# Fejezet 9: Hozzáférési listák 9.0.1.1 Bevezetés

# Hozzáférési listák

## Hozzáférési listák

A hálózati biztonság egy hatalmas téma, amelynek jelentős része kívül esik ezen kurzus hatókörén. Azonban egy nagyon fontos feladatot alaposan ismerniük kell a hálózati rendszergazdáknak, nevezetesen ez a hozzáférési listák (Access Control List, ACL) beállítása.

A hálózattervezők tűzfalakat alkalmaznak a hálózat védelmére, a jogosulatlan használat ellen. A tűzfalak olyan hardver vagy szoftver eszközök, amelyek megvalósítják és érvényre juttatják a hálózatbiztonsági rendszabályokat. Tekintsünk egy példát! Adott egy épület belsejében lévő szoba, zárt ajtóval! A zárat csak a kulccsal vagy belépőkártyával rendelkező jogosult személyek tudják kinyitni. Hasonlóképpen szűrik ki a tűzfalak a hálózatba való belépés előtt a jogosulatlan vagy potenciálisan veszélyes csomagokat. Egy Cisco forgalomirányítón is konfigurálhatunk egyszerű tűzfalat, amely hozzáférési listák (ACL) által biztosítja az alapvető forgalomszűrési képességeket. A rendszergazdák ACL-t használnak a hálózatukban a forgalom tiltására vagy bizonyos forgalom engedélyezésére.

Egy ACL engedélyező és tiltó utasítások sorozata, amely címekre vagy felsőbb rétegbeli protokollokra alkalmazható. A hozzáférési listák hatékony eszközök a ki- és bemenő irányú hálózati forgalom szabályozására. ACL-ek minden irányított protokollhoz megadhatók (pl.: IP, IPv6, IPX stb.)

Az ACL-ek beállításának legfőbb indoka a biztonságos hálózat kialakítása. A fejezet bemutatja, hogyan kell használni a normál és a kiterjesztett hozzáférési listákat egy Cisco forgalomirányító biztonsági megoldásának részeként, beleértve az ACL-ek alkalmazására vonatkozó javaslatokat, megfontolásokat, ajánlásokat és általános útmutatókat.

A fejezetben található tananyagok, feladatok és laborgyakorlatok lehetőséget adnak a hozzáférési listákkal kapcsolatos ismeretek fejlesztésére.

# Hozzáférési listák

## Hozzáférési listák

**Engedd meg, hogy segítsek!**

**Esetleírás**

Minden jelenlévő leír öt kérdést, amelyeket egy biztonsági ellenőrzés keretében feltesznek egy jelentkezőnek, aki egy középvállalkozás hálózati asszisztensi állására pályázik. A kérdéseket fontossági sorrendben kell rögzíteni, annak érdekében, hogy a legjobb jelölt nyerje el a munkát. Az elvárt válaszokat szintén le kell írni.

Az osztályból két kérdezőbiztos kerül kijelölésre. Az interjú folyamata a következő: A jelölt a feltett kérdésekre adott válaszok alapján léphet tovább vagy kerül kizárásra a következő szintről.

A mellékelt PDF dokumentumban találhatók a feladathoz tartozó részletes utasítások.

Végül az egész osztály együttesen beszélje meg a folyamattal kapcsolatos észrevételeit, hogy melyek engedélyezték vagy tiltották az interjú következő szintjére történő átlépést.

[Csoportos feladat - Permit Me to Assist You Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/9.0.1.2%20Permit%20Me%20to%20Assist%20You%20Instructions.pdf)

# Az IP ACL működése

## Az ACL célja

A hozzáférési lista (ACL) IOS parancsok sorozatán keresztül szabályozza, hogy a forgalomirányító továbbítsa vagy eldobja a csomagokat a bennük lévő fejléc információk alapján. Az ACL-ek az egyik leggyakrabban használt Cisco IOS szoftver funkciók.

A beállított hozzáférési listák a következő feladatokat látják el:

* Korlátozzák a hálózati forgalmat a hálózati teljesítmény növelése érdekében. Például, ha a vállalati házirend tiltja a video-átvitelt a hálózaton, akkor egy megfelelően konfigurált és alkalmazott ACL megakadályozza az ilyen típusú forgalmat. Ezáltal a hálózat terhelése jelentősen csökken, míg a teljesítménye nő.
* Biztosítják a forgalom szabályozását. Az ACL-ek segítségével az útvonalfrissítések továbbítása is korlátozható. Sávszélességet lehet megtakarítani, ha a hálózati környezet miatt nincs szükség a frissítésekre.
* Alapszintű hálózati hozzáférés-szabályozást biztosítanak. Az ACL-ek engedélyezhetik egy állomás számára a hálózat egy részének elérését, míg megtilthatják azt egy másiknak. Például lehetővé teszik, hogy a személyzeti osztály (HR) hálózatához csak jogosult felhasználók férhessenek hozzá.
* Szűrik a forgalmat annak típusa alapján. Például egy ACL engedélyezheti az e-mail forgalmat, ugyanakkor tilthatja a Telnet-et.
* Tiltják vagy engedélyezik az állomások számára a hálózati szolgáltatások elérését. Például az ACL-ek korlátozhatják a felhasználók hozzáférését az FTP- vagy a HTTP-szolgáltatásokhoz.

Alapértelmezés szerint a forgalomirányítón nincsenek hozzáférési listák konfigurálva, így az nem végez forgalomszűrést. A beérkező forgalom továbbítása kizárólag az irányítótábla információi alapján történik. Azonban, ha egy ACL elhelyezésre kerül egy interfészen, a forgalomirányító végrehajt az összes áthaladó csomagon egy további kiértékelő feladatot is, annak eldöntésére, hogy továbbítható-e az adott csomag.

A forgalom engedélyezésén és tiltásán túl, a hozzáférési listák alkalmasak a forgalom típus szerinti szétválogatására - elemzés, továbbítás, vagy további feldolgozás céljából. Például az ACL-ek használhatók a forgalom fontossági (priority) osztályokba sorolására is. Ez a képessége hasonlít egy koncert vagy sportesemény VIP-belépőjéhez. A VIP-jegy olyan jogokat biztosít a kiválasztott vendégeknek, amelyek nem illetik meg a normál jegytulajdonosokat, például elsőbbségi belépést vagy látogatást a mások számára lezárt területen.

Az ábrán egy példa topológia látható hozzáférési listákkal.

# Az IP ACL működése

## Az ACL célja

A rendszergazda hozzáférési listák segítségével vezérelheti a hálózat bejövő és kimenő forgalmát. A forgalom szabályozása lehet egyszerű engedélyezés vagy tiltás a hálózati cím szerint, vagy összetettebb szűrés az igényelt TCP-portszám alapján. Egyszerűbb megérteni az ACL működését a TCP-üzenetváltás vizsgálatával, például egy weboldal letöltési folyamatában.

**TCP-kommunikáció**

Mikor egy kliens adatokat kér egy webszervertől, az IP vezérli a kommunikációt a PC (forrás) és a szerver (cél) között. A TCP pedig a web böngésző (alkalmazás) és a hálózati szerver szoftver közötti párbeszédet irányítja.

Ha levelet küldünk, megnézünk egy weboldalt, vagy letöltünk egy fájlt, a TCP felelős az adatok szegmensekre tördeléséért, mielőtt az IP továbbítaná azokat. Szintén a TCP feladata a már megérkezett szegmensekből az adatok visszaállítása. A TCP-folyamat az esetek többségében egy olyan üzenetváltás, amelyben két hálózati állomás megegyezik az egymás közötti adattovábbításban.

A TCP összeköttetés-alapú, megbízható, bájtokból álló adatfolyam-szolgáltatás. Az összeköttetés-alapú azt jelenti, hogy a két alkalmazásnak TCP-kapcsolatot kell létesíteniük az adatcsere végrehajtása érdekében. A TCP teljes duplex protokoll, azaz a TCP-kapcsolat párokban kezeli az adatfolyamokat, mindegyiket egy adott irányban. A TCP rendelkezik adatfolyam-vezérlő mechanizmussal, amelyben a fogadó állomás korlátozni tudja a forrás által küldendő adatok mennyiségét. Továbbá a TCP-ben torlódás-kezelés is megvalósításra került.

Az 1. ábrán lévő animáció bemutatja a TCP/IP-üzenetváltás folyamatát. A TCP-szegmenseken lévő címkék mutatják azok rendeltetését: a SYN a munkamenet kezdetét; az ACK a kívánt szegmens megérkezésének nyugtázását; a FIN pedig a kapcsolat lezárását. A SYN/ACK nyugtázza, hogy az átvitel szinkronizálásra került. A TCP-adatszegmensekben lévő magasabb rétegbeli protokollok feladata az adatok továbbítása a megfelelő alkalmazáshoz.

A TCP-adatszegmensben található portszám azonosítja a kívánt alkalmazást. Például, a HTTP-t a 80-as port, az SMTP-t a 25-ös port, az FTP-t pedig 20-as és 21-es port. A 2. ábrán a TCP- és UDP-portok tartományai láthatók.

A 3-5. ábrákon példák találhatók TCP/UDP-portokra.

# Az IP ACL működése

## Az ACL célja

Hogyan használja csomagszűrésre egy ACL a TCP/IP-üzenetváltás során átküldött információt?

A csomagszűrés - amelyet néha statikus csomagszűrésnek is neveznek - a bejövő és kimenő csomagok vizsgálata alapján szabályozza a hálózati hozzáférést. Továbbítja vagy eldobja a csomagokat adott feltételek alapján, amelyek vonatkozhatnak a forrás IP-címre, cél IP-címre vagy a csomag által szállított protokollra.

A forgalomirányító csomagszűrőként működik, amikor továbbítja vagy eldobja a csomagokat a szűrési szabályok alapján. Amikor egy csomag a csomagszűrő forgalomirányítóhoz érkezik, az kiemeli a számára szükséges információt a csomag fejlécéből. Ezen információ felhasználásával a forgalomirányító döntést hoz a beállított szűrési szabály alapján, hogy továbbítsa-e vagy eldobja a csomagot. Ahogy az ábrán is látható, a csomagszűrés az OSI- vagy a TCP/IP-modell különböző rétegeiben működhet.

Egy csomagszűrő forgalomirányító szabályok alapján határozza meg, hogy engedélyezi-e vagy tiltja a forgalmat. A forgalomirányító képes a szállítási rétegben (Layer 4) való szűrésre is. Ebben az esetben a forgalomirányító a TCP- vagy UDP-szegmens forrás- és célportja alapján végezheti a csomagszűrést. A szabályok a hozzáférési listákban kerülnek meghatározásra.

Egy ACL engedélyező vagy tiltó utasítások sorozata, amelyeket hozzáférési lista bejegyzéseknek hívnak (Acces Control Entry, ACE). Ezeket a bejegyzéseket gyakran ACL-utasításoknak nevezik. Az ACE-k különféle kritériumok alapján hozhatók létre, például: forráscím, célcím, protokoll és portszám. Amikor a hálózati forgalom áthalad egy hozzáférési listával konfigurált interfészen, a forgalomirányító sorban, egymás után (szekvenciálisan) összeveti a csomagban található információt a lista minden egyes bejegyzésével, hogy meghatározza az egyezőséget. Amennyiben egyezést talál, a szabálynak megfelelően feldolgozza a csomagot (permit-deny). Ily módon lehet ACL-ekkel szabályozni a hálózathoz vagy alhálózathoz való hozzáférést.

A hozzáférési lista a forgalom kiértékeléséhez a következő információkat olvassa ki a 3. rétegbeli csomag fejlécéből:

* forrás IP-cím
* cél IP-cím
* ICMP-üzenettípus

A hozzáférési lista képes magasabb rétegbeli információk kiolvasására a Layer 4 fejlécből, ezek lehetnek:

* TCP/UDP-forrásport
* TCP/UDP-célport

# Az IP ACL működése

## Az ACL célja

**Csomagszűrés példa**

A forgalomirányító által használt csomagszűrés elvének megértéséhez képzeljük el, hogy egy őr áll egy bezárt ajtó előtt. Az őr utasításba kapta, hogy csak azokat a személyeket engedheti be az ajtón, akiknek a neve szerepel a listán. Tehát az őr azon feltétel alapján szűri az embereket, hogy a nevük szerepel-e a jogosultsági listán. Egy ACL is hasonló módon működik, döntéseket hoz beállított feltételek alapján.

Egy példa egy ACL beállítására: "A web hozzáférés engedélyezett az "A" hálózatból, de az összes többi szolgáltatás tiltott az "A" felhasználói számára. A HTTP-hozzáférés tiltott a "B" hálózatból, az összes többi elérés engedélyezett a "B" felhasználóinak." Tanulmányozzuk az ábrát, és nézzük végig a csomagszűrő által végrehajtott döntési folyamatot!

Ebben a példában a csomagszűrő a következőképpen vizsgál meg minden csomagot:

* Ha a csomag TCP SYN 80-as portszámmal az "A" hálózatból érkezik, akkor engedélyezett a továbbítása. Minden további hozzáférés tiltott ezen felhasználók számára.
* Ha a csomag TCP SYN 80-as portszámmal a "B" hálózatból érkezik, akkor nem továbbítható, blokkolt. Azonban az összes többi hozzáférés engedélyezett.

Ez csupán egy egyszerű példa, további engedélyező és tiltó szabályok konfigurálhatók adott felhasználók számára.

# Az IP ACL működése

## Az ACL célja

A hozzáférési lista által meghatározott szabályhalmaz segítségével szabályozhatók a bejövő interfészre érkező-, a forgalomirányítón keresztül továbbított- illetve a kimenő interfészen távozó csomagok. Fontos, hogy az ACL nincs hatással a forgalomirányító saját maga által indított csomagjaira.

A hozzáférési listák alkalmazhatók a bejövő vagy a kimenő forgalomra, ahogy az ábrán is látható.

* **Bejövő irányú ACL-ek** - A beérkező csomagokat még azelőtt feldolgozza a csomagszűrő, mielőtt irányításra kerülnének egy kimenő interfészhez. Egy bejövő irányú ACL azért hatékony, mert az eldobott csomagokon nem kell végrehajtani az útválasztási műveleteket, így nem okoznak azok többletterhelést. Ha a csomag átjut a szűrőn, csak akkor kerül irányításra. A bejövő irányú ACL-ek olyan csomagszűrésre a legjobbak, amikor a bemenő interfészre érkező csomagoknak csak a forráscímét kell vizsgálni.
* **Kimenő irányú ACL-ek** A beérkező csomagok irányításra kerülnek egy kimenő interfészhez, és csak ezután dolgozza fel őket a kimenő irányú ACL. Ez a hozzáférési lista akkor használható legjobban, amikor ugyanazt a szűrőt kell alkalmazni több különböző bejövő, de ugyanazon az interfészen távozó csomagokra.

Egy ACL utolsó utasítása mindig a implicit (kimondatlan) tiltás. Ez az utasítás automatikusan odakerül mindegyik ACL végére, még akkor is, ha a konfiguráció készítője nem írta oda. Az implicit tiltás semmilyen forgalmat nem engedélyez, ezért egy ACL-ben lennie kell legalább egy engedélyező utasításnak, különben minden forgalom blokkolásra kerül.

# Az IP ACL működése

## Normál és kiterjesztett IPv4 ACL-ek

A Cisco IPv4 hozzáférési listáknak két típusa van, a normál és a kiterjesztett.

**MEGJEGYZÉS**: A Cisco IPv6 ACL-ek hasonlóak az IPv4 kiterjesztett ACL-ekhez, és a fejezet későbbi részében kerülnek tárgyalásra.

**Normál ACL-ek**

A normál hozzáférési listák a forrás IPv4-cím alapján engedélyezik vagy tiltják a forgalmat. A célcím és a csomagba ágyazott portszám nem kerül kiértékelésre. Az 1. ábrán lévő példában az összes forgalom engedélyezett a 192.168.30.0/24 hálózatból. Az ACL végén található (de nem látható) impicit "deny any" utasítás miatt az összes többi forgalom blokkolásra kerül. A normál ACL-ek globális konfigurációs módban hozhatók létre.

**Kiterjesztett ACL-ek**

A kiterjesztett hozzáférési listák különféle tulajdonságaik alapján szűrik az IPv4-csomagokat:

* Protokoll típus
* Forrás IPv4-cím
* Cél IPv4-cím
* Forrás TCP- vagy UDP-port
* Cél TCP- vagy UDP-port
* Kiegészítő protokoll információk a finomhangoláshoz

A 2. ábrán, a 103-as ACL engedélyezi a forgalmat bármely 192.168.30.0/24 hálózatcímről bármely IPv4-hálózat felé, amennyiben a cél portszám 80 (HTTP). A kiterjesztett ACL-ek globális konfigurációs módban hozhatók létre.

A hozzáférési listák parancsai az elkövetkező témakörökben kerülnek kifejtésre.

**MEGJEGYZÉS**: A normál és kiterjesztett ACL-ek részletesebb ismertetése a fejezet későbbi részében található.

# Az IP ACL működése

## Normál és kiterjesztett IPv4 ACL-ek

A normál és a kiterjesztett hozzáférési listák létrehozásához használhatók számok vagy nevek, amelyek azonosítják az ACL-t és azzal együtt annak utasításait is.

A számozott ACL-ek alkalmazása hatékony módszer olyan kisebb hálózatok számára, ahol jobbára homogén a forgalom. Mivel a számok nem nyújtanak információt az ACL-ek rendeltetéséről, ezért a Cisco IOS 11.2-vel kezdődően nevek is használhatók azonosításukra.

Az ábrán a számozott és nevesített ACL-ek tervezésekor követendő szabályok összegzése látható.

A számozott ACL-ek esetében a 200-1299 tartomány kihagyásra került, mivel ezek más protokollok által használatosak (és ezek közül sok résztartomány már elavultnak számít). Bár e kurzus csak az IP hozzáférési listákat tárgyalja, álljon itt két példa a régebbi protokollok által használt ACL-sorszámokra: 600-699 között az AppleTalk, és a 800-899 között az IPX ACL található.

# Az IP ACL működése

## Helyettesítő maszkok az ACL-ekben

**Helyettesítő maszkolás**

Az IPv4 hozzáférési listák bejegyzéseiben (ACE) helyettesítő maszkokat használnak. A helyettesítő maszk egy 32 bites bináris karaktersorozat, amelyet a forgalomirányító annak megállapítására használ, hogy a cím mely bitjeinél kell egyezést keresnie.

**MEGJEGYZÉS**: Ellentétben az IPv4 ACL-ekkel, az IPv6 ACL-ekben nem használnak helyettesítő maszkot. Helyette az előtag hossza (prefix-length) határozza meg, hogy az IPv6 forrás- vagy célcím mekkora részének kell egyeznie. Az IPv6 hozzáférési listákról a fejezet későbbi részében lesz szó.

Ahogy az alhálózati maszkokban, úgy a helyettesítő maszkokban is 0-k és 1-ek jelzik, hogyan kell kezelni az IP-cím megfelelő bitjeit. Azonban a helyettesítő maszkban ezek a bitek más rendeltetésűek és eltérő szabályok szerint működnek.

Az alhálózati maszkban a bináris 1-ek és 0-k azonosítják az IP-cím hálózati, alhálózati és állomás részét. A helyettesítő maszkban lévő 1-ek és 0-k az erőforrások elérésének engedélyezésére vagy tiltásra valók az egyedi IP-címek vagy IP-címtartományok szűrése által.

A helyettesítő maszkok és az alhálózati maszkok különböző módon használják a bináris 1-et és 0-t a címegyeztetésben. A helyettesítő maszkok a következő szabályok szerint működnek:

* 0-s bit a helyettesítő maszkban - Egyezést követel a cím megfelelő bitjében.
* 1-es bit a helyettesítő maszkban - Figyelmen kívül hagyja a cím megfelelő bitjét.

Az 1. ábra bemutatja, hogyan szűrik a különböző helyettesítő maszkok az IP-címeket. A példában is látható, hogy a bináris 0 a bit kötelező egyezését jelenti, míg a bináris 1 esetén a bit figyelmen kívül hagyható.

**MEGJEGYZÉS**: A helyettesítő maszkokat gyakran inverz maszkoknak nevezik. Ennek oka az, hogy az alhálózati maszkban az 1-es egyezést, a 0-s pedig figyelmen kívül hagyást jelent, a helyettesítő maszkban pedig ennek az ellentettje igaz.

**A helyettesítő maszk használata**

A 2. ábrán lévő táblázatban egy IPv4-címre illesztett 0.0.255.255 helyettesítő maszkolás eredménye látható. Emlékezzünk, hogy a bináris 0 jelenti az egyezést!

Helyettesítő maszkot használnak még néhány IPv4 irányító protokoll konfigurálásánál is, például az OSPF engedélyezésére adott hálózaton vagy interfészen.

# Az IP ACL működése

## Helyettesítő maszkok az ACL-ekben

**Helyettesítő maszkok IPv4-hálózatokhoz**

A helyettesítő maszkok kiszámítása némi gyakorlatot igényel. Az 1. ábrán három példa látható a helyettesítő maszkokra.

Az első példában lévő helyettesítő maszk azt határozza meg, hogy a 192.168.1.1 IPv4-címben minden bitnek pontosan kell egyeznie.

A második példában a helyettesítő maszk azt jelenti, hogy az bármivel egyezni fog.

A harmadik példában lévő helyettesítő maszk azt határozza meg, hogy a 192.168.1.0/24 hálózat címei felelnek meg az egyezésnek.

Ezek a példák egyszerűek és könnyen érthetők. De a helyettesítő maszk kiszámítása jóval bonyolultabb is lehet.

**Helyettesítő maszkok címtartományokhoz**

A 2. ábrán található két példa bonyolultabb. Az első példában a cím első két oktettjének és a harmadik oktett első négy bitjének pontosan egyeznie kell. A harmadik oktett utolsó négy bitje és a negyedik oktett bármilyen értéket kaphat. Ennek eredményeképp a maszk által vizsgált hálózati címtartomány a 192.168.16.0 - 192.168.31.255.

A második példában lévő helyettesítő maszk egyezést keres az első két oktettben és a harmadik oktett utolsó bitjében. Az utolsó oktett és a harmadik oktett első hét bitje bármilyen érték lehet. A maszk engedélyezni vagy tiltani fogja a 192.168.0.0 főhálózat páratlan sorszámú alhálózatainak összes állomását.

# Az IP ACL működése

## Helyettesítő maszkok az ACL-ekben

A helyettesítő maszk kiszámítása kihívást jelenthet. Egy gyors módszer erre, ha a 255.255.255.255 értékéből kivonjuk az alhálózati maszkot.

**Helyettesítő maszk számítás: 1. példa**

Az ábrán levő első példában a 192.168.3.0 hálózat összes felhasználója számára engedélyezni szeretnénk a hozzáférést. Mivel az alhálózati maszk 255.255.255.0, ezért a 255.255.255.255-ből kivonjuk a 255.255.255.0-t. Eredményként a 0.0.0.255 helyettesítő maszkot kapjuk.

**Helyettesítő maszk számítás: 2. példa**

A második példában a 192.168.3.32/28 alhálózat 14 felhasználója számára szeretnénk hálózati hozzáférést engedélyezni. Az alhálózathoz tartozó maszk 255.255.255.240, így a 255.255.255.255-ből kivonjuk a 255.255.255.240-t. Így az eredményként kapott helyettesítő maszk a 0.0.0.15.

**Helyettesítő maszk számítás: 3. példa**

A harmadik példában csak két hálózatot szeretnénk engedélyezni, a 192.168.10.0-t és a 192.168.11.0-t. Ismét vonjuk ki a 255.255.255.255-ből a két hálózatot egybefogó alhálózati maszkot, ami jelen esetben 255.255.254.0 lesz. Az eredmény 0.0.1.255.

A példát megvalósíthatjuk az alábbi két utasítás segítségével is:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.11.0 0.0.0.255**

De sokkal hatékonyabb a következő konfiguráció:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.1.255**

Gondoljuk át az alábbi konfigurációt, ahol a 192.168.16.0-tól 192.168.31.0-ig hálózattartományt engedélyezzük:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.17.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.18.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.19.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.20.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.21.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.22.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.23.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.24.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.25.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.26.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.27.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.28.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.29.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.30.0 0.0.0.255**

R1(config)# **access-list 10 permit 192.168.31.0 0.0.0.255**

Az előző 16 konfigurációs utasítás helyettesíthető az alábbi egyetlen eggyel, ha a megfelelő helyettesítő maszkot használjuk:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**

# Az IP ACL működése

## Helyettesítő maszkok az ACL-ekben

**A helyettesítő maszkbitek kulcsszavai**

A bináris helyettesítő maszkbitek decimális jelölésmódjával nehézkes dolgozni. A folyamat egyszerűsíthető a **host** és **any** kulcsszavak segítségével, amelyeket gyakran használnak a helyettesítő maszkolásban. A kulcsszavak szükségtelenné teszik a helyettesítő maszk beírását, ha egy adott állomásról vagy az egész hálózatról van szó. Továbbá egyszerűsítik az ACL olvasását, mivel jól látható vezérfonalat biztosítanak a forrás és cél kritériumokhoz.

A **host** kulcsszó a 0.0.0.0 maszkot helyettesíti. Ez a maszk azt jelenti, hogy az összes IPv4-címbitnek egyeznie kell, azaz csak egy adott állomás felel meg a kritériumnak.

Az **any** kulcsszó egyszerre helyettesíti az IP-címet és a 255.255.255.255 maszkot. Ez azt jelenti, hogy a teljes IP-cím figyelmen kívül hagyható, azaz bármely cím elfogadható.

**1. példa: Helyettesítő maszkolás egyedi IP-cím esetén.**

Az ábrán látható 1. példában a **192.168.10.10 0.0.0.0**beírása helyett használható a **host 192.168.10.10**.

**2. példa: Helyettesítő maszkolás minden IP-címre.**

Az ábrán látható 2. példában a **0.0.0.0 és 255.255.255.255**beírása helyett használható az **any** önmagában is.

**MEGJEGYZÉS**: A **host** és **any** kulcsszavak az IPv6 ACL-ek konfigurálásakor is használhatók.

# Az IP ACL működése

## Helyettesítő maszkok az ACL-ekben

**Az** **any és a** **host kulcsszavak**

Az ábrán levő 1. példa bemutatja az **any** kulcsszó használatát a 0.0.0.0 IPv4-cím és 255.255.255.255 helyettesítő maszk rövidítésére.

A 2. példa bemutatja a **host** kulcsszó használatát a helyettesítő maszk rövidítésére egyedi állomáscím esetén.

# Az IP ACL működése

## Útmutató ACL létrehozáshoz

Az ACL-ek megszerkesztése nem mindig egyszerű feladat. Minden interfészre nézve különféle szabályok lehetnek, amelyeknek szabályoznia kell az interfészre bejövő vagy azon távozó forgalmat. Az ábrán lévő forgalomirányító mindkét interfésze rendelkezik IPv4- és IPv6-konfigurációval is. Ha mindkét protokoll igényel ACL-eket, mindkét interfészen és mindkét irányban, akkor összesen nyolc ACL-re lesz szükség. Ez interfészenként négy ACL-t jelent, kettőt-kettőt az IPv4 és az IPv6 számára, protokollonként egyet kimenő, egyet pedig bejövő irányban.

**MEGJEGYZÉS**: Az ACL-eket nem kötelező mindkét irányban konfigurálni. Az interfészen alkalmazott ACL-ek száma és iránya a megvalósításra kerülő igényektől függ.

Néhány irányelv az ACL-ek használatához:

* Használjunk ACL-eket a belső és a külső hálózat (pl.: internet) között elhelyezett forgalomirányítókon.
* Használjunk ACL-eket saját hálózatunk két része között lévő forgalomirányítón a beérkező és távozó forgalom szabályozására.
* Konfiguráljunk ACL-t a határ forgalomirányítókon, tehát azokon, amelyek saját hálózatunk peremén helyezkednek el. Ez alapvető ütközőként szolgál a külső hálózat felől, vagy saját hálózatunk kevésbé felügyelt és érzékenyebb területe között.
* Konfiguráljunk ACL-t minden protokollhoz a határ forgalomirányító interfészein.

**A három P**

A forgalomirányítón alkalmazott ACL alapvető szabályát a könnyebb megjegyezhetőség miatt "három P"-nek is nevezik. Azaz, egy darab ACL-t konfigurálhatunk per protokoll, per irány és per interfész alapon.

* **Egy ACL protokollonként** - Ha szabályozni szeretnénk egy adott interfész forgalmát, akkor a rajta engedélyezett protokollok mindegyikéhez külön ACL-t kell készíteni.
* **Egy ACL irányonként** - Az ACL egy interfészen egyszerre csak egy irány forgalmát szabályozza. Két különböző ACL-t kell konfigurálni a bejövő és a kimenő forgalom szabályozásához.
* **Egy ACL interfészenként** - Az ACL egy adott interfészen szabályozza a forgalmat, például a GigabitEthernet 0/0-n.

# Az IP ACL működése

## Útmutató ACL létrehozáshoz

Az ACL-ek használata a részletekre való odafigyelést és nagy körültekintést igényel. A hibák költségeket okozhatnak az állásidő, a hibaelhárítási műveletek és a gyenge hálózati szolgáltatások miatt. Az ACL konfigurálása előtt alapos tervezés szükséges. Az ábrán az ACL használatának bevált módszerei láthatók.

# Az IP ACL működése

## Útmutató az ACL elhelyezéséhez

Az ACL alkalmas elhelyezésével hatékonyabb hálózati működés érhető el, csökkenthető a felesleges forgalom. Például azt a forgalmat, amelyet egy távoli állomás le fog majd tiltani, nem szükséges továbbítani, hogy az majd feleslegesen foglalja az útvonalon lévő erőforrásokat.

Minden ACL-t ott kell elhelyezni, ahol a legnagyobb hatást fejti ki a teljesítményre. Ahogy az ábrán is látható, az alapvető szabályok:

* **Kiterjesztett ACL-ek** - Helyezzük a kiterjesztett ACL-t minél közelebb a szűrendő forgalom forrásához. Így a nemkívánatos forgalom már a forrás hálózatnál eldobásra kerül és nem halad végig a hálózati infrastruktúrán.
* **Normál ACL-ek** - Mivel a normál ACL-ek esetében nincs lehetőség célcím megadására, helyezzük ezeket minél közelebb a célállomáshoz. Ha egy normál ACL a forgalom forrásához kerül, akkor megakadályozza ezen az interfészen keresztül minden más hálózat elérését is.

Az ACL elhelyezése, így a használt ACL-típusa függ még a következőktől is:

* **A hálózati rendszergazda által felügyelt terület nagysága** - Az ACL elhelyezése függ attól, hogy a hálózati rendszergazdának van-e felügyeleti joga a forrás és célhálózat felett.
* **Az érintett hálózatok sávszélessége** - A felesleges forgalom a forrásnál történő szűrése megakadályozza, hogy a nem kívánt átvitel feleméssze a sávszélességet a célhoz vezető útvonalon. Ez különösen fontos az alacsony sávszélességű hálózatok esetén.
* **Konfiguráció egyszerűsítés** - Ha a hálózati rendszergazda különböző hálózatokból érkező forgalmat szeretne tiltani, akkor az egyik lehetőség az, hogy elhelyez egy normál ACL-t a célhoz legközelebb eső forgalomirányítón. A megoldás hátránya, hogy az ezekből a hálózatokból jövő forgalom feleslegesen használja a sávszélességet. Használható kiterjesztett ACL is a forgalmat indító forgalomirányítókon. Ez a megoldás sávszélességet takarít meg a forrásnál alkalmazott szűrés révén, de kiterjesztett ACL konfigurálását igényli több forgalomirányítón.

**MEGJEGYZÉS**: A CCNA minősítés követelményeinek alapvető szabálya, hogy a kiterjesztett ACL-eket a forráshoz lehető legközelebb, míg a normál ACL-eket a célhoz kell lehető legközelebb elhelyezni.

# Az IP ACL működése

## Útmutató az ACL elhelyezéséhez

Egy normál ACL csak a forráscím alapján képes a forgalomszűrésre. Alapvető szabály a normál ACL elhelyezésére, hogy tegyük azt a lehető legközelebb a célhálózathoz. Így a forgalom eljut minden hálózatba, kivéve azt, ahol a csomagok szűrése történik.

Az ábrán a rendszergazda gátolni szeretné a 192.168.10.0/24 hálózatból a 192.168.30.0/24 hálózat elérését.

Ha a normál ACL-t az R1 kimenő interfészére helyezi, akkor megakadályozza a 192.168.10.0/24 hálózatból minden olyan hálózat elérését, amely az R1 Serial 0/0/0 interfészén keresztül érhető el.

Követve a normál ACL-nek a célhoz legközelebb való elhelyezésére vonatkozó alapvető irányevet, az ábrán két lehetőség kínálkozik a normál ACL alkalmazására:

* **R3 S0/0/1 interfész** - A 192.168.10.0/24 hálózatból érkező forgalmat letiltó ACL elhelyezése a bejövő S0/0/1 interfészen meg fogja akadályozni a 192.168.30.0/24 hálózat elérését, de egyúttal az összes többiét is, melyek az R3-on keresztül érhetők el. Ebbe beleértendő a 192.168.31.0/24 hálózat is. Mivel az ACL célja csak a 192.168.30.0/24 hálózatba tartó forgalom szűrése, így az nem használható ezen az interfészen.
* **R3 G0/0 interfész** - A normál ACL alkalmazása a G0/0 interfészt elhagyó forgalomra ki fogja szűrni a 192.168.10.0/24-ból 192.168.30.0/24-ba tartó csomagokat. Az R3-ról elérhető más hálózatokra nem lesz hatással, a 192.16810.0/24-ból érkező csomagok eljutnak a 192.168.31.0/24 hálózatba.

# Az IP ACL működése

## Útmutató az ACL elhelyezéséhez

Hasonlóan a normál ACL-hez, a kiterjesztett ACL is képes forgalomszűrésre forráscím alapján, továbbá lehetőséget biztosít a célcím, a protokoll és a portszám szerinti vizsgálatra is. Ez nagyobb rugalmasságot enged a hálózati rendszergazdák számára a szűrendő forgalom típusának kiválasztásában és az ACL elhelyezésében. Az alapszabály a kiterjesztett ACL esetében az, hogy legyen minél közelebb a forráshoz. Ez megakadályozza a nemkívánatos forgalom keresztülhaladását az egész hálózaton, amelynek a végén az egyébként is eldobásra kerülne.

A hálózati rendszergazda csak az általa felügyelt eszközökön tud ACL-eket elhelyezni, ezért a hozzáférési listák elhelyezését a felügyeleti kör figyelembe vételével kell megtervezni. A példában az "A" vállalat rendszergazdája, akihez a 192.168.10.0/24 és a 192.168.11.0/24 hálózat tartozik (rövidítve .10 és .11 a későbbiekben), felügyelni kívánja a "B" vállalat felé tartó forgalmat. Konkrétan, tiltani akarja a .11 hálózatból a "B" vállalat 192.168.30.0/24 hálózatába (.30 a továbbiakban) tartó Telnet és FTP csomagokat. Ugyanakkor, minden más forgalmat engedélyezni kell a .11 hálózatból, amely az "A" vállalatot elhagyja.

Ezen célok végrehajtásának többféle módja van. Egy R3-on elhelyezett, Telnet és FTP forgalmat blokkoló kiterjesztett ACL megoldaná a feladatot, de a rendszergazdának nincs jogosultsága az R3 felügyeletéhez. Ráadásul, ebben az esetben a nem kívánt forgalom keresztülhalad az egész hálózaton, és csak a célnál kerül blokkolásra, amely hatással van az egész hálózat teljesítményére.

Jobb megoldás egy kiterjesztett ACL elhelyezése az R1-en, megadva a forrás és célcímeket (.11 és .30 hálózatok), valamint érvényre juttatva a szabályt: "Tiltott a Telnet és az FTP forgalom a .11-es hálózatból a .30-as hálózatba". Az ábrán látható az R1 két lehetséges interfésze, amelyekre a kiterjesztett ACL ráilleszthető:

* **R1 S0/0/0 interfész (kimenő)** - Az egyik lehetőség a kiterjesztett ACL elhelyezése az S0/0/0 interfészen, kimenő irányban. Mivel az ACL vizsgálja mind a forrás, mind a célcímeket, csak a 192.168.11.0/24 hálózatból érkező Telnet- és FTP-csomagok kerülnek eldobásra. A 192.168.11.0/24-ból és a többi hálózatokból érkező minden más forgalmat az R1 továbbítja. Az ACL ezen interfészen való elhelyezésének az a hátránya, hogy az S0/0/0 interfészt elhagyó összes forgalmat az ACL-nek fel kell dolgoznia, beleértve a 192.168.10.0/24-ból érkező csomagokat is.
* **R1 G0/1 interfész (bejövő)** - A kiterjesztett ACL illesztése a G0/1 bejövő forgalmára azt jelenti, hogy csak a 192.168.11.0/24 hálózatból érkező csomagok kerülnek feldolgozásra az R1-en. Mivel a szűrő csak a 192.168.11.0/24 hálózatot elhagyó csomagokra vonatkozik, a kiterjesztett ACL G0/1 interfészen való elhelyezése a legjobb megoldás.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

A forgalomirányítóba belépő csomagok összehasonlításra kerülnek a hozzáférési lista minden bejegyzésével (ACE), abban a sorrendben, ahogy az ACL-ben szerepelnek. A forgalomirányító addig folytatja az ACE-k feldolgozását, amíg egyezést nem talál. A csomagok vizsgálata csak eddig az első találatig tart, a többi bejegyzés nem kerül ellenőrzésre.

Ha a forgalomirányító nem talál egyezést a lista végéig, elutasítja a forgalmat. Ez azért van, mert alapértelmezés szerint az ACL végén egy implicit tiltás található a konfigurált bejegyzésekkel nem megegyező forgalom szűrésére. Az olyan ACL, amelyben csak egy tiltó bejegyzés van, minden forgalmat elutasít. Tehát legalább egy engedélyező utasításnak lenni kell az ACL-ben, különben minden blokkolódik.

Az ábrán lévő hálózatban, mindkét ACL kimenő irányban történő alkalmazása az R1 S0/0/0 interfészén azonos eredményre vezet. Míg a 192.168.10.0 hálózatból engedélyezett a hozzáférés az S0/0/0-n keresztül, addig a 192.168.11.0-ból ezek a hálózatok nem érhetők el.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

**A normál ACL algoritmusa**

Ahogy az ábrán is látható, a G0/0 interfészen érkező csomagok forráscímük alapján az alábbi bejegyzések szerint kerülnek vizsgálatra:

**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 0.255.255.255**

Amelyik csomagok engedélyezettek, azok továbbításra kerülnek a forgalomirányító egyik kimenő interfészére. Az elutasított csomagok már a bejövő interfészen eldobásra kerülnek.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

**Normál ACL-ek konfigurálása**

Számozott normál ACL-ek Cisco forgalomirányítón történő használatához először konfigurálnunk kell a normál ACL-t, majd aktiválni kell azt egy interfészen.

Az **access-list** globális konfigurációs parancs az 1 és 99 közötti listasorszámmal egy normál ACL-t definiál. A Cisco IOS 12.0.1 verziójától a normál ACL-ek számozására a 1300 és 1999 közötti tartományra is alkalmas. Így összesen 798 normál ACL hozható létre. Ezt az újabb tartományt kibővített IP ACL-nek nevezik.

A normál ACL-utasítások teljes szintaxisa a következő:

Router(config)# **access-list** *hozzáférési lista száma* { **deny** | **permit** | **remark** } *forrás* [ *forrás helyettesítő maszkja* ][ **log** ]

Az 1. ábrán a normál ACL szintaxisának részletes magyarázata található.

A listabejegyzések (ACE) tilthatnak vagy engedélyezhetnek egy egyedi állomást, vagy állomáscímek egy tartományát is. A 10-es sorszámú ACL-ben a 192.168.10.10 IP-című állomásra vonatkozó engedélyezésre gépeljük be a következőt:

R1(config)# **access-list 10 permit host 192.168.10.10**

Ahogy a 2. ábrán látható, a 10-es sorszámú ACL-ben a 192.168.10.0/24 hálózat összes IPv4-címére vonatkozó engedélyezésre gépeljük be a következőt:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.0.255**

Az ACL törléséhez használjuk a **no access-list** parancsot globális konfigurációs módban. A **show access-list** parancs kiadásával ellenőrizhetjük a hozzáférési lista eltávolítását.

Amikor egy rendszergazda létrehoz egy ACL-t, az utasítás rendeltetését ismeri és tudja. De a rendszergazda és mások emlékezetének frissítése céljából megjegyzés is illeszthető a parancsba. A **remark** kulcsszó használatával dokumentálható és érthetőbbé tehető a hozzáférési lista. A megjegyzés legfeljebb 100 karakter hosszú lehet. A 3. ábrán egy meglehetősen egyszerű ACL példája látható. Ha megtekintjük az ACL-konfigurációt a **show running-config** paranccsal, a megjegyzések is kiírásra kerülnek.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

A Cisco IOS egy belső logika szerint fogadja el és dolgozza fel az ACE-ket. Ahogy arról a korábbiakban már szó esett, a listabejegyzések szekvenciálisan kerülnek kiértékelésre, tehát a beírt ACE-k sorrendje nagyon fontos.

Például az 1. ábrán levő ACL két listabejegyzést tartalmaz. Az első ACE helyettesítő maszkkal tilt egy címtartományt, amelybe a 192.168.10.0/24 hálózat összes állomása beletartozik. A második ACE egy "host" utasítás, amely a 192.168.10.10 című állomást vizsgálja. Ez a cím része az előző utasításban konfigurált címtartománynak, más szóval a 192.168.10.10 állomás benne van a 192.168.10.0/24 hálózatban. Az IOS normál hozzáférési listájának belső algoritmusa elveti a második utasítást és hibaüzenetet küld arról, hogy ez már része egy korábbi bejegyzésnek. Figyeljük meg az ábrán, hogy a forgalomirányító automatikusan a 10-es sorszámot rendelte az elsőként bevitt utasításhoz. A forgalomirányító üzenetében az olvasható, hogy a kérdéses szabály "már része a létező 10-es számú szabálynak", ezért nem fogadja el az utasítást.

**MEGJEGYZÉS**: Jelenleg a kiterjesztett ACL-ek nem hoznak létre hasonló hibaüzenetet.

A 2. ábrán levő ACL 4-ben ugyanez a két utasítás található, csak fordított sorrendben. Így helyes a parancsok sorrendje, mivel az első egy adott állomásra vonatkozik, nem pedig egy tartományra.

A 3. ábrán levő ACL 5 bemutatja, hogy konfigurálható "host" utasítás egy tartományt jelölő utasítást követően is, de ekkor az állomás nem tartozhat egy korábbi utasításban szereplő tartományba. Mivel a 192.168.11.10 állomáscím nem része a 192.168.10.0/24 hálózatnak, így ez egy érvényes utasítás.

**MEGJEGYZÉS**: A normál hozzáférési lista bejegyzéseinek beviteli sorrendje nem feltétlenül egyezik meg a forgalomirányítón való tárolásuk, megjelenítésük és feldolgozásuk sorrendjével. Erről a fejezet későbbi részében esik majd szó.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

**A normál ACL beállításának lépései**

Miután a normál ACL konfigurálása megtörtént, csatoljuk azt egy interfészhez az **ip access-group** paranccsal interfész konfigurációs módban.

Router(config-if)# **ip access-group** { *hozzáférési lista száma* | *hozzáférési lista neve* } { **in** | **out** }

Egy ACL interfészről való eltávolításához gépeljük be a **no ip access-group** parancsot az interfészen, majd használjuk a globális **no access-list** parancsot a teljes ACL eltávolításához.

Az 1. ábrán egy számozott normál hozzáférési lista konfigurálásának és alkalmazásának lépései, azok szintaxisai láthatók.

A második ábrán levő példa egy szóló hálózatot engedélyező ACL-t mutat be.

Ez a hozzáférési lista csak a 192.168.10.0 forráshálózatból származó forgalmat engedi továbbítani a S0/0/0 interfészen keresztül. A többi hálózatból származó csomagok blokkolásra kerülnek.

Az első sor azonosítja az ACL-t az 1-es sorszámmal, és engedélyezi a forgalmat a beállított paramétereknek megfelelően. Ebben az esetben az IPv4-cím és helyettesítő maszk jelöli ki a 192.168.10.0 0.0.0.255 forrás hálózatot. Emlékezzünk, hogy a lista végén egy implicit "deny any" parancs áll, amely egyenértékű a következő utasítással: **access-list 1 deny 0.0.0.0 255.255.255.255**!

Az **ip access-group 1 out** interfész konfigurációs parancs köti össze az ACL 1-t a Serial 0/0/0 interfésszel és adja meg a szűrés kimenő irányát.

Tehát az ACL 1 kizárólag a 192.168.10.0/24 hálózat állomásinak forgalma számára teszi lehetővé az R1 forgalomirányító elhagyását. Minden más hálózattól megtagadja azt, beleértve a 192.168.11.0-t is.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

Az 1. ábra egy olyan ACL-t mutat be, amely engedélyez egy alhálózatot, kivéve annak egy állomását.

Ez az ACL helyettesíti az előző példában levőt, továbbá blokkolja egy adott állomás forgalmát. Az első parancs törli a korábbi ACL 1-t. A következő ACL-utasítás tiltja a 192.168.10.10 című PC1-t. Majd jön a 192.168.10.0/24 hálózat többi állomását engedélyező parancs. Végül az implicit "deny any" tilt minden további hálózatot.

Az ACL újból alkalmazásra kerül a S0/0/0 interfészen kimenő irányban.

A 2. ábrán látható ACL csak egy adott állomást tilt. Ez az ACL is felváltja az előző példában levőt, tiltja a PC1 állomást, de minden más forgalmat engedélyez.

Az első két parancs azonos a korábbi példák utasításaival. Az első törli az ACL 1-t, a második pedig tiltja a 192.168.10.10 című PC 1-t.

A harmadik sor új, engedélyez minden más állomást. Ez azt is jelenti, hogy a 192.168.10.0/24 hálózat állomásai engedélyezettek, kivéve az előző utasításban letiltott PC 1-t.

Ez az ACL a G0/0 interfészre kerül bejövő irányban. Mivel a szűrő csak a 192.168.10.0/24 LAN-ra vonatkozik, sokkal hatékonyabb a bejövő interfészen való elhelyezése. Alkalmazható lenne még a S0/0/0-on kimenő irányában, de akkor az R1-nek fel kellene dolgoznia az összes hálózat forgalmát, beleértve a 192.168.11.0/24-t is.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

Az ACL elnevezése megkönnyíti funkciójának értelmezését. Például, egy FTP tiltására konfigurált ACL neve lehet NO\_FTP. A névvel azonosított ACL konfigurációs módja és parancsszintaxisa kis mértékben eltérő a számozott ACL-hez képest.

Az 1. ábra a nevesített normál ACL létrehozásának lépéseit mutatja.

**1. lépés** Használjuk az **ip access-list** parancsot globális konfigurációs módban a nevesített hozzáférési lista létrehozására. Az ACL neve alfanumerikus karakterekből áll, nagybetű érzékeny, és egyedinek kell lennie. Az **ip access-list standard** *név* parancs szolgál a nevesített normál ACL, míg az **ip access-list extended** *név* a kiterjesztett hozzáférési lista létrehozására. A parancs végrehajtása után a forgalomirányító nevesített normál hozzáférési lista módba kerül, ahogy ezt a prompt is jelzi.

**MEGJEGYZÉS**: A számozott ACL-ek globális konfigurációs parancsa az **access-list** , míg a nevesített IPv4 ACL-eké az **ip access-list** .

**2. lépés** A nevesített ACL konfigurációs módban a **permit** vagy a **deny** utasításokat használjuk a csomagok továbbítását engedélyező vagy tiltó feltételek meghatározásához.

**3. lépés** Alkalmazzuk az ACL-t egy interfészen az **ip access-group** parancs használatával. Adjuk meg, hogy az ACL az interfészre beérkező (**in**) vagy az onnan távozó (**out**) csomagokra vonatkozzon.

A 2. ábrán egy nevesített normál ACL létrehozása látható az R1 G0/0 interfészén, amely tiltja a 192.168.11.10 állomást a 192.168.10.0 hálózat elérésében. Az ACL neve NO\_ACCESS.

A hozzáférési lista nevének nagybetűvel írása nem kötelező, de szembeötlővé teszi a konfiguráció listázásakor. Továbbá megelőzi az olyan véletlen eseteket, amikor két különböző ACL-t hoznánk létre azonos névvel, csupán a nagybetűs írásmódban való eltéréssel.

# Normál IPv4 ACL-ek

## Normál IPv4 ACL-ek konfigurálása

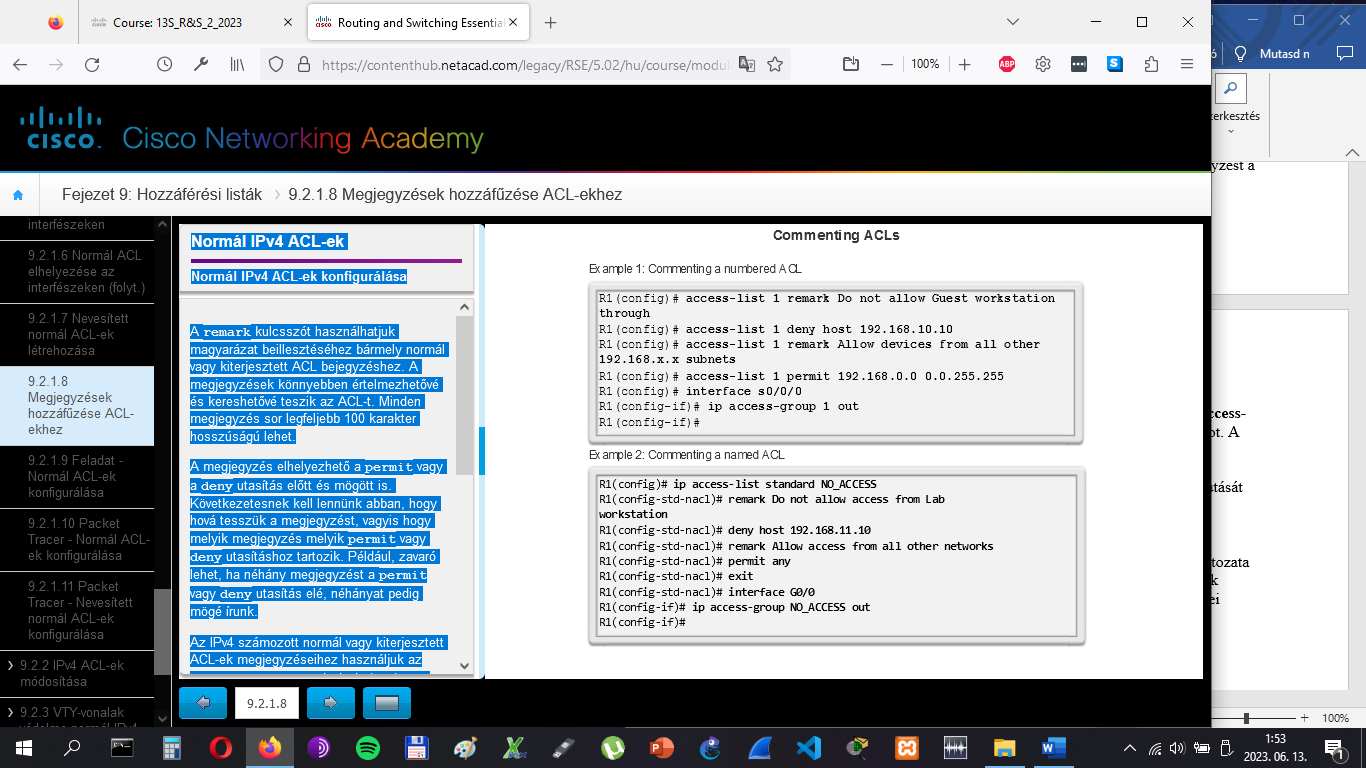
A **remark** kulcsszót használhatjuk magyarázat beillesztéséhez bármely normál vagy kiterjesztett ACL bejegyzéshez. A megjegyzések könnyebben értelmezhetővé és kereshetővé teszik az ACL-t. Minden megjegyzés sor legfeljebb 100 karakter hosszúságú lehet.

A megjegyzés elhelyezhető a **permit** vagy a **deny** utasítás előtt és mögött is. Következetesnek kell lennünk abban, hogy hová tesszük a megjegyzést, vagyis hogy melyik megjegyzés melyik **permit** vagy **deny** utasításhoz tartozik. Például, zavaró lehet, ha néhány megjegyzést a **permit** vagy **deny** utasítás elé, néhányat pedig mögé írunk.

Az IPv4 számozott normál vagy kiterjesztett ACL-ek megjegyzéseihez használjuk az **access-list** *hozzáférési lista száma* **remark** *megjegyzés szövege* globális konfigurációs parancsot. A megjegyzés eltávolítására a parancs **no** előtaggal ellátott változata szolgál.

Az első példában levő számozott ACL tiltja a 192.168.10.10 vendég munkaállomás kijutását az S0/0/0-on, de engedélyez minden eszközt a 192.168.0.0/16-ból.

Nevesített normál vagy kiterjesztett ACL esetén használjuk a **remark** hozzáférési lista konfigurációs parancsot. A megjegyzés eltávolítására a parancs **no** előtaggal ellátott változata szolgál. A 2. példában egy nevesített normál ACL látható, amelyben a megjegyzés sorok jelzik, hogy a 192.168.11.10 című labor munkaállomás tiltott, de más hálózatok eszközei mind engedélyezettek.



# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

**Számozott ACL-ek szerkesztése**

Ha normál ACL-t konfigurálunk, az utasítások bekerülnek az aktív konfigurációba, ahol nincs beépített szerkesztési lehetőség a hozzáférési lista módosítására.

Két módszer létezik a számozott normál hozzáférési lista szerkesztésére.

**1. módszer: Szövegszerkesztő használata**

Ha valaki már otthonosan mozog egy ACL létrehozásában és összeállításában, akkor azt a parancssor helyett sokkal egyszerűbben is megteheti egy szövegszerkesztőben, például a Microsoft Jegyzettömbben. Ez lehetőséget ad az ACL létrehozására és módosítására, majd a forgalomirányítóba való beillesztésére is. Egy létező ACL esetén használjuk a **show running-config** parancsot a hozzáférési lista megjelenítésére, majd másoljuk ki és illesszük be a szövegszerkesztőbe, végezzük el a szükséges módosításokat, végül illesszük vissza a helyére.

**Konfiguráció**: Példaként tegyük fel, hogy az állomás IPv4-címe helytelenül került beírásra (lásd ábra). 192.168.10.99 helyett ennek 192.168.10.10-nek kellene lennie. A következő lépések szerint szerkeszthető és javítható az ACL 1:

**1. lépés** Jelenítsük meg az ACL-t a **show running-config** paranccsal. A példában használt **include** kulcsszóval csak a hozzáférési lista bejegyzései kerülnek a képernyőre.

**2. lépés** Jelöljük ki az ACL-t, másoljuk, majd illesszük be a Jegyzettömbbe. Szerkesszük át a listát az igények szerint. Ha az ACL kifogástalannak látszik, jelöljük ki és másoljuk be a vágólapra.

**3. lépés** Globális konfigurációs módban töröljük a hozzáférési listát a **no access-list 1** paranccsal, mert ellenkező esetben az új utasítások hozzáfűződnek a létező ACL-hez. Ezután illesszük be az új ACL-t a forgalomirányító konfigurációjába.

**4. lépés** Használjuk a **show running-config** parancsot a változtatások ellenőrzésére.

Meg kell említeni, hogy a **no access-list** parancs a különböző IOS szoftver változatokban más-más módon működik. Ha egy kitörölt ACL még ráillesztve maradt egy interfészen, néhány IOS verzió nem védi tovább a hálózatot, míg más verziók tiltják az összes forgalmat. Emiatt a helyes gyakorlat a hozzáférési lista módosítása előtt annak eltávolítása az interfészről. Továbbá, legyünk elővigyázatosak, ha hiba kerül az új listába, tiltsuk le azt és hárítsuk el a hibát. Figyeljünk arra is, hogy a korrekció folyamán a hálózat ismét ACL nélkül marad.

# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

**2. módszer: Sorszámok használata**

Ahogy az ábrán is látható, az ACL 1 eredeti konfigurációjában van egy "host 192.168.10.99" utasítás, ami hibásan került beírásra. Az állomáscím 192.168.10.10 kellene legyen. Az ACL sorszámok segítségével történő szerkesztéséhez kövessük az alábbi lépéseket:

**1. lépés** Jelenítsük meg az aktuális ACL-t a **show access-lists 1** paranccsal. A parancskimenetről részletesebben a későbbiek során lesz szó. Minden utasítás előtt egy sorszám látható, amely automatikusan került hozzárendelésre a hozzáférési lista bejegyzés rögzítésekor. Vegyük észre, hogy a helytelenül konfigurált utasítás sorszáma 10!

**2. lépés** Írjuk be az **ip access-lists standard 1** parancsot, amely a nevesített ACL-ek konfigurálására hivatott. Itt az ACL száma, az 1 szolgál névként. Először a hibás utasítást kell törölnünk a **no 10** paranccsal, ahol a 10 a kívánt sorszám. Ezután adjuk meg az új 10-es sorszámú utasítást a **10 deny host 192.168.10.10**paranccsal.

**MEGJEGYZÉS**: Egy létező utasítás nem írható felül egy azonos sorszámú utasítással! A létező utasítást először törölni kell, az új csak ezután adható hozzá.

**3. lépés** Ellenőrizzük a módosításokat a **show access-lists** paranccsal.

Ahogy korábban már szóba került, a Cisco IOS egy belső algoritmussal kezeli a normál hozzáférési listákat. A normál hozzáférési lista bejegyzéseinek beviteli sorrendje nem feltétlenül egyezik meg a forgalomirányítón való tárolásuk, megjelenítésük és feldolgozásuk sorrendjével. A **show access-lists** parancs sorszámuk szerint mutatja az ACE-ket.

# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

Az előző példában sorszámok segítségével szerkesztettünk számozott normál ACL-t. Figyelve az utasítások sorszámát, a bejegyzések könnyen beilleszthetők vagy törölhetők. Ez a módszer a nevesített normál ACL-ek esetében is használható.

Az ábrán látható példában egy új sort illesztünk egy nevesített ACL-be.

* Az első **show** parancs kimenetében látható, hogy a NO\_ACCESS nevű ACL-ben két szabály van, az egyik a 192.168.11.10 IPv4-című állomásra vonatkozó.
* Az **ip access-list standard** paranccsal konfigurálhatók a nevesített ACL-ek, azaz a hozzáférési lista módban szúrhatók be vagy törölhetők utasítások. A **no** *sorszám* paranccsal törölhető egy adott utasítás.
* Egy másik munkaállomásra vonatkozó tiltás hozzáadásához egy sorszám beillesztése szükséges. Ebben a példában a 192.168.11.11 című munkaállomás került hozzáadásra 15-ös sorszámmal.
* Az utolsó **show** parancs kimenetében ellenőrizhető, hogy az új munkaállomás tiltásra került-e.

# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

Amint az 1. ábrán is látható, a **show ip interface** paranccsal ellenőrizhető az interfészen lévő ACL. A parancskimenet tartalmazza az alkalmazott hozzáférési lista számát vagy nevét, valamint a szűrés irányát. A példában az R1 forgalomirányító S0/0/0 interfészén kimenő irányban található az 1-es számú hozzáférési lista, a G0/0 interfészen pedig szintén kimenő irányban a NO\_ACCESS nevű.

A 2. ábrán levő példában az R1 forgalomirányítón kiadott **show access-lists** parancs kimenete látható. Egy adott hozzáférési lista megtekintéséhez használjuk a **show access-lists** parancsot, utána a lista számával vagy nevével. A NO\_ACCESS utasításai furcsának tűnhetnek, mivel a 15-ös sorszám a 10-t megelőzően szerepel. Ez a forgalomirányító belső folyamatának eredménye, és ez a későbbiekben részletesen tárgyalásra kerül.

# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

Amint az ACL elhelyezésre kerül egy interfészen és elkezdjük a tesztelését, a **show access-lists** parancs fogja megmutatni az egyezések statisztikáját. Az 1. ábra parancskimenetében látható, hogy néhány utasításnál található egyezés. Ha az ACL bejegyzésekhez illeszkedő forgalmat generálunk, akkor a **show access-lists** parancskimenetében lévő egyezések számának növekednie kell. A példával élve, ha megpingeljük a PC1-ről a PC3-at vagy a PC4-et, a parancskimenetben megnövekszik az ACL 1 tiltó utasításához tartozó számláló.

Az engedélyező és tiltó utasítások egyaránt számon tartják az egyezési adatokat, de ne feledjük, hogy minden ACL végén utolsóként ott van az implicit "deny any". Ez az utasítás nem jelenik meg a **show access-lists** parancskimenetében, így a rá vonatkozó statisztika sem látszik. Ha szeretnénk látni az implicit "deny any"-re vonatkozó adatokat, akkor kézzel kell konfigurálnunk az utasítást, amelynek hatására az megjelenik a kimenetben. Legyünk körültekintőek, ha kézzel konfigurálunk "deny any" utasítást, hisz ez minden forgalmat tiltani fog. Viszont, ha nincs beállítva az ACL utolsó utasításaként, az is váratlan dolgokat eredményezhet.

Az ACL tesztelése során a számlálókat a **clear access-list counters** paranccsal törölhetjük. A parancs önmagában is használható, vagy kiegészíthető a kívánt ACL számával vagy nevével. A 2. ábrán lévő parancs egy adott ACL számlálóit törli.

# Normál IPv4 ACL-ek

## IPv4 ACL-ek módosítása

A Cisco IOS egy belső algoritmust alkalmaz a normál ACL-ek esetében. Ahogy korábban már szóba került, ez a logikai eljárás meggátolja, hogy a címtartományra vonatkozó utasítások mögé állomásra vonatkozók kerüljenek, amennyiben azok részei a tartománynak (lásd 1. ábra).

A belső algoritmus másik része a bejegyzések (ACE) sorszámozása. A 2. ábrán egy normál hozzáférési lista konfigurálása látható, amelyben először a hálózatokat tiltó három utasítás került bevitelre, majd az állomásokra vonatkozó öt következett. Az állomás utasítások helyesek, mivel egyik IP-cím sem része az előzőekben szereplő tartományoknak.

A **show running-config** paranccsal ellenőrizhető az ACL-konfiguráció. Figyeljük meg, hogy az utasítások sorrendje nem egyezik meg bevitelük sorrendjével! Használjuk a **show access-lists** parancsot a belső logika értelmezéséhez az alábbiak szerint.

Amint a 3. ábra is mutatja, a **show access-lists** parancs kilistázza az ACE-ket a sorszámukkal együtt. Azt várnánk, hogy az utasítások bevitelük sorrendjében jelenjenek meg. Azonban a **show access-lists** parancskimenetében ez nem így van.

A normál ACE-k olyan sorrendben jelennek meg, ahogy az IOS a listát feldolgozza. Figyeljük meg, ahogy az utasítások két csoportba rendeződnek, elöl találhatók az állomásokra vonatkozók, majd a tartományra vonatkozók következnek. Az utasítások sorszámai nem a feldolgozásuk, hanem bevitelük sorrendjét mutatják.

Az elöl található állomásutasítások listája sem egyezik meg szükségszerűen begépelésük sorrendjével. Az IOS egy speciális hash eljárás alapján rendezi őket úgy, hogy optimális legyen az ACL-bejegyzések közötti keresési eljárás.

Ezután következnek a tartományokra vonatkozó utasítások, amelyek begépelésük sorrendjében láthatók.

Emlékezzünk vissza, hogy a számozott normál ACL-ek a bejegyzések sorszámai segítségével szerkeszthetők. A **show access-lists** parancskimenetében lévő sorszám használatával törölhető egy adott utasítás a listából. Egy új ACL-utasítás beillesztésekor a sorszám csak a tartományra vonatkozó bejegyzés esetén határozza meg annak helyét a listában. Az állomásutasítások mindig a hash eljárás által kijelölt sorrendben kerülnek elhelyezésre.

Folytassuk a példát, ahol az aktív konfiguráció mentése után újraindítjuk a forgalomirányítót. A 3. ábrán látható, hogy a **show access-lists** parancskimenetében az ACL-bejegyzések sorrendje változatlan, de az utasítások új sorszámot kaptak, immár növekvő rendben következnek.

**MEGJEGYZÉS**: A hash eljárás csak a normál hozzáférési lista állomásbejegyzéseire érvényes, az IPv4 kiterjesztett és az IPv6 ACL-ek nem használják ezt az algoritmust. Ennek oka az, hogy a kiterjesztett és az IPv6 ACL-ekben a szűrés nem csak a forráscím alapján történik. A hash eljárás részletei túlmutatnak ennek a kurzusnak a keretein.

# Normál IPv4 ACL-ek

## VTY-vonalak védelme normál IPv4 ACL-lel

**ACL használata VTY-hozzáférés szabályozására**

A Cisco a forgalomirányítók és kapcsolók felügyeletére az SSH-t javasolja. Ha a forgalomirányító Cisco IOS szoftvere nem támogatja az SSH-t, akkor a VTY-hozzáférés korlátozásával növelhetjük az adminisztratív kapcsolat biztonságát. A VTY-elérés korlátozása azt jelenti, hogy meghatározzuk, hogy melyik IP-címekről engedélyezett a belépés a forgalomirányító parancssorába a Telnet használatával. Egy ACL segítségével szabályozhatjuk, hogy melyik felügyeleti munkaállomás vagy hálózat kapcsolódhat a forgalomirányítóhoz. A hozzáférést az **access-class** paranccsal konfigurálhatjuk a VTY-vonalakon. Ugyanezt a módszert alkalmazhatjuk az SSH-ra is, tovább növelve a felügyeleti hozzáférés biztonságát.

Az **access-class** vonali konfigurációs mód parancs korlátozza a bejövő és kimenő kapcsolatokat egy adott VTY-vonalon a hozzáférési listában lévő címek alapján.

A normál és a kiterjesztett hozzáférési listák engedélyei és tiltásai a forgalomirányítókon keresztülhaladó csomagokra vonatkoznak. Magáról a forgalomirányítóról származó csomagok szűrésére ezek a hozzáférési listák nem alkalmasak. Alapértelmezés szerint, egy Telnet-re vonatkozó kimenő irányú kiterjesztett ACL nem akadályozza meg a forgalomirányító által kezdeményezett Telnet kapcsolatot.

A Telnet és SSH-forgalom szabályozása jellemzően egy kiterjesztett ACL feladata, mivel egy magasabb rétegbeli protokoll szűréséről van szó. De, mivel az **access-class** parancs alkalmas a bejövő és kimenő Telnet/SSH-kapcsolatok forráscím alapján való szűrésére, elég normál ACL-t használni.

Az **access-class** parancs szintaktikája a következő:

Router(config-line)# **access-class** *hozzáférési lista száma* { **in** [ **vrf-also** ] | **out** }

Az **in** paraméter lekorlátozza a Cisco eszközhöz tartó bejövő kapcsolatokat a hozzáférési listában szereplő címekre, míg az **out** paraméter meghatározza a Cisco eszközről indítható összeköttetéseket az ACL címei alapján.

Az első ábrán lévő példában a VTY 0-4 vonalak engedélyezése látható, amelyek csak a 192.168.10.0 hálózat számára hozzáférhetők, minden más elérés tiltott.

A VTY-vonalakon konfigurált hozzáférési listák esetén vegyük figyelembe a következőket:

* Csak számozott hozzáférési listák alkalmazhatók a VTY-vonalakon.
* Azonos korlátozást kell beállítani minden VTY-vonalra, mivel a felhasználó bármelyikhez csatlakozhat közülük.

A 2. ábrán gyakorolhatjuk a VTY-hozzáférés biztonságossá tételét a parancsszimulátorban.

# Normál IPv4 ACL-ek

## VTY-vonalak védelme normál IPv4 ACL-lel

Miután a VTY-vonalak hozzáférését korlátozó ACL beállítása megtörtént, fontos az elvárt működés ellenőrzése. Az ábrán két eszköz próbál SSH használatával kapcsolódni az R1-hez, amelyen a 21-es hozzáférési lista került konfigurálásra a VTY-vonalakon. A PC1 sikeresen, míg a PC2 sikertelenül létesít SSH-kapcsolatot. Ez az elvárt működés, mivel a beállított VTY-hozzáférés csak a 192.168.10.0/24 hálózatból engedélyez csatlakozást, minden más állomást letilt.

Az R1-en kiadott **show access-lists** parancskimenete bemutatja a PC1 és PC2 által végrehajtott SSH kapcsolódási kísérleteket. A "permit" utasítás sorában található egyezés a PC1 sikeres SSH-csatlakozására vonatkozik. Míg a "deny" sorban lévő találat a PC2 elutasított kapcsolódási kísérlete, amely a 192.168.11.0/24 hálózatból érkezett.

# IPv4 kiterjesztett ACL-ek

## A kiterjesztett IPv4 ACL felépítése

**Csomagok vizsgálata kiterjesztett ACL-ekkel**

Pontosabb csomagszűréshez létrehozhatunk kiterjesztett IPv4 hozzáférési listákat. A kiterjesztett ACL-ek számozása 100-199 és 2000-2699 közötti lehet, így összesen 799 kiterjesztett számozott listát használhatunk. A kiterjesztett ACL-ek lehetnek nevesítettek is.

A kiterjesztett hozzáférési listák használata sokkal gyakoribb, mint a normál ACL-eké, mivel nagyobb mértékű szabályozási lehetőséget biztosítanak. Amint az ábrán is látható, a kiterjesztett ACL-ek, hasonlóan a normál ACL-ekhez, ellenőrzik a csomagok forráscímét, de ezen felül vizsgálják még a célcímet, a protokollokat és a portszámokat (szolgáltatásokat) is. Ez az ACL osztályozási feltételeinek szélesebb skáláját biztosítja. Például egy kiterjesztett ACL egyidejűleg képes engedélyezni az e-mail forgalmat egy hálózatból egy adott cél felé és ugyanakkor tiltani a fájlátvitelt és a webböngészést.

# IPv4 kiterjesztett ACL-ek

## A kiterjesztett IPv4 ACL felépítése

**Portok és szolgáltatások ellenőrzése**

A protokollok és portszámok szűrése lehetőséget ad a hálózati rendszergazda számára, hogy nagyon specifikus kiterjesztett ACL-eket hozzon létre. Egy szolgáltatás megadható a portszámának vagy a hozzá tartozó jól ismert port nevének beállításával.

Az 1. ábrán levő példák bemutatják, hogyan tud a rendszergazda TCP- és UDP-portszámokat konfigurálni a kiterjesztett ACL utasítás végén. Ugyanitt logikai műveletek is végezhetők, úgymint egyenlő (equal, eq), nem egyenlő (not equal, neq), nagyobb (greater than, gt), és kisebb (less than, lt).

A 2. ábra bemutatja, hogyan jeleníthető meg az ACL elkészítéséhez szükséges portszámok és kulcsszavak listája:

R1(config)# **access-list 101 permit tcp any any eq ?**

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

A kiterjesztett hozzáférési listák beállításának lépései megegyeznek a normál ACL-ekével. A kiterjesztett ACL-t is először létre kell hozni, majd aktiválni kell egy interfészen. Azonban a parancsszintaxis és a paraméterek jóval bonyolultabbak a kiterjesztett ACL-ek által támogatott bővebb lehetőségek miatt.

**MEGJEGYZÉS**: A normál ACL-ek belső számozási algoritmusa nem vonatkozik a kiterjesztett ACL-ek utasításaira, azok konfigurálásuk sorrendjében jelennek meg és kerülnek feldolgozásra.

Az 1. ábra a kiterjesztett IPv4 ACL-ek általános parancsszintaxisát mutatja be. Vegyük észre, hogy a kiterjesztett ACL-ekhez nagyon sok kulcsszó és paraméter tartozik, de a konfigurálás során nem kötelező mindegyiket használni. Emlékezzünk rá, hogy a **?** jól használható segítség a bonyolult parancsok beírásakor!

A 2. ábrán egy kiterjesztett ACL példa látható, amelyben a hálózati rendszergazda a G0/0 interfész LAN-jából induló külső forgalmat csak webböngészés céljára nyitja meg. Az ACL 103 csak azokat a csomagokat engedélyezi, amelyek 192.168.10.0 hálózatból bármely cél felé tartanak, kiegészítve azzal a megszorítással, hogy a forgalom csak a 80 (HTTP) vagy 443 (HTTPS) portszámokat használhatja.

A HTTP működése megköveteli a visszafelé irányuló forgalom engedélyezését a webszervertől a kapcsolatot kezdeményező kliens felé. A hálózati rendszergazda engedélyezni kívánja ezt a visszatérő HTTP-válaszforgalmat, de minden mást tiltani akar. Az ACL 104 blokkol minden bejövő csomagot, kivéve azokat, amelyeket belülről kezdeményeztek és már létrejött kapcsolathoz tartoznak. Az ACL 104 "permit" utasítása az **established** paraméter által engedélyezi ezt a bejövő forgalmat.

Az **established** paraméter csak azokat a csomagokat engedi visszatérni, amelyek válaszok egy 192.168.10.0/24 hálózatból indított kérésre. Egyezés akkor történik, ha a visszajövő TCP-szegmens tartalmaz ACK vagy RST (reset) bitet, amely mutatja, hogy a csomag egy már létező kapcsolathoz tartozik. Ha az **established** paraméter nélkül használjuk az utasítást, a kliens bár képes adatokat küldeni a webszervernek, de az onnan visszaérkező forgalom nem érkezik meg hozzá.

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

Az előző példában a hálózati rendszergazda egy ACL-t konfigurált, amely engedélyezi a 192.168.10.0/24 hálózat felhasználói számára a normál és a biztonságos weboldalak böngészését. Bár az ACL létrehozása megtörtént, mindaddig nem fogja szűrni a forgalmat, míg alkalmazásra nem kerül egy interfészen. Ehhez először gondoljuk át, hogy a forgalomszűrés ki- vagy bemenő irányban történjen! Ha a belső hálózat felhasználója kapcsolódik egy internetes webhelyhez, a forgalom kimegy az internet felé. Ha a belső felhasználó kap egy email-t az internet felől, a forgalom bejön a helyi forgalomirányítóba. Tehát az ACL interfészen való elhelyezésekor a be és ki irányok különböző jelentést hordoznak. Fontos, hogy egy ACL szempontjából a ki és a be irányokat mindig a forgalomirányító interfészének vonatkozásában kell tekinteni!

Az ábrán látható topológiában az R1-nek három interfésze van, egy soros (S0/0/0) és két gigabit Ethernet (G0/0 és G0/1). Emlékezzünk vissza, hogy a kiterjesztett ACL-t jellemzően a forráshoz lehető legközelebb kell elhelyezni! Ebben a hálózatban a forrás forgalomhoz a G0/0 interfész található a legközelebb.

A 192.168.10.0/24 LAN felhasználóitól érkező webkérések a G0/0 interfészen bejövő irányban érkeznek, míg a létrejött kapcsolatok válaszforgalma kimenő irányban távozik a G0/0-ról. A példában a G0/0 interfészen mindkét irányban el kell helyezni hozzáférési listát, az ACL 103 bejövő irányban ellenőrzi a forgalmat típusa szerint, az ACL 104 pedig kimenő irányban szűri a visszaérkező csomagokat. Ez a beállítás korlátozza csak weboldalak böngészésére a 192.168.10.0 hálózat internet hozzáférését.

**MEGJEGYZÉS**: A hozzáférési lista elhelyezhető lenne az S0/0/0 interfészen is, de ebben az esetben az ACL-nek minden csomagot fel kellene dolgoznia, ami a forgalomirányítóba érkezik, tehát a 192.168.11.0 hálózathoz tartozókat is. Ez felesleges terhelést okozna a forgalomirányítónak.

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

Az 1. ábrán található példában az FTP-forgalom tiltott a 192.168.11.0 hálózatból a 192.168.10.0 hálózat felé, minden további forgalom engedélyezett. Figyeljük meg a helyettesítő maszkok használatát és a "permit any" utasítást! Emlékezzünk vissza, hogy az FTP a 20 és 21 TCP-portokat használja, ezért az ACL-ben szükség van az **ftp** és az **ftp-data** kulcsszavakra, vagy az **eq 20** és az **eq 21** paraméterekre az FTP tiltásához.

Ha portszámokat használunk portnevek helyett, a parancs a következőképpen fog kinézni:

**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20**

**access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21**

Annak megakadályozására, hogy az ACL végén levő implicit "deny any" utasítás minden forgalmat blokkoljon, a **permit ip any any** sor hozzáadása szükséges. Legalább egy **permit** utasításnak lennie kell az ACL-ben, különben az blokkolni fog minden forgalmat az interfészen. Az ACL-t a G0/1 interfészen bejövő irányban kell elhelyezni, hogy a 192.168.11.0/24 LAN-ból érkező forgalom már a belépéskor szűrésre kerüljön.

A 2. ábrán található példában a Telnet csomagok tiltottak bármely forrásból a 192.168.11.0/24 LAN felé, minden más IP-forgalom engedélyezett. Mivel a 192.168.11.0/24 LAN-ba tartó forgalom a G0/1 interfészen lép ki, az ACL-t itt kell elhelyezni az **out** kulcsszó használatával. Figyeljük meg az **any** kulcsszó alkalmazását a "permit" utasításban, amelynek hozzáadása biztosítja, hogy ne kerüljön tiltásra az összes forgalom.

**MEGJEGYZÉS**: Mindkét példában egy **permit ip any any** utasítás van az ACL végén. A nagyobb biztonság érdekében a **permit ip 192.168.11.0 0.0.0.255 any** parancs is használható.

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

A nevesített kiterjesztett ACL-ek létrehozása lényegében megegyezik a nevesített normál hozzáférési listáéival. Kövessük az alábbi lépéseket egy nevesített kiterjesztett ACL létrehozásához:

**1. lépés** Globális konfigurációs módban használjuk az **ip access-list extended** *név* parancsot a kiterjesztett lista nevének megadásához.

**2. lépés** Nevesített ACL konfigurációs módban adjuk meg a szabályozó feltételeket a **permit** vagy a **deny**kulcsszó után.

**3. lépés** Visszatérve privilegizált EXEC módba, ellenőrizzük az ACL-t a **show access-lists** *név* paranccsal.

**4. lépés** Mentsük a bejegyzéseket a konfigurációs fájlba a **copy running-config startup-config** paranccsal.

Egy nevesített kiterjesztett ACL eltávolításához használjuk a **no ip access-list extended** *név* globális konfigurációs parancsot.

Az ábrán az előző példában található ACL nevesített változatának létrehozása látható. A SURFING nevű ACL engedélyezi a 192.168.10.0/24 LAN felhasználói számára a webhelyekhez való hozzáférést. A BROWSING nevű ACL pedig engedélyezi a létrehozott kapcsolatok visszirányú forgalmát. A szabályok alkalmazása a G0/0 interfészen be- és kimenő irányban az ACL nevével történik.

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

Az ACL konfigurálása és interfészen való elhelyezése után használjuk a Cisco IOS **show** parancsokat a beállítás ellenőrzéséhez. Az ábrán, a példa elején látható az összes ACL tartalmát megjelenítő Cisco IOS parancs. A példa közepén pedig az R1-en kiadott **show ip interface g0/0** utasítás kimenete található.

A normál ACL-ekkel ellentétben, a kiterjesztett ACL-ek nem alkalmaznak belső algoritmust és hash eljárást. A **show access-lists** parancskimenetében megjelenő sorszámok megegyeznek az utasítások bevitelének sorrendjével. Az állomásokra vonatkozó bejegyzések nem kerülnek automatikusan a tartományokra vonatkozók elé.

A **show ip interface** parancs használható az interfészen alkalmazott ACL és annak irányának ellenőrzésére. A parancskimenet tartalmazza a hozzáférési lista számát vagy nevét, valamint alkalmazásának irányát. A nagybetűs ACL nevek (BROWSING és SURFING) szembeötlenek a képernyőn megjelenő kimenetben.

A hozzáférési lista konfigurációjának ellenőrzése után a következő lépés az ACL tervezett működésének vizsgálata; a forgalom elvárt módon való tiltása vagy engedélyezése.

A korábban tárgyalt útmutató alapján, javasolt az ACL teszthálózatban való kipróbálása, majd csak ezután az éles környezetben történő alkalmazása.

# IPv4 kiterjesztett ACL-ek

## Kiterjesztett IPv4 ACL-ek konfigurálása

Egy kiterjesztett ACL szerkesztése teljesen azonos módon végezhető el, mint az előzőekben tárgyalt normál ACL-eké. Módosításuk a következőképpen hajtható végre:

* **1. módszer: Szövegszerkesztő** - Ezzel a módszerrel az ACL kimásolható és beilleszthető a szövegszerkesztőbe, ahol a változtatások megvalósíthatók. Az aktuális hozzáférési lista a **no access-list** paranccsal távolítható el. Ezután a módosított ACL visszailleszthető a konfigurációba.
* **2. módszer: Sorszámok** - Az utasítások sorszámainak használatával törölhető vagy szúrható be egy ACL-bejegyzés. Az **ip access-list extended** *név* paranccsal érhető el a nevesített ACL konfigurációs mód. Ha a hozzáférési lista számozott, akkor a név helyett az ACL számát kell a *név* paraméterben használni. A bejegyzések sorszámuk segítségével illeszthetők be vagy távolíthatók el.

Az ábrán a rendszergazda a SURFING nevű ACL-t szeretné szerkeszteni, hogy a forrás hálózatban lévő gépelési hibát kijavítsa. Az aktuális sorszámok megjelenítéséhez a **show access-lists** parancs használható. A szerkesztésre váró bejegyzés sorszáma 10. Az eredeti utasítás a **no** *sorszám* paranccsal távolítható el. A javított utasítás az eredeti helyére kerül.

# ACL-ek hibaelhárítása

## Csomagfeldolgozás ACL-ekkel

**A bejövő ACL-folyamat**

Az 1. ábrán egy bejövő irányú ACL feldolgozási folyamata látható. Ha a csomag fejlécében lévő információ megegyezik egy ACL-bejegyzéssel, akkor a fennmaradó ACE-k nem kerülnek kiértékelésre, és a csomag engedélyezésre vagy tiltásra kerül a bejegyzésben foglaltak szerint. Ha a csomag fejléce nem egyezik az ACL-bejegyzéssel, akkor a csomag a lista következő elemével kerül összevetésre. Az összehasonlítási folyamat a lista végéig tart.

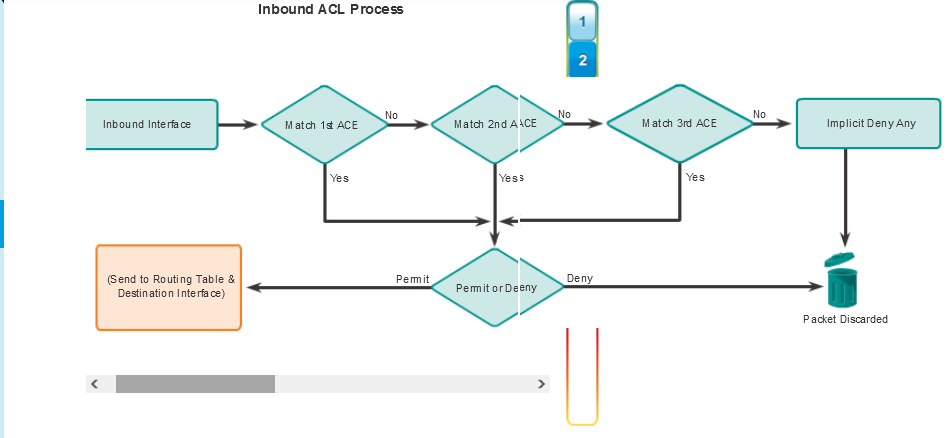
Itt minden esetben egy implicit "deny any" utasítás található, amely nem jelenik meg a parancskimenetben, de minden olyan csomagra érvényes, amelyre a korábbi feltételek összehasonlítása hamis eredménnyel végződött. Tehát a végső feltételvizsgálat minden fennmaradó csomag esetén egyezést talál és tiltást fog végrehajtani. A forgalomirányító nem továbbítja az interfészen ki- vagy befelé irányban ezeket a csomagokat, hanem eldobja őket. Ezt az utolsó utasítást gyakran "implicit deny any" utasításnak vagy "deny all traffic" utasításnak is nevezik. Mindezek miatt egy ACL-ben lennie kell legalább egy engedélyező bejegyzésnek, különben a hozzáférési lista blokkolni fog minden forgalmat.

**A kimenő ACL-folyamat**

A 2. ábrán egy kimenő irányú ACL feldolgozási folyamata látható. Mielőtt egy csomag a kimenő interfészhez kerül, a forgalomirányító megvizsgálja az útválasztó táblát, hogy a csomag irányítható-e. Ha nem, akkor eldobja azt, így a listabejegyzésekkel (ACE) sem kerül összehasonlításra. Ha a csomag irányítható, akkor a forgalomirányító megvizsgálja, hogy a kimenő interfészhez tartozik-e ACL. Ha nem, akkor a csomagot a kimenő pufferbe helyezi. A kimenő ACL-műveletek a következők lehetnek:

* **Nincs ACL az interfészhez rendelve:** Ha a kimenő interfészhez nem tartozik kimenő irányú ACL, akkor a csomag közvetlenül a kimenő interfészre kerül.
* **Van ACL az interfészhez rendelve:** Ha a kimenő interfészhez tartozik kimenő irányú ACL, akkor a csomag mindaddig nem továbbítódik a kimenő interfészre, míg az ACL-bejegyzésekkel összehasonlításra nem kerül. Az összehasonlítás eredményeképpen a csomagot a forgalomirányító vagy továbbítja vagy eldobja.

A kimenő irányú listák esetében a "permit" azt jelenti, hogy a csomag a kimeneti pufferbe továbbítódik, a "deny" pedig azt, hogy eldobásra kerül.



# ACL-ek hibaelhárítása

## Csomagfeldolgozás ACL-ekkel

**Irányítási és ACL-feldolgozási műveletek a forgalomirányítón**

Az ábrán az irányítás és az ACL-feldolgozás logikai folyamatábrája látható. Ha csomag érkezik a forgalomirányító egyik interfészére, az irányítási folyamat független attól, hogy van-e ACL használatban vagy sem. A keret beérkezése után a forgalomirányító ellenőrzi, hogy az adatkapcsolati réteg (Layer 2) célcíme egyezik-e az interfész azonos rétegbeli címével, vagy a keret egy szórásos üzenet-e.

Ha a keret címét elfogadta a forgalomirányító, akkor a keretadatokat eltávolítja, majd előkeresi a bejövő interfészre vonatkozó ACL-t. Ha van ilyen, ellenőrzi a csomagot a lista tartalma alapján.

Ha a csomag egyezik egy bejegyzéssel, akkor vagy engedélyezi azt, vagy eldobja. Ha a csomag elfogadásra került, akkor összeveti azt az irányítótábla bejegyzéseivel a kimenő interfész meghatározása céljából. Ha van bejegyzés a célcímhez az útválasztó táblában, akkor a csomagot a kimenő interfészre továbbítja, ha nincs, akkor eldobja.

Ezután a forgalomirányító megvizsgálja, hogy van-e a kimenő interfészen ACL. Ha van ilyen, a csomagot ellenőrzi a lista tartalma alapján.

Ha a csomag egyezik egy bejegyzéssel, akkor vagy engedélyezi azt, vagy eldobja azt.

Ha nincs az interfészen ACL vagy a csomag engedélyezett, akkor a forgalomirányító beágyazza azt az új adatkapcsolati réteg protokolljába és továbbítja az interfészen át a következő eszköz felé.

# ACL-ek hibaelhárítása

## Csomagfeldolgozás ACL-ekkel

A normál hozzáférési listák csak a forrás IPv4-címet vizsgálják, nem törődnek a csomag céljával és a benne levő portokkal.

Az ábra egy normál ACL döntési folyamatát mutatja be. A Cisco IOS szoftver egyesével veti össze az ACL-ben lévő feltételeket a címmel. Az első egyezésnél eldönti, hogy a csomagot elfogadja vagy eldobja. Mivel a szoftver az első egyezés megtalálása után leállítja a további vizsgálatot, nagyon fontos a feltételek sorrendisége. Ha a cím egyik feltétellel sem egyezik, eldobásra kerül.

# ACL-ek hibaelhárítása

## Csomagfeldolgozás ACL-ekkel

Az ábra egy kiterjesztett ACL döntési folyamatát mutatja be, amelyben megtalálhatók a forrás- és célcím, protokoll és portszám szerinti szűrések. A példában az ACL először a forráscímet, majd a forrásportot és a protokollt vizsgálja. Ezután szűri a célcímet, a célportot és protokollt, végül engedélyező vagy elutasító döntést hoz.

Emlékezzünk vissza, hogy az ACL-bejegyzések egymás után kerülnek feldolgozásra, tehát egy "No" elágazás nem feltétlenül jelent tiltást! A logikai döntési folyamat során a "No" a következő bejegyzésre való átlépést jelenti, mindaddig, míg a feltételek meg nem egyeznek.

# ACL-ek hibaelhárítása

## Gyakori ACL-hibák

A korábban megismert **show** parancsok használatával a legtöbb ACL-hiba könnyen feltárható. A leggyakoribb hibák forrása a listabejegyzések rossz sorrendben történő bevitele és az elégtelen feltételek alkalmazása a szabályokban.

**Hibaelhárítás - 1. példa**

Az ábrán a 192.168.10.10 állomás nem tud kapcsolatot létesíteni a 192.168.30.12-vel. Ha megnézzük a **show access-lists** parancskimenetét, láthatjuk, hogy egyezések vannak az első "deny" utasításnál. Ez jelzi, hogy a forgalom ennél a bejegyzésnél akadt el.

**Megoldás** - Nézzük meg az ACE-k sorrendjét! A 192.168.10.10 állomásnak a 10-es listabejegyzés miatt nincs kapcsolata a 192.168.30.12-vel. Mivel a forgalomirányító az ACL-utasításokat felülről lefelé dolgozza fel, így a 10-es bejegyzés letiltja a 192.168.10.10 állomást, következésképp a 20-as bejegyzéssel sohasem lehet egyezése. A 10-es és 20-as sorokat fel kell cserélni! Az utolsó utasítás engedélyez minden IP-alapú nem TCP-forgalmat (ICMP, UDP stb.)

# ACL-ek hibaelhárítása

## Gyakori ACL-hibák

**Hibaelhárítás - 2. példa**

Az ábrán a 192.168.10.0/24 hálózat nem tud TFTP-kapcsolatot létesíteni a 192.168.30.0/24 hálózat felé.

**Megoldás** - A 192.168.10.0/24 hálózat azért nem tud TFTP-kapcsolatot létesíteni a 192.168.30.0/24 hálózat felé, mert a TFTP az UDP szállítási rétegbeli protokollt használja. Ugyan az ACL 30-as sora minden egyéb TCP-forgalmat engedélyez, de ebbe nem tartozik bele a TFTP által használt UDP forgalom, így az implicit tiltásra kerül. Emlékezzünk vissza, hogy az implicit "deny any" utasítás nem jelenik meg a **show access-lists** parancskimenetében, ezért az egyezések sem látszanak.

A 30-as sornak **ip any any**kell lennie.

Ez az ACL egyaránt működőképes az R1 G0/0-n, az R3 S0/0/1-en, vagy az R2 S0/0/0-n is bejövő irányban. Az elhelyezési szabály alapján a kiterjesztett ACL-nek a forráshoz legközelebb kell lennie, így itt a legjobb megoldás az R1 G0/0-n történő aktiválás, mivel ez lehetővé teszi a nemkívánatos forgalom szűrését, mielőtt az áthaladna az egész hálózaton.

# ACL-ek hibaelhárítása

## Gyakori ACL-hibák

**Hibaelhárítás - 3. példa**

Az ábrán a 192.168.11.0/24 hálózat képes Telnet kapcsolatot létesíteni a 192.168.30.0/24-val, pedig a vállalati biztonsági szabályok szerint ez nem engedélyezett. A **show access-lists 130** parancskimenetében látszik, hogy a "permit" utasításnál vannak az egyezések.

**Megoldás** - A 192.168.11.0/24 hálózat azért tud Telnet-en kapcsolódni a 192.168.30.0/24 hálózathoz, mert a "telnet" kulcsszó rossz helyen van a hozzáférési lista 10-es során belül. Az utasítás most azokat a csomagokat tiltja, ahol a forrás portszám egyenlő a Telnet-tel (23). A Telnet forgalom tiltásához a G0/1-en bejövő irányban az szükséges, hogy a célportszám legyen egyenlő a Telnet-tel, azaz a helyes utasítás a **deny tcp any any eq telnet**.

# ACL-ek hibaelhárítása

## Gyakori ACL-hibák

**Hibaelhárítás - 4. példa**

Az ábrán a 192.168.30.12 állomás képes Telnet kapcsolatot létesíteni a 192.168.31.12-vel, pedig a vállalati biztonsági szabályok szerint ez nem engedélyezett. A **show access-lists 140** parancskimenetében látszik, hogy a "permit" utasításnál vannak az egyezések.

**Megoldás** - A 192.168.30.12 állomás azért tud Telnet-en kapcsolódni a 192.168.31.12-höz, mert nincs olyan szabály, ami tiltaná a 192.168.30.12 forráscímet vagy annak hálózatát. A hozzáférési lista 10-es utasítása a 192.168.30.1 címről (R3 G0/0) érkező forgalmat tiltja. A 10-es sorban lévő IPv4-állomáscímnek 192.168.30.12-nek kell lennie.

# ACL-ek hibaelhárítása

## Gyakori ACL-hibák

**Hibaelhárítás - 5. példa**

Az ábrán a 192.168.30.12 állomás képes Telnet kapcsolatot létesíteni a 192.168.31.12-vel, pedig a vállalati biztonsági szabályok szerint ez nem engedélyezett. A **show access-lists 150** parancskimenetében látszik, hogy nincsenek meg az elvárt egyezések a "deny" utasítással.

**Megoldás** - A 192.168.30.12 állomás azért tud Telnet-en kapcsolódni a 192.168.31.12-höz, mert a G0/1 interfészen rossz irányban van elhelyezve az ACL 150. Bár a 10-es utasítás tiltja minden forráscím Telnet kapcsolódását a 192.168.31.12 állomáshoz, de a szűrőt kimenő irányban kell elhelyezni a G0/1-en a helyes működés érdekében.

# IPv6 ACL-ek

## IPv6 ACL létrehozása

Az IPv6 ACL-ek működésben és konfigurációban is nagyon hasonlítanak az IPv4 ACL-ekhez. Az IPv4 hozzáférési listák ismerete megkönnyíti az IPv6 ACL-ek megértését és beállítását.

IPv4-ben két ACL-típus van, a normál és a kiterjesztett, amelyek egyaránt lehetnek számozottak vagy nevesítettek.

Az IPv6-ban csak egyféle ACL létezik, és az egyenértékű az IPv4 nevesített kiterjesztett ACL-lel. Számozott ACL-ek nincsenek az IPv6-ban. Összegezve, az IPv6 hozzáférési listák:

* Csak nevesített ACL-ek.
* Működésükben egyenértékűek az IPv4 kiterjesztett ACL-ekkel.

Egy IPv4 ACL és egy IPv6 ACL nem viselheti ugyanazt a nevet.

# IPv6 ACL-ek

## IPv6 ACL létrehozása

Bár az IPv4 és IPv6 ACL-ek nagyon hasonlók, három jelentős különbség is van közöttük.

* **IPv6 ACL alkalmazása**

Az első különbség az ACL interfészhez rendelésére használt parancs. Míg IPv4-ben az **ip access-group** parancs illeszti az IPv4 ACL-t az IPv4-interfészhez, addig az IPv6-ban a **ipv6 traffic-filter** parancs tölti be ezt a funkciót.

* **Nincsenek helyettesítő maszkok**

Ellentétben az IPv4 ACL-ekkel, az IPv6 ACL-ek nem használnak helyettesítő maszkokat. Ehelyett az előtag-hossz (prefix-lenght) határozza meg, hogy az IPv6 cél- vagy forráscímből mekkora rész kerüljön vizsgálatra.

* **További alapértelmezett utasítások**

Az utolsó jelentős különbség, hogy két további, implicit "permit" utasítás került minden IPv6 hozzáférési lista végére. Minden IPv4 normál és kiterjesztett ACL végén van egy implicit **deny any** vagy **deny any any** bejegyzés. Az IPv6 is tartalmaz egy hasonló **deny ipv6 any any** utasítást minden IPv6 ACL végén. A különbség pedig az, hogy alapértelmezés szerint az IPv6-ban még szerepel a két következő implicit bejegyzés:

* **permit icmp any any nd-na**
* **permit icmp any any nd-ns**

Ez a két utasítás teszi lehetővé a forgalomirányító számára, hogy részt vegyen az IPv4 ARP-jéhez hasonló IPv6-címfeloldásban. Emlékezzünk, hogy az IPv4 ARP-je oldja fel a 3. rétegbeli IP-címeket 2. rétegbeli MAC-címekké! Ahogy az ábrán is látható, az IPv6 ICMP Neighbor Discovery (ND) üzenetekkel végzi el ugyanezt. Az ND két üzenettípust használ, amelyek a Neighbor Solicitation (NS) és a Neighbor Advertisement (NA).

Az ND üzenetek IPv6-csomagokba ágyazva közlekednek, és igénybe veszik az IPv6 hálózati rétegének szolgáltatásait, míg az IPv4 ARP nem használja a harmadik réteget. Mivel az IPv6 alkalmaz 3. rétegbeli szolgáltatást a hálózatfelderítéshez (ND), ezért az IPv6 ACL-eknek értelemszerűen engedélyezniük kell az interfészen az ND-csomagok küldését és fogadását. Tehát, mind a Neighbor Discovery - Neighbor Advertisement (ND-NA), mind a Neighbor Discovery - Neighbor Solicitation (ND-NS) üzenetek engedélyezve vannak.

# IPv6 ACL-ek

## IPv6 ACL-ek konfigurálása

Az 1. ábrán látható topológiát fogjuk használni az IPv6 ACL-ek konfigurálásához. A hálózat összeállítása hasonló a korábbi IPv4-topológiához, kivéve az IPv6 címzési sémát. Három 2001:DB8:CAFE::/64 alhálózat található benne: a 2001:DB8:CAFE:10::/64, a 2001:DB8:CAFE:11::/64 és a 2001:DB8:CAFE:30::/64. Két soros hálózat köti össze a három forgalomirányítót: a 2001:DB8:FEED:1::/64 és a 2001:DB8:FEED:2::/64.

A 2.,3. és 4. ábrákon az egyes forgalomirányítók IPv6-címkonfigurációs parancsai láthatók. A **show ipv6 interface brief** parancskimenetében ellenőrizhetjük a címeket és az interfészek állapotát.

**MEGJEGYZÉS**: A **no shutdown** és a **clock rate** parancsok nem látszanak a konfigurációban.

# IPv6 ACL-ek

## IPv6 ACL-ek konfigurálása

Az IPv6-ban csak nevesített ACL-ek vannak, amelyek konfigurálása hasonlít az IPv4 nevesített kiterjesztett hozzáférési listákéhoz.

Az első ábrán az IPv6 ACL-ek parancsszintaxisa látható, amely hasonló az IPv4 kiterjesztett hozzáférési listáéhoz. Az egyetlen jelentős különbség az IPv6 előtag-hossz használata az IPv4 helyettesítő maszk helyett.

Egy IPv6 ACL konfigurálásának három alapvető lépése:

**1. lépés** Globális konfigurációs módban használjuk az **ipv6 access-list** *név* parancsot az IPv6 ACL létrehozásához. Mint az IPv4 nevesített ACL-ek esetében, az IPv6-nevek is alfanumerikusak, nagybetűérzékenyek és egyedinek is kell lenniük. Ellentétben az IPv4-gyel, itt nem szükséges a "standard" vagy az "extended" kulcsszó használata.

**2. lépés** Nevesített ACL konfigurációs módban használjuk a **permit** vagy a **deny** utasításokat a feltétek megadásához, melyek alapján a csomag továbbításra vagy eldobásra kerül.

**3. lépés** Térjünk vissza privilegizált EXEC módba az **end** paranccsal.

A 2. ábra bemutatja egy IPv6 ACL létrehozásának lépéseit az előző topológia egyszerű példáján keresztül. Az első utasítás elnevezi a hozzáférési listát NO-R3-LAN-ACCESS-nek. Hasonlóan az IPv4 nevesített ACL-ekhez, az IPv6 ACL nevek nagybetűs írása sem kötelező, de szembeötlővé teszi őket az aktív konfiguráció olvasásakor.

A második utasítás letiltja a 2001:DB8:CAFE:30::/64 hálózatból származó IPv6-csomagok továbbítását bármely más IPv6-hálózat felé. A harmadik utasítás engedélyez minden más IPv6-csomagot.

A 3. ábra hálózati környezetben mutatja az ACL-t.

# IPv6 ACL-ek

## IPv6 ACL-ek konfigurálása

Miután konfiguráltuk az IPv6 ACL-t, hozzá kell csatoljuk egy interfészhez a **ipv6 traffic-filter** paranccsal:

Router(config-if)# **ipv6 traffic-filter** *hozzáférési lista neve* { **in** | **out** }

Az ábrán a korábban konfigurált NO-R3-LAN-ACCESS hozzáférési lista S0/0/0 interfészen bejövő irányba elhelyezésére szolgáló parancs látható. Ennek eredményeképpen a 2001:DB8:CAFE:30::/64 hálózatból az R1 mindkét LAN-ja felé tartó csomagok eldobásra kerülnek.

Az ACL interfészről való eltávolításához előbb használjuk a **no ipv6 traffic-filter** parancsot az interfészen, majd a globális **no ipv6 access-list** paranccsal töröljük a hozzáférési listát.

**MEGJEGYZÉS**: Az IPv4 és az IPv6 is az **ip access-class** parancsot alkalmazza egy ACL elhelyezéséhez a VTY-vonalakon.

# IPv6 ACL-ek

## IPv6 ACL-ek konfigurálása

**Az FTP tiltása**

Az 1. ábrán a példákban használt topológia látható.

Az első példában (lásd 2. ábra) az R1 forgalomirányítón konfigurált IPv6 hozzáférési lista letiltja az FTP-forgalmat a 2001:DB8:CAFE:11::/64 felé. Mind az FTP-adatportot (20), mind az FTP-vezérlőportot (21) blokkolni kell. Mivel a szűrő az R1 G0/0 interfészén bejövő irányban van elhelyezve, csak a 2001:DB8:CAFE:10::/64 hálózatból érkező forgalom lesz letiltva.

**Korlátozott hozzáférés**

A második példában (lásd 3. ábra) beállított IPv6 ACL korlátozott hozzáférést biztosít az R3 LAN-jának az R1-hez csatlakozó LAN-ok eléréséhez. Az ACL dokumentálása céljából a konfiguráció megjegyzéseket is tartalmaz. A következő jellemzők kaptak címkét az ACL-ben:

1. Az első két permit utasítás minden eszköz számára hozzáférést biztosít a 2001:DB8:CAFE:10::10 című webszerverhez.

2. Minden más, a 2001:DB8:CAFE:10::/64 hálózatban lévő eszköz elérése tiltott.

3. A PC3 (2001:DB8:CAFE:30::12) Telnet-en kapcsolódhat a PC2-höz (2001:DB8:CAFE:11::11).

4. Minden más állomás számára tiltott a Telnet csatlakozás a PC2-höz.

5. Minden további IPv6-forgalom engedélyezett.

6. Az IPv6 hozzáférési lista a G0/0 interfészen bejövő irányban van, tehát csak a 2001:DB8:CAFE:30::/64 hálózatra vonatkozik.

# IPv6 ACL-ek

## IPv6 ACL-ek konfigurálása

Az IPv6 hozzáférési listák ellenőrzésére szolgáló parancsok megegyeznek az IPv4 ACL-eknél használtakkal. Így vizsgálható meg a korábban létrehozott RESTRICTED-ACCESS IPv6 hozzáférési lista is. Az 1. ábrán a **show ipv6 interface** parancskimenete látható, amely igazolja, hogy a RESTRICTED-ACCESS ACL a G0/0 interfészen bejövő irányban van konfigurálva.

A 2. ábrán látható **show access-lists** parancs megjeleníti a forgalomirányítón levő összes IPv4 és IPv6 hozzáférési listát. Figyeljük meg, hogy az IPv6 ACL-ek sorszámai a bejegyzések végén találhatók, nem pedig az elejükön, ahogy az IPv4-nél láttuk! Bár az utasítások beírásuk sorrendjében követik egymást, de sorszámaik nem mindig 10-zel növekednek. Ennek oka az, hogy a bevitt megjegyzések (remark) is kapnak sorszámot, de nem jelennek meg a **show access-lists** parancskimenetében.

Hasonlóan az IPv4 kiterjesztett ACL-ekhez, az IPv6 hozzáférési listák is az utasítások bevitelének sorrendjében jelennek meg és kerülnek feldolgozásra. Emlékezzünk vissza, hogy a normál ACL-ek egy belső algoritmust alkalmaznak, amely felcseréli az utasításokat és megváltoztatja feldolgozásuk sorrendjét.

A 3. ábrán a **show running-config** parancskimenete látható, benne az összes ACE-vel és a megjegyzéseket tartalmazó utasításokkal. A megjegyzés sorok lehetnek a **permit** vagy a **deny** utasítás előtt és mögött is, de legyünk következetesek elhelyezésükkel!

# Összefoglalás

## Összefoglalás

**FTP Denied**

**Esetleírás**

Az utóbbi időben többször jelezték, hogy vírusok terjednek egy középvállalati hálózatban. A hálózati rendszergazda felülvizsgálta a hálózata működését és megállapította, hogy egy bizonyos állomás folyamatosan fájlokat tölt le egy távoli FTP-szerverről. Valószínűleg ez az állomás a hálózaton végigterjedő vírusfertőzés forrása!

A feladat megoldásához használjuk a Packet Tarcert-t. Készítsünk egy nevesített ACL-t, amely tiltja az állomás hozzáférését az FTP-szerverhez. Helyezzük el az ACL-t a lehető leghatékonyabban a forgalomirányító egyik interfészén.

A fizikai hálózat felépítéséhez szükségünk lesz:

* 1 db. PC munkaállomásra,
* 2 db. kapcsolóra,
* 1 db. Cisco 1941-es forgalomirányítóra (ISR),
* 1 db. szerverre.

Rögzítsük az előkészített ACL-t a Packet Tracer szövegszerkesztőjébe (text tool). Ellenőrizzük az ACL működését, próbáljunk csatlakozni az FTP-szerverhez. Figyeljük meg szimulációs módban, hogy mi történik.

Mentsük el az állományt és készüljünk fel, hogy megosszuk azt egy diáktársunkkal vagy az egész osztállyal.

[Csoportos feladat - FTP Denied Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/9.6.1.1%20FTP%20Denied%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

A forgalomirányító alapértelmezés szerint nem szűri a csomagokat, azok kizárólag az útválasztó tábla információi alapján kerülnek irányításra.

A hálózati hozzáférés szabályozása céljából a csomagszűrés elemzi a bejövő és kimenő forgalmat, és továbbítja vagy eldobja azt bizonyos feltételek alapján, mint például a forrás IP-cím, a cél IP-cím, és a csomag által hordozott protokoll. A csomagszűrő forgalomirányító szabályokat használ a forgalom engedélyezésének vagy tiltásának meghatározására, továbbá képes a szállítási rétegbeli szűrésre is.

Egy ACL engedélyező és tiltó utasítások sorozata, amelynek utolsó eleme mindig egy, az összes forgalmat blokkoló implicit tiltás. Annak megakadályozására, hogy az ACL végén lévő beépített "deny any" blokkoljon minden forgalmat, legalább egy **permit** utasításnak szerepelni kell a hozzáférési listában.

Amikor a hálózati forgalom keresztülhalad egy ACL-lel konfigurált interfészen, a forgalomirányító összeveti a csomagban található információt a listabejegyzésekkel, és azokon sorrendben végighaladva egyezést keres. Ha talál, feldolgozza a csomagot az utasításban foglaltaknak megfelelően.

A konfigurált ACL-ek alkalmazhatók mind a bejövő, mind a kimenő forgalom szűrésére.

A normál ACL-ek csak a forrás IPv4-címet használják a forgalom engedélyezésére vagy tiltására. A célcím és a csomagba ágyazott portszám nem kerül kiértékelésre. A normál ACL-ek alapszabálya, hogy helyezzük őket a célhoz lehető legközelebb.

A kiterjesztett ACL-ek többféle jellemző alapján szűrik a csomagokat: forrás- és cél IPv4-cím, forrás- és célport. A kiterjesztett ACL-ek alapszabálya, hogy helyezzük őket a forráshoz lehető legközelebb.

Az **access-list** globális konfigurációs paranccsal definiálható normál ACL 1-től 99-ig, vagy kiterjesztett ACL 100-199 és 2000-2699 számozással. A normál és a kiterjesztett ACL-ek lehetnek nevesítettek is. Az **ip access-list standard** *név* paranccsal hozható létre nevesített normál ACL, míg a **ip access-list extended** *név* utasítással a kiterjesztett ACL. Az IPv4 hozzáférési lista bejegyzések (ACE) helyettesítő maszkokat tartalmaznak.

Konfigurálás után az ACL elhelyezésre kerül egy interfészen az **ip access-group** paranccsal interfész konfigurációs módban. Emlékezzünk vissza a három P szabályra: egy ACL per protokoll, per irány, per interfész!

Egy ACL eltávolításához először használjuk a **no ip access-group** parancsot az interfészen, majd alkalmazzuk a **no access-list** globális utasítást a teljes ACL törléséhez.

A **show running-config** és a **show access-lists** parancsokkal ellenőrizhető az ACL-konfiguráció. A **show ip interface** parancs pedig megmutatja, hogy melyik ACL van az interfészen és az milyen irányban szűr.

Az **access-class** vonali konfigurációs parancs a hozzáférési listában levő címekre korlátozza a bejövő és kimenő VTY-kapcsolatokat.

Hasonlóan az IPv4 nevesített ACL-ekhez, az IPv6 hozzáférési listák nevei is alfanumerikus karakterekből állnak, nagybetűérzékenyek és egyediek. Az IPv4-gyel ellentétben, itt nincs szükség a "standard" vagy "extended" beállítás használatára.

Globális konfigurációs módban az **ipv6 access-list** *név* paranccsal hozható létre egy IPv6 ACL. Az IPv4 ACL-ektől eltérően, az IPv6 ACL-ek nem használnak helyettesítő maszkokat. Helyette az előtag hossza (prefix-length) határozza meg, hogy az IPv6 forrás- vagy célcímből mennyi kerüljön egyeztetésre.

Konfigurálás után az IPv6 ACL az **ipv6 traffic-filter** paranccsal aktiválható az interfészen.

