# Fejezet 11: Egy Hálózat 11.0.1.1 Bevezetés

# Egy Hálózat

## Bevezetés

A kurzus során eddig áttekintettük az adathálózatoknak a humán hálózatok számra nyújtott szolgáltatásit, megvizsgáltuk az OSI-modell egyes rétegeinek tulajdonságait és a TCP/IP-protokollok működését, valamint foglalkoztunk a legnépszerűbb LAN-technológiával, az Ethernettel. Ebben a fejezetben következő lépésként megtanuljuk, miként lehet ezekből az elemekből egy működő és fenntartható hálózatot létrehozni.

# Egy Hálózat

## Bevezetés

**Emlékszünk még ...?**

**Megjegyzés:** A tanulók egyedül, párban, vagy osztály szinten is megoldhatják ezt a feladatot.

Figyeljük meg a két hálózati ábrát. Hasonlítsuk össze a két hálózatot, és keressük meg a különbségeket. Készítsünk feliratot az eszközökhöz mindkét hálózatban. Ha a címkézés elkészült, már tudni fogjuk, milyen közvetítő és végberendezések találhatók az egyes hálózatokban.

Miben különbözik a két hálózat? Csak abban, hogy a B-ben több eszköz van, mint az A-ban?

Válasszuk ki, melyiket használnánk egy kis- vagy középvállalat tulajdonosaként! Indokoljuk meg választásunkat a következő szempontok alapján: költség, sebesség, csatlakozás, bővíthetőség, felügyelet!

[Csoportos feladat - Did You Notice Instructions](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/11.0.1.2%20Class%20Activity%20-%20Did%20You%20Notice%20Instructions.pdf)

# Létrehozás és növekedés

## Kis hálózatok eszközei

Az üzleti világ jelentős része kisvállalkozás, így nem meglepő dolog, hogy a hálózatok többsége kis hálózat.

A kis hálózatok tervezése viszonylag egyszerű, mivel lényegesen kevesebb számú és típusú eszközt tartalmaznak, mint a nagyméretű hálózatok. A kis hálózati topológiák jellemzően egyetlen forgalomirányítóból és legfeljebb néhány kapcsolóból épülnek fel. Tartalmazhatnak még vezeték nélküli elérési pontokat (forgalomirányítóval egybeépítve is) és IP-telefonokat. Internet kapcsolatuk általában egyetlen WAN-csatlakozás, amely DSL, kábel vagy Ethernet szolgáltatáson keresztül valósul meg.

Egy kis hálózat felügyelete nagyon hasonló képességeket igényel, mint egy nagy hálózaté. A munka többségét a meglévő berendezések karbantartása és hibaelhárítása, valamint a hálózat- és információbiztonság megvalósítása jelenti. A kis hálózatok felügyeletét elláthatja a vállalat egy alkalmazottja vagy egy szerződéssel megbízott személy, függően a vállalat méretétől és típusától.

Az ábrán egy tipikus kisvállalati hálózat látható.

# Létrehozás és növekedés

## Kis hálózatok eszközei

A felhasználói igények kielégítése érdekében a kis hálózatok megvalósítása is átgondolást és tervezést igényel, mely magában foglalja az összes követelményt, költségelemet és fejlesztési lehetőséget.

A tervezés egyik első lépése a közvetítő eszközök típusának kiválasztása, melynek szempontjai az ábrán láthatók.

**Költség**

A költség az egyik legfontosabb szempont a kis hálózatok berendezéseinek kiválasztásakor. A kapcsolók és forgalomirányítók árát teljesítményük és képességeik határozzák meg. A teljesítmény magában foglalja a portok számát, típusát és az eszköz belső sebességét. A költséget befolyásoló tényezők még a hálózatfelügyeleti képességek, a beépített biztonsági funkciók és a választható bővítési lehetőségek. Figyelembe kell venni még a hálózati eszközök csatlakoztatásához szükséges kábelezés költségét is. Külön költségvetési elem, hogy milyen mértékű redundancia kerüljön beépítésre a hálózatba, beleértve az eszközöket és azok portjait, a réz vagy optikai kábeleket.

**Portsebesség és interfész típus**

A kapcsolók és forgalomirányítók portszámának és típusának kiválasztása kritikus döntés. Az ilyenkor felmerülő kérdések: "Válasszunk a jelenlegi kívánalmaknak megfelelő portszámot, vagy vegyük figyelembe a növekedési követelményeket is?", "Szükségünk van különböző UTP sebességekre?", "Kellenek UTP és optikai portok is?"

Az új számítógépek 1 Gbps-os hálózati kártyával rendelkeznek, 10 Gbps porttal csak néhány munkaállomás és szerver van felszerelve. Bár drágább, de érdemes nagyobb sebesség fogadására alkalmas Layer 2 eszközöket választani, megelőzve ezzel a hálózat fejlesztése során a központi eszközök cseréjét.

**Bővíthetőség**

A hálózati eszközök moduláris és rögzített fizikai összeállításban is kaphatók. Fix konfiguráció esetén adott a portok vagy interfészek száma és típusa. A moduláris berendezések bővítőhelyekkel rendelkeznek, így új modulok hozzáadásával rugalmasan lehet követni az igényeket. A legtöbb ilyen berendezés alap beépített portokkal és további üres bővítőhelyekkel kerül forgalomba. Kapcsolók esetében speciális kiegészítő portok szolgálják a nagy sebességű gerinchálózathoz való csatlakozást (uplink portok). Továbbá, mivel a forgalomirányítók több különböző típusú hálózatot kötnek össze, külön figyelmet kell fordítani az adott média számára megfelelő modul kiválasztására. A megfontolandó kérdések: "Válasszunk cserélhető modulokkal rendelkező eszközt?", "Kellenek WAN-interfészek a forgalomirányítóba, és ha igen, milyen típusúak?"

**Az operációs rendszer jellemzői és szolgáltatásai**

Az operációs rendszer verziójától függően a hálózati eszközök a következő jellemzőkkel és szolgáltatásokkal rendelkeznek:

* Biztonság
* QoS
* VoIP
* Layer 3 kapcsolás
* NAT
* DHCP

A forgalomirányítók költségeit megnövelhetik a szükséges interfészek és szolgáltatások, valamint a kiegészítő modulok, például a optikai kártyák is tovább növelik a hálózati eszközök költségét.

# Létrehozás és növekedés

## Kis hálózatok eszközei

Egy kis hálózat megvalósításához is szükséges IP-címzési terv. Egy hálózat állomásai számára egyedi címet kell biztosítani, és ezek kiosztása még egy kis hálózatban sem lehet véletlenszerű. A címzési séma tervezését, dokumentálását és karbantartását a megcímzett eszközök típusának figyelembevételével kell elvégezni.

Példa néhány eszköztípusra, mely hatással van az IP-címzési tervre:

* Felhasználói végberendezések
* Szerverek és perifériák
* Az internet felől elérhető állomások
* Közvetítő eszközök

Az IP-címzés tervezése és dokumentálása segíti a rendszergazdát az eszközök közötti eligazodásban. Például, ha az összes szerver az 50-100 közötti tartományból kap címet, akkor a forgalmuk könnyen azonosítható IP-cím alapján. Ez nagyon hasznos a hálózati forgalom problémáinak protokoll elemzővel történő hibaelhárítása során.

Továbbá egy jól meghatározott IP-címzési rendszer használata esetén a rendszergazdák hatékonyabban képesek a hálózati erőforrásokat felügyelni. Ez különösen fontos lehet azon állomások esetében, melyek a belső és a külső hálózatnak is nyújtanak szolgáltatásokat. Ebbe a körbe tartoznak például a web és az e-kereskedelem szerverei. Ha a hozzájuk rendelt IP-címek nem tervezettek és nem dokumentáltak, akkor az eszközök biztonsága és hozzáférhetősége nehezen ellenőrizhető. Ha egy szerver véletlenszerűen kap címet, akkor a szerverhez történő hozzáférés letiltása nehezen megoldható valamint az adott erőforrás a kliensek számára könnyen elérhetetlenné válhat.

A fenti eszköztípusokhoz különálló logikai címblokkot kell rendelni a hálózati címtartományból.

Kattintsunk a gombokra a hozzárendelési módszer megtekintéséhez!

# Létrehozás és növekedés

## Kis hálózatok eszközei

A hálózattervezés másik fontos eleme a megbízhatóság. A kisvállalkozások üzleti folyamatai számára gyakran elengedhetetlen a hálózat működése, és annak hibája jelentős veszteséget okozhat. A hálózat megtervezésekor a magas szintű megbízhatóság fenntartásához és az elsődleges meghibásodási pontok kiküszöböléséhez redundanciára van szükség. A hálózati redundancia megvalósításának többféle módja közül az egyik a berendezések másodpéldányainak telepítése, a másik a hálózati összeköttetések többszörözése, ahogy az ábrán is látható.

Minél kisebb a hálózat, annál kisebb az esély arra, hogy a berendezések duplikálása kifizetődő lesz. Ezért gyakori megoldás, hogy csak a kapcsoló-kapcsoló és a kapcsoló-forgalomirányító közötti összeköttetéseket kettőzik meg.

A szerverek körében is elterjedt a több porttal rendelkező hálózati kártya, mely támogatja a redundáns csatlakozást egy vagy több kapcsolóhoz. A kis hálózatokban rendszerint web, fájl és e-mail szerverek találhatók.

A kis hálózatoknak általában egy kijáratuk van az internet felé egy vagy több alapértelmezett átjárón keresztül. Az egyetlen forgalomirányítót tartalmazó topológiában redundancia csak a 3. rétegbeli útvonalak tekintetében valósítható meg, mégpedig a forgalomirányítón több belső oldali Ethernet interfész használatával. Ilyenkor a forgalomirányító meghibásodása a teljes hálózat internet kapcsolatának elvesztését eredményezi. Éppen ezért a kisvállalkozások számára is kifizetődő lehet egy olcsó másodlagos összeköttetés előfizetése (backup).

# Létrehozás és növekedés

## Kis hálózatok eszközei

A felhasználók állandó hozzáférést igényelnek elektronikus leveleikhez és osztott használatú állományaikhoz. A cél elérése érdekében a hálózat tervezőjének a következő feladatai vannak:

**1**. A fájl és levelező szerverek biztonságos elhelyezése egy központi helyiségben.

**2**. A helyiség védelme a jogosulatlan belépéstől fizikai és logikai eszközökkel.

**3**. Szerver redundancia létrehozása, mely biztosítja egy eszköz meghibásodása esetén a fájlok sértetlenségét.

**4**. Tartalék összeköttetések biztosítása a szerverekhez.

A modern hálózatokat gyakran használják a vásárlók és az üzleti partnerek közötti IP-alapú hang- és videokommunikációra. Az ilyen típusú konvergens hálózat beépített vagy kiegészítő lehetőségként tartalmazza a nyers adatok IP-hálózatba ágyazását. A hálózati rendszergazdának a rendszer tervezésekor tekintetbe kell vennie a különféle forgalomtípusokat és azok kezelésének módját. A kis hálózatok forgalomirányítóit és kapcsolóit úgy kell konfigurálni, hogy a valós idejű forgalmat, mint például a hang- és a videó átvitelt az egyéb adatforgalomtól elválasztva kezeljék. Egy jó hálózati tervben a forgalom prioritás alapján kerül osztályozásra, ahogy ez az ábrán is látható. Jellegzetes forgalmi osztályok lehetnek:

* Fájlátvitel
* E-mail
* Hang
* Videó
* Üzenetküldés
* Üzleti

Egy jó hálózati terv végső célja, kis hálózatok esetén is, a munka hatékonyságának növelése és a kiesési idő minimalizálása.

# Létrehozás és növekedés

## Protokollok egy kis hálózatban

Egy hálózat csak olyan mértékben hasznos, mint amennyire a rajta lévő alkalmazások. Az alkalmazási rétegben kétféle szoftver vagy folyamat van, ami hozzáférést biztosít a hálózathoz: a hálózati alkalmazások és az alkalmazási rétegbeli szolgáltatások (lásd ábra).

**Hálózati alkalmazások**

A hálózati alkalmazások olyan szoftverek, melyek alkalmasak a hálózaton keresztüli kommunikációra. Néhány felhasználói program hálózat-tudatos, ami azt jelenti, hogy a beléjük ágyazott alkalmazási rétegbeli protokollok képesek közvetlenül kommunikálni az alsóbb rétegbeli protokollokkal. Ilyen alkalmazások például az email kliensek és a böngészőprogramok.

**Alkalmazási rétegbeli szolgáltatások**

Más programoknak az alkalmazási réteg szolgáltatásai nyújtanak segítséget az olyan hálózati erőforrások használatához, mint a fájl átvitel vagy a hálózati nyomtatás. Noha a felhasználó számára a szolgáltatások láthatatlanok, mégis ezek a programok teremtenek kapcsolatot a hálózattal és készítik elő az adatokat az átvitelre. A különféle adattípusok, legyenek azok szöveg, grafika vagy videó, különféle szolgáltatásokat igényelnek, hogy megfelelően elő legyenek készítve az OSI-modell alsóbb rétegeiben való feldolgozásra.

Minden hálózati alkalmazás vagy szolgáltatás protokollokat használ, melyek szabályokat és adatformátumokat tartalmaznak. Protokollok nélkül a hálózat képtelen lenne az adatok kezelésére és továbbítására. A különféle hálózati szolgáltatások funkcióinak megértéséhez szükség van az őket irányító legfontosabb protokollokban való jártasságra.

# Létrehozás és növekedés

## Protokollok egy kis hálózatban

Egy szakember legtöbb feladatában valamilyen módon megjelennek a hálózati protokollok, legyen szó akár egy kis, akár egy nagy hálózatról. Kis hálózat felhasználói által használt alkalmazásokat és szolgáltatásokat támogató leggyakoribb hálózati protokollok a következők:

* DNS
* Telnet
* IMAP, SMTP, POP (email)
* DHCP
* HTTP
* FTP

Az ábrán lévő szerverekre kattintva azok hálózati szolgáltatásainak rövid leírását jeleníthetjük meg.

Ezek a hálózati protokollok tartalmazzák a hálózati szakember számára szükséges alapvető segédeszközöket is. A hálózati protokollokban meghatározásra kerülnek:

* A kommunikációs viszony kezdetének és végének folyamatai
* Üzenettípusok
* Az üzenetek szintaxisa
* Az információs mezők jelentése
* Az üzenetküldés módja és az arra adott válasz
* Az alsóbb rétegekkel való kölcsönhatás

Sok szervezet házirendje megköveteli e protokollok biztonságos változatainak használatát, ilyenek például a HTTPS, SFTP, SSH.

# Létrehozás és növekedés

## Protokollok egy kis hálózatban

Az előzőekben ismertetett protokollokon túl a mai cégek, még a kicsik is, gyakran használnak valósidejű alkalmazásokat az üzleti partnerekkel való kapcsolattartásra. Mivel a kisvállalkozások nem képesek a Cisco Telepresence megoldás finanszírozására, ezért olyan valósidejű alkalmazásokat választanak, melyek megfizethetők számukra, lásd 1. ábra. A valós idejű alkalmazások más adattípusokhoz képest több tervezést és magasabb szintű szolgáltatásokat igényelnek a hang és a videó forgalom megfelelő prioritással történő továbbításához. Ezért a hálózati rendszergazdának gondoskodni kell a megfelelő berendezések telepítéséről és konfigurálásáról. A 2. ábrán a kis hálózatok valósidejű alkalmazásaihoz szükséges eszközök láthatók.

**Infrastruktúra**

Az infrastruktúrának illeszkedni kell a jelenlegi és a tervezett valósidejű alkalmazások adatforgalmának jellemzőihez. A hálózat tervezőjének feladata annak eldöntése, hogy a meglévő kapcsolók és kábelezés képes-e a megnövekedett forgalom fogadására. Egy gigabites átvitelre képes hálózat megfelel ezen követelményeknek és nem szükséges az infrastruktúra módosítása. Ha a régi kapcsolók nem támogatják a PoE (Power over Ethernet, Etherneten keresztüli tápellátás) technológiát, vagy a kábelezés nem felel meg a sávszélesség követelményeknek, akkor mindkét esetben fejlesztés szükséges.

**VoIP**

A VoIP a hagyományos telefont használó szervezeteknél valósítható meg. A VoIP működéséhez hangtámogatással rendelkező forgalomirányítók szükségesek, melyek a hagyományos telefonvonal hangjeleit IP-csomagokká alakítják. A jelek IP-csomaggá alakítása után a forgalomirányító továbbítja azokat a megfelelő helyre. A VoIP lényegesen olcsóbb megoldás, mint egy integrált IP-telefon megvalósítás, de a kommunikáció minősége meg sem közelíti azt. A kisvállalatok számára is megvalósítható IP alapú hang- és videótovábbítás például a Skype vagy a Cisco WebEx alapváltozatának alkalmazásával.

**IP-telefónia**

IP-telefónia esetén maga a telefonkészülék végzi a hang átalakítását IP-csomaggá, ezért nincs szükség hangtámogatással rendelkező forgalomirányítóra. IP-telefonok esetében egy dedikált szerver végzi a hívások kezelését és felügyeletét. Ma már sok gyártó kínál IP-telefon megoldásokat kis hálózatok számára.

**Valósidejű alkalmazások**

Az adatfolyamok eredményes továbbításához a hálózatnak támogatni kell a késleltetésérzékeny alkalmazások követelményeit. Az RTP (Real-time Transport Protocol) és az RTCP (Real-time Transport Control Protocol) két olyan protokoll, mely megfelel az előbbi elvárásoknak. Az RTP és az RTCP azáltal képes a hálózati erőforrások vezérlésére és elosztására, hogy beépített QoS (Quality of Service) mechanizmusokkal rendelkezik. Ez a QoS-technika hatékony eszközöket biztosít a késleltetési hibák minimalizálására a valósidejű adattovábbítás során.

# Létrehozás és növekedés

## A hálózat növekedése

A növekedés a kisvállalkozások természetes folyamata, melyet hálózataiknak is követni kell. A kis hálózat rendszergazdája dolgozhat visszahatóan vagy előrehatóan, függően a vállalati vezetéstől, melynek gyakran ő is tagja. Ideális esetben a hálózati rendszergazdának elegendő ideje van a hálózat növekedésével kapcsolatos döntések meghozatalára, melyek illeszkednek a vállalat növekedési folyamatába.

A hálózat méretezéséhez szükséges elemek:

* **Hálózati dokumentáció** - fizikai és logikai topológia
* **Eszközleltár** - a hálózatot alkotó és használó berendezések listája
* **Költségvetés** - részletes IT-költségvetés, mely tartalmazza az üzleti év eszközbeszerzésre fordítandó kiadásait
* **Forgalom elemzés** - protokollok, alkalmazások és szolgáltatások, valamint a hozzájuk tartozó forgalmi követelmények

Ezek az információk szükségesek a kis hálózatok bővítésével kapcsolatos döntéshozatalban.

# Létrehozás és növekedés

## A hálózat növekedése

A kis hálózatok felügyelete és fejlesztése jártasságot kíván a protokollok és hálózati alkalmazások tekintetében. Ha egy kis hálózat rendszergazdája nem tud időt szakítani minden hálózati eszköz kihasználtságának külön megfigyelésére, akkor jelentős segítséget nyújthat neki egy szoftver vagy hardver alapú protokollelemző használata.

Mint az ábrán is látható, protokollelemző segítségével a hálózati szakember gyorsan össze tud állítani egy statisztikát a hálózati forgalomról.

A hálózati forgalom kezeléséhez, különösen bővülő hálózat esetén, nagyon fontos a forgalom típusának és mennyiségének ismerete. Ha a forgalom típusa ismeretlen, a protokollelemző segíthet az azonosításban és a forrás felkutatásában.

A hálózat forgalmi mintáinak meghatározása érdekében fontosak az alábbiak:

* A hálózat használatának csúcsidejében rögzítsük a csomagokat, így megfelelően jó mintát nyerhetünk a különböző típusú forgalmakból.
* Mivel bizonyos forgalomtípusok adott helyhez köthetőek, mindig vegyünk mintát több hálózati szegmensről is.

Ezután a begyűjtött adatok rendszerezhetők az üzenetek forrása, célja és típusa szerint is. Az elemzés alapján meghozhatók azok a döntések, melyekkel hatékonyabban felügyelhető a hálózati forgalom. Ilyen lehet például a szükségtelen forgalom csökkentése vagy az adatfolyam szerkezetének megváltoztatása egy szerver áthelyezésével.

Néha csupán egyetlen szerver vagy szolgáltatás áttelepítése egy másik hálózati szegmensbe, képes megnövelni a hálózat teljesítményét és elsimítani a megnövekedett forgalmi igényeket. Máskor azonban csak a hálózat újratervezésével vagy komolyabb beavatkozással lehet a hálózati teljesítményt optimalizálni.

# Létrehozás és növekedés

## A hálózat növekedése

A forgalmi trendek változásának megértésén túl a hálózati rendszergazdának tisztában kell lennie a hálózat használatával kapcsolatos változásokkal is. A kis hálózat rendszergazdájának feladata egy személyre szóló IT "pillanatfelvétel" elkészítése a dolgozók egy meghatározott csoportjának programfelhasználásról. Ez a pillanatfelvétel rendszerint a következőket tartalmazza:

* Operációs rendszer és annak verziója
* Lokális alkalmazások
* Hálózati alkalmazások
* CPU-használat
* Meghajtók használata
* Memória használat

A kis hálózat felhasználóiról rendszeresen készített pillanatfelvételek elemzése olyan információkhoz juttatja a hálózati rendszergazdát, melyek alapján teljesíthetők a protokoll és a hozzá kapcsolódó forgalom által támasztott követelmények. Tegyük fel, hogy néhány alkalmazott külső forrásokat, például közösségi oldalakat használ a vállalat marketing helyzetének javításához. Amikor ezek a dolgozók a vállalathoz kerültek, kevésbé foglalkoztak a internet alapú reklámozással. A hálózat felhasználói szokásainak megváltozása a rendszergazdától a hálózati erőforrások megfelelő átcsoportosítását igényli.

Ezért a hálózati rendszergazda feladata a hálózat kihasználtságának és az adatforgalom követelményeinek nyomon követése, valamint a termelékenység javítása és az üzlet növekedése érdekében a szükséges módosítások végrehajtása.

# Hálózatbiztonság

## Hálózati eszközök biztonsága

A vezetékes vagy vezeték nélküli számítógép hálózatok mindennapi életünk fontos kellékei. Mind a magánszemélyek, mind a szervezetek egyaránt függenek számítógépeiktől és hálózatuktól. Egy jogosulatlan személy behatolása költséges hálózati leállást és a munka elvesztését eredményezheti. Egy hálózat elleni támadás lehet végzetes, valamint a fontos információk és eszközök megrongálása vagy ellopása okozhat idő- és pénzveszteséget.

A behatolók hozzáférést szerezhetnek a hálózathoz a szoftver sebezhető pontjain keresztül, hardver elleni támadással vagy egy felhasználó nevének és jelszavának kitalálásával. Azt a behatolót, akik a szoftver módosításával vagy sebezhető pontjainak kihasználásával jut hálózati hozzáféréshez gyakran hacker-nek (hekker, számítógépkalóz) nevezik.

A hacker hozzáférése a hálózathoz négyféle fenyegetést jelenthet:

* Információlopás
* Azonosító lopás
* Adatvesztés és manipuláció
* Szolgáltatás megszakítása

Bővebb információért kattintsunk a képekre!

Kis hálózatok tervezése és megvalósítása során is szükség van a biztonsági fenyegetések és sebezhetőségek áttekintésére.

# Hálózatbiztonság

## Hálózati eszközök biztonsága

Amikor hálózati vagy számítógép biztonságról beszélünk, általában a szoftverek sebezhetőségét kihasználó támadóra gondolunk. Ugyanennyire fontos azonban az eszközök fizikai biztonsága is, hiszen egy támadó megakadályozhatja a hálózati erőforrások használatát, ha azokat fizikailag képes veszélyeztetni.

A fizikai fenyegetések négy formája:

* **Hardver fenyegetések** - szerverek, munkaállomások, forgalomirányítók, kapcsolók és a kábelezés fizikai megrongálása.
* **Környezeti fenyegetések** - szélsőséges hőmérséklet (túl meleg vagy hideg) vagy szélsőséges páratartalom (túl nedves vagy száraz)
* **Elektromos veszélyek** - feszültség tüskék, alacsony feszültségszint (feszültségesés), szűrés nélküli tápellátás (zaj), áramszünet
* **Karbantartási veszélyek** - az elektromos összetevők hanyag kezelése (elektrosztatikus feltöltődés), kritikus alkatrészek hiánya, hibás kábelezés és hiányos feliratozás

Ezen problémák egy részének szerepelni kell a vállalat házirendjében, más részük megoldása a szervezet vezetőségének hatáskörébe tartozik.

# Hálózatbiztonság

## Hálózati eszközök biztonsága

A három fontos hálózatbiztonsági tényező: sebezhetőség, fenyegetés és támadás.

A sebezhetőség a gyengeség fokmérője, mely minden hálózatban és eszközben eredendően benne rejlik, beleértve a forgalomirányítókat, kapcsolókat, szervereket, munkaállomásokat, és még a biztonsági eszközöket is.

Fenyegetésekbe beleszámítanak azok az emberek, akik érdekeltek és kellőképpen képzettek is a biztonsági sebezhetőségek kihasználására. Az ilyen személyek folyamatosan keresik az új lehetőségeket és gyengeségeket.

A fenyegetések különféle segédeszközök, szkriptek és programok formájában jelennek meg, melyek alkalmasak a hálózatok és a hálózati eszközök megtámadására. Ezek a hálózati eszközök általában végberendezések, például szerverek vagy asztali számítógépek.

A három elsődleges sebezhetőségi pont:

* Technológiai (lásd 1. ábra)
* Konfiguráció (lásd 2. ábra)
* Biztonsági házirend (lásd 3. ábra)

Mindhárom sebezhetőség vagy gyengeség különféle támadásokra ad lehetőséget, ilyenek például a rosszindulatú programok vagy a hálózati támadások.

# Hálózatbiztonság

## Sebezhetőségi pontok és hálózati támadások

A rosszindulatú kód támadások (malicious code attack) közé azokat a számítógép programokat soroljuk, melyeket adatvesztés vagy sérülés okozása céljából hoztak létre. Három fő típusuk a vírusok, a trójai lovak és a férgek.

A vírus egy rosszindulatú szoftver, mely más programokba ágyazva nemkívánatos hatást okoz egy munkaállomáson. Vírus például egy program, amely beágyazódik a command.com állományba (ez a Windows rendszerek elsődleges parancsértelmezője), letöröl bizonyos fájlokat és megfertőz minden más command.com állományt, amit talál.

A Trójai ló annyiban különbözik ettől, hogy az alkalmazás egészen másnak látszik, mint ami valójában, miközben igazából egy támadási eszköz. Trójai ló például egy olyan alkalmazás, mely egyszerű játékként fut a munkaállomáson. Miközben a felhasználót lefoglalja a játék, a trójai elküldi saját másolatát a felhasználói címjegyzékben szereplő összes címre. A címzettek megkapják és futtatják a játékot, ezáltal tovább terjesztik a Trójai lovat a saját címjegyzékükben szereplőknek.

A vírusoknak a víruskód más rendszerbe való átviteléhez egy továbbító mechanizmusra, például egy levélhez csatolt zip vagy exe fájlra van szükségük. A vírusok és férgek közötti alapvető különbség az, hogy a vírus továbbterjedéséhez emberi közreműködés szükséges.

A férgek önálló programok, melyek megtámadják a rendszert és megpróbálják kihasználni annak sebezhető pontjait. A sikeres támadás után a féreg átmásolja önmagát a megtámadott rendszerbe, és a folyamat kezdődik elölről. Egy féregtámadás anatómiája a következő:

* **A sebezhetőség** - A féreg feltelepíti magát a rendszer egy ismert gyenge pontját kihasználva, például amikor egy naiv felhasználó megnyit egy futtatható email csatolmányt.
* **Terjesztési mechanizmus** - Az állomáshoz való hozzáférés megszerzése után a féreg másolatot készít önmagáról, majd új célpontot választ.
* **Hasznosítás** - A megfertőzött állomáshoz a támadó gyakran olyan jogosultságot szerez, mellyel a helyi lehetőségeket kihasználva adminisztrátorrá válhat.

# Hálózatbiztonság

## Sebezhetőségi pontok és hálózati támadások

A rosszindulatú szoftver támadásokon kívül a hálózat áldozatul eshet különféle hálózati támadásoknak is. A hálózati támadások három fő kategóriába sorolhatók:

* **Felderítéses támadások** - a rendszerek, szolgáltatások és sebezhetőségek jogosulatlan feltérképezése
* **Hozzáférési támadások** - adatok, rendszerhozzáférések és felhasználói jogok illetéktelen kezelése
* **Szolgáltatásmegtagadás** - hálózatok, rendszerek és szolgáltatások megbénítása vagy elrontása

**Felderítéses támadások**

Egy külső támadó internetes eszközöket használva, például nslookup vagy whois segédprogramok segítségével könnyen megállapíthatja egy adott szervezet IP-címtartományát. Ezután a támadó a tartomány publikus IP-címeinek megpingelésével ki tudja választani az aktív állomásokat. Ez a feladat egy "ping sweep" (ping pásztázás) segédprogrammal, mint például az fping vagy a gping automatizálható is, hiszen ezek a programok szisztematikusan végigpingelik a összes címet egy adott tartományban vagy alhálózatban. Ez pont olyan, mint egy telefonkönyvben végighívni az összes számot azt figyelve, hogy melyiket veszik fel.

Kattintsunk az ábrán lévő felderítéses támadás eszközökre és figyeljük meg az animációt!

# Hálózatbiztonság

## Sebezhetőségi pontok és hálózati támadások

**Hozzáférési támadások**

A hozzáférési támadások a hitelesítési, FTP és web szolgáltatások ismert sebezhetőségi pontjait használják ki a bejelentkezési adatok, bizalmas információk megszerzéséhez. Ennek eredményeképpen a támadó személy jogosulatlan hozzáférés által jut hozzá számára titkos adatokhoz. A hozzáférési támadások négy csoportba oszthatók. Az egyik leggyakoribb támadástípus a jelszó elleni támadás, amely egy protokollelemző segítségével is végrehajtható, elfogva az egyszerű szövegként továbbított felhasználóneveket és jelszavakat. Szintén ide sorolhatók a megismételt bejelentkezési próbálkozások, melyek osztott erőforrások, például szerverek vagy forgalomirányítók felhasználónevének és jelszavának megszerzésére irányulnak. Az ismétléses támadásokat nevezik még szótár (dictionary) vagy nyers erő (brute-force) támadásoknak is.

Kattintsunk az ábrán lévő gombokra a hozzáférési támadások néhány példájának megtekintéséhez!

# Hálózatbiztonság

## Sebezhetőségi pontok és hálózati támadások

**Szolgáltatás megtagadás**

A DoS (Denial of Service, szolgáltatás megtagadás) támadás a legismertebb és a legnehezebben kiküszöbölhető támadásforma. Még a hekker társadalomban is jelentéktelennek és helytelennek számítanak a DoS-támadások, mivel csekély erőfeszítés árán végrehajthatók. Ugyanakkor pontosan a könnyű megvalósítás és a lehetséges jelentős károkozás miatt követelnek kiemelt figyelmet a biztonsági szakemberek részéről.

Sokféle DoS-támadás létezik, de végeredményként mindegyik a rendszer erőforrásainak felemésztésével akadályoz meg jogosult felhasználókat egy szolgáltatás használatában.

Kattintsunk az ábrán lévő gombokra a DoS és DDoS (Distributed DoS, szétosztott szolgáltatás megtagadás) támadások néhány példájának megtekintéséhez!

# Hálózatbiztonság

## Hálózati támadások elhárítása

A vírusirtó szoftverek felismerik a legtöbb vírust és trójai lovat, és megakadályozzák szétterjedésüket a hálózatban. Működhetnek helyi felhasználói vagy hálózati szinten is.

A legutóbbi fejlesztések eredményeinek folyamatos alkalmazása eredményesebb védekezést tehet lehetővé ezen támadások ellen. Amint egy új vírus vagy trójai megjelenik, a vállalkozásoknak frissíteniük kell víruskereső szoftvereik adatbázisát.

A féreg támadások elhárítása is odafigyelést igényel a hálózati adminisztrációval foglalkozó személyzettől. A védekezés javasolt lépései:

* **Elszigetelés** - A féreg terjedésének megakadályozása a hálózatban a fertőzésmentes részek leválasztásával.
* **Immunizálás** - Hibajavító csomagok telepítése és sebezhetőségi pontok keresése a rendszerben.
* **Karantén** - A fertőzött gépek azonosítása, majd leválasztása vagy eltávolítása a hálózatból.
* **Mentesítés** - A fertőzött rendszerek tisztítása és javítása, mely néhány féreg esetében teljes újratelepítést igényel.

A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch). Ennek megvalósítása nehézkes az ellenőrzés nélküli felhasználói rendszereket tartalmazó helyi hálózatban. Nagyszámú rendszer felügyelete maga után vonja egy általános szoftvercsomag, vagy más néven "image" létrehozását (operációs rendszer és kliens alkalmazások), amely telepítéskor vagy frissítéskor használható. Amennyiben a biztonsági követelmények változnak, a már üzemelő rendszereken is szükség van a biztonsági frissítések telepítésére.

Az egyik megoldás a kritikus biztonsági javítócsomagok kezelésére egy központi elosztó szerver létrehozása, mellyel időközönként minden rendszernek kommunikálni kell (lásd ábra). Az állomásról hiányzó frissítések automatikusan letöltődnek a patch szerverről és felhasználói beavatkozás nélkül települnek.

# Hálózatbiztonság

## Hálózati támadások elhárítása

A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, melyek a hálózati eszközök hozzáférés-szabályozásának alapját alkotják. Az AAA vezérli, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultság), és nyomon követi a használat során végrehajtott műveleteket (naplózás). Az AAA jobb méretezhetőséget biztosít, mint az önmagukban használt konzol, AUX, VTY és privilegizált EXEC hitelesítési parancsok.

**Hitelesítés**

A felhasználóknak és az adminisztrátoroknak igazolniuk kell, hogy azok, akiknek mondják magukat. Erre a hitelesítés nyújt lehetőséget felhasználónév és jelszó, ellenőrző kérdés és válasz, belépőkártya, vagy más módszer segítségével. Például: "Én a 'diák' nevű felhasználó vagyok. Igazolni tudom ezt azzal, hogy ismerem a hozzá tartozó jelszót."

Kis hálózatban gyakran használt megoldás a helyi hitelesítés, melynek során minden eszköz saját adatbázisában tárolja a hozzá tartozó felhasználónév/jelszó kombinációkat. Sok felhasználó esetén azonban a lokális adatbázisok karbantartása meglehetősen összetett művelet, a hálózat és az eszközök számának növekedésével pedig a helyi hitelesítés fenntartása bonyolult és követhetetlen. Például, ha 100 hálózati eszközünk van, akkor az összes felhasználói fiókot hozzá kell adnunk mind a 100 eszközhöz.

Nagyobb hálózatok számára jobban méretezhető megoldás a külső hitelesítés, mely a felhasználói bejelentkezések ellenőrzését egy távoli szerveren végzi el. A felhasználók külső hitelesítésére használt két legnépszerűbb módszer a RADIUS és a TACACS+.

* A RADIUS egy kis CPU és memóriaigényű nyílt szabvány, melyet főleg hálózati eszközök, például kapcsolók, forgalomirányítók és vezeték nélküli berendezések esetében alkalmaznak.
* A TACACS+ hitelesítési, jogosultság kezelési és naplózási szolgáltatást nyújtó biztonsági megoldás, amely kiszolgálói alkalmazásként egy szerveren fut.

**Jogosultság kezelés**

A hitelesítést követően a jogosultságokat kezelő szolgáltatás megállapítja, hogy a felhasználó mely erőforrásokat érheti el és milyen műveleteket végezhet. Például: "A 'diák' nevű felhasználó csak Telnet-en kapcsolódhat az XYZ szerverhez."

**Naplózás**

A naplózó szolgáltatás feljegyzést készít a felhasználó minden cselekedetéről, beleértve, hogy mihez kapcsolódott, mennyi ideig használta az erőforrást és milyen módosításokat hajtott végre. A naplózás nyomon követi, hogy miként történt a hálózati erőforrások használata. Például: "A 'diák' nevű felhasználó Telnet-en kapcsolódott az XYZ szerverhez 15 percen keresztül."

Az AAA fogalom a bankkártya használathoz hasonlítható. A kártya meghatározza, hogy ki használhatja, mennyit költhetnek el róla, és lekönyveli a felhasznált összeg sorsát. (lásd ábra)

# Hálózatbiztonság

## Hálózati támadások elhárítása

A hálózatra kapcsolt személyi számítógépek és szerverek védelmén kívül fontos a hálózatba érkező és onnan kimenő forgalom ellenőrzése is.

A tűzfal az egyik leghatékonyabb biztonsági eszköz, amely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is. A tűzfal termékek változatos technikákat használnak annak meghatározására, hogy mely forgalom számára legyen engedélyezve vagy tiltva a hálózathoz való hozzáférés. Ezek a módszerek a következők:

* **Csomagszűrés** - Tiltja vagy engedélyezi a hozzáférést IP-cím vagy MAC-cím alapján.
* **Alkalmazás szűrés** - Tiltja vagy engedélyezi a hozzáférést bizonyos alkalmazások számára portszámuk alapján.
* **URL-szűrés** - Tiltja vagy engedélyezi weboldalak elérését adott URL vagy kulcsszó alapján.
* **Állapot-alapú csomagszűrés (Stateful Packet Inspection, SPI)** - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nemkívánatos csomagok külön engedély hiányában kiszűrésre kerülnek. Az SPI képes arra is, hogy felismerjen és kiszűrjön bizonyos támadástípusokat, például a szolgáltatás megtagadást (DoS).

A tűzfalak egyidejűleg többféle szűrési módszert is támogathatnak, és gyakran hálózati címfordítást (Network Address Translation, NAT) is végeznek. A NAT a belső privát IP-címeket lecseréli egy külső publikus IP-címre, amellyel a csomagok továbbküldésre kerülnek a hálózaton. Ez egyben lehetővé teszi a belső címek külső felhasználók elől való elrejtését.

A tűzfalak különféle formában kerülnek forgalomba, amint az ábrán is látható.

* **Eszköz-alapú tűzfalak** - Az eszköz-alapú tűzfal olyan biztonsági berendezés, melybe a tűzfal célhardverként van beépítve.
* **Szerver-alapú tűzfalak** - A szerver-alapú tűzfal egy speciális alkalmazást tartalmaz, amely hálózati operációs rendszeren fut, például UNIX-on vagy Windows-on.
* **Integrált tűzfalak** - Az integrált tűzfal egy meglévő eszköz, például egy forgalomirányító tűzfalszolgáltatással kiegészítve.
* **Személyes tűzfalak** - Személyes tűzfal a munkaállomásokon található és nem a LAN védelmére tervezték. Képezheti az operációs rendszer részét vagy származhat külső gyártótól.

# Hálózatbiztonság

## Hálózati támadások elhárítása

Egy hálózat pontosan annyira biztonságos, mint amennyire a legsebezhetőbb összeköttetése. Bár a médiában leggyakrabban szereplő veszélyek a kívülről érkező fenyegetések, mint például az internetes férgek vagy DoS-támadások, de legalább ilyen jelentőséggel bír a belső és köztes hálózatok biztonsága is. A belső hálózat végpontokból, más néven állomásokból áll, melyek hálózati kliensként működő számítógépek vagy eszközök (lásd ábra). Gyakori végpont típusok a laptopok, asztali számítógépek, szerverek, okostelefonok és tabletek. Ha a felhasználók nem rendelkeznek gyakorlattal saját eszközeik biztonságával kapcsolatban, akkor nincs olyan óvintézkedés, mely garantálná a hálózat biztonságát.

Az állomások biztonsága az egyik legnagyobb kihívás a hálózati rendszergazda munkájában, mivel itt az emberi tényezőt is számításba kell venni. A vállalatnak rendelkezni kell jól dokumentált szabályzattal és a munkavállalóknak be kell tartaniuk az abban leírtakat. Ezenkívül az alkalmazottakat fel kell készíteni a hálózat megfelelő használatára is. A házirend szabályok gyakran tartalmazzák a víruskereső és behatolás megelőző szoftverek használatának módját. A minden részletre kiterjedő állomásbiztonsági megoldások a hálózati hozzáférés vezérlésén alapulnak.

A végpontok biztonsága megköveteli a hálózati infrastruktúra 2. rétegbeli eszközeinek védelmét is az olyan támadások ellen, mint például a MAC-cím hamisítás (MAC address spoofing), a MAC-címtábla túlcsordulás (MAC address table overflow), és a hálózati vihar (LAN storm). Ezt hívjuk támadás megelőzésnek.

# Hálózatbiztonság

## Eszközök biztonsága

A hálózatbiztonságnak része a valódi eszközök, köztük a végberendezések és a hálózati eszközök védelme is.

Egy új operációs rendszer telepítése után az eszköz biztonsági beállításai az alapértelmezett értéket veszik fel, mely a védelem szempontjából nem megfelelő. Cisco forgalomirányítók esetében a Cisco AutoSecure szolgáltatás segít a rendszer biztonságossá tételében (lásd ábra). A beállítás néhány egyszerű lépésből áll, melyek alkalmazhatók a legtöbb operációs rendszer esetében:

* Az alapértelmezett felhasználóneveket és jelszavakat azonnal meg kell változtatni.
* A rendszer erőforrásaihoz való hozzáférést csak az erre jogosult személyek számára szabad engedélyezni.
* A szükségtelen szolgáltatásokat és alkalmazásokat lehetőség szerint ki kell kapcsolni vagy le kell törölni.

A biztonsági frissítéseket megjelenésük után azonnal telepíteni kell az összes eszközre. Mivel a gyártótól szállított berendezések hosszabb időt is tölthetnek raktárakban, így nincsenek naprakész állapotban. Fontos a beüzemelés során a szoftver és biztonsági frissítések telepítése.

# Hálózatbiztonság

## Eszközök biztonsága

A hálózati eszközök védelme érdekében fontos az erős jelszavak használata, melynek irányelvei a következők:

* Használjunk legalább 8, de inkább 10 vagy annál több karakterből álló jelszavakat. A hosszabb jelszó biztonságosabb.
* Készítsünk bonyolult jelszavakat. Legyenek bennük kis- és nagybetűk, számok, speciális karakterek és szóközök, minden, ami megengedett.
* A jelszavakban kerüljük az ismétlődéseket, gyakori szavakat, betű- vagy számsorozatokat, felhasználóneveket, rokonok vagy háziállatok neveit, életrajzi adatokat, mint például a születési dátumok, azonosító számok, elődök nevei, vagy bármely könnyen azonosítható információ.
* Írjuk szándékosan rosszul a jelszót. Például: Smith=Smyth=5mYth vagy Security=5ecur1ty.
* Cseréljük gyakran a jelszavakat. Így ha a jelszó mégiscsak kitudódik, a támadónak kevesebb ideje marad annak használatára.
* Ne hagyjuk a leírt jelszavakat látható helyen, például az asztalon vagy a monitoron.

Az ábrán példákat láthatunk erős és gyenge jelszavakra.

A Cisco forgalomirányítókon a vezető szóközök törlődnek a jelszavakból, de az első karakter után begépeltek megmaradnak. Éppen ezért erős jelszót kapunk, ha a szóköz billentyű segítségével több szóból álló kifejezést hozunk létre. A "password" mintájára ezt "pass pharse"-nek nevezik, és sokkal könnyebben megjegyezhető a jelszónál, ráadásul hosszabb és nehezebb megfejteni is.

A rendszergazdának gondoskodni kell arról, hogy a hálózatban erős jelszavak legyenek használatban. Ennek vizsgálatára használhatók például azok a segédprogramok, melyeket a hekkerek egy jelszó erősségének meghatározásához alkalmaznak a "nyers erő" (brute force) támadások során.

# Hálózatbiztonság

## Eszközök biztonsága

Egy eszköz telepítésekor nagyon fontos a szervezet által támasztott biztonsági előírások betartása. Ez vonatkozik az elnevezési konvencióra is, mely egyszerű dokumentálást és következetességet tesz lehetővé, de egyben a biztonságot is figyelembe veszi. Például nem helyes az állomásnévben az eszköz használatával kapcsolatosan túl sok információt megadni. Ezen kívül még számos alapvető biztonsági intézkedést kell megtenni.

**További jelszóbiztonsági beállítások**

Az erős jelszavak csak akkor hasznosak, ha titokban maradnak. A következő lépések segíthetik a jelszavak titokban tartását. A globális konfigurációs módban kiadott **service password-encryption** parancs megakadályozza a jogosulatlan személyeket abban, hogy megnézhessék a konfigurációs állományban lévő titkosítatlan jelszavakat (lásd ábra). A parancs titkosítja az összes kódolatlan jelszót.

A konfigurált jelszavak minimális hosszának biztosítására globális konfigurációs módban a **security passwords min-length** parancs használható.

Egy másik módja a jelszavak megfejtésének a brute-force támadás, melynek során a hekker addig próbálgatja a különböző jelszavakat, amíg rá nem talál a megfelelőre. Az ilyen típusú támadások megelőzhetők a bejelentkezés letiltásával, ha a sikertelen próbálkozások száma meghalad egy értéket egy adott időtartamon belül.

Router(config)# **login block-for 120 attempts 3 within 60**

A parancs letiltja a bejelentkezést 120 másodperc időtartamra, ha 3 sikertelen kísérletet érzékel 60 másodpercen belül.

**Bejelentkezési üzenetek**

A bejelentkezési üzenet hasonlatos a "Tilos az átjárás!" táblához. Ez fontos a hivatalos eljárás során, ha valakit a rendszer illetéktelen használatával vádolnak meg. A bejelentkezési üzenetnek illeszkedni kell a szervezet biztonsági rendszabályaihoz.

Router(config)# **banner motd #message#**

**Időtúllépés**

Ajánlott ezen felül a végrehajtási időtúllépés beállítása, melynek során megmondjuk a Cisco eszköznek, hogy egy adott tétlenségi idő lejárta után jelentkeztesse ki a felhasználót. Időtúllépés konfigurálható a konzol, VTY és AUX portokra.

Router(config)# **line vty 0 4**

Router(config-vty)# **exec-timeout 10**

A parancs 10 perc tétlenség után kijelentkezteti a felhasználót .

# Hálózatbiztonság

## Eszközök biztonsága

**Távoli elérés SSH-n keresztül**

Az eszközök távolról történő kezelésének hagyományos protokollja a Telnet, mely nem biztonságos. A Telnet csomagokban lévő adatok titkosítás nélkül kerülnek átvitelre. Ezért a Wireshark vagy egy hozzá hasonló segédprogram használatával elfogható a Telnet párbeszéd és a jelszó megszerezhető. Éppen ezért a biztonságos távoli eléréshez nagyon ajánlott az SSH engedélyezése az eszközön . Az SSH támogatás Cisco eszközön való konfigurálásának négy lépése, mely az ábrán is látható, a következő:

**1.** Győződjünk meg a forgalomirányító állomásnevének egyediségéről, majd állítsuk be a hálózat IP-tartománynevét. Erre szolgál az **ip domain-name** *domain-name* parancs globális konfigurációs módban.

**2.** Szimmetrikus titkosító kulcspárt kell létrehozni a forgalomirányító SSH-folyamatának elindításához, az adatok kódolásához és dekódolásához. A kulcsgeneráláshoz globális konfigurációs módban a **crypto key generate rsa general-keys modulus** *modulus-size* parancs használható. A parancs egyes részeinek pontos jelentése összetett és túlmutat a kurzus keretein, így csak annyit jegyezzünk meg, hogy a modulus nagysága határozza meg a kulcs hosszát és értéke 360 és 2048 között lehet. A nagyobb modulus biztonságosabb kulcsot generál, de ekkor a titkosítási folyamat is több időt vesz igénybe. Az ajánlott minimális modulus hossz 1024 bit.

Router(config)# **crypto key generate rsa general-keys modulus 1024**

**3.** Hozzunk létre helyi felhasználót. Erre szolgál a **username** *"felhasználónév"* **secret** *"jelszó"* globális konfigurációs parancs.

**4.** Engedélyezzük vty vonali konfigurációs módban a bejövő SSH kapcsolódást a következő parancsokkal: **login local** és **transport input ssh**.

Ezután a forgalomirányító SSH szolgáltatása elérhető bármely SSH kliens alkalmazással.

# Hálózati teljesítmény

## Ping

A hálózat kiépítését követően a rendszergazda feladata a hálózati kapcsolatok megfelelő működésének ellenőrzése, továbbá a hálózati dokumentáció elkészítése.

**A ping** **parancs**

A **ping** parancs egy hatékony módja a kapcsolatok ellenőrzésének. Alkalmas a protokollkészlet vizsgálatára is, mivel a **ping** parancs működése a 3. rétegen túl az OSI-modell 2. és 1. rétegére is épül. A ping az ICMP-protokollt használja a kapcsolatok ellenőrzésére.

A **ping** parancs nem minden esetben tárja fel a probléma természetét, de segít a hibaforrás azonosításában. Ez egy nagyon fontos kezdeti lépés a hálózati hibaelhárításban.

A **ping** parancs nemcsak a protokollkészlet és az IP-konfiguráció ellenőrzésére, hanem a helyi és távoli állomásokkal való kapcsolat tesztelésére is alkalmas, amint az ábrán is látható. Léteznek olyan segédeszközök is, amelyek több információt szolgáltatnak, mint a **ping**parancs. Ilyen például a későbbiekben részletesen tárgyalásra kerülő Telnet és Trace.

**Az IOS ping jelei**

Az IOS parancssorában kiadott ping az általa küldött ICMP-üzenetekre kapott válaszokat különféle módon jelzi. A leggyakoribbak a következők:

* **!** - egy ICMP visszhang válasz (ICMP echo reply) megérkezését jelzi
* **.** - jelzi, hogy az ICMP visszhang (ICMP echo) üzenetre nem érkezett válasz a lejárati időn belül
* **U** - egy ICMP elérhetetlen (ICMP unreachable) üzentet érkezését jelzi

A "**!**" (felkiáltójel) azt jelenti, hogy a ping sikeresen befejeződött és a 3. rétegbeli kapcsolatok működnek.

A "**.**" (pont) azt jelenti, hogy hiba történt a kommunikáció során. Ez lehet kapcsolati probléma valahol az útvonalban, vagy jelezheti, hogy egy közbülső forgalomirányító nem talált útvonalat a cél felé és nem küldött "A cél nem érhető el" (ICMP destination unrechable) üzenetet. Továbbá mutathatja azt is, hogy a ping blokkolásra került egy eszköz biztonsági beállítása miatt.

Az "**U**" jelzi, hogy az útvonalon egy közbülső forgalomirányító nem rendelkezik elérési úttal a célcím felé, vagy a ping válasz blokkolásra került és feleletképpen egy ICMP unreachable üzenet érkezett.

**A visszacsatolási cím (loopback) tesztelése**

A **ping** parancs egy állomás belső IP-konfigurációjának ellenőrzésére is alkalmas. Emlékezzünk vissza, hogy ennek végrehajtásához a **ping** parancs mögé egy fenntartott, loopback címet írtunk (127.0.0.1). Ez a parancs leellenőrzi a protokollkészlet működését a hálózati rétegtől a fizikai rétegig és vissza, de nem küld jeleket a kommunikációs közegbe.

**Ping** utasításokat a parancssorban hajthatunk végre.

Gépeljük be a **ping loopback** parancsot a következő szintaxissal:

C:\> **ping 127.0.0.1**

A kapott válasz az alábbiakhoz hasonlóan fog kinézni:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Az eredmény azt jelzi, hogy négy 32 bájtos teszt csomag került kiküldésre és a válaszok kevesebb, mint 1 ms alatt megérkeztek a 127.0.0.1 állomástól. A TTL (Time-To-Live, élettartam) érték azt határozza meg, hogy a ping csomag hány ugrás után kerül eldobásra.

# Hálózati teljesítmény

## Ping

A Cisco IOS ping parancsa rendelkezik egy "kiterjesztett" móddal is, mely az utasítás IP-cím nélküli beírásával érhető el. Ekkor az alább példában látható paraméter-bekérő üzenetek jelennek meg. Az Enter billentyű leütésének hatására a []-ben lévő alapértelmezett értékek kerülnek elfogadásra. A példa azt mutatja be, hogyan kényszeríthető a ping parancs a 10.1.1.1 forráscím használatára (lásd az ábrán R2-t); bár normál ping esetén a forráscím 209.165.200.226 lenne. Ezáltal a hálózati rendszergazda távolról (R2-ről) is ellenőrizni tudja, hogy az R1 irányítótáblájában van-e bejegyzés a 10.1.1.0/24 hálózat felé.

R2# **ping**

Protocol [ip]:

Target IP address: **192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **10.1.1.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

Hosszabb időtúllépési (Timeout) periódus megadása lehetőséget ad a késleltetési hibák felderítésére. Ha a nagyobb értékkel sikeres a ping, akkor a kapcsolat él az állomással, de valamilyen késleltetési probléma van a hálózatban.

Figyeljük meg, hogy az "Extended commands" (Kiterjesztett utasítások) paraméternél beírt "y" további hasznos hibaelhárítási lehetőségeket nyit meg.

# Hálózati teljesítmény

## Ping

Az egyik leghatékonyabb eszköz a teljesítmény figyelésére és a hibaelhárításra a hálózat alapállapotának, más néven viszonyítási alapjának meghatározása. Az alapállapot meghatározásához a hálózat normál működés közbeni rendszeres vizsgálata szükséges. Ez több, mint egy szimpla beszámoló a hálózat adott időpontra vonatkozó állapotáról, mivel elkészítéséhez a teljesítmény hosszabb ideig történő megfigyelése szükséges. A különböző időpontokban történő mérések (lásd 1. és 2. ábra) segítenek teljesebb képet alkotni a hálózat összteljesítményéről.

A hálózat viszonyítási alapjához különféle parancsok kimenetei szolgáltatják az adatokat.

Az állapotfelmérés kezdőlépése lehet a ping, a trace és egyéb fontos parancsok eredményeinek elmentése egy időbélyeggel ellátott szövegállományba a későbbi visszakereshetőség céljából.

A tárolt információk tényleges használatára az aktuális eredményekkel való összehasonlításkor kerül sor (lásd 3. ábra). Figyelni kell a hibaüzeneteket és az állomások közötti válaszidőket, melyek növekedése késleltetési problémát jelenthet a címzett felé.

A dokumentáció elkészítésének fontosságát nem lehet elégszer hangsúlyozni. A végponttól végpontig tartó kapcsolatok ellenőrzésének adatai, a késleltetési hibák leírása, és az azonosított problémák megoldásai segíthetik a rendszergazdát a hálózat hatékony működtetésében.

A vállalati hálózatok fenntartásához széleskörű állapotfelmérés szükséges, sokkal bővebb, mint a jelen kurzusban leírtak. A viszonyítási információk kezelésére és tárolásához különféle professzionális alkalmazások állnak rendelkezésre. A kurzus keretében azonban csak az alapvető eljárásokat érintjük és a célokat tárgyaljuk meg.

A viszonyítási alap elkészítésének bevált gyakorlatait megtaláljuk [itt](http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014fb3b.shtml).

A **ping** utasítás kimenetének rögzítése megvalósítható a 4. ábrán bemutatott módon, az IOS parancssorából is.

# Hálózati teljesítmény

## Tracert

A nyomkövetés (trace) eredménye azon ugrások listája, melyek a csomagtovábbítás során a hálózati útvonalon történnek. A parancs formája az alkalmazott rendszertől függ. Windows számítógép esetében a **tracert**, míg egy forgalomirányító CLI esetén a **traceroute** parancs használható (lásd 1. ábra).

Hasonlóan a **ping** parancsokhoz, a **trace** utasítások is parancssorból használhatók és egy IP-címet használnak paraméterként.

Windows számítógépen használjuk a **tracert** parancsot az alábbiak szerint:

C:\> **tracert 10.1.0.2**

Tracing route to 10.1.0.2 over a maximum of 30 hops

1 2 ms 2 ms 2 ms 10.0.0.254

2 \* \* \* Request timed out.

3 \* \* \* Request timed out.

4 ^C

Sikeres válasz csak a Router A helyi hálózat felőli kijáratától érkezett, míg a következő ugrás követése időtúllépéssel zárult. Ez azt jelenti, hogy a következő ugrásnál lévő forgalomirányító nem válaszolt. A nyomkövetés eredménye azt mutatja, hogy a hiba valahol a LAN-on kívül, a külső hálózatban van.

A 2. ábrán a forgalomirányítón kiadott traceroute parancs eredményének rögzítése látható.

# Hálózati teljesítmény

## Show parancsok

A Cisco IOS parancssori felülete a **show** parancsokat használja az eszközök konfigurációjával és működésével kapcsolatos információk megjelenítésére.

A hálózati szakemberek gyakran használják a **show** parancsokat a konfigurációs fájlok megtekintéséhez, az eszközök interfészeinek és folyamatainak állapotellenőrzéséhez és a berendezés működőképességének vizsgálatához. A **show** parancsok az eszköz parancssorában vagy a Cisco Configuration Professional (CCP) segédprogramból érhetők el.

Szinte minden forgalomirányító folyamat és funkció állapotának megjelenítésére létezik **show** parancs. A leggyakrabban használt show parancsok közül néhány:

* **show running-config** (1. ábra)
* **show interfaces** (2. ábra)
* **show arp** (3. ábra)
* **show ip route** (4. ábra)
* **show protocols** (5. ábra)
* **show version** (6. ábra)

Az ábrán lévő gombokra kattintva részletes leírásukkal együtt jelennek meg a **show** parancsok.

# Hálózati teljesítmény

## Show parancsok

Az indító konfigurációs fájl betöltése és a forgalomirányító sikeres elindulása után a **show version** parancs használható az indításnál szerepet játszó hardver- és szoftverkomponensek ellenőrzésére és az esetleges hibák megkeresésére. A **show version** parancs kimenete a következőket tartalmazza:

* A használatban lévő Cisco IOS szoftver verziója.
* A ROM-ban tárolt, a forgalomirányító indításához használt rendszerbetöltő program verziója.
* A Cisco IOS szoftver teljes fájlneve, valamint a háttértár neve, ahol a rendszerindító program azt megtalálta.
* A forgalomirányítóban lévő CPU típusa és RAM mennyisége. A Cisco IOS szoftver frissítésekor szükség lehet a RAM mennyiségének bővítésére.
* A forgalomirányító fizikai interfészeinek száma és típusa.
* Az NVRAM mennyisége. Az NVRAM tárolja az indító konfigurációs fájlt (startup-config).
* A forgalomirányító flash memóriájának mérete. A Cisco IOS szoftver frissítésekor szükség lehet a flash memória bővítésére.
* A konfigurációs regiszter aktuális értéke hexadecimálisan.

Az ábrán lévő lejátszás gombra kattintva egy animációt láthatunk, amely bemutatja a felsorolt elemeket a show parancs kimenetében.

A konfigurációs regiszter határozza meg a forgalomirányító számára az indítási folyamat módját . Például, a konfigurációs regiszter gyári alapértelmezett értéke 0x2102. Ez azt jelenti, hogy a forgalomirányító a Cisco IOS szoftvert a flash-ből, az indító konfigurációs fájlt pedig az NVRAM-ból próbálja betölteni. A konfigurációs regiszter értéke megváltoztatható, ezáltal az indítási folyamat során a forgalomirányító máshol fogja keresni a Cisco IOS kódot, valamint az indító konfigurációs fájlt. Amennyiben egy második érték jelenik meg zárójelben, az a forgalomirányító következő újraindításakor érvénybe lépő konfigurációs regiszter értékét mutatja.

A konfigurációs regiszterről további információt a jobb alsó sarokban lévő "Jegyzet" ikonra kattintva találunk.

# Hálózati teljesítmény

## Show parancsok

A **show version** parancs információkat jelenít meg a kapcsolón aktuálisan betöltött szoftver verziójáról, valamint az eszköz hardver összetevőiről. Néhány ezek közül:

* **Cisco IOS Software** - Az IOS-szoftver verziója
* **ROM: Boot Loader** - A rendszerbetöltő program verziója
* **Switch uptime** - Az utolsó újraindulás óta eltelt idő
* **System returned to ROM** - Az újraindulás módja (pl.: áramkimaradás, rendszerösszeomlás)
* **System image file** - Az IOS-képfájl neve
* **Cisco "switch type" processor** - A készülék modell száma és a beépített processzor típusa
* **"main/shared" bytes of memory** - Alap processzor RAM és osztott I/O puffer memória mennyisége
* **Interfaces** - A kapcsolóban rendelkezésre álló interfészek
* **Configuration register** - Rendszertöltési beállítások, konzol sebesség, és ezek paraméterei

Az ábrán egy kapcsolón kiadott **show version** parancs kimenete látható.

# Hálózati teljesítmény

## Számítógép és IOS parancsok

Egy állomáson az alapértelmezett átjáró IP-címének lekérdezésére egy Windows-t futtató számítógép parancssorában az **ipconfig** utasítás használható. (lásd 1. ábra)

A MAC-cím megjelenítéséhez gépeljük be: **ipconfig /all**. Figyeljük meg a 2. ábrán, hogy a MAC-címen kívül kijelzésre került a számítógép néhány további 3. rétegbeli címinformációja is. Próbáljuk ki ezt a parancsot.

Ezen felül a MAC-cím alkalmas a számítógépben lévő hálózati kártya gyártójának azonosítására is. Erre a cím első 24 bitje (OUI) ad módot, mely visszakereshető az interneten.

A Windows PC DNS-kliens szolgáltatása a memóriában tárolja a korábban már meghatározott neveket és ezáltal javítja a névfeloldás teljesítményét. Az **ipconfig /displaydns** parancs megmutatja a rendszer DNS-gyorsítótárának bejegyzéseit.

# Hálózati teljesítmény

## Számítógép és IOS parancsok

Az **arp** parancs segítségével létrehozhatók, módosíthatók és megjeleníthetők a fizikai cím - IP-cím összerendelések. Az **arp** utasítás a Windows parancssorában futtatható.

Az **arp** végrehajtásához az állomás parancssorába gépeljük be:

C:\host1> **arp -a**

Amint az ábrán is látható, az **arp -a** parancs felsorolja az összes ARP-gyorsítótárban lévő eszközt, beleértve azok IPv4-címét, fizikai címét és a cím típusát (statikus/dinamikus).

A gyorsítótár az **arp -d** paranccsal törölhető, ha a hálózati rendszergazda szeretné friss információkkal újratölteni azt.

**Megjegyzés:** Az ARP-gyorsítótár csak azoknak az eszközöknek az információit tartalmazza, melyekhez mostanában történt hozzáférés. A cache feltöltéséhez pingeljük meg a kívánt eszközt, így biztosan lesz bejegyzés hozzá az ARP táblában.

# Hálózati teljesítmény

## Számítógép és IOS parancsok

Figyeljük meg a **show cdp neighbors** parancs kimenetét a 1. ábrán és vessük össze a 2. ábrán látható topológiával. Figyeljük meg, hogy az R3 milyen részletes információkat gyűjtött be az R2-ről és a FastEthernet interfészére csatlakoztatott kapcsolóról.

A CDP a Cisco saját protokollja, mely az adatkapcsolati rétegben működik. Ebből kifolyólag az egymással összekötött Cisco eszközök, például a különböző hálózati protokollt használó forgalomirányítók, képesek felismerni szomszédaikat még akkor is, ha 3. rétegbeli kapcsolat nincs is közöttük.

Egy Cisco eszköz elindulása után a CDP automatikusan betöltődik és felderíti a CDP-t futtató szomszédos Cisco berendezéseket, függetlenül attól, hogy milyen 3. rétegbeli protokoll vagy programcsomag fut rajtuk. A CDP hardverre és szoftverre vonatkozó adatokat cseré a közvetlenül csatlakozó szomszédok között.

A CDP által szolgáltatott információk:

* **Device ID** - Eszköz azonosítók, például a kapcsolón beállított állomásnév
* **Entry address(es)** - Hálózati rétegbeli cím, minden támogatott protokollhoz legfeljebb egy.
* **Local interface, Port ID** - A helyi és a távoli portok nevei ASCII formátumban, például Serial0/0/1
* **Capability** - Szolgáltatás lista, például, hogy a kapcsolódó eszköz forgalomirányító (R) vagy kapcsoló (S)
* **Platform** - Az eszköz hardver típusa, például Cisco 1841 sorozatú forgalomirányító

A **show cdp neighbors detail** parancs megmutatja a szomszéd eszköz IP-címét, még akkor is, ha pingelni sem tudjuk. Ez nagyon hasznos parancs, amikor két Cisco forgalomirányító nem talál egymásra a közös adatkapcsolaton. A **show cdp neighbors detail** parancs segítségével megállapítható a szomszédok IP-konfigurációs hibái.

Hálózatfelderítés esetén a CDP-szomszéd IP-címének ismerete elégséges információ az eszközbe való Telnet bejelentkezéshez.

Érthető okokból a CDP biztonsági kockázatot jelenthet. Mivel néhány IOS verzió alapértelmezett beállítása a CDP-hirdetések küldése, így fontos tudni a CDP kikapcsolásának módjait.

A CDP egész eszközre kiterjedő tiltásához használható globális konfigurációs parancs a **no cdp run**. A CDP egy adott interfészen történő tiltására a **no cdp enable** parancs szolgál.

# Hálózati teljesítmény

## Számítógép és IOS parancsok

Hasonlóan az állomások konfigurációjának vizsgálatához, a közvetítő eszközök interfészeinek ellenőrzéséhez is rendelkezésre állnak utasítások és segédprogramok. A Cisco IOS-ben számos parancs szolgál a forgalomirányító és a kapcsoló interfészeinek ellenőrzésére.

**A forgalomirányító interfészeinek ellenőrzése**

Az egyik leggyakrabban használt parancs a **show ip interface brief** . Ez az utasítás sokkal tömörebb kimenetet ad, mint a **show ip interface** parancs. Összegezve mutatja a forgalomirányító hálózati interfészeinek kulcsfontosságú információit.

Az 1. ábrán a példában használt hálózati topológia látható.

Kattintsunk a 2. ábrán lévő R1 gombra! A **show ip interface brief** kimenete felsorolja a forgalomirányító interfészeit, a hozzájuk rendelt IP-címet és a működési állapotukat.

Ennek alapján a FastEthernet 0/0 interfész IP-címe 192.168.254.254. Az utolsó két oszlop az interfész 1. és 2. rétegbeli állapotát mutatja. Az **up** a Status oszlopban azt jelzi, hogy az interfész 1. rétegbeli működése rendben van. Az **up** a Protocol oszlopban pedig azt mutatja, hogy a 2. rétegbeli protokoll is működik.

Ezenkívül figyeljük meg, hogy a Serial 0/0/1 interfész nincs engedélyezve. Ezt jelzi az **administratively down** bejegyzés a Status oszlopban.

A végberendezésekhez hasonlóan, a 3. rétegbeli kapcsolatok ellenőrzéséhez itt is használhatók a **ping** és **traceroute** parancsok. A példában mind a **ping** , mind a **trace** parancsok sikeres kapcsolódást mutatnak.

**A kapcsoló interfészeinek ellenőrzése**

Kattintsunk a 2. ábrán lévő S1 gombra! A **show ip interface brief** parancs a kapcsoló interfészeinek állapotáról ad jelentést. Kapcsoló esetében az IP-cím egy VLAN-interfészhez van hozzárendelve. Jelen esetben a VLAN1 címe 192.168.254.250, az interfész engedélyezett és működőképes.

A kimenetből az is látszik, hogy a FastEthernet0/1 interfész nem működik. Ez azt jelenti, hogy nincs hozzá eszköz csatlakoztatva, vagy a kapcsolódó eszköz hálózati interfésze nem működőképes.

Ezzel ellentétben a kimenet alapján a FastEthernet0/2 és a FastEthernet0/3 interfészek működőképesek, mivel mind a Status, mind a Protocol állapota **up**.

A kapcsolón is használhatók a 3. rétegbeli csatlakozás tesztelésére a **show ip interface brief** és a **traceroute** parancsok. Az ábrán látható példában mind a **ping** , mind a **traceroute** parancsok sikeres kapcsolódást mutatnak.

Nagyon fontos, hogy megjegyezzük: a kapcsolónak nincs szüksége IP-címre a 2. rétegbeli keretek továbbításához. Az IP-cím csupán a kapcsoló hálózaton keresztül történő kezeléséhez szükséges, ami történhet Telnet vagy SSH használatával. Ha a hálózati rendszergazda a helyi hálózaton kívülről szeretne a kapcsolóhoz csatlakozni, alapértelmezett átjárót is konfigurálnia kell.

# IOS konfigurációs fájlok kezelése

## Forgalomirányító és kapcsoló fájlrendszerek

Egy kis hálózat létrehozásán és a biztonság megvalósításán kívül a hálózati rendszergazda feladata a konfigurációs állományok kezelése is. Ennek fontos eleme a biztonsági mentés és eszközhiba esetén a helyreállítás.

A Cisco IOS File System (IFS) egyszerű hozzáférést biztosít a forgalomirányító összes fájlrendszeréhez, melyek a következők:

* Flash memória fájlrendszerek
* Hálózati fájlrendszerek (TFTP és FTP)
* További olvasható és írható adattárolók, például NVRAM, aktív konfiguráció, ROM stb.

A Cisco IFS segítségével minden fájl megtekinthető és rendezhető (képfájl, szöveges fájl stb.), beleértve a távoli szervereken lévő állományokat is. Például, ellenőrzés céljából lehetőség van a távoli szerveren tárolt konfigurációs fájl megtekintésére annak forgalomirányítóba való betöltése előtt.

A Cisco IFS-ben a rendszergazda szabadon mozoghat a különféle könyvtárak között, kilistázhatja a tartalmukat, valamint létrehozhat alkönyvtárakat a flash memóriában vagy a lemezen. A felhasználható könyvtárak száma eszközfüggő.

Az 1. ábrán a **show file systems** parancs látható, mely éppen kilistázza a Cisco 1941-es forgalomirányító elérhető fájlrendszereit. Az utasítás hasznos információkat nyújt például a teljes és a még felhasználható tárolóterület nagyságáról, a fájlrendszer típusáról és jogosultságairól. Az engedélyek a lista Flags oszlopában jelennek meg, jelentésük a következő: csak olvasható (read only, ro), csak írható (write only, wo), és írható-olvasható (read and write, rw).

Bár nagyon sokféle fájlrendszer létezik, bennünket a tftp, a flash és az nvram érdekel.

Figyeljük meg, hogy a flash fájlrendszer meg van jelölve egy csillaggal (\*), mely azt jelzi, hogy ez az aktuális alapértelmezett fájlrendszer. Mivel a flash tartalmaz egy betölthető IOS-t, így kettőskereszt (#) kerül a sor végére, jelezve ezzel az indítólemezt.

**A flash fájlrendszer**

A 2. ábrán az alapértelmezett fájlrendszer tartalma látható, mely jelen esetben a flash, amint azt az előző ábrán lévő \* is mutatta. Számos fájl található a flash-en, de külön figyelmet érdemel az utolsó, mivel ez az aktuálisan a RAM-ba betöltött Cisco IOS képfájl.

**Az NVRAM fájlrendszer**

Az NVRAM tartalmának megtekintéséhez meg kell változtatnunk az aktuális alapértelmezett fájlrendszert a **cd** (change directory, könyvtár váltás) parancs használatával, amint a 3. ábrán látható. A **pwd** (present working directory, jelenlegi munkakönyvtár) parancs ellenőrzi, hogy valóban az NVRAM-ot látjuk. Végül a **dir** (directory, könyvtár) parancs kilistázza az NVRAM tartalmát. Bár több konfigurációs állomány is látható, külön figyelmet a startup-config (indító konfigurációs) fájl érdemel.

# IOS konfigurációs fájlok kezelése

## Forgalomirányító és kapcsoló fájlrendszerek

A Cisco 2960-as kapcsoló flash fájlrendszerének segítségével másolhatók a konfigurációs állományok, valamint le- és feltölthetjük a szoftver képfájlokat.

A Catalyst kapcsoló fájlrendszerének megtekintésére a Cisco forgalomirányítókhoz hasonlóan a **show file systems** parancs használható (lásd ábra).

A Cisco kapcsolók és forgalomirányítók több alap UNIX parancsot is támogatnak, például: **cd** - fájlrendszer vagy könyvtár váltás, **dir** - könyvtár tartalmának megjelenítése, és **pwd** - aktuális munkakönyvtár megmutatása.

# IOS konfigurációs fájlok kezelése

## Konfigurációs fájlok mentése és visszaállítása

**Konfiguráció mentése szöveg rögzítéssel (Tera Term)**

A konfigurációs fájlok szövegfájlba menthetők (archiválhatók) Tera Term használatával.

Az ábrán is látható lépések a következők:

**1**. A File menüben kattintsunk a **Log** menüpontra.

**2**. Válasszunk elérési utat a mentéshez. A Tera Term megkezdi a szöveg rögzítését.

**3**. Ezután futtassuk a **show running-config** vagy a **show startup-config** parancsot privilegizált EXEC módban. A terminálablakban megjelenő szöveg a választott fájlba íródik.

**4**. A rögzítés befejezéséhez válasszuk a **Close** nyomógombot a Tera Term Log ablakában.

**5**. Nyissuk meg a fájlt és ellenőrizzük a sértetlenségét.

**Szöveges konfiguráció visszatöltése**

A konfigurációt átmásolhatjuk a fájlból az eszközre. Ha kimásolunk valamit egy szöveges állományból és beillesztjük a terminálablakba, akkor az IOS parancsként értelmezi a sorokat és végrehajtja azokat. Ezért a fájlt előzőleg meg kell szerkeszteni, azaz a titkosított jelszavakat egyszerű szöveggé kell alakítani és törölni kell a parancsként nem értelmezhető szövegeket, például a "-More-" és hozzá hasonló IOS-üzeneteket. A folyamatot a laborgyakorlatban tárgyaljuk részletesen.

Fontos még, hogy az eszköz parancssorában a globális konfigurációs módot kell kiválasztani a szövegfájl beillesztése előtt.

Tera Term esetén a lépések a következők:

**1**. A File menüben kattintsunk a **Send** file menüpontra.

**2**. Válasszuk ki az eszközre másolandó fájlt és kattintsunk az **Open** gombra.

**3**. A Tera Term beilleszti az állományt az eszközre.

A fájlban lévő szöveget a CLI parancsként értelmezi és bemásolja az eszköz aktív konfigurációjába. Ez egy kényelmes módja a forgalomirányító kézzel történő konfigurálásának.

# IOS konfigurációs fájlok kezelése

## Konfigurációs fájlok mentése és visszaállítása

**Konfiguráció mentése TFTP használatával**

A konfigurációs állományokról biztonsági másolatot kell lementeni, felkészülve ezzel a váratlan eseményekre. A konfigurációs fájlok, melyek a hálózati dokumentáció részét is képezik, tárolhatók TFTP-szerveren (Trivial File Transfer Protocol) vagy USB-meghajtón.

Az aktív vagy az indító konfiguráció TFTP-szerverre mentéséhez a **copy running-config tftp** vagy a **copy startup-config tftp** parancs használható. (lásd ábra) Az aktív konfiguráció TFTP-szerverre mentéséhez kövessük az alábbi lépéseket:

**1**. Gépeljük be a **copy running-config tftp** parancsot.

**2**. Írjuk be a konfigurációs fájlt tárolását végző állomás (TFTP-szerver) IP-címét.

**3**. Adjuk meg a konfigurációs fájl nevét.

**4**. Nyomjuk le az Enter billentyűt választásunk megerősítéséhez.

**Konfiguráció visszaállítása TFTP használatával**

Az aktív vagy az indító konfiguráció TFTP-szerverről történő visszaállítására a **copy tftp running-config** vagy a **copy tftp startup-config** parancs használható. Az aktív konfiguráció TFTP-szerverről történő visszaállításához kövessük az alábbi lépéseket:

**1**. Gépeljük be a **copy tftp running-config** parancsot.

**2**. Írjuk be a konfigurációs állomány tárolására szolgáló állomás IP-címét.

**3**. Adjuk meg a konfigurációs fájl nevét.

**4**. Nyomjuk le az Enter billentyűt választásunk megerősítéséhez.

# IOS konfigurációs fájlok kezelése

## Konfigurációs fájlok mentése és visszaállítása

Egyes Cisco forgalomirányítók támogatják az USB (Universal Serial Bus) tárolási szolgáltatást, mely lehetővé teszi az USB flash meghajtók használatát. Ezek másodlagos tárolóként és alternatív indítólemezként is szolgálhatnak. A képfájlok, konfigurációs állományok és egyéb fájlok ugyanolyan megbízhatóan használhatók és tárolhatók USB flash memórián, mint Compact Flash (CF) kártyán. Továbbá a moduláris ISR (Integrated Services Router) eszközök képesek indításkor egy USB flash memórián lévő IOS-képfájlt betölteni.

A Cisco USB flash modulok 64MB, 128MB és 256MB változatokban kaphatók.

A Cisco fogalomirányítón való használathoz az USB-meghajtót FAT16-szabvány szerint kell formázni. Amennyiben ez nem teljesül, a show file systems parancs "ismeretlen fájlrendszer" hibaüzenetet ad.

A következő példa a dir parancs használatát mutatja be USB-fájlrendszeren:

**Router# dir usbflash0:**

**Directory of usbflash0:/**

**1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T**

**63158272 bytes total (33033216 bytes free)**

Az USB flash memórián egyszerre több Cisco IOS-fájl és konfigurációs állomány is tárolható. Így a rendszergazda egyszerűen át tudja másolni ezeket fájlokat az egyik forgalomirányítóról a másikra, sok esetben jelentősen rövidebb idő alatt, mint LAN-on vagy WAN-on keresztül. Figyeljünk arra, hogy az IOS nem minden esetben ismeri fel helyesen az USB flash méretét, de ez nem feltétlenül jelenti annak használhatatlanságát. Végül jegyezzük meg, hogy a forgalomirányítón általában USB 2.0 szabványú portok találhatók.

# IOS konfigurációs fájlok kezelése

## Konfigurációs fájlok mentése és visszaállítása

**Konfiguráció mentése USB flash meghajtóra**

USB-re való mentés előtt a meghajtó nevének ellenőrzése érdekében célszerű kiadni a **show file systems** parancsot. (lásd 1. ábra)

Ezt követően a **copy run usbflash0:/** utasítás használatával másoljuk át a fájlt az USB flash lemezre. Ügyeljünk a rá, hogy a fájlrendszerben lévő nevet használjuk. A per jel (/) nem kötelező, de jelzi, hogy a meghajtó gyökérkönyvtáráról van szó.

Ezután az IOS bekéri a fájlnevet. Ha a fájl már létezik az USB meghajtón, a forgalomirányító a 2. ábrán látható módon figyelmeztet a felülírás veszélyére.

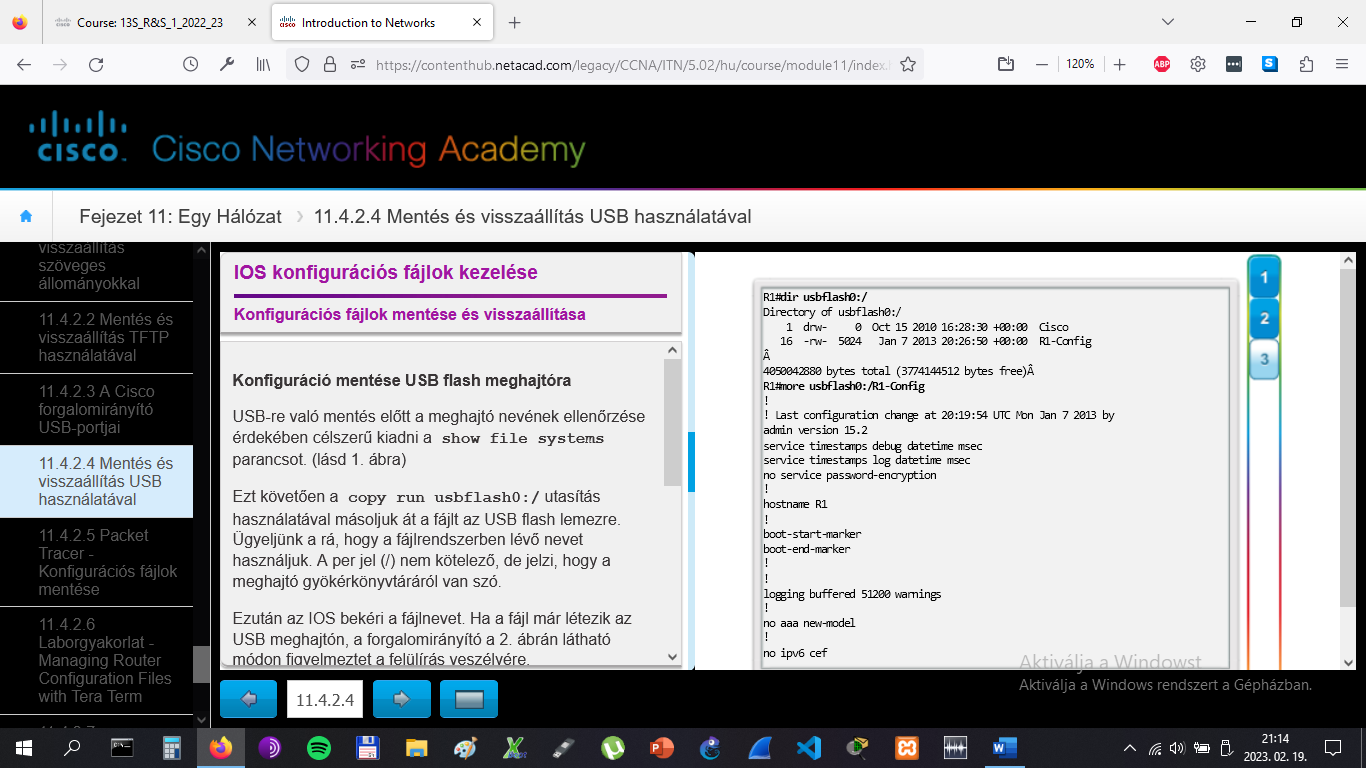
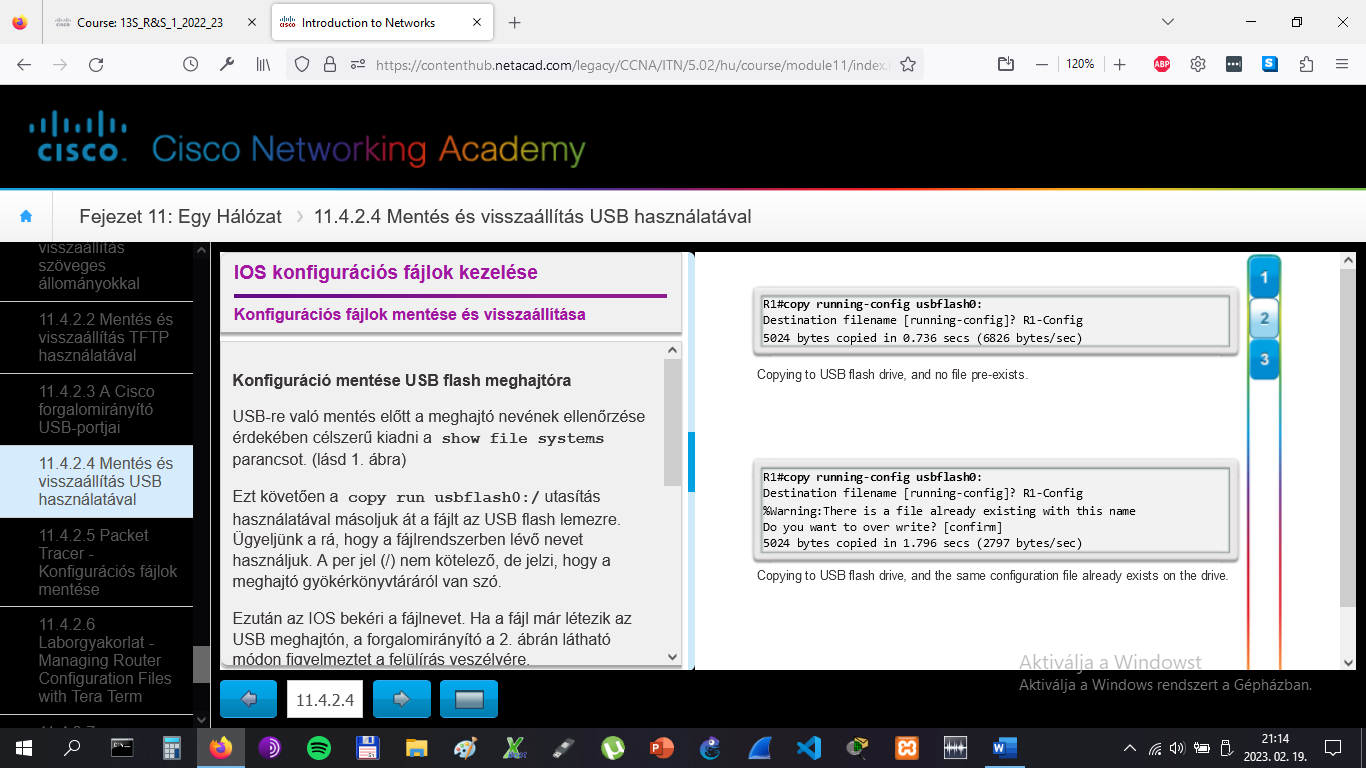
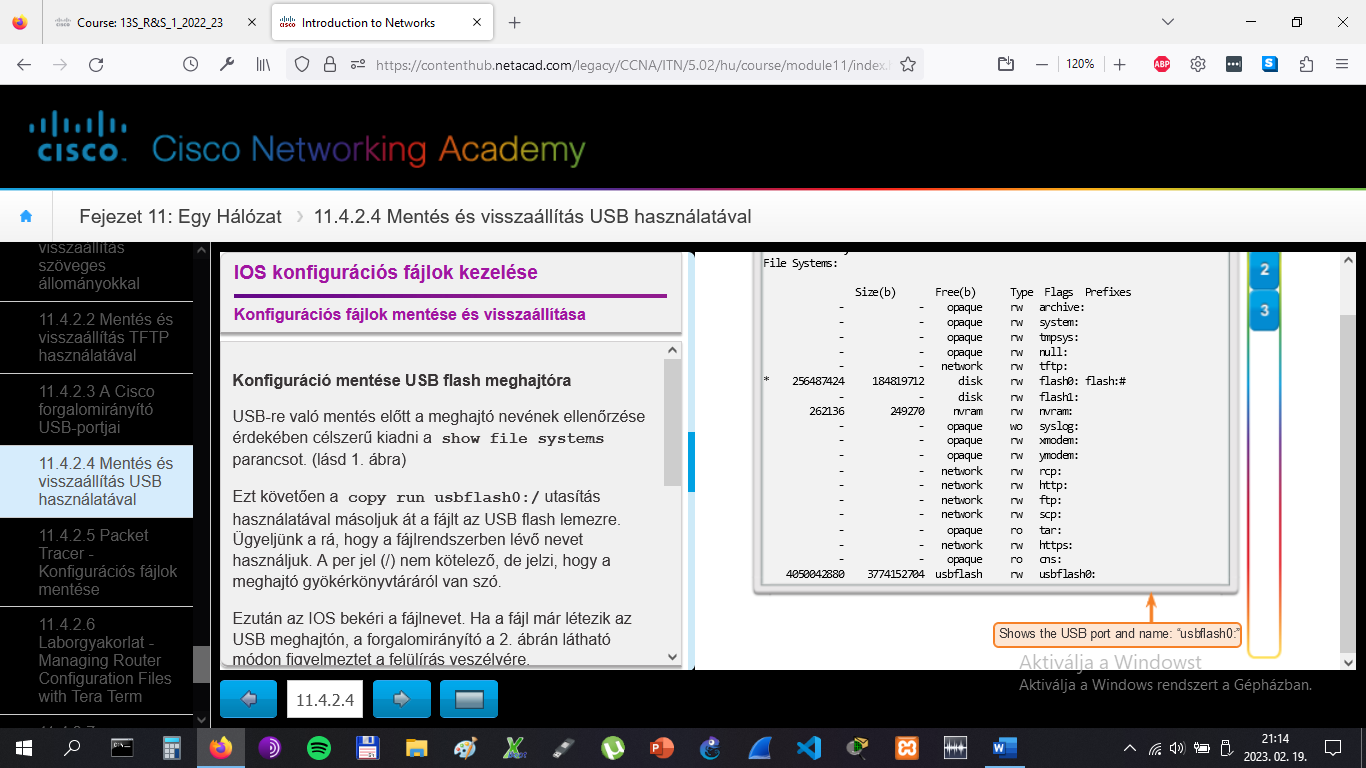
Használjuk a **dir** parancsot az USB-meghajtón lévő fájlok megtekintéséhez, és a **more** parancsot az állomány tartalmának megjelenítésére (lásd 3. ábra).

**Konfiguráció visszaállítása USB-meghajtóról**

A fájlt visszamásolás előtt feltétlenül nyissuk meg egy szövegszerkesztővel, és győződjünk meg annak helyességéről; ellenkező esetben érvénytelen parancsokat és nemlétező interfészeket tartalmazó bejegyzések kerülhetnek a konfigurációba.

R1# **copy usbflash0:/R1-Config running-config**

Destination filename [running-config]?



# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító

Hálózatokat nem csak a kisvállalkozások és a nagy szervezetek használnak.

Otthoni környezetben is egyre jobban terjed a hálózati technológiák alkalmazása. Az otthoni hálózatok a lakásban található különféle számítógépeket és laptopokat kötik össze, valamint internet kapcsolatot biztosítanak számukra. Ezenkívül számos szolgáltatást nyújtanak a felhasználóknak, úgymint hálózati nyomtatás, képek, zenék és filmek központi tárolása NAS berendezésen (Network Attached Storage, hálózatba kötött tároló), valamint internetelérést biztosítanak számos végfelhasználói készüléknek, melyek lehetnek táblaszámítógépek, mobiltelefonok vagy háztartási eszközök, mint például egy televízió.

Egy otthoni hálózat nagyon hasonlít egy kisvállalati hálózathoz, mivel legtöbbször egyik sem igényel felső kategóriás eszközöket, például dedikált forgalomirányítókat és kapcsolókat. Számukra megfelelnek olyan kisebb eszközök, melyek rendelkeznek útválasztási és kapcsolási funkcióval. Ez az oka annak, hogy sok otthoni és kisvállalati hálózatban többfunkciós, más néven multifunkciós eszközt használnak.

A kurzus folyamán ezekre a multifunkciós eszközökre mint integrált forgalomirányítókra hivatkozunk.

Az integrált forgalomirányító olyan, mintha számos különböző eszközt csatlakoztatnánk és építenénk egybe. Például a kapcsoló és a forgalomirányító közötti összeköttetés a berendezésen belül valósul meg. Amikor egy csomag a helyi hálózat egy végpontjától egy másik felé kerül kiküldésre, akkor a beépített kapcsoló továbbítja azt a céleszköznek. Ha a csomag egy távoli hálózat felé irányul, akkor is a beépített kapcsoló továbbítja azt, de ilyenkor a szintén beépített forgalomirányítónak. A forgalomirányító meghatározza a legjobb útvonalat és aszerint küldi tovább a csomagot.

A legtöbb integrált forgalomirányító vezetékes és vezeték nélküli kapcsolódási lehetőséget is biztosít, azaz elérési pontként (Access Point, AP) viselkedik, amint az 1. ábrán látható. A vezeték nélküli kapcsolódás közkedvelt, rugalmas és költséghatékony módszer végberendezések hálózati kiszolgálására otthoni és kisvállalati környezetben.

A 2. és 3. ábra a vezeték nélküli kapcsolat használatának szempontjait és előnyeit mutatja be.

Az integrált forgalomirányító az útválasztáson, kapcsoláson és vezeték nélküli csatlakozáson kívül még számos, például DHCP-szerver, tűzfal és NAS szolgáltatást is nyújthat.

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító

Az integrált forgalomirányítók kínálata az otthoni és kisvállalati felhasználásra tervezett eszközöktől egészen a nagy szervezetek igényeit is kielégítő berendezésekig terjed.

Egy tipikus példa integrált forgalomirányítóra az ábrán is látható Linksys vezeték nélküli forgalomirányító. Maga a készülék egyszerű kivitelű és általában egyetlen összetevőből áll, ami csökkenti a bekerülési költségét. Ebből következően hiba esetén nincs lehetőség a tönkrement alkatrész cseréjére. Mindezek miatt elsődleges meghibásodási pontnak tekinthető, ráadásul egyetlen beépített funkciója sincs optimalizálva.

Egy másik példa integrált forgalomirányítóra a Cisco ISR (Integrated Services Router, integrált szolgáltatású forgalomirányító). A Cisco ISR termékcsalád széles választékot kínál, ideértve az otthoni és kis irodai környezetbe tervezett eszközöket és a nagyobb hálózatokba valókat is. Számos ISR moduláris, azaz minden funkcióját különálló elemek valósítják meg, mint például egy kapcsoló és egy forgalomirányító modul. Ez szükség esetén lehetővé teszi egyedi összetevők hozzáadását, cseréjét és fejlesztését.

Minden integrált forgalomirányító azonos alapbeállításokra ad lehetőséget, mint például a jelszavak, IP-címek és DHCP-beállítások konfigurálása, melyek egyaránt vonatkoznak a vezetékkel és a vezeték nélkül csatlakozó állomásokra. A vezeték nélküli kapcsolódáshoz további paraméterek beállítása is szükséges, úgymint vezeték nélküli mód, SSID és vezeték nélküli csatorna.

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító

**Vezeték nélküli mód**

A vezeték nélküli mód a hálózat által használt IEEE 802.11 szabvány szerinti beállítást jelenti. Az IEEE 802.11 szabványhoz több kiegészítés is tartozik, melyek leírják a különféle vezeték nélküli kommunikációk jellemzőit. Ezek a 802.11a, 802.11b, 802.11g és a 802.11n szabványok. (továbbá a 802.11ac,ad,af,ah stb., a fordító megjegyzése). Az ábrára kattintva láthatjuk a különféle beállítási lehetőségeket.

A legtöbb integrált forgalomirányító támogatja a 802.11b,g,n szabványokat. Ezek kompatibilisek egymással, de a hálózat minden eszközének egyazon szabvány szerint kell működni. Például: Ha egy 802.11n forgalomirányító egy 802.11n laptophoz kapcsolódik, akkor a hálózat 802.11n szabvány szerint fog működni. Ha viszont hozzáadunk egy 802.11b nyomtatót a hálózathoz, akkor a forgalomirányító és a laptop is visszaáll a lassabb 802.11b szabvány használatára. Tehát a régi eszközök az egész hálózat működését lelassítják. Ezt fontos észben tartani, amikor egy régebbi eszköz megtartásáról vagy cseréjéről döntünk.

**SSID**

Mivel sok vezeték nélküli hálózat lehet a környezetünkben, ezért fontos, hogy a vezeték nélküli eszközök a megfelelő WLAN-hoz csatlakozzanak. Erre való az SSID (Service Set Identifier, szolgáltatás készlet azonosító).

Az SSID a vezeték nélküli hálózat neve, mely legfeljebb 32 alfanumerikus karakterekből állhat és nagybetű-kisbetű érzékeny. Az SSID-t arra használjuk, hogy a vezeték nélküli eszközöknek megmondjuk, melyik WLAN-hoz tartoznak és mely más eszközökkel kommunikálhatnak. Tekintet nélkül arra, hogy milyen típusú WLAN-ról van szó, a kommunikáció érdekében egy hálózat minden vezeték nélküli eszközét ugyanarra az SSID-re kell beállítani.

**Vezeték nélküli csatorna**

A csatornák a rendelkezésre álló rádiófrekvenciás (RF) tartomány részekre bontásával jönnek létre. Minden egyes csatorna egy különböző párbeszéd lebonyolítására alkalmas. Ez hasonló ahhoz, amikor több televíziós csatornát szolgáltatnak egyetlen átviteli közegen keresztül. Így több hozzáférési pont is képes egymáshoz közel üzemelni, feltéve hogy eltérő csatornákat használnak a kommunikációra.

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító

Biztonsági óvintézkedések megtervezése és beállítása is szükséges, mielőtt egy AP-t a hálózathoz vagy az internethez csatlakoztatnánk.

Néhány alapvető biztonsági rendszabály ezek közül, melyek az 1. ábrán is láthatók:

* Változtassuk meg az SSID, a felhasználó nevek és a jelszavak alapértelmezett értékeit
* Tiltsuk le az SSID-szórást
* Állítsunk be WEP vagy WPA titkosítást

A titkosítási folyamat az adatok olyan átalakítását jelenti, melynek eredményeként az elfogott információk használhatatlanok lesznek.

**WEP**

A WEP (Wired Equivalency Protocol, vezetékessel egyenértékű titkosítási protokoll) egy fejlett biztonsági lehetőség, mely a vezeték nélküli hálózati forgalom titkosítását végzi. Az adatok kódolására és dekódolására a WEP előre konfigurált kulcsokat használ (lásd 2. ábra).

A WEP-kulcsok szám- és betűkombinációból álló sorozatok, többnyire 64 vagy 128 bit hosszúsággal, mely egyes esetekben 256 bit is lehet. A kulcsok létrehozásának és beírásának egyszerűsítése érdekében számos eszköz felkínálja a Passphrase (jelmondat) lehetőséget. A passphrase egy könnyen észben tartható szó vagy kifejezés, melyet a kulcsok automatikus létrehozásához használhatunk.

A WEP megfelelő működéséhez a hozzáférési ponton és az összes engedélyezett állomáson ugyanazon WEP-kulcsot kell megadni. Ezen kulcs nélkül az eszközök nem tudják értelmezni az érkező vezeték nélküli jeleket.

A WEP használatának megvannak a hátrányai is, például, hogy az összes állomáson statikus (állandó érvényű) kulcsokat használ. Léteznek olyan interneten is fellelhető alkalmazások, melyek segítségével a támadók kideríthetik a WEP-kulcsot. Miután a támadó megfejtette a kulcsot, teljes hozzáférést szerez az összes továbbított információhoz.

A sebezhetőség elkerülésének egyik módja a WEP-kulcsok gyakori megváltoztatása. A másik módszer egy jóval fejlettebb és biztonságosabb titkosítási eljárás, a WPA (Wi-Fi Protected Access, Wi-Fi védett hozzáférés) alkalmazása.

**WPA**

A WPA (Wi-Fi Protected Access, Wi-Fi védett hozzáférés) is 64 és 256 bit közötti hosszúságú kulcsokat használ, de ellentétben a WEP-pel, automatikusan új kulcsokat hoz létre minden alkalommal, amikor egy kliens kapcsolódik a hozzáférési ponthoz. A dinamikus kulcsok használata miatt a WPA feltörése lényegesen nehezebb, így jóval biztonságosabb a WEP-nél.

Számos további biztonsági megoldás konfigurálható egy vezeték nélküli AP-n, például MAC-cím szűrés, hitelesítés és forgalomszűrés. Ezek megvalósítása azonban kívül esik a kurzus témakörén.

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító konfigurálása

A Linksys vezeték nélküli forgalomirányító gyakori eszköz az otthoni és kisvállalati hálózatokban, ezért a kurzus során az integrált forgalomirányító konfigurálásának bemutatásához fogjuk használni. A Linksys eszköz általában 5-8 Ethernet porttal rendelkezik a vezetékes kapcsolódáshoz, és vezeték nélküli elérési pontként (AP) is működik. Ezenkívül tartalmaz egy DHCP-szervert és egy mini webszervert, amely a grafikus felhasználói felületet (Graphical User Interface, GUI) biztosítja.

**Linksys forgalomirányító elérése és konfigurálása**

A Linksys forgalomirányítóhoz való első kapcsolódáshoz kössük össze a számítógépet a forgalomirányító egyik LAN Ethernet portjával (lásd ábra). A csatlakozás után a számítógép automatikusan címinformációkat kap az integrált eszköztől, többek között az alapértelmezett átjáró címét, amely egyben a Linksys eszköz IP-címe is. Ellenőrizzük a számítógép beállításait és állapítsuk meg ezt címet az **ipconfig /all** parancs használatával. Ezután gépeljük be a kapott IP-címet egy böngészőprogramba, hogy hozzáférjünk a webes konfigurációs felülethez (GUI).

A Linksys eszköz gyári konfigurációja alapvető útválasztási és kapcsolási szolgáltatásokat, valamint egy DHCP-szervert tartalmaz. Mielőtt egy AP-t az élő hálózathoz csatlakoztatunk, néhány kezdeti konfigurációs feladatot végre kell hajtanunk. Ezek közé tartozik az alapértelmezett felhasználónév és jelszó megváltoztatása, a Linksys IP-címének lecserélése és DHCP-ímtartományának módosítása.

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító konfigurálása

A vezeték nélküli kapcsolódás engedélyezéséhez be kell állítanunk a vezeték nélküli módot, az SSID-t, az RF-csatornát és a kívánt titkosítási eljárást.

Először válasszuk ki a megfelelő vezeték nélküli módot, ahogy az ábrán is látható. Bármelyik mód beállítása bizonyos többletterhelést jelent a forgalomirányító számára. Ha minden állomás ugyanazt a szabványt használja, akkor a forgalomirányítón is ezt konfigurálva csökkenthető a terhelés. Ezenfelül biztonságot növelő tényező is, ha a végberendezéseknek nem engedélyezzük a különböző módú csatlakozást. Ha az állomások mégis különféle szabványokat használnak a hálózat elérésére, akkor a "mixed" módot kell választanunk. Ebben az esetben a hálózat teljesítménye csökkenni fog a módok támogatása miatti többletterhelés miatt.

Ezután állítsuk be az SSID-t. A vezeték nélküli hálózatban (WLAN) lévő összes együttműködő eszköznek azonos SSID-vel kell rendelkezni. Biztonsági okokból változtassuk meg az alapértelmezett SSID-t. Az SSID-szórás gyárilag bekapcsolt állapotban van, hogy a WLAN kliensek könnyen felismerjék a hálózatot. Az SSID-szórás kikapcsolható, ilyenkor azonban a vezeték nélküli klienseken kézzel kell beállítani ezt az értéket.

Az RF-csatorna kiválasztásakor figyelembe kell venni az integrált forgalomirányító közelében működő más vezeték nélküli hálózatokat.

Az optimális átbocsátóképesség elérése érdekében a szomszédos hálózatoknak egymást át nem fedő csatornákat kell használni. Manapság a legtöbb AP-n megtalálható az a beállítás, amely automatikusan megkeresi a legkevésbé terhelt csatornát.

Végül válasszuk ki a kívánt titkosítási módszert, és adjuk meg a kulcsot vagy a jelszót (jelmondatot).

# Integrált útválasztási szolgáltatások

## Integrált forgalomirányító konfigurálása

**Vezeték nélküli kliens konfigurálása**

Vezeték nélküli állomásnak, más néven kliensnek nevezünk minden olyan eszközt, amely rendelkezik vezeték nélküli hálózati kártyával és a hozzá tartozó szoftverrel. Ez a kliensszoftver teszi lehetővé, hogy a hardver a WLAN része legyen. Vezeték nélküli kliensek például: okostelefonok, laptopok, asztali számítógépek, nyomtatók, televíziók, játékkonzolok és táblaszámítógépek.

A WLAN-hoz való sikeres csatlakozás érdekében a kliens és a forgalomirányító beállításainak összhangban kell lenni. Ilyenek például az SSID, a biztonsági beállítások, és a csatorna adatok (ha manuálisan lettek konfigurálva). A beállítások a kliensszoftverben kerülnek megadásra.

A használt kliensszoftver lehet az eszköz operációs rendszerébe integrált, vagy lehet különálló, letölthető szoftver, melyet vezeték nélküli NIC kezelésére terveztek.

A szoftver beállítása után ellenőrizzük a kliens és az AP közötti kapcsolatot.

Nyissuk meg a vezeték nélküli kapcsolat információs ablakát, melyben a következők láthatók: adatátviteli sebesség, kapcsolat állapot és csatorna használat (lásd ábra). A Link Information menüpont, ha rendelkezésre áll, megjeleníti a vezeték nélküli jel erősségét és minőségét.

A kapcsolat további ellenőrzéséhez győződjünk meg arról, hogy továbbíthatók-e az adatok. Az egyik leggyakrabban használt módszer az adatátvitel tesztelésére a ping. Ha a ping sikeres, az adatátvitel lehetséges.

# Összefoglalás

## Összefoglalás

**Capstone ("sarokkő") projekt**

**Kisvállalati hálózat tervezése és kivitelezése**

A feladat megoldásához használjuk a Packet Tracer-t és egy szövegszerkesztő. Dolgozzunk 2-3 fős csoportokban.

Tervezzük meg és építsük fel a hálózatot a következő rövid vázlat alapján.

* A tervezetben legyen legalább egy forgalomirányító, egy kapcsoló és egy PC.
* Teljesen konfiguráljuk fel a hálózatot IPv4- vagy IPv6-címzést használva (alhálózatokra bontás is legyen a címzési tervben).
* Teszteljük a hálózatot legalább 5 **show** parancs kiadásával.
* Ügyeljünk a hálózatbiztonságra, használjunk SSH-t, jelszótitkosítást és védjük a konzol hozzáférést is. (Minimum elvárás)

Készítsünk táblázatot a munka értékeléséhez, vagy használjuk az oktató által biztosítottat.

Mutassuk be saját tervünket az osztálynak és készüljünk fel a felmerülő kérdések megválaszolására.

[Csoportos feladat - Design and Build a Small Network Instructions](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/11.6.1.1%20Class%20Activity%20-%20%20Design%20and%20Build%20a%20Small%20Network%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

A felhasználói igények teljesítése érdekében a kisebb hálózatok is tervezést igényelnek (lásd ábra). Tervezéskor figyelembe kell venni az összes követelményt, költségelemet és fejlesztési lehetőséget, valamint biztosítani kell a megbízhatóságot, skálázhatóságot és a rendelkezésre állást.

A kis hálózatok felügyelete és fejlesztése jártasságot kíván a protokollok és hálózati alkalmazások tekintetében. A protokollelemzők segítségével a szakemberek gyorsan kaphatnak átfogó statisztikai információkat a hálózati forgalomról. Ezt követően a begyűjtött adatok rendszerezhetők az üzenetek forrása, célja és típusa szerint. A elkészült elemzés alapján a hálózati szakember döntést hozhat a forgalom hatékonyabbá tétele érdekében. A leggyakran vizsgált protokollok a következők: DNS, Telnet, SMTP, POP, DHCP, HTTP és FTP.

A hálózat tervezésekor figyelembe kell venni a biztonsági fenyegetéseket és sebezhetőségi pontokat. A hálózat összes készülékét védeni kell, beleértve a forgalomirányítókat, kapcsolókat és felhasználói eszközöket, sőt még a biztonsági berendezéseket is. A hálózatokat különféle kártékony szoftverek veszélyeztetik, például vírusok, trójai lovak és férgek. A vírusirtó szoftverek felismerik legtöbbjüket, és megakadályozzák szétterjedésüket a hálózatban. A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch).

A hálózatokat védeni kell a hálózati támadásoktól is, melyek három fő csoportja: a felderítési és a hozzáférési támadások, valamint a szolgáltatás megtagadás. A hálózatok többféle módon is megóvhatók ezektől a támadásoktól.

* A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, melyek a hálózati eszközök hozzáférés-szabályozásának alapját alkotják. Az AAA vezérli, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultság), és nyomon követi a használat során végrehajtott műveleteket (naplózás).
* A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is.
* A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. valamint távoli bejelentkezés esetén az SSH engedélyezése a könnyen támadható Telnet helyett.

A hálózat kiépítése után a rendszergazda következő feladata a hálózati összeköttetések vizsgálata és karbantartása, melyhez számos módszer áll rendelkezésre. A helyi és távoli hálózatokkal való kapcsolat tesztelésére leggyakrabban a **ping, telnet**és a **traceroute** parancsokat alkalmazzák.

A Cisco IOS eszközökön a **show version** parancs használható az indításnál szerepet játszó hardver- és szoftverkomponensek ellenőrzésére és az esetleges hibák megkeresésére. A forgalomirányító interfész információinak megtekintésére a **show ip interface** utasítás szolgál. A **show ip interface brief** egy tömörebb kimenetet jelenít meg, mint a **show ip interface** parancs. A CDP (Cisco Discovery Protocol) egy Cisco fejlesztésű protokoll, mely az adatkapcsolati rétegben működik. Ennek köszönhetően az egymással összekötött Cisco eszközök, például a különböző hálózati protokollt használó forgalomirányítók, képesek felismerni szomszédaikat még akkor is, ha 3. rétegbeli kapcsolat nincs is közöttük.

Az IOS konfigurációs állományait (pl.: startup-config vagy running-config) archiválni kell egy szövegfájlba vagy egy TFTP-szerverre. Néhány forgalomirányító típus rendelkezik USB-porttal, így a biztonsági mentés USB-meghajtóra is történhet. Szükség esetén a lementett fájlok a TFTP-szerverről vagy az USB-meghajtóról visszamásolhatók a forgalomirányítóra vagy kapcsolóra.

Hálózatokat nem csak kisvállalkozások és nagy szervezetek használnak. Otthoni környezetben is egyre jobban terjed a hálózati technológiák alkalmazása. Egy otthoni hálózat nagyon hasonlít egy kisvállalati hálózathoz, mivel egyik sem igényel felső kategóriás eszközöket, például dedikált forgalomirányítókat és kapcsolókat. Helyettük az otthoni hálózatokban multifunkciós eszközök működnek. A kurzus folyamán ezekre a multifunkciós eszközökre, mint integrált forgalomirányítókra hivatkozunk. A legtöbb integrált forgalomirányító vezetékes és vezeték nélküli kapcsolódási lehetőséget is biztosít, valamint vezeték nélküli elérési pontként (Access Point, AP) viselkedik. A vezeték nélküli kapcsolódás engedélyezéséhez be kell állítanunk a vezeték nélküli módot, az SSID-t, az RF-csatornát és a kívánt titkosítási eljárást.

