# Fejezet 5: Ethernet 5.0.1.1 Bevezetés

# Ethernet

## Bevezetés

Az OSI modell fizikai rétege biztosítja egy adatkapcsolati rétegbeli keret bitjeinek hálózati közegen történő továbbításának eszközeit.

Jelenleg az Ethernet az uralkodó LAN technológia a világon. Az Ethernet az OSI modell két rétegében működik: az adatkapcsolati és a fizikai rétegben. Az Ethernet protokoll szabványai a hálózati kommunikációt sok szempontból definiálják, beleértve a keret formátumát, a keret méretét, az időzítést és a kódolást. Amikor egy Ethernet hálózaton üzeneteket küldünk az állomások között, akkor azok a szabványokban meghatározott keretformátumúvá alakítják az üzeneteket. A kereteket protokoll adategységeknek (Protocol Data Unit, PDU) is nevezik.

Mivel az Ethernet-et ezen alsóbb rétegek szabványai tartalmazzák, legjobban talán az OSI modellre hivatkozva lehet megérteni. Az OSI modell elkülöníti az adatkapcsolati réteg címzési, keretezési és közeg-hozzáférési funkcióit a közeg fizikai rétegbeli szabványaitól. Az Ethernet szabványok mind a második rétegbeli protokollokat, mind pedig az első rétegbeli technológiákat meghatározzák. Bár az Ethernet szabvány különböző közegeket, sávszélességeket és eltérő 1. és 2. rétegbeli variációkat támogat, az alapvető keretformátum és a címzési rendszer az Ethernet mindegyik változatánál ugyanaz.

Ez a fejezet megvizsgálja az Ethernet működését és jellemzőit, ahogyan egy osztott közegű, versengésen alapuló adatkommunikációs technológiából napjaink nagy sebességű, full-duplex technológiájává fejlődött.

# Ethernet

## Bevezetés

**Csatlakozz az ismerősi körömhöz!**

A legtöbb hálózati kommunikációnk üzenetküldés (szöveges vagy azonnali), videó kapcsolat, közösségi média hozzászólások stb. formájában történik.

Ehhez a feladathoz válasszunk ki egyet az általunk leggyakrabban használt kommunikációs hálózatokból:

* Szöveges (vagy azonnali) üzenetküldés
* Audió / videó konferencia
* E-mailezés
* Játék

Miután kiválasztottunk egy hálózati kommunikációs típust, jegyezzük fel a válaszokat az alábbi kérdésekre:

* Van-e olyan eljárás, amit követnünk kell a magunk és mások regisztrálásához azért, hogy kommunikációs csoportot alkossunk?
* Hogyan kezdeményezzük a kapcsolatot azzal személlyel (vagy személyekkel), akivel kommunikálni szeretnénk?
* Hogyan korlátozzuk a párbeszédeket, hogy csak azok kapják meg az üzeneteket, akikkel kommunikálni szeretnénk?

Készüljünk fel, hogy megvitassuk a rögzített válaszokat az osztállyal.

[Csoportos feladat - Utasítások a Csatlakozz az ismerősi körömhöz! feladathoz](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.0.1.2%20Join%20My%20Social%20Circle%20Instructions.pdf)

# Az Ethernet protokoll

## Az Ethernet működése

Az Ethernet manapság a legelterjedtebb LAN technológia.

Az Ethernet az OSI modell adatkapcsolati és fizikai rétegeiben működik. Az IEEE 802.2 és 802.3 szabványok a hálózati technológiáknak egy egész családját definiálják Az Ethernet a következő sávszélességeket támogatja:

* 10 Mb/s
* 100 Mb/s
* 1000 Mb/s (1 Gb/s)
* 10000 Mb/s (10 Gb/s)
* 40000 Mb/s (40 Gb/s)
* 100000 Mb/s (100 Gb/s)

Amint az 1. ábrán látható, az Ethernet szabványok meghatározzák mind a 2. rétegbeli protokollokat, mind pedig az 1. rétegbeli technológiákat. Mint minden 802 IEEE-szabvány, az Ethernet működése is az adatkapcsolati rétegben lévő két különálló alrétegre, az LLC- (Logical Link Control) és a MAC- (Media Access Control) alrétegekre támaszkodik.

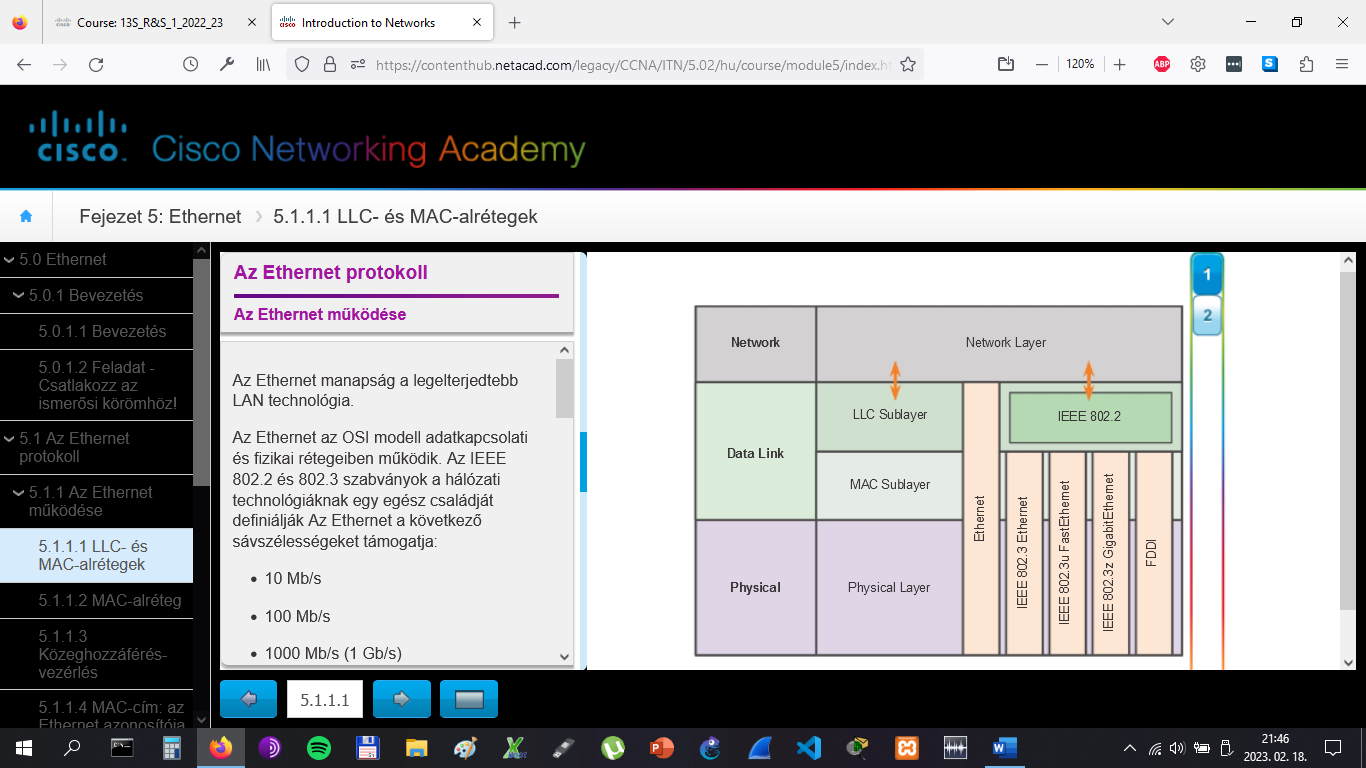
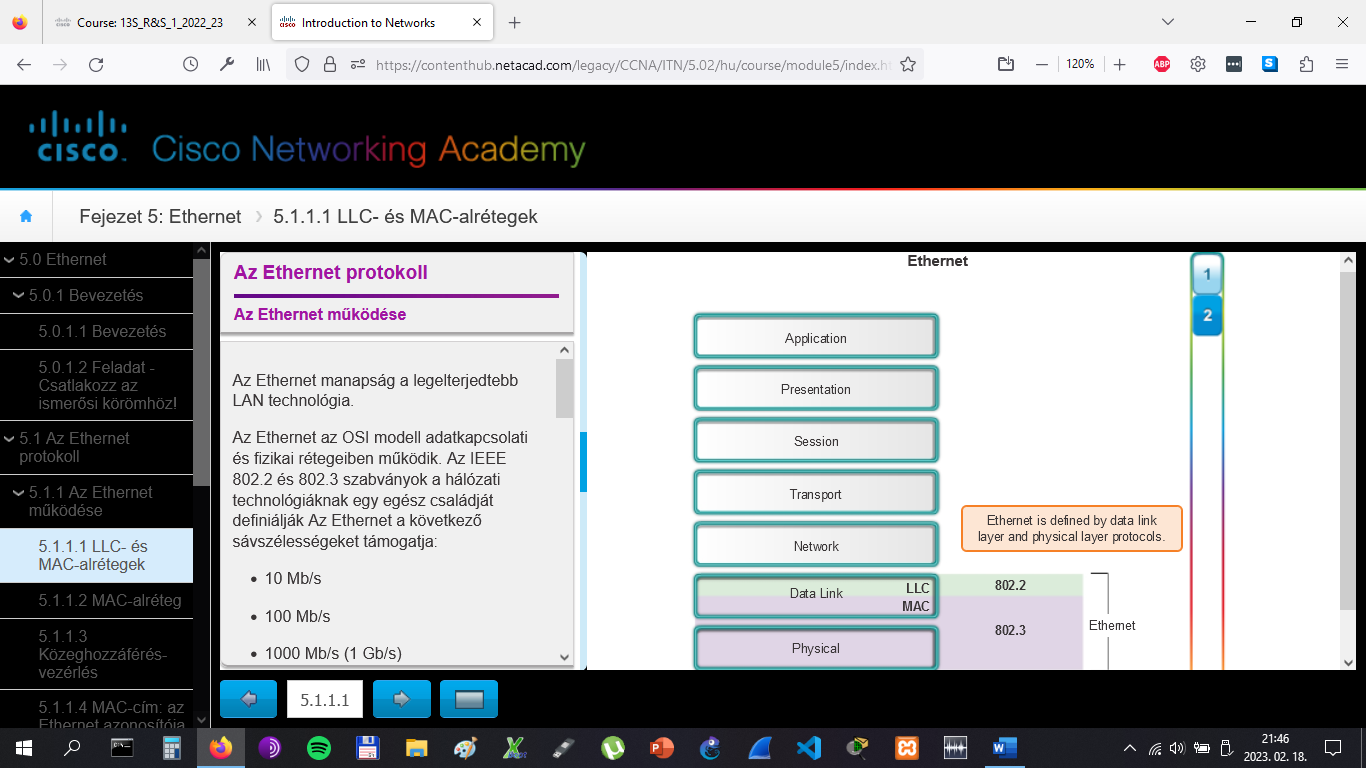
**LLC-alréteg**

Az Ethernet LLC-alréteg kezeli a felsőbb és az alsó rétegek közötti kommunikációt. Ez jellemzően a hálózati szoftver és a készülék hardvere között zajlik. Az LLC-alréteg veszi a hálózati protokoll adatait - ami jellemzően egy IPv4 csomag - és olyan vezérlő információkkal látja el, amelyek segítik a csomagnak a célállomáshoz történő eljuttatását. Az LLC-t az alkalmazás felsőbb rétegeivel történő kommunikációra, valamint a csomag átalakítására használjuk, hogy az alsóbb rétegek továbbítani tudják.

Az LLC szoftveresen van megoldva, és így a megvalósítása független a hardvertől. Egy számítógépen a hálózati kártya (NIC) meghajtóprogramja tekinthető az LLC-nek. A hálózati kártya meghajtóprogramja egy olyan program, amely közvetlen kölcsönhatásban van a kártya hardverével, hogy az adatokat továbbadja a MAC-alréteg és a fizikai közeg között.

**MAC-alréteg**

A MAC-alréteg az adatkapcsolati réteg alsó alrétege. A MAC-alréteget hardveresen valósítják meg, tipikusan a számítógép hálózati kártyájában. A részleteket az IEEE 802.3 szabványok határozzák meg. A 2. ábra az általános IEEE Ethernet szabványokat sorolja fel.



# Az Ethernet protokoll

## Az Ethernet működése

Amint az ábrán látható, az Ethernet MAC-alrétegnek két fő feladata van:

* Adatbeágyazás
* Közeghozzáférés-vezérlés

**Adatbeágyazás**

Az adatbeágyazási folyamat magában foglalja a keret összeállítását a továbbítás előtt, és a szétbontását a kézhezvétel után. A keret felépítésekor a MAC-réteg egy fejlécet és egy utótagot ad a hálózati réteg PDU-jához.

Az adatbeágyazás három fő funkciót biztosít:

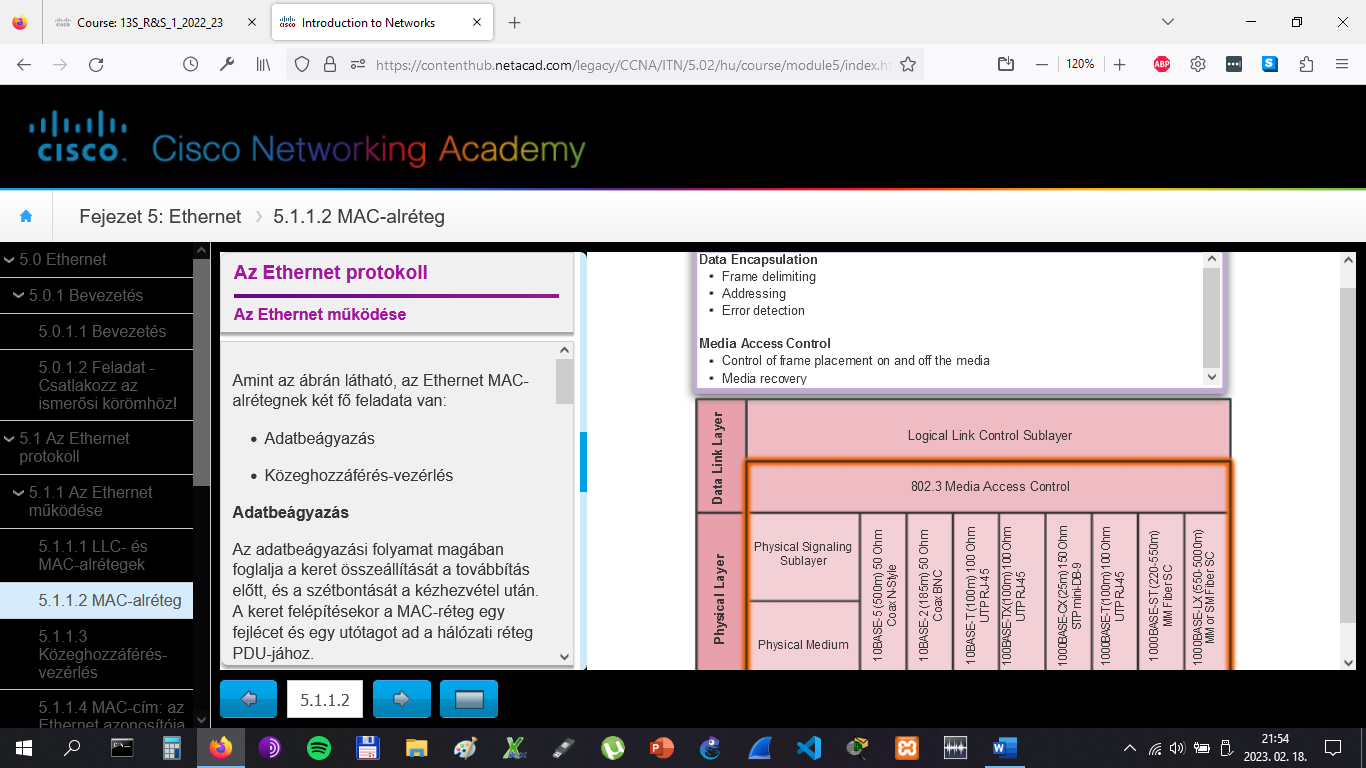
* **Keret határolás**: A keretezési folyamat fontos határolókat biztosít, amiket a keretet alkotó bitek csoportjának azonosítására használnak. Ez a folyamat biztosítja a szinkronizációt az adó és a vevő csomópontok között.
* **Címzés**: A beágyazási folyamat az adatkapcsolati réteg címzését is biztosítja. Minden Ethernet keret fejléce tartalmazza a fizikai címet (MAC-cím), amely lehetővé teszi a keret kézbesítését a rendeltetési helyére.
* **Hibafelismerés**: Mindegyik Ethernet keret tartalmaz egy utótagot a keret tartalmára vonatkozóan, ami egy ciklikus redundancia ellenőrzés (CRC). Egy keret vétele után a fogadó csomópont is készít egy CRC-t, hogy összehasonlítsa azt a keretben lévővel. Ha a két CRC-számítás eredménye megegyezik, a keret nagy valószínűséggel hiba nélkül érkezett.

A keretek használata segíti a közegre helyezett bitek átvitelét és a fogadó csomóponton a bitek csoportosítását is.

**Közeghozzáférés-vezérlés**

A MAC-alréteg másik feladata a közeghozzáférés-vezérlés. Ez felelős a keretek közegre való elhelyezéséért és azok eltávolításáért. Ahogy a neve is mutatja, ez szabályozza a közeghez való hozzáférést. Ez az alréteg közvetlenül a fizikai réteggel kommunikál.

Az Ethernet mögöttes logikai topológiája egy többszörös hozzáférésű sín (vagy busz), ezért az azonos hálózati szegmensen lévő csomópontok (eszközök) osztoznak a közegen. Az Ethernet a hálózatkezelés egy versengés alapú módszere. Emlékezzünk rá, hogy a versengés alapú, vagy nem-determinisztikus módszer azt jelenti, hogy bármelyik eszköz megpróbálhat adatot továbbítani a megosztott közegen, amennyiben van elküldendő adata. Hasonlóan ahhoz, mint amikor két ember próbál meg egyszerre beszélni, ha több eszköz próbál ugyanazon közegen és egy időben adatokat továbbítani, az adatok ütköznek, ami sérült vagy használhatatlan adatokat eredményez. Emiatt az Ethernet biztosít egy módszert a csomópontok közeghozzáférésének vezérlésére, ez a módszer a Vivőérzékeléses Többszörös Hozzáférés (Carrier Sense Multiple Access, CSMA) technológia.Ezért az Ethernet egy vivőérzékeléses többszörös hozzáférésnek (Carrier Sense Multiple Access, CSMA) nevezett technológiát alkalmazó módszert biztosít a csomópontok közeghozzáférés-vezérlésének kezelésére.



# Az Ethernet protokoll

## Az Ethernet működése

A CSMA-folyamatot először annak érzékelésére használjuk, hogy a közegen történik-e jeltovábbítását. Ha egy másik csomóponttól származó vivőjelet érzékelünk a közegen, az azt jelenti, hogy egy másik készülék adásban van. Ha a készülék - amelyik továbbítani próbál - azt látja, hogy a közeg foglalt, akkor vár és kis idő múlva újra próbálkozik. Ha nem észlel vivőjelet, akkor továbbítja az adatokat. Előfordulhat hogy a CSMA-folyamat meghiúsul, mert két eszköz ugyanabban az időben továbbít.. Ez az úgynevezett adatütközés, vagy röviden ütközés. Amennyiben ez történik, akkor mindkét készülék elküldött adatai megsérülnek és újra el kell őket küldeni.

A versengés alapú közeghozzáférési módszerek nem igényelnek olyan mechanizmusokat, amelyek nyomon követik, hogy ki fog legközelebb hozzáférni a közeghez, ezért nincs is bennük az ellenőrzött módszerekre jellemző többletterhelés. Ugyanakkor a versengés alapú rendszerek nagy mértékű közeghasználat esetén nem jól skálázhatók. Ahogy a közeghasználat és a csomópontok száma növekszik, egyre csökken annak a valószínűsége, hogy ütközés nélküli, vagyis sikeres legyen a közeghez való hozzáférés. Ezen felül az ütközési hibákat kijavító helyreállítási mechanizmusok tovább rontják a teljesítményt.

Amint az ábrán látható, a CSMA-t általában a közegért való versengés megoldására szolgáló módszerrel együtt valósítják meg. A két leggyakrabban használt módszer a következő:

**CSMA/CD (ütközésérzékelés)**

Az ütközésérzékelés (CSMA/Collision Detection, CSMA/CD) esetén a készülék figyeli, hogy van-e adatjel a közegen. Amennyiben az adatjel hiányzik, jelezve hogy a közeg szabad, a készülék továbbítja az adatokat. Ha ezek után adatjeleket érzékelünk - ami azt jelzi, hogy egy másik készülék is ugyanabban az időben forgalmazott -, minden más eszköz leállítja a küldést és később újra próbálkozik. Az Ethernet hagyományos változatait ennek a módszernek a használatára fejlesztették ki.

A kapcsolt technológiák széleskörű elterjedése a modern hálózatokban nagymértékben megváltoztatta a CSMA/CD használatával kapcsolatos igények. A LAN-eszközök között szinte az összes vezetékes kapcsolat manapság full-duplex, vagyis a készülék egyszerre képes küldeni és fogadni is. Ez azt jelenti, hogy míg az Ethernet hálózatokat a CSMA/CD-technológiára tervezték, a mai közvetítő eszközöknél ütközések nem fordulnak elő, és a CSMA/CD által használt folyamatok valójában feleslegesekké váltak.

A vezeték nélküli LAN-környezetben lévő kapcsolatoknál azonban még figyelembe kell venni az ütközéseket. A vezeték nélküli LAN-eszközök a CSMA/Collision Avoidance (ütközés elkerülés, CSMA/CA) közeg-hozzáférési módot alkalmazzák.

**CSMA/Collision Avoidance (ütközés elkerülés)**

A CSMA/CA estében a készülék megvizsgálja a közeget, hogy érzékelhető-e adatjel. Ha a közeg szabad, akkor a készülék küld egy értesítést a média használati szándékáról. A készülék ezután elküldi az adatokat. Ezt a módszert használják a 802.11 vezeték nélküli hálózati technológiák.

# Az Ethernet protokoll

## Az Ethernet működése

Mint korábban említettük, az Ethernet logikai topológiája egy többes hozzáférésű sín. Minden hálózati eszköz ugyanahhoz megosztott közeghez csatlakozik és minden csomópont megkapja a közegen továbbított összes keretet. A kérdés csupán az, hogy ha minden eszköz megkap minden keretet, akkor hogyan tudják az egyes eszközöknek beazonosítani, hogy ők-e a valódi címzettek, és mindezt anélkül, hogy fel kellene dolgozniuk és ki kellene bontaniuk a kereteket az IP-cím megszerzése érdekében? A kérdés még inkább problematikus nagyméretű és nagy forgalmú hálózatok esetében, ahol rengeteg keretet továbbítanak.

Az összes keretek feldolgozásából adódó túlzott mértékű többletterhelés megakadályozása érdekében egy MAC-címnek nevezett egyedi azonosítót hoztak létre, hogy a tényleges forrás- és célcsomópontokat azonosítani lehessen egy Ethernet hálózaton belül. Függetlenül attól, hogy melyik Ethernet verziót használjuk, az OSI modell alsóbb szintjén a MAC-címzés azonosítja az eszközt. Mint bizonyára emlékszünk rá, a MAC-címzés a második rétegbeli PDU-hoz adódik hozzá. Az Ethernet MAC-cím egy 48 bites bináris érték, amit 12 hexadecimális számjeggyel írunk le (egy hexadecimális számjegy 4 bitet jelöl).

**A MAC-címek szerkezete**

A MAC-címek az egész világon egyediek kell hogy legyenek. Az Ethernet eszközök MAC-címeinek globálisan is egyedi értékei az IEEE-szervezet gyártókra vonatkozó szabályozásának az eredménye. Az IEEE által létrehozott szabályok bármely Ethernet eszköz gyártójától elvárják, hogy regisztrálja magát az IEEE-nél. Az IEEE a gyártóhoz egy 3 bájtos (24 bites) kódot rendel hozzá, az úgynevezett egyedi szervezetazonosítót (OUI).

Az IEEE elvárja a gyártótól, hogy kövessenek két egyszerű szabályt, ahogy azt az ábra mutatja:

* A hálózati kártyának vagy más Ethernet eszköznek adott MAC-cím első 3 bájtjának tartalmaznia kell a gyártóhoz rendelt OUI-t.

Az ugyanolyan OUI-val rendelkező MAC-címeknek egy egyedi értéket (vendor kód vagy sorozatszám) kell tartalmazniuk az utolsó 3 bájtban.

# Az Ethernet protokoll

## Az Ethernet működése

A MAC-címet gyakran nevezik beégetett címnek (Burned-In Addresss, BIA), mert régen ezt a címet beleégették a hálózati kártya ROM-jába (Read-Only Memory). Ez azt jelenti, hogy a cím véglegesen bele van kódolva a ROM chipbe - nem lehet szoftveresen megváltoztatni.

**Megjegyzés**: A modern operációs rendszerek és a hálózati kártyák esetén szoftveresen is meg lehet változtatni a MAC-címet. Ezt például akkor használják, ha megpróbálnak behatolni olyan hálózatba, amely BIA alapján szűri a hozzáférést - következésképpen, a forgalom MAC-címen alapuló szűrése vagy ellenőrzése ma már nem olyan biztonságos.

A MAC-címet hozzárendelhetjük munkaállomásokhoz, szerverekhez, nyomtatókhoz, kapcsolókhoz és forgalomirányítókhoz - minden olyan eszközhöz, amelyről adat származik, és/vagy adatokat fogadhat a hálózaton. Minden Ethernet LAN-ra csatlakozott eszköz interfészének van egy MAC-címe. A különböző hardver- és szoftver-gyártók a MAC-címet különböző hexadecimális formátumban adhatják meg. A címformátumok az alábbiakhoz hasonlók lehetnek:

* 00-05-9A-3C-78-00
* 00:05:9A:3C:78:00
* 0005.9A3C.7800

A számítógép elindulásánál a NIC első teendője, hogy bemásolja a MAC-címet a ROM-ból a RAM-ba. Amikor egy eszköz üzenetet továbbít egy Ethernet hálózatra, fejléc információt csatol a csomaghoz. A fejléc információi tartalmazzák a forrás és a cél MAC-címeket. A forrás készülék elküldi az adatokat a hálózaton keresztül.

A hálózaton minden NIC megvizsgálja az adatokat a MAC-alrétegben, hogy a keretbeli cél MAC-cím megegyezik-e a készülék RAM-ban tárolt fizikai MAC-címével. Ha nincs egyezés, akkor a készülék eldobja a keretet. Amikor a keret eléri azt a helyet, ahol a cél MAC-cím megegyezik a NIC címével, a hálózati kártya átadja a keretet a felsőbb OSI-rétegeknek, ahol elkezdődik a kibontási folyamat.

# Az Ethernet protokoll

## Az Ethernet keret tulajdonságai

1973 - az Ethernet megalkotása - óta szabványok egész sora született a technológia egyre gyorsabb és rugalmasabb változatainak kifejlesztésére. Az Ethernet képes volt fejlődni az idők folyamán, ez a legfőbb oka annak, hogy ilyen népszerűvé vált. Az Ethernet korai változatai viszonylag lassúak, 10 Mb/s sebességűek voltak. A legújabb Ethernet verziók már 10 Gb/s vagy gyorsabb sebességgel működnek. Az 1. ábra a különböző Ethernet változatokban bekövetkezett változásait szemlélteti.

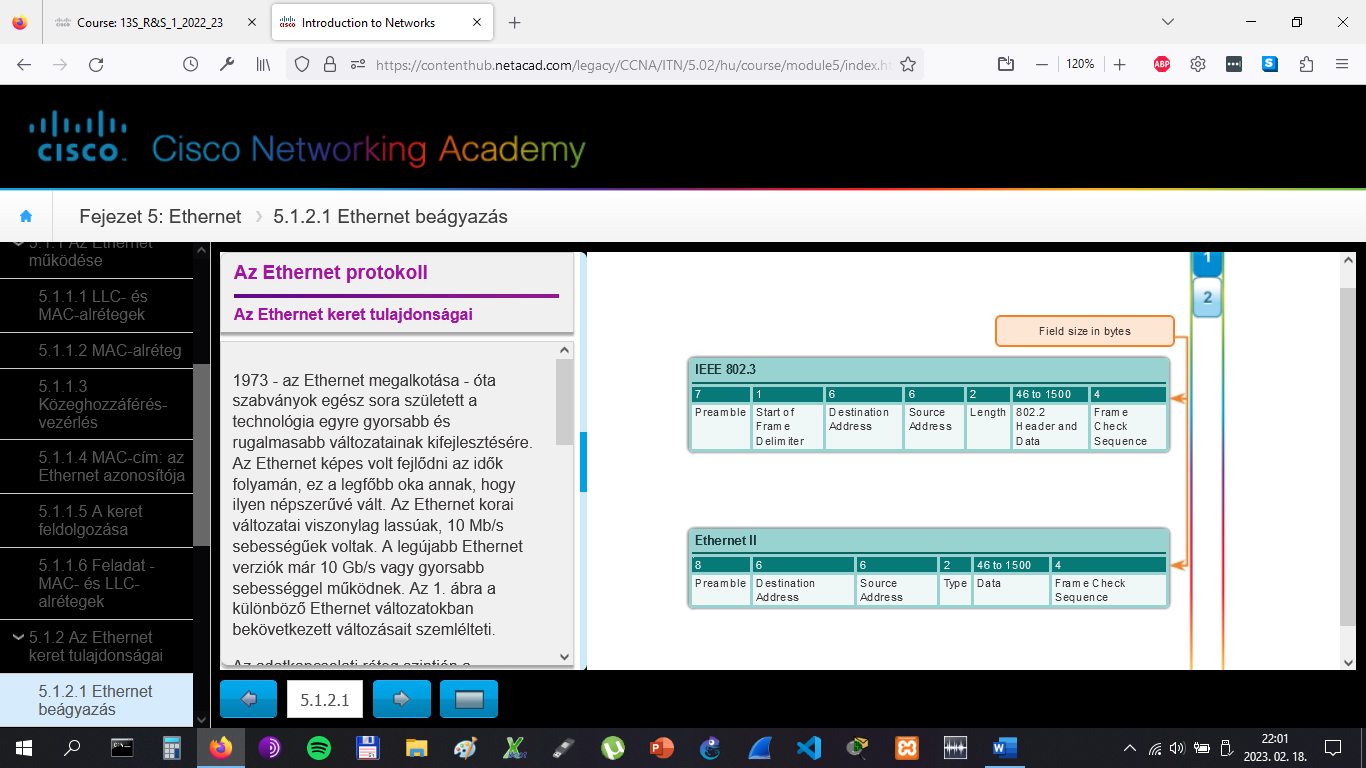
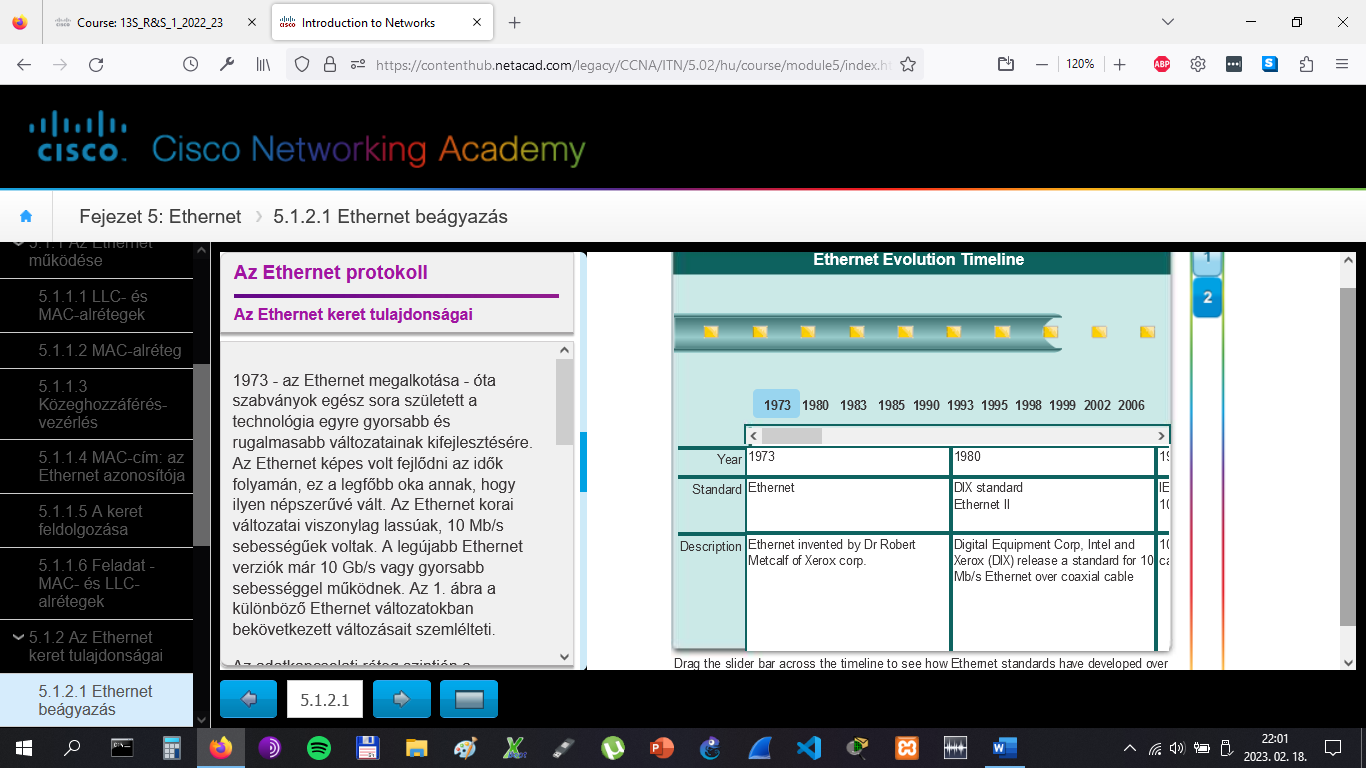
Az adatkapcsolati réteg szintjén a keretszerkezet gyakorlatilag az Ethernet összes változatánál azonos. Az Ethernet keretszerkezet fejléceket és utótagokat ad a 3. rétegbeli PDU elé és mögé, hogy beágyazza az elküldendő üzenetet.

Mind az Ethernet fejléc, mind az utótag több szakaszban tárol információkat, amelyet az Ethernet protokoll használ. A keret minden szakaszát mezőnek nevezzük. Amint a 2. ábrán látható, két típusú Ethernet keretezés létezik:

* Az IEEE 802.3 Ethernet szabvány, amely az új technológiák támogatására már többször változott.
* A DIX Ethernet szabvány, amelyet manapság Ethernet II-ként emlegetnek.

A keretezési szabványok közti különbség minimális. A legjelentősebb különbség a két szabvány között, hogy a 802.3-ban hozzáadtak egy keretkezdő mezőt (Start Frame Delimiter, SFD) és a típus mező hossz mezőre változott.

Az Ethernet II a TCP/IP-hálózatokon használt Ethernet keretformátuma.



# Az Ethernet protokoll

## Az Ethernet keret tulajdonságai

Mind az Ethernet II, mind az IEEE 802.3 szabványok úgy határozzák meg a keret méretét, hogy minimum 64 bájt, illetve maximum 1518 bájt lehet. Ez magában foglalja az összes bájtot a cél MAC-cím mezőtől kezdve a keretellenőrző (Frame Check Sequence, FCS) mezőig. Az előtag és keretkezdő mezőket nem vesszük figyelembe, amikor megadjuk a keret méretét.

Minden keretet, ami kevesebb, mint 64 bájt hosszúságú, ütközési töredéknek vagy runt-nak nevezünk és ezeket automatikusan eldobja a fogadó állomás.

Az 1998-ban megjelent IEEE 802.3ac szabvány 1522 bájtra terjesztette ki a megengedett legnagyobb keret méretét. A keret méretét azért növelték meg, hogy támogassa az úgynevezett virtuális helyi hálózat (VLAN) technológiát. A VLAN-ok egy kapcsolt hálózatban jönnek létre, és egy későbbi kurzus folyamán kerülnek bemutatásra. Továbbá a legtöbb szolgáltatásminőséggel (QoS) foglalkozó technológia kihasználja a felhasználói prioritás mezőt, hogy különböző szolgáltatási szinteket tudjon biztosítani, például prioritásos szolgáltatást a hangforgalom számára. Az ábrán a 802.1Q VLAN címkében lévő mezők láthatók.

Ha egy átvitt keret mérete kisebb, mint a minimális vagy nagyobb, mint a maximális érték, a fogadó készülék eldobja a keretet. Az eldobott keretek valószínűleg ütközések és más nem kívánt jelek eredményei, ezért érvénytelennek tekintendők.

Az adatkapcsolati réteg szintjén a keret szerkezete majdnem azonos. A fizikai rétegben az Ethernet különböző változatai eltérő módszereket használnak az adatok érzékelésére és közegre való helyezésére.

# Az Ethernet protokoll

## Az Ethernet keret tulajdonságai

Az elsődleges mezők az Ethernet kereten belül a következők:

* **Előtag és keretkezdő mezők**: Az előtag (7 bájt) és a keretkezdő (Start Frame Delimiter, SFD, más néven Start of Frame, 1 bájt) mezőket szinkronizálásra használják a küldő és fogadó készülékek között. A keretnek ezt az első nyolc bájtját használják, hogy a fogadó csomópontnak felhívják a figyelmét. Lényegében az első néhány bájt azt mondja a vevőnek, hogy álljon készen az új keret fogadására.
* **Cél MAC-cím mező**: Ez a 6 bájtos mező azonosítja a címzettet. Ha visszaemlékszünk, ezt a címet használja a második réteg, hogy segítse az eszközöket annak meghatározásában, hogy egy keret nekik szól-e. A keretben lévő címet összehasonlítják a készülék MAC-címével. Ha egyezés van, a készülék elfogadja a keretet.
* **Forrás MAC-cím mező**: Ez a 6 bájtos mező a keretet küldő hálózati kártyát vagy interfészt azonosítja.
* **Hossz mező**: Minden 1997-nél régebbi IEEE 802.3 szabványban a hossz mező határozza meg a keret adatmezejének pontos hosszát. Ezt később az FCS részeként használják, hogy biztosak legyünk abban, az üzenet megfelelően megérkezett. Egyéb esetekben a mező célja annak jelzése, hogy melyik magasabb szintű protokoll lett a keretbe beágyazva. Ha a két-oktettes érték nagyobb vagy egyenlő, mint 1536 (decimálisan) vagy 0x0600 hexadecimálisan, akkor az adatmező tartalmát aszerint dekódoljuk, amit az EtherType protokoll jelez. Ha az érték kisebb vagy egyenlő, mint az 1500 (decimálisan) vagy 0x05DC hexadecimális érték, akkor a hossz mezőt használják arra, hogy jelezze az IEEE 802.3 keretformátum használatát. Így különböztethetők meg az Ethernet II és a 802.3 keretek.
* **Adat mező**: Ez a mező (46-1500 bájt) tartalmazza a magasabb rétegbeli beágyazott adatokat, amely egy általános 3. rétegbeli PDU, vagy még gyakrabban egy IPv4 csomag. Minden keretnek legalább 64 bájt hosszúnak kell lennie. Ha egy kis csomagot ágyazunk be, akkor további biteket, úgynevezett kitöltést (pad) használnak, hogy megnöveljék a keret méretét a minimális méretre.
* **Keretellenőrző mező**: A keretellenőrző (Frame Check Sequence, FCS) mezőt (4 bájt) a hibák észlelésére használják a keretben. Ez a ciklikus redundancia-ellenőrzést (CRC) használja. A küldő készülék beleteszi a CRC-számítás eredményét a keret FCS-mezejébe. A fogadó készülék megkapja a keretet, és szintén generál egy CRC-t a hibakereséséhez. Ha a számítások megegyeznek, nem történt hiba. Ha a számítások nem egyeznek, az azt jelzi, hogy az adat megváltozott, ezért a keretet el kell dobni. Az adatban bekövetkezett változás annak a következménye lehet, hogy a biteket képviselő elektromos jelekben zavar keletkezett.

# Az Ethernet protokoll

## Az Ethernet MAC

A MAC-cím használata az egyik legfontosabb szempontja az Ethernet LAN technológiának. A MAC-címek hexadecimális számozást használnak.

A hexadecimális egy olyan szó, amit mind főnévként, mind melléknévként is használnak. (Megjegyzés: ez az eredeti angol "hexadecimal" kifejezésre igaz, ám a magyar nyelvben jellemzően melléknévként használt.) Amikor önmagában (mint főnév) használjuk, a tizenhatos (hexadecimális) számrendszert jelenti. A hexadecimális rendszer egy kényelmes módját biztosítja a bináris értékek leírásának. Ahogy a decimális egy tízes alapú, a bináris pedig egy kettes alapú számrendszer, úgy a hexadecimális egy tizenhatos alapú rendszer.

A tizenhatos alapú számrendszer 0 és 9 közötti számokat használ, valamint betűket az A és az F között. Az 1. ábra a 0000-1111 közötti bináris értékek decimális és hexadecimális megfeleltethetőségét ábrázolja. Könnyebb egy értéket egyetlen hexadecimális számjeggyel kifejezni, mint négy darab bináris jeggyel.

Tekintettel arra, hogy 8 bit egy közös bináris csoportot (bájtot) alkot, a bináris 00000000-11111111 közti értékeket ki lehet fejezni a hexadecimális 00-tól FF-ig terjedő tartománnyal. A bevezető nullákat mindig megjelenítjük a teljes 8 bites kiírásnál. Például a 0000 1010 bináris értéket hexadecimális 0A-ként írjuk le.

**Megjegyzés**: Fontos, hogy megkülönböztessük a hexadecimális értékeket a decimális értéktől a 0-9 karakterek tekintetében, amint azt az 1. ábra mutatja.

**Hexadecimális értékek leírása**

A hexadecimális értékeket általában szövegesen írjuk le, ahol a konkrét értéket egy 0x előzi meg (pl. 0x73), vagy használhatunk egy 16-os alsó index-et is a jelölésre. Ritkábban egy H is követheti a számot, például 73H. Mivel azonban az index szövegét nem ismeri fel a parancssor vagy egy programozási környezet, a műszaki leírásban a hexadecimális értéket a "0x" (nulla X) vezeti be. Ezért a fenti példák így jelennek meg: 0x0A és 0x73.

A hexadecimális jegyeket használják az Ethernet MAC-címek és az IPv6-címek leírására is.

**Hexadecimális számok átváltása**

A decimális és hexadecimális számok közti átváltás nem bonyolult művelet, de 16-tal gyorsan osztani vagy szorozni nem mindig könnyű. Ha ilyen átalakítások szükségesek, általában könnyebb a decimális vagy hexadecimális értéket binárissá átalakítani, majd azután a binárist értéket alakítani át decimális vagy hexadecimális értékké.

Megfelelő gyakorlattal fel lehet ismerni a decimális és hexadecimális értékeknek megfeleltethető bináris bitmintákat. A 2. ábra ezeket a mintákat mutatja a kiválasztott 8 bites értékekhez.

# Az Ethernet protokoll

## Az Ethernet MAC

Windows munkaállomáson az **ipconfig /all** paranccsal lehet megállapítani egy Ethernet adapter MAC-címét. Az 1. ábrán figyeljük meg a kimenetben a Physical Address (MAC) értéket, a számítógépen ez 00-18-DE-C7-F3-F8. Ha van hozzáférésünk, akkor érdemes ezt kipróbálni a saját számítógépen.

A készüléktől és az operációs rendszertől függően a MAC-címek különböző ábrázolásait figyelhetjük meg, mint ez a 2. ábrán látható. A Cisco forgalomirányítók és kapcsolók a következő formátumot használják: XXXX.XXXX.XXXX, ahol X egy hexadecimális karakter.

# Az Ethernet protokoll

## Az Ethernet MAC

Az Etherneten belül különböző MAC-címeket használunk a második rétegbeli egyedi címzésű, szórásos és csoportos kommunikációra.

Az egyedi címzésű (unicast) MAC-címet használunk, amikor egy keretet az adó eszközről egyetlen cél eszköznek küldünk.

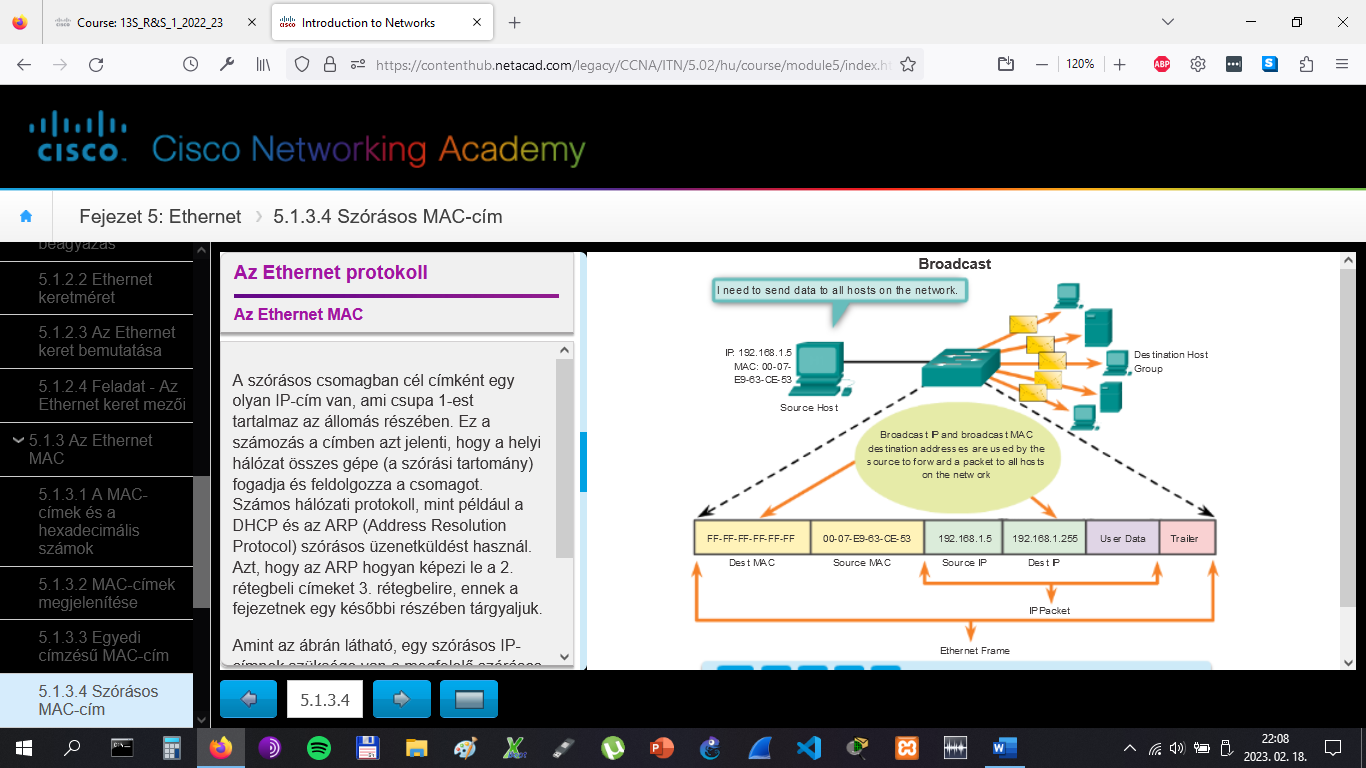
Az ábrán látható példában a 192.168.1.5 (forrás) IP-című állomás lekér egy weboldalt a 192.168.1.200 IP-című szervertől. Ahhoz, hogy egyedi címzésű csomagot küldhessünk és fogadhassunk, a cél IP-címnek szerepelnie kell az IP-csomag fejlécében. A megfelelő cél MAC-címnek szintén benne kell lennie az Ethernet keret fejlécében. Az IP-cím és a MAC-cím együttesen kézbesíti az adatokat egy adott célállomáshoz.

# Az Ethernet protokoll

## Az Ethernet MAC

A szórásos csomagban cél címként egy olyan IP-cím van, ami csupa 1-est tartalmaz az állomás részében. Ez a számozás a címben azt jelenti, hogy a helyi hálózat összes gépe (a szórási tartomány) fogadja és feldolgozza a csomagot. Számos hálózati protokoll, mint például a DHCP és az ARP (Address Resolution Protocol) szórásos üzenetküldést használ. Azt, hogy az ARP hogyan képezi le a 2. rétegbeli címeket 3. rétegbelire, ennek a fejezetnek egy későbbi részében tárgyaljuk.

Amint az ábrán látható, egy szórásos IP-címnek szüksége van a megfelelő szórásos MAC-címre is az Ethernet keretben. Az Ethernet hálózatokon a szórásos MAC-cím 48 darab egyesből áll, ez hexadecimálisan megjelenítve FF-FF-FF-FF-FF-FF.



# Az Ethernet protokoll

## Az Ethernet MAC

A csoportos címek lehetővé teszik a forráseszköz számára, hogy eszközök egy csoportjának küldjön csomagot. Azoknak az eszközöknek, amik többes címzésű csoporthoz tartoznak, csoportos IP-címe van. Az IPv4 multicast címek tartománya 224.0.0.0 - 239.255.255.255. Mivel a multicast cím a címek egy csoportját jelenti (néha állomás-csoportnak is hívják), csak csomagok cél címeként használható. A forrásnak mindig egyedi címe van.

A csoportos címzésre példaként említhetjük a távoli játékokat, ahol sok távoli játékos kapcsolódik össze, de mégis ugyanazt a játékot játsszák. Egy másik alkalmazása ezeknek a címeknek egy távoktatási videokonferencia lehet, ahol sok diák csatlakozik be ugyanabba az osztályba.

Mint a unicast és broadcast címek, a multicast IP-cím is igényel egy megfelelő csoportos MAC-címet, hogy el tudja juttatni a kereteket a helyi hálózaton. A csoportos MAC-cím egy speciális érték, ami hexadecimális 01-00-5E-vel kezdődik. A csoportos MAC-cím fennmaradó része úgy jön létre, hogy a csoportos IP-cím alsó 23 bitjét átalakítjuk 6 hexadecimális karakterré.

Az animáció példájában látható hexadecimális csoportcím a 01-00-5E-00-00-C8.

# Az Ethernet protokoll

## Az Ethernet MAC

**Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:**

* 1. rész: A topológia kiépítése és az eszközök kezdeti beállítása.
* 2. rész: Az eszközök konfigurálása és a kapcsolat ellenőrzése.
* 3. rész: Az Ethernet MAC-címek megjelenítése, leírása és elemzése.

[Laborgyakorlat - Viewing Network Device MAC Addresses](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.1.3.6%20Lab%20-%20Viewing%20Network%20Device%20MAC%20Addresses.pdf)

# Az Ethernet protokoll

## MAC és IP

Két fő címet rendelünk egy állomáshoz:

* fizikai címet (MAC-címet)
* logikai címet (IP-címet)

A MAC- és IP-cím közösen azonosítják be a készüléket a hálózaton. A folyamat, amelynek során a MAC-cím és az IP-cím segítségével megtalálunk egy számítógépet, hasonló ahhoz, mint amikor egy egyén nevét és címét használjuk levélküldés céljából.

Egy személy neve általában nem változik. Másrészről a személy címe lakóhelyéhez kötődik és változhat is.

Egy adott személy nevéhez hasonlóan az állomás MAC-címe sem változik, fizikailag rendelik hozzá a gép hálózati kártyájához és fizikai címként ismeretes. A fizikai cím nem változik, függetlenül attól, hogy a gép hova kerül.

Az IP-cím hasonló egy személy címéhez. Ez a cím azon alapul, hogy az állomás ténylegesen hol található. Ezt a címet felhasználva lehetséges az, hogy egy keret meghatározza azt a helyet, ahova a keretet el kell küldeni. Az IP-cím vagy hálózati cím úgynevezett logikai cím, mert logikailag rendeljük hozzá az állomáshoz. Minden állomáshoz aszerint rendeli hozzá a hálózati rendszergazda, hogy az állomás melyik helyi hálózatra csatlakozik. Az ábra annak a hierarchikus jellegét mutatja be, ahogyan egy egyént keresünk meg egy "logikai" címre alapozva. Kattintsunk az egyes csoportosításokra, hogy lássuk, a cím hogyan tevődik össze.

Mind a fizikai MAC-, mind pedig a logikai IP-cím szükséges a számítógép számára ahhoz, hogy egy hierarchikus hálózaton kommunikálni tudjon, mint ahogy egy személyről is szükséges tudni a nevét és a címét, hogy levelet tudjunk küldeni neki.

# Az Ethernet protokoll

## MAC és IP

A forrás eszköz a csomagot egy IP-cím alapján küldi el. Az egyik leggyakoribb módja annak, hogy a forrás eszköz meghatározza a cél eszköz IP-címét a DNS-szolgáltaatás (Domain Name Service), amelyben az IP-címhez egy tartománynevet társítunk. Például a www.cisco.com egyenértékű 209.165.200.225 címmel. Ez az IP-cím juttatja el a csomagot arra a hálózati helyre, ahol a cél eszköz van. A forgalomirányítók ezt az IP-címet fogják használni, hogy meghatározzák a cél eléréséhez a legjobb útvonalat. Röviden jellemezve, az IP-címzés határozza meg az IP-csomagok végpontok közötti viselkedését.

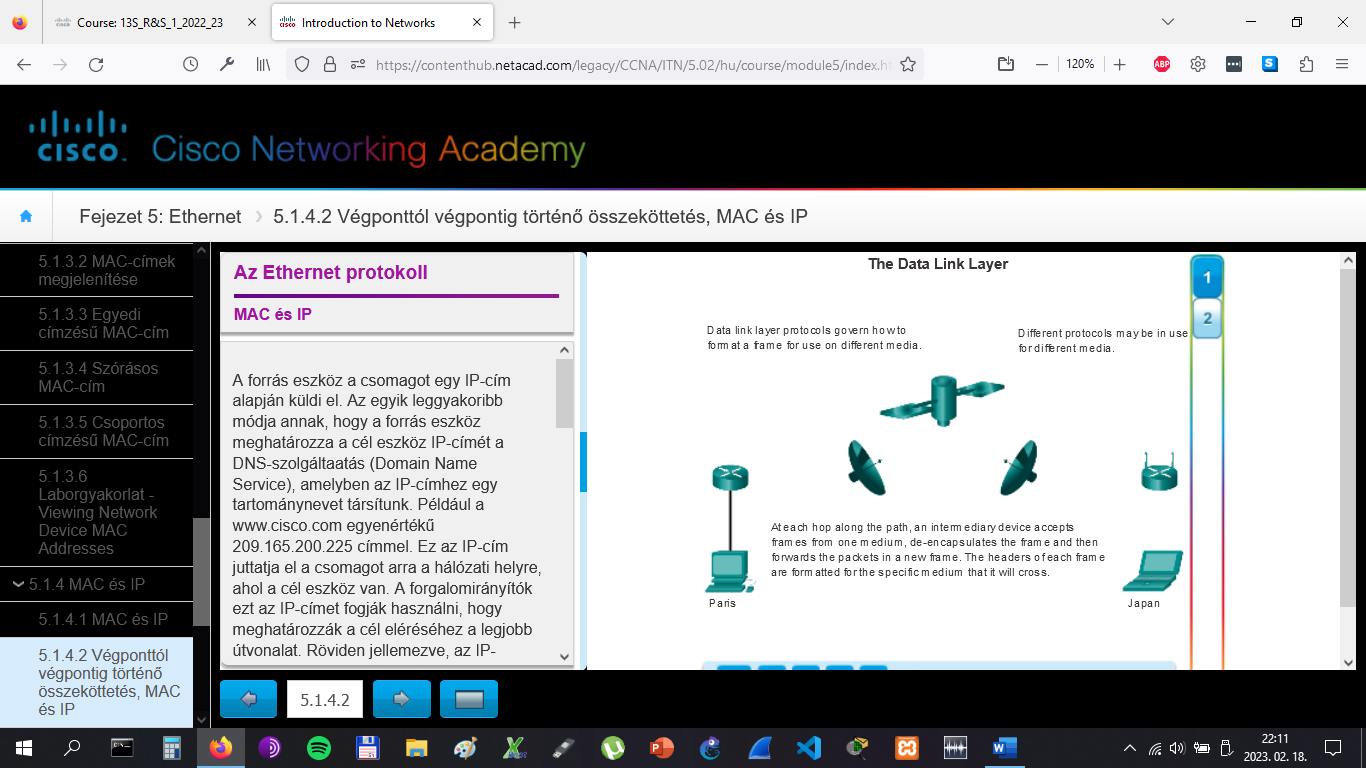
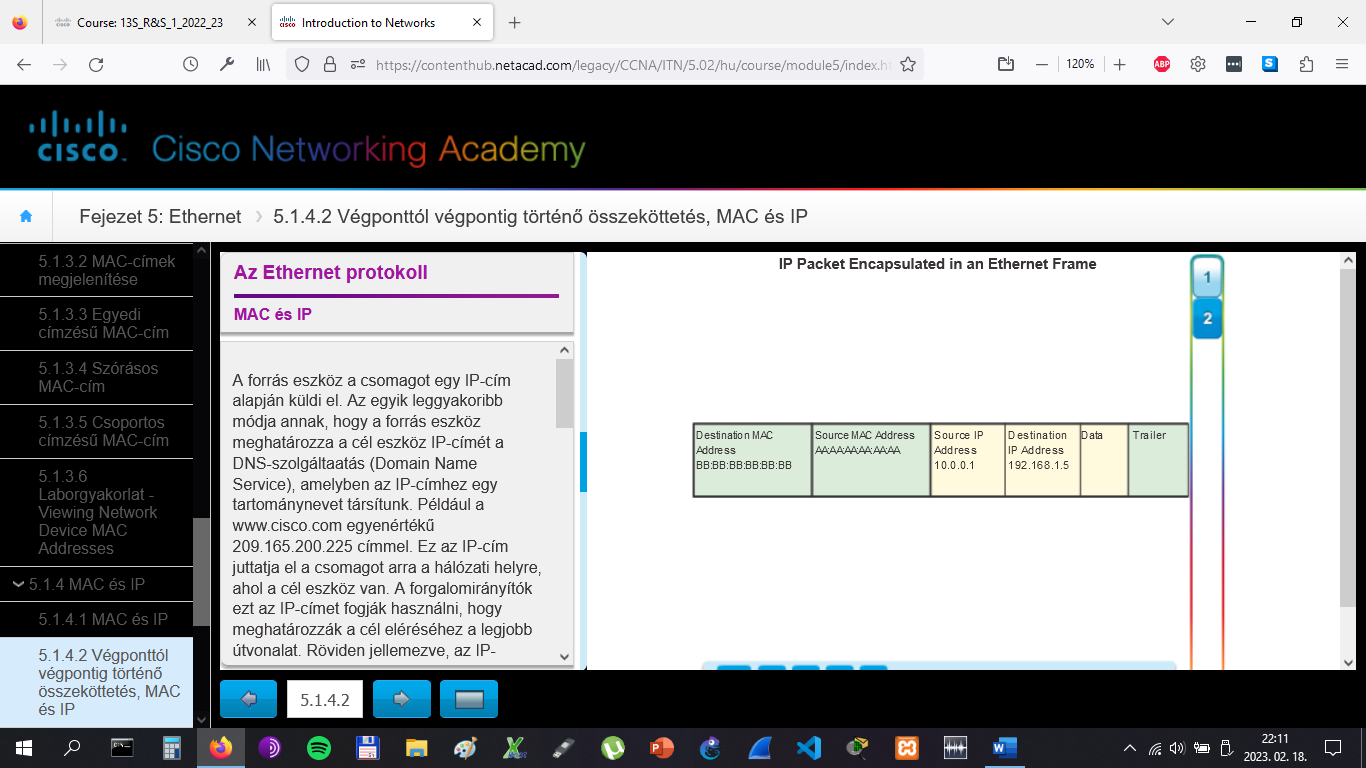
Mindamellett egy IP-csomag az útvonal mentén minden kapcsolatszakaszon külön-külön beágyazódik az arra a szakaszra jellemző keretbe, mint például amilyen az Ethernet is. Egy Ethernet hálózaton a végberendezések a kapott kereteket nem az IP-cím, hanem a MAC-cím alapján fogadják és dolgozzák fel.

Az Ethernet hálózatok a MAC-címeket használják a forrás és a cél állomások azonosítására. Amikor egy Ethernet hálózaton lévő állomás kommunikál, akkor olyan kereteket küld ki, amelyekben a saját MAC-címe a forráscím, és a kívánt címzett MAC-címe a célcím. Minden eszköz, amely a keretet megkapja kiolvassa belőle a cél MAC-címét. Az állomás kizárólag abban az esetben fogja a teljes üzenetet feldolgozni, amennyiben a cél MAC-cím megegyezik az állomás hálózati kártyáján beállított MAC-címmel.

Az 1. ábra azt mutatja, hogy egy IP-cím információkat tartalmazó adatcsomag hogyan ágyazódik be a MAC-címet is tartalmazó adatkapcsolati rétegbeli keretbe.

A 2. ábra azt szemlélteti, hogy a kereteket hogyan ágyazódnak be a tényleges kapcsolat technológiájára alapozva.

Hogyan társítjuk azonban a célhoz vezető valamennyi kapcsolaton egy adatfolyam csomagjaiban lévő IP-címeket a MAC-címekhez? Ezt a folyamatot az úgynevezett címfeloldási vagy címmeghatározó protokoll (Address Resolution Protocol, ARP) végzi.



# Az Ethernet protokoll

## MAC és IP

**Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:**

* 1. rész: Egy Ethernet II keret fejléc mezőinek vizsgálata.
* 2. rész: Wireshark használata Ethernet keretek elfogására és elemzésére.

[Laborgyakorlat - Using Wireshark to Examine Ethernet Frames](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.1.4.3%20Lab%20-%20Using%20Wireshark%20to%20Examine%20Ethernet%20Frames.pdf)

# Az Ethernet protokoll

## MAC és IP

Ezt a feladatot PDU-k megtekintésére optimalizálták. A készülékek már be vannak állítva. PDU információkat fogunk gyűjteni a szimulációs módban, és az összegyűjtött adatok alapján meg fogunk válaszolni néhány kérdést.

[Packet Tracer - Identify MAC and IP Addresses Instructions](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.1.4.4%20Packet%20Tracer%20-%20Identify%20MAC%20and%20IP%20Addresses%20Instructions.pdf)

[Packet Tracer - Identify MAC and IP Addresses - PKA](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.1.4.4%20Packet%20Tracer%20-%20Identify%20MAC%20and%20IP%20Addresses.pka)

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

Emlékezzünk vissza, hogy egy IP-hálózaton minden egyes csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Mindkét cím használata szükséges annak érdekében, hogy egy állomás adatokat küldhessen. Az állomásnak a saját MAC- és IP-címét kell használnia a forrás mezőkben, valamint meg kell adnia a célállomás MAC- és IP-címét is. Míg a cél IP-címet egy magasabb OSI-réteg fogja biztosítani, a küldő csomópontnak szüksége van egy módszerre ahhoz, hogy egy adott Ethernet kapcsolaton megtalálja a cél MAC-címét. Ez az ARP feladata.

Az ARP az Ethernet bizonyos szórásos és egyedi címzésű üzeneteire támaszkodik, az úgynevezett ARP-kérésekre és az ARP-válaszokra.

Az ARP-protokoll két alapvető funkciót biztosít:

* IPv4-címek összerendelése MAC-címekkel.
* Az összerendelési táblázat kialakítása.

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

**IPv4-címek összerendelése MAC-címekkel**

Ahhoz, hogy egy keretet a LAN átviteli közegére helyezhessünk, annak minimum egy cél MAC-címmel kell rendelkeznie. Amikor egy csomagot egy adatkapcsolati keretbe ágyazva elküldünk, az állomás a memóriájában lévő táblázatra támaszkodik, hogy megtalálja a cél IPv4-címhez tartozó adatkapcsolati rétegbeli címet. Ez a táblázat az úgynevezett ARP-táblázat vagy ARP-gyorsítótár (cache). Az ARP-táblázatot a készülék RAM-ja tárolja.

Az ARP-tábla minden bejegyzése vagy sora egy IP-címet köt össze egy MAC-címmel. A két érték közti kapcsolatot összerendelésnek vagy leképezésnek hívjuk - ez egyszerűen azt jelenti, hogy megkeresve az IP-címet a táblában megtalálhatjuk a megfelelő MAC-címet is. Az ARP-tábla csak ideiglenesen tárolja (cache-eli) a helyi LAN-eszközökhöz tartozó összerendeléseket.

A folyamat indításához a továbbító állomás megpróbálja megtalálni a cél IPv4-címhez társított MAC-címet. Ha ez az összerendelés megtalálható a táblázatban, akkor az állomás azt a MAC-címet fogja használni cél MAC-címként a keretben. A keretet ezután rákódolják a hálózati közegre.

**Az ARP-táblázat karbantartása**

Az ARP-táblázatot dinamikusan kezelik az eszközök. Két módja van, hogy egy készülék összegyűjthesse a MAC-címeket. Az egyik módszer az, hogy figyelemmel kíséri a helyi hálózati szegmensen előforduló forgalmat. Ahogy az állomás kereteket kap a közegen, a keret forrás IP- és MAC-címeit rögzíti az ARP-táblázatában. Miközben a keretek továbbításra kerülnek, addig a készülék folyamatosan fel is tölti az ARP-tábláját a megfelelő címpárokkal.

A készülék címpárokhoz jutásának egy másik módja, ha ARP-kéréseket küld ki, ahogy ezt az ábra is mutatja. Az ARP-kérés egy 2. rétegbeli szórás az Ethernet LAN minden eszközének . Az ARP-kérés tartalmazza a célállomás IP-címét és a szórásos MAC-címet, ami FFFF.FFFF.FFFF. Mivel ez egy szórás, minden állomás az Ethernet LAN-on megkapja és megnézi a tartalmát. Az az állomás fog válaszolni, amelynek az IP-címe megegyezik a kérésben lévő IP-címmel. A válasz egy egyedi címzésű keret lesz, amely magában foglalja a kérdéses IP-címhez tartozó MAC-címet is. Ezt a választ a küldő fél egy új tételként hozzá tudja majd adni ARP-táblájához.

Az ARP-táblázatban lévő bejegyzést hasonló időbélyeggel látják el, mint ahogy a kapcsolók kezelik a MAC-címtáblájuk bejegyzéseit. Ha a készülék nem kap keretet egy adott eszköztől az időbélyeg lejárta előtt, az eszközhöz tatozó bejegyzés kikerül az ARP-táblázatból.

Emellett statikus bejegyzéseket is lehet írni az ARP-táblába, de ez elég ritkán történik meg. A statikus ARP-bejegyzések nem járnak le az idő múlásával, és így kézzel kell őket eltávolítani.

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

**A keret létrehozása**

Mit tehet egy csomópont, ha egy keretet kell létrehoznia, és az ARP-cache nem tartalmaz bejegyzést a cél MAC-címhez tartozó IP-címről? Létrehoz egy ARP-kérést!

Amikor az ARP-nek meg kell állapítania egy IPv4-címhez tartozó MAC-címet, azt először az ARP-táblázatban keresi. Ha a bejegyzés nem található, az IPv4 csomag beágyazása nem sikerül és a 2. rétegbeli folyamatok értesítik az ARP-t, hogy szükség van egy új összerendelésre. Az ARP folyamat ekkor kiküld egy ARP-kérést, hogy felderítse a helyi hálózaton a cél eszköz MAC-címét. Amennyiben egy eszköz a kérésben kapott cél IP-címmel rendelkezik, akkor egy ARP-választ küld vissza. Így létrejön az összerendelés az ARP-táblázatban. Az erre az IPv4-címre szóló csomagokat immár be lehet ágyazni a keretekbe.

Ha egyetlen eszköz sem válaszol az ARP-kérésre, a csomagot eldobják, mivel a keret nem hozható létre. Ezt a beágyazási hibát jelenteni kell az eszköz felsőbb rétegei felé. Ha az eszköz egy közvetítő eszköz, például egy forgalomirányító, a felső rétegek dönthetnek úgy, hogy a forrás állomásnak egy hibát jelző ICMPv4-csomaggal válaszolnak.

Az 1-5 ábrák egy a helyi fizikai hálózaton lévő állomás MAC-címének megszerzésére alkalmazott folyamatot szemléltetik.

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

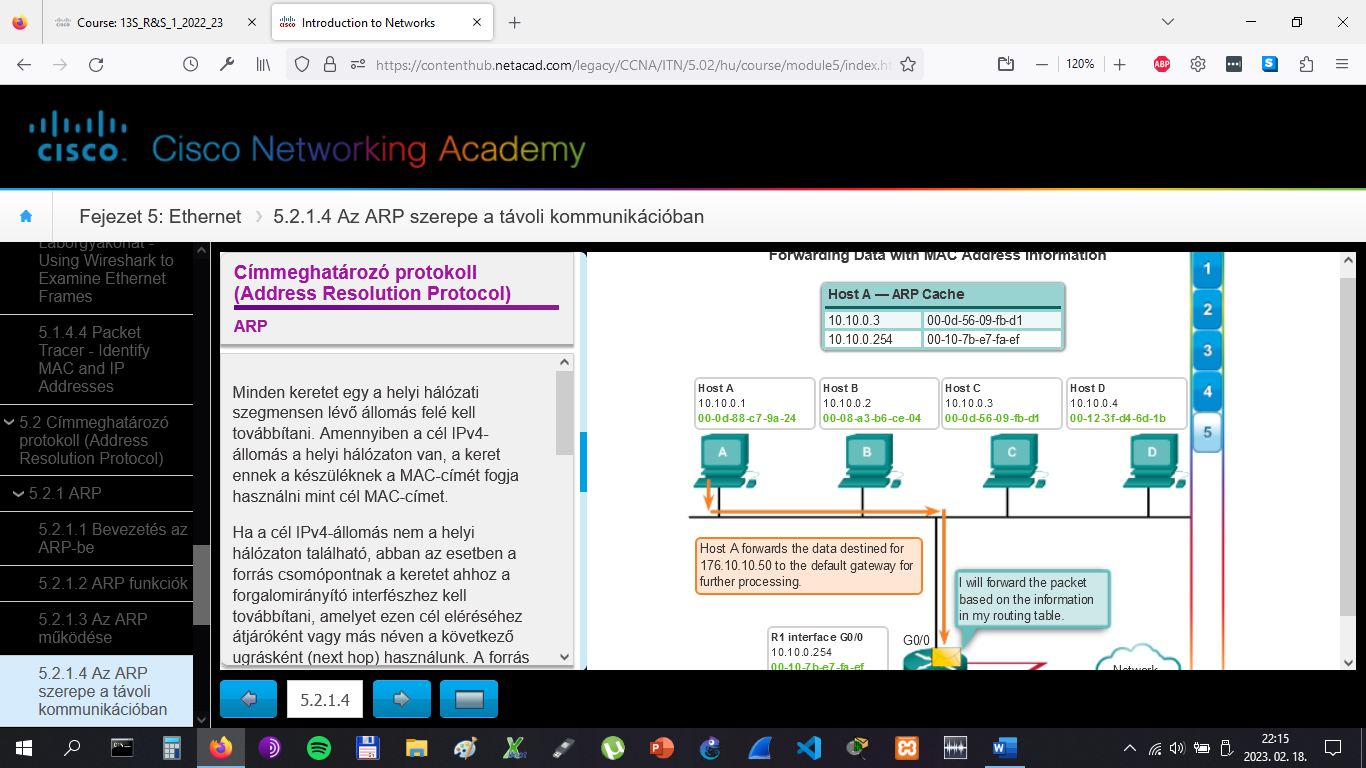
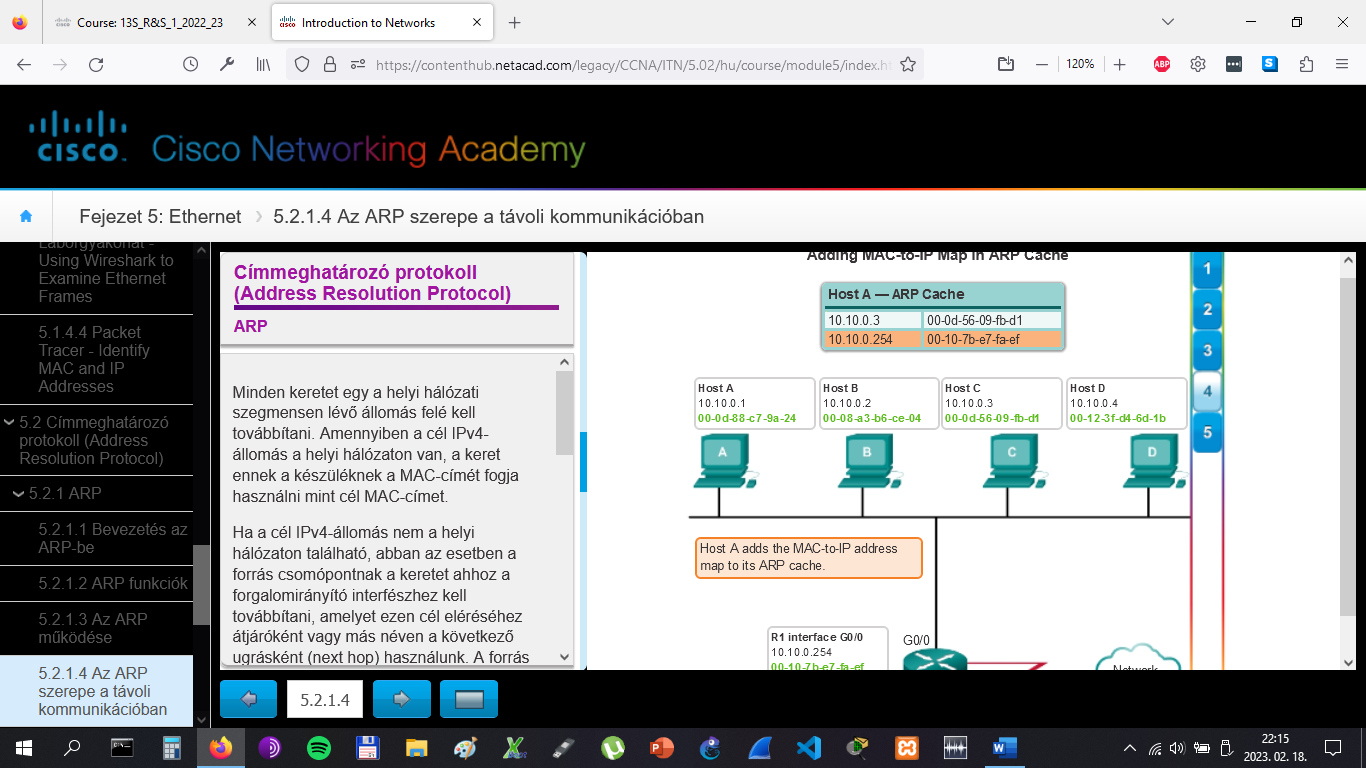
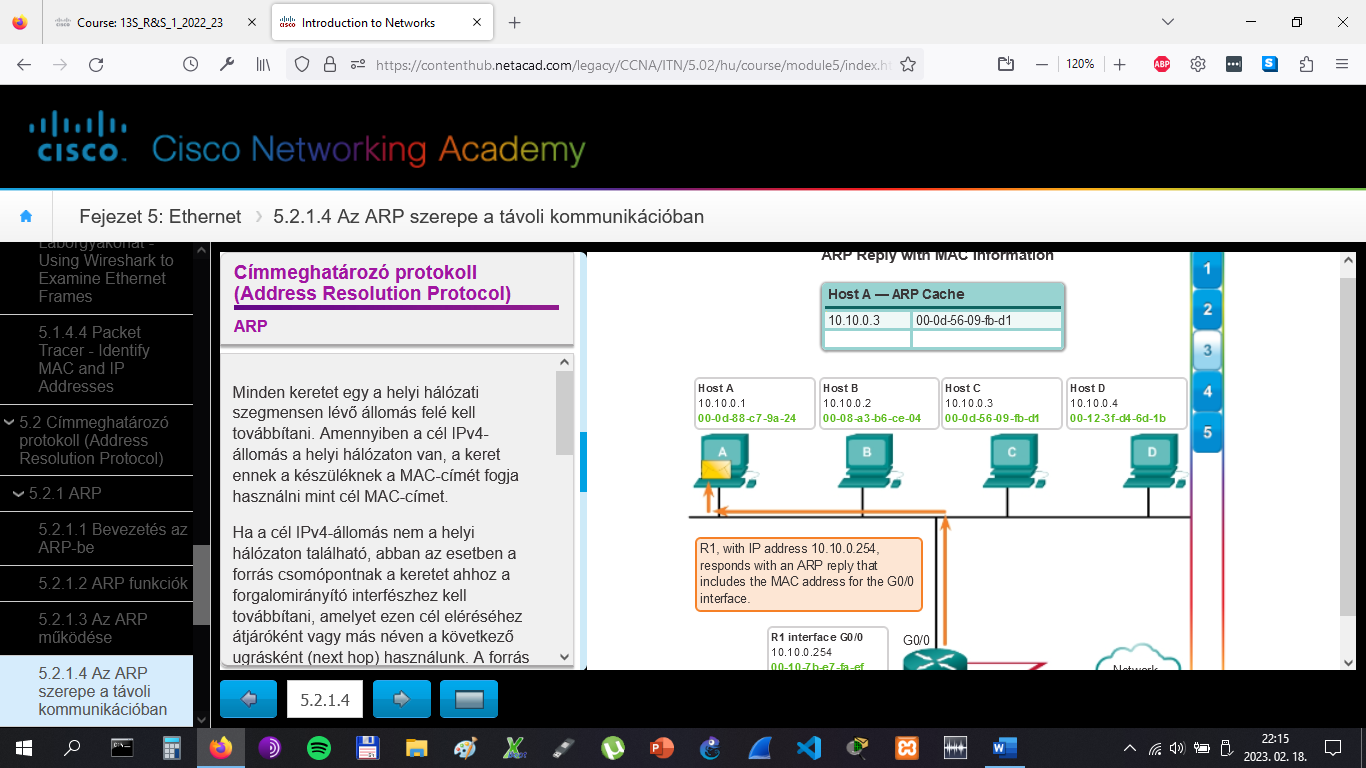
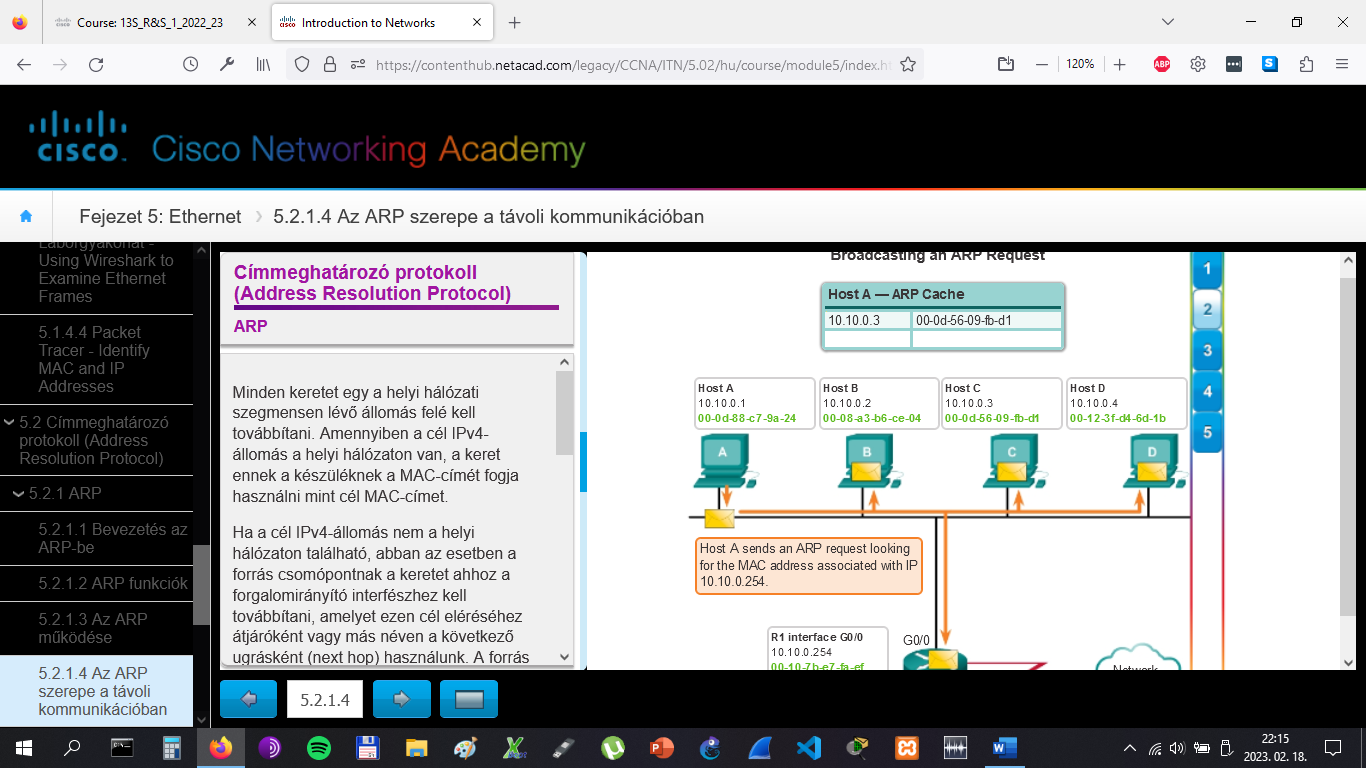
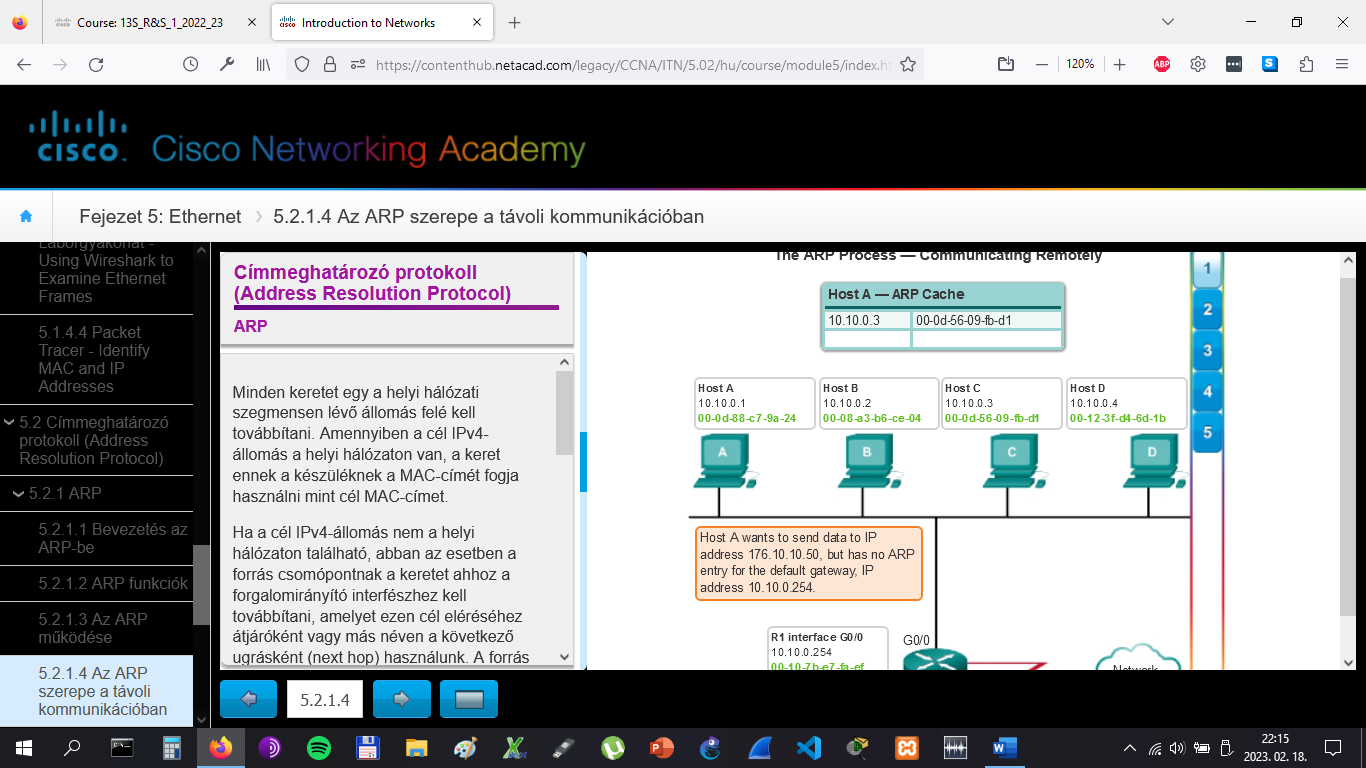
Minden keretet egy a helyi hálózati szegmensen lévő állomás felé kell továbbítani. Amennyiben a cél IPv4-állomás a helyi hálózaton van, a keret ennek a készüléknek a MAC-címét fogja használni mint cél MAC-címet.

Ha a cél IPv4-állomás nem a helyi hálózaton található, abban az esetben a forrás csomópontnak a keretet ahhoz a forgalomirányító interfészhez kell továbbítani, amelyet ezen cél eléréséhez átjáróként vagy más néven a következő ugrásként (next hop) használunk. A forrás csomópont az átjáró MAC-címét fogja használni a célállomás címeként minden olyan keret esetében, amely olyan IPv4-csomagot tartalmaz, amelyet másik hálózaton lévő állomásnak címeznek.

Az átjárónak, azaz a forgalomirányító interfészének a címét az állomások az IPv4-konfigurációjukban tárolják. Amikor az állomás létrehoz egy csomagot egy célállomásnak, összehasonlítja a cél IP-címet és a saját IP-címét annak meghatározására, hogy a két IP-cím ugyanazon a 3. rétegbeli hálózaton található-e. Ha a fogadó gép nem ugyanazon a hálózaton van, a forrás az ARP folyamatot az átjáró MAC-címének meghatározására használja.

Abban az esetben, ha az átjáró bejegyzés nem szerepel a táblázatban, a normál ARP folyamat kiküld egy ARP-kérést, hogy megszerezze a forgalomirányító interfész IP-címéhez társított MAC-címet.

Az 1-5 ábrák az átjáró MAC-címének megszerzésére alkalmazott folyamatot szemléltetik.



# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

# Egy ARP-cache időzítő távolítja el minden eszközön azokat az ARP-bejegyzéseket, amelyeket egy meghatározott idő óta nem használtak. Az időzítő függ a készüléktől és annak operációs rendszerétől. Egyes Windows operációs rendszerek például 2 percig tárolják az ARP-cache bejegyzéseket. Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

Egy Cisco forgalomirányítón a **show ip arp** parancsot használjuk az ARP-táblázat megjelenítéséhez, amint az 1. ábrán látható.

Egy Windows 7 PC-n az **arp -a** parancsot használjuk az ARP-táblázat megjelenítéséhez, amint a 2. ábrán látható.

Ha ez idő alatt a bejegyzést ismételten használják, a hozzá tartozó ARP-időzítő 10 percre meghosszabbodik.

Parancsokat is használhatunk, hogy az ARP-táblából manuálisan távolítsunk el bizonyos bejegyzéseket, vagy akár az összeset. Egy bejegyzés eltávolítása után, az ARP-kérés küldés és ARP-válasz fogadás folyamatának ismét meg kell történnie, hogy az összerendelés az ARP-táblázatba újból bekerülhessen.

Minden készülék egyedi, az operációs rendszertől függő paranccsal rendelkezik az ARP-cache tartalmának törlésére. Ezek a parancsok semmilyen módon nem eredményezik az ARP végrehajtását. Egyszerűen csak eltávolítják a bejegyzéseket az ARP-táblából. Az ARP-szolgáltatást az IPv4-protokollba integrálják és maga a készülék hajtja végre. Működése észrevehetetlen mind a felső rétegbeli alkalmazások, mind a felhasználók számára.

Amint az ábrán látható, bizonyos esetekben szükséges egy ARP-bejegyzés eltávolítása a táblából.

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP

**Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:**

* 1. rész: Felépítjük és konfiguráljuk a hálózatot.
* 2. rész: Használjuk a Windows ARP parancsát.
* 3. rész: Használjuk az IOS show arp parancsát.
* 4. rész: Wireshark-ot használunk az ARP adatcserék megvizsgálására.

[Laborgyakorlat - Observing ARP with the Windows CLI, IOS CLI, and Wireshark](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.2.1.8%20Lab%20-%20Observing%20ARP%20with%20the%20Windows%20CLI,%20IOS%20CLI,%20and%20Wireshark.pdf)

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP-vel kapcsolatos kérdések

Az ábra az ARP-hez kapcsolodó két lehetséges problémát szemléltet.

**A közeg túlterhelése**

Szórásos keret lévén egy ARP-kérést a helyi hálózaton minden eszköz megkap és feldolgoz. Egy általános üzleti hálózaton ezek a szórások valószínűleg minimális hatással vannak a hálózati teljesítményre. Ugyanakkor ha nagy számú készüléket kapcsolnak be egyszerre és az összes hálózati szolgáltatás elérése ugyanabban az időben kezdődik, a teljesítmény egy kis időre csökkenhet. Ha például a laborban minden diák egyszerre jelentkezik be a tantermi számítógépekre és próbálja meg elérni az internetet, előfordulhatnak késések. Azonban miután a készülékek kiküldték az első ARP-szórásokat és megtanulták a szükséges MAC-címeket, a későbbi tanulási folyamatok hatása már csak minimális terhelést fog jelenteni.

**Biztonság**

Bizonyos esetekben az ARP használata potenciális biztonsági kockázatot jelenthet. Az ARP-spoofing (hamisítás) vagy az ARP-mérgezés egy-egy olyan technika, amely által a támadó hamis MAC-cím összerendeléseket juttat a hálózatra hamis ARP-kérések segítségével. Ha a támadó meghamisítja egy eszköz MAC-címét, akkor azután a kereteket már nem a megfelelő helyre fogják küldeni.

Az ARP-hamisítás megakadályozásának egyik módja a manuálisan beállított statikus ARP-bejegyzések. Bizonyos hálózati eszközökön hitelesített MAC-címeket lehet beállítani, hogy a hálózati hozzáférést csak ezekre a listán szereplő eszközökre korlátozzuk.

# Címmeghatározó protokoll (Address Resolution Protocol)

## ARP-vel kapcsolatos kérdések

Az ARP-vel kapcsolatos szórási és biztonsági kérdések enyhíthetők a modern kapcsolókkal. A Cisco kapcsolók számos általános, de kifejezetten ARP jellegű biztonsági technológiát is alkalmaznak, hogy enyhítsék az Ethernet szórásokkal kapcsolatos problémákat.

A kapcsolók szegmentálást biztosítanak a LAN-on, felosztva a LAN-t önálló ütközési tartományokra. A kapcsolón minden port egy külön ütközési tartományt jelent, és biztosítja a közeg teljes sávszélességét a portra csatlakozó állomás vagy állomások számára. Bár a kapcsolók alapértelmezés szerint nem akadályozzák a szórások továbbítását, de elkülönítik az egyedi címzésű Ethernet kommunikációt, hogy azt csak a forrás és a cél eszközök "hallhassák". Tehát lehet akár nagyszámú ARP-kérés is, az ARP-válaszok mindegyike már csak két eszköz között fog létrejönni.

Tekintettel az Ethernet hálózatokon gyakori különféle szórásos támadások enyhítésére, a hálózati mérnökök különböző biztonsági beállításokkal védekezhetnek ezek ellen. Ilyenek lehetnek például a speciális hozzáférési listák és a portbiztonság alkalmazása.

# LAN-kapcsolók

## Kapcsolás

Emlékezzünk vissza, hogy egy Ethernet hálózat logikai topológiája egy többes hozzáférésű sín, amelyen az eszközök osztoznak a közeghez történő hozzáférésen. Ez a logikai topológia határozza meg, hogy a hálózaton lévő állomások hogyan látják és dolgozzák fel a küldött és fogadott kereteket. Ugyanakkor a legtöbb mai Ethernet hálózat csillag vagy kiterjesztett csillag fizikai topológiát használ. Ez azt jelenti, hogy a legtöbb Ethernet hálózaton a végberendezések jellemzően pont-pont alapon csatlakoznak egy 2. rétegbeli LAN-kapcsolóhoz.

Egy 2. rétegbeli (Layer 2) LAN-kapcsoló a kapcsolási és szűrési műveleteit kizárólag az OSI adatkapcsolati rétegbeli MAC-címek alapján végzi. A kapcsoló teljesen átlátszó - más néven transzparens - a hálózati protokollok és a felhasználói alkalmazások számára. Egy Layer 2 kapcsoló egy MAC-címtáblát épít fel, amelyet a továbbítási döntéseihez használ. A Layer 2 kapcsolók a forgalomirányítókra támaszkodnak az egymástól független IP-alhálózatok közötti adattovábbításhoz.

# LAN-kapcsolók

## Kapcsolás

A kapcsolók a MAC-címeket használják ahhoz, hogy mindig a megfelelő porton kerüljenek továbbításra a keretek a célállomás felé. A kapcsoló szerkezete az integrált áramkörökből, valamint a hozzá társuló gépi programból áll, amelyek lehetővé teszik, hogy az adatútvonalakat a kapcsolón keresztül szabályozni lehessen. Ahhoz, hogy egy kapcsoló megtudja, hogy melyik portot használja egy egyedi címzésű keret továbbításához, először meg kell tanulnia, mely állomások vannak az egyes portokon.

Egy kapcsoló a MAC-címtáblája segítségével határozza meg, hogyan kell kezelnie a beérkező adatkereteket. A kapcsoló úgy építi fel a MAC-címtábláját, hogy rögzíti a portjaihoz kapcsolódó állomások MAC-címeit. Miután a kapcsoló egyszer már egy adott porton lévő állomás MAC-címét rögzítette a címtáblájában, egy későbbi átvitel során már tudni fogja, hogy az adott állomásnak szánt forgalmat a hozzá társított porton keresztül kell továbbítania.

Amikor a kapcsoló egy bejövő adatkeretet kap, és a cél MAC-címe nem szerepel a táblázatban, a kapcsoló a keretet az összes portján keresztül kiküldi, kivéve azt a portot, amelyen a keret beérkezett. Amikor a címzett csomópont visszaválaszol, a kapcsoló rögzíti a keret forráscímét a MAC-címtáblájába. A több összekötött kapcsolót tartalmazó hálózatokban a MAC-címtáblák több MAC-címet is rögzíthetnek a kapcsolókhoz csatlakozó portokhoz, ami azt tükrözi, hogy azon a porton keresztül több állomás is elérhető. A két kapcsolót összekötő portokhoz általában több MAC-címet rögzítenek a címtáblában.

Hogy lássuk, hogyan is működik ez, tekintsük meg az egyes lépéseket az 1-6. ábrákon!

A következők írják le a folyamatot:

**1. lépés:** A kapcsoló kap egy szórásos keretet a PC1-től az 1-es porton.

**2. lépés:** A kapcsoló beírja a címtáblába a forrás MAC-címet és a portot, amelyen keresztül megkapta a keretet.

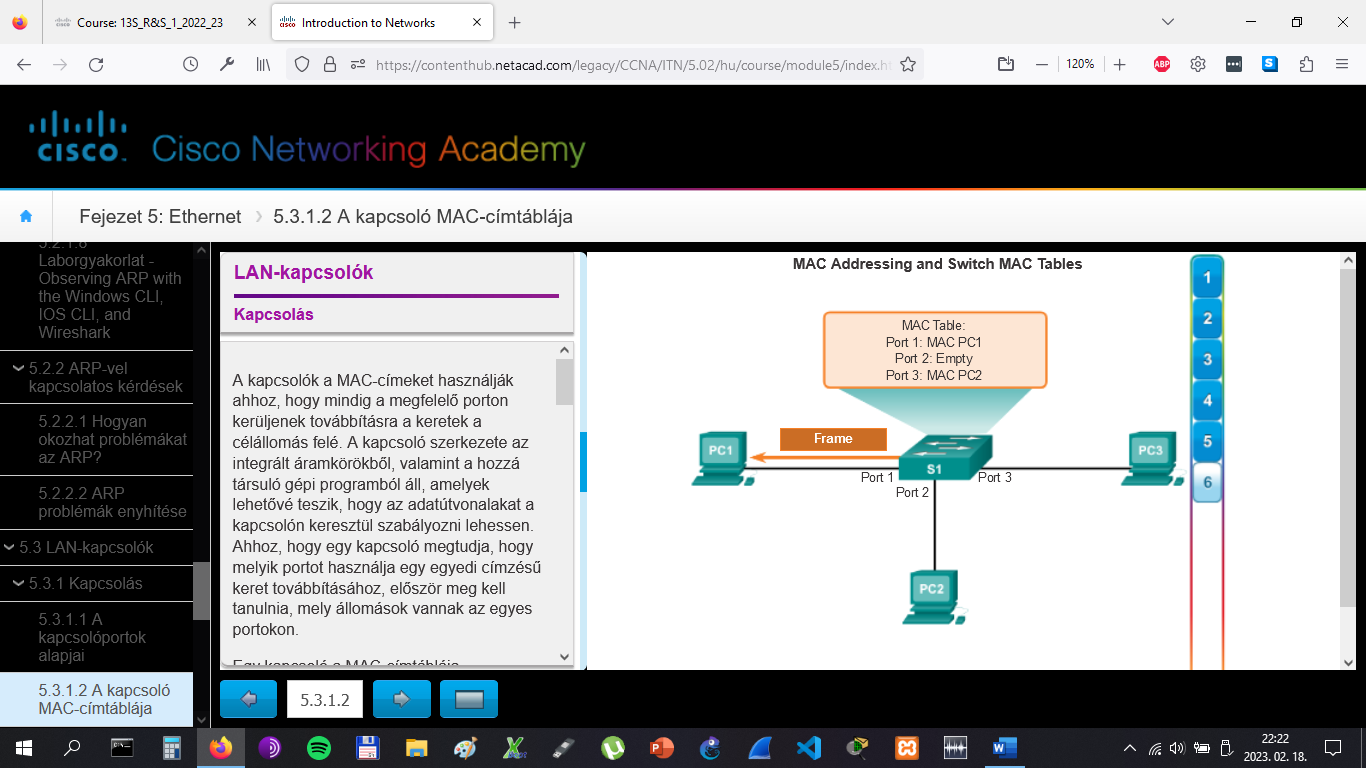
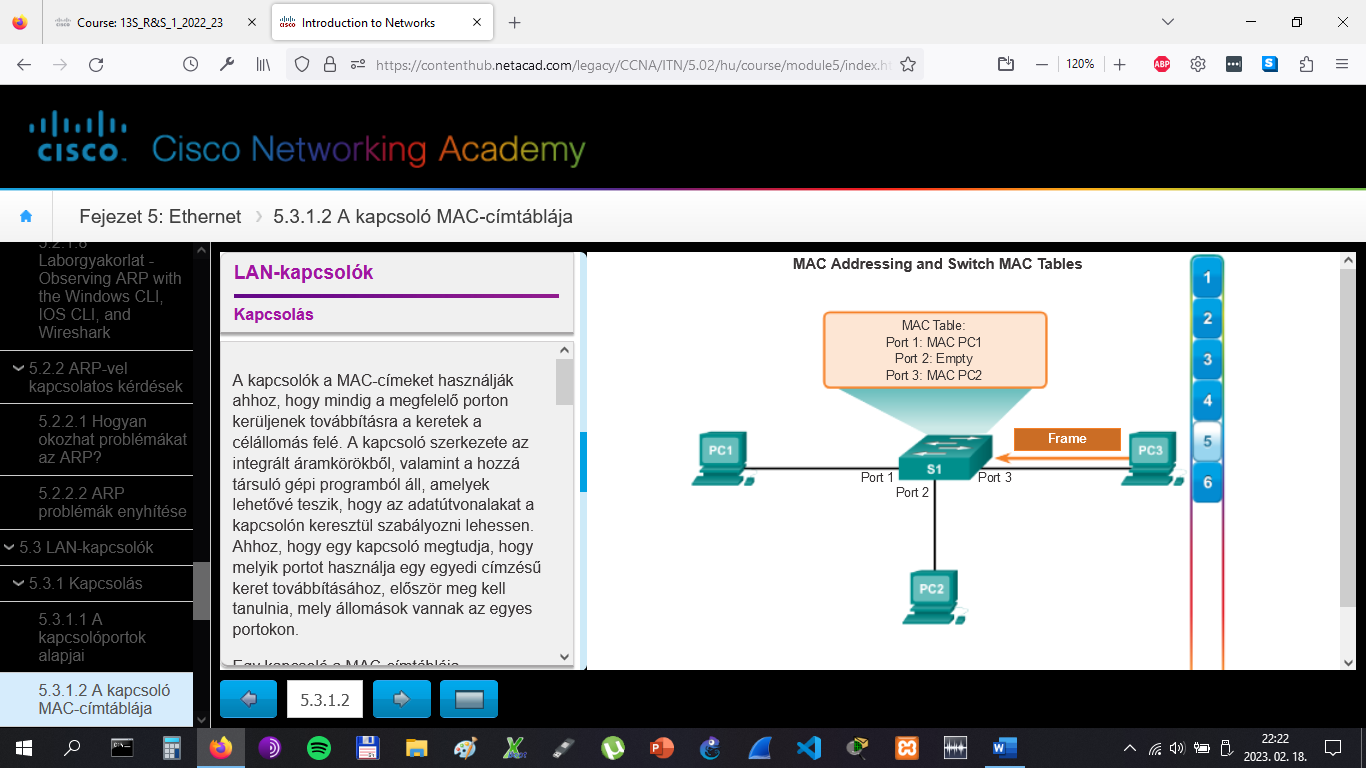
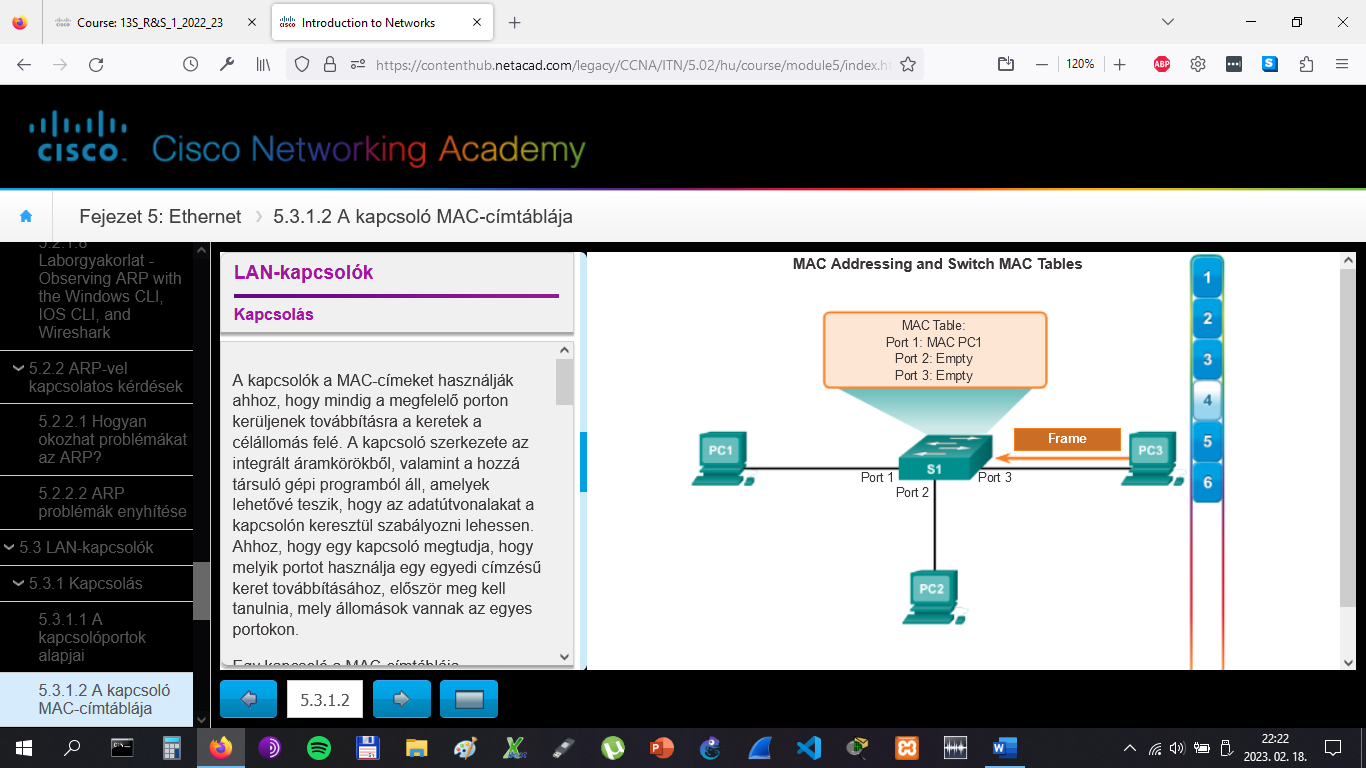
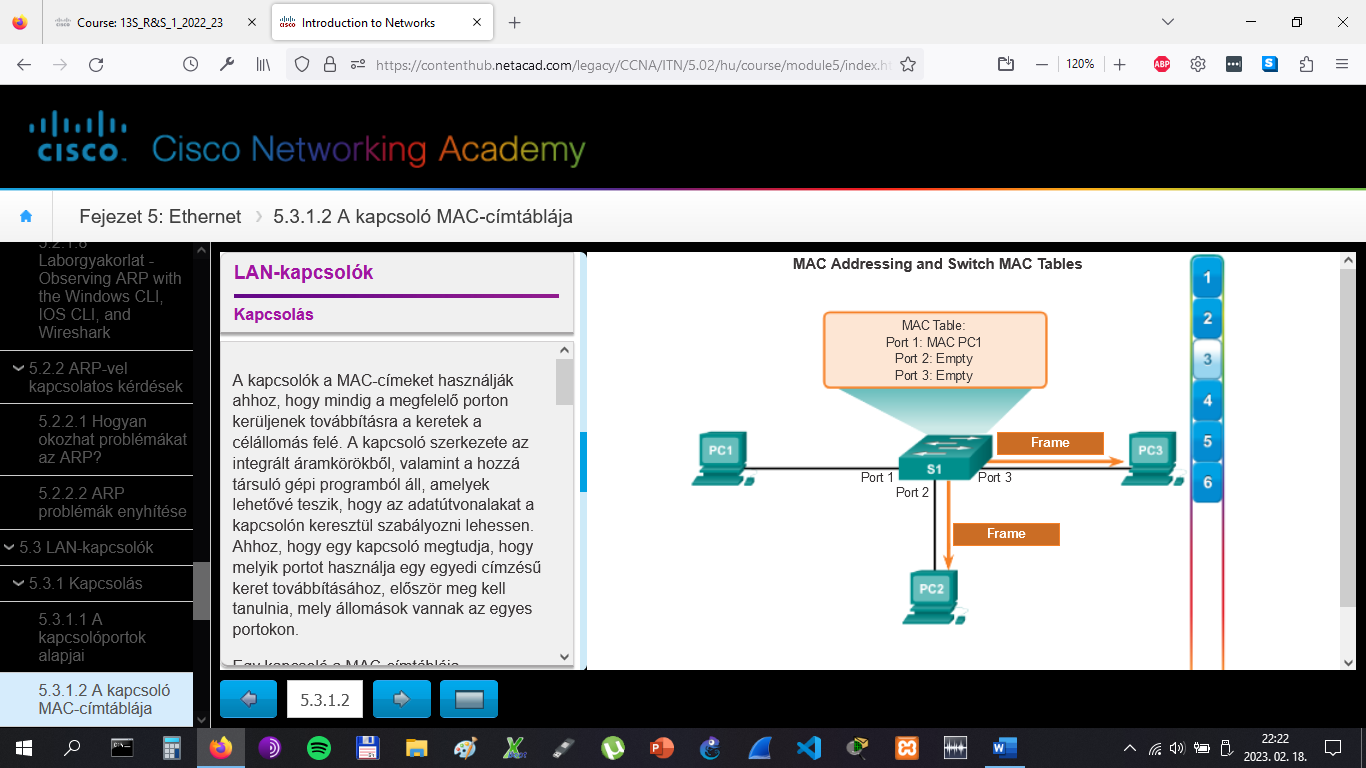
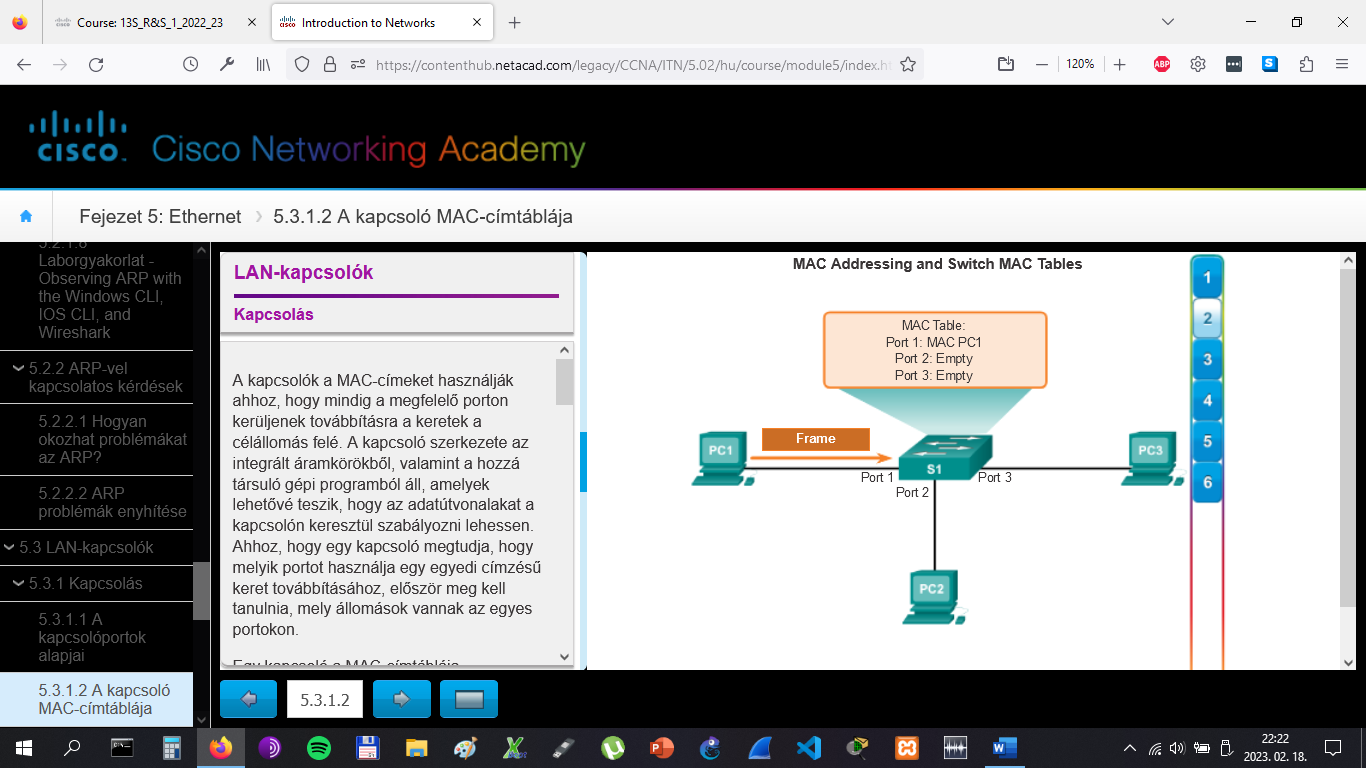
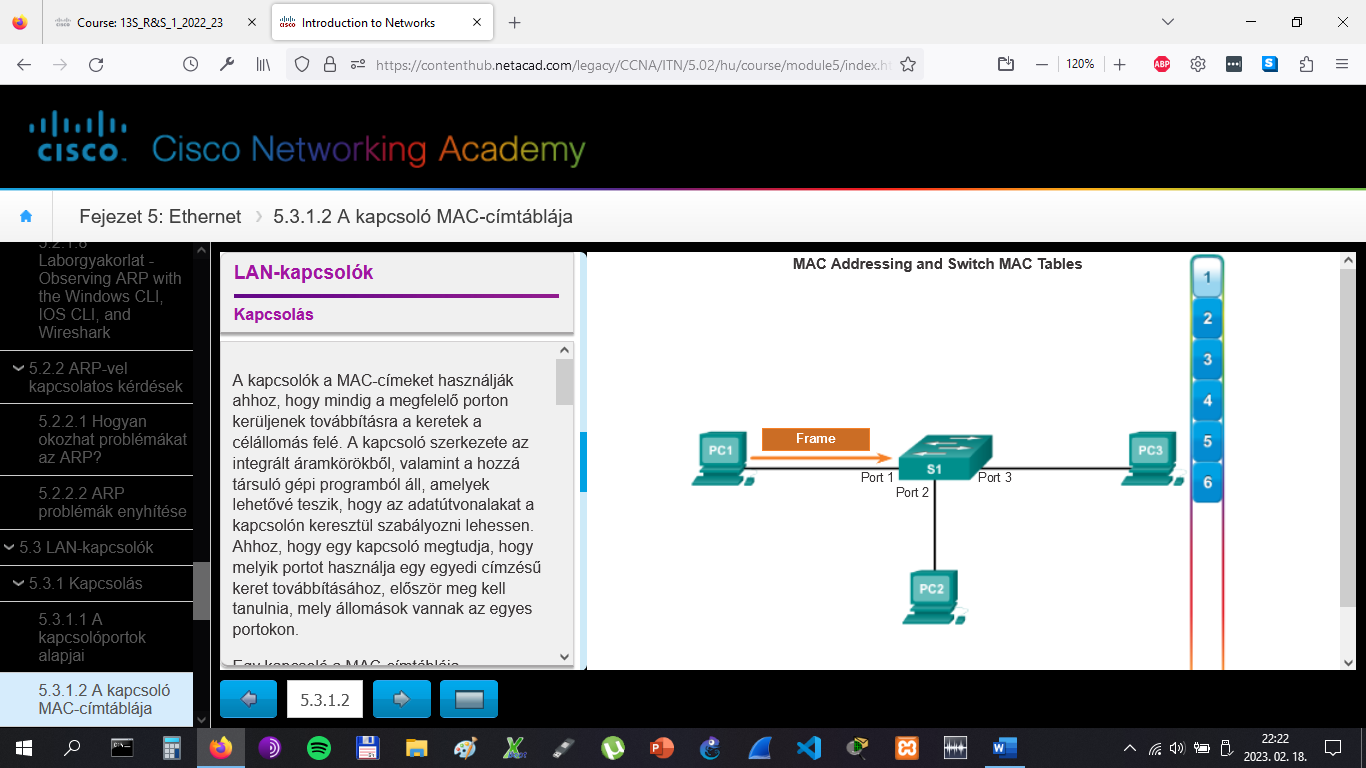
**3. lépés:** Mivel a cél cím szórásos, a kapcsoló elárasztja a kerettel az összes portot, kivéve azt, amelyen megkapta a keretet.

**4. lépés:** A cél eszköz egy egyedi címzésű kerettel válaszol, melynek címzettje a PC1.

**5. lépés:** A kapcsoló beírja a címtáblájába a PC2 forrás MAC-címét és annak a portnak a számát, amelyen át megkapta a keretet. A keret célcíme és a hozzá kapcsolódó port már megtalálhatók a MAC-címtáblában.

**6. lépés:** A kapcsoló most már elárasztás nélkül képes továbbítani a kereteket a forrás és a cél között, mert már megvannak a kapcsolóportokat beazonosító címtála bejegyzések.

**Megjegyzés**: A MAC-címtáblát gyakran nevezik tartalom szerint címezhető memória (Content Addressable Memory, CAM) táblázatnak is. Bár a CAM-tábla kifejezés meglehetősen gyakori, ebben a kurzusban MAC-címtáblaként hivatkozunk rá.



# LAN-kapcsolók

## Kapcsolás

Bár a kapcsolók transzparensek a hálózati protokollok és a felhasználói alkalmazások számára, különböző olyan módokban képesek működni, amiknek pozitív és negatív hatásai is vannak, amikor Ethernet kereteket továbbítanak a hálózaton. A kapcsoló minden egyes portjának az egyik alapvető beállítása a duplexitás. A kapcsoló egy portját úgy kell beállítani, hogy az megfeleljen a közegtípus duplexitási beállításainak. Az Ethernet hálózatokon történő kommunikációra kétféle duplexitási beállítást használunk: fél-duplex és teljes duplex.

**Fél-duplex**

A fél-duplex kommunikáció egyirányú adatfolyamokon alapszik, ahol az adatok küldését és fogadását nem ugyanabban az időben végzik. Ez hasonló ahhoz, ahogyan a walkie-talkie vagy kétirányú rádiók működnek, ahol egy időben csak egy ember beszélhet. Ha valaki beszélne, miközben már valaki más is beszél, akkor ütközés következik be. Ennek eredményeként a fél-duplex kommunikáció a CSMA/CD módszert hívja segítségül a lehetséges ütközések csökkentésére és felismerésére. A fél-duplex kommunikáció teljesítménybeli problémákkal küzd az állandó várakozás miatt, mivel az adatok egy időben csak egy irányban áramolhatnak. A fél-duplex kapcsolatokat tipikusan a régebbi hardvereken találjuk meg, mint például a hub-okon. A hub-okhoz csatlakozó állomások egymással osztozva férnek hozzá a közeghez, ezért hogy képesek legyenek felismerni az ütközéseket, fél-duplex módban kell működniük. Az állomásoknak akkor is fél-duplex módban kell működniük, ha a hálózati kártyájuk nem támogatja a teljes duplex működési módot. Ebben az esetben a kapcsoló portja is alapértelmezés szerint fél-duplex módban van. Ezen korlátozások miatt a legtöbb modern hardveren a teljes duplex kommunikáció váltotta fel a fél-duplexet.

**Teljes duplex**

A teljes duplex (full-duplex) kommunikációnál az adatáramlás kétirányú, így az adatok ugyanabban az időben küldhetők és fogadhatók is. A kétirányúság azáltal javítja a teljesítményt, hogy az átvitelek között csökkenti a várakozási időt. A legtöbb ma forgalomban lévő Ethernet, FastEthernet és Gigabit Ethernet hálózati csatoló (NIC) teljes duplex képességgel rendelkezik. Full-duplex módban az ütközést érzékelő áramkör le van tiltva. A két csatlakozó végpont keretei nem tudnak ütközni, mert az állomások két külön áramkört használnak a hálózati kábelen. Minden full-duplex kapcsolat csak egy portot használ. A full-duplex kapcsolatok olyan kapcsolót igényelnek, amely támogatja a full-duplex módot, vagy olyan közvetlen kapcsolatot két állomás között, ahol mindkét fél támogatja a full-duplex módot. Azokat az állomásokat, amelyek közvetlenül kapcsolódnak egy dedikált kapcsolóportra és a hálózati kártyájuk is támogatja a teljes duplex módot, olyan portra kell csatlakoztatni, ami full-duplex módra van beállítva.

Az ábrán a modern hálózati berendezéseken rendelkezésre álló két duplexitási beállítás látható.

Egy Cisco Catalyst kapcsoló három duplex beállítást támogat:

* A full opció beállítja a full-duplex módot.
* A half opció beállítja a fél-duplex üzemmódot.
* Az auto opció beállítja a duplex mód automatikus egyeztetését. Ha engedélyezett az automatikus egyeztetés, a két port kommunikációja dönti el a legjobb üzemmódot.

A FastEthernet és 10/100/1000 portokon az auto az alapértelmezett. A 100BASE-FX portokon a full az alapértelmezés. A 10/100/1000 portok működhetnek fél- vagy teljes duplex módban is, ha 10 vagy 100 Mb/s-ra vannak állítva, de amikor 1000 Mb/s-ra, akkor csak teljes duplex módban működhetnek.

# LAN-kapcsolók

## Kapcsolás

Amellett, hogy a megfelelő duplex beállítással rendelkezünk, az is szükséges, hogy minden porthoz a megfelelő típusú kábelt használjuk. Bizonyos eszközök összekapcsolásához (például kapcsoló-kapcsoló, kapcsoló-forgalomirányító, kapcsoló-állomás és forgalomirányító-állomás között) adott típusú kábel használata szükséges (kereszt- vagy egyeneskötésű). Ugyanakkor a legtöbb Cisco kapcsoló ma már támogatja az **mdix auto** interfész konfigurációs CLI-parancsot az automatikus közegfüggő interfész (Media Dependent Interface crossover, auto-MDIX) funkció engedélyezéséhez.

Amikor az Auto-MDIX funkciót bekapcsoljuk, a kapcsoló érzékeli a réz alapú Ethernet csatlakozáshoz szükséges kábeltípust és megfelelően bekonfigurálja az interfészeket. Ezért függetlenül a kapcsolat másik végén lévő készülék típusától, keresztkötésű és egyeneskötésű kábelt is használhatunk a kapcsoló 10/100/100 réz alapú portjaihoz.

Az automatikus MDIX-funkció alapértelmezés szerint engedélyezett a Cisco IOS 12.2(18)SE vagy újabb verziót futtató kapcsolókon. A Cisco IOS 12.1(14)EA1 és 12.2(18)SE kiadások között az automatikus MDIX-funkció alapértelmezés szerint tiltott.

# LAN-kapcsolók

## Kapcsolás

A múltban a kapcsolók az alábbi továbbítási módszerek valamelyikét használták az adatok hálózati portok közötti kapcsolásához:

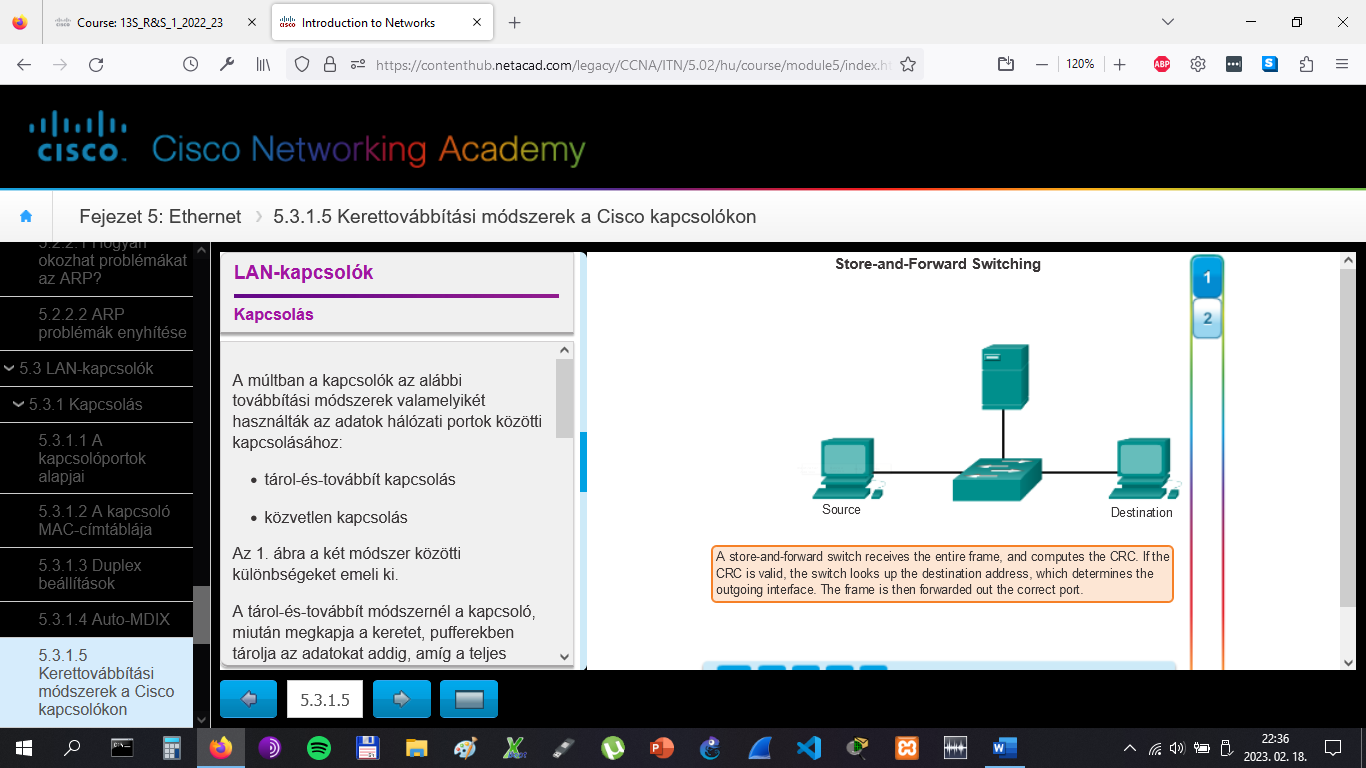
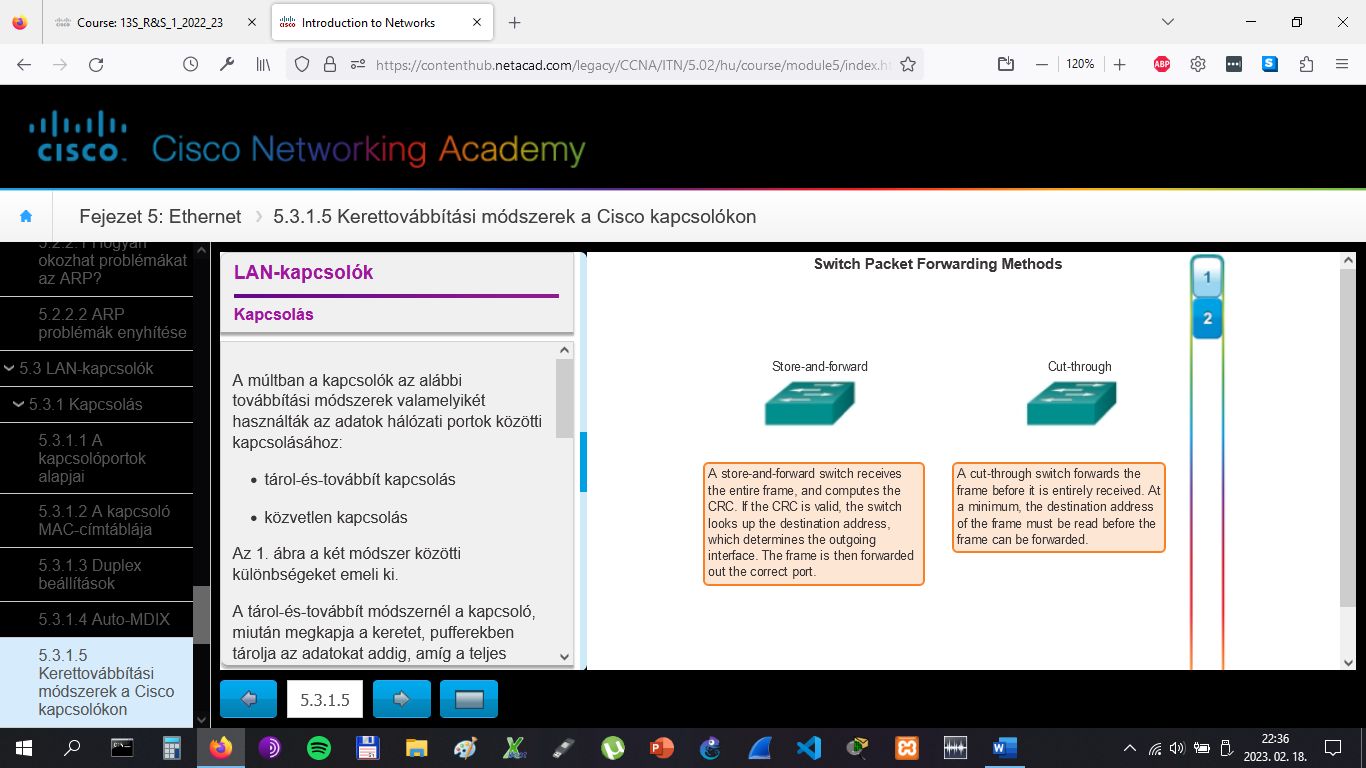
* tárol-és-továbbít kapcsolás
* közvetlen kapcsolás

Az 1. ábra a két módszer közötti különbségeket emeli ki.

A tárol-és-továbbít módszernél a kapcsoló, miután megkapja a keretet, pufferekben tárolja az adatokat addig, amíg a teljes keret meg nem érkezik. A tárolás során a kapcsoló elemzi a keret információit a rendeltetési hely megállapításához. Ebben a folyamatban a kapcsoló egy hibaellenőrzést is végrehajt az Ethernet keret CRC (Cyclic Redundancy Check) utótagját felhasználva.

A CRC egy matematikai képletet használ a keretben lévő bitek száma (1-esek) alapján annak meghatározására, hogy a fogadott keretben van-e hiba. Miután a keret sértetlensége megerősítést nyert, továbbítja azt a megfelelő portra a rendeltetési hely felé. Ha a kapcsoló hibát észlel a keretben, akkor eldobja azt. A hibás keretek eldobása csökkenti a sértetlen keretek számára rendelkezésre álló sávszélességet. A konvergált hálózatokban tárol-és-továbbít kapcsolásra van szükség a szolgáltatásminőség (Quality of Service, QoS) biztosítására, ahol a forgalom prioritásának meghatározásához szükséges a keretek osztályozása. Az IP-alapú hangátvitel (Voice over IP, VoIP) számára például elsőbbséget kell biztosítani a web-böngészési forgalommal szemben.

Játsszuk le az animációt a 2. ábrán a tárol-és-továbbít folyamat bemutatásához. A tárol-és-továbbít az egyetlen továbbítási módszer a jelenlegi Cisco Catalyst kapcsolómodelleken.



# LAN-kapcsolók

## Kapcsolás

A közvetlen kapcsolás esetén amint megérkezik az adat, a kapcsoló máris cselekszik, még ha az átvitel nem is teljes. A kapcsoló csak annyit tárol el a keretből, hogy ki tudja olvasni a cél MAC-címet annak meghatározásához, hogy melyik porton kell továbbítania az adatokat. A cél MAC-címe a keret első 6 bájtjában található, az előtagot követően. A kapcsoló megnézi a cél MAC-címet a kapcsolási táblájában, meghatározza a kimenő interfészt és továbbítja a keretet a rendeltetési helyére a kijelölt porton keresztül. A kapcsoló nem végez semmilyen hibaellenőrzést a kereten. Mivel a kapcsolónak nem kell megvárnia a keret teljes pufferelését, és mivel nem végez hibaellenőrzést, a közvetlen kapcsolás gyorsabb, mint a tárol-és-továbbít kapcsolás. Mivel azonban a kapcsoló nem végez hibaellenőrzést, a hibás kereteket is továbbítja a hálózaton keresztül. A hibás keretek a továbbításuk során sávszélességet használnak el. A cél NIC végül eldobja ezeket.

Játsszuk le az animációt a közvetlen kapcsolási folyamat bemutatásához!

A közvetlen kapcsolásnak két változata van:

* **Gyorskapcsolás**: A gyorskapcsolás esetén a legkisebb a késleltetés. A gyorskapcsolás a célcím kiolvasása után azonnal továbbítja a csomagot. Mivel a gyorskapcsolás a teljes csomag beérkezése előtt elkezdődik, lehet, hogy a csomagokat hibásan továbbítjuk. Ez ritkán történik meg, és a fogadó hálózati kártya a beérkező hibás kereteket egyébként is figyelmen kívül hagyja. Gyorstovábbító módban a késleltetést az első beérkezett bittől az első elküldött bitig számítjuk. A gyorskapcsolás a tipikus módszer közvetlen kapcsolás esetén.
* **Töredékmentes kapcsolás**: A töredékmentes kapcsoláskor a kapcsoló még a keret továbbítása előtt eltárolja az első 64 bájtot. A töredékmentes kapcsolás tulajdonképpen egy kompromisszum a tárol-és-továbbít kapcsolás, valamint a gyorskapcsolás között. Az ok, amiért a töredékmentes kapcsolás a keret első 64 bájtját tárolja el, hogy a legtöbb hálózati hiba és ütközés az első 64 bájt továbbítása alatt történik. A töredékmentes kapcsolás megpróbálja kibővíteni a gyorskapcsolást egy kisebb hibaellenőrzés elvégzésével a keret első 64 bájtján annak érdekében, hogy megbizonyosodjon, nem történt-e ütközés a keret továbbítása előtt. A töredékmentes kapcsolás tehát kompromisszum a nagy késleltetésű, de magas integritást nyújtó tárol-és-továbbít módszer, valamint az alacsony késleltetésű és csökkentett integritású gyorskapcsolás között.

Az ábra a közvetlen kapcsolásra mutat példát.

Bizonyos kapcsolók portonkénti közvetlen kapcsolásra vannak beállítva mindaddig, amíg a hibák száma el nem ér egy a felhasználó által definiált hibaküszöb szintet, ami után automatikusan átvált tárol-és-továbbít módra. Amikor a hibaarány a küszöbérték alá csökken, a port automatikusan visszavált közvetlen kapcsolásra.

# LAN-kapcsolók

## Kapcsolás

Mint említettük, egy kapcsoló megvizsgálja a kereteket vagy esetleg csak néhányat közülük, mielőtt azokat továbbítaná a célállomáshoz. Egy Ethernet kapcsoló különböző pufferelési technikákat alkalmazhat a keretek továbbítás előtti tárolására. A pufferelést abban az esetben is lehet alkalmazni, ha a célport egy esetleges torlódás miatt foglalt, és ilyenkor a kapcsoló a keretet eltárolja egészen addig, amíg azt továbbítani nem lehet.

Amint az ábrán látható, két módszer létezik memória pufferelésre: a port-alapú és az osztott.

**Port-alapú memória pufferelés**

A port-alapú memória pufferelésnél a kereteket várósorokban tároljuk, amelyek az adott bejövő és kimenő portokhoz kapcsolódnak. Egy keret csak akkor kerül át a kimeneti portra, ha a sorban előtte álló keretek már mind sikeresen továbbítódtak. Előfordulhat, hogy egyetlen keret késlelteti a memóriában lévő összes többi keret átvitelét egy foglalt kimeneti port miatt. Ez a késleltetés akkor is fellép, ha a többi keretet szabad portokra lehetne továbbítani.

**Osztott memória pufferelés**

Az osztott memória pufferelés minden keretet egy közös memória pufferbe helyez el, amelyen az összes port osztozik. Egy port számára szükséges memóriamennyiség kiosztása dinamikusan történik. A keretek a pufferben a célportokhoz dinamikusan kapcsolódnak. Ez teszi lehetővé, hogy anélkül lehessen fogadni a csomagokat az egyik porton majd továbbítani egy másikon, hogy egy másik sorba kellene áthelyezni őket.Ez teszi lehetővé azt, hogy a csomagokat anélkül lehessen az egyik porton fogadni majd egy másikon továbbítani, hogy egy másik sorba át kellene helyezni őket.

A kapcsoló egy nyilvántartást vezet a keret-port kapcsolatokról, amely megmutatja, hogy egy csomagot hol kell továbbítani. A keret sikeres továbbítása után törlődik ez a megfeleltetés. A pufferben tárolható keretek számát csak a teljes memóriapuffer mérete korlátozza, és az nem korlátozza le egyetlen portpuffer mérete. Így nagyobb keretek is továbbíthatók, és kevesebb keretet kell eldobni. Ez különösen fontos aszimmetrikus kapcsolás esetén. Az aszimmetrikus kapcsolás különböző portokon különböző adatátviteli sebességet biztosít. Ez lehetővé teszi nagyobb sávszélesség biztosítását bizonyos portoknak, mint például a szerverhez csatlakozó port.

# LAN-kapcsolók

## Fix vagy moduláris

Amikor kiválasztunk egy kapcsolót, fontos, hogy megértsük a kapcsoló legfontosabb jellemzőit és lehetőségeit. Ez azt jelenti, hogy olyan funkciókról kell dönteni, mint például hogy szükség van-e a Power over Ethernet-re (PoE), és hogy mi a kívánt továbbítási sebesség.

Amint az 1. ábrán látható, a PoE lehetővé teszi, hogy egy kapcsoló a meglévő Ethernet-kábelezésen keresztül biztosítson tápfeszültséget eszközöknek, mint például az IP-telefonok és egyes vezeték nélküli hozzáférési pontok. Ez nagyobb rugalmasságot tesz lehetővé a telepítéskor.

A továbbítási sebesség határozza meg egy kapcsoló feldolgozási képességeit, rangsorolva, hogy mennyi adatot képes feldolgozni másodpercenként. A kapcsolók termékcsaládját a továbbítási ráták alapján sorolják be. A belépő szintű kapcsolók alacsonyabb továbbítási rátákkal rendelkeznek, mint a vállalati szintű kapcsolók. Egyéb szempontok közé tartozik, hogy az eszközök egymáshoz köthetők-e (stackable), hogy mekkora egy kapcsoló magassága (ezt számszerűen rack-egységben, vagy unit-ban fejezik ki), valamint hogy mekkora a kapcsoló portsűrűsége (mennyi a kapcsolón a rendelkezésre álló portok száma). Egy eszköz portsűrűsége attól függően változhat, hogy az eszköz rögzített konfigurációjú vagy moduláris készülék.

Ezeket a tulajdonságokat néha a kapcsoló formai tényezőinek (form factor) nevezik.

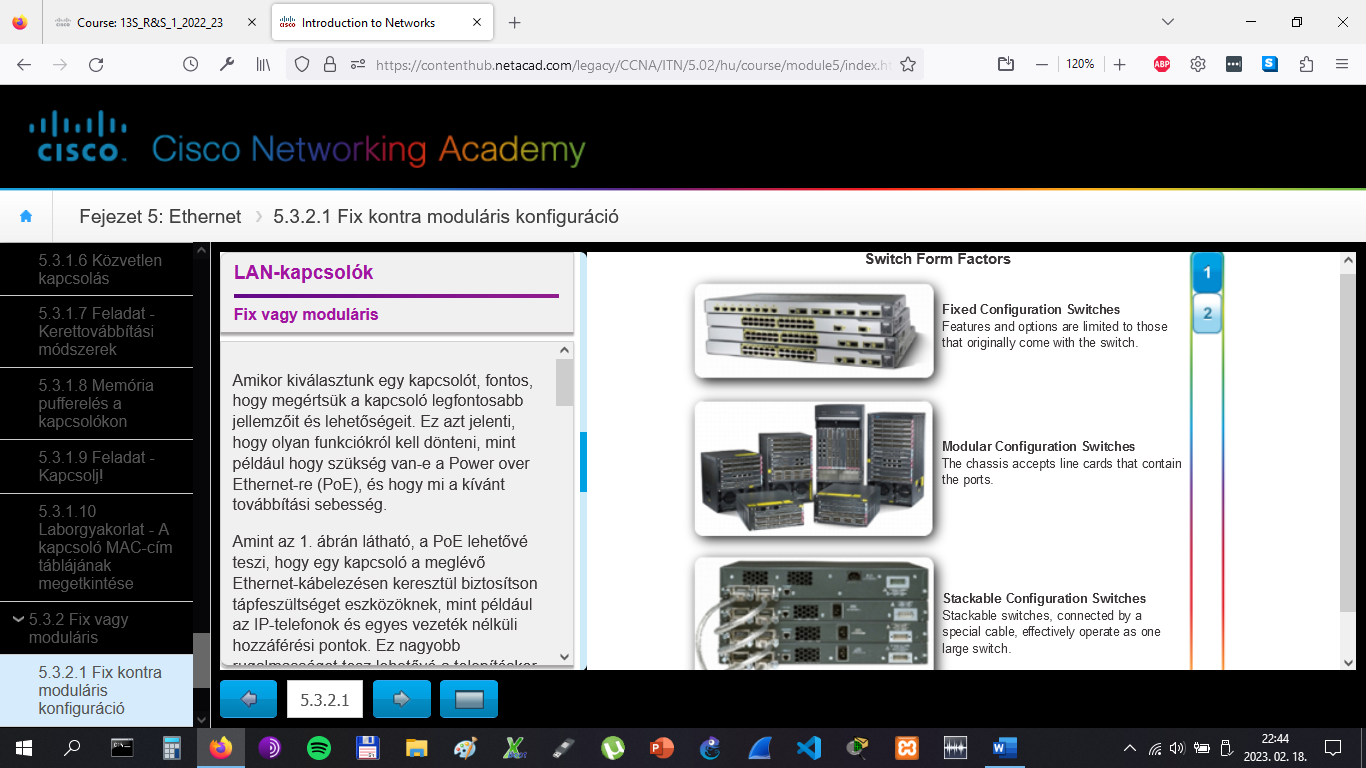
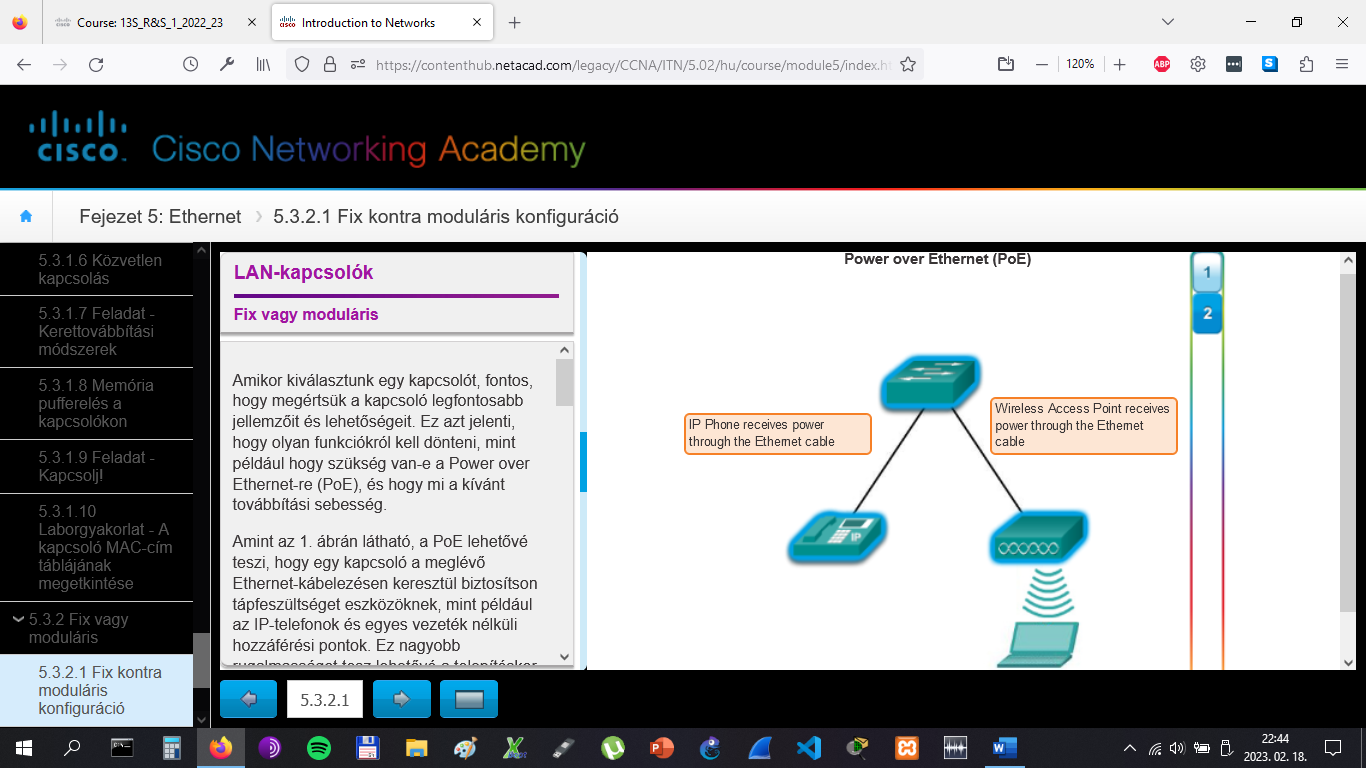
**Rögzített konfigurációjú kapcsolók**

A rögzített konfigurációjú kapcsolók - ahogy a nevük is utal rá - fix kiépítettséggel rendelkeznek. Ez azt jelenti, hogy nem lehet funkciókat és beállításokat hozzáadni a kapcsolóhoz azon túl, mint amivel eredetileg rendelkezett. A konkrét megvásárolt modell meghatározza a rendelkezésre álló funkciókat és lehetőségeket. Ha például vásárolunk egy 24 portos fix kiépítettségű gigabites kapcsolót, akkor szükség esetén azt nem lehet további portokkal bővíteni. Vannak jellemző kiépítettségű modellek (például 24 vagy 48 portos kapcsoló), amelyek aszerint változnak, hogy hány és milyen típusú portjaik van.

**Moduláris kapcsolók**

A moduláris kapcsolók kiépítettségükben nagyobb rugalmasságot biztosítanak. A moduláris kapcsolók általában különböző méretű házzal érkeznek, amely lehetővé teszi különböző számú moduláris vonali kártya telepítését. A vonali kártyák tartalmazzák tulajdonképpen a portokat. A vonali kártya úgy illeszkedik a kapcsoló házába, mint ahogy a bővítőkártyák illeszkednek a PC-be. Minél nagyobb a ház, annál több modult támogat. Mint az a 2. ábrán látható, számos különböző méretű készülékház közül lehet választani. Ha vásároltunk egy moduláris kapcsolót egy 24 portos vonali kártyával, akkor ahhoz könnyen hozzá lehet adni még egy további 24 portos vonali kártyát, így az összes port száma már 48 lesz.

A 2. ábra példákat mutat a fix, moduláris és egymáshoz köthető konfigurációjú kapcsolókra.



# LAN-kapcsolók

## Fix vagy moduláris

A Cisco kapcsolók termékcsaládjait világszerte széles körben alkalmazzák, nagy részben azért, mert rugalmasságot biztosítanak a bővítési lehetőségek tekintetében. A Cisco IOS más operációs rendszerekhez viszonyítva nemcsak a leggazdagabb funkciókkal rendelkezik, de testre szabottan alkalmazható minden Cisco hálózati eszközre, különösképpen a kapcsolókra.

A rendelkezésre álló lehetőségek illusztrálására, amelyek a szó szoros értelmében túl terjedelmesek ahhoz, hogy itt felsoroljuk, most csak a Catalyst 3560 kapcsolókra összpontosítunk. A Catalyst 3560 kapcsolók SFP-portokkal (Switch Form-Factor Pluggable) rendelkeznek, amelyek több SFP adóvevő modult támogatnak. Itt egy lista azon SFP-modulokról, amelyeket egy vagy több típusú 3560 kapcsoló támogat:

**FastEthernet SFP-modul** –

* 100BASE-FX (multimódusú optikai, MMF) 2 kilométer távolságra
* 100BASE-LX10 (egymódusú optikai, SMF) 2 kilométer távolságra
* 100BASE-BX10 (SMF) 10 km-re
* 100BASE-EX (SMF) 40 km-re
* 100BASE-ZX (SMF) 80 km-re

**Gigabit Ethernet SFP-modulok** –

* 1000BASE-SX 50/62.5 um (MMF), maximum 550/220 m
* 1000BASE-LX/LH (SMF / MMF) 10 km-ig
* 1000BASE-ZX (SMF) 70 km-ig
* 1000BASE-BX10-D és 1000BASE-BX10-U (SMF) 10 km-ig
* 1000BASE-T (réz vezetékes adóvevő)

**10 Gigabit Ethernet SFP-modulok** –

* 10G-SR (MMF) 400 m-ig
* 10G-SR-X (MMF), maximum 400 m-ig (támogatja a szélsőséges hőmérsékleti viszonyokat)
* 10G-LRM (MMF) 220 m-ig
* FET-10G (MMF), 100 m-ig (a Nexus belső szerkezeti uplink-ekhez)
* 10G-LR (SMF) 10 km-ig
* 10G-LR-X (SMF) 10 km-ig (támogatja a szélsőséges hőmérsékleti viszonyokat)
* 10G-ER (SMF) 40 km-ig
* 10G-ZR (SMF) 80 km-ig
* Twinax (réz vezetékes adóvevő), 10 m-ig
* Aktív optika 10 m-ig (rack-en belüli és azok közti csatlakozáshoz)

A 40 Gigabit Ethernet és a 100 Gigabit Ethernet modulokat a csúcsszintű Cisco eszközök támogatják, mint például a Catalyst 6500, a CRS és az ASR 9000 forgalomirányítók, valamint a Nexus 7000-es sorozatú kapcsolók.

# LAN-kapcsolók

## Layer 3 kapcsolás

A kapcsolók különböző formai tényezőinek meghatározása mellett arra is szükség lehet, hogy válasszunk egy Layer 2 (második rétegbeli) és egy Layer 3 (harmadik rétegbeli vagy többrétegű) kapcsoló között.

Emlékezzünk vissza, hogy egy Layer 2 LAN-kapcsolón a továbbítás és szűrés alapja kizárólag az OSI adatkapcsolati rétegbeli (Layer 2) MAC-cím, és független IP-alhálózatok közötti adattovábbításhoz forgalomirányító használatára szorul (lásd 1. ábra).

Amint a 2. ábrán látható, egy Layer 3 kapcsoló, mint például a Catalyst 3560, hasonlóan működik, mint egy Layer 2 kapcsoló (például a Catalyst 2960), de ahelyett, hogy kizárólag a 2. rétegbeli MAC-cím információkat használná a továbbítási döntésekhez, a Layer 3 kapcsoló az IP-címet is használja.Amint a 2. ábrán látható, egy Layer 3 kapcsoló (például a Catalyst 3560) is hasonlóan működik, mint egy Layer 2 kapcsoló (például a Catalyst 2960), de a 2. rétegbeli MAC-cím információk kizárólagos használata helyett a továbbítási döntésekhez egy Layer 3 kapcsoló az IP-címet is használja. Ahelyett, hogy csak azt tanulná meg, mely MAC-címek társulnak az egyes portjaihoz, egy Layer 3 kapcsoló azt is megtanulja, mely IP-címek társulnak az interfészeihez. Ez lehetővé teszi a Layer 3 kapcsoló számára, hogy a forgalmat a hálózaton keresztül az IP-cím alapján is irányítsa.

A Layer 3 kapcsolók forgalomirányítási funkciókat is képesek teljesíteni, így nincs szükség külön forgalomirányítóra a LAN-on. Mivel a többrétegű kapcsolók speciális kapcsolási hardverrel rendelkeznek, általában olyan sebességgel képesek irányítani az adatokat, mint amilyen gyorsan kapcsolni tudják azokat.

# LAN-kapcsolók

## Layer 3 kapcsolás

A Cisco Layer 3 kapcsolói a Cisco Express Forwarding (CEF) kapcsolást használják. Ez a továbbítási módszer meglehetősen bonyolult, de szerencsére, mint minden jó technológia, nagy része a "színfalak mögött" játszódik le. Általában nagyon kevés CEF konfigurálás szükséges egy Cisco eszközön.

Alapvetően, a CEF elválasztja egymástól a megszokott szoros kölcsönös függőséget a Layer 2 és Layer 3 döntéshozatalban. Amitől az IP-csomagok továbbítása lassú egy hálózati eszközön, az az, hogy állandóan oda-vissza kell hivatkozni a 2. és 3. rétegbeli szerkezetek között. Így amennyiben ezeket az adatszerkezeteket függetleníteni lehet, a továbbítás felgyorsulhat.

A CEF működésének két fő összetevője:

* Továbbítási információs adatbázis (Forwarding Information Base, FIB)
* Szomszédsági táblák

A FIB fogalmilag hasonló az irányítótáblához. A forgalomirányító az irányítótáblát használja, hogy meghatározza a legjobb útvonalat egy célhálózat felé a cél IP-cím hálózati része alapján. A CEF-nél a korábban cache-ben tárolt útvonal adatokat több adatstruktúrában tároljuk a CEF-kapcsoláshoz. Az adatstruktúrák optimalizált keresést nyújtanak a hatékony csomagtovábbításhoz. Egy hálózati készülék a FIB keresési táblát használja, hogy a célra vonatkozó döntéseket hozzon anélkül, hogy hozzáférne az irányítótábla caché-hez.

A FIB frissül, ha változás történik a hálózatban, és a változás után tartalmazni fogja az összes adott időpontban ismert útvonalat.

A szomszédsági táblázatok 2. rétegbeli következő ugrás címeket tartanak karban minden egyes FIB-bejegyzéshez.

Az elérhetőségi adatok (a FIB-táblázatban) és a továbbítási információk (a szomszédsági táblázatban) elválasztása számos előnnyel jár:

* A szomszédsági tábla külön is kialakítható a FIB-táblától, amely lehetővé teszi mindkettő felépítését anélkül, hogy a csomagok folyamat-kapcsolva lennének.
* A MAC-fejléc átírását arra használják, hogy továbbítsuk a cache bejegyzésekben nem tárolt csomagot, így a változások egy MAC-fejléc újraíró szövegben nem igénylik a cache bejegyzések érvénytelenítését.

A CEF a Layer 3 kapcsolást végző Cisco eszközök többségén alapértelmezés szerint engedélyezve van.

# LAN-kapcsolók

## Layer 3 kapcsolás

A Cisco hálózati eszközök több különböző típusú Layer 3 interfészt támogatnak. A Layer 3 interfész az IP-címek alapján végzi az IP-csomagok továbbítását a végső rendeltetési hely felé.

A Layer 3 interfészek fő típusai:

* **Switch Virtual Interface (SVI)** - Logikai interfész egy kapcsolón, amit virtuális helyi hálózathoz (VLAN) társítunk.
* **Irányított (routed) port** - Fizikai port egy Layer 3 kapcsolón, ami forgalomirányító portként konfigurálható.
* **Layer 3 EtherChannel** - Logikai interfész egy Cisco eszközön, amit kötegelt irányított porthoz társítunk.

Amint azt korábban bemutattuk, az alapértelmezett VLAN-ban (VLAN1) az SVI-t engedélyezni kell ahhoz, hogy IP-alapú kapcsolat lehessen egy állomás és a kapcsoló között, amely lehetővé teszi a kapcsoló távoli adminisztrálását. Az SVI-ket ahhoz is be kell állítani, hogy forgalomirányítás lehessen a VLAN-ok között. Ahogyan említettük, az SVI-k logikai interfészek az egyes VLAN-okoz beállítva; a forgalomirányításhoz két vagy több VLAN között minden VLAN-nak külön engedélyezett SVI-kre van szüksége.

A routed portok lehetővé teszik a (Layer 3) kapcsolóknak, hogy forgalomirányítóként viselkedjenek. Minden port egy ilyen kapcsolón úgy konfigurálható, mint egy független IP-hálózaton lévő interfész.

A Layer 3 EtherChannel-eket arra használják, hogy összefogjanak Layer 3 Ethernet kapcsolatokat a Cisco eszközökön annak érdekében, hogy növeljék a sávszélességet, jellemzően a főkapcsolati (uplink) kapcsolatokon.

**Megjegyzés**: Az SVI-k és L3 EtherChannel-ek mellett más logikai interfészek is vannak a Cisco eszközökön, például visszacsatoló (loopback) interfészek és alagút (tunnel) interfészek.

# LAN-kapcsolók

## Layer 3 kapcsolás

Egy kapcsolóportot be lehet úgy állítani, hogy Layer 3 irányított port legyen, és úgy viselkedjen, mint egy hagyományos forgalomirányító interfész. Pontosabban, egy irányított portra jellemző:

* nem társítjuk egyetlen adott VLAN-hoz sem,
* be lehet állítani rajta egy Layer 3 irányító protokollt,
* kizárólag Layer 3 interfész, és nem támogatja a Layer 2 protokollokat.

Az interfészt Layer 3 módba lehet állítani a **no switchport** interfész konfigurációs paranccsal. Ezután IP-címet adhatunk a porthoz. Ennyi az egész!

A következő fejezetben többet fogunk megtudni a forgalomirányításról.

# Összefoglalás

## Összefoglalás

**Keresd MAC az információt!**

**Megjegyzés**: Ezt a feladatot külön-külön, kis csoportokban vagy a teljes iskolai tanulói környezetben is végre lehet hajtani.

Nézzük meg az alábbi linken található videót:

<http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet>

A tárgyalt témakörök között nem csak az szerepel, hogy honnan indultunk az Ethernet fejlesztésében, hanem hogy hová juthatunk el a technológiával (egy futurisztikus megközelítésben).

A videó megtekintése, és tartalmának az 5. fejezettel történő összehasonlítása után menjünk ki a webre és keressünk információt az Ethernetről! Használjunk konstruktivista megközelítést:

* Hogyan nézett ki az Ethernet, amikor először kifejlesztették?
* Hogyan maradt ugyanaz az Ethernet az elmúlt 25 év során, és milyen változások történnek annak érdekében, hogy hasznos/alkalmazható legyen a mai adatátviteli módszerekhez?

Gyűjtsünk össze három képet régi, jelenlegi és jövőbeli Ethernet fizikai átviteli közegekről és eszközökről (a hangsúly a kapcsolókon legyen) - osszuk meg ezeket a képeket az osztállyal, és vitassuk meg:

* Hogyan változott az Ethernet fizikai közege és a közvetítő eszközök?
* Hogy maradtak ugyanazok az Ethernet fizikai közegei és közvetítő eszközei?
* Hogyan változik az Ethernet a jövőben?

[Csoportos feladat - utasítások a Keresd MAC az információt! feladathoz](https://contenthub.netacad.com/legacy/CCNA/ITN/5.02/hu/course/files/5.4.1.1%20MAC%20and%20Choose%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

Az Ethernet ma a legelterjedtebb LAN technológia. Az Ethernet hálózati technológiák egész családját alkotja, amelyeket az IEEE 802.2 és 802.3 szabványok határoznak meg. Az Ethernet szabványok meghatározzák a második rétegbeli protokollokat és az első rétegbeli technológiákat is. A második rétegbeli protokollok, mint minden 802 IEEE-szabvány, az adatkapcsolati rétegben két különálló alrétegre támaszkodnak, a Logical Link Control (LLC-) és a MAC-alrétegekre.

Az adatkapcsolati réteg szintjén a keretszerkezet gyakorlatilag az Ethernet összes változatánál azonos. Az Ethernet keretszerkezet fejléceket és utótagokat ad a 3. rétegbeli PDU köré, hogy beágyazza az elküldendő üzenetet.

Két Ethernet keretezési típus létezik: az IEEE 802.3 Ethernet szabvány és a DIX Ethernet szabvány, amelyet manapság Ethernet II néven ismerünk. A legjelentősebb különbség a két szabvány között, hogy a a 802.3 szabványban hozzáadtak egy keretkezdő mezőt (Start Frame Delimiter, SFD) és a "típus" mező "hossz" mezőre változott. Az Ethernet II a TCP/IP-hálózatokon használt Ethernet keretformátuma. Mint az IEEE 802.2/3 szabványok megvalósítása, az Ethernet keret MAC-címzést és hibajavítást biztosít.

Az Ethernet által biztosított 2. rétegbeli címzés támogatja az egyedi, csoportos és szórásos (unicast, multicast és broadcast) kommunikációt. Az Ethernet címfeloldási protokollja (ARP) meghatározza a célállomások MAC-címét és leképezi azokat az ismert hálózati rétegbeli címekre.

Egy IP-hálózaton minden csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Az állomásnak a saját MAC- és IP-címét kell használnia a forrás mezőkben, valamint meg kell adnia a célállomás MAC- és IP-címét is. Míg a cél IP-címét egy magasabb OSI-réteg fogja biztosítani, a cél MAC-címét a küldő csomópontnak kell megtalálni egy adott Ethernet kapcsolaton. Ez az ARP feladata.

Az ARP bizonyos típusú Ethernet szórásos és egyedi címzésű üzenetekre támaszkodik, az úgynevezett ARP-kérésekre és az ARP-válaszokra. Az ARP-protokoll megkeresi az IPv4-címekhez tartozó MAC-címeket és létrehoz egy táblázatot az összerendelésekről.

A legtöbb Ethernet hálózaton a végberendezések általában, pont-pont alapon, egy Layer 2 LAN-kapcsolóhoz csatlakoznak. A 2. rétegbeli (Layer 2) LAN-kapcsoló a kapcsolási és szűrési műveleteit kizárólag az OSI adatkapcsolati rétegbeli MAC-címek alapján végzi. A Layer 2 kapcsoló is felépít egy MAC-címtáblát, amelyet a továbbítási döntéseihez használ. A Layer 2 kapcsolók a forgalomirányítókra támaszkodnak az egymástól független IP-alhálózatok közötti adattovábbításhoz.

A Layer 3 kapcsolók forgalomirányítási funkciókat is képesek teljesíteni, így nincs szükség külön forgalomirányítóra a LAN-on. Mivel a többrétegű kapcsolók speciális kapcsolási hardverrel rendelkeznek, általában olyan sebességgel képesek irányítani az adatokat, mint amilyen gyorsan kapcsolni tudják azokat.

