

**Informatikai rendszer- és
alkalmazás-üzemeltető technikus
projektfeladat**

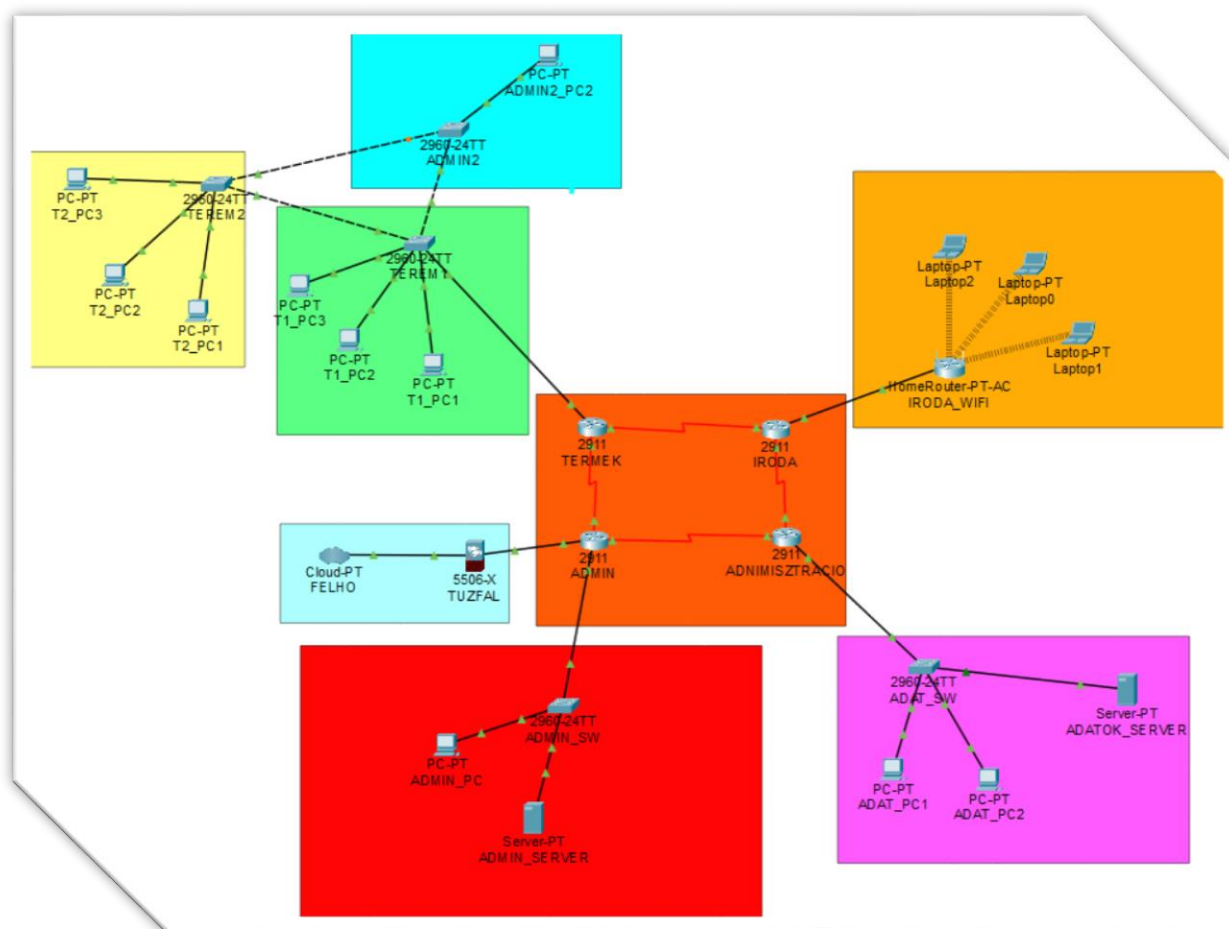
**Hálózat tervezési
dokumentáció**

Gacsal Ákos	2/14_IR
Lénárt Zsolt	
Kádár Zsolt	

A feladatunk egy összetett hálózat kiépítése volt az alábbi szempontok alapján:

- a hálózati infrastruktúrának legalább 3 telephelyet vagy irodát kell lefednie
- legalább egy telephelyen több VLAN kialakítását foglalja magában
- tartalmaz második és harmadik rétegbeli redundáns megoldásokat
- IPv4 és IPv6 címzési rendszert egyaránt használ
- Vezeték nélküli hálózatot is tartalmaz
- statikus és dinamikus forgalomirányítást egyaránt megvalósít
- statikus és dinamikus címfordítást alkalmaz
- WAN-összeköttetéseket is tartalmaz
- virtuális magánhálózati kapcsolatot (VPN) is megvalósít
- programozott hálózatkonfigurációt is használ
- forgalomirányítón megvalósított biztonsági funkciókat tartalmaz (pl. ACL-ek)
- hardveres tűzfaleszközt is alkalmaz
- Minimum 1-1 Linux és Windows kiszolgálót tartalmaz, melyek legalább az alábbi szolgáltatásokat nyújtják:
 - Címtár (pl. Active Directory)
 - DHCP

A mi csapatunk egy iskolai hálózatott tervezet amit az alábbi képpen oldottunk meg:



5 fő szegmensre osztottuk a hálózatot, amik az alábbiak:

- ❖ **Telephelyek**
- ❖ **Admin**
- ❖ **Adminisztráció**
- ❖ **Iroda**
- ❖ **Termek**

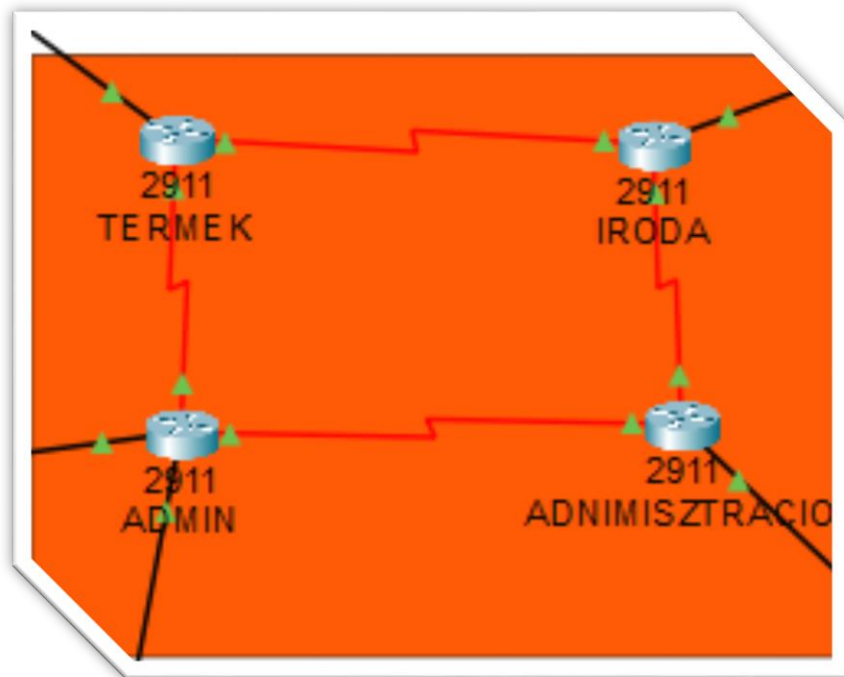
IP-cím kiosztás

Az alábbi IP-címeket használtunk a feladat megoldásához.

TELEPHELYEK	PORT NUMBER	IP ADDRESS	SUBNET MASK	DEFAULT GATEWAY	DEVICE NAME	
TERMEK	0/3/0	10.0.0.1			TEREM_ROUTER	
	0/3/1	20.0.0.1			TEREM_ROUTER	
	GIG/0	192.168.10.1	255.255.255.192		TEREM_ROUTER	
TEREM1	FA0/2	192.168.10.10	255.255.255.192	192.168.10.1	T1_PC1	
	FA0/3	192.168.10.20	255.255.255.192	192.168.10.1	T1_PC2	
	FA0/4	192.168.10.30	255.255.255.192	192.168.10.1	T1_PC3	
TEREM2	FA0/2	192.168.10.70	255.255.255.192	192.168.10.1	T2_PC1	
	FA0/3	192.168.10.80	255.255.255.192	192.168.10.1	T2_PC2	
	FA0/4	192.168.10.90	255.255.255.192	192.168.10.1	T2_PC3	
ADMIN2	FA0/3	192.168.10.130	255.255.255.192	192.168.10.1	ADMIN2_PC2	
		192.168.10.140	255.255.255.192	192.168.10.1	ADMIN2_SW	
Admin	0/3/1	20.0.0.2			ADMIN_ROUTER	
	0/3/0	30.0.0.1			ADMIN_ROUTER	
	GIG1/1	192.168.60.2	255.255.255.0		TÜZFAL	
Admin	GIG0/1	192.168.60.1	255.255.255.0		ADMIN_ROUTER	TÜZFAL
	GIG0/0	192.168.20.1	255.255.255.0		ADMIN_ROUTER	
	FA0/2	192.168.20.10	255.255.255.0	192.168.20.1	ADMIN_PC	
	FA0/3	2001:DB8:ABCD::1			ADMIN_SERVER	
	FA0/3	192.168.20.20	255.255.255.0	192.168.20.1	ADMIN_SERVER	
ADMINISZTRÁCIÓ	0/3/1	40.0.0.1				
	0/3/0	30.0.0.2				
	GIG0/0	192.168.30.1	255.255.255.0		ADMINI_ROUTER	
	FA0/2	DHCP	255.255.255.0	192.168.30.1	ADAT_PC1	
	FA0/3	DHCP	255.255.255.0	192.168.30.1	ADAT_PC2	
	FA0/4	DHCP	255.255.255.0	192.168.30.1	ADATOK_SERVER	
IRODA	0/3/1	40.0.0.2			IRODA_ROUTER	
	0/3/0	10.0.0.2			IRODA_ROUTER	DHCP POOL AD1
	GIG0/0	192.168.40.1	255.255.255.0		IDODA_WIFI	
IRODA	Wireless	192.168.40.2	255.255.255.0	192.168.40.1	DHCP	
	Wireless	192.168.50.1	255.255.255.0	192.168.40.2		WPA2PERSONAL

Telephelyek

A hálózati infrastruktúra tervezésekor és implementálásakor több kritikus szempontot kellett figyelembe venni, hogy biztosítsuk a hatékony, biztonságos és skálázható működést. Az alábbiakban részletezzük a választott konfigurációt, annak előnyeit, valamint a biztonsági és funkcionálitási szempontokat.



WAN-kommunikáció és OSPF használata

Az iskola négy routerből álló hálózatában az OSPF nevű útválasztási rendszert használjuk, mert ez biztosítja a gyors és megbízható adatáramlást az egyes telephelyek között.

Az OSPF előnyei:

Gyors reagálás ha egy kapcsolat megszakad vagy megváltozik, a rendszer gyorsan új útvonalat keres az adatok számára, így elkerülhetők a hosszabb leállások.

Kevesebb hálózati terhelés az OSPF csak a szükséges információkat küldi el a hálózatban, így csökkenti a felesleges adatforgalmat és növeli a rendszer hatékonyságát.

A hálózat tervezésekor a statikus és dinamikus útválasztás kombinációját alkalmaztuk, hogy biztosítsuk a megbízható, gyors és biztonságos adatáramlást az egyes telephelyek között.

Az alábbiakban részletesen kifejtjük, miért volt szükség mindkét megoldásra, és milyen előnyökkel jár az Önök vállalatának.

Speciális hálózati szegmensek védelme – Bizonyos szerverek vagy érzékeny adatok védelme érdekében az útvonalakat manuálisan állítottuk be, hogy ne legyenek elérhetőek minden eszköz számára.

- ❖ Biztonsági megfontolások – Egyes érzékeny adatforgalmat nem engedtünk át a dinamikus útválasztási rendszerbe, hogy elkerüljük az illetéktelen hozzáféréseket.
- ❖ Alternatív útvonalak vészhelyzet esetére – Ha az OSPF alapú útválasztás valamilyen hiba miatt nem működne, a statikus útvonalak biztosítják, hogy az alapvető kapcsolatok továbbra is működjenek.

Ezeknek az előnyöknek köszönhetően a különböző telephelyek közötti kommunikáció zavartalan, gyors és hatékony, ami elengedhetetlen a stabil működéshez.

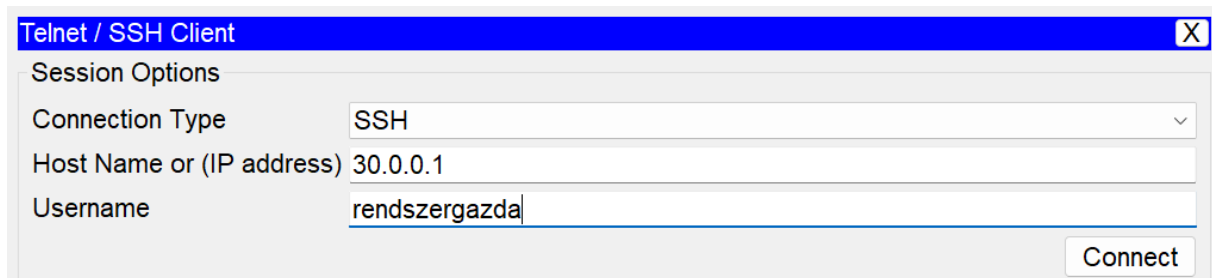
A WAN titkosítás során a CHAP használata növeli a kapcsolat biztonságát, mert a jelszót nem küldi ki nyílt szöveggént, folyamatos hitelesítést biztosít, és megakadályozza az adatlopásra irányuló támadásokat. Ezáltal a hálózat megbízhatóbb és ellenállóbb lesz a biztonsági fenyegetésekkel szemben.

A routerek között állítottunk clock ratet az adat kommunikáció megvalósításához.

Az SSH használata az összes routeren az ADMIN számára biztonságos és hatékony megoldás a routerek távoli kezelésére.

Titkosítja a kapcsolatot, így megvédi a bejelentkezési adatokat és a konfigurációs parancsokat a lehallgatástól.

A kulcsalapú hitelesítés csökkenti a gyenge jelszavak kockázatát, és kizárólag engedélyezett eszközökről teszi lehetővé a hozzáférést.



Telnet / SSH Client

Session Options

Connection Type SSH

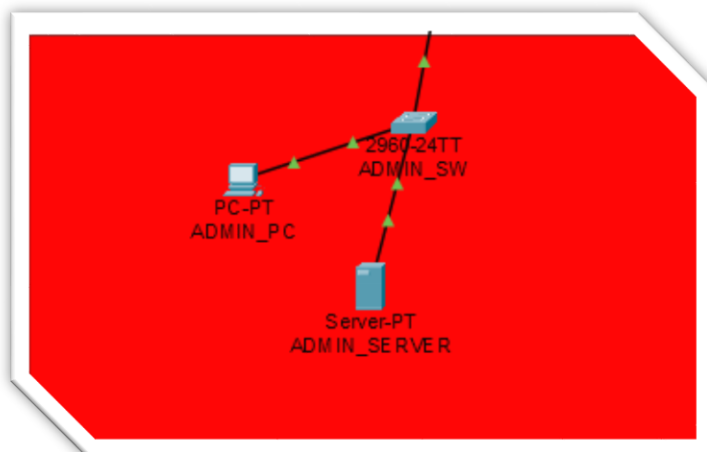
Host Name or (IP address) 30.0.0.1

Username rendszergazda

Connect

Admin

Az Admin Szoba egy lokális hálózat része, amely a vállalat belső adminisztratív eszközeinek kommunikációját biztosítja. A hálózat célja, hogy az adminisztrációs dolgozók számára gyors, megbízható és biztonságos kapcsolatot nyújtson a szükséges informatikai erőforrásokhoz.



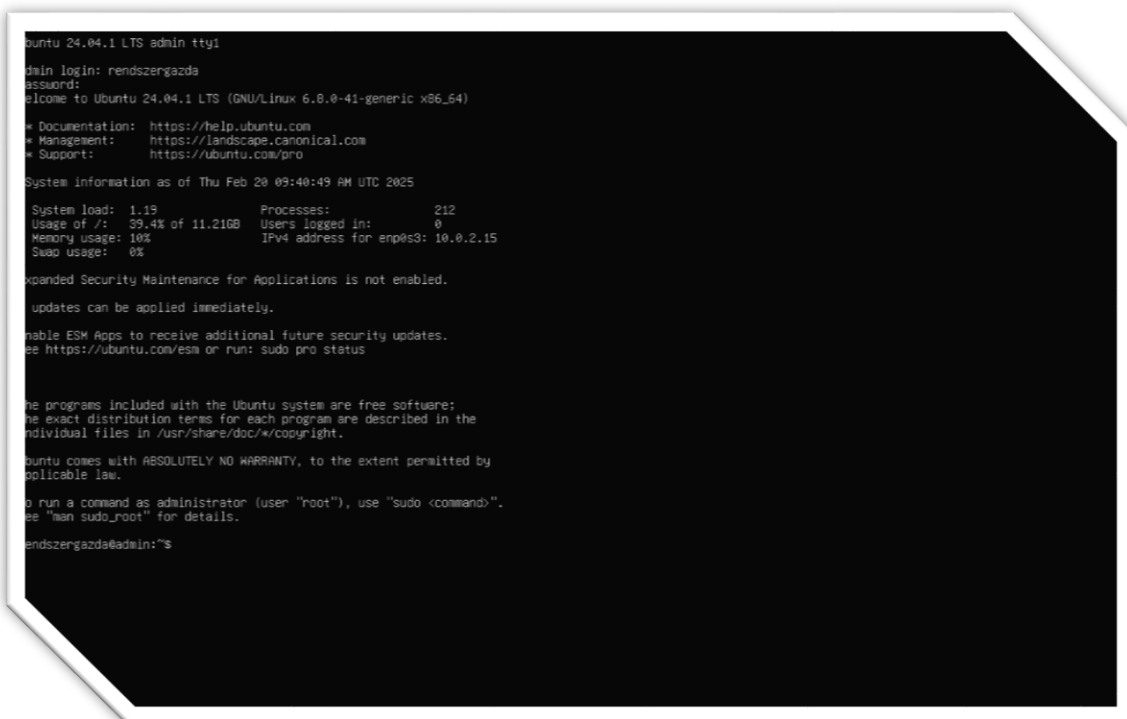
ADMIN_PC (PC-PT) – A rendszergazda által használt számítógép, amely csatlakozik a hálózathoz és hozzáfér a szerverhez.

```
interface "enp0s31f6";
fixed-address 192.168.2.248;
option subnet-mask 255.255.255.0;
option routers 192.168.2.254;
option dhcp-lease-time 7200;
option dhcp-message-type 5;
option domain-name-servers 192.168.2.254;
option dhcp-server-identifier 192.168.2.254;
option domain-name "sweet.home";
renew 1 2019/10/07 00:10:12;
rebind 1 2019/10/07 00:10:12;
expire 1 2019/10/07 00:10:12;
```

The image shows a terminal window with a dark background and white text, displaying the configuration for a DHCP client on the interface 'enp0s31f6'. The configuration includes a fixed IP address, subnet mask, default gateway, lease time, and domain name.

DHCP (Dynamic Host Configuration Protocol) konfiguráció látható egy Linux rendszerben, amely statikus IP-címet rendel egy hálózati interfészhez.

- ❖ A rendszergazdai számítógépre Linux operációs rendszert telepítettünk.
- ❖ A Linux és a Windows operációs rendszerek közötti választás nagyban függ attól, hogy milyen célra szeretnénk használni az adott rendszert.
- ❖ A mi esetünkben a megbízhatóság és a egyszerűség volt a fő szempont hiszen a Linux szervereket akár évekig lehet futtatni anélkül, hogy újra kellene indítani őket , jobban kezeli a memóriahasználatot és a többfeladatos működést, így kevésbé hajlamos a rendszerösszeomlásra.
- ❖ ADMIN_SERVER (Server-PT) – Egy dedikált szerver, amely tartalmazza a vállalat belső adatbázisait, fájlmegosztását.



```
ubuntu 24.04.1 LTS admin tty1
admin login: rendszergazda
password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-41-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Thu Feb 20 09:40:49 AM UTC 2025

System load:  1.15          Processes:    212
Usage of /:   39.4% of 11.21GB Users logged in: 0
Memory usage: 10%          IPv4 address for enp0s3: 10.0.2.15
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

Updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

rendszergazda@admin:~$
```

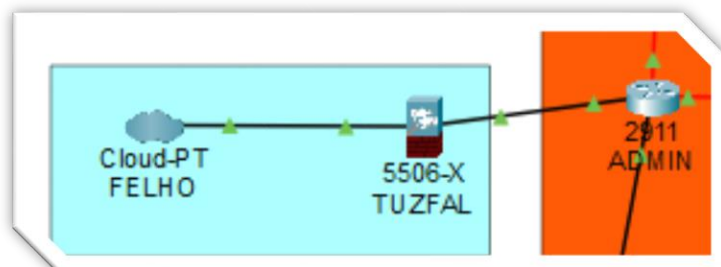
A szerver kapott egy IPv6-os címet is hiszen közel korlátlan címzési lehetőséget biztosít, így az admin szerver minden interfésze és eszköze saját egyedi IP-címet kaphat, könnyebben konfigurálható a hitelesített és titkosított adminisztrációs hozzáférés.

A szerveren titkosított módon tárolhatók a konfigurációs fájlok, így védve vannak illetéktelen hozzáférés és adatlopás ellen.

Ennek köszönhetően végeztünk biztonsági mentést is a konfigurációkról ami azt eredményezi ha egy router vagy switch meghibásodik, az eszközön tárolt konfiguráció elveszhet. A szerveren történő mentés biztosítja, hogy az adatok mindig elérhetők maradjanak.

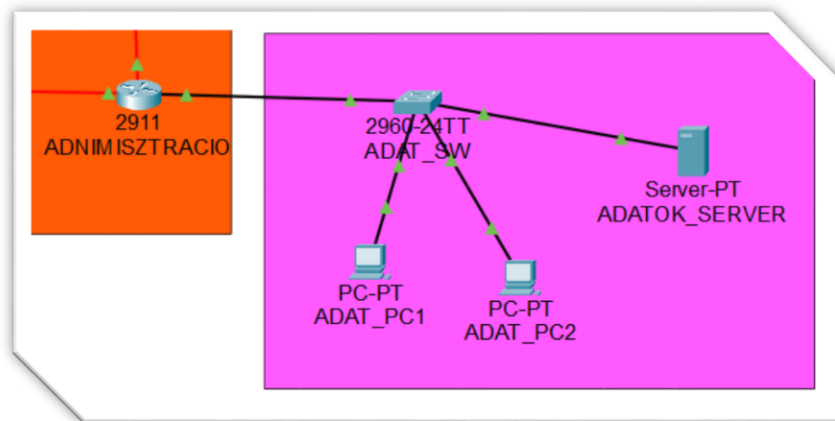
Szolgáltató (Admin)

- ❖ ADMIN_Router : Ha egy router nincs megfelelően védve, könnyen illetéktelen hozzáférés áldozata lehet, ami komoly biztonsági kockázatot jelenthet. Ezt megakadályozva beállítottunk egy jelszót ami a router konfigurációját védi így megakadályozva az imént említetteket.
- ❖ Dinamikus címfordítás(NAT)
- ❖ A belső, privát hálózaton található eszközök egy privát IP-címtartományból kommunikálnak.
- ❖ Amikor egy eszköz kifelé kommunikál az internetre vagy egy másik hálózatra, a router vagy tűzfal a privát IP-t egy nyilvános IP-re cseréli egy előre meghatározott címkészletből.
- ❖ A mi esetünkben a FELHŐ a szolgáltatótól kapott internetet jelképezi . A nagyobb biztonság érdekében elhelyeztünk egy hardveres TŰZFAL(at). Az iskolai hálózatról érkező kérést a dinamikus nat egy IP-címre fordítja át így megoldható hogy a hálózaton lévő összes eszköz ugyanazon IP-címmel kommunikáljon a szolgáltató felé.



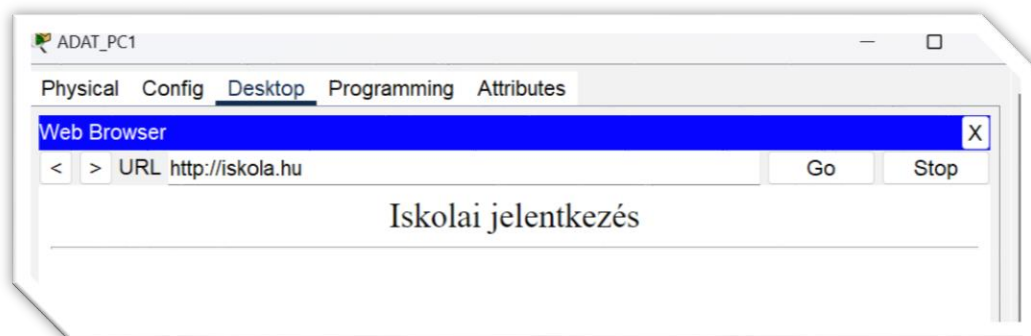
Adminisztráció

A hatékony működés érdekében egy modern, stabil és biztonságos hálózati rendszert hoztunk létre. Az alábbi megoldásokkal biztosítjuk a gyors és megbízható adatáramlást az adminisztrációs részlegen belül.



Az ADATOK_SERVER-re telepített **webszerver** lehetővé teszi, hogy az alkalmazottak könnyen és biztonságosan elérhessék a szükséges információkat, belső dokumentációkat és egyéb erőforrásokat egy böngészőn keresztül. Ez csökkenti a papíralapú adminisztrációt, és gyorsítja a munkafolyamatokat.

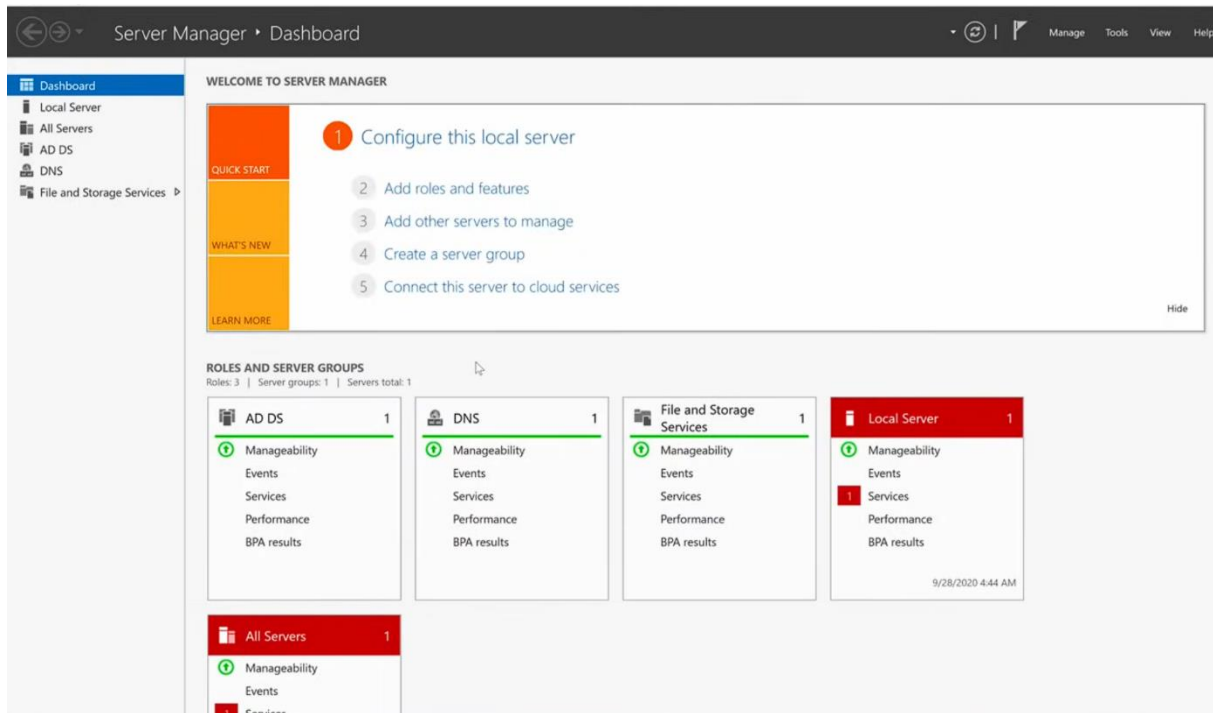
Létrehoztunk egy iskolai webszervert, amely lehetőséget biztosít a diákok és tanárok számára, hogy könnyen és gyorsan csatlakozzanak az iskola saját digitális felületeihez.



ADMINISZTRÁCIÓ ROUTER : A routeren beállított statikus NAT (Network Address Translation) biztosítja, hogy a belső szerver elérhető legyen az internet felől is, de csak az előre meghatározott, biztonságos módon. Ez azt jelenti, hogy például egy külső ügyfél vagy partner egy adott IP-címen keresztül érheti el a weboldalt, miközben a hálózat többi része védett marad a jogosulatlan hozzáférésektől.

A routeren konfigurált DHCP (Dynamic Host Configuration Protocol) automatikusan kiosztja az IP-címeket a számítógépek és egyéb eszközök számára. A DHCP biztosítja, hogy ne legyenek IP-cím ütközések, ami javítja a hálózat stabilitását és megbízhatóságát.

ADAT_PC1: Az Active Directory (AD) egy Microsoft által fejlesztett címtárszolgáltatás, amely lehetővé teszi a hálózati erőforrások, például felhasználók, számítógépek és csoportok központi kezelését. Az AD segítségével a rendszergazdák egyszerűen szabályozhatják a hozzáféréseket, beállíthatják a jogosultságokat és biztonsági házirendeket alkalmazhatnak.



A VPN (Virtual Private Network) beállítása során egy titkosított kapcsolatot hoztunk létre két hálózat között egy Cisco eszközön. Az IPsec (Internet Protocol Security) protokollt használtuk a biztonságos adatátvitelhez.



The screenshot shows a Cisco IOS Command Line Interface (CLI) window with tabs for Physical, Config, CLI, and Attributes. The CLI window displays the output of the command 'sh crypto ipsec sa' for interface Serial0/1/0. The output shows the configuration of the IPsec Security Association (SA) for the TGMAP crypto map. It includes details about the local and remote IP addresses, the current peer, and statistics for packets sent and received. The window also has a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons.

```
ADMIN>
ADMIN>en
ADMIN#sh crypto ipsec sa

interface: Serial0/1/0
  Crypto map tag: TGMAP, local addr 10.1.1.2

  protected vrf: (none)
  local ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port):
(192.168.20.0/255.255.255.0/0/0)
  current_peer 20.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.1.1.2, remote crypto endpt.: 20.1.1.2
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
    current outbound spi: 0x0(0)

  inbound esp sas:

--More--
```

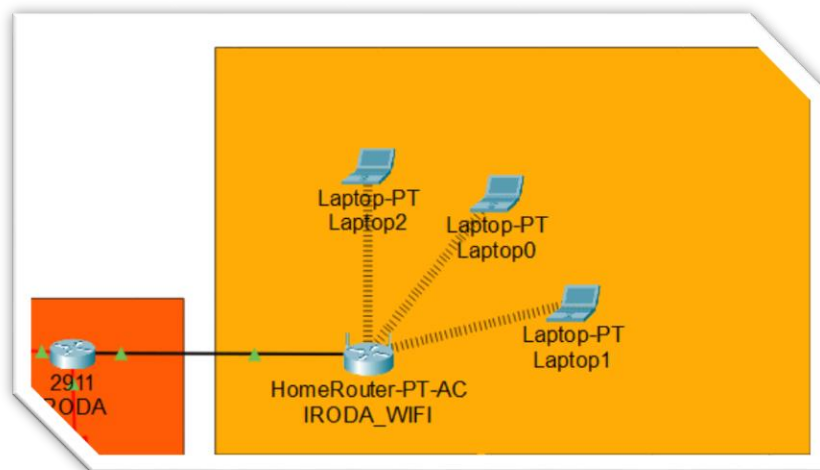
Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Iroda

A hatékony munkavégzés és a stabil hálózati kapcsolat érdekében létrehoztunk egy modern, vezeték nélküli hálózatot az iroda számára. Az IRODA_WIFI névre keresztelt Wi-Fi hálózat biztosítja a gyors és megbízható internetkapcsolatot az irodai laptopok és egyéb eszközök számára.



Az irodai dolgozók bárhol kényelmesen csatlakozhatnak a hálózatra, nincs szükség felesleges kábelezésre.

A beállított HomeRouter-PT-AC típusú eszköz erős és folyamatos jelet biztosít, így a munkavégzés zavartalan és hatékony.

A hálózatot WPA2-Personal védelemmel láttuk el, amely:

- ❖ Erős titkosítást biztosít a felhasználói adatok számára
- ❖ Megakadályozza a jogosulatlan hozzáférést, így csak a megfelelő hitelesítéssel rendelkező eszközök csatlakozhatnak
- ❖ Biztonságosabbá teszi az online munkavégzést, megvédve az adatokat a külső fenyegetésektől

Network Setup	
Router IP	IP Address: 192 . 168 . 50 . 1 Subnet Mask: 255.255.255.0
DHCP Server Settings	DHCP Server: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled DHCP Reservation
	Start IP Address: 192.168.50. 2
	Maximum number of Users: 30
	IP Address Range: 192 168 50 2 - 31

Basic Wireless Settings	
2.4 GHz	
Network Mode:	N-Only
Network Name (SSID):	IRODA_WIFI
SSID Broadcast:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Standard Channel:	1 - 2.412GHz
Channel Bandwidth:	Auto

Ez a DHCP-konfiguráció biztosítja a hatékony, biztonságos és automatizált IP-címkezelést a hálózat számára. Az optimális beállítások garantálják a gyors csatlakozást, a megbízható működést és a problémamentes hálózatkezelést.

Hálózat neve (SSID): IRODA_WIFI

- ❖ A hálózat kizárólag az 802.11n szabványt használja, amely jobb sebességet és stabilitást biztosít a régebbi b/g szabványokhoz képest.
- ❖ Ez biztosítja, hogy csak modernebb eszközök csatlakozhatnak, amelyek támogatják ezt a technológiát, így optimalizálva a teljesítményt.
- ❖ A csatorna sávszélessége automatikusan alkalmazkodik a környezethez, így csökkenti a zavaró jeleket és stabilabb kapcsolatot biztosít.

A hálózatunk védelme érdekében WPA2-Personal biztonsági módot alkalmaztunk, amely a AES titkosítást használja. Ez a megoldás garantálja, hogy az irodai Wi-Fi hálózat biztonságos és védett maradjon a jogosulatlan hozzáférésekkel szemben.

A WPA2-Personal jelenleg az egyik legbiztonságosabb Wi-Fi titkosítási mód, amely megakadályozza, hogy illetéktelenek hozzáférjenek a hálózathoz.

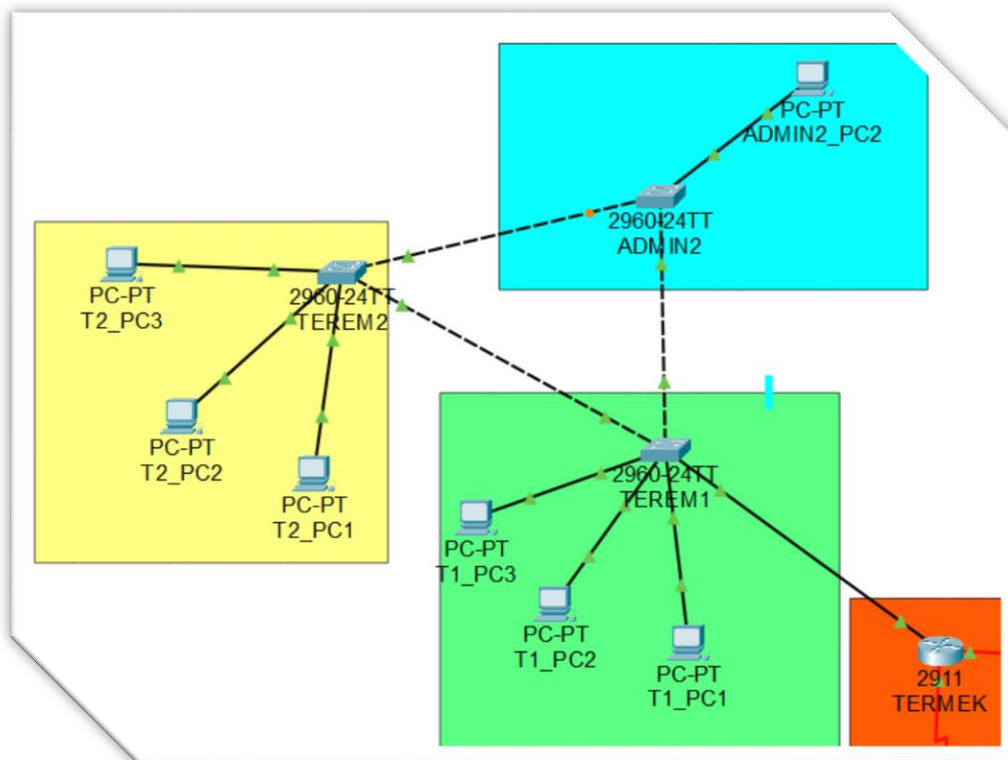
Az AES titkosítás nagyobb biztonságot nyújt, mint a korábbi TKIP titkosítás, és a modern eszközök is támogatják.

A jelszóvédelem biztosítja, hogy csak az engedélyezett felhasználók csatlakozhassanak a Wi-Fi hálózathoz.

Termek

A hálózatunk optimális működése érdekében VLAN (Virtual Local Area Network) és VTP (VLAN Trunking Protocol) technológiákat alkalmaztunk. Ezek a megoldások biztosítják, hogy az egyes tantermek és az ADMIN_2 hálózat logikailag elkülönüljön, miközben hatékony adatforgalmat és jobb hálózatkezelést tesznek lehetővé.

A mi esetünkben ez azt eredményezi hogy az egyes termek nem tudnak kommunikálni egymással.



A különböző termekhez különböző VLAN-okat hoztunk létre . Az ADMIN_2-höz tartozó eszközöket is külön VLAN-okba soroltuk, így a forgalom nem keveredik.

Például a tanulók számítógépei nem férnek hozzá az ADMIN_2 eszközökhöz, így védve vannak az érzékeny adatok.

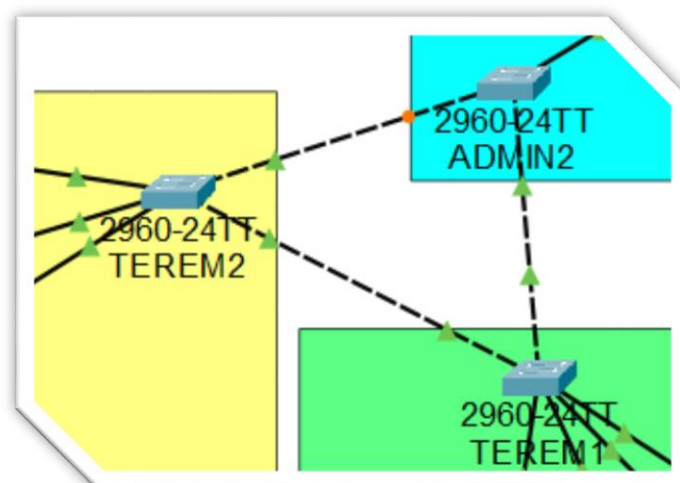
10	TEREM1	active
20	TEREM2	active
30	ADMIN1	active

A fenti hálózati topológia több különálló switchből és egy központi routerből áll, amely különböző termeket és az ADMIN_2 részt köti össze. A hatékony VLAN-kezelés érdekében VTP-t (VLAN Trunking Protocol) állítottunk be.

A VTP automatizálja és leegyszerűsíti a VLAN-kezelést, megkönnyíti az új eszközök hozzáadását, és csökkenti az adminisztrációs terheket. Ezzel a megoldással egy biztonságos, rugalmas és könnyen skálázható hálózatot hoztunk létre, amely hosszú távon is hatékonyan működik.

Az ADMIN2-re telnetet állítottunk be annak érdekében hogy a rendszergaza távolról is elérje ,konfigurálni tudja az eszközt.

Egy rendszergazda egyszerre több hálózati eszközhöz is hozzáférhet, így hatékonyabban kezelheti a hálózatot.



A hálózati diagramon jól látható, hogy több switch és kapcsolódási útvonal is van, ami egy redundáns hálózati topológiára utal. A redundancia célja, hogy növelje a hálózat megbízhatóságát és elérhetőségét, minimalizálva a kieséseket.

Az ACL (Access Control List) beállításával letiltottuk az internetelérést, biztosítva, hogy a diákok csak a belső hálózatot használhassák.

Összegzés

A modern oktatásban elengedhetetlen egy gyors, biztonságos és jól működő hálózat. Projektünk célja egy olyan rendszer kialakítása volt, amely négy telephelyet kapcsol össze, biztosítva a hatékony adatáramlást és biztonságot.

A hálózatot több VLAN-ra osztottuk, amelyeket statikus és dinamikus útválasztás támogat, OSPF protokollal. IPv4 és IPv6 címezést egyaránt alkalmaztunk, valamint VPN-t a biztonságos távoli elérés érdekében. A hálózatot ACL-ek és hardveres tűzfal védi.

Linux és Windows szerverek biztosítják az Active Directory, DHCP, DNS, HTTP, fájlmegosztás és biztonsági mentések szolgáltatásait. A vezeték nélküli hálózat WPA2 titkosítással védett, az irodák és tantermek VLAN-okkal elkülönülnek, csökkentve a biztonsági kockázatokat.

A rendszer skálázható, stabil és könnyen kezelhető, biztosítva az iskola adminisztrációjának és oktatási folyamatainak zavartalan működését.