2.a Mire szolgál a lokális és a központosított AAA (Authentication, Authorization Accounting)? Ismertesse a szerver-alapú megvalósítás lehetőségeit és a beállítás menetét!

AAA – **A**uthentication **A**uthorization **A**ccounting

Hogyan volt eddig?

- Legegyszerűbb hitelesítési módszer: login és password
  - console, vty és aux line-on
- Könnyű implementáció, nem biztonságos
- Telnet, SSH
  - Biztonságosabb, van accounting
  - Lokális adatbázishoz felhasználónév kell
    - Naplózza a rendszer
  - Minden eszközön helyileg kell konfigurálni

Jobb megoldás

- Tartalék megoldásokat is konfiguráljunk (ha valami meghibásodik)
- Minden eszköz egy központi szerver adatbázisára épít
  - Egyszerre kezeli a hitelesítést, jogosultságkezelést

AAA felügyeli

- 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 a felhasználókat.
    - Kis hálózatokban
  - Server-based
    - központi AAA szerveren
    - Több hálózati eszközt tartalmazó hálózat esetén

Local AAA Authentication működése

1. kliens kapcsolatot létesít a forgalomirányítóval
2. Az AAA router felhasználónevet és jelszót kér
3. Router hitelesíti a felhasználót és a jelszavát a lokális adatbázis alapján
4. Adatbázisban tárolt információ alapján a felhasználó jogosult a hálózat használatára

Server-Based AAA Authentication működése

1. kliens kapcsolatot létesít a forgalomirányítóval
2. AAA router felhasználónevet, jelszót kér
3. router hitelesíti a felhasználót és a jelszavát a távoli szerver alapján
4. szerveren tárolt információ alapján a felhasználó jogosult a hálózat használatára

Jogosultság-kezelés (szerver alapú)

- Hitelesítés után automatikusan: felhasználó által kért szolgáltatásokra engedélyt kér a forgalomirányító a szervertől.
    - Milyen erőforrásokat érhet el/műveleteket hajthat végre?
- AAA authorization egy nevesített listával konfigurálható, interfészhez kell rendelni
    - Privilege level, role-based CLI-hez hasonlóan jogokat biztosít

1. hitelesítése után egy viszony alakul ki a router, szerver között
2. felhasználó megpróbál privilegizált EXEC módba lépni, a router visszaigazolást kér az AAA szervertől, rendelkezik-e a jogokkal?
3. AAA szerver visszaküld egy “PASS/FAIL” választ

AAA Accounting

Jegyzőkönyvezi a használt adatokat: kezdés, végzés időpontja, parancsok, küldött/fogadott csomagok száma

1. felhasználó hitelesítése után egy start üzenetet generál, a könyvelés megkezdődik
2. kijelentkezést stop üzenet követi, lezárul a könyvelés

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
        - TACACS+ - Terminal Access Controller Access Control System Plus
        - Diameter

Local Authentication konfigurálása

1. Lokális adatbázis konfigurálása: *Username ADMIN algorithm-type scrypt secret Password*
2. AAA engedélyezése: *aaa new-model*
3. Hitelesítési lista: *aaa authentication login*
    - milyen hitelesítési módszert vegyen figyelembe és hogy milyen sorrendben
    - Megfelelő interfészhez rendelése

Felhasználói fiókok kizárása

- Ha a sikertelen belépési kísérletek száma meghalad egy értéket
  - *aaa local authentication attempts max-fail number-of-unsuccessful-attempts*
- sikertelen belépések közt eltelt idő beállítása
  - *login delay*

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 és kliens között
Bizalmasság	Egész csomag titkosított	Csak a jelszó titkosított
Testreszabhatóság	biztosítja az útválasztó parancsok jogosultságkezelését felhasználónként vagy csoportonként	nem biztosítja
Könyvelés	Limitált	Széleskörű

Diameter – a RADIUS továbbfejlesztése

- Kapcsolatorientált, TCP vagy SCTP – port 3868, megbízható
- Ugrástól ugrásig, Végpont-Végpont biztonság
- Alkalmazási és biztonsági szint egyeztetése
- Szerver által kezdeményezett üzenetet használ
- Statikus, dinamikus konfiguráció
- Gyártó specifikus tulajdonságok és üzenetek

Szerver alapú AAA konfigurációs lépései

1. AAA engedélyezése globális konfigurációs módban: *aaa new-model*
2. Security paraméterek konfigurálása: Server IP, kulcs (az adatok titkosításához)
3. Hitelesítési lista konfigurálása: *aaa authentication*
4. Megfelelő interfészhez rendelés

Globális konfigurációs módban opcionális
- Jogosultságkezelés: *aaa authorization*
- Könyvelés: *aaa accounting*