**Miskolci SZC**

**Kandó Kálmán Informatikai Technikum**

***VIZSGAREMEK***

Készítették:

1. Simon Viktor (13.C)
2. Kántor Bence (13.C)
3. Oleszka Attila (13.C)

**Miskolc, 2025.11.18.**

Tartalomjegyzék

Tartalom

[Bevezetés 3](#_Toc219969246)

[IP Cím tábla 4](#_Toc219969247)

[1.0 Telephelyek 5](#_Toc219969248)

[1.1 Packeta-Gyártósor (Fő hálózat) 5](#_Toc219969249)

[1.2 Alapbeállítások (SSH) 6](#_Toc219969250)

[1.3 Packeta R1 6](#_Toc219969251)

[1.4 Packeta R2 6](#_Toc219969252)

[1.5 Packeta-SW1 7](#_Toc219969253)

[1.6 Packeta-SW2 7](#_Toc219969254)

[1.8 HSRP beállítások 8](#_Toc219969255)

[1.9 Etherchannel beállításai 9](#_Toc219969256)

[1.10 VLAN 10](#_Toc219969257)

[1.11 Port-Security 11](#_Toc219969258)

[1.12 ASA Tűzfal 12](#_Toc219969259)

[1.13 OSPF 13](#_Toc219969260)

[1.14 PacketaR1 13](#_Toc219969261)

[1.15 PacketaR2 13](#_Toc219969262)

[1.16 Normál ACL 14](#_Toc219969263)

[1.17 Kiterjesztett ACL 15](#_Toc219969264)

[2.0 Packeta Iroda telephely 16](#_Toc219969265)

[2.1 LAN hálózat 16](#_Toc219969266)

[2.2 WAN hálózat 17](#_Toc219969267)

[2.3 SSID 17](#_Toc219969268)

[2.4 SECURITY 18](#_Toc219969269)

[2.5 Irányító router 19](#_Toc219969270)

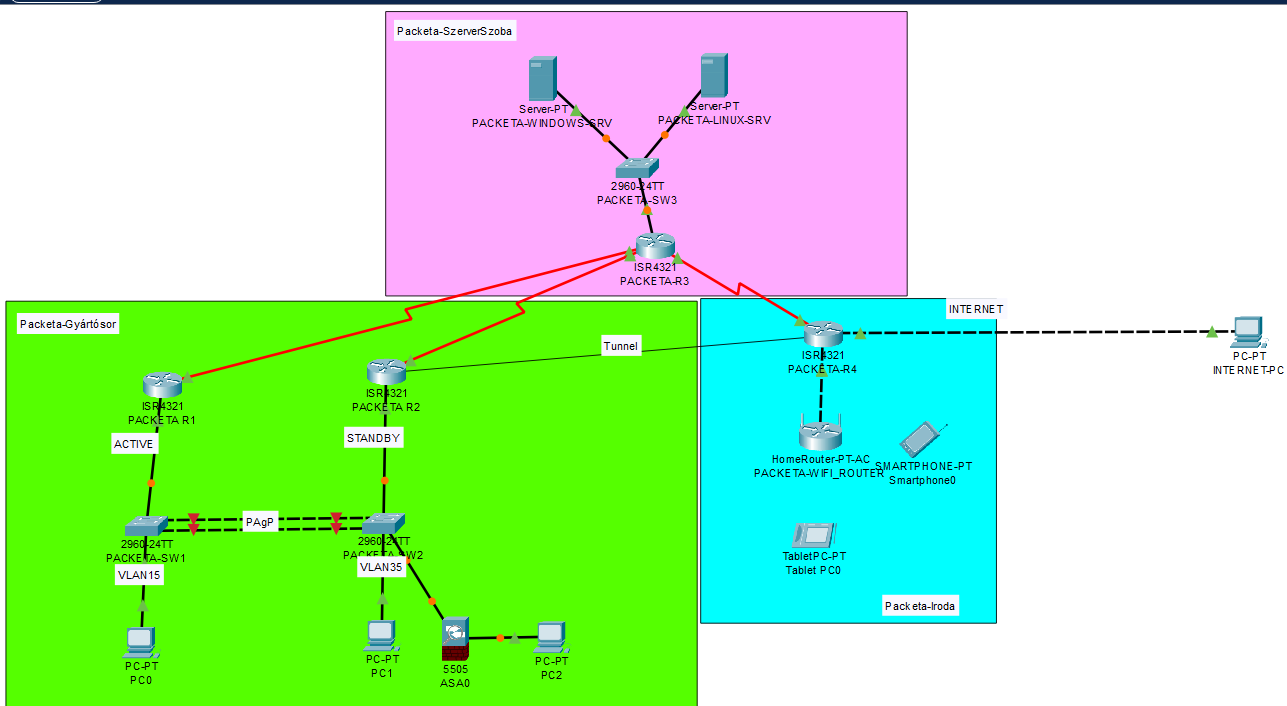
[2.6 OSPF 19](#_Toc219969271)

[2.7 NAT 20](#_Toc219969272)

# Bevezetés

**Cégünk neve: Packeta**

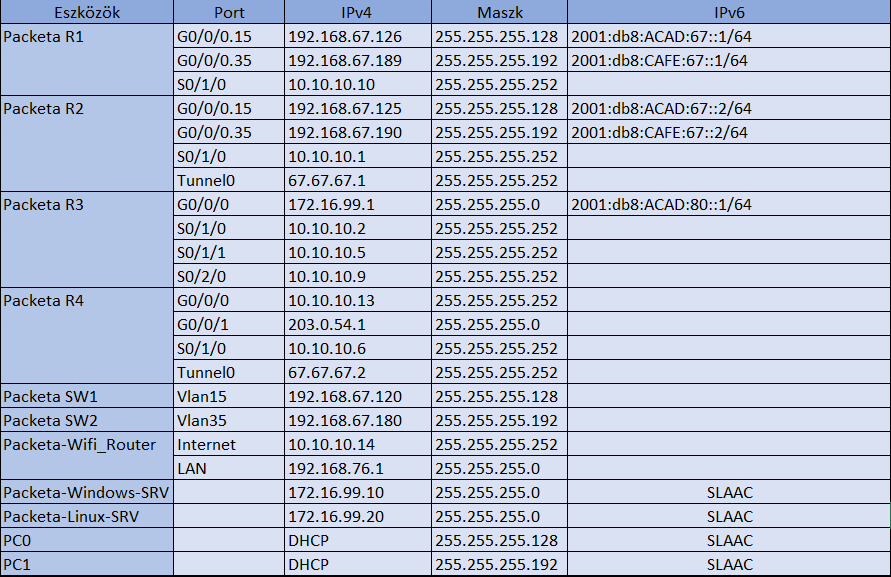
A hálózatot úgy terveztük és alakítottuk ki, hogy megfeleljen minden fontos szakmai szempontnak. Célunk az volt, hogy egy nagyvállalat számára is bebizonyítsuk: munkánk megbízható, átgondolt és precíz.

Jelen dokumentum célja ennek a hálózatnak a bemutatása, egyfajta referenciaanyagként, amely igazolja szakmai felkészültségünket és azt, hogy más vállalatok is bizalommal fordulhatnak hozzánk.

Telephelyek:

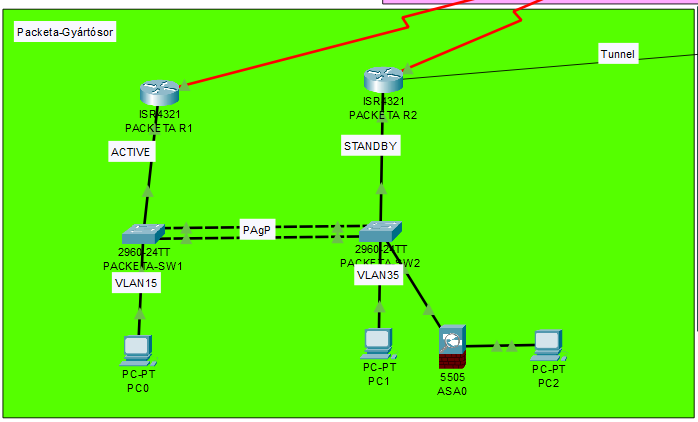
1. Fő telephely
2. WiFi telephely
3. Szerver telephely

# IP Cím tábla



# 1.0 Telephelyek

# 1.1 Packeta-Gyártósor (Fő hálózat)



Fő hálózatunk (Packeta-Gyártósor) több fajta technológiával van ellátva:

* **HSRP**
* **EtherChannel**
* **Portbiztonság**
* **GRE alagút**
* **DHCP**
* **VLAN-ok**

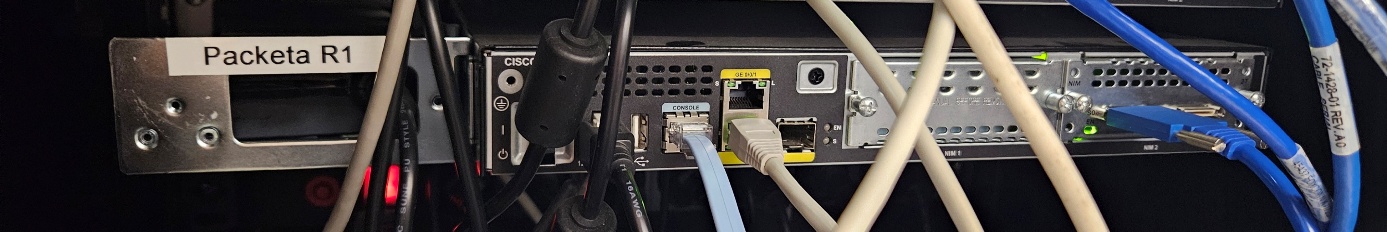
A telephelyen használt eszközök:

* 2 db 4221-es router
* 2 db 1000-es switch
* 6 db végeszköz

## 1.2 Alapbeállítások (SSH)

Az SSH (Secure Shell) egy olyan biztonságos hálózati protokoll, amely titkosított csatornán keresztül teszi lehetővé távoli gépek elérését és irányítását. Leggyakrabban rendszergazdák használják szerverek távoli kezelésére és konfigurálására, mivel megbízható védelmet nyújt az adatoknak az illetéktelen hozzáféréssel szemben.

### 1.3 Packeta R1



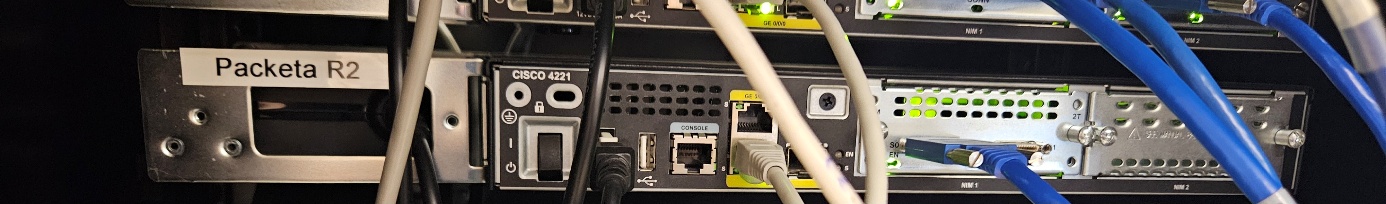
Alap beállítások:

* Hostname: R1
* Privilegizált jelszó:
* Konzol jelszó:

SSH:

* Crypto kulcs: 1024
* Domain név: PACKETA.LOCAL
* User: admin
* Password: Passw.rd
* line vty 0 4: login local | transport input ssh

### 1.4 Packeta R2



Alap beállítások:

* Hostname: R2
* Privilegizált jelszó:
* Konzol jelszó:

SSH:

* Crypto kulcs: 1024
* Domain név: PACKETA.LOCAL
* User: admin
* Password: Passw.rd
* line vty 0 4: login local | transport input ssh

### 1.5 Packeta-SW1



Alap beállítások:

* Hostname: SW1
* Privilegizált jelszó:
* Konzol jelszó:

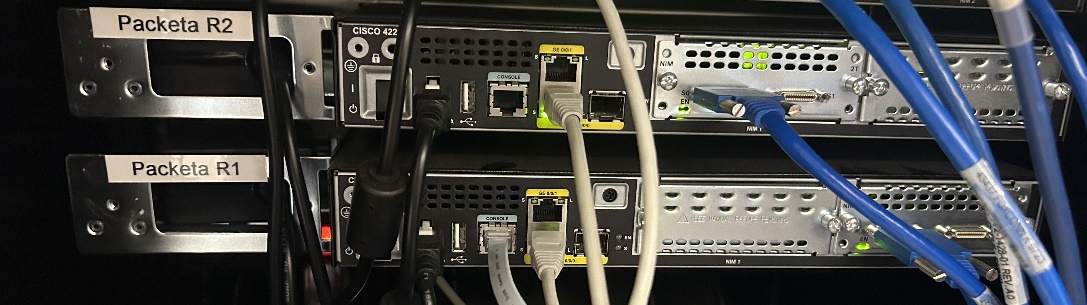
### 1.6 Packeta-SW2



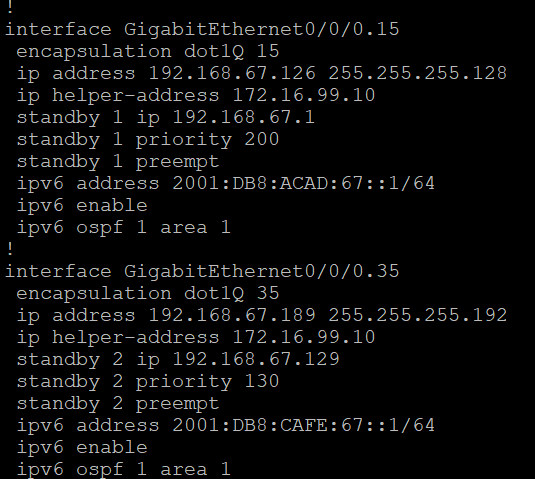
Alap beállítások:

* Hostname: SW2
* Privilegizált jelszó:
* Konzol jelszó:

## 1.8 HSRP beállítások



A HSRP (Hot Standby Router Protocol) egy Cisco által fejlesztett redundancia protokoll, amely biztosítja, hogy egy hálózatban mindig elérhető legyen az alapértelmezett átjáró. Több router egy virtuális IP-címet és MAC-címet oszt meg, ahol az egyik aktív, a másik pedig készenléti (standby) állapotban van. Ha az aktív router meghibásodik, a standby router automatikusan átveszi a szerepét, így a hálózati kapcsolat megszakítás nélkül működik tovább.

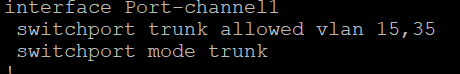


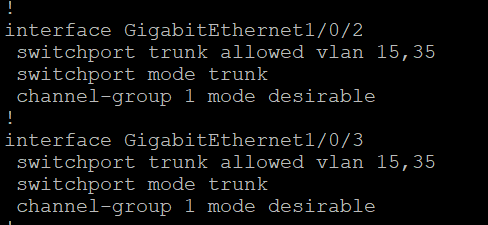
A HSRP (Hot Standby Router Protocol) egy Cisco által fejlesztett redundancia protokoll, amely biztosítja, hogy egy hálózatban mindig elérhető legyen az alapértelmezett átjáró. Több router egy virtuális IP-címet és MAC-címet oszt meg, ahol az egyik aktív, a másik pedig készenléti (standby) állapotban van. Ha az aktív router meghibásodik, a standby router automatikusan átveszi a szerepét, így a hálózati kapcsolat megszakítás nélkül működik tovább.

## 1.9 Etherchannel beállításai



Az EtherChannel egy olyan technológia, amely több fizikai hálózati kapcsolatot egyetlen logikai csatornává fog össze. Előnye, hogy növeli a sávszélességet és a redundanciát, mivel a forgalom megoszlik a linkek között, és egy kábel kiesése esetén is működőképes marad a kapcsolat. Gyakran használják switchek vagy switch és router között a teljesítmény és megbízhatóság növelésére.





PAgP-t használtunk az LACP helyett, mert Cisco eszközök között egyszerűbb és automatikusan egyeztetett kapcsolatot biztosít.

## 1.10 VLAN

A VLAN (Virtual Local Area Network) egy logikai hálózati felosztás, amely lehetővé teszi, hogy egy fizikai hálózatot több, egymástól elkülönített hálózatra bontsunk. Használatával növelhető a biztonság és csökkenthető a felesleges broadcast forgalom. Gyakran alkalmazzuk a hálózat átláthatóbb, hatékonyabb és könnyebben kezelhető kialakításához.

Ezeket a VLANokat hoztuk létre a Packeta-SW1-en:

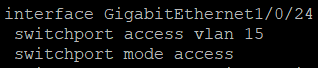
|  |  |  |
| --- | --- | --- |
| VLAN | Név | Használt portok |
| VLAN15 | Delutanos | G1/0/24 |
| VLAN35 | Ejszakas | Ezen az eszközön nem használtuk |
| VLAN99 | Szemetes | Minden nem használt port |

Packeta-SW2-n a következő VLANok lettek létrehozva:

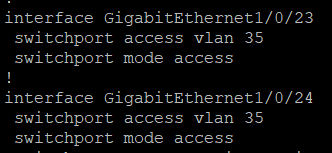
|  |  |  |
| --- | --- | --- |
| VLAN | Név | Használt portok |
| VLAN15 | Delutanos | Ezen az eszközön nem használtuk |
| VLAN35 | Ejszakas | G1/0/23,G1/0/24 |
| VLAN999 | Szemetes | Minden nem használt port |

A VLANokat azért hoztuk létre hogy a fizikai hálózatot elküönített logikaihálózatra bontsuk ez lehetővé teszi hogy a dolgozóink külön hálózatot kapjanak ez növeli a biztonságot és áttekinthetőbb lesz.

Packeta-SW1-en VLAN porthoz rendelése:

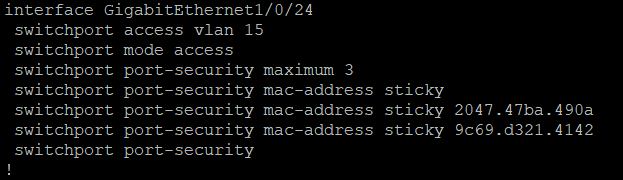


Packeta-SW2-n való porthoz rendelés:



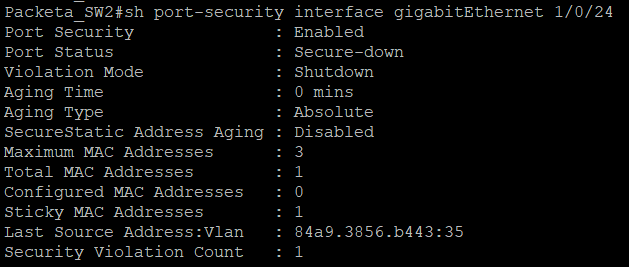
A VLANokat access módba tettük hogy utána hozzá adhassuk őket a VLANokhoz.

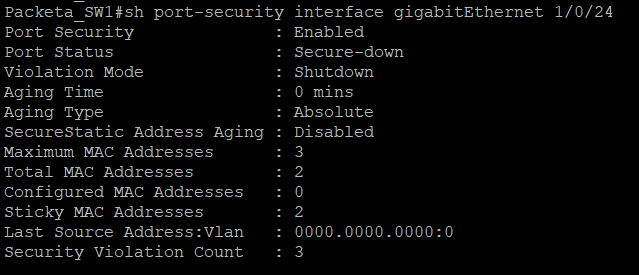
## 1.11 Port-Security

A port security egy olyan switch funkció, amely szabályozza, hogy egy adott portra milyen és hány eszköz csatlakozhat. Segítségével megakadályozható, hogy illetéktelen eszközök kerüljenek a hálózatba, ezáltal növeli a hálózat biztonságát. Ha a beállított szabályokat megsértik, a port automatikusan letiltható vagy korlátozható.



Látható hogy 3 külön mac-címet tud megtanulni a switch ha ezt a számot túllépné a port letiltásra kerül. A felső képen az látszik hogy azon az interfészen már 2 mac-címet megtanult szóval már csak 1 mac-címet képes megtanulni míg a másik még 2-t.





A megnézés idején a portok nem voltak használva azért van a Port Statusnál Secure-Down. Itt is írja hogy ha több mac-cím kerülne bele a mac-cím táblába a port lekapcsolásra kerül és csak egy addig már megtanult mec-címmel rendelkező eszköz tudja visszakapcsolni.

## 1.12 GRE Alagút

A GRE Tunnel (Generic Routing Encapsulation) egy alagút-technológia, amelyet Linux rendszerekben is gyakran használnak különálló hálózatok összekapcsolására egy IP-hálózaton keresztül. A GRE lehetővé teszi, hogy különböző protokollokat és teljes hálózati csomagokat „becsomagolva” továbbítsunk két végpont között, mintha azok közvetlen kapcsolatban lennének. Gyakran alkalmazzák VPN-megoldások alapjaként, belső hálózatok összekötésére vagy routing-szcenáriók megvalósítására, azonban önmagában nem biztosít titkosítást, ezért biztonságos kommunikációhoz általában IPsec-cel együtt használják.

## 

## 1.13 OSPF

Az OSPF egy dinamikus útvonalválasztó protokoll, amely automatikusan megosztja a hálózati útvonalakat a routerek között. Segítségével a hálózat gyorsan alkalmazkodik a változásokhoz, például egy kapcsolat megszakadásához, és mindig a legjobb útvonalat választja ki. Az OSPF nagyobb hálózatokban is jól használható, mert hatékony és megbízható működést biztosít.

### 1.14 PacketaR1

* RouterID: 1.1.1.1
* Folyamatazonosító: 10
* Area: 0
* Hálózatok: 192.168.67.0

192.168.67.128

10.10.10.8

### 1.15 PacketaR2

* RouterID: 2.2.2.2
* Folyamatazonosító: 10
* Area: 0
* Hálózatok: 192.168.67.0

192.168.67.128

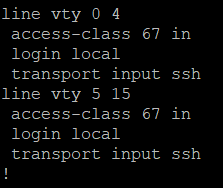
10.10.10.0

Megadtuk nekik a saját ismert hálózataikat hogy hirdessék őket. Areaból a nullásat használtuk mivel ez az alapértelmezett area.

## 1.16 Normál ACL

A normál ACL-t azért használtuk, hogy szabályozzuk, mely eszközök férhetnek hozzá a hálózati eszközhöz SSH kapcsolaton keresztül. Az ACL csak a forrás IP-címet vizsgálja, így egyszerűen megadható, hogy melyik gép vagy hálózat csatlakozhat. Ez növeli a biztonságot, mert megakadályozza az illetéktelen távoli bejelentkezést.

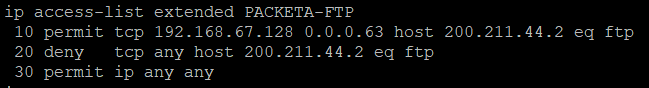


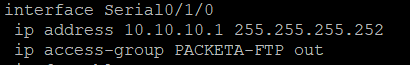


Ezzel azt eredményeztük hogy csak a 67.0-ás hálózat tudjon SSH-val felkapcsolódni a routerekre ennek magyarázata hogy csak a délutánban dolgozó dolgozóknak szükséges a munkájukhoz hogy elérjék a routereket.

## 1.17 Kiterjesztett ACL

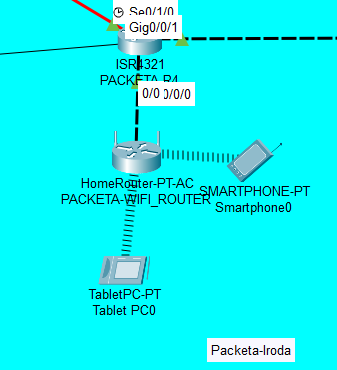
A kiterjesztett ACL-t azért használtuk, hogy pontosan szabályozzuk, mely eszközök érhetik el az FTP szervert. Ez az ACL nemcsak a forrás IP-címet, hanem a célcímet és a használt szolgáltatást (FTP) is figyeli, így csak az engedélyezett gépek férhetnek hozzá a szerverhez. Ezzel növeltük a hálózat biztonságát és megakadályoztuk az illetéktelen hozzáférést.

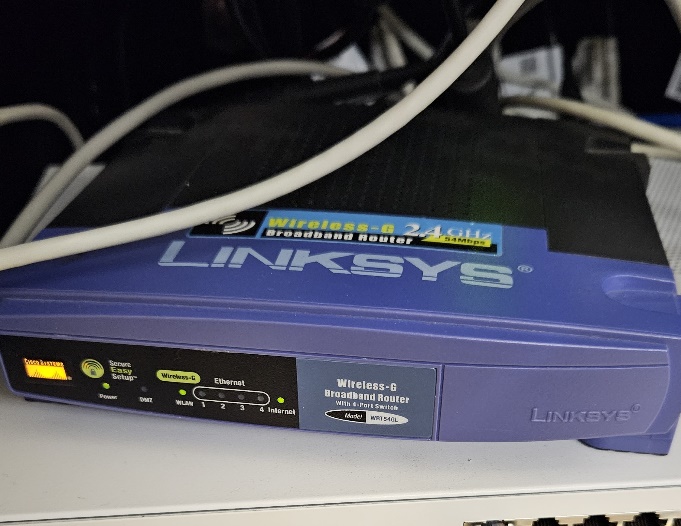




A kiterjeszett ACL a Linux szerverünkön lévő FTP szerverre vonatkozik mivel arra a szerverre NATolva is van ezért az ACL szabályoknál a publikus IP címét használtuk. Látható hogy csak a 67.128-as hálózatot azaz az éjszakás dolgozókat engedi elérni FTP-n keresztül mindenki mást tilt róla de enged minden mást. Ez azért így lett megoldva mivel a délutános műszakban dolgozók munkájához nem szükséges FTP-t használni ezzel is növeltük a hálózat biztonságát. Ezt minden ezen a telephelyen használt routeren megadtuk.

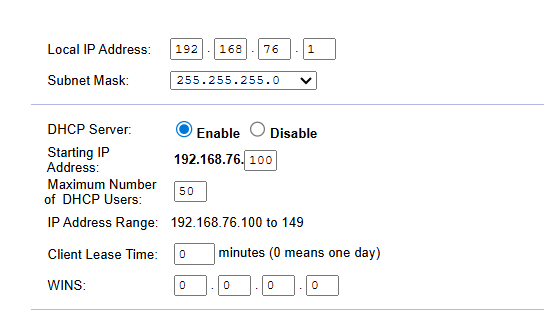
# 2.0 Packeta Iroda telephely





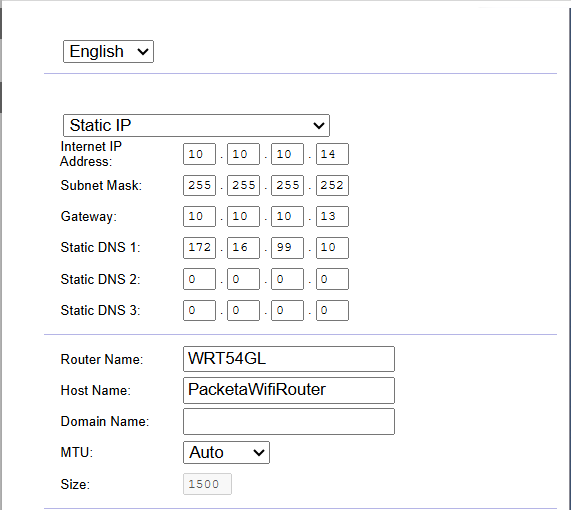
## 2.1 LAN hálózat

A LAN (Local Area Network) egy kisebb földrajzi területet, például egy irodát vagy épületet lefedő hálózat, amely lehetővé teszi az eszközök gyors és hatékony adatcseréjét.



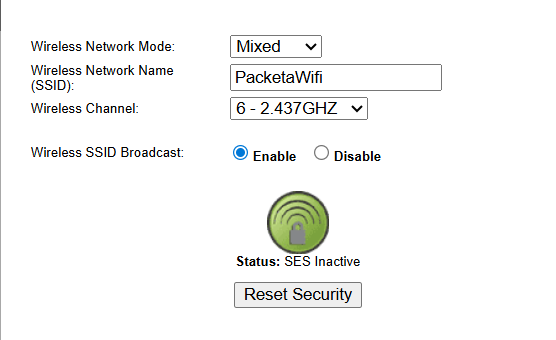
## 2.2 WAN hálózat

A WAN (Wide Area Network) olyan kiterjedt hálózat, amely nagy földrajzi területeket fed le, és lehetővé teszi az egymástól távol elhelyezkedő eszközök és rendszerek közötti adatcserét. Gyakran alkalmazzák vállalatok központi irodái és távoli telephelyei közötti kommunikációra, valamint internetkapcsolat biztosítására.



## 2.3 SSID

Az SSID (Service Set Identifier) egy vezeték nélküli hálózat egyedi azonosítója, amely megkülönbözteti azt más Wi-Fi hálózatoktól. Segítségével a felhasználók azonosítani és kiválasztani tudják a kívánt hálózatot, amelyhez csatlakozni szeretnének.



## 2.4 SECURITY

A vezeték nélküli hálózat biztonsági beállításai a hálózathoz való hozzáférést és az adatforgalom védelmét szabályozzák. A WPA2-Personal jelszóval védi a hálózatot, míg a titkosítási algoritmusok biztosítják az adatok biztonságos továbbítását.



## 2.6 Statikus NAT

A statikus NAT (Network Address Translation) egy olyan címfordítási eljárás, amely során egy belső, privát IP-címhez egy állandó, nyilvános IP-cím van hozzárendelve. Ez lehetővé teszi, hogy a belső hálózaton lévő eszközök kívülről is elérhetők legyenek, miközben a belső IP-címek rejtve maradnak.

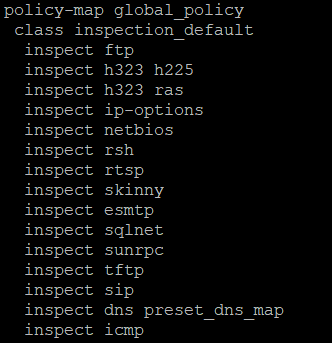


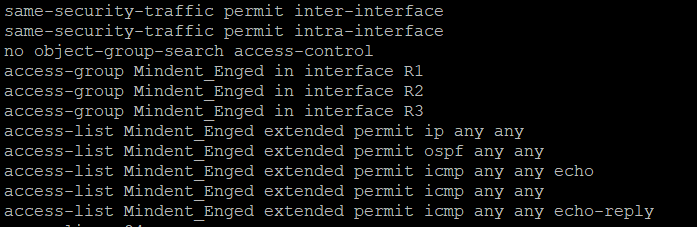
A Linux szerver felé alkalmazott statikus NAT azért szükséges, mert ez a rendszer konkrét, előre meghatározott hálózati kapcsolatokban vesz részt, ahol a belső és külső IP-címek egyértelmű és állandó megfeleltetése elvárás. A statikus NAT biztosítja, hogy a forgalom mindig kiszámítható módon, ugyanazon az útvonalon és címzésen keresztül érje el a szervert.

Más eszközök esetében nincs szükség NAT alkalmazására, mivel azok nem igényelnek külső–belső címfordítást, vagy kizárólag olyan hálózati szegmensekben kommunikálnak, ahol a címzés közvetlenül megoldott. A statikus NAT célzott használata így az átlátható forgalomkezelést, a stabil működést és a könnyebb hibakeresést szolgálja.

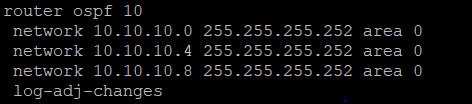
# 2.7 Tűzfal mint forgalom irányító

A tűzfal mint forgalomirányító nemcsak a hálózati biztonságot biztosítja, hanem az adatforgalom irányításában is kulcsszerepet játszik. Szabályok alapján dönti el, hogy az egyes hálózati csomagok mely irányba haladhatnak tovább, mely kapcsolatok engedélyezettek vagy tiltottak, illetve hogyan történjen a belső és külső hálózatok közötti adatáramlás. Ennek köszönhetően a tűzfal egyszerre lát el védelmi és irányítási feladatokat, biztosítva a hálózat biztonságos és hatékony működését.





a



Tűzfalat fő forgalomirányítóként használtuk ennek az az oka hogy 8db GigabitEthernetes portja van ezzel nő a hálózatunk sebessége.

## 2.8 Dinamikus NAT (PAT)

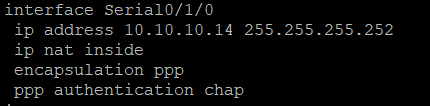
Az **internet felé irányuló PAT (Port Address Translation)** célja, hogy a belső hálózat több eszköze **egy közös publikus IP-címen keresztül** tudjon kifelé kommunikálni. A PAT a forrásportok módosításával különbözteti meg az egyes kapcsolatokat, így hatékonyan kihasználható a rendelkezésre álló publikus cím.



A PAT-ot az internet felé csináltuk a PacketaR4-en. Az internet csak szimulációs jelleggel volt egy kinevezett internet PC-vel mivel rendesen nem mentünk ki az internetre.

## 2.9 WAN Kapcsolat (PPP)

A **PPP (Point-to-Point Protocol)** egy adatkapcsolati rétegben működő protokoll, amelyet két hálózati végpont közötti kapcsolat létrehozására használnak, jellemzően szolgáltatói vagy WAN-kapcsolatok esetén. A PPP feladata a kapcsolat felépítése, konfigurálása, az adatok továbbítása, valamint a kapcsolat felügyelete.



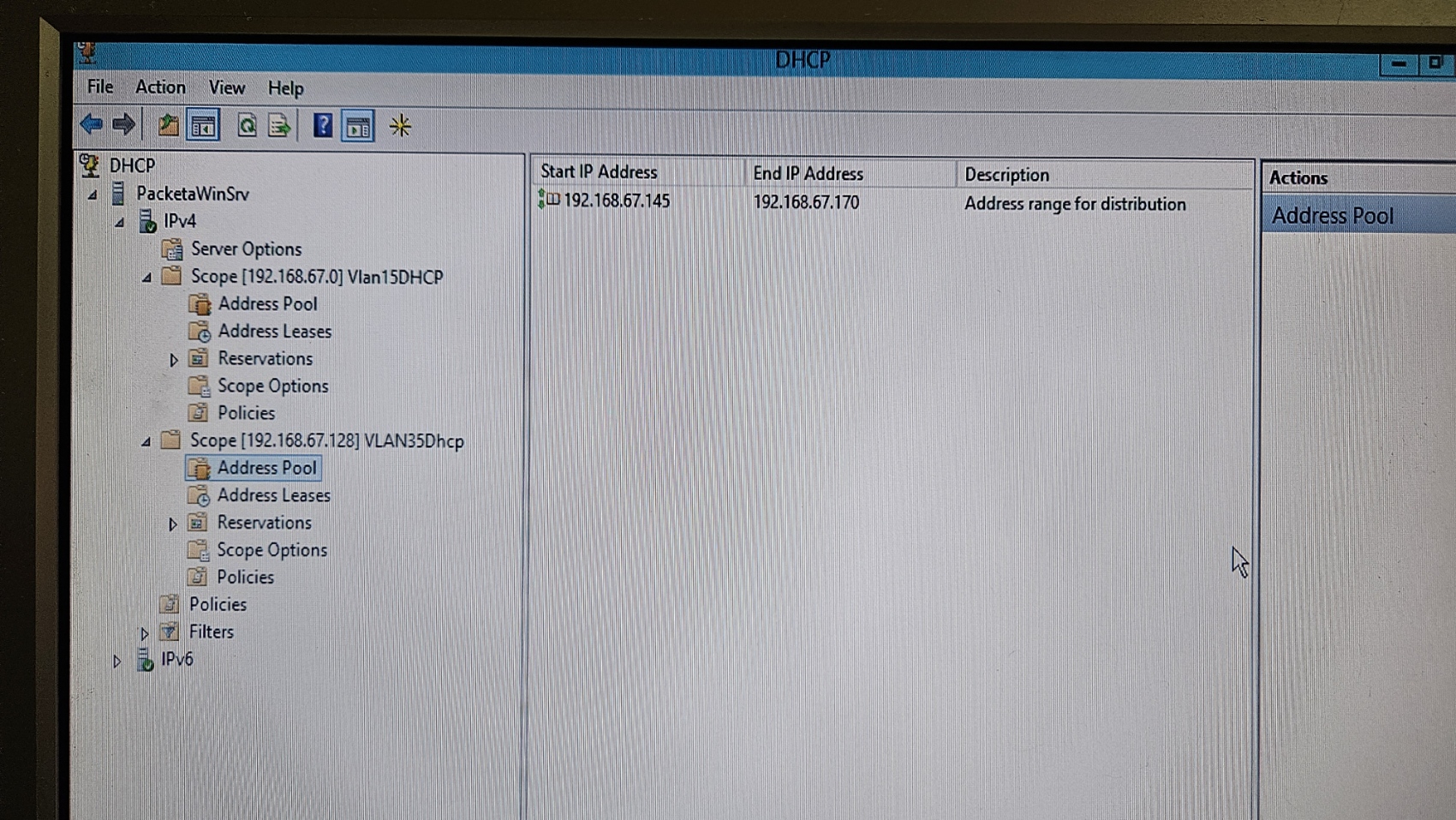
PPP kapcsolat a PacketaR3 és a PacketaR4 között található. Látható hogy adtunk egy felhasználó nevet és jelszót amelynek neve a másik router neve. Az alatt pedig az látható hogy a serial porton engedélyeztük a PPP-t és beállítottuk chap-ra mivel sokkal biztonságosabb mint a pap.

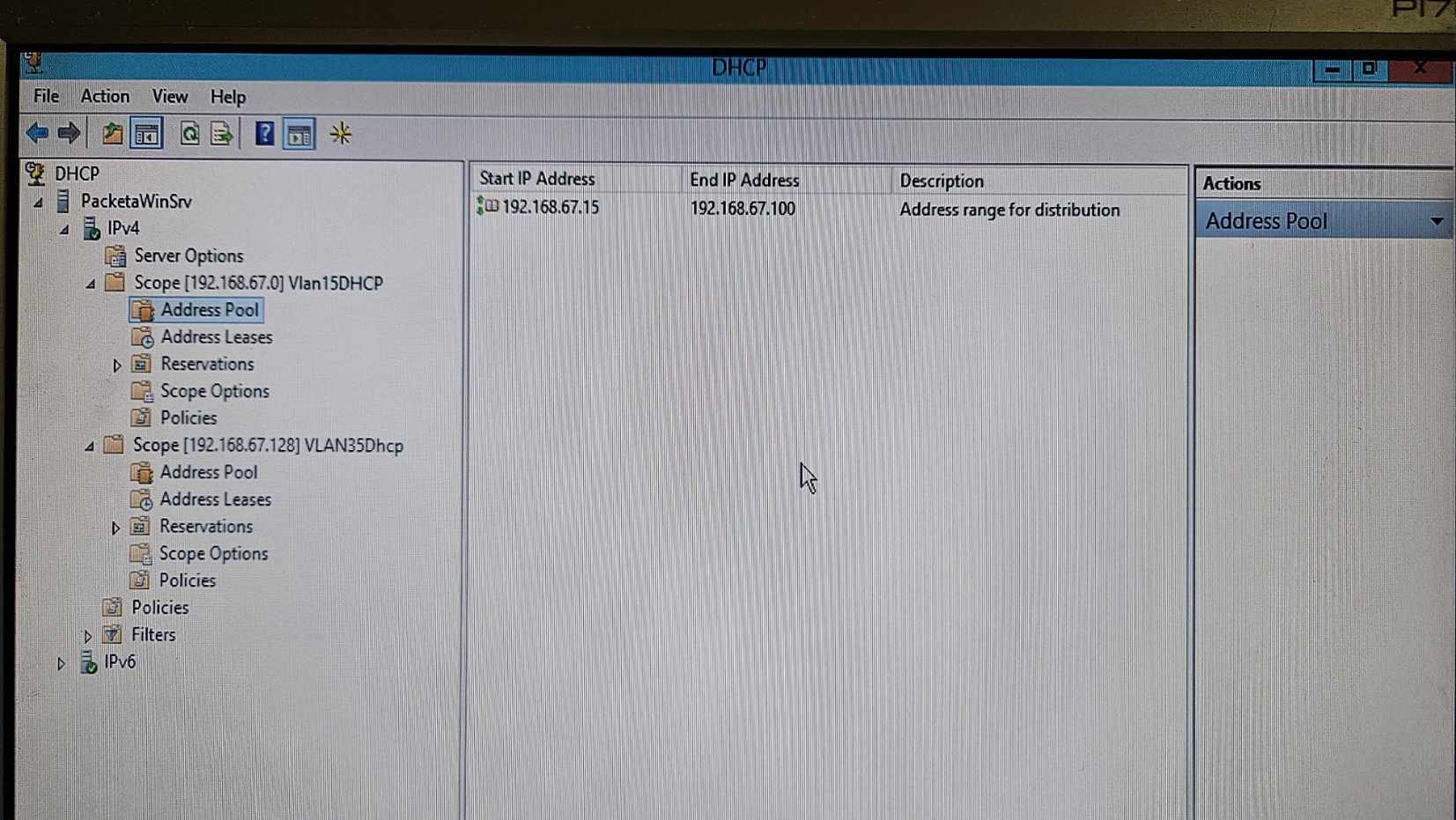
# 3.0 Szerver telephely

## 3.1 Windows Szerver

### 3.2 DHCP Szerver

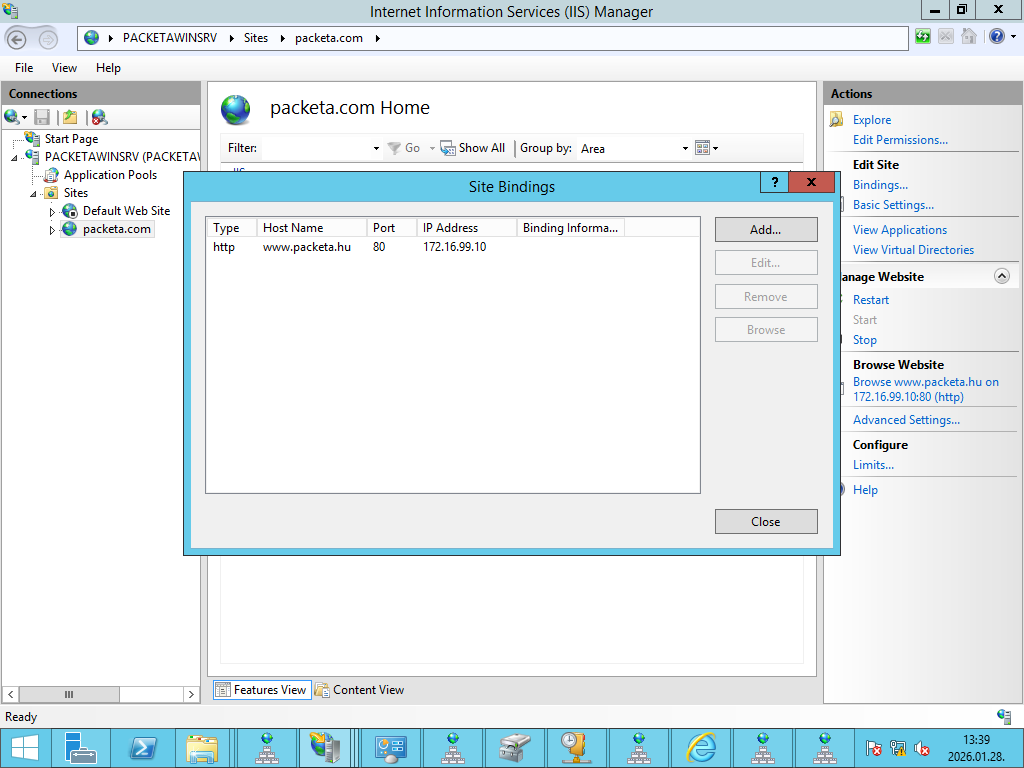
A Windows Server DHCP (Dynamic Host Configuration Protocol) szerepköre képes központosított IP-cím menedzsmentet biztosítani szegmentált hálózati környezetekben (VLAN-ok) is. Ebben a felállásban egyetlen fizikai vagy virtuális szerver képes kiszolgálni több, logikailag elkülönített alhálózatot, anélkül, hogy minden egyes VLAN-ba külön DHCP szervert kellene telepíteni.

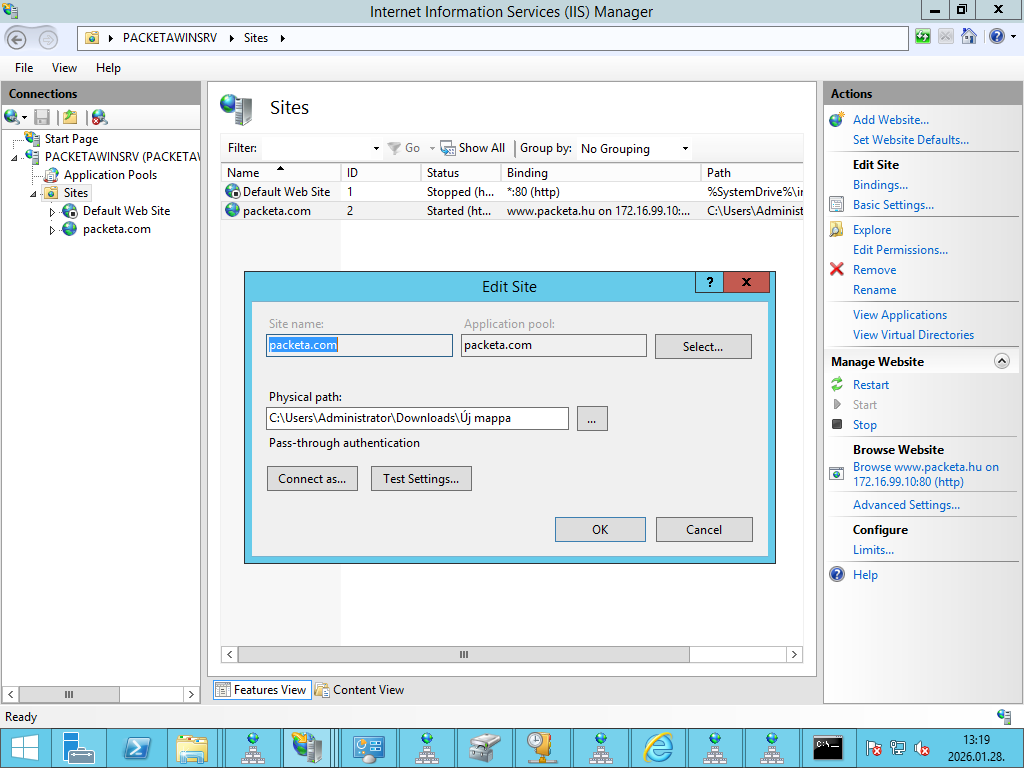




A két Scoope a két VLANunkat szolgálja ki IP címmel a routereken az alinterfészekre helper-addresst adtunk meg.

### 3.3 Web Szerver (IIS)

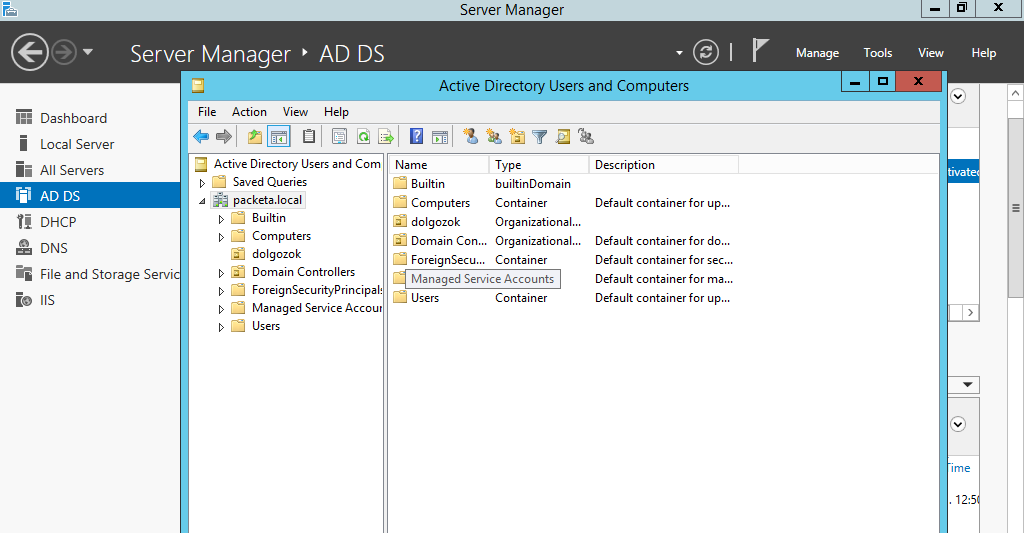
Az Internet Information Services (IIS) a Microsoft Windows Server operációs rendszerek rugalmas, biztonságos és bővíthető webkiszolgáló (Web Server) szerepköre. Elsődleges feladata weboldalak, webes alkalmazások (pl. ASP.NET, PHP) és szolgáltatások hosztolása, valamint tartalmak kiszolgálása HTTP, HTTPS, FTP, FTPS és SMTP protokollokon keresztül.

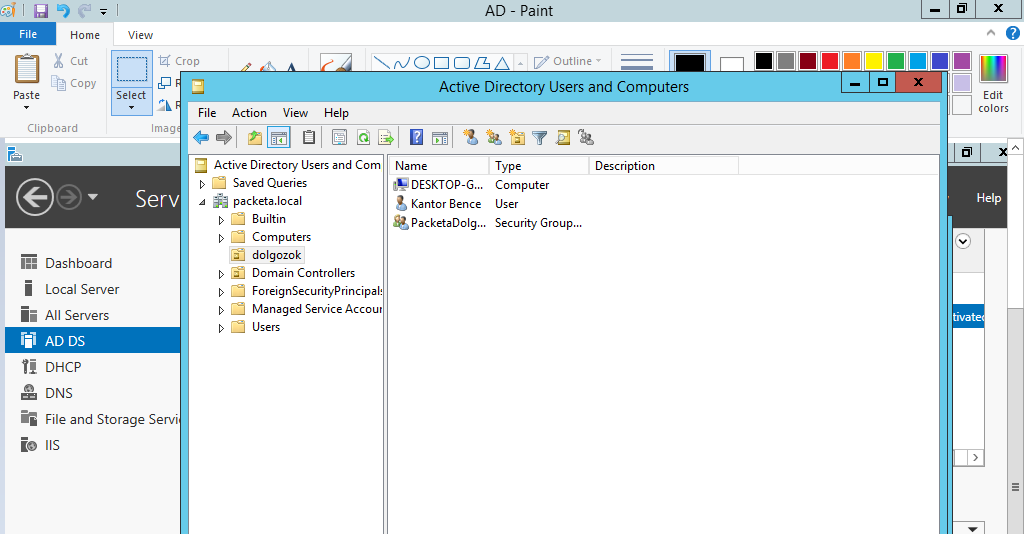


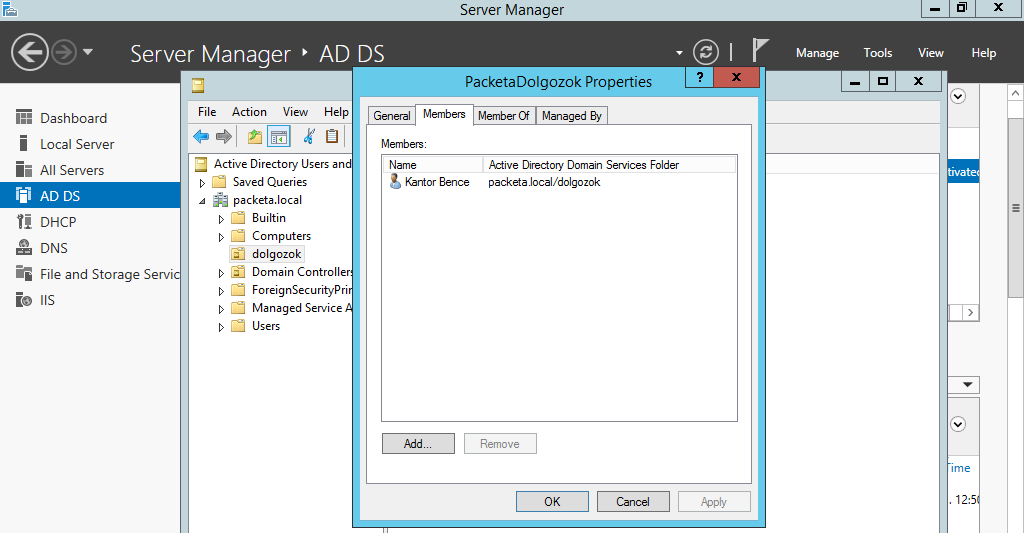
A Weboldalt HTTP-n keresztül érjük el a [www.packeta.hu](https://www.packeta.hu) néven ezt a nevet a DNS adja.

### 3.4 Active Directory

Az Active Directory (AD) a Microsoft által kifejlesztett címtárszolgáltatás, amely a Windows-alapú hálózatok „agyaként” funkcionál. Segítségével a rendszergazdák egyetlen központi felületen kezelhetik a felhasználókat, számítógépeket, jogosultságokat és egyéb erőforrásokat.



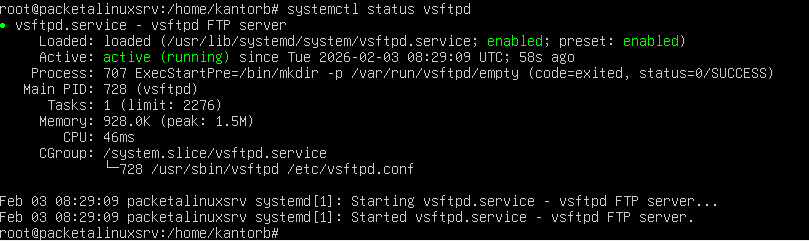
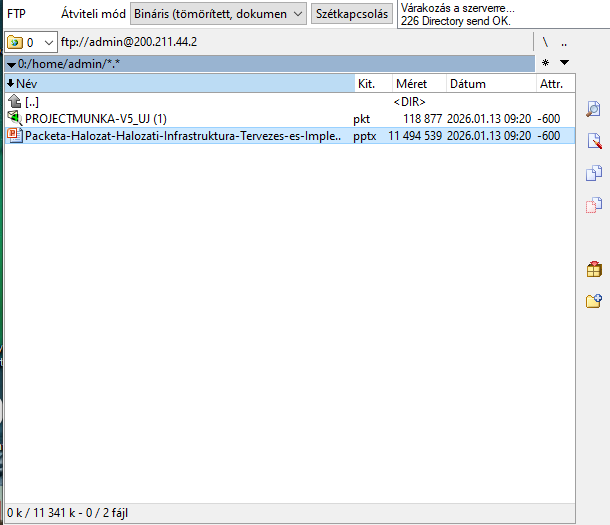




## 3.5 Linux Szerver

### 3.6 FTP Szerver

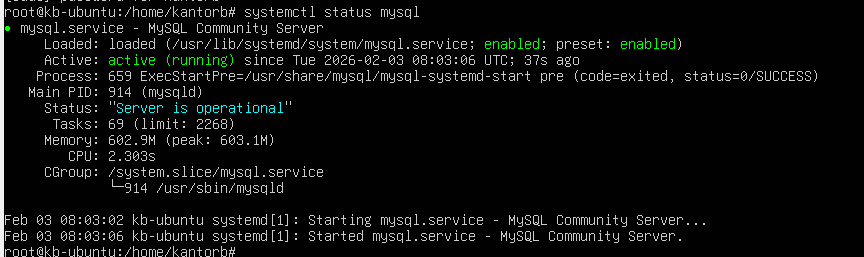
A VSFTPD a Unix-alapú rendszerek legbiztonságosabbnak tartott fájlátviteli kiszolgálója, amelynek szoftveres architektúrája kifejezetten a sebezhetőségek minimalizálására és a nagy teljesítményű kiszolgálásra épül.



Egy Admin felhasználót hoztunk létre és itt tároljuk a projektunk adatait.

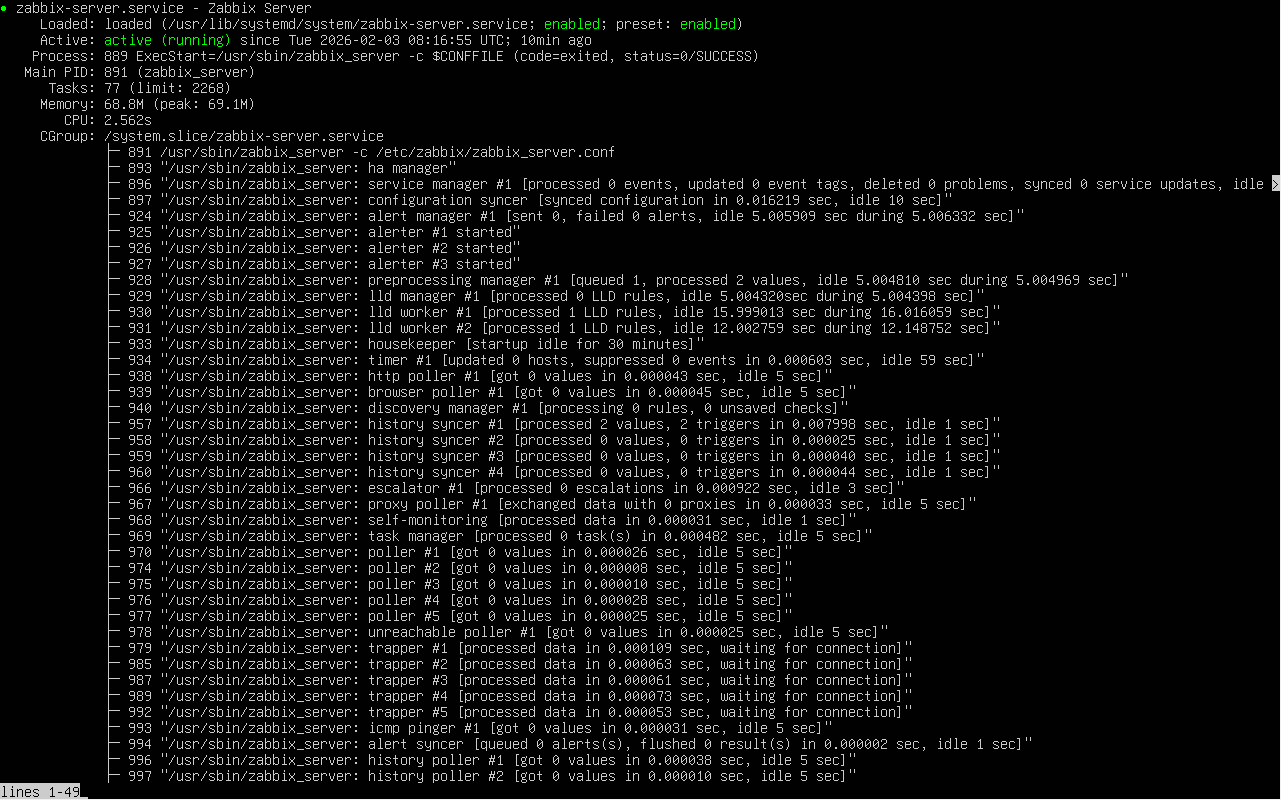
### 3.7 Adatbázis Szerver (MySQL)

A MySQL Server a világ egyik legelterjedtebb, nyílt forráskódú relációs adatbázis-kezelő rendszere (RDBMS), amely kliens-szerver architektúrában végzi a strukturált adatok tárolását, rendszerezését és kiszolgálását.

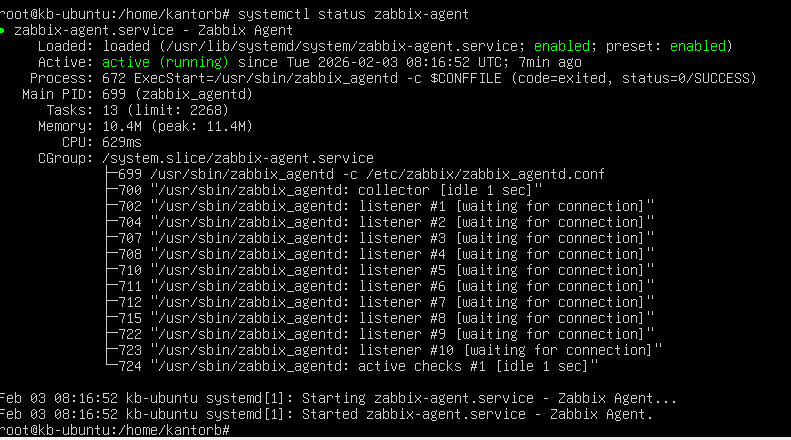
Az adatbázis szerveren vannak tárolva a cégnél dolgozó emberek adatai. Az adatbázis szerver az irodában található ahol a rendszergazda is tartózkodik és ő módosítja és tárolja az adatokat.

### 3.8 Monitoring Szerver (Zabbix)

A **Zabbix** egy nyílt forráskódú monitorozó rendszer, amelyet Linux környezetben gyakran használnak szerverek, hálózati eszközök, alkalmazások és szolgáltatások állapotának folyamatos figyelésére. Segítségével valós időben nyomon követhetők az erőforrás-használati adatok (CPU, memória, tárhely), valamint automatikus riasztások küldhetők hibák vagy rendellenességek esetén. A Zabbix központi szerver–agent architektúrára épül, webes felületen keresztül menedzselhető, és jól skálázható kisebb rendszerektől nagyvállalati környezetekig.

Zabbix-server:

Zabbix-agent:



A zabbix monitorozó szervert arra használjuk hogy nyomon tudjuk követni az esetleges szerver hibákat és minél kisebb legyen az állás idő. A Zabbix szerverünk az iroda telephelyen található a rendszergazda innen tudja monitorozni a hálózat szervereit.

## Windows Backup Server

