ACL – Hozzáférés-vezérlési listák

1. Elmélet:

- **ACL – Acces Control List**

  Az **Access Control List (ACL)**, azaz hozzáférés-vezérlési lista a forgalomszűrés egyik legelterjedtebb változata. Az ACL-ek segítségével hozzáférés vezérlést biztosítunk egy erőforráshoz. Segítségükkel ellenőrizhetjük a hálózatba bejövő illetve kimenő forgalmat, és szükség esetén még szűrhetjük is azt. A forgalomszűrés javítja a hálózat teljesítményét.
  Az ACL segítségével az elosztási rétegben korlátozható a hozzáférés, és megakadályozható a nem kívánt forgalom központi hálózatba jutása. A hozzáférési listával ellenőrizhető a forgalomirányító interfészein áthaladó hálózati forgalom. Ez azt jelenti, hogy az OSI modell 3. rétegében dolgozunk, vagyis megelőzzük jóval a szoftveres védelmet. Az ACL-ek engedélyezhetnek és tilthatnak is forgalmat a megfelelő szabályokkal. Az ACL-ek megadási sorrendben hajtódnak végre, a szoftver végigmegy szabályokon, és amelyik megfelelő neki, azt végrehajtja. Ha nincs a kérésre vonatkozó meghatározás, az egyéb beállítások lépnek érvénybe.
  Háromféle ACL típus különböztethetünk meg, ezek a normál, a kiterjesztett és a nevesített ACL

  - **Normál ACL:**
    A normál ACL (Standard ACL) a legegyszerűbb a három típusból. Forrás IP-cím alapján végzi a szűrést, teljes protokollműködés alapján tiltja vagy engedélyezi a forgalmat. Ha egy ilyen ACL nem engedélyezi egy munkaállomás IP forgalmát, az erről az állomásról érkező összes szolgáltatást letiltja. Lehetőségünk van egy adott felhasználó vagy helyi hálózat számára engedélyezni az összes szolgáltatás elérését a forgalomirányítón keresztül, míg az összes többi IP-cím esetén tilthatjuk a hozzáférést. A normál ACL-ek a hozzájuk rendelt azonosítási szám alapján azonosíthatók be. Az azonosítási számnak 1 és 99, illetve 1300 és 1999 közé kell esnie.
    Pl. a *Router(config)#access list 2 permit host 172.16.1.80*; ACL a 172.16.1.80 IP címet engedélyezi.

- **Kiterjesztett ACL:**

  A kiterjesztett ACL (Extended ACL) már nem csupán a forrás IP-cím alapján, hanem a cél IP-cím, a protokoll és a portszámok segítségével is szűrhet. Sokkal elterjedtebb, mint a normál ACL, mivel jobb ellenőrzést tesz lehetővé, és specifikusabb is. Azonosítási számuknak 100 és 199, illetve 2000 és 2699 közé kell esniük.

  Pl. a *Router(config)#access list 102 permit 192.168.2.0 0.0.0.255 any*; ACL a 192.168.2.0 hálózat minden állomását engedélyezi, ugyanakkor minden mást tilt.

  Továbbá a *Router(config)#access-list 103 deny tcp any 192.168.2.0 0.0.0.255 range 20 2*; a teljes FTP forgalmat letiltja.

  A *Router(config)#access-list 101 deny tcp 195.220.0.0 0.0.255.255 0.0.0.0 0.0.0.0 eq 80*; ACL-lel tiltjuk a 195.220.0.0/16 hálózat felől a HTTP (80-as port) kéréseket bármilyen célhálózat felé.

  Az ACL definiálását egy interfészhez történő hozzárendelés követi.

```
(config)#interface Serial 0
(config-if)#ip access-group 1 out (kimenő interfész)
(config)#interface Ethernet 0
(config-if)#ip access-group 101 in (bejövő interfész)
```

- **Nevesített ACL:**

  A nevesített ACL (Named ACL, NACL): normál vagy kiterjesztett hozzáférési lista, ahol az azonosító szám helyett egy névvel hivatkozunk a listára. A nevesített ACL-ek beállításához a forgalomirányítón NACL üzemmódban kell lennünk.

2. Gyakorlati példák:

   Engedélyez → permit

   Tilt → deny

   - **Normál ACL:**
     Hozzon létre 1-es azonosítóval egy standard ACL-t, amely engedélyezi a 10.100.1.0 hálózatból a hozzáférést és rendelje az ACL-t az összes virtuális terminál vonalhoz!
     Router(config)# **access-list** 1 permit 10.100.1.0 0.0.0.255
     Roter(config)#line vty 0 15
     Router(config-line)# **access-class** 1 in
   - **Kiterjesztett ACL:**
     Hozzon létre a forgalomirányítón egy hozzáférés-vezérlési listát 101-es azonosítóval. A lista tiltsa meg a régi iskolaépület diákjainak, hogy IP-szinten elérjék a régi épület tanárhálózatát, az új épület tanárhálózatát és az új épület WiFi alhálózatát. Minden egyéb forgalom engedélyezett bármilyen irányba. (Az ACL létrehozásánál vegye figyelembe a sorrendet a korrekt pontozás érdekében!)
     Router(config)# **access-list** 101 deny ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
     Router(config)# **access-list** 101 deny ip 172.16.2.0 0.0.0.255 172.16.3.0 0.0.0.255
     Router(config)# **access-list** 101 deny ip 172.16.2.0 0.0.0.255 172.16.5.0 0.0.0.255
     Router(config)# **access-list** 101 permit ip any any
     Alkalmazza a létrehozott ACL-t a megfelelő interfészre!
     Router(config)#int f0/0
     Router(config-if)#**ip access-group** 101 in