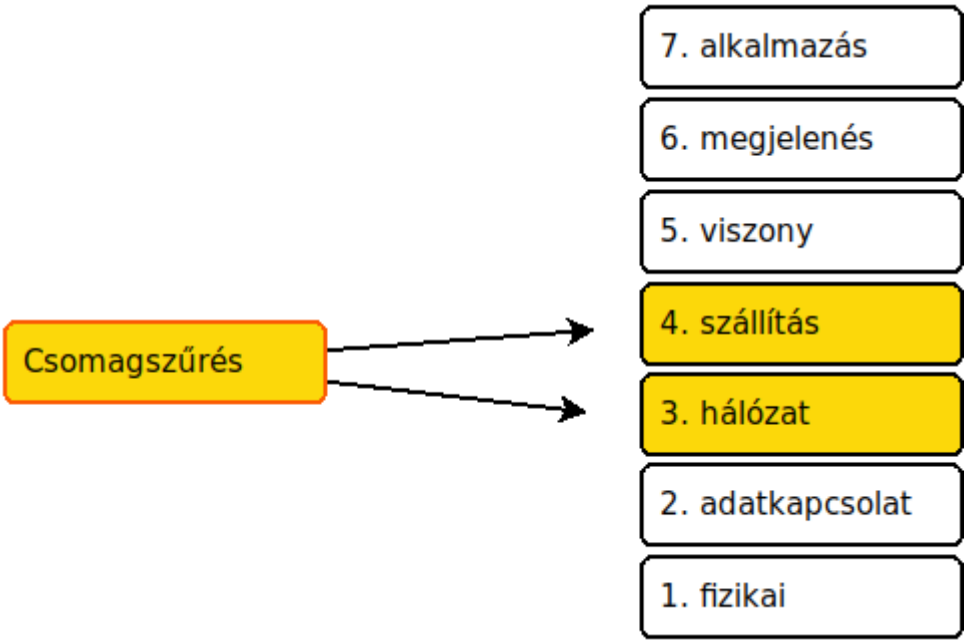
Az ACL

Az ACL az Access Control List rövidítése, magyarul hozzáférési lista. Egy forgalomirányítón a bejövő és kimenő csomagokat szűrhetjük IP címek vagy portszámok alapján.

A szűrést az OSI rétegmodell 3. és 4. rétegében végezzük.



Az ilyen szűréseket csomagszűrésnek nevezzük.

A szabályok összeállítása során a csomagok számára illeszkedési szabályokat írunk le. Az illeszkedés a következőket tartalmazhatja:

- bejövő vagy kimenő csomag
- forrás IP címre illesztés
- cél IP-re címre illesztés
- portra illesztés

A szabályhoz hozzátartozik, hogy a csomagot vagy megtartjuk vagy eldobjuk:

- engedés
- tiltás

Ezt nevezzük vezérlésnek.

A szabályokat szokás hozzáférésvezérlő bejegyzésnek vagy angolosan Access Control Entry néven nevezni; röviden ACE. De lehet simán ACL bejegyzés.

Az ACL-ek két csoportba oszthatók. Vannak a szabványos ACL-ek, amelyek csak forrás IP címre illeszthetők és vannak a kiterjesztett ACL-ek.

Csoportosítás:

- szabványos ACL
- kiterjesztett ACL

Az ACL-ek a forgalomirányító által előállított csomagokra nem vonatkoznak.

A működésről

A szabályokat sorba felvesszük, egy-egy parancs formájában.

Amikor egy csomag érkezik a forgalomirányítóra, sorba veszi a bejegyzett szabályokat, addig amíg nem talál egy illeszkedő szabályt. Ha illeszkedik egy szabályra (pl. forrás IP cím van csak megadva és arra egyezik a csomagban található információ), akkor alkalmazza a megadott utasítást, ami engedés vagy eldobás.

Ha egy csomag nem illeszkedik egyetlen szabályra sem, akkor a csomag eldobásra kerül, mivel a szabályok végén van egy implicit (ha nem állítjuk be, akkor is ott van) szabály, amit mindent tilt.

Bejövő/kimenő ACL-ek

Egy ACL konfigurálható úgy, hogy kimenő csomagokra illeszkedjen, vagy a bejövő csomagokra.

A bejövő ACL-ek hatékonyabbak, mivel ha tiltani kell egy csomagot, akkor vele megkíméljük az útválasztási folyamatban való részvételtől. Ha már kifele tiltunk, ezt nem tudjuk megtenni.

Szabványos ACL

A szabványos ACL vagy normál ACL.

Csak forrás IP cím alapján működik.

Például:

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

ACL azonosítása

Minden szabálynak szükséges egy azonosító. Az azonosítók a következők lehetnek:

- név
- szám

Használható számok:

- 1-99 és 1300-1999 szabványos IP ACL
- 100-199 és 2000-2699 kiterjesztett IP ACL

A használható nevek:

- lehet benne betű és szám
- lehet kapitális

Helyettesítő maszk kulcsszavak

- host
- any

Ezek használhatók IPv4 és IPv6 esetén is.

- 0.0.0.0 maszkot helyettesíti
- Csak egy adott állomás felé feleltetünk meg

Eredeti:

```
192.168.10.10 0.0.0.0
```

Helyette:

```
host 192.168.10.10
```

Az any kulcsszó:

A 255.255.255.255 maszk helyett használható bármely cím megadható.

Eredeti maszk:

```
0.0.0.0 255.255.255.255
```

Helyette:

```
any
```

Any host használat:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 permit any
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit host 192.168.10.10
```

Irányelvek

Hol használjunk ACL-t?

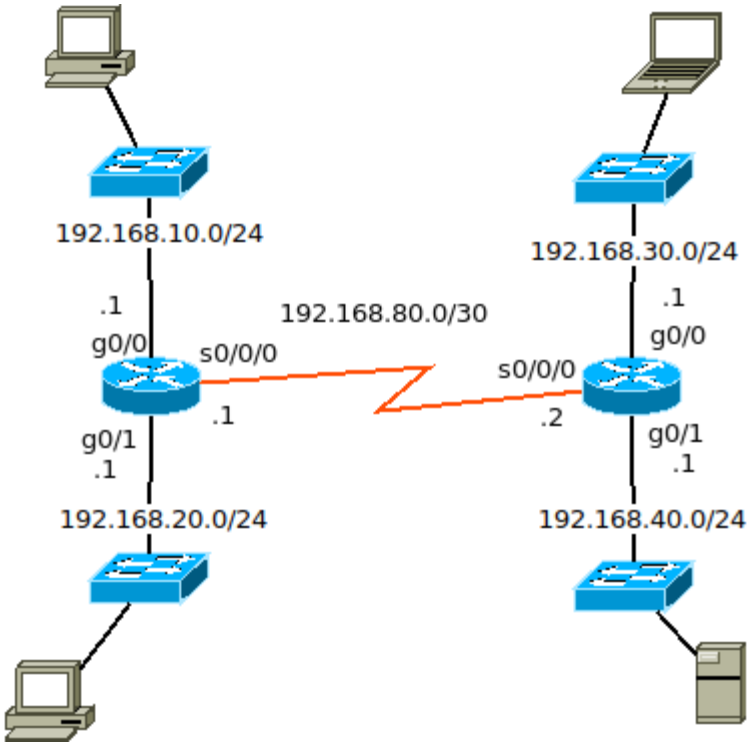
- használjuk belső és külső (Internet hálózat között
- hálózat két része között

A három P

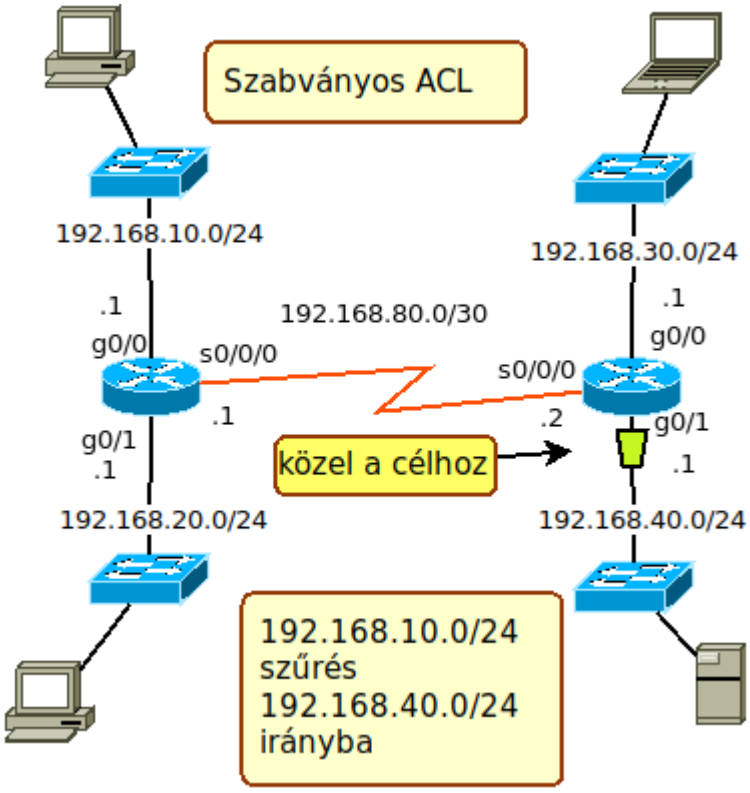
- egy ACL protokollonként
  - minden protokollhoz külön ACL
- egy ACL irányonként
  - külön bejövő és külön a kimenő
- egy ACL interfészenként

ACL-ek elhelyezése

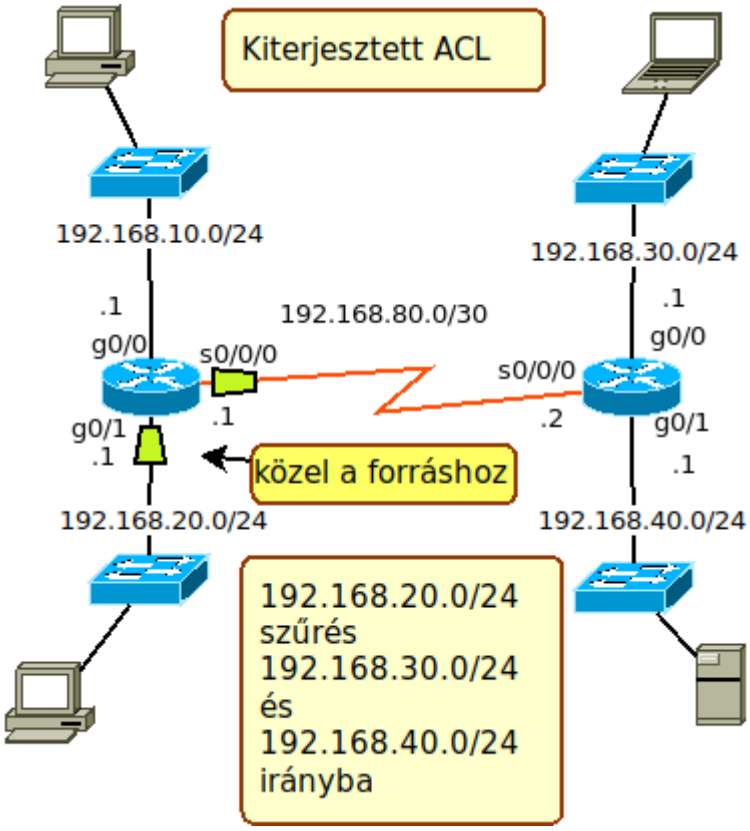
- szabványos ACL közel a célhoz.
- Kiterjesztett ACL közel a forráshoz.

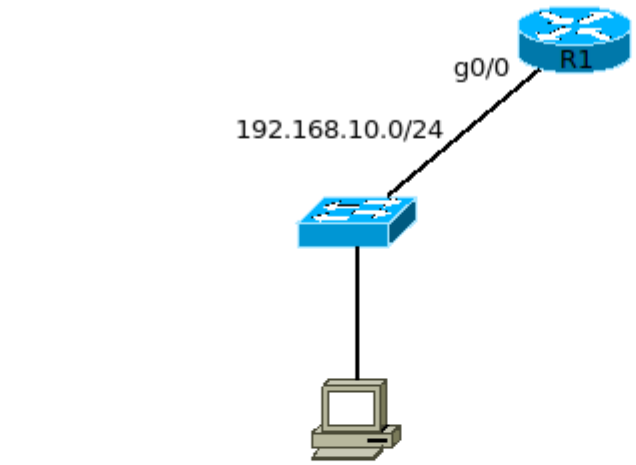


Szeretnénk szűrni a 192.168.10.0/24 hálózatból jövő csomagokat a 192.168.40.0/24 felé.



A szeretnénk a 192.168.20.0/24 hálózatból minden forgalmat szűrni a 192.168.30.0/24 és a 192.168.40.0/24 felé.



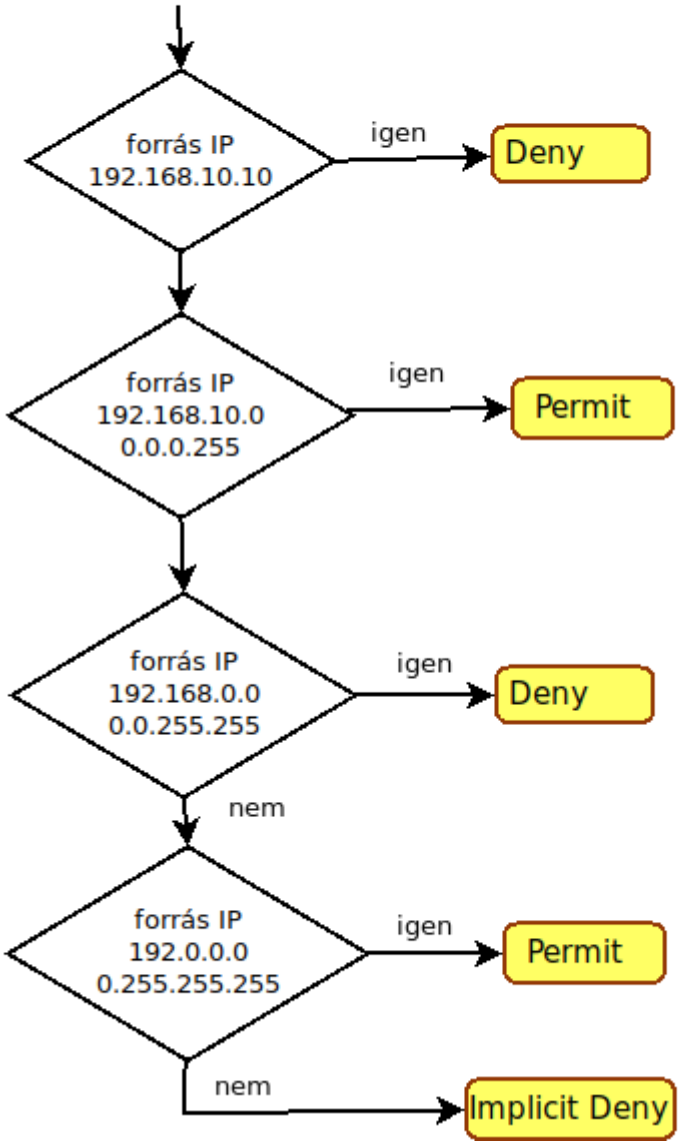



```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny any
```

azonos eredmény

```
access-list 2 deny 192.168.10.10
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 255.255.255.255
```



Szabványos ACL számozva

Lépések

Két lépés:

- beállítjuk az ACL-t
- interfészhez kötjük

Számozás

Az access-list parancsa számára első paraméterként meg kell adnunk egy számot. A szám 1-99 közötti szám. A Cisco IOS 12.0.1-től megadható a 1300-1999 közötti szám is.

Szintaxis

```
Router(config)# access-list lista_száma
```

```
{ deny | permit | remark } forrás
[ forrás_helyettesítő_maszk ][ log ]
```

- lista_száma – 1-99, 1300-1999 közötti szám, szabványos ACL esetén
- deny – tiltás
- permit – engedés
- remark – megjegyzés
- forrás – a forrás IP címe
- forrás_helyettesítő_maszk – a forrás helyettesítő maszkja
- log – naplózás

Példa

ACL létrehozása:

```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

Most lépjünk ki, nézzük meg:

```
R1#show access-list
```

Megjegyzés az ACL számhoz:

```
R1(config)#access-list 1 remark teszt megjegyzes
```

Megnézzük:

```
R1# show running-config
```

A megjegyzések maximum 100 karakter hosszúak lehetnek.

ACL megszüntetése:

```
R1(config)# no access-list 1
```

Ellenőrizzük:

```
R1# show access-list
```

Egy gép engedélyezése:

```
R1(config)# access-list 1 permit host 192.168.10.11
```

Nézzük a következ példát, ahol két bejegyzésünk van:

```
R1(config)# access-list 1 permit host 192.168.10.11
R1(config)# access-list 1 permit host 192.168.10.12
R1#show access-list
Standard IP access list 1
    10 permit host 192.168.10.11
    20 permit host 192.168.10.12
```

Itt jól látható, hogy az 1 számú listáról van szó, két bejegyzésünk van. Mindkét bejegyzés kapott egy sorszámot, 10 és 20 számmal.

Ha csinálunk két 2 számú bejegyzést, akkor listázásnál:

```
R1# show access-list
```

```
Standard IP access list 1
    10 permit host 192.168.10.11
    20 permit host 192.168.10.12
Standard IP access list 2
    10 permit host 192.168.20.11
    20 permit host 192.168.20.12
```

Interfészhez kötés

Az ACL attól, hogy létrehoztuk őket, nem fognak működni. Azokat interfészhez kell kötni.

Legyen a következő bejegyzés:

```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

Interfészhez kötéshez, lépjünk be a kívánt interfészbe.

```
R1(config)# int g0/0
```

Kössük össze az ACL-t és az interfészt:

```
R1(config-if)# ip access-group 1 in
```

Szabványos ACL névvel

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nad)# deny host 192.168.10.11
R1(config-std-nad)# permit any
R1(config-std-nad)# exit
R1(config)# interface g0/0
R1(config)# ip access-group NO_ACCESS out
```

Példa a szabványos ACL-re

Számozott

```
R1(config)# access-list 1 remark Tiltott vendég
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 remark Engedély a 192.168.x.x felől
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
R1(config-if)#
```

Nevesített

```
R1(config)#  ip access-list standard NO_ACCESS
R1(config-std-nacl)# remark Tiltjuk a Lab allomast
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# remark Engedjuk minden mast
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Ellenőrzés:

```
R1# show access-lists
R1#show ip int g0/0
```