését. Például automatizálhatjuk a beállításokat, vagy programozott módon vezérelhetjük, hogyan viselkedjenek a hálózati eszközök – ez különösen fontos a modern, nagy hálózatokban.

**• ACL (Access Control List):**

Ez egyfajta szűrő, amely meghatározza, hogy egy adott eszköz vagy felhasználó hozzáférhet-e bizonyos hálózati erőforrásokhoz. Használható például arra, hogy csak bizonyos IP-címek érjék el a szervert.

**• Tűzfal (Firewall):**

Olyan szoftver vagy hardver eszköz, amely figyeli és szabályozza a hálózaton áthaladó adatforgalmat. Segít megvédeni a hálózatot a külső támadásoktól és jogosulatlan hozzáférésektől.

**• VTP (VLAN Trunking Protocol):**

A VTP egy Cisco által fejlesztett protokoll, amely lehetővé teszi, hogy több switch között szinkronban legyenek a VLAN-beállítások. Ha egy switch-en létrehozol vagy módosítasz egy VLAN-t, a VTP segítségével ez a változtatás automatikusan eljut a többi switch-re is a hálózatban. Ez megkönnyíti a VLAN-ok kezelését nagyobb hálózatokban, és csökkenti a manuális hibák lehetőségét.

**• GRE (Generic Routing Encapsulation):**

A GRE egy olyan alagútprotokoll, amely lehetővé teszi, hogy különböző hálózati protokollokat „becsomagoljunk” egy másik protokollba. Ezt leggyakrabban akkor használják, ha két távoli hálózatot kell összekötni úgy, mintha egy helyi hálózat részei lennének – például VPN-ek esetén. A GRE önmagában nem titkosítja az adatokat, csak az „alagutat” hozza létre.

**• IPsec (Internet Protocol Security):**

Az IPsec egy biztonsági protokollkészlet, amely titkosítást és hitelesítést biztosít IP-alapú kommunikációhoz – például VPN-ek esetén. Az IPsec gondoskodik arról, hogy az adatok titkosítva haladjanak végig az interneten, így illetéktelenek nem tudják azokat elfogni vagy módosítani. Általában VPN-ek egyik legfontosabb építőeleme.

Fogalomtár(Szerverek)

**• Címtár (pl. Active Directory):**

A címtár olyan központi adatbázis, amely felhasználók, számítógépek és erőforrások adatait tartalmazza egy hálózaton belül. Az Active Directory a legelterjedtebb címtárszolgáltatás, amely lehetővé teszi a felhasználók hitelesítését, jogosultságkezelést, valamint az eszközök központi irányítását. Például egy rendszergazda egy helyen tudja beállítani, ki melyik nyomtatót használhatja, vagy kinek milyen jogosultsága van a fájlokhoz.

**• DHCP (Dynamic Host Configuration Protocol):**

Ez a protokoll automatikusan kiosztja az IP-címeket a hálózatban lévő eszközöknek. Így nem kell minden számítógépnek kézzel beállítani az IP-címet, alhálózatot, alapértelmezett átjárót és DNS-t. Ez különösen hasznos nagyobb hálózatokban, ahol sok eszköz van jelen.

**• DNS (Domain Name System):**

A DNS olyan szolgáltatás, amely a könnyen megjegyezhető domain neveket (pl. google.com) lefordítja IP-címekre (pl. 142.250.74.78). Enélkül nem lenne egyszerű az interneten navigálni, mert minden weboldalt IP-cím alapján kellene elérni. A DNS szerverek tehát az internet „névjegyzékei”.

**• HTTP/HTTPS:**

A **HTTP (Hypertext Transfer Protocol)** egy protokoll, amely az internetes oldalak kiszolgálásáért felel. A **HTTPS** ennek a titkosított, biztonságos változata, amely védi az adatokat például bejelentkezéskor vagy vásárláskor. A webszerverek ezen keresztül küldik el a weboldalakat a böngészőknek.

**• Fájl- és nyomtató megosztás:**

Ez a szolgáltatás lehetővé teszi, hogy egy központi szerveren elhelyezett fájlokat több felhasználó is elérjen, illetve hogy hálózati nyomtatókat közösen használjanak. Például egy irodában mindenki ugyanahhoz a megosztott mappához és nyomtatóhoz fér hozzá a saját számítógépéről.

**• Automatizált mentés:**

Ez a funkció gondoskodik arról, hogy a fontos adatokat rendszeresen elmentsék egy másik tárhelyre (pl. másik szerverre, felhőbe). Így ha hardverhiba, vírus vagy emberi hiba történik, az adatok visszaállíthatók. Az automatizálás biztosítja, hogy ne felejtsenek el mentést végezni.

**• Kliens számítógépekre automatizált szoftvertelepítés:**

Ez a szolgáltatás lehetővé teszi, hogy a rendszergazdák központilag, egyszerre több számítógépre telepítsenek szoftvereket, frissítéseket vagy beállításokat. Így nem kell minden egyes gépet külön-külön kezelni, ami rengeteg időt takarít meg, főleg nagy hálózatokban.

A képen szöveg, diagram, Tervrajz, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.Logikai Topológia

Vizsgaremek Megoldásaink:

|  |  |  |
| --- | --- | --- |
| (3 db telephely): | | |
| Pécs | Budapest | Szeged |
| A képen szöveg, diagram, képernyőkép, sor látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. | A képen szöveg, diagram, térkép, sor látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. | A képen szöveg, diagram, képernyőkép, sor látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |

### A képen szöveg, képernyőkép, diagram, zöld látható Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.VLAN + VTP

* Megtalálható: Szeged Routeren, Szeged\_SW\_1-2Beállítása:

SZR:

|  |  |
| --- | --- |
| 1.Létre kell hozni az alinterface-eket: |  |
| 2.létre kell hozni a VLAN-ok hoz szükséges DHCP-poolokat: -Név -Ipcím+maszk  -dns- cím |  |

SW1:

|  |  |
| --- | --- |
| Trunk módba kell tenni a router felé vezető portot |  |
| Létre kell hozni a switchen a Vlanokat + elnevezés |  |
| Hozzáadjuk a létrehozott VLAN-okat a megfelelő interface-nek |  |

|  |  |
| --- | --- |
| Pc: Példa | A képen szöveg, képernyőkép, Betűtípus, nyugta látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |

SW1 VTP:

|  |  |
| --- | --- |
| **-SW1** legyen a **VTP szerver** (server mode  - **VTP domain nevet**  használják  -VTP jelszó is be kell állítani.  -Az összekötő port legyen **trunk módban** |  |

SW2 VTP:

|  |  |
| --- | --- |
| **-SW2** legyen a **VTP szerver** client mode)  - **VTP domain nevet**  használják  -VTP jelszó is be kell állítani.  -Az összekötő port legyen **trunk módban** |  |
| Hozzáadjuk a t VLAN-okat a megfelelő interface-nek |  |

A képen szöveg, diagram, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### HSRP(3.rétegbeli redundáns megoldás):

* Megtalálható: BR1 + BR2

BR1:

|  |  |
| --- | --- |
| meg kell adni:  -Az HSRP virtuális IP címe, amit a kliensek gateway-ként használnak.  - Az eszköz prioritása; minél nagyobb, annál valószínűbb, hogy ő lesz az aktív  - Ez lehetővé teszi, hogy a router visszavegye az aktív szerepet, ha magasabb a prioritása.  - Ha ez az interfész leáll, csökken a prioritás → gyorsabb átváltás a másik routerre. |  |

BR2:

|  |
| --- |
|  |

### Etherchannel(2.rétegbeli redundáns megoldás):

|  |  |
| --- | --- |
| A képen szöveg, Betűtípus, képernyőkép, szám látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. | A képen szöveg, diagram, sor, térkép látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |
| SW1 | A képen szöveg, Betűtípus, képernyőkép, fehér látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |
| SW2 | A képen szöveg, képernyőkép, Betűtípus, szám látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |
| SW3 | A képen szöveg, képernyőkép, Betűtípus, algebra látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |
| SW4 | A képen szöveg, Betűtípus, képernyőkép, algebra látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen. |

### A képen szöveg, diagram, képernyőkép, sor látható Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.IVP6- IPV4:

* Megtalálható: PR + Pécs-PC

PR1(IPV6):

|  |  |
| --- | --- |
| Megadjuk az ip cimet: |  |

Pécs-IPV6-PC:

|  |
| --- |
|  |

PR1(IPV4):

|  |  |
| --- | --- |
| Megadjuk az ip cimet: |  |

Pécs-IPV4-PC:

|  |
| --- |
|  |

### SOHO router(wireless hálózat):

A képen szöveg, képernyőkép, diagram, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

|  |  |
| --- | --- |
| A router ip címét adjuk meg |  |
| DHCP szolgáltatást lát el és ezt állítjuk be |  |
| megadjuk a ssid-t |  |
| és titkositjuk |  |
| példa laptop: |  |

A képen diagram, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### Statikus route pl:

|  |  |
| --- | --- |
| Border routerektől az ISP felé:  Megadjuk a quad zero az ISP felé.  Miért?: minden ismeretlen hálózat forgalmát erre az útvonalra küld a router. |  |

A képen szöveg, képernyőkép, diagram látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### Dinamikus route(OSPF) pl:

|  |  |
| --- | --- |
| Budapest\_Border:  -megadjuk az ospf számát  -megadjuk: a router azonositóját,  -majd az összes router által ismert hálózatot + a wildcard maskot |  |
| BpR-1-2: ugyan ez |  |
| Ellenörzés (Border): |  |

### A képen szöveg, képernyőkép, diagram, sor látható Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### GRE+IPSEC+ACL:

* megtalálható: Budapest\_border, Szeged\_Border

BBR:

|  |  |
| --- | --- |
| GRE: |  |
| IPSEC: |  |
| ACL: |  |

SZBR:

|  |  |
| --- | --- |
| GRE: |  |
| IPSEC: |  |
| ACL: |  |

A képen képernyőkép, diagram, sor, kör látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### PAT:

* megtalálható pl: SZBR:

|  |  |
| --- | --- |
| Létrehozunk egy ACL-t |  |
| Engedélyezzük, hogy a belső IP-tartomány NAT-olva legyen. |  |
| majd megajelöljük a külső és belső interface-t |  |

A képen szöveg, diagram, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### NAT(elérjük az FTP-szervert):

|  |  |
| --- | --- |
| létrehozzuk a natot |  |
| megadjuk neki melyik a belső és a külső interface |  |

### A képen diagram, szöveg, sor, képernyőkép látható Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.Tüzfal(webszerver védelme):

|  |  |  |
| --- | --- | --- |
| IP cím: | |  |
|  |
| quad zero – statikus forgalomirányitás | |  |
| a WebVPN funkció bekapcsolása az „outside” interfészen. | |  |
| megadunk egy könyvjelzőt a WebVPN portálhoz. | |  |
| „ADMIN” nevű felhasználó kerül hozzárendelésre a „web” nevű könyvjelzőhöz. A felhasználó „admin” profilt és „fotest” nevű csoportházirendet kap, amely meghatározza a hozzáférési jogosultságait. | |  |
| PAT kell hozzá border routeren | | |
| SZR-től meg quad zero | | |
| Példa: |  | |

### Hálózat Prog:

Szerverek (packet tracerben):

### DHCP & ADDS & DNS & FTP:

|  |  |  |
| --- | --- | --- |
|  |  | |
| DHCP |  |  |
| DNS |  | |
| FTP |  | |

Szerverek