

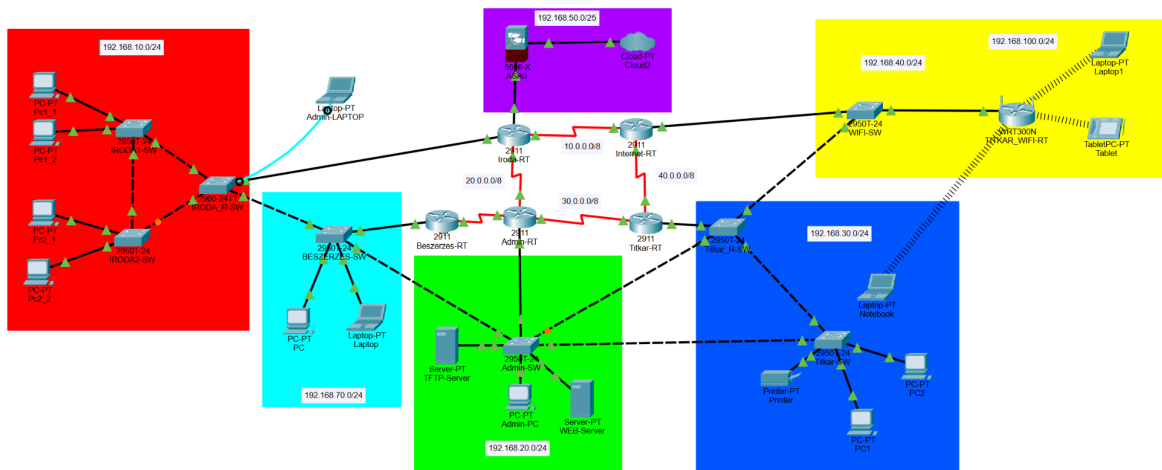
# **Informatikai rendszer és - alkalmazás-üzemeltető technikus(5 0612 12 02)**

## **Hálózat tervezési, működési dokumentáció 2025. április**

**Készítette:**

**Kis Kende Dominik és Nagy Botond Áron**

|   |           |
|---|-----------|
| <b>A hálózat szimulációs programban megvalósítva .....</b>          | <b>3</b>  |
| <b>IP cím táblázat .....</b>  | <b>3</b>  |
| <b>Cél és hatókör .....</b>   | <b>4</b>  |
| <b>Hálózati topológia áttekintése .....</b>                         | <b>4</b>  |
| <b>Dokumentáció felépítése .....</b>                                | <b>5</b>  |
| <b>VLAN (Virtual Local Area Network) .....</b>                      | <b>5</b>  |
| <b>2. és 3. rétegbeli redundancia .....</b>                         | <b>8</b>  |
| <b>IPv4 és IPv6 címezés .....</b>                                   | <b>8</b>  |
| <b>Vezeték nélküli hálózat .....</b>                                | <b>9</b>  |
| <b>Statisztikus és dinamikus forgalomirányítás .....</b>            | <b>10</b> |
| <b>Statisztikus és dinamikus címfordítás .....</b>                  | <b>10</b> |
| <b>WAN (Wide Area Network) – Frame Relay .....</b>                  | <b>11</b> |
| <b>VPN (Virtual Private Network) .....</b>                          | <b>12</b> |
| <b>Programozott hálózat konfiguráció (SDN) .....</b>                | <b>13</b> |
| <b>ACL (Access Control Lists) .....</b>                             | <b>14</b> |
| <b>Hardveres tűzfal eszköz .....</b>                                | <b>14</b> |
| <b>Windows Webkiszolgáló Bemutatása .....</b>                       | <b>15</b> |
| <b>Linux DNS Kiszolgáló Bemutatása .....</b>                        | <b>16</b> |
| <b>Összegzés .....</b>  | <b>16</b> |
| <b>Privilegizált módot védő titkosított jelszavas védelem .....</b> | <b>16</b> |
| <b>SSH(Secure Shell) .....</b>                                      | <b>17</b> |
| <b>Konzolos hozzáférést védő jelszó .....</b>                       | <b>18</b> |
| <b>Összefoglalás .....</b>  | <b>18</b> |



| ESZKÖZ       | IP CÍM            | ALHÁLÓZATI MASZK | ALAPÉRTELMEZET T ÁTJÁRÓ | NÉV          |
|--------------|-------------------|------------------|-------------------------|--------------|
| IRODA-RT     | 10.0.0.1          | 255.0.0.0        | -                       | IRODA-RT     |
|              | 20.0.0.1          | 255.0.0.0        | -                       |              |
|              | 192.168.10.1      | 255.255.255.0    | -                       |              |
|              | 192.168.50.1      | 255.255.255.0    | -                       |              |
| INTERNET-RT  | 10.0.0.2          | 255.0.0.0        | -                       | INTERNET-RT  |
|              | 40.0.0.1          | 255.0.0.0        | -                       |              |
|              | 192.168.40.1      | 255.255.255.0    | -                       |              |
| ADMIN-RT     | 20.0.0.2          | 255.0.0.0        | -                       | ADMIN-RT     |
|              | 30.0.0.1          | 255.0.0.0        | -                       |              |
|              | 192.168.20.1      | 255.255.255.0    | -                       |              |
|              | 192.168.60.1      | 255.255.255.128  | -                       |              |
|              | 50.0.0.1          | 255.0.0.0        | -                       |              |
| TITKAR-RT    | 30.0.0.2          | 255.0.0.0        | -                       | TITKAR-RT    |
|              | 40.0.0.2          | 255.0.0.0        | -                       |              |
|              | 192.168.30.1      | 255.255.255.0    | -                       |              |
| BESZERZES-RT | 192.168.70.1      | 255.255.255.0    | -                       | BESZERZES-RT |
|              | 50.0.0.2          | 255.0.0.0        | -                       |              |
| WIFI-RT      | 192.168.40.2      | 255.255.255.0    | 192.168.40.1            | WIFI-RT      |
|              | 192.168.100.1     | 255.255.255.0    | -                       |              |
| IRODA_R-SW   | 192.168.10.2      | 255.255.255.0    | 192.168.10.1            | -            |
| IRODA1-SW    | 192.168.10.3      | 255.255.255.0    | 192.168.10.1            | -            |
| IRODA2-SW    | 192.168.10.4      | 255.255.255.0    | 192.168.10.1            | -            |
| TFTP-SERVER  | 192.168.20.2      | 255.255.255.0    | 192.168.20.1            | -            |
| WEB-SERVER   | 192.168.20.3      | 255.255.255.0    | 192.168.20.1            | -            |
|              | F411:1:1::16:2/32 | -                | F411:1:1::16:1          | -            |

|               |                |                 |              |   |
|---------------|----------------|-----------------|--------------|---|
| LAPTOP1(WLAN) | DHCP-Kliens    |                 | 192.168.40.2 | - |
| TABLET(WLAN)  | DHCP-Kliens    |                 | 192.168.40.2 | - |
| NOTEBOOK      | DHCP-Kliens    |                 | 192.168.30.1 | - |
| PRINTER(TIT)  | DHCP-Kliens    |                 | 192.168.30.1 | - |
| PC1(TIT)      | DHCP-Kliens    |                 | 192.168.30.1 | - |
| PC2(TIT)      | DHCP-Kliens    |                 | 192.168.30.1 | - |
| ADMIN-LAPTOP  | 192.168.20.5   | 255.255.255.0   | 192.168.20.1 | - |
| ADMIN-PC      | 192.168.20.4   | 255.255.255.0   | 192.168.20.1 | - |
| PC1_1(IR)     | 192.168.10.10  | 255.255.255.0   | 192.168.10.1 | - |
| PC1_2(IR)     | 192.168.10.20  | 255.255.255.0   | 192.168.10.1 | - |
| PC2_1(IR)     | 192.168.10.11  | 255.255.255.0   | 192.168.10.1 | - |
| PC2_2(IR)     | 192.168.10.21  | 255.255.255.0   | 192.168.10.1 | - |
| PC(BSZ)       | 192.168.70.254 | 255.255.255.0   | 192.168.70.1 | - |
| LAPTOP(BSZ)   | 192.168.70.253 | 255.255.255.0   | 192.168.70.1 | - |
| BESZERZES-SW  | 192.168.70.252 | 255.255.255.0   | 192.168.70.1 | - |
| FIREWALL      | 192.168.50.2   | 255.255.255.128 | -            | - |
|               | 192.168.50.129 | 255.255.255.128 | -            | - |

## 1. Cél és hatókör

Ez a dokumentáció a Rubicon BT vállalat hálózati infrastruktúrájának tervezését és konfigurációját tartalmazza. A célunk egy megbízható, biztonságos, és bővíthető hálózati környezet kialakítása, amely képes támogatni a vállalat napi működését, az alkalmazottak munkavégzését, valamint a különböző üzleti folyamatokat. A dokumentációban szereplő konfigurációk és beállítások biztosítják a megfelelő adatátvitelt, figyeltünk arra, hogy az elvárásoknak megfelelően tartalmazzon a hálózat terhelés elosztást, hiba esetén is működőképes maradjon a hálózat, mivel több útvonal létezik a telephelyek között és a biztonságra, miközben a jövőbeli bővítések is figyelembevételre kerülnek.

## 2. Hálózati topológia áttekintése

A hálózat egy hierarchikus architektúrára épül, amely három fő rétegre tagolódik: a core, az aggregation és az access rétegre. Az access réteg biztosítja a végpontok, mint a munkaállomások, nyomtatók és Wi-Fi eszközök kapcsolódását. Az aggregation réteg közvetíti az adatforgalmat a helyi eszközök és a központi routerek között. A core réteg biztosítja a nagy

sebességű adatátvitelt és a redundáns kapcsolatokat a külső hálózatokkal, valamint az internetkapcsolatokhoz való elérést.

A hálózati infrastruktúra a következőket tartalmazza:

- **VLAN-ok:** A forgalom elkülönítése és az alkalmazottak közötti kommunikáció optimalizálása érdekében több különböző VLAN-t használunk.
- **Redundáns útvonalak:** A hálózat hibamentes működése érdekében a 2. és 3. rétegbeli redundanciát biztosítjuk a megfelelő routing protollokkal és eszközökkel.
- **IPv4 és IPv6 címezés:** A hálózat mindkét címezési formát használja az eszközök és szolgáltatások megfelelő azonosítása érdekében.
- **Vezeték nélküli hálózat:** A felhasználók mobilitásának és rugalmasságának támogatására biztonságos Wi-Fi hozzáférési pontok kerültek telepítésre.
- **VPN és WAN kapcsolatok:** A távoli telephelyek közötti kapcsolatok biztosítása érdekében VPN és WAN technológiák kerültek implementálásra.
- **Tűzfal és ACL szabályok:** A hálózat védelmét tűzfalak és hozzáférési vezérlő listák (ACL) biztosítják, amelyek szabályozzák a bejövő és kimenő forgalmat.
- **Statikus és dinamikus címfordítás:** A címfordítás lehetővé teszi a belső hálózaton található IP-címek átalakítását, hogy azok elérhetőek legyenek az interneten vagy egy másik hálózaton keresztül.
- **Statikus és dinamikus forgalomirányítás:** A statikus és dinamikus forgalomirányítás (routing) kétféleképpen segít a hálózati forgalom célba juttatásában, de más-más módon működnek.

### 3. Dokumentáció felépítése

A dokumentáció az alábbiakban részletezi a hálózati infrastruktúra minden fontos aspektusát, beleértve a VLAN konfigurációkat, a redundanciát, az IP címezést, a vezeték nélküli hálózat beállításait, valamint a biztonsági intézkedéseket és a tűzfalak kezelését. A cél, hogy minden hálózati elem és konfiguráció világos és könnyen érthető módon legyen bemutatva a későbbi karbantartás, hibaelhárítás és bővítés érdekében.

### 4. VLAN (Virtual Local Area Network)

Célja és előnyei

A VLAN-ok lehetővé teszik a hálózaton belüli logikai szegmentálást, ami biztosítja az adatok elkülönítését, a hálózati forgalom hatékony kezelését, valamint a biztonság növelését. A VLAN-ok használata segít csökkenteni a broadcast forgalmat, növeli a hálózati teljesítményt, és lehetővé teszi a hálózati erőforrások jobb elosztását. A VLAN-ok alkalmazásával különböző csoportokat hozhatunk létre, amelyek függetlenek egymástól, még ha ugyanazon fizikai eszközön osztoznak is.

## Használt VLAN-ok

A következő VLAN-ok kerültek kialakításra a vállalati hálózaton belül, figyelembe véve az egyes osztályok és alkalmazások igényeit:

- VLAN 10 - Munkaállomások (HR, Iroda1)

o IP tartomány: 192.168.10.0/24

o Eszközök: HR osztály munkaállomásai

o Cél: A HR osztály számára biztosít egy dedikált hálózati szegmenst, elkerülve a más osztályokkal való kommunikációt.

- VLAN 20 - Munkaállomások (Pénzügy, Iroda2)

o IP tartomány: 192.168.20.0/24

o Eszközök: Pénzügy osztály munkaállomásai, fájlserverek

o Cél: A pénzügyi osztály számára biztosított hálózati szegmens, amely elszigeteli az érzékeny adatokat.

## VLAN Routing (Inter-VLAN Routing)

A VLAN-ok közötti kommunikációt a Layer 3 Switch vagy Router végzi. Az alábbi konfiguráció biztosítja az egyes VLAN-ok közötti adatforgalmat:

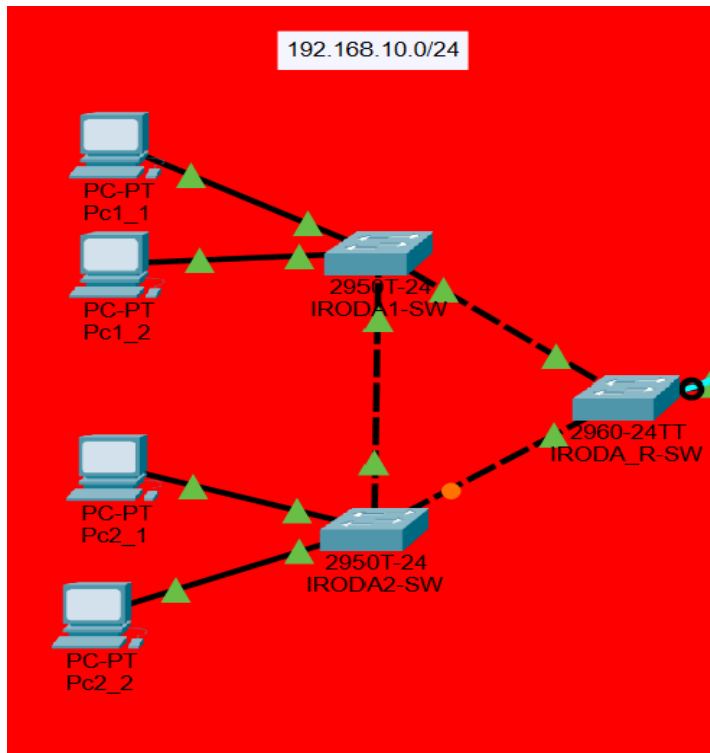
- A routingot Router on a Stick konfigurációval oldottuk meg, amely egyetlen fizikai interfészen biztosítja az inter-VLAN routingot.

## VLAN Security

A VLAN-ok biztonságos használatához a következő intézkedéseket alkalmazzuk:

- Port security: Csak engedélyezett eszközök csatlakozhatnak a különböző VLAN-okhoz.

- **DHCP snooping:** Megakadályozza, hogy nem megbízható DHCP szerverek osztogassanak IP-címeket a hálózaton.



## VLAN tagolás

A VLAN-ok megfelelő működéséhez a következő VLAN tagolást használjuk az eszközök közötti kommunikációban:

- **IEEE 802.1Q VLAN tagolás:** A hálózati eszközök közötti forgalom esetén a VLAN azonosítókat 802.1Q tag-ek formájában adunk hozzá a kerethez.
- Az access portok a megfelelő VLAN-hoz tartoznak, míg az uplink portok trunk portok, amelyek több VLAN-t is képesek továbbítani.

## VLAN hibakeresés és karbantartás

A VLAN-ok hibáinak elhárításához az alábbi eszközöket és parancsokat alkalmazzuk:

- Ping teszt a VLAN IP címek közötti elérhetőség ellenőrzésére.
- VLAN konfigurációk lekérdezése: show vlan brief és show running-config parancsok a VLAN beállítások megtekintésére.

## 5. 2. és 3. rétegbeli redundancia

Részletes magyarázat:

A redundancia célja, több útvonal biztosításával, hogy a hálózati eszközök hibája esetén is legyen folyamatos működés. A redundanciát két szinten érhetjük el:

**2. rétegbeli redundancia (STP):** A hurokmentes hálózati kapcsolatot biztosítja, amely megakadályozza az adatcsomagok végtelen körforgását.

**3. rétegbeli redundancia (HSRP):** A forgalmat több router között elosztja, így ha egy router meghibásodik, a másik átveszi a forgalmat.

Példa:

- STP (Spanning Tree Protocol) a hurokmentes kapcsolatokért.
- HSRP (Hot Standby Router Protocol), hogy biztosítsuk a hálózati kapcsolat folyamatosságát.

---

## 6. IPv4 és IPv6 címzés

Részletes magyarázat:

Az IPv4 és IPv6 címzés biztosítja, hogy a hálózati eszközök megfelelő címekkel legyenek ellátva. Az IPv4 címek 32 bit hosszúak, míg az IPv6 címek 128 bit hosszúak, ami az IPv4 címek kimerítését követően jelentkezett.

Példa:

- IPv4 címzés: Az IPv4 címeket a belső hálózatban használjuk az egyszerűsége miatt.
- IPv6 címzés: Az IPv6-t az új generációs címzéshez használjuk. Mivel az IPv6 címek sokkal nagyobb címtartományt biztosítanak, segítenek a jövőbeli bővítésben.



IP Configuration
X

IP Configuration

☐ DHCP
☒ Static

IPv4 Address

Subnet Mask

Default Gateway

DNS Server

---

IPv6 Configuration

☐ Automatic
☒ Static

IPv6 Address  /

Link Local Address

Default Gateway

DNS Server

## 7. Vezeték nélküli hálózat

### Részletes magyarázat:

A Wi-Fi hálózat célja a felhasználók mobilitásának biztosítása. A vezeték nélküli hozzáférés biztosítása mellett a biztonságra is oda kell figyelni, például WPA2-PS titkosítással, hogy megvédjük a hálózatot a potenciális támadásoktól.

### Példa:

- SSID : "Rubicon-Net" (WPA2-PS titkosítással)

Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Wireless-N Broadband Router
WRT300N
Status

Basic Wireless Settings
Wireless Security
Guest Network
Wireless MAC Filter
Advanced Wireless Settings

Wireless Security

Security Mode:

Encryption:

Passphrase:

Key Renewal:

WPA2 Personal

AES

alma1234

3600

seconds

[Help...](#)

## 8. Statisztikus és dinamikus forgalomirányítás

Részletes magyarázat:

A forgalomirányítás lehet statikus vagy dinamikus. A statikus útvonalakat manuálisan konfiguráljuk, míg a dinamikus forgalomirányítást az útválasztási protokollok (pl. OSPF) végzik automatikusan.

Példa:

- Statisztikus útvonal konfigurációja:

Ez a konfiguráció azt jelenti, hogy minden hálózatra irányuló forgalom a router IP-címén keresztül fog elérni.

```
| ip route 192.168.20.0 255.255.255.0 50.0.0.1
```

- Dinamikus forgalomirányítás (OSPF):

Az OSPF lehetővé teszi az útvonalak dinamikus frissítését és alkalmazását a hálózaton.

```
router ospf 1
log-adjacency-changes
network 20.0.0.0 0.255.255.255 area 0
network 30.0.0.0 0.255.255.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 50.0.0.0 0.255.255.255 area 0
```

---

## 9. Statisztikus és dinamikus címfordítás (NAT)

Részletes magyarázat:

A NAT (Network Address Translation) célja, hogy a magánhálózati címeket külső, nyilvános címekre cserélje. A NAT lehet statikus (fix) vagy dinamikus (változó).

Példa:

- Statisztikus NAT:

```
ip nat inside source static 192.168.20.3 200.10.10.254
```

- **Dinamikus NAT:** A belső hálózaton lévő eszközök egyetlen külső IP-címet használnak, amely a NAT fordításon keresztül érhető el.

A hálózati címfordítás biztonság szempontjából is fontos, hogy a hálózat belső IP címe, pl. WEB-Server kívülről rejtve maradjon.

```
ip nat pool CLOUD 200.20.20.253 200.20.20.254 netmask 255.255.255.0  
ip nat inside source list 1 pool CLOUD
```

```
access-list 1 permit 192.168.50.0 0.0.0.127
```

---

## 10. WAN (Wide Area Network) – Frame Relay

Részletes magyarázat:

A Frame Relay egy régebbi, de még mindig széles körben használt csomagkapcsolt WAN technológia. Ez biztosítja a távoli irodák közötti adatkapcsolatot dedikált vonalakon vagy megosztott linkeken keresztül. A Frame Relay PVC-ket (Permanent Virtual Circuits) alkalmaz a különböző helyek közötti adatátvitelhez. A Permanent Virtual Circuit (PVC) egy hálózaton keresztül létrehozott virtuális kapcsolat, amely állandó és dedikált adatátviteli útvonalat biztosít két végpont között anélkül, hogy gyakori beállítási és lebontási folyamatokra lenne szükség. Ezen a technológián keresztül az adatokat csomagokban küldik a hálózaton, és a routerek használják a DLCI (Data Link Connection Identifier) címezést a megfelelő célállomások azonosítására. A Data Link Connection Identifier (DLCI) egy egyedi azonosító, amelyet a Frame Relay hálózatokban használnak egy adott virtuális áramkör azonosítására két csomópont között. Ez egy 10 bites szám, amelyet az adatkeretek hálózaton keresztüli továbbítására használnak, és helyi jelentőségű, vagyis csak azon a hivatkozáson van értelme, ahol használják.

Példa Frame Relay WAN kapcsolatra két router között:

Az R1 és R2 routerek egy Frame Relay kapcsolaton keresztül kommunikálnak.

```
interface Serial0/0/0
  bandwidth 128
  ip address 20.0.0.2 255.0.0.0
  encapsulation frame-relay
  frame-relay interface-dlci 101
  clock rate 2000000
!
interface Serial0/0/1
  bandwidth 128
  ip address 30.0.0.1 255.0.0.0
  encapsulation frame-relay
  frame-relay interface-dlci 102
  clock rate 128000
!
interface Serial0/1/0
  bandwidth 128
  ip address 50.0.0.1 255.0.0.0
  encapsulation frame-relay
  frame-relay interface-dlci 103
  clock rate 2000000
```

---

## 11. VPN (Virtual Private Network)

Részletes magyarázat:

A VPN-ek lehetővé teszik a távoli hozzáférést a vállalati hálózathoz titkosított csatornán keresztül, így biztonságos kapcsolatot kínálnak.

Ez a beállítás biztosítja a távoli hozzáférést a vállalati hálózathoz SSL-alapú VPN-en keresztül.

```
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

---

## 12. Programozott hálózat konfiguráció (SDN)

### Részletes magyarázat:

Az SDN (Software-Defined Networking) lehetővé teszi a hálózatok központi vezérlését és automatizálását. Az SDN használatával könnyen módosítható a hálózati infrastruktúra a programozott eszközök segítségével.

```
{
  "hostname": "TITKAR-RT",
  "commands": [
    "TITKAR-RT>",
    "TITKAR-RT>en",
    "TITKAR-RT#sh running-config | section dhcp"
  ],
  "dhcp_pools": [
    {
      "name": "LAN_POOL",
      "network": "192.168.30.0",
      "subnet_mask": "255.255.255.0",
      "default_gateway": "192.168.30.1",
      "dns_servers": ["8.8.8.8", "8.8.4.4"],
      "lease_time": "24h",
      "excluded_addresses": ["192.168.30.1", "192.168.30.100-192.168.30.110"]
    }
  ],
  "dhcp_bindings": [
    {
      "mac_address": "00:1A:2B:3C:4D:5E",
      "ip_address": "192.168.30.50",
      "lease_expiration": "2025-02-07 12:00:00"
    }
  ],
  "dhcp_statistics": {
    "total_leases": 50,
    "active_leases": 45,
    "available_addresses": 5,
    "declined_addresses": 0
  }
}
```

---

### 13. ACL (Access Control Lists)

#### Részletes magyarázat:

Az ACL-ek hozzáférési listák, amelyek lehetővé teszik a forgalom szabályozását a hálózaton. Szűrhetjük a forgalmat IP-címek, protokollok, portok vagy egyéb kritériumok alapján.

```
access-list 100 deny udp 192.168.70.0 0.0.0.255 host 192.168.20.2 eq tftp
access-list 100 permit ip any any
```

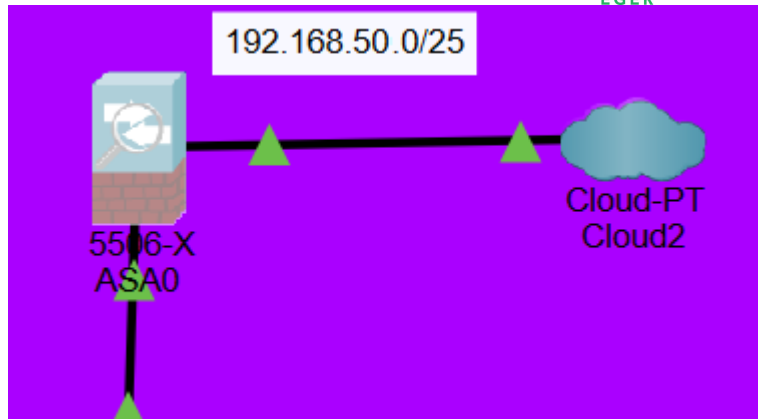
```
interface GigabitEthernet0/0
  ip address 192.168.70.1 255.255.255.0
  ip access-group 100 out
```

---

### 14. Hardveres tűzfal eszköz

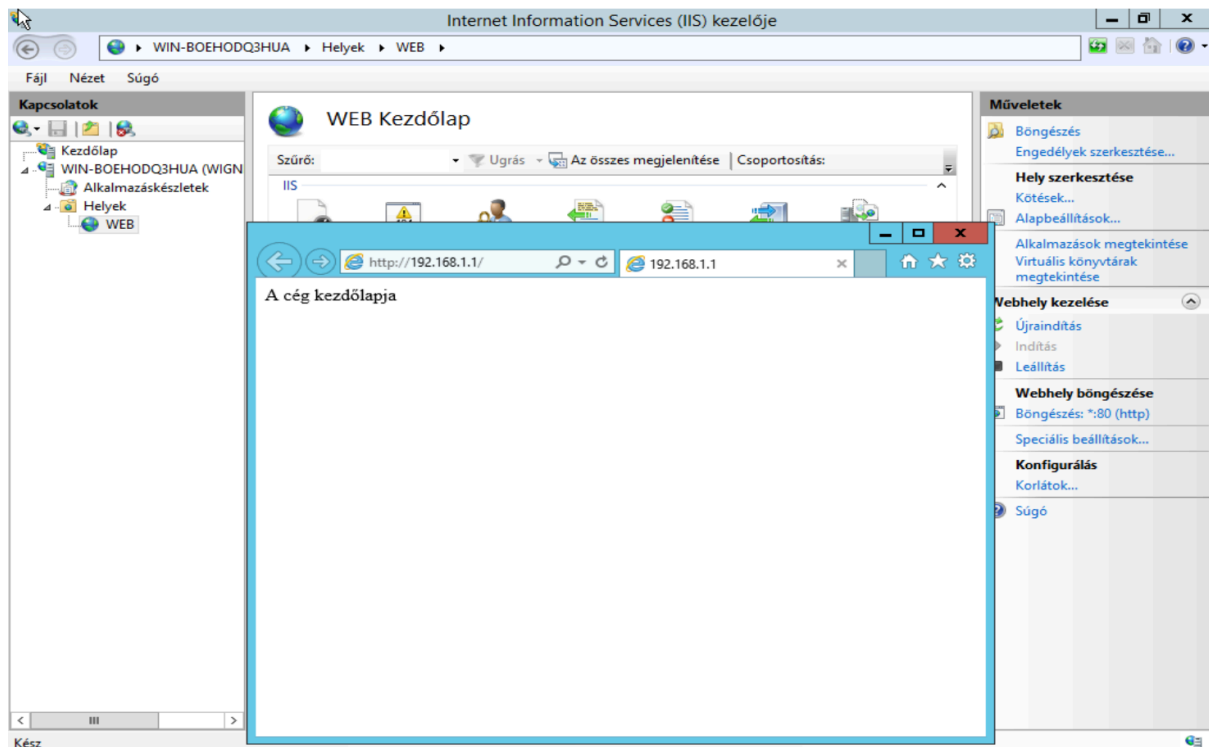
#### Részletes magyarázat:

A hardveres tűzfal biztosítja a hálózat védelmét, szűrve a bejövő és kimenő adatforgalmat, és biztosítva, hogy csak a jogosult forgalom érje el a védett hálózati erőforrásokat.



## 15. Windows Web Kiszolgáló Bemutatása

A Windows Web Kiszolgáló egy olyan szerver, amely az interneten vagy helyi hálózaton keresztül weboldalak, alkalmazások és egyéb webes tartalmak kiszolgálására szolgál. Az egyik legelterjedtebb webkiszolgáló szoftver a Microsoft Internet Information Services (IIS), amely beépített eszközként található meg a Windows Server operációs rendszerekben.

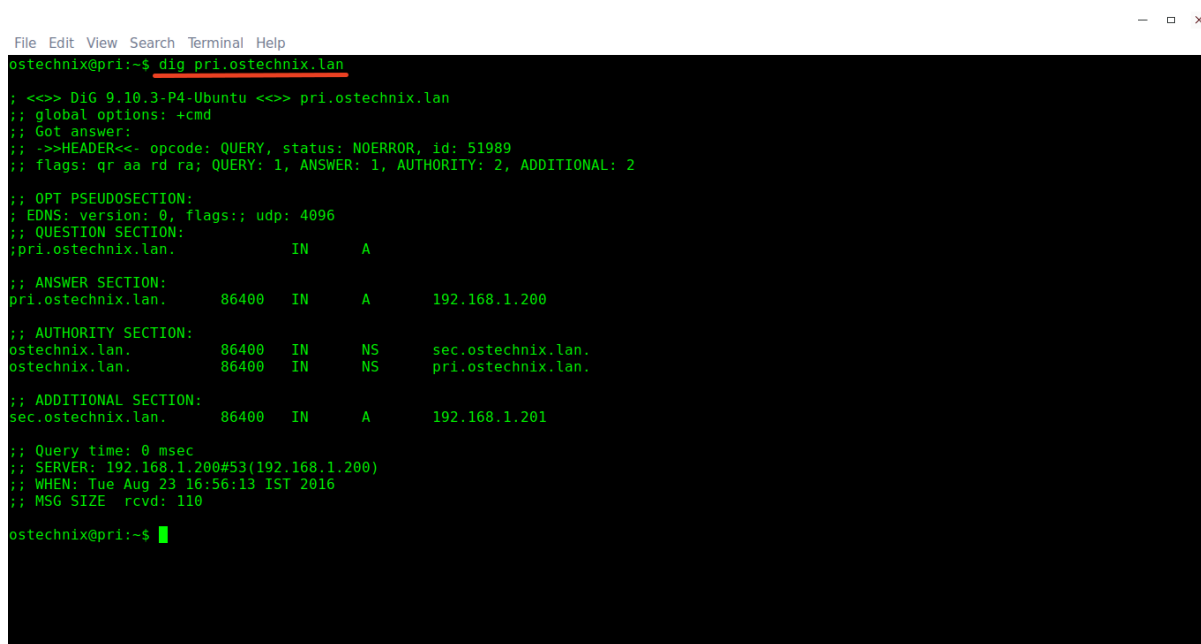


## 16. Linux DNS Kiszolgáló Bemutatása

A Linux DNS Kiszolgáló feladata, hogy feloldja a domain neveket IP-címekre, és lehetővé tegye az internetes vagy helyi hálózaton belüli kommunikációt a domain nevek használatával.

A legnépszerűbb DNS szerver szoftver Linux alatt a BIND (Berkeley Internet Name Domain), amely egy nyílt forráskódú DNS szerver implementáció.

Ennek a segítségével nem IP címet kell megadni a kívánt oldal eléréséhez, hanem a nevét. Pl.: 8.8.8.8 - Google.com



```
File Edit View Search Terminal Help
ostechnix@pri:~$ dig pri.ostechnix.lan
; <<>> DiG 9.10.3-P4-Ubuntu <<>> pri.ostechnix.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51989
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pri.ostechnix.lan.          IN      A
;; ANSWER SECTION:
pri.ostechnix.lan.         86400   IN      A      192.168.1.200
;; AUTHORITY SECTION:
ostechnix.lan.             86400   IN      NS      sec.ostechnix.lan.
ostechnix.lan.             86400   IN      NS      pri.ostechnix.lan.
;; ADDITIONAL SECTION:
sec.ostechnix.lan.         86400   IN      A      192.168.1.201

;; Query time: 0 msec
;; SERVER: 192.168.1.200#53(192.168.1.200)
;; WHEN: Tue Aug 23 16:56:13 IST 2016
;; MSG SIZE rcvd: 110

ostechnix@pri:~$
```

## 17. Összegzés

A két különböző operációs rendszer, Windows Server és Linux, más-más módszerekkel biztosítja a webes és DNS szolgáltatásokat, de mindkettő széles körben alkalmazható a vállalati és otthoni hálózatokban.



## 18. Egyéb, a hálózat biztonságát szolgáló megoldások

### 18.1 Privilegizált módot védő titkosított jelszó

Forgalomirányítók, hálózati kapcsolók állítottunk, hogy védjük az eszközöket az illetéktelen hozzáféréstől, konfigurálástól.

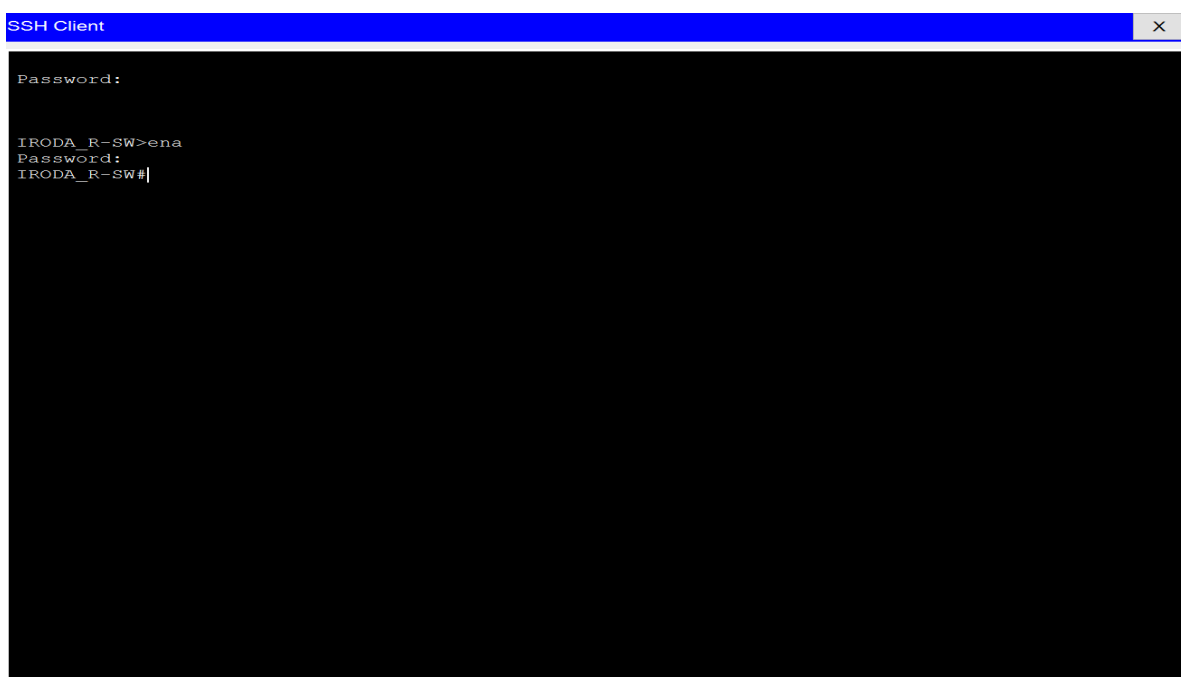
```
ADMIN-RT>ena  
Password: |
```

A titkosított jelszó a forgalomirányító futó konfigurációjában sem jelenik meg

```
enable secret 5 $1$mERr$i9tQCJtBOF3XAq2lumzon1
```

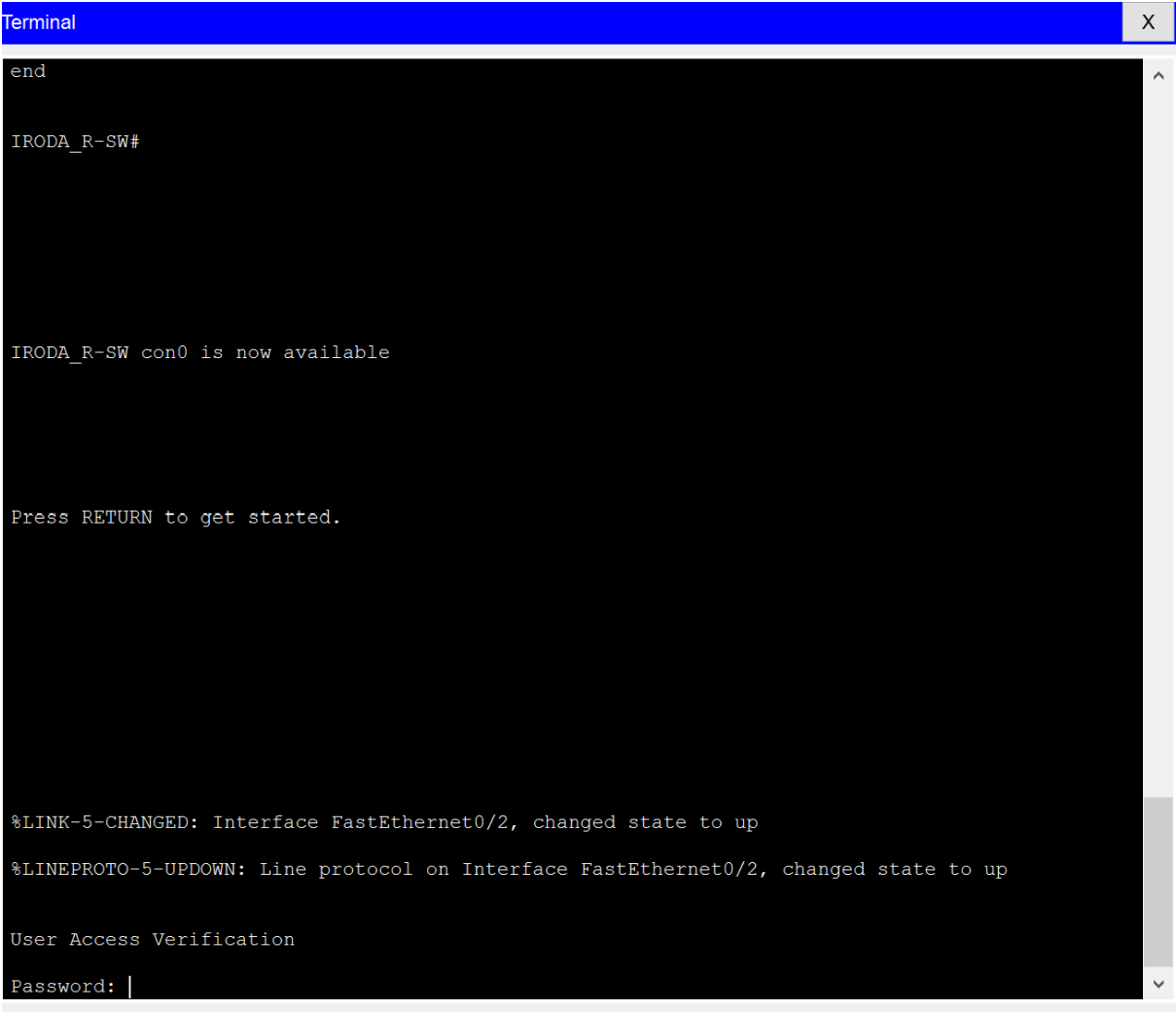
### 18.2. SSH(Secure Shell)

Ez egy nyilvános kulcsú titkosítás, egy távoli számítógép hitelesítésére. Titkosítja kettő munkaállomás között a kommunikációs csatornát, biztonságosabb mint a telnet. Ennek a segítségével távolról is elérhetünk egy konfigurálni kívánt eszközt, anélkül hogy közvetlenül fizikailag csatlakozzunk konzol kábel segítségével. Ezt az IRODA\_R-SW kapcsolóra állítottuk.



### 18.3. Konzolos hozzáférést védő jelszó

Az IRODA\_R\_SW kapcsolón ha a rendszergazdán kívül akarna valaki más konfigurálni, ehhez nem lesz hozzáférése.



```
Terminal X
end

IRODA_R-SW#

IRODA_R-SW con0 is now available

Press RETURN to get started.

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

User Access Verification
Password: |
```

## 19. Összefoglalás

A dokumentációban bemutatott hálózati konfigurációk és megoldások az általánosan alkalmazott best practice-eket és iparági szabványokat követik. A különböző technológiai szintek és protokollok, mint a VLAN, a NAT, a forgalomirányítás, az IPv4/IPv6 címzés, a redundancia biztosítása és a VPN-ek kialakítása lehetővé teszik a hálózati rendszer skálázhatóságát és biztonságát.

A dokumentáció célja, hogy átfogó képet adjon a hálózati infrastruktúra tervezéséről és implementálásáról, figyelembe véve a jövőbeli bővítéseket és a különböző technológiai változások alkalmazkodását. A beállítások és megoldásokat úgy alakítottuk ki, hogy könnyen karbantarthatók legyenek, valamint a lehetséges problémák gyors diagnosztizálása érdekében minden fontos konfigurációs lépés és hibaelhárítási módszer dokumentálásra került.

A dokumentáció további kiegészítéseként fontos, hogy a hálózati adminisztrátorok és fejlesztők rendszeres időközönként végezzenek auditálásokat és frissítéseket a biztonság és a teljesítmény fenntartása érdekében. A hálózati konfigurációk rendszeres felülvizsgálata és tesztelése segíti a problémák előrejelzését és megelőzését.