3.a Ismertesse az ISR (Integrated Sevices Router) forgalomirányítókon megvalósítható hitelesítési és jogosultságkezelési megoldásokat!

Integrated Services Router (ISR)

- Sokkal megbízhatóbb és biztonságosabb az általános routerknél.
- A Cisco ISR lehetővé teszi a biztonságos **felhőalapú computing**-ot a **Group Encrypted Transport Virtual Private Network** segítségével.
    - **Emiatt biztonságosabb a kommunikáció**
- Sokkal drágább, mint egy általános router, mert extra licenszt vagy modulokat kell vásárolni.

AAA

- Felügyeli a hálózatot
    - Ki érheti el (authentication)
    - Mit tehet (authorization)
    - Mit csinált (accounting)

AAA komponensek - keret a hozzáférés felügyeletére

Authentication

- Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel,
  token, smart cards

Authorization - Jogosultságkezelés

- Mely erőforrásokhoz férhetnek hozzá a felhasználók, milyen műveleteket végezhetnek

Accounting – Könyvelés

- Naplózza → mit csinált/változtatott a felhasználó, milyen erőforrást és mennyi ideig ért el

AAA Authentication

- Felhasználónevek és jelszavak tárolása
    - **Local**
        - lokálisan a Cisco forgalomirányítókon tárolja, ez alapján hitelesíti afelhasználókat.
        - Kis hálózatokban
    - **Server-based**
        - központi AAA szerveren
        - Több hálózati eszközt tartalmazó hálózat esetén

AAA előnyei

- Skálázhatóság, rugalmasság
    - Központi konfiguráció (lokális adatbázist routerenként kellene)
- Több backup rendszer használata → hiba esetén más hitelesítési módszerek
    - Szabványos hitelesítési módszerek
        - RADIUS - Remote Authentication Dial-In User Service
            - **Hálózati hozzáférésre használják inkább**
        - TACACS+ - Terminal Access Controller Access Control System Plus
            - **Eszközkezelésre (device management) tervezték**
        - Diameter (RADIUS továbbfejlesztése)

Szerver alapú AAA megvalósítására használható protokollok

	TACACS+	RADIUS
Funkcionalitás	AAA-t részekre osztja, modularitást lehetővé teszi	Kombinálja az hitelesítést és a jogosultságkezelést, külön könyvelés. Ezáltal nem olyan rugalmas, mint a TACACS+
Támogatottság	Cisco	Nyitott/RFC standard
Szállítási protokoll	TCP	UDP
CHAP	Kétirányú hívás és válasz, mint a Challenge Handshake Authentication Protocol (CHAP)	Egyirányú a RADIUS szerver éskliens között
Bizalmasság	Egész csomag titkosított	Csak a jelszó titkosított
Testreszabhatóság	biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként vagy csoportonként	nem biztosítja
Könyvelés	Limitált	Széleskörű

Az IOS különböző privilegizált szintjei által kínált lehetőségek kihasználása, beállítása

0. Szint

- Előre definiált felhasználói szintű hozzáférés
- Ritkán használt
- Parancsok: **disable, enable, exit, help, logout**

1. Szint – User Exec Mode

- Router CLI-vel történő bejelentkezés alapértelmezett szintje.
- Felhasználó nem hajthat végre változtatásokat és nem tekintheti meg a futó konfigurációs fájlt.

2. Szint – 2-14 Szint

- Testreszabható a felhasználói szintű jogosultságokhoz.
- Alacsonyabb szintek parancsai magasabb szintre hozhatóak.
- Magasabb szintek parancsai lejjebb vihetőek alacsonyabb szintre.

3. Szint – 15 Szint – Privileged Exec Mode

- Engedélyezési mód jogosultságainak fenntartva.
- Felhasználók megtekinthetik és módosíthatják a konfigurációt.

Hátrányok

- **Hierarchikus**
  - Egy szinten definiált parancsok a magasabb szinten mind elérhetők.
  - A magasabb szinten definiált parancsok az alacsonyabb szinten nem elérhetőek.
- **Több parancsszóból álló parancs**
  - Ha több parancsszóból álló parancsot definiálunk egy szinthez, minden parancs alkalmazható lesz az adott szinten, amiben az adott parancsszavak valamelyike megtalálható.
- **Nem lehet korlátozni**
  - Nem lehet korlátozni az egyes felhasználók meghatározott porthoz vagy interfészhez történő hozzáférést.

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

A szerep-alapú elérést korlátozó megoldás lényege, előnyei és konfigurálása

Lényege

- **Parser view**
- VIEW-kat, vagyis nézeteket hoz létre.
- A VIEW-k nem hierarchikusan szerveződnek.
- A parancsok specifikusabban rendelhetők a VIEW-hoz.
- **Root View** szükséges a **View** és **SuperViews** meghatározásához (Parancsokat tartalmaznak)
- Egy parancs több VIEW-ban is megjelenhet

Előnye

- VIEW és SuperViews létrehozása és módosítása csak gyökérnézetből lehetséges.
- Különbség a szerep-alapú menedzsment és a jogosultság alapú 15. szintje között az, hogy csak a Root View felhasználó hozhat létre vagy módosíthat View és SuperViewt.

Konfigurálása

Step 1

```
Router#
enable [view [view-name]]
```

Step 2

```
Router(config)#
parser view view-name
```

Step 3

```
Router(config-view)#
secret encrypted-password
```

Step 4

```
Router(config-view)#
commands parser mode {include | include-exclusive | exclude} [all]
[interface interface-name | command]
```