**Introduction to Networks**

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                   
*                       
*                     
*         
*                   
*               
*             
*                  

1. A hálózat jelene
2. Bevezetés

# Bevezetés

1.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Hálózatok ma fejezetben!

Gratulálunk! Ez a fejezet elindít a sikeres információtechnológiai karrier felé vezető úton azzal, hogy megmutatja a hálózatok létrehozásának, üzemeltetésének és karbantartásának alapjait. Bónuszként a Packet Traceres hálózatszimulációba is beleássuk magunkat. Ígérjük, hogy élvezetes lesz!

1.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe**: Hálózatok ma

**Fejezet célja**: Elmagyarázzuk a modern hálózati technológiák fejlődését.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A hálózatok hatása életünkre** | Megmutatjuk, hogy a hálózatok miként befolyásolják a mindennapi életünket. |
| **A hálózatok részei** | Elmagyarázzuk az állomások és hálózati eszközök szerepét. |
| **A hálózatok megjelenítése és a topológiák** | Megmutatjuk a hálózatok ábrázolását és azt, hogy a hálózati topológiákban ez miként használható. |
| **Gyakori hálózattípusok** | Összehasonlítjuk a hálózatok leggyakoribb fajtáinak jellemzőit. |
| **Internetkapcsolat** | Megnézzük, hogy a LAN-ok és WAN-ok miként kapcsolódnak az internethez. |
| **Megbízható hálózatok** | Megtanuljuk a megbízható hálózatok négy alapkövetelményét. |
| **Hálózati trendek** | Megnézzük azt, hogy a BYOD, az online együttműködés, a videók és a felhőalapú számítástechnika hogyan változtatja meg a kommunikációs szokásainkat. |
| **Hálózatbiztonság** | Megnézünk néhány alapvető hálózati biztonsági fenyegetést és azok megoldásait. |
| **Az IT szakértő** | Megnézzük a hálózattal kapcsolatos informatikai álláslehetőségeket. |

[Introduction to Networks](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok hatása az életünkre](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                        
*                               

1. A hálózat jelene
2. A hálózatok hatása az életünkre

# A hálózatok hatása az életünkre

1.1.1

## Hálózatok kötnek minket össze

Az emberi létezés összes szükséglete közül a kapcsolattartás igénye közvetlenül az életben maradás ösztöne után következik a rengsorban. A kommunikáció majdnem olyan fontos számunkra, mint a levegő, a víz, az élelmiszer és a menedék igénye.

A mai világban a hálózatoknak köszönhetően sose látott mértékben állunk összeköttetésben egymással. Ötleteinket azonnal megoszthatjuk másokkal, hogy azok valósággá válhassanak. Hírek, események, felfedezések másodpercek alatt terjednek el világszerte. Bárki közvetlen kapcsolatban állhat és játszhat egy barátjával, akitől amúgy óceánok és kontinensek választják el.

1.1.2

## Videó - A Cisco Networking Academy tanulási módszere

A világot megváltoztató emberek nem úgy születnek. Azzá válnak. 1997 óta a Cisco Networking Academy egyetlen cél elérése érdekében dolgozik: a digitális gazdasághoz szükséges tehetségek következő generációjának oktatása és készségfejlesztése.

Kattintsunk a Lejátszás gombra, hogy megtudjuk, hogy a Cisco Hálózati Akadémia miként tanít meg a technológia használatával jobbá tenni a világot!

1.1.3

## Nincsenek határok

A hálózati technológiák különböző fejlesztései talán a világunk legjelentősebb változásai. Olyan új világot segítenek létrehozni, ahol a nemzeti határok, a földrajzi távolságok és a fizikai korlátok kevésbé lesznek relevánsak, és a jelenleginél is kisebb akadályt fognak majd jelenteni.

Az internet már megváltoztatta a társadalmi, kereskedelmi, politikai és a személyes kapcsolattartásunk formáit. Az interneten történő közvetlen kommunikáció ösztönzi a globális közösségek kialakulását. A globális közösségek lehetővé tesznek olyanfajta közösségi együttműködést, amely független a helyszínektől vagy az időzónáktól.

Az online közösségek létrejötte és az információ szabad áramlása világszerte magában hordozza a termelékenység növekedését.

A felhőalapú számítástechnika lehetővé teszi, hogy dokumentumokat és képeket tároljunk, és azokhoz bárhol, bármikor hozzáférhessünk. Akár vonaton, akár parkban, akár hegy tetején állva, zökkenőmentesen hozzáférhetünk adatainkhoz és alkalmazásainkhoz bármilyen eszközön.



[1.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok részei](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                            
*                               

1. A hálózat jelene
2. A hálózatok részei

# A hálózatok részei

1.2.1

## Állomások

Ha egy globális online közösség tagjai szeretnénk lenni, a számítógépet, a táblagépet vagy az okostelefont először egy hálózathoz kell csatlakoztatni. Ennek a hálózatnak kapcsolódnia kell az internethez. Ez a témakör a hálózatok részeit tárgyalja. Keressük meg ezeket az összetevőket saját otthoni vagy iskolai hálózatunkban!

Minden olyan számítógépet állomásnak nevezünk, amely csatlakozik a hálózathoz és közvetlenül részt vesz a hálózati kommunikációban. Az állomásokat végberendezéseknek vagy hosztnak (host) is nevezzük. Bizonyos állomásokat kliensnek (client, ügyfél) is nevezünk. Az állomás kifejezés azonban kifejezetten azokra a hálózaton lévő eszközökre vonatkozik, amelyek kommunikációs célokra számot kapnak. Ez a szám azonosítja a gépet egy adott hálózaton belül. A számot Internet Protocol címnek vagy IP-címnek nevezzük. Az IP-cím meghatározza az állomást és a hálózatot, amelyhez csatlakozik.

A szerverek (kiszolgálók) olyan számítógépek, amelyeken olyan szoftverek futnak, amelyek információt (pl.: e-mail szolgáltatást vagy weboldalakat) biztosítanak más végberendezések számára. Minden szolgáltatás különálló szerverszoftvert igényel. Például, ha egy hálózaton webszolgáltatást szeretnénk biztosítani, akkor a szerveren webkiszolgáló programot kell telepíteni. A szerverszoftverrel ellátott számítógép egyidejűleg több kliens számára is nyújthat szolgáltatásokat.

Mint korábban említettük, a kliensek egyfajta állomások. A kliensek szoftverekkel rendelkeznek a szervertől kapott információk kéréséhez és megjelenítéséhez, az ábrán látható módon.

client PC and a server connected through a cloud symbolizing the Internet

ClientInternetServer

A Chrome-hoz vagy Firefoxhoz hasonló webböngészők is kliensprogramok. Egy számítógép többféle kliensprogramot is tud futtatni. Például, egy felhasználó megnézheti a elektronikus levelezését és böngészhet egy weboldalt, miközben azonnali üzenetküldőn beszél és egy audioközvetítést hallgat. The table lists three common types of server software.

| Type Description Email The email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server. Web The web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.File The file server stores corporate and user files in a central location. The client devices access these files with client software such as the Windows File Explorer. | |
| --- | --- |
| **Típus** | **Leírás** |
| E-mail | Az e-mail kiszolgáló e-mail szerverszoftvert futtat. A kliens valamilyen levelezőkliens (pl.: Microsoft Outlook) programot használ, amelynek segítségével eléri a szervert. |
| Web | A webszerver webszerver szoftvert futtat. A klliensek valamilyen böngészővel érik el a szerver weboldalait, ez lehet például az Internet Explorer. |
| Fájl | A fájlkiszolgáló központi helyen tárolja a vállalati és felhasználói fájlokat. A kliens valamilyen kliens szoftvert (pl.: a Windows Fájlkezelőt) használ. |

1.2.2

## Egyenrangú hálózatok

A kliens és a szerver programok általában külön számítógépeken futnak, de az is lehetséges hogy egy számítógép a két szerepet egyszerre töltse be. Kisvállalati és otthoni hálózatokban egy állomás gyakran egyszerre szerverként és kliensként is szolgál. Az ilyen hálózatot egyenrangú (peer-to-peer) hálózatnak nevezzük.

The image is a small peer-to-peer network with a printer on the left, connected to a print sharing peer in the middle, connected to a file sharing peer on the right. Under the topology is a list of the advantages and disadvantage of peer-to-peer networking. The advantages of peer-to-peer networking: easy to set up, less complex, lower cost because network devices and dedicated servers may not be required, and can be used for simple tasks such as transferring files and sharing printers. The disadvantages of peer-to-peer networking: no centralized administration, not as secure, not scalable, all devices may act as both clients and servers which can slow their performance.

I have a printer to shareI have files to sharePrint SharingFile Sharing

Az egyenrangú hálózatok előnyei:

* Könnyen konfigurálható
* Kevésbé összetett
* Alacsonyabb költségű, mivel hálózati eszközökre és dedikált kiszolgálókra nincs szükség
* Egyszerű feladatok (pl.: fájlátvitel és nyomtatómegosztás) elvégzésére alkalmas

Az egyenrangú hálózatok hátrányai:

* Nincs központosított adminisztráció
* Nem biztonságos
* Nem skálázható
* Minden eszköz működhet egyszerre kliensként és kiszolgálóként is, ami csökkentheti a teljesítményüket

1.2.3

## Végberendezések

A legtöbb ember csak a végberendezésekkel találkozik a hálózatokban. A végberendezések megkülönböztetésére mindegyiknek hálózati címet kell adni. Mikor egy végberendezés kommunikációt kezdeményez, a célállomás címével határozza meg, hogy hova kell az üzenetet továbbítani.

A végberendezés vagy a forrása, vagy a célja a hálózaton átvitt üzeneteknek.

A hálózaton keresztül áramló adatok animációjának megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

The physical network topology shows a LAN with two users an IP phone, a PC, and a server connected to a switch. A physical link connects the LAN switch to an edge router that boarders the LAN and an Internetwork. The Internetwork consists of four routers connected in a full mesh topology. An edge router boarders the Internetwork and a second LAN that also consists of two users, an IP phone, a PC, and a server. When the animation is started a message originates from one of the users in the first LAN and travels from the user, to the switch and to the edge router that boarders the Internetwork. At the Internetwork the message is routed through to the other edger router that boarders with the second LAN. The message is forwarded into the second LAN, through the switch and to the destination end user. Text under the graphic reads Data originates with an end device, flows through the network, and arrives at the end device.

**Internetwork**

**LAN**

**LAN**

Messages can take   
alternate routes.

Data originates with an end device, flows through the network, and arrives at an end device.

1.2.4

## Közvetítő eszközök

A közvetítő eszközök az egyes végberendezéseket csatlakoztatják a hálózathoz. Több különálló hálózatot is egymáshoz köthetnek, ezt internetworknek nevezzük. Ezek a közvetítő eszközök biztosítják az összeköttetést és az adatáramlást a hálózaton.

A közvetítő eszközök a céleszköz címének és a hálózati kapcsolatokról való saját információik segítségével meghatározzák az üzenetek útvonalát a hálózaton keresztül. Az ábrán néhány gyakran előforduló közvetítő eszközt és azok szerepét láthatjuk.

The picture shows symbols of five common intermediary devices and describes some of their functions. At the top is a wireless router, LAN switch, and router. Below is a multilayer switch and firewall appliance. Intermediary network devices perform some or all of these functions: regenerate and retransmit communication signals,maintain information about what pathways exist through the network and internetwork, notify other devices of errors and communication failures, direct data along alternate pathways when there is a link failure, classify and direct messages according to priorities, permit or deny the flow of data, based on security settings. Note: Not shown is a legacy Ethernet hub. An Ethernet hub is also known as a multiport repeater. Repeaters regenerate and retransmit communication signals. Notice that all intermediary devices perform the function of a repeater.

Intermediary DevicesWireless RouterLAN SwitchRouterMultilayer SwitchFirewall Appliance

A közvetítő hálózati eszközök az alábbi feladatok egy részét vagy akár mindegyikét látják el:

* A kommunikációs jelek újragenerálása és továbbítása
* A hálózaton belüli és a hálózatok közti különböző útvonalak információinak karbantartása
* Más eszközök értesítése hibákról és a kommunikáció sikertelenségéről
* Kapcsolati hiba esetén alternatív útvonalak biztosítása
* Üzenetek osztályozása és továbbítása prioritásuk alapján
* Az adat továbbításának engedélyezése vagy megtagadása a biztonsági beállítások alapján

**MEGJEGYZÉS:** Az ábrán nem tüntettük fel a régi Ethernet hubot. Az Ethernet hub más néven többportos ismétlő. Az ismétlő újragenerálja és újraküldi a kommunikációs jelet. Figyeljük meg, hogy az ismétlő funkciót mindegyik közvetítő eszköz megvalósítja.

1.2.5

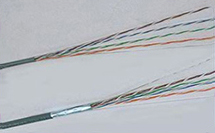
## Hálózati átviteli közeg

A kommunikáció valamilyen átviteli közegen halad a hálózaton. A közeg biztosítja a csatornát, hogy az üzenetek eljussanak a forrástól a céljukig.

A modern hálózatok elsősorban az ábrán látható háromféle közeg egyikét használják:

* **Fémdrót kábelben** - Az adat elektromos impulzusokká kódolva halad.
* **Üveg- vagy műanyag szálak kábelben (üvegszálas vagy optikai kábel)** - Az adat fényvillanások formájában halad.
* **Vezeték nélküli átvitel** - Az adatokat az elektromágneses hullámok bizonyos frekvenciáinak modulációjával kódolják.

There are three images of common network media followed by criteria to use when choosing network media. The top image shows twisted pair wires and connectors used with copper media. The middle image is a multi-strand fiber optic cable and fiber optic connectors. The bottom image shows wireless devices including a router and a camera. Criteria to consider when choosing network media: What is the maximum distance that the media can successfully carry a signal? Milyen környezetbe lesz telepítve a közeg? Mennyi adatot és milyen sebességgel kellene továbbítani? Mennyibe kerül a közeg és a telepítése?



CopperFiber-opticWireless

A hálózati közeg kiválasztásakor figyelembe kell venni:

* Az adott közeg milyen távolságra képes elvinni a jelet?
* Milyen környezetbe lesz telepítve a közeg?
* Mennyi adatot és milyen sebességgel kellene továbbítani?
* Mennyibe kerül a közeg és a telepítése?

Az egyes adatátviteli közegek egyedi sajátosságokkal és előnyökkel rendelkeznek. Nem mindegyik hálózati közeg rendelkezik ugyanolyan tulajdonságokkal, illetve nem mindegyik alkalmas ugyanarra a célra.

1.2.6

## Tudáspróba - A hálózatok összetevői

Az űrlap teteje

Check your understanding of network components by choosing the BEST answer to the following questions.

1. Which of the following is the name for all computers connected to a network that participate directly in network communication?

Az űrlap alja

When data is encoded as pulses of light, which media is being used to transmit the data?

Which two devices are intermediary devices? (Choose two)

[1.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok hatása az életünkre](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok megjelenítése és a topológiák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                            
*                               

1. A hálózat jelene
2. A hálózatok megjelenítése és a topológiák

# A hálózatok megjelenítése és a topológiák

1.3.1

## A hálózatok megjelenítése

A hálózattervezőknek és rendszergazdáknak képesnek kell lenniük arra, hogy megmutassák, hogyan fog kinézni a hálózatuk. Át kell látniuk, mely komponensek csatlakoznak más komponensekhez, hol helyezkednek el, és hogyan csatlakoznak egymáshoz. A hálózatdiagramok gyakran használják az ábrán látható szimbólumokat, amelyek a hálózatot alkotó különböző eszközöket és kapcsolatokat jelképezik.

A képen a hálózati diagramokban használt szimbólumok láthatók. A tetején a következő végeszközök találhatók: asztali számítógép, laptop, nyomtató, IP-telefon, vezeték nélküli asztal és TelePresence végpont. Középen a következő közvetítő eszközök találhatók: vezeték nélküli útválasztó, LAN-kapcsoló, útválasztó, többrétegű kapcsoló és tűzfal. Alul a következő hálózati adathordozók láthatók: kék hullámok a vezeték nélküli adathordozókat, egy folytonos fekete vonal a LAN adathordozót és egy piros világító villogó, amely a WAN adathordozót ábrázolja.

**Végeszközök** Asztali számítógép Laptop Nyomtató IP telefon Vezeték nélküli Tablet TelePresence Végpont **Közvetítő Eszközök** Vezeték nélküli útválasztó LAN kapcsoló Router Többrétegű kapcsoló tűzfal készülék **Hálózati média Vezeték nélküli média** LAN média WAN média

Egy ábra használata egyszerű módja annak, hogy megértsük egy nagy hálózat felépítését. Ezt a fajta hálózati "képet" topológiai ábrának nevezzük. Nagyon fontos, hogy a fizikai hálózat eszközeinek ábráit felismerjük, mert így tudjuk elképzelni a szervezet és a hálózat felépítését és működését.

A rajzjeleken kívül az eszközöknek és közegeknek speciális szókincse is van:

* **Network Interface Card (NIC)** \ - A hálózati kártya fizikailag csatlakoztatja a végberendezést a hálózathoz.
* **Fizikai port** \- Aljzat vagy csatlakozó egy hálózati eszközön, ide csatlakozik egy végberendezéshez vagy egy másik hálózati eszközhöz vezető kábel.
* **Interfész** \- Speciális port a hálózati eszközön, amely más hálózatokhoz csatlakozik. Mivel a routerek hálózatokat kötnek össze, ezért a router portjait hálózati interfészeknek nevezzük.

**MEGJEGYZÉS** : A port és interfész szavakat néha vegyesen használjuk.

1.3.2

## Topológiai ábrák

A topológiai ábrák használata elengedhetetlen azok számára, akik a hálózatokkal foglalkoznak. Vizuális térképet adnak a hálózat csatlakozásairól. A topológiai ábráknak két típusa létezik: fizikai és logikai.

**Fizikai topológiai ábra**

A fizikai topológiai diagramok szemléltetik a közvetítő eszközök fizikai helyét és a kábeltelepítést, az ábrán látható módon. Látjuk rajta azt, hogy melyik helyiségben vannak az eszközök.

A fizikai hálózati topológia hat szobát mutat, amelyek mindegyike világossárga mezőben van kiemelve, különféle hálózati eszközökkel és kábelezéssel. A bal oldalon a 2158-as szoba címkével ellátott szerverszoba található. Egy R1 feliratú útválasztót tartalmaz az 1. állványra 1 szerelve, hat kábelcsatlakozással. A tetején található kábel csatlakozik egy felhő feliratú Internethez. A bal oldali kábel egy S1 feliratú kapcsolóhoz csatlakozik, amely az 1. állvány 2. polcára van szerelve. Az S1 három szerverhez csatlakozik: egy webszerverhez a 2. rack 1. polcára, egy e-mail szerverhez a 2. polcra szerelve, és egy fájlszerverhez. a 2. állványon, a 3. polcon. Az R1 aljára csatlakoztatott kábel egy S2 feliratú kapcsolóhoz csatlakozik, amely az 1. rack 1 polcára van szerelve. Az S2 két csatlakozóval rendelkezik, amelyek egy nyomtatóhoz és egy PC-hez vezetnek az informatikai iroda 2159-es helyiségében. Az R1-nek három kábele van. jobbra a 2124-es helyiségben található három kapcsolóhoz csatlakozik. A felső kapcsoló S3 feliratú és az 1. állvány polcára van szerelve. A középső kapcsoló S4 feliratú, és az 1. állvány 2. polcára van felszerelve. Az alsó kapcsoló S5 feliratú és az állványra van felszerelve. 1 polc 3. Az S3 bal oldalán van egy kábel, amely egy laptophoz van csatlakoztatva egy 1. osztályú szoba 2125-ös helyiségben. Az S4 bal oldalán van egy kábel, amely egy 2. osztályú, 2126-os szoba 2. osztályú helyiségben lévő laptophoz van csatlakoztatva. laptophoz csatlakoztatva maradt egy 3. osztályú 2127-es szoba címkéjű helyiségben.

R1 S1 S2 S3 S4

S5

Internetes e-mail szerver   
2. állvány   
2. polc webszerver   
2. állvány   
1. polc fájlszerver   
2. állvány   
3. polc 1. állvány   
2. polc 1. állvány   
1. polc 1. állvány   
2. polc 1. állvány   
1. polc 1. állvány   
3. polc 1. állvány   
3. polc Szerverterem: Rm: 2158 Informatikai Iroda: Rm: 2159 1. osztály: Rm: 2125 2. osztály: Rm: 2126 3. osztály: Rm: 2127 Rm: 2124

**Logikai topológiai ábrák**

A logikai topológiai diagramok az ábrán látható módon illusztrálják a hálózat eszközeit, portjait és címzési sémáját. Láthatjuk, hogy melyik végberendezés melyik közvetítő eszközhöz csatlakozik, és milyen átviteli közeggel.

A logikai hálózati topológia az eszközöket, a portcímkéket és a hálózati címzési sémát mutatja. A kép közepén egy R1 feliratú router látható. A G0/0 feliratú port egy felhőhöz csatlakozik a tetején, az Internet felirattal. A G0/1 feliratú port bal oldalon csatlakozik a G0/1 porton lévő S1 feliratú kapcsolóhoz. Az S1 három szerverhez csatlakozik. Az S1 és a szerverek világossárga körrel vannak kiemelve, felül a 192.168.10.0 hálózattal. Az S1 F0/1 portja egy webszerverhez csatlakozik. Az S1 F0/2 portja egy e-mail szerverhez csatlakozik. Az S1 F0/3 portja egy fájlszerverhez csatlakozik. Az R1 F0/1 portja alul csatlakozik az S2 feliratú kapcsolóhoz. Az S2 nyomtatóhoz és PC-hez csatlakozik, amelyek mindegyike világossárga körrel van kiemelve, alul a 192.168.11.0 hálózattal. Az R1 bal oldalán három további csatlakozó található, amelyek mindegyike a G0/1 porton lévő kapcsolóhoz csatlakozik, amely az F0/1 porton egy laptophoz csatlakozik. Mindegyik kapcsoló és laptop sárga színnel van kiemelve, és megjelenik a hálózati cím. Az R1 G0/0 portja felül csatlakozik a 192.168.100.0 hálózaton található S3 kapcsolóhoz. Az R1 G1/1 portja középen csatlakozik egy S4 feliratú kapcsolóhoz a 192.169.101.0 hálózaton. Az R1 G1/2 portja alul csatlakozik egy S5 feliratú kapcsolóhoz a 192.168.102.0 hálózaton.

R1 Fa0/1 Fa0/2 Fa0/3 G0/1 G0/1 G0/0 G1/0 G0/1 G0/1 G1/1 G0/1 Fa0/1 Fa0/1 Fa0/1 G1/2 G0/1 G0/2 S1 S2 S3 S4 S5 Fa0/2

Fa0/1

Internetes e-mail kiszolgáló Webszerver fájlszerver hálózat   
192.168.10.0 Hálózat 192.168.11.0 Hálózat 192.168.100.0 Hálózat 192.168.101.0 Hálózat 192.168.102.0

A fizikai és logikai diagramokon látható topológiák egyelőre megfelelő mélységűek a tanfolyam jelenlegi szintjéhez. Bonyolultabb példákat találhatunk, ha rákeresünk az interneten a "network topology diagrams" kifejezésre. Ha a keresett kifejezésbe a Cisco szót is beleírjuk, sok olyan topológiát is találunk, amely ezekhez hasonló jeleket használ az ábrázolás során.

1.3.3

## Tudáspróba - A hálózatok megjelenítése és a topológiák

Az űrlap teteje

A következő kérdésekre a LEGJOBB válasz kiválasztásával ellenőrizze a hálózati reprezentációk és topológiák megértését.

1. Melyik kapcsolat köti fizikailag a végkészüléket a hálózathoz?

Az űrlap alja

Mely kapcsolatok speciális portok a hálózati eszközökön, amelyek az egyes hálózatokhoz csatlakoznak?

Milyen típusú hálózati topológia segítségével láthatja, hogy mely végeszközök milyen közvetítő eszközökhöz csatlakoznak, és milyen adathordozót használnak?

Milyen típusú hálózati topológia teszi lehetővé a közvetítő eszközök és a kábelek telepítésének tényleges helyét?

[1.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok részei](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakori hálózattípusok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                               
*                               

1. A hálózat jelene
2. Gyakori hálózattípusok

# Gyakori hálózattípusok

1.4.1

## Különböző méretű hálózatok

Most, hogy ismerjük a hálózatokat alkotó összetevőket és azok fizikai és logikai topológiákban való ábrázolását, készen állunk megismerni a különböző típusú hálózatokat.

A legkülönbözőbb méretű hálózatok léteznek, amelyek az egyszerű, két számítógépes hálózattól egészen a több millió eszközt tartalmazó hálózatokig terjednek.

Az egyszerű otthoni hálózatok lehetővé teszik az erőforrások (pl.: nyomtatók, dokumentumok, képek és zenék) megosztását néhány helyi végberendezés között.

A kisvállalati és otthoni irodai (SOHO) hálózatok lehetővé teszik az emberek számára, hogy otthonról vagy egy távoli irodából dolgozzanak. Sok egyéni vállalkozó használ otthoni vagy kisebb irodai hálózatot termékei eladására és reklámozására, eszközök megrendelésére vagy az ügyfelekkel való kapcsolattartásra.

A vállalatok és a nagy szervezetek hálózataikat arra használják, hogy a hálózat szerverein tárolják és onnan érjék el a céges információkat. A hálózatok e-mailt, azonnali üzenetküldést és csoportmunka lehetőségeket is biztosítanak. Számos szervezet használja a saját hálózatát arra, hogy azon keresztül termékeket vagy szolgáltatásokat nyújtson ügyfeleiknek.

Az internet a legnagyobb létező hálózat. Maga a kifejezés azt jelenti, hogy "a hálózatok hálózata". Egymással összekapcsolt magán- és nyilvános hálózatok alkotják.

Kisvállalatokban és otthonokban sok számítógép működik szerverként és kliensként is a hálózaton. Az ilyen hálózatot egyenrangú (peer-to-peer) hálózatnak nevezzük.

További információért kattintsunk a gombokra!

**Kisméretű otthoni hálózatok**

Egy kisméretű otthoni hálózat néhány számítógépet kapcsol össze egymással és az internettel.



1.4.2

## LAN-ok és WAN-ok

A hálózatokat több szempont szerint osztályozhatjuk:

* A lefedett terület mérete
* A kapcsolódott felhasználók száma
* Az elérhető szolgáltatások száma és típusa
* Felelősség mértéke

A hálózati infrastruktúrák két leggyakoribb típusa a helyi hálózat (LAN) és a nagy kiterjedésű hálózat (WAN). A LAN olyan hálózati infrastruktúra, amely kis földrajzi elhelyezkedésű területen biztosít összeköttetést felhasználók és végberendezések számára. A LAN lehet egy vállalat egy részlege, egy otthoni vagy egy kisvállalati hálózat. A WAN olyan hálózati infrastruktúra, amely más hálózatokhoz biztosít hozzáférést nagyobb földrajzi területen, jellemzően egy nagyobb vállalat vagy távközlési szolgáltató a tulajdonosa és karbantartója. Az ábra WAN-hoz csatlakoztatott LAN-okat mutat.

The network topology shows three LANs connected via a WAN link in the center. A legend shows that LANs are highlighted in yellow and WANs in light purple. The WAN is located in the center of the diagram. It contains a cloud symbol labeled cloud with red WAN connections to three routers. Each router is located partly in the WAN and partly in a LAN. At the bottom left is the Central LAN. It contains a server, two multilayer switches, two LAN switches, and four PCs. At the bottom right is the Branch LAN. It contains a switch, a server, a printer, two IP phones each connected to a PC, and a wireless access point with wireless connections to a laptop and a smartphone. At the top right is the home office LAN. It contains a wireless router with a wired connection to a printer and wireless conections to a laptop and a monitor.

Home OfficeCloudCentralBranchLANWAN

**LAN**

A helyi hálózat (LAN) kis földrajzi területet lefedő hálózat. A LAN sajátos jellemzőkkel rendelkezik:

* A LAN egy korlátozott nagyságú területen (pl.: otthon, az iskolában, egy irodaépületben vagy az egyetemi kampuszon) kapcsol össze végberendezéseket.
* A LAN-t rendszerint egyetlen szervezet vagy személy felügyeli. Az adminisztratív feladatok közé tartozik többek között a hálózati szintű biztonsági és hozzáférési házirendek alkalmazása.
* A LAN nagy sávszélességet biztosít a belső végberendezéseknek és a közvetítő eszközöknek (lásd az ábrát).

The diagram is an illustration of a LAN. At the center of the diagram is a switch. There are four Ethernet connections on the switch. At the top left is a connection to a PC. Below that is a connection to the computer at the desk of a worker. Below that is another connection to the computer at the desk of a worker. At the bottom left is a connection to an IP phone. To the right of the switch is a connection to a server. Text under the figure reads: a network serving a home, small building, or a small campus is considered a LAN.

Az otthonokat, kisebb épületeket vagy telephelyeket kiszolgáló hálózatokat LAN-nak nevezzük.

**WAN**

Az ábrán két LAN-t összekötő WAN látható. A WAN nagy földrajzi területet lefedő hálózati infrastruktúra. A WAN hálózatokat általában szolgáltatók vagy internetszolgáltatók (ISP, Internet Service Provider) üzemeltetik.

A WAN sajátos jellemzőkkel rendelkezik:

* A WAN biztosítja a nagy földrajzi területeket (pl.: városokat, államokat, tartományokat, országokat vagy kontinenseket) lefedő összeköttetést a LAN-ok között.
* A WAN hálózatokat rendszerint több szolgáltató biztosítja.
* A WAN jellemzően lassabb összeköttetést biztosít, mint a LAN.

The figure shows two branch LANs connected via a WAN link. Both LANs are highlighted in a light yellow box and consist of a central switch connected to three PCs, an IP phone, a server, and a router. The two routers are connected via a red WAN link. On the left is the branch 1 LAN and on the right is the branch 2 LAN.

**Branch 1 LANBranch 2 LAN**

1.4.3

## Az internet

Az internet egymással összekapcsolt hálózatok világméretű halmaza. Az ábra azt illusztrálja, hogy az internet egymással összekapcsolt LAN-okból és WAN-okból áll.

Five multilayer switches with redundant links are shown inside a large cloud. Around the edge of the cloud are seven routers connected to various LANs. There is a hospital LAN, a school LAN, a business LAN, a government LAN, and three home LANs. Text at the bottom reads LANs use WAN services to interconnect.

Home LANHospital LANGovernment LANBusiness LANSchool LAN

LANs use WAN services to interconnect.

A példában néhány LAN WAN-kapcsolaton keresztül kapcsolódik egymáshoz. A WAN-ok is össze vannak egymással kötve. A WAN-kapcsolatok piros vonalai a hálózatok összekapcsolásának összes fajtáját jelképezik. A WAN-ok rézvezetékeken, optikai kábeleken és vezeték nélküli átvitelen keresztül kapcsolódhatnak (ez utóbbi nincs az ábrán).

Az internet nincs egyetlen személy vagy csoport tulajdonában. A különböző hálózatok közti hatékony adatkommunikáció egységes és következetes szabványok alkalmazását igényli, egyben számos rendszerfelügyeleti szervezet együttműködését is feltételezi. Vannak olyan szervezetek, amelyek az internetes protokollok és folyamatok formai követelményeire és szabványosítására felügyelnek. Ezen szervezetek közé tartozik az Internet Engineering Task Force (IETF), az Internet Corporation for Assigned Names and Numbers (ICANN), az Internet Architecture Board (IAB) és még néhány más, hasonló szervezet.

1.4.4

## Intranet és extranet

Két másik kifejezés is van, amely hasonlít az internet kifejezéshez:

Az intranet kifejezést egy szervezet LAN-jai és WAN-jai közti privát kapcsolatra használják. Az intranet úgy van kialakítva, hogy csak a szervezet tagjai, alkalmazottai vagy más, engedéllyel rendelkező személyek férjenek hozzá.

Egy szervezet használhat extranetet, hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is. Íme néhány példa erre az esetre:

* Egy cég hozzáférést biztosít külső beszállítói és alvállalkozói számára.
* Egy kórház időpont-foglalási rendszert biztosít az orvosok számára, akik így találkozókat egyeztethetnek a betegeikkel.
* Egy oktatásügyi helyi kirendeltség költségvetési és személyzeti adatokat szolgáltat a kerületi iskolákról.

Az ábra a céges intranet, céges extranet és az internet hálózatokhoz való hozzáférés különböző szintjeit mutatja be különböző csoportok számára.

A center circle is labeled Intranet and has company only access. Surrounding that is another circle labeled Extranet and is accessible by suppliers, customers, and collaborators. Surrounding that is another circle labeled the Internet and is accessible by the world.

**The Internet**  
The World**Extranet**  
Suppliers, Customers, Collaborators**Intranet**  
Company Only

1.4.5

## Tudáspróba - Gyakori hálózattípusok

Az űrlap teteje

Check your understanding of common types of networks by choosing the BEST answer to the following questions.

1. Which network infrastructure provides access to users and end devices in a small geographical area, which is typically a network in a department in an enterprise, a home, or small business?

Az űrlap alja

Which network infrastructure might an organization use to provide secure and safe access to individuals who work for a different organization but require access to the organization’s data?

Which network infrastructure provides access to other networks over a large geographical area, which is often owned and managed by a telecommunications service provider?

[1.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózatok megjelenítése és a topológiák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Internetkapcsolat](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                
*                               

1. A hálózat jelene
2. Internetkapcsolat

# Internetkapcsolat

1.5.1

## Internet-hozzáférési technológiák

Már értjük, miből állnak a hálózatok, és milyen típusú hálózatok léteznek. De hogyan kapcsoljuk a felhasználókat és szervezeteket az internethez? Jól tippel, aki azt gondolja, hogy ennek is sokféle módja van.

Az otthoni felhasználók, a távmunkások (távoli dolgozók), és a kis irodák jellemzően egy ISP-hez csatlakoznak, hogy elérjék az internetet. Az elérhető csatlakozási lehetőségekben nagy különbségek találhatók az internetszolgáltatók és földrajzi területek között. Népszerű csatlakozási lehetőség a szélessávú kábel, a szélessávú digitális előfizetői vonal (DSL), a vezeték nélküli WAN és a különböző mobil szolgáltatások.

A szervezeteknek jellemzően más vállalati telephelyekhez és az internethez történő hozzáférésre van szükségük. Gyors kapcsolat szükséges olyan üzleti szolgáltatások támogatására, mint az IP-telefonok, videokonferencia megoldások és az adatközponti tárolás. A szolgáltatók (SP, service provider) vállalati szintű összeköttetéseket kínálnak. Népszerű vállalati szintű szolgáltatás az üzleti DSL, a bérelt vonal és a Metro Ethernet.

1.5.2

## Otthoni és kisvállalati internetkapcsolatok

Az ábrán a gyakoribb otthoni és kisvállalati internetcsatlakozás módjai láthatók.

közös csatlakozási lehetőségek kis irodai és otthoni irodai felhasználók számára

Otthoni felhasználó távmunkás kis irodai DSL kábel Mobil internet Műholdas betárcsázós telefon Internet szolgáltató

* **Kábeles, kábeltévés** - Kábeltévé szolgáltatók nyújtanak ilyen szolgáltatást, az internet adatjelei ugyanazon a kábelen haladnak, mint a kábeltévé adás. Nagy sávszélesség, magas rendelkezésre állás jellemzi, állandó kapcsolatot biztosít.
* **DSL** - A DSL vagy Digital Subscriber Line szintén nagy sávszélességet, magas rendelkezésre állást és folyamatos internetkapcsolatot nyújt. A DSL telefonvonalon működik. Általánosságban elmondható, hogy a kisvállalati és otthoni felhasználók aszimmetrikus DSL (ADSL) használatával csatlakoznak, ami azt jelenti, hogy a letöltési sebesség gyorsabb, mint a feltöltési sebesség.
* **Mobilnetes** \- A mobilnet vagy mobil adatkapcsolat (angol megfelelője: cellular) a mobilhálózatot használja. Ahol van mobilhálózati jel, ott internetezni is lehet. A teljesítmény függ a telefon képességeitől és attól, hogy épp milyen adótoronyhoz csatlakozik.
* **Műholdas** - A műholdas internet előnye az, hogy olyan helyeken is rendelkezésre áll, ahol semmilyen más internetkapcsolat nincs. A parabola antennának rá kell látnia a műholdra.
* **Betárcsázós** - A modemes vagy betárcsázós internethez egy bármilyen telefonvonal és egy modem kell, ez egy olcsó megoldás. A modem alacsony sávszélessége nagy adatok átvitelére nem alkalmas, de utazás közbeni mobil használatra hasznos.

A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei.

1.5.3

## Vállalati internetkapcsolatok

A vállalatok csatlakozási lehetőségei különböznek az otthoni felhasználók lehetőségeitől. A vállalatok nagyobb és dedikált sávszélességet, valamint menedzselt szolgáltatásokat igényelnek. A csatlakozási lehetőségek eltérőek attól függően, hogy hány szolgáltató működik a vállalat közelségében.

Az ábra a vállalatok gyakori csatlakozási lehetőségeit szemlélteti.

közös kapcsolódási lehetőségek a vállalkozások számára

Szervezet Internetszolgáltató Műholdas Üzleti DSL Metro Ethernet Dedikált bérelt vonalak Internet

* **Dedikált bérelt vonal** - A bérelt vonal a szolgáltató hálózatának fenntartott vonala, amellyel földrajzilag távol levő irodákat lehet összekötni hang- és/vagy adatkapcsolat céljából. A bérelt vonalat havi vagy éves díjszabással adják bérbe.
* **Metro Ethernet** - Néha Ethernet WAN néven is emlegetik. Ebben a fejezetben Metro Ethernetként fogunk rá hivatkozni. A Metro Ethernet LAN hozzáférési technológiákkal valósít meg WAN-t. Az Ethernet egy LAN-technológia, amelyet egy későbbi fejezetben ismerünk meg.
* **Üzleti DSL** - Az üzleti DSL-nek sok változata van. A legnépszerűbb változat a szimmetrikus digitális előfizetői vonal (SDSL), amely hasonló az aszimmetrikus digitális előfizetői vonalhoz (ADSL), de ugyanakkora feltöltési és letöltési sebességet biztosít.
* **Műholdas** \- Műholdas szolgáltatást ott is lehet nyújtani, ahol vezetékes megoldás nincs.

A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei.

1.5.4

## A konvergáló hálózat

**Hagyományos különálló hálózatok**

Vegyünk egy harminc évvel ezelőtt épült iskolát. Akkoriban a tantermek külön kábelezést használtak az adathálózathoz, a telefonhálózathoz és a televíziókhoz használt videohálózathoz. Ezek a különálló hálózatok nem tudtak kommunikálni egymással. Minden hálózat különböző technológiákat használt a kommunikációs jel hordozásához. Mindegyik hálózatnak saját szabályai és szabványai voltak a kommunikáció sikeres lebonyolításához. Több szolgáltatás futott több hálózaton.

külön számítógép-, telefon- és műsorszóró hálózatok

Eszközök Közepes Üzenet Szabályszerződés Szabványos Szabályszerződés Szabványos Szabályszerződés Szabvány Közepes Közepes üzeneteszközök Eszközök Számítógépes Telefonhálózatok Hálózatok Üzenet Hálózatok Műsorszórási

**Konvergált hálózatok**

Ma a különálló adatok, telefon- és videóhálózatok kezdenek összeolvadni. A dedikált hálózatokkal ellentétben a konvergált hálózatok adat-, hang- és videojelet is képesek átvinni ugyanazon a hálózaton, különböző típusú eszközök között. Ez a hálózati infrastruktúra már ugyanazokat a szabályokat, megállapodásokat és megvalósítási szabványokat használja. A konvergált adathálózat több szolgáltatást nyújt egy hálózaton.

Konvergált adathálózat, amely több szolgáltatást hordoz egy hálózaton.

Közepes Közepes Közepes Szabályszerződés Szabványos eszközök Eszközök Eszközök Üzenet Üzenet Üzenet Egy hálózat - Több eszköz

1.5.5

## Videómagyarázat - A Packet Tracer letöltése és telepítése

Ez a videó megmutatja, hogyan kell letölteni és telepíteni a Packet Tracer programot. A Packet Tracer segítségével hálózatok létrehozását és tesztelését szimuláljuk a számítógépünkön. A Packet Tracer egy szórakoztató, hazavihető, rugalmas program, amely lehetőséget ad arra, hogy az épp megtanult hálózati ábrák és elvek használatával egészen bonyolult LAN-okat és WAN-okat építsünk és vizsgáljunk.

A diákok gyakran használják a Packet Tracert:

* Vizsgára készülésre.
* A hálózatos tanfolyamokon tanultak gyakorlására.
* Állásinterjú előtt a tudásuk felfrissítésére.
* Meglevő hálózatok új technológiákkal való bővítésének hatásait vizsgálni.
* Az IoT-vel kapcsolatos álláshoz új képességeket tanulni.
* Másokkal versenyezni a Global Design Challenge-ben (lásd a 2017 PT7 Design Challenge oldalát a Facebookon).

A Packet Tracer egy alapvető tanulási eszköz, amelyet a Cisco Hálózati Akadémia számos tanfolyamon használnak.

A Cisco Packet Tracer példányának beszerzéséhez és telepítéséhez kövessük az alábbi lépéseket:

**1. lépés** Lépjünk be a Cisco Hálózati Akadémia weboldalán az "I'm Learning" oldalra.

**2. lépés** Kattintsunk a Resources menüpontra.

**3. lépés** Válasszuk a Download Packet Tracer lehetőséget.

**4. lépés** Válasszuk ki a kívánt Packet Tracer verziót.

**5. lépés** Mentsük a fájlt a számítógépre.

**6. lépés** Indítsuk el a Packet Tracer telepítőprogramot.

A Packet Tracer letöltési és telepítési folyamatának részletes bemutatásához kattintsunk az ábrán látható Lejátszás gombra!

1.5.6

## Videómagyarázat - Első lépések a Cisco Packet Tracerben

A Packet Tracer valódi hálózatok szimulációját lehetővé tevő eszköz. Három fő menüt biztosít:

* Eszközöket adhatunk hozzá, és kábellel vagy vezeték nélkül csatlakoztathatjuk őket.
* Kiválaszthatjuk, törölhetjük, megvizsgálhatjuk, címkézhetjük és csoportosíthatjuk a hálózati összetevőket.
* Megnyithatunk régi vagy mintahálózatot, menthetjük a jelenlegi hálózatot, megváltoztathatjuk a felhasználói profilunkat és beállításainkat.

Aki bármilyen programot, például szövegszerkesztőt vagy táblázatkezelőt használt már, az ismeri a felső menüsorban található File menü parancsait. A Megnyitás (Open), Mentés (Save), Mentés másként (Save as) és Kilépés (Exit) menüpontok ugyanúgy működnek, mint bármely programnál, de a Packet Tracer esetében két speciális parancs létezik.

Az Open Samples (Minták megnyitása) megjelenít egy Packet Tracerrel érkezett mappát, amelyben előre elkészített példák találhatók hálózati eszközök beállításaival és IoT-eszközökkel.

A Kilépés és Kijelentkezés (Exit and Logout) parancs eltávolítja a Packet Tracer ezen példányának regisztrációs adatait, és a Packet Tracer ezen példányának következő felhasználójának ismét be kell lépnie.

Kattintsunk az ábrán látható Lejátszás gombra, hogy megtudjuk, hogyan kell használni a menüket, és hogyan hozhatjuk létre első Packet Tracer hálózatunkat!

1.5.7

## Packet Tracer - Hálózatok ábrázolása

A feladat során kipróbáljuk, hogy a Packet Tracer miként segíti a hálózatok tervezését és ábrázolását.

[A hálózatok megjelenítése](https://contenthub.netacad.com/courses/itn/_common/1.5.7-packet-tracer---network-representation_hu-HU.pka)

[1.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakori hálózattípusok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Megbízható hálózatok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                
*                               

1. A hálózat jelene
2. Megbízható hálózatok

# Megbízható hálózatok

1.6.1

## Hálózati architektúrák

Volt már olyan, hogy online munka közben egyszer csak "elment az internet"? Persze nem az internet állt le, csak a mi kapcsolatunk szakadt meg. Nagyon idegesítő! Mivel a világon oly sok ember támaszkodik a hálózati hozzáférésre munkához és a tanuláshoz, elengedhetetlen, hogy a hálózatok megbízhatóak legyenek. Ebben az összefüggésben a megbízhatóság nemcsak az internetkapcsolatunkra értendő. Ez a témakör a hálózati megbízhatóság négy aspektusára összpontosít.

A hálózatok szerepe az idők során átalakult: adatátviteli hálózatból egy olyan multimédiás, konvergált hálózati környezetté változott, amely lehetővé teszi a kapcsolatot az emberek, az eszközök és a különböző információk között. Ahhoz, hogy a hálózatok hatékonyan működhessenek és növekedhessenek egy ilyen típusú környezetben, az egész hálózatot egy szabványos hálózati architektúra alapján kell kiépíteni.

A hálózatok számos alkalmazást és szolgáltatást támogatnak, ugyanakkor a fizikai infrastruktúrát alkotó különböző kábelekkel és eszközökkel is együtt kell működniük. A hálózati architektúra kifejezés ebben az összefüggésben azokra a technológiákra utal, amelyek támogatják azt az infrastruktúrát, valamint a különböző programozott szolgáltatásokat és szabályokat (más néven protokollokat), amelyek adatokat küldenek a hálózaton keresztül.

A hálózatok fejlődésével kialakult az a négy alapvető jellemző, amelyet a hálózat tervezőjének meg kell valósítania, ha teljesíteni szeretné a felhasználók elvárásait:

* Hibatűrés
* Skálázhatóság
* Szolgáltatás minősége (QoS)
* Biztonság

1.6.2

## Hibatűrés

Egy hibatűrő hálózat hiba előfordulása esetén minimalizálni tudja az érintett eszközök számát. A hiba után gyors helyreállítást tesz lehetővé. Az ilyen hálózatok azon alapulnak, hogy az üzenet forrása és a célja között több útvonal is létezik. Ha egy útvonal megszakad, az üzeneteket azonnal egy másik kapcsolaton továbbítják. Redundanciának hívják azt, amikor egy célállomáshoz több út is vezet.

A csomagkapcsolt hálózat megvalósítása egy lehetséges módja annak, hogy a megbízható hálózatok redundanciát biztosítsanak. A csomagkapcsolás a forgalmat szétdarabolja és egy megosztott hálózaton át továbbítja. Ilyenkor egyetlen üzenet (pl.: egy e-mail vagy videófolyam) több üzenetblokkra, úgynevezett csomagokra lesz bontva. Minden csomag rendelkezik a szükséges címzési információkkal az üzenet forrásáról és céljáról. A hálózat routerei a hálózat állapota alapján irányítják a csomagokat. Ez azt jelenti, hogy egy üzenet darabjai egészen különböző úton érhetik el ugyanazt a célt. Az ábrán azt látjuk, hogy a felhasználó tudta és befolyása nélkül fogja a router másfelé irányítani a csomagot egy kapcsolat hibája esetén.

A hálózati topológia négy routerből áll, redundáns kapcsolatokkal. A diagram tetején az internetes felhő látható, alul két kapcsolattal, amelyek mindegyike egy útválasztóhoz vezet. Ezek alatt a routerek alatt található egy másik útválasztóval való kapcsolat. Mindegyik alsó útválasztó visszacsatlakozik mindkét útválasztóhoz, amelyek az internethez csatlakoznak. A bal alsó sarokban lévő router három asztali számítógépet és három IP-telefont tartalmazó switch-hez csatlakozik. A jobb alsó sarokban lévő útválasztó egy három asztali számítógépet tartalmazó kapcsolóhoz csatlakozik. A bal felső routeren egy piros kör van átlós vonallal. A jobb felső routeren egy zöld nyíl látható, amely az internetre vezet. Egy szövegdobozban ez olvasható: a redundáns kapcsolatok alternatív útvonalakat tesznek lehetővé, ha egy eszköz meghibásodik; a felhasználói élményt ez nem érinti.

Az internetes redundáns kapcsolatok alternatív útvonalakat tesznek lehetővé, ha egy eszköz vagy egy hivatkozás meghibásodik. A felhasználói élményt ez nem érinti.

1.6.3

## Skálázhatóság

A skálázható hálózatot nagyon gyorsan lehet bővíteni az új felhasználók és alkalmazások támogatásához. Ezt anélkül lehet megvalósítani, hogy a jelenlegi felhasználók által igénybe vett szolgáltatások teljesítménye csökkenne. Az ábra azt mutatja, hogyan lehet egy új hálózatot könnyen hozzáadni egy meglévő hálózathoz. Ezek a hálózatok azért skálázhatók, mert a tervező követi az elfogadott szabványokat és protokollokat. Ez lehetővé teszi, hogy a szoftver- és hardvergyártók a termékek és szolgáltatások fejlesztésére összpontosítsanak anélkül, hogy új szabályokat kellene kidolgozniuk a hálózaton belüli működéshez.

A hálózati topológia négy routerből áll, redundáns hivatkozásokkal, köztük két kapcsolattal az internetes felhőhöz. Három LAN van, amelyek közül az egyiket nemrégiben adták hozzá. Egy szövegdobozban ez olvasható: további felhasználók és teljes hálózatok csatlakozhatnak az internethez anélkül, hogy a meglévő felhasználók teljesítménye csökkenne.

Internet További felhasználók és teljes hálózatok csatlakozhatnak az internethez anélkül, hogy a meglévő felhasználók teljesítménye csökkenne.

1.6.4

## Szolgáltatásminőség

A szolgáltatás minősége (QoS) egyre erősebb követelmény a jelenlegi hálózatokban. Egyre újabb hálózati alkalmazások állnak a felhasználók rendelkezésére, mint például az élő hang- és videoközvetítési szolgáltatások, és ezek egyben magasabb minőségi elvárásokat is támasztanak. Ki ne próbált már úgy megnézni egy videót, hogy az állandóan akadozott vagy leállt? Mivel az adat-, hang- és videotartalom ugyanazon a hálózaton utazik, a QoS az elsődleges módszer a torlódások kezelésére és a megbízható kézbesítés megvalósítására a felhasználók számára.

Torlódás akkor alakul ki, ha a sávszélességigény magasabb, mint amennyi rendelkezésre áll. A hálózati sávszélesség az egy másodperc alatt átvihető bitek száma, vagyis a mértékegysége a bit per másodperc (bps). Ha egyszerre több kommunikáció használja a hálózatot, akkor előfordulhat, hogy az összesített igény meghaladja a rendelkezésre álló hálózati sávszélességet, vagyis torlódás alakul ki.

Ha a forgalom nagyobb, mint amennyit át lehet vinni a hálózaton, az eszközök a memóriában tárolják a csomagokat addig, amíg nem tudják továbbítani. Az ábrán egy felhasználó weboldalt tölt le, egy másik pedig telefonbeszélgetést folytat. Egy QoS-házirenddel konfigurált router képes az adat- és hangforgalom kezelésére úgy, hogy a hang alapú kommunikációnak elsőbbséget biztosít hálózati torlódás esetén.

hálózati topológia PC-kkel és IP-telefonokkal egy switch-hez csatlakoztatva, amely egy routerhez csatlakozik, amely a forgalom prioritása révén kezeli a szolgáltatás minőségét

Az útválasztó által kezelt szolgáltatás minősége biztosítja, hogy a prioritások illeszkedjenek a kommunikáció típusához és annak fontosságához a szervezet számára. A weboldalak általában alacsonyabb prioritást kaphatnak. A Voice over IP (VoIP) hívásnak elsőbbséget kell biztosítania a zavartalan, zavartalan felhasználói élmény fenntartásához. Internet

1.6.5

## Hálózatbiztonság

A hálózati infrastruktúra, a különböző szolgáltatások és a hálózatra csatlakoztatott eszközökön átmenő adatforgalom létfontosságúakká váltak a személyes és az üzleti világban. Két típusú hálózatbiztonsági probléma létezik, amelyekkel foglalkozni kell: a hálózati infrastruktúra biztonsága és az információbiztonság.

A hálózati infrastruktúra biztosítása magában foglalja a kapcsolatokért felelős eszközök fizikai biztonságának a megteremtését, valamint ezen eszközök felügyeleti szoftvereihez történő illetéktelen hozzáférés megakadályozását is (lásd az ábrán).

hálózati topológia PC-k és IP-telefonok olyan switch-hez csatlakoztatva, amely egy routerhez csatlakozik, amely szoftver- és hardveres biztonsággal védi a hálózatot, és megakadályozza a hálózati eszközök fizikai elérését.

A rendszergazdák szoftveres és hardveres biztonsággal, valamint a hálózati eszközökhöz való fizikai hozzáférés megakadályozásával védhetik a hálózatot. Az internetes biztonsági intézkedések megvédik a hálózatot az illetéktelen hozzáféréstől. Belépés: ?   
Jelszó: ?

A rendszergazdának védenie kell a hálózaton átvitt csomagokban levő információkat és a hálózatra csatlakozó eszközökön tárolt információkat is. A hálózat biztonságának érdekében három alapvető elvárást kell teljesíteni:

* **Bizalmasság** \- Az adatok bizalmas kezelése azt jelenti, hogy csak a kívánt és jogosult személyek férnek hozzá és olvashatják az adatokat.
* **Integritás** - Az adatintegritás (adatok épsége) azt jelenti, hogy garantálható, hogy az információt a forrástól a célig tartó átvitel közben nem módosították.
* **Elérhetőség** \- Az elérhetőség azt jelenti, hogy a jogosult felhasználók naprakészen és megbízható módon férnek hozzá az adatokhoz.

1.6.6

## Tudáspróba - Megbízható hálózatok

Az űrlap teteje

Ellenőrizze, hogy megértette-e a megbízható hálózatokat, és válassza ki a megfelelő választ a következő kérdésekre.

1. Ha a tervezők követik az elfogadott szabványokat és protokollokat, a hálózati architektúra négy alapvető jellemzője közül melyik érhető el?

Az űrlap alja

A titkosság, az integritás és a rendelkezésre állás melyik követelménye a hálózati architektúra négy alapvető jellemzőjének?

Milyen típusú házirenddel tudja az útválasztó kezelni az adat- és hangforgalom áramlását, előnyben részesítve a hangkommunikációt, ha a hálózat torlódást tapasztal?

Having multiple paths to a destination is known as redundancy. This is an example of which characteristic of network architecture?

[1.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Internetkapcsolat](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati trendek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                
*                               

1. A hálózat jelene
2. Hálózati trendek

# Hálózati trendek

1.7.1

## Mai trendek

Sokat tudunk már a hálózatokról, miből állnak, hogyan kapcsolnak minket össze, és mitől lesznek megbízhatóak. De a hálózatok, mint minden más, folyton változnak. Néhány irányvonalról nekünk, NetAcad tanulóknak mindenképpen tudnunk kell.

Mivel folyamatosan új technológiák és felhasználói készülékek kerülnek a piacra, ezért a vállalkozásoknak és a fogyasztóknak is állandóan alkalmazkodniuk kell a mindig változó környezethez. Több hálózati trend van hatással a szervezetekre és a végfelhasználókra:

* Bring Your Own Device (Hozd a saját eszközödet)
* Online csoportmunka
* Videokommunikáció
* Felhőalapú szolgáltatások

1.7.2

## Bring Your Own Device (BYOD, Hozd a saját eszközödet)

Az az elv, hogy bármilyen eszközt, bármilyen tartalmat, bármilyen módszert használhatunk, egy fontos globális trend, amely jelentős változásokat hoz abban, ahogy az eszközeinket használjuk és a hálózatra csatlakoztatjuk. Ez a trend a "Hozd a saját eszközödet" (Bring Your Own Device, BYOD).

A BYOD lehetővé teszi a felhasználók számára, hogy a saját privát eszközeik használatával érjenek el információkat, vagy kommunikáljanak másokkal egy szervezet hálózatán belül. A fogyasztói eszközök számának növekedésével és az ehhez kapcsolódó költségek csökkenésével várható, hogy a munkavállalók és a diákok személyesen is rendelkezni fognak a legmodernebb számítástechnikai és hálózati eszközökkel. Ezek közé tartoznak a laptopok, notebookok, tabletek, okostelefonok, és az ebook-olvasók. Az eszközöket a cég vagy az iskola, illetve maga az egyén fogja megvásárolni, de akár közösen is megvehetik.

A BYOD lényege, hogy bármilyen eszközt bárhol használhatunk, akárki is legyen a tulajdonosa.



1.7.3

## Online csoportmunka

Az emberek nem csak azért szeretnének a hálózatra csatlakozni, hogy adatokhoz férhessenek hozzá, hanem azért is, hogy együttműködhessenek egymással. Az együttműködés "az a folyamat, amikor mással vagy másokkal egy közös projekten dolgozunk." A csoportmunkát segítő eszközök (pl.: az ábrán látható Cisco Webex) azonnali kapcsolatfelvételt, együttműködést és a közös célok elérését teszik lehetővé alkalmazottak, diákok, tanárok, vásárlók vagy egyéb partnerek számára.



A csoportmunka kritikus és stratégiai prioritás, amelyet a szervezetek a versenyképesség miatt használnak. Az oktatásban szintén fontos a csoportmunka. A diákoknak együtt kell működniük, hogy segítsék egymást a tanulásban, hogy kifejlessszék a munkavégzéshez szükséges közösségi képességeket, és hogy közreműködjenek egymással a csoportos projektek során.

A Cisco Webex Teams egy többfunkciós, együttműködést segítő eszköz, amellyel azonnali üzeneteket küldhetünk egy vagy több személynek, képeket, videókat és hivatkozásokat oszthatunk meg. Minden csoport oldala (Webex kifejezéssel "space") minden történést rögzít.

1.7.4

## Videokommunikáció

A kommunikáció és együttműködés egy másik kritikus összetevője a videók használata. A kommunikációban, együttműködésben és a szórakozásban egyaránt fontos szerepe van a videónak. Bárki indíthat és fogadhat videohívást, akinek internetkapcsolata van, bárhol is legyen.

A videokonferencia hatékony eszköz a másokkal való kommunikációhoz mind helyi, mind globális szinten. A videó kulcsfontosságú tényezővé vált a hatékony együttműködés tekintetében, mert a vállalatok gyakran terjeszkednek ország- vagy kulturális határokon keresztül.

1.7.5

## Videómagyarázat - Cisco Webex

Kattintsunk az ábrán látható Lejátszás gombra, hogy megnézzük, a Cisco Webex miként épül be a mindennapi életünkbe és az üzleti folyamatokba!

1.7.6

## Felhőalapú szolgáltatások

A felhőalapú számítástechnika az adatok elérésének és tárolásának egyik módja. A felhőalapú szolgáltatások lehetővé teszik, hogy személyes fájlokat vagy éppen egy egész merevlemez biztonsági másolatát tároljuk interneten lévő távoli szervereken. Alkalmazások (pl.: szövegszerkesztők és képszerkesztők) is elérhetők a felhőn keresztül.

A felhő megnöveli a vállalkozások informatikai lehetőségeit anélkül, hogy új infrastruktúrába kellene beruházni, új embereket kellene kiképezni, vagy éppen új szoftverlicenceket vásárolni. Ezek a szolgáltatások igény szerint elérhetők, és a biztonság vagy a funkció veszélyeztetése nélkül gazdaságosan juttathatók el bármely eszközre a világon.

A felhőalapú szolgáltatások terjedése az adatközpontok miatt vált lehetségessé. Az adatközpont egy olyan létesítmény, amely számítógépes rendszereknek és a hozzájuk tartozó eszközöknek ad otthont. Egy adatközpont lehet szoba méretű, de elfoglalhat egy vagy több emeletet is, vagy akár egy egész épületet. Adatközpontokat általában nagyon drága felépíteni és fenntartani. Emiatt csak a nagy szervezetek tehetik meg, hogy saját adatközpontot építsenek és nyújtsanak általuk szolgáltatásokat a felhasználóik számára. A kisebb szervezetek, amelyek nem engedhetik meg maguknak a saját adatközpontot, egy nagyobb adatközponttól vesznek bérbe szerver- és tárolási szolgáltatásokat.

A biztonság, a megbízhatóság és a hibatűrés érdekében a felhőszolgáltatók gyakran tárolják az adatokat elosztott adatközpontokban. Azért, hogy egy személy vagy szervezet összes adatát ne csak egy adatközpont tárolja, inkább több, különböző helyen lévő adatközpont használata preferált.

Négy elsődleges felhőtípus létezik: Publikus felhők, Privát felhők, Hibrid felhők és Közösségi felhők, amint azt a táblázat is mutatja.

### Felhőtípusok

| Táblázat felirata | |
| --- | --- |
| **Felhő típusa** | **Leírás** |
| **Publikus felhő** | A publikus felhő által biztosított alkalmazások és szolgáltatások mindenki számára elérhetők. A szolgáltatások lehetnek ingyenesek, de használat alapján fizetősek is, ilyen az online tárhely bérlése. A publikus felhő interneten biztosítja a szolgáltatásait. |
| **Privát felhő** | A privát felhő által biztosított alkalmazásokat és szolgáltatásokat egy bizonyos szervezet vagy felhasználói kör számára hozzák létre. A privát felhő üzemelhet a szervezet saját hálózatán belül, bár ennek létrehozása és üzemeltetése költséges. Üzemeltethető a szervezeten kívül is, ilyenkor természetesen szigorú hozzáférési biztonság megvalósításával. |
| **Hibrid felhő** | A hibrid felhő kettő vagy több felhőből áll (pl.: részben privát, részben publikus), ahol mindegyik rész elkülöníthető objektum, de ugyanaz az architektúra köti őket össze. A hibrid felhő felhasználói a felhasználói jogaiktól függően különböző fokú hozzáférést kapnak a felhő szolgáltatásaihoz. |
| **Közösségi felhő** | A közösségi felhőt egy bizonyos kör vagy szervezet kizárólagos használatára hozzák létre. A publikus és a közösségi felhő közti különbség az, hogy a közösségi felhő funkcióit a közösség igényeihez szabják. Például az egészségügyi szervezeteknek bizonyos szabályok és jogszabályok speciális hitelesítési és titoktartási előírásainak kell megfelelniük. A közösségi felhőt olyan szervezetek használják, amelyeknek hasonló szükségleteik és feltételeik vannak. A közösségi felhő hasonlít a publikus felhő környezetéhez, de meghatározott biztonsági, titoktartási és szabályozási előírásokkal. |

1.7.7

## Technológiai trendek az otthonunkban

A hálózati trendek nemcsak a munkahelyi vagy iskolai kommunikációnkat befolyásolják, de kifejtik hatásukat sok otthoni tevékenységünkre is. A legújabb ilyen otthoni tendencia az "intelligens otthon technológia" vagy "okosotthon technológia" (smart home technology).

Az intelligens otthon olyan technológia, amely beépül a nap mint nap használt készülékeinkbe, lehetővé téve, hogy azok más eszközökkel kapcsolódjanak össze, ezáltal "okosabbá" vagy automatizáltabbá téve őket. Például, mielőtt reggel elmegyünk otthonról, előkészítjük az ételt és berakjuk a sütőbe. Az intelligens sütőt beprogramozzuk, beállítjuk rajta, hogy mit szeretnénk sütni. A sütő a naptárunkkal is összekapcsolódik, meg tudja határozni, hogy mikorra legyen kész az étel, és annak megfelelően állítja be a kezdési időt és a sütés hosszát. Még a napirendünk váratlan változásához is hozzá tudná igazítani a sütés idejét és hőfokát. Ezen túl okostelefonnal vagy tablettel közvetlenül is csatlakozhatnánk a sütőhöz, és változtathatunk a beállításokon. Amikor az étel készen van, a sütő figyelmeztető üzenetet küld nekünk (vagy akit megadunk), hogy az étel elkészült, majd melegen tartja.

Az okosotthon technológiák az otthonunk minden szobájában meg fognak jelenni. Az otthoni hálózatok és a nagy sebességű internetkapcsolatok elterjedésével hétköznapi dolog lesz az okos otthon.

Intelligens otthoni technológia ábrázolása, amely egy felhőt mutat, nyilakkal egy házra, egy autóra és egy okostelefonra. Alul a következő szöveg olvasható: Az okos telefon a felhőből frissül az intelligens otthoni eszközök és az okosautó állapotával; a felhasználó ezután az okos telefon segítségével interakcióba léphet az okosotthonnal és az intelligens autóval.



Felhő

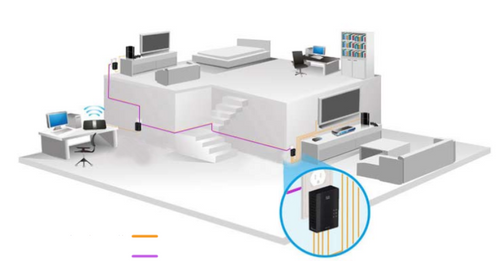
Az okostelefon a felhőből frissíti az okosotthon eszközeinek és az intelligens autó állapotát. A felhasználó ezután a telefon használatával kapcsolatba is léphet az otthonnal és az autóval.

1.7.8

## Hálózat az elektromos hálózaton

Az elektromos hálózatot használó adathálózat (powerline network) a már meglévő elektromos kábelezést használja az eszközök összeköttetésére, ahogy ezt az ábra is mutatja.

Egy otthon nyitott alaprajza elektromos hálózatot használó otthoni hálózathoz. Három PLEK400 4 portos tápvonali adapter van csatlakoztatva három különböző elektromos aljzathoz, amelyek mindegyike vezetékes csatlakozással van összekötve. Minden adapternek legalább egy hálózati csatlakozása van egy hálózati eszközhöz, beleértve az asztali számítógépeket és a tévéket.



**400 PLEK**   
4 portos Powerline   
Adapter Wireless-N   
Router **PLE400 PLSK400**   
4 portos Powerline   
Adapter Powerline csatlakozás Vezetékes csatlakozás

Egy szabványos powerline adapter segítségével egy eszköz bárhol a LAN-ra csatlakoztatható, ahol konnektor van. Nem kell adatkábeleket telepíteni, és alig használ plusz elektromos energiát. Az adatkommunikáció és az áramellátás ugyanazt a vezetéket használja, csak a powerline hálózat az adatokat más frekvencián küldi.

A powerline hálózat különösen akkor hasznos, ha vezeték nélküli hozzáférési pontokkal nem tudjuk lefedni az egész otthonunkat. A powerline hálózat nem a dedikált adatkábel helyettesítésére való. Ugyanakkor egy lehetséges alternatíva akkor, ha a kapcsolat hálózati kábellel vagy vezeték nélküli kommunikációval nem megoldható.

1.7.9

## Vezeték nélküli szélessávú hozzáférés

Számos olyan területen, ahol a kábel és a DSL nem áll rendelkezésre, vezeték nélküli kapcsolattal is megoldható az internethasználat.

**Vezeték nélküli internetszolgáltató**

A vezeték nélküli internetszolgáltató (Wireless Internet Service Provider, WISP) egy olyan szolgáltató, amely az otthoni WLAN-hálózatokhoz hasonló technológiát alkalmazva csatlakoztatja az előfizetőket egy kijelölt hozzáférési ponthoz vagy hot spothoz. WISP-ek gyakran találhatók olyan vidéki helyeken, ahol a DSL vagy kábeles szolgáltatások nem állnak rendelkezésre.

Habár külön adótornyot is lehet az antenna számára telepíteni, mégis gyakori, hogy az antenna egy már meglévő magas szerkezetre csatlakozik, mint például egy víztorony vagy egy rádiótorony. A WISP adóállomásának hatókörében az előfizetők házának a tetejére egy kis parabola vagy más típusú antennát kell telepíteni. Az előfizető hozzáférését biztosító eszköz a házon belüli vezetékes hálózatra csatlakozik. Az otthoni felhasználó szemszögéből ez a megoldás nem sokban különbözik a DSL vagy kábeles szolgáltatástól. A legfőbb különbség, hogy az előfizető és az ISP közötti kapcsolat a fizikai kábel helyett vezeték nélküli átvitellel van megoldva.

**Vezeték nélküli szélessávú szolgáltatás**

Az otthoni és kisvállalkozások számára egy másik vezeték nélküli megoldás a vezeték nélküli szélessávú hozzáférés, ez látható az ábrán.



Ez a megoldás ugyanazt a mobiltechnológiát használja, mint az okostelefonok. A házon kívül egy antenna kerül telepítésre, amely a házon belüli eszközöknek vezeték nélküli vagy akár vezetékes csatlakozást is biztosíthat. Számos helyen az otthoni vezeték nélküli szélessávú elérés egyenesen a DSL vagy a kábeles szolgáltatások versenytársa.

1.7.10

## Tudáspróba - Hálózati trendek

Az űrlap teteje

Ellenőrizze, hogy megértette-e a hálózati trendeket, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik szolgáltatás jó konferenciaeszköz a városodban vagy akár egy másik országban élő másokkal való használatra?

Az űrlap alja

Melyik funkció írja le személyes eszközök használatát az információk eléréséhez és az üzleti vagy egyetemi hálózaton keresztüli kommunikációhoz?

Melyik funkció tartalmaz olyan opciókat, mint a Nyilvános, Privát, Egyéni és Hibrid?

Melyik funkciót használja a rendszer, amikor egy eszközt elektromos aljzaton keresztül csatlakoztat a hálózathoz?

Which feature uses the same cellular technology as a smartphone?

[1.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Megbízható hálózatok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatbiztonság](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                         
*                               

1. A hálózat jelene
2. Hálózatbiztonság

# Hálózatbiztonság

1.8.1

## Biztonsági fenyegetések

Biztos mindenki hallott vagy olvasott híreket olyanról, hogy egy cég hálózatába betörtek, és több ezer ügyfél személyes adataihoz fértek hozzá. Emiatt a hálózatbiztonság a rendszergazdák elsődleges prioritása.

A hálózatbiztonság szerves része a számítógépes hálózatoknak, függetlenül attól, hogy ez csak egy otthoni környezetben lévő hálózat internetkapcsolattal, vagy egy nagyvállalati, több ezer felhasználós hálózat. A hálózatbiztonsági rendszernek figyelembe kell venni az adott környezetet, a hálózati eszközöket és a hálózat egyéb követelményeit. Meg kell tudni védeni az adatokat úgy, hogy a felhasználók által elvárt minőségű szolgáltatást továbbra is biztosítsuk.

A hálózat biztonságossá tétele és a fenyegetések kivédése speciális protokollok, technológiák, eszközök és technikák használatával érhető el. A fenyegetések érkezhetnek kívülről vagy belülről. Napjainkban sok fenyegetés érkezik az internetről.

A hálózatok gyakori külső fenyegetései:

* **Vírusok, férgek és trójai programok** - Rosszindulatú szoftvereket vagy kódokat tartalmaznak, és a felhasználó eszközén futnak.
* **Kémprogram (spyware) és reklámprogram (adware)** \ - A felhasználó eszközére telepített programok, amelyek titokban információkat gyűjtenek a felhasználóról.
* **Nulladik napi (zero-day) támadás** - Más néven nulladik órás támadás, egy biztonsági rés ismertté válásának napján megjelenő támadás.
* **Személyes fenyegetés** - Egy rosszindulatú személy felhasználói eszközöket vagy hálózati erőforrásokat támad meg.
* **Szolgáltatás-megtagadásos támadás** - Lelassít vagy elérhetetlenné tesz szolgáltatásokat és folyamatokat egy hálózati eszközön.
* **Adatlehallgatás és -lopás** — Ez a támadás személyes adatokat rögzít egy szervezet hálózatából.
* **Személyazonosság-lopás** - A támadó egy felhasználó belépési adatait lopja el, hogy privát adatokhoz férjen hozzá.

Ugyanilyen fontos, hogy figyelembe vegyük a belső fenyegetéseket is. Számos tanulmány kimutatta, hogy az adatokkal történő visszaélések leggyakrabban a hálózat belső felhasználói miatt történnek. Ez az elvesztett vagy ellopott eszközöknek, az alkalmazottak véletlen hibáinak, vagy üzleti környezetben akár még a rosszindulatú alkalmazottaknak is tulajdonítható. Az elterjedő BYOD-stratégiák miatt a vállalati adatok sokkal sérülékenyebbé válnak. Ezért egy biztonsági házirend kialakításakor egyformán kell figyelembe venni a külső és belső biztonsági fenyegetéseket is (lásd az ábrát).

two arrows leading to a compromised host; one coming from the Internet cloud going through a firewall, the other coming from an internal threat on the inside network

InternetInternal  
ThreatCompromised HostExternal  
Threat

1.8.2

## Biztonsági megoldások

Egyetlen megoldás nem képes megvédeni a hálózatot a különböző fenyegetésektől. A biztonságot emiatt több rétegben, több biztonsági megoldást is alkalmazva kell megvalósítani. Ha az egyik biztonsági összetevő nem azonosítja a támadást, vagy nem tudja megvédeni attól a hálózatot, akkor még mindig ott van egy másik összetevő is.

Az otthoni hálózatbiztonsági rendszerek általában meglehetősen egyszerűek. Általában a végberendezéseken valósítunk meg egy megoldást, valamint az internethez való csatlakozás pontjánál, de használhatunk a szolgáltató által biztosított eszközt is.

Az alapvető biztonsági összetevők egy otthoni vagy kisvállalati hálózathoz:

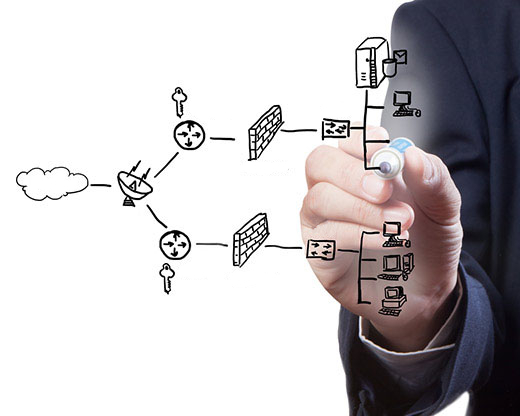
* **Vírus- és kémprogramkereső** - Ezek az alkalmazások segítenek megvédeni a végberendezéseket a kártékony szoftverekkel való fertőzéstől.
* **Tűzfal** - A tűzfal forgalomszűrése blokkolja a hálózathoz való jogosulatlan hozzáférést. Ez lehet munkaállomás alapú tűzfalrendszer, amely megakadályozza a jogosulatlan hozzáférést a munkaállomáshoz, vagy az otthoni router is képes lehet megakadályozni alapvető szűrési beállításokkal a külvilág irányából a belső hálózathoz történő jogosulatlan hozzáférést.

Ezzel szemben nagyvállalati környezetben a hálózatbiztonság megvalósítása több elemből tevődik össze, amelyek folyamatosan figyelik és szűrik a forgalmat. Ideális esetben minden összetevő együttműködik, ami minimálisra csökkenti a karbantartási feladatokat és növeli a biztonságot. A nagyobb hálózatok és a vállalati hálózatok víruskeresőt, kémprogramelhárítót és tűzfalszűrést használnak, de más biztonsági követelményekkel is rendelkeznek:

* **Dedikált tűzfalrendszerek** - Fejlettebb tűzfalfunkcióik vannak, és képesek részletesebb beállításokkal jóval nagyobb forgalom szűrésére.
* **Hozzáférési listák (ACL)** - IP-címek és alkalmazások alapján további szűrést valósítanak meg.
* **Behatolás-megelőző rendszerek (IPS)** - Képesek azonosítani a gyorsan terjedő fenyegetéseket, mint amilyenek a nulladik napi vagy nulladik órás támadások.
* **Virtuális magánhálózatok (VPN)** - Biztonságos hozzáférést biztosítanak a szervezethez távoli dolgozók számára.

A hálózatbiztonsági követelményeknek figyelembe kell venniük a hálózati környezetet, valamint a különféle alkalmazásokat és informatikai követelményeket. Mind az otthoni, mind pedig az üzleti környezeteknek képeseknek kell lenniük megvédeni az adatokat, miközben továbbra is biztosítaniuk kell minden technológia számára az elvárt szolgáltatásminőséget. Emellett a megvalósított biztonsági megoldásnak illeszkednie kell a folyamatosan növekvő és változó hálózati trendekhez.

A hálózati szolgáltatások rendszerezéséhez a hálózatbiztonsági fenyegetésekről és a védekezésről szóló tanulmányoknak a hálózat kapcsolási (switching) és forgalomirányítási (routing) infrastruktúrájának tiszta megértésével kell kezdődni.



InternetAccess ListFirewallLANLANFirewallACL

1.8.3

## Tudáspróba - Hálózatbiztonság

Az űrlap teteje

Check your understanding of network security by choosing the BEST answer to the following questions.

1. Which attack slows down or crashes equipment and programs?

Az űrlap alja

Which option creates a secure connection for remote workers?

Which option blocks unauthorized access to your network?

Which option describes a network attack that occurs on the first day that a vulnerability becomes known?

Which option describes malicious code running on user devices?

[1.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati trendek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IT szakértő](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                          
*                               

1. A hálózat jelene
2. Az IT szakértő

# Az IT szakértő

1.9.1

## CCNA

Van olyan NetAcad diák, aki már aktív informatikai karrierrel rendelkezik, de lehet, hogy van, aki még azért tanul, hogy felkészüljön a karrierjének indulására. Mindkét esetben hasznos ismerni az informatikai álláshelyekhez szükséges készségeket.

A hálózati mérnökök szerepe és készségei folyamatosan fejlődnek, és fontosabbak, mint valaha. A Cisco Certified Network Associate (CCNA) tanúsítvány igazolja, hogy a tulajdonosa ismeri az alapvető technológiákat, és garantálja, hogy a következő generációs technológiák elfogadásához szükséges kompetenciákkal kapcsolatban továbbra is naprakész tud maradni.

Az egységesített és frissített CCNA a hálózatépítő mérnökök számára három tanfolyamot és egy vizsgát jelent, ezek minden hálózati technológia alapvető témaköreit lefedik. Az új CCNA az IP alapjaira és a biztonságra, valamint a vezeték nélküli, virtualizálási, automatizálási és hálózati programozhatósági témákra összpontosít.

Új DevNet minősítések állnak rendelkezésre alap, specialista és professzionális szinteken, melyek a szoftverfejlesztői készségeket igazolják.

Speciális tanúsítási lehetőségek is rendelkezésre állnak, melyek a munkánknak és érdeklődésünknek megfelelő készségekhez kapcsolódnak. Ez magában foglalja a Cisco Enterprise Advanced Infrastructure Specialist tanúsítványt.

Ott kezdhetjük, ahol akarjuk. Nincsenek előfeltételei az alapszintű, specialista, professzionális vagy szakértői szintű minősítések megszerzésének. Már elérhetők az újraminősítéshez és továbbfejlődéshez szükséges továbbképzési kreditek a CCNA-ban.

1.9.2

## Hálózattal kapcsolatos állások

A CCNA tanúsítvány sokféle állásra felkészít a munkaerőpiacon. A [www.netacad.com](http://www.netacad.com) oldalon kattintsunk a Carreers menüre, majd ott az Employment opportunities lehetőségre. Az új program, a Talent Bridge Matching Engine segítségével lakhelyünkön is találhatunk munkalehetőségeket. Kereshetünk állást a Cisco-nál, valamint a Cisco partnereknél és forgalmazóknál, akik folyamatosan keresik a Cisco Hálózati Akadémia hallgatóit és már végzett diákjait.

Az Indeed, Glassdoor és Monster online keresőmotorok segítségével is kereshetünk informatikai állásokat. Használjunk olyan keresési kifejezéseket, mint az informatika, hálózati rendszergazda, hálózattervező vagy hálózati rendszeradminisztrátor. A Cisco CCNA kifejezés is hasznos lehet.

1.9.3

## Laborgyakorlat - Informatikai és hálózati állások keresése

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: Állásajánlatok keresése
  2. rész: A keresés tapasztalatainak megbeszélése

[1.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatbiztonság](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[1.10](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                         

1. A hálózat jelene
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

1.10.1

## Miről tanultunk ebben a fejezetben?

**A hálózatok hatása az életünkre**

A mai világban a hálózatoknak köszönhetően sose látott mértékben állunk összeköttetésben egymással. Ötleteinket azonnal megoszthatjuk másokkal, hogy azok valósággá válhassanak. Az online közösségek létrejötte és az információ szabad áramlása világszerte magában hordozza a termelékenység növekedését. A felhőalapú számítástechnika lehetővé teszi, hogy dokumentumokat és képeket tároljunk, és azokhoz bárhol, bármikor hozzáférhessünk.

**A hálózatok részei**

Minden olyan számítógépet állomásnak nevezünk, amely csatlakozik a hálózathoz és közvetlenül részt vesz a hálózati kommunikációban. Az állomásokat végberendezéseknek vagy hosztnak (host) is nevezzük. Bizonyos állomásokat kliensnek (client, ügyfél) is nevezünk. Sok számítógép kiszolgáló és ügyfél is a hálózaton. Az ilyen hálózatot egyenrangú hálózatnak nevezzük. A végberendezés vagy a forrása, vagy a célja a hálózaton átvitt üzeneteknek. A közvetítő eszközök kötik össze az egyes állomásokat a hálózattal, egyben más hálózatok felé is lehetővé téve az átjárást. A közvetítő eszközök a céleszköz címének és a hálózati kapcsolatokról való saját információik segítségével meghatározzák az üzenetek útvonalát a hálózaton keresztül. A közeg biztosítja a csatornát, hogy az üzenetek eljussanak a forrástól a céljukig.

**A hálózatok megjelenítése és a topológiák**

A hálózatdiagramok gyakran használnak olyan szimbólumokat, amelyek a hálózatot alkotó különböző eszközöket és kapcsolatokat jelképezik. Egy ábra használata egyszerű módja annak, hogy megértsük egy nagy hálózat felépítését. Ezt a fajta hálózati "képet" topológiai ábrának nevezzük. A fizikai topológiai diagramok szemléltetik a közvetítő eszközök fizikai helyét és a kábeltelepítést. A logikai topológiai diagramok a hálózat eszközeit, portjait és címzési sémáját szemléltetik.

**Gyakori hálózattípusok**

Egy kisméretű otthoni hálózat néhány számítógépet kapcsol össze egymással és az internettel. Az otthoni vagy kisvállalati (SOHO) hálózat az otthoni vagy távoli iroda számítógépeit kapcsolja össze a céges hálózattal, vagy központi, megosztott erőforrások elérését teszi lehetővé. A közepes és nagy hálózatok, mint például vállalati vagy iskolai hálózatok, sok helyszínen, több száz vagy ezer számítógépet kapcsolnak össze. Az internet a hálózatok hálózata, ami több száz millió számítógépet kapcsol össze világszerte. A hálózati infrastruktúrák két leggyakoribb típusa a helyi hálózat (LAN) és a nagy kiterjedésű hálózat (WAN). A helyi hálózat (LAN) kis földrajzi területet lefedő hálózat. A WAN nagy földrajzi területet lefedő hálózati infrastruktúra. Az intranet egy szervezethez tartozó LAN-ok és WAN-ok közötti privát kapcsolatra utal. Egy szervezet használhat extranetet, hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is.

**Internetkapcsolat**

SOHO internetkapcsolat például a kábeles, a DSL, a mobilnetes, a műholdas és a betárcsázós kapcsolat. Üzleti internetkapcsolat többek között a dedikált bérelt vonal, a Metro Ethernet, az üzleti DSL és a műholdas kapcsolat. A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei. A hagyományos különálló hálózatok különböző technológiákat, szabályokat és szabványokat alkalmaztak. A konvergált hálózatok adatokat, hangokat és videókat szállítanak különböző típusú eszközök között ugyanazon a hálózati infrastruktúrán keresztül. Ez a hálózati infrastruktúra már ugyanazokat a szabályokat, megállapodásokat és megvalósítási szabványokat használja. A Packet Tracer egy rugalmas program, amely lehetőséget ad arra, hogy hálózati ábrák és elvek használatával egészen bonyolult LAN-okat és WAN-okat építsünk és vizsgáljunk.

**Megbízható hálózatok**

A hálózati architektúra kifejezés azokra a technológiákra utal, amelyek támogatják azt az infrastruktúrát, valamint a különböző programozott szolgáltatásokat és szabályokat (más néven protokollokat), amelyek adatokat küldenek a hálózaton keresztül. A hálózatok fejlődésével kialakult az a négy alapvető jellemző, amelyet a hálózat tervezőjének meg kell valósítania, ha teljesíteni szeretné a felhasználók elvárásait: hibatűrés, skálázhatóság, szolgáltatásminőség és biztonság. Egy hibatűrő hálózat hiba előfordulása esetén minimalizálni tudja az érintett eszközök számát. Redundanciának hívják, ha egy célállomáshoz egyszerre több út is vezet. A skálázható hálózatot nagyon gyorsan lehet bővíteni az új felhasználók és alkalmazások támogatásához. A hálózatok azért skálázhatók, mert a tervező követi az elfogadott szabványokat és protokollokat. A QoS a torlódások kezelésére és a tartalom megbízható továbbítására használt elsődleges mechanizmus minden felhasználó számára. Két típusú hálózatbiztonsági probléma létezik, amelyekkel foglalkozni kell: a hálózati infrastruktúra biztonsága és az információbiztonság. A hálózatbiztonság céljainak elérése érdekében három elsődleges követelmény van: a bizalmasság, az integritás és a rendelkezésre állás.

**Hálózati trendek**

Több új hálózati trend van, amely a szervezetek és felhasználók munkáját befolyásolja: a Bring Your Own Device, az online csoportmunka, a videokommunikáció és a felhőalapú számítástechnika. A BYOD lényege, hogy bármilyen eszközt bárhol használhatunk, akárki is legyen a tulajdonosa. A csoportmunkát segítő eszközök (pl.: a Cisco Webex) azonnali kapcsolatfelvételt, együttműködést és a közös célok elérését teszik lehetővé alkalmazottak, diákok, tanárok, vásárlók vagy egyéb partnerek számára. A kommunikációban, együttműködésben és a szórakozásban egyaránt fontos szerepe van a videóknak. Bárki indíthat és fogadhat videohívást, akinek internetkapcsolata van, bárhol is legyen. A felhőalapú szolgáltatások lehetővé teszik, hogy személyes fájlokat vagy éppen egy egész merevlemez biztonsági másolatát tároljuk interneten lévő távoli szervereken. Alkalmazások (pl.: szövegszerkesztők és képszerkesztők) is elérhetők a felhőn keresztül. Négy elsődleges felhőtípus létezik: Publikus felhők, Privát felhők, Hibrid felhők és Közösségi felhők. Az okosotthon technológiák az otthonunk minden szobájában meg fognak jelenni. Az otthoni hálózatok és a nagy sebességű internetkapcsolatok elterjedésével hétköznapi dolog lesz az okos otthon. Az adatkommunikáció és az áramellátás ugyanazt a vezetéket használja, csak a powerline hálózat az adatokat más frekvencián küldi. A vezeték nélküli internetszolgáltató (Wireless Internet Service Provider, WISP) egy olyan szolgáltató, amely az otthoni WLAN-hálózatokhoz hasonló technológiát alkalmazva csatlakoztatja az előfizetőket egy kijelölt hozzáférési ponthoz vagy hot spothoz.

**Hálózatbiztonság**

A hálózatok gyakori külső fenyegetései:

* Vírusok, férgek és trójai programok
* Kémprogram és reklámprogram (spyware és adware)
* Nulladik napi támadások
* Személyes támadások
* Szolgáltatás-megtagadásos támadások
* Adatlehallgatás és -lopás
* Személyazonosság-lopás

Az alapvető biztonsági összetevők egy otthoni vagy kis irodai hálózathoz:

* Vírus- és kémprogramvédelem
* Tűzfalszűrés

A nagyobb hálózatok és a vállalati hálózatok víruskeresőt, kémprogramelhárítót és tűzfalszűrést használnak, de más biztonsági követelményekkel is rendelkeznek:

* Dedikált tűzfalrendszerek
* Hozzáférési listák (ACL)
* Behatolás-megelőző rendszerek (IPS)
* Virtuális magánhálózatok (VPN)

**Az IT szakértő**

A Cisco Certified Network Associate (CCNA) tanúsítvány igazolja, hogy a tulajdonosa ismeri az alapvető technológiákat, és garantálja, hogy a következő generációs technológiák elfogadásához szükséges kompetenciákkal kapcsolatban továbbra is naprakész tud maradni. A CCNA tanúsítvány a piac sokféle munkahelyére felkészít. A [www.netacad.com](http://www.netacad.com) oldalon kattintsunk a Carreers menüre, majd ott az Employment opportunities lehetőségre. A Talent Bridge Matching Engine segítségével lakhelyünkön is találhatunk munkalehetőségeket. Kereshetünk állást a Cisco-nál, valamint a Cisco partnereknél és forgalmazóknál, akik folyamatosan keresik a Cisco Hálózati Akadémia hallgatóit és már végzett diákjait.

1.10.2

## Ellenőrző kvíz - Hálózatok ma

Az űrlap teteje

1. Egy rutinellenőrzés során a szakember észrevette, hogy a számítógépre olyan programot telepítettek, amely titokban adatot gyűjt a számítógép felhasználói által meglátogatott weboldalakról. Hogy hívjuk ezt a fajta fenyegetést, támadás fajtát?

Az űrlap alja

Melyik kifejezés utal olyan hálózatra, amely a beszállítók, ügyfelek és partnerek számára biztonságos hozzáférést biztosít a vállalati irodákhoz?

Egy nagyvállalat módosította a hálózatot, hogy lehetővé tegye a felhasználók számára, hogy hozzáférjenek a hálózati erőforrásokhoz személyes laptopjaikról és okostelefonjaikról. Melyik hálózati trendet írja le ez?

Mi az ISP?

Milyen esetben javasolnánk WISP (vezetéknélküli internetszolgáltató) üzemeltetését?

A hálózat mely jellemzői teszik lehetővé annak gyors növekedését, hogy új felhasználókat és alkalmazásokat támogasson anélkül, hogy befolyásolná a meglévő felhasználóknak nyújtott szolgáltatás teljesítményét?

Egy főiskola új kollégiumot épít. A munkások árkot ásnak a földbe, hogy új vízvezetéket telepítsenek a kollégiumba. Egyikük véletlenül kárt tesz az optikai kábelben, amely a két meglévő kollégiumot összeköti az egyetemi adatközponttal. Bár a kábelt elvágták, a kollégiumi hallgatók csak a hálózati szolgáltatások nagyon rövid megszakadását tapasztalják. Mi jellemző erre a hálózatra?

Mi a skálázható hálózatok két jellemzője? (Két jó válasz van.)

Melyik eszköz feladata annak az útvonalnak a meghatározása, amelyen az üzenetek továbbítódnak a hálózatok között?

Melyik két internet kapcsolódási típus esetén nincs szükség fizikai kábelezést kiépíteni az épületig? (Két jó válasz van.)

Melyik hálózattípusra van szüksége egy otthoni felhasználónak, ha online szeretne vásárolni?

Hogyan változtatja meg a BYOD a hálózatok megvalósításának módját?

A munkavállaló távolról, a lehető legbiztonságosabb módon szeretne hozzáférni a szervezet hálózatához. Milyen hálózati funkció teszi lehetővé az alkalmazott számára, hogy biztonságos távoli hozzáférést szerezzen egy vállalati hálózathoz?

What is the Internet?

Milyen két funkciója van a végfelhasználói eszközöknek a hálózaton? (Két jó válasz van.)

[1.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IT szakértő](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                         

1. A hálózat jelene
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

1.10.1

## Miről tanultunk ebben a fejezetben?

**A hálózatok hatása az életünkre**

A mai világban a hálózatoknak köszönhetően sose látott mértékben állunk összeköttetésben egymással. Ötleteinket azonnal megoszthatjuk másokkal, hogy azok valósággá válhassanak. Az online közösségek létrejötte és az információ szabad áramlása világszerte magában hordozza a termelékenység növekedését. A felhőalapú számítástechnika lehetővé teszi, hogy dokumentumokat és képeket tároljunk, és azokhoz bárhol, bármikor hozzáférhessünk.

**A hálózatok részei**

Minden olyan számítógépet állomásnak nevezünk, amely csatlakozik a hálózathoz és közvetlenül részt vesz a hálózati kommunikációban. Az állomásokat végberendezéseknek vagy hosztnak (host) is nevezzük. Bizonyos állomásokat kliensnek (client, ügyfél) is nevezünk. Sok számítógép kiszolgáló és ügyfél is a hálózaton. Az ilyen hálózatot egyenrangú hálózatnak nevezzük. A végberendezés vagy a forrása, vagy a célja a hálózaton átvitt üzeneteknek. A közvetítő eszközök kötik össze az egyes állomásokat a hálózattal, egyben más hálózatok felé is lehetővé téve az átjárást. A közvetítő eszközök a céleszköz címének és a hálózati kapcsolatokról való saját információik segítségével meghatározzák az üzenetek útvonalát a hálózaton keresztül. A közeg biztosítja a csatornát, hogy az üzenetek eljussanak a forrástól a céljukig.

**A hálózatok megjelenítése és a topológiák**

A hálózatdiagramok gyakran használnak olyan szimbólumokat, amelyek a hálózatot alkotó különböző eszközöket és kapcsolatokat jelképezik. Egy ábra használata egyszerű módja annak, hogy megértsük egy nagy hálózat felépítését. Ezt a fajta hálózati "képet" topológiai ábrának nevezzük. A fizikai topológiai diagramok szemléltetik a közvetítő eszközök fizikai helyét és a kábeltelepítést. A logikai topológiai diagramok a hálózat eszközeit, portjait és címzési sémáját szemléltetik.

**Gyakori hálózattípusok**

Egy kisméretű otthoni hálózat néhány számítógépet kapcsol össze egymással és az internettel. Az otthoni vagy kisvállalati (SOHO) hálózat az otthoni vagy távoli iroda számítógépeit kapcsolja össze a céges hálózattal, vagy központi, megosztott erőforrások elérését teszi lehetővé. A közepes és nagy hálózatok, mint például vállalati vagy iskolai hálózatok, sok helyszínen, több száz vagy ezer számítógépet kapcsolnak össze. Az internet a hálózatok hálózata, ami több száz millió számítógépet kapcsol össze világszerte. A hálózati infrastruktúrák két leggyakoribb típusa a helyi hálózat (LAN) és a nagy kiterjedésű hálózat (WAN). A helyi hálózat (LAN) kis földrajzi területet lefedő hálózat. A WAN nagy földrajzi területet lefedő hálózati infrastruktúra. Az intranet egy szervezethez tartozó LAN-ok és WAN-ok közötti privát kapcsolatra utal. Egy szervezet használhat extranetet, hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is.

**Internetkapcsolat**

SOHO internetkapcsolat például a kábeles, a DSL, a mobilnetes, a műholdas és a betárcsázós kapcsolat. Üzleti internetkapcsolat többek között a dedikált bérelt vonal, a Metro Ethernet, az üzleti DSL és a műholdas kapcsolat. A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei. A hagyományos különálló hálózatok különböző technológiákat, szabályokat és szabványokat alkalmaztak. A konvergált hálózatok adatokat, hangokat és videókat szállítanak különböző típusú eszközök között ugyanazon a hálózati infrastruktúrán keresztül. Ez a hálózati infrastruktúra már ugyanazokat a szabályokat, megállapodásokat és megvalósítási szabványokat használja. A Packet Tracer egy rugalmas program, amely lehetőséget ad arra, hogy hálózati ábrák és elvek használatával egészen bonyolult LAN-okat és WAN-okat építsünk és vizsgáljunk.

**Megbízható hálózatok**

A hálózati architektúra kifejezés azokra a technológiákra utal, amelyek támogatják azt az infrastruktúrát, valamint a különböző programozott szolgáltatásokat és szabályokat (más néven protokollokat), amelyek adatokat küldenek a hálózaton keresztül. A hálózatok fejlődésével kialakult az a négy alapvető jellemző, amelyet a hálózat tervezőjének meg kell valósítania, ha teljesíteni szeretné a felhasználók elvárásait: hibatűrés, skálázhatóság, szolgáltatásminőség és biztonság. Egy hibatűrő hálózat hiba előfordulása esetén minimalizálni tudja az érintett eszközök számát. Redundanciának hívják, ha egy célállomáshoz egyszerre több út is vezet. A skálázható hálózatot nagyon gyorsan lehet bővíteni az új felhasználók és alkalmazások támogatásához. A hálózatok azért skálázhatók, mert a tervező követi az elfogadott szabványokat és protokollokat. A QoS a torlódások kezelésére és a tartalom megbízható továbbítására használt elsődleges mechanizmus minden felhasználó számára. Két típusú hálózatbiztonsági probléma létezik, amelyekkel foglalkozni kell: a hálózati infrastruktúra biztonsága és az információbiztonság. A hálózatbiztonság céljainak elérése érdekében három elsődleges követelmény van: a bizalmasság, az integritás és a rendelkezésre állás.

**Hálózati trendek**

Több új hálózati trend van, amely a szervezetek és felhasználók munkáját befolyásolja: a Bring Your Own Device, az online csoportmunka, a videokommunikáció és a felhőalapú számítástechnika. A BYOD lényege, hogy bármilyen eszközt bárhol használhatunk, akárki is legyen a tulajdonosa. A csoportmunkát segítő eszközök (pl.: a Cisco Webex) azonnali kapcsolatfelvételt, együttműködést és a közös célok elérését teszik lehetővé alkalmazottak, diákok, tanárok, vásárlók vagy egyéb partnerek számára. A kommunikációban, együttműködésben és a szórakozásban egyaránt fontos szerepe van a videóknak. Bárki indíthat és fogadhat videohívást, akinek internetkapcsolata van, bárhol is legyen. A felhőalapú szolgáltatások lehetővé teszik, hogy személyes fájlokat vagy éppen egy egész merevlemez biztonsági másolatát tároljuk interneten lévő távoli szervereken. Alkalmazások (pl.: szövegszerkesztők és képszerkesztők) is elérhetők a felhőn keresztül. Négy elsődleges felhőtípus létezik: Publikus felhők, Privát felhők, Hibrid felhők és Közösségi felhők. Az okosotthon technológiák az otthonunk minden szobájában meg fognak jelenni. Az otthoni hálózatok és a nagy sebességű internetkapcsolatok elterjedésével hétköznapi dolog lesz az okos otthon. Az adatkommunikáció és az áramellátás ugyanazt a vezetéket használja, csak a powerline hálózat az adatokat más frekvencián küldi. A vezeték nélküli internetszolgáltató (Wireless Internet Service Provider, WISP) egy olyan szolgáltató, amely az otthoni WLAN-hálózatokhoz hasonló technológiát alkalmazva csatlakoztatja az előfizetőket egy kijelölt hozzáférési ponthoz vagy hot spothoz.

**Hálózatbiztonság**

A hálózatok gyakori külső fenyegetései:

* Vírusok, férgek és trójai programok
* Kémprogram és reklámprogram (spyware és adware)
* Nulladik napi támadások
* Személyes támadások
* Szolgáltatás-megtagadásos támadások
* Adatlehallgatás és -lopás
* Személyazonosság-lopás

Az alapvető biztonsági összetevők egy otthoni vagy kis irodai hálózathoz:

* Vírus- és kémprogramvédelem
* Tűzfalszűrés

A nagyobb hálózatok és a vállalati hálózatok víruskeresőt, kémprogramelhárítót és tűzfalszűrést használnak, de más biztonsági követelményekkel is rendelkeznek:

* Dedikált tűzfalrendszerek
* Hozzáférési listák (ACL)
* Behatolás-megelőző rendszerek (IPS)
* Virtuális magánhálózatok (VPN)

**Az IT szakértő**

A Cisco Certified Network Associate (CCNA) tanúsítvány igazolja, hogy a tulajdonosa ismeri az alapvető technológiákat, és garantálja, hogy a következő generációs technológiák elfogadásához szükséges kompetenciákkal kapcsolatban továbbra is naprakész tud maradni. A CCNA tanúsítvány a piac sokféle munkahelyére felkészít. A [www.netacad.com](http://www.netacad.com) oldalon kattintsunk a Carreers menüre, majd ott az Employment opportunities lehetőségre. A Talent Bridge Matching Engine segítségével lakhelyünkön is találhatunk munkalehetőségeket. Kereshetünk állást a Cisco-nál, valamint a Cisco partnereknél és forgalmazóknál, akik folyamatosan keresik a Cisco Hálózati Akadémia hallgatóit és már végzett diákjait.

1.10.2

## Ellenőrző kvíz - Hálózatok ma

Az űrlap teteje

1. Egy rutinellenőrzés során a szakember észrevette, hogy a számítógépre olyan programot telepítettek, amely titokban adatot gyűjt a számítógép felhasználói által meglátogatott weboldalakról. Hogy hívjuk ezt a fajta fenyegetést, támadás fajtát?

Az űrlap alja

Melyik kifejezés utal olyan hálózatra, amely a beszállítók, ügyfelek és partnerek számára biztonságos hozzáférést biztosít a vállalati irodákhoz?

Egy nagyvállalat módosította a hálózatot, hogy lehetővé tegye a felhasználók számára, hogy hozzáférjenek a hálózati erőforrásokhoz személyes laptopjaikról és okostelefonjaikról. Melyik hálózati trendet írja le ez?

Mi az ISP?

Milyen esetben javasolnánk WISP (vezetéknélküli internetszolgáltató) üzemeltetését?

A hálózat mely jellemzői teszik lehetővé annak gyors növekedését, hogy új felhasználókat és alkalmazásokat támogasson anélkül, hogy befolyásolná a meglévő felhasználóknak nyújtott szolgáltatás teljesítményét?

Egy főiskola új kollégiumot épít. A munkások árkot ásnak a földbe, hogy új vízvezetéket telepítsenek a kollégiumba. Egyikük véletlenül kárt tesz az optikai kábelben, amely a két meglévő kollégiumot összeköti az egyetemi adatközponttal. Bár a kábelt elvágták, a kollégiumi hallgatók csak a hálózati szolgáltatások nagyon rövid megszakadását tapasztalják. Mi jellemző erre a hálózatra?

Mi a skálázható hálózatok két jellemzője? (Két jó válasz van.)

Melyik eszköz feladata annak az útvonalnak a meghatározása, amelyen az üzenetek továbbítódnak a hálózatok között?

Melyik két internet kapcsolódási típus esetén nincs szükség fizikai kábelezést kiépíteni az épületig? (Két jó válasz van.)

Melyik hálózattípusra van szüksége egy otthoni felhasználónak, ha online szeretne vásárolni?

Hogyan változtatja meg a BYOD a hálózatok megvalósításának módját?

A munkavállaló távolról, a lehető legbiztonságosabb módon szeretne hozzáférni a szervezet hálózatához. Milyen hálózati funkció teszi lehetővé az alkalmazott számára, hogy biztonságos távoli hozzáférést szerezzen egy vállalati hálózathoz?

What is the Internet?

Milyen két funkciója van a végfelhasználói eszközöknek a hálózaton? (Két jó válasz van.)

[1.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IT szakértő](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                               
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Bevezetés

# Bevezetés

2.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a switch-ek és végberendezések alapbeállításainak megadásával kapcsolatos fejezetben!

A hálózati munkánk részeként néha új hálózatot kell létrehoznunk, máskor egy régit kell karbantartanunk és fejlesztenünk. A switch-eket és végberendezéseket mindenképpen úgy kell beállítanunk, hogy biztonságosan és hatékonyan lássák el feladatukat.

A dobozból kivéve a switch-ek és a felhasználói végberendezések valamilyen alapbeállítással érkeznek. De ha egy bizonyos hálózatba illesztjük be őket, megfelelő beállításokkal és információval kell rendelkezniük. Ebben a fejezetben megtanuljuk, hogy miként férjünk hozzá a Cisco IOS-t futtató hálózati eszközökhöz. Megtanuljuk az alapvető beállítások parancsait, felkonfigurálunk IP-címeket és ellenőrizzük a Cisco eszközök és végberendezések beállításait.

Természetesen egy hálózat adminisztrációja sokkal több ennél, de minden az alapbeállításokkal kezdődik. Vágjunk bele!

2.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Switch-ek és végberendezések alapbeállításainak megadása

**Fejezet célja:** Switch-en és végberendezéseken végezzük el jelszavak, IP-címek és az alapértelmezett átjáró beállítását.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Cisco IOS hozzáférés** | Elmagyarázzuk, hogyan férhetünk hozzá egy Cisco IOS eszközhöz konfigurációs célokra. |
| **Navigálás az IOS-ban** | Megnézzük, hogyan navigálunk az IOS beállításai között. |
| **A parancsok szerkezete** | Megismerjük a Cisco IOS parancsainak szerkezetét. |
| **Alapbeállítások** | A Cisco IOS beállításait végezzük el parancssorból. |
| **Beállítások mentése** | Cisco IOS parancsok segítségével elmentjük a beállításokat. |
| **Portok és címek** | Elmagyarázzuk, hogyan kommunikálnak az eszközök a hálózati közegen. |
| **IP-címzés beállítása** | Beállítjuk egy állomás IP-címét. |
| **Kapcsolatok ellenőrzése** | Ellenőrizzük az összeköttetést két végberendezés között. |

[1.10](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Cisco IOS hozzáférés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                   
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Cisco IOS hozzáférés

# Cisco IOS hozzáférés

2.1.1

## Operációs rendszerek

Minden végberendezés és hálózati eszköz operációs rendszert (OS) igényel. Ahogy az ábrán is látható, az operációs rendszer azon részét, amely közvetlenül a számítógép hardverével kommunikál kernelnek nevezzük. Az alkalmazásokkal és a felhasználóval kapcsolatot teremtő része a felhasználói felület vagy shell. A felhasználói felület lehet parancssoros (command-line interface, CLI) vagy grafikus (graphical user interface, GUI).

There are three concentric circles that appear to radiate from the monitor of a computer labeled user interface. They show the relationship between the different portions of an operating system. The inner circle labeled hardware shows examples of computer hardware, the middle circle is labeled kernel, and the outer circle is labeled shell. Text at the bottom reads: Shell - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces; Kernel - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements; Hardware - The physical part of a computer including underlying electronics.

ShellKernelHardwareUser Interface

* **Felhasználói felület** - A felhasználók ezen keresztül avatkozhatnak be a számítógép működésébe. A beavatkozás történhet parancssoros (CLI) vagy grafikus (GUI) felhasználói felületről.
* **Kernel** - A hardver- és szoftverösszetevők közti kommunikációt végzi, ezen kívül a szoftverek igényeinek megfelelően a hardvererőforrások kezelése a feladata.
* **Hardver** - A számítógép fizikai alkatrészei, elektronikája.

A parancssor használata során a felhasználó karakteres környezetben kiadott utasításokkal közvetlenül a rendszerrel kommunikál, az ábrán látható módon. A rendszer végrehajtja a parancsot, amelynek végeredményéről általában szöveges üzenetet ad. A parancssor rendkívül kevés erőforrást igényel, viszont a felhasználónak elég részletesen meg kell ismernie a rendszer parancsainak struktúráját.

analyst@secOps ~]$ **ls**

Desktop Downloads lab.support.files second\_drive

[analyst@secOps ~]$

2.1.2

## Grafikus felhasználói felület

A grafikus felhasználói felület (pl.: a Windows, a macOS, a Linux KDE, az Apple iOS vagy az Android) grafikus ikonokkal, menükkel, ablakokkal teszik lehetővé a felhasználó beavatkozását a számítógép működésébe. Az ábrán látható grafikus felület felhasználóbarát, kevesebb tudást igényel az alatta levő rendszer belső szerkezetéről. Emiatt a legtöbb felhasználó a grafikus felületeket kedveli jobban.



Előfordulhat azonban, hogy a grafikus felület nem tud minden funkciót biztosítani, amit a parancssor tudna. A grafikus felületek néha meghibásodnak, összeomlanak, vagy nem úgy működnek, ahogy kellene. Ezen okok miatt a hálózati eszközöket általában parancssorból konfiguráljuk. A parancssor kevesebb erőforrást igényel és stabilabb, mint egy grafikus felület.

Szinte minden Cisco készülék a Cisco Internetwork Operating System (IOS) operációs rendszert használja. Cisco IOS fut a legtöbb Cisco eszközön tekintet nélkül annak típusára vagy méretére. Minden router vagy switch a Cisco IOS más-más verzióját használja. Egyéb Cisco operációs rendszerek például az IOS XE, az IOS XR és az NX-OS.

**MEGJEGYZÉS:** Az otthoni routerek operációs rendszerét általában \_firmware\_-nek nevezzük. Az otthoni eszközök konfigurálását legtöbbször böngésző alapú grafikus felületről végezzük.

2.1.3

## Az operációs rendszer feladata

A hálózati eszközök operációs rendszere hasonló a számítógépekéhez. A számítógépek grafikus felhasználói felületén keresztül a következőkre lehet képes a felhasználó:

* Kiválaszthat elemeket, és programokat futtathat egér segítségével.
* Szöveget vagy szöveges parancsokat írhat be.
* Monitoron nézheti a műveletek eredményét.

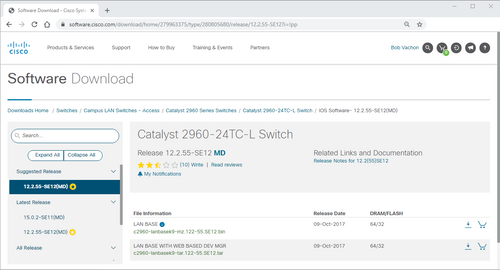
Egy parancssor alapú hálózati operációs rendszer (pl.: egy switch-ek és routerek által használt Cisco IOS) a következőket teszi lehetővé a hálózati szakember számára:

* Billentyűzettel parancssor alapú hálózati programokat futtathat.
* Szöveget vagy szöveges parancsokat írhat be.
* Monitoron nézheti a műveletek eredményét.

A Cisco hálózati eszközök a Cisco IOS meghatározott verzióit futtatják. A konkrét IOS-verzió a használt eszköz típusától és a szükséges funkcióktól függ. Bár az összes eszköz alap IOS-szel és szolgáltatáskészlettel kerül forgalomba, lehetőség van funkcióbővítés céljából az IOS-verzió vagy a szolgáltatáskészlet cseréjére.

Az ábra egy Cisco Catalyst 2960 switch IOS-szoftverkiadásait mutatja.

### Példa a Cisco IOS letöltésére



2.1.4

## Hozzáférési módok

Egy switch alapértelmezés szerint továbbítja a forgalmat, ehhez nem kell kifejezetten konfigurálni rajta semmit. Például két helyesen konfigurált állomás, amely ugyanahhoz az új switch-hez csatlakozik, képes lesz kommunikálni.

Az új switch alapértelmezett viselkedésétől függetlenül azonban minden switch-et fel kell konfigurálni és biztonságossá kell tenni.

| Table caption | |
| --- | --- |
| **Módszer** | **Leírás** |
| **Konzol** | Sávon kívüli elérést biztosító fizikai menedzsment port a Cisco eszközökön. A sávon kívüli azt jelenti, hogy ez egy dedikált felügyeleti csatorna kizárólag az eszköz karbantartására. A konzolport használatának előnye, hogy az eszköz akkor is elérhető, ha semmilyen hálózati szolgáltatás nincs még beállítva, mint például a kezdeti konfiguráció idején. A konzolkapcsolat létrehozásához a terminálemulációs szoftvert futtató számítógépet egy speciális konzolkábellel kell az eszközhöz csatlakoztatni. |
| **Secure Shell (SSH)** | Az SSH a javasolt sávon belüli módszer, hogy a hálózaton keresztül, virtuális interfész segítségével biztonságos parancssoros kapcsolatot létesítsünk. A konzolkapcsolattól eltérően az SSH-kapcsolatok aktív hálózati szolgáltatásokat igényelnek az eszközön, beleértve az aktivált és címmel beállított interfészt. A Cisco IOS legtöbb verziója tartalmaz SSH-szerver és SSH-kliens szoftvereket, amelyekkel más eszközökkel SSH-kapcsolatot létesíthetünk. |
| **Telnet** | A Telnet a parancssor nem biztonságos távoli elérési módja hálózaton keresztül, virtuális interfész segítségével. Az SSH-tól eltérően a Telnet nem kínál biztonságos, titkosított kapcsolatot, használata legfeljebb elkülönített teszthálózaton javasolt. A felhasználói hitelesítés, a jelszavak és a parancsok egyszerű szövegként kerülnek elküldésre a hálózaton. Ha tehetjük, használjunk SSH-t a Telnet helyett! A Cisco IOS Telnet szervert és klienset is tartalmaz. |

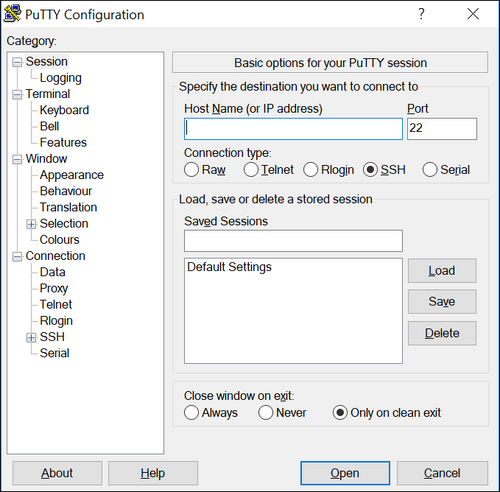
**MEGJEGYZÉS:** Néhány eszközön, általában a routereken találhatunk egy régi kiegészítő portot (auxilary port), amely arra volt használatos, hogy modem segítségével telefonvonalon keresztül férjünk hozzá a parancssorhoz. A konzolhoz hasonlóan az AUX-port is sávon kívüli, nem kellenek hozzá hálózati beállítások.

2.1.5

## Terminálemulációs programok

Sokfajta terminálemulátciós program létezik a hálózati eszközök konzolporton keresztüli soros eléréséhez és a távoli Telnet/SSH kapcsolódáshoz. Ezek a programok lehetővé teszik az ablakok méretezését, a betűkészlet változtatását és a színek beállítását, ezáltal is növelve a hatékonyságot.

Kattintsunk az egyes programok nevére a felületük képernyőfotójának megtekintéséhez!



2.1.6

## Tudáspróba - Cisco IOS hozzáférési módok

Az űrlap teteje

Check your understanding of Cisco IOS Access by choosing the BEST answer to the following questions.

1. Which access method would be most appropriate if you were in the equipment room with a new switch that needs to be configured?

Az űrlap alja

Which access method would be most appropriate if your manager gave you a special cable and told you to use it to configure the switch?

Which access method would be the most appropriate in-band access to the IOS over a network connection?

Which access method would be the most appropriate if you call your manager to tell him you cannot access your router in another city over the internet and he provides you with the information to access the router through a telephone connection?

[2.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Navigálás az IOS-ban](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                         
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Navigálás az IOS-ban

# Navigálás az IOS-ban

2.2.1

## Elsődleges módok

Az előző témakörben megtudtuk, hogy minden hálózati eszköznek operációs rendszerre van szüksége, és hogy ezek konfigurálhatók parancssorból vagy grafikus felületről. A parancssor pontosabb és rugalmasabb, mint a grafikus felület. Ez a témakör a Cisco IOS parancssoros elérésével foglalkozik.

Biztonsági okokból a Cisco IOS a felügyeletet az alábbi két parancssoros módra osztja:

* **Felhasználói EXEC mód** - Korlátozott lehetőségek, de alapvető műveletekhez megfelelő. Csak korlátozott számú lekérdező felügyeleti parancs használható, semmi olyan parancs nem engedélyezett, ami az eszköz beállításait megváltoztatná. A felhasználói EXEC módot a parancssor készenléti jelének (prompt) végén levő > szimbólum jelzi.
* **Privilegizált EXEC mód** - Beállításokat végző parancsok kiadásához a rendszergazdának privilegizált módban kell lennie. A magasabb beállítási módok (pl.: globális konfigurációs mód) csak innen érhetők el. A privilegizált EXEC módot a prompt jel végén levő # szimbólum jelzi.

A táblázat összefoglalja a két mód jellemzőit, és megmutatja az alapértelmezett prompt jelet switch és router esetében.

| Táblázat felirata | | |
| --- | --- | --- |
| **Parancsmód** | **Leírás** | **Készenléti (prompt) jel** |
| **Felhasználói EXEC mód** | * Korlátozott felügyeleti parancsok. * Néha megtekintő vagy lekérdező módnak is nevezik. | Kapcsoló>  Router> |
| **Privilegizált EXEC mód** | * Ebben a módban minden parancs és funkció elérhető. * A felhasználó bármilyen lekérdező és beállító parancsot használhat. | Kapcsoló#  Router# |

2.2.2

## Konfigurációs mód és alkonfigurációs módok

Az eszköz konfigurálásához a felhasználónak globális konfigurációs módba kell lépnie, amelyet röviden globális konfig módnak nevezünk.

A globális konfig módban az eszköz egészét érintő beállításokat hajtunk végre. A globális konfig módban a prompt jelben (config)# látható az eszköz neve után, például: **Switch(config)#** .

A többi specifikus konfigurációs mód előtt globális konfigurációs módba kell lépnünk. A globális konfig módból a felhasználó továbbléphet alkonfigurációs módokba. Mindegyik mód az IOS-eszköz valamelyik részének vagy funkciójának beállításához való. Két gyakran használt alkonfigurációs mód:

* **Vonalkonfigurációs mód -** Konzolos, SSH-, Telnet vagy AUX-hozzáférés konfigurálására szolgál.
* **Interfészkonfigurációs mód -** Switchport vagy router hálózati interfész beállítását végezzük innen.

A parancssor prompt jele minden módban más és más. Ezzel jelzi, hogy milyen módban vagyunk. Alapértelmezés szerint minden prompt jel az eszköz nevével kezdődik. A név utáni rész jelzi a módot. A vonalkonfigurációs mód prompt jele például **Switch(config)#** , az interfész konfigurációs mód alapértelmezett promptja pedig **Switch(config)#** .

2.2.3

## Videómagyarázat - Az IOS CLI elsődleges parancsmódjai

Az IOS-módok közötti navigációt bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

2.2.4

## Navigáció az IOS-módok között

Többféle parancs szolgál arra, hogy a különböző parancsmódok között ki-be járjunk. A felhasználói EXEC módból az **enable** paranccsal lehet privilegizált EXEC módba lépni. A **disable** paranccsal pedig visszajutunk a felhasználói EXEC módba.

**MEGJEGYZÉS:** A privilegizált módot néha \_enable módnak\_ is nevezzük.

Globális konfigurációs módba lépéshez használjuk a **configure terminal** privilegizált módú parancsot. Privilegizált módba visszatérés pedig az **exit** globális konfig módú paranccsal lehetséges.

Számos különböző alkonfigurációs mód létezik. Vonalkonfigurációs módba lépéshez a **line** parancsot kell használni, amelyet a vonal típusa és száma követ. Az **exit** paranccsal pedig kilépünk az alkonfigurációs módból, és visszakerülünk a globális konfig módba.

Switch(config)# **line console 0**

Switch(config-line)# **exit**

Switch(config)#

A globális konfigurációs mód bármelyik alkonfigurációs módjából a módok hierarchiáján eggyel feljebb léphetünk az **exit** paranccsal.

Ha bármelyik alkonfigurációs módból a privilegizált EXEC módba szeretnénk lépni, megtehetjük az **end** paranccsal vagy a **Ctrl+Z** billentyűkombinációval.

Switch(config-line)# **end**

Switch#

Közvetlenül is átléphetünk az egyik alkonfigurációs módból egy másikba. Figyeljük meg, hogy az interfész kiválasztása után hogyan változik meg a prompt jel: **(config-line)#** to **(config-if)#** .

Switch(config-line)# **interface FastEthernet 0/1**

Switch(config-if)#

2.2.5

## Videómagyarázat - Navigáció az IOS módok között

A különböző IOS-módok közötti navigációt bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

2.2.6

## Megjegyzés a parancsszimulátoros feladatokhoz

Amíg csak tanuljuk az eszközök konfigurációjának műveleteit, jobb, ha biztonságos tesztrendszerben próbáljuk ki, mielőtt éles eszközökhöz ülnénk. A NetAcad különféle szimulációs eszközöket biztosít a konfigurációs és hibaelhárítási készségek fejlesztéséhez. Mivel ezek szimulációs eszközök, általában nem rendelkeznek a valódi berendezések összes funkciójával. Az egyik ilyen eszköz a parancsszimulátor. Minden parancsszimulátorban utasításokat kapunk egy bizonyos parancssorozat kiadásához. A parancsszimulátor csak akkor enged tovább, ha a megfelelő, pontos, teljes parancsot beírtuk. A fejlettebb szimulációs eszközök, mint például a Packet Tracer, lehetővé teszik, hogy rövidített parancsokat is használhassunk ugyanúgy, mint a valódi eszközökön.

2.2.7

## Parancsszimulátor - Navigálás az IOS módok között

Használjuk a parancsszimulátort, hogy kipróbáljuk az IOS parancssoros módjai közötti navigációt egy switch-en.

Enter privileged EXEC mode using the **enable** command.

Switch>enable

Return to user EXEC mode using the **disable** command.

Switch#disable

Re-enter privileged EXEC mode.

Switch>enable

Enter global configuration mode using the **configure terminal** command.

Switch#configure terminal

Exit global configuration mode and return to privileged EXEC mode using the **exit** command.

Switch(config)#exit

Re-enter global configuration mode.

Switch#configure terminal

Enter line subconfiguration mode for the console port using the **line console 0** command.

Switch(config)#line console 0

Return to global configuration mode using the **exit** command.

Switch(config-line)#exit

Enter VTY line subconfiguration mode using the **line vty 0 15** command.

Switch(config)#line vty 0 15

Return to global configuration mode.

Switch(config-line)#exit

Enter the VLAN 1 interface subconfiguration mode using the **interface vlan 1** command.

Switch(config)# interfész vlan 1

Az interfész konfigurációs módból váltson át vonali konzol alkonfigurációs módra a **line console 0** globális konfigurációs paranccsal.

Switch(config-if)# sorkonzol 0

Térjen vissza a kiemelt EXEC módba az **end** paranccsal.

Switch(config-line)# vége

Sikeresen navigált a különböző IOS parancssori módok között.

2.2.8

## Tudáspróba - IOS-navigáció

Az űrlap teteje

Ellenőrizze, hogy megértette-e az IOS navigációt, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik IOS-mód teszi lehetővé az összes parancshoz és szolgáltatáshoz való hozzáférést?

Az űrlap alja

Melyik IOS módban van, ha megjelenik a Switch(config)# prompt?

Melyik IOS módban van, ha megjelenik a Switch> prompt?

Melyik két parancs adja vissza a privilegizált EXEC promptot, függetlenül attól, hogy milyen konfigurációs módban van? (Válassz kettőt.)

[2.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Cisco IOS hozzáférés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A parancsok felépítése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                               
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. A parancsok felépítése

# A parancsok felépítése

2.3.1

## Az IOS-parancsok alapvető felépítése

Ez a témakör a Cisco IOS parancsainak alapvető szerkezetét mutatja be. A hálózati rendszergazdának ismernie kell az alapvető IOS-parancsstruktúrát, hogy használni tudja az eszköz beállításához.

A Cisco IOS-nak sok parancsa van. Minden parancsnak adott formátuma vagy szintaxisa van, és csak a megfelelő módban lehet azokat kiadni. A parancsok általános szintaxisa az ábrán is látható: először a parancs, amelyet a megfelelő kulcsszavak és argumentumok követnek.

A diagram bemutatja a switch parancsok általános szintaxisát (amely a következő: prompt, parancs, szóköz és kulcsszó vagy argumentum), és két példát mutat be. Az első példában a prompt a Switch>, a parancs a show, a szóköz következik, a kulcsszó pedig az ip protokollok. A második példában a prompt a Switch>, a parancs ping, szóköz következik, az argumentum pedig 192.168.10.5.

Switch>show ip protocols

Switch>ping 192.168.10.5

Parancsszóköz Kulcsszó vagy argumentum

* **Kulcsszó** - Az operációs rendszerben meghatározott specifikus paraméter (az ábrán **ip protocols** ).
* **Argumentum** - Ez nincs előre definiálva; ez a felhasználó által meghatározott érték vagy változó (az ábrán **192.168.10.5** ).

Miután beírtuk a teljes parancsot kulcsszavakkal és argumentumokkal együtt, az **Enter** billentyűvel küldjük el a parancsértelmezőnek.

2.3.2

## IOS-parancsok szintaxisa

A parancsok egy vagy több paraméterrel (argumentummal) rendelkezhetnek. A parancshoz szükséges kulcsszavak és argumentumok megismeréséhez nézzük meg a parancs szintaxisának leírását. A szintaxis megadja azt a mintát vagy formátumot, amelyet a parancs beírásakor használni kell.

Amint a táblázat is mutatja, a félkövér szöveg jelenti a pontosan beírandó parancsokat és kulcsszavakat. Dőlt betűs szöveg jelzi a felhasználó által megadott értékeket jelentő paramétereket.

| Táblázat felirata | |
| --- | --- |
| **Jelölés** | **Leírás** |
| **félkövér** | A félkövér szöveg jelenti azokat a parancsokat és kulcsszavakat, amelyeket pontosan a megadott módon kell beírni. |
| dőlt | A dőlt betűs szöveg jelenti az általunk megadható argumentumot. |
| **[** x **]** | A szögletes zárójelek opcionális elemet jeleznek (kulcsszó vagy argumentum). |
| **{** x **}** | A kapcsos zárójel kötelező elemet jelent (kulcsszó vagy argumentum). |
| **[** x **{** y **|** z **}]** | A szögletes zárójelben levő kapcsos zárójelben a függőleges vonallal elválasztott lehetőségek azt jelentik, hogy egy opcionális elemen belül kötelezően választanunk kell a felsoroltak közül. A szóközök a parancs részeinek elválasztására szolgálnak. |

Például a **description** parancs használatának szintaxisa **description** szöveg. Az argumentum a felhasználó által megadott szöveg . A **description** parancs általában egy interfész céljának leírására szolgál. Ha például ezt írjuk be: **description Connects to the main headquarter office switch** , akkor leírtuk, hogy a kapcsolat hol végződik.

A következő példák a tananyagban szereplő IOS-parancsok használatát mutatják be.

* **ping** ip-address – A parancs kulcsszava a **ping** , a felhasználó által megadott paraméter pedig a cél állomás IP-címe ( ip-address ). Például: **ping 10.10.10.5** .
* **traceroute** ip-address - A parancs kulcsszava a **traceroute** , a felhasználó által megadott paraméter pedig a cél állomás IP-címe ( ip-address ). Például: **traceroute 192.168.254.254** .

Ha egy parancs összetett, több argumentummal, akkor ehhez hasonló leírást láthatunk:

Switch(config-if)#  **switchport port-security aging**  {  **static**  |  **idő**  idő |  **type**  {  **abszolút**  |  **inaktivitás**  }}

A parancs után általában a parancs részletes leírását és minden argumentum szerepét elolvashatjuk.

A Cisco IOS Command Reference a legjobb információforrás egy-egy adott parancsról.

2.3.3

## Az IOS súgófunkciói

Az IOS kétféle segítséget kínál: környezetérzékeny súgót és parancsszintaxis-ellenőrzést.

A környezetérzékeny súgó segítségével gyorsan megtalálhatjuk a választ ezekre a kérdésekre:

* Milyen parancsok állnak rendelkezésre az egyes parancsmódokban?
* Milyen parancsok kezdődnek bizonyos karakterekkel vagy karaktersorozattal?
* Milyen argumentumok és kulcsszavak használhatók adott parancsokhoz?

A környezetérzékeny súgót a parancssorba beírt **?** segítségével érjük el.

A parancsszintaxis-ellenőrzés megnézi, hogy a felhasználó érvényes parancsot írt-e be. A parancs bevitele után a parancsértelmező balról jobbra kiértékeli. Ha a parancs helyes, a megfelelő művelet végrehajtódik, a parancssor pedig a megfelelő prompt jellel tér vissza. Ha a parancsértelmező nem ismeri fel az utasítást, visszajelzést küld a hiba okáról.

2.3.4

## Videómagyarázat - Környezetérzékeny súgó és parancsszintaxis-ellenőrzés

A környezetérzékeny súgó és a parancsszintaxis-ellenőrzést bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

2.3.5

## Gyorsbillentyűk és billentyűkombinációk

Az IOS-parancssor gyorsbillentyűkkel és billentyűkombinációkkal teszi könnyebbé a konfigurálást, ellenőrzést és hibaelhárítást.

A parancsok és kulcsszavak egészen addig rövidíthetők, amíg még egyértelmű marad, hogy melyik szóról van szó. A **configure** parancs például lerövidíthető **conf** -ra, mert a **configure** az egyetlen parancs, amely **conf** -fal kezdődik. Ha tovább rövidítenénk, a **con** már nem működik, mert egynél több parancs kezdődik a **con** karaktersorozattal. A kulcsszavak is rövidíthetők.

A táblázat felsorolja a parancsok bevitelét megkönnyítő billentyűket.

| Táblázat felirata | |
| --- | --- |
| **Billentyűkombináció** | **Leírás** |
| **Tab** | Befejezi a részlegesen beírt parancsot. |
| **Backspace** | A kurzortól balra levő karaktert törli. |
| **Ctrl+D** | Törli a kurzornál levő karaktert. |
| **Ctrl+K** | Törli az összes karaktert a kurzortól a parancssor végéig. |
| **Esc D** | Törli az összes karaktert a kurzortól a szó végéig. |
| **Ctrl+U** vagy **Ctrl+X** | Törli az összes karaktert a kurzortól a parancssor elejéig. |
| **Ctrl+W** | Törli a kurzortól balra lévő szót. |
| **Ctrl+A** | A kurzort a sor elejére mozgatja. |
| **Balra nyíl** vagy **Ctrl+B** | A kurzort egy karakterrel balra mozgatja. |
| **Esc B** | A kurzort egy szóval balra mozgatja. |
| **Esc F** | A kurzort egy szóval jobbra mozgatja. |
| **Jobbra nyíl** vagy **Ctrl+F** | A kurzort egy karakterrel jobbra mozgatja. |
| **Ctrl+E** | A kurzort a sor végére mozgatja. |
| **Felfele nyíl** vagy **Ctrl+P** | A legutóbbi paranccsal kezdve visszalapoz a parancselőzményekben. |
| **Ctrl+R** vagy **Ctrl+I** vagy **Ctrl+L** | Egy konzolüzenet fogadása után újra megjeleníti a prompt jelet és a parancssort. |

**MEGJEGYZÉS:** Bár a **Delete** billentyű általában a jobbra levő karaktert törli, az IOS-parancssor nem ismeri a Delete billentyűt.

Ha egy parancs kimenete több sort eredményez, mint ami egy terminálablakban megjeleníthető, az IOS a **“--More--”** szót jeleníti meg. Az alábbi táblázat ismerteti azokat a billentyűket, amelyek ekkor használhatók.

| Táblázat felirata | |
| --- | --- |
| **Billentyű** | **Leírás** |
| **Enter** billentyű | Megjeleníti a következő sort. |
| **Hely** | Megjeleníti a következő oldalt. |
| Bármely más billentyű | Megszakítja a kimenet kiírását és visszatér a parancssorhoz. |

Ez a táblázat felsorolja a műveletből való kilépéshez használható billentyűkombinációkat.

| Táblázat felirata | |
| --- | --- |
| **Billentyűkombináció** | **Leírás** |
| **Ctrl-C** | Bármelyik konfigurációs módban is vagyunk, lezárja az adott módot és visszatér privilegizált EXEC módba. Az alapbeállítási (setup) módból kilép vissza a parancssorba. |
| **Ctrl-Z** | Bármelyik konfigurációs módban is vagyunk, lezárja az adott módot és visszatér privilegizált EXEC módba. |
| **Ctrl-Shift-6** | DNS-lekérdezések, traceroute, ping és egyéb hasonló műveletek megszakítására való billentyűkombináció. |

2.3.6

## Videómagyarázat - Gyorsbillentyűk és billentyűkombinációk

A gyorsbillentyűk és billentyűkombinációk működését bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

2.3.7

## Packet Tracer - Navigálás az IOS-ban

A feladat során gyakorlatot szerzünk a Cisco IOS használatáról, beleértve a különféle hozzáférési módokat, konfigurációs üzemmódokat és a gyakran előforduló parancsokat. Kipróbáljuk a környezetérzékeny súgót is a clock parancson keresztül.

[Az IOS használata](https://contenthub.netacad.com/courses/itn/_common/2.3.7-packet-tracer---navigate-the-ios_hu-HU.pka)

2.3.8

## Laborgyakorlat - Navigálás az IOS-ban a Tera Term alkalmazás segítségével

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: Belépés egy Cisco switch-be a soros konzolporton keresztül.
  2. rész: Az eszköz alapvető paramétereinek konfigurálása és megjelenítése.
  3. rész: (választható): A Cisco router elérése mini-USB konzolkábel segítségével.

[2.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Navigálás az IOS-ban](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alapbeállítások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                     
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Alapbeállítások

# Alapbeállítások

2.4.1

## Eszköznevek

Sokat tanultunk a Cisco IOS-ról, navigációról és a parancsok szerkezetéről. Készen állunk az eszközök konfigurálására! Szinte mindig a legelső parancs az eszközök saját egyedi nevének, állomásnevének beállítása. Alapértelmezés szerint minden eszköznek van gyárilag beállított neve. Például egy Cisco IOS switch neve "Switch."

Ha a hálózat összes switch-én változatlanul hagyjuk az alapértelmezett nevet, akkor nehéz megtalálni egy bizonyos eszközt. Honnan tudnánk, hogy a megfelelő eszközhöz csatlakoztunk-e, amikor távoli SSH-kapcsolatot hozunk létre? Az állomásnév segít ellenőrizni, hogy a megfelelő eszközbe léptünk-e be.

Az alapértelmezett nevet valami kifejezőbbre kell változtatni. Válasszunk olyat, amit könnyű megjegyezni, dokumentálni, és azonosítja az eszközt! Néhány fontos elnevezési szabály:

* betűvel kezdődik
* nem tartalmaz szóközt
* betűvel vagy számmal végződik
* betűt, számot, kötőjelet vagy aláhúzásjelet tartalmaz
* legfeljebb 63 karakter hosszú

A szervezet olyan nevezéktant alkosson, ami könnyűvé, magától értetődővé teszi az egyes eszközök azonosítását. Állomásnevek esetén a Cisco IOS megkülönbözteti a kis- és nagybetűket. Az ábra például azt mutatja, hogy három darab, három emeletet összekötő switch kapcsolódik egymáshoz egy hálózatban. Az itt használt nevezéktan tartalmazza az egyes eszközök helyét és célját. A hálózati dokumentációban le kell írni, hogy miként választották ki ezeket a neveket, hogy a későbbi eszközöknél ugyanezt a rendszert használhassák.

Az ábrán három egymáshoz kapcsolódó kapcsoló látható három emeleten. A felső kapcsoló neve Sw-Floor-3, a középső kapcsoló neve Sw-Floor-2, az alsó kapcsoló neve Sw-Floor-1. A gazdaszámítógépen ülő felhasználó csatlakozik az Sw-Floor-1 kapcsolóhoz. Alul olvasható szöveg: a hálózati eszközök elnevezésekor könnyen azonosíthatók konfigurációs célokra.

Sw-Floor-3 Sw-Floor-2 Sw-Floor-1

A hálózati eszközök elnevezésekor könnyen azonosíthatók konfigurációs célokra.

A nevezéktan kialakítása után parancssor segítségével beállítjuk az eszközök neveit. Ahogy a példában is látható, a privilegizált EXEC módból globális konfig módba lépünk a **configure terminal** paranccsal. Figyeljük meg a prompt jel megváltozását!

Switch# **configure terminal**

Switch(config)# **hostname Sw-Floor-1**

Sw-Floor-1(config)#

Globális konfigurációs módban írjuk be a **hostname** parancsot, majd a switch nevét, ezután nyomjuk meg az **Enter** billentyűt. Figyeljük meg a név megváltozását a prompt jelben!

**MEGJEGYZÉS:** A switch alapértelmezett prompt jelének visszaállítását elvégezhetjük a **no hostname** globális konfigurációs paranccsal.

A dokumentációt mindig frissítsük, ha új eszközt adunk a rendszerhez vagy módosítunk egy régit. A berendezések azonosítása a dokumentációban elhelyezkedésük, működésük célja és címzésük alapján történik.

2.4.2

## Jelszó irányelvek

A gyenge vagy könnyen kitalálható jelszavak használata folyamatosan a szervezetek legnagyobb biztonsági problémája. A hálózati eszközöknek, beleértve az otthoni vezeték nélküli routereket is, mindig rendelkezniük kell jelszóval, hogy korlátozzuk az adminisztrációs célú hozzáférést.

A Cisco IOS beállítható úgy, hogy hierarchikus jelszavakat használjon, hogy különböző hozzáférési jogosultságokat biztosítson egy hálózati eszközhöz.

Minden hálózati eszköznek korlátoznia kell a rendszergazdai hozzáférést azáltal, hogy jelszóval biztosítja a privilegizált EXEC, a felhasználói EXEC és a távoli Telnet hozzáférést. Ezen túl minden jelszót titkosítani kell és jogi figyelmeztetést kell kiírni.

Erős, nem kitalálható jelszót kell választani. Jelszavak választásának irányelvei:

* Használjunk 8 karakternél hosszabb jelszavakat.
* Használjunk kis- és nagybetűket, számokat, speciális karaktereket és/vagy számsorozatokat.
* Ne használjunk azonos jelszót minden eszközön.
* Ne használjunk gyakori szavakat, mert könnyen kitalálhatók.

Keressünk az interneten jelszógeneráló oldalakat. A legtöbbnél beállíthatjuk a jelszó hosszát, karaktereit és egyebeket is.

**MEGJEGYZÉS:** A tanfolyam laborgyakorlatainak során legtöbbször egyszerű jelszavakat használunk, mint a **cisco** vagy a **class** . Ezek gyenge és könnyen kitlálható jelszavak, éles eszközökön ne használjuk őket! Mi a kényelmesebb tanítás vagy a példák kedvéért használjuk őket.

2.4.3

## Jelszavak beállítása

Amikor csatlakozunk egy eszközhöz, először a felhasználói EXEC módba kerülünk. A biztonságát a konzolbeállítás adja.

A felhasználói EXEC mód biztonságossá tételéhez lépjünk konzolvonal konfigurációs módjába a **line console 0** globális konfig paranccsal, ez látható az ábrán is. A nulla az első (és általában egyetlen) konzolinterfészt jelenti. Ezután adjuk meg a felhasználói EXEC mód jelszavát a **password** jelszó paranccsal. Végül engedélyezzük a felhasználói EXEC hozzáférést a **login** paranccsal.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line console 0**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

Ezután a konzolhozzáférés jelszót fog kérni, mielőtt a felhasználói EXEC módba engedne minket.

Ahhoz, hogy rendszergazdai hozzáférésünk legyen minden IOS-parancshoz, és konfigurálhassuk az eszközt, privilegizált EXEC hozzáférés kell. Ez nagyon fontos mód, mert teljes hozzáférést kapunk az eszközhöz.

A privilegizált EXEC mód biztonságának beállításához adjuk ki az **enable secret** jelszó globális konfigurációs parancsot, az ábrán látható módon.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **enable secret class**

Sw-Floor-1(config)# **exit**

Sw-Floor-1#

A virtuális terminál (VTY) vonalak Telnet vagy SSH segítségével távoli hozzáférést biztosítanak az eszközhöz. Sok Cisco switch akár 16 VTY-vonalat is támogat, melyek számozása 0 és 15 közé esik.

A VTY-vonalak biztonságossá tételéhez lépjünk VTY-vonali módba a **line vty 0 15** globális konfigurációs paranccsal. Ezután pedig adjuk meg a VTY-jelszót a **password** jelszó parancs segítségével. Végül engedélyezzük a VTY-hozzáférést a **login** paranccsal.

Egy switch VTY-vonalainak beállítása látható a példán.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **line vty 0 15**

Sw-Floor-1(config-line)# **password cisco**

Sw-Floor-1(config-line)# **login**

Sw-Floor-1(config-line)# **end**

Sw-Floor-1#

2.4.4

## Jelszavak titkosítása

A startup-config és a running-config fájlok a legtöbb jelszót egyszerű szövegként jelenítik meg. Ez biztonsági fenyegetést jelent, mert bárki megláthatja a jelszavakat, ha hozzáfér ezekhez a fájlokhoz.

Az összes egyszerű szöveges jelszó titkosításához használjuk a **service password-encryption** globális konfigurációs parancsot a példában látható módon.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **service password-encryption**

Sw-Floor-1(config)#

Ez a parancs egy gyenge titkosítást alkalmaz a titkosítatlan jelszavakon. A titkosítás csak a konfigurációs fájlban eltárolt jelszavakra vonatkozik, a hálózaton átküldött jelszavakra nem. A parancs célja az, hogy illetéktelen személyek ne láthassák a konfigurációban szereplő jelszavakat.

Ellenőrizzük a **show running-config** paranccsal az immár titkosított jelszavainkat.

Sw-Floor-1(config)# **end**

Sw-Floor-1# **show running-config**

!

(Output omitted)

!

line con 0

password 7 094F471A1A0A

login

!

line vty 0 4

password 7 094F471A1A0A

login

line vty 5 15

password 7 094F471A1A0A

login

!

!

end

2.4.5

## Banner üzenetek

Bár a jelszavak megkövetelése jó módszer a jogosulatlan személyek kizárására a hálózatból, mégis lényeges annak kinyilvánítása, hogy az eszközbe csak az arra jogosultak léphetnek be. Ennek érdekében készítsünk banner üzenetet. A bannerek fontos szerepet játszhatnak egy olyan hivatalos eljárásban, amelyben valakit egy eszköz feltörésével vádolnak. Néhány jogszabály nem engedi a felelősségre vonást, de még a felhasználók figyelemmel kísérését sem, ha hiányoznak a figyelmeztető üzenetek.

Napi üzenet ("banner message of the day") létrehozásához használjuk a **banner motd #** napi üzenet **#** globális konfig parancsot. A parancs szintaxisában a „#” karaktert határoló karakternek nevezzük. Az üzenet előtt és után írjuk be. A határolójel tetszőleges karakter lehet, mely nem szerepel az üzenet szövegében. Emiatt sokszor írásjeleket, például a # karaktert használjuk. A parancs kiadása után a banner üzenet meg fog jelenni az eszközhöz való hozzáféréskor, amíg a parancsot vissza nem vonjuk.

A következő példa bemutatja a banner konfigurálását az Sw-Floor-1 eszközön.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **banner motd #Authorized Access Only#**

2.4.6

## Videómagyarázat - Biztonságos felügyeleti hozzáférés kapcsolóhoz

Egy kapcsoló biztonságossá tételét bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

2.4.7

## Parancsszimulátor - Alapvető eszközbeállítások

Tegyük biztonságossá a hozzáférést egy switch-hez!

* Adjunk nevet az eszköznek.
* Tegyük biztonságossá a felhasználói EXEC mód hozzáférését.
* Tegyük biztonságossá a privilegizált EXEC módot.
* Tegyük biztonságossá a VTY-hozzáférést.
* Titkosítsuk a szöveges jelszavakat.
* Állítsunk be bejelentkezési banner üzenetet.

Enter global configuration mode.

Switch#configure terminal

Name the switch “Sw-Floor-1”.

Switch(config)#hostname Sw-Floor-1

Secure user EXEC mode access by entering **line console 0**, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

Sw-Floor-1(config)#line console 0

Sw-Floor-1(config-line)#password cisco

Sw-Floor-1(config-line)#login

Sw-Floor-1(config-line)#exit

Secure privileged EXEC mode access using the password **class.**

Sw-Floor-1(config)#enable secret class

Secure the VTY lines 0 through 15, assign the password **cisco**, enable login, and return to the global configuration mode using **exit.**

Sw-Floor-1(config)#line vty 0 15

Sw-Floor-1(config-line)#password cisco

Sw-Floor-1(config-line)#login

Sw-Floor-1(config-line)#exit

Encrypt all plaintext passwords.

Sw-Floor-1(config)#service password-encryption

Create a banner message using the “**#**” symbol as the delimiter. The banner should display exactly: **Warning! Authorized access only!**

Sw-Floor-1(config)# banner motd #Figyelem! Csak engedélyezett hozzáférés!#

Sikeresen teljesítette az eszköz eléréséhez és biztonságossá tételéhez szükséges alapvető követelményeket.

2.4.8

## Tudáspróba - Alapvető eszközbeállítások

Az űrlap teteje

Ellenőrizze, hogy megértette-e az alapvető eszközkonfigurációt, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Mi a parancs az „Sw-Floor-2” névhez egy kapcsolóhoz?

Az űrlap alja

Hogyan biztosítható a kiemelt EXEC mód hozzáférés egy switchen?

Melyik parancs engedélyezi a jelszó-hitelesítést a felhasználói EXEC módhoz való hozzáféréshez egy kapcsolón?

Melyik parancs titkosítja az összes egyszerű szöveges jelszóhoz való hozzáférést egy kapcsolón?

Melyik paranccsal állíthatja be, hogy egy szalaghirdetés megjelenjen, amikor kapcsolóhoz csatlakozik?

[2.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A parancsok felépítése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Beállítások mentése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                        
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Beállítások mentése

# Beállítások mentése

2.5.1

## Konfigurációs fájlok

Már ismerjük néhány alapvető beállítás elvégzését egy switch-en: jelszavakat és banner üzeneteket is be tudunk állítani. Ez a témakör bemutatja a konfigurációk mentésének módját.

Két rendszerfájl tárolja az eszköz konfigurációját:

* **startup-config** - Az NVRAM-ban tárolt elmentett konfiguráció. Tartalmazza az összes olyan parancsot, amelyet az eszköz indításkor vagy újraindításkor végrehajt. Az eszköz kikapcsolásakor nem veszti el a tartalmát.
* **running-config** - Ez a RAM-ban van eltárolva. Az aktuális konfiguráció található benne. Az aktív konfiguráció módosítása azonnali hatással van a Cisco eszköz működésére. A RAM elfelejti a tartalmát, ha megszűnik az áramellátása. Az eszköz kikapcsolásakor vagy újraindításakor minden eltűnik belőle.

A **show running-config** privilegizált EXEC módú parancs megjeleníti az aktív konfigurációt. Amint a példában látható, a parancs kilistázza a RAM-ban jelenleg tárolt teljes konfigurációt.

Sw-Floor-1# **show running-config**

Building configuration...

Current configuration : 1351 bytes

!

! Last configuration change at 00:01:20 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname Sw-Floor-1

!

(output omitted)

Az indító konfigurációs fájl megtekintéséhez használjuk a **show startup-config** privilegizált módú parancsot.

Az eszköz újraindulása vagy tápellátásának megszűnése esetén a nem mentett konfigurációs módosítások elvesznek. A módosításokat az aktív konfigurációból az indító konfigurációba menti a **copy running-config startup-config** privilegizált módú parancs.

2.5.2

## Az aktív konfiguráció megváltoztatása

Ha az aktív konfigurációban létrehozott változtatás nem hozta meg a kívánt eredményt és a konfigurációt még nem mentettük el, az eszközt visszaállíthatjuk az előző állapotába. Visszavonhatjuk a parancsokat egyenként, vagy újraindíthatjuk az eszközt a **reload** privilegizált módú paranccsal, hogy az indító konfigurációt visszaállítsuk.

A **reload** parancs hátránya, hogy az aktív konfiguráció visszavonása miatt az eszköz és emiatt akár a hálózat is egy rövid ideig nem lesz elérhető.

Az újraindítási parancs kiadásakor az IOS észre fogja venni, hogy az aktív konfiguráció nem mentett változtatásokat tartalmaz az indítóhoz képest. Megjelenik egy prompt, amely megkérdezi, hogy mentsük-e a változtatásokat. A változtatások elvetéséhez írjuk be az **n** betűt vagy a **no** szót.

Lehet olyan is, hogy a nem kívánt változtatásokat már mentettük az indító konfigurációba, ilyenkor lehet, hogy minden beállítást törölnünk kell. Ez az indító konfiguráció törlését és az eszköz újraindítását jelenti. Az indító konfiguráció törlése az **erase startup-config** privilegizált EXEC módú paranccsal történik. A parancs kiadása után a switch megerősítést kér. Az elfogadáshoz nyomjuk meg az **Enter** billentyűt.

Miután az indító konfigurációt töröltük az NVRAM-ból, újra kell indítani az eszközt, hogy az aktív konfiguráció is eltűnjön a RAM-ból. Újraindításkor az eszköz azt az alapértelmezett indító konfigurációt fogja betölteni, amellyel újonnan érkezett.

2.5.3

## Videómagyarázat - Az aktív konfiguráció megváltoztatása

A switch konfigurációjának mentéséről szóló videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

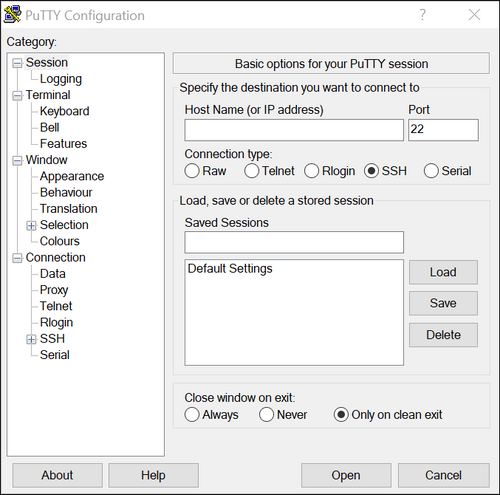
2.5.4

## Konfiguráció rögzítése szövegfájlba

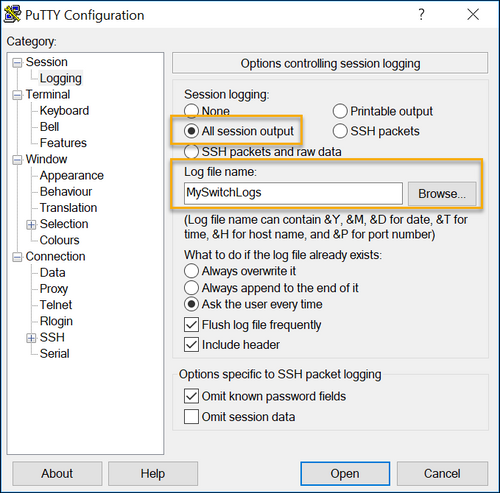
A konfigurációs fájlokat szövegfájlba is menthetjük és archiválhatjuk. A lépések végrehajtása után a konfigurációról egy szerkeszthető és újrafelhasználható másolatunk lesz.

Tegyük fel, hogy adott egy felkonfigurált switch, amelyen az aktív konfigurációt elmentették az eszközön.

**1. lépés** Nyissuk meg a terminálemulációs (pl.: PuTTY vagy Tera Term) programunkat, amellyel már csatlakoztunk a switch-hez.



**2. lépés** Engedélyezzük a naplózást a terminálszoftverben, és adjuk meg a leendő naplófájl nevét és helyét. Az ábrán azt látjuk, hogy minden kimenet (**All session output**) a megadott fájlba (MySwitchLogs) lesz elmentve.



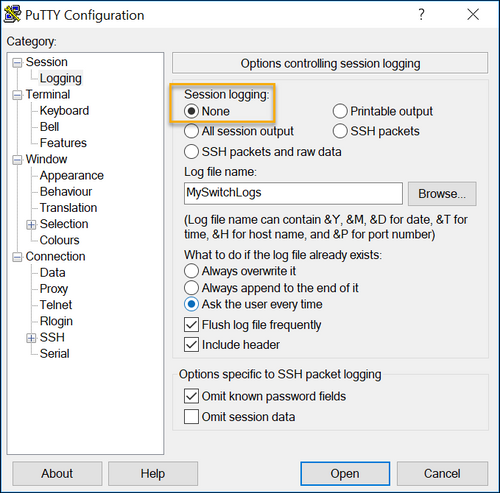
**3. lépés** Adjuk ki a **show running-config** vagy a **show startup-config** parancsot privilegizált módban. A terminálablakban megjelenő szöveg a kiválasztott állományba lesz mentve.

Sw-Floor-1# **show running-config**

Building configuration...

(output omitted)

**4. lépés** Kapcsoljuk ki a naplózást a terminálszoftverben. Az ábra az látható, hogy a naplózást kikapcsoljuk a "Semmi" (**None**) naplózási beállítás kiválasztásával.



A létrehozott szövegfájlba rögzítettük az eszköz jelenlegi konfigurációját. Lehet, hogy a fájlt szerkesztenünk kell, mielőtt egy eszközre visszatöltenénk mint biztonsági mentést.

Konfigurációs fájl visszaállítása egy eszközre:

**1. lépés:** Lépjünk be globális konfigurációs módba az eszközön.

**2. lépés:** Másoljuk és illesszük be a szövegfájlt a switch-hez csatlakozó terminálablakba.

A fájlban lévő szöveget a parancssor parancsként értelmezi, és beilleszti őket az aktív konfigurációba. Kényelmes módszer egy eszköz manuális konfigurálására.

2.5.5

## Packet Tracer - A switch alapbeállításainak megadása

A feladat során egy switch alapbeállításainak megadását fogjuk elvégezni. A parancssorhoz és a konzolporthoz biztonságos hozzáférést állítunk be titkosított és egyszerű szöveges jelszavak segítségével. Megtanuljuk, hogyan kell üzenetet küldeni a switch-be bejelentkező felhasználóknak. Ezek az üzenetek az illetéktelen felhasználók figyelmeztetésére is szolgálnak.

[Switch kezdeti beállítása](https://contenthub.netacad.com/courses/itn/_common/2.5.5-packet-tracer---configure-initial-switch-settings_hu-HU.pka)

[2.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alapbeállítások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Portok és címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                         
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Portok és címek

# Portok és címek

2.6.1

## IP-címek

Nagyszerű, már el tudunk végezni néhány alapvető beállítást! De a mókának még nincs vége. Ha szeretnénk, hogy a végberendezéseink kommunikálni tudjanak egymással, mindegyiknek megfelelő IP-címet kell adni, és megfelelően csatlakoztatni őket. Ebben a témakörben IP-címekről, portokról és az eszközöket összekötő közegekről lesz szó.

Az IP-címek teszik lehetővé, hogy az eszközök megtalálják egymást, és az interneten keresztül végponttól végpontig terjedő kommunikáció legyen lehetséges. Minden végberendezésnek rendelkeznie kell IP-címmel. Példa végberendezésekre:

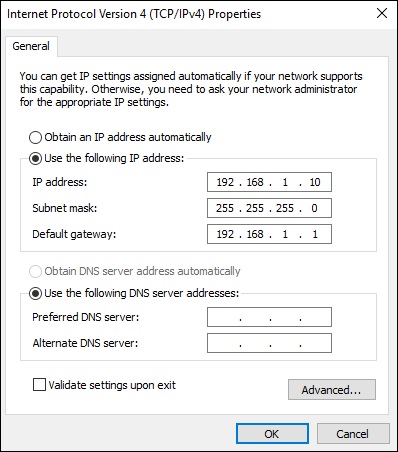
* Számítógépek (munkaállomások, laptopok, fájl- és webszerverek)
* Hálózati nyomtatók
* IP-telefonok
* Biztonsági kamerák
* Okostelefonok
* Hordozható eszközök (pl.: a vezeték nélküli vonalkód-leolvasó)

Az IPv4-címek szokásos formája a pontozott decimális forma, ami négy decimális, 0 és 255 közé eső számból áll. Az IPv4-címek a hálózati eszközökhöz rendelt egyedi számok.

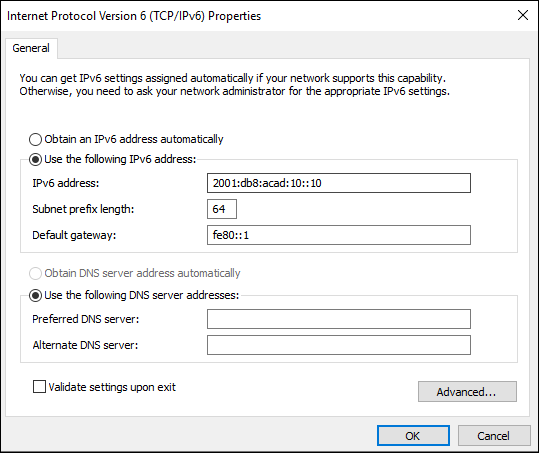
**MEGJEGYZÉS:** Amikor IP-ről beszélünk, akkor az IPv4- és IPv6-protokollt egyaránt értjük rajta. Az IPv6 az IP újabb verziója, felváltja az egyelőre gyakoribb IPv4-et.

Az IPv4-címhez alhálózati maszk is kell. Az IPv4 alhálózati maszk egy 32 bites érték, amely megkülönbözteti a cím hálózati részét az állomásazonosító résztől. Az IPv4-címmel párosítva az alhálózati maszk határozza meg, hogy az eszköz melyik alhálózat tagja.

Az ábrán látható példa az állomáshoz rendelt IPv4-címet (192.168.1.10), alhálózati maszkot (255.255.255.0) és alapértelmezett átjárót (192.168.1.1) jeleníti meg. Az alapértelmezett átjáró annak a routernek az IP-címe, amely az eszköz számára távoli hálózatok és az internet elérését is lehetővé teszi.



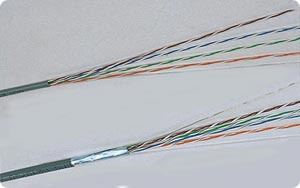
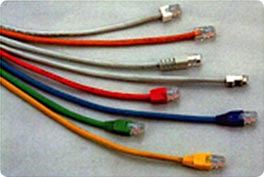
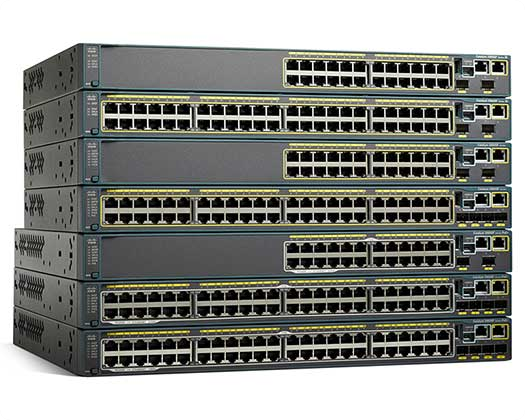
Az IPv6-címek 128 bit hosszúak és hexadecimális értékek sorozataként írjuk le őket. Mivel négy bit ad ki egy hexadecimális számjegyet, így a cím 32 hexadecimális számjegyből áll. A négy hexadecimális számjegyből álló csoportokat kettőspont (:) választja el. Az IPv6-címek esetében nem különböztetjük meg a kis- és nagybetűket, bármelyiket használhatjuk.



2.6.2

## Interfészek és portok

A hálózati kommunikáció fontos részét alkotják a végberendezések és a hálózati eszközök interfészei, valamint az őket összekötő kábelek. Minden fizikai interfészt specifikációk vagy szabványok írnak le. Az interfészhez csatlakoztatott kábelnek az interfész fizikai szabványainak megfelelőnek kell lennie. Az ábra bemutat néhány tipikus hálózati közeget: csavart érpáras kábel, optikai kábel, koaxiális kábel vagy vezeték nélküli átvitel.



CopperWirelessFiber-optics

Az egyes adatátviteli közegek egyedi sajátosságokkal és előnyökkel rendelkeznek. Nem minden hálózati közeg egyforma. Nem minden közeg alkalmas egy bizonyos célra. A különféle közegek néhány különböző tulajdonsága:

* Hatótávolság, azaz a jel által a közegben sikeresen megtett út
* A közeg telepítési környezete
* Az átvitt adat mennyisége és az átvitel sebessége
* Bekerülési és telepítési költség

Az internet összeköttetései nem csak egy konkrét átviteli közeget, hanem egy meghatározott átviteli technológiát is igényelnek. Napjainkban az Ethernet a leggyakoribb helyi hálózati (Local Area Network, LAN) kapcsolódási mód. Ethernet portok vannak azokon a végberendezéseken, switch-eken és egyéb hálózati eszközökön, melyek kábellel csatlakoznak a fizikai hálózathoz.

A 2. rétegbeli Cisco IOS switch-ek fizikai portokkal rendelkeznek az eszközök csatlakoztatásához. Ezek a portok nem támogatják a 3. rétegbeli IP-címeket. Ezért a kapcsolók egy vagy több virtuális switch interfésszel (SVI) rendelkeznek. A virtuális interfész azt jelenti, hogy nincs fizikai hardverelem hozzárendelve az eszközben. Az SVI-t szoftveresen hozzuk létre.

A virtuális interfész lehetőséget biztosít a switch távoli elérésére IPv4- vagy IPv6-hálózaton keresztül. A switch-ek alapértelmezett gyári konfigurációjában egyetlen SVI van. Az alapértelmezett SVI a VLAN1 interfész.

**MEGJEGYZÉS:** A 2. rétegbeli kapcsolóknak nincs szükségük IP-címre. Az SVI-hez rendelt IP-cím a switch távoli elérésére szolgál. A switch-nek nincs szüksége IP-címre a feladatainak ellátásához.

2.6.3

## Tudáspróba - Portok és címek

Az űrlap teteje

Ellenőrizze, hogy megértette-e a portokat és címeket, ha a következő kérdésekre a LEGJOBB választ választja.

1. Hogyan nevezzük az IPv4-cím szerkezetét?

Az űrlap alja

Hogyan jelenik meg az IPv4-cím?

Milyen típusú interfészhez nincs fizikai port társítva?

[2.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Beállítások mentése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IP-címzés beállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                             
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. IP-címzés beállítása

# IP-címzés beállítása

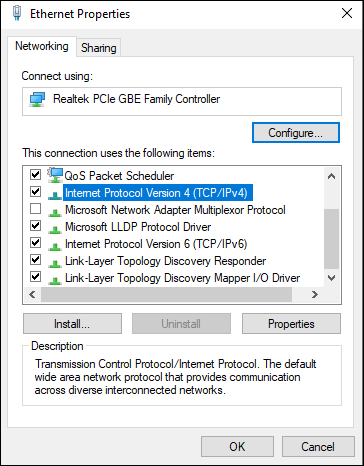
2.7.1

## Manuális IP-cím konfiguráció végberendezéseken

Ahogy a barátainknak is csak a megfelelő telefonszám ismeretében tudunk üzenetet küldeni vagy felhívni őket, a hálózat végberendezéseinek IP-címre van szükségük ahhoz, hogy a többi eszközzel kommunikálhassanak a hálózaton. Ebben a témakörben alapvető hálózati kapcsolatot hozunk létre switch-ek és PC-k IP-címeinek beállításával.

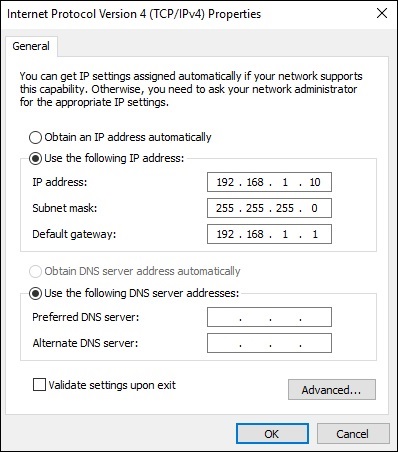
Az IPv4-címeket megadhatjuk manuálisan az eszközön, vagy kaphatja automatikusan a Dynamic Host Configuration Protocol (DHCP) segítségével.

Windows operációs rendszert futtató állomáson az IPv4-címet a **Vezérlőpult > Hálózati és megosztási központ > Adapterbeállítások módosítása** lehetőség alatt, az adapter kiválasztása után tudjuk beállítani. Ezután kattintsunk a jobb gombbal, és válasszuk a **Tulajdonságok** menüpontot a **Helyi hálózati adapter tulajdonságai** megnyitásához, ahogy az ábrán is látható.



Jelöljük ki A TCP/IP protokoll 4-es verziója (TCP/IPv4) sort, kattintsunk a **Tulajdonságok** gombra, hogy megnyíljon az ábrán látható **A TCP/IP protokoll 4-es verziója (TCP/IPv4) - tulajdonságok** ablak. Írjuk be az IPv4-címet, az alhálózati maszkot és az alapértelmezett átjárót.

**MEGJEGYZÉS:** Az IPv6-címzési és konfigurációs beállítások hasonlóak az IPv4-hez.



**MEGJEGYZÉS:** A DNS-szerver címhez annak a Domain Name System (DNS) szervernek az IPv4- vagy IPv6-címét kell beírni, amely IP-címekre fordítja a tartományneveket (pl.: a [www.cisco.com](http://www.cisco.com)).

2.7.2

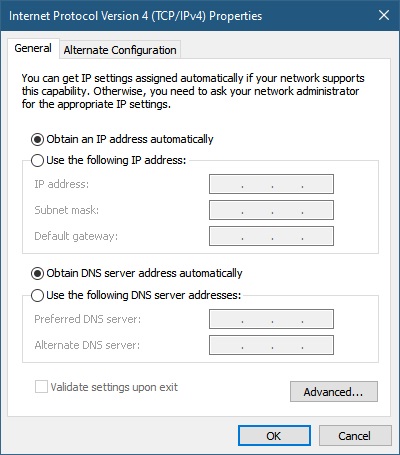
## Automatikus IP-cím konfiguráció végberendezéseken

A legtöbb végberendezés alapértelmezés szerint automatikus IPv4-cím konfigurációra, DHCP-re van beállítva. DHCP-t szinte minden hálózatban használnak. Népszerűségét könnyen megérthetjük, ha végiggondoljuk, hogy nélküle mennyi többletmunkát kellene végezni.

A DHCP automatikus végzi az IP-címkiosztást minden hálózati végberendezés számára, melyen a DHCP engedélyezve van. Gondoljuk végig, hogy mennyi időt emésztene fel, ha minden hálózatra való csatlakozás alkalmával manuálisan kellene megadni az IP-címet, a maszkot, az alapértelmezett átjárót és a DNS-szervert. Szorozzuk meg ezt az összes felhasználó és az általuk használt hálózati eszközök számával, így láthatjuk a probléma méretét. A manuális beállítás növeli a helytelen konfiguráció esélyét is, ha egy másik eszköz IPv4-címét állítjuk be duplán.

Ahogy az ábrán is látható, egy Windows PC-n a DHCP beállításához mindössze ki kell választanunk az **IP-cím automatikus kérése** és a **DNS-kiszolgáló címének automatikus kérése** pontokat. A számítógép keres egy DHCP-szervert, amely hozzánk rendeli a hálózaton való kommunikációhoz szükséges címbeállításokat.

**MEGJEGYZÉS:** Az IPv6 a DHCPv6 és a SLAAC (Stateless Address Autoconfiguration) szolgáltatásokat használja a dinamikus címkiosztáshoz.



2.7.3

## Parancsszimulátor — Windows PC IP-konfigurációjának ellenőrzése

A Windows PC IP-beállításait megjeleníthetjük parancssorból az **ipconfig** paranccsal. A kimenetben megjelenik az IP-cím, az alhálózati maszk és az átjáró, melyeket a PC a DHCP-szervertől kapott.

Írjuk be a parancsot a Windows PC IP-cím beállításainak megtekintéséhez!

Enter the command to display the IP configuration on a Windows PC.

Az űrlap teteje

C:\>

Az űrlap alja

2.7.4

## Virtuális switch interfész konfigurálása

Egy switch távoli eléréséhez IP-címet és alhálózati maszkot kell beállítanunk az SVI-n. A switch virtuális interfészének beállításához adjuk ki az **interface vlan 1** globális konfigurációs parancsot. A Vlan 1 nem tényleges fizikai interfész, hanem virtuális. Ezután állítsunk be egy IPv4-címet az **ip address** ip-cím alhálózati-maszk interfészkonfigurációs paranccsal. Végül aktiváljuk a virtuális interfészt a **no shutdown** interfészkonfigurációs paranccsal.

A beállítás után a switch rendelkezik minden olyan IP-beállítással, amely a hálózati kommunikációhoz szükséges.

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **interface vlan 1**

Sw-Floor-1(config-if)# **ip address 192.168.1.20 255.255.255.0**

Sw-Floor-1(config-if)# **no shutdown**

Sw-Floor-1(config-if)# **exit**

Sw-Floor-1(config)# **ip default-gateway 192.168.1.1**

2.7.5

## Parancsszimulátor - Virtuális switch interfész konfigurálása

Enter interface configuration mode for VLAN 1.

Az űrlap teteje

Switch(config)#

Az űrlap alja

2.7.6

## Packet Tracer - Alapvető hálózati kapcsolatok megvalósítása

A feladat során először a switch alapbeállításait adjuk meg. Ezután alapvető hálózati kapcsolatot hozunk létre switch-ek és PC-k IP-címeinek beállításával. Az IP-címek beállítását követően különféle **show** parancsokkal ellenőrizzük a beállításainkat, a **ping** paranccsal pedig az eszközeink közötti hálózati kapcsolatot.

[Alapvető hálózati kapcsolatok megvalósítása](https://contenthub.netacad.com/courses/itn/_common/2.7.6-packet-tracer---implement-basic-connectivity_hu-HU.pka)

[2.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Portok és címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kapcsolatok ellenőrzése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                             
*                             

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Kapcsolatok ellenőrzése

# Kapcsolatok ellenőrzése

2.8.1

## Videómagyarázat - Interfészek tesztelése

Az előző témakörben alapvető hálózati kapcsolatot hoztunk létre switch-ek és PC-k IP-címeinek beállításával. Ezután ellenőriztük a konfigurációt és a kapcsolatot, mert mi a lényege az eszköz konfigurálásának, ha nem ellenőrizzük, hogy a konfiguráció működik-e? Ezt a folyamatot folytatjuk ebben a témakörben. Parancssor segítségével ellenőrizzük az interfészeket és a hálózatunkban levő switch-ek és routerek címeit.

Csakúgy, mint amikor a **ipconfig** paranccsal (vagy ahhoz hasonló segédprogrammal) ellenőrizzük egy PC hálózati beállításait, szintén parancsokkal ellenőrizhetjük a közvetítő eszközök (switch-ek és routerek) interfészeit és címbeállításait.

A **show ip interface brief** parancsot szemléltető videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra! Ez a parancs hasznos a switch interfészek állapotának ellenőrzéséhez.

**Kövessük végig Packet Tracerben!**

Töltsük le ugyanazt a PKT-fájlt, amit a videóban használnak. Gyakoroljuk az **ipconfig** és a **show ip interface brief** parancsok használatát a videóban látható módon.

[Interfészek tesztelése](https://contenthub.netacad.com/courses/itn/_common/2.8.1-video-activity---test-the-interface-assignment_hu-HU.pkt)

2.8.2

## Videómagyarázat - Végponttól végpontig terjedő kapcsolat tesztelése

A **ping** parancs használható az összeköttetés tesztelésére egy másik hálózati eszközzel vagy egy internetes weboldallal.

Kattintsunk az ábrán látható Lejátszás gombra egy olyan videó megtekintéséhez, melyben a **ping** parancs segítségével tesztelik az összeköttetést egy switch-csel és egy másik számítógéppel!

**Kövessük végig Packet Tracerben!**

Töltsük le ugyanazt a PKT-fájlt, amit a videóban használnak. Gyakoroljuk a **ping** parancs használatát a videóban látható módon.

[Végpontok közötti kapcsolatok ellenőrzése](https://contenthub.netacad.com/courses/itn/_common/2.8.2-video-activity---test-end-to-end-connectivity_hu-HU.pkt)

[2.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IP-címzés beállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[2.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                            

1. Switch-ek és végberendezések alapbeállításainak megadása
2. Gyakorlás és ellenőrzés

Helyes

Sikeresen meghatározta a helyes válaszokat.

14 a 14 kérdésekből helyes.

# Gyakorlás és ellenőrzés

2.9.1

## Packet Tracer - Switch-ek és végberendezések alapbeállításainak megadása

Frissen felvett technikusként megkértek, hogy mutassuk be képességeinket egy kis hálózat konfigurálásán keresztül. Feladatunk két Cisco IOS switch alapbeállításainak megadása, valamint a munkaállomások IP-címeinek beállítása a végponttól végpontig terjedő összeköttetés biztosítása érdekében. Két switch-et és két állomást fogunk használni, melyek össze vannak kötve.

[Switch-ek és végberendezések alapbeállításainak megadása](https://contenthub.netacad.com/courses/itn/_common/2.9.1-packet-tracer---basic-switch-and-end-device-configuration_hu-HU.pka)

2.9.2

## Laborgyakorlat - Switch-ek és végberendezések alapbeállításainak megadása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: A hálózati topológia megépítése
  2. rész: PC-k konfigurálása
  3. rész: Switch alapbeállításainak megadása és ellenőrzése

2.9.3

## Miről tanultunk ebben a fejezetben?

Minden végberendezés és hálózati eszköz operációs rendszert (OS) igényel. A felhasználó az operációs rendszernek parancssoros felületről adhat utasításokat, billentyűzet segítségével használ hálózati programokat, illetve vihet be szöveget és szöveges parancsokat, az eredményt pedig monitoron látja.

Biztonsági okokból a Cisco IOS a felügyeletet a következő két parancssori módra osztja: felhasználói EXEC módra és privilegizált EXEC módra.

A többi specifikus konfigurációs mód előtt globális konfigurációs módba kell lépnünk. A globális konfig módból a felhasználó továbbléphet alkonfigurációs módokba. Mindegyik mód az IOS-eszköz valamelyik részének vagy funkciójának beállításához való. Két gyakran használt alkonfigurációs mód: vonalkonfigurációs mód és interfészkonfigurációs mód. Globális konfigurációs módba lépéshez használjuk a **configure terminal** privilegizált módú parancsot. Privilegizált módba visszatérés pedig az **exit** globális konfig módú paranccsal lehetséges.

Minden parancsnak adott formátuma vagy szintaxisa van, és csak a megfelelő módban lehet azokat kiadni. A parancsok alapvető formája a következő: parancsszó, majd a megfelelő kulcsszavak és paraméterek. Az IOS kétféle segítséget kínál: környezetérzékeny súgót és parancsszintaxis-ellenőrzést.

Szinte mindig a legelső parancs az eszközök saját egyedi nevének, állomásnevének beállítása. A hálózati eszközöknek mindig rendelkezniük kell jelszóval, hogy korlátozzuk az adminisztrációs célú hozzáférést. A Cisco IOS beállítható úgy, hogy hierarchikus jelszavakat használjon, hogy különböző hozzáférési jogosultságokat biztosítson egy hálózati eszközhöz. Beállíthatjuk és titkosíthatjuk az összes jelszót. Beállíthatunk egy üzenetet, amelyben leírjuk, hogy az eszközhöz való hozzáférés csak az arra jogosult személyek számára lehetséges.

Két rendszerfájl tárolja az eszköz konfigurációját: a startup-config és a running-config. Az aktív konfigurációs fájlok módosíthatók, amíg nincsenek elmentve. A konfigurációs fájlokat szövegfájlba is menthetjük és archiválhatjuk.

Az IP-címek teszik lehetővé, hogy az eszközök megtalálják egymást, és az interneten keresztül végponttól végpontig terjedő kommunikáció legyen lehetséges. Minden végberendezésnek rendelkeznie kell IP-címmel. Az IPv4-címek szokásos formája a pontozott decimális forma, ami négy decimális, 0 és 255 közé eső számból áll.

Az IPv4-címeket megadhatjuk manuálisan az eszközön, vagy kaphatja automatikusan a Dynamic Host Configuration Protocol (DHCP) segítségével. A DHCP automatikus végzi az IP-címkiosztást minden hálózati végberendezés számára, melyen a DHCP engedélyezve van. Egy switch távoli eléréséhez IP-címet és alhálózati maszkot kell beállítanunk az SVI-n. A switch virtuális interfészének beállítására az **interface vlan 1 global configuration** parancs használható. A Vlan 1 nem tényleges fizikai interfész, hanem virtuális.

Csakúgy, mint amikor parancs vagy ahhoz hasonló segédprogram segítségével ellenőrizzük egy PC hálózati beállításait, szintén parancsokkal ellenőrizhetjük a közvetítő eszközök (switch-ek és routerek) interfészeit és címbeállításait. A **show ip interface brief** parancs ellenőrzi a switch interfészek állapotát. A **ping** parancs használható az összeköttetés tesztelésére egy másik hálózati eszközzel vagy egy internetes weboldallal.

2.9.4

## Ellenőrző kvíz - Switch-ek és végberendezések alapbeállításainak megadása

Az űrlap teteje

1. Melyik állítás igaz egy Cisco IOS eszközön az aktív konfigurációs fájlra?

Konu 2.5.0 - A forgalomirányítón kiadott konfigurációs parancsok azonnal módosítják az eszköz működését. Az aktív konfigurációs fájlok nem törölhetők, és nem is mentődnek automatikusan.

Az űrlap alja

A felhasználói EXEC módot tekintve melyik két állítás helyes? (Két jó válasz van.)

Konu 2.2.0 - A felhasználói EXEC mód korlátozott hozzáférést ad néhány **show** és **debug** parancshoz. Ez a router konfigurálásakor használható felhasználói felület első szintje, és az eszköz bizonyos funkcióinak vizsgálatára szolgál. A felhasználói EXEC módot a „>” szimbólum jelzi

Minek a védelmét biztosítja az **enable secret** parancs egy Cisco routeren vagy switch-en?

Konu 2.4.0 - Az **enable secret** parancs biztosítja a hozzáférést a privilegizált EXEC módhoz egy Cisco eszközön.

Mi az alapértelmezett SVI egy Cisco switch-en?

Konu 2.6.0 - A 2. rétegbeli switch-ek virtuális interfészeket (SVI-k) használnak az IP-n keresztül történő távoli eléréshez. A Cisco switch-ek alapértelmezett SVI-je a VLAN1.

Ha egy állomásnevet a Cisco CLI segítségével állítunk be, melyik három elnevezési szabály része az irányelveknek? (Három jó válasz van.)

Konu 2.4.0 - Az állomásnév nagy- vagy kisbetűkkel adható meg, és betűvel vagy számjeggyel kell végződnie, nem pedig speciális karakterrel. Az állomásnévnek betűvel kell kezdődnie, és nem szabad szóközt tartalmaznia.

Mi a funkciója a parancshéjnak egy operációs rendszerben?

Konu 2.1.0 - A legtöbb operációs rendszer tartalmaz egy parancshéjat (shell) és egy kernelt. A kernel együttműködik a hardverrel, a shell pedig egy interfész a kernel és a felhasználók között.

Egy érvényes operációs rendszerrel rendelkező router az NVRAM-ban tárolt konfigurációs fájlt tartalmaz. A konfigurációs fájl enable titkos jelszót tartalmaz, de konzoljelszó nincs beállítva. Rendszerindulás után melyik mód jelenik meg a routeren?

Konu 2.2.0 - Ha egy Cisco IOS-eszköz érvényes IOS-t és konfigurációs fájlt tartalmaz, akkor a felhasználói EXEC módban indul. Jelszóra lesz szükség a privilegizált EXEC módba való belépéshez.

A rendszergazda megváltoztatta egy IOS eszköz egyik interfészének IP-címét. Mi egyebet kell tennie, hogy a változtatások életbe lépjenek?

Konu 2.5.0 - A forgalomirányító és kapcsoló konfigurációja azonnal életbe lép, amint beírjuk a parancsot. Emiatt fontos, hogy az éles rendszerben működő eszközök változtatásait alaposan tervezzük meg és gondoljuk át a megvalósítás előtt. Ha a kiadott parancsok után az eszköz instabil vagy elérhetetlenné válik, lehet, hogy újra kell indítanunk, ami leállási idővel jár.

A Cisco router vagy switch melyik memóriája veszíti el az összes tartalmat az eszköz újraindításakor?

Konu 2.5.0 - A RAM felejtő memória, és elveszíti az összes tartalmat, ha a router vagy a switch újraindul, illetve leáll.

Miért adja ki egy technikus a **copy startup-config running-config** parancsot?

Konu 2.5.0 - Legtöbbször a RAM-ban levő aktív konfigurációt módosítjuk, és azt másoljuk az NVRAM-ba. Ebben az esetben azonban a szakember be akar másolni egy korábban elmentett konfigurációt az NVRAM -ból a RAM-ba, hogy változtasson rajta.

Mely funkciókat biztosítja a DHCP?

Konu 2.7.0 - A DHCP dinamikus és automatikus IP-címkiosztást biztosít az állomásoknak.

Melyik két funkciót biztosítja a felhasználó számára a Cisco IOS parancssoros felületének környezetfüggő súgója? (Két jó válasz van.

Konu 2.3.0 - A környezetérzékeny súgó megmutatja a felhasználó számára az adott üzemmódban elérhető parancsokat és azok paramétereit. A szintaxis ellenőrző hibaellenőrzést végez a kiadott parancsokon, a TAB billentyű pedig részlegesen begépelt parancsok kiegészítésére használható.

A Cisco router vagy switch melyik memóriája tárolja az indítási konfigurációs fájlt?

Konu 2.5.0 - A Cisco router vagy switch indítási konfigurációs fájlját az NVRAM tárolja, amely nem felejtő memória.

Melyik alhálózathoz tartozik a 10.1.100.50 IP-cím, ha a 255.255.0.0 alhálózati maszkot használjuk?

Konu 2.6.0 - Az alhálózati maszk célja, hogy elválassza a cím hálózati részét az IP-cím állomásazonosító részétől. Az IP-cím hálózati részét az alhálózati maszk csupa bináris 1-esekből álló része azonosítja. A 255.255.0.0 alhálózati maszk használata az IP-cím első két oktetjét azonosítja hálózati részként.

[2.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kapcsolatok ellenőrzése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                   
*                           

1. Protokollok és modelle
2. Bevezetés

# Bevezetés

3.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Protokollok és modellek fejezetben!

Ismerjük az egyszerű hálózatok alapvető összetevőit, valamint a kezdeti konfigurálásának módját. De az összetevők csatlakoztatása és beállítása után hogyan fognak együttműködni egymással? Protokollok segítségével! A protokollok szabályrendszerek, amelyeket szabványszervezetek hoztak létre. De ha nem lehet felvenni egy szabályt és közelebbről megvizsgálni, hogyan értjük meg igazán, hogy miért van ez a szabály, és mit kellene tennie? Modellek segítségével! A modellek teszik lehetővé a szabályok és helyük megjelenítését a hálózatban. Ez a fejezet áttekintést nyújt a hálózati protokollokról és modellekről. Hamarosan sokkal mélyebben meg fogjuk érteni a hálózatok igazi működését!

3.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Protokollok és modellek

**Fejezet célja:** Elmagyarázzuk, hogy a hálózati protokollok hogyan teszik lehetővé az eszközök számára helyi és távoli hálózati erőforrások elérését.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A szabályok** | Megnézzük azokat a szabályokat, amelyek szükségesek a sikeres kommunikációhoz. |
| **Protokollok** | Elmagyarázzuk, miért van szükség protokollokra a hálózati kommunikációban. |
| **Protokollkészletek** | Elmagyarázzuk a protokollkészletek szerepét. |
| **Szabványügyi szervezetek** | Ismertetjük a szabványügyi szervezetek szerepét a protokollok létrehozásában, ami elősegíti a hálózatok együttműködését. |
| **Referenciamodellek** | Elmagyarázzuk, hogy a TCP/IP és az OSI modell hogyan segíti a kommunikációs folyamat szabványosítását. |
| **Adatbeágyazás** | Elmagyarázzuk, hogy az adatbeágyazás hogyan teszi lehetővé az adatok átvitelét a hálózaton. |
| **Adathozzáférés** | Elmagyarázzuk, hogy a helyi állomások hogyan érik el a hálózat erőforrásait. |

3.0.3

## Csoportos feladat - Kommunikációs rendszer tervezése

Épp most vásároltunk egy új autót személyes használatra. Nagyjából egy hét használat után úgy találjuk, hogy nem működik megfelelően. Miután megbeszéltük a problémát több ismerőssel, úgy döntünk, hogy elvisszük egy autószerelő műhelybe, amelyet nagyon ajánlanak. Ez az egyetlen javítóműhely a közvetlen közelben.

Amikor megérkezünk a műhelybe, azt halljuk, hogy a szerelők egy másik nyelven beszélnek. Nehezen tudjuk elmagyarázni az autó teljesítménybeli problémáit, de a javítást tényleg el kellene végezni. Nem vagyunk biztosak benne, hogy hazavezethetjük, hogy további lehetőségeket keressünk.

Meg kell találni annak a módját, hogy együttműködjünk a szakemberekkel az autó megfelelő javítása érdekében.

Hogyan kommunikáljunk a szerelővel? Tervezzünk kommunikációs modellt annak biztosítására, hogy az autó megfelelően javításra kerüljön.

[2.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A szabályok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                             
*                           

1. Protokollok és modelle
2. A szabályok

# A szabályok

3.1.1

## Videómagyarázat - Eszközök buborékban

Egy hálózati eszköz hálózaton belüli működésének megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

3.1.2

## Kommunikációs alapok

A hálózatok mérete, formája és funkciója különböző. Egy hálózat lehet annyira bonyolult, mint amikor eszközök az interneten keresztül kapcsolódnak egymáshoz, vagy olyan egyszerű, mint amikor két számítógép van összekötve egy kábellel, vagy bármi más e két véglet között. Mindamellett önmagában a fizikai kapcsolat kiépítése a végberendezések között még nem elegendő ahhoz, hogy biztosítsa a kommunikációt. A kommunikációhoz az is kell, hogy az eszközök tudják, "hogyan" kell kommunikálni.

Az emberek különböző kommunikációs módszerekkel osztják meg egymással gondolataikat. Minden kommunikációs módszerben van három közös alkotóelem.

* **Az üzenet forrása (küldő, feladó)** - Az üzenetek forrásai emberek vagy elektronikus eszközök, amelyeknek üzenetet kell küldeniük más személyeknek vagy eszközöknek.
* **﻿Az üzenet célja (címzett, fogadó)** \- A célállomás fogadja és értelmezi az üzenetet.
* **Csatorna** - Az a közeg (média) alkotja, amely azt az utat biztosítja, amelyen az üzenetek haladnak a forrástól a célig.

3.1.3

## Kommunikációs protokollok

Egy üzenet küldését, legyen az szemtől szembe vagy hálózaton keresztüli kommunikáció, szabályok irányítják, amiket protokolloknak nevezünk. Ezek a protokollok a használt kommunikációs módtól függnek. A hétköznapi személyes kommunikációnkban azok a szabályok, amelyeket egy adott közegben használunk (mint például egy telefonhíváskor), nem feltétlenül egyeznek meg azokkal a protokollokkal, amelyeket más közegben használunk (például levélküldéskor).

A levél küldésének folyamata hasonló a számítógépes hálózatokban előforduló kommunikációhoz.

Kattintsunk a gombokra egy analógia és egy hálózati kommunikációs példa megtekintéséhez!

**Analógia**

A két ember személyes kommunikációját bemutató animáció megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

A kommunikáció előtt meg kell egyezniük, hogy miként fognak kommunikálni. Ha a kommunikáció beszéddel történik, akkor először meg kell állapodni a nyelvben. Ezután ha van egy megosztandó üzenet, akkor képesnek kell lenniük arra, hogy érthetően megformázzák.

Például, ha valaki az angol nyelvet használja, de rossz a mondat szerkezete, az üzenet könnyen félreérthető lesz. Mindezek a feladatok jellemzik azokat a protokollokat, amelyeket a kommunikáció megvalósításához használni kell.

Az ábra egy nő és egy férfi közötti kommunikáció animált ábrázolása. Felül vannak a szavak, köztük jobbra nyilakkal: üzenet, üzenetforrás jeladó átviteli közeg jelvevő és üzenet, üzenet célállomása. Az animáció azt mutatja, hogy egy villanykörte jelenik meg a nőstény felett, aki a hímhez utazik, és egy villanykörte jelenik meg a feje fölött.

Üzenet

Jel

Jel

Üzenet

Üzenet   
forrás

Adó

Terjedés   
Közepes

Vevő

Üzenet   
Rendeltetési hely

3.1.4

## A szabályok kialakítása

A kommunikáció megkezdése előtt a feleknek meg kell állapodniuk a beszélgetés szabályaiban. Vegyük például ezt az üzenetet:

humans communication between govern rules. It is verydifficult tounderstand messages that are not correctly formatted and donot follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana compreensivel por muitos individuos diferentes.

Láthatjuk, milyen nehéz elolvasni az üzenetet, mert nincs megfelelően formázva. A hatékony kommunikációhoz szükséges szabályok (azaz protokollok) használatával kellene megírni. Ez a példa megmutatja megfelelően formázva a nyelv és a nyelvtan szabályai szerint.

Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.

A protokolloknak a következő követelményeket kell figyelembe venniük a vevő által érthető üzenet sikeres kézbesítéséhez:

* Azonosított küldő és fogadó
* Közös nyelv és nyelvtan
* A kézbesítés sebessége és időzítése
* Megerősítési vagy nyugtázási követelmények

3.1.5

## Hálózati protokoll követelményei

A hálózati kommunikációban használt protokollok sok ilyen alapvető tulajdonsággal rendelkeznek. Amellett, hogy azonosítják a forrást és a célt, a számítógépes és hálózati protokollok meghatározzák annak részleteit, hogyan kell egy üzenetet továbbítani a hálózaton keresztül. A leggyakoribb számítógépes protokollok a következő követelményeket teljesítik:

* Az üzenet kódolása
* Az üzenet formázása és beágyazása
* Az üzenet mérete
* Az üzenet időzítése
* Az üzenet szállítási feltételei

3.1.6

## Üzenet kódolása

Egy üzenet elküldésének egyik első lépése a kódolás. A kódolás az, amikor egy információt egy másik, a továbbításhoz megfelelő formába alakítunk át. A dekódolás ennek a fordítottja.

Kattintsunk a gombokra egy analógia és egy hálózati kódolás példájának megtekintéséhez!

**Analógia**

Képzeljük el, hogy egy személy felhívja a barátját, hogy megvitassa egy gyönyörű naplemente részleteit. Az üzenetkódolás animációjának megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

Az üzenet közléséhez gondolatait egy elfogadott nyelvre alakítja át. Beszéd közben a nyelv hangjait használva küldi el az üzenetet. A barátja meghallgatja a leírást, és dekódolja a hangokat, hogy megértse a kapott üzenetet.

**Üzenet**

**Jel**

**Jel**

**Üzenet**

Üzenetforrás

Kódoló

Adó

Terjedés   
Közepes   
"A csatorna"

Vevő

Dekóder

Üzenet célállomása

Forrás Kódolva

Cél dekódolva

3.1.7

## Üzenet formázása és a beágyazása

Amikor egy üzenetet küldünk a forrástól a célig, megfelelő formátumot vagy szerkezetet kell használni. Az üzenet formátuma, formája az üzenet típusától és az átvitelhez használt csatornától függ.

Kattintsunk az egyes gombokra egy analógiához és egy hálózati példához az üzenetek formázásáról és beágyazásáról!

**Analógia**

Az emberi kommunikáció helyes formájának használata talán egy levél elküldésével szemléltethető a legjobban. A levél formázását és beágyazását bemutató animáció megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

A borítékon szerepel a küldő és a fogadó címe, mindegyik a megfelelő helyen. Ha a célcím vagy a formátum helytelen, a levelet nem tudják kézbesíteni.

Beágyazásnak hívjuk azt a folyamatot, amikor egy üzenetformátumot (levél) egy másik üzenetformátumba (boríték) helyezünk. Ennek a fordítottja, a kicsomagolás az, amikor a címzett kiveszi a levelet a borítékból.

egy IPv6-csomag mezői, beleértve a forrás IP-címét és a cél IP-címét

Címzett (célállomás) Hely címe

Feladó (forrás) Hely címe

Üdvözlet (az üzenet kezdete jelző)

Címzett (cél) azonosító

A levél tartalma (kapszulázott adatok)

Feladó (forrás) azonosító

Képkocka vége (Üzenet vége jelző)

Borítékcímzés

Tokozott levél

Feladó   
4085 SE Pine Street   
Öcala, Florida 34471

Befogadó   
1400 Main Street   
Canton, Ohio 44203

4085 SE Pine Street   
Öcala, Florida 34471

4085 SE Pine Street   
Öcala, Florida 34471

1400 Main Street   
Canton, Ohio 44203

1400 Main Street   
Canton, Ohio 44203

Kedves Jane,   
  
Most tértem vissza az utazásomról. Gondoltam, szívesen megnéznéd a képeimet.   
  
János

kedves

Jane

Most tértem vissza az utazásomról. Gondoltam, szívesen megnéznéd a képeimet.

János

kedves

Jane

Most tértem vissza az utazásomról. Gondoltam, szívesen megnéznéd a képeimet.

János

3.1.8

## Üzenet mérete

A kommunikáció egy másik szabálya a mérettel kapcsolatos.

Kattintsunk az egyes gombokra egy analógia és egy üzenetmérettel kapcsolatos hálózati példa megtekintéséhez!

**Analógia**

A szemtől-szembe történő kommunikáció során használt üzenetméret animációjának megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

Amikor az emberek egymással kommunikálnak, a küldendő üzenetet általában kisebb részekre, rendszerint mondatokra tördelik. A mondatok méretét korlátozza az, hogy a fogadó személy mennyit képes egyszerre feldolgozni (lásd az ábrát). Megkönnyíti az olvasást és a megértést is.

3.1.9

## Üzenet időzítése

Az üzenet időzítése szintén nagyon fontos a hálózati kommunikációban. Az üzenet időzítése a következőket jelenti:

* **Adatfolyam-vezérlés -** Az adatátvitel sebességének kezelése. Az adatfolyam-vezérlés meghatározza, hogy mennyi információt küldhetünk el és milyen sebességgel, hogy sikeresen célba érjen. Például, ha egy ember túlságosan gyorsan beszél, a többieknek nehéz meghallani és megérteni az üzenetet. A hálózati kommunikációban vannak olyan hálózati protokollok, amelyeket a forrás- és céleszközök használnak az információ áramlásának egyeztetésére és kezelésére.
* **Válaszidő-túllépés -** Ha valaki feltesz egy kérdést, és nem hallja a választ elfogadható időn belül, akkor feltételezi, hogy már nem is jön válasz, és ennek megfelelően reagál. Lehet, hogy megismétli a kérdést, de az is lehet, hogy folytatja a párbeszédet. A hálózati állomásoknak szintén vannak szabályaik, amik meghatározzák, hogy mennyit kell várni a válaszra, és mit kell csinálni, ha válaszidő-túllépés történik.
* **Hozzáférési mód -** Meghatározza, hogy mikor küldhet valaki üzenetet. Kattintsunk az ábrán látható Lejátszás gombra egy olyan animáció megtekintéséhez, amelyben ketten egyszerre beszélnek, "információütközés" lép fel, ezért mindkettőjüknek be kell fejezniük, majd újra kell kezdeniük az egészet. Hasonlóképpen, ha egy eszköz vezeték nélküli LAN-on szeretne továbbítani, a WLAN hálózati interfész kártyának (NIC) meg kell állapítania, hogy a vezeték nélküli közeg rendelkezésre áll-e.

Az animációban egy nő és egy férfi egyszerre beszélnek. A nő azt mondja, hány óra van a filmben? és a férfi azt mondja: Mikor találkozunk vacsorázni?. Mivel egyszerre beszéltek, egyikük sem értette a másikat, és mindketten azt mondják: Elnézést? Nem értettelek.

3.1.10

## Üzenet szállítási feltételei

Egy üzenetet több különböző módon lehet kézbesíteni.

Kattintsunk az egyes gombokra egy analógiához és egy hálózati példához az üzenetek kézbesítéséről!

**Analógia**

Vannak olyan helyzetek, mikor csupán egyetlen emberrel szeretnénk valamilyen információt megosztani. Máskor előfordulhat, hogy emberek egy csoportjával, vagy akár egy adott területen lévő összes emberrel szeretnénk egyszerre közölni valamit.

Kattintsunk az ábra alatti címkékre (unicast, multicast, broadcast) a példák megtekintéséhez!

Unicast

Multicast

Broadcast

Source

3.1.11

## Megjegyzés a csomópont ikonról

A hálózati dokumentumok és topológiák gyakran egy csomópont ikon használatával jelenítik meg a hálózati és végberendezéseket. A csomópontok jellemzően körként jelennek meg. Az ábra a három különböző kézbesítés összehasonlítását mutatja a számítógép ikonjai helyett csomópont ikonokkal.

Az ábra a hálózati csomópontokat jelző köröket használja a három különböző üzenetküldési lehetőség bemutatására. Három topológia látható balról jobbra. A bal oldali topológia egy unicast üzenetet ábrázol, és egy piros csomópontból, egy zöld csomópontból és négy sárga csomópontból áll. Van rajta egy nyíl a piros csomópontról, amely a zöld csomóponthoz vezet. A középső topológia egy csoportos üzenetet ábrázol, és egy piros csomópontból, három zöld csomópontból és két sárga csomópontból áll. Van rajta egy nyíl a piros csomópontból, amely minden zöld csomóponthoz vezet. A jobb oldali topológia egy adást ábrázol. Egy piros és öt zöld csomópontja van. Van rajta egy nyíl a piros csomópontból, amely minden zöld csomóponthoz vezet.

Unicast Multicast Broadcast

3.1.12

## Tudáspróba - A szabályok

Az űrlap teteje

Ellenőrizze, hogy megértette-e a sikeres kommunikáció szabályait, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Mi a folyamata az információnak az átvitel megfelelő formájává alakításának?

Az űrlap alja

A kommunikációs folyamat melyik lépése foglalkozik a küldő és a fogadó címének megfelelő azonosításával?

Melyik három összetevője az üzenetidőzítésnek? (Válassz hármat.)

Melyik kézbesítési módot használják az információk továbbítására egy vagy több végkészülékhez, de nem minden eszközhöz a hálózaton?

[3.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Protokollok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                               
*                           

1. Protokollok és modelle
2. Protokollok

# Protokollok

3.2.1

## A hálózati protokollok áttekintése

Már tudjuk, hogy ahhoz, hogy a végberendezések hálózaton keresztül kommunikálhassanak, minden eszköznek ugyanazokat a szabályokat kell betartania. Ezeket a szabályokat protokolloknak nevezzük, és számos funkciójuk van a hálózaton. Ez a témakör áttekintést nyújt a hálózati protokollokról.

Az eszközök közti üzenettovábbítás közös formátumát és szabályrendszerét a hálózati protokollok határozzák meg. A protokollokat végberendezések és közvetítő eszközök valósítják meg szoftveresen, hardveresen vagy mindkettő módon. Minden hálózati protokoll saját funkcióval, formátummal és kommunikációs szabályokkal rendelkezik.

A táblázat felsorolja azokat a protokollokat, amelyek egy vagy több hálózaton keresztül történő kommunikáció sikerességéhez szükségesek.

| Táblázat felirata | |
| --- | --- |
| **Protokoll típusa** | **Leírás** |
| **Hálózati kommunikációs protokollok** | Lehetővé teszik, hogy két vagy több eszköz kommunikáljon egy vagy több hálózaton keresztül. Az Ethernet család számos protokollt foglal magában, ilyenek az IP, a Transmission Control Protocol (TCP), a HyperText Transfer Protocol (HTTP), és még sok más. |
| **Hálózatbiztonsági protokollok** | Ezek a protokollok az adatok biztonságával kapcsolatosak, hitelesítést, az adatok integritását és adattitkosítást biztosítanak. A biztonsággal kapcsolatos protokollok közé tartozik például a Secure Shell (SSH), a Secure Sockets Layer (SSL) és a Transport Layer Security (TLS). |
| **Irányító protokollok** | Ezek a protokollok lehetővé teszik routerek közt az útvonalinformációk cseréjét, az útvonalinformációk összehasonlítását, majd a célhálózat legjobb elérési útjának kiválasztását. Irányító protokoll például az Open Shortest Path First (OSPF) és a Border Gateway Protocol (BGP). |
| **Szolgáltatásfelderítési protokollok** | Ezeket a protokollokat eszközök vagy szolgáltatások automatikus észlelésére használják. A szolgáltatásfelderítési protokollok közé tartozik például a Dynamic Host Configuration Protocol (DHCP), amely az IP-címkiosztási szolgáltatásokat fedezi fel, valamint a nevek és IP-címek közötti fordításhoz használt Domain Name System (DNS). |

3.2.2

## Hálózati protokollok funkciói

A hálózati kommunikációs protokollok felelősek a végberendezések közötti hálózati kommunikációhoz szükséges különböző funkciókért. Például az ábrán levő számítógép hogyan küld üzenetet több hálózati eszközön keresztül a kiszolgálónak?

Az ábra azt mutatja be, hogy az IPv4 protokoll hogyan használható üzenet küldésére a számítógépről a hálózaton keresztül a szerverre. Az ábra közepén három router található, amelyek háromszögben vannak összekapcsolva. A bal oldali útválasztó egy számítógéphez csatlakozik. A jobb oldali útválasztó egy szerverhez csatlakozik. A számítógép alatt egy üzenet a következő: Ezt az üzenetet elküldöm a hálózaton keresztül IPv4-fejléc használatával. A csatolt útválasztó alatt egy üzenet a következő: Továbbíthatom ezt az üzenetet, mert értem az IPv4 fejlécet. A szerver alatt egy üzenet a következő: El tudom fogadni ezt az üzenetet, mert értem az IPv4-et.

Ezt az üzenetet a hálózaton keresztül IPv4 fejléc használatával küldöm el. Továbbíthatom ezt az üzenetet, mert értem az IPv4 fejlécet. El tudom fogadni ezt az üzenetet, mert értem az IPv4-et. IP adatok

A számítógépek és a hálózati eszközök közös protokollokat használnak a kommunikációhoz. A táblázat felsorolja a protokollok funkcióit.

| Táblázat felirata | |
| --- | --- |
| **Funkció** | **Leírás** |
| **Címzés** | Azonosítja az üzenet küldőjét és címzettjét egy meghatározott címzési rendszer szerint. Címzést biztosító protokoll például az Ethernet, az IPv4 és az IPv6. |
| **Megbízhatóság** | Ez a funkció szállítási mechanizmusokat biztosít abban az esetben, ha az üzenetek elvesznek vagy megsérülnek a továbbítás során. A TCP biztosít garantált kézbesítést. |
| **Adatfolyam-vezérlés** | Ez a funkció biztosítja, hogy az adatok hatékony sebességgel áramoljanak két kommunikáló eszköz között. A TCP adatfolyam-vezérlési szolgáltatásokat is nyújt. |
| **Sorrendhelyes kézbesítés** | Minden továbbított adatszegmens saját azonosítót kap. A fogadó eszköz az azonosítási információkat használja az információ megfelelő módon történő újbóli összeállításához. Akkor hasznos, ha elvesznek vagy rossz sorrendben érkeznek az adatszegmensek. A TCP azonosítást és sorba rendezést is biztosít. |
| **Hibafelismerés** | Ez a funkció annak meghatározására szolgál, hogy az adatok megsérültek-e az átvitel során. Hibadetektálást biztosít többek között az Ethernet, az IPv4, az IPv6 és a TCP. |
| **Alkalmazás interfész** | Ez a funkció a hálózati alkalmazások közötti folyamat-folyamat közti kommunikációhoz használt információkat tartalmazza. Weboldal elérésekor például HTTP vagy HTTPS protokollokat használnak a kliens és a szerver webes folyamatai közötti kommunikációra. |

3.2.3

## A protokollok együttműködése

A számítógépes hálózaton keresztül küldött üzenet általában több protokoll használatát igényli, amelyek mindegyike saját funkciókkal és formátummal rendelkezik. Az ábra néhány hálózati protokollt mutat be, amelyeket akkor használunk, amikor egy eszköz lekéri egy webszerver weboldalát.

Egy kis hálózati diagram balról jobbra mutatja az internetes felhőhöz csatlakoztatott laptopot, amely egy szerverhez csatlakozik. Egy boríték keresztezi a kapcsolatot a laptop és a felhő között. A boríték alatt azon protokollok listája található, amelyeket akkor használnak, amikor egy eszköz kérést küld egy webszervernek egy weboldalra vonatkozóan. Az ábra alján található szöveg ezeket a protokollokat írja le, és így szól: Hypertext Transfer Protocol (HTTP) – Ez a protokoll szabályozza a webszerver és a webkliens interakcióját. A HTTP határozza meg a kliens és a szerver között kicserélt kérések és válaszok tartalmát és formázását. Mind a kliens, mind a webszerver szoftver az alkalmazás részeként implementálja a HTTP-t. A HTTP más protokollokra támaszkodik, hogy szabályozza az üzenetek továbbítását az ügyfél és a szerver között. Transmission Control Protocol (TCP) – Ez a protokoll kezeli az egyes beszélgetéseket. A TCP felelős az információ megbízható továbbításának garantálásáért és a végberendezések közötti áramlásszabályozás kezeléséért. Internet Protokoll (IP) – Ez a protokoll felelős az üzenetek küldőtől a fogadó felé történő eljuttatásáért. Az IP-címet az útválasztók használják az üzenetek továbbítására több hálózaton keresztül. Ethernet – Ez a protokoll felelős az üzenetek kézbesítéséért az egyik hálózati kártyától egy másik hálózati kártyához ugyanazon az Ethernet helyi hálózaton (LAN).

HTTP TCP IP Ethernet Internet

Az ábrán szereplő protokollok leírása:

* **Hypertext Transfer Protocol (HTTP) -** Ez a protokoll felelős a webszerver és a kliens kommunikációjáért. A HTTP leírja a kliens és a szerver közötti kérések és válaszok formáját és tartalmát. A HTTP-t mind a kliens, mind pedig a webszerver szoftvere egyaránt használja. A HTTP más protokollokra bízza, hogy az üzenetek szállítása hogyan történjen a kliens és a szerver között.
* **Transmission Control Protocol (TCP)** - Ez a protokoll hozza létre az egyedi párbeszédeket. A TCP megbízható kézbesítést garantál, emellett adatfolyam-vezérlést is biztosít.
* **Internet Protocol (IP) -** Az IP végzi az üzenetek továbbítását a küldőtől a címzettig. Az IP segítségével továbbítják a routerek az üzeneteket több hálózaton keresztül is.
* **Ethernet** \- Ez a protokoll az azonos Ethernet LAN-on elhelyezkedő eszközök hálózati interfészei között továbbítja az üzenetet.

3.2.4

## Tudáspróba - Protokollok

Az űrlap teteje

Ellenőrizze, hogy megértette-e a hálózati kommunikációban használt protokollokat, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. A BGP és az OSPF milyen típusú protokollok példái?

Az űrlap alja

Melyik két protokoll szolgáltatásfelderítési protokoll? (Válassz kettőt.)

Mi a szekvenáló funkció célja a hálózati kommunikációban?

This protocol is responsible for guaranteeing the reliable delivery of information.

[3.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A szabályok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Protokollkészletek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                   
*                           

1. Protokollok és modelle
2. Protokollkészletek

# Protokollkészletek

3.3.1

## Hálózati protokollkészletek

Sok esetben a protokolloknak képesnek kell lenniük más protokollokkal való együttműködésre, hogy teljes legyen az online élményünk. A protokollkészleteket zökkenőmentes együttműködésre tervezték.

A protokollkészlet egymáshoz kapcsolódó protokollok csoportja.

Az egyik legjobb mód annak szemléltetésére, hogy a protokollok a készleten belül hogyan lépnek kölcsönhatásba, ha az együttműködést egy veremként szemléljük. A protokollverem (protocol stack) megmutatja, hogy az egyes protokollok a készleten belül hogyan hajtódnak végre. A protokollokat rétegek formájában szemléltetjük, ahol minden egyes magasabb szintű szolgáltatás az alsóbb rétegekben definiált protokollok szolgáltatásaitól függ. A verem alsóbb rétegei az adatok hálózaton belüli mozgatását és a felsőbb rétegek számára történő szolgáltatások nyújtását végzik, amelyek középpontjában az üzenet tartalmának elküldése áll.

Amint az ábra mutatja, a rétegeket használhatjuk a szemtől szembeni kommunikációs példában lévő tevékenységek leírására is. Az alsó rétegben (fizikai réteg) két ember szavakat mond ki hangosan. Középen a szabályok rétege, amely meghatározza a kommunikációs követelményeket, például a közös nyelvet. A tetején van a tartalmi réteg, ez az, ahol a kommunikáció tartalma ténylegesen elhangzik.

Az ábra három különböző réteget mutat be, amelyekkel leírják, mi történik a szemtől szembeni kommunikáció során. Az alsó, fizikai réteg címkével ellátott réteg két embert jelenít meg, akik üzenetet váltanak. A középső, szabályos címkével ellátott réteg felsorolja a használni kívánt beszélgetési protokollcsomagot, beleértve: közös nyelv használata; várj a sorodra; és jelezze, ha végzett. A felső réteg tartalomréteggel van ellátva, és a következő üzenetet tartalmazza: Hol van a kávézó? Alul a következő szöveg olvasható: A protokollcsomagok olyan szabálykészletek, amelyek együttesen segítik a probléma megoldását.

Hol van a kávézó? Tartalomréteg szabályai Layer Fizikai réteg **Beszélgetési protokollcsomag**   
1. Használjon közös nyelvet   
2. Várja meg a sorát   
3. Jelezzen, ha végzett

A protokollcsomagok olyan szabálykészletek, amelyek együtt segítik a probléma megoldását.

3.3.2

## A protokollkészletek evolúciója

A protokollkészlet egy sor protokoll, amelyek együttműködnek annak érdekében, hogy átfogó hálózati kommunikációs szolgáltatásokat biztosítsanak. Az 1970-es évek óta számos különböző protokollkészlet létezik, néhányat szabványszervezetek fejlesztettek ki, másokat pedig különböző gyártók.

A hálózati kommunikáció és az internet fejlődése során számos rivális protokollkészlet létezett, ahogy az ábrán is látható.

Az ábra egy táblázat, alatta szöveggel. A táblázat négy sorból és öt oszlopból áll. Az első oszlopfejléc a TCP/IP-réteg neve, és fentről lefelé olvasható: Application, Transport, Internet és Network Access. A második oszlopfejléc a TCP/IP. Az alkalmazásprotokollok a következők: HTTP, DNS, DHCP és FTP. A szállítási protokollok a TCP és az UDP. Az internetes protokollok az IPv4, IPv6, ICMPv4 és ICMPv6. A hálózati hozzáférési protokollok az Ethernet, ARP és WLAN. A harmadik oszlopfejléc az ISO. Az alkalmazásprotokollok a következők: ACSE, ROSE, TRSE és SESE. A szállítási protokollok a TP0, TP1, TP2, TP3 és TP4. Az internetes protokollok a CONP/CMNS és a CLNP/CLNS. A hálózati hozzáférési protokollok az Ethernet, ARP és WLAN. A negyedik oszlopfejléc az AppleTalk. Az alkalmazás protokollja az AFP. A szállítási protokollok az ATP, AEP, NBP és RTMP. Az internetes protokollok AARP. A hálózati hozzáférési protokollok az Ethernet, ARP és WLAN. Az ötödik oszlopfejléc a Novell Netware. Az alkalmazási protokoll az NDS. A szállítási protokoll SPX. Az Internet protokoll IPX. A hálózati hozzáférési protokollok az Etherent, az ARP és a WLAN. A táblázat alatti szöveg a következő: Internet Protocol Suite vagy TCP/IP – Ez a ma legáltalánosabb és legrelevánsabb protokollcsomag. A TCP/IP protokollcsomag egy nyílt szabványú protokollcsomag, amelyet az Internet Engineering Task Force (IETF) tart fenn. Open Systems Interconnection (OSI) protokollok – Ez a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Távközlési Unió (ITU) által 1977-ben közösen kifejlesztett protokollcsalád. Az OSI protokoll egy hétrétegű modellt is tartalmazott, az OSI referenciamodellnek nevezett. Az OSI referenciamodell kategorizálja a protokolljainak funkcióit. Ma az OSI főként réteges modelljéről ismert. Az OSI protokollokat nagyrészt a TCP/IP váltotta fel. AppleTalk – Az Apple Inc. által 1985-ben kiadott, rövid életű szabadalmaztatott protokollcsomag Apple eszközökhöz. 1995-ben az Apple elfogadta a TCP/IP-t az AppleTalk helyett. Novell NetWare – A Novell Inc. által 1983-ban IPX hálózati protokollt használó, rövid életű szabadalmaztatott protokollcsomag és hálózati operációs rendszer. 1995-ben a Novell elfogadta a TCP/IP-t az IPX helyére.

TCP/IP ISO AppleTalk Novell   
Netware HTTP   
DNS   
DHCP   
FTP ACSE   
RÓZSA   
TRSE   
SESE AFP NDS TCP   
UDP TP0 TP1   
TP2   
TP3 TP4 ATP AEP   
NBP RTMP SPX IPv4 IPv6   
ICMPv4   
ICMPv6 CONP/CMNS   
CLNP/CLNS AARP IPX Ethernet ARP WLAN TCP/IP rétegnév Alkalmazás szállítása Internet hálózati hozzáférés

* **Internet vagy TCP/IP protokollkészlet** - Ez a legszélesebb körben használt protokollkészlet. Az TCP/IP nyílt protokollkészlet, az Internet Engineering Task Force (IETF) kezeli.
* **Open Systems Interconnection (OSI) protokollok** - A Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Távközlési Unió (ITU) által közösen kifejlesztett protokollcsalád. Az OSI egy hét rétegű modellt, az OSI-referenciamodellt is megalkotott. Az OSI referenciamodell kategorizálja a protokollok funkcióit. Az OSI főleg a rétegmodellről ismert. Az OSI protokollokat lényegében felváltotta a TCP/IP.
* **AppleTalk** - Az Apple által 1985-ben kiadott rövid életű, zárt protokollkészlet Apple eszközökre. 1995-ben az Apple a TCP/IP-re cserélte az AppleTalkot.
* **Novell NetWare** - Rövid életű, zárt protokollkészlet és hálózati operációs rendszer, amelyet a Novell fejlesztett ki 1983-ban az IPX hálózati protokoll használatával. A Novell az IPX-et 1995-ben TCP/IP-re cserélte.

3.3.3

## TCP/IP protokoll példa

TCP/IP protokollok léteznek az alkalmazási, a szállítási és az internet rétegben egyaránt. A hálózatelérési rétegben viszont nincsenek TCP/IP protokollok. A leggyakoribb hálózatelérési rétegbeli LAN-protokoll az Ethernet és a WLAN (vezeték nélküli LAN). A hálózatelérési rétegben lévő protokollok az IP-csomag fizikai közegen történő továbbításáért felelősek.

Az ábra egy példát mutat a három TCP/IP protokollra, amelyek csomagokat szállítanak egy állomás webböngészője és a webszerver között. Most a HTTP, a TCP és az IP protokollokat használjuk. A példában szereplő hálózatelérési protokoll az Ethernet. De lehetne egy vezeték nélküli szabvány is, mint a WLAN vagy mobil adatkapcsolat.

Az ábra azokat a TCP/IP protokollokat mutatja, amelyek segítségével csomagokat küldenek egy gazdagép webböngészője és egy webszerver között. A hálózati topológia az internetes felhőhöz csatlakoztatott gazdagépet mutatja, amely egy webkiszolgálóhoz kapcsolódik. Egy csomagot jelképező boríték látható az internet és a szerver között. A csomagból sugárzó információ az egyes rétegekben használt protokollokról. Felülről lefelé: alkalmazási réteg és hipertext átviteli protokoll (HTTP); szállítási réteg és átvitelvezérlő protokoll (TCP); Internet réteg és Internet protokoll (IP); valamint a hálózati hozzáférési réteg és az Ethernet.

Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) Internet Protocol (IP) Ethernet Web   
Szerverprotokoll veremréteg neve Alkalmazás Szállítás Internet Hálózati hozzáférés Internet

3.3.4

## A TCP/IP protokollkészlet

Mára a TCP/IP protokollkészlet számos protokollt tartalmaz, és folyamatosan fejlődik az új szolgáltatások támogatása érdekében. A népszerűbbek közül néhányat az ábrán mutatunk be.

Az ábra a TCP/IP rétegeket és a kapcsolódó protokollokat mutatja. Az alkalmazási rétegben: A DNS egy névrendszer-protokoll; A DHCPv4, DHCPv6 és SLAAC gazdagép konfigurációs protokollok; Az SMTP, a POP3 és az IMAP e-mail protokollok; Az FTP, SFTP és TFTP fájlátviteli protokollok; a HTTP, HTTPS és REST pedig webes és webszolgáltatási protokollok. A szállítási rétegben: A TCP egy kapcsolatorientált protokoll, az UDP pedig egy kapcsolat nélküli protokoll. Az internetes rétegben: az IPv4, az IPv6 és a NAT internetes protokollok; Az ICMPv4, ICMPv6 és ICMPv6 ND üzenetküldési protokollok; az OSPF, az EIGRP és a BGP pedig útválasztási protokollok. A hálózati hozzáférési rétegben: Az ARP egy címfeloldó protokoll; az Ethernet és a WLAN pedig adatkapcsolati protokollok. Alul a következő szöveg olvasható: A TCP/IP az internet és a mai hálózatok által használt protokollcsomag. A TCP/IP-nek két fontos szempontja van a szállítók és a gyártók számára: Nyílt szabványos protokollcsomag – Ez azt jelenti, hogy szabadon elérhető a nyilvánosság számára, és bármely gyártó használhatja hardverén vagy szoftverén. Szabvány alapú protokollcsomag – Ez azt jelenti, hogy a hálózati iparág jóváhagyta, és egy szabványügyi szervezet jóváhagyta. Ez biztosítja, hogy a különböző gyártók termékei sikeresen együttműködjenek egymással.

A TCP/IP rétegei Alkalmazási réteg Névfeloldás   
Állomás   
konfiguráció E-mail Fájlátvitel   
Web és   
webes szolgáltatások Szállítási réteg Összeköttetés alapú Összeköttetésmentes Internet réteg Internet protokoll Üzenetküldés Irányító protokollok Hálózatelérési réteg Címfeloldás Adatkapcsolati protokollok TCP/IP protokollok DNS DHCPv4 DHCPv6 SLAAC SMTP POP3 IMAP FTP SFTP TFTP HTTP HTTPS REST TCP UDP IPv4 IPv6 NAT ICMPv4 ICMPv6 ICMPv6 ND OSPF EIGRP BGP ARP Ethernet WLAN

A TCP/IP az internet és a mai hálózatok által használt protokollkészlet. A TCP/IP-nek két fontos tulajdonsága van a gyártók számára:

* **Nyílt szabványú protokollkészlet** - Ez azt jelenti, hogy szabadon hozzáférhető a nyilvánosság számára, és bármely gyártó használhatja a hardverén vagy szoftverében.
* **Szabványosított protokollkészlet** - A hálózattal foglalkozó ipar által elfogadott, szabványügyi szervezet által jóváhagyott protokollkészlet. Ez teszi lehetővé, hogy különböző gyártók termékei képesek legyenek együttműködni egymással.

A rétegek protokolljainak rövid leírásához kattintsunk a gombokra!

**Hálózatelérési réteg**

Címfeloldás

* **ARP** - Address Resolution Protocol. Dinamikus címfeloldást biztosít IPv4-címek és hardvercímek között.

Adatkapcsolati protokollok

* **Ethernet** - Kábelezési és jelzési szabályokat határoz meg a hálózatelérési rétegben.
* **WLAN** - Wireless Local Area Network. Meghatározza a 2,4 GHz-es és 5 GHz-es rádiófrekvenciákon keresztüli vezeték nélküli jelzés szabályait.

**Internet réteg**

Internet Protokoll (IP)

* **IPv4** - Internet Protocol version 4. Üzenetszegmenseket fogad a szállítási rétegtől, csomagokba ágyazza az üzeneteket, és megcímzi őket a hálózaton keresztül végponttól végpontig történő kézbesítéshez. Az IPv4 32 bites címet használ.
* **IPv6** - IP version 6. Hasonló az IPv4-hez, de 128 bites címet használ.
* **NAT** - Network Address Translation. Egy privát hálózat IPv4-címeit globális egyedi publikus címekre fordítja.

Üzenetküldés

* **ICMPv4** - Internet Control Message Protocol for IPv4. A célállomástól a forrás számára ad visszajelzést a csomagtovábbítás hibáiról.
* **ICMPv6** - ICMP for IPv6. Hasonló az ICMPv4-hez, de IPv6-csomagokhoz.
* **ICMPv6 ND** - ICMPv6 Neighbor Discovery. Négy protokollüzenetet tartalmaz, amelyek címfeloldáshoz és duplikált cím detektálásához használhatók.

Irányító protokollok

* **OSPF** - Open Shortest Path First. Kapcsolatállapot alapú irányító protokoll, amely területeken alapuló hierarchikus rendszert használ. Az OSPF nyílt szabványú, belső irányító protokoll.
* **EIGRP** - Enhanced Interior Gateway Routing Protocol. A Cisco saját irányító protokollja, amely a sávszélesség, a késleltetés, a terhelés és a megbízhatóság alapján összetett metrikát számol.
* **BGP** - Border Gateway Protocol. Szolgáltatók által használt nyílt szabványú, külső irányító protokoll. A BGP-t gyakran használják a szolgáltatók és a nagy hálózatot üzemeltető ügyfeleik közötti irányítási információk cseréjéhez.

**Szállítási réteg**

Összeköttetés alapú

* **TCP** - Transmission Control Protocol. Megbízható kommunikációt tesz lehetővé a különböző állomásokon futó folyamatok között, és megbízható, nyugtázott átvitelt biztosít, amely visszajelzést ad a sikeres kézbesítésről.

Összeköttetésmentes

* **UDP** - User Datagram Protocol. Egy állomáson futó folyamat csomagokat küldhet egy másik állomáson futó folyamatnak. Az UDP nem ad visszajelzést az átvitel sikerességéről.

**Alkalmazási réteg**

Névfeloldás

* **DNS** - Domain Name System. A neveket (pl.: cisco.com) IP-címekké oldja fel.

Állomáskonfiguráció

* **DHCPv4** - Dynamic Host Configuration Protocol for IPv4. A DHCPv4-szerver IPv4-címzési információkat biztosít DHCPv4-kliensek számára, és lehetővé teszi a felszabadult címek újbóli felhasználását.
* **DHCPv6** - Dynamic Host Configuration Protocol for IPv6. A DHCPv6 hasonló a DHCPv4-hez. A DHCPv6-szerver dinamikusan rendel IPv6-címzési adatokat a DHCPv6-kliensekhez indításkor.
* **SLAAC** - Stateless Address Autoconfiguration. Olyan módszer, amely lehetővé teszi az eszköz számára, hogy az IPv6-címzési adatait DHCPv6-szerver használata nélkül szerezze be.

Email

* **SMTP** - Simple Mail Transfer Protocol. Lehetővé teszi a kliensek számára, hogy e-maileket küldjenek egy levelezőszervernek, a szerverek számára pedig, hogy a leveleket más szervereknek küldjék tovább.
* **POP3** - Post Office Protocol version 3. Lehetővé teszi a kliensek számára, hogy e-maileket kérjenek le egy levelezőszerverről és letöltsék azokat egy helyi alkalmazás számára.
* **IMAP** - Internet Message Access Protocol. Lehetővé teszi a kliensek számára, hogy hozzáférjenek és kezeljék a szerveren tárolt leveleiket.

Fájlátvitel

* **FTP** - File Transfer Protocol. Olyan szabályok, amelyek segítségével a felhasználó egy állomás előtt ülve hozzáfér egy másik állomáson tárolt fájlokhoz a hálózaton keresztül, és akár át is másolhatja őket. Megbízható, összeköttetés alapú, nyugtázott fájlátviteli protokoll
* **SFTP** - SSH File Transfer Protocol. Az SFTP az SSH protokoll kiegészítése, biztonságos, titkosított fájlátviteli munkamehetet létesít. Az SSH a biztonságos távoli bejelentkezés módszere, amelyet általában egy eszköz parancssorának eléréséhez használnak.
* **TFTP** - Trivial File Transfer Protocol. Egyszerű, kapcsolat nélküli fájlátviteli protokoll, legjobb szándékú, nem nyugtázott fájlkézbesítéssel. Kevesebb többletterheléssel jár, mint az FTP.

Weboldalak és webes szolgáltatások

* **HTTP** - Hypertext Transfer Protocol. Szövegek, képek, hang, videó és más multimédiafájlok weben történő átvitelét meghatározó szabályok.
* **HTTPS** - HTTP Secure. A HTTP biztonságos formája, amely titkosítja a világhálón átadott adatokat.
* **REST** - Representational State Transfer. Olyan webes szolgáltatás, amely alkalmazásprogramozási felületeket (API-kat) és HTTP-kéréseket használ webalkalmazások létrehozásához.

3.3.5

## A TCP/IP kommunikációs folyamata

Az ábrák bemutatják a teljes kommunikációs folyamatot, ahogyan egy webszerver adatokat továbbít a kliensnek.

Kattintsunk az ábrán látható Lejátszás gombra, hogy megtekintsük az animációt, amelyben a webszerver egy weboldal beágyazását és a klienshez küldését hajtja végre.

Az animáció egy kis hálózatot mutat be webszerverrel és webklienssel. Van egy grafika, amely bemutatja az üzenetet alkotó összetevőket. Egy Ethernet-keret és egy IP-csomag, egy TCP-szegmens és a felhasználói adatok. Az animáció azzal kezdődik, hogy a webszerver előkészíti a hiperszöveg jelölőnyelv (HTML) oldalt küldendő adatként. Az alkalmazásprotokoll HTTP-fejléce a HTML-adatok elejére kerül (előléírva). A fejléc különféle információkat tartalmaz, beleértve a kiszolgáló által használt HTTP-verziót és egy állapotkódot, amely jelzi, hogy a webkliens számára információkat tartalmaz. A HTTP-alkalmazási réteg protokoll a HTML-formátumú weboldaladatokat a TCP-átviteli rétegnek szállítja. A szállítási réteg protokoll további információkat fűz a HTTP adatokhoz a webszerver és a webkliens közötti információcsere kezeléséhez. Az IP-információ a TCP-információ elé kerül. Az IP hozzárendeli a megfelelő forrás és cél IP-címeket. Ezt az információt IP-csomagnak nevezik. Az Ethernet-protokoll az IP-csomag elé fűzi és a végéhez ad hozzá (hozzáfűzi) az adatokat, hogy adatkapcsolati keretet hozzon létre. A keret ezután bináris bitek láncává alakul, amelyeket a hálózati úton továbbítanak a webklienshez.

Web Server

Web Client

Data

TCP

IP

Ethernet

User Data

TCP Segment

IP Packet

Ethernet Frame

Data

TCP

IP

Protocol Encapsulation Terms

Ethernet



Kattintsunk a Lejátszás gombra a következő ábrán, ahol a kliens megkapja és kicsomagolja a weboldalt, hogy a böngészőben megjelenhessen!

Az animáció egy kis hálózatot mutat be szerverrel és klienssel. A kliens egy bináris bitsort kap a szervertől. A kliens veszi a bináris bitsort, és Ethernet keretté alakítja. A keret tartalmazza az Ethernet fejlécet, az IP-csomagot, a TCP-szegmenst és az adatokat. Az egyes protokollfejlécek feldolgozása, majd eltávolítása a hozzáadással ellentétes sorrendben történik. A rendszer feldolgozza és eltávolítja az Ethernet-információkat, majd az IP-protokoll-információkat, a TCP-információkat és végül a HTTP-információkat. A HTML weboldal információit ezután továbbítják az ügyfél webböngésző szoftveréhez.

Ethernet

IP

TCP

Data

User Data

TCP Segment

IP Packet

Ethernet Frame

Ethernet

IP

TCP

Data

3.3.6

## Tudáspróba - Protokollkészletek

Az űrlap teteje

A következő kérdésekre a LEGJOBB válasz kiválasztásával ellenőrizze, hogy megértette-e a protokollcsomagokat.

1. UDP and TCP belong to which layer of the TCP/IP protocol?

Az űrlap alja

Which two protocols belong in the TCP/IP model application layer?

Which protocol operates at the network access layer of the TCP/IP model?

Which of the following are protocols that provide feedback from the destination host to the source host regarding errors in packet delivery? (Choose two.)

A device receives a data link frame with data and processes and removes the Ethernet information. What information would be the next to be processed by the receiving device?

Which services are provided by the internet layer of the TCP/IP protocol suite? (Choose three.)

[3.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Protokollok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Szabványügyi szervezetek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                      
*                           

1. Protokollok és modelle
2. Szabványügyi szervezetek

# Szabványügyi szervezetek

3.4.1

## Nyílt szabványok

Aki új gumiabroncsokat vásárol egy autóhoz, sok gyártó közül választhat. Mindegyiknek legalább egy gumiabroncsa biztos lesz, amely jó az autóhoz. Ez azért van, mert az autóipar szabványokat alkalmaz az autógyártás során. Ugyanez van a protokollok esetében is. Mivel számos gyártó készít hálózati berendezéseket, fontos, hogy ugyanazokat a szabványokat használják. A hálózati szabványokat nemzetközi szabványügyi szervezetek fejlesztik ki.

A nyílt szabványok elősegítik az együttműködést, a versenyt és az innovációt. Azt is garantálják, hogy egyetlen cég ne sajátíthassa ki a piacot, vagy szerezhessen tisztességtelen előnyt a versenyben.

Jó példa erre, amikor otthoni vezeték nélküli routert vásárolunk. Számos különböző gyártó termékei közül választhatunk, amelyek mindegyike megvalósítja ugyanazokat a szabványos protokollokat, mint az IPv4, IPv6, DHCP, SLAAC, Ethernet vagy a 802.11-es vezeték nélküli LAN. A nyílt szabványok teszik lehetővé azt is, hogy egy Apple OS X operációs rendszert futtató kliens egy Linuxot futtató webszervertől kérjen le egy weboldalt. Ez azért lehetséges, mert mindkét operációs rendszer ugyanazokat a nyílt protokollokat valósítja meg, a TCP/IP protokollcsalád elemeit.

A szabványügyi szervezetek általában gyártófüggetlen, non-profit szervezetekként jönnek létre, hogy fejlesszék és támogassák a nyílt szabványok koncepcióját. Ezek a szervezetek fontosak a internet nyitottságának fenntartásában, szabadon hozzáférhető előírásokat és protokollokat készítenek, amelyeket minden gyártó alkalmazhat.

Egy szabványügyi szervezet magától is kidolgozhat egy szabályrendszert, vagy bizonyos esetekben kiválaszthat egy zárt protokollt is, ami majd az alapját képezheti a szabványnak. Ha egy gyártóspecifikus protokollt használ, ez általában annak a gyártónak a bevonásával történik, aki a protokollt megalkotta.

Az ábra szabványszervezetek logóit mutatja meg.

szabványügyi szervezetek logói, köztük az IEEE, IETF, IANA, ICANN, ITU és TIA



3.4.2

## Internetes szabványok

A különböző szervezeteknek különböző felelőssége van az internet és a TCP/IP protokoll szabványainak előmozdítása és létrehozása terén.

Az ábrán az internet fejlesztésében és támogatásában részt vevő szabványszervezetek láthatók.

The figure shows standards organizations involved with the development and support of the internet. At the top of the figure is the Internet Society (ISOC) logo. A line underneath connects to the Internet Architecture Board (IAB) logo. Underneath and to the left is the Internet Engineering Task Force (IETF) and to the right is the Internet Research Task Force (IRTF). Below the IETF is the Internet Engineering Steering Group (IESG) and below that are working group #1 and working group #2. Below the IRTF is the Internet Research Steering Group (IRSG) and below that are research group #1 and research group #2. Text at the bottom reads: Internet Society (ISOC) - Responsible for promoting the open development and evolution of internet use throughout the world. Internet Architecture Board (IAB) - Responsible for the overall management and development of internet standards. Internet Engineering Task Force (IETF) - Develops, updates, and maintains internet and TCP/IP technologies. This includes the process and documents for developing new protocols and updating existing protocols, which are known as Request for Comments (RFC) documents. Internet Research Task Force (IRTF) - Focused on long-term research related to internet and TCP/IP protocols such as Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), and Peer-to-Peer Research Group (P2PRG).



Internet Society (ISOC) Internet Architecture Board (IAB) Internet Engineering   
Task Force (IETF) Internet Engineering Steering Group (IESG) Internet Research   
Munkacsoport (IRTF) Internet Research Steering Group (IRSG) dolgozik   
1. csoport dolgozik   
2. csoport kutatás   
1. csoport kutatás   
2. csoport

* **Internet Society (ISOC)** – Felelős az internethasználat nyílt fejlődésének és fejlődésének előmozdításáért világszerte.
* **Internet Architecture Board (IAB)** – Az internetes szabványok átfogó kezeléséért és fejlesztéséért felelős.
* **Internet Engineering Task Force (IETF)** \- Internetes és TCP/IP technológiák fejlesztése, frissítése és karbantartása. Ez magában foglalja az új protokollok fejlesztésének és a meglévő protokollok frissítésének folyamatát és dokumentumait, amelyeket megjegyzéskérés (RFC) dokumentumként ismerünk.
* **Internet Research Task Force (IRTF)** \- Az internetes és TCP/IP-protokollokkal kapcsolatos hosszú távú kutatásra összpontosít, mint például az Anti-Spam Research Group (ASRG), a Crypto Forum Research Group (CFRG) és a Peer-to-Peer Research Group (P2PRG).

A következő ábra a TCP/IP fejlesztésével és támogatásával foglalkozó szabványszervezeteket mutatja be, mint az IANA és az ICANN.

Az ábra a TCP/IP fejlesztésében és támogatásában részt vevő szabványügyi szervezeteket mutatja be. A képen az ICANN látható a jobb oldalon, az IANA-ra mutató nyíllal. Az IANA alatt három nyíl látható az IP-címekhez, tartománynevekhez és TCP/UDP portszámokhoz. Alul a következő szöveg olvasható: Internet Corporation for Assigned Names and Numbers (ICANN) – Az egyesült államokbeli székhelyű ICANN koordinálja az IP-címek kiosztását, a domain nevek kezelését és a TCP/IP protokollokban használt egyéb információk hozzárendelését. Internet Assigned Numbers Authority (IANA) – Az ICANN IP-címek kiosztásának, tartománynév-kezelésének és protokollazonosítóinak felügyeletéért és kezeléséért felelős.

IANA ICANN Domain nevek TCP/UDP portszámok IP-címek

* **Internet Corporation for Assigned Names and Numbers (ICANN)** \- Az egyesült államokbeli székhelyű ICANN koordinálja az IP-címek kiosztását, a tartománynevek kezelését és a TCP/IP protokollokban használt egyéb információk hozzárendelését.
* **Internet Assigned Numbers Authority (IANA)** \- Felelős az ICANN IP-címek kiosztásának, tartománynév-kezelésének és protokollazonosítóinak felügyeletéért és kezeléséért.

3.4.3

## Elektronikai és kommunikációs szabványok

Más szabványügyi szervezetek az IP-csomagok vezetékes vagy vezeték nélküli közegen, elektromos jelként történő szállításához használt elektronikus és kommunikációs szabványok terjesztéséért és létrehozásáért felelnek.

Ezek a szervezetek a következők:

* **Institute of Electrical and Electronics Engineers** ( **IEEE** ) - Elektronikai, elektrotechnikai szervezet, technológiai újításokat és új szabványokat dolgoznak ki nagyon széles körben az energiaellátástól, az egészségügyön át, a telekommunikációig és a hálózatokig. Fontos IEEE hálózati szabvány a 802.3 Ethernet és a 802.11 WLAN. Keressünk rá az interneten más IEEE hálózati szabványokra!
* **Electronic Industries Alliance (EIA)** \- A szervezet legismertebb szabványai a vezetékezéshez, csatlakozókhoz és a hálózati eszközök beszereléséhez használt 19 colos szekrényekhez kapcsolódnak.
* **Telecommunications Industry Association (TIA)** \- Kommunikációs szabványokat fejlesztenek számos területen: rádióátvitel, mobil adótornyok, VoIP eszközök, műholdas kommunikáció, stb. The figure shows an example of a certified Ethernet cable which was developed cooperatively by the TIA and the EIA.
* **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T** ) - Az egyik legnagyobb és legrégebbi kommunikációs szabványügyi szervezet. Az ITU-T olyan területek számára ír elő szabványokat, mint a videótömörítés, az IPTV (Internet Protocol Television) és a szélessávú kommunikáció (pl.: DSL).

3.4.4

## Laborgyakorlat - Hálózati szabványok keresése

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: Hálózati szabványügyi szervezetek keresése.
  2. rész: Internetes és számítógéphálózati tapasztalatunk felmérése.

3.4.5

## Tudáspróba - Szabványügyi szervezetek

Az űrlap teteje

Ellenőrizze, hogy megértette-e a szabványügyi szervezeteket, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Igaz vagy hamis. A szabványügyi szervezetek általában szállítósemlegesek.

Az űrlap alja

This standards organization is concerned with the Request for Comments (RFC) documents that specify new protocols and update existing ones.

This standards organization is responsible for IP address allocation and domain name management.

What types of standards are developed by the Electronics Industries Alliance (EIA)?

[3.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Protokollkészletek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Referenciamodellek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Bevezetés a hálózatokba

v 7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                  
*                           

1. Protokollok és modelle
2. Referenciamodellek

# Referenciamodellek

3.5.1

## A rétegmodellek előnyei

Nem tudjuk a valóságban megnézni, ahogy a csomagok igazi hálózaton keresztül utaznak ugyanúgy, ahogy egy autót a futószalag mellett összeraknak. Segít azonban, ha van egy olyan gondolatmenet, amellyel el tudjuk képzelni, hogy mi történik éppen. Modellre van szükségünk.

Az olyan összetett folyamatokat, mint egy hálózat működése nehéz megmagyarázni és megérteni. A hálózat egyes műveleteit lebontjuk és kezelhetőbb rétegekbe rendezzük, ez lesz a rétegmodell.

A rétegmodellnek számos előnye van a hálózati protokollok és műveletek leírása során:

* Segít a protokollok tervezésében, mert egy adott rétegben működő protokoll esetén egyértelműen meghatározza, hogy mit kell tennie, és hogyan kapcsolódik az alatta és felette lévő rétegekhez.
* Elősegíti a versenyt, mert a különböző gyártóktól származó termékek képesek lesznek együttműködni.
* Megakadályozza, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta és felette levő rétegekre.
* Közös nyelvet biztosít a hálózat működésének és képességeinek leírásához.

Ahogy az ábrán is látható, két rétegmodellt használunk a hálózati műveletek leírására:

* Open System Interconnection (OSI) referenciamodell
* TCP/IP referenciamodell

A kép tetején két WAN-on keresztül összekapcsolt LAN látható, a következő szöveggel: A hálózati modell csak egy hálózati művelet ábrázolása. A modell nem a tényleges hálózat. Alatta az OSI és a TCP/IP modellrétegek és protokollok találhatók. Az OSI modell hét rétege felülről lefelé és a hozzájuk tartozó protokollok a következők: alkalmazás, prezentáció, munkamenet (a felső három réteg protokolljai a HTTP, DNS, DHCP és FTP), szállítás (TCP és UDP), hálózat (IPv4). , IPv6, ICMPv4 és ICMPv6), adatkapcsolati és fizikai (az alsó két réteg protokolljai: Ethernet, WLAN, SONET és SDH). A TCP/IP modell négy rétege felülről lefelé és a hozzájuk tartozó protokollok a következők: alkalmazás (HTTP, DNS, DHCP és FTP), szállítás (TCP és UDP), Internet (IPv4, IPv6, ICMPv4 és ICMPv6), és hálózati hozzáférés (Ethernet, WLAN, SONET és SDH).



HTTP, DNS, DHCP, FTP TCP, UDP IPv4, IPv6,   
ICMPv4, ICMPv6 Ethernet, WLAN, SONET, SDH TCP/IP Protocol Suite A hálózati modell csak egy hálózati műveletet ábrázol. A modell nem a tényleges hálózat. Alkalmazásszállítás adatkapcsolat Internet hálózati hozzáférés TCP/IP-modell bemutatása Munkamenet szállítási hálózat Alkalmazás fizikai OSI -modell

3.5.2

## Az OSI-referenciamodell

Az OSI-modell részletes listát ad valamennyi réteg funkcióiról és szolgáltatásairól. Ez a modell az egységességet biztosítja hálózati protokollok és szolgáltatások valamennyi típusán belül azzal, hogy leírja, mit kell tenni egy bizonyos rétegben, de nem írja elő, hogy miként kell azt megvalósítani.

Leírja továbbá a rétegek kölcsönhatását a közvetlenül alattuk és felettük lévő rétegekkel. Az ebben a tanfolyamban tárgyalt TCP/IP protokollok mind az OSI, mind a TCP/IP modellek köré szerveződnek. A táblázat az OSI-modell egyes rétegeit írja le. Az egyes rétegek funkcionalitása és a rétegek közötti kapcsolat nyilvánvalóbbá válik majd a kurzus során, ahogy a protokollokat részletesebben tárgyaljuk.

| 7. OSI-modell rétegleírás – Alkalmazás Az alkalmazási réteg a folyamatok közötti kommunikációhoz használt protokollokat tartalmazza. 6 - Prezentáció A megjelenítési réteg biztosítja az alkalmazási réteg szolgáltatásai között átvitt adatok közös megjelenítését. 5 - SessionA munkamenet réteg szolgáltatásokat nyújt a prezentációs réteg számára a párbeszéd megszervezéséhez és az adatcsere kezeléséhez. 4 – Szállítás A szállítási réteg szolgáltatásokat határoz meg az adatok szegmentálására, átvitelére és újraösszeállítására a végeszközök közötti egyéni kommunikációhoz. 3 - Hálózat A hálózati réteg szolgáltatásokat nyújt az egyes adatok hálózaton keresztüli cseréjéhez az azonosított végeszközök között. 2 - Adatkapcsolat Az adatkapcsolati réteg protokollok az eszközök közötti adatkeretek közös adathordozón keresztüli cseréjének módszereit írják le. 1 - Fizikai A fizikai réteg protokolljai a fizikai kapcsolatok aktiválásának, karbantartásának és deaktiválásának mechanikai, elektromos, funkcionális és eljárási eszközeit írják le. bitátvitelhez hálózati eszközre és onnan. | |
| --- | --- |
| **OSI-modell réteg** | **Leírás** |
| **7 - Alkalmazási** | Az alkalmazási réteg folyamat-folyamat közti kommunikációhoz használt protokollokat tartalmaz. |
| **6 - Megjelenítési** | A megjelenítési réteg az alkalmazási rétegbeli szolgáltatások közt átvitt adatok közös ábrázolását valósítja meg. |
| **5 - Viszony** | A viszony réteg a megjelenítési réteg számára biztosít szolgáltatásokat párbeszédek megvalósításához és adatok cseréjéhez. |
| **4 - Szállítási** | A szállítási réteg a végberendezések közti kommunikáció adatainak szegmentálását, szállítását és összeillesztésével kapcsolatos szolgáltatásokat nyújt. |
| **3 - Hálózati** | A hálózati réteg végberendezések közti egyedi adatelemek cseréjét megvalósító szolgáltatásokat biztosít. |
| **2 - Adatkapcsolati** | Az adatkapcsolati réteg protokolljai adatkeretek továbbítását végzik egy közös közegen elhelyezkedő eszközök között. |
| **1 - Fizikai** | A fizikai rétegbeli protokollok mechanikai, elektromos, funkcionális és folyamatbeli módszerekkel foglalkoznak, melyek hálózati eszközről induló vagy oda megérkező bitsorozatokat továbbító fizikai kapcsolatok aktiválását, karbantartását és deaktiválását végzik. |

**MEGJEGYZÉS:** A TCP/IP modell rétegeire főleg a nevükkel hivatkozunk, az OSI-modell hét rétegét gyakrabban emlegetjük a számuk alapján. Például a fizikai réteget az OSI-modell első rétegének, az adatkapcsolatit a második rétegnek hívjuk, és így tovább.

3.5.3

## TCP/IP protokollmodell

A TCP/IP protokollmodellt a hálózatközi kommunikációhoz hozták létre a 1970-es években, néha internetmodellnek is nevezik. Ez a modell szorosan illeszkedik egy bizonyos protokollkészlet szerkezetéhez. A TCP/IP azért protokollmodell, mivel a TCP/IP protokollkészletben lévő protokollok valamennyi rétegének funkcióit leírja. A TCP/IP referenciamodellként is használható. A táblázat az OSI-modell egyes rétegeit írja le.

| TCP/IP-modell rétegleírás 4 – Alkalmazás Adatokat jelenít meg a felhasználó számára, valamint kódolást és párbeszédvezérlést.3 – Szállítás Támogatja a kommunikációt a különböző eszközök között, különböző hálózatokon keresztül. 2 - Internet Meghatározza a legjobb útvonalat a hálózaton keresztül.1 - Hálózati hozzáférés A hálózatot alkotó hardvereszközöket és adathordozókat vezérli. | |
| --- | --- |
| **TCP/IP modell réteg** | **Leírás** |
| **4 - Alkalmazási** | Adatok megjelenítése a felhasználónak, ezen kívül kódolás és párbeszédek vezérlése. |
| **3 - Szállítási** | Különböző eszközök közötti kommunikáció különböző hálózatokon keresztül. |
| **2 - Internet** | Meghatározza a hálózaton keresztül a legjobb elérési utat. |
| **1 - Hálózatelérési** | A hálózatot alkotó hardvereszközök és közegek. |

A szabvány és a TCP/IP protokollok definícióját egy nyilvános fórum tárgyalja, és nyilvánosan elérhető RFC-kben vannak meghatározva. Az RFC-ket a hálózatépítő mérnökök alkotják, és megküldik más IETF-tagoknak észrevételek céljából.

3.5.4

## Az OSI és a TCP/IP modell összehasonlítása

A TCP/IP protokollkészlet protokolljai leírhatók az OSI-referenciamodellből kiindulva is. Az OSI-modellben a TCP/IP modell hálózatelérési és alkalmazási rétege további részekre van felosztva, hogy leírják a rétegekben előforduló különálló funkciókat.

A hálózatelérési rétegben a TCP/IP protokollkészlet nem határozza meg, hogy mely protokollokat kell használni egy fizikai közegen való továbbításkor, hanem csak azok átadását írja le az internet rétegből a fizikai hálózati protokollok felé. Az OSI 1. és 2. rétege tárgyalja a közeghozzáféréshez szükséges eljárásokat és a hálózaton keresztül történő adattovábbítás fizikai eszközeit.

Az ábra az OSI és a TCP/IP modellrétegek összehasonlítása. Az OSI modell a bal oldalon látható. Felülről lefelé a következő rétegszámok és -nevek láthatók: 7) Alkalmazás, 6) Prezentáció, 5) Munkamenet, 4) Közlekedés, 3) Hálózat, 2) Adatkapcsolat és 1) Fizikai. A TCP/IP modell a jobb oldalon látható. Felülről lefelé a rétegnevek és a kapcsolódó OSI modell rétegszámok a következők: Alkalmazás (OSI Layers 7, 6 és 5), Transport (OSI Layer 4), Internet (OSI Layer 3) és Network Access (OSI Layers 2 és 1). Alul a következő szöveg olvasható: A legfontosabb hasonlóságok a szállítási és hálózati rétegben vannak; azonban a két modell különbözik az egyes rétegek feletti és alatti rétegekhez való viszonyulásában: az OSI Layer 3, a hálózati réteg közvetlenül a TCP/IP internetes réteghez van leképezve. Ez a réteg olyan protokollok leírására szolgál, amelyek az üzeneteket egy hálózaton keresztül címzik és továbbítják. Az OSI Layer 4, a szállítási réteg közvetlenül a TCP/IP szállítási réteghez van leképezve. Ez a réteg olyan általános szolgáltatásokat és funkciókat ír le, amelyek rendezett és megbízható adattovábbítást biztosítanak a forrás- és célállomások között. A TCP/IP alkalmazási réteg számos protokollt tartalmaz, amelyek specifikus funkciókat biztosítanak számos végfelhasználói alkalmazás számára. Az OSI modell 5., 6. és 7. rétegét referenciaként használják az alkalmazásszoftver-fejlesztők és -szállítók számára a hálózatokon működő alkalmazások előállításához. Mind a TCP/IP, mind az OSI modellt gyakran használják, amikor különböző rétegeken lévő protokollokra hivatkoznak. Mivel az OSI-modell elválasztja az adatkapcsolati réteget a fizikai rétegtől, általában ezt használják, amikor ezekre az alsóbb rétegekre hivatkoznak.

7 6 5 4 3 2

1

OSI-modell alkalmazás bemutatása munkamenet átviteli hálózat adatkapcsolat fizikai TCP/IP modell alkalmazás szállítása internetes hálózati hozzáférés

A legfontosabb hasonlóságok a szállítási és hálózati rétegekben vannak, azonban a két modell különbözik abban, hogy miként viszonyulnak a felsőbb és alsóbb rétegekhez:

* Az OSI 3. rétege, a hálózati réteg megfelel a TCP/IP internet rétegének. Ez a réteg olyan protokollokat ír le, amelyek címzéssel és az üzenetek hálózatok közti irányításával foglalkoznak.
* Az OSI 4. rétege, a szállítási megfelel a TCP/IP szállítási rétegének. Ez a réteg általános szolgáltatásokat és funkciókat tartalmaz, amelyek sorrendhelyes és megbízható átvitelt tesznek lehetővé az adatforrástól a címzettig.
* A TCP/IP alkalmazási rétege számos protokollt tartalmaz, ezek a felhasználói alkalmazások számos fajtájának nyújtanak specifikus szolgáltatásokat. Az OSI-modell 5., 6. és 7. rétegei az alkalmazások fejlesztőinek biztosítanak referenciát a hálózatokon kommunikáló alkalmazások tervezése során.
* A TCP/IP és az OSI-modellt egyaránt gyakran használjuk, amikor bizonyos rétegek protokolljaira szeretnénk hivatkozni. Mivel az OSI-modell elkülöníti az adatkapcsolati réteget a fizikaitól, ha ezekre a rétegekre szeretnénk hivatkozni, akkor általában ezt a modellt használjuk.

3.5.5

## Packet Tracer - A TCP/IP és az OSI-modell vizsgálata működés közben

Ennek a szimulációs feladatnak a célja, hogy alapot nyújtson a TCP/IP protokollkészlet és az OSI-modell kapcsolatának megértéséhez. A szimulációs mód lehetővé teszi, hogy megnézzük az adatok tartalmát minden rétegben a hálózaton való továbbítás közben.

Ahogy az adatok áthaladnak a hálózaton, kisebb darabokra bontják szét őket és megjelölik, hogy a darabokat újra egyesíteni lehessen, amikor megérkeznek a rendeltetési helyre. Minden darabnak saját neve van, és a TCP/IP és az OSI-modell valamelyik rétegéhez kötődik. Ezt a nevet protokoll adategységnek (protocol data unit, PDU) nevezik. A Packet Tracer szimulációs módja lehetővé teszi, hogy megtekintsük az egyes rétegeket és a kapcsolódó PDU-kat. A következő lépések végigvezetik a felhasználót azon a folyamaton, ahogy lekérünk egy weboldalt egy webszerverről a kliens PC-n levő webböngésző segítségével.

Annak ellenére, hogy sok megjelenített információról csak később lesz szó részletesebben, kihasználhatjuk ezt a lehetőséget a Packet Tracer funkcióinak megvizsgálására és a beágyazási folyamat szemléltetésére.

[A TCP-IP és az OSI-modell vizsgálata működés közben](https://contenthub.netacad.com/courses/itn/_common/3.5.5-packet-tracer---investigate-the-tcp-ip-and-osi-models-in-action_hu-HU.pka)

[3.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Szabványügyi szervezetek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adatbeágyazás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                          
*                           

1. Protokollok és modelle
2. Adatbeágyazás

# Adatbeágyazás

3.6.1

## Üzenetek szegmentálása

Az OSI-referenciamodell és a TCP/IP protokollmodell ismerete hasznos lesz, amikor az adatok beágyazásáról és a hálózaton való mozgásáról tanulunk. Ez nem olyan egyszerű, mint egy hagyományos levelet feladni a postán.

Elméletileg egy átlagos kommunikáció adatait, mint egy videó vagy egy e-mail sok nagy csatolmánnyal a forrástól a célig egyetlen megszakítatlan bitfolyam formájában is átvihetnénk. Ez azonban problémákat okozna más eszközök számára, amelyek ugyanazokat a kommunikációs csatornákat vagy összeköttetéseket használnák. Ez a nagy adatfolyamok továbbításakor jelentős késleltetéseket okozna. Továbbá, ha ebben az összefonódott hálózati infrastruktúrában megszakadna akár egyetlen kapcsolat is, akkor a teljes üzenet elveszne, vagyis az egészet újra kellene küldeni.

Jobb megoldás, ha az adatokat kisebb, könnyebben kezelhető részekre osztjuk, és így küldjük el a hálózaton keresztül. A szegmentálás az adatfolyam kisebb egységekre történő felosztása a hálózaton keresztüli átvitelhez. A szegmentálásra azért van szükség, mert az adathálózatok a TCP/IP protokollkészletet használják, ami külön IP-csomagokban továbbítja az adatokat. Minden csomagot külön küldenek el, mintha egy hosszú levelet külön képeslapok sorozataként adnánk fel. Az ugyanazon célállomás felé haladó szegmensek lehet, hogy különböző útvonalakat járnak be.

Ezzel eljutottunk a szegmentálás két legfontosabb előnyéhez:

* **Növeli a sebességet** - Mivel a nagy adatfolyam csomagokra van bontva, nagy mennyiségű adat küldhető a hálózaton keresztül egyetlen kommunikációs kapcsolat lefoglalása nélkül. Több párbeszéd haladhat át összefésülve ugyanazon a hálózaton, amit multiplexelésnek is nevezünk.
* **Növeli a hatékonyságot** - Ha egy szegmens nem éri el a célállomást a hálózat meghibásodása vagy hálózati torlódás miatt, csak ezt a szegmenset kell újraküldeni a teljes adatfolyam helyett.

Kattintsunk a gombokra a szegmentálást és a multiplexelést bemutató animációk megtekintéséhez!

The animation shows a small LAN with two hosts and a server. When the Segmentation button is pressed a large message from the first host is broken up into smaller messages that are sent arcross the network to the server. Then the Multiplexing button is pressed messages from both hosts are sent onto the network one after the other to the server.

Segmentation

Multiplexing

3.6.2

## Sorrendhelyes kézbesítés

A hálózati adattovábbítás során használt szegmentálás és multiplexelés hátránya, hogy növeli a folyamat összetettségét. Képzeljük el, hogy egy 100 oldalas levelet kell feladnunk, de minden borítékba csak egy lap fér. 100 borítékra lenne szükség, és minden borítékot külön meg kellene címezni. Lehet, hogy a 100 oldalas levél 100 borítékja nem a megfelelő sorrendben érkezik meg. Következésképpen a borítékban szereplő információknak tartalmazniuk kell egy sorszámot ahhoz, hogy a címzett a megfelelő sorrendben össze tudja állítani az oldalakat.

A hálózati kommunikáció minden egyes üzenetszegmensének egy hasonló folyamaton kell keresztülmennie ahhoz, hogy biztosítva legyen a megfelelő célállomáshoz történő eljutása és az eredeti üzenet tartalmának a visszaállítása, ezt látható az ábrán is. A TCP felel az egyes szegmensek sorszámozásáért.

The figure shows two computers sending messages on a network to a server. Each message has been divided up into multiple pieces shown as yellow and orange envelopes, some are interleaved and numbered. Text reads: Multiple pieces are labeled for easy direction and re-assembly. Labeling provides for ordering and assembling the pieces when they arrive.

3 2 1 3 2

1



Labeling provides for ordering and assembling the pieces when they arrive.Multiple pieces are labeled for easy direction and   
re-assembly.

3.6.3

## Protokoll adategységek

Ahogy az alkalmazás adatai haladnak lefelé a protokollveremben, a különböző protokollok minden szinten további adatokkal egészítik ki. Ezt a folyamatot hívjuk beágyazásnak.

**MEGJEGYZÉS:** Bár az UDP-protokoll adategységét nevezzük datagramnak, néha az IP-csomagokra is az IP-datagram kifejezést használjuk.

Az egyes rétegekhez tartozó adatok formáját protokoll adategységnek nevezzük (Protocol Data Unit, PDU). Az adatbeágyazás során minden újabb réteg becsomagolja a felsőbb rétegből származó PDU-t az alkalmazott protokollnak megfelelő módon. A folyamat minden egyes szakaszában a PDU új nevet kap, jelezve ezáltal az új funkcióját is. Bár nincs általános érvényű elnevezés a PDU-kra, ebben a kurzusban a PDU-kat a TCP/IP protokollcsaládnak megfelelően nevezzük meg. Az egyes adattípusokhoz tartozó PDU-k az ábrán láthatók.

The figure shows the protocol data units (PDUs) at various layers of the OSI model. At the top of the image is a person sitting at a computer workstation sending email data. That data is passed down the stack and encapsulated into a new PDU at each layer. At the top, the email data is divided into smaller chunks of data. Below that, a transport header is added in front of the chunk of data and it becomes a segment. Below that, a network header is added in front of the transport header and it becomes a packet. Below that, a frame header is added in front of the network header and a frame trailer is added behind the data and it becomes a frame (medium dependent). The frame is shown as a stream of bits prior to being received by a router which is connected to the cloud. Text at the bottom reads: Data - The general term for the PDU used at the application layer; Segment - Transport layer PDU; Packet - Network layer PDU; Frame - Data Link layer PDU; Bits - Physical layer PDU used when physically transmitting data over the medium. Note: If the Transport header is TCP, then it is a segment. If the Transport header is UDP then it is a datagram.

1100010101000101100101001010101001

Email DataDataDataDataDataNetwork headerDataFrame headerNetwork headerDataFrame   
trailerDataSegmentPacketFrame  
(medium dependent)BitsPassing down the stack.Transport headerTransport headerTransport header

* Adat - Az alkalmazási réteg PDU-jának általános neve
* Szegmens - A szállítási réteg PDU-ja
* Csomag - A hálózati réteg PDU-ja
* Keret - Az adatkapcsolati réteg PDU-ja
* Bitek - Az átviteli közegen történő fizikai adattovábbításhoz használt PDU

**MEGJEGYZÉS:** Ha a szállítási réteg fejléce TCP, akkor szegmensnek nevezzük. Ha a szállítási protokoll UDP, akkor datagramnak.

3.6.4

## Példa beágyazásra

Amikor üzenetet küldünk a hálózaton, a beágyazási folyamat felülről lefelé történik. Minden egyes rétegben a felsőbb réteg információira a beágyazást végző protokoll adatként tekint. A TCP-szegmens például az IP-csomagon belül adatnak számít.

Már láttuk ezt az animációt korábban. Kattintsunk a Lejátszás gombra, és ezúttal a beágyazási folyamatot figyeljük, amelyben a webszerver a kliensnek egy weboldal adatait küldi el!

The animation shows a small network with a Web Server and a Web Client. Theres is a graphic that shows the components that make up a message. An Ethernet Frame, and IP Packet, a TCP segment, and the user data. The animation begins with the web server preparing the Hypertext Markup Language (HTML) page as data to be sent. The application protocol HTTP header is added (prepended) to the front of the HTML data. The header contains various information, including the HTTP version the server is using and a status code indicating it has information for the web client. The HTTP application layer protocol delivers the HTML-formatted web page data to the TCP transport layer. The transport layer protocol prepends additional information to the HTTP data to manage the exchange of information between the web server and web client. The IP information is prepended to the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet. The Ethernet protocol prepends and adds to the end (appends) information to the IP packet to create a data link frame. The frame is then converted into a string of binary bits that are sent along the network path to the web client.

Web Server

Web Client

Data

TCP

IP

Ethernet

User Data

TCP Segment

IP Packet

Ethernet Frame

Data

TCP

IP

Protocol Encapsulation Terms

Ethernet



3.6.5

## Példa a kicsomagolásra

A fogadó oldal fordított irányú folyamatát kicsomagolásnak nevezzük. A kicsomagolási folyamat során a fogadó fél eltávolít egy vagy több protokollfejlécet. Az adatot kicsomagolják, ahogy halad felfelé a protokollkészleten a végfelhasználói alkalmazás irányába.

Már láttuk ezt az animációt korábban. Ezúttal kattintsunk a Lejátszás gombra, és figyeljük a kicsomagolási folyamatot!

The animation shows a small network with a Server and a Client. The client receives a string of binary bits from the server. The client takes the binary string of bits and converts it into an Ethernet frame. The Frame contains the Ethernet header, the IP packet, the TCP segment, and the data. Each protocol header is processed and then removed in the opposite order it was added. The Ethernet information is processed and removed, followed by the IP protocol information, the TCP information, and finally the HTTP information. The HTML web page information is then passed on to the web browser software of the client.

Ethernet

IP

TCP

Data

User Data

TCP Segment

IP Packet

Ethernet Frame

Ethernet

IP

TCP

Data

3.6.6

## Tudáspróba - Adatbeágyazás

Az űrlap teteje

Check your understanding of data encapsulation by choosing the BEST answer to the following questions.

1. What is the process of dividing a large data stream into smaller pieces prior to transmission?

Az űrlap alja

What is the PDU associated with the transport layer?

Which protocol stack layer encapsulates data into frames?

What is the name of the process of adding protocol information to data as it moves down the protocol stack?

[3.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Referenciamodellek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adathozzáférés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                   
*                           

1. Protokollok és modelle
2. Adathozzáférés

# Adathozzáférés

3.7.1

## Címek

Már megtanultuk, hogy az üzeneteket darabolni kell a hálózaton történő továbbításhoz. De ezek a szegmentált üzenetek nem mennek sehova, ha nem címezzük meg őket helyesen. Ez a témakör áttekintést ad a hálózati címekről. Lehetőséget kapunk a Wireshark eszköz használatára is, amely segít a hálózati forgalom szemléltetésében.

A hálózati és az adatkapcsolati réteg feladata az adatok eljuttatása a forrástól a célig. Mindkét réteg protokolljai használnak forrás- és célcímeket, de a címek feladata különböző:

* **Hálózati rétegbeli forrás- és célcímek** - Eljuttatják az IP-csomagokat az eredeti forrástól a végső célig, amely lehet ugyanazon, de akár egy távoli hálózaton is.
* **Adatkapcsolati réteg forrás- és célcímei** - Eljuttatják az adatkapcsolati keretet ugyanazon hálózat egyik hálózati kártyájától a másikig.

The figure shows the addressing and labeling used at various layers of the OSI model for delivering data. Starting from left to right, it shows: the physical layer provides timing and synchronization bits; the data link layer provides destination and source physical addresses; the network layer provides destination and source logical network addresses; the transport layer provides destination and source process number (ports); and the upper layers provide encoded application data.

PhysicalData LinkNetworkTransportUpper LayersTiming and synchronization bitsDestination and source physical addressesDestination and source logical network addressesDestination and source process number (ports)Encoded application data

3.7.2

## Harmadik rétegbeli logikai cím

Az IP-cím a hálózati vagy harmadik rétegbeli logikai cím, amely segítségével az IP-csomagot a küldőtől a címzettig továbbíthatjuk, az ábrán látható módon.

The figure shows a layer 3 IP packet moving from the original source to the final destination. The original source is PC1, shown on the left, with IP address 192.168.1.110. The final destination is a web server, shown on the far right, with IP address 172.16.1.99. An IP packet is shown leaving PC1 heading to router R1. The IP packet is then shown leaving router R1 and heading to router R2. The IP packet is then shown leaving R2 and heading towards the web server. Below the network topology is a diagram of a layer 3 IP packet header showing 192.168.1.110 as the source and 172.16.1.99 as the destination.

R1

R2

Web Server   
172.16.1.99Source IP   
192.168.1.110Destination IP   
172.16.1.99...PC1   
192.168.1.110IP PacketFinal DestinationLayer 3 IP PacketIP PacketIP PacketOriginal Source

Az IP-csomagban két IP-cím található:

* **Forrás IP-cím**- A küldő eszköz IP-címe, ami a csomag eredeti forrása.
* **Cél IP-cím**- A fogadó vagy címzett eszköz IP-címe, ami a csomag végső rendeltetési helye.

Az IP-címek az eredeti forrást és a végső célt azonosítják. Ez akkor is igaz, ha a forrás és a cél ugyanazon az IP-hálózaton van, de akkor is, ha különböző hálózatban.

Az IP-címnek két része van:

* **Hálózati rész (IPv4) vagy előtag (IPv6)**- A cím bal szélső része, azt a hálózatot jelöli, amelynek az IP-cím tagja. Azonos hálózatban levő eszközök IP-címének az alhálózati része ugyanaz.
* **Állomásazonosító rész (IPv4) vagy interfészazonosító (IPv6)**- A cím fennmaradó része, a hálózat egy bizonyos eszközét azonosítja. Ez a rész a hálózaton belül egyedileg azonosít egy eszközt vagy interfészt.

**MEGJEGYZÉS:** Az alhálózati maszk (IPv4) vagy az előtag hossza (IPv6) segítségével különíthető el a cím hálózati és állomásazonosító része.

3.7.3

## Azonos hálózaton levő eszközök

A következő példában a PC1 kliens számítógép kommunikál az azonos IP-hálózaton levő FTP-szerverrel.

* **Forrás IPv4-cím** - A küldő számítógép, vagyis a PC1 kliens IPv4-címe: 192.168.1.110.
* **Cél IPv4-cím** - A fogadó vagy címzett, vagyis az FTP-szerver IPv4-címe: 192.168.1.9.

Figyeljük meg az ábrán, hogy a forrás IPv4-cím és a cél IPv4-cím hálózati része ugyanazon a hálózaton található. Figyeljük meg, hogy a forrás IPv4-cím hálózati része és a cél IPv4-cím hálózati része azonos, ezért a forrás és a cél ugyanazon a hálózaton található.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source to a destination on the same network. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP address 192.168.1.110 and MAC address AA-AA-AA-AA-AA-AA, an FTP server with IP address 192.168.1.9 and MAC address CC-CC-CC-CC-CC-CC, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. At the right is another switch connected to a server. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of CC-CC-CC-CC-CC-CC and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (host) and a destination of 192.168.1 (network) 9 (host). Lastly is the data.

PC1  
192.168.1.110  
AA-AA-AA-AA-AA-AAFTP Server  
192.168.1.9  
CC-CC-CC-CC-CC-CCData Link  
Ethernet Frame HeaderNetwork Layer  
IP Packet HeaderDestinationSourceSourceDestinationDataCC-CC-CC-CC-CC-CCAA-AA-AA-AA-AA-AANetwork  
192.168.1.Host  
110Network  
192.168.1.Host  
9

3.7.4

## Az adatkapcsolati réteg címeinek szerepe: azonos IP-alhálózat

Amikor az IP-csomagot küldő és fogadó állomások azonos hálózaton vannak, akkor az adatkapcsolati keret közvetlenül a fogadó eszköznek kerül elküldésre. Ethernet hálózaton az adatkapcsolati címet Ethernet MAC-címnek nevezzük (lásd az ábrát).

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source to a destination on the same network, highlighting the role of the MAC address. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP address 192.168.1.110 and MAC address AA-AA-AA-AA-AA-AA (shown highlighted), an FTP server with IP address 192.168.1.9 and MAC address CC-CC-CC-CC-CC-CC (shown highlighted), and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. At the right is another switch connected to a server. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of CC-CC-CC-CC-CC-CC and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (host) and a destination of 192.168.1 (network) 9 (host). Lastly is the data.

PC1  
192.168.1.110  
AA-AA-AA-AA-AA-AAFTP Server  
192.168.1.9  
CC-CC-CC-CC-CC-CCData Link  
Ethernet Frame HeaderNetwork Layer  
IP Packet HeaderDestinationSourceSourceDestinationDataCC-CC-CC-CC-CC-CCAA-AA-AA-AA-AA-AANetwork  
192.168.1.Host  
110Network  
192.168.1.Host  
9

A MAC-címeket az Ethernet hálózati kártya fizikailag tartalmazza.

* **Forrás MAC-cím** - A beágyazott IP-csomagot szállító adatkapcsolati keret forráseszközének adatkapcsolati vagy MAC-címe. A PC1 Ethernet hálózati kártyájának MAC-címe hexadecimális alakban AA-AA-AA-AA-AA-AA.
* **Cél MAC-cím** - Amikor a céleszköz azonos alhálózaton van a küldővel, ez a céleszköz adatkapcsolati címe. Ebben a példában a cél MAC-cím az FTP-szerver MAC-címe, hexadecimális alakban CC-CC-CC-CC-CC-CC.

A keretet a beágyazott IP-csomaggal a PC1 már közvetlenül továbbíthatja az FTP-szerver számára.

3.7.5

## Eszközök távoli hálózaton

De mi a szerepe a hálózati réteg címeinek és az adatkapcsolati réteg címeinek akkor, amikor egy eszköz egy távoli hálózaton levő eszközzel kommunikál? Ebben a példában a PC1 kliens számítógép a Web Server nevű webszerverrel kommunikál, ami egy másik IP-alhálózatban van.

3.7.6

## A hálózati réteg címeinek szerepe

Amennyiben a csomag küldője és címzettje két különböző hálózaton található, akkor a forrás és cél IP-címek is különböző hálózati tartományokból kerülnek ki. Ez a célállomás IP-címének hálózati részéből derül ki.

* **Forrás IPv4-cím** - A küldő számítógép, vagyis a PC1 kliens IPv4-címe: 192.168.1.110.
* **Cél IPv4-cím** - A címzett IPv4-címe, vagyis a Web Server nevű szerver IPv4-címe: 172.16.1.99.

Figyeljük meg az ábrán, hogy a forrás IPv4-cím és a cél IPv4-cím hálózati része különböző hálózatokon található.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source on one network to a destination on a different network. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP 192.168.1.110 and MAC AA-AA-AA-AA-AA-AA, a server, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. The router on the left is labeled R1 with IP 192.168.1.1 and MAC 11-11-11-11-11-11. The middle router is unlabeled. The router on the right is labeled R2 with IP 172.16.1.1 and MAC 22-22-22-22-22-22. At the right is another switch connected to a Web server with IP 172.16.1.99 and MAC AB-CD-EF-12-34-56. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of 11-11-11-11-11-11-11 and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (device) and a destination of 172.16.1 (network) 99 (device). Lastly is the data.

Data Link  
Ethernet Frame HeaderNetwork Layer  
IP Packet HeaderDestinationSourceSourceDestinationData11-11-11-11-11-11AA-AA-AA-AA-AA-AANetwork  
192.168.1.Device  
110Network  
172.16.1.Device  
99**PC1**  
192.168.1.110  
AA-AA-AA-AA-AA-AA**R1**  
192.168.1.1  
11-11-11-11-11-11**R2**  
172.16.1.1  
22-22-22-22-22-22**Web Server**  
172.16.1.99  
AB-CD-EF-12-34-56

3.7.7

## Az adatkapcsolati réteg címeinek szerepe: különböző IP-alhálózat

Amikor az IP-csomag küldője és a címzettje nem ugyanabban a hálózatban található, akkor az adatkapcsolati rétegbeli Ethernet keretet nem lehet közvetlenül a célállomásnak küldeni, mert az a küldő hálózatán közvetlenül nem elérhető. Az Ethernet keretet egy másik készüléknek, a routernek vagy alapértelmezett átjárónak kell elküldeni. A példánkban az R1 az alapértelmezett átjáró. Az R1 Ethernet adatkapcsolati címmel rendelkezik, és ugyanazon a hálózaton található, mint a PC1. Ez teszi lehetővé a PC1 számára, hogy közvetlenül érhesse el a routert.

* **Forrás MAC-cím** - A küldő eszköz, vagyis a PC1 MAC-címe. A PC1 Ethernet hálózati kártyájának MAC-címe AA-AA-AA-AA-AA-AA.
* **Cél MAC-cím** - Amikor a fogadó eszköz, a cél IP-cím másik alhálózaton van, mint a küldő, a küldő eszköz az alapértelmezett átjáró vagy router MAC-címét használja. Ebben a példában a cél MAC-cím az R1 Ethernet interfészének címe, vagyis 11-11-11-11-11-11. Ez az interfész ugyanahhoz a hálózathoz csatlakozik, mint a PC1, ahogy az ábrán is látható.

The figure shows the data link Ethernet frame header and network layer IP packet header for information flowing from a source on one network to a destination on a different network, highlighting the role of the MAC address. At the bottom is a network topology. Starting at the left, it consists of PC1 with IP 192.168.1.110 and MAC AA-AA-AA-AA-AA-AA(shown highlighted), a server, and another PC, all connected to the same switch. In the middle of the topology is a string of three routers to which the switch is connected. The router on the left is labeled R1 with IP 192.168.1.1 and MAC 11-11-11-11-11-11 (shown highlighted). The middle router is unlabeled. The router on the right is labeled R2 with IP 172.16.1.1 and MAC 22-22-22-22-22-22. At the right is another switch connected to a Web server with IP 172.16.1.99 and MAC AB-CD-EF-12-34-56. Above the topology is the message broken down into its various components. It begins on the left with the data link Ethernet frame header showing a destination of 11-11-11-11-11-11-11 and a source of AA-AA-AA-AA-AA-AA. Next is the network layer IP packet header showing a source of 192.168.1 (network) 110 (device) and a destination of 172.16.1 (network) 99 (device). Lastly is the data.

R1

R2



Data Link  
Ethernet Frame HeaderNetwork Layer  
IP Packet HeaderDestinationSourceSourceDestinationData11-11-11-11-11-11AA-AA-AA-AA-AA-AANetwork  
192.168.1.Device  
110Network  
172.16.1.Device  
99**PC1**  
192.168.1.110  
AA-AA-AA-AA-AA-AA**R1**  
192.168.1.1  
11-11-11-11-11-11**R2**  
172.16.1.1  
22-22-22-22-22-22**Web Server**  
172.16.1.99  
AB-CD-EF-12-34-56

Az Ethernet keret a beágyazott IP-csomaggal most már elküldhető az R1-nek. Az R1 ezek után a csomagot a célállomás, a Web Server felé továbbítja. Ez azt jelenti, hogy az R1 a csomagot vagy egy másik routernek, vagy közvetlenül a Web Server állomásnak továbbítja, amennyiben az az R1 egyik közvetlenül csatlakozó hálózatán van.

Fontos, hogy az alapértelmezett átjáró IP-címét a helyi hálózat minden állomásán be kell állítani. Minden távoli hálózaton levő célállomásra irányuló csomagot az alapértelmezett átjáróra kell küldeni. Az Ethernet MAC-címeket és az alapértelmezett átjárót részletesebben tárgyaljuk más fejezetekben.

3.7.8

## Adatkapcsolati címek

Az adatkapcsolati vagy második rétegbeli fizikai címnek más szerepe van. Az adatkapcsolati cím célja, hogy a keretet ugyanazon hálózaton lévő két hálózati interfész között továbbíthassuk.

Mielőtt egy IP-csomagot elküldenénk vezetékes vagy vezeték nélküli hálózaton keresztül, adatkapcsolati keretbe kell ágyazni, hogy a fizikai közegen továbbítható legyen.

Kattintsunk az egyes gombokra egy illusztráció megtekintéséhez arról, hogy az adatkapcsolati réteg címei miként változnak minden egyes ugrásnál a forrástól a célig!

**Host to Router**

The figure shows the L2 header in the first hop as information flows from a host on one network to a server on a different network. A network topology shows the original source PC1 at 192.168.1.10 connected to a router, connected to another router, connected to the final destination Web server at 172.16.1.99. Below the topology is an L3 IP packet with source IP 192.168.1.110 and destination IP 172.16.1.99. In front of the packet is the L2 header with destination NIC and source NIC. These L2 header addresses match the NIC of the original source (PC1) and the interface of the next hop router.



Original SourceFinal DestinationPC1  
192.168.1.110Web Server  
172.16.1.99NICNICNICNICNICNICL2L3L2L3L2L3Destination NICSource NICSource IP  
192.168.1.110L2 HeaderL3 IP PacketDestination IP  
172.16.1.99

Ahogy a csomag az állomástól routerig, majd routertől routerig, végül routertől állomásig halad, az IP-csomag minden lépésnél új adatkapcsolati keretbe kerül. Minden adatkapcsolati keret tartalmazza a keretet küldő és a keretet fogadó eszköz hálózati kártyájának adatkapcsolati címét.

A 2. rétegbeli adatkapcsolati protokoll csak arra szolgál, hogy a csomagot ugyanazon a hálózaton levő két hálózati kártya között szállítsa. A router megérkezéskor eltávolítja a 2. rétegbeli információkat, majd elküldés előtt új adatkapcsolati információkat ad hozzá, mielőtt továbbküldené a célja felé.

Az IP-csomag adatkapcsolati keretbe ágyazódik, amely a következő adatkapcsolati információkat tartalmazza:

* **Forrás adatkapcsolati cím** - A keretet küldő hálózati kártya fizikai címe.
* **Cél adatkapcsolati cím** - A keret címzettjének fizikai címe. Ez vagy a következő ugrást jelentő (next-hop) router címe, vagy a végső célberendezésé.

3.7.9

## Laborgyakorlat — A Wireshark telepítése

A Wireshark egy szoftveres protokollanalizátor, amelyet hálózati hibaelhárításkor, elemzésre, szoftver vagy protokoll fejlesztésekor, illetve oktatási célra használunk. A Wireshark a tanfolyam során a hálózati elvek szemléltetésére szolgál. A laborgyakorlat során letöltjük és feltelepítjük a Wiresharkot.

3.7.10

## Laborgyakorlat - A Wireshark használata hálózati forgalom vizsgálatára

A laborgyakorlat során a Wireshark segítségével elfogunk és elemzünk forgalmat.

3.7.11

## Tudáspróba - Adathozzáférés

Az űrlap teteje

Check your understanding of data encapsulation by choosing the BEST answer to the following questions.

1. True or false? Frames exchanged between devices in different IP networks must be forwarded to a default gateway.

Az űrlap alja

True or false? The right-most part of an IP address is used to identify the network that a device belongs to.

What is used to determine the network portion of an IPv4 address?

Which of the following statements are true regarding network layer and data link layer addresses? (Choose three.)

What is the order of the two addresses in the data link frame?

True or False? Data Link addresses are physical so they never change in the data link frame from source to destination.

[3.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adatbeágyazás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[3.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                              

1. Protokollok és modelle
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

3.8.1

## Miről tanultunk ebben a fejezetben?

**A szabályok**

Minden kommunikációs módszernek három közös eleme van: üzenetforrás (feladó), üzenet célja (címzett) és csatorna. Az üzenet küldését protokollnak nevezett szabályok szabályozzák. A protokollok közös elvárásai: azonosított küldő és címzett, közös nyelv és nyelvtan, a továbbítás sebessége és időzítése, visszajelzés vagy nyugtázás. A gyakori számítógépes protokollok a következő követelményeket tartalmazzák: üzenetkódolás, formázás és beágyazás, méret, időzítés és kézbesítési lehetőségek. A kódolás az, amikor egy információt egy másik, a továbbításhoz megfelelő formába alakítunk át. A dekódolás ennek a fordítottja. Az üzenet formátuma, formája az üzenet típusától és az átvitelhez használt csatornától függ. Az üzenet időzítése magában foglalja az adatfolyam-vezérlést, a válaszidő-túllépést és a hozzáférési módot. Az üzenetkézbesítési lehetőségek közé tartozik az egyedi küldés, a csoportos küldés és a szórás.

**Protokollok**

A protokollokat végberendezések és közvetítő eszközök valósítják meg szoftveresen, hardveresen vagy mindkettő módon. A számítógépes hálózaton keresztül küldött üzenet általában több protokoll használatát igényli, amelyek mindegyike saját funkciókkal és formátummal rendelkezik. Minden hálózati protokoll saját funkcióval, formátummal és kommunikációs szabályokkal rendelkezik. Az Ethernet protokollcsaládba tartozik az IP, a TCP, a HTTP és még sok más is. Az adatok biztonságával kapcsolatos protokollok, melyek hitelesítést, adatintegritást és titkosítást biztosítanak: az SSH, az SSL és a TLS. Protokollok, amelyek lehetővé teszik routerek közt az útvonalinformációk cseréjét, az útvonalinformációk összehasonlítását, majd a célhálózat legjobb elérési útjának kiválasztását: az OSPF és a BGP. Protokollok eszközök vagy szolgáltatások automatikus észlelésére: a DHCP és a DNS. A számítógépek és hálózati eszközök által használt protokollok a következő funkciókat biztosítják: címzés, megbízhatóság, adatfolyam-vezérlés, sorszámozás, hibadetektálás és alkalmazás interfész.

**Protokollkészletek**

A protokollkészlet egymáshoz kapcsolódó protokollok csoportja egy bizonyos kommunikációs célra. A protokollverem (protocol stack) megmutatja, hogy az egyes protokollok a készleten belül hogyan hajtódnak végre. Az 1970-es évek óta számos különböző protokollkészlet létezik, néhányat szabványszervezetek fejlesztettek ki, másokat pedig különböző gyártók. TCP/IP protokollok léteznek az alkalmazási, a szállítási és az internet rétegben egyaránt. A TCP/IP az internet és a mai hálózatok által használt protokollkészlet. A TCP/IP két fontos előnyt kínál a gyártók számára: nyílt és szabványosított protokollkészlet. A TCP/IP protokollkészlet kommunikációs folyamata lehetővé teszi egy webszerver számára a weboldal beágyazását és elküldését a kliens számára, a kliens pedig ki tudja csomagolni a weboldalt a böngészőben való megjelenítéshez.

**Szabványügyi szervezetek**

A nyílt szabványok elősegítik az együttműködést, a versenyt és az innovációt. A szabványügyi szervezetek általában gyártófüggetlen, non-profit szervezetekként jönnek létre, hogy fejlesszék és támogassák a nyílt szabványok koncepcióját. A különböző szervezeteknek különböző felelőssége van az internetre vonatkozó szabványok előmozdítása és létrehozása terén, ilyen szervezetek az ISOC, az IAB, az IETF és az IRTF. A TCP/IP-t fejlesztő és támogató szabványszervezetek közé tartozik az ICANN és az IANA. Elektronikus és kommunikációs szabványszervezetek a következők: IEEE, EIA, TIA és ITU-T.

**Referenciamodellek**

A hálózati műveletek leírására használt két referenciamodell az OSI és a TCP/IP. Az OSI-modell hét rétegből áll:

7 - Alkalmazási

6 - Megjelenítési

5 - Viszony

4 - Szállítási

3 - Hálózati

2 - Adatkapcsolati

1 - Fizikai

A TCP/IP modell négy réteget tartalmaz:

4 - Alkalmazási

3 - Szállítási

2 - Internet

1 - Hálózatelérési

**Adatbeágyazás**

Az üzenetek szegmentálásának két fő előnye:

* Ha kisebb egységeket küldünk a forrástól a célig, akkor egyszerre számos különböző párbeszéd adatai is összefűzhetők és szállíthatók a hálózaton. Ezt hívják multiplexelésnek.
* A szegmentálás a hálózat hatékonyságát is növeli. Ha az üzenet egy darabja nem ér el a célhoz, csak a hiányzó részeket kell újraküldeni.

A TCP felel az egyes szegmensek sorszámozásáért. Az egyes rétegekhez tartozó adatok formáját protokoll adategységnek nevezzük (Protocol Data Unit, PDU)\_. Az adatbeágyazás során minden újabb réteg becsomagolja a felsőbb rétegből származó PDU-t az alkalmazott protokollnak megfelelő módon. Amikor üzenetet küldünk a hálózaton, a beágyazási folyamat felülről lefelé történik. A fogadó oldal fordított irányú folyamatát kicsomagolásnak nevezzük. A kicsomagolási folyamat során a fogadó fél eltávolít egy vagy több protokollfejlécet. Az adatot kicsomagolják, ahogy halad felfelé a protokollkészleten a végfelhasználói alkalmazás irányába.

**Adathozzáférés**

A hálózati és az adatkapcsolati réteg feladata az adatok eljuttatása a forrástól a célig. Mindkét réteg protokolljai használnak forrás- és célcímeket, de a címek feladata különböző:

* **Hálózati rétegbeli forrás- és célcímek** - Eljuttatják az IP-csomagokat az eredeti forrástól a végső célig, amely lehet ugyanazon, de akár egy távoli hálózaton is.
* **Adatkapcsolati réteg forrás- és célcímei** - Eljuttatják az adatkapcsolati keretet ugyanazon hálózat egyik hálózati kártyájától a másikig.

Az IP-címek az eredeti forrást és a végső célt azonosítják. Az IP-cím két részből áll: a hálózati rész (IPv4) vagy előtag (IPv6) és az állomásazonosító rész (IPv4) vagy interfészazonosító (IPv6). Amikor az IP-csomagot küldő és fogadó állomások azonos hálózaton vannak, akkor az adatkapcsolati keret közvetlenül a fogadó eszköznek kerül elküldésre. Ethernet hálózaton az adatkapcsolati címet Ethernet MAC-címnek nevezzük. Amennyiben a csomag küldője és címzettje két különböző hálózaton található, akkor a forrás és cél IP-címek is különböző hálózati tartományokból kerülnek ki. Az Ethernet keretet egy másik készüléknek, a routernek vagy alapértelmezett átjárónak kell elküldeni.

3.8.2

## Ellenőrző kvíz - Protokollok és modellek

Az űrlap teteje

1. Melyik három mozaikszó/rövidítés képvisel szabványügyi szervezeteket? (Három jó válasz van.)

Az űrlap alja

Milyen típusú kommunikáció küld üzenetet a helyi hálózat összes eszközének?

A számítógépes kommunikációban mi az üzenetkódolás célja?

Melyik üzenetkézbesítési lehetőséget használjuk, ha ugyanazt az üzenetet egyszerre minden eszköznek meg kell kapnia?

Milyen két előnye van a réteges hálózati modell használatának? (Két jó válasz van.)

Mi a protokollok feladata az adatkommunikáció során?

Melyik logikai cím használatos adatok távoli hálózatba küldésekor?

Mi az általános megnevezése a hálózati modell tetszőleges rétegében található adatrészek leírásának?

Melyik két protokoll működik az Internet rétegben? (Két jó válasz van.)

Az OSI-modell melyik rétege határozza meg a végberendezések közötti egyedi kommunikáció adatainak szegmentálását és újraépítését célzó szolgáltatásokat?

Milyen típusú kommunikáció küld üzenetet a fogadó célállomások egy csoportjának egyszerre?

Milyen folyamatot használnak a továbbított adatok fogadására és olvasható üzenetté történő átalakítására?

Mi történik egy IP-csomaggal, mielőtt továbbítják a fizikai közegen?

Milyen eljárás helyezhet el egy üzenetet egy másik üzenetbe a forrástól a célállomásra történő átvitel céljából?

A web kliens egy kérést küld a webszerver felé egy weboldal megnyitására. A kliens szemszögéből nézve mi a helyes sorrendje azon protokollok rétegződésének, amelyek a kérést felkészítik a továbbításra?

[3.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adathozzáférés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                    
*                         

1. Fizikai réteg
2. Bevezetés

# Bevezetés

4.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a fizikai réteg című fejezetben.

Az OSI modell legalsó rétege a fizikai réteg. A TCP/IP modellben a hálózatelérési réteg részét képezi. A fizikai réteg nélkül nem lenne hálózatunk. Ez a modul részletesen foglalkozik a fizikai réteghez való csatlakozás három módjával. A Packet Tracer feladatok és laborgyakorlatok megadják azt a magabiztosságot, amelyre szükségünk lesz a saját hálózatunk kábelezésekor. Vágjunk is bele!

4.0.2

## Miről fogunk tanulni ebben a modulban?

**Fejezet címe:** Fizikai réteg

**Fejezet célja:** Annak ismertetése, hogy a fizikai réteg protokolljai, szolgáltatásai és a hálózati átviteli közegek milyen módon támogatják az adathálózatok közötti kommunikációt.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A fizikai réteg célja** | A fizikai réteg céljának és funkcióinak leírása. |
| **A fizikai réteg jellemzői** | A fizikai réteg jellemzőinek ismertetése. |
| **Rézkábelek** | A rézkábelek alapvető jellemzőinek meghatározása. |
| **UTP kábelezés** | Az UTP kábel Ethernet hálózatokban történő felhasználásának ismertetése. |
| **Optikai kábelek** | Az optikai kábeleknek és főbb előnyeiknek ismertetése a többi közeggel szemben. |
| **Vezeték nélküli átvitel** | Vezetékes és vezeték nélküli eszközök csatlakoztatása. |

[3.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A fizikai réteg célja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                     
*                         

1. Fizikai réteg
2. A fizikai réteg célja

# A fizikai réteg célja

4.1.1

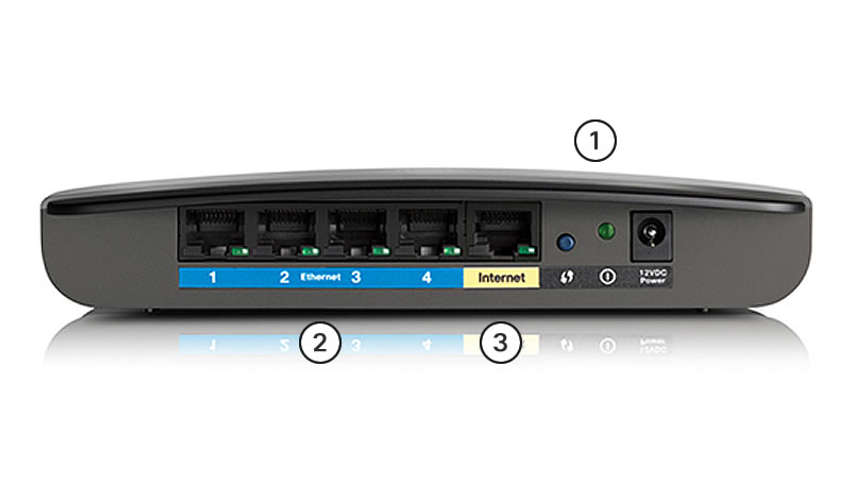
## Fizikai kapcsolat

Akár egy helyi nyomtatóhoz, akár egy távoli országban található weboldalhoz szeretnénk kapcsolódni, mielőtt bármilyen hálózati kommunikációt folytatnánk, a fizikai kapcsolatot kell kialakítani a helyi hálózaton. A kapcsolat lehet vezetékes vagy vezeték nélküli, attól függően, hogy kábelt vagy rádióhullámokat használunk az átvitelhez.

A fizikai kapcsolat típusa a hálózat kialakításától függ. Például számos vállalati irodában az alkalmazottak asztali és hordozható számítógépei egyaránt kábellel csatlakoznak egy switch-hez. Ez a beállítás vezetékes hálózatot jelent. Az adatok továbbítása fizikai kábelen keresztül történik.

A vezetékes összeköttetés mellett számos vállalat kínál vezeték nélküli kapcsolatot laptopok, táblagépek és okostelefonok számára. Vezeték nélküli eszközök esetében az adatok továbbítását rádióhullámok végzik. A vezeték nélküli kapcsolatok is egyre terjednek, mivel az egyéni és vállalati felhasználók egyaránt felfedezik annak előnyeit. A vezeték nélküli hálózat eszközeit olyan vezeték nélküli hozzáférési ponthoz (AP) vagy vezeték nélküli routerhez kell csatlakoztatni, amely az ábrán is látható.

### Vezeték nélküli router



A hozzáférési pont összetevői a következők:

1. Vezeték nélküli antennák (A fenti ábrán látható routerben ezek be vannak építve.)
2. Ethernet switchportok
3. Internet port

Egy vállalati irodához hasonlóan a legtöbb lakásban is van lehetőség vezetékes és vezeték nélküli hálózathoz való csatlakozásra. Az ábrákon egy otthoni router és egy laptop látható, amely a helyi hálózatra (LAN) csatlakozik.

### Vezetékes kapcsolat vezeték nélküli routerhez



**Hálózati illesztőkártya**

A hálózati kártyák (NIC) eszközöket csatlakoztatnak a hálózathoz. Az Ethernet kártyák vezetékes, míg a WLAN kártyák vezeték nélküli kapcsolatok létrehozására használhatók. A végfelhasználói eszközökben a két típus legalább egyike megtalálható. Ha egy hálózati nyomtató például csak Ethernet csatlakozóval rendelkezik, akkor a hálózathoz csak kábel használatával tud kapcsolódni. Más eszközök, például a táblagépek és az okostelefonok, csak WLAN adapterrel rendelkeznek, így csak vezeték nélküli kapcsolatot képesek létesíteni.

### Vezetékes kapcsolat Ethernet hálózati kártya használatával



Hálózati kapcsolódás esetén nem minden fizikai kapcsolat egyenértékű a teljesítmény tekintetében.

4.1.2

## A fizikai réteg

Az OSI modell fizikai rétege biztosítja a adatkapcsolati réteg kereteit alkotó bitek továbbítását a hálózati közegen. Ez a réteg egy teljes keretet fogad az adatkapcsolati rétegtől, és olyan jelek sorozatává alakítja, amelyek továbbíthatók az átviteli közegen. A keretet alkotó bitek származhatnak végberendezéstől vagy közvetítő eszköztől egyaránt.

Kattintsunk a Lejátszás gombra az ábrán a beágyazási folyamat példájának megtekintéséhez. A folyamat utolsó része a fizikai közegen keresztül küldött biteket mutatja. A fizikai réteg kódolja a kereteket és létrehozza azokat az elektromos, optikai vagy rádióhullámú jeleket, amelyek a keret bitjeinek felelnek meg. A jelek ezután egyesével elküldésre kerülnek az átviteli közegen.

A célállomás fizikai rétege fogadja ezeket a jeleket, bitekké alakítja őket, majd a biteket teljes keretként továbbítja az adatkapcsolati rétegnek.

The animation shows a small network with a Web Server and a Web Client. Theres is a graphic that shows the components that make up a message. An Ethernet Frame, and IP Packet, a TCP segment, and the user data. The animation begins with the web server preparing the Hypertext Markup Language (HTML) page as data to be sent. The application protocol HTTP header is added (prepended) to the front of the HTML data. The header contains various information, including the HTTP version the server is using and a status code indicating it has information for the web client. The HTTP application layer protocol delivers the HTML-formatted web page data to the TCP transport layer. The transport layer protocol prepends additional information to the HTTP data to manage the exchange of information between the web server and web client. The IP information is prepended to the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet. The Ethernet protocol prepends and adds to the end (appends) information to the IP packet to create a data link frame. The frame is then converted into a string of binary bits that are sent along the network path to the web client.

Web Server

Web Client

Data

TCP

IP

Ethernet

User Data

TCP Segment

IP Packet

Ethernet Frame

Data

TCP

IP

Protocol Encapsulation Terms

Ethernet



4.1.3

## Tudáspróba - A fizikai réteg célja

Az űrlap teteje

Check your understanding of the physical layer by choosing the correct answer to the following questions.

1. True or false? The physical layer is only concerned with wired network connections.

Az űrlap alja

True or false? When a frame is encoded by the physical layer, all bits are sent over the media at the same time.

The physical layer of the receiving device passes bits up to which higher level layer?

What PDU is received by the physical layer for encoding and transmission?

[4.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A fizikai réteg jellemzői](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                          
*                         

1. Fizikai réteg
2. A fizikai réteg jellemzői

# A fizikai réteg jellemzői

4.2.1

## A fizikai réteg szabványai

Az előző témakörben részletes áttekintést kaphattunk a fizikai rétegről és annak hálózatban elfoglalt helyéről. Ez a fejezet még jobban elmélyed a fizikai réteg sajátosságaiban. Tartalmazza a hálózat építéséhez használt összetevőket és átviteli közegeket, valamint azokat a szabványokat, amelyek ahhoz szükségesek, hogy minden együtt tudjon működni.

Az OSI modell felső rétegeiben található protokollok szoftveres megvalósítását szoftvertervező mérnökök és számítógépes szakemberek felügyelik. A TCP/IP modell szolgáltatásait és protokolljait például az IETF (Internet Engineering Task Force) nevű szervezet definiálja.

A fizikai réteg elektromos áramkörökből, átviteli közegekből és mérnökök által kifejlesztett csatlakozókból áll. Emiatt szükséges, hogy a hardverelemek működését irányító szabványokat a megfelelő villamosmérnöki és hírközlési szervezetek hozzák létre.

Számos különböző nemzetközi és nemzeti szervezet, kormányzati szerv és magánvállalat vesz részt a fizikai réteg szabványainak létrehozásában és továbbfejlesztésében. A hardverelemekre, az átviteli közegre, a kódolásra és jelátalakításra vonatkozó szabványokat például a következő szervezetek szabályozzák:

* Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO)
* Távközlési Ipari Szövetség (Telecommunications Industry Association, TIA) és az Elektronikai Iparágak Szövetsége (Electronic Industries Association, EIA)
* Nemzetközi Távközlési Szövetség (International Telecommunication Union, ITU)
* Amerikai Nemzeti Szabványügyi Intézet (American National Standards Institute, ANSI)
* Mérnököket egyesítő nemzetközi szervezet (Institute of Electrical and Electronics Engineers, IEEE)
* Nemzeti távközlési hatóságok, mint például az Egyesült Államokban található Szövetségi Kommunikációs Bizottság (Federal Communication Commission, FCC) és az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI)

A fentieken kívül gyakran helyi kábelezési szabványokért felelős szervezetekkel is találkozhatunk, ilyenek például a kanadai CSA (Canadian Standards Association), az európai CENELEC (European Committee for Electrotechnical Standardization), valamint a japán JSA/JSI (Japanese Standards Association).

The physical layer standards are implemented in hardware and are governed by many organizations including:

* ISO
* ANSI/TIA
* ITU-T
* ANSI
* IEEE

The TCP/IP standards are implemented in software and governed by the IETF.ApplicationPresentationSessionTransportNetworkData LinkPhysical

4.2.2

## Fizikai összetevők

A fizikai réteg szabványai három fő területtel foglalkoznak:

* Fizikai összetevők
* Kódolás
* Jelzés

**Fizikai összetevők**

Fizikai összetevők alatt olyan elektronikus hardvereszközöket, átviteli közegeket és csatlakozókat értünk, amelyek a biteket reprezentáló jelek továbbítását végzik. A hardverösszetevők, mint például a hálózati kártyák (NIC), az interfészek és csatlakozók, a kábelezési anyagok és tervek leírásait a fizikai réteghez kapcsolódó szabványok tartalmazzák. Ilyen szabványosított fizikai összetevőket találhatunk például a Cisco 1941 típusú routerben is.

4.2.3

## Kódolás

A kódolás vagy vonali kódolás bitek sorozatának előre meghatározott kóddá történő átalakítási módszerét jelenti. A kódok bitek olyan csoportját jelentik, amelyek elősegítik egy meghatározott minta felismerését a küldő és a fogadó fél által egyaránt. Más szóval, a kódolás a digitális információk ábrázolására használt módszert vagy mintát jelenti. Ez hasonló ahhoz, ahogy a Morze-kód kódolja az üzenetet pontok és vonalak sorozatával.

A Manchester kódolásnál például a nullát a magasról-alacsonyra, az 1-et pedig az alacsonyról-magasra feszültségátmenet jelenti. Az ábrán egy példa látható a Manchester kódolásra. Az átmenet az egyes bitidőszakok közepén történik. Ezt a kódolástípust 10 Mbps sebességű Ethernet esetén használják. A gyorsabb adatátviteli sebesség összetettebb kódolást igényel. A Manchester kódolást régebbi Ethernet-szabványokban használják, mint például a 10BASE-T. A 100BASE-TX Ethernet 4B/5B kódolást, az 1000BASE-T pedig 8B/10B kódolást használ.

The image is a line graph of voltage over time depicting Manchester encoding of a stream of seven bits. There are horizontal lines spaced evenly apart that represent bit periods. There is also a vertical line drawn halfway up the y axis used as a reference point. As the stream of bits (signal) is sent, there are drops and rises in voltage levels in the middle of each bit period. If the bit is a binary zero, then the voltage drops in the middle. If the bit is a binary one, then the voltage rises in the middle. The bits transmitted are 0100110.

1 1 1 0 0 0 0 0 1 0 0 1 1

0

VoltageTime

Az átmenet az egyes bitidőszakok közepén történik.

4.2.4

## Jelzés

A fizikai rétegnek kell előállítania a közegen továbbított 1-eseket és 0-kat ábrázoló elektromos, optikai vagy vezeték nélküli jeleket. A bitek ily módon történő megjelenítésének módját nevezzük jelzési módszernek. A fizikai réteg szabványaiban kell meghatározni az 1 és a 0 megjelenítésére használható jelek típusát. Ezt a megfeleltetést akár olyan egyszerű dolog is jelentheti, mint az elektromos vagy optikai jelek szintjének megváltozása. A hosszú impulzus például jelentheti az 1-et, a rövid pedig a 0-t.

Ez hasonló a Morze-kódnál használt jelzési módszerhez, ahol a be- és kikapcsolt hang-, fény- vagy csettintésjelek sorozatát használják szöveges tartalom telefonvonalon keresztüli vagy tengeri hajók közötti továbbítására.

Az ábrákon a jelzésre láthatunk példákat.

Kattintsunk az egyes gombokra a rézkábel, száloptikai kábel és vezeték nélküli adathordozó jelzéseinek megtekintéséhez.

**Electrical Signals Over Copper Cable**

graph of voltage over time showing square waves with varying levels of peaks and troughs

VoltageTime

4.2.5

## Sávszélesség

Az egyes átviteli közegek különböző sebességgel biztosítják a bitek továbbítását. Az adatátvitelt általában a sávszélességgel kapcsolatban emlegetik. A sávszélesség a közeg adatátviteli kapacitását jelenti. A digitális sávszélességet adott idő alatt egyik helyről a másikra átvitt adatmennyiséggel jellemezhetjük. Nagyságát általában kilobit per másodpercben (kb/s), megabit per másodpercben (Mb/s) vagy gigabit per másodpercben (Gb/s) mérjük. A sávszélességre néha úgy tekintünk, mint a bitek sebességére, ez azonban nem pontosan így van. Például a 10 Mb/s és 100Mb/s sebességű Ethernet esetén a bitek küldése egyaránt a villamos energia terjedésének sebességével történik. A különbséget a másodpercenként továbbított bitek száma jelenti.

Egy hálózatban a sávszélesség tényleges értékét az alábbi tényezők kombinációja határozza meg:

* Az átviteli közeg jellemzői.
* A jelátvitelre és jelfelismerésre használt módszerek.

Az átviteli közeg tulajdonságai, az alkalmazott technológiák és a fizikai törvényszerűségek mind szerepet játszanak a rendelkezésre álló sávszélesség meghatározásában.

A táblázat a sávszélesség általánosan használt mértékegységeit tartalmazza.

| Table caption | | |
| --- | --- | --- |
| **Sávszélesség egysége** | **Rövidítés** | **Átváltások** |
| Bit/szekundum | bit/s | 1 bit/s = sávszélesség alapegysége |
| Kilobit/szekundum | Kb/s | 1 Kb/s = 1,000 bps = 103 bps |
| Megabit/szekundum | Mbit/s | 1 Mbps = 1,000,000 bps = 106 bps |
| Gigabit/szekundum | Gbit/s | 1 Gbps = 1,000,000,000 bps = 109 bps |
| Terabit/szekundum | Tbit/s | 1 Tbps = 1,000,000,000,000 bps = 1012 bps |

4.2.6

## A sávszélesség szakszókincse

A sávszélesség mérésére használt kifejezések a következők:

* Késleltetés
* Átbocsátóképesség
* Hasznos átbocsátóképesség (goodput)

**Késleltetés**

A késleltetés azt az időtartamot jelenti, ami az adat egyik pontból a másikba történő eljuttatásához szükséges.

Egy több szegmensből álló hálózatban az átbocsátóképesség nem lehet nagyobb, mint a forrástól a célig tartó útvonal leglassabb kapcsolatának sebessége. Ez akkor is igaz, ha az összes vagy majdnem az összes szegmens nagy sávszélességű. Elég mindössze egyetlen kis átbocsátóképességű szegmens, amely szűk keresztmetszetet képezhet az egész hálózaton.

**Átbocsátóképesség**

Az átbocsátóképesség a közegen adott idő alatt átvitt bitek mennyiségét jelenti.

Számos tényezőt figyelembe véve az átbocsátóképesség nem egyezik meg az adott fizikai közegre megadott sávszélesség értékével. Az átbocsátóképesség általában alacsonyabb, mint a sávszélesség. Több tényező is befolyással van az átbocsátóképességre:

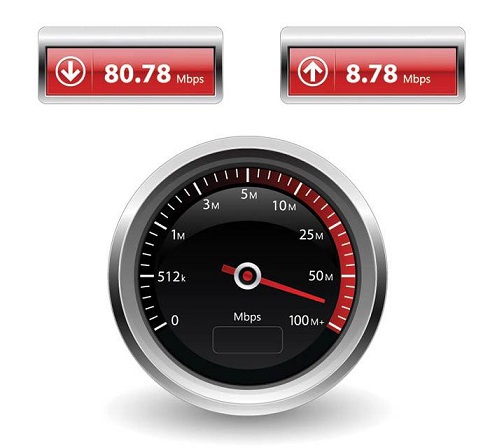
* A forgalom nagysága.
* A forgalom típusa.
* A hálózati eszközök által létrehozott, a forrás és a cél között felmerülő késleltetés.

Számos online sebességmérő teszt létezik, amelyekkel meghatározható az internetkapcsolat átbocsátóképessége. Az ábra egy sebességmérő teszt mintaeredményét mutatja.

**Hasznos átbocsátóképeség (goodput)**

Létezik egy harmadik módszer az adattovábbítás mérésére, ez az úgynevezett hasznos átbocsátóképesség (goodput). A goodput értéke az adott idő alatt átvitt használható adatok mennyiségét jelenti. A goodput értékét megkaphatjuk, ha az átbocsátóképességből kivonjuk a kapcsolat felépítésére, nyugtázásra és beágyazásra fordított forgalomtöbbletet. A goodput mindig alacsonyabb, mint az átbocsátóképesség, ami pedig általában alacsonyabb a sávszélességnél.

a meter measuring Mbps ranges from 0 - 100 Mbps with a display showing 80.78 Mbps for a download speed and another display showing 8.78 Mbps for an upload speed



Download SpeedUpload Speed

4.2.7

## Tudáspróba - A fizikai réteg jellemzői

Az űrlap teteje

Check your understanding of physical layer characteristics by choosing the correct answer to the following questions.

1. Which media uses patterns of microwaves to represent bits?

Az űrlap alja

Which media uses patterns of light to represent bits?

Which media uses electrical pulses to represent bits?

Which of these is the name for the capacity of a medium to carry data?

Which of these is a measure of the transfer of bits across the media?

[4.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A fizikai réteg célja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Rézkábelek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                              
*                         

1. Fizikai réteg
2. Rézkábelek

# Rézkábelek

4.3.1

## A rézkábelek jellemzői

A rézkábelek a leggyakrabban használt kábeltípusok a mai hálózatokban. A rézkábel valójában nem csak egyfajta kábeltípust jelent. Három különböző típusa létezik, amelyek mindegyike meghatározott körülmények között használható.

A hálózatokban azért használunk rézkábelt, mert olcsó, könnyen telepíthető és kicsi az ellenállása az elektromos árammal szemben. Hátránya viszont, hogy korlátozott a kábelhossz és érzékeny az interferenciára.

A rézkábelben az adatok elektromos impulzusok formájában továbbítódnak. A vevőkészülék hálózati interfészének érzékelője fogadja azokat a jeleket, amelyekből sikeresen vissza tudja állítani az elküldött jelet. Azonban minél távolabbra jut el a jel, annál inkább gyengül. Ezt nevezik jelcsillapításnak. Emiatt minden réz alapú kábelnél be kell tartani a szabványokban meghatározott szigorú hosszúsági korlátozásokat.

Az elektromos impulzusok időzítési és feszültségértékei két forrásból származó interferenciára érzékenyek:

* **Elektromágneses interferencia (EMI) vagy rádiófrekvenciás interferencia (RFI)** - Az EMI és RFI jelek torzíthatják és meghamisíthatják a réz alapú adathordozók által továbbított adatjeleket. A jellemző zavarforrások közé tartoznak a rádióhullámok és az elektromágneses eszközök, például a fluoreszkáló lámpák vagy az elektromos motorok.
* **Áthallás** - Áthallás alatt azt értjük, ha egy vezetéken haladó jel elektromos vagy mágneses mezője által keltett zavar átterjed a szomszédos vezetéken található jelre. Telefonvonalakon az áthallás következménye lehet, hogy halljuk egy szomszédos vonalon zajló másik beszélgetés részleteit. Tehát amikor egy vezetéken elektromos áram folyik keresztül, a huzal körül kis méretű, körkörös mágneses mező alakul ki, amely a szomszédos vezetékre is kifejti hatását.

Az ábrán megtekinthetjük, hogyan befolyásolja az interferencia az adatátvitelt.

The diagram is four graphs, each with voltage over time. The first graph shows square waves of a pure digital signal and its binary equivalent, 1011001001101. The second graph is of an interference signal with varying degrees of voltage. The third graph shows the digital signal with the interference. The fourth graph shows how the computer reads the changed signal as the binary equivalent of 1011001011101.

1 0 1 1 0 0 1 0 0 1 1 0 1 1 0 1 1 0 0 1 0 0 1 1 0 1 1 0 1 1 0 0 1 0 1 1 1 0 1 1 2 3

4

**Pure Digital Signal**VoltageTime**Interference Signal**VoltageTime**Digital Signal with Interference**VoltageTime**What the Computer ReadsChanged Signal**

1. Továbbításra kerülő tiszta digitális jel
2. A közegen interferencia jelenik meg
3. A digitális jel megsérül az interferencia miatt
4. A fogadó számítógép megváltozott jelet olvas. Figyeljük meg, hogy a 0 bit most 1-es bitként értelmezhető.

Az EMI és az RFI negatív hatásainak ellensúlyozására néhány rézkábel típusban fémes árnyékolást alkalmaznak és előírják a kapcsolat megfelelő földelését.

Az áthallás negatív hatásainak csökkentése érdekében bizonyos rézkábel fajtákban az ellentétes áramköri érpárokat összesodorják, ezzel tudnak hatékonyan fellépni ellene.

A rézkábel elektromos zajokra való érzékenysége az alábbi tényezők használatával korlátozható:

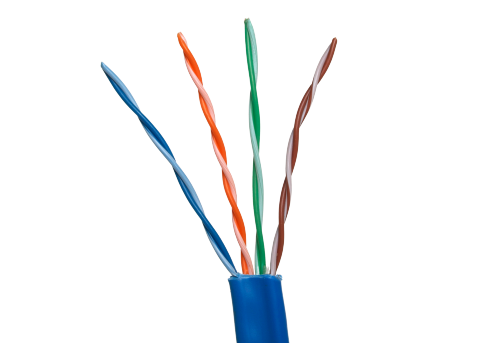
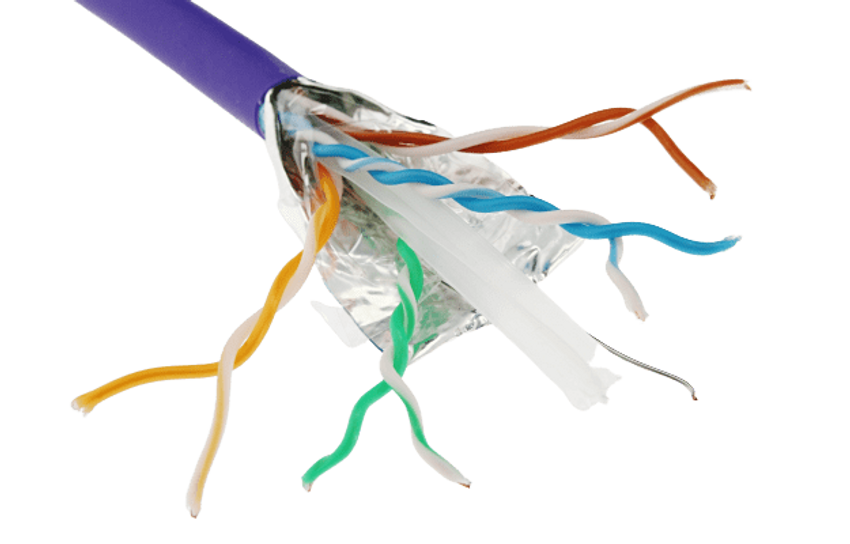
* Az adott hálózati környezetben leginkább alkalmazható kábel típusának vagy kategóriájának kiválasztása.
* Kábelezési terv készítése az ismert és az előre látható interferencia források elkerülésére.
* A kábelek megfelelő kezelésére és lezárására vonatkozó kábelezési technikák használata.

4.3.2

## A rézkábelek típusai

A hálózatokban használt réz alapú átviteli közegeknek három fő típusa létezik.

The figure is composed of pictures showing the three types of copper cabling, each with a portion of the outer cable jacket stripped to expose the cable construction. The first picture shows unshielded twisted-pair (UTP) cable with four color pairs of twisted wires - blue, orange, green, and brown. The second picture is shielded twisted-pair (STP) cable showing four pairs of twisted wires - blue, green, brown, and orange - with a foil shield surrounding all four pairs. The last picture shows a center copper conductor surrounded by plastic insulation surrounded by a braided shield.



Unshielded Twisted-Pair (UTP) CableShielded Twisted-Pair (STP) CableCoaxial Cable

4.3.3

## Árnyékolatlan csavart érpár (UTP)

Az árnyékolatlan csavart érpáras kábel (UTP) a leggyakrabban használt hálózati átviteli közegtípus. Az UTP kábelek RJ-45-ös csatlakozókban végződnek, hálózati állomások és hálózati eszközök (pl. switch-ek és routerek) közötti összeköttetés létrehozására használják.

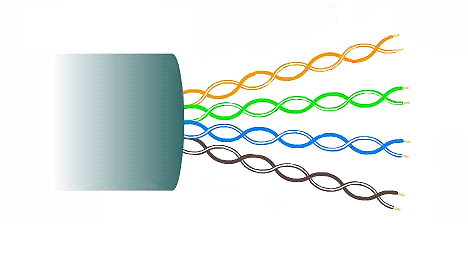
A helyi hálózatokban használt UTP kábel négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amely rugalmas műanyag köpenybe van befoglalva a fizikai károsodástól történő védelem miatt. A vezetékek csavarása a más vezetékekről származó jelinterferencia elleni védelemre szolgál.

Ahogy az ábrán is látható, a színkódok az egyes vezetékpárok és a párokban található vezetékek azonosítására szolgálnak, valamint segítenek a kábelek végződtetéseinek létrehozásában.

UTP cable showing the outer cable jacket (labeled 1), the twisted wire pairs (labeled 2), and the orange, green, blue, and brown insulation (labeled 3)

1 2

3



The numbers in the figure identify some key characteristics of unshielded twisted pair cable:

1. The outer jacket protects the copper wires from physical damage.
2. Twisted-pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates wires from each other and identifies each pair.

4.3.4

## Árnyékolt csavart érpár (STP)

Az árnyékolt csavart érpáras kábel (STP) jobb zaj elleni védelmet biztosít, mint az UTP kábel. Viszont az UTP-hez hasonlítva az STP kábel lényegesen drágább, és nehezebb is telepíteni. Az UTP-hez hasonlóan RJ-45-ös csatlakozót használ.

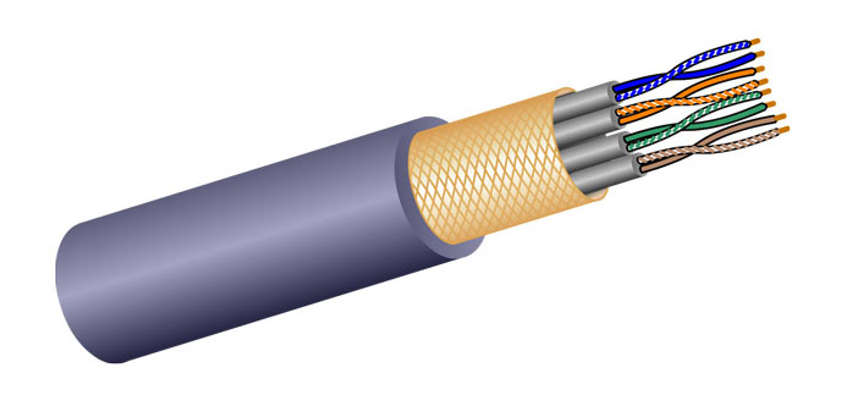
Az STP kábelek az EMI és az RFI ellen használt árnyékolási technikákat kombinálják az áthallás elleni védelmet szolgáló vezetékcsavarással. A teljes értékű árnyékolás eléréséhez az STP kábelek speciálisan árnyékolt STP csatlakozókban végződnek. Ha a kábel nem megfelelően van leföldelve, az árnyékolás antennaként viselkedve összegyűjtheti a nemkívánatos jeleket.

Ahogy látható, az STP kábel négy érpárat használ. Ezek mindegyike fóliaárnyékolással van borítva, amelyek aztán még egy fémhálóval vagy fóliával is be vannak burkolva.

STP cable showing the outer cable jacket (labeled 1), a braided shield around all the wire pairs (labeled 2), foil shields around the individual wire pairs (labeled 3), and the twisted colored wire pairs (labeled 4)

1 2 3

4



The numbers in the figure identify some key features of shielded twisted pair cable:

1. Outer jacket
2. Braided or foil shield
3. Foil shields
4. Twisted pairs

4.3.5

## Koaxiális kábel

A koaxiális kábel - vagy röviden koax - elnevezés a vezeték szerkezetéből származik, mivel két vezető egy közös tengelyen (axis) osztozik. Ahogy az ábrán is látható, a koaxiális kábel az alábbi részekből áll:

* Egy rézvezető, amely az elektronikus jelek továbbítását végzi.
* A rézvezetőt körülvevő rugalmas műanyag szigetelőréteg.
* A szigetelőanyagot beborító rézfonat vagy fémfólia, amely az áramkör második vezetékeként és a belső vezető árnyékolójaként működik. Ez a második réteg (más néven árnyékolás) a külső elektromágneses interferencia hatását is csökkenti.
* A kisebb fizikai sérülések elleni védelem érdekében az egész kábel egy borítással van bevonva.

A koaxiális kábelhez különböző típusú csatlakozók használhatók. A bajonett Neill—Concelman (BNC), N és F típusú csatlakozók az ábrán láthatók.

Annak ellenére, hogy a mai modern Ethernet hálózatokban az UTP kábel lényegében felváltotta a koax kábelt, a koax kábelnek a következő felhasználási területei léteznek:

* **Vezeték nélküli berendezések** -A koaxiális kábel antennákat kapcsol össze vezeték nélküli eszközökkel. A kábel hordozza a rádiófrekvenciás (RF) energiát az antennák és a rádiós berendezés között.
* **Kábelnetes berendezések** - A kábelnetes szolgáltatók úgy biztosítják az internetkapcsolatot az ügyfelek számára, hogy a koax kábel egyes részeit és az erősítő elemeket optikai kábellel helyettesítik. Az ügyfél telephelyén azonban még mindig koax kábelt használnak.

three figures showing the construction of a coaxial cable, a cross-section of a coaxial cable, and three types of coaxial cable connectors

1 2 4

3



Coaxial ConnectorsF typeN typeBNC

The numbers in the figure identify some key features of coaxial cable:

1. Külső köpeny
2. Rézfonatú árnyékolás
3. Műanyag szigetelés
4. Réz vezető

4.3.6

## Tudáspróba - Rézkábelek

Az űrlap teteje

Check your understanding of copper cabling by choosing the correct answer to the following questions.

1. Which of the following attaches antennas to wireless devices? It can also be bundled with fiber-optic cabling for two-way data transmission.

Az űrlap alja

Which of the following counters EMI and RFI by using shielding techniques and special connectors?

Which of the following is the most common network media?

Which of the following terminates with BNC, N type and F type connectors?

[4.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A fizikai réteg jellemzői](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[UTP kábel](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                
*                         

1. Fizikai réteg
2. UTP kábel

# UTP kábel

4.4.1

## Az UTP kábel tulajdonságai

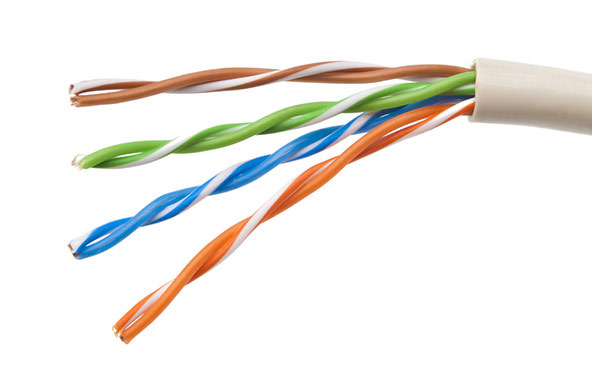
Az előző témakörben foglalkoztunk egy keveset az árnyékolatlan csavart érpáras (UTP) rézkábellel. Mivel az UTP kábelt a helyi hálózatokban történő használatra szabványosították, ez a fejezet részletesebben is ismerteti annak előnyeit és korlátait, valamint hogy mit lehet tenni a különböző problémák elkerülése érdekében.

Hálózati átviteli közegként használva az árnyékolatlan csavart érpár (UTP) négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amelyek rugalmas műanyag köpenybe vannak befoglalva. Kis mérete előnyös lehet a telepítés során.

Az UTP kábel nem használ árnyékolást az EMI és az RFI hatásainak kivédésére. A kábeltervezők ehelyett felismerték, hogy mivel tudják ellensúlyozni az áthallás negatív hatásait:

* **Kioltás -** A tervezők a vezetékpárokat egy áramkörként hozzák létre. Ha az áramkörben ezt a két vezetéket közel helyezzük el egymáshoz, a két vezeték által keltett mágneses mező pontosan ellentétes irányú lesz. Emiatt a két mágneses mező kioltja egymást, valamint a külső forrásból származó EMI és RFI jeleket is.
* **A vezetékpárok csavarásszámának változtatása -** A kioltási effektus hatásának fokozása érdekében eltérő számú csavarást alkalmaznak az egyes vezetékpárokban. UTP kábel használatakor szigorú előírásokat kell követni a méterenkénti csavarások számát illetően. Figyeljük meg az ábrán, hogy a narancs/narancs-fehér vezetékpár kevésbé csavart, mint a kék/kék-fehér pár! Mindegyik színezett vezetékpár eltérő számú csavarást tartalmaz.

Az UTP kábel kizárólag a vezetékek csavarásából eredő kioltási hatásra támaszkodik a jelromlás csökkentésének érdekében, valamint hatékonyan biztosítja a vezetékpárok önárnyékolását a közegen belül.



4.4.2

## UTP kábelezési szabványok és csatlakozók

Az UTP kábel a TIA/EIA által közösen összeállított szabványokban foglaltaknak felel meg. Pontosabban a TIA/EIA-568 szabvány az, amely meghatározza a LAN hálózatok kábelezési előírásait, és a leggyakrabban előforduló LAN kábelezési szabványnak számít. Néhány, a szabványban definiált elem a következő:

* Kábeltípusok
* Kábelhosszak
* Csatlakozók
* Kábelvégződés
* Kábeltesztelési módszerek

A rézkábel elektromos jellemzőit a mérnököket egyesítő nemzetközi szervezet, az IEEE határozza meg. Az IEEE az UTP kábeleket a teljesítményük alapján minősíti. Kategóriákba sorolja őket aszerint, hogy mekkora adatátviteli sebességre képesek. Az 5-ös kategóriájú kábelt például a 100BASE-TX FastEthernet típusú megvalósításoknál használják. A további kategóriák közé tartozik a továbbfejlesztett 5-ös kategóriájú, 6-os kategóriájú és a 6a kategóriájú kábel is.

A magasabb kategóriájú kábelek nagyobb adatátviteli sebességeket támogatnak. Az új, gigabites sebességű Ethernet technológiák bevezetésével az 5e kategória kevésbé elfogadott kábeltípussá vált, helyette a 6-os kategória használata javasolt új kábelezések kiépítésekor.

Az ábra az UTP kábel három kategóriáját mutatja:

* A 3-as kategóriát eredetileg hangátvitelre használták telefonvonalakon, de később adatátvitelre is alkalmazták.
* Az 5 és 5e kategóriákat adatátvitelre használják. Az 5-ös kategória 100 Mbps, az 5e kategória pedig 1000 Mbps adatátviteli sebességet támogat.
* A 6-os kategóriában minden vezetékpár között található egy elválasztó rész a nagyobb átviteli sebesség támogatása érdekében. Ez a kategória legfeljebb 10 Gbps-ot támogat.
* A 7-es kategória szintén támogatja a 10 Gbps-ot.
* A 8-as kategória képes a 40 Gbps adatátviteli sebességre is.

Néhány gyártó a 6a kategória követelményeit túlteljesítő kábeleit 7-es kategória jelzővel látja el.

The figure shows the difference in construction between categories of UTP cable. At the top is category 3 with four wires. In the middle is category 5 and 5e with four twisted wire pairs. At the bottom is category 6 with four twisted wire pairs, each with a plastic separator.

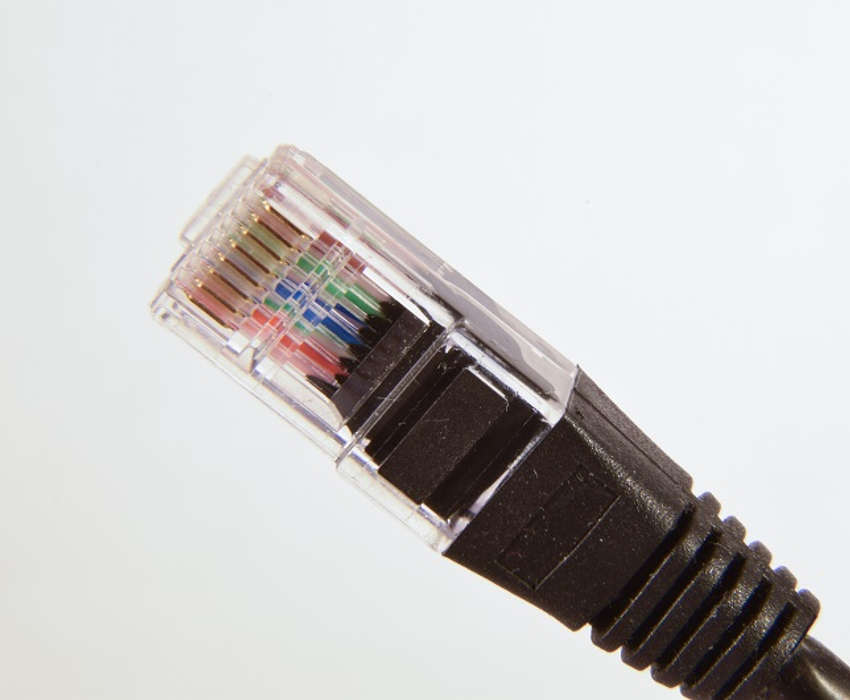
Category 3 Cable (UTP)Category 5 and 5e Cable (UTP)Category 6 Cable (UTP)

Az UTP kábel végződéseit általában RJ-45 csatlakozóval zárjuk le. A TIA/EIA-568 szabvány az Ethernet kábelben található vezetékek színkódjait és az aljzatok bekötését (lábkiosztást) írja le.

Az ábrán látható, hogy az RJ-45 csatlakozó a kábel végére szorított (krimpelt) dugaszt jelenti.

an RJ45 connector and a cable terminated with an RJ45 connector

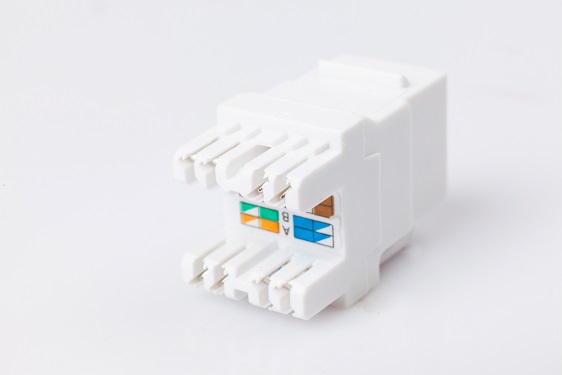
### RJ-45 UTP csatlakozók



Az ábrán látható csatlakozóaljzat a konnektor (anya) típusú összetevőt jelenti, amelyet hálózati eszközbe, falba, kabinszerű munkahelyi fülkékbe vagy patch panelbe szerelnek bele. Minden egyes helytelenül szerelt csatlakozó potenciális forrása lehet a fizikai jelek teljesítménycsökkenésének.

front and side view of an RJ45 UTP socket, including the color code for wire termination

### RJ-45 UTP aljzatok



Az ábrán egy helytelen lezárással készült UTP kábelre láthatunk példát. Ez a hibás csatlakozó olyan vezetékeket tartalmaz, amelyek kilógnak, a csavarásuk ki van bontva, és a burkolat nem teljesen fedi őket.

poorly terminated UTP cable showing untwisted wires extending outside of the RJ45 connector

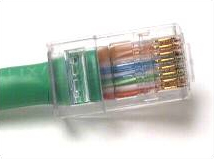
### Helytelenül lezárt UTP kábel



A következő ábrán egy megfelelően lezárt UTP kábelt láthatunk. Ez egy jó csatlakozó, amelyben a vezetékek csak a szükséges hosszon vannak kibontva.

properly termination UTP cable showing the cable jacket extending into the RJ45 connector enough to be crimped securely with all eight wires reaching the end of the connector

### Megfelelően lezárt UTP kábel



**MEGJEGYZÉS**: A kábel nem megfelelő lezárása hatással lehet az átviteli teljesítményre.

4.4.3

## Egyenes- és keresztkötésű UTP kábel

Különböző helyzetek különböző szabványú UTP kábelbekötések használatát követelik meg. Ez azt jelenti, hogy az egyes vezetékeket a kábelben különböző sorrendben kell csatlakoztatni az RJ-45 csatlakozó különböző érintkezőihez.

A kábelezési szabványoknak megfelelően a fő kábeltípusok az alábbiak:

* **Egyeneskötésű Ethernet kábel -** A leggyakrabban használt hálózati kábeltípus. Általában állomás és switch, valamint switch és router közötti összeköttetéseknél használjuk.
* **Keresztkötésű Ethernet kábel -** Hasonló eszközök összekapcsolására használjuk. Összeköthetünk vele például switch-et switch-el, állomást állomással vagy routert routerrel. A keresztkötésű kábelek azonban már elavultnak számítanak, mivel a hálózati kártyák az automatikus közegfüggő interfész fordítás (automatic medium-dependent interface crossover, Auto-MDIX) segítségével automatikusan felismerik a kábel típusát és létrehozzák a kapcsolatot.

**MEGJEGYZÉS**: Egy másik kábeltípus is létezik, az úgynevezett rollover kábel, amely a Cisco saját tervezésű kábele. Használatával a routerek vagy switch-ek konzolportjához lehet csatlakozni egy munkaállomásról.

A kereszt- vagy egyeneskötésű kábelek helytelen használata nem károsítja az eszközt, ilyen esetben viszont nem jön létre az eszközök közötti kapcsolat és adatkommunikációra sem kerül sor. Ez gyakori hibának számít, ezért ha a kapcsolat nem elérhető, a hibaelhárítás első lépéseként az eszközök összeköttetéseinek helyességét kell ellenőrizni.

Az ábrán a T568A és T568B szabványok szerinti vezetékpárok azonosítása látható..

The figure shows diagrams of the T568A and T568B wiring standards. Each shows the correct pinout for the individual wire pairs. Each color wire pair is numbered and consists of a solid color wire and a white striped wire. Pair 1 is blue, pair 2 is orange, pair 3 is green, and pair 4 is brown. Each standard alternates between white striped and solid wires. For the T568A standard, the blue pair are terminated at pins 4 and 5, the orange pair are terminated at pins 3 and 6, the green pair is terminated at pins 1 and 2, and the brown pair is terminated at pins 7 and 8. For the T568B standard, the blue pair is terminated at pins 4 and 5, the orange pair is terminated at pins 1 and 2, the green pair is termination at pins 3 and 6, and the brown pair is terminated at pins 7 and 8.

### T568A and T568B Standards

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7

8

Pair 2Pair 2Pair 4Pair 1Pair 3T568AT568BPair 3Pair 4Pair 1

A táblázatban az UTP kábeltípusok, a kapcsolódó szabványok és a kábelek jellemző alkalmazási területei láthatóak.

### Kábeltípusok és szabványok

| Kábeltípus Szabvány Felhasználás Egyeneskötésű Ethernet kábel Mindkét végén T568A vagy T568B szabványú Egy hálózati állomást csatlakoztat egy hálózati eszközhöz, például switch-hez vagy hub-hoz Keresztkötésű Ethernet kábel Egyik vége T568A, másik vége T568B szabványú Két hálózati állomást vagy két közvetítő eszközt (switch-et switch-hez vagy routert routerhez) kapcsol össze Rollover kábel A Cisco saját fejlesztésű protokollja A munkaállomás soros portját csatlakoztatja egy router konzolportjához adapter használatával. | | |
| --- | --- | --- |
| **Kábeltípus** | **Szabvány** | **Alkalmazás** |
| Egyeneskötésű Ethernet kábel | Mindkét végén T568A vagy T568B szabványú | Egy hálózati állomást csatlakoztat egy hálózati eszközhöz, például switch-hez vagy hub-hoz |
| Keresztkötésű Ethernet kábel | Az egyik vége T568A, a másik vége T568B szabványú | Két hálózati állomást vagy két közvetítő eszközt kapcsol össze (switch-et switch-hez vagy routert routerhez) |
| Rollover kábel | A Cisco saját fejlesztésű protokollja | A munkaállomás soros portját csatlakoztatja egy router konzolportjához adapter használatával. |

4.4.4

## Feladat - A kábelek érintkezőkiosztása

For this activity, correctly order the wire colors to a TIA/EIA cable pinout. Select a wire case color by clicking it. Then click a wire to apply that casing to it.

Select the pin case, then the cable pin to apply the casing.

T568A Pinout

Select the pin case, then the cable pin to apply the casing.

T568B Pinout

[4.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Rézkábelek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Optikai kábelek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                     
*                         

1. Fizikai réteg
2. Optikai kábelek

# Optikai kábelek

4.5.1

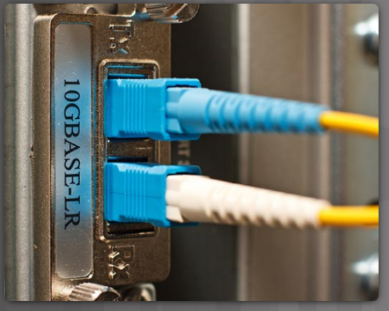
## Az optikai kábelek tulajdonságai

Megtanultuk, hogy a hálózatokban használt másik kábeltípus az optikai kábel. A magas ára miatt nem olyan elterjedt a használata, mint a különböző típusú rézkábeleké. Az optikai kábel viszont bizonyos tulajdonságai alapján a legjobb választást jelentheti adott helyzetekben, ezekről is szó lesz ebben a fejezetben.

Bármely más hálózati közeghez képest nagyobb távolságú és nagyobb sávszélességű adatátvitelt tesz lehetővé. A réz vezetékekkel ellentétben az optikai kábel kisebb csillapítással képes a jeltovábbításra, valamint teljesen érzéketlen az EMI és az RFI okozta zavarokra. Az optikai szálakat általában hálózati eszközök összekapcsolására használják.

Az optikai szál egy rugalmas, de rendkívül vékony, átlátszó anyagú nagyon tiszta üvegszál, amely nem sokkal vastagabb az emberi hajszálnál. A bitek fényimpulzusként jelennek meg rajta. A száloptikai kábel hullámvezetőként vagy '"fénycsőként" viselkedik, amikor minimális veszteséggel továbbítja a fényt két végpont között.

Ennek analógiájaként képzeljünk el egy üres papírtörlő tekercset, amelynek belseje tükörrel van bevonva. Ezer méter hosszú, és egy kis lézermutatót használnak Morse kódjelek fénysebességgel történő küldésére. A száloptikai kábel lényegében így működik, kivéve, hogy kisebb az átmérője és kifinomultabb fény alapú technológiákat használ.



4.5.2

## Az optikai kábelek típusai

Az optikai kábelek nagyjából két csoportba sorolhatók:

* Egymódusú kábel (Single-mode fiber, SMF)
* Többmódusú kábel (Multimode Fiber, MMF)

Az egyes típusokhoz tartozó illusztrációk és magyarázatok megjelenítéséhez kattintsunk az egyes gombokra.

**Egymódusú szál**

Az ábrán látható, hogy az egymódusú szál nagyon vékony magból áll, valamint lézeres technológiát használ a fénysugár elküldésére. Főleg az egymástól nagy távolságra, akár több száz kilométerre lévő helyek összekötésére használják, például hosszútávú telefonos és kábeltelevíziós felhasználás során.

A cross-section of a single-mode fiber optic cable consisting of a center glass core of 9 microns in diameter, surrounded by a glass cladding of 125 microns in diameter, surrounded by a polymeric coating. An x-ray vision sideview shows that this type of cable construction produces a single straight path for the light.

Glass Core diameter = 9 micrometer (µm)Glass Cladding 125 microns diameterPolymeric CoatingProduces single straight path for light

Az MMF és SMF közötti legnagyobb különbségek egyike a szóródás (diszperzió) mértéke. A szóródás arra utal, hogy a fényimpulzus mennyire terjed szét egy bizonyos idő eltelte után. A nagymértékű szóródás a jelerősség fokozottabb gyengülését is jelenti. A többmódusú szálnak nagyobb a diszperziója, mint az egymódusúnak. Ezért egymódusú szál esetén a jelet csak 500 méter távolságig lehet továbbítani veszteség nélkül.

4.5.3

## Optikai kábelek felhasználási területei

Az optikai kábelnek jelenleg az alábbi négy ipari felhasználási területe létezik:

* **Vállalati hálózatok -** Gerinchálózat kábelezése és a hálózat infrastruktúráját alkotó eszközök összekötése.
* **Üvegszál az otthonig (Fiber-to-the-home, FTTH) -** Folyamatos szélessávú kapcsolatot biztosít az otthoni és kisvállalati felhasználók számára.
* **Nagytávolságú hálózatok -** Szolgáltatók használják országok és városok összekötésére.
* **Tenger alatti kábelhálózatok -** Nagy sebességet és kapacitást biztosít akár óceánnyi távolságok áthidalására is, valamint képes ellenállni a tengerek alatt lévő mostoha körülményeknek. Keressünk rá az interneten a „tengeralatti kábelek telegeográfiai térképe” kifejezésre a különböző térképek online megtekintéséhez.

Ebben a fejezetben a vállalati hálózatokban használt optikai kábelekre fektetjük a hangsúlyt.

4.5.4

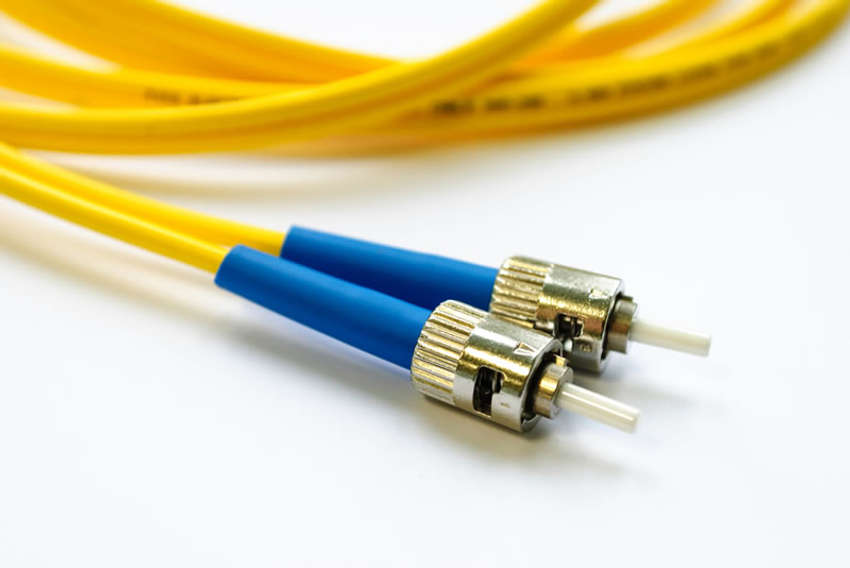
## Optikai csatlakozók

Az optikai csatlakozók az optikai szálak végződéseit zárják le. Ezeknek számos típusa elérhető. A fő különbség közöttük a méretből és a kapcsolódás módjából adódik. Annak kiválasztása, hogy a különböző típusok közül melyik kerül felhasználásra, a vállalat eszközeitől függ.

**MEGJEGYZÉS**: Egyes switchek és routerek olyan portokkal rendelkeznek, amelyek támogatják az SFP (small form-factor pluggable) típusú optikai csatlakozókat. Keressünk az interneten különböző típusú SFP-ket.

Az egyes optikai csatlakozó típusokhoz tartozó kép és információ megjelenítéséhez kattintsunk a típusok nevére.

Az egyik legkorábban használt csatlakozótípus. A csatlakozót fel- és lecsavarható (twist-on/twist-off) bajonettzáras módszerrel lehet biztonságosan rögzíteni.



Egészen a közelmúltig a fényt csak egy irányban lehetett továbbítani az optikai szálon keresztül. A teljes duplex működés megvalósításához két szálra volt szükség. Az optikai lengőkábelek (patch kábelek) emiatt két optikai szálat foglalnak magukban, a végződésüket pedig szabványos optikai csatlakozópárral valósítják meg. Bizonyos optikai csatlakozók, amelyeket duplex csatlakozó néven ismerünk, képesek a küldő és a fogadó szálat egy csatlakozóba bekötni, ez duplex többmódusú LC csatlakozó néven látható az ábrán. A BX szabványok (például a 100BASE-BX) különböző hullámhosszakat használnak egyetlen szálon keresztül történő küldéshez és fogadáshoz.

4.5.5

## Optikai patch kábelek

Az optikai patch kábelt a hálózatok gerincét alkotó eszközök összekötésére használják. Az egy- és többmódusú kábelek között a kábel színe tesz különbséget. A sárga szín az egymódusú, a narancssárga (vagy kék) pedig a többmódusú kábeleket jelöli.

Az egyes optikai patch kábelekhez tartozó kép megtekintéséhez kattintsunk a kábeltípusok nevére.



**MEGJEGYZÉS**: A kábeleket műanyag lezáró kupakkal kell védeni, amikor nem használjuk őket.

4.5.6

## A réz- és optikai kábelek összehasonlítása

Az optikai kábel használatának számos előnye van a rézkábelekhez képest. A táblázatban a főbb különbségek vannak kiemelve.

Napjainkban az optikai kábelt vállalati környezetben elsősorban gerinchálózati kábelezésnél használják különböző létesítmények nagyforgalmú pont-pont összeköttetéseinek megvalósításakor. Emellett egyetemi kampuszokon is használható az egyes épületek összekötésére. Az optikai kábel remekül alkalmazható ezen célokra, mivel nem vezeti az elektromosságot és kicsi a jelvesztesége.

### UTP és optikai kábelek összehasonlítása

| Table caption | | |
| --- | --- | --- |
| **Felhasználás tényezői** | **UTP kábel** | **Optikai kábel** |
| Támogatott sávszélesség | 10 Mb/s - 10 Gb/s | 10 Mb/s - 100 Gb/s |
| Hatótávolság | Viszonylag kicsi (1 - 100 méter) | Viszonylag nagy (1 - 100 000 méter) |
| EMI és RFI elleni védettség | Alacsony | Magas (teljesen védett) |
| Elektromos veszélyekkel szembeni védettség | Alacsony | Magas (teljesen védett) |
| Vezetékek és csatlakozók költségei | Legalacsonyabb | Legmagasabb |
| Telepítéshez szükséges ismeretek | Legalacsonyabb | Legmagasabb |
| Biztonsági óvintézkedések | Legalacsonyabb | Legmagasabb |

4.5.7

## Tudáspróba - Optikai kábelek

Az űrlap teteje

Check your understanding of fiber-optic cabling by choosing the correct answer to the following questions.

1. Which of the following fiber-optic cable types can help data travel approximately 1.24 miles or 2 km/2000m?

Az űrlap alja

Which of the following fiber-optic cable types use light emitting diodes (LEDs) as a data light source transmitter?

Which of the following fiber-optic cable types use lasers in a single stream as a data light source transmitter?

Which of the following fiber-optic cable types is used to connect long-distance telephony and cable TV applications?

Which of the following fiber-optic cable types can travel approximately 62.5 miles or 100 km/100000 m?

Which of the following fiber-optic cable types is used within a campus network?

[4.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[UTP kábel](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Vezeték nélküli átvitel](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                         
*                         

1. Fizikai réteg
2. Vezeték nélküli átvitel

# Vezeték nélküli átvitel

4.6.1

## A vezeték nélküli átvitel jellemzői

Előfordulhat, hogy ezen a kurzuson táblagép vagy okostelefon használatával veszünk részt. Ez csak vezeték nélküli átvitel használatával lehetséges, amely a harmadik módja annak, hogy csatlakozzunk a hálózat fizikai rétegéhez.

A vezeték nélküli közegek rádió- vagy mikrohullámok használatával továbbítják az elektromágneses jeleket, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg.

A vezeték nélküli átvitel biztosítja a legnagyobb mobilitást az összes közegtípus közül, emellett a vezeték nélküli eszközök száma is folyamatosan növekszik. Mostanra a felhasználók leginkább vezeték nélkül csatlakoznak az otthoni és vállalati hálózatokhoz.

A vezeték nélküli átvitel korlátai a következők:

* **Lefedettségi terület** - A vezeték nélküli adatátviteli technológiák kiválóan működnek szabadtéren. Ugyanakkor az épületekben használt egyes építési anyagok és a helyi földrajzi viszonyok korlátozzák a tényleges lefedettséget.
* **Interferencia** - A vezeték nélküli átvitel érzékeny az interferenciára, és olyan hétköznapi eszközök is zavarhatják az átvitelt, mint például a vezeték nélküli telefonok, bizonyos fénycsőtípusok, mikrohullámú sütők és más vezeték nélküli eszközök.
* **Biztonság** - A lefedettségi területen belül nem kell fizikailag a közeghez kapcsolódni annak használatához. Emiatt az erre nem jogosult eszközök és felhasználók is hozzáférhetnek a hálózathoz. A hálózatbiztonság a vezeték nélküli hálózatok felügyeletének egyik fő összetevője.
* **Osztott átviteli közeg** - A WLAN-ok fél-duplex módban működnek, ami azt jelenti, hogy egyidejűleg csak egy eszköz végezhet adatküldést vagy fogadást. A vezeték nélküli közeg az összes vezeték nélküli felhasználó között meg van osztva. Ha a WLAN-hoz egyszerre több felhasználó is hozzáfér, akkor az minden felhasználó számára csökkenti a sávszélességet.

Habár a vezeték nélküli technológia egyre népszerűbb a kis távolságú összeköttetések esetében, a legnépszerűbb fizikai közegnek még mindig a réz- és optikai kábel számít a közvetítő eszközökkel (mint routerek és switchek ) megvalósított hálózatokban.

4.6.2

## A vezeték nélküli átvitel típusai

A vezeték nélküli átvitelre vonatkozó IEEE és ipari távközlési szabványok mind az adatkapcsolati, mind pedig a fizikai rétegre kiterjednek. Ezen szabványok mindegyikének a fizikai rétegre vonatkozó specifikációja a következő területeket foglalja magában:

* Az adatok rádiójelekké történő átalakítása
* Átviteli frekvencia és teljesítmény
* A jel vételére és dekódolására vonatkozó követelmények
* Antennák tervezése és kivitelezése

A vezeték nélküli szabványok a következők:

* **Wi-Fi (IEEE 802.11)** - Vezeték nélküli LAN (WLAN) technológia, közismert nevén Wi-Fi. A WLAN-ok egy versengés alapú protokollt használnak, amelyet vivőjel-érzékeléses többszörös hozzáférés ütközéselkerüléssel (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA) néven ismerünk. A vezeték nélküli hálózati kártyának küldés előtt figyelnie kell a csatornát annak megállapítására, hogy az szabad-e. Ha éppen egy másik vezeték nélküli eszköz végez továbbítást, akkor a hálózati kártyának várnia kell, amíg a csatorna szabaddá nem válik. A Wi-Fi védjegy tulajdonosa a Wi-Fi Szövetség (Wi-Fi Alliance). A Wi-Fi megnevezés azokra a tanúsított WLAN eszközökre vonatkozik, amelyek a 802.11 szabványok alapján működnek.
* **Bluetooth (IEEE 802.15)** - Ez egy vezeték nélküli személyes hálózati (WPAN) szabvány, amelynek közismert neve „Bluetooth”. Társított eszközpárok közötti kommunikációra alkalmas maximum 100 méter távolságig.
* **WiMAX (IEEE 802:16)** - Pont-multipont topológiát használ a szélessávú vezeték nélküli hozzáférés biztosításához, közismert neve WiMAX (Worldwide Interoperability for Microwave Access).
* **Zigbee (IEEE 802.15.4)** - A Zigbee egy olyan szabvány, amelyet alacsony adatsebességű és kis energiaigényű kommunikációhoz használunk. Olyan alkalmazásokhoz készült, amelyek rövid hatótávolságot, alacsony adatátviteli sebességet és hosszú akkumulátor-élettartamot igényelnek. A Zigbee-t jellemzően ipari és IoT (Internet of Things) környezetekben használják, például vezeték nélküli villanykapcsolóknál és orvostechnikai eszközök adatgyűjtésénél.

**MEGJEGYZÉS**: Más vezeték nélküli technológiák, például a mobil és a műholdas kommunikáció szintén nyújthat adathálózati kapcsolatot. Ezek a technológiák azonban nem képezik részét a fejezetnek.

4.6.3

## Vezetéknélküli LAN

A vezeték nélküli hálózat közös adatátviteli közege lehetővé teszi az eszközök számára, hogy vezeték nélkül csatlakozzanak egymáshoz egy LAN-on keresztül. Egy WLAN általában a következő hálózati eszközök használatát követeli meg:

* **Vezeték nélküli hozzáférési pont (Access Point, AP)** - Fogadja a felhasználók vezeték nélküli jeleit, és csatlakozik a meglévő rézvezetékes hálózathoz, például az Ethernethez. Az otthoni és kisvállalati környezetben használt vezeték nélküli router egy eszközben tartalmazza a router, a switch és a hozzáférési pont funkcióit. A képen egy ilyen eszköz látható.
* **Vezeték nélküli hálózati adapterek** - Vezeték nélküli kommunikáció képességét biztosítják a hálózati állomásoknak.

A technológia fejlődésével számos Ethernet alapú WLAN szabvány alakult ki. Vezeték nélküli eszközök vásárlásakor meg kell győződni annak kompatibilitási és az együttműködési képességeiről.

A vezeték nélküli kommunikáció előnyei nyilvánvalóak, különösen ha a költséges kábelezés megtakarításáról és a hordozhatóságból adódó kényelemről beszélünk. A hálózati rendszergazdának úgy kell megalkotnia és alkalmaznia a szigorú biztonsági szabályokat, hogy a vezeték nélküli LAN védve legyen az illetéktelen hozzáférésektől és támadásoktól.

### Cisco Meraki MX64W



4.6.4

## Tudáspróba - Vezeték nélküli átvitel

Az űrlap teteje

Check your understanding of wireless media by choosing the BEST answer to the following questions.

1. True or false. Wireless is not well suited for enterprise networks.

Az űrlap alja

True or false. Wireless LANs operate in full-duplex allowing all devices to send or receive data at the same time so the number of users does not impact performance.

Which of the following wireless standards is best suited for industrial and IoT environments?

Which of the following wireless standards is used for Personal Area Networks (PANs) and allows devices to communicate over distances of 1 to 100 meters?

4.6.5

## Packet Tracer - Kapcsolódás vezetékes és vezeték nélküli LAN-hoz

Packet Tracer-rel, valamint laboratóriumi vagy vállalati környezetben történő munkavégzés során tudnunk kell, hogyan válasszuk ki a megfelelő kábeltípust és hogyan csatlakoztassuk megfelelően az eszközöket. A feladat megoldása során Packet Tracer-ben kell bizonyos eszközök konfigurációját megvizsgálni, a beállításoknak megfelelő kábeltípust kiválasztani, majd az eszközök csatlakoztatását elvégezni. A feladat a hálózat fizikai nézetével is foglalkozik.

[Vezetékes és vezetéknélküli LAN csatlakoztatása](https://contenthub.netacad.com/courses/itn/_common/4.6.5-packet-tracer---connect-a-wired-and-wireless-lan_hu-HU.pka)

4.6.6

## Laborgyakorlat - Vezetékes és vezeték nélküli hálózati kártya információinak megtekintése

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: A számítógép hálózati kártyáinak azonosítása és a velük történő munkavégzés
* Bölüm 2: A tálcán lévő Hálózatok ikon azonosítása és használata

[4.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Optikai kábelek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[4.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                   

1. Fizikai réteg
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

4.7.1

## Packet Tracer - Csatlakozás a fizikai réteghez

A feladat során a hálózati eszközökön elérhető lehetőségeket vizsgáljuk meg. Emellett meghatározzuk, hogy mely lehetőségek biztosítják a szükséges kapcsolatot különböző eszközök csatlakoztatásakor. Végezetül a megfelelő modul kiválasztásával és beépítésével csatlakoztatjuk az eszközöket.

[Csatlakozás a fizikai réteghez](https://contenthub.netacad.com/courses/itn/_common/4.7.1-packet-tracer---connect-the-physical-layer_hu-HU.pka)

4.7.2

## Miről tanultunk ebben a fejezetben?

**A fizikai réteg célja**

Mielőtt bármilyen hálózati kommunikációt folytatnánk, a fizikai kapcsolatot kell kialakítani a helyi hálózaton. A kapcsolat lehet vezetékes vagy vezeték nélküli, attól függően, hogy kábelt vagy rádióhullámokat használunk az átvitelhez. A hálózati kártyák (NIC) eszközöket csatlakoztatnak a hálózathoz. Az Ethernet kártyák vezetékes, míg a WLAN kártyák vezeték nélküli kapcsolatok létrehozására használhatók. Az OSI modell fizikai rétege biztosítja a adatkapcsolati réteg kereteit alkotó bitek továbbítását a hálózati közegen. Ez a réteg egy teljes keretet fogad az adatkapcsolati rétegtől, és olyan jelek sorozatává alakítja, amelyek továbbíthatók az átviteli közegen. A keretet alkotó bitek származhatnak végberendezéstől vagy közvetítő eszköztől egyaránt.

**A fizikai réteg jellemzői**

A fizikai réteg elektromos áramkörökből, átviteli közegekből és mérnökök által kifejlesztett csatlakozókból áll. A fizikai réteg szabványai három fő területtel foglalkoznak: fizikai összetevők, kódolás és jelzés. A sávszélesség a közeg adatátviteli kapacitását jelenti. A digitális sávszélességet adott idő alatt egyik helyről a másikra átvitt adatmennyiséggel jellemezhetjük. Az átbocsátóképesség a közegen adott idő alatt átvitt bitek mennyiségét jelenti, az értéke általában kisebb mint a sávszélességé. A késleltetés azt az időtartamot jelenti, amely az adatok egyik pontból a másikba történő eljuttatásához szükséges. A goodput értéke az adott idő alatt átvitt hasznos adatok mennyiségét fejezi ki. A fizikai réteg a következő típusú átviteli közegekre állítja elő a bitek megfelelőjét:

* **Rézkábel** - A jelek elektromos impulzusoknak felelnek meg.
* **Száloptikai kábel** - A jelek fényimpulzusoknak felelnek meg.
* **Vezeték nélküli átvitel** - A jelek a mikrohullámú átvitel mintáinak felelnek meg.

**Rézkábel**

A hálózatokban azért használunk rézkábelt, mert olcsó, könnyen telepíthető és kicsi az ellenállása az elektromos árammal szemben. Hátránya viszont, hogy korlátozott a kábelhossz és érzékeny az interferenciára. Az elektromos impulzusok időzítési és feszültségértékei két forrásból származó interferenciára érzékenyek: az EMI-re és az áthallásra. A háromféle rézkábel típus a következő: UTP, STP és koaxiális kábel (koax). Az UTP kábel külső burkolata a fizikai sérülések ellen nyújt védelmet, a vezetékpárok csavarása védi a jelet az interferenciától, a színkódokkal jelölt műanyag szigetelés pedig elektromosan szigeteli a vezetékeket egymástól, és azonosítja a vezetékpárokat. Az STP kábel négy érpárt használ. Ezek mindegyike fóliaárnyékolással van borítva, amelyek aztán még egy fémhálóval vagy fóliával is be vannak burkolva. A koaxiális kábel vagy röviden koax elnevezés a vezeték szerkezetéből származik, azaz két vezető (conductor) egy közös tengelyen (axis) osztozik. A koax kábel antennákat kapcsol össze vezeték nélküli eszközökkel. A kábelnetes szolgáltatók szintén koaxot használnak ügyfeleik telephelyén.

**UTP kábel**

Az UTP kábel négy pár színkóddal jelölt, egymással összecsavart vezetékből áll, amelyek rugalmas műanyag köpenybe vannak befoglalva. Az UTP kábel nem használ árnyékolást az EMI és az RFI hatásainak kivédésére. A kábeltervezők ehelyett felismerték, hogy milyen más módokon tudják ellensúlyozni az áthallás negatív hatásait: kioltással és a vezetékpárok csavarásszámának változtatásával. Az UTP kábel a TIA/EIA által közösen összeállított szabványokban foglaltaknak felel meg. A rézkábel elektromos jellemzőit a villamosmérnököket egyesítő nemzetközi szervezet, az IEEE határozza meg. Az UTP kábel végződéseit általában RJ-45 csatlakozóval zárjuk le. A fő kábeltípusok, amelyeket speciális kábelezési szabályok alkalmazásával kapunk, az egyenes- és keresztkötésű Ethernet kábelek. A Cisco egy saját tervezésű UTP kábellel is rendelkezik, amelyet rollover kábelnek hívunk, ez egy munkaállomást köt össze a router konzolportjával.

**Optikai kábelek**

Bármely más hálózati közeghez képest nagyobb távolságú és nagyobb sávszélességű adatátvitelt tesz lehetővé. Az optikai kábel kisebb csillapítással képes a jeltovábbításra, mint a rézvezetékek, valamint teljesen érzéketlen az EMI és az RFI okozta zavarokra. Az optikai szál egy rugalmas, de rendkívül vékony, átlátszó anyagú nagyon tiszta üvegszál, amely nem sokkal vastagabb az emberi hajszálnál. A bitek fényimpulzusként jelennek meg a szálon. Az optikai kábeleket jelenleg négy iparágban használják: vállalati, FTTH (üvegszál az otthonig), nagytávolságú valamint tengeralatti hálózatokban. Négyféle optikai csatlakozótípussal találkoztunk: ST, SC, LC és duplex többmódusú LC. Az optikai patch kábelek közé tartoznak az SC-SC többmódusú, az LC-LC egymódusú, az ST-LC többmódusú és az SC-ST egymódusú típusok. Az optikai kábelt vállalati környezetben elsősorban gerinchálózati kábelezésnél használják különböző létesítmények nagyforgalmú pont-pont összeköttetéseinek megvalósításakor, illetve egyetemi kampuszokon az egyes épületek összekötésére.

**Vezeték nélküli átvitel**

A vezeték nélküli közegek rádió- vagy mikrohullámok használatával továbbítják az elektromágneses jeleket, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg. A vezeték nélküli hálózatoknak vannak bizonyos korlátai, többek között a lefedettségi terület, az interferencia, a biztonság és a megosztott átviteli közeggel kapcsolatos problémák. A vezeték nélküli szabványok a következők: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16) és Zigbee (IEEE 802.15.4). Egy vezeték nélküli LAN (WLAN) hálózatban vezeték nélküli hozzáférési pont (AP) és vezeték nélküli hálózati adapterek használata szükséges.

4.7.3

## Ellenőrző kvíz - Fizikai réteg

Az űrlap teteje

1. A hálózati rendszergazda kapcsolódási problémák hibaelhárítását végzi egy szerveren. Kábeltesztelővel észreveszi, hogy a szerver hálókártyája által generált jelek torzultak, és nem használhatók. Az OSI modell melyik rétegébe tartozik a hiba?

Az űrlap alja

Milyen típusú kábelt használnak a munkaállomás soros portjának a Cisco router konzolportjához való csatlakoztatásához?

Miért használnak két optikai szálat egy optikai kapcsolat esetén?

ilyen eljárást használnak arra, hogy csökkentsék az áthallás hatását a rézkábelekben?

Mi az előnye az optikai szálak használatának a réz kábelezéssel szemben?

A hálózati rendszergazda egy új hálózati infrastruktúrát tervez, amely vezetékes és a vezeték nélküli kapcsolatokat is tartalmaz. Milyen feltételek mellett ajánlott a vezeték nélküli kapcsolat?

Milyen típusú UTP-kábellel csatlakoztatják a számítógépet egy switchporthoz?

Mi a sávszélesség meghatározása?

Melyik állítás írja le helyesen a keretkódolást?

Mi a jellemző az UTP-kábelezésre?

A wireless LAN is being deployed inside the new one room office that is occupied by the park ranger. The office is located at the highest part of the national park. After network testing is complete, the technicians report that the wireless LAN signal is occasionally affected by some type of interference. What is a possible cause of the signal distortion?

Mi az OSI fizikai rétegének célja?

Melyik jellemző írja le az áthallást?

Mit jelent az áteresztőképesség kifejezés?

Melyik szabványszervezet felügyeli a vezeték nélküli LAN-szabványok fejlesztését?

[4.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Vezeték nélküli átvitel](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[5.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                   
*                       

1. Számrendszerek
2. Bevezetés

# Bevezetés

5.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Számrendszerek című fejezetben!

Találgassunk! Ez egy állomás 32 bites IPv4-címe a hálózaton: 11000000.10101000.00001010.00001010. Bináris formában írtuk le. Ez ugyanannak a számítógépnek az IPv4-címe pontozott decimális formában: 192.168.10.10. Melyikkel dolgoznánk inkább? Az IPv6-címek 128 bit hosszúak. Ahhoz, hogy ezek a címek kezelhetőbbek legyenek, az IPv6 a hexadecimális számrendszer 0-9 és A-F értékeit használja.

Hálózati rendszergazdaként ismernünk kell a címek bináris és pontozott decimális alakja közötti átalakításokat oda és vissza. Azt is tudnunk kell, hogyan lehet a pontozott decimális alakot hexadecimálissá alakítani és fordítva. (Tipp: A bináris konverziós tudásunkra is szükségünk lesz, hogy ez sikerüljön.)

Meglepő módon ez nem is olyan nehéz, ha megtanulunk néhány trükköt. A fejezet tartalmaz egy Bináris játék (Binary Game) nevű feladatot, ami valóban segít az elindulásban. Szóval, mire várunk?

5.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Számrendszerek

**Fejezet célja:** Decimális, bináris és hexadecimális számrendszerek közötti átváltások számítása.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Kettes (bináris) számrendszer** | Számok átváltása decimális és bináris számrendszer között. |
| **Tizenhatos (hexadecimális) számrendszer** | Számok átváltása decimális és hexadecimális számrendszer között. |

[4.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[5.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kettes (bináris) számrendszer](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                   
*                       

1. Számrendszerek
2. Bevezetés

# Bevezetés

5.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Számrendszerek című fejezetben!

Találgassunk! Ez egy állomás 32 bites IPv4-címe a hálózaton: 11000000.10101000.00001010.00001010. Bináris formában írtuk le. Ez ugyanannak a számítógépnek az IPv4-címe pontozott decimális formában: 192.168.10.10. Melyikkel dolgoznánk inkább? Az IPv6-címek 128 bit hosszúak. Ahhoz, hogy ezek a címek kezelhetőbbek legyenek, az IPv6 a hexadecimális számrendszer 0-9 és A-F értékeit használja.

Hálózati rendszergazdaként ismernünk kell a címek bináris és pontozott decimális alakja közötti átalakításokat oda és vissza. Azt is tudnunk kell, hogyan lehet a pontozott decimális alakot hexadecimálissá alakítani és fordítva. (Tipp: A bináris konverziós tudásunkra is szükségünk lesz, hogy ez sikerüljön.)

Meglepő módon ez nem is olyan nehéz, ha megtanulunk néhány trükköt. A fejezet tartalmaz egy Bináris játék (Binary Game) nevű feladatot, ami valóban segít az elindulásban. Szóval, mire várunk?

5.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Számrendszerek

**Fejezet célja:** Decimális, bináris és hexadecimális számrendszerek közötti átváltások számítása.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Kettes (bináris) számrendszer** | Számok átváltása decimális és bináris számrendszer között. |
| **Tizenhatos (hexadecimális) számrendszer** | Számok átváltása decimális és hexadecimális számrendszer között. |

[4.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[5.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kettes (bináris) számrendszer](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                            
*                       

1. Számrendszerek
2. Kettes (bináris) számrendszer

# Kettes (bináris) számrendszer

5.1.1

## Bináris értékek és IPv4-címek

Az IPv4-címek bináris formában jelennek meg, csak 1-es és 0-ás számjegyek sorozataként. Ezt a formát nehéz kezelni, ezért a hálózati rendszergazdáknak decimális formába kell átváltaniuk őket. A témakör számos lehetőséget mutat erre.

A bináris egy olyan számrendszer, amely a biteknek nevezett 0 és 1 számjegyekből áll. Ezzel szemben a tízes számrendszer 10 számjegyből (0-9) áll.

A bináris értékek megértése fontos számunkra, mert az állomások, szerverek és hálózati eszközök bináris címzést használnak. Pontosabban bináris IPv4-címeket használnak egymás azonosítására, ahogy az ábrán is látható.

There is a central router with two LANs directly connected and one WAN connected to a cloud. Each LAN has a switch and a PC. The WAN has one PC. Each device has an IPv4 address that is in dotted binary notation instead of dotted decimal notation.

PC1 PC2 11000000.10101000.00001010.00001010 11000000.10101000.00001011.00001010 11000000.10101000.00001010.00000001 11000000.10101000.00001011.00000001 G0/0/0 G0/0/1 11010001.10100101.11001000.11100001 PC1 R1

PC2

**LAN A Network Address**  
11000000.10101000.00001010.00000000 /24**LAN B Network Address**  
11000000.10101000.00001011.00000000 /24

Minden cím 32 bit hosszúságú, és négy, oktettnek nevezett részre van felosztva. Minden oktett 8 bitet (vagyis 1 bájtot) tartalmaz, ezek ponttal vannak elválasztva egymástól. Például az ábrán szereplő PC1 IPv4-címe a 11000000.10101000.00001010.00001010. Az alapértelmezett átjárójának címe az R1 Gigabit Ethernet interfésze lesz, vagyis a 11000000.10101000.00001010.00000001.

A bináris alak jól működik állomások és hálózati eszközök esetén. Viszont az emberek számára nagy kihívást jelent a vele történő munkavégzés.

Hogy az emberek számára is könnyű legyen a használata, az IPv4-címeket általában pontozott decimális jelöléssel írják le. Az ábrán látható, hogy a PC1-hez a 192.168.10.10 IPv4-cím van rendelve, az alapértelmezett átjárójának címe pedig 192.168.10.1.

This diagram is the same as the first, a central router with two LANs and a WAN connected to a cloud. This has the same devices as the first diagram; however, instead of having the IPv4 addressing in binary, it is in dotted decimal notation.

PC1 PC2 192.168.10.10 192.168.11.10 192.168.10.1 192.168.11.1 G0/0/0 G0/0/1 209.165.200.225 PC1 R1

PC2

**LAN A Network Address**  
192.168.10.0 /24**LAN B Network Address**  
192.168.11.0 /24

A hálózati címzés alapos megértéséhez ismernünk kell a címek bináris alakját és gyakorlati készségeket kell szereznünk az IPv4-címek bináris és pontozott decimális alakja közötti átváltásban. Ez a rész a kettes (bináris) és a 10-es (decimális) számrendszerek közötti átváltási módokat ismerteti.

5.1.2

## Videó - Bináris és decimális számrendszerek közötti átváltás

A bináris és decimális számrendszerek közötti átváltásokat bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

5.1.3

## Bináris helyiértékes ábrázolás

A binárisból decimálisba történő átalakításhoz szükség van a helyiérték fogalmának megértésére. A helyiérték azt jelenti, hogy egy számjegy különböző értékeket képvisel attól függően, hogy melyik helyen áll a számon belül. Már tudjuk, hogy a leggyakoribb számrendszer a tízes (10-es alapú).

A tízes helyiértékes rendszer a táblázatban leírtak szerint működik.

| Radix10101010Position in Number3210Calculate(103)(102)(101)(100)Position value1000100101 | | | | |
| --- | --- | --- | --- | --- |
| **Alapszám** | **10** | **10** | **10** | **10** |
| A számon belüli pozíció | 3 | 2 | 1 | 0 |
| Számított érték | (103) | (102) | (101) | (100) |
| Helyiérték | 1000 | 100 | 10 | 1 |

A következő felsorolás elemei a táblázat sorait írják le.

* 1. sor, Az alapszám értéke. A decimális jelölés 10-es alapú, ezért az alapszám a 10.
  2. sor, A szám pozíciója a decimális érték helyét adja meg jobbról balra tekintve, 0 (1. pozíció), 1 (2. pozíció), 2 (3. pozíció), 3 (4. pozíció). Ezek a számok a 4. sor értékeinek kiszámításához használt exponenciális kitevőt is jelentik.
* A 3. sort úgy kapjuk, hogy vesszük az alapszámot, majd hatványozzuk a 2. sorban található értékre.   
  **MEGJEGYZÉS:** n0 = 1.
* A 4. sor helyiértéke az ezreseket, százasokat, tízeseket és egyeseket jelenti.

A helyiértékes rendszer használatához párosítsuk a számot a pozíciójához. A táblázatban látható példa bemutatja, hogyan használjuk a helyiértékes jelölést az 1234 decimális szám esetén.

| ThousandsHundredsTensOnesPositional Value1000100101Decimal Number (1234)1234Calculate1 x 10002 x 1003 x 104 x 1Add them up…1000+ 200+ 30+ 4Result1,234 | | | | |
| --- | --- | --- | --- | --- |
|  | **Ezresek** | **Százasok** | **Tízesek** | **Egyesek** |
| Helyiérték | 1000 | 100 | 10 | 1 |
| Decimális szám (1234) | 1 | 2 | 3 | 4 |
| Számított érték | 1 x 1000 | 2 x 100 | 3 x 10 | 4 x 1 |
| Adjuk össze őket... | 1000 | + 200 | + 30 | + 4 |
| **Eredmény** | **1.234** | | | |

Ezzel szemben a bináris helyiértékes jelölés a táblázatban leírtak szerint működik.

| Radix22222222Position in Number76543210Calculate(27)(26)(25)(24)(23)(22)(21)(20)Position value1286432168421 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Alapszám** | **2** | **2** | **2** | **2** | **2** | **2** | **2** | **2** |
| A számon belüli pozíció | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Számított érték | (27) | (26) | (25) | (24) | (23) | (22) | (21) | (20) |
| Helyiérték | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

A következő felsorolás elemei a táblázat sorait írják le.

* 1. sor, Az alapszám értéke. A bináris jelölés 2-es alapú, ezért az alapszám a 2.
  2. sor, A szám pozíciója a bináris érték helyét adja meg jobbról balra tekintve, 0 (1. pozíció), 1 (2. pozíció), 2 (3. pozíció), 3 (4. pozíció). Ezek a számok a 4. sor értékeinek kiszámításához használt exponenciális kitevőt is jelentik.
* A 3. sort úgy számítjuk ki, hogy vesszük az alapszámot, majd hatványozzuk a 2. sorban található értékre.   
  **MEGJEGYZÉS:** n0 = 1.
* A 4. sor helyiértéke az egyeseket, ketteseket, négyeseket, nyolcasokat stb. jelenti.

A táblázatban látható példa azt mutatja be, hogy az 11000000 bináris érték hogyan feleltethető meg a 192-es számnak. Ha a bináris érték az 10101000 lett volna, akkor a neki megfelelő decimális szám a 168 lenne.

| Positional Value 1286432168421 Binary Number (11000000)11000000 Calculate 1 x 1281 x 640 x 320 x 160 x 80 x 40 x 20 x 1 Add Them Up..128+ 64+ 0+ 0+ 0+ 0+ 0+ 0Result192 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Helyiérték** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| Bináris szám (11000000) | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Számított érték | 1 x 128 | 1 x 64 | 0 x 32 | 0 x 16 | 0 x 8 | 0 x 4 | 0 x 2 | 0 x 1 |
| Adjuk össze őket... | 128 | + 64 | + 0 | + 0 | + 0 | + 0 | + 0 | + 0 |
| **Eredmény** | **192** | | | | | | | |

5.1.4

## Tudáspróba - Bináris számrendszer

Az űrlap teteje

Check your understanding of binary number systems by choosing the correct answer to the following questions.

1. Which is the binary equivalent to the 192.168.11.10 IP address?

Az űrlap alja

Which of the following is the binary equivalent to the 172.16.31.30 IP address?

5.1.5

## Átváltás binárisról decimálisra

Ha egy IPv4-cím bináris alakját pontozott decimális formára szeretnénk átalakítani, akkor osszuk fel a címet négy 8 bites oktettre. Ezután határozzuk meg az első oktett bináris helyiértékeit, majd ennek megfelelően számításuk ki a számot.

Tegyük fel például, hogy az 11000000.10101000.00001011.00001010 egy állomás IPv4-címének bináris alakja. A bináris alak decimálisra történő alakításához kezdjük az első oktettel a táblázatban látható módon. Írjuk fel a 8 bites bináris számot az 1. sor helyiértékei alá, majd számoljuk ki a decimális eredményt: 192. Ez a szám kerül a pontozott decimális jelölés első oktettjébe.

| Positional Value 1286432168421 Binary Number (11000000)11000000Calculate1286432168421 Add Them Up...128+ 64+ 0+ 0+ 0+ 0+ 0+ 0Result192 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Helyiérték** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| Bináris szám (11000000) | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Számított érték | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Adjuk össze őket... | 128 | + 64 | + 0 | + 0 | + 0 | + 0 | + 0 | + 0 |
| **Eredmény** | **192** | | | | | | | |

Ezután váltsuk át a második oktettet (10101000) is a táblázatban látható módon. A kapott decimális érték a 168 és a második oktettbe kerül.

| Positional Value 1286432168421 Binary Number (11000000)10101000 Calculate 1286432168421 Add Them Up...128+ 0+ 32+ 0+ 8+ 0+ 0+ 0 Result 168 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Helyiérték** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| Bináris szám (10101000) | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| Számított érték | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Adjuk össze őket... | 128 | + 0 | + 32 | + 0 | + 8 | + 0 | + 0 | + 0 |
| **Eredmény** | **168** | | | | | | | |

Váltsuk át a harmadik oktettet (00001011) a táblázatban látható módon.

| Positional Value 1286432168421 Binary Number (11000000)00001011 Calculate 1286432168421 Add Them Up...0+ 0+ 0+ 0+ 8+ 0+ 2+ 1 Result 11 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Helyiérték** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| Bináris szám (00001011) | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| Számított érték | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Adjuk össze őket... | 0 | + 0 | + 0 | + 0 | + 8 | + 0 | + 2 | + 1 |
| **Eredmény** | **11** | | | | | | | |

Váltsuk át a negyedik oktettet is (00001010) a táblázatban látható módon. Ezzel létrejön a teljes IP-cím, vagyis a **192.168.11.10**.

| Positional Value1 286432168421 Binary Number (11000000)00001010 Calculate 1286432168421Add Them Up...0+ 0+ 0+ 0+ 8+ 0+ 2+ 0 Eredmény 10 | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Helyiérték** | **128** | **64** | **32** | **16** | **8** | **4** | **2** | **1** |
| Bináris szám (00001010) | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| Számított érték | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Adjuk össze őket... | 0 | + 0 | + 0 | + 0 | + 8 | + 0 | + 2 | + 0 |
| **Eredmény** | **10** | | | | | | | |

5.1.6

## Activity - Binary to Decimal Conversions

Utasítások

Ebben a feladatban 8 bites bináris értékek decimálisra történő átváltását gyakorolhatjuk szükség szerint. Ajánlott a feladatokat egészen addig gyakorolni, amíg hiba nélkül meg tudjuk oldani az átváltásokat. Váltsuk át az oktettben megadott bináris számot a decimális megfelelőjére!

Enter decimal answer below.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Decimal Value |  | | | | | | | | |
| Base | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |  |
| Exponent | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |  |
| Position | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |  |
| Bit | **1** | **1** | **0** | **1** | **1** | **1** | **0** | **1** |  |

Binary number.

5.1.7

## Átváltás decimálisból binárisba

Fontos ismerni azt is, hogyan lehet egy pontozott decimális formátumú IPv4-címet binárissá alakítani. Ennek egy hasznos eszköze a bináris helyiérték táblázat.

Kattintsunk minden helyiértékre a 128-tól kezdve, és haladjunk balról jobbra az 1-es helyiértékig.

Az oktett decimális értéke (n) nagyobb vagy egyenlő, mint a legnagyobb helyiértékű bit (**128**)?

* Ha nem, akkor írjuk be a bináris **0** értéket a **128** helyiértékhez.
* Ha igen, akkor írjunk be egy bináris **1**-et a **128** helyiértékhez, és vonjunk ki **128**-at a decimális számból.

The graphic shows a table that has 8 columns for one Byte or 8 bits. The top row shows the values from left to right; 128, 64, 32, 16, 8, 4, 2, 1. To the left of this top line are the words Positional Value. The bottom row is blank, but field under 128 is highlighted when selecting the 128 tab. Above the table is a flow chart that has only one proposition n > or = 128. No is to the left and Yes is to the right. There is a line going from the proposition in the center, one line to the left and one line to the right. The line moves across the top and then once it clears the chart, the line points straight down. On the No side or the left is a box with Add zero in it and a new line points to the highlighted field. On the right or Yes side the box has Add one. The line then continues and points to the highlighted field under 128. Under the Add one box is another line that points down to another box that has n - 128. Where the original number will subtract 128 from it and then consider the next column with 64.

128 64 32 16 8 4 2

1

No*n* >= 128YesPositional ValueAdd 0Add 1*n* - 128

5.1.8

## Példa decimálisból binárisba történő átváltásra

A művelet elvégzéséhez használjuk a 192.168.10.11 IP-címet.

Az első oktett (192) értékét a korábban ismertetett helyiértékes műveletsor használatával alakítjuk át binárissá.

Egyszerűbb vagy kisebb decimális számokkal lehetőség van a kivonási művelet elkerülésére. Vegyük észre például, hogy a harmadik oktett bináris számmá alakítását elég könnyű elvégezni anélkül, hogy ténylegesen végigmennénk a kivonási műveleteken (8 + 2 = 10). A harmadik oktett bináris értéke: 00001010.

A negyedik oktett a 11 (8 + 2 + 1). A negyedik oktett bináris értéke: 00001011.

A bináris és decimális számok közötti átváltás először bonyolultnak tűnhet, de a gyakorlatban idővel egyszerűbbé válik.

A 192.168.10.11 IP-cím binárissá alakításának megtekintéséhez kattintsunk az egyes lépésekre!

Az első oktett értéke (192) legalább akkora, mint a legmagasabb helyiértékű bit (128)?

* Igen, ezért írjunk be 1-et a legmagasabb helyiértékhez (128).
* Vonjuk ki a 192-ből a 128-at, a maradék a 64.

When selecting the Step 1 button, the graphic states Example: 192.168.10.11 with 192 in a different color. To the Right of that is a diamond that states: 192 > or = 128. There is a Yes on the right side of the diamond. A table is shown below that contains 8 columns for one Byte or 8 bits. The top row shows the values from left to right: 128, 64, 32, 16, 8, 4, 2, and 1 with the words Positional Value to the left. The bottom row field under 128 is highlighted. Above the table, from the flow chart diamond with Yes is to the right is line that moves across the top and then once it clears the chart, the line points straight down to a box that has Add one. The line then continues under the chart and points to the highlighted field under 128. Under the Add one box is another line that points down to another box that has 192 - 128 = 64. There is also a 1 under the 128 in the highlighted field; the other columns are still blank on this line.

1 128 64 32 16 8 4 2

1

Example: 192.168.10.11YesPositional Value192 >= 128192 - 128 = 64Add 1

5.1.9

## Activity - Decimal to Binary Conversions

Utasítások

Ebben a feladatban decimális számok 8 bites bináris értékre történő átváltását gyakorolhatjuk. Ajánlott a feladatokat egészen addig gyakorolni, amíg hiba nélkül meg tudjuk oldani az átváltásokat. Váltsuk át a megadott decimális számot a bináris megfelelőjére!

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Decimal Value | **173** | | | | | | | | |
| Base | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |  |
| Exponent | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |  |
| Position | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |  |
| Bit |  |  |  |  |  |  |  |  |  |

5.1.10

## Feladat - Bináris játék

Ez egy szórakoztató módja annak, hogy megtanuljuk a hálózatokban használt bináris számokat.

A **játék** linkje: <https://learningnetwork.cisco.com/docs/DOC-1803>

A hivatkozás használatához be kell jelentkeznünk a cisco.com oldalra. Ha még nincs fiókunk, létre kell hoznunk egyet.

5.1.11

## IPv4-címek

Ahogy a fejezet elején említettük, a routerek és a számítógépek csak bináris értékeket tudnak értelmezni, míg az emberek decimális számokkal dolgoznak. Fontos, hogy alaposan megértsük ezt a két számrendszert és a hálózatban történő használatukat.

A pontozott decimális cím és a 32 bites cím összehasonlításához kattintsunk az egyes gombokra!

A számítógéphez rendelt IP-cím a 192.168.10.10.

The graphic shows the numbers 192.168.10.10 with the binary in an orange box around the dotted decimal numbers 192.168.10.10. 11000000 is under 192 in the first octet, 10101000 under 168 in the second octet, 00001010 under 10 in the third octet, and 00001010 under the last 10 in the fourth octet.

11000000 10101000 00001010 00001010 192 168 10 10 . . . 11000000 10101000 00001010 00001010 192 168 10 10 . .

.

[5.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[5.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Tizenhatos (hexadecimális) számrendszer](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                               
*                       

1. Számrendszerek
2. Tizenhatos (hexadecimális) számrendszer

# Tizenhatos (hexadecimális) számrendszer

5.2.1

## Hexadecimális értékek és IPv6-címek

Most már tudjuk, hogyan lehet binárisból decimálisba és decimálisból binárisba átváltani. Erre a tudásra IPv4-címzést használó hálózatban van szükség. Viszont az IPv6-címek használatának is ugyanekkora a valószínűsége egy hálózatban. Az IPv6-címzés megértéséhez képesnek kell lennünk hexadecimálisból decimálisba és visszafelé irányú átváltásokra.

Ahogy a decimális egy tízes alapú, úgy a hexadecimális egy tizenhatos alapú rendszer. A tizenhatos alapú számrendszer 0 és 9 közötti számokat, valamint A és F közötti betűket használ. Az ábra a 0000-1111 közötti bináris értékek decimális és hexadecimális megfeleltethetőségét ábrázolja.

This graphic has three columns. The first column has the numbers 0 through 15 in decimal. The second column has the numbers 0 through 15 in binary. All of the numbers in binary are expressed with 4 place values. For example 0 is 0000, 10 is 1010, 15 is 1111, etc. The third column is parallel with the other two columns. This column has the numbers 0 through 15 in hexadecimal. These are expressed with one value. For example 5 is 5, 10 is A, 11 is B, 12 is C, 13 is D, 14 is E, and 15 is F. It should be noted that these may be expressed with upper or lower case. In this diagram they are all upper case letters representing the numeric values.

0 15 3 4 5 6 7 8 9 10 11 12 13 14 2 1 0000 1111 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 0010 0001 0 F 3 4 5 6 7 8 9 A B C D E 2

1

DecimalBinaryHexadecimal

A bináris és hexadecimális értékek jól együttműködnek, mert könnyebb egy értéket egyetlen hexadecimális számjeggyel kifejezni, mint négy darab binárissal.

A hexadecimális számrendszert a hálózatokban az IPv6-címek és az Ethernet MAC-címek megjelenítésére használják.

Az IPv6-címek 128 bit hosszúak, és minden négy bit egy hexadecimális számjegyet ad ki, így a cím 32 hexadecimális számjegyből áll. Az IPv6-címek esetén nem különböztetjük meg a kis- és nagybetűket, bármelyiket használhatjuk.

Ahogy az ábrán látjuk, az IPv6-címek preferált formátuma x:x:x:x:x:x:x:x, ahol minden "x" négy hexadecimális értéket helyettesít. Az IPv4-címek 8 bites részeit oktettnek hívtuk. Az IPv6 esetén egy 16 bites címrész, vagyis négy hexadecimális számjegy nem hivatalos elnevezése hextett. Minden "x" egy-egy hextettet, azaz 16 bitet, vagyis négy hexadecimális számjegyet jelent.

This graphic has a top line with the 8 hextets of the IPv6 address expressed as X:X:X:X:X:X:X:X. Beneath each X are the numbers 0000 representing the first number that can be in this field below each 0 is the to and below that are the lower case numbers ffff representing the maximum value that can be made in a single hextet. Under the X in the fourth hextet is an orange arrow pointing to the numbers 0000 to ffff, which are in a box. Under the box is another arrow point down to to a section of numbers. At the center of the arrow is the statement 4 hexadecimal digits = 16 binary digits. Under the arrow are a section of numbers with four parts. Each of the four parts has 0000 under that the word to under that the numbers 1111. This is to represent the binary of each hexadecimal number, since each number is made of 4 binary digits and there are 4 hexadecimal digits in each hextet for a total of 16 bits.

X : X : X : X : X : X : X : X 0000 0000 0000 0000 0000 0000 0000 0000 ffff ffff ffff ffff ffff ffff ffff ffff : : : : : : : 1111 1111 1111 1111 0000 0000 0000

0000

**4 hexadecimal digits = 16 binary digits**totototototototototototo

Az ábrán látható minta topológia IPv6 hexadecimális címeket jelenít meg.

This graphic displays a central router labeled R1. Out of G0/0 interface is the first LAN to the left. A switch is connected directly to the router R1 and PC1 is connected to the left of the switch. Above this LAN is the IPv6 Network segment address of 2001:db8:acad:1::/64. On the G0/0 interface is assigned :1 and :10 is assigned to PC1. Below G0/0 and also to the left on R1 is the G0/1 interface for the second LAN. A switch is connected directly to the routers G0/1 and PC2 is connected to the left of this switch. Above this LAN is the IPv6 Network segment address of 2001:db8:acad:2::/64. On the G0/1 interface is assigned :1 and :10 is assigned to PC2. On the right side of R1 is the S0/0/0 interface and it is connected to a cloud. Above the red serial cable that is connected to the cloud is the IPv6 address 2001:db8:acad:3::/64. The S0/0/0 interface has been assigned the :1 IPv6 address.

:10 :10 G0/0:1 S0/0/0 :1G0/1 2001:db8:acad:3::/64 2001:db8:acad:1::/64 2001:db8:acad:2::/64 PC1 PC2 :1

R1

5.2.2

## Videó - Hexadecimális és bináris számrendszerek közötti átváltás

A hexadecimális és bináris számrendszerek közötti átváltásokat bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

5.2.3

## Átváltás decimálisból hexadecimálisba

A decimális számok hexadecimális értékekre történő átváltása egyszerű feladat. Kövessük a felsorolt lépéseket:

1. Konvertáljuk a decimális számot 8 bites bináris karaktersorozattá.
2. Osszuk fel a bináris karakterláncot négyes csoportokra a jobb szélső bitpozíciótól kezdve.
3. Alakítsuk át az összes négy bites bináris számot a vele egyenértékű hexadecimális számjegyre.

A példa a **168** hexadecimálissá alakításának lépéseit mutatja be.

A háromlépcsős folyamat segítségével fogjuk az átváltást elvégezni.

1. **168** bináris alakja: **10101000.**
2. **10101000** négy bináris számjegyből álló két csoportja a **1010** és **1000**.
3. Az **1010** a hexadecimális **A**, az **1000** pedig a hexadecimális **8** értéket jelenti.

**A válasz**: A **168** hexadecimális alakja az **A8**.

5.2.4

## Átváltás hexadecimálisból decimálisba

A hexadecimális számok decimális értékekre történő átváltása szintén egyszerű. Kövessük a felsorolt lépéseket:

1. Alakítsuk a hexadecimális számot 4 bites bináris karaktersorozattá.
2. Hozzunk létre 8 bites bináris csoportokat a jobb szélső bitpozíciótól kezdve.
3. Alakítsuk át az összes 8 bites bináris csoportot a vele egyenértékű decimális számjegyre.

A példa a D2 decimálissá alakításának lépéseit mutatja be.

1. A **D2** 4 bites bináris karaktersorozat alakja az **1101** és **0010**.
2. **1101** és **0010** 8 bites csoportot alkotva **11010010**.
3. Az **11010010** bináris értéke a **210** decimális értéknek felel meg.

**A válasz**: A hexadecimális **D2** decimális alakja a **210**.

5.2.5

## Tudáspróba - Hexadecimális számrendszer

Az űrlap teteje

Check your understanding of hexadecimal number system by choosing the correct answer to the following questions.

1. Which is the hexadecimal equivalent of 202?

Az űrlap alja

Which is the hexadecimal equivalent of 254?

Which is the decimal equivalent of A9?

Which of the following is the decimal equivalent of 7D?

[5.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kettes (bináris) számrendszer](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[5.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                      

1. Számrendszerek
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

5.3.1

## Miről tanultunk ebben a fejezetben?

**Kettes (bináris) számrendszer**

A bináris egy olyan számrendszer, amely a biteknek nevezett 0 és 1 számjegyekből áll. Ezzel szemben a tízes számrendszer 10 számjegyből (0-9) áll. A bináris értékek ismerete fontos számunkra, mivel az állomások, szerverek és hálózati eszközök bináris címzéssel, konkrétan bináris IPv4-címekkel azonosítják egymást. Ismernünk kell a bináris címzést, valamint az IPv4-címek bináris és pontozott decimális alakja közötti átváltást. Ebben a fejezetben bemutatásra került néhány módszer a bináris és decimális értékek közötti átváltásokról.

**A tizenhatos (hexadecimális) számrendszer**

Ahogy a decimális egy tízes alapú, úgy a hexadecimális egy tizenhatos alapú rendszer. A tizenhatos alapú számrendszer számokat tartalmaz 0-tól 9-ig valamint betűket A-tól Z-ig. A hexadecimális számrendszert a hálózatokban az IPv6-címek és az Ethernet MAC-címek megjelenítésére használják. Az IPv6-címek 128 bit hosszúak, és minden négy bit egy hexadecimális számjegyet ad ki, így a cím 32 hexadecimális számjegyből áll. Hexadecimálisról decimálisra konvertálás esetén először a hexadecimális értéket binárissá kell alakítani, majd a binárist decimálissá. Decimálisról hexadecimálisra konvertáláskor először a decimálist kell binárissá konvertálni.

5.3.2

## Ellenőrző kvíz - Számrendszerek

Az űrlap teteje

1. Mi a bináris ábrázolása a 173 decimális számnak?

Az űrlap alja

Adott az 11101100 00010001 00001100 00001010 bináris cím. Melyik címet jelöli ez pontozott decimális formátumban?

Hány bináris bit van egy IPv6-címben?

Mennyi a decimális 232 bináris megfelelője?

Melyik két állítás igaz az IPv4 és IPv6-címekre? (Két jó válasz van.)

Melyik IPv4-címformátumot hozták létre az emberek számára a könnyű kezelhetőség érdekében, amit 201.192.1.14 formában adnak meg?

Mi a pontozott decimális értéke a következő IPv4-címnek: 11001011.00000000.01110001.11010011?

Mennyi az 10010101 bináris szám decimális értéke?

Mennyi a hexadecimális 0x3F értéke decimálisan?

Mi a 00001010.01100100.00010101.00000001 bináris karakterláncként ábrázolt IPv4-cím pontozott decimális ábrázolása?

Mi a 0xC9 decimális megfelelője?

Melyik érvényes hexadecimális számjegy?

Mi a 0xCA bináris ábrázolása?

How many bits are in an IPv4 address?

[5.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Tizenhatos (hexadecimális) számrendszer](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[6.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                          
*                     

1. Adatkapcsolati réteg
2. Bevezetés

# Bevezetés

6.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az Adatkapcsolati réteg című fejezetben!

Minden hálózatban találhatók fizikai összetevők, valamint átviteli közegek, amelyek összekötik őket. A különböző típusú adathordozók eltérő információkat igényelnek az adatokról ahhoz, hogy fogadják és továbbítsák őket a fizikai hálózaton. Gondolkodjunk így: egy jól elütött golflabda gyorsan és messzire mozog a levegőben. A vízben is képes lenne a mozgásra, a sebessége és a megtett távolság viszont kisebb lenne, amíg egy erőteljesebb ütés nem segítene rajta. Ez azért van, mert a golflabda egy másik közegen halad át; vízben a levegő helyett.

Az adatoknak segítségre van szükségük a különböző adathordozókon történő áthaladáshoz. Az adatkapcsolati réteg biztosítja ezt a segítséget. Ahogy sejthettük, ez a segítség számos tényezőben eltér egymástól. A fejezetben áttekintjük ezeket a tényezőket és az adatokra kifejtett hatásukat, valamint azokat a protokollokat, amelyek a sikeres kézbesítés biztosítására lettek tervezve. Vágjunk bele!

6.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Adatkapcsolati réteg

**Fejezet célja:** Az adatkapcsolati réteg közeghozzáférés vezérlésének bemutatása a hálózatok közötti kommunikációban.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Az adatkapcsolati réteg célja** | Az adatkapcsolati réteg céljának és funkciójának bemutatása a kommunikáció előkészítésében egy adott adathordozón történő továbbítás esetén. |
| **Topológiák** | WAN és LAN topológiákban használt közeghozzáférés-vezérlési módszerek jellemzőinek összehasonlítása. |
| **Adatkapcsolati keret** | Az adatkapcsolati keret jellemzőinek és funkcióinak bemutatása. |

[5.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[6.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az adatkapcsolati réteg célja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                             
*                     

1. Adatkapcsolati réteg
2. Az adatkapcsolati réteg célja

# Az adatkapcsolati réteg célja

6.1.1

## Az adatkapcsolati réteg

Az ábrán látható, hogy az OSI modell adatkapcsolati rétege (2. réteg) a hálózati adatokat készíti elő a fizikai hálózat számára. Az adatkapcsolati réteg felelős a hálózati kártyák (NIC) egymás közti kommunikációjáért. Az adatkapcsolati réteg a következőkkel foglalkozik:

* Lehetővé teszi a felsőbb rétegek számára a közeghez való hozzáférést. A felsőbb rétegbeli protokoll számára teljes mértékben ismeretlen, hogy az adatok továbbítása milyen adatátviteli közegen zajlik.
* Fogadja az adatokat, amelyek általában a 3. rétegbeli csomagok (például IPv4 vagy IPv6), majd beágyazza őket 2. rétegbeli keretekbe.
* Szabályozza, hogy milyen módon történjen az adatok közegre helyezése és fogadása.
* Keretek cseréjét végzi a végpontok között a közegen keresztül.
* Fogadja a beágyazott adatokat, amelyek általában 3. rétegbeli csomagok, és a megfelelő felsőbb rétegbeli protokollhoz irányítja őket.
* Hibakeresést hajt végre, és elutasítja a hibás kereteket.

The image shows the seven layers of the OSI model in order from the top down, Layer 7, Application, Layer 6 Presentation, Layer 5 Session, Layer 4 Transport, Layer 3 Network, Layer 2 Data Link, Layer 1 Physical. The data link layer is highlighted and next to the data link layer is text stating The data link layer prepares network data for the physical network. An arrow representing traffic flow from a user sitting above the application layer is drawn over the OSI model down to a router and ending at a network cloud.

7 6 5 4 3 2

1

ApplicationPresentationSessionTransportNetworkData LinkPhysicalNetworkThe data link layer prepares network data for the physical network

Számítógépes hálózatokban a csomópont olyan eszközt jelent, amely képes adatokat fogadni, létrehozni, tárolni vagy továbbítani egy kommunikációs útvonal mentén. A csomópont jelenthet végberendezést (pl. laptop vagy mobiltelefon) vagy közvetítő eszközt (pl. Ethernet switch).

Az adatkapcsolati réteg nélkül a hálózati réteg protokolljainak (például az IP-nek) kellene gondoskodnia az összes olyan közegtípushoz történő csatlakozásról, amely a szállítási útvonalon előfordulhat. Továbbá, minden egyes új hálózati technológia vagy közeg megjelenésekor az IP-t is tovább kellene fejleszteni.

Az ábrán egy példa látható arra, hogy az adatkapcsolati réteg milyen módon adja hozzá a 2. rétegbeli Ethernet cél- és forrás címadatokat egy 3. rétegbeli csomaghoz. Ezt követően átalakítja ezt az információt a fizikai réteg (azaz 1. réteg) által támogatott formátumba.

The image shows a user at a desktop computer with and IP address of 192.168.1.110 sending traffic from its NIC to the NIC of a Web Server with the IP address of 192.168.1.5. A box with the label L2, representing the Layer 2 header and a box with label L3 representing the Layer 3 header are shown by the user. An arrow from the L2 box points to a larger rectangular box with the text destination NIC and Source NIC to represent the destination Layer 2 address and the destination Layer 3 address. To the right of the L2 header is a rectangular box called L3 IP Packet which has text indicating the source IP address of 192.168.1.110 and the destination IP address of 192.168.1.5.

L2 HeaderL3 IP PacketDestination NICSource NICSource IP  
192.168.1.110Destination IP  
192.168.1.5 PC1  
192.168.1.110 Web Server  
192.168.1.5NIC NICL2L3L2 = Layer 2  
L3 = Layer 3

6.1.2

## IEEE 802 LAN/MAN adatkapcsolati alrétegek

Az IEEE 802 szabványcsalád LAN/MAN szabványai az Ethernet LAN-okra, a vezeték nélküli LAN-okra (WLAN), a vezeték nélküli személyes hálózatokra (WPAN) és a helyi és nagyvárosi hálózatok egyéb típusaira vonatkoznak. Az IEEE 802 LAN/MAN adatkapcsolati rétege a következő két alrétegből áll:

* **Logikai kapcsolatvezérlés (Logical Link Control, LLC)**- Ez az alréteg kommunikál a felsőbb rétegek hálózati szoftverei és az alsóbb rétegek hardverei között. Információkat helyez el a keretben annak a hálózati rétegbeli protokollnak az azonosítására, amelyik a keretet használni fogja. Ez az információ lehetővé teszi, hogy több 3. rétegbeli protokoll (pl. IPv4 és IPv6) is ugyanazt a hálózati interfészt és közeget használja.
* **Közeghozzáférés vezérlés (Media Access Cotrol, MAC)**— Ezt az alréteget (IEEE 802.3, 802.11 vagy 802.15) hardveres formában valósítják meg. Az adatbeágyazásért és a közeghozzáférés vezérlésért felelős. Az adatkapcsolati réteg címzését biztosítja, és a különböző fizikai rétegbeli technológiákkal építették egybe.

Az ábrán az adatkapcsolati réteg két alrétege (LLC és MAC) látható.

The image is of a table with three rows for Network, Data Link, and Physical layers. The top row of the table has Network and Network Layer Protocol. The second row has Data link and is furthur split into two rows, one for LLC Sublayer and one for MAC Sublayer. The LLC Sublayer has a column stating LLC Sublayer - IEEE 802.2.The MAC Sublayer has three columns stating Ethernet IEEE 802.3, WLAN 802.11, and WPAN IEEE 802.15. Under the Ethernet 802.3 column, between the MAC sublayer and the Physical layer it states Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc. Under the WLAN IEEE 802.11 column, between the MAC sublayer and the Physical layer it states Various WLAN standards for different types of wireless communications. Under the WPAN column between the MAC sublayer and the Physical layer it states Various WPAN standards for Bluetooth, RFID, etc.

Network Layer ProtocolNetworkData LinkLLC Sublayer - IEEE 802.2LLC SublayerMAC SublayerEthernet   
IEEE 802.3WLAN   
IEEE 802.11WPAN   
IEEE 802.15Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.Various WLAN standards for different types of wireless communicationsVarious WPAN standards for Bluetooth, RFID, etc.Physical

Az LLC-alréteg fogadja a hálózati protokoll adatait (ami jellemzően egy IPv4 vagy IPv6 csomag ) és olyan 2. rétegbeli vezérlő információkkal látja el, amelyek segítik a csomag célállomáshoz történő eljuttatását.

A MAC alréteg vezérli a hálózati kártyát és más hardvereket, amelyek a vezetékes vagy vezeték nélküli LAN/MAN közegen történő adatküldésért és fogadásért felelősek.

A MAC alréteg biztosítja az adatbeágyazást:

* **Kerethatárolás** - A keretezési folyamat fontos határolókat biztosít a kereten belüli mezők azonosításához. Ezek a határoló bitek biztosítják a szinkronizációt az adó és a vevő csomópontok között.
* **Címzés** - Biztosítja a forrás- és célcímeket a 2. rétegbeli keret továbbításához a megosztott közeg eszközei között.
* **Hibadetektálás** - Tartalmaz egy keret lezáró részt, amelyet az átviteli hibák észlelésére használnak.

A MAC alréteg közeghozzáférés-vezérlést is biztosít, amely több eszköz számára is lehetővé teszi egy megosztott (fél-duplex) közegen keresztül történő kommunikációt. A teljes duplex kommunikáció nem igényel hozzáférés-vezérlést.

6.1.3

## Közeghozzáférés biztosítása

A csomagok a helyi állomástól a távoli állomás felé tartó útjuk során számos, különböző tulajdonságokkal rendelkező hálózati környezettel találkozhatnak. Az Ethernet hálózat például az átviteli közeg használatáért versengő állomásokból áll. A MAC alréteg végzi ennek megvalósítását. Soros kapcsolatok esetén a hozzáférési mód mindössze két eszköz (általában routerek) közötti közvetlen összeköttetésből áll. Ezért itt nincs szükség az IEEE 802 MAC alrétegben alkalmazott technikákra.

A router interfészei a megfelelő keretbe ágyazzák be a csomagot. Mindegyik összeköttetéshez a neki megfelelő közeghozzáférés-vezérlési módszer van használatban. A hálózati rétegbeli csomagok továbbítása során többször változhat az adatkapcsolati réteg és az átviteli közeg.

A router a következő 2. rétegbeli funkciókat hajtja végre minden egyes ugrásnál az útvonal mentén:

1. Fogadja a keretet a közegtől.
2. Kibontja a keretet.
3. A csomagot egy új keretbe ágyazza be.
4. Továbbítja az új keretet a hálózati szegmens közegének megfelelő formában.

Kattintsunk a lejátszás gombra az animáció megtekintéséhez! Az ábrán látható router Ethernet interfésze egy LAN-hoz, a soros interfésze pedig egy WAN hálózathoz csatlakozik. A router a keretek feldolgozásakor az adatkapcsolati réteg szolgáltatásaira támaszkodik, amikor fogadja a keretet az egyik közegtől, kibontja a keretből a 3. rétegbeli adategységet, újra keretbe ágyazza azt, majd az új keretet a kimeneti vonal közegére helyezi.

This animation illustrates how a Layer 2 frame is encapsulated and de-encapsulated as it travels in a network. A user sends an Ethernet frame to the default gateway router. When the router receives the frame, it decapsulates the Ethernet frame to read its content. It then processes the Layer 3 packet and makes a routing decision to choose a serial interface as the exit interface to the next hop IP address. The router then re-encapsulate the packet into a new Layer 2 frame and sends it to the next router across the serial link.

LAN Header

Packet

LAN Trailer

WAN Trailer

WAN Header

Serial Connection

The data link layer is responsible for controlling the transfer of frames across the media.

Ethernet Connection

6.1.4

## Az adatkapcsolati réteg szabványai

A TCP/IP modell felsőbb rétegeiben található protokollokkal ellentétben, az adatkapcsolati réteg protokolljait általában nem RFC (Request for Comments) dokumentumokban definiálják. Az Internet Mérnöki Munkacsoport (Internet Engineering Task Force, IETF) felelős a TCP/IP felsőbb rétegeiben működő protokollok és szolgálatatások karbantartásáért, a hálózatelérési réteg működését és feladatait viszont már nem ez a szervezet szabályozza.

A hálózatelérési rétegre (pl. OSI modell fizikai és adatkapcsolati rétege) vonatkozó nyílt szabványokat és protokollokat létrehozó mérnöki szervezetek az alábbiak:

* Mérnököket egyesítő nemzetközi szervezet (Institute of Electrical and Electronics Engineers, IEEE)
* Nemzetközi Távközlési Szövetség (International Telecommunication Union, ITU)
* Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO)
* Amerikai Nemzeti Szabványügyi Intézet (American National Standards Institute, ANSI)

Az ábrán ezen szervezetek logói láthatók.

### Mérnöki szervezetek logói



6.1.5

## Tudáspróba - Az adatkapcsolati réteg célja

Az űrlap teteje

Check your understanding of the data link layer by choosing the BEST answer to the following questions.

1. What is another name for the OSI data link layer?

Az űrlap alja

The IEEE 802 LAN/MAN data link layer consists of which two sublayers? (Choose two.)

What is the responsibility of the MAC sublayer?

What Layer 2 function does a router perform? (Choose three.)

The media access control method used depends on which two criteria?

Which organization defines standards for the network access layer (i.e., the OSI physical and data link layers)?

[6.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[6.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Topológiák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                    
*                     

1. Adatkapcsolati réteg
2. Topológiák

# Topológiák

6.2.1

## Fizikai és logikai topológiák

Az előző témakörben megtanultuk, hogy az adatkapcsolati réteg készíti elő az adatokat a fizikai hálózat számára. Ismernie kell a hálózat logikai topológiáját annak érdekében, hogy meg tudja határozni, mi szükséges a keretek egyik eszközről a másikra történő átviteléhez. Ebben a témakörben bemutatásra kerül, hogy az adatkapcsolati réteg milyen módon működik a különböző logikai topológiákban.

A hálózat topológiája a hálózati eszközök elrendezését és a köztük lévő összeköttetéseket jelenti.

A LAN és WAN hálózatok leírására kétféle topológiát használnak:

* **Fizikai topológia** – A fizikai összeköttetéseket, valamint a végberendezések és a közvetítő eszközök (pl.: routerek, switchek és vezeték nélküli hozzáférési pontok) kapcsolódási módját határozza meg. A topológia tartalmazhatja egy adott eszköz helyét is, például a helyiség számát és a rack szekrényben elfoglalt helyét. A fizikai topológia általában pont-pont vagy csillag típusú.
* **Logikai topológia** - Arra utal, hogy a hálózat miként szállítja a kereteket egyik állomástól a másikig. Ez a topológia azonosítja a virtuális kapcsolatokat eszközinterfészekkel és 3. rétegbeli IP-címzési sémák használatával.

Az adatkapcsolati réteg a hálózat logikai topológiáját figyeli a közeghozzáférés vezérlése közben. A logikai topológia befolyással van a keretezés típusára és a használt közeghozzáférési módra.

Az ábrán egy kis mintahálózat **fizikai** topológiája látható.

The physical network topology shows six rooms, each highlighted in a light yellow box, with various networking devices and cabling. On the left side is the server room labeled room 2158. It contains a router labeled R1 mounted on rack 1 shelf 1 with six cable connections. A cable at the top connects to a cloud labeled Internet. A cable to the left connects to a switch labeled S1 mounted on rack 1 shelf 2. S1 is connected to three servers: a web server mounted on rack 2 shelf 1, an email server mounted on rack 2 shelf 2, and a file server mounted on rack 2 shelf 3. A cable connected to the bottom of R1 connects to a switch labeled S2 mounted on rack 1 shelf 3. S2 has two connections leading to a printer and a PC in the IT office labeled room 2159. R1 has three cables to the right connected to three switches located in room 2124. The top switch is labeled S3 and mounted on rack 1 shelf 1. The middle switch is labeled S4 and mounted on rack 1 shelf 2. The bottom switch is labeled S5 and mounted on rack 1 shelf 3. S3 has a cable on the left connected to a laptop in a room labeled class 1 room 2125. S4 has a cable on the left connected to a laptop in a room labeled class 2 room 2126. S5 has a cable on the left connected to a laptop in a room labeled class 3 room 2127.

### Fizikai topológia

R1 S1 S2 S3 S4

S5

InternetEmail Server  
Rack 2  
Shelf 2Web Server  
Rack 2  
Shelf 1File Server  
Rack 2  
Shelf 3Rack 1  
Shelf 2Rack 1  
Shelf 1Rack 1  
Shelf 2Rack 1  
Shelf 1Rack 1  
Shelf 3Rack 1  
Shelf 3**Server Room: Rm: 2158IT Office: Rm: 2159** **Class 1: Rm: 2125Class 2: Rm: 2126Class 3: Rm: 2127Rm: 2124**

A következő ábrán az előző mintahálózat **logikai** topológiája látható.

The logical network topology shows devices, port labels, and the network addressing scheme. In the middle of the picture is a router labeled R1. A port labeled G0/0/0 connects to a cloud at the top labeled Internet. A port labeled G0/2/0 connects at the left to a switch labeled S1 at port G0/1. S1 is connected to three servers. S1 and the servers are highlighted in a light yellow circle with the network 192.168.10.0/24 written at the top. Port F0/1 on S1 connects to a web server. Port F0/2 on S1 connects to an email server. Port F0/3 on S1 connects to a file server. Port G0/0/1 on R1 connects at the bottom to a switch labeled S2. S2 connects to a printer and a PC, all of which are highlighted in a light yellow circle with the network 192.168.11.0/24 written on the bottom. At the right of R1 are three additional connections, each connecting to a switch at port G0/1 which is then connected to a laptop at port F0/1. Each switch and laptop are highlighted in yellow and the network address shown. Port G0/0/1 of R1 connects at the top to a switch labeled S3 on network 192.168.100.0. Port G0/1/0 of R1 connects in the middle to a switch labeled S4 on network 192.169.101.0. Port G0/1/1 on R1 connects at the bottom to a switch labeled S5 on network 192.168.102.0. R1 connects to the Internet on interface G0/0/0.

### Logikai topológia

R1 F0/1 F0/2 F0/3 G0/0/0 G0/1 G0/0/1 G0/1 G0/1/0 G0/1/1 G0/1 S1 S2 S3 S4 S5 G0/2/0 G0/2/1 G0/1

G0/1

InternetEmail ServerWeb ServerFile Server**Network  
192.168.10.0/24Network  
192.168.11.0/24Network 192.168.100.0/24Network 192.168.101.0/24Network 192.168.102.0/24**

6.2.2

## WAN topológiák

Az ábrákon a WAN-ok általános kapcsolódási módjai láthatók három gyakori fizikai WAN topológia használatával.

További információért kattintsunk a gombokra!

Ez a legegyszerűbb és leggyakoribb WAN topológia. Két végpont közötti állandó kapcsolatból áll.

The image shows two routers with a single line, representing a link, connecting them.

A hibrid topológiát ezen topológiák variációja vagy kombinációja alkotja. A részleges háló például egy hibrid topológia, amelyben néhány, de nem az összes végberendezés kapcsolódik egymáshoz.

6.2.3

## Pont-pont WAN topológia

A fizikai pont-pont összeköttetések közvetlenül két végpontot kapcsolnak össze egymással az ábrán látható módon. Ebben az elrendezésben a két végpontnak nem kell más állomásokkal megosztozniuk a közegen. Továbbá, soros kommunikációs protokoll, például pont-pont protokoll (Point-to-Point Protocol, PPP) használatakor az állomásnak nem kell eldöntenie, hogy a beérkező keretet neki vagy egy másik csomópontnak szánták. Emiatt a logikai adatkapcsolati protokollok nagyon egyszerű felépítésűek is lehetnek, hiszen a keretek csak a két állomás egyikének lehetnek címezve vagy csak tőlük származhatnak. A kereteket a pont-pont kapcsolat egyik végén az állomás ráhelyezi a közegre, majd a túlsó végén lévő másik állomás leveszi azokat.

The image shows a point-to-point network example consisting of two routers, labeled Node 1 and Node 2, each connected to a network cloud over WAN links.

Node 1Node 2Network

A pont-pont topológiák két végpontra korlátozódnak.

**MEGJEGYZÉS**: Etherneten keresztül történő pont-pont kapcsolat használatakor az eszköznek meg kell határoznia, hogy a bejövő keretet neki címezték-e.

A forrás- és célállomás közvetve, nagy földrajzi távolságok áthidalásával kapcsolódik egymáshoz számos közvetítő eszköz használatával. Ahogy az ábra is mutatja, a hálózatban használt fizikai eszközök nincsenek befolyással a logikai topológiára. Az ábrán új közvetítő fizikai kapcsolatok hozzáadása nem változtatja meg a logikai topológiát. A logikai pont-pont kapcsolat ugyanaz marad.

The image shows a point-to-point network example consisting of two routers, labeled Source Node and Destination Node, each connected to a network cloud over WAN links. The two routers are shown sending frames to the network cloud.

Source  
NodeFrameFrameFrameFrameDestination  
Node

6.2.4

## LAN topológiák

A többes hozzáférésű helyi hálózatokban a végberendezések (azaz csomópontok) csillag- vagy kiterjesztett csillag topológiákkal vannak összekapcsolva, ahogy az ábrán is látható. Az ilyen típusú topológiában a végberendezések egy központi közvetítő eszközhöz csatlakoznak, ebben az esetben egy Ethernet switch-hez. Egy **kiterjesztett csillag** topológia több Ethernet switch összekapcsolásával bővíti ezt ki. A csillag és kiterjesztett csillag topológiák telepítése egyszerű, nagymértékben méretezhetők (könnyedén hozzáadhatunk és eltávolíthatunk végberendezéseket), valamint hibaelhárításuk is egyszerűen elvégezhető. A korai csillag topológiáknál a végberendezések Ethernet hub használatával kapcsolódtak egymáshoz.

Időnként előfordulhat, hogy csak két eszköz csatlakozik az Ethernet hálózaton. Például két egymással összekapcsolt router. Ez egy példa lehet az Etherneten használt pont-pont topológiára.

**Régi LAN topológiák**

A korai Ethernet és a régi vezérjeles gyűrű (Token Ring) LAN technológiák két másik topológia típust tartalmaztak:

* **Busz** \- Az állomások egymás után vannak láncolva és valamilyen formában a lánc mindkét vége le van zárva. A végberendezések összekapcsolásához nincs szükség (a kapcsolóhoz hasonló) hálózati eszközökre. Az Ethernet korábbi változataiban busz topológiát használtak koax kábellel, az alacsony ára és könnyű telepíthetősége miatt.
* **Gyűrű** - Az állomások a megfelelő szomszédaikkal összeköttetésben állva alkotnak egy gyűrűt. A busz topológiával ellentétben a gyűrűt nem kell lezárni. A gyűrű topológiát az FDDI hálózatok korábbi változataiban és a vezérjeles gyűrűben használták.

Az ábrák azt mutatják, hogy a végberendezések miként kapcsolódhatnak egymáshoz LAN hálózatok esetében. Gyakori, hogy a hálózati rajzok egyenes vonalai egy egyszerű csillagot és kiterjesztett csillagot tartalmazó Ethernet LAN-t jelölnek.

comparison of four physical topologies: star, extended star, bus, and ring

### Fizikai topológiák

Star TopologyExtended Star TopologyBus TopologyRing Topology

6.2.5

## Fél- és teljes duplex kommunikáció

A LAN topológiák tekintetében fontos a duplex kommunikáció megértése, mivel az két eszköz közötti adatátvitel irányára utal. A duplex kommunikációnak két általános módja van.

**Félduplex kommunikáció**

Mindkét eszköz képes adatküldésre és -fogadásra a közegen, de nem egyidejűleg. A WLAN-ok és a korai Ethernet hubokkal rendelkező busztopológiák félduplex módot használnak. A félduplex mód egyszerre csak egy eszköz számára teszi lehetővé a küldést vagy a fogadást egy megosztott közegen. A félduplex kommunikációról szóló animáció megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra! .

half duplex communication between a server and a hub

**Teljes duplex kommunikáció**

Mindkét eszköz egyidejűleg képes adatküldésre és -fogadásra a megosztott közegen. Az adatkapcsolati réteg feltételezi, hogy a közeg bármikor elérhető mindkét állomás számára. Az Ethernet kapcsolók alapértelmezés szerint teljes duplex üzemmódban működnek, de félduplex módban is működhetnek, ha olyan eszközhöz csatlakoznak, mint például az Ethernet hub. A teljes duplex kommunikációról szóló animáció megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra! .

full duplex communication between a server and a hub

Server

Switch

Összefoglalva, a félduplex kommunikáció egyszerre egy irányba korlátozza az adatküldést. A teljes duplex az adatok egyidejű küldését és fogadását teszi lehetővé.

Fontos, hogy két összekapcsolt interfész, például egy állomás hálózati kártyája és egy switch Ethernet interfésze ugyanazt a duplex módot használja. Ellenkező esetben eltérés lesz a duplexitásban, ami teljesítménycsökkenést és késleltetést eredményez a kapcsolaton.

6.2.6

## Hozzáférés-vezérlési módszerek

Az Ethernet LAN és a WLAN hálózatok a többes hozzáférésű hálózatok közé tartoznak. A többes hozzáférésű hálózat olyan hálózat, amelyben két vagy több végberendezés egyszerre próbál hozzáférni a hálózathoz.

Számos többes hozzáférésű hálózatban szabályokra van szükség ahhoz, hogy az eszközök meg tudjanak osztozni a fizikai adathordozón. Két alapvető hozzáférési módszer létezik osztott átviteli közeg esetében:

* Versengéses hozzáférés
* Szabályozott hozzáférés

**Versengéses hozzáférés**

A versengés alapú többes hozzáférésű hálózatokban a csomópontok félduplex módban működnek és versenyeznek a közeg használatáért. Egyszerre azonban csak egy eszköz küldhet. Ezért arra az esetre, ha egynél több eszköz végezne adatküldést egyszerre, egy eljárást dolgoztak ki. A versengéses hozzáférési módok például a következők:

* Vivőérzékeléses többszörös hozzáférés ütközésfigyeléssel (Carrier Sense Multiple Access with Collision Detection, CSMA/CD), a korai busz topológiájú Ethernet LAN-okban használták.
* Vivőérzékeléses többszörös hozzáférés ütközés-elkerüléssel (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA), a vezeték nélküli LAN-okban használják.

The image shows three PCs connected to an Ethernet hub. Two of the PCs are sending frames simultaneously.

FrameFrameEthernet HubShared Media

**Szabályozott hozzáférés**

Egy szabályozott többes hozzáférésű hálózatban minden csomópontnak megvan a maga időrése a közeg használatára. A korai hálózatok ezen determinisztikus típusai nem hatékonyak, mivel az eszköznek ki kell várnia a sorát, hogy hozzáférjen a közeghez. Szabályozott hozzáférést használó többes hozzáférésű hálózatok például a következők:

* Régi vezérjeles gyűrű
* Régi ARCNET

The image shows four PCs connected to a token ring network.

Token Ring Network

Minden csomópontnak ki kell várnia a sorát a hálózati közeg eléréséhez.

**MEGJEGYZÉS**: A mai Ethernet hálózatok teljes duplex módban működnek és nem igényelnek hozzáférési módot.

6.2.7

## Versengéses hozzáférés - CSMA/CD

Versengéses hozzáférési módot használó hálózatok például a következők:

* Vezeték nélküli LAN (CSMA/CA)
* Régi Ethernet LAN busztopológiával (CSMA/CD-t használ)
* Régi Ethernet LAN hub használatával (CSMA/CD-t használ)

Ezek a hálózatok félduplex módban működnek, ami azt jelenti, hogy egyszerre csak egy eszköz tud küldeni vagy fogadni. Ez egy folyamatot igényel, amelyik szabályozza, hogy az eszköz mikor végezhet adatküldést, és mi történik akkor, ha több eszköz egyidejűleg küld adatot.

Ha két eszköz egyszerre ad, ütközés történik. A régi Ethernet LAN-ok esetében mindkét eszköz észleli az ütközést a hálózaton. Ez a CSMA/CD ütközésérzékelés (CD) része. A hálózati kártya összehasonlítja az elküldött adatokat a fogadott adatokkal, vagy felismeri, hogy a jel amplitúdója magasabb a közegen használt normál értékhez képest. Mindkét készülék elküldött adatai megsérülnek és újra el kell őket küldeni.

A hubot használó régi Ethernet hálózatokban működő CSMA/CD folyamatról szóló kép és leírás megtekintéséhez kattintsunk az egyes gombokra!

PC1 Ethernet keretet szeretne küldeni PC3-nak. A PC1 hálózati kártyájának meg kell határoznia, hogy végez-e továbbítást bármely eszköz a közegen. Ha nem érzékel vivőjelet (más szóval, nem érzékel átvitelt egy másik eszköztől), akkor feltételezi, hogy a hálózat elérhető a küldéshez.

Az ábrán az látható, hogy a PC1 hálózati kártyája akkor küldi el az Ethernet keretet, ha a közeg elérhető.

The image shows three PCs (PC1, PC2, and PC3) connected to an Ethernet hub. PC1 is sending a frame. A text box above PC1 reads The medium is available so I will send the Ethernet frame to PC3.

FrameThe medium is available so I will send the Ethernet frame to PC3.PC1PC2PC3

6.2.8

## Versengéses hozzáférés - CSMA/CA

A CSMA egy másik formája az IEEE 802.11 WLAN-ok által használt vivőjel-érzékeléses többszörös hozzáférés ütközéselkerüléssel (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA).

A CSMA/CA a CSMA/CD-hez hasonló módszert használ a közeg foglaltságának érzékelésére. A CSMA/CA további technikákat is alkalmaz. Vezeték nélküli környezetben előfordulhat, hogy az eszköz nem érzékeli az ütközést. A CSMA/CA nem észleli az ütközéseket, de megpróbálja elkerülni őket úgy, hogy küldés előtt várakozik. Minden továbbítást végző eszköz tárolja az átvitelhez szükséges időtartamot. Az összes többi vezeték nélküli eszköz megkapja ezt az információt, és tudni fogja, mennyi ideig lesz foglalt a közeg.

Ha az A állomás egy vezeték nélküli keretet fogad a hozzáférési ponttól, a B és C állomások is látni fogják a keretet, valamint azt, hogy mennyi ideig lesz foglalt a közeg.

The image shows a wireless network consisting of an access point and three laptops, laptop A, B, and C. Laptop A has a text box that reads Im receiving this wireless frame. Laptop B has text box that reads I see in the wireless frame that the is channel is unavailable for a specific amount of time so I cannot send. Laptop C has a text box that reads I see in the wireless frame that the channel is going to be unavailable for a specific amount of time so I cannot send.

I'm receiving this wireless frame.I see in the wireless frame   
that the channel is going to be unavailable for a specific  
amount of time so I cannot send.I see in the wireless frame that the channel is   
unavailable for a specific amount of  
time so I cannot send.ABC

Miután a vezeték nélküli eszköz elküld egy 802.11 keretet, a címzett nyugtát küld vissza, amelyben jelzi a küldő számára, hogy a keret megérkezett.

Akár hubokat használó Ethernet LAN-ról, akár WLAN-ról van szó, a versengéses rendszerek nem teljesítenek jól a közeg nagyfokú kihasználtsága esetén.

**MEGJEGYZÉS**: A switcheket használó Ethernet LAN-ok nem használnak versengéses rendszert, mert a switch és az állomás hálózati kártyája teljes duplex üzemmódban működnek.

6.2.9

## Tudáspróba - Topológiák

Az űrlap teteje

Check your understanding of topologies by choosing the BEST answer to the following questions.

1. Which topology displays networking device layer IP addresses?

Az űrlap alja

What kind of network would use point-to-point, hub and spoke, or mesh topologies?

Which LAN topology is a hybrid topology?

Which duplex communication method is used in WLANs?

Which media access control method is used in legacy Ethernet LANs?

[6.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az adatkapcsolati réteg célja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[6.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adatkapcsolati keret](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                       
*                     

1. Adatkapcsolati réteg
2. Adatkapcsolati keret

# Adatkapcsolati keret

6.3.1

## Keret

Ez a fejezet részletesen tárgyalja, hogy mi történik az adatkapcsolati kerettel a hálózati továbbítás során. A kerethez csatolt információkat a használt protokoll határozza meg.

Az adatkapcsolati réteg egy fejléccel és utótaggal ellátott keretbe ágyazza be az adatot (általában IPv4 vagy IPv6-csomagot), ezzel készíti elő azt a közegen való továbbításra.

Az adatkapcsolati protokoll felelős az ugyanazon hálózaton belül található hálózati kártyák egymás közti kommunikációjáért. Annak ellenére, hogy számos különböző adatkapcsolati protokoll létezik az adatkapcsolati keretek leírására, mindegyik kerettípus három fő részből áll:

* Fejléc
* Adatrész
* Utótag

A többi beágyazást végző protokolltól eltérően az adatkapcsolati réteg a keret végéhez is csatol információkat egy utótag formájában.

Az adatkapcsolati rétegben található protokollok mindegyike a keret adat mezőjébe ágyazza be a felsőbb rétegbeli adatokat. A keret felépítése, valamint a fejlécben és az utótagban található mezők viszont protokollonként eltérőek lehetnek.

Olyan keretszerkezet nem létezik, amely mindenféle átviteli közegre kielégítené az összes adattovábbítási igényt. A keretben lévő vezérlési információk mennyisége a környezettől függően változik, amiatt, hogy megfeleljen a közeg és a logikai topológia hozzáférési követelményeinek. A WLAN keretnek például tartalmaznia kell az ütközések elkerülésére szolgáló eljárásokat, ezért további vezérlési információkat igényel az Ethernet kerethez képest.

Az ábrán is látható érzékeny környezetben több ellenőrzésre van szükség a kézbesítés biztosításához. A fejléc és utótag mezők nagyobb méretűek, mivel több ellenőrzési információra van szükség.

Two routers communicating over a wireless WAN through a satellite connection

FrameFrame

Több ellenőrzésre van szükség az átvitel biztosításához. Ez nagyobb terhelést és lassabb átviteli sebességet eredményez.

6.3.2

## A keret mezői

A keretezéssel olyan csoportokra bontjuk a bitfolyamot, amelyeknek fejlécében és utótagjában megtalálható vezérlőinformációk különböző adatmezők értékeiként jelennek meg. Ez a formátum egy olyan szerkezetet ad a jelsorozatnak, amelyet a fogadó állomás felismer és képes belőle visszaalakítani az adatcsomagokat.

Az ábrán a keret általános mezői láthatók. Nem minden protokoll tartalmazza ezen mezők mindegyikét. Az adatkapcsolati protokollok szabványai határozzák meg a tényleges keretformátumot.

The image shows a data packet encapsulated by a data link header and a data link trailer. The data link header is broken down to for fields: Frame start, addressing, type, and control. The data link trailer is broken down to two fields: Error detection and frame stop.

Packet  
(Data)HeaderTrailerDataFrame StartAddressingTypeControlError DetectionFrame Stop

A keret mezői a következőket tartalmazzák:

* **Keretkezdet és vége jelzők** - A keret kezdetének és végének azonosítására szolgál.
* **Címzés** -A közegen található forrás- és célállomásokat jelzi.
* **Típus** - A 3. rétegbeli protokollt azonosítja az adatmezőben.
* **Vezérlés** - Speciális adatfolyam szolgáltatásokat azonosít, mint például a szolgáltatásminőség (QoS). A QoS bizonyos típusú üzenetek számára elsőbbséget biztosít a továbbítás során. Például az IP alapú hangtovábbítás (VoIP) keretei általában elsőbbséget élveznek, mert érzékenyek a késleltetésre.
* **Adat** - A keret adatrészét tartalmazza (azaz a csomag fejrészt, a szegmens fejrészt és az adatot).
* **Hibaellenőrzés** - Az adatrész után található, az utótagot alkotja.

Az adatkapcsolati protokoll minden keret végéhez egy utótagot ad hozzá. A hibakeresésnek nevezett folyamat során az utótag határozza meg, hogy a keret hibamentesen érkezett-e meg. A keretet alkotó bitek logikai vagy matematikai összegzését helyezi el az utótagba. Azért az adatkapcsolati rétegben történik a hibadetektálás, mert a közegen továbbított jelek interferencia, torzítás vagy veszteség következtében jelentős mértékben megváltoztathatják az általuk ábrázolt bitek értékét.

A továbbítást végző csomópontok készítik el a keret tartalmának logikai összegzését, amelyet ciklikus redundancia-ellenőrzésnek (Cyclic redundancy check, CRC) hívunk. A kiszámított értéket a keretellenőrző összeg (Frame Check Sequence, FCS) mezőbe helyezik, hogy a keret tartalmát képviselje. Az Ethernet utótagban az FCS egy módszert biztosít a fogadó csomópont számára a keret átviteli hibáinak megállapítására.

6.3.3

## 2. rétegbeli címek

Az adatkapcsolati réteg biztosítja azt a címzést, amelyet a megosztott közegen történő kerettovábbításnál használunk. Az eszközök címét ebben a rétegben fizikai címnek hívjuk. Az adatkapcsolati réteg címzését a keret fejlécében találhatjuk, ez határozza meg a keret cél csomópontját a helyi hálózaton. Ez általában a keret elején található, így a hálózati kártya gyorsan, még a keret többi részének fogadása előtt meghatározhatja, hogy egyezik-e a saját 2. rétegbeli címével. A keret fejléce tartalmazhatja a forráscímet is.

A 3. rétegben található, hierarchikus felépítésű logikai címmel ellentétben, a fizikai cím nem jelzi azt, hogy a készülék melyik hálózaton található. A fizikai cím inkább az eszközre jellemző egyedi cím. Attól, hogy a készülék egy másik hálózatba vagy alhálózatba kerül át, még ugyanazzal a 2. rétegbeli címmel működik tovább. Ezért a 2. rétegbeli címeket csak olyan eszközök csatlakoztatására használjuk, amelyek azonos megosztott közegen és azonos IP-hálózaton belül találhatók.

Az ábrák a 2. és 3. rétegbeli címek funkcióját szemléltetik. Ahogy a csomag az állomástól routerig, majd routertől routerig, végül routertől állomásig halad, az IP-csomag minden lépésnél új adatkapcsolati keretbe kerül. Minden adatkapcsolati keret tartalmazza a keretet küldő és a keretet fogadó eszköz hálózati kártyájának adatkapcsolati címét.

További információért kattintsunk a gombokra!

A forrásállomás a 3. rétegbeli IP-csomagot egy 2. rétegbeli keretbe ágyazza be. A keret fejlécében az állomás a saját 2. rétegbeli címét adja hozzá forrásként, az R1 router 2. rétegbeli címét pedig célként.

The image shows a network consisting of a source PC, router R1, router R2, and a final destination web server. A text box representing the NIC of each device interface is shown. PC1 has IP address 192.168.1.100. The server has IP address 172.16.1.99. PC1 is sending an L2 frame with a Destination NIC address of R1 and a source NIC address of its own NIC. The frame is encapsulating a L3 IP packet with a Source IP address of 192.168.1.110 and a destination IP address of 172.16.1.99.

R1

R2



Original SourceFinal DestinationPC1 192.168.1.110Web Server 172.16.1.99L2 = Layer 2L3 = Layer 3NICNICNICNICNICNICL2L3L2L3L2L3Source IP 192.168.1.110CDestination IP 172.16.1.99L2 HeaderL3 IP PacketDestination NICSource NICCSource IP 192.168.1.110CDestination IP 172.16.1.99

Az adatkapcsolati rétegbeli címeket csak helyi kézbesítésre használjuk. Az ebben a rétegben található címek nem jelentenek semmit a helyi hálózaton túl. Vessük össze ezt a 3. réteggel, ahol a csomag fejlécében szereplő címek a forrásállomástól a célállomásig utaznak, függetlenül az út során megtett hálózati ugrások számától.

Ha az adatokat egy másik hálózati szegmensbe kell továbbítani, egy közvetítő eszközre (pl. routerre) van szükség. A router a keretet a fizikai cím alapján fogadja, majd kibontja azt annak érdekében, hogy megvizsgálja a hierarchikus címet, ami az IP-cím. Az IP-cím alapján a router meg tudja állapítani a célkészülék hálózati helyét és a hozzá vezető legjobb útvonalat. Ha megtudja, hogy hova továbbítsa a csomagot, egy új keretet állít össze a számára, majd elküldi ezt a keretet a végső cél felé vezető következő hálózati szegmensre.

6.3.4

## LAN és WAN keretek

Az Ethernet protokollokat vezetékes helyi hálózatokban használják. A vezeték nélküli kommunikáció a WLAN (IEEE 802.11) protokollok hatálya alá tartozik. Ezeket a protokollokat többes hozzáférésű hálózatokhoz tervezték.

A WAN hálózatok hagyományosan más típusú protokollokat használnak a különböző pont-pont, csillagpont és teljes hálós topológiákhoz. Néhány gyakori WAN protokoll az elmúlt évekből:

* Pont-pont protokoll (Point-to-Point Protocol, PPP)
* Felső szintű adatkapcsolat-vezérlés (High-Level Data Link Control, HDLC)
* Frame Relay
* Aszinkron átviteli mód (Asynchronous Transfer Mode, ATM)
* X.25

Ezeket a 2. rétegbeli protokollokat a WAN hálózatban az Ethernet váltja fel.

Egy TCP/IP hálózatban az OSI modell 2. rétegében működő összes protokoll a 3. rétegben található IP-vel működik együtt. A használt 2. rétegbeli protokoll viszont a hálózat logikai topológiájától és a fizikai közegtől függ.

Bizonyos 2. rétegbeli logikai topológiákon minden protokoll közeghozzáférés-vezérlést végez. Ez azt jelenti, hogy számos különböző hálózati eszköz viselkedhet adatkapcsolati rétegben működő csomópontként, miközben ezeket a protokollokat használja. Ezen eszközök közé a számítógépek hálózati kártyái, valamint a routerek és a 2. rétegbeli switchek interfészei tartoznak.

Az, hogy egy bizonyos hálózati topológiánál melyik 2. rétegbeli protokollt használjuk, azon múlik, hogy a topológia megvalósításához milyen technológiára van szükség. A használt technológiát az állomások számától és a földrajzi kiterjedéstől függő hálózatméret, valamint a hálózaton nyújtandó szolgáltatások határozzák meg.

A helyi hálózatokban jellemzően nagyszámú állomás kiszolgálására alkalmas, nagy sávszélességű technológiát használunk. Ezt a technológiát a hálózat viszonylag kis földrajzi területe (egy vagy több épületből álló egyetem), valamint a felhasználók sűrű elhelyezkedése teszi költséghatékonnyá.

Ugyanakkor a nagy sávszélességű technológiák általában nem költséghatékonyak WAN hálózatok esetében, mivel azok nagy földrajzi területeket fednek le (például városok vagy nagyvárosok). A nagytávolságú fizikai kapcsolatok magas költsége és az ekkora távolságokra használt jeltovábbító technológiák miatt jellemzően alacsonyabb sávszélességet kapunk.

A sávszélességben jelentkező különbség általában eltérő protokollok használatát eredményezi LAN és WAN hálózatok esetében.

Az adatkapcsolati réteg protokolljai a következők:

* Ethernet
* 802.11 szabványú vezeték nélküli
* Pont-pont protokoll (PPP)
* Felső szintű adatkapcsolat-vezérlés (HDLC)
* Frame Relay

A 2. rétegbeli protokollok példáinak megtekintéséhez kattintsunk a Lejátszás gombra!

a depiction of a network consisting of interconnected LANs and WANs

802.11 Wireless Frame

PPP Frame

HDLC

Frame Relay

Ethernet Frame

6.3.5

## Tudáspróba - Adatkapcsolati keret

Az űrlap teteje

Check your understanding of topologies by choosing the BEST answer to the following questions.

1. What does the data link layer add to a Layer 3 packet to create a frame? (Choose two.)

Az űrlap alja

What is the function of the last field in a data link layer frame?

Which lists the Layer 2 and Layer 3 address fields in the correct order?

Which of the following are data link layer protocols? (Choose three)

[6.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Topológiák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[6.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                            

1. Adatkapcsolati réteg
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

6.4.1

## Miről tanultunk ebben a fejezetben?

**Az adatkapcsolati réteg célja**

Az OSI modell adatkapcsolati rétege (2. réteg) a hálózati adatokat készíti elő a fizikai hálózat számára. Az adatkapcsolati réteg felelős a hálózati kártyák (NIC) egymás közti kommunikációjáért. Az adatkapcsolati réteg nélkül a hálózati réteg protokolljainak (például az IP-nek) kellene gondoskodnia az összes olyan közegtípushoz történő csatlakozásról, amely a szállítási útvonalon előfordulhat. Az IEEE 802 LAN/MAN adatkapcsolati rétege a következő két alrétegből áll: LLC és MAC. A MAC alréteg adatbeágyazást biztosít kerethatárolással, címzéssel és hibaérzékeléssel. A router interfészei a megfelelő keretbe ágyazzák be a csomagot. Minden összeköttetésnél a neki megfelelő közeghozzáférés-vezérlési módszer van használatban. Az adatkapcsolati rétegre vonatkozó nyílt szabványokat és protokollokat létrehozó mérnöki szervezetek az alábbiak: IEEE, ITU, ISO, és ANSI.

**Topológiák**

A LAN és WAN hálózatokban használt két topológia típus a fizikai és a logikai. Az adatkapcsolati réteg a hálózat logikai topológiáját figyeli a közeghozzáférés vezérlése közben. A logikai topológia befolyással van a keretezés típusára és a használt közeghozzáférési módra. A fizikai WAN topológiák három gyakori típusa: pont-pont, csillagpont, valamint hálós. A fizikai pont-pont összeköttetések közvetlenül két végberendezést (csomópontot) kapcsolnak össze egymással. Köztes fizikai kapcsolatok hozzáadása nem változtatja meg a logikai topológiát. A többes hozzáférésű helyi hálózatokban a csomópontok csillag- vagy kiterjesztett csillag topológiákkal vannak összekapcsolva egymással. Az ilyen típusú topológiában a csomópontok egy központi közvetítő eszközhöz csatlakoznak. A fizikai LAN topológiák a következők: csillag, kiterjesztett csillag, busz és gyűrű. A félduplex kommunikáció egyszerre egy irányba korlátozza az adatküldést. A teljes duplex egyidejűleg képes a küldésre és fogadásra. Két összekapcsolt interfésznek ugyanazt a duplex módot kell használnia, különben eltérés lép fel a duplexitásban, ami teljesítményromlást és késleltetést eredményez a kapcsolaton. Az Ethernet LAN és a WLAN hálózatok a többes hozzáférésű hálózatok közé tartoznak. A többes hozzáférésű hálózat olyan hálózat, amelyben két vagy több csomópont egyszerre próbál hozzáférni a hálózathoz. Számos többes hozzáférésű hálózatban szabályokra van szükség ahhoz, hogy az eszközök meg tudjanak osztozni a fizikai közegen. Megosztott közeg esetén két alapvető hozzáférés-vezérlési módszer létezik: a versengéses alapú és az ellenőrzött hozzáférés. A versengéses alapú többes hozzáférésű hálózatokban minden csomópont félduplex módban működik. Arra az esetre, ha egynél több eszköz végezne adatküldést egyszerre, egy eljárást dolgoztak ki. Versengéses alapú hozzáférési módszerek közé a következő példák tartoznak: CSMA/CD a busztopológiát használó Ethernet LAN-ok, valamint CSMA/CA a vezeték nélküli LAN-ok esetében.

**Adatkapcsolati keret**

Az adatkapcsolati réteg egy fejléccel és utótaggal ellátott keretbe ágyazza be az adatot (általában IPv4 vagy IPv6-csomagot), ezzel készíti elő azt a közegen való továbbításra. Az adatkapcsolati protokoll felelős az ugyanazon hálózaton belül található hálózati kártyák egymás közti kommunikációjáért. Számos különböző adatkapcsolati protokoll létezik az adatkapcsolati keretek leírására, mindegyik kerettípus három fő részből áll: fejléc, adatrész, utótag. A többi beágyazást végző protokolltól eltérően az adatkapcsolati réteg a keret utótagjához is csatol információkat. Olyan keretszerkezet nem létezik, amely mindenféle átviteli közegre kielégítené az összes adattovábbítási igényt. A keretben lévő vezérlési információk mennyisége a környezettől függően változik, amiatt, hogy megfeleljen a közeg és a logikai topológia hozzáférési követelményeinek. A keretmezők közé a következők tartoznak: keretkezdet és vége jelzők, címzés, típus, vezérlés, adatok és hibaérzékelés. Az adatkapcsolati réteg biztosítja azt a címzést, amelyet a megosztott helyi közegen történő kerettovábbításnál használunk. Az eszközök címét ebben a rétegben fizikai címnek hívjuk. Az adatkapcsolati réteg címzését a keret fejlécében találhatjuk, ez határozza meg a keret cél csomópontját a helyi hálózaton. Az adatkapcsolati rétegbeli címeket csak helyi kézbesítésre használjuk. Egy TCP/IP hálózatban az OSI modell 2. rétegében működő összes protokoll a 3. rétegben található IP-vel működik együtt. A használt 2. rétegbeli protokoll viszont a hálózat logikai topológiájától és a fizikai közegtől függ. Bizonyos 2. rétegbeli logikai topológiákon minden protokoll közeghozzáférés-vezérlést végez. Az, hogy egy bizonyos hálózati topológiánál melyik 2. rétegbeli protokollt használjuk, azon múlik, hogy a topológia megvalósításához milyen technológiára van szükség. Az adatkapcsolati réteg protokolljai közé a következők tartoznak: Ethernet, 802.11 vezeték nélküli, PPP, HDLC és Frame Relay.

6.4.2

## Ellenőrző kvíz - Adatkapcsolati réteg

Az űrlap teteje

1. Milyen azonosítót használnak az adatkapcsolati rétegben egy Ethernet eszköz egyedi azonosítására?

Az űrlap alja

A hálózati kártya melyik attribútuma használható adatként az OSI-modell adatkapcsolati rétegében?

Melyik két mérnöki szervezet határoz meg nyílt szabványokat és protokollokat az adatkapcsolati réteg számára? (Két jó válasz van.)

Melyik igaz a fizikai és logikai topológiákkal kapcsolatban?

Milyen módszer kezeli a vezeték nélküli hálózatokban a versengés alapú közeghozzáférést?

Egy szakembert felkértek, hogy dolgozzon ki olyan fizikai topológiát a hálózat számára, amely magas szintű redundanciát biztosít. Melyik fizikai topológia írja elő, hogy minden csomópont minden másik csomóponttal összeköttetésben legyen a hálózatban?

Melyik utasítás írja le az adatátvitel fél-duplex módját?

Mi a logikai kapcsolatvezérlés (Logical Link Control, LLC) alréteg feladata?

Melyik adatkapcsolati rétegbeli közeghozzáférés-vezérlési módszert használja az Ethernet?

Mi az OSI-modell adatkapcsolati rétegének két alrétege? (Két jó válasz van.)

Az OSI modell melyik rétege felelős az eltérő közegtípusok beágyazási módszereinek meghatározásáért?

Milyen típusú fizikai topológiát hozhatunk létre, ha az összes Ethernet kábelt egy központi eszközhöz csatlakoztatjuk?

Melyik két szolgáltatást biztosítja az OSI-modell adatkapcsolati rétege? (Két jó válasz van.)

Habár a CSMA/CD az Ethernet alkotórésze, miért nincs rá szükség többé?

[6.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Adatkapcsolati keret](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                    
*                   

1. Ethernet kapcsolás
2. Bevezetés

# Bevezetés

7.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az Ethernet kapcsolás fejezetben.

Ha hálózati rendszergazdák vagy hálózatépítők szeretnénk lenni, akkor feltétlenül tudnunk kell az Ethernet-ről és az Ethernet kapcsolásról. A manapság használt két legjelentősebb LAN-technológia az Ethernet és a WLAN. Az Ethernet akár 100 Gbps sávszélességet is támogat, ami megmagyarázza népszerűségét. A fejezet laborgyakorlataiban Wireshark segítségével megtekinthetjük az Ethernet kereteket és a hálózati eszköz MAC-címeit. Az oktató videók segítenek az Ethernet jobb megértésében. A fejezetet végén már létre tudunk hozni egy kapcsolt hálózatot, amely Ethernetet használ!

7.0.2

## Miről tanulunk ebben a fejezetben?

**Fejezet címe:** Ethernet kapcsolás

**Fejezet célja:** Az Ethernet működésének magyarázata egy kapcsolt hálózatban.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Ethernet keret** | Az Ethernet alrétegek kapcsolata a keret mezőivel. |
| **Ethernet MAC-címek** | Az Ethernet MAC-címek leírása. |
| **MAC-címtábla** | A kapcsoló MAC-címtáblájának felépítése és a kerettovábbítás. |
| **Switch kapcsolási módok és sebességek** | Kapcsolási módszerek és portbeállítások ismertetése 2. rétegbeli switcheken. |

[6.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ethernet keretek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                        
*                   

1. Ethernet kapcsolás
2. Ethernet keretek

# Ethernet keretek

7.1.1

## Ethernet beágyazás

Ez a fejezet az Ethernet technológia leírásával kezdődik, beleértve a MAC-alréteg és az Ethernet keret mezőinek magyarázatát.

Az Ethernet a manapság használt két LAN-technológia egyike, a másik a vezeték nélküli LAN (WLAN). Az Ethernet vezetékes kommunikációt használ, csavart érpárat, száloptikai kapcsolatokat és koaxiális kábeleket.

Az Ethernet az OSI-modell két rétegében működik: az adatkapcsolati és a fizikai rétegben. Hálózati technológiák egész családját jelenti, amelyeket az IEEE 802.2 és 802.3 szabványok határoznak meg. Az Ethernet a következő sávszélességeket támogatja:

* 10 Mbit/s
* 100 Mbit/s
* 1000 Mbit/s (1 Gbit/s)
* 10 000 Mbit/s (10 Gbit/s)
* 40 000 Mbit/s (40 Gbit/s)
* 100 000 Mbit/s (100 Gbit/s)

Az Ethernet szabványok meghatározzák mind a 2. rétegbeli protokollokat, mind pedig az 1. rétegbeli technológiákat (lásd ábra).

### Az Ethernet és az OSI-modell

ApplicationPresentationSessionTransportNetworkData LinkPhysicalLLCMAC802.2802.3Ethernet

Az Ethernetet az adatkapcsolati és a fizikai rétegbeli protokollok határozzák meg.

7.1.2

## Az adatkapcsolati réteg alrétegei

Az IEEE 802 LAN/MAN protokollok, beleértve az Ethernetet is, az adatkapcsolati réteg két különálló alrétegét használják a működéshez. Ezek a logikai kapcsolatvezérlési (LLC) és a közeghozzáférés-vezérlési (MAC) alrétegek, ahogy az ábrán látható.

Az LLC és a MAC a következő szerepekkel rendelkezik az adatkapcsolati rétegben:

* **LLC alréteg**- Ez az IEEE 802.2 alréteg biztosítja a kommunikációt a felső rétegek hálózati szoftverei és az alsó rétegek eszközhardverei között. Információkat helyez el a keretben annak a hálózati rétegbeli protokollnak az azonosítására, amelyik a keretet használni fogja. Ez az információ lehetővé teszi, hogy több 3. rétegbeli protokoll (pl. IPv4 és IPv6) is ugyanazt a hálózati interfészt és közeget használja.
* **MAC-alréteg** - Ez az alréteg (például IEEE 802.3, 802.11 vagy 802.15) a hardverben valósul meg, és felelős az adatbeágyazásért és a közeghozzáférés-vezérléséért. Biztosítja az adatkapcsolati réteg címzését, és együttműködik a különböző fizikai rétegbeli technológiákkal.

The diagram shows the OSI network, data link, and physical layers. It also shows the data link layer LLC and MAC sublayers and various LAN/WAN protocols. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the LLC sublayer as specified in IEEE 802.2. Next is the MAC sublayer with three columns representing different types of network technologies. The first column is Ethernet IEEE 802.3 at the upper part of the MAC sublayer. Below this are various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer. The next column is WLAN IEEE 802.11 at the upper part of the MAC sublayer. Below this are the various WLAN standards for different types of wireless communications that span across the lower part of the MAC sublayer and the entire OSI physical layer. The last column is WPAN IEEE 802.15 at the upper part of the MAC sublayer. Below this are various WPAN standards for Bluetooth, RFID, etc. that span across the lower part of the MAC sublayer and the entire OSI physical layer.

Network Layer ProtocolNetworkData LinkLLC Sublayer - IEEE 802.2LLC SublayerMAC SublayerEthernet   
IEEE 802.3WLAN   
IEEE 802.11WPAN   
IEEE 802.15Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.Various WLAN standards for different types of wireless communicationsVarious WPAN standards for Bluetooth, RFID, etc.Physical

7.1.3

## MAC-alréteg

A MAC-alréteg felelős az adatbeágyazásért és a közeghez való hozzáférésért.

**Adatbeágyazás**

Az IEEE 802.3 adatbeágyazás a következőket tartalmazza:

* **Ethernet keret** - Az Ethernet keret belső szerkezete.
* **Ethernet címzés** — Az Ethernet keret forrás- és cél MAC-címet is tartalmaz, hogy a keretet az egyik Ethernet hálózati kártyától egy másik Ethernet hálózati kártyához ugyanazon a LAN-on keresztül továbbítsa.
* **Ethernet hibajelzés** - Az Ethernet keret tartalmaz egy hibaészleléshez használt keret-ellenőrző bitsorozat utótagot (Frame Check Sequence, FCS).

**Közeghozzáférés**

Az IEEE 802.3 MAC-alréteg tartalmazza az Ethernet kommunikációs szabványok specifikációit a különböző típusú adathordozókhoz, beleértve a réz és üvegszál alapú közegeket is (lásd ábra).

The diagram is showing various Ethernet standards in the MAC sublayer. At the top of the diagram is the network layer and the network layer protocol. Below that is the data link layer and its sublayers. The top sublayer is the IEEE 802.2 LLC sublayer. Next is the Ethernet IEEE 802.3 MAC sublayer. Below that are five columns with various Ethernet standards and media types that span the lower part of the MAC sublayer and the entire OSI physical layer. From left to right the columns are: IEEE 802.3u Fast Ethernet; IEEE 802.3z Gigabit Ethernet over Fiber; IEEE 802.ab Gigabit Ethernet over Copper; IEEE 802.3ae 10 Gigabit Ethernet over Fiber; and Etc.

### Ethernet szabványok a MAC-alrétegben

Ethernet-IEEE 802.3IEEE 802.3z   
Gigabit Ethernet   
over FiberIEEE 802.3ab   
Gigabit Ethernet   
over CopperIEEE 802.3u   
Fast EthernetNetwork Layered ProtocolNetworkData LinkLLC alayer-IEE 802.2LLC SublayerPhysicalMAC SublayerEtc.IEEE 802.3ae   
10 Gigabit Ethernet   
over Fiber

A korai Ethernet busz topológiát vagy hub-okat használt, és megosztott, fél-duplex közegen működött. Az Ethernet a fél-duplex közegen egy ütközés-alapú hozzáférési módszert használ, a vivőjel érzékeléses többszörös hozzáférésű ütközésérzékelést (CSMA/CD). Ez biztosítja, hogy egyszerre csak egy eszköz továbbítson adatot. A CSMA/CD lehetővé teszi, hogy több eszköz ugyanazon a fél-duplex közegen osztozzon, és észlelje az ütközést, amikor egynél több eszköz egyszerre próbál kommunkálni. Ezenkívül egy visszalépéses algoritmust is biztosít az újraküldéshez.

A mai Ethernet LAN-ok olyan switch-eket használnak, amelyek teljes duplex módban működnek. Az Ethernet switch-ekkel megvalósított teljes duplex kommunikáció nem igényel CSMA/CD hozzáférés-vezérlést.

7.1.4

## Az Ethernet keretek mezői

Az Ethernet keret mérete minimum 64 bájt, maximum 1518 bájt. Ez magában foglalja az összes bájtot a cél MAC-cím mezőtől kezdve a keret ellenőrző összeg mezőig (Frame Check Sequence, FCS). Az előtag és a keretkezdő mezőket nem vesszük figyelembe, amikor megadjuk a keret méretét.

Minden keretet, ami kevesebb, mint 64 bájt hosszúságú, ütközési töredéknek (runt) nevezünk. Ezeket a fogadó állomás automatikusan eldobja. A több mint 1500 bájt adattal rendelkező kereteket „jumbo” vagy „óriás" kereteknek hívjuk.

Ha egy átvitt keret mérete kisebb, mint a minimális vagy nagyobb, mint a maximális érték, a fogadó készülék eldobja azt. Az eldobott keretek valószínűleg ütközések vagy más, nem kívánt jelenségek eredményei, ezért érvénytelennek minősülnek. A jumbo kereteket azonban a legtöbb Fast Ethernet és Gigabit Ethernet switch és hálózati kártya támogatja.

Az ábrán az Ethernet keret mezői láthatók. Az egyes mezők funkciójával kapcsolatos további információkért tekintsük meg a táblázatot.

The diagram shows the fields of an Ethernet frame. From left to right the fields and their length are: Preamble and SFD, 8 bytes; Destination MAC address, 6 bytes; Source MAC address, 6 bytes; Type/length, 2 bytes; data, 45 - 1500 bytes; and FCS, 4 bytes. Excluding the first field, the total number of bytes in the remaining fields is between 64 - 1518.

### Ethernet Frame Fields

FCSDataType / LengthSource MAC AddressPreamble and SFDDestination MAC Address8 bytes6 bytes6 bytes2 bytes46-1500 bytes4 bytes64-1518 bytes

### Az Ethernet keretek mezői részletesen

| Table caption | |
| --- | --- |
| **Mező** | **Leírás** |
| Előtag és keretkezdő mezők | Az előtag (Preamble, 7 bájt) és a keretkezdő (Start Frame Delimiter, SFD, 1 bájt) mezők szinkronizálásra szolgálnak a küldő és fogadó készülékek között. A keretnek ezt az első nyolc bájtját használják arra, hogy a fogadó csomópont figyelmét felhívják a keret érkezésére. 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. Ezt a címet használja a második réteg, hogy segítse az eszközöket a nekik szóló keretek meghatározásában. A keretben lévő címet a készülék összehasonlítja a saját MAC-címével. Ha egyezés van, az eszköz elfogadja a keretet. Lehet unicast, multicast vagy broadcast cím is. |
| Forrás MAC-cím mező | Ez a 6 bájtos mező a keretet küldő hálózati kártyát vagy interfészt azonosítja. |
| Típus/Hossz mező | Ez a 2 bájtos mező azonosítja az Ethernet keretbe ágyazott felsőbb rétegbeli protokollt. Gyakori hexadecimális értékek: 0x800 (IPv4), 0x86DD (IPv6) és 0x806 (ARP).  **MEGJEGYZÉS**: Ezzel a mezővel EtherType néven is találkozhatunk. |
| Adat mező | Ez a mező (46-1500 bájt) tartalmazza a magasabb rétegbeli beágyazott adatokat, amely egy általános 3. rétegbeli PDU, például egy IPv4-csomag. Minden keretnek legalább 64 bájt hosszúnak kell lennie. Ha egy kis csomagot ágyaznak 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-mezőbe. A fogadó készülék megkapja a keretet, és szintén kiszámít egy CRC-t a hibakereséséhez. Ha a számítások megegyeznek, nem történt hiba. Ha a számított értékek nem egyeznek, az azt jelzi, hogy az adat megváltozott, ezért a keretet el kell dobni. Az értékben bekövetkezett változás annak a következménye lehet, hogy a biteket leíró elektromos jelekben zavar keletkezett. |

7.1.5

## Tudáspróba - Ethernet kapcsolás

Az űrlap teteje

Check your understanding of Ethernet frames by choosing the correct answer to the following questions.

1. Which part of an Ethernet Frame uses a pad to increase the frame field to at least 64 bytes?

Az űrlap alja

Which part of an Ethernet frame detects errors in the frame?

Which part of an Ethernet Frame describes the higher-layer protocol that is encapsulated?

Which part of an Ethernet Frame notifies the receiver to get ready for a new frame?

Which data link sublayer controls the network interface through software drivers?

Which data link sublayer works with the upper layers to add application information for delivery of data to higher level protocols?

What is a function of the MAC sublayer? (Choose three.)

7.1.6

## Laborgyakorlat - A Wireshark használata Ethernet keretek vizsgálatához

A laborgyakorlat során az alábbi feladatokat végezzük el:

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

[7.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ethernet MAC-címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                             
*                   

1. Ethernet kapcsolás
2. Ethernet MAC-címek

# Ethernet MAC-címek

7.2.1

## A MAC-címek és a hexadecimális számok

A hálózatkezelésben a bináris IPv4-címeket a tízes számrendszer segítségével ábrázolják. Az IPv6-címek és az Ethernet-címek a hexadecimális alapú, vagyis tizenhatos számrendszerbeli értékként jelennek meg. A hexadecimális számrendszer megértéséhez jól kell ismerni a bináris és a decimális számrendszert.

A hexadecimális rendszer a 0-9 számokat és az A-tól F-ig terjedő betűket használja.

Az Ethernet MAC-cím 48 bit bináris értékből áll. Az Ethernet-cím hexadecimális számjegyei egyenként négy bitet jelölnek. Ezért a 48 bites Ethernet MAC-cím mindössze 12 hexadecimális számjeggyel kifejezhető.

Az ábra összehasonlítja a megfelelő decimális és hexadecimális értékeket a bináris 0000 és 1111 között.

The figure is three columns showing the decimal and hexadecimal equivalents of select 4-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 16 rows below the header.

### 0 és F közötti hexadecimális számok tizedes és bináris megfelelői

0 15 3 4 5 6 7 8 9 10 11 12 13 14 2 1 0000 1111 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 0010 0001 0 F 3 4 5 6 7 8 9 A B C D E 2

1

DecimálisBinárisHexadecimális

Mivel 8 bit alkot egy bináris csoportot (vagy bájtot), a bináris 00000000-11111111 közti értékeket a hexadecimális 00-tól FF-ig terjedő tartománnyal lehet kifejezni, ahogy a következő ábrán látható.

The figure is three columns showing the decimal and hexadecimal equivalents of select 8-bit binary numbers. From left to right, the column headings are: decimal, binary, and hexadecimal. Each column has 18 rows below the header.

### Kiválasztott decimális, bináris és hexadecimális egyenértékek

0 255 3 5 7 10 15 32 128 192 202 240 2 1 8 16 64 6 4 0000 0000 1111 1111 0000 0011 0000 0101 0000 0111 0000 1010 0000 1111 0010 0000 1000 0000 1100 0000 1100 1010 1111 0000 0000 0010 0000 0001 0000 1000 0001 0000 0100 0000 0000 0110 0000 0100 00 FF 03 05 07 0A 0F 20 80 C0 CA F0 02 01 08 10 40 06

04

DecimálisBinárisHexadecimális

Hexadecimális ábrázolást használva a vezető nullákat is mindig megjelenítjük a teljes 8 bites kiírásnál. Például a 0000 1010 bináris értéket hexadecimális 0A-ként írjuk le.

A hexadecimális számokat gyakran a **0x** (pl. 0x73) előzi meg, hogy megkülönböztessék a decimális és hexadecimális értékeket a dokumentációban.

A hexadecimális értéket képviselheti egy alsó indexbeli 16-os, vagy a hexadecimális számot követő H betű is (pl. 73H).

Előfordulhat, hogy decimális és hexadecimális értékek között kell konvertálnunk. Ha ilyen átalakítások szükségesek, általában könnyebb a decimális vagy hexadecimális értéket binárissá átalakítani, majd azután a bináris értéket konvertálni át decimális vagy hexadecimális értékké.

7.2.2

## Ethernet MAC-címek

Egy Ethernet LAN-ban minden hálózati eszköz ugyanahhoz a megosztott közeghez csatlakozik. A MAC-cím a helyi hálózati szegmens forrás- és céleszközeinek (hálózati kártya, NIC) fizikai azonosítására szolgál. A MAC-címzés az OSI-modell adatkapcsolati rétegében biztosítja az eszközök megkülönböztethetőségét.

Az Ethernet MAC-cím egy 48 bites érték, amelyet 12 hexadecimális számjegy használatával írunk le (lásd ábra). Mivel egy bájt 8 bitnek felel meg, azt is mondhatjuk, hogy a MAC-cím 6 bájt hosszúságú.

The diagram shows that MAC address are composed of 48 bits total. These 48 bits can be divided into twelve 4-bit groupings, or 12 hex digits. Combining two hex digits together makes a byte, therefore the 48 bits is also equivalent to 6 bytes.

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

ByteByteByteByteByteByte= 6 bytesHexHexHexHexHexHexHexHexHexHexHexHex= 12 hex= 48 bits

Minden MAC-címnek egyedinek kell lennie az Ethernet eszközre vagy az Ethernet interfészre nézve. Ennek biztosítása érdekében minden, Ethernet-eszközt értékesítő gyártónak regisztrálnia kell az IEEE-nél, hogy kapjon egy egyedi, 6 hexadecimális jegyből álló (azaz 24 bites vagy 3 bájtos) kódot, amelyet egyedi szervezetazonosítónak (Organizatonally Unique Identifier, OUI) neveznek.

Amikor egy gyártó MAC-címet rendel egy eszközhöz vagy Ethernet interfészhez, a következőket kell tennie:

* A kapott OUI-t használja az első 6 hexadecimális számjegyként.
* Egyedi értéket ad az utolsó 6 hexadecimális számjegyhez.

Ezért az Ethernet MAC-cím egy 6 jegyű, hexadecimális gyártói OUI-kóddal kezdődik, amelyet egy 6 hexadecimális jegyből álló, gyártó által generált érték követ (lásd ábra).

the first six hex digits of a MAC address (AKA first 6 hex digits or first 3 bytes) is the organizational unique identifier and the last six hex digits is vendor assigned

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111

1111

ByteByteByteByteByteByteHexHexHexHexHexOrganizationally Unique Identifier, OUIHexHexHexHexHexHexVendor AssignedHex

Például, a Ciscónak egyedi MAC-címet kell hozzárendelnie egy új eszközhöz. Az IEEE által a Cisco-hoz rendelt egyik OUI a **00-60-2F**. A Cisco ezután konfigurálhatja a készüléket egy egyedi gyártói kóddal, mint például **3A-07-BC**. Ezért az eszköz Ethernet MAC-címe 00-60-2F-3A-07-BC lesz. **00-60-2F-3A-07-BC.**

A gyártó felelőssége annak biztosítása, hogy egyik eszköze sem kapja ugyanazt a MAC-címet. Lehetséges azonban, hogy azonos MAC-címek keletkeznek a gyártás során elkövetett hibák, a virtuális gépek megvalósítási módszereiben rejlő algoritmusok vagy valamely szoftvereszköz egyikével végrehajtott módosítások miatt. Mindegyik esetben a MAC-címet módosítani kell szoftver segítségével vagy egy új NIC beépítésével.

7.2.3

## A keret feldolgozása

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

**MEGJEGYZÉS**: A modern operációs rendszerek és a hálózati kártyák esetén szoftveresen is meg lehet változtatni a MAC-címet. Ez akkor hasznos, ha olyan hálózathoz próbálunk hozzáférni, amely a BIA alapján szűr. Következésképpen a forgalom MAC-cím alapján történő szűrése vagy ellenőrzése már nem olyan biztonságos.

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, az Ethernet fejléc a következőket tartalmazza:

* **Forrás MAC-cím** - Ez a forrás állomás hálózati kártyájának MAC-címe.
* **Cél MAC-cím** - Ez a céleszköz hálózati kártyájának MAC-címe.

Kattintsunk a Lejátszás gombra a keret továbbítási folyamat megtekintéséhez.

The animation has a topology consisting of a switch with links to four host PCs labeled, H1, H2, H3 and H4. H1 says I need to send information to H3. A frame appears on the screen of the PC and an expanded view of the frame appears above the PC. The frame consists of the framing addressing and data. The destination address CC:CC:CC:CC:CC:CC, the source address AA:AA:AA:AA:AA:AA and the data part of the frame is encapsulated. The frame from H1 is forwarded to the switch. The switch then forwards the frame out every interface but the interface connected to H1. When H2 and H4 receive the frame and they say This is not addressed to me. I shall ignore it. When H3 receives the frame it says This is mine.

This is not addressed to me. I shall ignore it.

This is not addressed to me. I shall ignore it.

This is mine.

I need to send information to H3.

Destination Address

Source Address

CC:CC:CC:CC:CC:CC

A:A:A:A:A:A:A:AA

Encapsulated data

Frame Addressing

Amikor egy hálózati kártya Ethernet keretet kap, összehasonlítja a benne levő cél MAC-címet a RAM-ban tárolt fizikai MAC-címmel. Ha nincs egyezés, akkor a készülék eldobja a keretet. Ha egyezik, akkor átadja a keretet a felsőbb OSI-rétegeknek, ahol a kibontási folyamat megtörténik.

**MEGJEGYZÉS**: Az Ethernet hálózati kártya akkor is elfogadja a kereteket, ha a cél MAC-cím szórásos vagy olyan csoportos címzésű, amelynek az állomás tagja.

Minden eszköz, amely a forrása vagy célja egy Ethernet keretnek, rendelkezik egy Ethernet hálózati kártyával, és ezért egy MAC-címmel is. Ide tartoznak a munkaállomások, a kiszolgálók, a nyomtatók, a mobileszközök és a routerek.

7.2.4

## Egyedi címzésű MAC-cím

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

Egyedi címzésű (unicast) MAC-címet használunk, amikor egy keretet egyetlen cél eszközre küldünk.

Kattintsunk a Lejátszás gombra az egyedi címzésű keret feldolgozásának megtekintéséhez! Ebben a példában a cél MAC-cím és a cél IP-cím egyaránt unicast.

The animation shows a host with IPv4 address 192.168.1.5 (source) requesting a web page from a server at IPv4 unicast address 192.168.1.200. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 00-07-E9-42-AC-28, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send this frame to Server. A frame is sent from H1 to the switch. The switch then forwards the frame to the server with the IP and MAC matching the destination IP and MAC address.

**Server**  
IP: 192.168.1.200  
MAC: 00-07-E9-42-AC-28

**Source Host**  
IP: 192.168.1.5  
MAC: 00-07-E9-63-CE-53

00-07-E9-42-AC-28

00-07-E9-63-CE-53

192.168.1.5

192.168.1.200

User Data

Trailer

Dest MAC

Source MAC

Source IP

Dest IP

IP Packet

Ethernet Frame

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 a folyamat, amelyet a forrásállomás használ az IPv4-címhez társított cél MAC-cím meghatározásához, az úgynevezett címfeloldási protokoll (ARP). Az a folyamat, amelyet a forrásállomás használ az IPv6-címhez társított cél MAC-cím meghatározásához, a szomszédfelderítés (Neighbor Discovery, ND).

**MEGJEGYZÉS:** A forrás MAC-címnek mindig egyedi címzésűnek kell lennie.

7.2.5

## Szórásos MAC-cím

Az Ethernet LAN minden eszköze megkapja és feldolgozza az Ethernet szórásos kereteket (broadcast). Az Ethernet szórás jellemzői a következők:

* A cél MAC-cím FF-FF-FF-FF-FF-FF-FF-FF hexadecimálisan (48 darab egyes binárisan).
* Kiküldésre kerül az összes Ethernet switchporton, kivéve a bejövő portot (elárasztás).
* A routerek nem továbbítják ezt a forgalmat.

Ha a beágyazott adat egy IPv4 szórásos csomag, akkor a csomag célcímként egy olyan IP-címet tartalmaz, amiben csupa 1-es áll az állomásazonosító részben. Ennek következtében a helyi hálózat összes gépe (a szórási tartomány) fogadja és feldolgozza a csomagot.

Kattintsunk a Lejátszás gombra a szórásos keret feldolgozásának megtekintéséhez! Ebben a példában a cél MAC-cím és a cél IP-cím egyaránt broadcast.

The animation shows a source host sending an IPv4 broadcast packet to all devices on its network. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC FF-FF-FF-FF-FF-FF, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 192.168.1.255, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send data to all hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out all its interfaces except the one connected to H1. The three other PC hosts and the two servers receive the frames.

**Destination  
Host Group**

**Source Host**  
IP: 192.168.1.5  
MAC: 00-07-E9-63-CE-53

FF-FF-FF-FF-FF-FF

00-07-E9-63-CE-53

192.168.1.5

192.168.1.255

User Data

Trailer

Dest MAC

Source MAC

Source IP

Dest IP

IP Packet

Ethernet Frame

Amint azt az animáció mutatja, a forrásállomás IPv4 szórási csomagot küld a hálózat összes eszközének. Az IPv4-célcím egy szórási cím: 192.168.1.255. Amikor az IPv4 szórásos csomag az Ethernet keretbe van ágyazva, a cél MAC-cím az FF-FF-FF-FF-FF-FF hexadecimális (48 bináris egyes) szórási cím.

Az IPv4 DHCP példa egy olyan protokollra, amely Ethernet- és IPv4-szórási címeket használ.

Azonban nem minden Ethernet szórás hordoz IPv4 szórásos csomagot. Az ARP-kérések például nem használnak IPv4-et, de az ARP-üzenetet Ethernet-szórásként küldik el.

7.2.6

## Csoportos címzésű MAC-cím

Az Ethernet csoportos címzésű kereteket (multicast) a LAN azon eszközcsoportjai fogadják és dolgozzák fel, amelyek ugyanahhoz a csoporthoz tartoznak. Az Ethernet csoportos küldés jellemzői a következők:

* A cél MAC-cím 01-00-5E, ha a beágyazott adat egy IPv4 csoportos küldésű csomag, illetve 33-33, ha a beágyazott adat IPv6 csoportos küldésű csomag.
* Vannak más fenntartott csoportos címzésű cél MAC-címek is, amikor a beágyazott adat nem IP, hanem például STP (Spanning Tree Protocol) vagy LLDP (Link Layer Discovery Protocol).
* A bejövő port kivételével az összes Ethernet switchporton kiküldésre kerül (kivéve, ha a switch multicast snooping-ra van konfigurálva).
* A router nem továbbítja (kivéve, ha csoportos címzésű csomagokat is továbbít).

Ha a beágyazott adat egy IP multicast csomag, akkor a csoporthoz tartozó eszközöknek csoportos IP-címe van. Az IPv4 multicast címek tartománya 224.0.0.0 - 239.255.255.255. Az IPv6 csoportos címzésű címek tartománya ff00።/8. Mivel egy multicast cím a címek egy csoportját jelenti (néha állomás-csoportnak is hívják), csak csomagok célcímeként használható. A forrásnak mindig egyedi címe van.

Ugyanúgy, mint az egyedi vagy szórási címek esetében, a csoportos címekhez is szükség van egy megfelelő csoportos MAC-címre, hogy kézbesíteni lehessen a kereteket a helyi hálózaton. A csoportos címzésű MAC-cím az IPv4 vagy IPv6 csoportos küldési címhez van társítva.

Kattintsunk a Lejátszás gombra a csoportos küldésű keret feldolgozásának megtekintéséhez! Ebben a példában a cél MAC-cím és a cél IP-cím egyaránt multicast.

The animation shows a source host sending a multicast frame to devices that belong to the multicast group. The animation has a topology consisting of a host PC named H1 linked to a switch. The switch has connections to three other host PCs and two servers. At the bottom of the animation is an expanded view of an ethernet frame. The frame consists of the destination MAC 01-00-5E-00-00-C8, source MAC 00-07-E9-63-CE-53, Source IP 192.168.1.5, destination IP address 224.0.0.200, user data and trailer. The IP packet portion of the frame is the source IP, destination IP address, and user data. In the animation, H1 says I need to send to a group of hosts on the network. A frame is sent from H1 to the switch. The switch then forwards the frame out to only the devices in the multicast group. Two of the three PC hosts and one server receive the multicast frame.

**Destination  
Host Group**

**Source Host**  
IP: 192.168.1.5  
MAC: 00-07-E9-63-CE-53

01-00-5E-00-00-C8

00-07-E9-63-CE-53

192.168.1.5

224.0.0.200

User Data

Trailer

Dest MAC

Source MAC

Source IP

Dest IP

IP Packet

Ethernet Frame

Az útválasztási és más hálózati protokollok csoportos címzést használnak. A videó- és képkezelő szoftverek is alkalmazhatnak multicast címzést, bár ezek nem túl gyakoriak.

7.2.7

## Laborgyakorlat - Hálózati eszközök MAC címeinek megtekintése

A laborgyakorlat során az alábbi feladatokat végezzük el:

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

[7.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ethernet keretek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A MAC-címtábla](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                  
*                   

1. Ethernet kapcsolás
2. A MAC-címtábla

# A MAC-címtábla

7.3.1

## A kapcsolás alapjai

Az Ethernet MAC-címekről tanultak alapján most beszéljünk arról, hogyan használja egy switch ezeket a címeket a keretek továbbítására (vagy eldobására) a hálózat más eszközei felé. Ha egy switch továbbítana minden megkapott keretet az összes portjára, akkor hálózati torlódás keletkezne, és valószínűleg teljes leállás következne be.

Egy 2. rétegbeli Ethernet switch a 2. rétegbeli MAC-címeket használja a továbbítási döntések meghozatalához. Nem foglalkozik a keret adatrészével (protokoll), például az IPv4-csomagokkal, ARP-üzenetekkel vagy IPv6 ND-csomagokkal. A switch a továbbítási döntéseket kizárólag a 2. rétegbeli Ethernet MAC-címek alapján hozza meg.

Minden egyes keret esetén megvizsgálja a MAC-címtáblát, hogy továbbítási döntést hozzon, ellentétben az Ethernet hubokkal, amelyek a bejövő port kivételével az összes portra kiküldik a biteket. Az ábrán látható négyportos switch éppen most be lett bekapcsolva. A MAC-címtábla még üres, mert a switch még nem tanulta meg a négy csatlakoztatott számítógép MAC-címét.

**MEGJEGYZÉS**: A MAC-címek a bemutatás céljából rövidítve szerepelnek.

The diagram shows four hosts, along with their associated MAC addresses, connected to ports 1 - 4 on a switch. The MAC address table which maps ports to MAC addresses is currently empty.

A B C D 1 2 3

4

| Table caption | |
| --- | --- |
| **MAC Address Table** | |
| **Port** | **MAC Address** |
|  |  |
|  |  |

MAC  
00-0AMAC  
00-0BMAC  
00-0CMAC  
00-0D

The switch MAC address table is empty.

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

7.3.2

## A switch tanulási és továbbítási folyamatai

A switch a bejövő keretek forrás MAC-címét megvizsgálva dinamikusan építi fel a MAC-címtáblát.A kereteket úgy továbbítja, hogy egyezést keres a keretben lévő cél MAC-cím és a MAC-címtábla bejegyzései között.

Kattintsunk a Tanulás és a Továbbítás gombra a folyamat magyarázatának megjelenítéséhez!

**A forrás MAC-cím vizsgálata**

Minden beérkező keret ellenőrzésre kerül, hogy van-e benne új információ a switch számára. A switch megvizsgálja a keret forrás MAC-címét és a port számát, ahol a keret belépett. Ha a forrás MAC-cím nincs benne a táblázatban, akkor a bejövő portszámmal együtt hozzáadásra kerül. Ha a forrás MAC-címe létezik, a switch frissíti az adott bejegyzéshez tartozó időzítőt. Alapértelmezés szerint a legtöbb Ethernet switch 5 percig tart meg egy bejegyzést a táblázatban.

Az ábrán a PC-A Ethernet keretet küld a PC-D-nek. A switch hozzáadja a PC-A MAC-címét a MAC-címtáblához.

**MEGJEGYZÉS**: Ha a forrás MAC-cím létezik a táblázatban, de egy másik porton, a switch ezt új bejegyzésként kezeli. A bejegyzést ugyanazzal a MAC-címmel, de az aktuális portszámmal helyettesíti.

The figure shows four hosts, A - D, are connected to a switch at ports 1 - 4. Host A with MAC address 00-0A (simplified in this example) is connected to the switch at port 1. Host A sends a frame with a destination MAC address of 00-0D. The source MAC in the frame is 00-0A. The switch maps port 1 to MAC address 00-0A in its MAC address table.

A B C D 1 2 3

4

| Table caption | |
| --- | --- |
| **MAC Address Table** | |
| **Port** | **MAC Address** |
| 1 | 00-0A |
|  |  |

MAC  
00-0AMAC  
00-0BMAC  
00-0CMAC  
00-0DDestination MAC  
00-0DSource MAC  
00-0ATypeDataFCS

1. PC-A sends an Ethernet frame.
2. The switch adds the port number and MAC address for PC-A to the MAC Address Table.

7.3.3

## Keretek szűrése

Amikor egy switch különböző eszközöktől kap kereteket, kitölti a MAC-címtábláját a keretek forrás MAC-címe alapján. Ha a switch MAC-címtáblája tartalmazza a beérkező keret cél MAC-címét, felismeri a keretet, és továbbítja azt a megfelelő portjára.

Kattintsunk a gombokra az egyes továbbítási folyamatok megismeréséhez!

Az ábrán a PC-D válaszol a PC-A-nak. A switch látja a PC-D MAC-címét a 4-es porton bejövő keretben. A switch beírja a PC-D MAC-címét a MAC-címtábla 4-es porthoz tartozó bejegyzésébe.

The figure shows four hosts, A - D, are connected to a switch at ports 1 - 4. Host D with MAC address 00-0D is connected to the switch at port 4. Host D sends a frame with a destination MAC address of 00-0A and a source MAC of 00-0D. The switch maps port 4 to MAC address 00-0D in its MAC address table.

A B C D 1 2 3

4

| Table caption | |
| --- | --- |
| **MAC Address Table** | |
| **Port** | **MAC Address** |
| 1 | 00-0A |
| 4 | 00-0D |

MAC  
00-0AMAC  
00-0BMAC  
00-0CMAC  
00-0DDestination MAC  
00-0ASource MAC  
00-0DTypeDataFCS

A switch hozzáadja a PC-D portszámát és MAC-címét a címtáblához.

7.3.4

## Videó - Egymáshoz csatlakoztatott switch-ek MAC-címtáblái

Egy kapcsolóban több MAC-cím is lehet egyetlen porthoz társítva. Ez általában akkor van így, ha egy másik switch csatlakozik a kapcsoló ezen portjához. A switch-nek külön MAC-címtábla bejegyzése lesz minden egyes különböző forrás MAC-címmel kapott kerethez.

Kattintsunk a Lejátszás gombra a bemutató megtekintéséhez, amelyben két összekapcsolt switch építi fel saját MAC-címtábláit.

7.3.5

## Videó - Keret küldése az alapértelmezett átjáróra

Ha egy céleszköz távoli hálózaton található IP-címmel rendelkezik, az Ethernet keret nem küldhető ki rá közvetlenül. Ehelyett az Ethernet keretet az alapértelmezett átjáró, a router MAC-címére küldjük.

Kattintsunk a Lejátszás gombra a PC-A és az alapértelmezett átjáró kommunikációjának megtekintéséhez!

**MEGJEGYZÉS**: A videóban a PC-A-ról egy távoli hálózat célállomására küldött IP-csomagnak a PC-A a forrás IP-címe, és a célcím a távoli állomás IP-címe. A visszaérkező IP-csomagban a távoli állomás IP-címe lesz a forrás, a cél IP-cím pedig a PC-A címe.

7.3.6

## Feladat - Kapcsolj át!

A forrás és cél MAC-cím, valamint a MAC-címtáblában lévő információk alapján határozzuk meg, hogyan fogja a switch továbbítani a keretet! Válaszoljuk meg az alábbi kérdéseket a rendelkezésre álló információk felhasználásával!

##### Frame

| **Preamble** | **Destination MAC** | **Source MAC** | **Type / Length** | **Frame** | **End of Frame** |
| --- | --- | --- | --- | --- | --- |
|  | 0B | 0E |  |  |  |

##### MAC Table

| **Fa1** | **Fa2** | **Fa3** | **Fa4** | **Fa5** | **Fa6** | **Fa7** | **Fa8** | **Fa9** | | **Fa10** | **Fa11** | **Fa12** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 0B |  |  |  | 0D |  |  |  |  |  |  |

##### Question 1 - Where will the switch forward the frame?

##### Question 2 - When the switch forwards the frame, which statement(s) are true?

7.3.7

## Laborgyakorlat - Switch MAC-címtábla megtekintése

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Hálózat felépítése és konfigurálása
* Bölüm 2: Switch MAC-címtáblájában tárolt adatok vizsgálata

[7.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ethernet MAC-címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Switch kapcsolási sebességek és módok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                      
*                   

1. Ethernet kapcsolás
2. Switch kapcsolási sebességek és módok

# Switch kapcsolási sebességek és módok

7.4.1

## Kerettovábbítási módszerek Cisco switch-eken

Amint azt az előző témakörben megtanultuk, a switch-ek MAC-címtáblázataikkal határozzák meg, hogy melyik portot kell használni a keretek továbbításához. A Cisco switch-ek valójában két kerettovábbítási módszert alkalmaznak a használt eszközök és működési körülmények függvényében.

A switch-ek az alábbi továbbítási módszerek valamelyikét használják az adatok hálózati portok közötti kapcsolásához:

* **Tárol-és-továbbít kapcsolás** - A switch beolvassa a teljes keretet, és kiszámítja a CRC-t. A CRC egy matematikai képletet használ a keretben lévő bitek (1-esek) száma alapján annak meghatározására, hogy a fogadott keretben van-e hiba. Ha érvényes a CRC, a switch beolvassa a célcímet, aminek alapján megállapítja, hogy melyik interfészen küldje ki a keretet. Ezután a megfelelő porton kiküldi azt.
* **Közvetlen kapcsolás** - Ez a módszer a teljes keret megérkezése előtt elkezdi a keretet továbbítani. A keret továbbításának megkezdése előtt legalább a keret célcímét ki kell olvasni.

A tárol-és-továbbít kapcsolás nagy előnye, hogy a keret kiküldése előtt meghatározza, vannak-e benne hibák. Ha a switch hibát észlel a keretben, akkor eldobja azt. A hibás keretek eldobása csökkenti a sérült keretek által lefoglalt sávszélességet. A konvergált hálózatokban tárol-és-továbbít kapcsolásra van szükség a szolgáltatásminőség (Quality of Service, QoS) biztosítására, ahol a forgalom prioritásának meghatározásához a keretek osztályozása szükséges. Az IP-alapú hangátvitel (Voice over IP, VoIP) számára például elsőbbséget kell biztosítani a web-böngészési forgalommal szemben.

Kattintsunk a Lejátszás gombra a tárol-és-továbbít folyamat megtekintéséhez!

The animation shows as source host sending a frame to a cut-through switch. The animation has a topology consisting of a Source host linked to a switch. The switch has a link to a destination host and a server. In the animation, the source host forwards a frame to the switch. The switch receives the frame and looks at its switching table to determine which interface to forward the frame. The switch then sends the frame to the destination host.

Source

Destination

Destination Address

Source Address

Data

CRC

7.4.2

## Közvetlen kapcsolás

A közvetlen kapcsolás esetén, amint megérkezik az adat, a switch máris továbbításba kezd, még ha az átvitel nem is teljes. A switch csak annyit tárol el a keretből, hogy ki tudja olvasni a cél MAC-címet annak meghatározásához, hogy melyik porton kell továbbítani az adatokat. A cél MAC-cím a keret első 6 bájtjában található, az előtagot követően. A switch megnézi a cél MAC-címet a kapcsolási táblájában, meghatározza a kimenő interfészt és továbbítja a keretet a rendeltetési helyére a kijelölt porton keresztül. Ilyenkor nem végez semmilyen hibaellenőrzést a kereten.

Kattintsunk a Lejátszás gombra a közvetlen kapcsolás folyamatának megtekintéséhez!

The animation shows as source host sending a frame to a store-and-forward switch. The switch computes the CRC and if valid sends the frame to the destination host. The animation has a topology consisting of a Source host linked to a switch. The switch has a link to a destination host and a server. In the animation, the source host shows the contents of the frame consisting of a destination address, source address, data and CRC. The frame is forwarded to the switch from the source host. The switch receives the frame and computes the CRC in the frame. The CRC in the packet is 435869123 and the computed CRC is 435869123, both matching. The switch says Frame is good and then looks at its switching table to determine which interface to forward the frame. The switch then sends the frame to the destination host.

Source

Destination

A közvetlen kapcsolásnak két változata van:

* **Gyorskapcsolás-** Ebben az esetben 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 azonban csak ritkán történik meg, a cél hálózati kártya pedig eldobja a hibás csomagot, amikor az beérkezik. 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 switch még a keret továbbítása előtt eltárolja az első 64 bájtot. A töredékmentes kapcsolás tulajdonképpen egy kompromisszum a tárol-és-továbbít módszer, 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.

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

7.4.3

## Memória pufferelés a switch-eken

Egy Ethernet kapcsoló különböző pufferelési technikákat alkalmazhat a keretek továbbítás előtti tárolására. Akkor is szükség lehet pufferelésre, ha torlódás miatt foglalt a célport. A switch addig tárolja a keretet, amíg továbbítható nem lesz.

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

### Memóriapufferelési módok

| Table caption | |
| --- | --- |
| **Módszer** | **Leírás** |
| **Port-alapú memória** | * A port-alapú memória pufferelésnél a kereteket az adott bejövő és kimenő portokhoz kapcsolódó várósorokban tárolják. * 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** | * Az összes keretet egy közös memória pufferbe helyezi, amelyet az összes switchport között megoszt, és a portok által igényelt puffermemória mennyiségét dinamikusan osztja el. * Így csomagokat lehet fogadni az egyik porton, majd továbbítani egy másikon anélkül, hogy egy másik várósorba kellene áthelyezni őket. |

A megosztott memóriapufferelés azt is eredményezi, hogy nagyobb keretek tárolhatók potenciálisan kevesebb számú eldobott keret mellett. Ez fontos az aszimmetrikus kapcsolásnál, amikor a különböző portok különböző adatátviteli sebességet használnak. Például, a kiszolgálót csatlakoztatjuk egy 10 Gbit/s kapcsolóporthoz, PC-ket pedig 1 Gbit/s sebességű portokhoz.

7.4.4

## Sebesség és duplexitás beállítások

Egy switch két legalapvetőbb beállítása a sávszélesség (néha „sebesség”) és a duplexitási értékek minden egyes kapcsolóporthoz. Fontos, hogy a duplexitás és sávszélesség beállítások egyezzenek a kapcsolóport és a csatlakoztatott eszközök, például egy számítógép vagy egy másik switch között.

Az Ethernet hálózatokon történő kommunikációra kétféle duplexitási beállítást használunk:

* **Full-duplex**- (teljes duplex): A kapcsolat mindkét vége egyszerre küldhet és fogadhat is.
* **Half-duplex**- (fél duplex): Egyszerre csak a kapcsolat egyik vége küldhet.

A legtöbb Ethernet switch-en és hálózati kártyán megtalálható az automatikus egyeztetési (auto negotiation) funkció. Ez lehetővé teszi a két kapcsolódó eszköz számára, hogy automatikusan beállítsák a legjobb sebességi és duplexitási képességeiket. A full-duplex akkor kerül kiválasztásra, ha mindkét eszköz rendelkezik ezzel a legnagyobb közös sávszélesség mellett.

Az ábrán a PC-A Ethernet NIC teljes duplex vagy fél duplex módban is működhet, és 10 Mbps vagy 100 Mbps sebességre képes.

S2

PC A

DuplexDuplexSpeedSpeedFullHalfFullHalf100 Mbps10 Mbps100 Mbps10 Mbps1000 MbpsPort 1AutonegotiationAutonegotiation

A PC-A az S2 switch-hez csatlakozik az 1-es porton, amely teljes vagy fél duplex, valamint 10 Mbps, 100 Mbps vagy 1000 Mbps (1 Gbps) üzemmódokra képes. Ha mindkét eszköz automatikus egyeztetést használ, akkor a működési üzemmód teljes duplex és 100 Mbps lesz.

**MEGJEGYZÉS**: A legtöbb Cisco switch és Ethernet hálózati kártya alapértelmezetten egyezteti a sebesség és duplexitás értékeket. A Gigabit Ethernet portok csak teljes duplex módban működnek.

A 10/100 Mbps Ethernet kapcsolatok teljesítményproblémáinak egyik leggyakoribb oka a duplexitás eltérés. Ez akkor fordul elő, ha a kapcsolat egyik portja fél duplex, míg a másik port teljes duplex módban működik (lásd ábra).

Switch S1 is connected to switch S2. S1 is operating in full-duplex and S2 is operating in half-duplex. A callout above S1 reads: Im full duplex so I can send whenever I want. A callout above S2 reads: Im half duplex so I can only send when the link is clear but I am also getting a lot of collisions! The graphic shows both switches sending data at the same time that has resulted in a collision.

S1

S2

Half-duplexFull-duplexI'm half-duplex so I can only send when the link is clear  
but I am also getting a lot of collisions!I'm full-duplex so I can send whenever I want.

Az S2 folyamatosan ütközéseket tapasztal, mivel az S1 bármikor továbbíthatja a kereteket.

A duplexitás eltérés akkor fordul elő, ha egy kapcsolaton belül az egyik vagy mindkét port visszaáll alaphelyzetbe, és az automatikus egyeztetési folyamat során nem sikerül a partnereknek azonos konfigurációt beállítani. hasonló probléma adódik, ha a felhasználók újrakonfigurálják a kapcsolat egyik oldalát, de elfelejtik újrakonfigurálni a másikat. A kapcsolat mindkét oldalán automatikus egyeztetést kell beállítani, vagy mindkét oldalon ki kell kapcsolni azt. A legjobb módszer az Ethernet switch portok teljes duplexre történő konfigurálása.

7.4.5

## Auto-MDIX

Az eszközök egymáshoz való csatlakoztatására egyenes- vagy keresztkötésű kábelt használnak. A szükséges kábel típusa az összekötendő eszközök típusától függ.

Az ábra például azokat a kábeltípusokat mutatja be, amelyek a switch-switch, a router-switch, állomás-switch vagy a router-állomás párosok összekapcsolásához szükségesek. A hasonló eszközök között keresztkötésű kábelt, a különböző típusú eszközök közötti csatlakoztatáshoz pedig egyenes kábelt alkalmaznak.

**MEGJEGYZÉS**: A router és az állomás közötti közvetlen kapcsolatnál keresztkötésű kábelre van szükség.

The diagram shows the correct cable type to use when connecting various types of networking devices together. From top to bottom, the devices and cable types are: switch to switch is a crossover cable; switch to router is a straight-through cable; switch to host is a straight-through cable; and router to host is a crossover cable.

Crossover cableStraight-through cableStraight-through cableCrossover cable

A legtöbb switch támogatja az Auto-MDIX funkciót. Ha ez engedélyezve van, a switch automatikusan észleli a porthoz csatlakoztatott kábel típusát, és ennek megfelelően konfigurálja az interfészeket. Ezért, függetlenül a kapcsolat másik végén lévő készülék típusától, kereszt- és egyenes kötésű kábelt is használhatunk a kapcsoló 10/100/1000 réz alapú portjaihoz.

Az automatikus MDIX-funkció alapértelmezés szerint engedélyezett a Cisco IOS 12.2(18)SE vagy újabb verziót futtató switch-eken. A funkció azonban le is tiltható. Ebben az esetben mindig a megfelelő kábeltípust használjuk. Az auto-MDIX újra engedélyezhető az **mdix auto** interfész konfigurációs paranccsal.

7.4.6

## Tudáspróba - Sebesség és kapcsolási módszerek

Az űrlap teteje

Check your understanding of switch speeds and forwarding methods by choosing the correct answer to the following questions.

1. What are two methods for switching data between ports on a switch? (Choose two.)

Az űrlap alja

Which switching method can be implemented using fast-forward switching or fragment-free switching?

Which two types of memory buffering techniques are used by switches? (Choose two.)

What feature automatically negotiates the best speed and duplex setting between interconnecting devices?

[7.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A MAC-címtábla](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[7.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                         

1. Ethernet kapcsolás
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

7.5.1

## Miről tanultunk ebben a fejezetben?

**Ethernet keret**

Az Ethernet az OSI-modell két rétegében működik: az adatkapcsolati és a fizikai rétegben. Az Ethernet szabványok mind a második rétegbeli protokollokat, mind pedig az első rétegbeli technológiákat meghatározzák. Az Ethernet az adatkapcsolati réteg LLC- és MAC-alrétegeit használja a működéshez. Az adatbeágyazás a következőket foglalja magában: Ethernet keretezés, Ethernet címzés és Ethernet hibaészlelés. Az Ethernet LAN switch-eket használ, amelyek teljes duplex módban működnek. Az Ethernet keret mezői a következők: előtag és keretkezdő, cél MAC-cím, forrás MAC-cím, Típus/Hossz, adatok és FCS.

**Ethernet MAC-címek**

A bináris számrendszerben két számjegyet használunk: a 0-át és az 1-et. A tízes számrendszerben 0 és 9 közötti számokat. A hexadecimális rendszer a 0-tól 9-ig terjedő számokat és az A-tól F-ig terjedő betűket használja. A MAC-cím a helyi hálózati szegmens forrás- és céleszközeinek (hálózati kártya, NIC) fizikai azonosítására szolgál. A MAC-címzés az OSI-modell adatkapcsolati rétegében biztosítja az eszközök megkülönböztethetőségét. Az Ethernet MAC-cím egy 48 bites érték, amelyet 12 hexadecimális számjegy használatával írunk le. Ez egy 6 jegyű, hexadecimális gyártói OUI-kóddal kezdődik, amelyet egy 6 hexadecimális jegyből álló, gyártó által generált érték követ. Amikor egy eszköz Ethernet-hálózatra továbbít egy üzenetet, az Ethernet-fejléc tartalmazza a forrás és a cél MAC-címeket. Az Etherneten belül különböző MAC-címeket használunk a második rétegbeli egyedi címzésű, szórásos és csoportos kommunikációra.

**A MAC-címtábla**

Egy switch a továbbítási döntéseket kizárólag a 2. rétegbeli Ethernet MAC-címek alapján hozza meg. A switch a bejövő keretek forrás MAC-címét megvizsgálva dinamikusan építi fel a MAC-cím táblát. A kereteket úgy továbbítja, hogy egyezést keres a keretben lévő cél MAC-cím és a MAC-címtábla egy bejegyzése között. Amikor egy switch különböző eszközöktől kap kereteket, kitölti a MAC-címtábláját a keretek forrás MAC-címe alapján. Ha a switch MAC-címtáblája tartalmazza a beérkező keret cél MAC-címét, felismeri a keretet, és továbbítja azt a megfelelő portjára.

**Switch kapcsolási módok és sebességek**

A switch-ek az alábbi továbbítási módszerek valamelyikét használják az adatok hálózati portok közötti kapcsolásához: tárol-és-továbbít, közvetlen kapcsolás. A közvetlen kapcsolás két formája a gyorstovábbítás (fast-forward) és a töredékmentes (fragment-free) kapcsolás. A memória pufferelésének két módja a port alapú memória és a megosztott memória. Az Ethernet hálózatokon történő kommunikációra kétféle duplexitási beállítást használunk: félduplex és teljes duplex. A legtöbb Ethernet switch-en és hálózati kártyán megtalálható az automatikus egyeztetési (auto negotiation) funkció. Ez lehetővé teszi a két kapcsolódó eszköz számára, hogy automatikusan beállítsák a legjobb sebességi és duplexitási képességeiket. A full-duplex akkor kerül kiválasztásra, ha mindkét eszköz rendelkezik ezzel a legnagyobb közös sávszélesség mellett. A legtöbb switch támogatja az Auto-MDIX funkciót. Ha ez engedélyezve van, a switch automatikusan észleli a porthoz csatlakoztatott kábel típusát, és ennek megfelelően konfigurálja az interfészeket.

7.5.2

## Ellenőrző kvíz - Ethernet kapcsolás

Az űrlap teteje

1. Melyik két állítás jellemzi az Ethernet technológiát? (Két jó válasz van.)

Az űrlap alja

Melyik állítás írja le a MAC-címek jellemzőjét?

Milyen különleges értéket rendelünk a csoportos címzésű MAC-cím első 24 bitjéhez?

Mit tesz egy állomás az Ethernet hálózaton, ha olyan keretet kap, amiben a cél MAC-cím nem egyezik meg a saját MAC-címével?

Melyik hálózati eszköz hoz továbbítási döntést a keretben található cél MAC-cím alapján?

Melyik hálózati eszköz rendelkezik azzal az elsődleges funkcióval, hogy adatokat küldjön egy adott helyre a MAC-címtáblázatban található információk alapján?

Melyik funkciót vagy műveletet végzi az LLC-alréteg?

Mit tesz a Cisco Ethernet switch az általa kapott runt (töredék) keretekkel?

Milyen címzési információkat rögzít egy switch, hogy létrehozza a MAC-címtáblát?

Mi az Auto-MDIX?

Milyen típusú cím a 01-00-5E-0A-00-02?

Melyik állítás igaz a MAC-címekre

Mekkora az Ethernet keret méretének két szélső értéke (minimum és maximum)? (Két jó válasz van.)

Melyik két állítás igaz a MAC alréteg feladataira? (Két jó válasz van.)

[7.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Switch kapcsolási sebességek és módok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                     
*                 

1. Hálózati réteg
2. Bevezetés

# Bevezetés

8.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Hálózati réteg fejezetben.

Mostanra már észrevehettük, hogy a kurzus fejezetei az OSI-modell alsó rétegétől indulva haladnak a felső rétegek felé. Az OSI-modell hálózati rétegén keresztül ismerkedünk meg a kommunikációs és az útválasztó protokollokkal. Tegyük fel, hogy e-mailt szeretnénk küldeni egy barátunknak, aki egy másik városban, vagy akár egy másik országban él. Ez a személy nem ugyanazon a hálózaton van, mint mi. Egy egyszerű kapcsolt hálózat nem tudja az üzenetünket a saját hálózatunkon túlra továbbítani. Segítségre van szükség ahhoz, hogy ez az üzenet egy útvonalon eljusson a barátunk eszközéhez. Ha e-mailt (videót vagy fájlt stb.) szeretnénk küldeni bárkinek, aki nem a helyi hálózaton található, hozzá kell férnünk egy routerhez. A routerek eléréséhez hálózati rétegbeli protokollokat kell használnunk. Ezen folyamatok könnyebb megértéséhez a fejezet két Wireshark feladatot is tartalmaz. Jó szórakozást hozzájuk!

8.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Hálózati réteg

**Fejezet célja:** Ismertetni, hogyan használják a routerek a hálózati réteg protokolljait és szolgáltatásait a végpontok közötti kapcsolat érdekében.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Hálózati réteg jellemzői** | Ismerteti, hogy a hálózati réteg milyen módon használja az IP-protokollokat a megbízható kommunikáció érdekében. |
| **IPv4-csomag** | Ismerteti az IPv4-csomagban található fő fejlécmezők szerepét. |
| **IPv6-csomag** | Ismerteti az IPv6-csomagban található fő fejlécmezők szerepét. |
| **Az állomás irányítótáblái** | Bemutatja, hogy a hálózati eszközök milyen módon használják az irányítótáblákat, amikor csomagokat továbbítanak a célhálózathoz. |
| **A router irányítótáblái** | Bemutatja a router irányítótábla mezőinek feladatait. |

[7.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózati réteg jellemzői](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                          
*                 

1. Hálózati réteg
2. A hálózati réteg jellemzői

# A hálózati réteg jellemzői

8.1.1

## A hálózati réteg

A hálózati réteg, más néven az OSI 3. rétege, olyan szolgáltatásokat biztosít, amelyek lehetővé teszik a végberendezések közötti kommunikációt a hálózatokon. Ahogy az ábrán is látható, a hálózati réteg két alapvető kommunikációs protokollja az IP-protokoll 4-es (IPv4) és 6-os (IPv6) verziója. A hálózati réteg más típusú protokolljai az irányító protokollok (például Open Shortest Path First, OSPF) és az üzenetküldő protokollok (például Internet Control Message Protocol, ICMP).

### A hálózati réteg protokolljai

7 6 5 4 3 2

1

* Internet Protocol version 4 (IPv4)
* Internet Protocol version 6 (IPv6)

ApplicationPresentationSessionTransportNetworkData LinkPhysical

A hálózati határokon átívelő, végpontok közötti kommunikáció megvalósításához a hálózati réteg protokolljai négy alapvető műveletet hajtanak végre:

* **Végberendezések címzése**- A végberendezéseken a hálózati azonosításhoz egyedi IP-címet kell beállítani.
* **Beágyazás-**A hálózati réteg egy csomagba ágyazza a szállítási rétegtől származó protokoll adategységet (PDU). A beágyazás során olyan IP-fejrész információk kerülnek hozzáadásra, mint például a forrás- és célállomás IP-címe. A beágyazási folyamatot az IP-csomag küldője hajtja végre.
* **Útválasztás-** A hálózati réteg szolgáltatásainak segítségével a csomagok egy másik hálózaton lévő célállomáshoz irányíthatók. A csomag másik hálózatba történő továbbításához routerre van szükség. A router feladata a célállomás felé vezető legjobb útvonal kiválasztása és a csomagok cél felé továbbítása. Ezt a folyamatot nevezzük útválasztásnak. A csomag számos routeren haladhat keresztül, mielőtt megérkezik a célállomáshoz. Minden egyes routert, amelyen a csomag áthalad a célállomáshoz vezető útvonalon, ugrásnak nevezzük.
* **Kicsomagolás -** Amikor a csomag megérkezik a célállomás hálózati rétegéhez, az állomás ellenőrzi a csomag IP-fejlécét. Ha a fejlécben lévő cél IP-cím megegyezik a saját IP-címével, akkor eltávolítja a csomagról az IP-fejlécet. A hálózati rétegben történő kicsomagolást követően a keletkezett 4. rétegbeli PDU a szállítási réteg megfelelő szolgáltatásához kerül. A kicsomagolási folyamatot az IP-csomag címzettje hajtja végre.

Míg a szállítási réteg (OSI 4. réteg) az állomásokon futó folyamatok közötti adattovábbítást kezeli, addig a hálózati réteg protokolljai (pl. az IPv4 és az IPv6) a csomagok felépítését és feldolgozását definiálja, ami az adatok állomásról állomásra történő továbbításához szükséges. A csomagokban szállított adatoktól független működésnek köszönhetően a hálózati réteg képes az állomások közötti különböző típusú kommunikáció továbbítására.

Az adatátvitelt bemutató animáció megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

Host

Host

Network layer protocols forward transport layer PDUs between hosts.

Encapsulation

Routing

De-encapsulation

Data

Segment

Packet

Frame

110101011011

Addressing

8.1.2

## IP-beágyazás

Az IP-protokoll IP-fejléc hozzáadásával ágyazza be a szállítási réteg (közvetlenül a hálózati réteg felett található réteg) szegmenseit vagy más adatokat. Ez a fejléc teszi lehetővé a csomag célállomáshoz való továbbítását.

Az ábra azt szemlélteti, hogy a szállítási rétegbeli protokoll adategység (PDU) hogyan ágyazódik be a hálózati rétegbeli PDU-ba, létrehozva ezzel egy IP-csomagot.

The illustration shows the transport layer PDU being encapsulated into an IP packet. At the top of the graphic is the transport layer encapsulation. It shows the segment header followed by data. This comprises the transport layer PDU. This is passed down to the network layer for further encapsulation and becomes the data part of the network layer PDU. An IP header is added in front of the data to create the IP packet.

DataIP HeaderDataSegment HeaderTransport Layer PDUTransport Layer EncapsulationNetwork Layer EncapsulationNetwork Layer PDUIP Packet

Az adatok rétegről rétegre történő becsomagolásának folyamata teszi lehetővé, hogy az egyes rétegek szolgáltatásai más rétegektől függetlenül fejlődjenek és bővüljenek. Ez azt jelenti, hogy a szállítási réteg szegmensei becsomagolhatók IPv4, IPv6 vagy akár egy új, a jövőben kifejlesztett protokoll segítségével.

A cél felé továbbítás során az IP-csomag fejlécét a 3. rétegbeli eszközök (azaz routerek és 3. rétegbeli switchek) vizsgálják meg. Fontos megjegyezni, hogy az IP-címzési információ változatlan marad attól kezdve, hogy a csomag elhagyja a forrásállomást midaddig, amíg meg nem érkezik a célállomásra, kivéve, ha egy IPv4 hálózati címfordítást (NAT) végző eszköz meg nem változtatja.

**MEGJEGYZÉS**: A NAT későbbi fejezetekben kerül ismertetésre.

A routerek útválasztó protokollokat alkalmaznak a csomagok hálózatok közötti továbbítására. A közvetítő eszközök által végzett irányítás során a hálózati rétegbeli címzés kerül vizsgálatra a csomag fejlécében. A csomag adat része (a szállítási rétegbeli PDU vagy más adat) a hálózati rétegbeli feldolgozás során minden esetben változatlan marad.

8.1.3

## Az IP tulajdonságai

Az IP-protokollt kis többletterhelésre tervezték. Éppen ezért, csak azokat a funkciókat biztosítja, amelyek feltétlenül szükségesek egy csomag forrástól a célig eljuttatásához összekapcsolt hálózatokon keresztül. A protokollnak nem feladata a csomagok nyomon követése és felügyelete. Ezeket a funkciókat szükség esetén más rétegbeli protokollok biztosítják, elsősorban a TCP a 4. rétegben.

Az IP alapvető tulajdonságai a következők:

* **Összeköttetés-mentes** - Az adatküldést megelőzően nem épül ki kapcsolat a küldő és a fogadó állomás között.
* **Legjobb szándékú** - IP alapvetően nem megbízható, mert a csomagok kézbesítése nem garantált.
* **Közegfüggetlen** - A működése független az adatok továbbítását végző közegtől (réz, száloptika vagy vezeték nélküli)

8.1.4

## Összeköttetés-mentes

Az IP összeköttetés-mentes, ami azt jelenti, hogy az adatküldést megelőzően a végpontok között nem épül ki külön kapcsolat. Az összeköttetés-mentes kommunikáció hasonló ahhoz, amikor egy levelet küldünk anélkül, hogy a címzettet előre értesítenénk róla. Az ábra ezt a kulcsfontosságú elemet vázolja fel.

a packet, consisting of an IP header and segment, is sent from a source on one network to a destination on another network

### Összeköttetés-mentes - Analógia

A letter is sent.LetterLetterMail box

Az összeköttetés-mentes kommunikáció is hasonló elven működik. Ahogy az ábrán is látható, IP esetén nincs szükség vezérlési információk cseréjére a csomagtovábbítás előtt a végpontok közötti kapcsolat kiépítéséhez.

### Összeköttetés-mentes - Hálózat

A packet is sent.IP headerSegmentIP headerSegment

8.1.5

## Legjobb szándék

IP esetén szintén nincsen szükség a fejrészben olyan további mezőkre, amelyek a felépített kapcsolat kezelését segítenék. Mindez nagy mértékben csökkenti az IP többletterhelését. Mivel nem épül fel kapcsolat a végpontok között, így a küldőnek nincs információja a megcímzett eszköz létezéséről vagy működéséről. Így arról sem, hogy a csomagja megérkezik-e vagy hogy a címzett fel tudja-e azt dolgozni.

Az IP-protokoll nem garantálja, hogy a küldött csomagokat ténylegesen megkapják-e. Az ábra az IP protokoll nem megbízható, más néven legjobb szándékú tulajdonságát szemlélteti.

The diagram shows a source on one network and a destination on another network. Between the two hosts is a cloud consisting of four routers in a mesh topology. Three IP packets leave the source host but only two arrive at the destination host. Text in the graphic reads: Packets are routed through the network quickly; Some Packets may be lost en route.

Packets are routed through the network quicklySome Packets may be lost en routeIP PacketIP PacketIP PacketIP PacketIP Packet

Nem megbízható hálózati rétegbeli protokollként az IP nem garantálja, hogy az összes elküldött csomag kézbesítésre kerül. Más protokollok kezelik a csomagok nyomon követésének folyamatát és azok kézbesítésének biztosítását.

8.1.6

## Közegfüggetlen

A nem megbízható annyit jelent, hogy az IP nem képes kezelni és helyreállítani a nem kézbesített vagy hibás csomagokat. Ez amiatt van, mert az IP-csomag a feladási helyen kívül semmilyen információt nem tartalmaz, ami alapján a küldőt értesíteni lehetne a sikeres kézbesítésről. Előfordulhat, hogy a csomagok hibásan, rossz sorrendben vagy egyáltalán nem érkeznek meg a célállomáshoz. Hiba esetén az IP nem biztosít lehetőséget a csomagok újraküldésére.

A rossz sorrendben érkező vagy elveszett csomagok esetén az adatot használó alkalmazások vagy magasabb rétegbeli szolgáltatások feladata a probléma megoldása. A fentieknek is köszönhetően az IP hatékony működésre képes. A TCP/IP protokollkészletben a megbízhatóságot a szállítási rétegben található TCP-protokoll biztosítja.

Az IP teljesen függetlenül működik az átviteli közegtől, ahol az alacsonyabb rétegekben zajló adatátvitel történik. Ahogy az ábrán is látható, az IP-csomagok továbbíthatók elektromos úton kábelen keresztül, optikai jelként üvegszálat használva, vagy vezeték nélküli környezetben rádió jelként.

The diagram shows a network topology within a cloud with a packet traveling over various media types between two hosts. An IP packet is shown moving between a host and a router over a copper Ethernet connection. The first router is connected to second router via a copper serial connection. An IP packet is shown moving between the second router and a third router over an optical fiber connection. The third router is connected to a fourth router, which is a wireless router. An IP packet is shown moving between the fourth router and a host over a wireless connection.

IP PacketIP PacketIP PacketCopper EthernetCopper SerialOptical FiberWirelessCopper Ethernet

IP packets can travel over different media.

Az OSI adatkapcsolati rétegének feladata az IP-csomagok fogadása és felkészítése az átviteli közegen történő továbbításra. Mindez azt jelenti, hogy az IP-csomagok továbbítása nincs korlátozva egyetlen átviteli közegre sem.

Az átviteli közeg egy fő jellemzőjét azonban figyelembe veszi a hálózati réteg: a közegen átvihető maximális PDU méretét. Ezt a jellemzőt nevezik maximális átviteli egységnek (Maximum Transmission Unit, MTU). A csomagok maximális méretének meghatározása az adatkapcsolati és a hálózati réteg közötti vezérlő kommunikáció során történik. Az adatkapcsolati réteg megadja a hálózati réteg számára az MTU értékét. A hálózati réteg pedig meghatározza a maximális csomagméretet.

Bizonyos esetekben a közvetítő eszköznek (általában egy routernek) át kell méreteznie az IPv4-csomagokat ahhoz, hogy egy kisebb MTU-értékkel rendelkező közegen továbbítani tudja őket. Ezt a folyamatot nevezik tördelésnek vagy feldarabolásnak (fragmentation). Ami késleltetést okoz. Az IPv6-csomagokat a router nem darabolhatja fel.

8.1.7

## Tudáspróba - Az IP jellemzői

Az űrlap teteje

Check your understanding of IP characteristics by choosing the correct answer to the following questions.

1. Which OSI layer sends segments to be encapsulated in an IPv4 or IPv6 packet?

Az űrlap alja

Which layer is responsible for taking an IP packet and preparing it for transmission over the communications medium?

What is the term for splitting up an IP packet when forwarding it from one medium to another medium with a smaller MTU?

Which delivery method does not guarantee that the packet will be delivered fully without errors?

[8.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IPv4-csomag](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                            
*                 

1. Hálózati réteg
2. Az IPv4-csomag

# Az IPv4-csomag

8.2.1

## Az IPv4-csomag fejléce

Az egyik elsődleges hálózati rétegbeli kommunikációs protokoll az IPv4. Az IPv4-csomag fejléce biztosítja azt, hogy a csomag a célállomás felé vezető úton a következő csomóponthoz kerüljön.

A fejléc mezői a csomagról tartalmaznak fontos információkat. Ezek a mezők bináris számokat tartalmaznak, amelyeket a 3. réteg dolgoz fel.

8.2.2

## Az IPv4-csomag fejléc mezői

Az egyes mezők bináris értékei az IP-csomag különböző tulajdonságait határozzák meg. Az alábbi protokoll fejlécdiagram a protokollmezőkről nyújt vizuális képet, kiolvasása balról jobbra és felülről lefelé történik. Az ábrán az IP-protokoll fejlécdiagramja látható, amely az IPv4-csomag mezőit azonosítja.

names and bit length of fields in an IPv4 packet header

### Az IPv4-csomag fejlécében található mezők

Byte 1Byte 2Byte 3Byte 4VersionInternet Header LengthDSDSCPECNTotal LengthIdentificationFlagFragment OffsetTime-to-LiveProtocolHeader ChecksumSource IP AddressDestination IP Address...20 Bytes

A legfontosabb IPv4-fejléc mezők a következők:

* **Verzió -** 4 bites bináris 0100 érték, amely mutatja, hogy IPv4-es a csomagról van szó.
* **Differenciált szolgáltatások (Differentiated Services, DS) -** A korábban szolgáltatás típusnak (Type of Service, ToS) nevezett DS-mező egy 8 bites érték, ami a csomagok prioritását adja meg. A DS-mező hat legmagasabb helyi értékű bitjei a differenciált szolgáltatások kódpont (Differentiated Services Code Point, DSCP) bitek, az utolsó két bit pedig az explicit torlódásjelző (Explicit Congestion Notification, ECN) bit.
* **Fejléc ellenőrzőösszeg (Header Checksum) —** Az IPv4-fejléc hibáinak érzékelésére szolgál.
* **Élettartam (Time-To-Live, TTL) –** A csomag élettartamát korlátozó 8 bites bináris szám. Az IPv4-csomag küldője állítja be a TTL kezdeti értékét. Értéke minden alkalommal eggyel csökken, amikor a csomagot egy router feldolgozza. Ha a TTL értéke nullára csökken, a router eldobja a csomagot és egy ICMP-időtúllépés (Time Exceeded) üzenetet küld a forrás állomásnak. Mivel a router minden csomag TTL-jét csökkenti, újra kell számolnia a fejléc ellenőrzőösszeget.
* **Protokoll —**Ez a mező a felsőbb rétegbeli protokoll azonosítására szolgál. 8 bites érték, ami meghatározza a csomagban szállított adattartalom típusát. Ennek segítségével továbbítja a hálózati réteg az adatot a megfelelő felsőbb rétegbeli protokoll számára. A leggyakoribb értékei: ICMP (1), TCP(6) és UDP (17).
* **Forrás IPv4-cím –** A csomag forrásállomásának IPv4-címét megadó 32 bites bináris szám. A forrás IPv4-cím mindig egyedi (unicast) cím.
* **Cél IPv4-cím –** A csomag célállomásának IPv4-címét megadó 32 bites bináris szám. A cél IPv4-cím lehet egyedi (unicast), csoportos (multicast) vagy szórásos (broadcast).

A két leggyakrabban emlegetett mező a forrás és cél IP-cím. Ezek határozzák meg, hogy a csomag honnan indult és hová tart. Általában ezek a címek nem változnak a forrástól a célállomásig vezető út során.

Az Internet fejléc hossz (Internet Header Length, IHL), a Teljes hossz (Total Length) és a Fejléc ellenőrzőösszeg (Header Checksum) mezők segítségével végezhető el a csomag azonosítása és ellenőrzése.

A többi mező a feldarabolt csomag sorba rendezésére használható. Az IPv4-csomag az Azonosítás (Identification), a Jelzők (Flags) és a Csomagdarab eltolás (Fragment Offset) mezőket használja a darabok nyomon követéséhez. Amikor a router egy kisebb MTU-értékkel rendelkező átviteli közegre továbbítja a csomagokat, akkor kisebb egységekre kell feldarabolnia őket.

Az Opciók (Options) és a Kitöltés (Padding) mezők használata igen ritka, így a tananyag ezeket nem tárgyalja.

8.2.3

## Videó — IPv4-fejléc példák a Wiresharkban

A Wiresharkban rögzített IPv4-csomagok fejléceinek vizsgálatáról szóló bemutató megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

8.2.4

## Tudáspróba - IPv4-csomag

Az űrlap teteje

Check your understanding of the IPv4 packet by choosing the correct answer to the following questions.

1. Which are the two most commonly referenced fields in an IPv4 packet header that indicate where the packet is coming from and where it is going? (Choose two.)

Az űrlap alja

Which statement is correct about IPv4 packet header fields?

Which field is used to detect corruption in the IPv4 header?

Which field includes common values such as ICMP (1), TCP (6), and UDP (17)?

[8.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A hálózati réteg jellemzői](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IPv6-csomag](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                
*                 

1. Hálózati réteg
2. Az IPv6-csomag

# Az IPv6-csomag

8.3.1

## Az IPv4 korlátai

Az IPv4 jelenleg is használatban van. Ez a fejezet az IPv6-ról szól, amely végül felváltja majd az IPv4-et. Az IPv4 korlátainak és az IPv6 előnyeinek megismerése segít annak megértésében, hogy miért van szükség az IPv6-protokollra.

Időről időre további protokollokat és folyamatokat fejlesztettek ki az új kihívások kezelésére. Mindezek ellenére az IPv4-nek három alapvető problémája még így is megmaradt:

* **Az IPv4-címek elfogyása -** Az IPv4 korlátozott számú egyedi nyilvános címmel rendelkezik. Bár megközelítőleg 4 billió IPv4-cím létezik, az IP-alapú eszközök számának növekedése, az állandó kapcsolatok és a fejlődő országok várható igényei nagyban megnövelték a szükséges címek számát.
* **Végponttól végpontig tartó kapcsolatok hiánya -** A hálózati címfordítás (NAT, Network Address Translation) az IPv4-hálózatokban gyakorta alkalmazott technológia. A NAT lehetővé teszi, hogy több eszköz egyetlen nyilvános IPv4-címet használjon. Bár a nyilvános IPv4-cím megosztott, a belső állomások IPv4-címe rejtve marad. Ez problémát okozhat a végponttól végpontig terjedő kapcsolatokat igénylő technológiák esetén .
* **Bonyolultabb hálózatok** — A NAT ugyan meghosszabbította az IPv4 élettartamát, de ez csak az IPv6-ra való átállás folyamatában jelentkezett. A NAT különböző megvalósításai további bonyolultságot teremtettek a hálózatban, késleltetést és a hibaelhárítás nehézségét eredményezve.

8.3.2

## Az IPv6 áttekintése

Az 1990-es évek elején az IETF (Internet Engineering Task Force) egyre nagyobb aggodalommal figyelte az IPv4 kapcsán felmerülő problémákat, és elkezdte keresni a megoldást. Ez vezetett az IPv6 kifejlesztéséhez. Az IPv6 megoldja az IPv4 problémáit, és egy olyan robusztus megoldást biztosít, amely tulajdonságainak köszönhetően alkalmasabb a jelenlegi és a várható hálózati kihívások megoldására.

Az IPv6 a következő kibővített tulajdonságokkal rendelkezik:

* **Megnövekedett címtér** - Az IPv6-címek 128 bites hierarchikus felépítésűek, ellentétben a 32 bites IPv4-címekkel.
* **Továbbfejlesztett csomagkezelés** - Az IPv6-fejléc kevesebb mezőt tartalmaz.
* **Nincs szükség címfordításra** - A nagy számú nyilvános IPv6-címnek köszönhetően nincs szükség a privát és publikus IPv4-címek közötti címfordításra (NAT). Ez kiküszöböli azokat a NAT-problémákat, amelyek a végpontól végpontig tartó kapcsolatot igénylő alkalmazásokat érintik.

A 32 bites IPv4-címtér megközelítőleg 4.294.967.296 egyedi címet tartalmaz. Az IPv6-címtartomány 340.282.366.920.938.463.463.374.607.431.768.211.456, vagyis 340 szextillió címet tartalmaz. Ez megközelítőleg annyi, mint a Föld összes homokszeme.

Az ábrán az IPv4- és az IPv6-címtér összehasonlítását láthatjuk.

comparison of IPv4 and IPv6 address space

### Az IPv4- és az IPv6-címtér összehasonlítása

| **Number Name** | **Scientific Notation** | **Number of Zeros** |
| --- | --- | --- |
| 1 Thousand | 10^3 | 1 000 |
| 1 Million | 10^6 | 1,000,000 |
| 1 Billion | 10^9 | 1,000,000,000 |
| 1 Trillion | 10^12 | 1,000,000,000,000 |
| 1 Quadrillion | 10^15 | 1,000,000,000,000,000 |
| 1 Quintillion | 10^18 | 1,000,000,000,000,000,000 |
| 1 Sextillion | 10^21 | 1,000,000,000,000,000,000,000 |
| 1 Septillion | 10^24 | 1,000,000,000,000,000,000,000,000 |
| 1 Octillion | 10^27 | 1,000,000,000,000,000,000,000,000,000 |
| 1 Nonillion | 10^30 | 1,000,000,000,000,000,000,000,000,000,000 |
| 1 Decillion | 10^33 | 1,000,000,000,000,000,000,000,000,000,000,000 |
| 1 Undecillion | 10^36 | 1,000,000,000,000,000,000,000,000,000,000,000,000 |

**Legend**There are 4 billion IPv4 addressesThere are 340 undecillion IPv6 addresses

8.3.3

## IPv4- és az IPv6-csomag fejléce

Az IPv6 esetén a legfőbb tervezési változás az IPv4-hez képest az egyszerűsített fejléc.

Például, az IPv4-fejléc változó hosszúságú, 12 alapvető mezőből áll, és legalább 20 oktett nagyságú (maximum 60 byte az Opciók mezővel együtt).

Az ábrán látható, hogy IPv6 esetén néhány IPv4-mező változatlan maradt, némelyikük neve és elhelyezkedése megváltozott, és vannak amikre már nincs szükség .

The diagram shows an IPv4 packet header and indicates which fields kept the same name, which fields changed names and position, and which fields were not kept in IPv6. The fields that kept the same name are: version, source address, and destination address. The fields that changed names and position are: type of service, total length, time-to-live, and protocol. The fields that were not kept in IPv6 are: IHL, identification, flags, fragment offset, header checksum, options, and padding.

### Az IPv4-csomag fejléce

Byte 1Byte 2Byte 3Byte 4VersionIHLType of ServiceOptionsPaddingTotal LengthDestination Address**Legend**- Fields name kept from IPv4 to IPv6IdentificationFlagsFragment OffsetTime-to-LiveProtocolHeader ChecksumSource Address- Name and position changed in IPv6 - Fields no longer required in IPv620 Bytes

The figure shows IPv4 packet header fields that were kept, moved, changed, as well as those that were not kept in the IPv6 packet header.

Ezzel szemben az egyszerűsített IPv6-fejléc fixen 40 oktett méretű (nagyrészt a forrás és a cél IPv6-címek mérete miatt).

Az IPv6 egyszerűsített fejléce lehetővé teszi annak hatékonyabb feldolgozását.

The diagram shows an IPv6 packet header and indicates which fields kept the same name from IPv4 to IPv6, which fields changed names and position in IPv6, which fields were not kept in IPv6, and new fields in IPv6. The field names that were kept the same are: version, source IP address, and destination IP address. The fields that changed names and position in IPv6 are: traffic class, payload length, next header, and hop limit. The field that is NEW to IPv6 is flow label.

### Az IPv6-csomag fejléce

Byte 1Byte 2Byte 3Byte 4VersionTraffic ClassFlow LabelNext HeaderPayload LengthHop LimitDestination IP AddressSource IP Address- Fields name kept from IPv4 to IPv6- Name and position changed in IPv6 - Fields no longer required in IPv6**Legend**40 bytes

The figure shows the IPv4 packet header fields that were kept or moved along with the new IPv6 packet header fields.

8.3.4

## Az IPv6-csomag fejléce

Az ábrán az IP-protokoll fejléc látható, amely az IPv6-csomag mezőit azonosítja.

names and bit length of fields in an IPv6 header

### Fields in the IPv6 Packet Header

Byte 1Byte 2Byte 3Byte 4VersionTraffic ClassFlow LabelNext HeaderPayload LengthHop LimitDestination IP AddressSource IP Address40 Bytes

A IPv6-fejléc mezői a következők:

* **Verzió -** 4 bites bináris 0110 érték, amely mutatja, hogy IPv6-os a csomagról van szó.
* **Forgalom osztály (Traffic Class) -** Ez a 8 bit megegyezik az IPv4-fejléc differenciált szolgáltatások (Differentiated Services, DS) mezőjével.
* **Folyamcímke (Flow Label) -**Ez a 20 bites mező azt jelenti, hogy az azonos folyamcímkével rendelkező csomagokat egyformán kezeljék a routerek.
* **Adatmező hossza (Payload Length) -**Ez a 16 bites mező jelzi az IPv6-csomag adat részének vagyis a hasznos tehernek a méretét. A fix 40 bájt méretű IPv6-fejlécet nem tartalmazza.
* **Következő fejléc (Next Header) -**Ez a 8 bites mező megegyezik az IPv4 Protokoll mezőjével. Ez adja meg a csomagban lévő adattartalom típusát, lehetővé téve ezzel a hálózati réteg számára, hogy az adatokat a megfelelő felsőbb rétegbeli protokollnak továbbítsa.
* **Ugrás korlát (Hop Limit)** - Ez a 8 bit felel meg az IPv4-csomag TTL-mezőjének. Értéke mindig eggyel csökken, amikor egy router továbbítja a csomagot. Amikor a számláló értéke eléri a 0-át, a csomag eldobásra kerül, a küldő állomás pedig egy ICMPv6 időtúllépés üzenettel értesül erről. Ez azt jelzi, hogy a csomag nem érte el a célját, mert túllépte az ugráskorlátot. Az IPv4-től eltérően az IPv6 nem tartalmaz IPv6 fejléc ellenőrző összeget, mivel ez a funkció az alsóbb és a felsőbb rétegekben egyaránt működik. Tehát az ellenőrző összeget nem kell minden routernek újraszámolnia, amikor csökkenti az ugráskorlát értékét, ami szintén javítja a hálózati teljesítményt.
* **Forrás IPv6-cím -** Ez a 128 bites mező tartalmazza a küldő állomás IPv6-címét.
* **Cél IPv6-cím -** Ez a 128 bites mező tartalmazza a fogadó állomás IPv6-címét.

Az IPv6-csomag kiterjesztett fejrészt (Extension Header, EH) is tartalmazhat, ami opcionális hálózati réteg információkat biztosít. Ez a kiterjesztett fejrész opcionális és az IPv6-fejrész és az adat között helyezkedhet el. Használják például csomagok feldarabolása vagy biztonság és mobilitás támogatás esetén is.

Az IPv4-től eltérően a routerek nem darabolják a továbbított IPv6-csomagokat.

8.3.5

## Videó — IPv6-fejléc példák a Wiresharkban

A Wiresharkban rögzített IPv6-csomagok fejléceinek vizsgálatáról szóló bemutató megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

8.3.6

## Tudáspróba - IPv6-csomag

Az űrlap teteje

Check your understanding of the IPv6 packet by choosing the correct answer to the following questions.

1. Which three options are major issues associated with IPv4? (Choose three.)

Az űrlap alja

Which two options are improvements provided by IPv6 as compared to IPv4? (Choose two.)

Which is true of the IPv6 header?

Which is true of the IPv6 packet header?

[8.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IPv4-csomag](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az állomás irányítótáblája](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                   
*                 

1. Hálózati réteg
2. Az állomás irányítótáblája

# Az állomás irányítótáblája

8.4.1

## Az állomás csomagtovábbítási döntései

A csomagokat IPv4 és IPv6 esetén is egy forrásállomás hozza létre. A forrásállomásnak képesnek kell lennie arra, hogy a csomagot a célállomás felé továbbítsa. Ehhez az állomások saját irányítótáblát hoznak létre. Ez a fejezet bemutatja, hogyan használják a végberendezések az útválasztó táblákat.

A hálózati réteg másik feladata a csomagok állomások közötti irányítása. Egy állomás által küldött csomag címzettje lehet:

* **Saját maga** - Egy állomás képes saját magát megpingelni úgy, hogy a csomagot egy speciális IPv4- (127.0.0.1) vagy IPv6-címre (::/1) küldi. Ezt visszahurkolási (loopback) interfésznek nevezzük. A loopback interfész pingelése a TCP/IP-protokollkészletet teszteli az állomáson.
* **Helyi állomás** - A küldő- és a célállomás ugyanazon a helyi hálózaton van. A két állomás hálózati címe azonos.
* **Távoli állomás** - A célállomás egy távoli hálózaton található. A két állomás hálózati címe különböző.

Az ábra azt mutatja, hogy a PC1 egy vele azonos hálózaton lévő helyi állomáshoz, és egy másik hálózatban található távoli állomáshoz csatlakozik.

The diagram shows a host, PC1, connecting to a local host, PC2, on the same network and to a remote host, a server, on another network. PC1 and PC2 are connected to a switch on network 192.168.10.0/24. PC1 has an address of .10 and PC2 has an address of .15. The switch is connected to a router, R1, at address .1. On the other side of the R1 is a connection to the cloud where the remote host resides.

PC1 R1 .10 .1 PC2

.15

Local  
HostRemote  
Host192.168.10.0/24

A küldő eszköz határozza meg, hogy a csomagot egy helyi vagy egy távoli állomáshoz kell-e továbbítani. Ez az eszköz állapítja meg azt is, hogy a cél IP-címe ugyanazon a hálózaton van-e, amelyen maga a küldő is található. A meghatározás módja az IP-protokoll verziójától függően változik:

* **IPv4 esetén** - A küldő eszköz a saját alhálózati maszkját és IPv4-címét, valamint a cél IPv4-címét használva hozza meg ezt a döntést.
* **IPv6 esetén** - A helyi router hirdeti a helyi hálózati címet (előtagot) a hálózat összes állomása számára.

Otthoni vagy vállalati hálózatokban számos vezetékes és vezeték nélküli eszköz kapcsolódik össze közvetítő hálózati eszköz, például LAN-switch és/vagy vezeték nélküli hozzáférési pont (Wireless Access Point, WAP) segítségével. Ezek a köztes eszközök biztosítják a kapcsolatot a helyi hálózat állomásai között. A helyi állomások további eszközök használata nélkül képesek egymást elérni és információt megosztani. Amikor egy állomás a vele azonos hálózaton lévő másik állomásnak küld üzenetet, a csomag az állomás interfészéről a közvetítő eszközön keresztül a célállomáshoz kerül továbbításra.

A legtöbb esetben szeretnénk, hogy eszközeink a helyi hálózaton kívüli állomásokhoz, vállalatokhoz és az internethez is csatlakozni tudjanak. A helyi hálózaton kívüli berendezéseket távoli állomásoknak nevezzük. Amikor egy állomás távoli célállomásnak küld üzenetet, akkor routerre és útválasztásra (routing) van szükség. Az irányítási folyamat feladata a legjobb útvonal megtalálása a célállomáshoz. A helyi hálózati szegmenshez csatlakozó routert alapértelmezett átjárónak nevezzük.

8.4.2

## Alapértelmezett átjáró

Az alapértelmezett átjáró az a hálózati eszköz (router vagy 3. rétegbeli switch), amely más hálózatokba irányítja a forgalmat. Ha a hálózatot egy szobához hasonlítjuk, akkor az alapértelmezett átjáró olyan, mint egy ajtó. Ha egy másik helyiségbe vagy hálózatba szeretnénk eljutni, akkor meg kell találnunk az ajtót.

A hálózatban az alapértelmezett átjáró általában egy router a következő funkciókkal:

* Rendelkezik egy helyi IP-címmel, amely ugyanabban a címtartományban van, mint a helyi hálózat többi állomása.
* Fogadja a helyi hálózatba irányuló adatokat, és továbbítja a helyi hálózatból érkező adatokat.
* Más hálózatok felé irányítja a forgalmat.

A helyi hálózaton kívüli forgalom továbbításához alapértelmezett átjáróra van szükség. A forgalom nem továbbítható a helyi hálózaton kívülre, ha nincs alapértelmezett átjáró, a címe nincs beállítva, vagy az alapértelmezett átjáró le van kapcsolva.

8.4.3

## Az állomás kommunikációja az alapértelmezett átjáróval

Egy állomás irányítótáblája általában tartalmaz alapértelmezett átjárót. IPv4 esetén az állomás az alapértelmezett átjáró IPv4-címét a DHCP-protokolltól kapja meg, vagy manuálisan állítják be rajta. IPv6 esetén az alapértelmezett átjáró címét a router hirdeti, vagy kézzel állítják be az állomáson.

Az ábrán a PC1 és a PC2 állomásokon a 192.168.10.1 IPv4-cím van alapértelmezett átjáróként beállítva.

The diagram shows two hosts, PC1 and PC2, connected to a switch on network 192.168.10.0/24, the local network route. The switch is connected to a router, R1, which is then connected to the cloud representing remote networks. PC1 has an address of .10, PC2 has an address of .15, and the router interface to which the switch is connected has an address of .1. The PCs, the switch, and the router interface all have a direct connection.

.10 .1 192.168.10.0/24 .15 PC1 R1

PC2

Local Network RouteRemote NetworksDirect Connection

Az alapértelmezett átjáró beállítása egy alapértelmezett útvonalat hoz létre a számítógép irányítótáblájában. Az alapértelmezett útvonal azt az útvonalat jelöli, amelyet a számítógép egy távol hálózathoz való csatlakozáshoz használ.

A PC1 és PC2 állomások egyaránt rendelkeznek alapértelmezett útvonallal, amely minden távoli hálózatba szánt forgalmat az R1 felé küld.

8.4.4

## Az állomás irányítótáblája

Egy Windows számítógépen a **route print** vagy a **netstat -r** parancs használható az állomás irányítótáblájának megjelenítésére. A két parancs kimenete megegyezik. A kimenet első ránézésre bonyolultnak tűnhet, azonban könnyen megérthető.

Az ábrán egy minta topológia és a **netstat –r** parancs kimenete látható.

The diagram shows a network topology consisting of a host, PC1, connected to a switch on network 192.168.10.0/24. The switch is connected to a router, R1, which is then connected to the cloud. PC1 has an address of .10 and the router interface to which the switch is connected has an address of .1.

192.168.10.0/24 .10 .1 PC1

R1

### PC1 IPv4 irányítótáblája

C:\Users\PC1> **netstat -r**

(output omitted)

IPv4 Route Table

===========================================================================

Active Routes:

Network Destination Netmask Gateway Interface Metric

0.0.0.0 0.0.0.0 192.168.10.1 192.168.10.10 25

127.0.0.0 255.0.0.0 On-link 127.0.0.1 306

127.0.0.1 255.255.255.255 On-link 127.0.0.1 306

127.255.255.255 255.255.255.255 On-link 127.0.0.1 306

192.168.10.0 255.255.255.0 On-link 192.168.10.10 281

192.168.10.10 255.255.255.255 On-link 192.168.10.10 281

192.168.10.255 255.255.255.255 On-link 192.168.10.10 281

224.0.0.0 240.0.0.0 On-link 127.0.0.1 306

224.0.0.0 240.0.0.0 On-link 192.168.10.10 281

255.255.255.255 255.255.255.255 On-link 127.0.0.1 306

255.255.255.255 255.255.255.255 On-link 192.168.10.10 281

(output omitted)

**MEGJEGYZÉS:** A parancskimenet csak az IPv4-irányítótáblát jeleníti meg.

A **netstat -r**vagy a vele egyenértékű **route print** parancsok az aktuális TCP/IP hálózati kapcsolatokra vonatkozóan az alábbi három információt jelenítik meg:

* **Interfész lista -** Megadja az állomás minden hálózati interfészének (Ethernet, Wi-Fi és Bluetooth) MAC-címét és hozzárendelt interfész azonosítóját.
* **IPv4-irányítótábla -** Tartalmazza az állomás által ismert összes IPv4-útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.
* **IPv6-irányítótábla -** Tartalmazza az állomás által ismert összes IPv6-útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.

8.4.5

## Tudáspróba - Az állomás irányítótáblája

Az űrlap teteje

Check your understanding of how a host routes by choosing the correct answer to the following questions.

1. Which statement about host forwarding decisions is true?

Az űrlap alja

Which default gateway statement is true?

Which two commands could be entered on a Windows host to view its IPv4 and IPv6 routing table? (Choose two.)

[8.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az IPv6-csomag](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés a forgalomirányításba](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                        
*                 

1. Hálózati réteg
2. Bevezetés a forgalomirányításba

# Bevezetés a forgalomirányításba

8.5.1

## A router csomagtovábbítási döntései

Az előző fejezet az állomás irányítótábláiról szólt. A legtöbb hálózat routereket is tartalmaz, amelyek közvetítő eszközök. A routerek szintén rendelkeznek irányítótáblával. Ez a fejezet a routerek hálózati rétegbeli működésével foglalkozik. Amikor egy állomás csomagot küld egy másik állomásnak, akkor az irányítótáblája segítségével dönti el, hogy hova továbbítsa azt. Ha a célállomás egy távoli hálózaton van, akkor a csomagot az alapértelmezett átjárónak kell küldeni, ami általában a helyi hálózatban lévő router.

Mi történik, ha egy csomag érkezik egy router interfészére?

Megvizsgálja a csomag cél IP-címét, és megkeresi az irányítótáblában, hogy hova továbbítsa a csomagot. Az irányítótábla tartalmazza az összes ismert hálózati cím (előtag) listáját, és a csomagok továbbításának helyét. Ezeket a bejegyzéseket útvonal-bejegyzéseknek vagy útvonalaknak nevezzük. A router a csomagot a legjobb (leghosszabb) egyezést mutató útvonal-bejegyzés alapján küldi tovább.

The diagram is a network topology showing what happens to an IPv4 packet as it is routed between networks. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A packet with destination IPv4 address 10.1.1.10 is sent from PC1 to R1. R1 then sends the packet with destination IPv4 address 10.1.1.10 to R2.

1 3 2 PC2 R2 .10 .1 .1 G0/0/1 .226 .10 209.165.200.224/30 192.168.10.0/24 10.1.1.0/24 R1 .225 G0/0/0

PC1

InternetDestination IPv4 Address:  
10.1.1.10Destination IPv4 Address:  
10.1.1.10

1. Csomag érkezik az R1 GigabitEthernet 0/0/0 interfészére. R1 kicsomagolja a 2. rétegbeli Ethernet keretet (eltávolítja a fejlécet és az utótagot).
2. R1 megvizsgálja a csomag IPv4-célcímét, és az IPv4-irányítótáblában megkeresi a legjobb egyezést. Az útvonalbejegyzés alapján ezt a csomagot az R2 routernek kell továbbítani.
3. R1 beágyazza a csomagot egy új Ethernet keretbe, majd továbbítja azt a következő ugrás routernek, azaz R2-nek.

Az alábbi táblázat az R1 irányítótáblájában található információkat mutatja.

### R1 irányítótáblája

| Table caption | |
| --- | --- |
| **Route** | **Next Hop or  Exit Interface** |
| 192.168.10.0 /24 | G0/0/0 |
| 209.165.200.224/30 | G0/0/1 |
| **10.1.1.0/24** | **via R2** |
| Default Route 0.0.0.0/0 | via R2 |

8.5.2

## A router irányítótáblája

A router irányítótáblája hálózati útvonalbejegyzéseket tartalmaz az összes lehetséges hálózati célhoz.

Az irányítótábla háromféle útvonalbejegyzést tartalmaz:

* **Közvetlenül csatlakozó hálózatok -** Ezek a hálózati útvonalak aktív router interfészeket jelölnek. A router akkor jegyez be a táblájába közvetlenül csatlakozó útvonalat, amikor egy interfésze aktívvá válik és van IP-címe. A router minden interfésze külön hálózathoz kell tartozzon. Az ábrán látható topológiában az R1 IPv4-irányítótáblájában a közvetlenül csatlakozó hálózatok a 192.168.10.0/24 és a 209.165.200.224/30.
* **Távoli hálózatok -** Ezek az útvonalbejegyzések más routerekhez csatlakozó hálózatokat jelölnek. A routerek a rendszergazda kézi beállításának eredményeként vagy dinamikus forgalomirányító protokollok útvonalinformációinak cseréjével ismerhetik meg a távoli hálózatokat. Az ábrán látható topológiában az R1 router IPv4-irányítótáblájában a 10.1.1.0/24 egy távoli hálózat.
* **Alapértelmezett útvonal** — Az állomáshoz hasonlóan a legtöbb router is tartalmaz alapértelmezett útvonalat, úgynevezett végső átjárót. Az alapértelmezett útvonal akkor használatos, ha nincs jobb (hosszabb) egyezés az IP-irányítótábla bejegyzéseivel. Az ábrán látható topológiában R1 irányítótáblája valószínűleg tartalmaz egy alapértelmezett útvonalat, amely az összes csomagot az R2 routerhez továbbítja.

Az ábrán az R1 router közvetlenül csatlakozó és távoli hálózatai láthatók.

The diagram is a network topology identifying directly connected networks and remote networks of a router. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226 on G0/0/1. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. Networks 192.168.10.0/24 and 209.165.200.224/30 are shown as directly connected networks to R1 and network 10.1.2.0/24 (should this be 10.1.1.0/24?) is shown as a remote network to R2.

.10 .1 .1 G0/0/1 .226 .10 209.165.200.224/30 192.168.10.0/24 10.1.1.0/24 .225 G0/0/0 G0/0/0 G0/0/1 PC2 R2 R1

PC1

InternetDirectly connnected networkDirectly connnected networkRemote Network

R1 két közvetlenül csatlakozó hálózattal rendelkezik:

* 192.168.10.0/24
* 209.165.200.224/30

R1 olyan távoli hálózatokkal is rendelkezik (például a 10.1.1.0/24 és az internet), amelyeket valahonnan megtanult.

Egy router a távoli hálózatokat kétféleképpen ismerheti meg:

* **Manuálisan** - A távoli hálózatok statikus útvonalként, manuálisan megadva kerülnek az irányítótáblába.
* **Dinamikusan** - A távoli hálózatokról a router egy dinamikus irányító protokoll segítségével értesül.

8.5.3

## Statikus forgalomirányítás

A statikus útvonalak olyan bejegyzések, amelyeket manuálisan állítunk be. Az ábra egy olyan statikus útvonalra mutat példát, amelyet manuálisan konfiguráltak az R1 routeren. A statikus útvonal tartalmazza a távoli hálózat címét és a következő ugrás router IP-címét.

The diagram is a network topology showing a static route configuration to reach a remote network. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud. A static route configuration on R1 to the network 10.1.1.0/24 reads: R1(config)#ip route 10.1.1.0 255.255.255.0 209.165.200.226. In the configuration, 10.1.1.0 255.255.255.0 is labeled remote network and 209.165.200.226 is labeled IP address of next hop router.

R1(config)# ip route 10.1.1.0 255.255.255.0 209.165.200.226 .10 .1 .1 G0/0/1 .226 .10 209.165.200.224/30 192.168.10.0/24 10.1.1.0/24 .225 G0/0/0 PC2 R2 R1

PC1

InternetRemote network addressIP adress of next hop router

Az R1 routeren kézzel be van állítva egy statikus útvonal a 10.1.1.0/24 hálózat elérésére. Ha ez az útvonal megváltozik, R1-nek új statikus útvonalra lesz szüksége.

A statikus útvonalak nem frissülnek automatikusan, a topológia megváltozásakor kézzel kell őket újra beállítani. Például, az ábrán az R1 tartalmaz egy statikus útvonalat a 10.1.1.0/24 hálózathoz R2-n keresztül. Ha ez az útvonal már nem érhető el, R1-en új statikus útvonalat kell létrehozni a 10.1.1.0/24 hálózathoz az R3 routeren keresztül. Az R3 routernek tehát rendelkeznie kell egy bejegyzéssel az irányítótáblájában, amely a 10.1.1.0/24 hálózatba szánt csomagokat R2-nek küldi.

The diagram is a network topology showing a failed link in a static route. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. R1 is connected to router R2 and router R3 which are also directed connected. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. A static route has been configured on R1 that points to R2 as the next hop. A red X indicates that this link has failed.

.10 .1 192.168.10.0/24 G0/0/0 PC2 R2 R1 PC1 R3 10.1.1.0/24

.10

Statikus útvonal

Ha az R1 és az R2 közötti kapcsolat megszakad, új statikus útvonalat kell létrehozni az R3-on keresztül. A statikus útvonal nem alkalmazkodik automatikusan a topológia változásaihoz.

A statikus útvonalak a következő jellemzőkkel rendelkeznek:

* Kézzel kell őket létrehozni.
* Ha egy statikus útvonal elérhetetlenné válik a topológia változásakor, akkor a rendszergazdának létre kell hoznia egy újat.
* Megfelelőek kisméretű hálózatban és ott, ahol a redundáns kapcsolatok száma kevés vagy nincs is.
* Általában egy dinamikus forgalomirányító protokollal együtt használják alapértelmezett útvonal létrehozásához.

8.5.4

## Dinamikus forgalomirányítás

Egy dinamikus útválasztó protokoll lehetővé teszi a routerek számára, hogy más routerektől automatikusan megtanulják a távoli hálózatokat, és az alapértelmezett útvonalakat. A dinamikus forgalomirányító protokollt használó routerek automatikusan cserélnek információkat egymás között, és a hálózati rendszergazda beavatkozása nélkül képesek a topológia változásaihoz alkalmazkodni. Ha változás következik be a hálózati topológiában, a routerek dinamikus irányító protokoll használatával megosztják ezt az információt egymással, és automatikusan frissítik az irányítótáblájukat.

A dinamikus útválasztó protokollok közé tartozik az OSPF (Open Shortest Path First) és az EIGRP (Enhanced Interior Gateway Routing Protocol). Az ábrán egy példa látható arra, ahogy az R1 és az R2 routerek automatikusan megosztják egymással a hálózati információkat OSPF-protokoll segítségével.

The diagram is a network topology showing routers using dynamic routing protocols to exchange information. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 has an interface with address .1 connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. Arrows show R1 and R2 sharing information with each other.

.10 .1 .1 G0/0/1 .226 .10 209.165.200.224/30 192.168.10.0/24 10.1.1.0/24 .225 G0/0/0 PC2 R2 R1

PC1

* R1 az OSPF-forgalomirányító protokollt használja, hogy hirdetést küldjön R2-ek a 192.168.10.0/24 hálózatról.
* R2 az OSPF-forgalomirányító protokollt használja, hogy hirdetést küldjön R1-ek a 10.1.1.0/24 hálózatról.

Az alapbeállításokhoz a hálózati rendszergazdának csak engedélyeznie kell a közvetlenül csatlakozó hálózatokat a dinamikus forgalomirányító protokollon belül. A dinamikus protokoll a következőket hajtja végre automatikusan:

* Távoli hálózatok felderítése
* Az aktuális irányítási információk karbantartása
* A célhálózatokhoz vezető legjobb útvonal kiválasztása
* Az aktuális útvonal elérhetetlenné válása esetén egy új legjobb útvonal keresése

Az irányítótáblába a távoli hálózat címe és a következő ugrás IP-címe kerül bele. Ez származhat a routeren kézzel létrehozott statikus útvonalból, vagy a dinamikus forgalomirányító protokoll használatával automatikusan megtanult távoli hálózatból. Ahogy az ábrán is látható, a hálózati topológia megváltozását a routerek automatikusan érzékelik és megpróbálnak új legjobb útvonalat találni.

The diagram shows a network topology in which routers using dynamic routing protocols are adjusting best paths after a topology change. Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. R1 is connected to router R2 and router R3 which are also directed connected. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. A red X indicates that the link between R1 and R2, labeled as the previous best path, has failed. A new best path is shown going from R1 to R3 to R2.

.10 .1 192.168.10.0/24 G0/0/0 PC2 R2 R1 PC1 R3 10.1.1.0/24

.10

Previous best pathNew best path

Az R1, az R2 és az R3 routerek OSPF dinamikus forgalomirányító protokollt használnak. A hálózati topológia változásakor automatikusan egy új legjobb útvonalat próbálnak keresni.

**MEGJEGYZÉS**: Számos router esetén előfordul, hogy statikus útvonalakat és dinamikus forgalomirányító protokollt is használ.

8.5.5

## Videó - A router irányítótáblái

Az állomás irányítótáblájával ellentétben, itt nincsenek oszlopfejlécek, amik az útválasztó táblában szereplő információkat azonosítják. Ezért fontos megtanulni a bejegyzésekben szereplő különböző elemek jelentését.

Az IPv4-irányítótábláról szóló bemutató megtekintéséhez kattintsuk az ábrán látható Lejátszás gombra!

8.5.6

## Az IPv4-irányítótábla bemutatása

Figyeljük meg az ábrán, hogy R2 az internethez csatlakozik. Ezért a rendszergazda az R1-en létrehozott egy alapértelmezett statikus útvonalat, amely az R2-nek továbbítja a csomagokat, ha nincs a cél IP-címnek megfelelő konkrét bejegyzés az irányítótáblában. Az R1 és az R2 routerek OSPF-protokollt használnak a közvetlenül csatlakozó hálózatok hirdetésére.

Host PC1, with an address of .10, is connected to a switch on network 192.168.10.0/24 which is connected to the G0/0/0 interface of router R1 with an address of .1. Network 209.165.200.224/30 connects the G0/0/1 interface on R1, address .225, to another router, R2 at address .226. R2 is connected to a switch on network 10.1.1.0/24 to which host PC2, address .10, is connected. R2 also has a connection to the Internet cloud.

.10 .1 .1 G0/0/1 .226 .10 209.165.200.224/30 192.168.10.0/24 10.1.1.0/24 .225 G0/0/0 PC2 R2 R1

PC1

Internet

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1

10.0.0.0/24 is subnetted, 1 subnets

O 10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/1

L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/1

R1#

A **show ip route** EXEC módbeli parancs segítségével megtekinthetjük az IPv4-irányítótáblát egy Cisco IOS-routeren. A példa az R1 router IPv4-irányítótábláját mutatja. Minden irányítótábla bejegyzés előtt egy kód található, amely azonosítja az útvonal típusát vagy az útvonal megtanulásának módját. Az útvonalak forrásai (kódjai) a következők:

* **L** - Közvetlenül csatlakozó helyi interfész IP-címe
* **C** – Közvetlenül csatlakozó hálózat
* **S** – A rendszergazda által kézzel létrehozott statikus útvonal
* **O** - OSPF
* **D** - EIGRP

Az irányítótábla az összes IPv4-útvonalat megjeleníti, amit az R1 ismer.

A közvetlenül csatlakozó útvonal automatikusan létrejön, amikor egy router interfész aktívvá válik és IP-címet állítunk be rajta. A router két útvonalbejegyzést ad hozzá a C (csatlakozó hálózat) és az L (csatlakozó hálózat helyi interfészének IP-címe) kódokkal. Az útvonalbejegyzések azt a kimenő interfészt is meghatározzák, amelyet a hálózat eléréséhez használni kell. Ebben a példában a két közvetlenül csatlakozó hálózat a 192.168.10.0/24 és a 209.165.200.224/30.

Az R1 és az R2 routerek az OSPF dinamikus forgalomirányító protokollt is használják az irányítási információk cseréjére. Az ábrán látható irányítótáblában az R1 egy olyan útvonalbejegyzéssel rendelkezik a 10.1.1.0/24 hálózathoz, amelyet dinamikusan tanult az R2 routertől OSPF-protokoll használatával.

Az alapértelmezett útvonal hálózati címe csupa nullából áll. Az IPv4 esetében ez a hálózati cím a 0.0.0.0. Az ábrán kiemelve látható, hogy a statikus alapértelmezett útvonal bejegyzése S\* kóddal kezdődik.

8.5.7

## Tudáspróba - Bevezetés a forgalomirányításba

Az űrlap teteje

Check your understanding of the introduction to routing by choosing the correct answer to the following questions.

1. What is the command used on a Cisco IOS router to view the routing table?

Az űrlap alja

What does a code of “O” indicate next to a route in the routing table?

This type of route is also known as a gateway of last resort.

Which is a characteristic of static routes?

True or False? A router can be configured with a combination of both static routes and a dynamic routing protocol.

[8.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az állomás irányítótáblája](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[8.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                         

1. Hálózati réteg
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

8.6.1

## Miről tanultunk ebben a fejezetben?

**A hálózati réteg jellemzői**

A hálózati réteg (az OSI 3. rétege) olyan szolgáltatásokat biztosít, amelyek lehetővé teszik a végberendezések közötti kommunikációt a hálózatokon. Az IPv4 és az IPv6 a hálózati réteg elsődleges kommunikációs protokolljai. A hálózati rétegbe tartozik az OSPF forgalomirányító protokoll, valamint üzenetküldő protokollok, például az ICMP. A hálózati rétegbeli protokollok négy alapvető műveletet hajtanak végre: végberendezések címzése, beágyazás, forgalomirányítás és kicsomagolás. Az IPv4 és IPv6 meghatározza az adatok egyik állomásról a másikra történő átviteléhez használt csomagok struktúráját és feldolgozását. Az IP a szállítási réteg szegmensét egy IP-fejléc hozzáadásával ágyazza be, amelyet a csomag célállomás felé továbbításához használ. Az IP-csomag fejlécét a 3. rétegbeli eszközök (routerek) vizsgálják meg, miközben az a hálózaton keresztül a cél felé továbbítódik. Az IP legfőbb jellemzői: összeköttetés-mentes, a legjobb szándékú és közegfüggetlen. Az összeköttetés-mentes azt jelenti, hogy az adatküldést megelőzően a végpontok között nem épül ki külön kapcsolat. Az IP-protokoll nem garantálja, hogy minden küldött csomagot ténylegesen megkapnak-e. Ez a nem megbízható (legjobb szándékú) jellemző definíciója. Az IP teljesen függetlenül működik az átviteli közegtől, ahol a protokollkészlet alacsonyabb rétegeiben zajló adatátvitel történik.

**IPv4-csomag**

A fejléc mezői a csomagról tartalmaznak információkat. Ezek a mezők bináris számok, amelyeket a 3. réteg dolgoz fel. Az egyes mezők bináris értékei az IP-csomag különböző tulajdonságait határozzák meg. Az IPv4-fejléc fontosabb mezői a következők: verzió, DS, fejléc ellenőrzőösszeg, TTL, protokoll, valamint a forrás és cél IPv4-címek.

**IPv6-csomag**

Az IPv6 célja az IPv4 korlátainak leküzdése, amelyek a következők: az IPv4-címtartomány kimerülése, a végponttól végpontig tartó kapcsolatok hiánya és a hálózat összetettségének növekedése. Az IPv6 megnöveli a rendelkezésre álló címteret, továbbfejleszti a csomagok kezelését, és kiküszöböli a NAT használatát. Az IPv6-csomag fejléc mezői a következők: verzió, forgalom osztály, folyamcímke, adatmező hossza, következő fejléc, ugrás korlát, forrás IP-cím és cél IP-cím.

**Állomás irányítótáblái**

Az állomás küldhet csomagot saját magának, egy másik helyi állomásnak vagy egy távoli állomásnak. IPv4 esetén a küldő eszköz a saját alhálózati maszkját és IPv4-címét, valamint a cél IPv4-címét használva dönti el, hogy a célállomással azonos hálózatban van-e. IPv6 esetén a helyi router hirdeti a helyi hálózat címét (előtagot) a hálózat összes állomása számára ugyanezen döntés meghozatala miatt. Az alapértelmezett átjáró az a hálózati eszköz (vagyis router), amely más hálózatokba irányítja a forgalmat. Egy hálózatban az alapértelmezett átjáró általában egy router, amelynek helyi IP-címe ugyanabban a címtartományban van, mint a helyi hálózat többi állomása. Feladata a helyi hálózatba szánt adatok kiküldése, a helyi hálózatból érkezett adatok fogadása, valamint a forgalom továbbítása más hálózatokba. Egy állomás irányítótáblája általában tartalmaz alapértelmezett átjárót. IPv4 esetén az állomás az alapértelmezett átjáró IPv4-címét a DHCP-protokolltól kapja meg dinamikusan, vagy manuálisan állítják be rajta. IPv6 esetén az alapértelmezett átjáró címét a router hirdeti, vagy kézzel állítják be az állomáson. Windows állomáson a **route print** vagy a **netstat -r** parancs használható az állomás irányítótáblájának megjelenítésére.

**Bevezetés a forgalomirányításba**

Amikor egy állomás csomagot küld egy másik állomásnak, akkor az irányítótáblája segítségével dönti el, hogy hova továbbítsa azt. Ha a célállomás egy távoli hálózaton van, akkor a csomagot az alapértelmezett átjárónak kell küldeni, ami általában egy helyi hálózatban lévő router. Mi történik, ha egy csomag érkezik egy router interfészére? Megvizsgálja a csomag cél IP-címét, és megkeresi az irányítótáblában, hogy hova továbbítsa azt. Az irányítótábla tartalmazza az összes ismert hálózati cím (előtag) listáját, és a csomagok továbbításának helyét. Ezeket a bejegyzéseket útvonal-bejegyzéseknek vagy útvonalaknak nevezzük. A router a csomagot a legjobb (leghosszabb) egyezést mutató útvonal-bejegyzés alapján küldi tovább. A router irányítótáblája háromféle útvonalbejegyzést tárol: közvetlenül csatlakozó hálózatokat, távoli hálózatokat és alapértelmezett útvonalat. A távoli hálózatokat a routerek kézi beállítás útján vagy dinamikus irányító protokollok használatával tanulják meg. A statikus útvonalak olyan bejegyzések, amelyeket manuálisan állítunk be. A statikus útvonalak tartalmazzák a távoli hálózat címét és a következő ugrás router IP-címét. Az OSPF és az EIGRP dinamikus irányító protokollok. A **show ip route** privilegizált EXEC módbeli parancs segítségével megtekinthetjük az IPv4-irányítótáblát egy Cisco IOS-routeren. Minden irányítótábla bejegyzés előtt egy kód található, amely azonosítja az útvonal típusát vagy az útvonal megtanulásának módját. Az útvonalak leggyakoribb forrásai a következők:

**L** - Közvetlenül csatlakozó helyi interfész IP-címe

**C** - Közvetlenül csatlakozó hálózat

**S** - A rendszergazda által kézzel létrehozott statikus útvonal.

**O** - OSPF

**D** - EIGRP

8.6.2

## Ellenőrző teszt - Hálózati réteg

Az űrlap teteje

1. Melyik parancs használható egy Windows gépen az irányítótábla megjelenítésére?

Az űrlap alja

Milyen információkat adnak hozzá az OSI 3. rétegében történő beágyazás során?

Hogyan használja a hálózati réteg az MTU értéket?

Melyik jellemző írja le az IPv6 továbbfejlesztését az IPv4-hez képest?

Melyik állítás írja le pontosan az IPv4 jellemzőit?

Amikor egy router csomagot kap, milyen információkat kell megvizsgálnia ahhoz, hogy a csomagot egy távoli célállomásra továbbítsa?

Egy számítógép csomagot szeretne küldeni a saját helyi hálózatában lévő célállomásnak. Hogyan küldi ki a csomagot?

Melyik IPv4-címet használhatjuk az állomás loopback interfészének pingelésére?

Ha egy kapcsolat nélküli protokollt használnak az OSI-modell alsó rétegében, hogyan észlelik a hiányzó adatokat és továbbítják azokat, ha szükséges?

Mi volt az oka az IPv6 létrehozásának és alkalmazásának?

Milyen információkat használnak a routerek az adatcsomag célállomás felé történő továbbítására?

Az IPv4 csomag fejlécének melyik mezője marad általában változatlanul a csomag továbbítása során?

Az IPv6-csomag melyik mezőjét használja a router annak megállapítására, hogy egy csomag élettartama lejárt-e és el kell-e dobni?

[8.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés a forgalomirányításba](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[9.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                   
*               

1. Címfeloldás
2. Bevezetés

# Bevezetés

9.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a címfeloldásról szóló fejezetben!

A hosztok és a routerek forgalomirányító táblákat hoznak létre annak biztosítása érdekében, hogy adatokat küldhessenek és fogadhassanak hálózatokon keresztül. Hogyan jön létre ez az információ az irányító táblázatban? Hálózati rendszergazdaként manuálisan is megadhatnánk ezeket a MAC és IP-címeket. De ez sok időbe telne, és nagy a valószínűsége annak, hogy közben néhány hibát követnénk el. Biztosan kell lennie valamilyen módnak, hogy ezt maguk az állomások és a routerek automatikusan elvégezhessék, nem? Természetesen! És bár automatikusan történik, meg kell értenünk, hogyan is működik ez, mert előfordulhat, hogy hibaelhárítást kell végeznünk egy probléma esetén, vagy ami még rosszabb, a hálózatot megtámadhatja egy rosszindulatú felhasználó. Készen állunk a címfeloldás megismerésére? Ez a fejezet számos nagyon jó videót tartalmaz, hogy segítsen a fogalmak megmagyarázásában, valamint három Packet Tracer tevékenységet a jobb megértés érdekében. Kezdjünk is bele!

9.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe**: Címfeloldás

**Fejezet célja**: Annak elmagyarázása, hogy az ARP és az ND hogyan teszi lehetővé a kommunikációt a hálózaton.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **MAC és IP** | A MAC-cím és az IP-cím szerepeinek összehasonlítása. |
| **ARP** | Az ARP céljának bemutatása. |
| **Szomszédfelderítés** | Az IPv6 szomszédfelderítés működésének leírása. |

[8.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[9.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[MAC és IP](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                     
*               

1. Címfeloldás
2. MAC és IP

# MAC és IP

9.1.1

## Saját hálózaton belüli cél

Néha egy hosztnak üzenetet kell küldenie, de csak a céleszköz IP-címét ismeri. Az állomásnak ismernie kell a céleszköz MAC-címét is, de azt honnan fogja megtudni? Ez az, ahol a címfeloldás fontossá válik.

Egy Ethernet LAN-on két fő címet rendelünk egy állomáshoz:

* **Fizikai cím (MAC cím)** – A hálókártyák közti forgalomhoz használjuk ugyanazon az Ethernet hálózaton belül.
* **Logikai cím (IP-cím)**— A csomag forráseszközről a céleszközre történő elküldésére szolgál. A cél IP-címe lehet ugyanazon az IP-hálózaton, mint a forrás, vagy lehet egy távoli hálózaton is.

A 2. rétegbeli fizikai címek (azaz Ethernet MAC-címek) arra szolgálnak, hogy az adatkapcsolati keretet a beágyazott IP-csomaggal egy hálózati kártyáról egy másik hálózati kártyára szállítsák, ami ugyanazon a hálózaton található. Ha a cél IP-címe ugyanazon a hálózaton található, a cél MAC-címe a céleszköz címe lesz.

Tekintsük meg a következő példát egyszerűsített MAC-címábrázolások használatával.

The image is a network diagram with PC 1 at IP 192.168.10.10/24 with simplified MAC aa-aa-aa, connected to a switch at IP 192.168.10.0/24, connected to PC 2 at IP 192.168.10.11/24 with simplified MAC 55-55-55. Below the diagram are four boxes reading from left to right: Destination MAC 55-55-55, Source MAC aa-aa-aa, Source IPv4 192.168.10.10, and Destination IPv4 192.168.10.11.

|  |  |  |  |
| --- | --- | --- | --- |
| Destination MAC | Source MAC | Source IPv4 | Destination IPv4 |
| 55-55-55 | aa-aa-aa | 192.168.10.10 | 192.168.10.11 |

55-55-55aa-aa-aaPC 1PC 2**192.168.10.10/24192.168.10.0/24192.168.10.11/24**

Ebben a példában a PC1 csomagot szeretne küldeni a PC2-nek. Az ábra a 2. rétegbeli cél- és forrás MAC-címeket, valamint a 3. rétegbeli IPv4-címzést jeleníti meg, amely a PC1-ről küldött csomagban szerepelne.

A 2. rétegbeli Ethernet keret a következőket tartalmazza:

* **Cél MAC-cím**— Ez a PC2 egyszerűsített MAC-címe, 55-55-55.
* **Forrás MAC-cím**— Ez a PC1 Ethernet hálózati kártyájának egyszerűsített MAC-címe, aa-aa-aa.

A 3. rétegbeli IP-csomag a következőket tartalmazza:

* **Forrás IPv4-cím**— Ez a PC1 IPv4-címe, 192.168.10.10.
* **Cél IPv4-cím**— Ez a PC2 IPv4-címe, 192.168.10.11.

9.1.2

## Távoli hálózaton lévő cél

Ha a cél IP-cím (IPv4 vagy IPv6) távoli hálózaton van, a cél MAC-cím az állomás alapértelmezett átjárójának (azaz a router interfészének) címe lesz.

Tekintsük meg a következő példát egy egyszerűsített MAC-címábrázolással.

The image is a network diagram showing the source and destination MAC and IPv4 addressing for the first hop when information is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 192.168.10.0/24 are four boxes reading from left to right: Destination MAC bb-bb-bb, Source MAC aa-aa-aa, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1 R2 PC 2 PC 1 .10 .1 .225 .226 .1 .10 G0/0/1 G0/0/1 G0/0/0

G0/0/0

|  |  |  |  |
| --- | --- | --- | --- |
| Destination  MAC | Source  MAC | Source IPv4 | Destination  IPv4 |
| bb-bb-bb | aa-aa-aa | 192.168.10.10 | 10.1.1.10 |

55-55-55aa-aa-aa**192.168.10.0/24209.165.200.224/3010.1.1.0/24Internet**bb-bb-bbcc-cc-ccdd-dd-ddee-ee-ee

Ebben a példában a PC1 csomagot akar küldeni a PC2-nek. A PC2 távoli hálózaton található. Mivel a cél IPv4-cím nem ugyanazon a helyi hálózaton van, mint a PC1, a cél MAC-cím a router, mint alapértelmezett helyi átjáró címe.

A routerek megvizsgálják a cél IPv4-címét, hogy meghatározzák az IPv4-csomag továbbításához a legjobb elérési utat. Amikor a router megkapja az Ethernet keretet, lebontja a 2. rétegbeli információkat. A cél IPv4-cím használatával meghatározza a következő ugrás eszközt, majd az IPv4-csomagot egy új adatkapcsolati keretbe foglalja a kimenő interfész számára.

Példánkban az R1 most a csomagot az ábrán látható új 2. rétegbeli címinformációkkal látja el.

The image is a network diagram showing the source and destination MAC and IPv4 addressing when information is passed between two routers as it is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 209.165.200.224/30 are four boxes reading from left to right: Destination MAC dd-dd-dd, Source MAC cc-cc-cc, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1 R2 PC 2 PC 1 .10 .1 .225 .226 .1 .10 G0/0/1 G0/0/1 G0/0/0

G0/0/0

|  |  |  |  |
| --- | --- | --- | --- |
| Destination  MAC | Source  MAC | Source IPv4 | Destination  IPv4 |
| dd-dd-dd | cc-cc-cc | 192.168.10.10 | 10.1.1.10 |

55-55-55aa-aa-aa**192.168.10.0/24209.165.200.224/3010.1.1.0/24Internet**bb-bb-bbcc-cc-ccdd-dd-ddee-ee-ee

Az új cél MAC-cím az R2 G0/0/1 interfészének, az új forrás MAC-cím pedig az R1 G0/0/1 interfészének címe.

Egy útvonal minden egyes lépése során IP-csomag van beágyazva keretbe. A keret az adott kapcsolathoz tartozó adatkapcsolati technológiára vonatkozik, például az Ethernetre. Ha a következő ugrás eszköz a végső cél, a cél MAC-címe az eszköz Ethernet hálózati kártyájának címe lesz, amint az az ábrán látható.

The image is a network diagram showing the source and destination MAC and IPv4 addressing when information exits a router to the final destination as it is sent from a PC on one network to a destination on a remote network. The description that follows are the names, connections, and addressing of devices from left to right. PC 1 is connected to a switch which is connected to router R1 interface G0/0/0 on network 192.168.10.0/24. PC 1 has an IP of 192.168.10.10 and MAC of aa-aa-aa. The R1 G0/0/0 interface has an IP of 192.168.10.1 and MAC of bb-bb-bb. R1 has a G0/0/1 interface connected to router R2 interface G0/0/1 on network 209.165.200.224/30. The R1 G0/0/1 interface has an IP of 209.165.200.225 and MAC cc-cc-cc. The R2 G0/0/1 interface has an IP of 209.165.200.226 and MAC dd-dd-dd. R2 has a G0/0/0 interface connected to a switch connected to PC 2 on network 10.1.1.0/24. The R2 G0/0/0 interface has an IP of 10.1.1.1 and MAC ee-ee-ee. PC 2 has an IP of 10.10.10.10 and MAC 55-55-55. R2 also has a connection at the top leading to the Internet cloud. Below the diagram under network 10.1.1.0/24 are four boxes reading from left to right: Destination MAC 55-55-55, Source MAC ee-ee-ee, Source IPv4 192.168.10.10, and Destination IPv4 10.1.1.10.

R1 R2 PC 2 PC 1 .10 .1 .225 .226 .1 .10 G0/0/1 G0/0/1 G0/0/0

G0/0/0

|  |  |  |  |
| --- | --- | --- | --- |
| Destination  MAC | Source  MAC | Source IPv4 | Destination  IPv4 |
| 55-55-55 | ee-ee-ee | 192.168.10.10 | 10.1.1.10 |

55-55-55aa-aa-aa**192.168.10.0/24209.165.200.224/3010.1.1.0/24Internet**bb-bb-bbcc-cc-ccdd-dd-ddee-ee-ee

Hogyan társítjuk a célhoz vezető valamennyi kapcsolaton egy adatfolyam csomagjaiban lévő IP-címeket a MAC-címekhez? IPv4 csomagok esetében ez a címfeloldási protokoll (Address Resolution Protocol, ARP) nevű folyamat segítségével történik. IPv6-csomagok esetében ez a folyamat az ICMPv6 szomszédfelderítés (Neighbor Discovery, ND).

9.1.3

## Packet Tracer - MAC-és IP-címek azonosítása

Ebben a Packet Tracer feladatban a következőket fogjuk elvégezni:

* PDU-információk összegyűjtése a helyi hálózati kommunikációhoz
* PDU-adatok gyűjtése távoli hálózati kommunikációhoz

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.

[MAC- és IP-címek azonosítása](https://contenthub.netacad.com/courses/itn/_common/9.1.3-packet-tracer---identify-mac-and-ip-addresses_hu-HU.pka)

9.1.4

## Tudáspróba - MAC és IP

Az űrlap teteje

Check your understanding of MAC and IP addressing by choosing the BEST answer to the following questions.

1. What destination MAC address would be included in a frame sent from a source device to a destination device on the same local network?

Az űrlap alja

What destination MAC address would be included in a frame sent from a source device to a destination device on a remote local network?

What two protocols are used to determine the MAC address of a known destination device IP address (IPv4 and IPv6)?

[9.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[9.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[ARP](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                             
*               

1. Címfeloldás
2. ARP

# ARP

9.2.1

## Az ARP áttekintése

Ha a hálózat IPv4 kommunikációs protokollt használ, az IPv4-címek MAC-címekhez való hozzárendeléséhez az Address Resolution Protocol (ARP) protokollra van szükség. Ez a témakör az ARP működését ismerteti.

Az Ethernet-hálózat minden IP-eszköze egyedi Ethernet MAC-címmel rendelkezik. Amikor egy eszköz 2. rétegbeli Ethernet keretet küld, az a következő két címet tartalmazza:

* **Cél MAC-cím**- A céleszköz Ethernet MAC-címe ugyanazon a helyi hálózati szegmensen. Ha a célállomás egy másik hálózaton van, akkor a keretben lévő célcím az alapértelmezett átjáró (azaz router) címe lesz.
* **Forrás MAC-cím**- Az Ethernet hálózati kártya MAC-címe a forrásállomáson.

Az ábra azt a problémát szemlélteti, amikor egy keretet küldünk egy másik állomásnak ugyanazon a szegmensen belül egy IPv4-hálózatban.

Four hosts, H1, H2, H3, and H4, are connected to the same switch. H1 has an IP of 192.168.1.5/24, H2 has an IP of 192.168.1.6/24, H3 has an IP of 192.168.1.8/24, and H4 has an IP of 192.168.1.7/24. H1 has a callout that reads: I need to send information to 192.168.1.7, but I only have the IP address. I dont know the MAC address of the device that has that IP.

H2 HI H4 H3 192.168.1.5/24 192.168.1.6/24 192.168.1.8/24

192.168.1.7/24

I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.

Ha egy csomagot ugyanazon a helyi IPv4-hálózaton lévő másik állomásra szeretnénk küldeni, ismerni kell a céleszköz IPv4-címét és MAC-címét is. Az céleszközök IPv4-címei vagy ismertek, vagy eszköznév alapján oldhatók fel. A MAC-címeket azonban ki kell deríteni.

Egy eszköz a címfeloldó protokoll (Address Resolution Protocol, ARP) segítségével határozza meg a helyi eszköz cél-MAC-címét, ha ismeri az IPv4-címét.

Az ARP-protokoll két alapvető funkciót biztosít:

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

9.2.2

## ARP funkciók

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 az átmenetileg a RAM-ban tárolt táblázat az úgynevezett ARP-táblázat vagy ARP-gyorsítótár (cache).

A küldő eszköz az ARP táblában keresi a cél IPv4-címet és az ennek megfelelő MAC-címet.

* Ha a csomag cél IPv4-címe ugyanazon a hálózaton található, mint a forrás IPv4-címe, az eszköz az ARP táblában keresi a cél IPv4-címet.
* Ha a cél IPv4-cím a forrás IPv4-címtől eltérő című hálózaton található, akkor az eszköz az alapértelmezett átjáró IPv4-címét keresi az ARP-táblában.

Mindkét esetben a keresés IPv4-címre és a készülék megfelelő MAC-címére vonatkozik.

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

Ha az eszköz megtalálja az IPv4-címet, a rendszer a megfelelő MAC-címet használja a keretben cél MAC-címként. Ha nem talál bejegyzést, akkor az eszköz ARP kérést küld.

Kattintsunk a Lejátszás gombra az ARP animációjának megtekintéséhez!

This animation illustrates how a host will use ARP to discover the MAC address of a known IP address. Host H1 needs to send some information to a host with IP address 192.168.1.7. However, H1 does not have the MAC address for that address. Therefore, it sends an ARP request to IP address 192.168.1.7. All hosts on the network will receive the ARP request. However, only host H4 with IP address 192.168.1.7 will send an ARP reply containing its MAC address.

I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.

This isn't me.

This isn't me.

This is me, I will send back my MAC address.

Now I have the MAC. I can forward my information.

Thanks. I got it.

9.2.3

## Videó - ARP kérés

ARP-kérés akkor kerül elküldésre, ha egy eszköznek meg kell határoznia az IPv4-címhez társított MAC-címet, és nincs bejegyzése az IPv4-címhez az ARP-táblában.

Az ARP üzenetek közvetlenül egy Ethernet-keretbe vannak beágyazva. Nincs IPv4 fejléc. Az ARP kérést Ethernet-keretbe ágyazzuk a következő fejléc-információk segítségével:

* **Cél MAC-cím** — Ez a FF-FF-FF-FF-FF-FF szórási cím, amely ahhoz szükséges, hogy a LAN-on található összes Ethernet hálózati kártya elfogadja és feldolgozza a kérést.
* **Forrás MAC-cím** — Az ARP-kérés feladójának MAC-címe.
* **Típus** - Az ARP üzenetek típus mezőjének értéke 0x806. Ez tájékoztatja a fogadó hálózati kártyát arról, hogy a keret adatrészét az ARP folyamatnak kell átadni.

Mivel az ARP kérések szórások, a switch elárasztással küldi ki az összes portján, kivéve a fogadó portot. A LAN-on lévő összes Ethernet hálózati kártya feldolgozza a szórást, és az ARP kérést az operációs rendszeréhez továbbítja feldolgozás céljából. Minden eszköznek fel kell dolgoznia az ARP kérést, hogy ellenőrizze, hogy a cél IPv4-cím egyezik-e a sajátjával. A router nem továbbítja kifelé a szórásokat más interfészein.

A LAN-on csak egy eszköz rendelkezik azzal az IPv4-címmel, ami megfelel az ARP-kérésben szereplő cél IPv4-címnek. A többi eszköz nem válaszol.

Kattintsunk az ábrán a Lejátszás gombra a helyi hálózaton található IPv4-címhez tartozó ARP-kérés bemutatásának megtekintéséhez!

9.2.4

## Videó - Az ARP működése - ARP Válasz

Csak az a készülék fog válaszolni a kérésre, amelyiknek az IP-címe az ARP kérésben szerepel. Az ARP-válasz Ethernet-keretbe van ágyazva a következő fejléc-információk segítségével:

* **Cél MAC-cím** — Ez az ARP-kérés feladójának MAC-címe.
* **Forrás MAC-cím** — Ez az ARP-válasz feladójának MAC-címe.
* **Típus** - Az ARP üzenetek típus mezőjének értéke 0x806. Ez tájékoztatja a fogadó hálózati kártyát arról, hogy a keret adatrészét az ARP folyamatnak kell átadni.

Csak az ARP kérést eredetileg elküldő eszköz kapja meg az egyedi címzésű (unicast) ARP választ. Az ARP válasz beérkezése után a készülék hozzáadja az IPv4-címet és a megfelelő MAC-címet az ARP táblához. Az erre az IPv4-címre szóló csomagokat immár be lehet ágyazni a keretekbe a megfelelő MAC-címmel.

Ha egyetlen eszköz sem válaszol az ARP-kérésre, a csomagot eldobják, mivel a keret nem hozható létre.

Az ARP táblázatban szereplő bejegyzések időbélyeggel vannak ellátva. Ha egy készülék nem kap keretet egy adott eszköztől az időbélyeg lejárta előtt, az eszközhöz tartozó 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.

**Megjegyzés**: Az IPv6 az IPv4 ARP-jához hasonló eljárást használ, amit ICMPv6 szomszédfelderítésnek (ND) nevezünk. Az IPv6 az IPv4 ARP kérésekhez és az ARP válaszokhoz hasonlóan a szomszéd keresés és a szomszéd hirdetés üzeneteket használja.

Kattintsunk az ábrán a Lejátszás elemre az ARP válasz bemutatásának megtekintéséhez!

9.2.5

## Videó - Az ARP szerepe a távoli kommunikációban

Ha a cél IPv4-cím nem ugyanazon a hálózaton található, mint a forrás IPv4-cím, a forráseszköznek el kell küldenie a keretet az alapértelmezett átjárójára. Ez a helyi router interfésze. Ha egy forráseszköz IPv4-címmel ellátott csomagot küld egy másik hálózatra, a csomagot a router cél-MAC-címével ellátva ágyazza be egy keretbe.

Az átjárónak, azaz a router interfészének a címét az állomások az IPv4-konfigurációjukban tárolják. Amikor az állomás létrehoz egy csomagot egy célállomás számára, 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 célállomás nem ugyanazon a hálózaton található, a küldő ellenőrzi az ARP-táblában, hogy nincs-e olyan bejegyzés, amelyben az alapértelmezett átjáró IPv4-címe szerepel. Ha nincs bejegyzés, az ARP eljárással határozza meg az alapértelmezett átjáró MAC-címét.

Kattintsunk a Lejátszás gombra az alapértelmezett átjáróhoz társított ARP-kérés és ARP-válasz bemutatásának megtekintéséhez!

9.2.6

## Bejegyzések eltávolítása az ARP-táblázatból

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. Az újabb Windows operációs rendszerek például 15 és 45 másodperc közötti időszakra tárolják az ARP táblázatbejegyzéseket, amint az az ábrán látható.

A C B R1 S1

G0/0/0

192.168.1.110/24   
MAC 00-0A192.168.1.120/24   
MAC 00-0B192.168.1.50/24   
MAC 00-0C192.168.1.1/24   
MAC 00-0DI will remove this ARP entry if I have not used it within 15 to 45 seconds.InternetNote: MAC addresses are shortened for demonstration purposes.

| **PC A's ARP Cache** |
| --- |
| **IPv4 Address** | **MAC Address** |
| 192.168.1.1 | 00:0D |

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.

9.2.7

## ARP-táblázat hálózati eszközökön

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

R1# **show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.10.1 - a0e0.af0d.e140 ARPA GigabitEthernet0/0/0

Internet 209.165.200.225 - a0e0.af0d.e141 ARPA GigabitEthernet0/0/1

Internet 209.165.200.226 1 a03d.6fe1.9d91 ARPA GigabitEthernet0/0/1

R1#

Egy Windows 10 PC-n az **arp –a** parancsot használjuk az ARP-táblázat megjelenítéséhez, amint az ábrán látható.

C:\Users\PC> **arp -a**

Interface: 192.168.1.124 --- 0x10

Internet Address Physical Address Type

192.168.1.1 c8-d7-19-cc-a0-86 dynamic

192.168.1.101 08-3e-0c-f5-f7-77 dynamic

192.168.1.110 08-3e-0c-f5-f7-56 dynamic

192.168.1.112 ac-b3-13-4a-bd-d0 dynamic

192.168.1.117 08-3e-0c-f5-f7-5c dynamic

192.168.1.126 24-77-03-45-5d-c4 dynamic

192.168.1.146 94-57-a5-0c-5b-02 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\PC>

9.2.8

## ARP problémák - ARP szórások és ARP hamisítás

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. 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.

The diagram shows seven devices on shared media (multiple access) all powered on at the same time. A text box reads: ARP broadcasts can flood the local media.

All devices powered on at the same timeARP broadcasts can flood the local media.Shared Media (multiple access)

Bizonyos esetekben az ARP potenciális biztonsági kockázatot jelenthet. Egy rosszindulatú felhasználó ARP hamisítást használhat ARP mérgezéses támadáshoz. Ezt a technikát a támadó arra használja, hogy válaszoljon egy másik eszközhöz tartozó IPv4-címre vonatkozó ARP-kérésére, például az alapértelmezett átjáróéra, az ábrán látható módon. A támadó ARP-választ küld a saját MAC-címével. Az ARP válasz vevője rossz MAC-címet ad hozzá az ARP táblájához, és elküldi ezeket a csomagokat a támadónak

A vállalati szintű switch-ek tartalmaznak egy dinamikus ARP ellenőrzés (DAI) néven ismert védelmi technikát. Ez viszont nem része a kurzus anyagának.

The image is a network diagram showing two hosts, Host A with IP 192.168.1.110/24 and MAC 00-0A and Host B with IP 192.168.1.120/24 and MAC 00-0B, connected to switch S1 which is connected to router R1 at port G0/0/0 (the default gateway with IP 192.168.1.1/24 and MAC 00-0D) which is connected to the Internet cloud. Also connected to S1 is a threat actor at host C with IP 192.168.1.50/24 and MAC 00-0C. Host A has a callout that reads: ARP Request: I need the MAC address of default gateway, 192.168.1.1. The threat actor host C has a callout that reads: I will send an ARP reply and pretend to be the default gateway! Note: MAC addresses are shortened for demonstration purposes.

A B S1 R1 C A 192.168.1.110/24MAC 00-0A 192.168.1.120/24MAC 00-0B 192.168.1.50/24MAC 00-0C 192.168.1.1/24MAC 00-0D

G0/0/0

NetworkNote: MAC addresses are shortened for demonstration purposes.I will send an ARP reply and pretend to be the default gateway!ARP Request: I need the MAC address of default gateway, 192.168.1.1

9.2.9

## Packet Tracer - Az ARP-táblázat vizsgálata

Ebben a Packet Tracer feladatban a következőket fogjuk elvégezni:

* ARP-kérés vizsgálata
* Switch MAC-címtáblájának vizsgálata
* Az ARP folyamat vizsgálata a távoli kommunikációban

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.

[Az ARP-tábla vizsgálata](https://contenthub.netacad.com/courses/itn/_common/9.2.9-packet-tracer---examine-the-arp-table_hu-HU.pka)

9.2.10

## Tudáspróba - ARP

Az űrlap teteje

Check your understanding of ARP by choosing the correct answer to the following questions.

1. What two functions are provided by ARP? (Choose two.)

Az űrlap alja

Where is the ARP table stored on a device?

Which statement is true about ARP?

Which command could be used on a Cisco router to view its ARP table?

What is an attack using ARP?

[9.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[MAC és IP](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[9.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 szomszédfelderítés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                
*               

1. Címfeloldás
2. IPv6 szomszédfelderítés

# IPv6 szomszédfelderítés

9.3.1

## Videó - IPv6 szomszédfelderítés

Ha a hálózat IPv6 kommunikációs protokollt használ, akkor az IPv6-címek MAC-címekkel való megfeleltetéséhez a szomszédfelderítés (Neighbor Discovery, ND) protokollra van szükség. Ez a témakör ismerteti az ND működését.

Kattintsunk az ábrán a Lejátszás elemre az IPv6 Neighbor Discovery bemutatásához!

9.3.2

## IPv6 szomszédfelderítési üzenetek

Az IPv6 Neighbor Discovery protokollt néha ND vagy NDP néven is említik. Ebben a kurzusban ND-nek nevezzük. Az ND címfeloldást, routerfelderítést és átirányítási szolgáltatásokat nyújt az IPv6 számára az ICMPv6 használatával. Az ICMPv6 ND öt ICMPv6 üzenetet használ az alábbi szolgáltatások végrehajtásához:

* Szomszéd keresés (Neighbor Solicitation, NS) üzenet
* Szomszéd hirdetés (Neighbor Advertisement, NA) üzenet
* Router keresés (Router Solicitation, RS) üzenet
* Router hirdetés (Router Advertisement, RA) üzenet
* Üzenet átirányítás

A szomszéd keresési és a szomszéd hirdetési üzeneteket eszköztől-eszközig történő üzenetküldéshez használják, például a címfeloldáshoz (hasonlóan az IPv4 ARP-hez). Az eszközök közé tartoznak mind az állomások, mind a routerek.

:11 :10 2001:db8:acad:1::/64 PC1

PC2

Eszköz-eszköz közötti  
üzenetküldés

A routerkeresés és a routerhirdetés üzenetek állomások és routerek között zajlanak. Általában a routerfelderítést használják a dinamikus címkiosztáshoz és az állapot nélküli automatikus címkonfigurálásához (SLAAC).

:1 2001:db8:acad:1::/64 PC1

R1

Eszköz-router közötti  
üzenetküldés

**Megjegyzés**: Az ötödik ICMPv6 ND üzenet egy átirányítási üzenet, amelyet egy kedvezőbb next-hop kiválasztásához használnak. Ez viszont nem része a kurzus anyagának.

Az IPv6 ND leírása az IETF RFC 4861-ben található.

9.3.3

## IPv6 szomszédfelderítés - Címfeloldás

Az ARP-hez hasonlóan az IPv4-ben, az IPv6-eszközök IPv6 ND-t használnak egy ismert IPv6-címmel rendelkező eszköz MAC-címének meghatározásához.

Az ICMPv6 szomszéd keresés (Neighbor Solicitation) és szomszéd hirdetés (Neighbor Advertisement) üzeneteket használják a MAC-címek feloldására. Ez hasonló az ARP által az IPv4-ben használt ARP-kérésekhez és ARP-válaszokhoz. Tegyük fel például, hogy a PC1 pingelni akarja a PC2-t a 2001:db8:acad።11 IPv6 címen. Az ismert IPv6-címhez tartozó MAC-cím meghatározásához a PC1 ICMPv6 szomszéd keresés üzenetet küld az ábrán látható módon.

The diagram shows PC1 and PC2 connected to the same switch on network 2001:db8:acad:1::/64. PC1 has an IPv6 address 2001:db8:acad:1::10 and PC2 has an IPv6 address of 2001:db8:acad:1::11. PC1 is sending an ICMPv6 neighbor solicitation message that reads: Hey whoever has 2001:db8:acad:1::11, send me your MAC address? PC2 is replying with an ICMPv6 neighbor advertisement message that reads: Hey 2001:db8:acad:1::10, I am 2001:db8:acad:1::11 and my MAC address is f8-94-c3-e4-c5-0A.

:11 :10 2001:db8:acad:1::/64 PC1

PC2

**ICMPv6 Neighbor Advertisement Message**  
*"Hey 2001:db8:acad:1::10, I am 2001:db8:acad:1::11 and my MAC address is f8-94-c3-e4-c5-0A."***ICMPv6 Neighbor Solicitation Message**  
*"Hey whoever has 2001:db8:acad:1::11, send me your MAC address?"*

Az ICMPv6 szomszéd keresési üzeneteket speciális Ethernet és IPv6 csoportos címmel küldjük el. Ez lehetővé teszi a fogadó eszköz Ethernet hálózati kártyája számára annak megállapítását, hogy a szomszéd keresés üzenet neki szól-e, anélkül, hogy el kellene küldenie feldolgozásra az operációs rendszernek.

A PC2 válaszol a kérésre egy ICMPv6 szomszéd hirdetési üzenettel, amely tartalmazza a MAC-címét.

9.3.4

## Packet Tracer - IPv6 szomszédfelderítés

Ahhoz, hogy egy eszköz kommunikálhasson egy másik eszközzel, ismernie kell a céleszköz MAC-címét. Az IPv6 esetében a Neighbor Discovery nevű folyamat felelős a cél MAC-címének meghatározásáért. A folyamat jobb megértése érdekében a PDU-információkat szimulációs módban gyűjtjük össze. A Packet Tracer nem pontozza ezt a tevékenységet.

[IPv6 szomszédfelderítés](https://contenthub.netacad.com/courses/itn/_common/9.3.4-packet-tracer---ipv6-neighbor-discovery_hu-HU.pka)

9.3.5

## Tudáspróba - Szomszédfelderítés

Az űrlap teteje

Check your understanding of by choosing the BEST answer to the following questions.

1. Which two ICMPv6 messages are used in SLAAC?

Az űrlap alja

Which two ICMPv6 messages are used in to determine the MAC address of a known IPv6 address?

To what type of address are ICMPv6 neighbor solicitation messages sent?

[9.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[ARP](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[9.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                               

1. Címfeloldás
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

9.4.1

## Miről tanultunk ebben a fejezetben?

**MAC és IP**

A 2. rétegbeli fizikai címek (azaz Ethernet MAC-címek) arra szolgálnak, hogy az adatkapcsolati rétegbeli keretet a beágyazott IP-csomaggal egy hálózati kártyáról egy másik hálózati kártyára szállítsák. Ha a cél IP-cím ugyanazon a hálózaton található, a cél MAC-cím a céleszköz címe lesz. Ha a cél IP-cím (IPv4 vagy IPv6) távoli hálózaton van, a cél MAC-cím az állomás alapértelmezett átjárójának (azaz a router interfészének) címe lesz. Egy útvonal minden egyes lépése során IP-csomag van beágyazva keretbe. A keret az adott szegmenshez kapcsolódó adatkapcsolati technológiára vonatkozik, például az Ethernetre. Ha a következő ugrás eszköz a végcél, a cél MAC-címe az eszköz Ethernet hálózati kártyájának címe lesz. Hogyan társítjuk a célhoz vezető valamennyi kapcsolaton egy adatfolyam csomagjaiban lévő IP-címeket a MAC-címekhez? IPv4 csomagok esetében ez egy címfeloldási protokoll (Address Resolution Protocol, ARP) nevű folyamat segítségével történik. IPv6-csomagok esetében a folyamat az ICMPv6 szomszédfelderítés (Neighbor Discovery, ND) nevet viseli.

**ARP**

Az Ethernet-hálózat minden IP-eszköze egyedi Ethernet MAC-címmel rendelkezik. Amikor egy eszköz 2. rétegbeli Ethernet keretet küld, az a következő két címet tartalmazza: cél MAC-cím és forrás MAC-cím. Az eszköz ARP segítségével határozza meg a helyi eszköz cél-MAC-címét, ha ismeri az IPv4-címét. Az ARP két alapvető funkciót biztosít: az IPv4-címek MAC-címekhez történő hozzárendelése és az IPv4-MAC-cím hozzárendelések táblázatának karbantartása. Az ARP kérést Ethernet-keretbe ágyazzák a következő fejlécadatok felhasználásával: forrás és cél MAC-címek és típus. A LAN-on csak egy eszköz rendelkezik azzal az IPv4-címmel, ami megfelel az ARP-kérésben szereplő cél IPv4-címnek. A többi eszköz nem válaszol. Az ARP-válasz ugyanazokat a fejlécmezőket tartalmazza, mint a kérés. Csak az ARP kérést eredetileg elküldő eszköz kapja meg az egyedi címzésű (unicast) ARP választ. Az ARP válasz beérkezése után a készülék hozzáadja az IPv4-címet és a megfelelő MAC-címet az ARP táblához. Ha a cél IPv4-cím nem ugyanazon a hálózaton található, mint a forrás IPv4-cím, a forráseszköznek el kell küldenie a keretet az alapértelmezett átjárójára. Ez a helyi router interfésze. Egy ARP-cache időzítő távolítja el minden eszközön azokat az ARP-bejegyzéseket, amelyeket egy meghatározott idő óta nem használtak. Parancsokat is használhatunk, hogy az ARP-táblából manuálisan távolítsunk el bizonyos bejegyzéseket, vagy akár az összeset. Szórásos keret lévén az ARP-kérést a helyi hálózaton minden eszköz megkapja és feldolgozza, ami lelassíthatja a hálózatot. Egy rosszindulatú felhasználó ARP hamisítást használhat ARP mérgezéses támadáshoz.

**Szomszéd felderítés**

Az IPv6 nem ARP protokollt használ, hanem az ND protokollt használja a MAC-címek feloldásához. Az ND címfeloldást, router-felderítést és átirányítási szolgáltatásokat nyújt az IPv6 számára az ICMPv6 használatával. Az ICMPv6 ND öt ICMPv6 üzenetet használ a szolgáltatások elvégzéséhez: szomszéd keresés, szomszéd hirdetés, router keresés, router hirdetés és átirányítás. Hasonlóan az IPv4 ARP-hez, az IPv6 eszközök IPv6 ND segítségével oldják fel az eszköz MAC-címét egy ismert IPv6-címre.

9.4.2

## Ellenőrző kvíz - Címfeloldás

Az űrlap teteje

1. A router melyik összetevője tartalmazza az irányítótáblát, az ARP-gyorsítótárat és az aktív konfigurációt?

Az űrlap alja

Milyen típusú információt tartalmaz az ARP-táblázat?

A számítógép úgy van beállítva, hogy automatikusan kapjon IP-címet a 192.168.1.0/24 hálózatból. A hálózati rendszergazda kiadja az **arp -a** parancsot és észreveszi ezt a bejegyzést: 192.168.1.255 ff-ff-ff-ff-ff-ff. Melyik állítás igaz erre a bejegyzésre?

A kiberbiztonsági elemző úgy véli, hogy a támadó az alapértelmezett átjáró MAC-címét hamisítja meg, hogy közbeékelődéses támadást hajtson végre. Melyik parancsot használja az elemző az alapértelmezett átjáró eléréséhez használt MAC-cím megtekintésére?

Mit tesz egy második rétegbeli kapcsoló, ha a fogadott keret cél MAC-címe nincs a MAC-táblában?

Melyik két ICMPv6-üzenetet használja az Ethernet a MAC-cím feloldása során? (Két jó válasz van.)

How does the ARP process use an IPv4 address?

Mi az ARP-protokoll funkciója?

Mit csinál egy második rétegbeli kapcsoló, amikor második rétegbeli szórásos keretet kap?

Milyen címeket képez le az ARP?

mikor IP-csomagot küldünk egy távoli hálózaton lévő állomásnak, milyen információkat nyújt az ARP?

Az ARP tábla egy kapcsolón melyik két fajta címet képez le egymásra?

Mi az ARP célja egy IPv4-hálózatban?

Milyen célcímet tartalmaz egy ARP-kérés keret??

[9.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 szomszédfelderítés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[10.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                           
*             

1. Alapvető forgalomirányító-konfiguráció
2. Bevezetés

# Bevezetés

10.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a router alapbeállításainak megadásáról szóló fejezetben.

Ha valaha is futottunk váltót, akkor tudjuk, hogy az első személy a verseny első szakaszát futja, majd átadja a stafétabotot a következő futónak, aki továbbhalad a verseny második szakaszán, majd átadja a stafétabotot a harmadik futónak, és így tovább. A csomagok irányítása hasonlít a váltófutásra. De ha az első futó nem tudja, hol találja a második futót, vagy elejti a stafétabotot az első szakaszon, akkor az a váltócsapat minden bizonnyal elveszíti a versenyt.

A csomagok irányítása tényleg hasonlít a váltófutásra. Mint tudjuk, az irányítótáblákat a routerek hozzák létre, hogy a csomagokat továbbítsák a helyi hálózataikról más hálózatokra. A router azonban nem hozhat létre irányítótáblát és nem továbbíthat csomagokat, amíg nincs megfelelően beállítva. Ha hálózati rendszergazdák szeretnénk lenni, feltétlenül tudnunk kell, hogyan tehetjük ezt meg. Mi a jó hír? Ez könnyű! Ez a fejezet parancsszimulátoros feladatokat tartalmaz, így gyakorolhatjuk a konfigurációs parancsokat és megtekinthetjük a kimenetet. Van még néhány Packet Tracer feladat is az induláshoz. Gyerünk!

10.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** A router alapbeállításainak megadása

**Fejezet célja:** Adjuk meg a kezdőbeállításokat egy routeren és a végberendezéseken.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A router kezdőbeállításainak megadása** | Állítsuk be a kezdőbeállításokat egy Cisco IOS routeren. |
| **Interfészek konfigurálása** | Konfiguráljunk két aktív interfészt egy Cisco IOS routeren. |
| **Az alapértelmezett átjáró beállítása** | Állítsuk be az alapértelmezett átjárót az eszközökön. |

[9.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[10.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A router kezdőbeállításainak megadása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                             
*             

1. Alapvető forgalomirányító-konfiguráció
2. A router kezdőbeállításainak megadása

# A router kezdőbeállításainak megadása

10.1.1

## A router alapvető beállításának lépései

A router kezdőbeállításainak megadása az alábbi lépésekkel történik:

1. Állítsuk be az eszköz nevét.

Router(config)# **hostname**

2. Tegyük biztonságossá a privilegizált EXEC módot.

Router(config)# **enable secret** password

3. Tegyük biztonságossá a felhasználói EXEC mód hozzáférését.

Router(config)# **line console 0**  
Router(config-line)# **password** password  
Router(config-line)# **login**

4. Tegyük biztonságossá a Telnet / SSH távelérést.

Router(config-line)# **line vty 0 4**  
Router(config-line)# **password** password  
Router(config-line)# **login**  
Router(config-line)# **transport input** {**ssh** | **telnet**}

5. Tegyük biztonságossá a konfigurációs fájlban tárolt összes jelszót.

Router(config-line)# **exit**  
Router(config)# **service password-encryption**

6. Jelenítsünk meg egy jogos használatra vonatkozó üzenetet.

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

7. Mentsük el a beállításokat!

Router(config)# **end**  
Router# **copy running-config startup-config**

10.1.2

## Példa a router alapbeállításainak megadására

Ebben a példában a topológia részét képező R1 router kezdőbeállításait adjuk meg.

The figure shows a network topology diagram with two PCs, two switches, two routers, and an internet cloud. From left to right PC 1 connects to a switch which connects to R1 which connects to R2 which connects to a second switch, which connects to PC2. PC1 is on the 192.168.10.0/24 IPv4 network and has IPv4 address 192.168.10.10. PC1 also connects to the 2001.db8:acad:10::/64 IPv6 network and has IPv6 address 2001:db8:acad:10::10. Router R1 G0/0/0 interface is on the same network as PC1. The IPv4 and IPv6 address of the G0/0/0 interface of R1 is 192.168.10.1 and 2001:db8:acad:10::1. The IPv4 network connecting R1 and R2 is 209.165.200.224/30. The IPv6 network connecting R1 and R2 is 2001:db8:feed:224::/64. R1 connects to R2 over interface G0/0/1 which has IPv4 address 209.165.200. 225 and IPv6 address 2001:db8:feed:224::1. The IP addresses for R2 on the shared network with R1 are 209.165.200. 226 and 2001:db8:feed:224::2. PC2 and R2 are connected on IPv4 network 10.1.1.0/24 and IPv6 network 2001:db8:cafe:1::/64. PC1 has IPv4 address 10.1.1.10 and IPv6 address 2001:db8:cafe::10. R2 has IPv4 address 10.1.1.1 and IPv6 address 2001:db8:cafe::1.

.10 ::10 192.168.10.0/24 .1 ::1 G0/0/0 G0/0/1 .225 ::1 .226 ::2 .1 ::1 209.165.200.224/30 10.1.1.0/24 .10 ::10 2001:db8:acad:10::/64 2001:db8:feed:224::/64 2001:db8:cafe:1::/64 PC1 PC2 R1

R2

Internet

Az R1 eszköznevének beállításához használjuk a következő parancsokat.

Router> **enable**

Router# **configure terminal**

Enter configuration commands, one per line.

End with CNTL/Z.

Router(config)# **hostname R1**

R1(config)#

**MEGJEGYZÉS:** Figyeljük meg, hogy a router promptja miként jeleníti meg a router állomásnevét.

A routerhez való minden hozzáférést biztonságossá kell tenni. A privilegizált EXEC mód a felhasználó számára teljes hozzáférést biztosít az eszközhöz és annak konfigurációjához. Ezért az a legfontosabb, hogy ezt a módot biztonságossá tegyük.

Az alábbi parancsok biztonságossá teszik a privilegizált EXEC módot és a felhasználói EXEC módot, engedélyezik a Telnet és az SSH távelérést, és titkosítják az összes, egyszerű szöveges formában tárolt (pl.: felhasználói EXEC és VTY vonali) jelszót.

R1(config)# **enable secret class**

R1(config)#

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)#

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **transport input ssh telnet**

R1(config-line)# **exit**

R1(config)#

R1(config)# **service password-encryption**

R1(config)#

A jogos használatra vonatkozó üzenet figyelmezteti a felhasználókat, hogy az eszközhöz csak az arra jogosult felhasználók férhetnek hozzá. A jogi figyelmeztetés beállítása az alábbiak szerint történik.

R1(config)# **banner motd #**

Enter TEXT message. End with a new line and the #

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**WARNING: Unauthorized access is prohibited!**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**#**

R1(config)#

Ha az előző parancsok kiadása megtörtént a routeren, de áramkimaradás lép fel, minden beállított parancsot elfelejt. Ezért fontos a konfiguráció mentése a módosítások végrehajtása során. A következő parancs az NVRAM-ba menti a konfigurációt.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

10.1.3

## Parancsszimulátor - A router kezdőbeállításainak megadása

A parancsszimulátor segítségével gyakorolhatjuk a router kezdőbeállításainak megadását.

* Állítsuk be az eszköz nevét.
* Tegyük biztonságossá a privilegizált EXEC módot.
* Tegyük biztonságossá a Telnet és SSH távelérést.
* Titkosítsuk a szöveges jelszavakat.
* Jelenítsünk meg egy jogos használatra vonatkozó üzenetet.

Lépjünk be a globális konfigurációs módba a router nevének „R1”-re való beállításához.

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

Állítsuk be, hogy az enable titkos jelszó "class" legyen.

R1(config)#enable secret class

Konfiguráljuk a „cisco” -t a konzolvonal jelszavaként, követeljük meg a felhasználók hitelesítését és térjünk vissza globális konfigurációs módba.

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

A 0–4 vty vonalon állítsuk be a „cisco” jelszót, írjuk elő a felhasználóknak a bejelentkezést, engedélyezzük az SSH és a Telnet hozzáférést, és térjünk vissza a globális konfigurációs módba.

R1(config)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#transport input ssh telnet

R1(config-line)#exit

Titkosítsuk az összes egyszerű szöveges jelszót.

R1(config)#service password-encryption

Írjuk be napi üzenetnek az „Authorized Access Only!” szöveget és használjuk a # határoló karaktert.

R1(config)#banner motd #Authorized Access Only!#

Lépjünk ki globális konfigurációs módból.

R1(config)#exit

R1#

Sikeresen konfiguráltuk az R1 router kezdeti beállításait.

10.1.4

## Packet Tracer - A router kezdőbeállításainak megadása

A feladat során a router alapbeállításait adjuk meg. A parancssorhoz és a konzolporthoz biztonságos hozzáférést állítunk be titkosított és egyszerű szöveges jelszavak segítségével. Ezen kívül megtanuljuk, hogyan kell üzenetet küldeni a routerre bejelentkező felhasználóknak és egyben figyelmeztetni a jogosulatlan belépőket a tiltott hozzáférésre. Végezetül ellenőrizzük és elmentjük az aktív konfigurációt.

[A router kezdeti beállításainak megadása](https://contenthub.netacad.com/courses/itn/_common/10.1.4-packet-tracer---configure-initial-router-settings_hu-HU.pka)

[10.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[10.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Interfészek konfigurálása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                
*             

1. Alapvető forgalomirányító-konfiguráció
2. Interfészek konfigurálása

# Interfészek konfigurálása

10.2.1

## Interfészek konfigurálása

Ezen a ponton a router már rendelkezik egy alapkonfigurációval. A következő lépés az interfészek konfigurálása. Ennek az oka, hogy a routerek nem érhetők el a végberendezésekről, amíg az interfészek nincsenek beállítva. A Cisco routerek számos különböző típusú interfésszel rendelkezhetnek. A Cisco ISR 4321 router például két Gigabit Ethernet interfésszel rendelkezik:

* **GigabitEthernet 0/0/0 (G0/0/0)**
* **GigabitEthernet 0/0/1 (G0/0/1)**

A router interfészeinek beállítása nagyon hasonlít a switch felügyeleti SVI-jének beállításához. Konkrétan az alábbi parancsok kiadását jelenti:

Router(config)# **interface** type-and-number  
Router(config-if)# **description** description-text  
Router(config-if)# **ip address** ipv4-address subnet-mask  
Router(config-if)# **ipv6 address** ipv6-address/prefix-length  
Router(config-if)# **no shutdown**

**MEGJEGYZÉS:** Ha a router interfésze engedélyezve van, információs üzeneteknek kell megjelenniük, amelyek megerősítik, hogy a kapcsolat működik.

Bár a **description** parancs nem szükséges az interfész engedélyezéséhez, célszerű használni. Valódi hálózatokban a leírásban található információk, mint például az adott interfészhez csatlakozó hálózat típusa, segíthetnek az esetleges hibaelhárításban. Ha például az interfész egy szolgáltatóhoz csatlakozik, a **description** parancs segítségével hasznos lehet megadni a szolgáltatói kapcsolat információit és a kapcsolattartó adatait is.

**MEGJEGYZÉS:** Ez a szöveg maximálisan 240 karakter lehet.

A **no shutdown** parancs használata aktiválja az interfészt, és hasonló az interfész felkapcsolásához, mely csak abban az esetben lesz aktív, ha fizikailag egy másik eszközhöz (pl:. switch-hez vagy routerhez) kapcsolódik.

**MEGJEGYZÉS:** Az olyan routerek közötti kapcsolatokon, ahol nincs Ethernet switch, az egymást összekötő mindkét interfészt konfigurálni és engedélyezni kell.

10.2.2

## Példa a router interfész beállítására

Ebben a példában a topológia részét képező R1 közvetlenül csatlakoztatott interfészeit engedélyezzük.

The diagram is a network topology showing the IPv4 and IPv6 addressing of the network devices. What follows is a description of the topology from left to right. PC1 is connected to a switch connected to router R1. The network IPv4 address is 192.168.10.0/24 and the IPv6 address is 2001:db8:acad:10::/64. PC1 has an address of .10 and ::10. Interface G0/0/0 on R1 has an address of .1 and ::1. R1 interface G0/0/1 is then connected to router R2 on IPv4 network 209.165.200.224/30 and IPv6 network 2001:db8:feed:224::/64. Interface G0/0/1 on R1 has an address of .225 and ::1. The interface on R2 has an address of .226 and ::2. R2 is then connected to a switch which is connected to PC2 on IPv4 network 10.1.1.0/24 and IPv6 network 2001:db8:cafe:1::/64. The R2 interface has an address of .1 and ::1. PC2 has an address of .10 and ::10. R2 also has a connection to the Internet cloud.

.10 ::10 192.168.10.0/24 .1 ::1 G0/0/0 G0/0/1 .225 ::1 .226 ::2 .1 ::1 209.165.200.224/30 10.1.1.0/24 .10 ::10 2001:db8:acad:10::/64 2001:db8:feed:224::/64 2001:db8:cafe:1::/64 PC1 PC2 R1

R2

Internet

Az R1 interfészeinek konfigurálásához használjuk az alábbi parancsokat.

R1> **enable**

R1# **configure terminal**

Enter configuration commands, one per line.

End with CNTL/Z.

R1(config)# **interface gigabitEthernet 0/0/0**

R1(config-if)# **description Link to LAN**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:10::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)#

\*Aug 1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down

\*Aug 1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up

\*Aug 1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config)#

R1(config)#

R1(config)# **interface gigabitEthernet 0/0/1**

R1(config-if)# **description Link to R2**

R1(config-if)# **ip address 209.165.200.225 255.255.255.252**

R1(config-if)# **ipv6 address 2001:db8:feed:224::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)#

\*Aug 1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down

\*Aug 1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up

\*Aug 1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config)#

**MEGJEGYZÉS:** Figyeljük meg azokat az információs üzeneteket, amelyek arról tájékoztatnak, hogy a G0/0/0 és a G0/0/1 engedélyezve vannak.

10.2.3

## Az interfész konfigurációjának ellenőrzése

Számos olyan parancs létezik, amivel egy interfész konfigurációját ellenőrizhetjük. Ezek közül a leghasznosabb parancs a példában látható **show ip interface brief** és **show ipv6 interface brief**.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 192.168.10.1 YES manual up up

GigabitEthernet0/0/1 209.165.200.225 YES manual up up

Vlan1 unassigned YES unset administratively down down

R1# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

FE80::201:C9FF:FE89:4501

2001:DB8:ACAD:10::1

GigabitEthernet0/0/1 [up/up]

FE80::201:C9FF:FE89:4502

2001:DB8:FEED:224::1

Vlan1 [administratively down/down]

unassigned

R1#

10.2.4

## A konfigurációt ellenőrző parancsok

A táblázat összefoglalja az interfész konfigurációjának ellenőrzéséhez használt legnépszerűbb **show** parancsokat.

| Table caption | |
| --- | --- |
| **Parancsok** | **Leírás** |
| **show ip interface brief** **show ipv6 interface brief** | A parancs kimenete megjelenít minden interfészt, azok IP-címét és aktuális állapotát. A beállított és csatlakoztatott interfészeknél a Status (állapot) és a Protocol (protokoll) oszlopokban is “up” értéknek kell szerepelni. Bármilyen egyéb érték azt jelzi, hogy a konfigurációval vagy a kábelezéssel probléma van. |
| **show ip route** **show ipv6 route** | Megjeleníti a RAM-ban tárolt IP-irányítótáblát. |
| **show interfaces** | Megjeleníti az eszköz interfészeire vonatkozó statisztikai adatokat. Ez a parancs azonban csak az IPv4-címzési információkat jeleníti meg. |
| **show ip interfaces** | Megjeleníti a router interfészeinek IPv4 statisztikai adatait. |
| **show ipv6 interface** | Megjeleníti a router interfészeinek IPv6 statisztikai adatait. |

Az egyes konfigurációt ellenőrző parancsok kimenetének megtekintéséhez kattintsunk az alábbi gombokra!

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 192.168.10.1 YES manual up up

GigabitEthernet0/0/1 209.165.200.225 YES manual up up

Vlan1 unassigned YES unset administratively down down

R1#

10.2.5

## Parancsszimulátor - Interfészek konfigurálása

A parancsszimulátor segítségével gyakorolhatjuk a GigabitEthemet 0/0 interfész konfigurálását egy routeren.

* Az összeköttetést jellemző leírásnál adjuk meg a „Link to LAN” kifejezést.
* Állítsuk be a 192.168.10.1 IPv4-címet, a 255.255.255.0 alhálózati maszkkal.
* Configure the IPv6 address as 2001:Állítsuk be a 2001:db8:acad:10::1 IPv6-címet a /64 előtaggal.
* Aktiváljuk az interfészt.

Lépjünk be a globális konfigurációs módba.

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Konfiguráljuk a Gigabitethernet 0/0/0 interfészt.

R1(config)#interface gigabitethernet 0/0/0

Írjuk le a kapcsolatot „Link to LAN” néven.

R1(config-if)#description Link to LAN

Lássuk el az interfészt IPv4 címmel **192.168.10.1** és netmaszkkal **255.255.255.0**.

R1(config-if)#ip address 192.168.10.1 255.255.255.0

Konfiguráljuk az interfészt az IPv6-címmel **2001:db8:acad:10::1** és az előtag hosszával **/64**.

R1(config-if)#ipv6 address 2001:db8:acad:10::1/64

Engedélyezzük az interfészt, és térjünk vissza a globális konfigurációs módba.

R1(config-if)#no shutdown

\*Aug 1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down

\*Aug 1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up

\*Aug 1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#exit

R1#

Sikeresen konfiguráltuk az R1 router kezdeti beállításait.

[10.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A router kezdőbeállításainak megadása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[10.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az alapértelmezett átjáró beállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                    
*             

1. Alapvető forgalomirányító-konfiguráció
2. Az alapértelmezett átjáró beállítása

# Az alapértelmezett átjáró beállítása

10.3.1

## Állomás alapértelmezett átjárója

Ha a helyi hálózat csak egy routerrel rendelkezik, akkor ez lesz az átjáró, és a hálózat összes állomásán és switch-én be kell állítani ezt az információt. Ha a helyi hálózat több routerrel rendelkezik, ki kell választanunk közülük az alapértelmezett átjárót. Ez a témakör bemutatja, hogy miként állíthatjuk be az alapértelmezett átjárót az állomásokon és a switch-eken.

Egy végberendezés hálózati működéséhez megfelelő IP-cím információkat, köztük az alapértelmezett átjáró címét kell az eszközön beállítani. Az alapértelmezett átjáróra csak abban az esetben van szükség, ha egy állomás egy másik hálózaton lévő eszköznek szeretne csomagot küldeni. Az alapértelmezett átjáró címe rendszerint az állomás helyi hálózatához csatlakozó router interfész címe. Az állomás IP-címének és a router interfész címének ugyanabban a hálózatban kell lennie.

Tegyük fel például, hogy egy IPv4-hálózat részét képezi egy olyan router, amely két különálló LAN-t köt össze. A G0/0/0 interfész a 192.168.10.0, a G0/0/1 pedig a 192.168.11.0 hálózathoz csatlakozik. Minden állomáson a megfelelő alapértelmezett átjáró van beállítva.

Ebben a példában, ha a PC1 csomagot küld a PC2-nek, akkor nincs szükség az alapértelmezett átjáró használatára, hiszen a PC1 a PC2-nek címzett csomagot a switch-en keresztül közvetlenül a PC2-nek továbbítja.

The diagram is a network topology with one router, two switches, and four PCs showing the flow of information between devices on the same network. PC1 and PC2 are connected to the switch on network 192.168.10.0/24 at interface G0/0/0 on router R1. PC3 and PC4 are connected to another switch on network 192.168.11.0/24 at interface G0/0/1 on R1. An arrow shows the flow of information sent from PC1 passing through the attached switch on its way to PC2.

PC! PC! .10 .11 192.168.10.0/24 .1G0/0/0 G0/0/1.1 .10 .11 192.168.11.0/24 R1 PC1 PC2 PC3

PC4

Mi a helyzet, ha a PC1 küld csomagot a PC3-nak? A PC1 a PC3 IPv4-címével címzi meg a csomagot, de az alapértelmezett átjárónak küldi el, ami az R1 G0/0/0 interfésze. A router fogadja a csomagot, az irányítótáblájában a célcím alapján megkeresi a megfelelő kimenő interfészt. Az R1 ezután továbbítja a csomagot a megfelelő interfészről a PC3-nak.

The diagram is a network topology with one router, two switches, and four PCs showing the flow of information between devices on different networks. PC1 and PC2 are connected to the switch on network 192.168.10.0/24 at interface G0/0/0 on router R1. PC3 and PC4 are connected to another switch on network 192.168.11.0/24 at interface G0/0/1 on R1. An arrow shows the flow of information sent from PC1 passing through R1 and onto PC3.

PC! PC! .10 .11 192.168.10.0/24 .1G0/0/0 G0/0/1.1 .10 .11 192.168.11.0/24 R1 PC1 PC2 PC3

PC4

Ugyanez a folyamat menne végbe egy IPv6-hálózaton is, bár ez nem látható az ábrán. Az eszközök a helyi router IPv6-címét használnák alapértelmezett átjáróként.

10.3.2

## Switch alapértelmezett átjárója

A kliens számítógépeket összekötő switch jellemzően 2. rétegbeli eszköz. Mint ilyen, a 2. rétegbeli switch nem igényel IP-címet a megfelelő működéshez. Egy IP-konfiguráció azonban beállítható a switch-en, hogy a rendszergazda távolról hozzáférjen.

Ahhoz, hogy a helyi IP-hálózaton keresztül elérjük és felügyeljük a switch-et, annak egy konfigurált SVI-vel (Switch Virtual Interface, virtuális switch interfész) kell rendelkeznie. Az SVI-t IPv4-címmel és alhálózati maszkkal konfiguráljuk a helyi LAN-on. A switch-nek rendelkeznie kell egy alapértelmezett átjáró címével is, hogy távolról felügyelni tudjuk egy másik hálózatról.

Az alapértelmezett átjáró címe általában minden olyan eszközön be van állítva, amely a helyi hálózaton kívüli eszközökkel kommunikál.

A switch alapértelmezett átjárójának megadásához használjuk a **ip default-gateway** ip-cim globális konfigurációs parancsot. A beállított ip-cim a switch-hez csatlakoztatott helyi router interfész IPv4-címe.

Az ábrán a rendszergazda egy távoli hálózatról csatlakozik az S1 switch-hez.

The diagram is a network topology showing a router R1 connected to two switches, S1 on network 192.168.10.0/24, and S2 on network 192.168.11.0/24. A user is connected to S2 and an arrow shows the user is accessing S1 remotely. Above the user is a box showing the user has CLI access to S1 and is displaying the running configuration.

S1# show running-configBuilding configuration...!service password-encryption!hostname S1!Interface Vlan1 ip address 192.168.10.50.255.255.255.0!!ip default-gateway 192.168.10.1 .1G0/0/0 .1G0/0/1 PC1 PC2 S2 .10 .11 192.168.10.0/24 192.168.11.0/24 S1 R1

.50



Output OmittedOutput OmittedOutput Omitted

Ebben a példában a rendszergazdai állomás az alapértelmezett átjáróját használja, hogy a csomagot az R1 G0/0/1 interfészére küldje. Az R1 a G0/0/0 interfészéről továbbítja a csomagot az S1-nek. Mivel a csomag forrás IPv4-címe egy másik hálózatról való, az S1-nek szüksége van egy alapértelmezett átjáróra a csomag továbbításához az R1 G0/0/0 interfészére. Ezért az S1-en be kell állítani az alapértelmezett átjárót, hogy képes legyen válaszolni és SSH-kapcsolatot létrehozni a felügyeleti állomással.

**MEGJEGYZÉS:** A switch-hez csatlakoztatott számítógépekről származó csomagoknak már rendelkezniük kell a számítógép operációs rendszerén beállított alapértelmezett átjáró címével.

A munkacsoportos switch SVI-je IPv6-címmel is konfigurálható. A switch esetében azonban nincs szükség az alapértelmezett átjáró IPv6-címének manuálisan történő megadására. A switch automatikusan megkapja az alapértelmezett átjárót a router ICMPv6 router hirdetés üzenetéből.

10.3.3

## Parancsszimulátor - Az alapértelmezett átjáró beállítása

A parancsszimulátor segítségével gyakorolhatjuk a 2. rétegbeli switch alapértelmezett átjárójának konfigurálását.

Lépjünk be a globális konfigurációs módba.

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Állítsuk be az alapértelmezett átjárót 192.168.10.1-re az S1-en.

S1(config)#ip default-gateway 192.168.10.1

S1(config)#

Sikeresen beállítottuk az alapértelmezett átjárót az S1 switch-en.

10.3.4

## Packet Tracer - Router csatlakoztatása egy LAN-hoz

A feladat során különféle **show** parancsokat használunk a router aktuális állapotának megjelenítéséhez. A címzési táblázat alapján beállítjuk az Ethernet interfészeket, majd ellenőrizzük és teszteljük a konfigurációt.

[Build a Switch and Router Network](https://contenthub.netacad.com/courses/itn/_common/build-a-switch-and-router-network.pksz)

10.3.5

## Video - Troubleshoot a Default Gateway

Press the Play button to watch the video.

10.3.6

## Packet Tracer - Az alapértelmezett átjáró problémáinak elhárítása

Egy eszköz hálózati működéséhez IP-címet, alhálózati maszkot és alapértelmezett átjárót kell rajta beállítani. Alapértelmezett átjáróra csak abban az esetben van szükség, ha egy állomás egy másik hálózaton lévő eszköznek szeretne csomagot küldeni. Az alapértelmezett átjáró címe rendszerint az állomás helyi hálózatához csatlakozó router interfész címe. Ebben a feladatban befejezzük a hálózat dokumentálását, majd ellenőrizzük azt a végpontok közötti kapcsolatok tesztelésével és a felmerülő hibák kijavításával. A hibaelhárítás lépései a következők lesznek:

1. A dokumentáció ellenőrzése és a problémák felfedése tesztek segítségével.
2. Alkalmas megoldás keresése egy adott problémára.
3. A kiválasztott megoldás megvalósítása.
4. A megoldás ellenőrzése teszteléssel.
5. A megoldás dokumentálása.

[Az alapértelmezett átjáró problémáinak elhárítása](https://contenthub.netacad.com/courses/itn/_common/10.3.5-packet-tracer---troubleshoot-default-gateway-issues_hu-HU.pka)

[10.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Interfészek konfigurálása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[10.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                     

1. Alapvető forgalomirányító-konfiguráció
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

10.4.1

## Videómagyarázat - Hálózati eszközök közötti különbségek: 1. rész

A Packet Tracer feladatok és a laborgyakorlatok során megtapasztalt különböző routereket és switch-eket bemutató videó 1. részének megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

10.4.2

## Videómagyarázat - Hálózati eszközök közötti különbségek: 2. rész

A Packet Tracer feladatok és a laborgyakorlatok során megtapasztalt különböző routereket és switch-eket bemutató videó 2. részének megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

10.4.3

## Packet Tracer - Alapvető eszközkonfiguráció

A hálózati vezető elégedett a LAN rendszergazdai teljesítményünkkel. Szeretné, ha megmutatnánk, hogy képesek vagyunk olyan router konfigurálására is, mely két LAN-hoz csatlakozik. Feladatunk egy Cisco IOS router és egy switch alapbeállításainak megadása, majd a végpontok közötti kapcsolatok tesztelésével az eszközök konfigurációjának ellenőrzése.

[Alapbeállítások](https://contenthub.netacad.com/courses/itn/_common/10.4.3-packet-tracer---basic-device-configuration_hu-HU.pka)

10.4.4

## Laborgyakorlat - Switch-ből és routerből álló hálózat építése

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: A topológia felépítése és az eszközök kezdeti beállításainak megadása.
  2. rész: Az eszközök konfigurálása és a kapcsolat ellenőrzése.
  3. rész: Eszközinformációk megjelenítése.

10.4.5

## Miről tanultunk ebben a fejezetben?

**A router kezdőbeállításainak megadása**

A router kezdőbeállításainak megadása az alábbi lépésekkel történik:

1. Állítsuk be az eszköz nevét.
2. Tegyük biztonságossá a privilegizált EXEC módot.
3. Tegyük biztonságossá a felhasználói EXEC mód hozzáférését.
4. Tegyük biztonságossá a Telnet / SSH távelérést.
5. Tegyük biztonságossá a konfigurációs fájlban tárolt összes jelszót.
6. Jelenítsünk meg egy jogos használatra vonatkozó üzenetet.
7. Mentsük el a beállításokat!

**Interfészek konfigurálása**

A routerek eléréséhez annak interfészeit konfigurálni kell. A Cisco ISR 4321 router két Gigabit Ethernet interfésszel van felszerelve: Gigabitethernet 0/0/0 (G0/0/0) és Gigabitethernet 0/0/1 (G0/0/1). A router interfészeinek beállítása nagyon hasonlít a switch felügyeleti SVI-jének beállításához. A **no shutdown** parancs használata aktiválja az interfészt, mely csak abban az esetben lesz aktív, ha fizikailag egy másik eszközhöz (pl:. switch-hez vagy routerhez) kapcsolódik. Számos olyan parancs létezik, amivel egy interfész konfigurációját ellenőrizhetjük: a **show ip interface brief**, a **show ipv6 interface brief**, a **show ip route**, a **show ipv6 route**, a **show interfaces**, a **show ip interface** és a **show ipv6 interface.**.

**Az alapértelmezett átjáró beállítása**

Egy végberendezés hálózati működéséhez megfelelő IP-cím információkat, köztük az alapértelmezett átjáró címét kell az eszközön beállítani. Az alapértelmezett átjáró címe rendszerint az állomás helyi hálózatához csatlakozó interfész címe. Az állomás IP-címének és a router interfész címének ugyanabban a hálózatban kell lennie. Ahhoz, hogy a helyi IP-hálózaton keresztül elérjük és felügyeljük a switch-et, a switch-nek egy konfigurált SVI-vel (Switch Virtual Interface, virtuális switch interfész) kell rendelkeznie. Az SVI-t IPv4-címmel és alhálózati maszkkal konfiguráljuk a helyi LAN-on. A switch-nek rendelkeznie kell egy alapértelmezett átjáró címével is, hogy távolról felügyelni tudjuk egy másik hálózatról. A switch alapértelmezett átjárójának megadásához használjuk a **ip default-gateway ip-address** globális konfigurációs parancsot. Használjuk a switch-hez csatlakoztatott helyi router interfész IPv4-címét.

10.4.6

## Ellenőrző kvíz - A router alapbeállításainak megadása

Az űrlap teteje

1. A router elindul, majd beállítási (setup) módba lép. Mi ennek az oka?

Az űrlap alja

Melyik parancsot használjuk a router konfigurációs fájljában lévő összes jelszó titkosítására?

A vállalati házirend a legbiztonságosabb módszert használja a routerek privilegizált exec és konfigurációs módjához való hozzáférés biztosítása érdekében. A privilegizált EXEC mód jelszava trustknow1. Az alábbi router parancsok közül melyik éri el a legmagasabb szintű biztonságot?

Hogyan reagál a router, miután a, "router(config)# **hostname portsmouth**" parancsot kiadták?

A rendszergazda egy új routert konfigurál, amely lehetővé teszi a sávon kívüli felügyeleti hozzáférést. Melyik parancskészlet teszi lehetővé a szükséges bejelentkezést a **cisco** jelszóval?

Melyik parancs használható a Cisco routeren az összes interfész, a hozzájuk rendelt IPv4-címek és ezek aktuális állapotának megjelenítéséhez?

Melyik CLI-mód teszi lehetővé a felhasználók számára, hogy hozzáférjenek az összes (pl.: konfiguráláshoz, felügyelethez és hibaelhárításhoz használt) eszközparancshoz?

Mi a célja az indítási konfigurációs fájlnak a Cisco routeren?

Melyik jellemző írja le a számítógép alapértelmezett átjáróját?

Mi a **banner motd** parancs célja?

A technikus konfigurál egy routert, hogy lehetővé tegye a menedzsment minden formáját. A különböző típusú hozzáférések részeként a technikus megpróbálja beírni a **login** parancsot. Melyik konfigurációs módban kell beírni ezt az utasítást?

Mit tárol a Cisco router NVRAM-ja?

Melyik állítás igaz a **service password-encryption** parancsra vonatkozóan?

[10.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az alapértelmezett átjáró beállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                               
*           

1. IPv4-címzés
2. Bevezetés

# Bevezetés

11.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az IPv4-címzésről szóló fejezetben.

Jelenleg még mindig rengeteg IPv4-címzést használó hálózat van, annak ellenére, hogy az ezeket használó szervezetek folyamatosan térnek át az IPv6-ra. Tehát még mindig nagyon fontos, hogy a hálózati rendszergazdák mindent tudjanak az IPv4-címzésről. Ez a fejezet részletesen tárgyalja az IPv4-címzéssel kapcsolatos alapvető szempontokat. Ez magában foglalja, hogyan szegmentálhatunk egy hálózatot kisebb alhálózatokra, és hogyan hozhatunk létre változó hosszúságú alhálózati maszkot (VLSM) egy átfogó IPv4-címzési struktúra részeként. Az alhálózatokra bontás olyan, mintha egy tortát szelnénk egyre kisebb szeletekre. Az alhálózatokra bontás elsőre kissé bonyolultnak tűnhet, de mutatunk néhány trükköt, amellyel könnyebben elsajátítható. Ez a fejezet számos videót, az alhálózat-számítás gyakorlását segítő feladatot, valamint Packet Tracer feladatot és egy laborgyakorlatot is tartalmaz. Ahogy erre ráérzünk, jó úton indulunk afelé, hogy hálózati rendszergazdává váljunk.

11.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** IPv4-címzés

**Fejezet célja:** Egy olyan IPv4-es alhálózati terv kiszámítása, amellyel hatékonyan szegmentálhatjuk a hálózatunkat.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **IPv4-címzési struktúra** | IPv4-es címek szerkezetének leírása, beleértve a hálózati részt, az állomásazonosító részt és az alhálózati maszkot. |
| **IPv4 egyedi címzés, szórás és csoportos címzés** | Az egyedi, a szórásos és a csoportos címzésű IPv4-címek jellemzőinek és felhasználásának összehasonlítása. |
| **IPv4-címek típusai** | A publikus, privát és fenntartott IPv4-címeket elmagyarázása. |
| **Hálózatszegmentálás** | Annak elmagyarázása, hogy az alhálózat szegmensei miként teszik lehetővé a jobb kommunikációt. |
| **Egy IPv4-hálózat alhálózatokra bontása** | Egy /24 előtagú IPv4-hálózat alhálózatainak kiszámítása. |
| **Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása** | Egy /16 és egy /8 előtagú IPv4-hálózat alhálózatainak kiszámítása. |
| **Követelményeket kielégítő alhálózatok kialakítása** | Egy IPv4-címzési rendszert kialakítása az alhálózatokra vonatkozó követelmények figyelembe vételével. |
| **Változó hosszúságú alhálózati maszk** | Annak bemutatása, hogy miként hozhatunk létre rugalmas címzési struktúrát változó hosszúságú alhálózati maszk (VLSM) segítségével. |
| **Strukturált tervezés** | Egy VLSM címzési struktúra kialakítása. |

[10.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-címzési struktúra](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                     
*           

1. IPv4-címzés
2. IPv4-címzési struktúra

# IPv4-címzési struktúra

11.1.1

## Hálózati és állomásazonosító részek

Az IPv4-cím egy 32 bites hierarchikus cím, amely egy hálózati és egy állomásazonosító részből áll. A hálózati rész és az állomásazonosító rész meghatározásához vegyük szemügyre az ábrán látható 32 bites adatfolyamot.

The diagram shows the breakdown of an IPv4 address into the network and host portions. The IPv4 address is 192.168.10.10. Underneath, the address is converted into 11000000 10101000 00001010 00001010. A dashed line shows the separation between the network and host portions. This occurs after the third octet and the 24th bit.

### IPv4-címek

11000000 10101000 00001010 00001010

192 . 168 . 10 . 10

Hálózati részÁllomásazonosító részIPv4-címek

Az egy hálózatban lévő valamennyi eszköz címének hálózati részében az egyes biteknek meg kell egyezniük. Az állomásazonosító rész bitjeinek pedig az alhálózaton belül egyedinek kell lenniük, hogy az állomás azonosítható legyen. Ha két állomás 32 bites címének hálózati része megegyezik, akkor az állomások ugyanazon a hálózaton vannak.

De honnan tudják az állomások, hogy a 32 bit melyik része a hálózati és melyik az állomásazonosító rész? Ennek meghatározása az alhálózati maszk feladata.

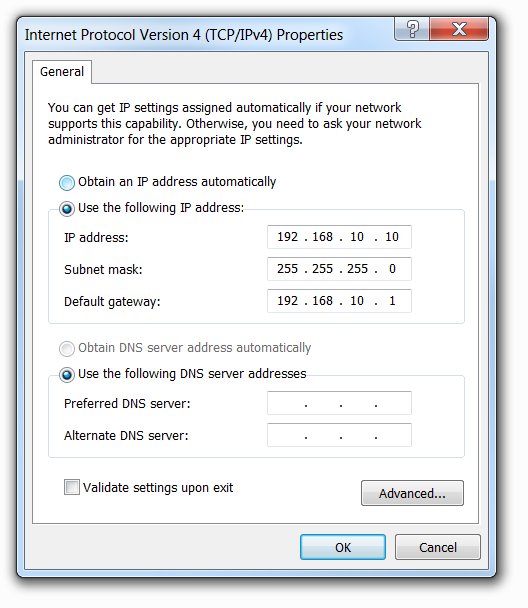
11.1.2

## Alhálózati maszk

Ahogy az ábrán is látható, egy IPv4-cím állomáshoz történő hozzárendelése az alábbiakat igényli:

* **IPv4-cím** - Ez az állomás egyedi IPv4-címe.
* **Alhálózati maszk** - Az alhálózati maszkot az IPv4-cím hálózati részének meghatározására használjuk.

### IPv4-konfiguráció Windows számítógépen



**MEGJEGYZÉS:** A távoli hálózatok eléréséhez egy alapértelmezett átjáró IPv4-címe, a tartománynevek IPv4-címekre történő lefordításához pedig egy DNS-szerver IPv4-címe szükséges.

Az IPv4-es alhálózati maszk segítségével megkülönböztethető az IPv4-cím hálózati része és állomásazonosító része. Amikor egy eszköznek IPv4-címet adunk, az eszköz az alhálózati maszk segítségével állapítja meg, hogy a hálózatának mi a címe. A hálózatcím az a cím, amely egy hálózat minden eszköze számára azonos.

Az alábbi ábra a 32 bites alhálózati maszkot pontozott decimális és bináris formátumban jeleníti meg.

subnet mask of 255.255.255.0 on top with the binary representation of 11111111 111111111 11111111 0000000 underneath; a dashed line is drawn after the third octet and the 24th bit

### Alhálózati maszk

255 . 255 . 255 . 11111111 00000000 0 11111111

11111111

Alhálózati maszk

Figyeljük meg, hogy az alhálózati maszk egy csupa egyesekből (1), majd azt követően csupa nullákból (0) álló bitszekvencia.

Egy IPv4-cím hálózati részének és állomásazonosító részének azonosításához az alhálózati maszkot bitről-bitre össze kell hasonlítani az IPv4-címmel, balról jobbra az ábrán látható módon.

The figure shows an IPv4 address, written in both dotted-decimal and binary, with the subnet mask below, also written in dotted-decimal and binary, used to show the division between the network portion and host portion of the address. The IPv4 address is 192.168.10.10 which is converted to 11000000 10101000 00001010 00001010. The subnet mask is 255.255.255.0 which is converted to 11111111 11111111 11111111 00000000. A dashed line shows the separation between the network and host portions. This occurs after the third octet and 24th bit.

### IPv4-cím társítása alhálózati maszkkal

255 . 255 . 255 . 0 11000000 10101000 00001010 00001010 192 . 168 . 10 . 10 11111111 00000000 11111111

11111111

Hálózati részÁllomásazonosító részIPv4-címekAlhálózati maszk

Figyeljük meg, hogy az alhálózati maszk nem tartalmazza a cím hálózati vagy állomásazonosító részét, csak azt mondja meg a számítógépnek, hogy egy adott IPv4-címben melyek ezek a részek.

A hálózati rész és az állomásazonosító rész azonosítására használt tényleges folyamat a logikai ÉS művelet (ÉSelés).

11.1.3

## Az előtag hossza

A hálózatcímek és állomáscímek pontozott decimális alhálózati maszk címével történő kifejezése nehézkessé válhat. Szerencsére van egy alternatív módszer az alhálózati maszk meghatározására, mégpedig az előtag hosszának megadása.

Az előtag hossza az alhálózati maszk egyeseinek száma. A perjellel megadott előtagban a perjel (/) után az 1-es bitek számát kell írni. Ezért számoljuk össze az alhálózati maszk bitjeinek számát, és tegyünk elé egy perjelet.

Nézzük meg a táblázat példáit. Az első oszlop állomáscímekkel használható különböző alhálózati maszkokat sorol fel. A második oszlop a konvertált 32 bites bináris maszkot jeleníti meg. Az utolsó oszlop az eredményül kapott előtag hosszát mutatja.

### Alhálózati maszk és előtag (prefix) hosszának összehasonlítása

| Subnet Mask 32-bit Address Prefix Length255.0.0.011111111.00000000.00000000.00000000/8255.255.0.011111111.11111111.00000000.00000000/16255.255.255.011111111.11111111.11111111.00000000/24255.255.255.12811111111.11111111.11111111.10000000/25255.255.255.19211111111.11111111.11111111.11000000/26255.255.255.22411111111.11111111.11111111.11100000/27255.255.255.24011111111.11111111.11111111.11110000/28255.255.255.24811111111.11111111.11111111.11111000/29255.255.255.25211111111.11111111.11111111.11111100/30 | | |
| --- | --- | --- |
| **Alhálózati maszk** | **32 bites cím** | **Előtag hossza** |
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

**MEGJEGYZÉS:** A hálózatcímet előtagnak vagy hálózati előtagnak is nevezik. Ezért az előtag hossza az alhálózati maszk egyeseinek száma.

Amikor egy IPv4-címet az előtag hosszával adunk meg, akkor az IPv4-címet ez az előtag hossz követi szóköz nélkül. A 192.168.10.10 255.255.255.0 például a következőképpen lenne leírva: 192.168.10.10/24. A különböző típusú előtag hosszúságok használatát később tárgyaljuk. A hangsúly egyelőre a /24 (azaz 255.255.255.0) előtagon lesz.

11.1.4

## A hálózat meghatározása: logikai ÉS

A logikai ÉS (AND) a digitális (Boolean) logikában használt három logikai művelet egyike. A másik kettő a VAGY (OR) és a NEM (NOT). Az ÉS művelet a hálózatcím meghatározásához használjuk.

A logikai ÉS művelet elvégzése után két bitből a következő eredményeket kapjuk: Figyeljük meg, hogy kizárólag az 1 ÉS 1 művelet eredménye 1. Bármely más kombináció eredménye 0.

* 1 ÉS 1 = 1
* 0 ÉS 1 = 0
* 1 ÉS 0 = 0
* 0 ÉS 0 = 0

**MEGJEGYZÉS:** A digitális logikában az 1 az Igaz, a 0 pedig a Hamis. Egy ÉS művelet használatakor mindkét bemeneti értéknek Igaz (1) értékűnek kell lennie ahhoz, hogy az eredmény Igaz (1) legyen.

Az IPv4-es állomás hálózatcímének meghatározásához az IPv4-címen és az alhálózati maszkon bitről bitre el kell végezni a logikai ÉS műveletet. Vagyis a bitenkénti ÉS művelet elvégzése után a hálózatcímet kapjuk eredményül.

Annak szemléltetéséhez, hogy a logikai ÉS művelet hogyan használható a hálózatcím meghatározásához, vegyük az ábrán látható, 192.168.10.10 IPv4-címmel rendelkező állomást és a 255.255.255.0 alhálózati maszkot:

* **IPv4 állomáscím (192.168.10.10)** - Az állomás IPv4-címe pontozott decimális és bináris formátumban.
* **Alhálózati maszk (255.255.255.0)** - Az állomás alhálózati maszkja pontozott decimális és bináris formátumban.
* **Hálózatcím (192.168.10.0)** — Az IPv4-cím és az alhálózati maszk közötti logikai ÉS művelet egy pontozott decimális és bináris formátumú IPv4-hálózatcímet eredményez.

The diagram shows the ANDing process between an IPv4 host address and a subnet mask resulting in the IPv4 network address of the host. The IPv4 host address is 192.168.10.10. Below that, the address is converted into 11000000 10101000 00001010 00001010. Below that, the subnet mask of 255.255.255.0 is written. Below that, the subnet mask is converted to 11111111 11111111 11111111 00000000. A line is drawn underneath the binary equivalent of the subnet mask. Below the line is the dotted-decimal and binary equivalent of the IPv4 network address as determined by the ANDing process. A blue shaded box shows the first bit of the IPv4 host address, a 1, compared to the first bit of the subnet mask, also a 1, resulting in a 1 as the first bit value in the IPv4 network address. The IPv4 network address is 192.168.10.0 with a binary equivalent of 11000000 101001000 00001010 00000000.

0000 1010 1100 0000 1010 1000 0000 1010 192 168 . . . 10 10 0000 0000 1111 1111 1111 1111 1111 1111 0000 0000 1100 0000 1010 1000 0000 1010 255 255 . . . 255 0 192 168 . . . 10

0

IPv4 állomáscím  
Alhálózati maszkIPv4  
hálózatcím  
ÉSEgyenlő

Használjuk példaként az első (kékkel jelölt) bitsorozatot, és figyeljük meg, hogy az állomáscím 1-es bitjén és az alhálózati maszk 1-es bitjén hajtjuk végre az ÉS műveletet, amely a hálózatcím esetében is 1-es bitet eredményez. 1 ÉS 1 = 1.

Az IPv4 állomáscím és az alhálózati maszk közötti ÉS művelet eredménye az állomás IPv4 hálózatcíme. Ebben a példában a 192.168.10.10 állomáscím és a 255.255.255.0 (/24) alhálózati maszk közötti ÉS művelet a 192.168.10.0/24 IPv4 hálózatcímet eredményezi. Ez egy fontos IPv4-művelet, mivel megadja az állomás számára, hogy melyik hálózatba tartozik.

11.1.5

## Videómagyarázat - Hálózat-, állomás- és szórási címek

Egy adott IPv4-címhez és alhálózati maszkhoz tartozó hálózat-, állomás- és szórási cím meghatározásának megtekintéséhez kattintsunk az ábrán látható lejátszás gombra.

11.1.6

## Hálózat-, állomás- és szórási címek

Az egyes hálózatokon belül háromféle IP-cím található:

* hálózatcímek
* állomáscímek
* szórási címek

Az ábrán látható topológia segítségével ezt a három típusú címet vizsgáljuk meg.

The diagram is network topology with four hosts connected to a switch which is connected to a router. The router interface has an IP address of 192.168.10.1/24 and the hosts have the following IP addreses: 192.168.10.10/24, 192.168.10.55/24, 192.168.10.101/24, and 192.168.10.12/24. The fourth octet of the router interface and the hosts is shown in a different color. A circle encompasses the router interface, switch, and all the hosts within which the network address of 192.168.10.0/24 is written, also with the fourth octet shown in a different color.

192.168.10.1/24 192.168.10.10/24 192.168.10.55/24 192.168.10.101/24 192.168.10.12/24

192.168.10.0/24

Hálózatcímek

**Hálózatcímek**

A hálózatcím egy konkrét hálózatot reprezentáló cím. Egy eszköz akkor tartozik ehhez a hálózathoz, ha megfelel három kritériumnak:

* Ugyanazt az alhálózati maszkot használja, mint a hálózatcím.
* Ugyanazokkal a hálózati bitekkel rendelkezik, mint a hálózatcím, amint azt az alhálózati maszk jelzi.
* Ugyanabban a szórási tartományban található, mint az azonos hálózatcímmel rendelkező többi állomás.

Az állomás úgy határozza meg a hálózat címét, hogy az IPv4-címe és alhálózati maszkja között ÉS műveletet hajt végre.

Amint az a táblázatban látható, az állomásazonosító részhez tartozó hálózatcím csupa 0 bitet tartalmaz, az alhálózati maszk által meghatározottak szerint. Ebben a példában a hálózatcím 192.168.10.0/24. Hálózatcím egyetlen eszközhöz sem rendelhető hozzá.

### Hálózat-, állomás- és szórási címek

| Table caption | | | |
| --- | --- | --- | --- |
|  | **Hálózati rész** | **Állomásazonosító rész** | **Állomásbitek** |
| Alhálózati maszk **255.255.255.**0 vagy **/24** | 255 255 255 11111111 11111111 11111111 | 0 00000000 |  |
| Hálózatcím **192.168.10.**0 vagy **/24** | 192 168 10 11000000 10100000 00001010 | 0 00000000 | Csupa 0 |
| Első cím **: 192.168.10**.1 vagy **/24** | 192 168 10 11000000 10100000 00001010 | 1 00000001 | csupa 0 és 1-es |
| Utolsó cím **: 192.168.10**.254 vagy **/24** | 192 168 10 11000000 10100000 00001010 | 254 11111110 | csupa 1-es és 0 |
| Szórási cím **192.168.10**.255 vagy **/24** | 192 168 10 11000000 10100000 00001010 | 255 11111111 | csupa 1-es |

**Állomáscímek**

Az állomáscím olyan cím, amely hozzárendelhető egy eszközhöz, például számítógéphez, laptophoz, okostelefonhoz, webkamerához, nyomtatóhoz, routerhez, stb. A cím állomásazonosító részét az alhálózati maszk által nullákkal jelölt bitek mutatják. Az állomáscím az állomásazonosító rész bitjeinek tetszőleges kombinációjából állhat, kivéve a csupa nullás bitet (ez lenne a hálózatcím) vagy a csupa egyes bitet (ez pedig a szórási cím lenne).

Egyazon hálózaton belül az összes eszköznek ugyanazzal az alhálózati maszkkal és megegyező hálózati bitekkel kell rendelkeznie. Csak az állomásbitek különböznek egymástól, ezeknek egyedinek kell lenniük.

Figyeljük meg, hogy a táblázatban szerepel egy első és egy utolsó állomáscím:

* **Első állomáscím** - A hálózaton belüli első állomás címe csupa 0-ból áll, az utolsó (jobb szélső) bit pedig 1-es. Ebben a példában 192.168.10.1/24.
* **Utolsó állomáscím** - A hálózaton belüli utolsó állomás címe csupa 1-esből áll, az utolsó (jobb szélső) bit pedig 0. Ebben a példában 192.168.10.254/24.

A 192.168.10.1/24 és a 192.168.10.254/24 közötti címek kioszthatók a hálózaton lévő eszközök számára.

**Szórási címek**

A szórási cím olyan cím, amelyet akkor használunk, amikor az IPv4-hálózat összes eszközét el szeretnénk érni. Amint az a táblázatban látható, a hálózat szórási címének állomásazonosító része csupa 1-esből áll, az alhálózati maszk által meghatározottak szerint. Ebben a példában a szórási cím 192.168.10.255/24. A szórási cím nem rendelhető hozzá egy eszközhöz.

11.1.7

## Activity - ANDing to Determine the Network Address

**Instructions:**

Use the ANDing process to determine the network address (in binary and decimal formats).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host Address | 172 | 29 | 226 | 91 |
| Subnet Mask | 255 | 255 | 224 | 0 |
| Host Address in binary | 10101100 | 00011101 | 11100010 | 01011011 |
| Subnet Mask in binary | 11111111 | 11111111 | 11100000 | 00000000 |
| Network Address in binary |  |  |  |  |
| Network Address in decimal |  |  |  |  |

11.1.8

## Check Your Understanding - IPv4 Address Structure

Az űrlap teteje

Check your understanding of IPv4 address structure by choosing the correct answer to the following questions.

1. Host-A has the IPv4 address and subnet mask 10.5.4.100 255.255.255.0. What is the network address of Host-A?

Az űrlap alja

Host-A has the IPv4 address and subnet mask 172.16.4.100 255.255.0.0. What is the network address of Host-A?

Host-A has the IPv4 address and subnet mask 10.5.4.100 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

Host-A has the IPv4 address and subnet mask 172.16.4.100 255.255.0.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

Host-A has the IPv4 address and subnet mask 192.168.1.50 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

[11.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4 egyedi címzés, szórás és csoportos címzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                       
*           

1. IPv4-címzés
2. IPv4 egyedi címzés, szórás és csoportos címzés

# IPv4 egyedi címzés, szórás és csoportos címzés

11.2.1

## Egyedi címzés (unicast)

Az előző témakörben megismerkedtünk az IPv4-címek szerkezetével; mindegyiknek van egy hálózati része és egy állomásazonosító része. A csomag forráseszközről történő küldésének különböző módjai vannak, és ezek a különböző átvitelek hatással vannak a cél IPv4-címekre.

Az egyedi címzésű átvitel egyetlen eszközre vonatkozik, amely közvetlen (egy-az-egynek típusú) kommunikáció során küld üzenetet egy másik eszköznek.

Az egyedi címzésű csomagnak van egy cél IP-címe, amely egyetlen címzettnek szól. A forrás IP-cím csak egyedi cím lehet, mivel a csomag csak egyetlen forrásból származhat. Ez független attól, hogy a cél IP-cím egyedi, szórásos vagy csoportos címzésű.

Az animáció lejátszásával egyedi címzéses átvitelre láthatunk példát.

This animation consists of three hosts and a printer connected to a switch and router. The animation illustrates the host with IP address 172.16.4.1 sending a unicast packet to IP address 172.16.4.253. When the switch receives the frame, it forwards it out to the printer with IP address 172.16.4.253.

Destination: 172.16.4.253/24

Source: 172.16.4.1/24

**MEGJEGYZÉS:** Ebben a kurzusban az eszközök közti kommunikáción, ha nem jelezzük külön, egyedi címzésű átvitelt értünk.

Az IPv4 állomáscímek egyedi címzésű címek, az 1.1.1.1 és a 223.255.255.255 közötti tartományból kerülhetnek ki. Azonban ebben a tartományban is számos, speciális célra fenntartott cím van. Ezekről a speciális célú címekről később lesz szó a fejezet során.

11.2.2

## Szórás

A szórásos átvitel olyan eszközre vonatkozik, amely egy-a-mindenkinek típusú kommunikáció során küld üzenetet a hálózaton lévő összes eszköznek.

A szórásos csomagban célcímként egy olyan IP-cím van, ami csupa 1-et tartalmaz az állomásazonosító részben.

**MEGJEGYZÉS:** Az IPv4 használ szórásos címzésű csomagokat, az IPv6 protokoll viszont már nem támogatja a szórásos címzést.

Egy szórásos üzenetet az egyazon szórási tartományba tartozó összes eszköznek fel kell dolgoznia. A szórási tartomány azonosítja az ugyanabban a hálózati szegmensben lévő összes állomást. A szórás lehet irányított vagy korlátozott. Az irányított szórás egy bizonyos hálózat minden állomásának küldött üzenetet jelenti. Például, a 172.16.4.0/24 hálózat egyik állomása küld egy csomagot a 172.16.4.255 címre. A korlátozott szórást a 255.255.255.255 címre kell küldeni. Alapértelmezés szerint a routerek nem továbbítják a szórásokat.

Az animáción a korlátozott szórásos átvitelre láthatunk példát.

This animation consists of three hosts and a printer connected to a switch and router. The animation illustrates the host with IP address 172.16.4.1 sending a broadcast packet. When the switch receives the broadcast packet, it forwards it out all ports to the other hosts, printer, and router.

Source: 172.16.4.1/24

Destination: 255.255.255.255

Limited Broadcast

A szórásos üzenetek hálózati erőforrásokat használnak, és minden fogadó állomást a csomagok feldolgozására kényszerítenek. Emiatt a szórásos forgalmat korlátozni kell annak érdekében, hogy ne rontsa le a hálózat vagy a többi eszköz teljesítményét. Mivel a routerek elkülönítik egymástól a szórási tartományokat, a nagymértékű szórást forgalmazó hálózatok felosztásával növelni tudjuk a hálózat teljesítményét.

**Irányított szórás**

A 255.255.255.255 szórási cím mellett minden hálózatnak van egy saját IPv4 szórási címe. Ez az irányított szórásnak nevezett cím a hálózat legmagasabb címét használja, ahol az összes állomásbit 1-es. Például a 192.168.1.0/24 hálózat irányított szórási címe a 192.168.1.255. Ez a cím lehetővé teszi a kommunikációt az adott hálózat összes állomásával. Ehhez a küldőnek egyszerűen egy csomagot kell küldenie a hálózat szórási címére, ezt a hálózat minden állomása meg fogja kapni és feldolgozza azt.

Egy olyan eszköz, amely nem kapcsolódik közvetlenül a célhálózathoz, az irányított szórást ugyanúgy továbbíthatja, mint az adott hálózaton lévő állomásnak szánt egyedi címzésű IP-csomagokat. Amikor egy irányított szórási csomag olyan routert ér el, amely közvetlenül kapcsolódik a célhálózathoz, a csomag szórással kerül továbbításra a célhálózaton.

**MEGJEGYZÉS:** A biztonsági aggályok és a rosszindulatú felhasználók korábbi visszaélései miatt az irányított szórás alapértelmezés szerint ki van kapcsolva a Cisco IOS Release 12.0 verziójával kezdve a globális konfigurációs paranccsal **no ip directed-broadcasts**.

11.2.3

## Csoportos küldés

A forgalmat azáltal csökkenti, hogy lehetővé teszi az állomás számára egyetlen csomag egyszerre több, a csoportcímre feliratkozott állomásnak történő elküldését.

A csoportos címzésű (multicast) csomag olyan csomag, amelynek cél IP-címe csoportos címzésű cím. Az IPv4 a 224.0.0.0 és a 239.255.255.255 közötti címeket a csoportos címzési tartomány számára tartja fenn.

Azokat az állomásokat, amelyek adott multicast kommunikációt fogadnak multicast klienseknek nevezzük. A multicast kliensek a kliens program által igényelt szolgáltatások segítségével iratkoznak fel a multicast csoportba.

Minden multicast csoportot egyetlen IPv4 multicast célcím képvisel. Amikor egy IPv4 állomás feliratkozik egy multicast csoportba, az állomás a multicast címre érkező csomagokat éppúgy feldolgozza, mint az ő saját egyedi címére érkezőket.

Az irányítóprotokollok, mint például az OSPF, csoportos címzésű átvitelt használnak. Az OSPF-et használó routerek például az OSPF számára fenntartott csoportos címen (224.0.0.5) kommunikálnak egymással. Kizárólag az OSPF-et futtató eszközök dolgozzák fel ezeket a 224.0.0.5 címre, mint cél IPv4-címre küldött csomagokat. Minden más eszköz figyelmen kívül hagyja ezeket a csomagokat.

Az animáció bemutatja, amint kliensek multicast csomagokat fogadnak.

This animation consists of three hosts and a printer connected to a switch and router. The animation illustrates the host with IP address 172.16.4.1 sending a multicast packet to the multicast group IP address 224.10.10.5. When the switch receives the multicast packet, it forwards it out all ports to the other hosts, printer, and router. However, only two hosts which are members of the multicast group address, will process the packets. All other hosts drop the packet.

Source: 172.16.4.1/24

Destination: 224.10.10.5

11.2.4

## Activity - Unicast, Broadcast, or Multicast

**Instructions:**

Click **New Problem** to view the destination IP address. Next, click the host or hosts which will receive a packet based on the address type (unicast, broadcast or multicast). Click **Check** to verify your answer. Click **New Problem** to get a new problem.

**Destination IP Address =**

Source Host

Start

Check

[11.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-címzési struktúra](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-címek típusai](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                             
*           

1. IPv4-címzés
2. IPv4-címek típusai

# IPv4-címek típusai

11.3.1

## Publikus és privát IPv4-címek

Ahogy az IPv4-csomagok továbbításának különböző módjai vannak, az IPv4-címeknek is különféle típusai léteznek. Bizonyos IPv4-címek nem használhatók internetes forgalomban, másokat pedig kifejezetten az interneten történő irányítás céljából osztanak ki. Némelyek a kapcsolat ellenőrzésére szolgálnak, mások pedig maguktól kerülnek hozzárendelésre. Hálózati rendszergazdaként előbb-utóbb alaposan megismerjük az IPv4-címek típusait, de egyelőre elég azt tudnunk, hogy mik ezek és mikor kell használni őket.

A publikus IPv4-címek olyan címek, amelyek globálisan címezhetők (route-olhatók) az internetszolgáltató (ISP) routerei között. A rendelkezésre álló IPv4-címek közül azonban nem mindegyik használható az interneten. Vannak olyan címtartományok, amelyeket a legtöbb szervezet az IPv4-címek belső állomásokhoz való hozzárendelésére használ.

Az 1990-es évek közepén, a World Wide Web (WWW) megjelenésével az IPv4-címtartomány kimerülése miatt privát IPv4-címeket vezettek be. A privát IPv4-címek nem egyediek, és bármely hálózaton belül felhasználhatók.

**MEGJEGYZÉS:** Az IPv4-cím kimerülésének hosszú távú megoldása az IPv6 volt.

### A privát címtartományok

| Network Address and Prefix RFC 1918 Private Address Range 10.0.0.0/81 0.0.0.0 - 10.255.255.255172.16.0.0/12172.16.0.0 - 172.31.255.255 192.168.0.0/16 192.168.0.0 - 192.168.255.255 | |
| --- | --- |
| **Hálózatcím és prefix** | **RFC 1918 privát címtartomány** |
| 10.0.0.0/8 | 10.0.0.0 - 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 - 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 |

**MEGJEGYZÉS:** A privát címeket az RFC 1918 határozza meg, ezért néha RFC 1918 címtartománynak is nevezik.

11.3.2

## Internetes forgalomirányítás

A legtöbb belső hálózat, a nagyvállalatoktól az otthoni hálózatokig, privát IPv4-címeket használ a belső eszközök (intranet) címzésére (beleértve az állomásokat és a routereket is). Ugyanakkor ezek a privát címek globálisan nem irányíthatók.

Az ábrán az 1., 2. és 3. ügyfélhálózatok csomagokat küldenek belső hálózataikon kívülre. Ezek a csomagok egy privát forrás IPv4-címmel és egy (globálisan címezhető) publikus cél IPv4-címmel rendelkeznek. A privát címmel rendelkező csomagokat szűrni kell (el kell dobni) vagy le kell fordítani egy publikus címre, mielőtt továbbítanánk a csomagot egy internetszolgáltató irányába.

The diagram is a network topology with three networks, each connected to a different ISP router. The ISP routers are performing NAT between each network and the Internet.

### Private IPv4 Addresses and Network Address Translation (NAT)

10.0.0.0/8 172.16.0.0/16 192.168.0.0/24 ISP1 ISP2

ISP3

This packet has a source IPv4 address that is a private address. I will translate it to a public IPv4 address using NATNetwork 1Network 2Network 3Internet

Mielőtt az internetszolgáltató továbbítaná ezt a csomagot, le kell fordítania a (privát) forrás IPv4-címet egy publikus IPv4-címre a hálózati címfordítás (Network Address Translation, NAT) segítségével. A NAT a privát és a publikus IPv4-címek közötti fordításra szolgál. Ez általában azon a routeren történik, amely összeköti a belső hálózatot az ISP hálózatával. A szervezet belső hálózatának privát IPv4-címeit a rendszer publikus IPv4-címekre fordítja le, mielőtt az internetre továbbítaná azokat.

**MEGJEGYZÉS:** Bár egy privát IPv4-címmel rendelkező eszköz nem érhető el közvetlenül egy másik eszközről az interneten keresztül, az IETF nem tekinti a magántulajdonú IPv4-címek vagy a hálózati címfordítás használatát hatékony biztonsági intézkedésnek.

Az interneten elérhető erőforrásokkal (például webszerverrel) rendelkező szervezeteknek vannak publikus IPv4-címmel rendelkező eszközeik is. Amint az az ábrán látható, a hálózat ezen része DMZ (demilitarizált zóna) néven ismert. Az ábrán látható router nemcsak útválasztást, hanem hálózati címfordítást is végez, és tűzfalként működik a biztonság érdekében.

The diagram is a network topology showing a router in the center with three connections; one to the company Intranet, one to a DMZ, and one to the Internet. On the left is the Intranet with devices using private IPv4 addresses. At the top, is the DMZ with two servers using public IPv4 addresses. On the right is the Internet cloud. The router is acting as a firewall and performing NAT.

Private IPv4  
addressesRouter to the Internet**Internet**Public IPv4  
addresses**DMZIntranet**

**MEGJEGYZÉS:** A privát IPv4-címeket gyakran használják oktatási célokra, mivel így nem kell publikus IPv4-címet használni, amely valószínűleg egy szervezethez tartozik.

11.3.3

## Activity - Pass or Block IPv4 Addresses

Instructions:

Decide to Pass or Block each IP address depending on whether it is Public (the Internet) or Private (small local network). Click Start to begin and click on either Pass or Block.

Points

Start

Reset

Block

Pass

11.3.4

## Speciális használatú IPv4-címek

Vannak bizonyos címek (pl.: a hálózatcím és a szórási cím), amelyek nem rendelhetők hozzá az állomásokhoz. Vannak olyan speciális címek is, amelyeket kioszthatunk ugyan állomásoknak, de ezek az állomások csak bizonyos korlátozásokkal kommunikálhatnak a hálózaton.

**Loopback címek**

A loopback (visszacsatolási) címeket (a 127.0.0.0 /8, vagy a 127.0.0.1 és a 127.255.255.254 között) sokszor csak a 127.0.0.1 címmel azonosítjuk, ezek olyan speciális címek, amelyeket az állomás használ, hogy a forgalmat visszairányítsa önmagához. Használhatók például egy állomáson annak tesztelésére, hogy a TCP/IP konfiguráció működőképes-e, amint az az ábrán látható. Figyeljük meg, hogyan válaszol a 127.0.0.1 loopback cím a **ping** parancsra. Azt is vegyük észre, hogy az ezen címtartományon belüli bármely cím visszairányít a helyi állomásra (localhost), amely az ábra **ping** második felében látható.

### A loopback interfész pingelése

C:\Users\NetAcad> **ping 127.0.0.1**

Pinging 127.0.0.1 with 32 bytes of data:

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

C:\Users\NetAcad> **ping 127.1.1.1**

Pinging 127.1.1.1 with 32 bytes of data:

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Reply from 127.1.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.1.1.1:

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

Approximate round trip times in milli-seconds:

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

C:\Users\NetAcad>

**Link-lokális címek**

A link-lokális (link-local) címek (a 169.254.0.0 /16, vagy a 169.254.0.1 és 169.254.255.254 között), ismertebb nevükön az automatikus privát IP-címzés (Automatic Private IP Addressing, APIPA) címei vagy önkiosztó címek. Ezeket egy Windows DHCP-kliens használja saját magának a beállítására abban az esetben, ha nincsenek elérhető DHCP-szerverek. A link-lokális címek használhatók egyenrangú (peer-to-peer) kapcsolatokban, de erre a célra nem túl gyakran használják őket.

11.3.5

## Az eredeti, osztály alapú címzés

1981-ben az IPv4-címek hozzárendelése az RFC 790 (<https://tools.ietf.org/html/rfc790>), Assigned Numbers című dokumentumban meghatározott osztály alapú címzéssel történt. Az ügyfelek számára kiosztott hálózatcím a három osztály (A, B vagy C) egyikébe volt besorolható. Az RFC az egyedi címzési tartományokat az alábbiak szerint osztotta meghatározott osztályokra:

* **A osztály (a 0.0.0.0/8 és a 127.0.0.0/8 között)** \- Az A osztályú blokkokat rendkívül nagy hálózatokhoz tervezték, amelyek több, mint 16 millió állomással rendelkeznek. Az A osztály egy rögzített /8 előtagot használt az első oktettel a hálózatcímet, a fennmaradó három oktettel pedig az állomáscímeket (hálózatonként több mint 16 millió állomáscímet) meghatározva.
* **B osztály (128.0.0.0 /16 - 191.255.0.0 /16)** - A B osztályú tartományt közép- és nagyvállalatok számára alkották meg, ahol nagyjából 65.000 állomás üzemel. A B osztály rögzített /16 előtagot használt az első két oktettel a hálózatcímet, a fennmaradó két oktettel pedig az állomáscímeket (hálózatonként több mint 65.000 állomáscímet) azonosítva.
* **C osztály (192.0.0.0 /24 - 223.255.255.0 /24)** \- Legfeljebb 254 állomást tartalmazó, kis hálózatok támogatására tervezték. A C osztály rögzített /24 előtagot használt az első három oktettel a hálózatot és a fennmaradó oktettel az állomáscímeket (hálózatonként csak 254 állomáscímet) meghatározva.

**MEGJEGYZÉS:** Van egy D osztályú csoportos címzési blokk is, amely a 224.0.0.0 és 239.0.0.0 közötti címeket foglalja magába, valamint egy E osztályú kísérleti címtartomány, amely a 240.0.0.0 - 255.0.0.0 közötti címeket foglalja magába.

Abban az időben, az internetet használó korlátozott számú számítógéppel, az osztály alapú címzés hatékony eszköz volt a címek kiosztására. Amint az ábrán is látható, az A és B osztályú hálózatoknak nagyon sok állomáscíme van, a C osztálynak pedig nagyon kevés. Az A osztályú hálózatok az IPv4-hálózatok 50%-át tették ki. Ennek következtében a rendelkezésre álló IPv4-címek többsége nem volt használatban.

The diagram is a pie chart showing the percentage of Class A, B, C, D, & E IPv4 addressing with the total number of networks and hosts per class A, B, and C networks. Percentages are: class A = 50%, class B = 25%, class C = 12.5%, and class D and E = 12.5%. For the total number of networks and total number of hosts per network: class A = 128 networks with 16,777,214 total hosts per network; class B = 16,384 networks with 65,534 total hosts per network; and class C = 2,097,152 networks with 254 total hosts per network.

Class D & E  
12.5%Class A  
50%Class C  
12.5%Class B  
25%Class ATotal Networks: 128  
Total Hosts/Net: 16 777214Class BTotal Networks: 16,384  
Total Hosts/Net: 65,534Class CTotal Networks: 2,097,152  
Total Hosts/Net: 254

Az 1990-es évek közepén, a World Wide Web (WWW) megjelenésével az osztály alapú címzés már nem volt képes hatékonyan kezelni a korlátozott IPv4-címtér kiosztását. Az osztály alapú címkiosztást az osztály nélküli címzés váltotta fel, amelyet ma is használunk. Az osztály nélküli címzés figyelmen kívül hagyja az (A, B, C) osztályokra vonatkozó szabályokat. A publikus IPv4 hálózatcímek (hálózatcímek és alhálózati maszkok) az indokolható címek száma alapján kerülnek kiosztásra.

11.3.6

## Az IP-címek szétosztása

A publikus IPv4-címek olyan címek, amelyek az interneren globális címzésr alkalmasak. A publikus IP-címek egyediek.

Az IPv4- és IPv6-címeket az Internet Assigned Numbers Authority (IANA) kezeli. Az IANA kezeli és osztja ki az IP-címek blokkjait a regionális regisztrációs szervezetek (Regional Internet Registries, RIR) számára. Az öt RIR az ábrán látható.

Az regionális internetregisztrátorok felelnek az IP-címek olyan internetszolgáltatók számára történő kiosztásáért, amelyek IPv4-címtartományokat biztosítanak a szervezetek és a kisebb internetszolgáltatók számára. A szervezetek a címüket közvetlenül egy RIR-től is megkaphatják (az adott RIR irányelveinek megfelelően).

This figure shows the geographic locations of the Reginal Internet Registries (RIR). The regions governed by each RIR are as follows: AfriNIC (African Network Information Center) – serving the Africa Region, APNIC (Asia Pacific Network Information Centre) – serving the Asia/Pacific Region, ARIN (American Registry for Internet Numbers) – serving the North America Region, LACNIC (Regional Latin-American and Caribbean IP Address Registy) – serving Latin America and some Caribbean Islands, and RIPE NCC (Reseaux IP Europeens Network Coordination Centre) – serving Europe, the Middle East, and Central Asia.

### Regional Internet Registries



* **AfriNIC** (African Network Information Centre) - Africa Region
* **APNIC** (Asia Pacific Network Information Centre) - Asia/Pacific Region
* **ARIN** (American Registry for Internet Numbers) - North America Region
* **LACNIC** (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands
* **RIPE NCC** (Réseaux IP Européens Network Coordination Centre) - Europe, the Middle East, and Central Asia

11.3.7

## Activity - Public or Private IPv4 Address

**Instructions:**

Click the drop down arrow for each address to choose the correct network type “Public” or “Private” for each address.

Choose the correct network type “Public” or “Private” for each address

172.16.35.2

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

192.168.3.5

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

192.0.3.15

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

64.104.0.22

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

209.165.201.30

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

192.168.11.5

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

172.16.30.30

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

10.55.3.168

[Public](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "public)

[Private](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "private)

11.3.8

## Check Your Understanding - Types of IPv4 Addresses

Az űrlap teteje

Check your understanding of the types of IPv4 addresses by choosing the BEST answer to the following questions.

1. Which two statements are correct about private IPv4 addresses? (Choose two.)

Az űrlap alja

Which two statements are correct about public IPv4 addresses? (Choose two.)

Which organization or group of organizations receives IP addresses from IANA and is responsible for allocating these addresses to ISPs and some organizations?

[11.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4 egyedi címzés, szórás és csoportos címzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatszegmentálás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                               
*           

1. IPv4-címzés
2. Hálózatszegmentálás

# Hálózatszegmentálás

11.4.1

## Szórási tartományok és szegmentálás

Ha kaptunk már valaha olyan e-mailt, amelyet a munkahelyünk vagy iskolánk mindegyik felhasználója megkapott, akkor az egy szórásos e-mail volt. Remélhetőleg olyan információt tartalmazott, amit mindenkinek tudnia kellett. De gyakran a szórás nem igazán releváns mindenki számára a levelezési listán. Néha csak a címzettek egy részének kell elolvasnia ezt az információt.

Egy Ethernet LAN esetében az eszközök szórások és a címfeloldási protokoll (Address Resolution Protocol, ARP) segítségével keresik meg a többi eszközt. Az ARP 2. rétegbeli szórásokat küld egy ismert IPv4-címre a helyi hálózaton, hogy kiderítse a hozzá rendelt MAC-címet. Az Ethernet LAN-okon lévő eszközök más eszközöket is felkutatnak a szolgáltatások segítségével. Az állomások általában a DHCP-protokoll segítségével kapják meg az IPv4-címkonfigurációt, amely szórási üzeneteket küld a DHCP-szerver megkereséséhez a helyi hálózaton keresztül.

A switch-ek a szórást valamennyi interfészükön továbbküldik, kivéve azon, amelyiken az beérkezett. Például, ha az ábrán látható valamelyik switch kapna egy szórásos üzenetet, akkor azt továbbítja a többi switch és a hálózatra csatlakozó többi felhasználó felé.

A router, R1, is connected to a switch via interface G0/0. The switch has connections to three other switches. The broadcast domain consists of the four switches and the router interface to which they are connected. A connection from the router to the Internet is not within the broadcast domain.

### A routerek szegmentálják a szórási tartományokat

R1

G0/0

InternetBroadcast Domain

A router nem továbbítja a szórásokat. Amikor egy router szórásos üzenetet kap, nem továbbítja azt más interfészekre. Ha például az R1 szórásos üzenetet kap a Gigabit Ethernet 0/0 interfészen, akkor azt nem továbbítja egy másik interfészre.

Ezért a router mindegyik interfésze egy szórási tartományhoz kapcsolódik, és a szórások csak az adott szórási tartományon belül terjednek.

11.4.2

## Problémák a nagyméretű szórási tartományokkal

A nagyméretű szórási tartomány egy olyan hálózat, amely sok állomást köt össze. A nagyméretű szórási tartomány egyik problémája az, hogy az állomások túlzott mértékű szórásos forgalmat generálhatnak, és így negatív hatással lehetnek a hálózatra. Az ábrán látható LAN 1 hálózat 400 felhasználót köt össze, ez pedig túlzott mértékű szórásos forgalmat generálhat. Ez lassú hálózati működést eredményez a jelentős forgalom miatt, valamint lassítja az eszköz működését is, mivel az eszköznek el kell fogadnia és fel kell dolgoznia minden egyes szórásos csomagot.

A router, R1, is connected to a switch via interface G0/0. The switch has connections to three other switches. The broadcast domain consists of the four switches and the router interface to which they are connected. This is identified as LAN1 with an address of 172.16.0.0/16. A connection from the router to the Internet is not within the broadcast domain.

### Egyetlen nagy szórási tartomány

R1 G0/0

LAN 1: 172.16.0.0/16

Internet(400 users)

A megoldás a hálózat méretének csökkentése, hogy kisebb szórási tartományokat hozzunk létre az alhálózatokra bontásnak nevezett folyamat segítségével. Ezeket a kisebb hálózati tereket alhálózatoknak nevezzük.

Az ábrán a 172.16.0.0 /16 hálózati címmel rendelkező LAN 1 hálózat 400 felhasználója két 200 felhasználós alhálózatra osztható: 172.16.0.0 /24 és 172.16.1.0 /24. A szórások csak a kisebb szórási tartományokat árasztják el, ezért egy LAN 1-ben keletkező szórás nem árasztja el a LAN 2-t.

A router, R1, is connected to two LANs which represent two different broadcast domains. Connected on the left via G0/0 is a switch supporting 200 users in LAN 1 with a network address of 172.16.0.0/24. Connected on the right via G0/1 is a switch supporting 200 users in LAN 2 with a network address of 172.16.1.0/24.

### Kommunikáció a hálózatok között

LAN 1: 172.16.0.0/24 LAN 2: 172.16.1.0/24 G0/1 R1

G0/0

Internet(200 users)(200 users)

Figyeljük meg, hogyan változott az előtag hossza egyetlen /16 előtagú hálózatról két /24 előtagú hálózatra. Ez az alhálózat-számítás alapja: az állomásbiteket használjuk fel további alhálózatok létrehozásához.

**MEGJEGYZÉS:** Az alhálózat és a hálózat kifejezéseket gyakran szinonimaként használjuk. A legtöbb hálózat valamely nagyobb címtartományú hálózat alhálózata.

11.4.3

## A hálózatok szegmentálásának okai

Az alhálózatokra bontás a teljes hálózat forgalmának csökkentésével növeli a hálózat teljesítményét. Azt is lehetővé teszi a rendszergazda számára, hogy olyan biztonsági házirendeket alkalmazzon, mint például, hogy mely alhálózatok kommunikálhatnak egymással, és melyek nem. A másik ok az, hogy csökkenti a helytelen konfigurációból, a hardver- és szoftverproblémákból, illetve az ártó szándékból adódó rendellenes szórási forgalom által érintett eszközök számát.

A hálózati eszközök kezeléséhez többféle módon lehet alhálózatokat használni.

Az alábbi gombokra kattintva megtudhatjuk, hogy a hálózati rendszergazdák miként szervezhetik az eszközöket és szolgáltatásokat alhálózatokba.

**Subnetting by Location**

The diagram shows a five floor building with a switch on each floor. Each switch is on a different LAN/subnet with a different network address, all connected to the same router, R1, via a different gigabit Ethernet interface. The following subnets are shown from the first to the fifth floor: LAN 1 has a network address of 10.0.1.0/24 and is connected to G0/0; LAN 2 has a network address of 10.0.2.0/24 and is connected to G0/1; LAN 3 has a network address of 10.0.3.0/24 and is connected to G0/2; LAN 4 has a network address of 10.0.4.0/24 and is connected to G0/3; and LAN 5 has a network address of 10.0.5.0/24 and is connected to G0/4. R1 also has a connection to the Internet.

R1 G0/0 G0/1 G0/2 G0/3

G0/4

**LAN 5: 10.0.5.0 /24** (Fifth floor)**LAN 4: 10.0.4.0 /24** (Fourth floor)**LAN 3: 10.0.3.0 /24** (Third floor)**LAN 2: 10.0.2.0 /24** (Second floor)**LAN 1: 10.0.1.0 /24** (First floor)Internet

A hálózati rendszergazdák alhálózatokat hozhatnak létre bármely, a hálózat szempontjából hasznos és értelmes felosztással. Figyeljük meg az egyes ábrákon, hogy az alhálózatok nagyobb előtag hosszt használnak a hálózatok azonosításához.

Az alhálózatokra bontás megértése alapvető készség, amelyet minden hálózati rendszergazdának el kell sajátítania. Különböző módszerek léteznek, amelyek segítenek megérteni ezt a folyamatot. Bár először túl bonyolultnak tűnhet, fordítsunk különös figyelmet a részletekre, és gyakorlással egyre könnyebbé válik az alhálózatokra bontás.

11.4.4

## Check Your Understanding - Network Segmentation

Az űrlap teteje

Check your understanding of the network segmentation by choosing the BEST answer to the following questions.

1. Which devices will not forward an IPv4 broadcast packet by default?

Az űrlap alja

Which two situations are the result of excessive broadcast traffic? (Choose two)

[11.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-címek típusai](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egy IPv4-es hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                  
*           

1. IPv4-címzés
2. Egy IPv4-es hálózat alhálózatokra bontása

# Egy IPv4-es hálózat alhálózatokra bontása

11.5.1

## Alhálózatokra bontás az oktethatárok mentén

Az előző témakörben számos jó okot megismerhettünk a hálózat szegmentálására. Azt is megtanultuk, hogy a hálózat szegmentálását alhálózatokra bontásnak nevezzük. Az alhálózatokra bontás az IPv4-hálózatok felügyeletéhez szükséges kulcsfontosságú képesség. Egy kicsit ijesztőnek tűnhet az elején, de némi gyakorlással sokkal könnyebb lesz.

Az IPv4-alhálózatok egy vagy több állomásbit hálózati bitként való felhasználásával keletkeznek. Ez az alhálózati maszk kiterjesztésével történik, kibővítve a cím hálózati részét az állomásazonosító részből kölcsönvett bitekkel. Minél több állomásbitet veszünk el, annál több alhálózat kialakítására van lehetőség. Minél több bitet veszünk el az alhálózatok számának növeléséhez, annál kevesebb lesz az alhálózatonkénti állomások száma.

A hálózatok legegyszerűbben a /8, /16 és /24 oktetthatárok mentén bonthatók alhálózatokra. Az alábbi táblázatban ezek az előtagok szerepelnek. Figyeljük meg, hogy a hosszabb előtaghossz használata csökkenti az állomások alhálózatonkénti számát.

### Alhálózati maszkok az oktethatárok mentén

| Prefix LengthSubnet MaskSubnet Mask in Binary (n = network, h = host)# of hosts/8255.0.0.0nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh 11111111.00000000.00000000.0000000016,777,214/16255.255.0.0nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh 11111111.11111111.00000000.0000000065,534/24255.255.255.0nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000254 | | | |
| --- | --- | --- | --- |
| **Prefix Length** | **Subnet Mask** | **Subnet Mask in Binary (n = network, h = host)** | **# of hosts** |
| **/8** | **255**.0.0.0 | **nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh  **11111111**.00000000.00000000.00000000 | 16,777,214 |
| **/16** | **255.255**.0.0 | **nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh  **11111111.11111111**.00000000.00000000 | 65,534 |
| **/24** | **255.255.255**.0 | **nnnnnnnn.nnnnnnnn**.nnnnnnnn.hhhhhhhh  **11111111.11111111.11111111**.00000000 | 254 |

Ha meg szeretnénk tudni, hogy az oktetthatár mentén történő alhálózatokra bontás miként lehet hasznos, vegyük a következő példát. Tegyük fel, hogy egy vállalat a 10.0.0.0/8 privát címet választotta a belső hálózat címének. Ez a hálózatcím 16.777.214 állomást tud összekötni egy szórási tartományban. Nyilvánvaló, hogy több mint 16 millió állomás egyetlen alhálózatban nem ideális.

A vállalat a 10.0.0.0/8 címet a /16 oktetthatár mentén további alhálózatokra tudja bontani, a táblázatban látható módon. Ez lehetővé tenné a vállalat számára, hogy legfeljebb 256 alhálózatot (azaz 10.0.0.0/16 - 10.255.0.0/16) definiáljon, amelyek alhálózatonként 65.534 állomás csatlakoztatását teszi lehetővé. Figyeljük meg, hogy az első két oktet miként azonosítja a cím hálózati részét, míg az utolsó két oktet az állomások IP-címeit.

### A 10.0.0.0/8 hálózat alhálózatokra bontása /16 előtag használatával

| Subnet Address (256 Possible Subnets)Host Range (65,534 possible hosts per subnet)Broadcast 10.0.0.0/1610.0.0.1 - 10.0.255.25 410.0.255.255 10.1.0.0/16 10.1.0.1 - 10.1.255.254 10.1.255.255 10.2.0.0/16 10.2.0.1 - 10.2.255.254 10.2.255.255 10.3.0.0/16 10.3.0.1 - 10.3.255.254 10.3.255.255 10.4.0.0/16 10.4.0.1 - 10.4.255.254 10.4.255.25510.5.0.0/16 10.5.0.1 - 10.5.255.254 10.5.255.255 10.6.0.0/16 10.6.0.1 - 10.6.255.254 10.6.255.255 10.7.0.0/16 10.7.0.1 - 10.7.255.254 10.7.255.255.........10.255.0.0/16 10.255.0.1 - 10.255.255.254 10.255.255.255 | | |
| --- | --- | --- |
| **Subnet Address  (256 Possible Subnets)** | **Host Range  (65,534 possible hosts per subnet)** | **Broadcast** |
| **10.0**.0.0**/16** | **10.0**.0.1 - **10.0**.255.254 | **10.0**.255.255 |
| **10.1.**0.0**/16** | **10.1**.0.1 - **10.1**.255.254 | **10.1**.255.255 |
| **10.2**.0.0**/16** | **10.2**.0.1 - **10.2**.255.254 | **10.2**.255.255 |
| **10.3**.0.0**/16** | **10.3**.0.1 - **10.3**.255.254 | **10.3**.255.255 |
| **10.4**.0.0**/16** | **10.4**.0.1 - **10.4**.255.254 | **10.4**.255.255 |
| **10.5**.0.0**/16** | **10.5**.0.1 - **10.5**.255.254 | **10.5**.255.255 |
| **10.6**.0.0**/16** | **10.6**.0.1 - **10.6**.255.254 | **10.6**.255.255 |
| **10.7**.0.0**/16** | **10.7**.0.1 - **10.7**.255.254 | **10.7**.255.255 |
| ... | ... | ... |
| **10.255**.0.0**/16** | **10.255**.0.1 - **10.255**.255.254 | **10.255**.255.255 |

Alternatív megoldásként a vállalat választhatja a 10.0.0.0/8 hálózat alhálózatokra bontását a /24 oktethatár mentén, a táblázatban látható módon. Ez lehetővé tenné a vállalat számára, hogy 65.536 alhálózatot határozzon meg, amelyek mindegyike 254 állomás csatlakoztatására képes. A /24 határ nagyon népszerű az alhálózatokra bontás során, mert kellő számú állomást biztosít, valamint kényelmesen végezhető az alhálózatokra bontás az oktetthatár mentén.

### A 10.0.0.0/8 hálózat alhálózatokra bontása /24 előtag használatával

| Subnet Address (65,536 Possible Subnets)Host Range (254 possible hosts per subnet)Broadcast10.0.0.0/2410.0.0.1 - 10.0.0.25410.0.0.25510.0.1.0/2410.0.1.1 - 10.0.1.25410.0.1.25510.0.2.0/2410.0.2.1 - 10.0.2.25410.0.2.255………10.0.255.0/2410.0.255.1 - 10.0.255.25410.0.255.25510.1.0.0/2410.1.0.1 - 10.1.0.25410.1.0.25510.1.1.0/2410.1.1.1 - 10.1.1.25410.1.1.25510.1.2.0/2410.1.2.1 - 10.1.2.25410.1.2.255………10.100.0.0/2410.100.0.1 - 10.100.0.25410.100.0.255.........10.255.255.0/2410.255.255.1 - 10.2255.255.25410.255.255.255 | | |
| --- | --- | --- |
| **Subnet Address  (65,536 Possible Subnets)** | **Host Range  (254 possible hosts per subnet)** | **Broadcast** |
| **10.0.0**.0**/24** | **10.0.0**.1 - **10.0.0**.254 | **10.0.0**.255 |
| **10.0.1**.0**/24** | **10.0.1**.1 - **10.0.1**.254 | **10.0.1**.255 |
| **10.0.2**.0**/24** | **10.0.2**.1 - **10.0.2**.254 | **10.0.2**.255 |
| … | … | … |
| **10.0.255**.0**/24** | **10.0.255**.1 - **10.0.255**.254 | **10.0.255**.255 |
| **10.1.0**.0**/24** | **10.1.0**.1 - **10.1.0**.254 | **10.1.0**.255 |
| **10.1.1**.0**/24** | **10.1.1**.1 - **10.1.1**.254 | **10.1.1**.255 |
| **10.1.2**.0**/24** | **10.1.2**.1 - **10.1.2**.254 | **10.1.2**.255 |
| … | … | … |
| **10.100.0**.0**/24** | **10.100.0**.1 - **10.100.0**.254 | **10.100.0**.255 |
| ... | ... | ... |
| **10.255.255**.0**/24** | **10.255.255**.1 - **10.2255.255**.254 | **10.255.255**.255 |

11.5.2

## Alhálózatokra bontás az oktetthatárokon belül

Az eddig bemutatott példák az állomásbiteket az elterjedt /8, /16 és /24 hálózati előtagokból vették kölcsön. Az alhálózatok azonban bármely állomásbit pozícióból vehetnek kölcsön biteket más maszkok létrehozásához.

Például, egy /24 előtagú hálózatcímet általában hosszabb előtag használatával bontunk alhálózatokra, a negyedik oktet bitjeinek kölcsönvételével. Ez további rugalmasságot biztosít a rendszergazdának, amikor kevesebb végberendezésnek kell címet kiosztani.

Tekintsük meg a táblázatban a /24 előtagú hálózat alhálózatokra bontásának hat módját.

### Egy /24 előtagú hálózat alhálózatokra bontása

| Prefix LengthSubnet MaskSubnet Mask in Binary (n = network, h = host)# of subnets# of hosts/25255.255.255.128nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.100000002126/26255.255.255.192nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000462/27255.255.255.224nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000830/28255.255.255.240nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.111100001614/29255.255.255.248nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000326/30255.255.255.252nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100642 | | | | |
| --- | --- | --- | --- | --- |
| **Prefix Length** | **Subnet Mask** | **Subnet Mask in Binary  (n = network, h = host)** | **# of subnets** | **# of hosts** |
| /25 | 255.255.255.128 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000 | **2** | 126 |
| /26 | 255.255.255.192 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000 | **4** | 62 |
| /27 | 255.255.255.224 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000 | **8** | 30 |
| /28 | 255.255.255.240 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000 | **16** | 14 |
| /29 | 255.255.255.248 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000 | **32** | 6 |
| /30 | 255.255.255.252 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00 | **64** | 2 |

A negyedik oktettből kölcsönvett minden egyes bittel a rendelkezésre álló alhálózatok száma megduplázódik, miközben az alhálózatonkénti állomáscímek száma csökken:

* **/25 sor** - 1 bit kölcsönvétele a negyedik oktettből 2 alhálózatot hoz létre, amelyek egyenként 126 állomást támogatnak.
* **/26 sor** - 2 bit kölcsönvétele 4 alhálózatot hoz létre, amelyek egyenként 62 állomást támogatnak.
* **/27 sor** - 3 bit kölcsönvétele 8 alhálózatot hoz létre, amelyek egyenként 30 állomást támogatnak.
* **/28 sor** - 4 bit kölcsönvétele 16 alhálózatot hoz létre, amelyek egyenként 14 állomást támogatnak.
* **/29 sor** - 5 bit kölcsönvétele 32 alhálózatot hoz létre, amelyek egyenként 6 állomást támogatnak.
* **/30 sor** - 6 bit kölcsönvétele 64 alhálózatot hoz létre, amelyek egyenként 2 állomást támogatnak.

11.5.3

## Videómagyarázat - Az alhálózati maszk

Az alhálózati maszk magyarázatának megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

11.5.4

## Videómagyarázat - Alhálózatokra bontás a bűvös számmal

A bűvös szám magyarázatának megtekintéséhez kattintsunk az ábrán látható lejátszás gombra!

11.5.5

## Packet Tracer - Egy IPv4-hálózat alhálózatokra bontása

A feladat során egyetlen hálózatcímből és hálózati maszkból kiindulva, a Customer hálózatot több alhálózatra kell bontanunk. Az alhálózati struktúrának az egyes alhálózatonként szükséges állomások számát, valamint egyéb hálózati megfontolásokat (pl.: a hálózati állomások jövőbeli bővítését) kell alapul venni.

Miután létrehoztunk egy alhálózati sémát, és kitöltöttük a táblázatot a hiányzó állomások és interfészek IP-címeivel, konfiguráljuk a PC-ket, switch-eket és router interfészeket.

A hálózati eszközök és a PC-k konfigurálása után a **ping** parancs segítségével ellenőrizzük a hálózati kapcsolatokat.

[Egy IPv4-hálózat alhálózatokra bontása](https://contenthub.netacad.com/courses/itn/_common/11.5.5-packet-tracer---subnet-an-ipv4-network_hu-HU.pka)

[11.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatszegmentálás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                      
*           

1. IPv4-címzés
2. Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása

# Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása

11.6.1

## Alhálózatok létrehozása /16 előtaggal

Az alhálózatokra bontás egyes esetekben könnyebb, máskor nehezebb. Ez a témakör bemutatja, hogy miként hozhatunk létre olyan alhálózatokat, amelyek mindegyike azonos számú állomást tartalmaz.

Nagyobb számú alhálózatot igénylő helyzetekben olyan IPv4-hálózatra van szükség, amelyben több állomásbit kölcsönvételére van lehetőség. Például, a 172.16.0.0 hálózat címének alapértelmezett maszkja a 255.255.0.0 vagy /16. Az ebbe a tartományba eső címeknek 16 bites hálózati és 16 bites állomásazonosító része van. A 16 bites állomásazonosító rész áll rendelkezésre, hogy az alhálózatok kialakításához szükséges biteket elvegyük. A táblázat kiemeli a /16 előtagú hálózat alhálózatokra bontásának összes lehetséges forgatókönyvét.

### Egy /16 előtagú hálózat alhálózatokra bontása

| Prefix LengthSubnet MaskNetwork Address (n = network, h = host)# of subnets# of hosts/17255.255.128.0nnnnnnnn.nnnnnnnn.nhhhhhhh.hhhhhhhh 11111111.11111111.10000000.00000000232766/18255.255.192.0nnnnnnnn.nnnnnnnn.nnhhhhhh.hhhhhhhh 11111111.11111111.11000000.00000000416382/19255.255.224.0nnnnnnnn.nnnnnnnn.nnnhhhhh.hhhhhhhh 11111111.11111111.11100000.0000000088190/20255.255.240.0nnnnnnnn.nnnnnnnn.nnnnhhhh.hhhhhhhh 11111111.11111111.11110000.00000000164094/21255.255.248.0nnnnnnnn.nnnnnnnn.nnnnnhhh.hhhhhhhh 11111111.11111111.11111000.00000000322046/22255.255.252.0nnnnnnnn.nnnnnnnn.nnnnnnhh.hhhhhhhh 11111111.11111111.11111100.00000000641022/23255.255.254.0nnnnnnnn.nnnnnnnn.nnnnnnnh.hhhhhhhh 11111111.11111111.11111110.00000000128510/24255.255.255.0nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh 11111111.11111111.11111111.00000000256254/25255.255.255.128nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.10000000512126/26255.255.255.192nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000102462/27255.255.255.224nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000204830/28255.255.255.240nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.11110000409614/29255.255.255.248nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.1111100081926/30255.255.255.252nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100163842 | | | | |
| --- | --- | --- | --- | --- |
| **Prefix Length** | **Subnet Mask** | **Network Address  (n = network, h = host)** | **# of subnets** | **# of hosts** |
| /17 | 255.255.128.0 | nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh  11111111.11111111.**1**0000000.00000000 | **2** | 32766 |
| /18 | 255.255.192.0 | nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh  11111111.11111111.**11**000000.00000000 | **4** | 16382 |
| /19 | 255.255.224.0 | nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh  11111111.11111111.**111**00000.00000000 | **8** | 8190 |
| /20 | 255.255.240.0 | nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh  11111111.11111111.**1111**0000.00000000 | **16** | 4094 |
| /21 | 255.255.248.0 | nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh  11111111.11111111.**11111**000.00000000 | **32** | 2046 |
| /22 | 255.255.252.0 | nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh  11111111.11111111.**111111**00.00000000 | **64** | 1022 |
| /23 | 255.255.254.0 | nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh  11111111.11111111.**1111111**0.00000000 | **128** | 510 |
| /24 | 255.255.255.0 | nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh  11111111.11111111.**11111111**.00000000 | **256** | 254 |
| /25 | 255.255.255.128 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh  11111111.11111111.**11111111.1**0000000 | **512** | 126 |
| /26 | 255.255.255.192 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh  11111111.11111111.**11111111.11**000000 | **1024** | 62 |
| /27 | 255.255.255.224 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh  11111111.11111111.**11111111.111**00000 | **2048** | 30 |
| /28 | 255.255.255.240 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh  11111111.11111111.**11111111.1111**0000 | **4096** | 14 |
| /29 | 255.255.255.248 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh  11111111.11111111.**11111111.11111**000 | **8192** | 6 |
| /30 | 255.255.255.252 | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh  11111111.11111111.**11111111.111111**00 | **16384** | 2 |

Bár nem kell memorizálnunk a fenti táblázatot, ettől függetlenül értenünk kell, hogy a táblázat egyes értékei hogyan állnak elő. Ne hagyjuk, hogy a táblázat mérete megijesszen minket! A nagy méret oka, hogy 8 további bit kölcsönvehető, ezért az alhálózatok és az állomások száma egyszerűen nagyobb.

11.6.2

## 100 alhálózat létrehozása /16 előtaggal

Vegyünk egy nagyvállalatot, amely legalább 100 alhálózatot igényel, és a 172.16.0.0/16 privát címet választotta a belső hálózat címének.

Amikor biteket veszünk el egy /16 előtagú címből, kezdjük a harmadik oktettben, balról jobbra haladva. Egyszerre csak egy bitet vegyünk el, amíg el nem érjük a 100 alhálózat létrehozásához szükséges bitek számát.

Az ábra azon alhálózatok számát jeleníti meg, amelyek a harmadik és negyedik oktett bitjeinek kölcsönvételével hozhatók létre. Figyeljük meg, hogy most már akár 14 állomásbitet is kölcsön lehet venni.

The graphic shows how to compute the number of subnets created when borrowing bits from the third and fourth octets of an IPv4 network address. The formula to determine the number of subnets created is 2 to the power of the number of bits borrowed. The graphic shows an address of 172.16.0.0. Underneath, are the letters nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh. It starts by borrowing the first h bit in the third octet which results in 2 to the power of 1 = 2 subnets. When the first two h bits in the third octet are borrowed, the formula is 2 to the power of 2 = 4. This continues until the first 14 h bits are borrowed from the third and fourth octets resulting in 2 to the power of 14 = 16384. The last two h bits in the fourth octet remain the same.

### Létrehozott alhálózatok száma

n n n n n n n n . n n n n n n n n . h h h h h h h h . h h h h h h h h 172 . 0 16 . 0

.

Borrowing **1** bit:2^**1** = **2**Borrowing **2** bit:2^**2** = **4**Borrowing **3** bit:2^**3** = **8**Borrowing **4** bit:2^**4** = **16**Borrowing **5** bit:2^**5** = **32**Borrowing **6** bit:2^**6** = **64**Borrowing **7** bit:2^**7** = **128**Borrowing **8** bit:2^**8** = **256**Borrowing **9** bit:2^**9** = **512**Borrowing **10** bit:2^**10** = **1024**Borrowing **11** bit:2^**11** = **2048**Borrowing **12** bit:2^**12** = **4096**Borrowing **13** bit:2^**13** = **8192**Borrowing **14** bit:2^**14** = **16384**

A vállalat 100 alhálózatával szemben támasztott követelmények teljesítéséhez 7 bitet (azaz 27 = 128 alhálózatot) kell kölcsönvenni (összesen 128 alhálózathoz), az ábrán látható módon.

The graphic shows the decimal and bit representation of a network address, and below it a subnet mask, when seven bits are borrowed in the third octet to create subnets. The first two octets are shown in decimal and the last two octets are shown in binary. The network address is 172.16.0000 0000.0000 0000. The subnet mask is 255.255.1111 1110.0000 0000.

### A 172.16.0.0/23 hálózat

172. 16. 0000 000 0. 0000 0000

255. 255. 1111 111 0. 0000 0000

Ne feledjük, hogy a kölcsönvett biteknek megfelelően az alhálózati maszk is változik! A példánkban 7 bitet vettünk kölcsön, így a maszk a harmadik oktettben 7 bittel bővült. A harmadik oktet binárisan 11111110, a negyedik oktet pedig 00000000, ezért a maszk decimális formában 255.255.254.0, vagy előtaggal felírva /23.

Az ábrán az eredményül kapott, 172.16.0.0 /23 és 172.16.254.0 /23 közötti alhálózatok jelennek meg.

The graphic shows the subnets created when using a /23 subnet mask with the address 172.16.0.0. First, it shows the decimal and bit representation of the network address, and below it the subnet mask. The first two octets are shown in decimal and the last two octets are shown in binary. The network address is 172.16.0000 0000.0000 0000. The subnet mask is 255.255.1111 1110.0000 0000. The first two octets and the first seven bits in the third octet are shaded gray and the last bit in the third octet and the entire fourth octet are shaded purple. Below, the text reads: borrowing 7 bits creates 128 subnets. Below that, it shows the first three subnets and the last subnet created. Again, the first two octets are shown in decimal and the last two octets are shown in binary. The first subnet is 172.16.0000 0000.0000 0000 or 172.16.0.0/23. The second subnet is 172.16.0000 0010.0000 0000 or 172.16.2.0/23. The third subnet is 172.16.0000 0100.0000 0000 or 172.16.4.0/23. The text ..to.. is used to show that this process continues until you reach the last subnet created which is 172.16.1111 1110.0000 0000 or 172.16.254.0/23.

### Az eredményül kapott /23 előtagú alhálózatok

172.16.0.0/23 172.16.2.0/23 172.16.4.0/23 1 7 2 . 1 6 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 2 5 5 . 2 5 5 . 1 1 1 1 1 1 1 0 . 0 0 0 0 0 0 0 0 172.16.254.0/23 1 7 2 . 1 6 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 7 2 . 1 6 . 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 1 7 2 . 1 6 . 0 0 0 0 0 1 0 0 . 0 0 0 0 0 0 0 0 1 7 2 . 1 6 . 1 1 1 1 1 1 1 0 . 0 0 0 0 0 0 0

0

Borrowing 7 bits creates 128 subnets. . to . .

Az alhálózatok számára 7 bit kölcsönvételét követően 1 állomásbit marad a harmadik, és 8 állomásbit marad a negyedik oktettben. A 29 eredménye 512 teljes állomáscím. Az első cím a hálózatcím számára, az utolsó cím pedig a szórási cím számára van fenntartva, így a két cím (29 - 2) kivonása után 510 elérhető állomáscím marad minden /23 előtagú alhálózathoz.

Ahogy az ábrán is látható, az első alhálózat első állomáscíme a 172.16.0.1, az utolsó pedig a 172.16.1.254.

The graphic shows the address range for the 172.16.0.0/23 subnet. The first two octets are shown in decimal and the last two octets are shown in binary, then the address is shown in its dotted decimal format. The network address is 172.16.0000 0000.0000 0000 = 172.16.0.0/23. The first host address is 172.16.0000 0000.0000 0001 = 172.16.0.1/23. The last host address is 172.16.0000 0001.1111 1110 = 172.16.255.254/23 (change to 172.16.1.254 when fixed). The broadcast address is 172.16.0000 0001.1111 1111 = 172.16.255.255/23 (change to 172.16.1.255 when fixed).

### A 172.16.0.0/23 alhálózat címtartománya

1 7 2 . 1 6 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 7 2 . 1 6 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 1 1 7 2 . 1 6 . 0 0 0 0 0 0 0 1 . 1 1 1 1 1 1 1 0 1 7 2 . 1 6 . 0 0 0 0 0 0 0 1 . 1 1 1 1 1 1 1 1 = 172.16.0.0/23 = 172.16.0.1/23 = 172.16.1.254/23

= 172.16.1.255/23

Network AddressFirst Host AddressLast Host AddressBroadcast Address

11.6.3

## 1000 alhálózat létrehozása /8 előtaggal

Egyes szervezeteknek, például a kisebb szolgáltatóknak vagy a nagyvállalatoknak még több alhálózatra lehet szükségük. Vegyünk például egy kisebb internetszolgáltatót, amelynek 1000 alhálózatra van szüksége az ügyfelei számára. Minden ügyfélnek sok helyre lesz szüksége az állomásazonosító részben ahhoz, hogy saját alhálózatokat hozzon létre.

Az internetszolgáltató a 10.0.0.0 255.0.0.0 vagy 10.0.0.0/8 hálózatcímmel rendelkezik. Ez azt jelenti, hogy 8 bitjük van a hálózati részben és 24 állomásbit áll rendelkezésre a további alhálózati bitek kölcsönvételére. Ezért a kisebb internetszolgáltató alhálózatotokra bontja a 10.0.0.0/8 hálózatot.

Mint mindig, az alhálózatok létrehozásának érdekében most is biteket kell kölcsönvennünk a meglévő hálózathoz rendelt IPv4-cím állomásazonosító részéből. Balról jobbra haladva az első használható állomásbittel kezdve egyesével fogjuk a biteket kölcsönvenni, míg el nem érjük a kívánt 1000 alhálózatot biztosító bitszámot. Amint az ábrán is látható, 10 bitet kell kölcsönvennünk 1024 alhálózat létrehozásához (210 = 1024). Ez magában foglalja a második oktett 8 bitjét és 2 további bitet a harmadik oktettből.

The graphic shows how to compute the number of subnets created when borrowing bits from the second and third octets of an IPv4 network address. The formula to determine the number of subnets created is 2 to the power of the number of bits borrowed. The graphic shows an address of 10.0.0.0. Underneath, are the letters nnnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh. It starts by borrowing the first h bit in the second octet which results in 2 to the power of 1 = 2 subnets. When the first two h bits in the second octet are borrowed, the formula is 2 to the power of 2 = 4. This continues until the first 10 h bits are borrowed from the second and third octets resulting in 2 to the power of 10 = 1024.

### Létrehozott alhálózatok száma

n n n n n n n n . h h h h h h h h . h h h h h h h h . h h h h h h h h 10 . 0 0 . 0 . 2^1 = 2 2^2 = 4 2^3 = 8 2^4 = 16 2^5 = 32 2^6 = 64 2^7 = 128 2^8 = 256 2^9 = 512

2^10 = 1024

Borrowing **1** bit:Borrowing **2** bit:Borrowing **3** bit:Borrowing **4** bit:Borrowing **5** bit:Borrowing **6** bit:Borrowing **7** bit:Borrowing **8** bit:Borrowing **9** bit:Borrowing **10** bit:

Az alábbi ábra megjeleníti a hálózatcímet és az eredményül kapott alhálózati maszkot, amely a 255.255.192.0 vagy 10.0.0.0/18 értékre konvertálható.

The graphic shows the decimal and bit representation of a network address, and below it a subnet mask, when 10 bits are borrowed in the second and third octets to create subnets. The first octet is shown in decimal and the last three octets are shown in binary. The network address is 10.1111 1111.1100 0000.0000 0000 (should be 10.0000 0000.0000 0000.0000 0000 when fixed). The subnet mask is 255.255.1111 1110.0000 0000.

### A 10.0.0.0/18 hálózat

1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 2 5 5 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0

0

Az alábbi ábra a 10 bit kölcsönvételéből származó, a 10.0.0.0/18 és 10.255.128.0/18 közötti alhálózatokat jeleníti meg.

The graphic shows the subnets created when using a /18 subnet mask with the address 10.0.0.0. First, it shows the decimal and bit representation of the network address, and below it the subnet mask. The first octet is shown in decimal and the last three octets are shown in binary. The network address is 10.0000 0000.0000 0000.0000 0000. The subnet mask is 255.1111 1111.1100 0000.0000 0000. The first octet and the next 10 bits are shaded gray and the remaining bits are shaded purple. Below, the text reads: borrowing 10 bits creates 1024 subnets. Below that, it shows the first five subnets and the last subnet created. Again, the first octet is shown in decimal and the last three octets are shown in binary. The first subnet is 10.0000 0000.0000 0000.0000 0000 or 10.0.0.0/18. The second subnet is 10.0000 0000.0100 0000.0000 0000 or 10.0.64.0/18. The third subnet is 10.0000 0000.1000 0000.0000 0000 or 10.0.128.0/18. The fourth subnet is 10.0000 0000.1100 0000.0000 0000 or 10.0.192.0/18. The fifth subnet is 10.0000 0001.0000 0000.0000 0000 or 10.1.0.0/18. The text ..to.. is used to show that this process continues until you reach the last subnet created which is 10.1111 1111.1100 0000.0000 0000 or 10.255.192.0/18.

### Az eredményül kapott /18 előtagú alhálózatok

10.0.0.0/18 10.0.64.0/18 10.0.128.0/18 2 5 5 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 0 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 10.0.192.0/18 10.1.0.0/18 1 0 . 0 0 0 0 0 0 0 0 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 1 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0

10.255.192.0/18

Borrowing 10 bits creates 1024 subnets . . to . .

Az alhálózatok létrehozásához kölcsönvett 10 bit 14 állomásbitet hagy meg minden alhálózat számára. Alhálózatonként a két állomást (a hálózatcímet és a szórási címet) levonva 214 - 2 = 16.382 állomást kapunk alhálózatonként. Ez azt jelenti, hogy az 1000 alhálózat mindegyike maximum 16.382 állomást támogat.

Az alábbi ábra az első alhálózat sajátosságait jeleníti meg.

The graphic shows the address range for the 10.0.0.0/18 subnet. The first octet is shown in decimal and the last three octets are shown in binary, then the address is shown in its dotted decimal format. The network address is 10.0000 0000.0000 0000.0000 0000 = 10.0.0.0/18. The first host address is 10.0000 0000.0000 0000.0000 0001 = 10.0.0.1/18. The last host address is 10.0000 0000.0011 1111.1111 1110 = 10.0.63.254/18. The broadcast address is 10.0000 0000.0011 1111. 1111 1111 = 10.0.63.255/18.

### A 10.0.0.0/18 alhálózat címtartománya

1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 1 1 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0 1 0 . 0 0 0 0 0 0 0 0 . 0 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 1 0 . 0 0 0 0 0 0 0 0 . 0 0 1 1 1 1 1 1 . 1 1 1 1 1 1 1 0 = 10.0.0.0/18 = 10.0.0.1/18 = 10.0.63.254/18

= 10.0.63.255/18

Network AddressFirst Host AddressLast Host AddressBroadcast Address

11.6.4

## Videómagyarázat - Oktethatárokon átívelő alhálózatok

A bűvös szám oktethatárokon átívelő használatának megtekintéséhez kattintsunk az ábrán látható lejátszás gombra!

11.6.5

## Feladat – Alhálózati maszk kiszámítása

Instructions:

In this activity, you are given a subnet mask in decimal format. Enter the binary representation of the subnet mask in the octet fields provided. Additionally, convert the mask to prefix notation format in the Prefix Notation field.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet Mask | 255 | 255 | 255 | 254 |
| Subnet Mask in binary |  |  |  |  |
| Prefix notation | **/** |  | |  |

11.6.6

## Laborgyakorlat – IPv4 alhálózatok számítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: IPv4 alhálózati címek meghatározása
* Bölüm 2: IPv4 alhálózati címek számítása

[11.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egy IPv4-es hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alhálózatok kialakítása a követelményeknek megfelelően](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                         
*           

1. IPv4-címzés
2. Alhálózatok kialakítása a követelményeknek megfelelően

# Alhálózatok kialakítása a követelményeknek megfelelően

11.7.1

## A privát és publikus IPv4-címtartomány alhálózatokra bontása közötti különbségek

Bár jó, ha gyorsan alhálózatokra szegmentálhatunk egy hálózatot, egy vállalati hálózat publikus és privát IPv4-címeket egyaránt használhat. Ez befolyásolja, hogy miként bontsuk a hálózatunkat alhálózatokra.

Az ábrán egy tipikus vállalati hálózat látható:

* **Intranet -** Ez a vállalat hálózatának belső része, amely csak a szervezeten belül érhető el. Az intranetes eszközök privát IPv4-címeket használnak.
* **DMZ -** Ez a vállalati hálózat azon része, amely az internet felől is elérhető erőforrásokat (pl.: webkiszolgálót) tartalmaz. A DMZ-ben lévő eszközök publikus IPv4-címeket használnak.

The diagram is a network topology showing a router in the center with three connections; one to the company Intranet, one to a DMZ, and one to the Internet. On the left is the Intranet with devices using private IPv4 addresses. At the top, is the DMZ with two servers using public IPv4 addresses. The router is labeled router to the Internet and has a connection to the Internet cloud.

### Publikus és privát IPv4-címtér

InternetRouter to the InternetPrivate IPv4 AddressesintranetPublic IPv4 AddressesDMZ

Mind az intranet, mind a DMZ saját alhálózati követelményekkel és kihívásokkal rendelkezik.

Az intranet privát IPv4 címtartományt használ. Ez lehetővé teszi a szervezet számára, hogy a privát IPv4 hálózatcímek bármelyikét használja, beleértve a 10.0.0.0/8 előtagot 24 állomásbittel és több mint 16 millió állomással. A 24 állomásbittel rendelkező hálózatcím használata könnyebbé és rugalmasabbá teszi az alhálózatokra bontást. Ebbe beletartozik az oktetthatár mentén történő alhálózatokra bontás a /16 vagy /24 előtag használatával.

Például a 10.0.0.0/8 privát IPv4 hálózatcím alhálózatokra bontható egy /16 maszk használatával. A táblázat szerint ez 256 alhálózatot eredményez, alhálózatonként 65.534 állomással. Ha egy szervezetnek kevesebb mint 200 olyan alhálózatra van szüksége, ami némi növekedést is lehetővé tesz, akkor ez több mint elegendő állomáscímet biztosít alhálózatonként.

### A 10.0.0.0/8 hálózat alhálózatokra bontása a /16 előtag használatával

| Subnet Address (256 Possible Subnets)Host Range (65,534 possible hosts per subnet)Broadcast10.0.0.0/1610.0.0.1 - 10.0.255.25410.0.255.25510.1.0.0/1610.1.0.1 - 10.1.255.25410.1.255.25510.2.0.0/1610.2.0.1 - 10.2.255.25410.2.255.25510.3.0.0/1610.3.0.1 - 10.3.255.25410.3.255.25510.4.0.0/1610.4.0.1 - 10.4.255.25410.4.255.25510.5.0.0/1610.5.0.1 - 10.5.255.25410.5.255.25510.6.0.0/1610.6.0.1 - 10.6.255.25410.6.255.25510.7.0.0/1610.7.0.1 - 10.7.255.25410.7.255.255.........10.255.0.0/1610.255.0.1 - 10.255.255.25410.255.255.255 | | |
| --- | --- | --- |
| **Subnet Address  (256 Possible Subnets)** | **Host Range  (65,534 possible hosts per subnet)** | **Broadcast** |
| **10.0**.0.0**/16** | **10.0**.0.1 - **10.0**.255.254 | **10.0**.255.255 |
| **10.1**.0.0**/16** | **10.1**.0.1 - **10.1**.255.254 | **10.1**.255.255 |
| **10.2**.0.0/16 | **10.2**.0.1 - **10.2**.255.254 | **10.2**.255.255 |
| **10.3**.0.0**/16** | **10.3**.0.1 - **10.3**.255.254 | **10.3**.255.255 |
| **10.4**.0.0**/16** | **10.4**.0.1 - **10.4**.255.254 | **10.4**.255.255 |
| **10.5**.0.0**/16** | **10.5**.0.1 - **10.5**.255.254 | **10.5**.255.255 |
| **10.6**.0.0**/16** | **10.6**.0.1 - **10.6.**255.254 | **10.6**.255.255 |
| **10.7**.0.0**/16** | **10.7**.0.1 - **10.7**.255.254 | **10.7**.255.255 |
| ... | ... | ... |
| **10.255**.0.0**/16** | **10.255**.0.1 - **10.255**.255.254 | **10.255**.255.255 |

Egy másik lehetőség a 10.0.0.0/8 privát IPv4 hálózatcím alhálózatokra bontása a /24 maszk használatával. Amint az a táblázatban látható, ez 65.536 alhálózatot eredményez, 254 állomást biztosítva alhálózatonként. Ha egy szervezetnek több mint 256 alhálózatra van szüksége, akkor a /24 előtag használatával alhálózatonként 254 állomás biztosítható.

### A 10.0.0.0/8 hálózat alhálózatokra bontása a /24 előtag használatával

| Subnet Address (65,536 Possible Subnets)Host Range(254 possible hosts per subnet)Broadcast10.0.0.0/2410.0.0.1 - 10.0.0.25410.0.0.25510.0.1.0/2410.0.1.1 - 10.0.1.25410.0.1.25510.0.2.0/2410.0.2.1 - 10.0.2.25410.0.2.255………10.0.255.0/2410.0.255.1 - 10.0.255.25410.0.255.25510.1.0.0/2410.1.0.1 - 10.1.0.25410.1.0.25510.1.1.0/2410.1.1.1 - 10.1.1.25410.1.1.25510.1.2.0/2410.1.2.1 - 10.1.2.25410.1.2.255………10.100.0.0/2410.100.0.1 - 10.100.0.25410.100.0.255.........10.255.255.0/2410.255.255.1 - 10.2255.255.25410.255.255.255 | | |
| --- | --- | --- |
| **Subnet Address  (65,536 Possible Subnets)** | **Host Range  (254 possible hosts per subnet)** | **Broadcast** |
| **10.0.0**.0**/24** | **10.0.0**.1 - **10.0.0**.254 | **10.0.0**.255 |
| **10.0.1**.0**/24** | **10.0.1**.1 - **10.0.1**.254 | **10.0.1**.255 |
| **10.0.2**.0**/24** | **10.0.2**.1 - **10.0.2**.254 | **10.0.2**.255 |
| … | … | … |
| **10.0.255**.0**/24** | **10.0.255**.1 - **10.0.255**.254 | **10.0.255**.255 |
| **10.1.0**.0**/24** | **10.1.0**.1 - **10.1.0**.254 | **10.1.0**.255 |
| **10.1.1**.0**/24** | **10.1.1**.1 - **10.1.1**.254 | **10.1.1**.255 |
| **10.1.2**.0**/24** | **10.1.2**.1 - **10.1.2**.254 | **10.1.2**.255 |
| … | … | … |
| **10.100.0**.0**/24** | **10.100.0**.1 - **10.100.0**.254 | **10.100.0**.255 |
| ... | ... | ... |
| **10.255.255**.0**/24** | **10.255.255**.1 - **10.2255.255**.254 | **10.255.255**.255 |

A 10.0.0.0/8 hálózat bármely más (pl.: a /12, /18, /20) előtaggal is alhálózatokra bontható, amely sokféle lehetőséget biztosít a hálózati rendszergazdának. A 10.0.0.0/8 privát IPv4 hálózatcím használata megkönnyíti az alhálózatok tervezését és megvalósítását.

**Mi a helyzet a DMZ-vel?**

Mivel ezeknek az eszközöknek nyilvánosan hozzáférhetőnek kell lenniük az internetről, a DMZ eszközeihez publikus IPv4-címek szükségesek. A publikus IPv4-címtartomány kimerülése az 1990-es évek közepén vált problémává. 2011 óta az IANA és az öt RIR közül négy esetében elfogyott a rendelkezésre álló IPv4-címtartomány. Bár a szervezetek folyamatosan térnek át az IPv6-ra, a fennmaradó IPv4-címtartomány továbbra is erősen korlátozott. Ez azt jelenti, hogy a szervezetnek maximálisan ki kell használniuk a saját, korlátozott számú publikus IPv4-címeiket. Ehhez a hálózati rendszergazdának különböző maszkokkal rendelkező alhálózatokra kell bontania a publikus címtartományt annak érdekében, hogy minimálisra csökkentse a fel nem használt állomáscímek alhálózatonkénti számát. Ez az úgynevezett változó hosszúságú alhálózati maszk (Variable Length Subnet Masking, VLSM) használata.

11.7.2

## A fel nem használt IPv4-állomáscímek minimalizálása és az alhálózatok maximalizálása

Az alhálózatok tervezésekor két szempontot kell megfontolnunk: az egyes hálózatokban szükséges állomásszámot és az igényelt független alhálózatok számát.

A táblázat a /24 előtagú hálózat alhálózatokra bontásának sajátosságait jeleníti meg. Vegyük észre, hogy az alhálózatok száma és az állomások száma fordított arányban áll egymással! Minél több bitet veszünk kölcsön az alhálózatok számára, annál kevesebb állomásbit marad, ezért csökken az egyes alhálózatokban az állomások száma is. Ha több állomáscímre van szükségünk, akkor több állomásbit kell, így kevesebb alhálózat kialakítására van lehetőség.

A legnagyobb alhálózat állomásainak száma határozza meg, hogy hány bitnek kell maradnia az állomásazonosító részben. Ne feledjük, hogy ezen címekből 2 nem osztható ki, így a használható címek száma 2n-2!

### Egy /24 előtagú hálózat alhálózatokra bontása

| Prefix Length Subnet Mask Subnet Mask in Binary (n = network, h = host)# of subnets# of hosts per subnet/25255.255.255.128nnnnnnnn.nnnnnnnn.nnnnnnnn.nhhhhhhh 11111111.11111111.11111111.100000002126/26255.255.255.192nnnnnnnn.nnnnnnnn.nnnnnnnn.nnhhhhhh 11111111.11111111.11111111.11000000462/27255.255.255.224nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnhhhhh 11111111.11111111.11111111.11100000830/28255.255.255.240nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnhhhh 11111111.11111111.11111111.111100001614/29255.255.255.248nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnhhh 11111111.11111111.11111111.11111000326/30255.255.255.252nnnnnnnn.nnnnnnnn.nnnnnnnn.nnnnnnhh 11111111.11111111.11111111.11111100642 | | | | |
| --- | --- | --- | --- | --- |
| **Prefix Length** | **Subnet Mask** | **Subnet Mask in Binary  (n = network, h = host)** | **# of subnets** | **# of hosts per subnet** |
| /25 | 255.255.255.128 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000 | **2** | 126 |
| /26 | 255.255.255.192 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000 | **4** | 62 |
| /27 | 255.255.255.224 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000 | **8** | 30 |
| /28 | 255.255.255.240 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000 | **16** | 14 |
| /29 | 255.255.255.248 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000 | **32** | 6 |
| /30 | 255.255.255.252 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00 | **64** | 2 |

A hálózati rendszergazdának kell alkalmas belső címzési struktúrát kialakítania annak érdekében, hogy a hálózatok biztosítani tudják a maximális állomásszámot. A címzési struktúrának lehetővé kell tennie mind az alhálózatonkénti állomáscímek számának, mind az alhálózatok teljes számának növekedését.

11.7.3

## Példa: Hatékony alhálózatokra bontás IPv4 esetében

Ebben a példában a vállalati központ internetszolgáltatója a 172.16.0.0/22 (10 állomásbit) publikus hálózatcímet osztotta ki. Amint az ábrán is látható, ez 1022 állomáscímet biztosít.

**MEGJEGYZÉS:** A 172.16.0.0/22 hálózat az IPv4 privát címtartományának része. Ezt a címet használjuk egy ténylegesen publikus IPv4-cím helyett.

The graphic shows the number of hosts provided when using a 172.16.0.0/22 network. The network portion of the address in binary is: 10101100.00010100.000000. The host portion in binary is: 00.00000000. The host portion consists of 10 host bits therefore 2 to the power of 10 - 2 = 1,022 hosts.

### Hálózatcím

172.16.0.0/22 10101100.00010000.000000

00. 00000000

10 host bits  
2^10 - 2 = 1,022 hostsNetwork portionHost portion

A vállalati központnak van egy DMZ-je és négy fiókirodája, amelyek mindegyikének saját, publikus IPv4-címtartományra van szüksége. A vállalati központnak a lehető legjobban ki kell használnia a korlátozott IPv4-címtartományt.

Az ábrán látható topológia öt telephelyből, egy vállalati irodából és négy fióktelepből áll. Minden telephely internetkapcsolatot igényel, ezért összesen öt internetkapcsolatra van szükség. Ez azt jelenti, hogy a szervezet 10 alhálózatot igényel a vállalat 172.16.0.0/22 publikus címéből. A legnagyobb alhálózat 40 állomást tartalmaz.

The diagram is a corporate network topology with five sites. In the middle is the ISP cloud. Connected to the cloud are five sites, each shown with a router, several servers, and the public IPv4 addressing requirements. The sites are: Corporate headquarters with 40 addresses; Branch 1 with 25 addresses; Branch 2 with 30 addresses; Branch 3 with 10 addresses; and Branch 4 with 15 addresses.

### Vállalati topológia öt telephellyel

Corporate Headquarters40 public IPv4 addressesBranch 125 public IPv4 addresses30 public IPv4 addresses10 public IPv4 addresses15 public IPv4 addressesBranch 2ISPPublic IPv4 addressesBranch 3Branch 4

Ahogy az ábrán is látható, a 172.16.0.0/22 hálózatcím 10 állomásbitet tartalmaz. Mivel a legnagyobb alhálózat 40 állomást igényel, a 40 állomás címzéséhez legalább 6 bitre van szükség. Ezt a 26 - 2 = 62 összefüggéssel határozhatjuk meg.

The diagram shows the subnet scheme for the given address 172.16.0.0/22 with 4 bits borrowed from the host portion to create subnets. All four octets are shown in binary followed by the dotted decimal format for the given network address and for several subnets created. The given network address in binary is 10101100.00010000.000000 (network portion highlighted in gray) 00.00000000 (host portion highlighted in purple) = 172.16.0.0/22. For the subnets listed below, the first 22 bits are highlighted in gray (network portion), the next 4 bits are shaded in blue, and the last 6 bits are the remaining host portion shaded in purple. Subnet 0 is 10101100.00010000.00000000.00000000 = 172.16.0.0/26. Subnet 1 is 10101100.00010000.0000000.01000000 = 172.16.0.64/26. Subnet 2 is 10101100.00010000.00000000.10000000 = 172.16.0.128/26. Subnet 3 is 10101100.00010000.00000000.11000000 = 172.16.0.192/26. Subnet 4 is 10101100.00010000.00000001.00000000 = 172.16.1.0/26. Subnet 5 is 10101100.00010000.00000001.01000000 = 172.16.1.64/26. Subnet 6 is 10101100.00010000.00000001.10000000 = 172.16.1.128/26. Subnet 7 - 13 are not shown. Subnet 14 is 10101100.00010000.00000011.10000000 = 172.16.3.128/26. Subnet 15 is 10101100.00010000.00000011.11000000 = 172.16.3.192/26.

### Alhálózati séma

10101100.00010000.000000 14 172.16.0.0/22 11.11 000000 172.16.3.192/26 11.10 000000 172.16.3.128/26 10101100.00010000.000000 10101100.00010000.000000 00.00 000000 15 5 01.01 172.16.1.64/26 000000 10101100.00010000.000000 6 01.10 000000 172.16.1.128/26 10101100.00010000.000000 4 000000 172.16.1.0/26 01.00 10101100.00010000.000000 3 00.11 172.16.0.192/26 000000 10101100.00010000.000000 2 00.10 172.16.0.128/26 000000 10101100.00010000.000000 1 00.01 172.16.0.64/26 000000 10101100.00010000.000000 0 00.00 000000 172.16.0.0/26

10101100.00010000.000000

Network portionHost portionDotted DecimalNets 7 - 13 not shown4-bits borrowed from host portion to create subnets

Ez az alhálózatok számát meghatározó összefüggés alapján 16 alhálózat: 24 = 16. Mivel a példában szereplő hálózat 10 alhálózatot igényel, ez pont megfelelő, és még némi bővítési lehetőséget is tartalmaz.

Ezért az első 4 állomásbitet használhatjuk az alhálózatok kijelölésére. Ez azt jelenti, hogy két bitet a 3. oktettből, két bitet pedig a 4. oktettből kell kölcsönvennünk. Amikor 4 bitet veszünk kölcsön, az új előtag hossza /26, az alhálózati maszk pedig 255.255.255.192.

Ahogy az ábrán is látható, az alhálózatok az egyes helyszínekhez és a router-ISP kapcsolatokhoz rendelhetők.

The diagram shows the subnet assignments for a corporate topology with five sites connected to an ISP cloud. Each site shows a router connected to the ISP, several servers, the public IPv4 addressing requirements, and the assigned subnet address. Each router-to-ISP connection has also been assigned a subnet address. The Corporate headquarters connection is assigned subnet 172.16.0.0/26 and the site with 40 addresses is assigned subnet 172.16.0.64/26. The Branch 1 connection is assigned subnet 172.16.0.128/26 and the site with 25 addresses is assigned 172.16.0.192/26. The Branch 2 connection is assigned subnet 172.16.1.0/26 and the site with 30 addresses is assigned subnet 172.16.1.64/26. The Branch 3 connection is assigned subnet 172.16.1.128/26 and the site with 10 addresses is assigned subnet 172.16.1.192/26. The Branch 4 connection is assigned subnet 172.16.2.0/26 and the site with 15 addresses is assigned subnet 172.16.2.64/26.

### Az alhálózatok hozzárendelése az egyes telephelyekhez és az internetszolgáltatóhoz

172.16.2.64/26 172.16.1.192/26 172.16.1.64/26 172.16.0.0/26 172.16.1.0/26 172.16.1.128/26 172.16.2.0/26 172.16.0.128/26 172.16.0.192/26

172.16.0.64/26

Corporate Headquarters40 public IPv4 addressesBranch 125 public IPv4 addresses30 public IPv4 addresses10 public IPv4 addresses15 public IPv4 addressesBranch 2ISPPublic IPv4 addressesBranch 3Branch 4

11.7.4

## Feladat – A kölcsönvett bitek számának meghatározása

Instructions:

In this activity, you are given the number of hosts that are needed. Determine the subnet mask that would support the number of hosts as specified. Enter your answers in binary, decimal, and prefix notation format in the fields provided.

| **Hosts Needed** | **Subnet Mask (binary)** | **Subnet Mask (decimal)** | **Prefix Notation(/x)** |
| --- | --- | --- | --- |
| **250** | **11111111.11111111.11111111.00000000** | **255.255.255.0** | **/24** |
| 25 | **...** |  | **/** |
| 1000 | **...** |  | **/** |
| 75 | **...** |  | **/** |
| 10 | **...** |  | **/** |
| 500 | **...** |  | **/** |

11.7.5

## Packet Tracer - Alhálózatok kialakítása

A feladat során a 192.168.100.0/24 hálózatcímet felhasználva kell a bemutatott topológián alhálózatokat kialakítani és IP-címeket kiosztani. A hálózat valamennyi LAN-jának legalább 25 állomáscímet kell biztosítania a végberendezések, a switch-ek és a routerek számára. Az R1 és R2 közötti kapcsolat a vonal mindkét végén egy-egy IP címet igényel.

[Alhálózati forgatókönyv](https://contenthub.netacad.com/courses/itn/_common/11.7.5-packet-tracer---subnetting-scenario_hu-HU.pka)

[11.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[VLSM](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                             
*           

1. IPv4-címzés
2. VLSM

# VLSM

11.8.1

## Videómagyarázat - A VLSM alapjai

Az előző témakörben említettek szerint a publikus és privát címek befolyásolják a hálózat alhálózatokra bontásának módját. Vannak más problémák is, amelyek befolyásolják az alhálózat kialakítási sémákat. A szabványos /16 előtagú alhálózati sémák olyan alhálózatokat hoznak létre, amelyek mindegyike azonos számú állomással rendelkezik. Nem minden létrehozott alhálózatnak lesz szüksége ennyi állomásra, így sok IPv4-cím kihasználatlanul marad. Előfordulhat, hogy olyan alhálózatra lesz szükségünk, amelyik sokkal több állomást tartalmaz. Ezért fejlesztették ki a változó hosszúságú alhálózati maszkot (VLSM).

Az alapvető VLSM technikák megtekintéséhez kattintsunk az ábrán látható lejátszás gombra!

11.8.2

## Videómagyarázat - VLSM példa

A VLSM alhálózat-számítás megtekintéséhez kattintsunk az ábrán látható lejátszás gombra!

11.8.3

## Az IPv4-címek megóvása

A publikus IPv4-címtartomány kimerülése miatt elsődleges szempont a rendelkezésre álló állomáscímek kiaknázása az IPv4-hálózatok alhálózatokra bontásának során.

**MEGJEGYZÉS:** A hosszabb IPv6-cím sokkal könnyebb címtervezést és -kiosztást tesz lehetővé, mint amennyit az IPv4 megenged. Az IPv6-címek megóvása nem jelent problémát. Ez az egyik hajtóereje az IPv6-ra való áttéréshez.

Hagyományos alhálózatokra bontás esetében az egyes alhálózatokhoz rendelt címek száma megegyezik. Ha minden egyes alhálózat állomásszám igénye ugyanannyi lenne vagy az IPv4-címtartomány kiürülése nem lenne probléma, az ilyen a rögzített méretű címtartományok használata is hatékony lenne. A publikus IPv4-címek esetében ez jellemzően nem így van.

Például, az ábrán látható topológia hét alhálózatot igényel, mind a négy LAN és a routerek közötti mindhárom kapcsolat egyet-egyet.

The diagram shows a network topology consisting of seven subnets. There are four routers, each with an attached LAN and host addressing requirements, and three router-to-router connections requiring 2 hosts each. The R1 router LAN is Building A with 25 hosts; the R2 router LAN is Building B with 20 hosts; the R3 router LAN is Building C with 15 hosts; and the R4 router LAN is Building D with 28 hosts.

R1 R2 R3

R4

Building ABuilding BBuilding CBuilding D25 hosts20 hosts15 hosts28 hosts2 hosts2 hosts2 hosts

A hagyományos alhálózatokra bontást alkalmazva az adott 192.168.20.0/24 hálózatcím utolsó oktettjének állomásazonosító részéből 3 bitet elvéve alakítható ki a hét alhálózat. Ahogy az ábrán is látható, a 3 bit elvétele 8 alhálózatot eredményez, melyekben alhálózatonként a maradék 5 állomásbitnek köszönhetően 30 állomás lehet. Ez a módszer előállítja a kívánt alhálózatokat és teljesíti a legnagyobb LAN állomásszám igényét is.

The diagram shows the basic subnet scheme for a given address of 192.168.20.0/24 with three bits borrowed for subnetting. Having 3 bits for subnetting results in 2 to the power of 3 = 8 subnets. Having 5 bits for hosts results in 2 to the power of 5 - 2 = 30 host IP addresses per subnet. All four octets are shown in binary followed by the dotted decimal format for the given address and for all the subnets created. The given network address in binary is 11000000.10101000.00010100 (network portion highlighted in gray) .00000000 (host portion highlighted in purple) = 192.168.20.0/24. For the subnets listed below, the first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue (subnet portion), and the last five bits are the remaining host bits highlighted in purple. Subnet 0 is 11000000.10101000.00010100.00000000 = 192.168.20.0/27. Subnet 1 is 11000000.10101000.00010100.00100000 = 192.168.20.32/27. Subnet 2 is 11000000.10101000.00010100.01000000 = 192.168.20.64/27. Subnet 3 is 11000000.10101000.00010100.01100000 = 192.168.20.96/27. Subnets 0 - 3 are assigned to building LANs A, B, C, and D. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Subnets 4, 5, and 6 are assigned to the site to site WANs. Subnet 7 is 11000000.10101000.00010100.11100000 = 192.168.20.224/27. Subnet 7 is unused/available.

### Hagyományos alhálózat kialakítás

11000000.10101000.00010100 .000 00000 192.168.20.0/24 6 .110 00000 11000000.10101000.00010100 192.168.20.192/27 5 .101 00000 11000000.10101000.00010100 192.168.20.160/27 4 .100 00000 11000000.10101000.00010100 192.168.20.128/27 3 .011 00000 11000000.10101000.00010100 192.168.20.96/27 2 .010 00000 11000000.10101000.00010100 192.168.20.64/27 1 .001 00000 11000000.10101000.00010100 192.168.20.32/27 0 .000 00000 11000000.10101000.00010100 192.168.20.0/27 7 .111 00000 11000000.10101000.00010100

192.168.20.224/27

Building LANs A, B, C, and DSite to Site WANsUnused / AvailableNetwork PortionHost PortionSubnet portion  
2^3 = 8 subnetsHost portion  
2^5 – 2 = 30 host IP addresses per subnet

Ez a hét alhálózat hozzárendelhető a LAN és a WAN hálózatokhoz az ábrán látható módon.

The diagram shows the subnet assignments for a network topology consisting of seven subnets. There are four routers, each with an attached LAN and host addressing requirements, and three router-to-router connections requiring 2 hosts each. The R1 router Building A LAN has 25 hosts and is assigned subnet 192.168.20.0/27. The R2 router Building B LAN has 20 hosts and is assigned the subnet 192.168.20.32/27. The R3 router Building C LAN has 15 hosts and is assigned subnet 192.168.20.64/27. The R4 router Building D LAN has 28 hosts and is assigned subnet 192.168.20.96/27. The R1 to R2 connection is assigned subnet 192.168.20.128/27. The R2 to R3 connection is assigned subnet 192.168.20.160/27. The R3 to R4 connection is assigned subnet 192.168.20.192/27.

R1 R2 R3 R4 192.168.20.128/27 192.168.20.160/27

192.168.20.192/27

Building A  
192.168.20.0/27Building B  
192.168.20.32/27Building C  
192.168.20.64/27Building D  
192.168.20.96/2725 hosts20 hosts15 hosts28 hosts2 hosts2 hosts2 hosts

Bár a hagyományos alhálózatkialakítási módszer teljesíti a legnagyobb LAN állomásszám igényét és kellő számú alhálózatra osztja a címtartományt, jelentős mennyiségű kihasználatlan címet eredményez.

Például a három WAN kapcsolat alhálózatain mindössze két-két címre van szükség. Mivel mindegyik alhálózat 30 címet tartalmaz, így ezen alhálózatok mindegyikén 28 kihasználatlan cím marad. Ahogy ezt az ábra is szemlélteti, ez 84 kihasználatlan (28x3) címet eredményez.

The graphic shows the unused addresses of four WAN subnets using a /27 subnet mask. All four octets are shown in binary followed by the dotted decimal format for the subnet. The first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue, and the last five bits are the remaining host bits highlighted in purple. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Having 5 bits for hosts results in 2 to the power of 5 - 2 = 30 host IP addresses per subnet. 30 - 2 = 28; each WAN subnet wastes 28 addresses. 28 x 3 = 84; 84 addresses are unused.

### Kihasználatlan címek a WAN alhálózatokon

5 .101 00000 11000000.10101000.00010100 192.168.20.160/27 6 .110 00000 11000000.10101000.00010100 192.168.20.192/27 11000000.10101000.00010100 .100 00000 4

192.168.20.128/27

Network PortionHost PortionHost portion  
2^5 – 2 = 30 host IP addresses per subnet  
  
30 – 2 = 28  
Each WAN subnet wastes 28 addresses  
  
28 x 3 = 84  
84 addresses are unusedDotted Decimal

Mindezek mellett ez korlátozza a jövőben rendelkezésre álló alhálózatok számát is. Ez a címpazarlás a jellemzője az osztály alapú hálózatok hagyományos alhálózatokra bontásának. Ebben a helyzetben a hagyományos alhálózat kialakítási módszer nem túl hatékony és pazarló.

Az alhálózatok további alhálózatokra bontása, vagy más néven a változó hosszúságú alhálózati maszk (VLSM) alkalmazása elkerülhetővé teszi a címveszteséget.

11.8.4

## VLSM

Az összes korábbi példában ugyanazt az alhálózati maszkot alkalmaztuk valamennyi alhálózatban. Ez azt jelenti, hogy valamennyi alhálózatban ugyanannyi állomáscím kerülhet kiosztásra. Ahogy az ábra bal oldalán is látható, hagyományos alhálózatokra bontás esetén azonos méretű alhálózatok jönnek létre. A hagyományos módszer szerint valamennyi alhálózatban ugyanazt az alhálózati maszkot használjuk. Ahogy az ábra jobb oldalán látható, a VLSM lehetővé teszi egy hálózati tartomány különböző méretekre történő felosztását. A VLSM esetében az alhálózati maszk az egyes alhálózatokban kölcsönvett bitek számától függően változik, ez jelenti a „változót” a VLSM névben.

The graphic shows two pie charts that compare traditional subnetting to VLSM. On the right is a pie chart titled: traditional subnetting creates equal sized subnets. The pie is divided into 8 equal sized slices, each with 30 hosts. On the left is a pie chart titled: subnets of varying sizes. This pie has 7 slices identical to the first pie. The 8th slice has been further divided into 8 smaller slices. Text pointing to 8th slice reads: one subnet was further divided using a /30 subnet mask to create 8 smaller subnets of 2 hosts each.

One subnet was further divided using a /30 subnet mask to create 8 smaller subnets of 2 hosts each.30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 Hosts30 HostsTraditional Subnetting Creates Equal Sized SubnetsSubnets of Varying Sizes

A VLSM egyszerűen egy alhálózatot bont fel további alhálózatokra. Az ábrán a korábban használt topológia látható. Ismét a 192.168.20.0/24 hálózatot fogjuk használni, és hét alhálózatra bontjuk. Egyet-egyet a négy LAN mindegyikéhez rendelünk, és egyet-egyet pedig a routerek közötti három kapcsolathoz.

The diagram shows a network topology consisting of seven subnets. There are four routers, each with an attached LAN and host addressing requirements, and three router-to-router connections requiring 2 hosts each. The R1 router LAN is Building A with 25 hosts; the R2 router LAN is Building B with 20 hosts; the R3 router LAN is Building C with 15 hosts; and the R4 router LAN is Building D with 28 hosts.

R1 R2 R3

R4

Building ABuilding BBuilding CBuilding D25 hosts20 hosts15 hosts28 hosts2 hosts2 hosts2 hosts

Az ábrán látható, hogy a 192.168.20.0/24 hálózatot nyolc egyenlő méretű alhálózatra osztottuk, alhálózatonként 30 használható állomáscímmel. Négy alhálózat kellett a LAN-okhoz, három pedig a routerek közötti kapcsolatokhoz.

The diagram shows the basic subnet scheme for a given address of 192.168.20.0/24 with three bits borrowed for subnetting. All four octets are shown in binary followed by the dotted decimal format for the given address and for all the subnets created. The given network address in binary is 11000000.10101000.00010100 (network portion highlighted in gray) .00000000 (host portion highlighted in purple) = 192.168.20.0/24. For the subnets listed below, the first 24 bits are highlighted in gray (network portion), the next three bits are highlighted in blue (subnet portion), and the last five bits are the remaining host bits highlighted in purple. Subnet 0 is 11000000.10101000.00010100.00000000 = 192.168.20.0/27. Subnet 1 is 11000000.10101000.00010100.00100000 = 192.168.20.32/27. Subnet 2 is 11000000.10101000.00010100.01000000 = 192.168.20.64/27. Subnet 3 is 11000000.10101000.00010100.01100000 = 192.168.20.96/27. Subnets 0 - 3 are assigned to building LANs A, B, C, and D. Subnet 4 is 11000000.10101000.00010100.10000000 = 192.168.20.128/27. Subnet 5 is 11000000.10101000.00010100.10100000 = 192.168.20.160/27. Subnet 6 is 11000000.10101000.00010100.11000000 = 192.168.20.192/27. Subnets 4, 5, and 6 are unused/available. Subnet 7 is 11000000.10101000.00010100.11100000 = 192.168.20.224/27. Subnet 7 will be subnetted further.

### Hagyományos alhálózat kialakítás

11000000.10101000.00010100 .00000000 192.168.20.0/24 0 11000000.10101000.00010100 .000 00000 192.168.20.0/27 1 11000000.10101000.00010100 .001 00000 192.168.20.32/27 2 11000000.10101000.00010100 .010 00000 192.168.20.64/27 3 11000000.10101000.00010100 .011 00000 192.168.20.96/27 4 11000000.10101000.00010100 .100 00000 192.168.20.128/27 5 11000000.10101000.00010100 .101 00000 192.168.20.160/27 6 11000000.10101000.00010100 .110 00000 192.168.20.192/27 7 11000000.10101000.00010100 .111 00000 192.168.20.224/27

Network portionHost portionDotted DecimalLAN  
A, B, C, DUnused /   
AvailableSubnet 7 will be subnetted further.

A routerek közötti kapcsolatok azonban alhálózatonként csak két állomáscímet igényelnek (minden router interfészhez egy állomáscímet). Jelenleg minden alhálózat 30 használható állomáscímet tartalmaz alhálózatonként. Az alhálózatonkénti 28 állomáscím elpazarlását elkerülendő, használhatunk VLSM-et, hogy a routerek közötti kapcsolatokhoz kisebb méretű alhálózatokat rendeljünk.

Ahhoz, hogy a routerek közötti kapcsolatokhoz kisebb méretű alhálózatokat hozzunk létre, az egyik alhálózatot bontjuk tovább. Ebben a példában a 192.168.20.224/27 az utolsó alhálózat, ezt fogjuk most továbbosztani. Az ábra azt mutatja, hogy az utolsó alhálózat továbbosztása a 255.255.255.252 alhálózati maszkkal vagy /30 előtaggal történt.

The diagram show the VLSM subnetting scheme when the subnet 192.168.20.224/27 is further subnetted by borrowing 3 more bits. For the original subnet, the first 24 bits represent the network portion and are 11000000.10101000.00010100. The next three bits represent the subnet portion and are 111. The last five bits represent the host portion and are 00000. The address in dotted decimal is 192.168.20.224/27. Borrowing 3 additional bits, subnetting a subnet, results in dividing the original subnet into 8 smaller subnets. For the smaller subnets, the first 24 bits are the network portion, the next six bits are the subnet portion, and the last two bits are the remaining host portion. Subnet 7:0 is 11000000.10101000.00010100.11100000 = 192.168.20.224/30. Subnet 7:1 is 11000000.10101000.00010100.11100100 = 192.168.20.228/30. Subnet 7:2 is 11000000.10101000.00010100.11101000 = 192.168.20.232/30. Subnet 7:3 is 11000000.10101000.00010100.11101100 = 192.168.20.236/30. Subnet 7:4 is 11000000.10101000.00010100.11110000 = 192.168.20.240/30. Subnet 7:5 is 11000000.10101000.00010100.11110100 = 192.168.20.244/30. Subnet 7:6 is 11000000.10101000.00010100.11111000 = 192.168.20.248/30. Subnet 7:7 is 11000000.10101000.00010100.11111100 = 192.168.20.252/30. Subnets 7:0, 7:1, and 7:2 are assigned to the WANs and the remaining subnets are unused/available.

### VLSM alhálózat kialakítás

7 11000000.10101000.00010100 .111 00000 192.168.20.224/277:0 11000000.10101000.00010100 .111000 00 192.168.20.224/30 7:1 11000000.10101000.00010100 .111001 00 192.168.20.228/30 7:2 11000000.10101000.00010100 .111010 00 192.168.20.232/30 7:3 11000000.10101000.00010100 .111011 00 192.168.20.236/30 7:4 11000000.10101000.00010100 .111100 00 192.168.20.240/30 7:5 11000000.10101000.00010100 .111101 00 192.168.20.244/30 7:6 11000000.10101000.00010100 .111110 00 192.168.20.248/30 7:7 11000000.10101000.00010100 .111111 00 192.168.20.252/30

Network portionHost portionDotted DecimalWANsUnused / AvailableSubnetting a subnet3 more bits borrowed from subnet ?

Miért a /30 előtag? Ne feledjük, hogy amikor a szükséges állomáscímek száma ismert, akkor a 2n-2 (ahol n a megmaradó állomásbitek száma) összefüggést használhatjuk. Ahhoz, hogy két kiosztható címünk legyen, 2 állomásbitnek kell maradnia az állomásazonosító részben.

Mivel a 192.168.20.224/27 címtartományban 5 állomásbit van, ezért 3 bitet vehetünk kölcsön, így az állomásazonosító részben 2 bit marad. Itt a számítások teljesen megegyeznek a hagyományos alhálózatok kialakításánál látottakkal. Biteket veszünk el és meghatározzuk az alhálózati tartományokat. Az ábrán látható, hogy a négy /27 előtagú alhálózat miként lett hozzárendelve a LAN-okhoz, és a /30 előtagú alhálózatok közül három van hozzárendelve a routerek közötti kapcsolatokhoz.

The diagram shows the VLSM subnet assignments for a network topology consisting of four LANs and three WANs. There are four routers, each with an attached LAN and host addressing requirements, and three router-to-router connections requiring 2 hosts each. The R1 router Building A LAN has 25 hosts and is assigned subnet 192.168.20.0/27. The R2 router Building B LAN has 20 hosts and is assigned the subnet 192.168.20.32/27. The R3 router Building C LAN has 15 hosts and is assigned subnet 192.168.20.64/27. The R4 router Building D LAN has 28 hosts and is assigned subnet 192.168.20.96/27. The R1 to R2 connection is assigned subnet 192.168.20.224/30. The R2 to R3 connection is assigned subnet 192.168.20.228/30. The R3 to R4 connection is assigned subnet 192.168.20.232/30.

192.168.20.0/27 192.168.20.32/27 192.168.20.64/27 192.168.20.96/27 192.168.20.224/30 192.168.20.228/30 192.168.20.232/30 R1 R2 R3

R4

Building ABuilding BBuilding CBuilding D25 hosts20 hosts15 hosts28 hosts2 hosts2 hosts2 hosts

A VLSM alhálózat kialakítási módszer a kevesebb alhálózatot igénylő hálózatok elvárásainak megfelelően csökkenti le az alhálózatonkénti állomáscímek számát. A 7. alhálózat további alhálózatokra bontása létrehozza még a 4., 5. és 6. alhálózatokat, melyek további hálózatok vagy routerek közötti kapcsolatok kialakítására alkalmasak.

**MEGJEGYZÉS:** A VLSM használatakor kezdjük mindig a legnagyobb alhálózat állomásigényeinek kielégítésével! Folytassuk addig az alhálózatokra bontást, amíg a legkisebb alhálózat állomáskövetelményei nem teljesülnek.

11.8.5

## A VLSM topológia címkiosztása

A VLSM alhálózatok használatával a LAN és a routerek közötti szegmensek felesleges pazarlás nélkül címezhetők.

Az ábrán a hálózati címek kiosztása és az egyes router interfészekhez rendelt IPv4-címek láthatók.

The diagram shows the VLSM subnet assignments and interface IP addressing for a network topology consisting of four LANs and three WANs. There are four routers, each with an attached LAN and host addressing requirements, and three router-to-router connections requiring 2 hosts each. The R1 router Building A LAN is connected to the G0/0/0 interface of R1 at 192.168.20.1/27, has 25 hosts, and is assigned subnet 192.168.20.0/27. The R2 router Building B LAN is connected to the G0/0/0 interface of R2 at 192.168.20.33/27, has 20 hosts, and is assigned the subnet 192.168.20.32/27. The R3 router Building C LAN is connected to the G0/0/0 interface of R3 at 192.168.20.65/27, has 15 hosts, and is assigned subnet 192.168.20.64/27. The R4 router Building D LAN is connected to the G0/0/0 interface of R4 at 192.168.20.97/27, has 28 hosts, and is assigned subnet 192.168.20.96/27. The R1 to R2 connection, assigned subnet 192.168.20.224/30, connects the G0/0/1 interface of R1 with address .225 to the G0/0/1 interface of R2 with address .226. The R2 to R3 connection, assigned subnet 192.168.20.228/30, connects the G0/1/0 interface of R2 with address .229 to the G0/0/1 interface of R3 with address .230. The R3 to R4 connection, assigned subnet 192.168.20.232/30, connects the G0/1/0 interface of R2 with address .233 to the G0/0/1 interface of R4 with address .234.

G0/0/1 G0/0/1 G0/1/0 G0/0/1 G0/0/1 G0/1/0 .225 .234 .233 .230 .229 .226 G0/0/0 G0/0/0 G0/0/0 G0/0/0 192.168.20.224/30 192.168.20.228/30 192.168.20.232/30 R1-R2 R2-R3 R3-R4 192.168.20.1/27 192.168.20.33/27 192.168.20.65/27 192.168.20.97/27 192.168.20.0/27 192.168.20.32/27 192.168.20.64/27 192.168.20.96/27 R1 R2 R3

R4

Building ABuilding BBuilding CBuilding D25 hosts20 hosts15 hosts28 hosts2 hosts2 hosts2 hosts

Egy bevált címzési felfogás szerint valamennyi alhálózat első IPv4 állomáscímét a router LAN interfésze kapja. Valamennyi alhálózat állomásai saját alhálózatukból kapnak érvényes állomáscímet és maszkot. Az állomások a kapcsolódó router LAN interfészének címét használják az alapértelmezett átjáró címeként.

A táblázat az egyes hálózatok hálózatcímeit és az állomáscímek tartományát mutatja. A négy LAN mindegyikénél megjelenik az alapértelmezett átjáró címe is.

| Network AddressRange of Host AddressesDefault Gateway AddressBuilding A192.168.20.0/27192.168.20.1/27 to 192.168.20.30/27192.168.20.1/27Building B192.168.20.32/27192.168.20.33/27 to 192.168.20.62/27192.168.20.33/27Building C192.168.20.64/27192.168.20.65/27 to 192.168.20.94/27192.168.20.65/27Building D192.168.20.96/27192.168.20.97/27 to 192.168.20.126/27192.168.20.97/27R1-R2192.168.20.224/30192.168.20.225/30 to 192.168.20.226/30R2-R3192.168.20.228/30192.168.20.229/30 to 192.168.20.230/30R3-R4192.168.20.232/30192.168.20.233/30 to 192.168.20.234/30 | | | |
| --- | --- | --- | --- |
|  | **Network Address** | **Range of Host Addresses** | **Default Gateway Address** |
| **Building A** | 192.168.20.0/27 | 192.168.20.1/27 to 192.168.20.30/27 | 192.168.20.1/27 |
| **Building B** | 192.168.20.32/27 | 192.168.20.33/27 to 192.168.20.62/27 | 192.168.20.33/27 |
| **Building C** | 192.168.20.64/27 | 192.168.20.65/27 to 192.168.20.94/27 | 192.168.20.65/27 |
| **Building D** | 192.168.20.96/27 | 192.168.20.97/27 to 192.168.20.126/27 | 192.168.20.97/27 |
| **R1-R2** | 192.168.20.224/30 | 192.168.20.225/30 to 192.168.20.226/30 |  |
| **R2-R3** | 192.168.20.228/30 | 192.168.20.229/30 to 192.168.20.230/30 |  |
| **R3-R4** | 192.168.20.232/30 | 192.168.20.233/30 to 192.168.20.234/30 |  |

11.8.6

## Feladat – VLSM gyakorlás

### 192.168.5.0/24 | Table 1 - First Subnets Calculation

Table 1 uses regular subnetting to accommodate the network shown. Table 2 uses **VLSM** to further subnet the network. Calculate 50 users per subnet.

Click the new subnet mask (decimal).

[192.168.5.0-  
192.168.5.63](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/26](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[255.255.255.192](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[192.168.5.192-  
192.168.5.255](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the **first** prefix notation.

[192.168.5.0-  
192.168.5.63](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/26](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[255.255.255.192](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[192.168.5.192-  
192.168.5.255](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the first **full** subnet range.

[192.168.5.0-  
192.168.5.63](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/26](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[255.255.255.192](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[192.168.5.192-  
192.168.5.255](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the second **full** subnet range.

[192.168.5.0-  
192.168.5.63](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/26](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[255.255.255.192](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[192.168.5.192-  
192.168.5.255](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the last **full** subnet range.

[192.168.5.0-  
192.168.5.63](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/26](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[255.255.255.192](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[192.168.5.192-  
192.168.5.255](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

### 192.168.5.0/24 | Table 2 - VLSM Calculation

Use the second full subnet range from Table 1 and VLSM to calculate for 20 users per subnet.

Click the second **full** subnet range (/26) from Table 1.

[192.168.5.96-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/27](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[255.255.255.224](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.95](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the new VLSM subnet mask (decimal).

[192.168.5.96-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/27](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[255.255.255.224](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.95](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the **VLSM** prefix notation.

[192.168.5.96-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/27](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[255.255.255.224](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.95](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the first **full VLSM** subnet range.

[192.168.5.96-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/27](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[255.255.255.224](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.95](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

Click the last **full VLSM** subnet range.

[192.168.5.96-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "1)

[/27](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "2)

[192.168.5.64-  
192.168.5.127](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "3)

[255.255.255.224](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "4)

[192.168.5.64-  
192.168.5.95](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "5)

[11.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alhálózatok kialakítása a követelményeknek megfelelően](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Strukturált tervezés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                              
*           

1. IPv4-címzés
2. Strukturált tervezés

# Strukturált tervezés

11.9.1

## IPv4 hálózatok címzési terve

Mielőtt elkezdenénk az alhálózatok kialakítását, ki kell dolgoznunk egy IPv4 címzési struktúrát a teljes hálózatra vonatkozóan. Tudnunk kell, hogy hány alhálózatra van szükségünk, hány állomást igényel egy adott alhálózat, mely eszközök tartoznak az alhálózathoz, a hálózat mely részei használnak privát ill. publikus címeket, és sok más lényeges szempontot is figyelembe kell vennünk. A jó címzési struktúra lehetővé teszi a növekedést. A jó címzési struktúra egy jó hálózati rendszergazda ismérve is egyben.

Az alhálózati terv elkészítéséhez az intézményi hálózat használatának és a struktúrájának az elemzése egyaránt szükséges. Az első lépés a hálózattal szemben támasztott igények felmérése. Ez azt jelenti, hogy megvizsgáljuk a teljes hálózatot (beleértve az intranetet és a DMZ-t egyaránt), és meghatározzuk, hogy az egyes területek miként lesznek szegmentálva. A címzési terv magában foglalja annak meghatározását, hogy hol szükséges a címek megóvása (általában a DMZ-ben), és hol van nagyobb rugalmasság (általában az intraneten belül).

Ahol szükséges a címek megóvása, a tervnek meg kell határoznia, hogy hány alhálózatra és alhálózatonként hány állomásra van szükség. Amint azt korábban tárgyaltuk, ez általában a DMZ-n belüli publikus IPv4-címtartomány esetében szükséges. Ez valószínűleg magában foglalja a VLSM használatát.

A vállalati intraneten belül a címek megóvása általában kevésbé probléma Ez nagyrészt a privát IPv4-címzés használatának köszönhető, beleértve a 10.0.0.0/8 hálózatot, több mint 16 millió IPv4-állomáscímmel.

A legtöbb szervezet esetében a privát IPv4-címek több mint elegendő belső (intranetes) címet biztosítanak. Számos nagyobb szervezet és internetszolgáltató esetében még a privát IPv4-címtartomány sem elég nagy ahhoz, hogy kielégítse a belső igényeket. Ez egy másik ok, amiért a szervezetek áttérnek az IPv6-ra.

A privát IPv4-címeket használó intranetek és a publikus IPv4-címeket használó DMZ-k esetében fontos a címtervezés és -kiosztás.

Szükség esetén a címzési terv magában foglalja az egyes alhálózatok szükségleteinek meghatározását a méret szempontjából. Hány állomás lehet alhálózatonként? A címzési tervnek azt is tartalmaznia kell, hogy miként lesznek a címek kiosztva, mely állomások igényelnek statikus IPv4-címeket, és mely állomások esetében lehet DHCP-t használni a címzési információk megszerzéséhez. Ez segít megakadályozni a címek megkettőzését, miközben teljesítménybeli és biztonsági okokból lehetővé teszi a címek felügyeletét és kezelését.

Az IPv4-címmel kapcsolatos követelmények ismerete meghatározza a kialakítandó állomáscímek tartományát vagy tartományait, és segít biztosítani, hogy elegendő cím álljon rendelkezésre a hálózati igények kielégítésére.

11.9.2

## Eszközök címkiosztása

A hálózatban különböző eszköztípusok találhatók, például:

* **Végfelhasználói kliensek** — A legtöbb hálózat dinamikusan osztja ki az IPv4-címeket a kliens oldali eszközök számára, a DHCP protokoll használatával. Ez csökkenti a hálózati támogató személyzetre nehezedő terhet, és gyakorlatilag kiküszöböli a belépési hibákat. A DHCP esetében a címek bérbeadása csak egy bizonyos ideig lehetséges, és a bérleti idő lejártakor újra felhasználhatóvá válnak. Ez fontos funkció az átmeneti felhasználókat és vezeték nélküli eszközöket támogató hálózatok esetében. Az alhálózati séma módosítása azt jelenti, hogy a DHCP-szervert újra kell konfigurálni, és az ügyfeleknek meg kell újítaniuk az IPv4-címeiket. Az IPv6-kliensek a DHCPv6 vagy a SLAAC segítségével szerezhetik meg a címadatokat.
* **Szerverek és perifériák** - Ezeknek rögzített, statikus IP-címmel kell rendelkezniük. Használjunk következetes számozási rendszert ezen eszközök esetében.
* **Az internetről elérhető szerverek** - Azoknak a szervereknek, amelyeknek nyilvánosan elérhetőnek kell lenniük az interneten, publikus IPv4-címmel kell rendelkezniük, amelyet leggyakrabban a hálózati címfordítás (NAT) révén szereznek meg. Egyes szervezetekben a távoli felhasználók számára elérhetővé kell tenni a (nyilvánosan nem elérhető) belső szervereket. A legtöbb esetben ezek a szerverek privát címmel rendelkeznek, és a felhasználónak virtuális magánhálózaton (VPN) keresztüli kapcsolatot kell létrehoznia a szerver eléréséhez. Ennek ugyanaz a hatása, mintha a felhasználó egy intraneten belüli állomásról érné el a szervert.
* **Közvetítő eszközök** - Ezek az eszközök hálózatkezelési, -felügyeleti és -biztonsági célból kapnak címet. Mivel a közvetítő eszközökkel tudnunk kell kommunikálni, ezeknek is rögzített, statikus címekkel kell rendelkezniük.
* **Átjáró** - A routerek és a tűzfaleszközök minden egyes interfészéhez IP-címet rendelünk, amely átjáróként szolgál az adott hálózatban lévő állomások számára. A router interfésze általában a hálózat legalacsonyabb vagy legmagasabb címét kapja.

Az IP-címzési terv elkészítésekor célszerű egy sémát kialakítani arra, hogy miként osszuk ki a címeket az egyes eszköztípusok számára. Ez hasznára van a rendszergazdának, amikor új eszközöket állít be vagy távolít el, amikor IP alapon szűri a forgalmat, vagy egyszerűen csak megkönnyíti a dokumentációt.

11.9.3

## Packet Tracer - VLSM tervezési és megvalósítási gyakorlat

A feladat során egy /24 előtagú hálózatcímet kapunk, amelyet egy VLSM címzési struktúra tervezéséhez kell használnunk. A követelmények alapján ki kell alakítanunk az alhálózatokat és a címzési struktúrát, konfigurálnunk kell az eszközöket, és ellenőriznünk kell a köztük lévő kapcsolato(ka)t.

[VLSM tervezési és megvalósítási gyakorlat](https://contenthub.netacad.com/courses/itn/_common/11.9.3-packet-tracer---vlsm-design-and-implementation-practice_hu-HU.pka)

[11.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[VLSM](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[11.10](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                           

1. IPv4-címzés
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

11.10.1

## Packet Tracer - Egy VLSM címzési terv elkészítése és megvalósítása

A feladat során egy VLSM címzési struktúrát kell terveznünk egy hálózatcím és az állomásokkal szemben támasztott követelmények alapján. A címeket routereken, switch-eken és hálózati állomásokon kell beállítanunk.

* A tervezési követelményeknek megfelelő VLSM IP-címzési struktúra megválasztása
* A címek beállítása hálózati eszközökön és állomásokon
* Összeköttetések ellenőrzése
* Kapcsolódási problémák szükség szerinti hibaelhárítása

[VLSM címzési terv elkészítése és megvalósítása](https://contenthub.netacad.com/courses/itn/_common/11.10.1-packet-tracer---design-and-implement-a-vlsm-addressing-scheme_hu-HU.pka)

11.10.2

## Laborgyakorlat - Design and Implement a VLSM Addressing Scheme

A laborgyakorlat során a 192.168.33.128/25 hálózatcím használatával alakítsuk ki a topológia szerinti hálózat címzési struktúráját. Használjunk VLSM-et, hogy megfeleljünk az IPv4-címzési követelményeknek. Miután megterveztük a VLSM címzési struktúrát, állítsuk be a megfelelő IP-címeket a routerek interfészein. A BR2 jövőbeli LAN-jaihoz címeket kell rendelnünk, de interfész(ek) konfigurálására jelenleg nem kerül sor.

11.10.3

## Miről tanultunk ebben a fejezetben?

**IPv4-címzési struktúra**

Az IPv4-cím egy 32 bites hierarchikus cím, amely egy hálózati és egy állomásazonosító részből áll. Szükséges, hogy a hálózati részt adó bitek minden olyan eszköznél azonosak legyenek, amelyek ugyanazon a hálózaton tartózkodnak. Az állomásazonosító rész bitjeinek az alhálózaton belül egyedinek kell lenniük, hogy az állomást azonosítani tudják. Az állomásoknak egyedi IPv4-címre és alhálózati maszkra van szükségük a cím hálózati/állomásazonosító részeinek megjelenítéséhez. Az előtag hossza az alhálózati maszk egyeseinek száma. A perjellel megadott előtagban a perjel (/) után az 1-es bitek számát kell írni. A logikai ÉS művelet tulajdonképpen két bit összehasonlítása. Csak az 1 ÉS 1 eredménye lesz 1, minden más kombináció nullát eredményez. Bármely más kombináció eredménye 0. Minden hálózaton belül vannak hálózatcímek, állomáscímek és egy szórási cím.

**IPv4 egyedi címzés, szórás és csoportos címzés**

Az egyedi címzésű átvitel egy eszközre vonatkozik, amely közvetlen (egy-az-egynek típusú) kommunikáció során küld üzenetet egy másik eszköznek. Az egyedi címzésű csomagnak van egy cél IP-címe, amely egyetlen címzettnek szól. A szórásos átvitel olyan eszközre vonatkozik, amely egy-a-mindenkinek típusú kommunikáció során küld üzenetet a hálózaton lévő összes eszköznek. A szórásos csomagban célcímként egy olyan IP-cím van, ami csupa 1-est tartalmaz az állomásazonosító részen. A forgalmat azáltal csökkenti, hogy lehetővé teszi az állomás számára egyetlen csomag egyszerre több, a csoportcímre feliratkozott állomásnak történő elküldését. A csoportos címzésű (multicast) csomag olyan csomag, amelynek cél IP-címe csoportos címzésű cím. Az IPv4 a 224.0.0.0 és 239.255.255 közötti címeket a csoportos címzési tartomány számára tartja fenn.

**IPv4-címek típusai**

A publikus IPv4-címek olyan címek, amelyek globálisan címezhetők (route-olhatók) az internetszolgáltató (ISP) routerei között. Nem minden rendelkezésre álló IPv4-cím használható az interneten. Vannak olyan címtartományok, amelyeket a legtöbb szervezet az IPv4-címek belső állomásokhoz való hozzárendelésére használ. A legtöbb belső hálózat privát IPv4-címeket használ az összes belső eszköz (intranet) kezelésére, azonban ezek a privát címek globálisan nem címezhetők. A loopback címet az állomások használják, hogy visszairányítsák a forgalmat önmagukhoz. A link-lokális címek, ismertebb nevükön az automatikus privát IP-címzés (APIPA) címei vagy önkiosztó címek. 1981-ben az IPv4-címek kiosztása (A, B vagy C) osztály alapú címzéssel történt. A publikus IPv4-címeknek globálisan egyedinek kell lenniük, és továbbíthatók az interneten keresztül. Az IANA kezeli és osztja ki az IPv4- és IPv6-címek blokkjait a regionális címregisztrációs szervezetek (RIR) számára.

**Hálózatszegmentálás**

Az Ethernet LAN esetében az eszközök az ARP szórásos üzeneteinek segítségével keresik meg a többi eszközt. A switch elárasztja a szórási üzenetekkel az összes interfészt, kivéve azt, amelyen fogadta. A routerek nem továábbítják a szórásokat, ehelyett a router mindegyik interfésze egy szórási tartományhoz kapcsolódik, és a szórások csak az adott tartományon belül terjednek. A nagyméretű szórási tartomány egy olyan hálózat, amely sok állomást köt össze. A nagyméretű szórási tartomány egyik problémája az, hogy az állomások túlzott mértékű szórásokat generálhatnak, és így negatív hatással lehetnek a hálózatra. A megoldás a hálózat méretének csökkentése, hogy kisebb szórási tartományokat hozzunk létre az alhálózatokra bontásnak nevezett folyamat során. Ezeket a kisebb hálózati tereket alhálózatoknak nevezzük. Az alhálózatokra bontás a teljes hálózat forgalmának csökkentésével növeli a hálózat teljesítményét. A rendszergazda az alhálózatok kialakítását helyszín alapján, hálózatok között vagy eszköztípus szerint is végezheti.

**Egy IPv4-hálózat alhálózatokra bontása**

Az IPv4 alhálózatok egy vagy több állomásbit hálózati bitként való értelmezésével keletkeznek. Ez az alhálózati maszk kiegészítésével történik, kibővítve a cím hálózati részét az állomásazonosító részből kölcsönvett bitekkel. Minél több állomásbitet veszünk kölcsön, annál több alhálózat kialakítására van lehetőség. Minél több bitet veszünk kölcsön az alhálózatok számának növeléséhez, annál kevesebb lesz az alhálózatonkénti állomások száma. A hálózatok legegyszerűbben a /8, /16 és /24 oktetthatárok mentén bonthatók alhálózatokra. Az alhálózatok bármely állomásbit-pozícióból vehetnek kölcsön biteket más maszkok létrehozásához.

**Egy /16 és egy /8 előtagú hálózat alhálózatokra bontása**

Nagyobb számú alhálózatot igénylő helyzetekben olyan IPv4-hálózatra van szükség, amelyben több állomásbit kölcsönvételére nyílik lehetőség. Mint mindig, az alhálózatok létrehozásának érdekében most is biteket kell kölcsönvennünk a meglévő hálózathoz rendelt IPv4-cím állomásazonosító részéből. Balról jobbra haladva az első használható állomásbittel kezdve egyesével fogjuk a biteket kölcsönvenni, míg el nem érjük a kívánt alhálózatot biztosító bitszámot. Amikor biteket veszünk kölcsön egy /16 előtagú címből, kezdjük a harmadik oktettben, balról jobbra haladva. Az első cím a hálózat címének, az utolsó cím pedig a szórási címnek van fenntartva.

**Alhálózatok kialakítása a követelményeknek megfelelően**

Egy tipikus vállalati hálózat intranetet és DMZ-t is tartalmaz. Mindkettő saját alhálózati követelményekkel és kihívásokkal rendelkezik. Az intranet privát IPv4-címtartományt használ. A 10.0.0.0/8 hálózat bármely más (pl.: a /12, /18, /20) előtaggal is alhálózatokra bontható, amely sokféle lehetőséget biztosít a hálózati rendszergazdának. Mivel ezeknek az eszközöknek nyilvánosan hozzáférhetőnek kell lenniük az internetről, a DMZ eszközeihez publikus IPv4-címek szükségesek. A szervezeteknek maximálisan ki kell használniuk a saját, korlátozott számú publikus IPv4-címeiket. Ahhoz, hogy minimálisra csökkenjen a fel nem használt állomáscímek alhálózatonkénti száma, a hálózati rendszergazdának különböző maszkokkal rendelkező alhálózatokra kell bontania a publikus címtartományt. Ez az úgynevezett változó hosszúságú alhálózati maszk (VLSM) használata. A rendszergazdának meg kell fontolnia, hogy hány állomáscím szükséges az egyes hálózatokhoz, és hány alhálózatra van szükség.

**Változó hosszúságú alhálózati maszk (VLSM)**

Bár a hagyományos alhálózat-kialakítási módszer teljesítheti a legnagyobb LAN állomásszám igényét és kellő számú alhálózatra oszthatja a címtartományt, de valószínűleg a fel nem használt címek jelentős pazarlását is eredményezi. A VLSM lehetővé teszi egy hálózati tartomány különböző méretekre történő felosztását. A VLSM esetében az alhálózati maszk az egyes alhálózatokban kölcsönvett bitek számától függően változik, ez jelenti a „változót” a VLSM nevében. A VLSM az alhálózatok alhálózatokra bontásának elve A VLSM használatakor kezdjük mindig a legnagyobb alhálózat állomásigényeinek kielégítésével! Folytassuk addig az alhálózatokra bontást, amíg a legkisebb alhálózat állomáskövetelményei nem teljesülnek. Az alhálózatokat mindig a megfelelő bithatáron kell kezdeni.

**Strukturált tervezés**

A hálózati rendszergazdának tanulmányoznia kell a hálózati követelményeket, hogy jobban megtervezhesse az IPv4 hálózat alhálózatainak struktúráját. Ez azt jelenti, hogy megvizsgáljuk a teljes hálózatot (beleértve az intranetet és a DMZ-t egyaránt), és meghatározzuk, hogy az egyes területek miként lesznek szegmentálva. A címzési terv magában foglalja annak meghatározását, hogy hol szükséges a címek megóvása (általában a DMZ-ben), és hol van nagyobb rugalmasság (általában az intraneten belül). Ahol szükséges a címek megóvása, a tervnek meg kell határoznia, hogy hány alhálózatra és alhálózatonként hány állomásra van szükség. Ez általában a DMZ-n belüli publikus IPv4-címtartomány esetében szükséges. Ez valószínűleg magában foglalja a VLSM használatát. A címzési tervnek tartalmaznia kell, hogy miként lesznek a címek kiosztva, mely állomások igényelnek statikus IPv4-címeket, és mely állomások esetében lehet DHCP-t használni a címzési információk megszerzéséhez. A hálózaton belül különböző típusú eszközök vannak, amelyek címeket igényelnek: végfelhasználói kliensek, szerverek és perifériák, internetről elérhető szerverek, közvetítő eszközök és átjárók. Az IP-címzési terv kialakításakor célszerű egy sémát kialakítani arra, hogy miként osszuk ki a címeket az egyes eszköztípusok számára. Ez segít, amikor új eszközöket állítunk be vagy távolítunk el, amikor IP alapon szűrjük a forgalmat, vagy egyszerűen csak megkönnyíti a dokumentációt.

11.10.4

## Module Quiz - IPv4 Addressing

Az űrlap teteje

1. Milyen hosszú a hálózati előtag (prefix) a 255.255.255.224 alhálózati maszk esetében?

Az űrlap alja

Hány érvényes állomáscím érhető el egy /26 maszkkal konfigurált IPv4-alhálózaton?

Melyik alhálózati maszkot használjuk, ha 5 állomásbit áll rendelkezésre?

A hálózati rendszergazda a 192.168.10.0/24 hálózatot /26 előtagú alhálózatokra osztja. Hány egyforma méretű alhálózat jön létre?

Milyen alhálózati maszkot képvisel a /20 jelölés?

Melyik állítás igaz a változó hosszúságú alhálózati maszkolásra?

Miért hajtja végre a 3. rétegbeli eszköz az ÉS műveletet egy cél IP-címen és az alhálózati maszkon?

Hány használható IP-cím érhető el a 192.168.1.0/27 hálózaton?

Melyik alhálózati maszkot használjuk, ha pontosan 4 állomásbit áll rendelkezésre?

Melyik két részből áll egy IPv4-cím? (Két jó válasz van.)

Ha egy hálózati eszköznek /26 előtagú maszkja van, hány IP-cím érhető el az ezen a hálózaton lévő gépek számára?

Milyen típusú a 172.17.4.250/24 IP-cím?

Ha egy hálózati eszköznek /28 előtagú maszkja van, hány IP-cím érhető el az ezen a hálózaton lévő állomások számára?

Mi az alhálózati maszk célja az IP-címmel együtt?

Egy hálózati rendszergazda különböző méretű alhálózatokat hoz létre. A legkisebb alhálózat maszkja a 255.255.255.224. Hány használható állomáscímet fog tartalmazni ez az alhálózat?​

[11.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Strukturált tervezés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                     
*         

1. IPv6-címzés
2. Bevezetés

# Bevezetés

12.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az IPv6-címzésről szóló fejezetben!

Most nagyszerű alkalom kínálkozik arra, hogy hálózati rendszergazdák legyünk! Hogy miért? Mert sok hálózatban az IPv4 és az IPv6 egyszerre működik. Az IPv4-hálózatok alhálózatokra bontásának elsajátítása után (ami kemény munka volt), azt fogjuk tapasztalni, hogy az IPv6-hálózat alhálózatokra osztása sokkal könnyebb. Valószínűleg nem erre számítottunk, ugye? A modul végén található Packet Tracer feladat lehetőséget ad arra, hogy alhálózatokra bontsunk egy IPv6-hálózatot. Gyerünk, kezdjünk is bele!

12.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** IPv6-címzés

**Fejezet célja:** IPv6-címzési rendszer megvalósítása.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **IPv4-problémák** | Bemutatja az IPv6-címzés szükségességét. |
| **IPv6-címek ábrázolása** | Ismerteti az IPv6-címek felépítését. |
| **IPv6-címtípusok** | Az IPv6 hálózati címek típusainak összehasonlítása. |
| **Globális és link-local statikus címkonfiguráció** | Ismerteti a statikus globális egyedi és a link-local IPv6-címzés beállítását. |
| **Globális dinamikus címkonfiguráció** | Ismerteti az IPv6 globális egyedi címek dinamikus konfigurálását. |
| **Link-local dinamikus címkonfiguráció** | Ismerteti az IPv6 link-locali címek dinamikus konfigurálását. |
| **IPv6 csoportos címzés** | Az IPv6 multicast címek ismertetése. |
| **IPv6 alhálózatokra bontás** | IPv6-alhálózatok címzési tervének megvalósítása. |

[11.10](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-problémák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                      
*         

1. IPv6-címzés
2. IPv4-problémák

# IPv4-problémák

12.1.1

## Az IPv6 szükségessége

Már tudjuk, hogy a szabadon felhasználható IPv4-címek hamarosan elfogynak. Ezért kell megismerkedni az IPv6-tal.

Az IPv6-ot az IPv4 utódjának tervezték. Az IPv6 jóval nagyobb, 128 bites címtartományt használ, amely 340 szextillió (340 és utána 36 nulla) címet jelent. Az IPv6 azonban több, mint egy nagyobb címtér.

Amikor az IETF elkezdte az IPv4 utódjának kidolgozását, ezt a folyamatot egyben arra is felhasználta, hogy az IPv4 korlátait kijavítsa és további fejlesztéseket adjon hozzá. Példa erre az ICMPv6 (Internet Control Message Protocol version 6), amely címfeloldást és automatikus címkonfigurációt is megvalósít. Az ICMP IPv4-es változatában ilyen nem létezik.

Az IPv6-ra történő átállás motiváló tényezője az IPv4-címtér kimerülése volt. Ahogy Afrika, Ázsia és a világ más területei egyre nagyobb mértékben kapcsolódnak az internethez, ekkora mértékű növekedéshez nincs elég IPv4-cím. Az öt RIR-ből négy már kifogyott az IPv4-címekből (lásd ábra).

The graphic shows a global map of the five regional internet registries and there IPv4 exhaustion dates. ARINs IPv4 exhaustion date is July 2015, RIPE NCCs exhaustion data is September 2012, APNICs exhaustion date is June 2014, LACNICs exhaustion date is April 2011, and AfriNICs projected exhaustion date is 2020.

### RIR IPv4 Exhaustion Dates



IPv4 exhaustion date  
July 2015IPv4 exhaustion date  
September 2012IPv4 exhaustion date  
June 2014IPv4 exhaustion date  
2020IPv4 exhaustion date  
April 2011

Az IPv4-tartomány elméleti maximuma kb. 4,3 milliárd cím. A privát címek hálózati címfordítással (NAT) való kombinálása fontos szerepet játszott az IPv4-címtér kimerülésének lassításában. A NAT azonban sok alkalmazás esetében problémás, késleltetést okoz, és olyan korlátozásokkal jár, amelyek jelentősen akadályozzák a végponttól végpontig terjedő kommunikációt.

A mobileszközök egyre növekvő száma miatt a mobilszolgáltatók vezető szerepet töltenek be az IPv6-ra való áttérésben. Az Egyesült Államok két legnagyobb mobilszolgáltatója arról számolt be, hogy forgalmuk több mint 90% -a IPv6-on zajlik.

A legtöbb ismert internet- és tartalomszolgáltató, mint például a YouTube, a Facebook és a NetFlix, szintén elvégezte az áttérést. Számos vállalat, például a Microsoft, a Facebook és a LinkedIn a belső hálózatán tisztán IPv6-ra áll át. 2018-ban a Comcast nevű szélessávú internetszolgáltató több mint 65% -os, míg a brit Sky Broadcasting több mint 86% -os telepítési rátát jelentett be.

**Dolgok internete (Internet of Things, IoT)**

A mai internet lényegesen különbözik attól, mint amilyen az elmúlt évtizedekben volt. Az internet ma többet jelent e-mail üzenetek, weboldalak és fájlok számítógépek közötti átvitelénél. A folyamatosan fejlődő internet a dolgok internetévé válik. Már nem csak a számítógépek, táblagépek és okostelefonok fogják használni az internetet. A jövő érzékelőkkel felszerelt, internetre köthető eszközei közé fog tartozni minden, az autóktól és orvosi eszközöktől kezdve egészen a háztartási gépekig és a természetes ökoszisztémákig.

A növekvő internetes populáció, az IPv4-címtartomány korlátozott mérete, a NAT problémái és az IoT azt bizonyítják, hogy itt az ideje IPv6-ra váltani.

12.1.2

## Az IPv4 és az IPv6 együttélése

Az IPv6-ra váltásnak nincs rögzített határideje. Az IPv4 és az IPv6 együtt fog működni a közeljövőben, és az átmenet több évig eltart. Az IETF különféle protokollokat és eszközöket fejlesztett ki a hálózati rendszergazdák számára, hogy elősegítse az IPv6-ra történő átállást. Az áttérési technikákat három kategóriába soroljuk:

További információért kattintsunk a gombokra!

A kettős protokollkészlet lehetővé teszi az IPv4 és az IPv6 együttes működését egy hálózaton belül. A dual stack eszközök egyszerre futtatják az IPv4- és az IPv6-protokollkészletet. Ez natív IPv6 néven ismert, ami azt jelenti, hogy a hálózat IPv6-kapcsolattal rendelkezik az internetszolgáltatóhoz, és az ügyfelek képesek IPv6-on keresztül hozzáférni az interneten található tartalmakhoz.

Physical topology showing three dual stack PCs and a dual stack router

Dual Stack  
IPv4 and IPv6Dual Stack  
IPv4 and IPv6Dual Stack  
IPv4 and IPv6Dual Stack  
IPv4 and IPv6

**MEGJEGYZÉS:** Az alagút technika és a címfordítás a natív IPv6-ra való áttérést segíti, és csak szükséges esetben használandó. A cél az IPv6-alapú natív kommunikáció a forrástól a célállomásig.

12.1.3

## Tudáspróba - IPv4-problémák

Az űrlap teteje

Check your understanding of IPv4 issues by choosing the BEST answer to the following questions.

1. What is the most important motivating factor for moving to IPv6?

Az űrlap alja

True or False: 4 out of 5 RIRs no longer have enough IPv4 addresses to allocate to customers on a regular basis.

Which of the following techniques use native IPv6 connectivity?

[12.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-címek ábrázolása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                        
*         

1. IPv6-címzés
2. IPv6-címek ábrázolása

# IPv6-címek ábrázolása

12.2.1

## IPv6-címformátum

Az IPv6-hálózatok megismerésének első lépése az IPv6-os címek írásmódjának és formátumának megértése. Az IPv6-címekből sokkal több van, mint az IPv4-címekből, ezért nem valószínű, hogy kifogyunk belőlük.

Ezek a címek 128 bit hosszúak és hexadecimális értékek sorozataként írjuk fel őket. Mivel négy bit ad ki egy hexadecimális számjegyet, így a cím 32 hexadecimális számjegyből áll (lásd ábra). Az IPv6-címek esetén nem különböztetjük meg a kis- és nagybetűket, bármelyiket használhatjuk.

### 16 bites szegmensek vagy hextettek

X : X : X : X : X : X : X : X 0000 0000 0000 0000 0000 0000 0000 0000 ffff ffff ffff ffff ffff ffff ffff ffff : : : : : : : 1111 1111 1111 1111 0000 0000 0000

0000

4 hexadecimal digits = 16 binary digitstotototototototototototo

**Elsődleges formátum**

Az IPv6-címek formátuma x:x:x:x:x:x:x:x, ahol minden "x" négy hexadecimális számjegyet helyettesít. Az oktett kifejezés az IPv4-cím nyolc bitjére utal. Az IPv6 esetén egy 16 bites címrész, vagyis négy hexadecimális számjegy nem hivatalos elnevezése hextett. Minden "x" egy-egy hextettet, azaz 16 bitet, vagyis négy hexadecimális számjegyet jelent.

Az IPv6-címek elsődleges formátuma az, amikor mind a 32 hexadecimális számjegyet kiírjuk. Ez nem feltétlenül jelenti azt, hogy ez egyben az IPv6-címek megjelenítésének ideális formátuma is lenne. A következőkben megismerünk két szabályt, amelyeknek segítségével az IPv6-cím számjegyeinek száma lényegesen lerövidíthető.

Az alábbi ábra néhány példát mutat az elsődleges formátumú IPv6-címekre.

2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000: 0200   
2001 : 0db8 : 0000 : 00a3 : abcd : 0000 : 0000: 1234   
2001 : 0db8 : 000a : 0001 : c012 : 9aff : fe9a: 19ac   
2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000: 0000   
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef   
fe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001   
fe80 : 0000 : 0000 : 0000 : c012 : 9aff : fe9a: 19ac   
fe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab: cdef   
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0001   
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000: 0000

12.2.2

## Első szabály - A vezető nullák elhagyása

Az első szabály az IPv6-címek rövidítésére az, hogy a 16 bites részek vagy hextettek vezető nulláit elhagyhatjuk. Íme négy példa a vezető nullák elhagyására:

* a 01ab rövidítve 1ab
* a 09f0 rövidítve 9f0
* a 0a00 rövidítve a00
* a 00ab rövidítve ab

A szabály csak a vezető nullákra alkalmazható, a záró nullákra nem, különben a rövidítés nem lenne egyértelmű. Például az "abc" hextettről nem tudnánk eldönteni, hogy "0abc" vagy "abc0" volt-e.

### A vezető nullák elhagyása

| TypeFormatPreferred2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200No leading 0s2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200Preferred2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234No leading 0s2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234Preferred2001 : 0db8 : 000a : 0001 : c012 : 90ff : fe90 : 0001No leading 0s2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1Preferred2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000No leading 0s2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0Preferredfe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdefNo leading 0sfe80 : 0 : 0 : 0 : 123 : 4567 : 89ab : cdefPreferredfe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001No leading 0sfe80 : 0 : 0 : 0 : 0 : 0 : 0 : 1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001No leading 0s 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000No leading 0s 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 | |
| --- | --- |
| **Type** | **Format** |
| Preferred | 2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200 |
| No leading 0s | 2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200 |
|  |  |
|  |  |
| Preferred | 2001 : **0**db8 : **000**0 : **00**a3 : ab00 : **0**ab0 : **00**ab : 1234 |
| No leading 0s | 2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234 |
|  |  |
|  |  |
| Preferred | 2001 : **0**db8 : **000**a : **000**1 : c012 : 90ff : fe90 : **000**1 |
| No leading 0s | 2001 : db8 : a : 1 : c012 : 90ff : fe90 : 1 |
|  |  |
|  |  |
| Preferred | 2001 : **0**db8 : aaaa : **000**1 : **000**0 : **000**0 : **000**0 : **000**0 |
| No leading 0s | 2001 : db8 : aaaa : 1 : 0 : 0 : 0 : 0 |
|  |  |
|  |  |
| Preferred | fe80 : **000**0 : **000**0 : **000**0 : **0**123 : 4567 : 89ab : cdef |
| No leading 0s | fe80 : 0 : 0 : 0 : 123 : 4567 : 89ab : cdef |
|  |  |
|  |  |
| Preferred | fe80 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**1 |
| No leading 0s | fe80 : 0 : 0 : 0 : 0 : 0 : 0 : 1 |
|  |  |
|  |  |
| Preferred | **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**1 |
| No leading 0s | 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 |
|  |  |
|  |  |
| Preferred | **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 : **000**0 |
| No leading 0s | 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 |

12.2.3

## Második szabály - Dupla kettőspont

Az IPv6-címek rövidítésének második szabálya az, hogy bármelyik, csak nullákat tartalmazó 16 bites szegmens (hextett) sorozat helyettesíthető dupla kettősponttal (::). Például a 2001:db8:cafe:1:0:0:0:1 (a vezető nullákat kihagyva) leírható így: 2001:db8:cafe:1::1. A dupla kettőspontot (።) használjuk a három, csupa nullából álló hextett (0:0:0) helyett.

A dupla kettőspont (::) egy címen belül csak egyszer használható, különben több lehetséges cím rövidítése is ugyanaz lenne. A vezető nullák elhagyásával együtt használva az IPv6-címek mérete lényegesen lerövidülhet. Ezt időnként tömörített formátumnak hívják.

Íme egy példa a dupla kettőspont helytelen használatára: 2001:db8። abcd። 1234.

A dupla kettőspontot kétszer használtuk a fenti példában. A helytelen tömörített formátumú cím lehetséges kibontásai:

* 2001:db8::abcd:0000:0000:1234
* 2001:db8::abcd:0000:0000:0000:1234
* 2001:db8:0000:abcd::1234
* 2001:db8:0000:0000:abcd::1234

Ha egy címben egynél több egymás melletti csupa nullás hextettet is van, használjuk a dupla kettőspontot (።) a leghosszabb egybefüggő karakterlánc esetében. Ha a karakterláncok egyenlőek, az első karakterláncnál kell a kettőspontot (።) használni.

### A vezető nullák és a 0-ból álló szakaszok kihagyása

| TypeFormatPreferred2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200Compressed/spaces2001 : db8 : 0 : 1111 : : 200Compressed2001:db8:0:1111::200Preferred2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000Compressed/spaces2001 : db8 : 0 : 0 : ab00 :: Compressed2001:db8:0:0:ab00::Preferred2001 : 0db8 : aaaa : 0001 : 0000 : 0000 : 0000 : 0000Compressed/spaces2001 : db8 : aaaa : 1 ::Compressed2001:db8:aaaa:1::Preferredfe80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89ab : cdefCompressed/spacesfe80 : : 123 : 4567 : 89ab : cdefCompressedfe80::123:4567:89ab:cdefPreferredfe80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001Compressed/spacesfe80 : : 1Compressedfe80::0Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001Compressed/spaces:: 1Compressed::1Preferred0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000Compressed/spaces::Compressed:: | |
| --- | --- |
| **Type** | **Format** |
| Preferred | 2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200 |
| Compressed/spaces | 2001 : db8 : 0 : 1111 : : 200 |
| Compressed | 2001:db8:0:1111::200 |
|  |  |
| Preferred | 2001 : **0**db8 : **000**0 : **000**0 : ab00 : **0000** : **0000** : **0000** |
| Compressed/spaces | 2001 : db8 : 0 : 0 : ab00 :: |
| Compressed | 2001:db8:0:0:ab00:: |
|  |  |
| Preferred | 2001 : **0**db8 : aaaa : **000**1 : **0000** : **0000** : **0000** : **0000** |
| Compressed/spaces | 2001 : db8 : aaaa : 1 :: |
| Compressed | 2001:db8:aaaa:1:: |
|  |  |
| Preferred | fe80 : **0000** : **0000** : **0000** : **0**123 : 4567 : 89ab : cdef |
| Compressed/spaces | fe80 : : 123 : 4567 : 89ab : cdef |
| Compressed | fe80::123:4567:89ab:cdef |
|  |  |
| Preferred | fe80 : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **000**1 |
| Compressed/spaces | fe80 : : 1 |
| Compressed | fe80::0 |
|  |  |
| Preferred | **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **000**1 |
| Compressed/spaces | :: 1 |
| Compressed | ::1 |
|  |  |
| Preferred | **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** : **0000** |
| Compressed/spaces | :: |
| Compressed | :: |

12.2.4

## Tudáspróba - IPv6-címek ábrázolása

Instructions:

Convert the IPv6 addresses into short (omit the leading zeroes) and compressed forms. Enter letters in lowercase. Click Next to advance the activity to the next address.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Preferred format | **2001** | **0db8** | **ef01** | **2345** | **0678** | **0910** | **aaaa** | **bbbb** |
| Omit leading zeroes |  |  |  |  |  |  |  |  |
| Compressed format |  | | | | | | | | |

[12.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv4-problémák](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-címtípusok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                              
*         

1. IPv6-címzés
2. IPv6-címtípusok

# IPv6-címtípusok

12.3.1

## Egyedi címzés, csoportcímzés, bárki-címzés

Az IPv4-hez hasonlóan különböző típusú IPv6-címek léteznek. Három nagyobb kategória van:

* **Egyedi címek** \- (Unicast) - Ez a cím egyértelműen azonosítja egy IPv6-képes készülék valamely interfészét.
* **Csoportcímek** \- (Multicast) A csoportcím arra való, hogy egyetlen IPv6 csomagot több címzettnek is elküldjünk.
* **Bárki címek** \- (Anycast) Ez egy olyan IPv6-cím, amelyet több eszközhöz is hozzá lehet rendelni. Az anycast címre küldött csomagot ahhoz a legközelebbi eszközhöz irányítják, amelynek ez a címe. Az anycast címek használatát ebben a kurzusban nem részletezzük.

Az IPv4-gyel ellentétben az IPv6-ban nincsenek szórási címek. Viszont van egy IPv6 "minden-állomás" csoportcím (all-node multicast), amivel lényegében ugyanezt a hatást érhetjük el.

12.3.2

## IPv6 előtag (prefix) hossz

Emlékezzünk rá, hogy az IPv4-cím előtagját (prefixét) vagy hálózati részét pontokkal elválasztott decimális alhálózati maszk formájában, vagy a prefix hosszával (perjeles jelöléssel) azonosíthatjuk. Például a 192.168.1.10 IP-cím pontozott decimális alhálózati maszkja 255.255.255.0, amit így is írhatunk: 192.168.1.10/24.

Az IPv4-ben a /24-et előtagnak vagy prefixnek nevezzük. Az IPv6-ban ezt az előtag hosszának nevezik. A pontozott decimális alhálózati maszk jelölést IPv6-nál nem használjuk. Az IPv4-hez hasonlóan az előtag hossza perjeles formátumban jelenik meg, és az IPv6-cím hálózati részének azonosítására szolgál.

Az előtag hossza 0 és 128 közé eshet. A LAN-ok és a legtöbb más típusú hálózat ajánlott IPv6-előtagjának hossza /64, amint az az ábrán látható.

The graphic shows an IPv6 address divided into a 64-bit prefix and a 64-bit interface ID. The 64-bit prefix is 2001:0db8:000a:0000. The 64-bit interface ID is 0000:0000:0000:0000.

### IPv6 előtag (prefix) hossz

PrefixInterface ID0000:0000:0000:00002001:0db8:000a:000064 bit64 bitExample: 2001:db8:a::/64

Az előtag, vagyis a cím hálózatazonosító része 64 bit hosszú, ami az interfész azonosító (állomás rész) számára szintén 64 bitet hagy.

Erősen ajánlott 64 bites interfészazonosítót használni a legtöbb hálózathoz. Ennek az az oka, hogy az állapot nélküli automatikus címkonfiguráció (Stateless Address Autoconfiguration, SLAAC) 64 bitet használ az interfészazonosítóhoz. Emellett megkönnyíti az alhálózatok létrehozását és kezelését.

12.3.3

## Az IPv6 egyedi címek típusai

Az IPv6 egyedi cím egy IPv6-képes eszköz interfészét azonosítja. Az egyedi címre küldött csomagot az az interfész fogadja, amelyhez a címet rendelték. Az IPv4-hez hasonlóan a forrás IPv6-címnek is egyedi címnek kell lennie. A cél IPv6-cím lehet akár egyedi, akár multicast cím is. Az ábrán az IPv6 egyedi címek hat típusát láthatjuk néhány példával.

The graphic shows a chart of six types of IPv6 unicast addresses. From top to bottom, the types of Ipv6 addresses in the chart are: Global Unicast, Link-local, Loopback ::1/128, Unspecified ::/128, Unique local fc00::/7 - fdff::/7, and Embedded IPv4.

### IPv6 egyedi címzéses címek

::1/128 ::

fc00::/7 - fdff::/7

Global UnicastLink-localLoopbackUnspecified AddressUnique LocalEmbedded IPv4IPv6 Unicast  
Addresses

Az IPv4-eszközökkel ellentétben, amelyeknek csak egy címe van, az IPv6-interfészek általában két egyedi címmel rendelkeznek:

* **Globális egyedi cím (Global Unicast Address, GUA)** - Ez a cím a publikus IPv4-címekre hasonlít. Az ilyen címek globálisan egyedi, interneten továbbítható címek. A globális egyedi címeket konfigurálhatjuk statikusan, vagy kioszthatjuk dinamikusan is.
* **Helyi cím (Link-local address, LLA)** — Ez minden IPv6-eszközhöz szükséges. A link-local címeket az azonos helyi kapcsolaton levő eszközökkel történő kommunikációra használják. IPv6-nál a kapcsolat (link) kifejezés az alhálózatra vonatkozik. A link-local címek csak egyetlen kapcsolatra korlátozódnak. Az egyediségüket csak a kapcsolaton belül kell biztosítani, mert azon túlra nem továbbítódnak. Vagyis a forgalomirányítók link-local forrás- vagy célcímekkel rendelkező csomagokat nem továbbítanak más hálózatba.

12.3.4

## Megjegyzés az egyedi helyi címről

Az egyedi helyi (unique local) címeket (tartományuk fc00። /7 és fdff። /7 közé esik) még nem implementálták általánosan. Ezért ez a modul csak a GUA és LLA konfigurációval foglalkozik. Előfordulhat azonban, hogy egyedi helyi címeket használnak olyan eszközök kezelésére, amelyekhez kívülről nem szabad hozzáférni, ilyenek például a belső kiszolgálók és nyomtatók.

Az IPv6 egyedi helyi címek mutatnak némi hasonlóságot az IPv4 RFC 1918 privát címeivel, de van néhány lényeges különbség is közöttük.

* Az egyedi helyi címeket helyi címzésre használják egy adott telephelyen vagy korlátozott számú telephely között.
* Ezek a címek használhatók olyan eszközökhöz, amelyeknek soha nem kell hozzáférniük egy másik hálózathoz.
* Az egyedi helyi címeket a rendszer nem irányítja és nem fordítja át globális IPv6-címre.

**MEGJEGYZÉS**: Számos telephely az RFC 1918 címek privát tulajdonságát használja ki arra is, hogy biztonságosabbá tegye a hálózatát, vagy elrejtse azt a biztonsági támadások elől. Ezeknek a technológiáknak azonban nem ez a célja. Az IETF javaslata szerint a megfelelő biztonsági megoldásokat az internetre kapcsolódó routeren kell megvalósítani.

12.3.5

## IPv6 globális egyedi cím

Az IPv6 globális egyedi címzésű címek (GUA) a teljes címtérben egyediek, és továbbíthatók az interneten. Ezek a publikus IPv4-címek megfelelői. Az ICANN (Internet Committee for Assigned Names and Numbers) és az IANA (Internet Assigned Numbers Authority) üzemeltetői osztják ki az IPv6-címblokkokat az öt RIR számára. Jelenleg csak azokat a globális egyedi címeket osztják ki, amelyek első három bitje 001 (2000::/3), ahogy az ábrán látható.

Az ábra az első hextett értéktartományát mutatja, ahol a jelenleg rendelkezésre álló GUA-k első hexadecimális számjegye 2-vel vagy 3-mal kezdődik. Ez az elérhető IPv6-címtartománynak csupán az 1/8 része, kivéve egy egészen kis részt, amit más típusú egyedi és csoportos címzés használ.

**MEGJEGYZÉS**: A 2001:0DB8::/32 címet dokumentációs célokra tartják fenn, beleértve a példákban való használatot is.

The graphic shows the three parts of a GUA: First is the global routing prefix, then the Subnet ID, then finally the Interface ID. The first three bits of the Global routing prefix are 001. The Range of the first hextext is shown to be from 0010 0000 0000 0000 (2000) to 0011 1111 1111 1111 (3fff)

0010 0000 0000 0000 (2000) 0011 1111 1111 1111 (3fff)

001

Interface IDSubnet IDGlobal Routing PrefixRange of first hextet:to

A következő ábra egy globális egyedi cím szerkezetét és hatókörét mutatja.

The graphic shows the three parts of a GUA: First is the global routing prefix which is 48 bits in length, then the Subnet ID which is 16 bits in length, then finally the Interface ID which is 64 bits in length. Text under the graphic states A /48 routing prefix + 16 bit Subnet ID = /64 prefix.

### IPv6-cím /48 globális útválasztási előtaggal és /64 előtaggal

48 bit16 bit64 bitA /48 routing prefix + 16 bit Subnet ID = /64 prefix.64 bitInterface IDSubnet ID Global Routing Prefix

Egy globális egyedi cím három részből áll:

* Globális útválasztási előtag
* Alhálózat azonosító
* Interfész azonosító

12.3.6

## IPv6 globális egyedi cím felépítése

**Globális útválasztási előtag**

A globális útválasztási előtag vagy hálózati rész a cím azon része, amelyet az internetszolgáltató (ISP) rendel hozzá egy ügyfélhez vagy telephelyhez. Az internetszolgáltatók általában egy /48 globális útválasztási előtagot rendelnek ügyfeleikhez. A globális útválasztási előtag általában az internetszolgáltató belső szabályaitól függően változik.

Az előző ábrán egy /48 globális útválasztási előtagot használó GUA látható. A /48-as a leggyakrabban kiosztott globális előtag, a kurzus folyamán a legtöbb példában ezt fogjuk használni.

Például a 2001:DB8:ACAD::/48 IPv6-cím azt jelenti, hogy az első 48 bit (3 hextett) (2001:DB8:ACAD) a cím előtagja vagy hálózati része. A /48 prefix hossz előtti dupla kettőspont azt jelenti, hogy a cím további része csupa 0. A globális útválasztási előtag mérete határozza meg az alhálózati azonosító (subnet ID) méretét.

**Alhálózat azonosító**

Az alhálózat azonosító mező a globális útválasztási előtag és az interfészazonosító közötti terület. Az IPv4-től eltérően, ahol az alhálózatok létrehozásához biteket kellett kölcsönvenni az állomásazonosító részből, az IPv6-ot a könnyebb alhálózatokra való bontás szem előtt tartásával tervezték. Az alhálózat azonosítót a szervezet a saját telephelyén belüli alhálózatok azonosítására használhatja. Minél nagyobb az alhálózati azonosító, annál több alhálózat áll rendelkezésre.

**MEGJEGYZÉS**: Számos szervezet kap /32 globális útválasztási előtagot. A 64 bites interfészazonosító létrehozása után ilyenkor 32 bites alhálózati azonosító marad a címen belül. Ez azt jelenti, hogy egy /32 globális útválasztási előtaggal és egy 32 bites alhálózati azonosítóval rendelkező szervezet 4,3 milliárd alhálózattal rendelkezik, mindegyik alhálózaton 18 kvintillió eszközzel. Ez annyi alhálózat, mint a teljes nyilvános IPv4-címtartomány!

Az előző ábrán szereplő IPv6-cím /48 globális útválasztási előtaggal rendelkezik, amely gyakori sok vállalati hálózatnál. Ez különösen megkönnyíti a cím különböző részeinek vizsgálatát. Egy tipikus /64-es prefix hossz esetén a globális egyedi címben az első négy hextett a cím hálózati része, amiből a negyedik az alhálózat azonosító. A maradék négy hextett pedig az interfész azonosító.

**Interfész azonosító**

Az IPv6 interfész azonosító az IPv4-cím állomás részének felel meg. Azért hívjuk interfész azonosítónak, mert egyetlen állomásnak több interfésze is lehet, és mindegyik interfész rendelkezhet több IPv6-címmel is. Az ábra egy IPv6 globális egyedi cím szerkezetére mutat példát. A legtöbb esetben ajánlott /64-es alhálózatot használni, ami 64 bites interfészazonosítót hoz létre. A 64 bites interfészazonosító alhálózatonként 18 kvintillió eszköz vagy hoszt címzését teszi lehetővé.

A /64-es alhálózat vagy előtag (globális útválasztási előtag + alhálózati azonosító) 64 bitet hagy az interfész azonosítójának. Ez azért ajánlott, hogy lehetővé tegyük az SLAAC-kompatibilis eszközök számára saját 64 bites interfészazonosító létrehozását. Emellett egyszerűvé és hatékonyabbá teszi az IPv6-címzési terv kidolgozását.

**MEGJEGYZÉS**: Az IPv4-től eltérően az IPv6-ban a csupa 0-ás és a csupa 1-es állomáscímek is hozzárendelhetők egy eszközhöz. A csupa 1-es cím azért használható, mert a szórási címeket nem használják az IPv6-on belül. A csupa nullás cím viszont fenntartott, ez az alhálózati router anycast címe, ezt csak routereknek lehet kiosztani.

12.3.7

## IPv6 link-local cím

Az IPv6 link-local címek (LLA) lehetővé teszik, hogy az eszköz más IPv6-eszközökkel kommunikáljon ugyanazon a kapcsolaton, de csakis azon az egy kapcsolaton (alhálózaton) belül. Azok a csomagok, amelyeknek a forrása vagy célja link-local cím, nem továbbíthatók a kiindulási kapcsolaton kívülre.

Míg a globális egyedi cím megléte nem alapkövetelmény, viszont minden IPv6 hálózati interfésznek rendelkeznie kell egy link-local címmel.

Ha az interfészen nem állítunk be kézzel link-local címet, az eszköz automatikusan létrehoz magának egyet DHCP-szerver nélkül is. Az IPv6-állomások akkor is létrehoznak maguknak IPv6 link-local címet, ha globális egyedi címet nem rendeltünk az eszközhöz. Ez lehetővé teszi, hogy azonos alhálózaton belül az IPv6-eszközök kommunikálhassanak egymással. Ebbe az alapértelmezett átjáróval (routerrel) való kommunikáció is beletartozik.

Az IPv6 link-local címtartomány az fe80። /10. A /10 azt jelenti, hogy az első 10 bit 1111 1110 10xx xxxx. Az első hextett 1111 1110 10**00 0000** (fe80) és 1111 1110 10**11 1111** (febf) közé esik.

Az ábra egy IPv6 link-local címekkel zajló kommunikációra mutat példát. A számítógép közvetlenül képes kommunikálni a nyomtatóval az LLA segítségével.

Physical topology showing two PCs, a server, a printer, a switch, and a router. It depicts that link-local communications are not routed outside the network.

### IPv6 link-local kommunikáció

fe80::bbbb/64 fe80::cccc/64 fe80::dddd/64 fe80::1/64 fe80::aaaa fe80::dddd

fe80::aaaa/64

Source IPv6 AddressDestination IPv6 AddressIPv6 Packet

A következő ábra az IPv6 LLA-k egyes felhasználási területeit mutatja be.

The graphic shows two routers connect by a link with their LLA addresses. The number 1 with a bidirectional arrow pointing to each router is over the link along with the text Routing Protocol Messages. A PC is connected to the router on the left with a number 2 an arrow pointing from the PC to the router. Text under the graphic reads 1. Routers use the LLA of neighbor routers to send routing updates. 2. Hosts use the LLA of a local router as the default-gateway.

1

2

Routing Protocol  
MessagesLLA  
AddressLLA  
AddressLLA  
Address

1. A routerek a szomszédos routerek LLA-ját használják irányítási frissítések küldésére.
2. A hosztok a helyi router LLA-ját használják alapértelmezett átjáróként.

**MEGJEGYZÉS**: Általában a router link-local címe az, amit az eszközök egy kapcsolatban alapértelmezett átjáróként használnak, nem pedig a globális egyedi címe.

Egy eszköz kétféleképpen szerezhet be egy link-local címet:

* **Statikusan** - Ez azt jelenti, hogy az eszközt manuálisan konfigurálják.
* **Dinamikusan** - Ez azt jelenti, hogy az eszköz véletlenszerűen generált értékek használatával vagy az EUI-módszerrel (Extended Unique Identifier) hozza létre saját interfészazonosítóját, amely a kliens MAC-címét és további biteket használ fel.

12.3.8

## Tudáspróba - IPv6-címtípusok

Az űrlap teteje

Check your understanding of IPv6 address types by choosing the correct answer to the following questions.

1. What is the recommended prefix length for most IPv6 subnets?

Az űrlap alja

Which part of a GUA is assigned by the ISP?

Which type of IPv6 unicast address is not routable between networks?

True or false? The Subnet ID field in an GUA must borrow bits from the interface ID.

What type of IPv6 address begins with fe80?

[12.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-címek ábrázolása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[GUA és LLA statikus konfigurálása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                
*         

1. IPv6-címzés
2. GUA és LLA statikus konfigurálása

# GUA és LLA statikus konfigurálása

12.4.1

## Globális egyedi cím statikus konfigurációja egy routeren

Amint azt az előző témakörben megtudtuk, az IPv6 GUA-k megegyeznek a nyilvános IPv4-címekkel. Globálisan egyediek és továbbíthatók az interneten. Egy IPv6 LLA csak azt teszi lehetővé, hogy két IPv6-eszköz ugyanazon a linken (alhálózaton) belül kommunikáljon egymással. Az IPv6 GUA-k és az LLA-k statikus konfigurálása egyszerű művelet a routereken. Ebben a részben megtanuljuk, hogyan kell ezt végrehajtani.

A legtöbb Cisco IOS konfigurációs és ellenőrző parancs IPv6-os megfelelője hasonló az IPv4-es változathoz. Sok esetben mindössze annyi a különbség, hogy az **ipv6** használatos az **ip** helyett a parancsokon belül.

Például, a Cisco IOS-parancs egy IPv4-cím beállításához egy interfészen: **ip address** ip-cím netmaszk. Ezzel szemben az IPv6 GUA konfigurálásának parancsa: **ipv6 address** ipv6-cím/prefix-hossz.

Figyeljük meg, hogy nincs szóköz a ipv6-cím és a prefix-hossz között.

A minta konfiguráció az ábrán lévő topológiát használja a következő IPv6-alhálózatokkal:

* 2001:db8:acad:1:/64
* 2001:db8:acad:2:/64
* 2001:db8:acad:3:/64

The graphic shows two PCs, PC1 and PC2. PC1 is connected to a switch and has the IPv6 address 2001:db8:acad:1::10/64. PC2 is connected to a switch and has the IPv6 address 2001:db8:acad:2::10/64. The two switches are connected to a router, R1. PC1 is connected through the switch to R1s G0/0/0 interface which has IPv6 address 2001:db8:acad:1::1/64. PC2 is connected through the switch to R1s G0/0/1 interface which has IPv6 address 2001:db8:acad:2::1/64. R1 connects to the cloud through its S0/1/0 interface which has IPv6 address 2001:db8:acad:3::1/64.

### Minta topológia

R1 ::10 ::10 S0/1/0::1 PC1 PC2 2001:db8.acad:2::/64 2001:db8.acad:1::/64 2001:db8.acad:3::/64 G0/0/0::1 G0/0/1::1

R1

A következő példa bemutatja az IPv6 GUA konfigurálásához szükséges parancsokat az R1 Gigabitethernet 0/0/0, Gigabitethernet 0/0/1 és Serial 0/1/0 interfészén.

### IPv6 globális egyedi címkonfiguráció az R1 routeren

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ipv6 address 2001:db8:acad:2::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1/0**

R1(config-if)# **ipv6 address 2001:db8:acad:3::1/64**

R1(config-if)# **no shutdown**

12.4.2

## Globális egyedi cím statikus konfigurációja egy Windows rendszerben

Egy állomás IPv6-címének beállítása hasonló, mintha IPv4-címet adnánk meg.

A PC1-hez konfigurált alapértelmezett átjárócím 2001:db8:acad:1። 1 (lásd ábra). Ez az R1 Gigabitethernet interfészének GUA-címe ugyanazon a hálózaton. Másik megoldás, ha az alapértelmezett átjárócím az R1 Gigabitethernet interfész linl-local címe. A legtöbb esetben a router LLA-címét használják alapértelmezett átjárócímként. Bármelyik konfiguráció működőképes.

The graphic shows the Windows Internet Protocol Version 6 (TCP/IPv6) Prosperities window. The Use the following IPv6 address button is selected. The IPv6 address is 2001:db8:acad:1::1. The Subnet prefix length is 64. The Default gateway is 2001:db8:acad:1::1. The Use the following DNS server address button is selected.



Ugyanúgy, mint az IPv4-nél, a nagyobb hálózatokban nem praktikus a klienseket statikusan címezni. Emiatt a legtöbb rendszergazda az IPv6-címek dinamikus hozzárendelését alkalmazza.

Két módszer van egy eszköz IPv6 globális egyedi címének automatikus beállítására:

* SLAAC (Stateless Address Autoconfiguration, állapotmentes automatikus címkonfiguráció)
* Állapottartó DHCPv6

A SLAAC és a DHCPv6 leírásával a következő témakör foglalkozik.

**MEGJEGYZÉS**: DHCPv6 vagy SLAAC használata esetén a router link-local címe lesz az alapértelmezett átjárócím.

12.4.3

## Link-local egyedi cím statikus konfigurációja

A link-local címek kézi konfigurációja lehetővé teszi, hogy könnyen felismerhető és megjegyezhető címeket válasszunk. A router kézi beállítása általában csak a könnyen felismerhető LLA-k létrehozása miatt szükséges. Ez azért előnyös, mert a router LLA-k alapértelmezett átjárócímként és router hirdetési üzenetekben használatosak.

Az LLA-k manuálisan konfigurálhatók az **ipv6 address** ipv6-link-local-cím **link-local** paranccsal. Amikor egy cím az fe80 - febf hextett tartománnyal kezdődik, a **link-local** paraméternek kell követnie azt.

Az ábrán egy minta topológia látható az egyes interfészek LLA-adataival.

The graphic shows two PCs, PC1 and PC2. PC1 is connected to a switch and has the IPv6 address 2001:db8:acad:1::10/64. PC2 is connected to a switch and has the IPv6 address 2001:db8:acad:2::10/64. The two switches are connected to a router, R1. PC1 is connected through the switch to R1s G0/0/0 interface which has IPv6 address 2001:db8:acad:1::1/64 and the LLA address of fe80::1:1. PC2 is connected through the switch to R1s G0/0/1 interface which has IPv6 address 2001:db8:acad:2::1/64 and the LLA address of fe80::2:1. R1 connects to the cloud through its S0/1/0 interface which has IPv6 address 2001:db8:acad:3::1/64 and the LLA address of fe80::3:1.

### Minta topológia link-local címekkel

R1 ::10 ::10 S0/1/0::1fe80::3:1 PC1 2001:db8.acad:2::/64 2001:db8.acad:1::/64 2001:db8.acad:3::/64 G0/0/0::1fe80::1:1 G0/0/1::1fe80::2:1 PC2

R1

Az alábbi példában az R1 router LLA-konfigurációja látható

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **ipv6 address fe80::1:1 link-local**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ipv6 address fe80::2:1 link-local**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1/0**

R1(config-if)# **ipv6 address fe80::3:1 link-local**

R1(config-if)# **exit**

A statikusan konfigurált LLA-kat arra használják, hogy könnyebben felismerhetővé tegyék az R1 routerhez való tartozásukat. Ebben a példában az R1 router összes interfésze egy **fe80::1:**n betűvel kezdődő LLA és egy egyedi jobb szélső „n” számjeggyel lett konfigurálva. A „**1**” az R1 routert képviseli.

Ugyanazt a szintaxist követve, mint az R1 routeren, ha a topológia tartalmazná az R2 routert, akkor három interfészén így lennének konfigurálva az LLA-k: fe80። 2:1, fe80። 2:2 és fe80። 2:3.

**MEGJEGYZÉS**: Konfigurálható pontosan ugyanaz az LLA minden egyes linken, amennyiben az egyedi a kapcsolaton belül. Ez azért lehetséges, mert a link-local interfészcímnek csak a kapcsolaton belül kell egyedinek lennie. Az általános gyakorlat azonban az, hogy másik LLA-t hozunk létre a router minden egyes interfészén, hogy megkönnyítsük a router és az adott interfész azonosítását.

12.4.4

## Parancsszimulátor - GUA és LLA statikus konfigurációja

Állítsunk be IPv6 globális és link-local címeket az R1 router megadott interfészeihez.

The graphic shows two PCs, PC1 and PC2. PC1 is connected to a switch and has the IPv6 address 2001:db8:acad:1::10/64. PC2 is connected to a switch and has the IPv6 address 2001:db8:acad:2::10/64. The two switches are connected to a router, R1. PC1 is connected through the switch to R1s G0/0/0 interface which has IPv6 address 2001:db8:acad:1::1/64 and the LLA address of fe80::1:1. PC2 is connected through the switch to R1s G0/0/1 interface which has IPv6 address 2001:db8:acad:2::1/64 and the LLA address of fe80::2:1. R1 connects to the cloud through its S0/1/0 interface which has IPv6 adress 2001:db8:acad:3::1/64 and the LLA address of fe80::3:1.

R1 ::10 ::10 S0/1/0::1fe80::3:1 PC1 2001:db8.acad:2::/64 2001:db8.acad:1::/64 2001:db8.acad:3::/64 G0/0/0::1fe80::1:1 G0/0/1::1fe80::2:1 PC2

R1

Configure and activate IPv6 on the Gigabit Ethernet 0/0/0 interface with the following addresses:

* Use **g0/0/0** as the interface name
* LLA - fe80::1:1
* GUA - 2001:db8:acad:1::1/64
* Activate the interface
* Exit interface configuration mode

R1(config)#interface g0/0/0

R1(config-if)#ipv6 address fe80::1:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:1::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up

R1(config-if)#exit

Configure and activate IPv6 on the Gigabit Ethernet 0/0/1 interface with the following addresses:

* Use **g0/0/1** as the interface name
* LLA - fe80::2:1
* GUA - 2001:db8:acad:2::1/64
* Activate the interface
* Exit interface configuration mode

R1(config)#interface g0/0/1

R1(config-if)#ipv6 address fe80::2:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:2::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit

Configure and activate IPv6 on the serial 0/1/0 interface with the following addresses:

* Use **s0/1/0** as the interface name
* GUA - 2001:db8:acad:3::1/64
* LLA - fe80::1:3
* Activate the interface
* Exit interface configuration mode

R1(config)#interface s0/1/0

R1(config-if)#ipv6 address fe80::3:1 link-local

R1(config-if)#ipv6 address 2001:db8:acad:3::1/64

R1(config-if)#no shutdown

%LINK-3-UPDOWN: Interface Serial0/1/0, changed state to up

R1(config-if)#exit

R1(config)#

You successfully configured IPv6 GUAs on the interfaces of router R1.

[12.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-címtípusok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Globális IPv6-címek dinamikus konfigurációja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                      
*         

1. IPv6-címzés
2. Globális IPv6-címek dinamikus konfigurációja

# Globális IPv6-címek dinamikus konfigurációja

12.5.1

## RS- és RA-üzenetek

Ha nem szeretnénk statikusan konfigurálni az IPv6 GUA-kat, nem kell aggódnunk. A legtöbb eszköz dinamikusan kapja meg ezeket a címeket. Ez a témakör ismerteti, hogyan működik a folyamat a router hirdetés (Router Advertisement, RA) és a router keresés (Router Solicitation, RS) üzenetekkel. A témakör meglehetősen technikai jellegű, de fontos megértenünk a különbséget a három módszer között, amelyet egy router hirdetmény használhat. Valamint azt is, hogy az EUI-64 interfészazonosító létrehozásának folyamata eltér egy véletlenszerűen generált folyamattól. Ha sikerül, akkor hatalmas ugrást tettünk az IPv6-szakértőség felé!

A GUA esetében az eszköz dinamikusan szerzi meg a címet ICMPv6-üzeneteken (Internet Control Message Protocol version 6) keresztül. Az IPv6-routerek rendszeres időközönként küldenek ki ICMPv6 RA-üzeneteket a hálózat minden IPv6-eszközének. Szintén egy RA-üzenetet küld válaszul egy ICMPv6 RS-üzenetet küldő hoszt számára, amely RA-információkat kért. Mindkét üzenet az ábrán látható.

The graphic shows LAN with a host sending an RS message towards are router and the router sending an RA message in return towards the PC. Also on the LAN is a DHCPv6 Server. Text under the gaphic reads 1. RS messages are sent to all IPv6 routers by hosts requesting addressing information. 2. RA messages are sent to all IPv6 nodes. If Method 1 (SLAAC only) is used, the RA includes the prefix, refix-lenght and default-gateway information.

### ICMPv6 RS- és RA-üzenetek

1

2

RA MessagesRS Messages**DHCPv6  
Server**

1. Az RS-üzeneteket a címzési információkat kérő állomások küldik az összes IPv6-router felé.
2. Az RA-üzeneteket az összes IPv6-eszköz megkapja. Ha a SLAAC-módszert használjuk, akkor az RA a hálózati előtagot, az előtag hosszát és az alapértelmezett átjáróinformációt tartalmazza.

Az RA-üzenetek az IPv6-router Ethernet interfészein jelennek meg. A routeren engedélyezni kell az IPv6-forgalomirányítást, amely alapértelmezés szerint ki van kapcsolva. Az IPv6-útválasztás engedélyezéséhez az **ipv6 unicast-routing** globális konfigurációs parancsot kell használni.

Az ICMPv6 RA-üzenet megoldás arra nézve, hogyan szerezzen be egy eszköz IPv6 globális címet. A végső döntés az eszköz operációs rendszerén múlik. Az ICMPv6 RA-üzenet a következőket tartalmazza:

* **Hálózati előtag és előtag hossz** - Ez megmondja az eszköznek, hogy melyik hálózathoz tartozik.
* **Alapértelmezett átjáró cím** - Ez egy IPv6 link-local cím, az RA-üzenet forrásának IPv6-címe.
* **DNS-címek és tartománynév** - Ezek a DNS-kiszolgálók és a tartománynév címei.

Az RA-üzenetek felhasználására három módszer létezik:

* **SLAAC** \ - „Mindenem megvan, amire szükséged van, beleértve az előtagot, az előtag hosszát és az alapértelmezett átjárócímet.”
* **SLAAC állapot nélküli DHCPv6-kiszolgálóval** - „Itt vannak az én információim, de más információkat, például DNS-címeket kell beszerezned egy állapot nélküli DHCPv6-kiszolgálótól.”
* **Állapotartó DHCPv6 (nincs SLAAC)** - „Megadhatom az alapértelmezett átjáró címét. Minden egyéb információt meg kell kérdezni egy állapottartó DHCPv6-kiszolgálótól.”

12.5.2

## SLAAC

A SLAAC egy olyan módszer, amely lehetővé teszi a készülék számára, hogy saját GUA-t hozzon létre a DHCPv6 szolgáltatásai nélkül. SLAAC használatakor az eszköz a helyi router ICMPv6 RA-üzeneteiből szerzi be a szükséges információkat.

Alapértelmezés szerint az RA-üzenet azt javasolja, hogy a fogadó eszköz az RA-üzenetben található információkat használja fel a saját IPv6 címzési információ létrehozásához. Ehhez DHCPv6-kiszolgáló szolgáltatásai nem szükségesek.

A SLAAC állapot nélküli, tehát nincs központi szerver (például egy állapottartó DHCPv6-szerver), amely kiosztja a GUA-kat, és listát tart fenn az eszközökről és címeikről. A SLAAC esetén a kliens eszköz az RA-üzenetben található információkat használja a saját globális címének létrehozásához. Amint az az ábrán látható, a cím két része a következőképpen jön létre:

* **Előtag** - Ezt az RA-üzenetben hirdetik.
* **Interfész ID** - EUI-64 folyamat révén, vagy véletlenszerű 64 bites számként jön létre, az eszköz operációs rendszerétől függően.

The graphic shows LAN with a router sending an ICMPv6 Router Advertisement message towards a PC. The PC has the IPv6 address of 2001:db8:acad:1:fc99:47ff:fe75:cee0/64. The is a graphic indicating that the network prefix recieved in the RA message is 2001:db8:acad:1: and the Interface ID which was created by the client device EUI-64 or random 64-bit number is fc99:47ff:fe75:cee0. Text under the graphic reads 1. The router sends an RA message with the prefix for the local link. 2. The PC uses SLAAC to obtain a prefix from the RA message and creates its own Interface ID.

/64 2001:db8:acad:1::/64 2001:db8:acad:1:fc99:47ff:fe75:cee0/64 2001:db8:acad:1: fc99:47ff:fe75:cee0 1

2

ICMPv6 Router  
AdvertisementRA MessageCreated by client device  
EUI-64 or random 64-bit numberPrefixInterface ID

1. A router RA-üzenetet küld a helyi kapcsolat előtagjával.
2. A számítógép az SLAAC segítségével szerzi meg az előtagot az RA-üzenetből, és létrehozza saját interfész-azonosítóját.

12.5.3

## SLAAC és állapot nélküli DHCPv6

Egy interfész beállítható úgy, hogy router hirdetést küldjön SLAAC és állapot nélküli DHCPv6 együttes használatával.

Amint az az ábrán látható, ezzel a módszerrel az RA-üzenet az eszközök számára a következőket nyújtja:

* SLAAC a saját IPv6 GUA létrehozásához
* A router LLA, amely az RA-üzenet forrás IPv6-címe, mint alapértelmezett átjáró cím
* Állapot nélküli DHCPv6-kiszolgáló, más információk, például DNS-szerver cím és tartománynév a beszerzésére

**MEGJEGYZÉS**: Az állapot nélküli DHCPv6-kiszolgáló kiosztja a DNS-szerverek címeit és a tartományneveket. Viszont nem osztja ki a globális egyedi címeket.

The graphic shows LAN with a PC that is sending an RS Messages (labled #1) to the router. The router is sending in return an RA message (labled #2). The PC is also sending a DHCPv6 Solicit message (labled #3) to a stateless DHCPv6 server. Text under the graphic reads 1. The PC sends an RS to all IPv6 routers, I need addressing information. 2. The router sends an RA message to all IPv6 nodes with Method 2 (SLAAC and DHCPv6) specified. Here is your prefix prefix-length, and default gateway information. but you will need to get DNS information form a DHCPv6 server. 3. The PC sends a DHCPv6 solicit message to all DHCPv6 servers. I used SLAAC to create my IPv6 address and get my default gateway address but I need other information from a stateless DHCPv6 server.

1 2

3

RA MessageRS Message**Stateless DHCPv6 Server**DHCPv6 Solicit

1. A számítógép RS-kérést küld minden IPv6-routernek: „Címzési információra van szükségem”.
2. A router kiküld egy RA-üzenetet minden IPv6-állomásnak, benne megadva a címzési módszert (SLAAC + DHCPv6). "Itt van az előtag, az előtag hossza és az alapértelmezett átjáró. De a DNS-adatokat egy DHCPv6-kiszolgálóról kell beszerezni.”
3. A számítógép DHCPv6-kérés (solicit) üzenetet küld az összes DHCPv6-kiszolgálónak. „A SLAAC-t használtam az IPv6-cím létrehozásához és az alapértelmezett átjárócím megszerzéséhez, de más információkra is szükségem van egy állapot nélküli DHCPv6-kiszolgálótól."

12.5.4

## Állapottartó DHCPv6

Egy router interfész konfigurálható úgy, hogy RA-t küldjön kizárólag az állapottartó (stateful) DHCPv6 használatára.

Az állapottartó DHCPv6 nem sokban különbözik a DHCPv4-től. Az eszköz automatikusan megkaphatja a címzési információkat (globális egyedi cím, előtag hossz, alapértelmezett átjáró, DNS-szerverek címei) egy DHCPv6-szerver szolgáltatásainak segítségével.

Amint az az ábrán látható, ezzel a módszerrel az RA-üzenet az eszközök számára a következőket nyújtja:

* A router LLA, amely az RA-üzenet forrás IPv6-címe, mint alapértelmezett átjáró cím
* Állapottartó DHCPv6-kiszolgáló a GUA, a DNS-szerver címének, a tartománynévnek és az egyéb szükséges információknak a megszerzéséhez.

The graphic shows LAN with a PC that is sending (labled #1) to a router. The router is sending a message (labled #2) to the PC. The PC is also sending a message (labled #3) to s server. Text under the graphic reads 1. The PC sends an RS to all IPv6 routers, I need addressing information. 2. The router sends an RA message to all IPv6 nodes with Method 3 (statefull DHCPv6) specified I am your default gateway, but you need to ask a statefull DHCPv6 server for your IPv6 addressign information. 3. The PC sends a DHCPv6 solicit message to all DHCPv6 servers, I received my default gateway address from the RA message, but I need an IPv6 address and all other addressing information from a stateful DHCPv6 server.

1 2

3

RA MessageRS Message**Stateful DHCPv6 Server**DHCPv6 Solicit

1. A számítógép RS-t küld minden IPv6-routernek: „Címzési információra van szükségem”.
2. A router RA-üzenetet küld minden IPv6-eszköznek, hogy állapottartó DHCPv6 van érvényben: „Én vagyok az alapértelmezett átjáró, de meg kell kérdezni egy állapottartó DHCPv6-kiszolgálót az IPv6-cím és egyéb címzési információk megszerzése érdekében."
3. A számítógép DHCPv6-kérés üzenetet küld az összes DHCPv6-kiszolgálónak, "Megkaptam az alapértelmezett átjárócímet az RA-üzenetből, de szükségem van egy IPv6-címre és minden más címzési információra egy állapottartó DHCPv6-kiszolgálótól."

Egy állapottartó DHCPv6-kiszolgáló kiosztja IPv6-címeket és karbantartja az azokat igénybe vevő eszközök listáját. Az IPv4 DHCP-je is állapottartó.

**MEGJEGYZÉS:** Az alapértelmezett átjárócím csak az RA-üzenetből érhető el dinamikusan. Az állapot nélküli és az állapottartó DHCPv6-kiszolgáló nem adja meg az alapértelmezett átjárócímet.

12.5.5

## EUI-64 módszer, vagy véletlenszerű generálás

Ha az RA-üzenetben SLAAC, vagy SLAAC állapot nélküli DHCPv6-tal szerepel, akkor az ügyfélnek saját interfészazonosítót kell létrehoznia. Az ügyfél ismeri a cím előtagját az RA-üzenetből, de létre kell hoznia saját interfészazonosítóját. Az interfész-azonosító az EUI-64 folyamattal vagy véletlenszerűen generált 64 bites számmal hozható létre, amint az ábrán látható.

The graphic shows a router sending an ICMPv6 Router Advertisement message (labled #1) to a PC. The PC is shown in a step labled #2 creating its /64 prefix from the RA messageand creating its interface ID using EUI-64 or random 64-bit number. Text under the graphic reads 1. The router sends and RA message. 2. The PC uses the prefix in the RA message and uses either EUI-64 or a random 64-bit number to generate an interface ID

### Interfész azonosító dinamikus létrehozása

/64 1

2

ICMPv6 Router AdvertisementFrom RA MessageCreated by client devicePrefixInterface IDEUI-64 or random 64-bit number

1. A router RA-üzenetet küld.
2. A számítógép felhasználja az RA-üzenetből az előtagot, majd EUI-64 vagy véletlen 64 bites számot használ az interfészazonosító létrehozásához.

12.5.6

## Az EUI-64 módszer

Az IEEE meghatározott egy EUI-64 nevű folyamatot (Extended Unique Identifier, kiterjesztett egyedi azonosító). A művelet a kliens 48 bites Ethernet MAC-címének közepébe beszúr további 16 bitet, így állítja elő a 64 bites interfész azonosítót.

Az Ethernet MAC-címeket legtöbbször hexadecimális formában ábrázolják és két részből állnak:

* **Egyedi szervezetazonosító (Organizationally Unique Identifier, OUI)** - Az OUI az IEEE által kiosztott 24 bites gyártói kód (6 hexadecimális számjegy).
* **Eszközazonosító** - Az eszközazonosító szintén 24 bit (6 hexadecimális számjegy), az OUI-n belül egyedi.

Az EUI-64 interfészazonosító bináris ábrázolása három részből áll:

* A kliens MAC-címének 24 bites OUI-része, amelyben a hetedik bitet megfordítjuk (U/L bit, univerzális/helyi). Tehát ha a hetedik bit 0, akkor 1 lesz és fordítva.
* 16 bites FFFE (hexadecimális) érték, ezt illesztjük be középre.
* Végül a MAC-cím 24 bites eszközazonosító része.

Az EUI-64 folyamatot az ábra mutatja be az R1 Gigabit Ethernet MAC-címével, ami FC99:4775:CEE0.

The graphic shows the steps in the EUI-64 process. At the top of the graphic is the MAC address fc:99:47:75:ce:e0. In step 1: Split the MAC address, The first 24-bits of the OUI fc:99:47 in binary is 1111 1100 1001 1001 0100 0111. The final 24-bits of the device identifiere 75:ce:e0 in binary is 1111 0101 1100 1110 1110 0000. Instep 2: Insert ffee the binary representation becomes 1111 1100 1001 1001 0100 0111 1111 1111 1111 1110 1111 0101 1100 1110 1110 0000. In step three Flip the u/l bit. the 7th bit from the left is changed from a 0 to a 1. The address in binary is now 1111 1110 1001 1001 0100 0111 1111 1111 1111 1110 1111 0101 1100 1110 1110 0000. The modified EUI-64 Interface ID in Hexadecimal notation is now: fe:99:47:ff:fe:75:ce:e0. Test under the graphic reads: Step 1: Divide the MAC address between the OUI and device identifier. Step 2: Insert the hexadecimal value fffe, which in binary is: 1111 1111 1111 1110. Step 3. Convert the first 2 hexadecimalvalues of the OUI to binary and flip the U/L bit (bit 7). In this example, the 0 in bit 7 is change to at 1. Az eredmény az EUI-64 generált interfész azonosító: FE99:47FF:FE75:CEE0. Note: The use of the U/L bit, and the reasons for reversign its value, are discussed in RFC 5342.

fc 99 47 75 ce e0 fe 99 47 75 ce e0 ff

fe

OUI  
24 bitDevice Identifier  
24 bitsEUI-64 ProcessBinaryBinaryBinaryBinaryStep 1: Split the MAC addressStep 2: Insert fffeStep 3: Flip the u/l bitModified EUI-64 Interface ID in Hexadecimal Notation1111 11001001 10010100 01111111 01011100 11101110 00001111 11001001 10010100 01111111 11111111 11100111 01011100 11101110 00001111 11101001 10010100 01111111 11111111 11100111 01011100 11101111 0000

**1.** A MAC-cím kettéosztása az OUI és az eszközazonosító között.

**2.** A hexadecimális FFFE beszúrása, ami binárisan 1111 1111 1111 1110.

**3.** Az OUI első 2 hexadecimális számjegyének binárissá alakítása, majd az U/L bit (7. bit) invertálása. Ebben a példában a hetedik bit 0, amiből tehát 1 lesz.

Az eredmény az EUI-64 interfész azonosító: FE99:47FF:FE75:CEE0.

**MEGJEGYZÉS**: Az U/L bit szerepét és invertálásának okát az RFC 5342 tárgyalja.

Az alábbi **ipconfig** parancskimenetben látszik, hogy az IPv6 GUA dinamikusan jön létre a SLAAC és az EUI-64 folyamat használatával. Itt egy egyszerű módszert láthatunk annak megállapítására, hogy egy cím nagy valószínűséggel EUI-64-gyel készült vagy sem. Nézzük meg, hogy az **fffe** érték megtalálható-e az interfész-azonosító közepén.

Az EUI-64 előnye az, hogy interfész-azonosító generálható az Ethernet MAC-cím segítségével. Lehetővé teszi a hálózat rendszergazdáinak azt is, hogy az egyedi MAC-cím alapján az IPv6-címet egészen a végberendezésig követhessék. Azonban ez sok felhasználónál okozott adatvédelmi aggályokat, hogy a csomagokat nyomon lehet követni egészen a tényleges fizikai számítógépig. Ezen problémák miatt használhatunk véletlenszerűen generált interfész ID-t is.

### EUI-64 interfész-azonosító

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : **2001:db8:acad:1:fc99:47ff:fe75:cee0**

Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0

Default Gateway . . . . . . . . . : fe80::1

C:\>

12.5.7

## Véletlenszerűen generált interfész azonosító

Operációs rendszertől függően az eszköz a MAC-cím és az EUI-64 algoritmus helyett véletlenszerűen generált interfész azonosítót is használhat. Például a Windows operációs rendszerek a Vista verzióval kezdődően az EUI-64 helyett már véletlenszerűen generált interfész ID-t használnak. A Windows XP és a korábbi Windows operációs rendszerek az EUI-64-et alkalmazták.

Miután az EUI-64, vagy a véletlen generálás eredményeképpen előállt interfész azonosítót az IPv6-előtaggal összekombináljuk, létrejön egy globális egyedi és egy link-local cím, ahogy az ábrán látható.

### Véletlenszerűen generált interfész azonosító

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : **2001:db8:acad:1:50a5:8a35:a5bb:66e1**

Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1

Default Gateway . . . . . . . . . : fe80::1

C:\>

**MEGJEGYZÉS**: Bármely IPv6 egyedi cím kizárolagosságának biztosítása érdekében az ügyfél a DAD néven ismert folyamatot használhatja (Duplicate Address Detection, címütközés ellenőrzés). Ez hasonló a saját címre vonatkozó ARP-kéréshez. Ha erre a kérésre nincs válasz, akkor a cím egyedi.

12.5.8

## Tudáspróba - IPv6 GUA dinamikus címzése

Az űrlap teteje

Check your understanding of dynamically addressing for IPv6 GUAs by choosing the correct answer to the following questions.

1. True or false? RA messages are sent to all IPv6 routers by hosts requesting addressing information.

Az űrlap alja

Which dynamic addressing method for GUAs is the one where devices rely solely on the contents of the RA message for their addressing information?

Which dynamic addressing method for GUAs is the one where devices rely solely on a DHCPv6 server for their addressing information?

Which dynamic addressing method for GUAs is the one where devices get their IPv6 configuration in a RA message and request DNS information from a DHCPv6 server?

What are the two methods a device can use to generate its own IPv6 interface ID?

[12.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[GUA és LLA statikus konfigurálása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 dinamikus link-local címzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                          
*         

1. IPv6-címzés
2. IPv6 dinamikus link-local címzés

# IPv6 dinamikus link-local címzés

12.6.1

## Dinamikus link-local címek

Minden IPv6-eszközön kell link-local címnek (LLA) lennie. Az IPv6 GUA-khoz hasonlóan dinamikusan is létrehozhatunk LLA-kat. Függetlenül attól, hogy miként hozzuk létre ezeket a címeket, fontos az összes IPv6-cím konfigurációjának ellenőrzése. Ez a témakör ismerteti a dinamikusan generált LLA-kat és az IPv6-konfiguráció ellenőrzését.

Az ábrán egy dinamikus LLA látható az fe80።/10 előtaggal és az interfész azonosítóval, amely az EUI-64 folyamat vagy egy véletlenszerűen generált 64 bites szám segítségével jött létre.

The graphic shows the Prefix of an LLA in binary: 1111 1110 10, and in hexadecimal: fe80::/10.

fe80::/10 1111 1110 10

/64

Interface IDEUI-64 Process64 bitRandomly Generated Number

12.6.2

## Dinamikus link-local címek Windows-ban

Az operációs rendszerek, például a Windows, általában ugyanazt a módszert használják a SLAAC-alapú GUA és a dinamikusan létrehozott LLA esetében is. Tekintsük meg a kiemelt területeket az alábbi példákban, amelyeket korábban már láthattunk.

### EUI-64 segítségével generált interfész-azonosító

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : **2001:db8:acad:1:fc99:47**ff:fe**75:cee0**

Link-local IPv6 Address . . . . . : **fe80::fc99:47**ff:fe**75:cee0**

Default Gateway . . . . . . . . . : fe80::1

C:\>

### Véletlenszerűen generált interfész azonosító

C:\> **ipconfig**

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : **2001:db8:acad:1:50a5:8a35:a5bb:66e1**

Link-local IPv6 Address . . . . . : fe80::**50a5:8a35:a5bb:66e1**

Default Gateway . . . . . . . . . : fe80::1

C:\>

12.6.3

## Dinamikus link-local címek Cisco routereken

A Cisco routerek automatikusan létrehozzák az IPv6 LLA-t, amikor egy GUA-t rendelünk hozzá az interfészhez. A Cisco IOS-t futtató routerek IPv6-interfészei alapértelmezésben az EUI-64-gyel generálják a link-local címek interfész azonosítóját. Soros interfészek esetén a router egy Ethernet interfész MAC-címét fogja használni. Ne feledjük, hogy a link-local címnek csak az adott kapcsolaton vagy hálózaton belül kell egyedinek lennie. A dinamikusan kiosztott link-local címek hátrányaként a hosszukat lehet megemlíteni, ami miatt nehéz felismerni és emlékezni a kiosztott címekre. Az alábbi példa elején az R1 router GigabitEthernet 0/0/0 interfészének MAC-címe látható. Ez a cím szolgál az LLA dinamikus létrehozására ezen az interfészen, valamint a Serial 0/1/0 interfészen is.

Annak érdekében, hogy könnyebben felismerjük és emlékezzünk a címekre, gyakori módszer az IPv6 LLA-k statikus konfigurálása a routereken.

### IPv6 LLA az EUI-64 használatával

R1# **show interface gigabitEthernet 0/0/0**

GigabitEthernet0/0/0 is up, line protocol is up

Hardware is ISR4221-2x1GE, address is **7079.b392.3640** (bia 7079.b392.3640)

(Output omitted)

R1# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

FE80::**7279:B3FF:FE92:3640**

2001:DB8:ACAD:1::1

GigabitEthernet0/0/1 [up/up]

FE80::**7279:B3FF:FE92:3641**

2001:DB8:ACAD:2::1

Serial0/1/0 [up/up]

FE80::**7279:B3FF:FE92:3640**

2001:DB8:ACAD:3::1

Serial0/1/1 [down/down]

unassigned

R1#

12.6.4

## IPv6-címzés konfigurációjának ellenőrzése

Az ábrán egy minta topológia látható.

The graphic shows two PCs, PC1 and PC2. PC1 is connected to a switch and has the IPv6 address 2001:db8:acad:1::10/64. PC2 is connected to a switch and has the IPv6 address 2001:db8:acad:2::10/64. The two switches are connected to a router, R1. PC1 is connected through the switch to R1s G0/0/0 interface which has IPv6 address 2001:db8:acad:1::1/64 and the LLA address of fe80::1:1. PC2 is connected through the switch to R1s G0/0/1 interface which has IPv6 address 2001:db8:acad:2::1/64 and the LLA address of fe80::2:1. R1 connects to the cloud through its S0/1/0 interface which has IPv6 adress 2001:db8:acad:3::1/64 and the LLA address of fe80::3:1.

Kattintsunk a gombokra a parancsok kimenetének és leírásainak megtekintéséhez!

A **show ipv6 interface brief** parancs megjeleníti az Ethernet interfészek IPv6-címeit. A link-local cím interfész azonosítójának automatikus előállításához az EUI-64 a MAC-címet használja. A **show ipv6 interface brief** parancs egy rövidített kimenetet jelenít meg minden interfészhez. Az [up/up] jelölés az interfész első és második rétegbeli állapotát jelenti. Ez a megfelelő IPv4-parancs Status és Protocol oszlopainak felel meg.

Figyeljük meg, hogy minden interfésznek két IPv6-címe van. A második cím egy manuálisan beállított globális egyedi cím. Az első, az FE80-nal kezdődő cím pedig az interfész link-local egyedi címe, amely lehet kézzel beállított vagy automatikusan hozzárendelt. Emlékezzünk vissza, hogy link-local címet akkor kap automatikusan az interfész, ha globális egyedi címet rendelünk hozzá, de a link-local címet nem állítjuk be.

Az R1 Serial 0/1/0 interfészének link-local címe is lehet kézzel beállított vagy automatikusan hozzárendelt. Mivel a soros interfészeknek nincs Ethernet MAC-címük, ezért az automatikus beállításhoz a Cisco IOS az első elérhető Ethernet interfész MAC-címét használja. Ebben az esetben a két interfész link-local címe azonos lesz. Ez azért lehetséges, mert a link-local interfészcímnek csak a kapcsolaton belül kell egyedinek lennie.

**A show ipv6 interface brief parancs az R1-en**

R1# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

FE80::7279:b3ff:fe92:3640

2001:DB8:ACAD:1::1

GigabitEthernet0/0/1 [up/up]

FE80::8320:e4ff:fe79:2830

2001:DB8:ACAD:2::1

Serial0/1/0 [up/up]

FE80::7279:b3ff:fe92:3640

2001:DB8:ACAD:3::1

Serial0/1/1 [down/down]

unassigned

R1#

12.6.5

## Parancsszimulátor - Az IPv6-címzés konfigurációjának ellenőrzése

A **show** parancsokkal ellenőrizhetjük az IPv6-címek konfigurációját az R1 router interfészein.

The graphic shows two PCs, PC1 and PC2. PC1 is connected to a switch and has the IPv6 address 2001:db8:acad:1::10/64. PC2 is connected to a switch and has the IPv6 address 2001:db8:acad:2::10/64. The two switches are connected to a router, R1. PC1 is connected through the switch to R1s G0/0/0 interface which has IPv6 address 2001:db8:acad:1::1/64 and the LLA address of fe80::1:1. PC2 is connected through the switch to R1s G0/0/1 interface which has IPv6 address 2001:db8:acad:2::1/64 and the LLA address of fe80::2:1. R1 connects to the cloud through its S0/1/0 interface which has IPv6 adress 2001:db8:acad:3::1/64 and the LLA address of fe80::3:1.

R1 ::10 ::10 S0/1/0::1fe80::3:1 PC1 2001.db8.acad:2::/64 2001.db8.acad:1::/64 2001.db8.acad:3::/64 G0/0/0::1fe80::1:1 G0/0/1::1fe80::2:1 PC2

R1

Enter the show command that will display a brief summary of the IPv6 interface status.

R1#show ipv6 interface brief

GigabitEthernet0/0/0 [up/up]

FE80::1:1

2001:DB8:ACAD:1::1

GigabitEthernet0/0/1 [up/up]

FE80::2:1

2001:DB8:ACAD:2::1

Serial0/1/0 [up/up]

FE80::3:1

2001:DB8:ACAD:3::1

Serial0/1/1 [down/down]

unassigned

GigabitEthernet0 [administratively down/down]

unassigned

Verify connectivity from R1 to PC2 at 2001:db8:acad:1::10.

R1#show ipv6 route

IPv6 Routing Table - default - 7 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP

H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt

lr - LISP site-registrations, ld - LISP dyn-eid, a - Application

C 2001:DB8:ACAD:1::/64 [0/0]

via GigabitEthernet0/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via GigabitEthernet0/0, receive

C 2001:DB8:ACAD:2::/64 [0/0]

via GigabitEthernet0/1, directly connected

L 2001:DB8:ACAD:2::1/128 [0/0]

via GigabitEthernet0/1, receive

C 2001:DB8:ACAD:3::/64 [0/0]

via Serial0/0/1, directly connected

L 2001:DB8:ACAD:3::1/128 [0/0]

via Serial0/0/1, receive

L FF00::/8 [0/0]

via Null0, receive

R1#ping 2001:db8:acad:1::10

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

You successfully verified IPv6 address configuration.

12.6.6

## Packet Tracer feladat - IPv6-címek beállítása

Ebben a feladatban egy router, valamint szerverek és kliensek IPv6-címeinek beállítását gyakoroljuk. Emellett az IPv6-címzés megvalósításának ellenőrzését is el kell végezni.

[IPv6-címzés konfigurálása](https://contenthub.netacad.com/courses/itn/_common/12.6.6-packet-tracer---configure-ipv6-addressing_hu-HU.pka)

[12.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Globális IPv6-címek dinamikus konfigurációja](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 csoportos címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                            
*         

1. IPv6-címzés
2. IPv6 csoportos címek

# IPv6 csoportos címek

12.7.1

## Kiosztott IPv6-csoportcímek

A korábbi fejezetekből már megtudtuk, hogy az IPv6-címeknek három főbb kategóriája létezik: unicast, anycast és multicast. Ez a témakör részletesebben ismerteti a csoportos címeket.

Az IPv6-csoportcímek hasonlóak az IPv4 csoportcímekhez. Emlékezzünk vissza, a csoportcím (multicast cím) arra való, hogy egyetlen csomagot küldhessünk egy vagy több célállomásnak (multicast csoportnak). Az IPv6-csoportcímek előtagja FF00::/8.

**MEGJEGYZÉS**: Multicast címek csak célcímek lehetnek, forrás címek nem.

Kétéle IPv6 csoportos cím létezik:

* Jól ismert (well-known) csoportcímek
* Solicited node (kérelmezett, elvárt) csomóponti csoportcímek

12.7.2

## Jól ismert (well-known) csoportcímek

A jól ismert IPv6 csoportos címeket központilag osztják ki. A kiosztott (hozzárendelt) multicast címek bizonyos előre definiált eszközcsoportok számára fenntartott multicast címek. Ez egy olyan önálló cím, amellyel közös protokollt vagy szolgáltatást futtató eszközök csoportját érhetjük el. Az ilyen címeket meghatározott protokollokkal kapcsolatban használjuk, mint például a DHCPv6.

Két gyakori hozzárendelt IPv6 multicast csoport:

* **ff02::1 All-nodes (minden-állomás) multicast csoport** - Ennek a csoportnak minden IPv6-eszköz tagja. A csoportnak küldött csomagot a kapcsolaton vagy a hálózaton lévő összes IPv6-interfész megkapja és feldolgozza. Hatása ugyanaz, mint az IPv4 szórási címnek. Az ábrán egy példa látható a minden-állomás multicast cím használatával történő kommunikációra. Az IPv6-router az all-nodes multicast csoportnak küld ICMPv6 RA-üzenetet.
* **ff02::2 All-routers (minden-router) multicast csoport** - Ez egy olyan csoport, amelynek minden IPv6-router tagja. A router akkor válik a csoport tagjává, amikor IPv6-routerként konfiguráljuk az **ipv6 unicast-routing** globális konfigurációs paranccsal. A csoportnak küldött csomagokat a kapcsolaton vagy hálózaton lévő minden IPv6-router megkapja és feldolgozza.

The graphic shows two PCs wtih IPv6 addresses of 2001:db8:acad:1::10/64 and 2001:db8:acad:1::20/64, a server with IPv6 address 2001:db8:acad:1::8/64, and a printer with IPv6 address 2001:db8:acad:1::9/64 connected to a switch which is connected to a router. Above the graphic is indicated the source IPv6 address of fe80::1 and the destination IPv6 address of ff02::1. Text under the graphic reads IPv6-enabled devices send ICMPv6 RS messages to the all-routers multicast address. The RS message requests an RA message form the IPv6 router assist the device in its address configuation. The IPv6 router responds with an RA message, as shown.

### IPv6 minden-állomás csoportos küldés: RA-üzenet

2001:db8:acad:1::20/64 2001:db8:acad:1::8/64 2001:db8:acad:1::9/64 2001:db8:acad:1::10/64 ff02::1

fe80::1

Source IPv6 AddressDestination IPv6 Address

Az IPv6-eszközök az ICMPv6 router keresés (RS) üzeneteket a minden-router multicast címre küldik. Az RS-üzenet RA-választ kér az IPv6-routertől, hogy segítséget kapjon a cím konfigurációjának beállításához. Az IPv6-router RA-üzenettel válaszol.

12.7.3

## Solicited-node IPv6 multicast címek

A solicited-node (elvárt, kérelmezett) multicast hasonló a minden-állomás (all-nodes) multicast címhez. A kérelmezett multicast cím előnye, hogy egy speciális Ethernet csoportcímhez van hozzárendelve. A cél MAC-cím vizsgálatával az Ethernet hálózati kártya kiszűrheti a keretet anélkül, hogy elküldené az IPv6-folyamatnak vizsgálatra, miszerint az eszköz az IPv6-csomag célpontja-e, vagy sem.

The graphic shows three PCs recieving a message from a router. Each PC has the following informational text: My Ethernet NIC determined this multicast is not for me. Above the graphic is indicated that the Destination MAC address is a multicast and the Destination IPv6 address is a Solicited-Node multicast.

IPv6EthernetDestination IPv6: Solicited-Node MulticastDestination MAC: MulticastMy Ethernet NIC determined this multicast is not for me.My Ethernet NIC determined this multicast is not for me.My Ethernet NIC determined this multicast is for me!

12.7.4

## Laborgyakorlat - IPv6-címek azonosítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: IPv6-címek típusainak meghatározása
  2. rész: Egy állomás IPv6 hálózati interfészének és címének vizsgálata
  3. rész: IPv6-címek rövidítésének gyakorlása

[12.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 dinamikus link-local címzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                               
*         

1. IPv6-címzés
2. IPv6-hálózat alhálózatokra bontása

# IPv6-hálózat alhálózatokra bontása

12.8.1

## Alhálózatok kialakítása az alhálózat azonosítóval (Subnet ID)

A fejezet bevezetésében megemlítettük az IPv6-hálózatok alhálózatokra bontását. Azt is mondtuk, hogy ez egy kicsit könnyebb, mint egy IPv4-hálózat alhálózatokra osztása. Most megtudjuk, igaz-e ez!

Emlékezzünk vissza, hogy az IPv4-nél az alhálózatok létrehozásához biteket kell kölcsönöznünk az állomásazonosító részből. Ez azért van, mert az alhálózatokra bontás az IPv4-ben egy utólag kigondolt megoldás. Az IPv6-ot azonban úgy tervezték, hogy az alhálózatokat könnyű legyen létrehozni. Az IPv6 globális címekben külön alhálózati azonosító mezőt van alhálózatok létrehozására. Az alhálózati azonosító mező a globális útválasztási előtag és az interfészazonosító közötti terület (lásd ábra).

The graphic shows the parts of a GUA. First is the 48 bit Global Routing Prefix followed by the 16 bit Subnet ID, then finally the 64 bit Interface ID. Text under the graphic reads A /48 routing prefix + 16 bit Subnet ID = /64 prefix.

### Globális egyedi cím 16 bites alhálózati azonosítóval

48 bit16 bit64 bitGlobal Routing PrefixSubnet IDInterface IDA /48 routing prefix + 16 bit Subnet ID = /64 prefix

A 128 bites cím előnye, hogy hálózatonként több mint elegendő alhálózatot és állomást tud támogatni. A címekkel való spórolással nem kell foglalkozni. Például, ha a globális útválasztási előtag /48, és egy tipikus 64 bites interfészazonosítót használunk, akkor ez 16 bites alhálózati azonosítót jelent:

* **16 bites alhálózati azonosító** — Legfeljebb 65 536 alhálózat hozható létre.
* **64 bites** interfész-azonosító - Alhálózatonként akár kvintillió hoszt IPv6-cím lehetséges (azaz 18.000,000,000,000,000,000).

**MEGJEGYZÉS**: Az alhálózatot a 64 bites interfész azonosítójába (állomás rész) is be lehet illeszteni, de erre ritkán van szükség.

Az IPv6-alhálózatot könnyebb megvalósítani, mint az IPv4-et, mivel nincs szükség bináris formátumra történő átalakításra. A következő szabad alhálózat meghatározásához elég eggyel növelni a hexadecimális értéket.

12.8.2

## Példa IPv6 alhálózatokra bontásra

Tegyük fel, hogy egy szervezethez a 2001:db8:acad። /48 globális útválasztási előtagot rendelték hozzá egy 16 bites alhálózati azonosítóval. Ez lehetővé teszi a szervezet számára, hogy 65536 darab /64-es alhálózatot hozzon létre az ábrán látható módon. Figyeljük meg, hogy a globális előtag azonos valamennyi alhálózatban. Egyedül az alhálózatot azonosító hextettek értéke növekszik mindenhol.

The graphic shows the IPv6 address prefix 2001:db8:acad::/48 subnetted into /64 subnets. A note reads Increment subnet ID to create 65,536 subnets. The subnets are: 2001:db8:acad:0000::/64, 2001:db8:acad:0001::/64, 2001:db8:acad:0002::/64, 2001:db8:acad:0003::/64, 2001:db8:acad:0004::/64, 2001:db8:acad:0005::/64, 2001:db8:acad:0006::/64, 2001:db8:acad:0007::/64, 2001:db8:acad:0008::/64, 2001:db8:acad:0009::/64, 2001:db8:acad:000a::/64, 2001:db8:acad:000b::/64, 2001:db8:acad:000c::/64. Subnets 13-65,534 not shown, 2001:db8:acad:ffff::/64.

### Alhálózatok kialakítása a16 bites alhálózat azonosítóval

2001:db8:acad:0000::/642001:db8:acad:0001::/642001:db8:acad:0002::/642001:db8:acad:0003::/642001:db8:acad:0004::/642001:db8:acad:0005::/642001:db8:acad:0006::/642001:db8:acad:0007::/642001:db8:acad:0008::/642001:db8:acad:0009::/642001:db8:acad:000a::/642001:db8:acad:000b::/642001:db8:acad:000c::/642001:db8:acad:ffff::/64

Increment subnet ID to create 65,536 subnetsSubnets 13 – 65,534 not shown

12.8.3

## IPv6-alhálózat kiosztás

A hálózati rendszergazdák feladata a hálózat logikai címtervének elkészítése a rendelkezésre álló 65536 alhálózatból.

A minta topológián alhálózatokat kell kialakítani valamennyi LAN-ra és az R1- R2 közötti WAN-kapcsolatra nézve. Ellentétben az IPv4-ban megszokottal, az IPv6 esetén a soros kapcsolat alhálózatának ugyanolyan prefix hossza lesz, mint a LAN-oknak. Ez ugyan „címpazarlásnak” tűnhet, de ennek IPv6 esetén nincs jelentősége.

The graphic shows four PCs, PC1, PC2, PC3, and PC4, each with the interface ID of ::10. Each PC is connected to a switch. PC1 is in network 2001:db8:acad:1::/64 and connects through a switch to the G0/0/0 interface, with interface ID ::1, of router 1. PC2 is in network 2001:db8:acad:2::/64 and connects through a switch to the G0/0/1 interface, with interface ID ::1, of router 1. PC3 is in network 2001:db8:acad:4::/64 and connects through a switch to the G0/0/0 interface, with interface ID ::1, of router 2. PC4 is in network 2001:db8:acad:5::/64 and connects through a switch to the G0/0/1 interface, with interface ID ::1 of router 2. Router 1 and 2 are connected over their S0/1/0 interfaces with R1 having an interface ID of ::1 and R2 having an interface ID of ::2 in the 2001:db8:acad:3::/64 network.

### Minta topológia

2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 2001:db8:acad:3::/64 G0/0/1::1 ::10 ::10 ::10 ::10 S0/1/0::1 S0/1/0::2 G0/0/0::1 G0/0/0::1 G0/0/1::1 PC1 PC2 PC3

PC4

A következő ábra azt szemlélteti, 5 darab, 0001-től 0005-ig terjedő alhálózat azonosítójú IPv6-alhálózatot osztunk ki. Valamennyi /64-es alhálózat jóval több címet biztosít, mint amire valaha is szükségünk lehet.

The graphic shows subnets from the address block: 2001:db8:acad::/48. The subnets are: 2001:db8:acad:0000::/64, 2001:db8:acad:0001::/64, 2001:db8:acad:0002::/64, 2001:db8:acad:0003::/64, 2001:db8:acad:0004::/64, 2001:db8:acad:0005::/64, 2001:db8:acad:0006::/64, 2001:db8:acad:0007::/64, 2001:db8:acad:0008::/64, 2001:db8:acad:ffff::/64. A note reads 5 subnets allocated from 65,536 available and indicates the five subnets allocated are: 2001:db8:acad:0001::/64, 2001:db8:acad:0002::/64, 2001:db8:acad:0003::/64, 2001:db8:acad:0004::/64, 2001:db8:acad:0005::/64.

...

2001:db8:acad:0000::/642001:db8:acad:0001::/642001:db8:acad:0002::/642001:db8:acad:0003::/642001:db8:acad:0004::/642001:db8:acad:0005::/642001:db8:acad:0006::/642001:db8:acad:0007::/642001:db8:acad:0008::/642001:db8:acad:ffff::/64

5 subnets allocated from 65,536 available subnetsAddress Block: 2001:0db8:acad::/48

12.8.4

## Router konfigurálása IPv6-alhálózatokkal

Az IPv4 konfigurációjához hasonlóan, valamennyi router interfész különböző IPv6-alhálózatba esik.

### IPv6-cím konfigurálása az R1 routeren

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ipv6 address 2001:db8:acad:2::1/64**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1/0**

R1(config-if)# **ipv6 address 2001:db8:acad:3::1/64**

R1(config-if)# **no shutdown**

12.8.5

## Tudáspróba - IPv6 alhálózatokra bontás

Az űrlap teteje

Check your understanding of subnetting an IPv6 network by choosing the BEST answer to the following questions.

1. True or False? IPv6 was designed with subnetting in mind.

Az űrlap alja

Which field in an IPv6 GUA is used for subnetting?

Given a /48 Global Routing Prefix and a /64 prefix, what is the subnet portion of the following address: 2001:db8:cafe:1111:2222:3333:4444:5555

Given a /32 Global Routing Prefix and a /64 prefix, how many bits would be allocated for the Subnet ID?

[12.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6 csoportos címek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[12.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                          

1. IPv6-címzés
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

12.9.1

## Packet Tracer feladat – IPv6-alhálózatok címzési tervének megvalósítása

A hálózat rendszergazdája arra kér bennünket, hogy a topológián látható hálózatra osszunk ki 5 darab /64-es IPv6-alhálózatot. Feladatunk az IPv6-alhálózatok meghatározása, az IPv6-címek routerekre való kiosztása, és a PC-k automatikus IPv6-cím konfigurációjának engedélyezése. Az utolsó lépés az IPv6-állomások közötti kapcsolatok ellenőrzése.

[IPv6-alhálózatok címzési tervének megvalósítása](https://contenthub.netacad.com/courses/itn/_common/12.9.1-packet-tracer---implement-a-subnetted-ipv6-addressing-scheme_hu-HU.pka)

12.9.2

## Laborgyakorlat - IPv6-címek beállítása hálózati eszközökön

A laborgyakorlat során az alábbi feladatokat végezzük el:

* 1. rész: Topológia megvalósítása, a routerek és a switch-ek alapvető beállításainak konfigurálása.
  2. rész: IPv6-címek manuális beállítása.
  3. rész: Végpontól-végpontig terjedő kapcsolat ellenőrzése

12.9.3

## Miről tanultunk ebben a fejezetben?

**IPv4-problémák**

Az IPv4-tartomány elméleti maximuma kb. 4,3 milliárd cím. A privát címek és a NAT együttesen segítettek lassítani az IPv4-címterület kimerülését. Az internet elterjedése, az IPv4-címtartomány korlátozott mérete, a NAT problémái és az IoT mind azt bizonyítják, hogy itt az idő IPv6-ra váltani. Az IPv4 és az IPv6 együtt fog működni a közeljövőben, és az átmenet több évig eltart. Az IETF különféle protokollokat és eszközöket fejlesztett ki a hálózati rendszergazdák számára, hogy elősegítse az IPv6-ra történő átállást. Az áttérési technikákat három kategóriába soroljuk: dual stack, alagút technológia és címfordítás.

**IPv6-címek ábrázolása**

Az IPv6-címek 128 bit hosszúak és hexadecimális értékek sorozataként írjuk fel őket. Mivel négy bit ad ki egy hexadecimális számjegyet, így a cím 32 hexadecimális számjegyből áll. Az IPv6-címek preferált formátuma x:x:x:x:x:x:x:x, ahol minden "x" négy hexadecimális számjegyet helyettesít. Például: 2001:0 db 8:0000:1111:0000:0000:0200. Két szabály segít, hogy csökkenthessük az IPv6-címek megjelenítéséhez szükséges számjegyek számát. Az első szabály az IPv6-címek rövidítésére az, hogy a hextettek vezető nulláit elhagyhatjuk. Például: 2001:db 8:0:1111:0:0:0:200. A második szabály az, hogy a csak nullákat tartalmazó 16 bites hextett sorozat helyettesíthető dupla kettősponttal (::). Például: 2001:db 8:0:1111። 200.

**IPv6 címtípusok**

Háromféle IPv6-címet különböztetünk meg: egyedi (unicast), csoportos (multicast) és bárki (anycast) cím. A pontozott decimális alhálózati maszk jelölést IPv6-nál nem használjuk. Az IPv4-hez hasonlóan az előtag hossza perjeles formátumban jelenik meg, és az IPv6-cím hálózati részének jelölésére szolgál. Az IPv6 egyedi cím egy IPv6-eszköz interfészét azonosítja. Kétféle egyedi IPv6-cím létezik: globális (GUA) és link-local (LLA). A helyileg egyedi (unique local)IPv6-címeket a következőkre használják: helyi címzésre egy webhelyen belül vagy korlátozott számú webhely között. Valamint olyan eszközökhöz, amelyeknek soha nem kell hozzáférniük egy másik hálózathoz, és nincsenek globálisan irányítva vagy nincsenek lefordítva globális IPv6-címre. Az IPv6 globális egyedi címzésű címek (GUA) a teljes címtérben egyediek, és továbbíthatók az interneten. Ezek a publikus IPv4-címek megfelelői. A GUA három részből áll: globális útválasztási előtag, alhálózati azonosító és interfészazonosító. Az IPv6 link-local címek (LLA) lehetővé teszik, hogy az eszköz más IPv6-eszközökkel kommunikáljon ugyanazon a kapcsolaton, de csakis azon az egy kapcsolaton (alhálózaton) belül. Az eszközök statikusan vagy dinamikusan szerezhetnek link-local címet.

**GUA és LLA statikus konfiguráció**

Egy IPv4-cím beállításához egy interfészen az **ip address** ip-cím alhálózati maszk Cisco IOS-parancs használható. Egy IPv6 globális egyedi cím interfészen történő konfigurálásának parancsa az **ipv6 address** ipv6-cím/prefixhossz. Ugyanúgy, mint az IPv4-nél, nagyobb hálózatokban nem praktikus a klienseknek statikusan címeket adni. Emiatt a legtöbb IPv6-hálózat rendszergazdája az IPv6-címek dinamikus hozzárendelését alkalmazza. A link-local címek kézi konfigurációja könnyen felismerhető és megjegyezhető címek választását teszi lehetővé. A router kézi beállítása általában csak a könnyen felismerhető LLA-k létrehozása miatt szükséges. Az LLA-k manuálisan konfigurálhatók az **ipv6 address** ipv6-link-local-cím**link-local** paranccsal.

**Globális IPv6-címek dinamikus konfigurációja**

Egy készülék ICMPv6-üzenetek segítségével kaphat dinamikusan globális egyedi címet. Az IPv6-routerek rendszeres időközönként küldenek ki ICMPv6 RA-üzeneteket a hálózat minden IPv6-eszközének. Szintén egy RA-üzenetet küldenek válaszul egy ICMPv6 RS-üzenetet küldő hoszt számára, amely RA-információkat kért. Az ICMPv6 RA-üzenet a következőket tartalmazza: hálózati előtag és előtag hossza, alapértelmezett átjáró címe, valamint a DNS-címek és tartománynév. Az RA-üzenetek három módszert alkalmazhatnak: SLAAC, SLAAC állapot nélküli DHCPv6-szerverrel, és állapottartó DHCPv6 (nincs SLAAC). Az SLAAC esetén a kliens eszköz az RA-üzenetben található információkat használja egy saját GUA létrehozásához, mivel az üzenet tartalmazza az előtagot és az előtag hosszát. Az SLAAC állapot nélküli DHCPv6 esetén az RA-üzenet azt javasolja, hogy az eszközök az SLAAC-t alkalmazzák saját IPv6 GUA-juk létrehozásához, a router LLA-t alapértelmezett átjárócímként használják, és egy állapot nélküli DHCPv6-kiszolgálót keressenek fel az egyéb szükséges információk megszerzéséhez. Az állapottartó DHCPv6 esetén az RA azt javasolja, hogy az eszközök a router LLA-t alapértelmezett átjárócímként használják, az állapottartó DHCPv6-kiszolgálót pedig a GUA, a DNS-kiszolgáló cím, a tartománynév és az összes többi szükséges információ megszerzéséhez. Az interfészazonosító az EUI-64 eljárással vagy véletlenszerűen generált 64 bites számmal hozható létre. Az EUI-64 művelet a kliens 48 bites Ethernet MAC-címének közepébe beszúr további 16 bitet, így állítja elő a 64 bites interfész azonosítót. Operációs rendszertől függően az eszköz a MAC-cím és az EUI-64 algoritmus helyett véletlenszerűen generált interfész azonosítót is használhat.

**IPv6 dinamikus link-local címzés**

Minden IPv6-eszközön kell link-local címnek (LLA) lennie. Az LLA-konfigurálható manuálisan, vagy dinamikusan is létrehozható. Az operációs rendszerek, például a Windows, általában ugyanazt a módszert használják mind az SLAAC-alapú GUA, mind a dinamikusan létrehozott LLA esetében. A Cisco routerek automatikusan létrehozzák az IPv6 link-local címet, amikor egy GUA-t rendelünk hozzá az interfészhez. A Cisco IOS-t futtató routerek az IPv6-interfészeiken alapértelmezésben az EUI-64-gyel generálják a link-local címek interfész azonosítóját. Soros interfészek esetén a forgalomirányító egy Ethernet interfész MAC-címét fogja használni. Annak érdekében, hogy könnyebben felismerjük és emlékezzünk ezekre a címekre, gyakori az IPv6 LLA-k statikus konfigurálása a routereken. Az IPv6-címkonfiguráció ellenőrzéséhez használjuk a következő három parancsot: **show ipv6 interface brief**, **show ipv6 route** és **ping**.

**IPv6 csoportos címek**

Az IPv6 csoportos (multicast) címeknek két típusa létezik: jól ismert és kérelmezett (solicited-node) multicast címek. A kiosztott (hozzárendelt) multicast címek bizonyos előre definiált eszközcsoportok számára fenntartott címek. A jól ismert csoportos címeket központilag osztják ki. Két általánosan ismert IPv6 hozzárendelt csoportcím az ff02። 1 (minden-állomás) és az ff02። 2 (minden-router) multicast cím. A solicited-node multicast hasonló a minden állomás (all-nodes) multicast címhez. A kérelmezett multicast cím előnye, hogy egy speciális Ethernet csoportcímhez van hozzárendelve.

**IPv6 alhálózatokra bontás**

Az IPv6-ot úgy tervezték, hogy az alhálózatokat könnyű legyen létrehozni. Az IPv6 GUA külön alhálózati azonosító mezőt használ alhálózatok létrehozására. Az alhálózati azonosító mező a globális útválasztási előtag és az interfészazonosító közötti terület. A 128 bites cím előnye, hogy hálózatonként több mint elegendő alhálózatot és állomást tud támogatni. A címekkel való spórolással nem kell fogllakozni. Például, ha a globális útválasztási előtag /48, és egy tipikus 64 bites interfészazonosítót használunk, akkor ez 16 bites alhálózati azonosítót jelent:

* 16 bites alhálózati azonosító — Legfeljebb 65 536 alhálózat hozható létre.
* 64 bites interfész-azonosító - Alhálózatonként akár 18 kvintillió hoszt IPv6-cím lehetséges (azaz 18.000,000,000,000,000,000).

A hálózati rendszergazdák feladata a hálózat logikai címtervének elkészítése a rendelkezésre álló 65536 alhálózatból. Az IPv6 használatakor a címekkel való spórolás nem jelent gondot. Az IPv4 konfigurációjához hasonlóan valamennyi router interfész különböző IPv6-alhálózatba esik.

12.9.4

## Ellenőrző teszt - IPv6-címzés

Az űrlap teteje

1. Mi az érvényes lehető legtömörebb formátuma a 2001: 0DB8: 0000: AB00: 0000: 0000: 0000: 1234 IPv6-címnek?

Az űrlap alja

Milyen előtag tartozik a 2001:CA48:D15:EA:CC44። 1/64 IPv6 címhez?

Milyen típusú cím rendelődik hozzá automatikusan egy IPv6-interfészhez?

Melyik IPv6-előtag (prefix) használható csak helyi összeköttetésen és nem irányítható?

Mi a **ping ::1** parancs célja?

Mi az interfészazonosítója a 2001:DB8። 1000:A9CD:47FF:FE57:FE94/64 IPv6-címnek?

What is the network address for the IPv6 address 2001:DB8:AA04:B5::1/64?

Melyik címtípus nem támogatott IPv6 esetén?

Mit jelent egy sikeres ping a ::1 IPv6-célcím felé?

Mi a 2001:0000:0000:abcd:0000:0000:0000:0001 IPv6-cím legrövidebb formája?

Mi az IPv6-útválasztásban részt vevő router interfész minimális konfigurációja?

Legalább melyik cím szükséges az IPv6-kompatibilis interfészeken?

Melyek egy globális egyedi (global unicast) IPv6-cím részei? (Három jó válasz van.)

Egy vállalat a 2001:0000:130F::/48 IPv6-előtagot kapta a szolgáltatótól. Ezzel az előtaggal hány bit áll a szervezet rendelkezésére alhálózatok létrehozásához, ha további interfészazonosító biteket nem veszünk kölcsön?

Melyik IPv6-cím nem irányítható és csak az alhálózaton belül történő kommunikációra alkalmas?

[12.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IPv6-hálózat alhálózatokra bontása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[13.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                          
*       

1. ICMP
2. Bevezetés

# Bevezetés

13.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az ICMP fejezetben!

Képzeljük el, hogy van egy bonyolult vasútmodell készletünk. A vágányok és a vonatok a helyükön vannak, a rendszer be van kapcsolva és készen áll az indításra. Elfordítjuk a kapcsolót. A vonat elindul, majd valahol pálya közepénél egyszer csak megáll. Sejthetjük, hogy a probléma valószínűleg ott van, ahol a vonat megállt, ezért ott nézzük meg legelőször. Egy hálózat esetében ezt nehezebb már elképzelni. Szerencsére vannak eszközök, amelyek segítségünkre lehetnek egy hálózat problémás részeinek a beazonosításában, és ezek ráadásul egyaránt használhatók IPv4 és IPv6 hálózatok esetében is. Örömünkre szolgálhat, hogy a fejezet több Packet Tracer gyakorlatot is tartalmaz, amelyek segítenek ezeknek az eszközöknek a begyakorlásában, úgyhogy vágjunk is bele!

13.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** ICMP

**Fejezet célja:** Különböző segédprogramok használata a hálózati kapcsolat ellenőrzéséhez.

| Táblázat fejléc | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **ICMP üzenettípusok** | Annak elmagyarázása, hogy az ICMP hogyan használható a hálózati kapcsolatok ellenőrzésére. |
| **Ping és Traceroute tesztelés** | Ping és Traceroute parancsok használata a hálózati kapcsolatok ellenőrzésére. |

[12.9](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[13.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[ICMP üzenetek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                              
*       

1. ICMP
2. ICMP üzenetek

# ICMP üzenetek

13.1.1

## ICMPv4 és ICMPv6 üzenetek

Ebben a fejezetben megismerkedünk az ICMP (Internet Control Message Protocol, internet vezérlő üzenet protokoll) különböző üzenettípusaival, és azokkal az eszközökkel, amelyekkel ilyenek küldhetők.

Bár az IP csupán legjobb szándékú (best-effort) protokoll, a TCP/IP protokollcsomag az IP eszközök kommunikációjához hiba- és információs üzeneteket is biztosít. Ezen üzenetek elküldése az ICMP szolgáltatásain keresztül történik. Az üzenetek célja nem az IP protokoll megbízhatóvá tétele, hanem az IP csomagok feldolgozása során bizonyos körülmények között előforduló hibák visszajelzése. Az ICMP üzenetek nem feltétlenül szükségesek, és a hálózatokban biztonsági okokból gyakran nincsenek is engedélyezve.

Az ICMP mind az IPv4, mind pedig az IPv6 felett egyaránt rendelkezésre áll. Az ICMPv4 az IPv4 üzenetküldő protokollja. Az ICMPv6 ugyanezeket a szolgáltatásokat biztosítja az IPv6 számára, de további funkciókat is tartalmaz. Ebben a fejezetben az ICMP kifejezést egyaránt használjuk az ICMPv4 és az ICMPv6 esetére.

Az ICMP üzenettípusok száma, valamint az okok, ami miatt küldjük őket, nagyon széleskörű. A fejezetben tárgyalt ICMPv4 és ICMPv6 közös üzettípusok:

* Hoszt elérhetősége
* Cél vagy szolgáltatás nem elérhető
* Időtúllépés

13.1.2

## Hoszt elérhetősége

Az ICMP visszhang (Echo) üzenete használható egy IP hálózatban lévő konkrét hoszt elérhetőségének az ellenőrzésére. A helyi gép ilyenkor egy ICMP visszhang kérés (Echo Request) üzenetet küld a hosztnak. Amennyiben elérhető, akkor ő egy visszhang válasz (Echo Reply) üzenettel válaszol. Kattintsunk a lejátszás gombra az ICMP a visszhang kérés/visszhang válasz üzenetek szemléltetéséhez! Ez egy példa az ICMP Echo üzeneteket alkalmazására a **ping** parancs használatával.

animation of host 1 sending a ping ICMP echo request to host 2 and the ICMP echo reply from host 2 back to host 1

Yes, I am here.

**ping 192.168.30.1**

13.1.3

## Cél vagy szolgáltatás nem elérhető

Ha egy hoszt vagy egy router olyan csomagot kap, amelyet nem tud kézbesíteni, az ICMP cél nem elérhető (Destination Unreachable) üzenetét használhatja arra, hogy a küldőt értesítse a cél vagy a szolgáltatás elérhetetlenségéről. Az üzenet tartalmaz egy kódot, amely leírja, hogy a csomagot miért nem sikerült kézbesíteni.

Néhány ezek közül a kódok közül az ICMPv4-ben:

* 0 - Célhálózat nem elérhető (Net unreachable)
* 1 - Hoszt nem elérhető (Host unreachable)
* 2 - Protokoll nem elérhető (Protocol unreachable)
* 3 - Port nem elérhető (Port unreachable)

Néhány ezek közül a kódok közül az ICMPv6-ban:

* 0 - Nincs útvonal a cél felé (No route to destination)
* 1 - A célállomással való kommunikáció adminisztratív módon tiltott (pl. tűzfal miatt). (Communication with the destination is administratively prohibited)
* 2 — A forráscím hatókörén kívül (Beyond scope of the source address)
* 3 - Cím nem elérhető (Address unreachable)
* 4 - Port nem elérhető (Port unreachable)

**Megjegyzés:**: Az ICMPv6 hasonló, de kissé eltérő kódokat használ a cél elérhetetlenségét jelző üzenetekhez.

13.1.4

## Időtúllépés

Az ICMPv4 időtúllépés (Time Exceeded) üzenetet a routerek használják annak jelzésére, hogy a csomagot nem továbbíthatják, mert az élettartam (Time To Live, TTL) mezőjének értéke nullára csökkent. Amikor a router fogad egy csomagot és az IP-fejlécben a TTL mező értékét nullára csökkenti, akkor a csomagot eldobja, és ezzel egyidejűleg a forrás hosztnak egy időtúllépés üzenetet küld.

Az ICMPv6 szintén időtúllépés üzenetet küld, ha a router IPv6-csomagot azért nem tudja továbbítani, mert lejárt. Az IPv6 esetében nem TTL mezőt használnak, hanem egy ugrási korlát (Hop Limit) nevű mező jelzi, ha a csomag élettartama lejárt.

**Megjegyzés**: Az időtúllépés üzeneteket a **traceroute** parancs is használja.

13.1.5

## ICMPv6 üzenetek

Az ICMPv6 információs- és hibaüzenetei nagyon hasonlítanak az ICMPv4 vezérlő- és hibaüzeneteihez. Ugyanakkor az ICMPv6 olyan új funkciókat is tartalmaz, melyek az ICMPv4-ben még nem voltak jelen. Az ICMPv6 üzenetei IPv6-csomagokba kerülnek beágyazásra.

Az IPv6 a szomszédfelderítő protokolljának (Neighbor Discovery Protocol, ND vagy NDP) részeként négy új protokollt is tartalmaz.

A dinamikus címkiosztást lehetővé tevő üzenetek egy IPv6-os router és egy IPv6-os eszköz között a következők:

* Router keresés (Router Solicitation, RS) üzenet
* Router hirdetmény (Router Advertisement, RA) üzenet

A duplikált címek érzékelését és a címfeloldást biztosító üzenetek két IPv6-os eszköz között a következők:

* Szomszéd keresés (Neighbor Solicitation, NS) üzenet
* Szomszéd hirdetmény (Neighbor Advertisement, NA) üzenet

**Megjegyzés**: Az ICMPv6 ND tartalmazza az átirányítási üzenetet is, amely hasonló funkcióval rendelkezik, mint az ICMPv4 átirányítási üzenete.

Az ICMPv6 üzenetek illusztrálásához és magyarázatához kattintsunk az alábbi elemekre.

Az RA üzeneteket az IPv6-os router-ek küldik 200 másodpercenként, hogy címzési információkat biztosítsanak az IPv6-os hosztoknak. Az RA üzenet olyan címzési információkat tartalmaznak, mint az előtag és az előtag hossza, a DNS címe és a tartománynév. Egy állapotmentes cím autokonfigurációt (Stateless Address Autoconfiguration, SLAAC) használó hoszt az RA üzenetet küldő router link-local címét állítja be alapértelmezett átjáróként.

Az R1 egy router hirdetmény (Router Advertisment, RA) üzenetet küld az FF02::1 all-nodes (minden állomás) csoportos címre, amely így eljut PC1-hez is.

2001:db8:acad:1::1/64 PC1 2001:db8:acad:1::1/64 fe80::1

R1

RA üzenet

R1 elküld egy RA üzenetet: "Hello minden IPv6-os eszköz. Én R1 vagyok, és SLAAC alkalmazásával létrehozhatod a saját egyedi globális IPv6 címedet. Az előtag 2001:db8:acad:1::/64. Egyébiránt pedig alapértelmezett átjáróként használd az FE80::1 link-local címemet."

13.1.6

## Tudáspróba - ICMP üzenetek

Az űrlap teteje

Check your understanding of ICMP messages by choosing the BEST answer to the following questions.

1. Which two types of ICMP messages are common to both ICMPv4 and ICMPv6? (Choose two.)

Az űrlap alja

Which type of ICMPv6 message would a host send to acquire an IPv6 configuration when booting up?

[13.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[13.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ping és Traceroute ellenőrzések](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                   
*       

1. ICMP
2. Ping és Traceroute ellenőrzések

# Ping és Traceroute ellenőrzések

13.2.1

## Ping - A kapcsolatok ellenőrzése

Az előző témakörben bemutattuk a **ping** és traceroute (**tracert**) parancsokat. Ebben a témakörben azokról a szituációkról fogunk tanulni, amelyekben ezek az eszközök felhasználhatók, és ahogyan ezeket használnunk kell. A ping egy IPv4 és IPv6 segédprogram, amely ICMP visszhang kérés (Echo Request) és visszhang válasz (Echo Reply) üzeneteket használ a hosztok közötti kapcsolat ellenőrzésére.

Egy másik hálózati hoszt elérhetőségének ellenőrzésére egy visszhang kérés üzenetet küldünk neki a **ping** parancsot használva. Ha az adott címen lévő hoszt megkapja a visszhang kérés üzenetet, akkor ő erre egy visszhang válasz üzenettel fog reagálni. Ahogy ez a visszhang válasz megérkezik, a **ping** az elküldés és a megérkezés között eltelt idő megjelenítésével ad erről visszajelzést. Ebből következtethetünk a hálózat teljesítményére is.

A ping a válaszra csak egy bizonyos ideig vár. Ha az adott időn belül nem érkezik válasz, a ping egy üzenetben közli, hogy nem érkezett válasz. Egyfelől ez jelezhet egy problémát, de jelentheti azt is, hogy biztonsági megfontolásokból a hálózaton blokkolják a ping üzeneteket. Gyakran előfordul, hogy az első ping csomag időtúllépést jelez, amennyiben az ICMP visszhang kérés elküldése előtt még egy címfeloldást (ARP vagy ND) is el kell végezni.

Az összes kérés elküldése után a **ping** egy összefoglalót ad, amely tartalmazza sikeres küldések arányát, valamint az átlagos megfordulási időt (Round-trip Time, RTT).

A **ping** által elvégezhető kapcsolatvizsgálati tesztek a következők:

* A helyi loopback cím pingelése.
* Az alapértelmezett árjáró pingelése.
* Egy távoli hoszt pingelése.

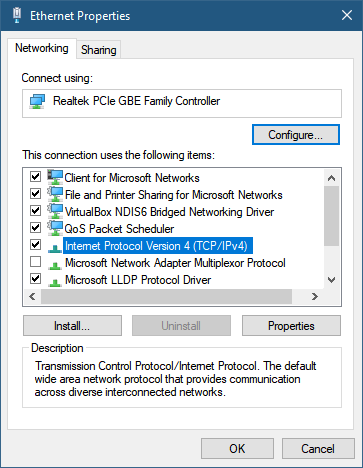
13.2.2

## A helyi loopback cím pingelése

A ping használható a helyi gép belső IPv4 és IPv6 beállításainak ellenőrzésére is. Ennek elvégzésére a **ping** utasítást a 127.0.0.1 helyi visszahurkolásos IPv4 címre kell alkalmazni (IPv6 esetén a cím ::1).

Amennyiben IPv4 esetén a 127.0.0.1, IPv6 esetén pedig a ::1 cím válaszol, akkor azt jelzi, hogy a helyi hoszton az IP megfelelően telepítve van. A válasz a kérésre a hálózati rétegtől érkezik. Ez a válasz azonban nem jelenti azt, hogy a cím, a maszk és az átjáró is megfelelően vannak beállítva. Nem jelez semmit a hálózat alsóbb rétegeinek állapotáról sem. Egyszerűen csak az IP-t ellenőrzi a hálózati rétegig. Egy hibaüzenet a TCP/IP működésképtelenségét jelzi az adott hoszton.

shows the Ethernet properties dialogue box shows that Internet Protocol Version 4 (TCP/IPv4) is installed and active which is proved with a ping to 127.0.0.1



C:\>ping 127.0.0.1

* A helyi hoszt pingelése megerősíti, hogy a TCP/IP telepítve van és megfelelően működik.
* A 127.0.0.1 pingelésekor az eszköz saját magát pingeli.

13.2.3

## Az alapértelmezett átjáró pingelése

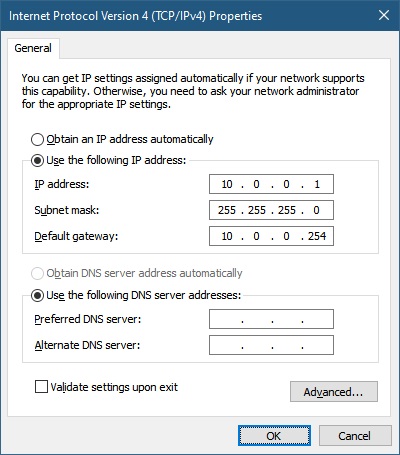
A **ping** segítségével azt is ellenőrizhetjük, hogy egy adott hoszt képes-e kommunikálni a helyi hálózaton. Ez általában a hoszt alapértelmezett átjárójának a megpingelését jelenti. Egy sikeres **ping** az alapértelmezett átjáróhoz azt jelzi, hogy mind a hoszt, mind pedig az alapértelmezett átjáróként szolgáló router interfész megfelelően működik a hálózaton.

Ehhez az ellenőrzéshez azért az alapértelmezett átjárót használjuk a leggyakrabban, mert a router jellemzően mindig működik. Ha az alapértelmezett árjáró nem válaszol, akkor a **ping** parancsot alkalmazhatjuk a helyi hálózaton egy olyan másik hosztra, amelyről biztosan tudjuk, hogy működik.

Ha az alapértelmezett átjáró, vagy egy másik hoszt válaszol, akkor helyi hoszt képes sikeresen kommunikálni a helyi hálózaton. Ha az alapértelmezett átjáró nem válaszol, de egy másik hoszt viszont igen, akkor az problémát jelez az alapértelmezett átjáró szerepét betöltő router interfésszel.

Lehetséges ok, hogy az alapértelmezett átjáró hibásan lett beállítva az adott hoszton. Egy másik lehetőség pedig, hogy a router interfész teljesen működőképes, viszont olyan biztonsági szabályokat állítottak be rajta, amelyek megakadályozzák a ping kérések feldolgozását vagy megválaszolását.

The graphic shows the Ethernet properties dialogue box configured with a static IP address, subnet mask, and default gateway. The topology shows the PC sending an echo request to the router default gateway and the routers echo response reply.



ECHO REQUESTECHO REPLY10.0.0.1  
255.255.255.010.0.0.254  
255.255.255.0G0/0/0

A hoszt az alapértelmezett átjáróját pingeli, egy ICMP visszhang kérés (Echo Request) üzenet küld neki. Az alapértelmezett átjáró egy visszhang választ (Echo Reply) küld az elérhetőségének megerősítésére.

13.2.4

## Távoli hoszt pingelése

A ping arra is jó, hogy egy helyi állomás távoli hálózatok irányába történő kommunikációját teszteljük. A helyi állomás megpingelhet egy távoli hálózaton lévő IPv4 hosztot is (lásd ábra). A router az irányítótábláját használja a csomagok továbbításához.

Ha a ping sikeres, akkor azzal a köztes hálózat nagy részének megfelelő működését igazolhatjuk. Egy sikeres **ping** az interneten keresztül megerősíti a helyi hálózat kommunikációját, az alapértelmezett átjáróként szolgáló router, valamint a helyi és a távoli hálózatok között lévő köztes router-ek működését is.

Mindezek mellett nyilván ellenőrizhetjük a távoli hoszt elérhetőségét is. Ha a távoli hoszt nem tudna a saját helyi hálózatán kívülre kommunikálni, akkor válaszolni sem tudna.

**Megjegyzés**: Számos hálózati rendszergazda korlátozza vagy tiltja az ICMP üzenetek bejutását a vállalati hálózatba, ezért a **ping** válaszok hiányát biztonsági megszorítások is okozhatják.

animation shows a ping echo request to a remote network that is routed through a router and the echo reply that is routed back from the remote network

Echo request

Echo reply

IP Routing Table

13.2.5

## Traceroute - Az útvonal ellenőrzése

A pinget két hoszt közötti kapcsolat ellenőrzésére használjuk, de semmi információt nem ad a két gép közötti egyéb eszközök részleteiről. A traceroute (**tracert**) olyan segédprogram, amely listát generál az útvonal során érintett ugrásokról. Ez a lista fontos ellenőrzési és hibakeresési információkat tartalmazhat. Ha egy adat eléri a célját, akkor ez a nyomkövetés a két hoszt közötti útvonalon lévő routerek interfészeit listázza ki. Ha az adat elakad valamelyik ugrásnál, az utolsóként választ adó router címe fontos információ lehet a probléma vagy biztonsági korlátozás helyének megállapításában.

**Megfordulási idő**

A traceroute az útvonal minden egyes ugrásához megfordulási időt (Round Trip Time, RTT) ad és jelzi, ha nem reagál. A megfordulási idő az az időintervallum, amely alatt a csomag eléri a távoli hosztot és tőle a válasz vissza is érkezik. Az elveszett vagy megválaszolatlan csomagok jelzésére egy csillagot (\*) használnak.

Ez az információ segít megtalálni a problémás routert az útvonalon, vagy azt jelezheti, hogy a router úgy van beállítva, hogy ne az válaszoljon. Ha a kimenetében egy bizonyos ugrásnál magas válaszidőket vagy adatvesztést mutat, akkor az annak a jele, hogy a router vagy a kapcsolatai leterheltek.

**IPv4 TTL és IPv6 ugrási korlát**

A traceroute az IPv4 TTL mezőjét, valamint az IPv6 ugrási korlát mezőjét használja ki a 3. rétegbeli fejlécekben, kiegészítve az ICMP időtúllépés (Time Exceeded) üzenetével.

Az ábrán lévő animáció lejátszásával megnézhetjük, hogy a traceroute hogyan használja ki a TTL értéket.

animation shows a traceroute to a remote network that crosses three routers. The traceroute will take 4 echo requests to reach its destination

ICMP Echo reply

ICMP  
Time Exceeded

ICMP  
Time Exceeded

ICMP  
Time Exceeded

Traceroute  
192.168.1.2  
(TTL = 4)

Traceroute  
192.168.1.2  
(TTL = 3)

Traceroute  
192.168.1.2  
(TTL = 2)

Traceroute  
192.168.1.2  
(TTL = 1)

A traceroute által kiküldött első üzenetek TTL értéke 1 lesz. Emiatt az első forgalomirányítónál a csomag TTL értéke lejár, ami időtúllépést eredményez. A router erre egy visszaküldött ICMPv4 időtúllépés üzenettel reagál. A traceroute ebből az üzenetből tudta meg az első ugrás címét.

A traceroute ezután fokozatosan növeli az üzenetekben a TTL mező értékét (2, 3, 4...). Ezzel kapja meg az egyes ugrások címeit, ahogy a csomagok egyre előrébb jutnak az útvonalon. A TTL mező értéke fokozatosan növekszik, amíg el nem érjük a célállomást, vagy amíg el nem ér egy előre meghatározott értéket.

Ha elértük a végső célt, a hoszt az ICMP időtúllépés helyett egy ICMP port nem elérhető (Port Unreachable), vagy egy visszhang válasz (Echo Reply) üzenettel válaszol.

13.2.6

## Packet Tracer - IPv4 és IPv6-címek ellenőrzése

Ugyanabban a hálózatban az IPv4 és IPv6 egymás mellett is működhetnek. A PC parancssorának használata közben néhány különbséget fedezhetünk fel a parancsok használatában és a kimenet formátumában.

[IPv4- és IPv6-címzés ellenőrzése](https://contenthub.netacad.com/courses/itn/_common/13.2.6-packet-tracer---verify-ipv4-and-ipv6-addressing_hu-HU.pka)

13.2.7

## Packet Tracer - Ping és Traceroute használata a hálózati kapcsolat ellenőrzésére

A feladat kapcsolódási problémákat mutat be. A hálózatról történő információ gyűjtés és dokumentálása mellett meg kell kell keresni problémákat és elfogadható megoldást kell találni a kapcsolat helyreállítására.

[Ping és traceroute használata a hálózati kapcsolatok ellenőrzésére](https://contenthub.netacad.com/courses/itn/_common/13.2.7-packet-tracer---use-ping-and-traceroute-to-test-network-connectivity_hu-HU.pka)

[13.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[ICMP üzenetek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[13.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                            

1. ICMP
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

13.3.1

## Packet Tracer - Az ICMP használata a hálózati kapcsolat ellenőrzéséhez és javításához

Ebben a laborgyakorlatban az ICMP segítségével ellenőrizzük a hálózati kapcsolatot és megkeressük a problémákat. Kijavítunk egyszerűbb konfigurációs hibákat és helyreállítjuk a hálózati kapcsolatot.

Használjuk az ICMP-t a kapcsolódási hibák megtalálásához.

A hálózati eszközök konfigurálásával javítsuk a csatlakozási hibákat.

[Az ICMP használata a hálózati kapcsolat ellenőrzéséhez és javításához](https://contenthub.netacad.com/courses/itn/_common/13.3.1-packet-tracer---use-icmp-to-test-and-correct-network-connectivity_hu-HU.pka)

13.3.2

## Laborgyakorlat - Ping és traceroute használata a hálózati kapcsolatok ellenőrzésére

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Hálózat építése és konfigurálása
* Bölüm 2: Ping használata alapszintű hálózattesztelésre
* Bölüm 3: Tracert és traceroute parancsok használata alapszintű hálózattesztelésre
* Bölüm 4: Topológia hibaelhárítása

13.3.3

## Miről tanultunk ebben a fejezetben?

**Az ICMP üzenettípusok**

A TCP/IP protokollcsomag hiba- és információs üzeneteket biztosít az IP-eszközökkel történő kommunikációhoz. Ezek az üzenetek az ICMP által kerülnek elküldésre. Az üzeneteknek a célja, hogy visszajelzést adjanak az IP-csomagok feldolgozásával kapcsolatos problémákról. Az ICMPv4-re és az ICMPv6-ra egyaránt jellemző üzenetek az alábbiakra vonatkozhatnak: hosztok elérhetősége, cél vagy szolgáltatás elérhetetlensége és az időtúllépés. Az ICMP Echo üzenet egy IP-hálózaton lévő hoszt elérhetőségét vizsgálja. A helyi gép egy ICMP visszhang kérés üzenetet küld a hosztnak. Ha a hoszt elérhető, akkor egy visszhang válasz üzenettel válaszol. Ezen alapul a **ping** segédprogram. Ha egy hoszt vagy egy átjáró olyan csomagot kap, amelyet nem tud továbbítani, akkor egy ICMP cél nem elérhető (Destination Unreachable) üzenettel jelezheti ezt a forrás felé. Az üzenet tartalmaz egy kódot is, amely leírja, hogy a csomagot miért nem sikerült kézbesíteni. Az ICMPv4 időtúllépés üzenetét használja egy router annak jelzésére, hogy egy csomag élettartam (TTL) mezője nullára csökkent, ezért nem tudja azt továbbítani. Ha egy router fogad egy csomagot és annak TTL mezőjét nullára csökkenti, akkor a csomagot eldobja, és egy időtúllépés üzenetet küld a forrás felé. Az ICMPv6 szintén egy időtúllépés üzenetet küld el ebben a helyzetben. Az ICMPv6 az IPv6 ugrási korlát (Hop Limit) mezőjét használja annak jelzésére, hogy egy csomag lejárt-e. A **traceroute** segédprogram is az időtúllépés üzeneteket használja. Egy IPv6-os router és eszköz közötti üzenetváltás dinamikus címkiosztás, RS és RA üzeneteket tartalmaz. Az IPv6-os eszközök közötti üzenetei az átirányítás (hasonló az IPv4-hez), az NS és az NA üzenetek.

**Ping és traceroute ellenőrzés**

A ping (IPv4 és IPv6 esetén egyaránt) ICMP visszhang kérés és visszhang válasz üzeneteket használ a hosztok közötti kapcsolat ellenőrzésére. A hálózaton egy másik hoszt elérhetőségének ellenőrzésére a ping parancs alkalmazásával egy visszhang kérés üzenetet küldünk a hoszt címére. Ha a hoszt az adott címen megkapja a visszhang kérést, akkor erre egy visszhang válasz üzenettel válaszol. Minden egyes visszhang válasz megérkezésekor a ping kiírja a kérés elküldése és a válasz megérkezése közt eltelt időt. Az összes kérés elküldése után a ping egy összegzést is ad, amelyben kiírja a sikerességi arányt, valamint az átlagos megfordulási időt. A ping használható egy gép belső IPv4 és IPv6 beállításainak ellenőrzésére is. Ehhez a helyi visszahurkolásos 127.0.0.1 IPv4 címet (IPv6 esetén ::1) kell pingelni. Egy hoszt alapértelmezett átjárójának IP-címének pingelésével a **ping** parancsot használhatjuk annak ellenőrzésére is, hogy a hoszt képes-e a helyi hálózaton kommunikálni. Az alapértelmezett átjáró sikeres pingelése azt jelzi, hogy a hoszt és az alapértelmezett átjáró szerepét betöltő router interfész egyaránt működnek a helyi hálózaton. A ping arra is jó, hogy egy helyi hoszt távoli hálózatok irányába történő kommunikációját teszteljük. A helyi hosztról **ping**elhetjük egy távoli hálózat egy működő IPv4 állomását is. A traceroute (tracert) egy listát generál azokról az ugrásokról, amelyeket az útvonal során elért. Ez a lista ellenőrzési és hibakeresési információkat biztosít. Ha egy adat eléri a célját, akkor ez a nyomkövetés a két hoszt közötti útvonalon lévő routerek interfészeit listázza ki. Ha az adat elakad valamelyik ugrásnál, az utolsóként választ adó router címe fontos információ lehet a probléma vagy biztonsági korlátozás helyének megállapításában. A megfordulási idő az az időintervallum, amely alatt egy csomag eléri a távoli hosztot és tőle a válasz vissza is érkezik. A traceroute a IPv4 TTL és az IPv6 ugrási korlát 3. rétegbeli fejlécmezőket használja, valamint a ICMP időtúllépés üzenetét.

13.3.4

## Ellenőrző kvíz - ICMP

Az űrlap teteje

1. A technikus egy olyan hálózatban végez hibaelhárítást, amelyben azt gyanítják, hogy a hálózati útvonal egy hibás csomópontja csomagok elvesztését okozza. A technikus csak a végponti készülék IP címét ismeri, a köztes eszközökről semmilyen információ nincs a birtokában. Melyik parancsot használhatja a hibás csomópont azonosítására?

Az űrlap alja

Egy felhasználó az ügyfélszolgálathoz fordul, mert nem tud a fájlszerverhez csatlakozni. Az ügyfélszolgálati technikus megkéri a felhasználót, hogy pingelje meg az állomáson beállított alapértelmezett átjárót. Mi a célja ennek a **ping** parancsnak?

Mi a **tracert** parancs funkciója, amely eltér a **ping** parancstól, amikor munkaállomáson használják őket?

Melyik ICMP-üzenetet használja a traceroute segédprogram a két végállomás közötti elérési út megkeresésekor?

Melyik segédprogram használja az Internet Control Messaging Protocol (ICMP) protokollt?

Melyik protokollt használja az IPv4 és az IPv6 a hibaüzenetekhez?

A hálózati rendszergazda egy routeren kiadott **ping** parancs segítségével teszteli a hálózati kapcsolatot. Melyik szimbólum jelenik meg annak jelzésére, hogy az ICMP visszhangválasz üzenetére történő várakozás közben lejárt az idő?

Melyik két információ határozható meg a **ping** paranccsal? (Két jó válasz van.)

Konu 13.2.0 - A **ping** parancs visszajelzést ad arról az időről, ami eltelik egy távoli állomásra küldött visszhangkérés elküldésétől a visszhangválasz megérkezéséig. Ebből következtethetünk a hálózat teljesítményére is. A sikeres **ping** azt is jelzi, hogy a célállomás elérhető volt a hálózaton keresztül.

Melyik parancs használható két eszköz közötti kapcsolat tesztelésére a visszhangkérés és a visszhangválasz üzenetek használatával?

Melyik mező tartalmát használja az ICMPv6 annak meghatározására, hogy a csomag már lejárt-e?

Melyik protokoll ad visszajelzést a célállomásról a forrásállomás felé a csomagkézbesítés hibáival kapcsolatban?

Egy hálózati rendszergazda sikeresen tudja pingelni a [www.cisco.com](http://www.cisco.com) URL-en elérhető szervert, de nem tudja pingelni a vállalat webszerverét, ami egy másik városban lévő internetszolgáltató területén helyezkedik el. Melyik eszköz vagy parancs segítségével határozható meg az a router, ahol a csomagvesztés vagy -késleltetés történik?

Milyen üzenetet küld az állomás, hogy ellenőrizze az IPv6-cím egyediségét annak használata előtt?

[13.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Ping és Traceroute ellenőrzések](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                        
*     

1. Szállítási réteg
2. Bevezetés

# Bevezetés

14.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a szállítási réteget bemutató fejezetben.

A szállítási rétegben, ahogy a neve is sugallja, történik az adatok állomások közötti szállítása. Itt lendül igazán mozgásba a hálózatunk! Két szállítási rétegbeli protokoll létezik: a TCP és az UDP. Gondoljunk úgy a TCP-re, mintha egy ajánlott postai levelet kapnánk. Alá kell írnunk, mielőtt a postás odaadná. Ez kissé lassítja a folyamatot, de a feladó biztosan tudja, hogy megkaptuk a levelet. Ezzel szemben az UDP inkább egy hagyományos, felbélyegzett levélre emlékeztet. Megérkezik a postaládánkba (már ha igen), valószínűleg nekünk címezték, de előfordulhat, hogy valaki másnak, aki nem is lakik itt. Az is előfordulhat, hogy egyáltalán nem érkezik meg a postaládánkba. A feladó nem lehet biztos benne, hogy megkaptuk. Mindazonáltal vannak olyan esetek, amikor mégis az UDP, mint egy felbélyegzett levél, a szükséges protokoll. Ez a témakör azt mutatja be, hogy miként működik a TCP és az UDP a szállítási rétegben. Lesznek később a fejezetben olyan videók is, amelyek segítenek megérteni ezeket a folyamatokat.

14.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe: Szállítási réteg**

**Fejezet célja:** A szállítási rétegbeli protokollok műveleteinek összehasonlítása a végpontok közötti kommunikáció támogatásában betöltött szerepük szerint.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Az adatok szállítása** | A szállítási réteg céljának ismertetése a végpontok közötti kommunikáció során történő adatátvitel felügyeletében. |
| **A TCP áttekintése** | A TCP jellemzőinek ismertetése. |
| **Az UDP áttekintése** | Az UDP jellemzőinek ismertetése. |
| **Portszámok** | A TCP- és az UDP-portszámok használatának elmagyarázása. |
| **A TCP kommunikációs folyamata** | Annak ismertetése, hogy a TCP-munkamenet létrehozási és lezárási folyamata miként könnyíti meg a megbízható kommunikációt. |
| **Megbízhatóság és forgalomszabályozás** | Annak ismertetése, hogy miként zajlik a TCP-protokoll adategységeinek továbbítása és nyugtázása, a garantált kézbesítés érdekében. |
| **UDP-kommunikáció** | A szállítási rétegbeli protokollok működésének összehasonlítása a végpontok közötti kommunikációban betöltött szerepük szerint. |

[13.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az adatok szállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                             
*     

1. Szállítási réteg
2. Az adatok szállítása

# Az adatok szállítása

14.1.1

## A szállítási réteg szerepe

Az alkalmazási réteg programjai olyan adatokat generálnak, amelyeket mozgatni kell a forrás- és célállomások között. A szállítási réteg felel a különböző állomásokon futó alkalmazások közötti logikai kommunikációért. Ez magában foglalhat olyan szolgáltatásokat, mint például a két állomás közötti ideiglenes munkamenet létrehozását és az alkalmazás információinak megbízható továbbítását.

Ahogy az ábrán is látható, a szállítási réteg egyfajta kapocs az alkalmazási réteg, valamint a hálózati átvitelért felelős alsóbb rétegek között.

shows a diagram of how devices use the transport layer to move data between applications in the TCP/IP model

The transport layer moves data between applications on devices in the network.ApplicationTransportInternetNetwork AccessTCP/IP ModelApplicationTransportInternetNetwork AccessTCP/IP Model

A szállítási rétegnek nincs tudomása a célállomás típusáról, az adathordozó típusáról, az adatok által megtett útvonalról, a kapcsolat torlódásáról vagy a hálózat méretéről.

A szállítási rétegben két protokoll található:

* TCP
* UDP

14.1.2

## A szállítási réteg feladatai

A szállítási rétegnek számos feladata van.

További információért kattintsunk a gombokra!

**Az egyedi párbeszédek nyomon követése**

A szállítási rétegben a forrás- és a célalkalmazás között áramló minden egyes konkrét adathalmazt párbeszédnek nevezünk. A párbeszédek nyomon követése egyesével történik. A szállítási réteg feladata, hogy fenntartsa és nyomon kövesse az ilyen többszörös párbeszédeket.

Ahogy az ábrán is látható, egy állomás számos alkalmazást futtathat, amelyek egyidejűleg kommunikálnak a hálózaton keresztül.

A legtöbb hálózat korlátozza az egy csomag által szállítható adatmennyiséget. Ezért az adatokat kezelhető darabokra kell osztani.

The PC simultaneously runs multiple network applications including an email client, instant messaging client, web browser web pages, streaming video, and a video conference client.



To: you@example.com  
From: me@example.com  
Subject: VacationE-mailOnline Video ChattingStreaming VideoMultiple Web PagesInstant MessagingNetwork

14.1.3

## Szállítási rétegbeli protokollok

Az IP csak a struktúrával, a címzéssel és csomagok irányításával törődik. Az IP nem határozza meg, hogy miként történjen a csomagok szállítása és kézbesítése.

A szállítási rétegbeli protokollok határozzák meg azt, hogy az üzenetek miként szállíthatók az állomások között, valamint a párbeszédek megbízhatósági követelményeinek kezeléséért felelnek. A szállítási réteg tartalmazza a TCP- és az UDP-protokollokat.

A különböző alkalmazások eltérő megbízhatósági feltételeket támasztanak. Ezért a TCP/IP az ábrán látható két szállítási rétegbeli protokollt biztosítja.

shows how application layer protocols like FTP, HTTP, SMTP use TCP at the transport layer and DNS and TFTP use UDP. How they all use IP at the internet layer regardless of whether they connect to a LAN or a WAN at the network access layer

ApplicationTransportInternetNetwork AccessFTPHTTP  
(www)SMTP  
(email)DNSTFTPTCPUDPIPLAN  
connectionsWAN  
connections

14.1.4

## TCP (Transmission Control Protocol)

Az IP csak a struktúrával, a címzéssel és a csomagok irányításával törődik a forrás és a végső cél között. Az IP-nek nem feladata, hogy garantálja a kézbesítést, vagy eldöntse, hogy szükség van-e a küldő és a címzett közötti kapcsolat létrehozására.

A TCP egy megbízható, teljes körű szállítási rétegbeli protokoll, amely garantálja az összes adat célba érkezését. A TCP olyan mezőket tartalmaz, amelyek biztosítják az alkalmazásadatok kézbesítését. Ezek a mezők további feldolgozást igényelnek a küldő és fogadó állomásokon.

**MEGJEGYZÉS:** A TCP szegmensekre bontja az adatokat.

A TCP-átvitel sok hasonlóságot mutat a forrástól a célig nyomon követhető postai csomagküldéssel. Ha egy rendelést több szállítmányra bontanak szét, akkor az ügyfél online ellenőrizheti a kiszállítások sorrendjét.

A TCP megbízhatóságot és adatfolyam-vezérlést biztosít az alábbi alapvető műveletek segítségével:

* Adott alkalmazástól valamely eszközig küldött adatszegmensek számozása és nyomon követése.
* A megérkezett adatok nyugtázása.
* A nem nyugtázott adatok újraküldése egy bizonyos idő után.
* Az esetlegesen rossz sorrendben érkező adatszegmensek sorbarendezése.
* Hatékony, a fogadó fél által elfogadható sebességgel történő adatküldés.

A párbeszéd állapotának fenntartása és az információ nyomon követése érdekében a TCP-nek először kapcsolatot kell létesítenie a küldő és a címzett között. Ezért a TCP egy kapcsolatorientált protokoll.

A küldő és a címzett között továbbított TCP-szegmensek és nyugták megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

animation shows a connection to an FTP server initiated with a TCP 3-way handshake and the data segments accounted for using sequence numbers and acknowledgements

A file is sent to a server using the File Transfer Protocol (FTP) application. TCP tracks the conversation and divides the data to be sent into 6 segments.

The first 3 out of 6 segments are forwarded to the server.

The file server acknowledges the first 3 segments received.

The client forwards the next 3 segments.

No segments are received, no acknowledgement is sent.

The client resends the final 3 segments.

The final 3 segments are received and acknowledged.

**ISP 1**

FTP

Server Farm

Internet

**ISP 2**

14.1.5

## UDP (User Datagram Protocol)

Az UDP egyszerűbb szállítási rétegbeli protokoll, mint a TCP. Nem kínál megbízhatóságot és adatfolyam-vezérlést, ami azt jelenti, hogy kevesebb fejlécmezőre van szüksége. Mivel a küldő és fogadó UDP-folyamatoknak nem kell kezelniük a megbízhatóságot és az adatfolyam-vezérlést, ez azt jelenti, hogy az UDP-datagramok gyorsabban feldolgozhatók, mint a TCP-szegmensek. Az UDP csupán alapfunkciókat biztosít az adatcsomagok (datagramok) alkalmazások között történő szállítása során, így nagyon csekély többletterhelést okoz és adatellenőrzést sem végez.

**MEGJEGYZÉS:** Az UDP az adatokat datagramokra bontja, amelyeket szegmenseknek is nevezünk.

Az UDP egy összeköttetés-mentes protokoll. Mivel az UDP nem kínál megbízhatóságot vagy adatfolyam-vezérlést, nincs szüksége kapcsolat létrehozására. Mivel az UDP nem követi nyomon a kliens és a szerver között küldött vagy fogadott információkat, az UDP-t állapot nélküli protokollnak is nevezzük.

Az UDP legjobb szándékú kézbesítési protokoll néven is ismert, mivel nem nyugtázza az adatok célba érkezését. UDP esetén nincs olyan szállítási rétegbeli folyamat, amely tájékoztatná a küldőt a sikeres kézbesítés tényéről.

Az UDP sokban hasonlít a normál, nem ajánlott postai levél kézbesítéséhez. A levél feladója ilyenkor nincs tisztában azzal, hogy tudja-e valaki fogadni az adott levelet. Ugyanakkor a postahivatal sem felelős a levél nyomon követéséért vagy a feladó tájékoztatásáért, amennyiben a levél nem éri el végcélját.

A küldő és a fogadó állomások között továbbított UDP-szegmensek megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

animation shows a connection to a TFTP server using UDP datagrams which are sent without sequence numbers or acknowledgments

A file is sent to a server using the Trivial File Transfer Protocol (TFTP) application. UDP divides the data into datagrams and sends them using best-effort delivery.

The file server receives all 6 segments, no acknowledgment is sent.

**ISP 1**

TFTP

Server Farm

Internet

**ISP 2**

14.1.6

## Megfelelő szállítási protokoll a megfelelő alkalmazáshoz

Néhány alkalmazás elvisel ugyan bizonyos mértékű adatvesztést a hálózati átvitel során, de elfogadhatatlannak tekint bármilyen késést. Az ilyen alkalmazások számára a kisebb mértékű hálózati többletterhelés miatt az UDP jobb választás. Az UDP-t olyan alkalmazások részesítik előnyben, mint az IP alapú hangátvitel (VoIP). A nyugtázás és az újraküldés lassítaná a kézbesítést, és vállalhatatlanná tenné a hang alapú beszélgetést.

Az UDP-t a kérés-válasz típusú alkalmazások is használják, ahol az adatmennyiség minimális, és az újraküldés gyorsan elvégezhető. A tartománynév-szolgáltatás (DNS) például UDP-t használ az ilyen típusú tranzakciókhoz. A kliens lekéri egy ismert tartománynévhez tartozó IPv4- és IPv6-címeket egy DNS-szervertől. Ha a kliens előre meghatározott időn belül nem kap választ, egyszerűen újraküldi a kérést.

Például, ha a videofolyam egy vagy két szegmense nem érkezik meg, az csupán pillanatnyi zavart okoz a közvetítésben. Ilyenkor torzulhat a megjelenített kép és a hang, de a legtöbb esetben a felhasználó észre sem veszi. A másik esetben viszont az online közvetítés képe vagy hangja esne szét, ha a céleszköznek minden elveszett adattal foglalkozni kellene, és így az újraküldésre történő várakozás késést okozna. Ilyenkor célravezetőbb lehet, ha a beérkezett szegmensek alapján előállítjuk a lehető legjobb képet és hangot, valamint lemondunk a megbízhatóságról.

Más alkalmazások esetében fontos, hogy az összes adat megérkezzen, és a megfelelő sorrendben feldolgozható legyen. Az ilyen típusú alkalmazásoknál a TCP szállítási protokollt használják. Például az adatbázisok, a webböngészők, az e-mail kliensek és a hasonló alkalmazások megkívánják, hogy minden adat az eredeti sorrendben és hiánytalanul érkezzen meg. Bármely elveszett adat tönkreteheti a kommunikációt, amely így hiányos és feldolgozhatatlan lesz. Például fontos, hogy amikor webes felületen férünk hozzá a banki adatainkhoz, akkor megbizonyosodjunk arról, hogy az összes információ elküldése és fogadása megfelelően történik.

A fejlesztőknek kell kiválasztani, hogy melyik protokolltípus felel meg az alkalmazások által támasztott követelményeknek. A videóküldés TCP-n és UDP-n keresztül is történhet. A letárolt (mentett) hangot és videót közvetítő alkalmazások általában TCP-t használnak. Az alkalmazás TCP-t használ a puffereléshez, a sávszélesség vizsgálatához és a torlódásvezérléshez annak érdekében, hogy jobb felhasználói élményt biztosítson.

A valós idejű videó és hang általában UDP-t használ, de TCP, illetve a kettő együtt is használható. A videokonferencia-alkalmazások alapértelmezés szerint UDP-t használhatnak, de mivel sok tűzfal blokkolja az UDP-t, az alkalmazás TCP-t is használhat.

A letárolt (mentett) hangot és videót közvetítő alkalmazások TCP-t használnak. Ha például a hálózat hirtelen nem tudja biztosítani az igény szerinti videó (Video on Demand) megtekintéséhez szükséges sávszélességet, az alkalmazás szünetelteti a lejátszást. A szünet alatt megjelenik egy „pufferelés...” üzenet, miközben a TCP az adatfolyam helyreállításán dolgozik. Amikor az összes szegmens sorba van rendezve és helyreáll a minimális sávszélesség, a TCP-munkamenet és a film lejátszása folytatódik.

Az ábrán lévő táblázat az UDP és TCP közötti különbségeket foglalja össze.

lists the differences between UDP: fast, low overhead, no acknowledgements, no resending and TCP: reliable, acknowledges data, resends lost data, and delivers data with sequence numbers



TCPUDPVoIP   
(IP telephony)DNS   
(Domain Name Resolution)SMTP/IMAP   
(E-mail)HTTP/HTTPS   
(World Wide Web Required protocol properties:

* Fast
* Low overhead
* Does not require acknowledgements
* Does not resend lost data
* Delivers data as it arrives

Required protocol properties:

* Reliable
* Acknowledges data
* Resends lost data
* Delivers data in sequenced order

14.1.7

## Tudáspróba - Az adatok szállítása

Az űrlap teteje

Check your understanding of the transport layer by choosing the correct answer to the following questions.

1. Which layer is responsible for establishing a temporary communication session between the source and destination host applications?

Az űrlap alja

Which three are transport layer responsibilities? (Choose three.)

Which transport layer protocol statement is true?

Which transport layer protocol would be used for VoIP applications?

[14.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A TCP áttekintése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                
*     

1. Szállítási réteg
2. A TCP áttekintése

# A TCP áttekintése

14.2.1

## TCP-funkciók

Az előző témakörben megtanultuk, hogy a szállítási réteg két protokollja a TCP és az UDP. Ez a témakör további részleteket ad arról, hogy mit csinál a TCP, és mikor érdemes használni az UDP helyett.

A TCP és az UDP közötti különbségek megértéséhez tisztában kell lenni azzal, hogy az egyes protokollok miként valósítanak meg bizonyos megbízhatóságot szolgáló funkciókat, illetve hogyan követik nyomon a párbeszédeket.

Az adatok szegmentálását és ismételt összeállítását támogató alapfunkciókon felül a TCP az alábbiakat is biztosítja:

* **Munkamenet létrehozása -** A TCP egy összeköttetés alapú protokoll, amely még a forgalom megkezdése előtt egyezteti, majd létrehozza a forrás- és céleszközök közötti állandó kapcsolatot (más néven munkamenetet). A munkamenet létrehozása során az eszközök egyeztetik az adott idő alatt továbbítható forgalom mennyiségét, valamint szorosan felügyelik a két fél közötti adatkommunikációt.
* **Megbízható kézbesítés biztosítása -** Számos oka lehet annak, hogy a hálózaton keresztül átvitt adatszegmensek megsérülnek vagy teljesen elvesznek. A TCP biztosítja, hogy a forrás által küldött minden szegmens megérkezzen a célállomásra.
* **Sorrendtartó kézbesítés biztosítása -** Mivel a hálózatok számos, különböző átviteli sebességgel rendelkező útvonalat kínálnak, előfordulhat, hogy az adatok rossz sorrendben érkeznek meg. A TCP a szegmensek számozásával és sorba rendezésével garantálja, hogy azok a megfelelő sorrendben legyenek újra összeállítva.
* **Adatfolyam-vezérlés támogatása -** A hálózati állomások korlátozott erőforrásokkal (pl.: memóriával és feldolgozási teljesítménnyel) rendelkeznek. Ha a TCP értesül ezen erőforrások túlzott mértékű igénybevételéről, kérheti, hogy a küldő alkalmazás csökkentse az adatátvitel sebességét. Ezt a TCP a forrás által küldött adatmennyiség szabályozásával éri el. Az adatfolyam-vezérlés megakadályozhatja az adatok újraküldésének szükségességét, ha a fogadó állomás erőforrásai túlterheltek.

Bővebb információért a TCP-vel kapcsolatban keressünk rá az interneten az RFC 793 kifejezésre.

14.2.2

## TCP-fejléc

A TCP egy állapottartó protokoll, amely nyomon követi a munkamenet minden változását. A munkamenet állapotának nyomon követéséhez a TCP rögzíti, hogy mely információk küldése, illetve nyugtázása történt meg. Az állapottartó kapcsolat a munkamenet létrehozásával indul, majd a munkamenet lezárásával ér véget.

A TCP-szegmens 20 bájtot (azaz 160 bitet) ad hozzá az alkalmazási réteg adatainak beágyazásakor. Az ábra a TCP-fejlécben lévő mezőket mutatja.

shows the fields in the TCP header

20 BytesSource Port (16)Destination Port (16)Acknowledgement Number (32)Header Length(4)Window (16)Checksum (16)Urgent (16)Options (0 or 32\*3 if any)Application Layer Data(Size Varies) Sequence Number (32)Reserved (6)Control Bits (6)

14.2.3

## A TCP-fejléc mezői

A táblázat azonosítja és leírja a TCP-fejléc tíz mezőjét.

| TCP Header Field DescriptionSource Port A 16-bit field used to identify the source application by port number.Destination PortA 16-bit field used to identify the destination application by port number.Sequence Number A 32-bit field used for data reassembly purposes.Acknowledgment Number A 32-bit field used to indicate that data has been received and the next byte expected from the source.Header Length A 4-bit field known as ʺdata offsetʺ that indicates the length of the TCP segment header.Reserved A 6-bit field that is reserved for future use.Control bits A 6-bit field used that includes bit codes, or flags, which indicate the purpose and function of the TCP segment.Window size A 16-bit field used to indicate the number of bytes that can be accepted at one time.Checksum A 16-bit field used for error checking of the segment header and data.Urgent A 16-bit field used to indicate if the contained data is urgent. | |
| --- | --- |
| **TCP-fejléc mező** | **Leírás** |
| **Forrásport** | 16 bites mező, amely a forrásalkalmazás portszám szerinti azonosítására szolgál. |
| **Célport** | 16 bites mező, amely a célalkalmazás portszám szerinti azonosítására szolgál. |
| **Sorszám** | 32 bites mező, amelyet az adatok ismételt összeállításához használnak. |
| **Nyugtaszám** | 32 bites mező, amely jelzi, hogy az adatok megérkeztek, és a forrástól várható a következő bájt. |
| **Fejléc hossza** | 4 bites mező, amelyet ʺadatkezdetʺ néven ismerünk, és amely a a TCP-szegmens fejlécének hosszát jelzi. |
| **Fenntartott** | 6 bites mező, amely későbbi használatra van fenntartva. |
| **Vezérlőbitek** | 6 bites mező, amely olyan bitkódokat vagy jelzőbiteket tartalmaz, amelyek a TCP-szegmens célját és funkcióját jelzik. |
| **Ablakméret** | 16 bites mező, amely jelzi az egyszerre fogadható bájtok számát. |
| **Ellenőrző összeg (Checksum)** | 16 bites mező, amellyel az adatszegmens fejlécének és adattartalmának sértetlensége ellenőrizhető. |
| **Sürgősség** | 16 bites mező, amely jelzi, ha az adattartalom sürgős. |

14.2.4

## TCP-t használó alkalmazások

A TCP kiváló példája annak, hogy a TCP/IP protokollkészlet különböző rétegeinek milyen konkrét szerepük van. A TCP kezeli az adatfolyam szegmensekre történő felosztásával kapcsolatos összes feladatot, biztosítva a megbízhatóságot, az adatfolyam-vezérlést és a szegmensek sorba rendezését. A TCP mentesíti az alkalmazást a fenti feladatok elvégzése alól. Az ábrán látható és azokhoz hasonló alkalmazások egyszerűen átküldhetik az adatfolyamot a szállítási rétegnek, majd használják a TCP szolgáltatásait.

shows arrows pointing both directions from HTTP, FTP, SMTP, and SSH to TCP and then from TCP to IP

TCPIPFTPSMTPHTTPSSH

14.2.5

## Tudáspróba - A TCP áttekintése

Az űrlap teteje

Check your understanding of TCP by choosing the correct answer to the following questions.

1. Which transport layer protocol ensures reliable same-order delivery?

Az űrlap alja

Which TCP header statement is true?

Which two applications would use the TCP transport layer protocol? (Choose two.)

[14.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az adatok szállítása](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az UDP áttekintése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                   
*     

1. Szállítási réteg
2. Az UDP áttekintése

# Az UDP áttekintése

14.3.1

## UDP-funkciók

Ez a témakör az UDP-vel foglalkozik. Mit csinál és mikor érdemes használni a TCP helyett? Az UDP egy legjobb szándékú szállítási protokoll. Az UDP egy könnyed szállítási protokoll, amely az adatok szegmentálását és ismételt összeállítását kínálja ugyanúgy, mint a TCP, leszámítva ez utóbbi megbízhatóságát és adatfolyam-vezérlési képességét.

Az UDP olyan egyszerű protokoll, amelyet gyakran azzal jellemeznek, hogy mit nem tud a TCP-hez képest.

Az UDP-funkciók az alábbiak:

* Az adatokat a beérkezés sorrendjében állítja össze.
* Az elveszett szegmenseket nem küldi újra.
* Nem hoz létre munkamenetet.
* A küldő nem értesül az erőforrások elérhetőségéről.

Az UDP-vel kapcsolatos további információkért keressünk rá az interneten az RFC dokumentumára.

14.3.2

## Az UDP-fejléc

Az UDP állapot nélküli protokoll, ami azt jelenti, hogy sem a kliens, sem pedig a szerver nem követi nyomon az adott munkamenet állapotát. Amennyiben az UDP szállítási protokoll használata mellett mégis szükség van a megbízhatóságra, azt már az alkalmazásnak kell lekezelnie.

Az élő videó és hang hálózaton keresztüli továbbításával szemben támasztott egyik legfontosabb feltétel a gyors adatáramlás. Az élő videó- és hangalkalmazások képesek elviselni az adatvesztést úgy, hogy annak kicsi vagy egyáltalán nem érzékelhető hatása legyen, így tökéletesen illeszkednek az UDP-protokollhoz.

Az UDP adategységeit datagramnak vagy szegmensnek nevezzük, melyeket a legjobb szándékkal továbbít.

Az UDP-fejléc sokkal egyszerűbb, mint a TCP-fejléc, mert csak négy mezőt tartalmaz, és mindössze 8 bájtot (azaz 64 bitet) igényel. Az ábra az UDP-fejlécben lévő mezőket mutatja.

UDP datagram diagram shows 4 header fields: source port, destination port, length, and checksum as well as the non header application layer data

8 BytesSource Port (16)Destination Port (16)Length (16)Checksum (16)Application Layer Data (Size varies)

14.3.3

## Az UDP-fejléc mezői

A táblázat azonosítja és leírja az UDP-fejléc négy mezőjét.

| UDP Header Field DescriptionSource Port A 16-bit field used to identify the source application by port number.Destination PortA 16-bit field used to identify the destination application by port number.Length A 16-bit field that indicates the length of the UDP datagram header.Checksum A 16-bit field used for error checking of the datagram header and data. | |
| --- | --- |
| **UDP-fejléc mező** | **Leírás** |
| **Forrásport** | 16 bites mező, amely a forrásalkalmazás portszám szerinti azonosítására szolgál. |
| **Célport** | 16 bites mező, amely a célalkalmazás portszám szerinti azonosítására szolgál. |
| **Hossz** | 16 bites mező, amely jelzi az UDP-datagram fejlécének hosszát. |
| **Ellenőrző összeg (Checksum)** | 16 bites mező, amellyel a datagram fejlécének és adattartalmának sértetlensége ellenőrizhető. |

14.3.4

## UDP-t használó alkalmazások

Az alkalmazásoknak három olyan típusa létezik, amelyek számára az UDP a legjobb választás:

* **Élő videó- és multimédiás alkalmazások** - Ezek az alkalmazások elviselnek némi adatvesztést, de megkövetelik, hogy alig vagy egyáltalán ne legyen késés. Ilyen például a VoIP és az élő videóközvetítés.
* **Egyszerű kérés-válasz típusú alkalmazások** - Egyszerű tranzakciókkal rendelkező alkalmazások, ahol az állomás küld egy kérést, amelyre lehet, hogy nem kap választ. Ilyen például a DNS és a DHCP.
* **Olyan alkalmazások, amelyek maguk kezelik a megbízhatóságot** - Egyirányú kommunikáció, ahol az adatfolyam-vezérlés, a hibafelismerés, a nyugtázás és a hibák helyreállítása nem szükséges, vagy az alkalmazás maga végzi. Ilyen például az SNMP és a TFTP.

Az ábra felsorolja azokat az alkalmazásokat, amelyek UDP-t igényelnek.

shows arrows pointing both directions from DHCP, DNS, SNMP, TFTP, VoIP, and IPTV to UDP and then from UDP to IP

UDPIPSNMPTFTPDNSVoIPDHCPVideo Conferencing

Bár a DNS és az SNMP alapértelmezés szerint UDP-t használ, mindkettő használhatja a TCP protokollt is. A DNS akkor használja a TCP-t, ha a DNS-kérés vagy a DNS-válasz mérete több mint 512 bájt, például ha a DNS-válasz számos névfeloldást tartalmaz. Hasonlóképpen, bizonyos esetekben a hálózati rendszergazda konfigurálhatja az SNMP protokollt a TCP használatára.

14.3.5

## Tudáspróba - Az UDP áttekintése

Az űrlap teteje

Check your understanding of UDP by choosing the correct answer to the following questions.

1. Which of the following is a stateless best-effort delivery transport layer protocol?

Az űrlap alja

Which UDP header statement is true?

Which two applications would use the UDP transport layer protocol? (Choose two.)

Which two fields are the same in a TCP and UDP header? (Choose two.)

[14.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A TCP áttekintése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Portszámok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                      
*     

1. Szállítási réteg
2. Portszámok

# Portszámok

14.4.1

## Az egyidejű kommunikációk szétválasztása

Megtanultuk, hogy vannak olyan helyzetek, amikor a TCP a megfelelő protokoll a feladathoz, más helyzetekben pedig az UDP-t kell használni. A szállított adatok típusától függetlenül a TCP és az UDP egyaránt portszámokat használ.

Mind a TCP, mind pedig az UDP portszámokat használ több, egyidejű párbeszéd kezelésére. A TCP- és az UDP-fejléc mezői azonosítják a forrás- és a célalkalmazás portszámát, az ábrán látható módon.

shows the source port and destination port header fields which are 2 bytes each

Source Port (16)Destination Port (16)

A forrásport száma a helyi állomás forrásalkalmazásához, míg a célport száma a távoli állomás célalkalmazásához van társítva.

Tegyük fel például, hogy egy állomás weboldal-kérést küld egy webszervernek. Amikor az állomás létrehozza a weboldal-kérést, a forrásport számát dinamikusan generálja, hogy azonosítsa a párbeszédet. Az állomás által generált kérések különböző dinamikusan létrehozott forrásportszámokat fognak használni. Ez egyidejűleg több párbeszédet tesz lehetővé.

A kérésben a célport száma azonosítja a webszervertől igényelt szolgáltatás típusát. Például amikor a kliens célportként a 80-as portot adja meg, az üzenetet fogadó szerver tudja, hogy webszolgáltatást kértek tőle.

A szerver egyszerre több szolgáltatást is kínálhat, például webszolgáltatásokat a 80-as porton, és emellett FTP-kapcsolat létrehozását a 21-es porton.

14.4.2

## Socket párok

A forrás- és célportok a szegmensben kerülnek elhelyezésre. A szegmensek ezt követően egy IP-csomagba ágyazódnak be. Az IP-csomag tartalmazza a forrás és a cél IP-címét. A forrás IP-címének és a forrásport számának, vagy a cél IP-címének és a célport számának kombinációját socketnek nevezzük.

Az ábrán látható példában a számítógép egyidejűleg FTP- és webszolgáltatásokat kér a célszervertől.

shows a PC making both a web request and an FTP request to a server. The requests have source and destination port numbers which identify the host PC and the requested application service respectively

00-07-E9-42-AC- 2800-07-E9-63-CE-53192.168.1.5192.168.1.7109980User DataTrailerDest MACSource MACSrc IPDest. IPSource PortDest. Port00-07-E9-42-AC- 2800-07-E9-63-CE-53192.168.1.5192.168.1.7130521User DataTrailerFTP client Source Port: 1305Web Client Source Port: 1099FTP Server Dest Port: 21Web Server Dest Port: 80FTP ConnectionWeb ConnectionDest MACSource MACSrc. IPDest IPSource  
PortDest.  
Port**Source**  
192.168.1.5  
00-07-E9-63-CE-53**Destination**  
192.168.1.7  
00-07-E9-42-AC-28FTPWeb

A példában a számítógép által generált FTP-kérés tartalmazza a 2. rétegbeli MAC-címeket és a 3. rétegbeli IP-címeket. A kérés azonosítja az 1305-ös (azaz az állomás által dinamikusan generált) forrásportot és a célportot is, azonosítva a 21-es porton elérhető FTP-szolgáltatásokat. Az állomás ugyanazokkal a 2. és 3. rétegbeli címekkel kért egy weboldalt is a kiszolgálótól. Ez viszont az 1099-es (azaz az állomás által dinamikusan generált) forrásportot és azt a célportot használja, amely azonosítja a webszolgáltatást a 80-as porton.

A socket-et használjuk a kliens által kért kiszolgáló és szolgáltatás azonosítására. Egy kliens socket, 1099-es portszámmal például a következőképpen nézhet ki: 192.168.1.5:1099

A webszerverhez tartozó socket pedig ilyen lehet: 192.168.1.7:80

Ezek együttesen egy socket-párt alkotnak: 192.168.1.5:1099, 192.168.1.7:80

Ez teszi lehetővé egy kliensállomáson futó több alkalmazás, valamint egy kiszolgáló több kapcsolatának megkülönböztetését.

A forrás portszám a kérést indító alkalmazás címének felel meg. A szállítási réteg nyomon követi a forrásportot és a kérést kezdeményező alkalmazást, így a válasz a megfelelő alkalmazáshoz érkezik vissza.

14.4.3

## Portszám-csoportok

Az IANA (Internet Assigned Numbers Authority) egy szabványszervezet, amely különböző címzési szabványok, köztük a 16 bites portszámok hozzárendeléséért felel. A forrás- és célportszámok azonosítására használt 16 bit a 0 és 65.535 közötti portok tartományát biztosítja.

Az IANA a számtartományt a következő három portcsoportra osztotta.

| Port GroupNumber RangeDescriptionWell-known Ports0 to 1,023These port numbers are reserved for common or popular services and applications such as web browsers, email clients, and remote access clients. Defined well-known ports for common server applications enables clients to easily identify the associated service required.Registered Ports1,024 to 49,151These port numbers are assigned by IANA to a requesting entity to use with specific processes or applications. These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number. For example, Cisco has registered port 1812 for its RADIUS server authentication process.Private and/or Dynamic Ports49,152 to 65,535These ports are also known as ephemeral ports.The client’s OS usually assign port numbers dynamically when a connection to a service is initiated. The dynamic port is then used to identify the client application during communication. | | |
| --- | --- | --- |
| **Port csoport** | **Számtartomány** | **Leírás** |
| **Jól ismert portok** | **0 - 1.023** | * Ezek a portszámok gyakori vagy népszerű szolgáltatások és alkalmazások számára vannak fenntartva, mint például a webböngészők, a levelezőprogramok és a távoli hozzáférés ügyfelei. * A meghatározott jól ismert portok lehetővé teszik a kiszolgálók alkalmazásai számára, hogy az ügyfelek könnyen azonosíthassák a hozzárendelt szolgáltatást. |
| **Bejegyzett portok** | **1.024 - 49.151** | * Ezeket a portszámokat az IANA rendeli hozzá a kérelmező entitáshoz, hogy bizonyos folyamatok vagy alkalmazások használják őket. * Ezek a folyamatok elsősorban külön alkalmazások, amelyeket a felhasználó telepít, nem pedig a gyakori alkalmazások, amelyek egy jól ismert portszámot kapnak. * Például a Cisco az 1812-es portot regisztrálta a RADIUS-kiszolgáló hitelesítési folyamatához. |
| **Privát** és/vagy **dinamikus portok** | **49.152 - 65.535** | * Ezeket a portokat ideiglenes portoknak is nevezik. * Az ügyfél operációs rendszere általában dinamikusan rendeli hozzá a portszámokat, amikor kapcsolatot kezdeményez egy szolgáltatással. * Ezután a dinamikus portot használja a kliensalkalmazás azonosítására a kommunikáció alatt. |

**MEGJEGYZÉS:** Egyes kliens operációs rendszerek a dinamikus portszámok helyett bejegyzett portszámokat használhatnak a forrásportok hozzárendeléséhez.

A táblázat néhány jól ismert portszámot és a hozzájuk kapcsolódó alkalmazásokat jeleníti meg.

### Jól ismert portszámok

| Port NumberProtocolApplication20TCPFile Transfer Protocol (FTP) - Data 21TCPFile Transfer Protocol (FTP) - Control 22TCPSecure Shell (SSH)23TCPTelnet25TCPSimple Mail Transfer Protocol (SMTP)53UDP, TCPDomain Name Service (DNS) 67UDPDynamic Host Configuration Protocol (DHCP) - Server68UDPDynamic Host Configuration Protocol - Client 69UDPTrivial File Transfer Protocol (TFTP)80TCPHypertext Transfer Protocol (HTTP)110TCPPost Office Protocol version 3 (POP3)143TCPInternet Message Access Protocol (IMAP)161UDPSimple Network Management Protocol (SNMP) 443TCPHypertext Transfer Protocol Secure (HTTPS) | | |
| --- | --- | --- |
| **Portszám** | **Protokoll** | **Alkalmazás** |
| **20** | TCP | File Transfer Protocol (FTP) - Adat |
| **21** | TCP | File Transfer Protocol (FTP) - Vezérlés |
| **22** | TCP | Secure Shell (SSH) |
| **23** | TCP | Telnet |
| **25** | TCP | Simple Mail Transfer Protocol (SMTP) |
| **53** | UDP, TCP | Domain Name System (DNS) |
| **67** | UDP | Dynamic Host Configuration Protocol (DHCP) - Kiszolgáló |
| **68** | UDP | Dynamic Host Configuration Protocol - Ügyfél |
| **69** | UDP | Trivial File Transfer Protocol (TFTP) |
| **80** | TCP | Hypertext Transfer Protocol (HTTP) |
| **110** | TCP | Post Office Protocol version 3 (POP3) |
| **143** | TCP | Internet Message Access Protocol (IMAP) |
| **161** | UDP | Simple Network Management Protocol (SNMP) |
| **443** | TCP | Hypertext Transfer Protocol Secure (HTTPS) |

Némelyik alkalmazás TCP-t és UDP-t egyaránt használhat. A DNS például UDP-t használ, amikor a kliensek kéréseket küldenek egy DNS-szervernek. A két DNS-szerver közötti kommunikáció azonban mindig TCP-t használ.

A portszámok és a kapcsolódó alkalmazások teljes listájának megtekintéséhez keressük meg az IANA webhelyén a portok regisztrációs adatbázisát.

14.4.4

## A netstat parancs

Az ismeretlen TCP-kapcsolatok komoly biztonsági fenyegetettséget okozhatnak. Jelezhetik, hogy valami vagy valaki csatlakozott a helyi állomáshoz. Néha szükséges tudni, hogy egy hálózatba kötött állomáson mely aktív TCP-kapcsolatok vannak nyitva, és melyek futnak. A netstat egy fontos hálózati segédprogram, mely ezen kapcsolatok ellenőrzésére használható. Ahogy az ábrán is látható, a **netstat** parancs kilistázza a használt protokollokat, a helyi címeket és portszámokat, a külső címeket és portszámokat, valamint a kapcsolatok állapotát.

C:\> **netstat**

Active Connections

Proto Local Address Foreign Address State

TCP 192.168.1.124:3126 192.168.0.2:netbios-ssn ESTABLISHED

TCP 192.168.1.124:3158 207.138.126.152:http ESTABLISHED

TCP 192.168.1.124:3159 207.138.126.169:http ESTABLISHED

TCP 192.168.1.124:3160 207.138.126.169:http ESTABLISHED

TCP 192.168.1.124:3161 sc.msn.com:http ESTABLISHED

TCP 192.168.1.124:3166 www.cisco.com:http ESTABLISHED

(output omitted)

C:\>

Alapértelmezés szerint a **netstat** parancs megpróbálja feloldani az IP-címeket tartománynevekre és a portszámokat közismert alkalmazásokra. Az **-n** opció használható az IP-címek és portszámok numerikus formában történő megjelenítéséhez.

14.4.5

## Tudáspróba - Portszámok

Az űrlap teteje

Check your understanding of port numbers by choosing the BEST answer to the following questions.

1. Assume a host with IP address 10.1.1.10 wants to request web services from a server at 10.1.1.254. Which of the following would display to correct socket pair?

Az űrlap alja

Which port group includes port numbers for FTP, HTTP, and TFTP applications?

Which windows command would display the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state?

[14.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az UDP áttekintése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A TCP kommunikációs folyamata](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                          
*     

1. Szállítási réteg
2. A TCP kommunikációs folyamata

# A TCP kommunikációs folyamata

14.5.1

## TCP-szerverfolyamatok

Már ismerjük a TCP alapjait. A portszámok szerepének ismerete segít megérteni a TCP kommunikációs folyamat részleteit. Ebben a témakörben megismerkedünk a TCP háromfázisú kézfogás és munkamenet-lezárás folyamataival is.

A szerveren futó minden egyes alkalmazási folyamat esetén be kell állítani egy portszám használatát, amely történhet automatikusan, de végezheti a rendszergazda is.

Egy szervernek nem lehet két olyan szolgáltatása, amely ugyanannak a szállítási rétegbeli protokollnak (TCP vagy UDP) ugyanahhoz a portjához van rendelve. Egy webszolgáltatást és fájlátvitelt egyaránt kínáló szerveren nem állítható be mindkét alkalmazás számára ugyanazon port használata (pl.: a TCP 80-as portja).

Az aktív szerver oldali alkalmazásokhoz rendelt konkrét portokat nyitott portnak tekintjük, ami azt jelenti, hogy a szállítási réteg elfogadja és feldolgozza az ezekre a portokra küldött szegmenseket. Bármely bejövő ügyfélkérés elfogadásra kerül, amelyet megfelelő socket címmel láttak el, az adatok pedig a szerveralkalmazáshoz lesznek továbbítva. Egy szerveren számos port lehet egyidejűleg nyitva, minden aktív szerveralkalmazáshoz egy.

A TCP szerverfolyamataival kapcsolatos további információért kattintsunk a gombokra!

**TCP-kérést küldő kliensek**

Az 1-es kliens webszolgáltatásokat, a 2-es kliens pedig e-mail szolgáltatást vesz igénybe a jól ismert portok használatával (azaz webszolgáltatások = 80-as port, e-mail szolgáltatások = 25-ös port).

HTTP Request:  
Source Port: 49152  
Destination Port: 80 SMTP Request:  
Source Port: 51152  
Destination Port: 25ServerClient 1Client 2HTTP: Port 80  
SMTP: Port 25Client requests to TCP server

14.5.2

## TCP-kapcsolatok létrehozása

Egyes kultúrákban, ha két személy találkozik, kézfogással üdvözlik egymást. Ilyenkor mindkét fél tudja, hogy a kézfogás a baráti üdvözlés jele. A hálózati kapcsolatok is hasonlóan működnek. A TCP-kapcsolatok esetében a kliens számítógép háromfázisú kézfogás használatával kapcsolódik a szerverhez.

A TCP-kapcsolat létrehozásának lépéseivel kapcsolatos további információért kattintsunk a gombokra.

**1. lépés: SYN**

A kezdeményező ügyfél egy kliens-szerver irányú kapcsolat létrehozását kéri a kiszolgálótól.

PCA initiates a three way handshake by sending a syn segment to PCB.

1 A

B

Send SYN(SEQ=100 CTL=SYN)SYN receivedA sends SYN request to B

A háromfázisú kézfogás ellenőrzi, hogy a célállomás elérhető-e kommunikáció céljából. Ebben a példában az A állomás megállapította, hogy a B állomás elérhető.

14.5.3

## A munkamenet lezárása

A kapcsolat lezárásához be kell állítani a szegmens fejlécében található FIN vezérlőbit értékét. Minden egyes, egyirányú TCP-munkamenet lezárásához kétfázisú kézfogást használunk, amely egy FIN és egy ACK szegmensből áll. Ezért egy TCP által támogatott párbeszéd bontásához, mindkét munkamenetet meg kell szüntetni, amelyhez négy adatcsere szükséges. A kliens és a szerver egyaránt kezdeményezheti a lezárást.

A példában az egyszerűség kedvéért a kliens és szerver fogalmakat használjuk, de a lezárás folyamatát bármely, nyitott munkamenettel rendelkező állomás kezdeményezheti.

A munkamenet lezárásának lépéseivel kapcsolatos további információért kattintsunk a gombokra.

**1. lépés: FIN**

Amikor már nincs több átküldendő adat, a kliens egy olyan szegmenset küld, amelyben a FIN jelzőbit beállítása megtörtént.

PCA sends a fin segment to PCB to end the session when there is no more data to send

1 A

B

Send FINFIN receivedA sends FIN request to B.

Miután az összes szegmens nyugtázása megtörtént, a munkamenet is lezárul.

14.5.4

## A TCP háromfázisú kézfogásának elemzése

Az állomások nyomon követik az egyes adatszegmenseket egy munkameneten belül, valamint a TCP-fejlécben szereplő adatok alapján arról is információt cserélnek, hogy mely adatok érkeztek meg. A TCP egy teljes duplex (full-duplex) protokoll, ahol minden egyes kapcsolatnak két, egyirányú kommunikációs adatfolyam, más néven munkamenet felel meg. A kapcsolat létrehozásához az állomásoknak egy háromfázisú kézfogást kell végrehajtaniuk. Az ábrán látható TCP-fejlécben lévő vezérlőbitek jelzik a kapcsolat állapotát és előrehaladását.

A háromfázisú kézfogás feladatai az alábbiak:

* Megállapítja a céleszköz jelenlétét a hálózaton.
* Ellenőrzi, hogy a céleszköz aktív szolgáltatással rendelkezik-e, és elfogadja-e az olyan célportra érkező kéréseket, amelyet a kezdeményező kliens használni kíván a munkamenet idejére.
* Tájékoztatja a céleszközt arról, hogy a küldő kliens kapcsolatot kíván létrehozni az adott porton.

Miután a kommunikáció befejeződött, a munkameneteket le kell zárni, a kapcsolatot pedig bontani kell. A kapcsolathoz és munkamenethez tartozó mechanizmusok adják a TCP megbízhatóságát.

shows the tcp segment header fields with the control bits field of 6 bits highlighted

### A Vezérlőbitek mező

20 BytesSource Port (16)Destination Port (16)Acknowledgement Number (32)Header Length (4)Window (16)Checksum (16)Urgent (16)Options (0 or 32 if any)Application Layer Data (Size varies)Sequence Number (32)Reserved (6)Control Bits (6)

A TCP-szegmens fejlécének Vezérlőbitek mezőjében található hat bit jelzőbitekként is ismert. A jelzőbit (flag) egy olyan bit, amely be (on) vagy ki (off) értéket vehet fel.

A Vezérlőbitek mező hat jelzőbitje a következő:

* **URG** - sürgősségi jelző
* **ACK** - a kapcsolat létrehozásakor és a munkamenet lezárásakor nyugtázásra használt jelzőbit
* **PSH** - áttöltési funkció
* **RST** - a kapcsolat bontása hiba vagy időtúllépés esetén
* **SYN** - a kapcsolat létrehozásakor használt sorszámok szinkronizálása
* **FIN** - ha nincs több adat a küldőtől, valamint a munkamenet lezárásakor használatos

A PSH és URG jelzőbitekkel kapcsolatos további információkra keressünk rá az interneten.

14.5.5

## Videómagyarázat - A TCP háromfázisú kézfogása

A TCP háromfázisú kézfogását bemutató videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

14.5.6

## Tudáspróba - A TCP kommunikációs folyamata

Az űrlap teteje

Check your understanding of the TCP communication process by choosing the correct answer to the following questions.

1. Which of the following would be valid source and destination ports for a host connecting to an email server?

Az űrlap alja

Which control bit flags are used during the three-way handshake?

How many exchanges are needed to end both sessions between two hosts?

[14.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Portszámok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Megbízhatóság és forgalomszabályozás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                
*     

1. Szállítási réteg
2. Megbízhatóság és forgalomszabályozás

# Megbízhatóság és forgalomszabályozás

14.6.1

## A TCP megbízhatósága - Garantált és sorrendtartó kézbesítés

Az ok, amiért a TCP a megfelelőbb protokoll egyes alkalmazásokhoz, hogy az UDP-től eltérően, újraküldi az eldobott csomagokat és sorszámozza őket, hogy jelezze azok megfelelő sorrendjét a kézbesítés előtt. A TCP segíthet a csomagok áramlásának fenntartásában is, így az eszközök nem lesznek túlterhelve. Ez a témakör részletesen tárgyalja a TCP ezen funkcióit.

Előfordulhat, hogy a TCP-szegmensek nem érkeznek meg a rendeltetési helyükre. Máskor előfordulhat, hogy a TCP-szegmensek nem sorrendben érkeznek meg. Ahhoz, hogy a fogadó fél megértse az eredeti üzenetet, minden adatnak meg kell érkeznie, és a szegmensekben lévő adatokat ismét az eredeti sorrendben kell összeállítani. Ennek érdekében minden egyes csomag fejlécében szerepel egy sorszám. A sorszám a TCP-szegmens első adatbájtját jelöli.

A kapcsolat felépítése során egy kezdősorszám (ISN) kerül beállításra. Az ISN tulajdonképpen a fogadó alkalmazásnak átküldött bájtok kezdőértéke. A kapcsolat ideje alatt továbbított adatoknak megfelelően a sorszám értéke is növekszik az átvitt bájtok számával. Az adatbájtok ilyenfajta nyomon követése lehetővé teszi az egyes szegmensek egyedileg történő azonosítását és nyugtázását. Így a hiányzó szegmensek szintén azonosíthatók.

Az ISN nem eggyel kezdődik, hanem gyakorlatilag egy véletlenszerű szám. Ez megakadályozza a rosszindulatú támadások bizonyos típusait. Az egyszerűség kedvéért az ebben a fejezetben szereplő példákban az ISN értéke 1-es lesz.

Ahogy az ábrán is látható, a szegmensek sorszámai jelzik, hogy miként kell ismételten összeállítani és sorba rendezni a megérkezett szegmenseket.

shows that even though segments may take different routes and arrive out of order at the destination, TCP has the ability to reorder the segments

### A TCP-szegmensek sorba rendezése a célhelyen

Segment 1Segment 2Segment 3Segment 4Segment 5Segment 6Segment 1Segment 2Segment 6Segment 5Segment 4Segment 3Segment 1Segment 2Segment 3Segment 4Segment 5Segment 6Having taken different routes to the destination, segments arrive out of order.TCP reorders the segments to the original order.Different segments may take different routes.**Data**  
  
Data is divided into segments.

A fogadó TCP-folyamat a szegmensek adatait egy vételi pufferbe helyezi át. A szegmensek a sorszámuknak megfelelő sorrendben kerülnek a pufferbe, majd onnan az ismételt összeállítást követően az alkalmazási rétegbe. A nem folytonos sorszámmal érkező szegmenseket későbbi feldolgozás céljából visszatartják. Amikor megérkeznek a hiányzó bájtokat tartalmazó szegmensek, akkor ezek is sorban feldolgozásra kerülnek.

14.6.2

## Videómagyarázat - A TCP megbízhatósága - Sorszámok és nyugták

A TCP egyik feladata, hogy garantálja minden egyes szegmens célba érkezését. A célállomáson működő TCP-szolgáltatások nyugtázzák a forrásalkalmazás által küldött adatokat.

A TCP-sorszámokról és nyugtákról szóló lecke megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

14.6.3

## A TCP megbízhatósága - Adatvesztés és újraküldés

Nem számít, hogy mennyire jól megtervezett a hálózat, adatvesztés időnként előfordul. A TCP ezen szegmensveszteségek kezelésére is biztosít módszereket. Ezek közé tartozik a nem nyugtázott adatszegmensek újraküldésének mechanizmusa is.

Az utóbbi fejlesztéseket megelőzően a TCP csak a következő várható bájtot tudta nyugtázni. Az ábra példáján az egyszerűség kedvéért a szegmensek számát használjuk, az A állomás elküldi az 1-10 közötti sorszámmal rendelkező szegmenseket a B állomásnak. Ha a 3-as és 4-es szegmens kivételével az összes szegmens megérkezik, a B állomás egy nyugtával válaszol, amely megadja, hogy a következő várható szegmens a 3-as sorszámú. Az A állomásnak fogalma sincs, hogy más szegmensek megérkeztek-e vagy sem. Ezért az A állomás újraküldi a 3-10 közötti sorszámmal rendelkező szegmenseket. Ha az összes újraküldött szegmens sikeresen megérkezik, az 5-10 közötti sorszámmal rendelkező szegmensek duplikátumok lennének. Ez késleltetéshez, torlódáshoz és rossz hatásfokhoz vezethet.

shows PCA sending 10 segments to PCB, but segments 3 and 4 fail to arrive. So starting with segment 3, PCA resends segments 3 through 10, even though PCB only needed segments 3 and 4

A B A

B

Segment 1Segment 2Segment 3Segment 5Segment 6Segment 7Segment 8Segment 9Segment 10Segment 4Segment 3Segment 4Segment 5Segment 6Segment 7Segment 8Segment 9Segment 10ACK 3ACK 11Duplicate  
segments

A kliens operációs rendszerek ma már jellemzően egy opcionális TCP-funkciót alkalmaznak, amelyet a háromfázisos kézfogás során tárgyalt szelektív nyugtázásnak (SACK) nevezünk. Ha mindkét állomás támogatja a SACK szolgáltatást, a fogadó fél egyértelműen nyugtázhatja, hogy mely szegmensek (bájtok) érkeztek meg, beleértve a nem folytonos szegmenseket is. A küldő állomásnak ezért csak a hiányzó adatokat kell újraküldenie. Az alábbi ábra példájában ismét a szegmensek számát használjuk. Az A állomás elküldi az 1-10 közötti sorszámmal rendelkező szegmenseket a B állomásnak. Ha a 3-as és 4-es szegmens kivételével az összes szegmens megérkezik, a B állomás nyugtázhatja, hogy megkapta az 1-es és 2-es szegmenset (ACK 3), és szelektíven nyugtázza az 5—10 közötti sorszámmal rendelkező szegmenseket (SACK 5-10). Az A állomásnak így csak a 3-as és 4-es szegmenseket kellene újraküldenie.

show PCA sending 10 segments to PCB, but segments 3 and 4 fail to arrive. This time PCB sends an ack 3 and a sack 5-10 letting PCA know to resend missing segments 3 and 4 and the continue with segment 11

A B A

B

Segment 1Segment 2Segment 3Segment 5Segment 6Segment 7Segment 8Segment 9Segment 10Segment 4Segment 3Segment 4Segment 11Segment 12ACK 3,SACK 5-10ACK 13

**MEGJEGYZÉS:** A TCP általában minden második csomaghoz küld ACK-t, de a témakörön túlmutató egyéb szempontok is megváltoztathatják ezt a viselkedést.

A TCP időzítőket használ, hogy tudja, mennyi ideig kell várnia a szegmens újraküldése előtt. Játsszuk le az ábrán látható videót, és kattintsunk a linkre a PDF fájl letöltéséhez. A videóban és a PDF fájlban a TCP adatvesztés és újraküldés vizsgálatáról esik szó.

14.6.4

## Videómagyarázat - A TCP megbízhatósága - Adatvesztés és újraküldés

A TCP újraküldésről szóló lecke megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

14.6.5

## TCP adatfolyam-vezérlés - Ablakméret és nyugtázás

A TCP az adatfolyam-vezérléshez is kínál módszereket. Az adatfolyam-vezérlés azt az adatmennyiséget jelenti, amelyet a cél megbízhatóan fogadhat és dolgozhat fel. Az adatfolyam-vezérlés azzal segíti a TCP-átvitel megbízhatóságának megőrzését, hogy mindig az adott munkamenethez igazítja az adatátvitel sebességét a forrás és a cél között. A TCP-fejléc tartalmaz egy 16 bites mezőt, amelynek ablakméret (window size) a neve.

Az ábrán egy példa látható az ablakméretre és a nyugtázásra.

shows PCB sending PCA a negotiated window size of 10,000 bytes and a maximum segment size of 1,460 bytes. PCA starts sending segments starting with sequence number 1. An acknowledgement from PCB can be sent without waiting until the window size is reached and the window size can be adjusted by PCA creating a sliding window

### Példa a TCP ablakméretre

A

B

**MSS = Maximum Segment Size**During three-way handshake Window size 10,000, MSS 1,460Sequence number 1,4611,460 bytesACK 2,921  
Window size 10,0001,460 bytesACK 4,381  
Window size 10,000Send window 10,000Sequence number 11,460 bytesReceive acknowledgement   
Send window 12,920Sequence number 2,921Receive acknowledgement  
Send window 14,380Receive 1 – 1,460Receive 1,461 – 2,920Receive 2,921 – 4,380

Az ablakméret határozza meg a várható nyugtázás előtt elküldhető bájtok számát. A nyugtaszám a következő várható bájt száma.

Ez nem más, mint egy adott TCP-munkamenet céleszköze által egyszerre fogadható és feldolgozható bájtok száma. A példában szereplő A állomás TCP-munkamenetre vonatkozó kezdeti ablakmérete 10.000 bájt. Az első, vagyis az 1-es sorszámú bájttal kezdve az A állomás által nyugtázás nélkül elküldhető utolsó bájt a 10.000-es sorszámú. Ezt az A állomás küldési ablakának nevezzük. Az ablakméretet minden TCP-szegmens tartalmazza, így a cél bármikor módosíthatja az ablak méretét a puffer elérhetőségétől függően.

A kezdeti ablakméret megállapítása akkor történik, amikor a TCP-munkamenet létrejön a háromfázisú kézfogás során. A forráseszköznek a cél ablakmérete alapján korlátoznia kell a céleszközre küldött bájtok számát. A forráseszköz kizárólag a bájtok kézbesítését igazoló nyugta visszaérkezése után küldhet további adatokat az adott munkamenet során. A cél jellemzően nem várja meg az ablakméretet kitöltő összes bájt beérkezését, mielőtt egy nyugtával válaszolna. Ahogy a bájtok fogadása és feldolgozása történik, a cél egy nyugtával tájékoztatja a forrást arról, hogy folytathatja a további bájtok küldését.

A B állomás például jellemzően nem várna egy nyugta megküldésével addig, amíg mind a 10.000 bájt beérkezik. Ez azt jelenti, hogy az A állomás változtathat a küldési ablak méretén a B állomástól kapott nyugták alapján. Ahogy az ábrán is látható, amikor az A állomás visszaigazolást kap a 2.921-es nyugtaszámmal, amely a következő várható bájt, az A állomás küldési ablaka 2.920 bájttal nőni fog. Ez módosíthatja a küldési ablakot 10.000 bájtról 12.920-ra. Az A állomás mostantól küldhet akár 10.000 bájtot a B állomásnak, amennyiben az elküldött adatmennyiség nem haladja meg az új küldési ablak 12.920-as méretét.

A beérkezett bájtok feldolgozása során a nyugtát küldő cél és a forrás küldési ablakméretének folyamatos változtatása csúszóablakként ismert. Az előző példában az A állomás küldési ablaka további 2.921 bájttal 10.000-ről 12.920-ra nőtt vagy csúszott.

Ha a célállomás rendelkezésre álló pufferterülete csökken, az ablakméret csökkentésével tájékoztathatja a forrást, hogy csökkentse a nyugtázás nélkül küldendő bájtok számát.

**MEGJEGYZÉS:** Az eszközök manapság a csúszóablak protokollt használják. A fogadó általában minden második szegmens után nyugtát küld. A nyugtát megelőzően kapott szegmensek száma változhat. A csúszóablak előnye, hogy lehetővé teszi a küldő számára, hogy mindaddig folyamatosan továbbítsa a szegmenseket, amíg a fogadó nyugtázza a korábbi szegmenseket. A csúszóablak részletei túlmutatnak ennek a kurzusnak a keretein.

14.6.6

## TCP adatfolyam-vezérlés - Maximális szegmensméret (MSS)

Az ábrán látható forrás 1.460 bájt adatot továbbít minden TCP-szegmensben. Ez jellemzően a céleszköz által fogadható maximális szegmensméret (MSS). Az MSS a TCP-fejléc opciós mezőjének része, amely bájtban adja meg a legnagyobb adatmennyiséget, amelyet egy eszköz egyetlen TCP-szegmensben fogadhat. Az MSS méret nem tartalmazza a TCP-fejlécet. Az MSS jellemzően a háromfázisú kézfogás során kap szerepel.

shows the same diagram as before but the emphasis is on the MSS of maximum segment size of 1460

A

B

**MSS = Maximum Segment Size**During three-way handshake Window size 10,000, MSS 1,460Sequence number 1,4611,460 bytesACK 2,921  
Window size 10,0001,460 bytesACK 4,381  
Window size 10,000Send window 10,000Sequence number 11,460 bytesReceive acknowledgement   
Send window 12,920Sequence number 2,921Receive acknowledgement  
Send window 14,380Receive 1 – 1,460Receive 1,461 – 2,920Receive 2,921 – 4,380

Az IPv4 használata során az elterjedt MSS érték 1.460 bájt. Az állomás az MSS mező értékét úgy határozza meg, hogy kivonja az IP- és a TCP-fejléceket az Ethernet maximális átviteli egységből (MTU). Egy Ethernet interfészen az alapértelmezett MTU 1500 bájt. A 20 bájtos IPv4-fejlécet és a 20 bájtos TCP-fejlécet kivonva az alapértelmezett MSS-méret 1460 bájt lesz, ahogy az ábrán is látható.

shows a diagram of an entire Ethernet frame of which the MTU is 1500 bytes, with 20 bytes being the IP header, and 20 bytes being the TCP header, this leaves 1460 bytes which is the TCP maximum segment size MSS

**EthernetIPv4TCPPayloadFCS**Ethernet MTUIP MTU20 bytes20 bytes1460 bytes1500 bytesTCP MSS

14.6.7

## TCP adatfolyam-vezérlés - Torlódások elkerülése

Ha a hálózaton torlódás következik be, akkor a csomagokat a túlterhelt router eldobja. Ha a TCP-szegmenseket tartalmazó csomagok nem érik el a céljukat, akkor nem nyugtázzák őket. Az elküldött, de nem nyugtázott TCP-szegmensek arányának meghatározásával a forrás bizonyos szintű hálózati torlódást feltételezhet.

Ha torlódás van, az elveszett TCP-szegmenseket a forrás újraküldi. Ha az újraküldés nem megfelelően ellenőrzött, a TCP-szegmensek további újraküldése még ronthat is a helyzeten. Nem csak TCP-szegmensekkel rendelkező új csomagok kerülnek a hálózatra, hanem az elveszett és újraküldött TCP-szegmensek visszajelzési hatása is növeli a torlódást. A torlódások elkerülése és ellenőrzése érdekében a TCP számos torlódáskezelési mechanizmust, időzítőt és algoritmust alkalmaz.

Ha a forrás megállapítja, hogy a TCP-szegmenseket egyáltalán nem nyugtázzák vagy nem megfelelő időben, akkor csökkentheti a nyugta fogadása előtt elküldött bájtok számát. Amint az ábrán is látható, az A állomás érzékeli, hogy torlódás van, ezért csökkenti a B állomástól kapott nyugta előtt elküldött bájtok számát.

shows PCA sending segments to PCB where lost segments and retransmission can cause congestion

### TCP torlódásvezérlés

A

B

TCP segment 1TCP segment 2TCP segment 3TCP segment 4Acknowledgement segment 2TCP segment 2TCP segment 3I’m not getting the acknowledgments I expect from PC B so I will reduce the number of bytes I send before getting an acknowledgement.

A nyugtaszámok a következő várt bájtra vonatkoznak, nem pedig a szegmensre. A szegmensek számát az egyszerűség kedvéért használjuk a példában.

Figyeljük meg, hogy a forrás az elküldött, de nem nyugtázott bájtok számát csökkenti, nem pedig a cél által meghatározott ablakméretet.

**MEGJEGYZÉS:** A torlódáskezelési mechanizmusok, időzítők és algoritmusok magyarázata túlmutat ezen a kurzuson.

14.6.8

## Tudáspróba - Megbízhatóság és adatfolyam-vezérlés

Az űrlap teteje

Check your understanding of the TCP reliability and flow control process by choosing the correct answer to the following questions.

1. What field is used by the destination host to reassemble segments into the original order?

Az űrlap alja

What field is used to provide flow control?

What happens when a sending host senses there is congestion?

[14.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[A TCP kommunikációs folyamata](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az UDP-kommunikáció](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                   
*     

1. Szállítási réteg
2. Az UDP-kommunikáció

# Az UDP-kommunikáció

14.7.1

## UDP: Alacsony többletteher kontra megbízhatóság

Amint azt korábban kifejtettük, az UDP tökéletes minden olyan kommunikációhoz, amelynek gyorsnak kell lennie (pl. VoIP). Ez a témakör részletesen elmagyarázza, hogy az UDP miért tökéletes bizonyos típusú átvitelekhez. Amint az ábrán is látható, az UDP nem épít fel kapcsolatot. Az UDP alacsony többletterhet jelentő adatátvitelt biztosít, mivel a datagram fejléce kicsi, és nincs hálózatfelügyeleti forgalom.

shows a host sender needing to send voice and video data which is sent with UDP which requires no prior negotiated connection

NetworkSenderReceiverDataUDP does not establish a connection before sending data.

14.7.2

## UDP-adategységek újbóli összeállítása

A TCP-szegmensekhez hasonlóan, amikor UDP-datagramot küldünk egy célállomásnak, azok különböző útvonalat választhatnak, így gyakran előfordulhat, hogy az adatok rossz sorrendben érkeznek meg. Az UDP nem követi nyomon a sorszámokat, mint a TCP. Ahogy az ábrán is látható, az UDP semmilyen módszerrel nem rendelkezik a datagramok eredeti sorrendjének helyreállításához.

Ezért az UDP érkezési sorrendben állítja össze az adatokat, majd továbbküldi azokat az alkalmazásnak. Ha az adatsorrend lényeges az alkalmazás szempontjából, akkor az alkalmazásnak kell meghatároznia a helyes sorrendet, valamint az adatok feldolgozásának módját.

shows UDP datagrams being sent in order but arriving out of order due to the possibility of different routes to reach the destination

### UDP: Összeköttetés-mentes és nem megbízható

Datagram 1Datagram 2Datagram 3Datagram 4Datagram 5Datagram 6Datagram 1Datagram 2Datagram 6Datagram 5Datagram 4Having taken different routes to the destination, datagrams arrive out of order.Out of order datagrams are not re-ordered.Different datagrams may take different routes.Lost datagrams are not re-sent.Data   
  
Data is divided into datagrams.

14.7.3

## UDP-szerverfolyamatok és kérések

Hasonlóan a TCP-hez, az UDP-t használó szerveralkalmazásokhoz is közismert vagy bejegyzett portszámok vannak hozzárendelve, az ábrán látható módon. Amikor ezek az alkalmazások és folyamatok futnak egy szerveren, akkor csak a hozzájuk rendelt portszámra illeszkedő adatokat fogadják el. Ha olyan datagram érkezik, amelyet ezen portok egyikének címeztek, az UDP a portszám alapján továbbítja az adatokat a megfelelő alkalmazáshoz.

shows that a RADIUS server application uses UDP to listen for requests on port 53

### Kéréseket figyelő UDP-szerver

ServerClient 1Client 2**Server Applications**  
Client DNS requests will be received on Port 53.  
  
Client RADIUS requests will be received on Port 1812.DNS requestRADIUS request

**MEGJEGYZÉS:** Az ábrán látható RADIUS-szerver hitelesítési, jogosultságkezelési és naplózási szolgáltatásokat nyújt a felhasználói hozzáférés kezeléséhez. A RADIUS működése viszont nem része a kurzus anyagának.

14.7.4

## UDP-kliensfolyamatok

A TCP-hez hasonlóan, a kliens-szerver kommunikációt itt is egy kliensalkalmazás kezdeményezi, amely adatokat kér egy szerverfolyamattól. Az UDP-kliensfolyamat dinamikusan választ egy portszámot a portszámok tartományából, amelyet később a párbeszéd forrásportjaként használ. A célport általában egy szerverfolyamathoz rendelt közismert vagy bejegyzett portszám.

Miután a kliens kiválasztotta a forrás- és célportot, a tranzakció során végig ugyanaz a portpár szerepel az összes datagram fejlécében. Ami a szervertől a klienshez visszaérkező adatokat illeti, a datagramok fejlécében szereplő forrás- és célportok felcserélődnek.

Két állomás DNS-sel és RADIUS hitelesítő kiszolgálóval folytatott szolgáltatás iránti kéréseinek bemutatásához kattintsunk az egyes gombokra!

**UDP-kéréseket küldő ügyfelek**

Az 1-es kliens DNS-kérést küld a jól ismert 53-as portra, míg a 2-es kliens RADIUS hitelesítési szolgáltatásokat kér az 1812-es bejegyzett port használatával.

Two different PC clients need to make a request to a DNS server

Client 1 DNS Request:  
Source Port 49152  
Destination Port 53Client 2 RADIUS User Authentication Request:  
Source Port 51152  
Destination Port 1812Client 1ServerClient 2DNS: Port 53  
RADIUS: Port 1812

14.7.5

## Tudáspróba - UDP-kommunikáció

Az űrlap teteje

Check your understanding of the UDP communication by choosing the correct answer to the following questions.

1. Why is UDP desirable for protocols that make a simple request and reply transactions?

Az űrlap alja

Which UDP datagram reassembly statement is true?

Which of the following would be valid source and destination ports for a host connecting to a DNS server?

[14.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Megbízhatóság és forgalomszabályozás](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[14.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                         

1. Szállítási réteg
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

14.8.1

## Packet Tracer - TCP- és UDP-kommunikáció

A feladat során tanulmányozni fogjuk a TCP- és az UDP-protokollok funkcionalitását, a multiplexelést, valamint a portszámok helyi alkalmazások meghatározásában betöltött szerepét.

[TCP és UDP kommunikáció](https://contenthub.netacad.com/courses/itn/_common/14.8.1-packet-tracer---tcp-and-udp-communications_hu-HU.pka)

14.8.2

## Miről tanultunk ebben a fejezetben?

**Az adatok szállítása**

A szállítási réteg egyfajta kapocs az alkalmazási réteg, valamint a hálózati átvitelért felelős alsóbb rétegek között. A szállítási réteg felel a különböző állomásokon futó alkalmazások közötti logikai kommunikációért. A szállítási réteg részét képezi a TCP- és az UDP-protokoll. A szállítási rétegbeli protokollok határozzák meg, hogy az üzenetek miként szállíthatók az állomások között, valamint felelnek a párbeszédek megbízhatósági követelményeinek kezeléséért. A szállítási réteg felel a párbeszédek (munkamenetek) nyomon követéséért, az adatok szegmentálásáért és a szegmensek újraösszeállításáért, a fejléc adatainak hozzáadásáért, az alkalmazások azonosításáért és a párbeszédek multiplexeléséért. A TCP állapottartó, megbízható, nyugtázza az adatokat, újraküldi az elveszett adatokat, és szekvenciális sorrendben kézbesíti őket. Használjunk TCP-t az e-mailek és a webes kommunikáció esetében! Az UDP állapot nélküli, gyors, kis többletterhet okoz, nem igényel nyugtázást, nem küldi újra az elveszett adatokat, és érkezési sorrendben kézbesíti őket. Használjunk UDP-t a VoIP- és DNS-szolgáltatás esetében!

**A TCP áttekintése**

A TCP létrehozza a munkameneteket, garantálja a megbízhatóságot, biztosítja a sorrendtartó kézbesítést és támogatja az adatfolyam-vezérlést. A TCP-szegmens egy 20 bájtos többletterhet jelentő fejlécet ad hozzá az alkalmazási réteg adatainak beágyazásakor. A TCP-fejléc mezői: Forrás- és Célport, Sorszám, Nyugtaszám, Fejléc hossza, Fenntartott, Vezérlőbitek, Ablakméret, Ellenőrző összeg és Sürgős. A TCP-t használó alkalmazások: a HTTP, az FTP, az SMTP és a Telnet.

**Az UDP áttekintése**

Az UDP az adatokat érkezési sorrendben állítja össze, az elveszett szegmenseket nem küldi újra, nincs munkamenet-létrehozás, és nem tájékoztatja a küldőt az erőforrások rendelkezésre állásáról. Az UDP-fejléc mezői: Forrás- és Célport, Hossz és Ellenőrző összeg. UDP-t használó alkalmazások: DHCP, DNS, SNMP, TFTP, VoIP és a videokonferencia.

**Portszámok**

Mind a TCP, mind pedig az UDP portszámokat használ több, egyidejű párbeszéd kezelésére. Ezért a TCP- és az UDP-fejléc mezői azonosítják a forrás- és a célalkalmazás portszámát. A forrás- és célportok a szegmensben kerülnek elhelyezésre. A szegmensek ezt követően egy IP-csomagba ágyazódnak be. Az IP-csomag tartalmazza a forrás és a cél IP-címét. A socket a forrás IP-címének és a forrásport számának, vagy a cél IP-címének és a célport számának kombinációja. A socket-et használjuk a kliens által kért kiszolgáló és a szolgáltatás azonosítására. A portszámok 0 és 65.535 közötti értéket vehetnek fel. Ez a tartomány csoportokra oszlik: jól ismert portok, bejegyzett portok, privát és/vagy dinamikus portok. Van néhány közismert portszám, amely az elterjedt alkalmazások (pl. FTP, SSH, DNS, HTTP) számára van fenntartva. Néha szükséges tudni, hogy mely aktív TCP-kapcsolatok vannak nyitva és melyek futnak egy hálózatba kötött állomáson. A netstat egy fontos hálózati segédprogram, mely ezen kapcsolatok ellenőrzésére használható.

**A TCP kommunikációs folyamata**

A szerveren futó minden egyes alkalmazási folyamat esetében be kell állítani egy portszám használatát, amely történhet automatikusan, de végezheti a rendszergazda is. A TCP szerverfolyamatai az alábbiak: TCP-kéréseket küldő kliensek, célportok kérése, forrásportok kérése, a cél- és forrásportokra vonatkozó kérések válaszai. Egy TCP által támogatott párbeszéd bontásához, mindkét munkamenetet meg kell szüntetni, amelyhez négy adatcsere szükséges. A kliens és a szerver egyaránt kezdeményezheti a megszüntetést. A háromfázisú kézfogás megállapítja, hogy a céleszköz jelen van-e a hálózaton, ellenőrzi, hogy a céleszköz rendelkezik-e aktív szolgáltatással, fogadja-e a kezdeményező kliens által használni kívánt célportra küldött kéréseket, valamint tájékoztatja a céleszközt, hogy a forráskliens az adott portszámon kommunikációs munkamenetet kíván létrehozni. A Vezérlőbitek mező hat jelzőbitje: URG, ACK, PSH, RST, SYN és FIN.

**Megbízhatóság és forgalomszabályozás**

Ahhoz, hogy a fogadó fél megértse az eredeti üzenetet, minden adatnak meg kell érkeznie, és a szegmensekben lévő adatokat ismét az eredeti sorrendben kell összeállítani. Minden egyes csomag fejlécében szerepel egy sorszám. Nem számít, hogy mennyire jól megtervezett a hálózat, adatvesztés időnként előfordul. A TCP lehetőséget nyújt a szegmensveszteségek kezelésére. Ilyen például a nem nyugtázott adatszegmensek újraküldésének mechanizmusa is. A kliens operációs rendszerek ma már jellemzően egy opcionális TCP-funkciót alkalmaznak, amelyet a háromfázisos kézfogás során tárgyalt szelektív nyugtázásnak (SACK) nevezünk. Ha mindkét állomás támogatja a SACK szolgáltatást, a fogadó fél egyértelműen nyugtázhatja, hogy mely szegmensek (bájtok) érkeztek meg, beleértve a nem folytonos szegmenseket is. A küldő állomásnak ezért csak a hiányzó adatokat kell újraküldenie. Az adatfolyam-vezérlés azzal segíti a TCP-átvitel megbízhatóságának megőrzését, hogy mindig az adott munkamenethez igazítja az adatátvitel sebességét a forrás és a cél között. Ennek céljából a TCP-fejléc tartalmaz egy 16 bites mezőt, amelynek ablakméret (window size) a neve. A beérkezett bájtok feldolgozása során a nyugtát küldő cél és a forrás küldési ablakméretének folyamatos változtatása csúszóablakként ismert. A forrás 1.460 bájt adatot továbbíthat minden TCP-szegmensben. Ez a céleszköz által fogadható tipikus MSS érték. A torlódások elkerülése és ellenőrzése érdekében a TCP számos torlódáskezelési mechanizmust alkalmaz. A forrás az elküldött, de nem nyugtázott bájtok számát csökkenti, nem pedig a cél által meghatározott ablakméretet.

**UDP-kommunikáció**

Az UDP egy egyszerű protokoll, amely a szállítási réteg alapfeladatait látja el. Amikor UDP-datagramot küldünk egy célállomásnak, azok különböző útvonalat választhatnak, így gyakran előfordulhat, hogy az adatok rossz sorrendben érkeznek meg. Az UDP nem követi nyomon a sorszámokat, mint a TCP. Az UDP semmilyen módszerrel nem rendelkezik a datagramok eredeti sorrendjének helyreállításához. Ezért az UDP érkezési sorrendben állítja össze az adatokat, majd továbbküldi azokat az alkalmazásnak. Ha az adatsorrend lényeges az alkalmazás szempontjából, akkor az alkalmazásnak kell meghatároznia a helyes sorrendet, valamint az adatok feldolgozásának módját. Az UDP-t használó szerveralkalmazásokhoz is közismert vagy bejegyzett portszámok vannak hozzárendelve. Ha olyan datagram érkezik, amelyet ezen portok egyikének címeztek, az UDP a portszám alapján továbbítja az adatokat a megfelelő alkalmazáshoz. Az UDP-kliensfolyamat dinamikusan választ egy portszámot a portszámok tartományából, amelyet később a párbeszéd forrásportjaként használ. A célport általában egy szerverfolyamathoz rendelt jól ismert vagy bejegyzett portszám. Miután a kliens kiválasztotta a forrás- és célportot, a tranzakció során végig ugyanaz a portpár szerepel az összes datagram fejlécében. Ami a szervertől a klienshez visszaérkező adatokat illeti, a datagramok fejlécében szereplő forrás- és célportok felcserélődnek.

14.8.3

## Ellenőrző kvíz - Szállítási réteg

Az űrlap teteje

1. Melyik szállítási rétegbeli jellemző garantálja egy összeköttetés létrehozását?

Az űrlap alja

Melyik tartományba esnek a TCP és UDP "gyakran használt" (well-know) portjai?

Mi a socket?

Hogy kezeli egy hálózati szerver a több klienstől beérkező különböző szolgáltatásokra vonatkozó kéréseket?

Mi történik, amikor egy FTP-üzenet egy része nem érkezik meg a célállomáshoz?

Milyen típusú alkalmazások alkalmasak az UDP használatára?

A hálózati torlódások eredményeként a forrás a célállomásra küldött TCP-szegmensek elvesztését tapasztalja. Mi az egyik módja annak, hogy a TCP-protokoll megoldja ezt a problémát?

Melyik két műveletet biztosítja a TCP, amit az UDP nem? (Két jó válasz van.)

Qual é o propósito de usar um número da porta origem em uma comunicação TCP?

Quais duas flags no cabeçalho TCP são usadas em um handshake triplo de TCP para estabelecer conectividade entre dois dispositivos de rede? (Escolha duas.)

elyik TCP-mechanizmust használják a torlódások elkerülése érdekében?

Milyen műveletet végez el egy kliens, amikor UDP-protokoll használatával kommunikációs kapcsolatot létesít egy szerverrel?

Melyik két szolgáltatás vagy protokoll használja az UDP-protokollt a gyors átvitelhez és az alacsony terheléshez? (Két jó válasz van)

Melyik szám vagy számok jelölnek egy socket-et?

Mi a szerepe a szállítási rétegbeli protokolloknak?

[14.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Az UDP-kommunikáció](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                   
*   

1. alkalmazási réteg
2. Bevezetés

# Bevezetés

15.0.1

## Miért érdemes elvégezni ezt a modult?

Üdvözöljük az Alkalmazási réteg című fejezetben!

Ahogy megtanultuk, a szállítási réteg biztosítja az adatok átkerülését egyik állomásról a másikra. A helyes adatszállítás érdekében azonban sok fontos részletet kell még meghatározni. Ezért van egy alkalmazási réteg mind az OSI, mind a TCP/IP modellekben. Például, az internetes videómegosztás lehetőségének megjelenése előtt számos más módon kellett otthoni filmeket néznünk. Képzeljük el, hogy videóra vettük a gyerekünk focimeccsét. A nagyszülőknek egy másik városban csak videokazettás lejátszójuk van. A felvételt egy megfelelő típusú videokazettára kell másolnunk és elküldeni nekik. Az öcsénknek pedig DVD-lejátszója van, ezért átmásoljuk a videót egy DVD-re és úgy küldjük el neki. Az alkalmazási réteg pontosan ezt teszi, ügyelve arra, hogy az adatok olyan formátumban legyenek, amelyet a fogadó eszköz képes használni. Merüljünk bele!

15.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe**: Alkalmazási réteg

**Fejezet célja**: Az alkalmazási rétegbeli protokollok működésének ismertetése, és a végfelhasználói alkalmazások támogatásában játszott szerepének bemutatása.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Alkalmazási, megjelenítési és viszony réteg.** | Bemutatni, hogyan működnek együtt az alkalmazási, megjelenítési és viszony rétegek funkciói a végfelhasználói alkalmazások hálózati szolgáltatásainak biztosítása érdekében. |
| **Egyenrangú (peer-to-peer) hálózatok** | Bemutatni, hogyan működnek a végfelhasználói alkalmazások egy egyenrangú hálózatban. |
| **Web és e-mail protokollok** | Bemutatni, hogyan működnek a webes és e-mail protokollok. |
| **IP címszolgáltatások** | Ismertetni a DNS és a DHCP működését. |
| **Fájlmegosztási szolgáltatások** | Bemutatni, hogyan működnek a fájlátviteli protokollok. |

[14.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alkalmazási, megjelenítési és viszony réteg](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                     
*   

1. alkalmazási réteg
2. Alkalmazási, megjelenítési és viszony réteg

# Alkalmazási, megjelenítési és viszony réteg

15.1.1

## Alkalmazási réteg

Az OSI és a TCP/IP modellekben az alkalmazási réteg a végfelhasználóhoz legközelebb eső réteg. Ez a réteg biztosítja az interfészt az alkalmazások és az üzenetek továbbítását végző hálózat között (lásd ábra). Az alkalmazási rétegbeli protokollokat a forrás- és célállomásokon futó programok közötti adatcserére használjuk.

Az ábrán az OSI és a TCP/IP modell rétegeinek összehasonlítása látható. The OSI model is shown on the left. From top to bottom are the following layer numbers and names: 7) Application, 6) Presentation, 5) Session, 4) Transport, 3) Network, 2) Data Link, and 1) Physical. The TCP/IP Model is shown on the right. From top to bottom the layer names and the associated OSI model layer numbers are: Application (OSI Layers 7, 6, and 5), Transport (OSI Layer 4), Internet (OSI Layer 3), and Network Access (OSI Layers 2 and 1). Text at the bottom reads: The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer:OSI Layer 3, the network layer, maps directly to the TCP/IP internet layer. This layer is used to describe protocols that address and route messages through an internetwork. OSI Layer 4, the transport layer, maps directly to the TCP/IP transport layer. This layer describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts. The TCP/IP application layer includes several protocols that provide specific functionality to a variety of end user applications. The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce applications that operate on networks. Both the TCP/IP and OSI models are commonly used when referring to protocols at various layers. Because the OSI model separates the data link layer from the physical layer, it is commonly used when referring to these lower layers. The Application layer ofthe OSI model specifically identifies Domain Name System, Hypertest Transfer Protocol, Simple Mail Tansfer Protocol, Post Office Protocol, Dynamic Host Configuration Protocol, FIle transfer Protocol, and Internet Message Access Protocol.

OSI Model7. Application6. Presentation5. Session4. Transport3. Network2. Data Link1. PhysicalTCP/IP ModelApplicationTransportInternetNetwork  
AccessApplication  
LayersData Flow  
LayersDomain Name System  
  
Hypertext Transfer Protocol  
  
Simple Mail Transfer Protocol  
  
Post Office Protocol  
  
Dynamic Host Configuration Protocol  
  
File Transfer Pro  
  
Internet Message Access Protocol

Az OSI modell felső három rétege (alkalmazási, megjelenítési és viszony ) határozza meg a TCP/IP alkalmazási réteg funkcióit.

Számos alkalmazási rétegbeli protokoll létezik, és több új is fejlesztés alatt áll. A legismertebb alkalmazási rétegbeli protokollok a HTTP (Hypertext Transfer Protocol), az FTP (File Transfer Protocol), a TFTP (Trivial File Transfer Protocol), az IMAP (Internet Message Access Protocol) és a DNS (Domain Name System) protokoll.

15.1.2

## Megjelenítési és viszony réteg

**Megjelenítési réteg**

A megjelenítési rétegnek három fő funkciója van:

* Az adatok átalakítása a forrás eszközön olyan formátumba, hogy azokat a cél eszköz fogadni tudja.
* Adatok tömörítése a céleszköz által kibontható módon.
* Adatok titkosítása a továbbításhoz és azok visszafejtése kézhezvételkor.

A megjelenítési réteg szabványos fájlformátumba alakítva adja át az adatokat az alkalmazási rétegnek (lásd ábra). Néhány jól ismert videó szabvány: MKV (Matroska Video), MPG (Motion Picture Experts Group), és MOV (QuickTime Video). Néhány jól ismert grafikus képformátum: GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group) és PNG (Portable Network Graphics).

The figure is a comparision of the OSI and TCP/IP model layers. The OSI model is shown on the left. From top to bottom are the following layer numbers and names: 7) Application, 6) Presentation, 5) Session, 4) Transport, 3) Network, 2) Data Link, and 1) Physical. The TCP/IP Model is shown on the right. From top to bottom the layer names and the associated OSI model layer numbers are: Application (OSI Layers 7, 6, and 5), Transport (OSI Layer 4), Internet (OSI Layer 3), and Network Access (OSI Layers 2 and 1). Text at the bottom reads: The key similarities are in the transport and network layers; however, the two models differ in how they relate to the layers above and below each layer:OSI Layer 3, the network layer, maps directly to the TCP/IP internet layer. This layer is used to describe protocols that address and route messages through an internetwork. OSI Layer 4, the transport layer, maps directly to the TCP/IP transport layer. This layer describes general services and functions that provide ordered and reliable delivery of data between source and destination hosts. The TCP/IP application layer includes several protocols that provide specific functionality to a variety of end user applications. The OSI model Layers 5, 6, and 7 are used as references for application software developers and vendors to produce applications that operate on networks. Both the TCP/IP and OSI models are commonly used when referring to protocols at various layers. Because the OSI model separates the data link layer from the physical layer, it is commonly used when referring to these lower layers. The Presentation layer specifically identifies Matroska Video(MKV), Motion Pictures Expert Group(MPG), QuickTime(MOV), Graphics Interchange Format(GIF), Joint Photographic Experts Group(JPG), and Portable Network Graphics(PNG).

OSI Model7. Application6. Presentation5. Session4. Transport3. Network2. Data Link1. PhysicalTCP/IP ModelApplicationTransportInternetNetwork  
AccessApplication  
LayersData Flow  
LayersMatroska video (MKV)  
  
Motion Pictures Expert Group (MPG)  
  
Quick Time (MOV)  
  
Graphics Interchange Format (GIF)  
  
Joint Photographic Experts Group (JPG)  
  
Portable Nerwork Graphics (PNG)

**Viszony réteg**

Ahogy a neve is utal rá, a viszony réteg feladata a forrás- és célalkalmazások közötti párbeszédek (munkamenetek) létrehozása és fenntartása. A viszonyréteg kezeli a párbeszédek kialakításához, fenntartásához, valamint a megszakadó vagy hosszabb ideje tétlen viszonyok újraindításához szükséges információcserét.

15.1.3

## TCP/IP alkalmazási rétegbeli protokollok

A TCP/IP alkalmazási protokolljai határozzák meg az internetes kommunikációs szolgáltatások formátumát és vezérlőinformációit. A kommunikációs folyamat során az alkalmazási rétegbeli protokollokat mind a forrás-, mind pedig a célállomás egyaránt használja. A kommunikáció sikere érdekében a forrás- és célállomásokon használt alkalmazási rétegbeli protokolloknak egymással kompatibilisnek kell lenniük.

Kattintsunk az egyes alkalmazási protokoll típusokra a részletek megtekintéséhez!

**﻿﻿﻿﻿﻿Névkezelő rendszer﻿** **﻿Tartománynév-kezelő rendszer (vagy szolgáltatás) (DNS - Domain Name System)﻿**

* TCP, UDP kliens 53
* Tartományneveket (mint pl.: cisco.com) lefordítja IP címekre

15.1.4

## Tudáspróba - Alkalmazási, megjelenítési és viszony réteg

Az űrlap teteje

Check your understanding of the application, presentation, and session layers by choosing the BEST answer to the following questions.

1. This layer of the OSI model is concerned with the protocols that exchange data between programs running on hosts.

Az űrlap alja

MKV, GIF, and JPG standards are associated with which OSI layer?

These three OSI layers define the same functions as the TCP/IP model application layer.

Which two are protocols that belong in the OSI application layer?

This is a function of the OSI session layer.

[15.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egyenrangú (peer-to-peer) hálózatok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                        
*   

1. alkalmazási réteg
2. Egyenrangú (peer-to-peer) hálózatok

# Egyenrangú (peer-to-peer) hálózatok

15.2.1

## Kliens-szerver modell

Az előző témakörben megtanultuk, hogy a forrás- és a célállomáson alkalmazott TCP/IP alkalmazási rétegbeli protokolloknak kompatibiliseknek kell lenniük. Ebben a témakörben megismerjük a kliens/szerver modellt és az alkalmazási rétegben használt folyamatokat. Ugyanez igaz a peer-to-peer hálózatra is. A kliens-szerver modellben az információt kérő eszközt kliensnek, a kérésre válaszoló eszközt pedig szervernek vagy kiszolgálónak nevezzük. A kliens egy hardverből és szoftverből álló eszköz, amelyet az emberek a kiszolgálón tárolt erőforrások közvetlen elérésére használnak.

A kliens- és szerverfolyamatokat az alkalmazási réteghez soroljuk. A párbeszédet a kliens kezdeményezi azzal, hogy adatokat kér a szervertől, amely egy vagy több adatfolyam elküldésével válaszol. A kliensek és szerverek közötti kérések és válaszok formátumát az alkalmazási rétegbeli protokollok határozzák meg. A tényleges adatátvitel mellett ez a párbeszéd a felhasználó hitelesítését, valamint az átvitt adatfájl azonosítását is megkövetelheti.

A kliens-szerver hálózat egy példája, amikor egy ISP e-mail szolgáltatását használjuk levelek küldésére, fogadására és tárolására. Az otthoni számítógépen lévő levelezőprogram kérést intéz az ISP szerveréhez az olvasatlan levelekért. A szerver a válaszüzenetében elküldi a kért levelet a kliensnek. A kliensről a szerverre történő adatátvitelt feltöltésnek (upload), míg a szerverről a kliensre történőt letöltésnek (download) nevezzük.

Az ábrán látható, hogy fájlok töltődnek le a kiszolgálóról az ügyfélre.

The figure depicts the client server model. A client which is depicted as a cell phone, computer, or VoIP phone is connected to a server and downloading files from the server.



DownloadNetworkClientServer

15.2.2

## Egyenrangú (Peer-to-Peer) hálózatok

Az egyenrangú (P2P, peer-to-peer) hálózati modellben az adatok elérése dedikált szerver használata nélkül, egy társ eszközről (peer) történik.

A P2P hálózati modell két részre bontható: P2P hálózatokra és P2P alkalmazásokra. Mindkét résznek hasonlók a tulajdonságaik, de a gyakorlatban egészen másként működnek.

Egy P2P hálózatban két vagy több számítógép csatlakozik egymáshoz a hálózaton keresztül úgy, hogy dedikált szerver nélkül oszthatják meg egymás között az erőforrásaikat (pl. nyomtatókat vagy fájlokat). Minden csatlakoztatott végberendezés (más néven peer) működhet szerverként és kliensként is egyben. Egy számítógép az egyik adatátviteli folyamatban betöltheti a szerver szerepkörét, míg egy másikban ezzel egyidejűleg kliens is lehet. A szerver és kliens szerepköröket az egyes kérések határozzák meg.

Egy ilyen hálózat a fájlok megosztásán kívül a felhasználóknak a hálózati játékok használatát, vagy egy internetkapcsolat megosztását is biztosíthatja.

A peer-to-peer működés során mindkét eszköz egyenrangúnak tekinthető a kommunikációs folyamatban. Peer 1 fájlokat oszt meg Peer 2 számára, ugyanakkor hozzáfér a Peer 2-höz közvetlenül csatlakozó megosztott nyomtatóhoz. Az ábrán látható, hogy Peer 2 megosztja a közvetlenül csatlakoztatott nyomtatót Peer 1-gyel, miközben hozzáfér a megosztott fájlokhoz a Peer 1 oldalon.

The figure depicts the peer to peer model. Two computers are connected by a switch and are communicating directly with each other. In addition a printer is shared by one of the computers and can be accessed by either computer in the figure.

Peer 1Print client File ServerPeer 2Directly connected printerPrinterPrint Server File Client

15.2.3

## Peer-to-Peer Applications

Egy peer-to-peer (P2P) alkalmazás lehetővé teszi, hogy egy eszköz ugyanabban a kommunikációban egyszerre kliens és szerver is lehessen (lásd ábra). Ebben a modellben minden kliens szerver is és minden szerver kliens is egyben. A P2P-alkalmazások megkövetelik, hogy minden végberendezés biztosítson egy felhasználói felületet és egy háttérszolgáltatást is futtasson.

Bizonyos P2P-alkalmazások úgynevezett hibrid rendszert használnak, ahol az erőforrások megosztása ugyan decentralizált, de az erőforrások helyeire mutató indexeket már egy központi címtárban tárolják. A hibrid rendszerekben minden csomópont (peer) hozzáfér egy indexszerverhez, ahonnan lekérdezheti a más csomópontokon tárolt erőforrások helyét.

Az ábra egy P2P-alkalmazást mutat be, amely a peer-to-peer modell hibrid verziója. A két azonnali üzenetküldő alkalmazás egymással kommunikál a hálózaton keresztül, ahol mindkét alkalmazás kliensként és kiszolgálóként is működik.

Good.I'll be there.Meeting tonight.I'll be there.Good.Meeting tonight.Client and ServerNetworkClient and ServerInstant MessageInstant MessageSendReceiveReceiveSend

Mindkét kliens egyidejűleg kezdeményezi és fogadja az üzeneteket.

15.2.4

## Gyakori P2P-alkalmazások

Egy P2P-alkalmazást futtató hálózati számítógép kliensként és szerverként is működhet a hálózat azon többi számítógépe számára, amelyek ugyanazt az alkalmazást használják. Néhány ismert P2P-hálózat:

* BitTorrent
* Direct Connect
* eDonkey
* Freenet

Egyes P2P-alkalmazások a Gnutella protokollon alapulnak, ahol minden felhasználó fájlokat oszt meg más felhasználókkal. A Gnutella kompatibilis kliensszoftver lehetővé teszi a felhasználóknak, hogy az interneten Gnutella szolgáltatásokhoz kapcsolódjanak, és más Gnutella csomópontok által megosztott állományokat találjanak meg és férjenek hozzájuk (lásd ábra). Gnutella kliens alkalmazás például a μTorrent, a BitComet, a DC++, a Deluge és az eMule.

The figure shows a P2P application searching for shared resources. The P2papplication is asking its pers if the have the resource in this case mysong.mp3.

Where is: mysong.mp3I've got it.I've got it.NetworkI've got it.

Gnutella P2P applications search for shared resources on multiple peers.

Számos P2P-alkalmazás lehetővé teszi a felhasználók számára, hogy a fájlok egyes részeit osszák meg egymással. Az ügyfelek egy torrent fájlt használnak arra, hogy megkeressék a keresett állomány darabjait megosztó felhasználókat, így közvetlenül kapcsolódhatnak hozzájuk. Ez a fájl tartalmazza az úgynevezett tracker számítógépek információit, amelyek nyomon követik, hogy mely felhasználóknál találhatók bizonyos fájlok konkrét darabjai. Az ügyfelek egyszerre több felhasználótól kérnek darabokat. A módszer neve swarm (nyüzsgés, rajzás), a technológia neve pedig BitTorrent. A BitTorrentnek saját ügyfélszoftvere van. De van sok más BitTorrent ügyfél is, például: uTorrent, Deluge, és qBitTorrent.

**MEGJEGYZÉS:** Bármilyen típusú fájl megosztható a felhasználók között. Sok ilyen fájl szerzői jogvédelem alatt áll, ami azt jelenti, hogy csak az alkotónak van joga használni és terjeszteni őket. Törvényellenes a szerzői jog által védett fájlok letöltése vagy terjesztése a szerzői jog tulajdonosának engedélye nélkül. A szerzői jog megsértése büntetőjogi felelőséggel jár és polgári pereket eredményezhet.

15.2.5

## Tudáspróba - Egyenrangú (peer-to-peer) hálózatok

Az űrlap teteje

Check your understanding of peer-to-peer by choosing the BEST answer to the following questions.

1. True or false? The peer-to-peer networking model requires the implementation of a dedicated server for data access.

Az űrlap alja

True or false? In a peer-to-peer network environment every peer can function as both a client and a server.

Which peer-to-peer application allows users to share pieces of many files with each other at the same time?

Which of the following is a feature of the Gnutella protocol?

[15.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Alkalmazási, megjelenítési és viszony réteg](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Web és e-mail protokollok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                           
*   

1. alkalmazási réteg
2. Web és e-mail protokollok

# Web és e-mail protokollok

15.3.1

## HTTP (HyperText Transfer Protocol) és HTML (Hypertext Markup Language)

Vannak olyan alkalmazási rétegbeli protokollok, amelyeket specifikus célokra terveztek, mint például a webböngészés és az elektronikus levelezés (e-mail). Az első témakör ezekről a protokollokról adott áttekintést. Most egy részletesebb ismertetés következik.

Amikor egy webcímet vagy URL-t (Uniform Resource Locator) begépelünk egy webböngészőbe, a böngésző a HTTP-protokollt használva építi ki a kapcsolatot a szerveren futó web-szolgáltatással. A webszolgáltatás egy HTTP-protokollt használó kiszolgálón fut. Az URL-ek és az URI-k (Uniform Resource Identifier, egységes erőforrás-azonosító) olyan nevek, amelyeket a legtöbb ember a webcímekkel társít.

A webböngésző és a webszerver interakciójának jobb megértése érdekében megvizsgáljuk, hogyan nyílik meg egy oldal a böngészőben. Példaként használjuk a <http://www.cisco.com/index.html> URL-t.

További információért kattintsunk a gombokra!

**1. lépés**

A böngésző az URL három részét vizsgálja:

* http (az alkalmazott protokoll vagy séma)
* [www.cisco.com](http://www.cisco.com) (a kiszolgáló neve)
* index.html (a kért fájl neve)

shows a http server connected thru the internet to a client computer. The client computer is requesting the url [www.cisco.com](http://www.cisco.com) which is the HTTP server.

HTTP ServerNetworkClienthttp://www.cisco.com/index.html

15.3.2

## HTTP és HTTPS

A HTTP egy kérés/válasz protokoll. Amikor egy kliens, általában egy webböngésző, kérést küld a webszervernek, a kommunikációhoz HTTP-üzenettípusokat használ. A három leggyakoribb üzenettípus a GET, a POST és a PUT (lásd ábra).

* **GET** - A kliens adatkérése. A kliens (webböngésző) egy GET-üzenetet küld a webszervernek a HTML-oldalak lekérésére.
* **POST** \ - Adatfájlokat tölt fel a webkiszolgálóra, például űrlapadatokat.
* **PUT** - Állományokat vagy egyéb tartalmakat tölt fel a webszerverre, például képeket.

The figure depicts a client performing a HTTP request to a HTTP server. THe file requested is a Fully Qualified Domain Name. The request uses a Get to retrieve the web page. The URL field is shown on the client computer as a <http://www.cisco.com> request.



HTTP ServerClientUniform Resource Locator (URL)HTTP RequestFile RequestedHost : www.cisco.com  
GET /index.html HTTP/1.1Fully qualified domain name

Bár a HTTP rendkívül rugalmas, de nem biztonságos protokoll. A kérés üzenetek az információt kódolatlan szövegként továbbítják a szerverhez, amely így elfogható és mások által is elolvasható. A kiszolgálói válaszok, jellemzően HTML-oldalak, ugyancsak titkosítatlanok.

A biztonságos internetes kommunikáció megvalósítására a HTTPS (HTTP Secure) protokollt alkalmazzák. A kliens és a szerver közötti adatbiztonság megvalósítására a HTTPS hitelesítést és titkosítást alkalmaz. A HTTPS ugyanazt a kliens-szerver folyamatot használja mint a HTTP, csak a hálózati átvitelt megelőzően az adatfolyamot SSL-el (Secure Socket Layer) titkosítja.

15.3.3

## E-mail protokollok

Az elektronikus levelezés az ISP-k által nyújtott egyik elsődleges szolgáltatás. Az elektronikus levelezés működéséhez számos alkalmazásra és szolgáltatásra van szükség (lásd ábra). Az elektronikus levelezés szolgáltatás a tárol és továbbít módszert alkalmazza az üzenetek hálózaton történő küldésére, tárolására és elérésére. Az elektronikus leveleket a levelezőkiszolgálók adatbázisokban tárolják.

The figure depicts an email transaction from a sender using the SMTP protocol sending an email to [recipient@cisco.com](mailto:recipient@cisco.com) thru an ISP mail server A arriving at the recipients ISP email server B and the recipient reading the email using either IMAP or POP protocol.



InternetIMAP or POP3SMTPISP AISP BSenderRecipientMail ServerMail Server SMTPSend to  
recipient@cisco.com

A levelezőkliensek szervereken keresztül küldik és fogadják a leveleket. Az üzenetek egyik tartományból a másikba történő továbbítása esetén a levelezőszerverek más levelezőszerverekkel is kapcsolatba kerülnek. Levélküldéskor a kliensek nem közvetlenül egymással kommunikálnak. Ehelyett mindkét kliens a levelezőszervert bízza meg az üzenetek továbbításával.

Az e-mail három különböző protokollt használ a működéséhez: SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) és IMAP (Internet Message Access Protocol). A levelet elküldő alkalmazási rétegbeli folyamat az SMTP-t használja. Az ügyfél pedig a POP vagy az IMAP alkalmazási rétegbeli protokollok valamelyikével tölti le a leveleket.

15.3.4

## SMTP, POP és IMAP

További információért kattintsunk a gombokra!

**SMTP**

Az SMTP üzenetformátuma egy üzenetfejlécből és egy üzenettörzsből áll. Míg az üzenet törzse tetszőleges mennyiségű szöveget tartalmazhat, addig a fejlécnek megfelelő formátumban kell tartalmaznia a címzett és a feladó e-mail címét.

Amikor az ügyfél e-mailt küld, akkor az SMTP folyamata kapcsolódik a kiszolgáló SMTP folyamatához a jól ismert 25-ös porton. A kapcsolat létrejötte után a kliens megpróbálja a levelet elküldeni a szervernek. Ha a kiszolgáló megkapja az üzenetet, akkor vagy elhelyezi egy helyi levelezőfiókban vagy továbbítja egy másik kiszolgálónak ugyanazon az SMTP-folyamaton keresztül.

Előfordulhat, hogy az üzenetek küldésekor a címzett levelezőszervere nem elérhető. Ilyenkor az SMTP várakoztatja az üzeneteket, hogy azokat egy későbbi időpontban elküldhesse. A kiszolgáló periódikus időközönként ellenőrzi az üzenetsort és újra megpróbálja elküldeni. Ha az üzenetet nem sikerült egy előre meghatározott lejárati időn belül kézbesíteni, akkor az visszakerül a feladóhoz.

This is a figure with a sender computer and recipient computer. Two SMTP/POP3 servers are connected between the two. A mail message is sent from the sender computer labeled [recipient@domain.com](mailto:recipient@domain.com) using smtp protocol. The first SMTP/POP3 receives the message from the sender and asks Is the recipient in my list of recipients? No. forward email to another server. The second SMTP/POP3 server receives the message via the SMTP protocol and forwards the message to the recipient.

Recipientrecipient@domain.comSend EmailSenderSMTP/POP3   
ServerSMTP/POP3   
ServerIs the recipient in my list of recipients ?  
No.  
Forward email to another server.SMTPSMTP

15.3.5

## Tudáspróba - Web és ﻿E-mail protokollok

Az űrlap teteje

Check your understanding of web and email protocols by choosing the BEST answer to the following questions.

1. This message type is used when uploading data files to a web server.

Az űrlap alja

This protocol is used by a web browser to establish a connection to a web server.

This protocol is used by a client to send email to a mail server.

Which is a feature of IMAP?

True or false? HTTP is a secure protocol.

[15.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Egyenrangú (peer-to-peer) hálózatok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IP-címzési szolgáltatások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                  
*   

1. alkalmazási réteg
2. IP-címzési szolgáltatások

# IP-címzési szolgáltatások

15.4.1

## Tartománynév szolgáltatás (Domain Name System, DNS)

Vannak olyan alkalmazási rétegbeli protokollok, amelyek megkönnyítik a hálózati eszközök címének megszerzését. Ezek a szolgáltatások elengedhetetlenek, mert nagyon időigényes lenne megjegyezni az IP-címeket URL-ek helyett, vagy manuálisan konfigurálni az összes eszközt egy közepes vagy nagy hálózaton. A fejezet első témaköre ezekről a protokollokról adott áttekintést. Ez a témakör részletesen ismerteti az IP-címzési szolgáltatásokat, a DNS-t és a DHCP-t.

Az adathálózatok eszközei a hálózaton keresztüli adatküldéséhez és fogadáshoz numerikus IP-címeket használnak. A tartományneveket a numerikus címek egyszerű, megjegyezhető nevekké alakítása érdekében hozták létre.

A tartománynevek, mint például a [www.cisco.com](http://www.cisco.com) sokkal könnyebben megjegyezhetők az emberek számára, mint mondjuk a 198.133.219.25, ami ennek a szervernek a tényleges IP-címe. Ha a Cisco úgy dönt, hogy megváltoztatja a [www.cisco.com](http://www.cisco.com) webhely IP-címét, akkor ez a változtatás nem érinti a felhasználót, mivel a tartománynév ugyanaz marad. Az új címet egyszerűen a meglévő tartománynévhez kötik és így az elérhetőség továbbra is fennmarad.

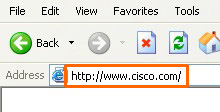
A DNS-protokoll egy automatikus szolgáltatást definiál, amely erőforrásneveket társít a kért numerikus hálózati címhez. Tartalmazza még a lekérdezések, a válaszok és az adatok formátumát. A DNS-protokollra épülő kommunikációk egyetlen, üzenetnek nevezett formátumot használnak. Ezt az üzenetformátumot használják a klienslekérdezések és a szerverválaszok minden fajtájához, a hibaüzenetekhez, valamint az erőforrásrekordok szerverek közötti továbbításához.

További információért kattintsunk a gombokra!

**1. lépés**

A felhasználó beírja a teljes tartománynevet a böngészőalkalmazás cím mezőjébe.

this is a figure with a client contacting a DNS sever thru the network with a FQDN typed in a browser URL field because the name of a website is easier for people to used



The name is easy for people to use.DNS ServerNetworkClient

15.4.2

## A DNS üzenetformátuma

A DNS-szerver a nevek feloldásához különböző típusú erőforrásrekordokat tárol. Ezek a bejegyzések a rekord nevét, címét és típusát tartalmazzák. Néhány rekordtípus:

* **A** - Egy állomás IPv4-címe
* **NS** - Mértékadó névszerver
* **AAAA** - Egy állomás IPv6-címe
* **MX** - Levelezőszerver bejegyzés

A kliens lekérdezésére a szerver a névfeloldáshoz először saját rekordjait vizsgálja meg. Ha a tárolt rekordjai alapján nem tudja a nevet feloldani, más szerverekkel lép kapcsolatba. Miután a keresés eredményre vezetett, és a válasz visszajutott az eredeti kérelmező szerverhez, az a névhez tartozó címet átmenetileg eltárolja, arra az esetre, ha a címet újra kérnék.

A Windows-os PC-k DNS-kliense a névfeloldás teljesítményét úgy optimalizálja, hogy a korábban feloldott neveket a saját memóriájában is eltárolja. Az **ipconfig /displaydns** ipconfig /displaydns parancs megjeleníti az összes gyorsítótárazott DNS-bejegyzést.

A táblázatban az látható, hogy a DNS ugyanazt az üzenetformátumot használja a kérésekhez, a válaszokhoz, az engedélyezéshez és a kiegészítő információkhoz a kliens és a szerver közötti kommunikáció során, beleértve a hibaüzeneteket és az erőforrásrekord információk átvitelét is.

| DNS message section Description Question The question for the name server Answer Resource Records answering the question Authority Resource Records pointing toward an authorityAdditionalResource Records holding additional information | |
| --- | --- |
| **DNS-üzenet** | **Leírás** |
| Kérés (Question) | Kérés a névkiszolgáló felé |
| Válasz (Answer) | A kérésre válaszul adott erőforrásrekord |
| Engedélyezés (Authority) | Engedélyező felé mutató erőforrásrekord |
| További információk (Additional) | További információkat tartalmazó erőforrásrekord |

15.4.3

## DNS-hierarchia

A DNS-protokoll a névfeloldásra egy hierarchikusan felépített adatbázist használ (lásd ábra). A DNS a tartománynevekből építi fel a hierarchiát.

Az elnevezési struktúra kisebb, könnyen kezelhető zónákra lett osztva. Minden DNS-kiszolgáló egy meghatározott adatbázis fájlt tárol és a DNS-struktúra csak kis részének név – IP-cím hozzárendeléséért felelős. Amikor egy DNS-szerver olyan névfeloldási kérést kap, amely nincs benne a zónájában, akkor azt a szerver egy másik, a megfelelő zónához tartozó DNS-szerverhez továbbítja. A DNS egy skálázható szolgáltatás, mivel a névfeloldás több kiszolgálóra támaszkodik.

A legfelső szintű tartományok a szervezet típusát vagy a származási országot jelölik. Példák legmagasabb szintű tartományokra:

* **.com** - ipari vagy üzleti vállalat
* **.org** - nonprofit szervezet
* **.au** - Ausztrália
* **.hu** - Magyarország

The figure shows the DNS Hierachy tree. At the top is the Root Level Domain with the TOp-Level Domains(TLD) connected undererneath the Root Level Domainmain. THe TLDs are .net, .edu, .com,.au, .co, and other top-level doamins. Under the .com TLD is the Second Level domain [www.cisco.com](http://www.cisco.com) and under cisco.com are [www.cisco.com](http://www.cisco.com) , ftp.cisco.com, and mail.cisco.com.

Root Level DomainTop-Level Domain (TLD)Second Level Domaincisco.comwww.cisco.comftp.cisco.commail.cisco.com.net.edu.com.au.coOther   
Top-Level   
Domains

15.4.4

## Az nslookup parancs

Egy hálózati eszköz konfigurálásakor általában egy vagy több DNS-szerver címét is megadjuk, amelyeket a DNS-kliens a névfeloldáskor használ. A DNS-szerverek címeit rendszerint az internetszolgáltató (ISP) biztosítja. Amikor egy felhasználói alkalmazás név alapján szeretne egy távoli eszközhöz csatlakozni, a DNS-kliens ezen névszerverek egyikét kérdezi le, hogy a nevet numerikus címmé alakítsa.

Az operációs rendszereknek van egy nslookup nevű segédprogramja is, amely lehetővé teszi a felhasználó számára egy adott állomásnév feloldását a névszerverek manuális lekérdezésével. Ezt a segédprogramot névfeloldási problémák hibakereséséhez és a névszerverek pillanatnyi állapotának ellenőrzésére is használhatjuk.

Az ábrán a **nslookup** parancs kiadása után az állomáson alapértelmezettként beállított DNS-szerver jelenik meg. Az **nslookup** parancssorában az állomás vagy tartomány neve adható meg. Az nslookup számos lehetőséget biztosít a DNS-folyamat átfogó tesztelésre és ellenőrzésére.

C:\Users> **nslookup**

Default Server: dns-sj.cisco.com

Address: 171.70.168.183

> **www.cisco.com**

Server: dns-sj.cisco.com

Address: 171.70.168.183

Name: origin-www.cisco.com

Addresses: 2001:420:1101:1::a

173.37.145.84

Aliases: www.cisco.com

> c**isco.netacad.net**

Server: dns-sj.cisco.com

Address: 171.70.168.183

Name: cisco.netacad.net

Address: 72.163.6.223

>

15.4.5

## Parancsszimulátor - Az nslookup parancs

Gyakoroljuk az nslookup parancs használatát Windows és Linux rendszerben!

From the Windows command prompt, enter the **nslookup** command to begin a manual query of the name servers.

C:\> nslookup

Default Server: Unknown

Address: 10.10.10.1

The output lists the name and IP address of the DNS server configured in the client. Note that the DNS server address can be manually configured, or dynamically learned, through DHCP. You are now in **nslookup** mode. Enter the domain name www.cisco.[]()com.

>www.cisco.com

Server: UnKnown

Address: 10.10.10.1

Non-authoritative answer:

Name: e2867.dsca.akamaiedge.net

Addresses: 2600:1404:a:395::b33

2600:1404:a:38e::b33

172.230.155.162

Aliases: www.cisco.com

www.cisco.com.akadns.net

wwwds.cisco.com.edgekey.net

wwwds.cisco.com.edgekey.net.globalredir.akadns.net

The output lists the ‘www.cisco.[]()com’ related IP addresses that the server ‘e2867’ currently has in its database. Notice that IPv6 addresses are also listed. In addition, various aliases are shown that will resolve to ‘www.cisco.[]()com’.

Enter the **exit** command to leave nslookup mode and return to the Windows command line.

>exit

You can directly query the DNS servers by simply adding the domain name to the **nslookup** command.

Enter **nslookup www.google.[]()com**.

C:\> nslookup www.google.com

Server: UnKnown

Address: 10.10.10.1

Non-authoritative answer:

Name: www.google.com

Addresses: 2607:f8b0:4000:80f::2004

172.217.12.36

=========================================

You are now working from Linux command prompt. The nslookup command is the same.

* Enter the **nslookup** command to begin a manual query of the name servers.
* Enter **www.cisco.[]()com** at the > prompt.
* Enter the **exit** command to leave nslookup mode and return to the Linux command line.

user@cisconetacad$nslookup

Server: 127.0.1.1

Address: 127.0.1.1#53

>www.cisco.com

Non-authoritative answer:

www.cisco.com canonical name = www.cisco.com.akadns.net.

www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.

wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.

wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e144.dscb.akamaiedge.net.

Name: e144.dscb.akamaiedge.net

Address: 23.60.112.170

>exit

As in Windows, you can directly query the DNS servers by simply adding the domain name to the **nslookup** command. Enter **nslookup www.google.[]()com**.

user@cisconetacad$nslookup www.google.com

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: www.google.com

Address: 172.217.6.164

Name: www.google.com

Address: 2607:f8b0:4000:812::2004

You successfully used the \*\*nslookup\*\* command to verify the status of domain names.

15.4.6

## Dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP)

A dinamikus állomáskonfiguráló protokoll (DHCP) automatizálja az IP-címek, alhálózati maszkok, átjárók és egyéb IP-hálózati paraméterek kiosztását. Ezt dinamikus címzésnek nevezzük. A dinamikus címzés alternatívája a statikus címzés. Statikus címzés alkalmazásakor a rendszergazda manuálisan állítja be az IP-címzési információkat az állomásokon.

Amikor egy állomás csatlakozik a hálózathoz, felveszi a kapcsolatot a DHCP-kiszolgálóval és egy címet kér. A DHCP-szerver kiválaszt egy címet a készletnek (pool) nevezett, előre konfigurált címtartományból és egy meghatározott időtartamra kiutalja (bérbe adja) azt az állomásnak.

Nagyobb helyi hálózatokban, vagy ahol a felhasználók gyakran változnak, a DHCP a javasolt címkiosztási módszer. Új felhasználók jöhetnek, akiknek csatlakozásra van szükségük, mások új munkaállomásokat kaphatnak, amiket ugyancsak csatlakoztatni kell. A kapcsolatok statikus címzése helyett sokkal hatékonyabb, ha azok hozzárendelése automatikusan, DHCP-vel történik.

A DHCP képes IP-címeket kiosztani egy beállítható időtartamra, az úgynevezett bérleti időszakra. A bérleti időszak fontos DHCP-beállítás. Amikor a bérleti időszak lejár, vagy a DHCP-kiszolgáló DHCPRELEASE üzenetet kap, a cím visszakerül a DHCP-készletbe újrafelhasználás céljából. A DHCP segítségével a felhasználók szabadon mozoghatnak egyik helyről a másikra és csatlakozhatnak újra a hálózathoz.

Az ábrán is látható, hogy különböző típusú eszközök lehetnek DHCP-szerverek. A legtöbb közepes és nagyméretű hálózatban a DHCP-kiszolgáló általában egy erre a célra kinevezett PC-alapú szerver. Otthoni hálózatokban a DHCP-szerver általában a helyi router, amely az otthoni hálózatot az ISP-hez csatlakoztatja.

The figure depicts a ISP DHCP server connected to the Internet with three ISP routers labelled ISP1, ISP2, ISP#. Each ISP reouter is connected to a different network. ISP1 connects to a wireless antenna to a mobile worker who is the DCHP client. ISP2 is connected to a coporate network router which connects to a coporate LAN with its own local DHCP server connected to a swith connected to six DHCP clients. ISP3 is connected to a wireless DHCP server for a Home and Small Business network the three DHCP clients connected.



InternetISP 2ISP 1ISP 3ISP DHCP ServerRouter DHCP ServerMobile WorkerHome and Small Business NetworkDHCP ClientCorporate NetworkDHCP ClientsDHCP ClientsLocal DHCP ServerDHCP Server

Sok hálózat használ egyszerre DHCP-t és statikus címzést is. A DHCP általános célú állomásokhoz, például végfelhasználói eszközökhöz használható. A statikus címzés hálózati eszközökhöz alkalmazható (például routerek, switch-ek, szerverek és nyomtatók).

Az IPv6-alapú DHCP (DHCPv6) hasonló szolgáltatásokat nyújt az IPv6-ügyfelek számára. Az egyik fontos különbség az, hogy a DHCPv6 nem osztja ki az alapértelmezett átjáró címét. Ez csak router RA-üzenetéből (Router Advertisement) érhető el dinamikusan.

15.4.7

## A DHCP működése

Amikor egy DHCP-re konfigurált eszköz elindul vagy csatlakozik a hálózatra, a kliens egy szórásos DHCP-felfedező (DHCPDISCOVER) üzenetet küld szét az elérhető DHCP-szerverek megtalálásához (lásd ábra). A DHCP-szerver egy DHCP-ajánlás (DHCPOFFER) üzenettel válaszol, amely a kliensnek felajánl egy címbérletet. Az ajánlat tartalmazza a kiosztott IP-címet és az alhálózati maszkot, valamint a DNS-szerver és az alapértelmezett átjáró IP-címét. A címbérleti ajánlat tartalmazza még a bérlet időtartamát is.

The figure shows a protocol ladder with a DHCP client on one side and a DHCP client on the other. The DHCP client sends a DHCPDISCOVER message to the DHCP Server. The DHCP server sends a DHCPOFFER message to the DHCP client. The DHCP client sends a DHCPREQUEST message in repoonse to the DHCPOFFER from the DHCP server. THE DHCP server sends a DHCPACK message back to the DHCP client. The process is called DORA.

DHCP ClientDHCP ServerDHCPDISCOVERDHCPOFFERDHCPREQUESTDHCPACK

Az ügyfél több DHCPOFFER üzenetet is kaphat, ha egynél több DHCP-kiszolgáló van a helyi hálózaton. Ezért választania kell közülük, majd egy DHCP-igénylés (DHCPREQUEST) üzenet küldésével válaszolni az elfogadott bérleti ajánlatra az azt kibocsátó szervernek. A kliens dönthet úgy is, hogy egy olyan címet kér, amelyet a szerver egyszer korábban már kiosztott neki.

Abban az esetben, ha a kliens által megigényelt vagy a szerver által kiajánlott IPv4-cím továbbra is rendelkezésre áll, a szerver egy DHCP-nyugta (DHCPACK) üzenettel válaszol, amely visszaigazolja a kliensnek a bérlet véglegesítését. Ha az ajánlat már nem érvényes, akkor a kiválasztott szerver egy negatív DHCP-nyugta (DHCPNAK) üzenettel válaszol. Amennyiben egy DHCPNAK-üzenet érkezik vissza, akkor a kérelmezési folyamatot újra kell kezdeni egy DHCPDISCOVER üzenet kiküldésével. Miután a kliens megszerezte a címbérletet, a bérleti idő lejártakor azt egy újabb DHCPREQUEST üzenettel meg kell újítania.

Az IP-címek egyediségét a DHCP-szerver biztosítja (ugyanazt az IP-címet nem lehet párhozamosan két hálózati eszközhöz hozzárendelni). A legtöbb internetszolgáltató DHCP használatával rendel címeket az ügyfeleihez.

A DHCPv6 olyan üzenetkészletet tartalmaz, amely hasonló a DHCPv4-hez. A DHCPv6-üzenetek: SOLICIT, ADVERTISE, INFORMATION REQUEST és REPLY.

15.4.8

## Laborgyakorlat - DNS névfeloldás vizsgálata

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Egy URL IP-címmé alakításának megfigyelése.
* Bölüm 2: Egy webhely DNS névfeloldásának megfigyelése az **nslookup** paranccsal
* Bölüm 3: Egy levelezőkiszolgáló DNS névfeloldásának megfigyelése az **nslookup** paranccsal

15.4.9

## Tudáspróba - IP-címzési szolgáltatások

Az űrlap teteje

Check your understanding of DNS services by choosing the correct answer to the following questions.

1. Which of the following DNS record types is used to resolve IPv6 addresses?

Az űrlap alja

True or false? A DNS server that receives a request for a name resolution that is not within its DNS zone will send a failure message to the requesting client.

Which of the following is displayed by the nslookup utility?

Which of the following DNS resource record types resolves authoritative name servers?

[15.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Web és e-mail protokollok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Fájlmegosztási szolgáltatások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                   
*   

1. alkalmazási réteg
2. Fájlmegosztási szolgáltatások

# Fájlmegosztási szolgáltatások

15.5.1

## Fájlátviteli protokoll (File Transfer Protocol, FTP)

Az előző témakörökben megtudtuk, hogy a kliens-szerver modellben az ügyfél adatokat tölthet fel- és le a kiszolgálóról, ha mindkét eszköz fájlátviteli protokollt (File Transfer Protocol, FTP) használ. A HTTP-hez, az e-mailhez és a címzési protokollokhoz hasonlóan az FTP is általánosan használt alkalmazási rétegbeli protokoll. Ez a témakör az FTP-t tárgyalja részletesebben.

Az FTP-t egy kliens és egy szerver közötti adatátvitelre fejlesztették ki. Az FTP-kliens egy számítógépen futó alkalmazás, amelynek segítségével egy FTP-szolgáltatást futtató szerverre fájlokat tölthetünk fel vagy le.

The figure depicts a FTP transasction. A client is contacting a server thru a network. The first message from the client is a control connection: the client opens first connection to the server for control traffic. The second message from the client is a data connection: the client opens a second connection for draffic data. The client the requests data from the server using the Get Data command.

ServerClientNetwork**1. Control Connection:**  
Client opens first connection to the server for control traffic.**2. Data Connection:**  
Client opens second connection for data traffic.Get Data**3. Data Transfer:**  
Server transfers data to the client.

Based on commands sent across the control connection, data can be downloaded from the server or uploaded from the client.

Az ügyfél először létrehozza kapcsolatot a kiszolgálóval a 21-es TCP port használatával a forgalom vezérléséhez. Ez a forgalom az ügyfél parancsaiból és a kiszolgáló válaszaiból áll.

Ezután szintén a kliens kezdeményezi a tényleges adatátvitelre szolgáló második kapcsolatot is a szerverrel. Ez a kapcsolat minden egyes adatátvitel alkalmával létrejön.

A tranzakció mindkét irányban folyhat. A kliens tölthet le adatokat a szerverről és tölthet is oda fel adatokat.

15.5.2

## Server Message Block (SMB)

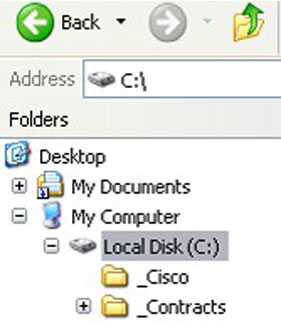
Az SMB (Server Message Block) egy kliens-szerver fájlmegosztó protokoll, amely olyan osztott hálózati erőforrások szerkezetét írja le, mint például könyvtárak, fájlok, nyomtatók és soros portok. Ez egy kérés-válasz protokoll. Minden SMB-üzenetnek közös a formátuma. Ez a formátum egy állandó hosszúságú fejlécet és egy azt követő változó méretű paraméter- és adatkomponenst használ.

Az SMB-üzeneteknek három funkciójuk van:

* Párbeszédek indítása, hitelesítése és lezárása.
* Fájl- és nyomtatóelérés vezérlése.
* Egy alkalmazás és egy másik eszköz üzenetváltásainak biztosítása.

Az SMB-alapú fájlmegosztás és nyomtatás a Microsoft legfőbb hálózati szolgáltatásaivá vált. A Windows 2000 szoftversorozat megjelenésével a Microsoft megváltoztatta az SMB által használt mögöttes struktúrát. A Microsoft termékek korábbi verzióiban az SMB-szolgáltatások még nem TCP/IP-re épülő protokollt használtak a névfeloldásra. A Windows 2000 verziótól kezdve minden Microsoft termék már DNS-neveket használ, ami közvetlenül támogatja az SMB-erőforrások TCP/IP protokoll alapú megosztását (lásd ábra).

The first figure shows a Microsoft Windows shared resource of My Documents with a client requests from a Server My Documents. The client sends a SMB request and receives an SMB response of the shared resource My Documents. Shared Resources include File systems, Pronters shown as a icon, Mail slots, and APIs.



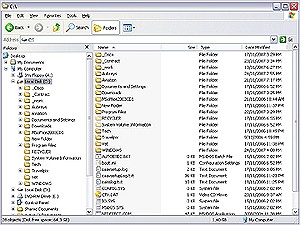
ClientSMB RequestsSMB ResponsesServerPrinterShared Resources

* File systems
* Printers
* Mail slots
* APIs

SMB is a client/server, request-response protocol. Servers can make their own resources available to clients on the network.

A következő ábra két Windows PC közötti SMB-alapú fájlcsere folyamatot szemlélteti.

The second figure depicts a copy file taking place between two Windows computers form one filesystem to the other thru the network.



NetworkCopy File

A file may be copied from PC to PC with Windows Explorer using the SMB protocol.

Az FTP-vel ellentétben, a fájlmegosztásra a kliensek tartós kapcsolatokat építenek ki a szerverekkel. A kapcsolat létrejötte után a felhasználó a szerveren lévő erőforrásokat helyi erőforrásként tudja elérni.

A Linux és Unix operációs rendszerek egy SAMBA nevű SMB-verzió alkalmazásával biztosítanak lehetőséget a Microsoft hálózatokkal történő erőforrás-megosztásához. Az Apple Macintosh operációs rendszerek ugyancsak támogatják az SMB-protokoll alapú erőforrás-megosztást.

15.5.3

## Tudáspróba - Fájlmegosztási szolgáltatások

Az űrlap teteje

Check your understanding of file sharing services by choosing the BEST answer to the following questions.

1. How many connections are required by FTP between client and server?

Az űrlap alja

True or false? FTP data transfers take place from client to server (push) and from server to client (pull).

Which of these ports are used by FTP? (Choose two.)

True or false? Resource sharing over SMB is only supported on Microsoft operating systems.

[15.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[IP-címzési szolgáltatások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[15.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                      

1. alkalmazási réteg
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

15.6.1

## Miről tanultunk ebben a fejezetben?

**Alkalmazási, megjelenítési és viszonyréteg.**

Az OSI- és a TCP/IP-modellekben az alkalmazási réteg a végfelhasználóhoz legközelebb eső réteg. Az alkalmazási rétegbeli protokollokat a forrás- és célállomásokon futó programok közötti adatcserére használjuk. A megjelenítési rétegnek három fontos funkciója van: a forráseszközön lévő adatok formázása egy olyan kompatibilis formába, amelyet a céleszköz fogadhat, az adatok tömörítése olyan módon, hogy a céleszköz számára kitömöríthető legyen, valamint az adatok titkosítása a továbbítás és visszafejtése a vétel során. A viszonyréteg feladata a forrás- és célalkalmazások közötti párbeszédek (munkamenetek) létrehozása és fenntartása. A viszonyréteg kezeli a párbeszédek kialakításához, fenntartásához, valamint a megszakadó vagy hosszabb ideje tétlen viszonyok újraindításához szükséges információcserét. A TCP/IP alkalmazási protokolljai határozzák meg az internetes kommunikációs szolgáltatások formátumát és vezérlőinformációit. Ezeket a protokollokat a kommunikációs folyamat során a forrás- és a célállomás egyaránt használja. A forrás- és célállomásokon működő protokolloknak kompatibiliseknek kell lenniük.

**Egyenrangú (peer-to-peer) hálózatok**

A kliens-szerver modellben az információt kérő eszközt kliensnek, a kérésre válaszoló eszközt pedig szervernek vagy kiszolgálónak nevezzük. A párbeszédet a kliens kezdeményezi azzal, hogy adatokat kér a szervertől, amely aztán a kliensnek egy vagy több adatfolyam elküldésével válaszol. Egy P2P-hálózatban két vagy több számítógép csatlakozik egymáshoz úgy, hogy dedikált szerver nélkül oszthatják meg az erőforrásaikat. Minden eszköz működhet szerverként és kliensként is. Egy számítógép az egyik adatátviteli folyamatban betöltheti a szerver szerepkörét, míg egy másikban ezzel egyidejűleg kliens is lehet. A P2P-alkalmazások megkövetelik, hogy minden végberendezés biztosítson egy felhasználói felületet és egy háttérszolgáltatást is futtasson. Bizonyos P2P-alkalmazások úgynevezett hibrid rendszert használnak, ahol az erőforrások megosztása ugyan decentralizált, de az erőforrások helyeire mutató indexeket már egy központi címtárban tárolják. Számos P2P-alkalmazás lehetővé teszi a felhasználók számára, hogy a fájlok egyes részeit osszák meg egymással. Az ügyfelek egy kisméretű, úgynevezett torrent fájlt használnak arra, hogy megkeressék a keresett állomány darabjait megosztó felhasználókat, így közvetlenül kapcsolódhatnak hozzájuk. Ez a fájl tartalmazza az úgynevezett tracker számítógépek információit, amelyek nyomon követik, hogy mely felhasználóknál találhatók bizonyos fájlok konkrét darabjai.

**Web és e-mail protokollok**

Amikor egy webcímet vagy URL-t begépelünk egy webböngészőbe, a böngésző a HTTP-protokollt használva építi ki a kapcsolatot a szerveren futó web-szolgáltatással. A webszolgáltatás egy HTTP-protokollt használó kiszolgálón fut. A HTTP egy kérés/válasz protokoll. Amikor egy kliens, általában egy webböngésző, kérést küld a webszervernek, a kommunikációhoz HTTP-üzenettípusokat használ. A három leggyakoribb üzenettípus a GET, a POST és a PUT. A HTTPS ugyanazt a kliens-szerver folyamatot használja mint a HTTP, csak a hálózati átvitelt megelőzően az adatfolyamot SSL-el titkosítja. Az elektronikus levelezés három különböző protokollt támogat: SMTP, POP3 és IMAP. A levelet elküldő alkalmazási rétegbeli folyamat az SMTP-t használja. Az ügyfél POP vagy IMAP használatával kéri le az e-maileket. Az SMTP üzenetformátuma egy üzenetfejlécből és egy üzenettörzsből áll. Míg az üzenet törzse tetszőleges mennyiségű szöveget tartalmazhat, addig a fejlécnek megfelelő formátumban tartalmaznia kell a címzett és a feladó e-mail címét. A POP-ot az alkalmazások használják a levelek lekérésére a levelező kiszolgálóról. POP használatakor a levelek a szerverről letöltődnek a kliensre, majd törlődnek a szerverről. A POP-pal ellentétben, amikor a felhasználó egy IMAP-szerverhez csatlakozik, a kliensalkalmazáshoz csak az üzenetek másolata töltődik le. Az eredeti üzenetek továbbra is a szerveren maradnak, míg azokat külön le nem töröljük.

**IP-címzési szolgáltatások**

A DNS-protokoll erőforrásneveket társít a kért numerikus hálózati címhez. A DNS protokoll kommunikációi egy üzenetformátumot használnak a klienslekérdezések és a szerverválaszok minden fajtájához, a hibaüzenetekhez, valamint az erőforrásrekordok szerverek közötti továbbításához. A DNS a tartománynevekből építi fel a hierarchiát. Minden DNS-kiszolgáló egy meghatározott adatbázis fájlt tárol és a DNS-struktúra csak kis részének név – IP-cím hozzárendeléséért felelős. Az operációs rendszerek nslookup nevű segédprogramja lehetővé teszi egy adott állomásnév feloldásához a névszerverek manuális lekérdezését. A DHCP-szolgáltatás automatizálja az IPv4-címek, alhálózati maszkok, átjárók és egyéb IPv4-hálózati paraméterek kiosztását. A DHCPv6 hasonló szolgáltatásokat nyújt az IPv6-ügyfelek számára, kivéve, hogy nem adja meg az alapértelmezett átjáró címét. Amikor egy DHCP-re konfigurált eszköz elindul vagy csatlakozik a hálózatra, a kliens egy szórásos DHCPDISCOVER üzenetet küld szét az elérhető DHCP-szerverek megtalálásához. A DHCP-szerver egy DHCPOFFER üzenettel válaszol, amely a kliensnek felajánl egy címbérletet. A DHCPv6 olyan üzenetkészletet tartalmaz, amely hasonló a DHCPv4-hez. A DHCPv6-üzenetek: SOLICIT, ADVERTISE, INFORMATION REQUEST és REPLY.

**Fájlmegosztási szolgáltatások**

Az FTP-kliens egy számítógépen futó alkalmazás, amelynek segítségével egy FTP-szolgáltatást futtató szerverre fájlokat tölthetünk fel vagy le. Az ügyfél először létrehozza kapcsolatot a kiszolgálóval a 21-es TCP port használatával a forgalom vezérléséhez. Ezután szintén a kliens kezdeményezi a tényleges adatátvitelre szolgáló második kapcsolatot is a szerverrel. A kliens tölthet le adatokat a szerverről és tölthet is oda fel adatokat. Az SMB-üzeneteknek három funkciójuk van: munkamenetek indítása, hitelesítése és megszüntetése, fájl- és nyomtatóhozzáférés vezérlése, valamint lehetőség biztosítása az alkalmazások számára, hogy üzeneteket küldjenek vagy fogadjanak egy másik eszközről. Az FTP-vel ellentétben, a fájlmegosztásra a kliensek tartós kapcsolatokat építenek ki a szerverekkel. A kapcsolat létrejötte után a felhasználó a szerveren lévő erőforrásokat helyi erőforrásként tudja elérni.

15.6.2

## Ellenőrző kvíz - Alkalmazási réteg

Az űrlap teteje

1. Otthoni hálózaton melyik eszköz a legvalószínűbb, hogy dinamikus IP-címzést biztosít a klienseknek?

Az űrlap alja

A ht&#8203;tp://ww&#8203;w.cisco.com/index.html URL-cím melyik része képviseli a legfelső szintű DNS-tartományt?

Mi a két jellemzője a TCP/IP modell alkalmazási rétegének? (Két jó válasz van.)

Milyen üzenettípust használ a HTTP-kliens, amikor adatot kér egy webszervertől?

Melyik protokoll használható az üzenetek továbbítására egy e-mail szerverről egy e-mail kliensre?

Melyik alkalmazási rétegbeli protokollt használják fájlmegosztási és nyomtatási szolgáltatások nyújtására a Microsoft alkalmazásai számára?

Melyik három protokollt vagy szabványt használják a TCP/IP modell alkalmazási rétegében? (Három jó válasz van.)

Miért előnyös a DHCP használata nagy hálózatokon??

A szerző egy dokumentum egyik fejezetét tölti fel egy személyi számítógépről a könyvkiadó fájlszerverére. Milyen szerepet játszik a személyi számítógép ebben a hálózati modellben?

Melyik állítás igaz az FTP-protokollra?

Egy vezeték nélküli állomásnak IP-címet kell kérnie. Milyen protokollt használnak a kérés feldolgozásához?

A TCP/IP modell melyik rétege van legközelebb a végfelhasználóhoz?

Kis- és középvállalatok esetében melyik protokoll biztosítja az emailek egyszerű, központi tárolását és biztonsági mentését?

Melyik protokoll használ titkosítást?

Mely két feladatot hajthat végre egy helyi DNS-szerver? (Két jó válasz van.)

[15.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Fájlmegosztási szolgáltatások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                
* 

1. Hálózatbiztonsági alapok
2. Bevezetés

# Bevezetés

16.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Hálózatbiztonsági alapok fejezetben!

Lehet, hogy már létrehoztunk egy hálózatot, vagy éppen most készülünk erre. Van valami, amire mindenképpen gondolnunk kell. Hálózat létrehozása biztonsági elemek nélkül olyan, mintha kinyitnánk az összes ajtót és ablakot az otthonunkban, majd nyaralni indulnánk. Bárki beugorhat, beléphet, lophat vagy összetörhet tárgyakat, vagy csak rendetlenséget csinálhat. Ahogy a hírekben is láthatjuk, bármelyik hálózatba be lehet törni! Hálózati rendszergazdaként feladatunk része, hogy megnehezítsük a rosszindulatú személyek hozzáférését a hálózathoz. Ez a modul áttekintést nyújt a hálózati támadások típusairól, és a fenyegetés sikerének csökkentése érdekében elvégzendő feladatokról. Packet Tracer feladatok segítségével elsajátíthatunk néhány alapvető hálózatbiztonsági technikát. Ha nem kellően biztonságos a hálózatunk, akkor gyorsan olvassuk el ezt a fejezetet!

16.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Hálózatbiztonsági alapok

**Fejezet célja:** Router és switch konfigurálás a biztonság növelése érdekében.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Biztonsági fenyegetések és sebezhetőségek** | Elmagyarázza, miért szükséges alapvető biztonsági intézkedések végrehajtása a hálózati eszközökön. |
| **Hálózati támadások** | A biztonsági rések azonosítása. |
| **Hálózati támadás elkerülése** | Az alapvető biztonsági technikák megismerése. |
| **Eszközbiztonság** | Hálózati eszközök konfigurálása a biztonsági fenyegetések enyhítése érdekében. |

[15.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Biztonsági fenyegetések és sebezhetőségek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                  
* 

1. Hálózatbiztonsági alapok
2. Biztonsági fenyegetések és sebezhetőségek

# Biztonsági fenyegetések és sebezhetőségek

16.1.1

## Fenyegetések típusai

A vezetékes és a vezeték nélküli számítógép hálózatok mindennapi életünk fontos kellékei. Magánszemélyek és szervezetek egyaránt nagyban függenek számítógépeiktől és hálózatuktól. Egy jogosulatan személy behatolása költséges hálózati üzemszünetet és a munka elvesztését eredményezheti. Egy hálózat elleni támadás végzetes lehet, a fontos információk és eszközök megrongálása vagy ellopása idő- és pénzveszteséget okoz.

A behatolók hozzáférést szerezhetnek a hálózathoz a szoftverek sebezhető pontjain keresztül, a hardverek elleni támadással vagy egy felhasználó nevének és jelszavának megszerzésével. Azokat a behatolókat, akik a szoftver módosításával vagy a szoftver sebezhető pontjait kihasználva jutnak hozzáféréshez hekkereknek (hacker) nevezzük.

A hekker hozzáférése a hálózathoz négyféle fenyegetést jelenthet:

Az egyes fenyegetésekkel kapcsolatos információkért kattintsunk a gombokra!

Az **információlopás** betörés egy számítógépbe bizalmas információk megszerzése céljából. Az információ felhasználható vagy értékesíthető különböző célokra. Például: egy szervezet tulajdonát képező kutatási és fejlesztési információk eltulajdonítása.

The figure shows an open folder

16.1.2

## Sebezhetőségek típusai

A sebezhetőség a hálózat és az eszköz gyengeségének fokmérője. Valamilyen szintű sérülékenységet minden router, switch, munkaállomás, szerver és biztonsági eszköz tartalmaz. A veszélyeztettett eszközök általában a végberendezések, például a szerverek vagy az asztali számítógépek.

Három elsődleges biztonsági rés vagy hiányosság van: technológiai, konfigurációs és biztonsági házirend. Mindhárom sebezhetőség különféle támadásokra ad lehetőséget, ilyenek például a rosszindulatú programok vagy a hálózati támadások.

Kattintsunk az egyes gombokra a táblázatok megtekintéséhez, amelyekben példák és a típusok leírásai találhatók!

### Technológiai sebezhetőségek

| Table caption | |
| --- | --- |
| **Sebezhetőség** | **Leírás** |
| TCP/IP protokoll gyengeség | * A HTTP (Hypertext Transfer Protocol), az FTP (File Transfer Protocol), és az ICMP (Internet Control Message Protocol) eredendően nem biztonságos. * Az SNMP (Simple Network Management Protocol) és az SMTP (Simple Mail Transfer Protokoll) olyan TCP-struktúrára támaszkodik, amely természeténél fogva nem biztonságos. |
| Operációs rendszer gyengeség | * Minden operációs rendszernek vannak biztonsági problémái, amelyekkel foglalkozni kell. * UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 * Dokumentálva vannak a CERT (Computer Emergency Response Team) archívumában: http://www.cert.org |
| Hálózati eszköz gyengeség | A különböző típusú hálózati eszközök, például routerek, tűzfalak és switch-ek biztonsági hiányosságokkal rendelkeznek, amelyeket fel kell ismerni és ki kell küszöbölni. Ezek közé tartozik a jelszóvédelem, a hitelesítés hiánya, a routing protokollok és a tűzfalon található lyukak. |

16.1.3

## Fizikai biztonság

Fontos sérülékenységi terület a hálózati eszközök fizikai biztonsága. Egy támadó megakadályozhatja a hálózati erőforrások használatát, ha azokat fizikailag képes veszélyeztetni.

A fizikai fenyegetések négy formája:

* **Hardver fenyegetések -** A szerverek, a munkaállomások, a routerek, a switchek vagy 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.

E problémák megoldása érdekében szabályzatot kell létrehozni és végrehajtani a fizikai biztonságra is. Az ábra egy példát mutat a fizikai biztonsági tervre.

The figure is a square that depicts a computer room. Inside the computer room on the top left corner, is a small rectangle labeled, AC. On the top right corner, four squares are connected and labeled, UPS BAY. In the center of the computer room there are three rows of squares, labeled servers, WAN, and LAN. The lower part of the computer room is divided to create a separate room. There is a dotted section of the divider labeled, locked door. Inside the separate room is a Help desk, a card reader as well as another door on the exterior.

### Fizikai biztonság terv a berendezések károsodásának korlátozása érdekében

Locked DoorDoorCard  
ReaderHelp DeskACWANSVRSUPS BAYLAN

* Biztonságos szerver helyiség kialakítása.
* Fizikai biztonság megvalósítása a berendezések károsodásának megelőzésére.

**1. lépés** Zárjuk el a berendezéseket, és akadályozzuk meg a jogosulatlan bejutást minden lehetséges irányból (ajtók, mennyezet, emelt padló, ablakok, csatornák és szellőzők).

**2. lépés** A belépést elektronikus úton vezéreljük és naplózzuk.

**3. lépés** Használjunk biztonsági kamerákat.

16.1.4

## Tudáspróba — Biztonsági fenyegetések és sebezhetőségek

Az űrlap teteje

Check your understanding of security threats and vulnerabilities by choosing the BEST answer to the following questions.

1. What kind of threat is described when a threat actor sends you a virus that can reformat your hard drive?

Az űrlap alja

What kind of threat is described when a threat actor makes illegal online purchases using stolen credit information?

What kind of threat is described when a threat actor prevents legal users from accessing data services?

What kind of threat is described when a threat actor steals scientific research data?

What kind of threat is described when a threat actor overloads a network to deny other users network access?

What kind of threat is described when a threat actor alters data records?

What kind of threat is described when a threat actor is stealing a company’s user database?

What kind of threat is described when a threat actor impersonates another person to obtain credit information about that person?

[16.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati támadások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                      
* 

1. Hálózatbiztonsági alapok
2. Hálózati támadások

# Hálózati támadások

16.2.1

## Kártevőtípusok

Az előző témakörben megismertük a hálózati fenyegetések típusait és a fenyegetéseket lehetővé tevő biztonsági réseket. Ez a témakör részletesebben ismerteti, hogyan férnek hozzá a hálózathoz a támadók, vagy hogyan korlátozhatják a jogosult felhasználók hozzáférését.

A "malware" a rosszindulatú szoftverek rövid neve (malicious software). Ez a kód vagy szoftver kifejezetten az adatok, számítógépek és hálózatok károsítására, megzavarására, ellopására, vagy törvénytelen műveletek végrehajtására készült. A rosszindulatú programok típusai a vírusok, férgek és trójaiak.

**Vírusok**

A számítógépes vírus egy olyan típusú malware, amely a terjedéshez beilleszti saját másolatát egy másik programba, ezáltal annak szerves része lesz. Egyik számítógépről a másikra terjed, fertőzéseket hagyva hátra. A vírusok súlyossága az enyhén bosszantó hatásúaktól kezdve az adatokat vagy szoftvereket károsító és szolgáltatás-megtagadást (DoS) okozókig terjed. Szinte az összes vírus egy futtatható fájlhoz kapcsolódik, ami azt jelenti, hogy a vírus benne van a rendszerben, de addig nem lesz aktív és nem képes terjedni, amíg a felhasználó le nem futtatja vagy meg nem nyitja a fertőzött állományt. A gazda kód végrehajtásakor a víruskód is végrehajtásra kerül. Normális esetben a gazdaprogram a vírusfertőzés után is működőképes marad. Egyes vírusok azonban felülírják a másik programot saját másolatukkal, ami teljesen elpusztítja a gazdaprogramot. A vírusok akkor terjednek, amikor a szoftver vagy dokumentum, amelyhez csatolva vannak, a hálózat, egy lemez, egy fájlmegosztás vagy egy email melléklet használatával átkerül az egyik számítógépről a másikra.

**Férgek**

A számítógépes férgek hasonlóak a vírusokhoz, mivel működőképes másolatokat készítenek saját magukról, és ugyanolyan típusú károkat okozhatnak. A fertőzött gazdafájlt igénylő vírusokkal ellentétben a férgek önálló szoftverek, és nem igényelnek gazdaprogramot vagy emberi segítséget a terjedéshez. Egy féregnek nem kell kapcsolódnia egy programhoz, hogy megfertőzze a gazdagépet, és belépjen a számítógépbe a rendszer biztonsági résén keresztül. A férgek a rendszer funkcióit használják ki, hogy segítség nélkül terjedhessenek a hálózaton.

**Trójai programok**

A trójai egy másik típusú rosszindulatú program, nevét a görögök által használt falóról kapta, amelyet Trója bevételére alkalmaztak. Ez egy valódinak látszó káros szoftver. Becsapja a felhasználókat, hogy azok letöltésék és végrehajtsák a saját rendszerükben. Az aktiválódásuk után különféle támadásokat indítanak a gazdagép ellen, kezdve azzal, hogy irritálják a felhasználót (állandóan felugró ablakokkal vagy az asztal megváltoztatásával), egészen a károkozásig (fájlok törlése, adatok lopása, vagy vírusok aktiválása és terjesztése). A trójaiak képesek kiskapukat (back doors) is létrehozni, hogy a rosszindulatú támadók hozzáférhessenek a rendszerhez.

A vírusokkal ellentétben a trójai programok nem más fájlok megfertőzésével reprodukálódnak. Önmagukat másolják. A trójaiak terjedéséhez felhasználói beavatkozás szükséges, például egy email melléklet megnyitása vagy egy fájl internetről történő letöltése és futtatása.

Kattintsunk a Lejátszás gombra a három rosszindulatú programtípus animált magyarázatának megtekintéséhez!

The animation shows a network with two PCs and two routers with the routers are connected to each other sit between the two PCs with each PC connected to one of the routers. The PC on the left has an attacker. As the animation plays a text box opens that reads “The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks. As the animation continues to play the attacker at the PC on the left sends a virus attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A virus is malicious software which executes a specific unwanted, and often harmful, function on a computer”. As the animation continues to play the attacker at the PC on the left sends a worm attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is to automatically replicate itself and spread across the network from system to system”. As the animation continues to play the attacker at the PC on the left sends a Trojan Horse attack on the network that travels over the network routers to the PC on the right. A text box opens that reads “A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within”.

The primary vulnerabilities for end-user workstations are virus, worm, and Trojan Horse attacks.

A virus is malicious software which executes a specific unwanted, and often harmful, function on a computer.

A worm executes arbitrary code and installs copies of itself in the memory of the infected computer. The main purpose of a worm is to automatically replicate itself and spread across the network from system to system.

A Trojan horse is a non-self-replicating type of malware. It often contains malicious code that is designed to look like something else, such as a legitimate application or file. When an infected application or file is downloaded and opened, the Trojan horse can attack the end device from within.

16.2.2

## Felderítéses támadások

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

* **Felderítéses támadások** - Rendszerek, szolgáltatások és sebezhetőségi pontok felkutatása.
* **Hozzáférési támadások** - Adatok, rendszerhozzáférések és felhasználói jogok illetéktelen kezelése.
* **Szolgáltatásmegtagadási támadások** - Hálózatok, rendszerek és szolgáltatások megbénítása vagy elrontása.

Felderítéses támadás esetén egy hekker internetes eszközöket használva, például **nslookup** és **whois** segédprogramok segítségével könnyen megállapíthatja egy adott szervezet IP-címtartományát. Ezután a támadó a tartomány publikus IP-címeinek pingelésével ki tudja választani az aktív állomásokat. A lépés automatizálásához a támadó használhat ping pásztázást, amilyen például a **fping** vagy a **gping**. Ez szisztematikusan pingel minden hálózati címet egy adott tartományban vagy alhálózatban. Úgy, mint egy telefonkönyvben végighívni az összes számot azt figyelve, hogy melyiket veszik fel.

Kattintsunk a felderítéses támadás eszközökre és figyeljük meg az animációkat!

**Internetes lekérdezések**

Kattintsunk a Lejátszás gombra az animáció megtekintéséhez! A támadó alapvető információkat keres egy célpontról. Különböző eszközök használhatók, például: Google keresés, szervezetek weboldalai, a whois stb.

Threat Actor

16.2.3

## 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 tiltott adatokhoz. A hozzáférési támadások négy típusba sorolhatók: jelszó elleni támadások, bizalom kihasználás, portátirányítás és közbeékelődés (man-in-the middle).

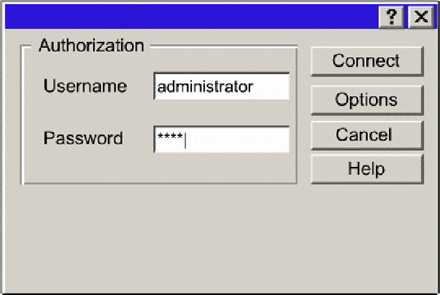
Az egyes támadástípusok magyarázatához kattintsunk a gombokra!

**Jelszó elleni támadások**

A hekkerek többféle módszerrel is végrehajthatják a jelszó elleni támadásokat:

* Brute-force (nyers erő) támadások
* Trójai faló támadások
* Protokollelemző alkalmazások

The first figure shows a login prompt box with the username, administrator and the password, \*\*\*\*.



16.2.4

## Szolgáltatásmegtagadásos támadások

A DoS (Denial of Service, szolgáltatás megtagadás) támadás a legismertebb és a legnehezebben kiküszöbölhető támadásforma. Ugyanakkor pontosan a könnyű megvalósítás és a lehetséges jelentős károkozás miatt követelnek kiemelt figyelmet a biztonsági szakemberek részéről.

A DoS-támadások számos formát ölthetnek, de végeredményben mindegyik a rendszer erőforrásainak felemésztésével akadályozza meg a jogosult felhasználókat egy szolgáltatás használatában. A DoS-támadások megelőzése érdekében fontos, hogy az operációs rendszerek és az alkalmazások a legújabb biztonsági frissítések telepítésével naprakészek legyenek.

Kattintsunk a gombokra a DoS és az elosztott DoS (DDoS) támadások példáinak megtekintéséhez!

**DoS-támadás**

A DoS-támadások nagy kockázatot jelentenek, mivel megakadályozzák a kommunikációt, és jelentős idő- és pénzveszteséget okoznak. Ezek a támadások viszonylag egyszerűek, még egy képzetlen hekker is végrehajthatja őket.

Kattintsunk a Lejátszás gombra az animáció megtekintéséhez!

This animation shows a Web server, [www.XYZcorp.com](http://www.XYZcorp.com), an internet user, two PCs, and a threat actor all connected to an internet cloud. As the animation plays a text box appears above the threat actor stating “I’ll send so many pings that the server can’t respond to anyone else. A series of pings leaves the treat actor’s PC toward the Internet. From the internet the series of pings are sent to the [www.XYZcorp.com](http://www.XYZcorp.com) web server. A text box appearing above the web server states “Help, I can’t accomplish any work!”. As the pings continue from the threat actor to the web server a text box appears above the internet user stating “This website is very slow today!”.

I'll send so many pings that the server can't respond to anyone else.

Help, I can't accomplish any work!

Internet

Web Server www.XYZcorp.com

Threat Actor

This website is very slow today!

16.2.5

## Tudáspróba - Hálózati támadások

Az űrlap teteje

Check your understanding of network attacks by choosing the BEST answer to the following questions.

1. Angela, an IT staff member at ACME Inc., notices that communication with the company’s web server is very slow. After investigating, she determines that the cause of the slow response is a computer on the internet sending a very large number of malformed web requests to ACME’S web server. What type of attack is described in this scenario?

Az űrlap alja

George needed to share a video with a co-worker. Because of the large size of the video file, he decided to run a simple FTP server on his workstation to serve the video file to his co-worker. To make things easier, George created an account with the simple password of “file” and provided it to his co-worker on Friday. Without the proper security measures or a strong password, the IT staff was not surprised to learn on Monday that George’s workstation had been compromised and was trying to upload work related documents to the internet. What type of attack is described in this scenario?

Jeremiah was browsing the internet from his personal computer when a random website offered a free program to clean his system. After the executable was downloaded and running, the operating system crashed. Crucial operating system related files had been corrupted and Jeremiah’s computer required a full disk format and operating system re-installation. What type of attack is described in this scenario?

Arianna found a flash drive lying on the pavement of a mall parking lot. She asked around but could not find the owner. She decided to keep it and plugged it into her laptop, only to find a photo folder. Feeling curious, Arianna opened a few photos before formatting the flash drive for her own use. Afterwards, Arianna noticed that her laptop camera was active. What type of attack is described in this scenario?

A computer is used as a print server for ACME Inc. The IT staff failed to apply security updates to this computer for over 60 days. Now the print server is operating slowly, and sending a high number of malicious packets to its NIC. What type of attack is described in this scenario?

Sharon, an IT intern at ACME Inc., noticed some strange packets while revising the security logs generated by the firewall. A handful of IP addresses on the internet were sending malformed packets to several different IP addresses, at several different random port numbers inside ACME Inc. What type of attack is described in this scenario?

16.2.6

## Laborgyakorlat - Hálózatbiztonsági fenyegetések

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: A SANS weboldal megismerése.
* Bölüm 2: A legújabb hálózatbiztonsági fenyegetések azonosítása.
* Bölüm 3: Egy jellegzetes hálózatbiztonsági fenyegetés részletei.

[16.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Biztonsági fenyegetések és sebezhetőségek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati támadások elkerülése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                            
* 

1. Hálózatbiztonsági alapok
2. Hálózati támadások elkerülése

# Hálózati támadások elkerülése

16.3.1

## Mélységi védelem

Most, hogy többet tudunk a támadók hálózatokba való bejutásának módjáról, meg kell tanulnunk, hogyan megakadályozzuk meg a jogosulatlan hozzáférést. Ez a témakör számos olyan műveletet ismertet, amelyeket a hálózat biztonságosabbá tétele érdekében végrehajthatunk.

A hálózati támadások elkerülése érdekében először az eszközöket kell megvédeni: a routereket, a switch-eket, a kiszolgálókat és a munkaállomásokat. Sok szervezet alkalmaz mélységi védelmet (defense-in-depth), más néven a védelem rétegzésének stratégiáját. Ez a hálózati eszközök és szolgáltatások kötelékben való működését követeli meg.

Figyeljük meg az ábrán lévő hálózatot! Ebben számos biztonsági eszköz és szolgáltatás található, hogy megvédje a felhasználóikat és a berendezéseket a TCP/IP-fenyegetésekkel szemben.

Az összes hálózati eszköz, a router és a switch-ek is, meg vannak erősítve. Ezt az ikonjaikon lévő lakat is jelzi. Az eszközök védelme úgy lett beállítva, hogy a támadók ne férhessenek hozzájuk illetéktelenül.

The figure depicts a campus area network. A cloud representing the Internet is connected to a router, labeled VPN. The VPN router is connected to an ASA firewall. The firewall has two additional connections; one to an IPS and another to a switch. The switch is connected to a DHCP server, email server, web server, and ESA/WSA. The IPS is connected to a multilayer switch. The multilayer switch has a connection to an AAA server as well as to two layer 2 switches and a to another multilayer switch. The second multilayer switch also has connections to the same layer 2 switches, creating redundancy. Below the layer 2 switches are three laptops and three pcs which are labeled as hosts.

**Campus Area Network**InternetAAA ServerASA  
FirewallLayer 3 SwitchesVPNIPSESA/WSALayer 2 SwitchesDHCP ServerEmail ServerWeb ServerHosts

Számos biztonsági eszköz és szolgáltatás működik a felhasználók és a berendezések védelme érdekében.

* **VPN** - A router feladata, hogy biztonságos VPN-szolgáltatásokat nyújtson a vállalati telephelyek között, valamint titkosított alagutak segítségével biztosítsa a távoli felhasználók hozzáférését.
* **ASA Firewall** - Ez a dedikált eszköz állapottartó tűzfalszolgáltatásokat biztosít. Garantálja a belülről induló adatforgalom kijutását és visszatérését, viszont megakadályozza a kívülről érkező kapcsolati kezdeményezéseket a belső számítógépek irányába.
* **IPS** - A behatolásmegelőző rendszer (Intrusion Prevention System, IPS) kártevőket, hálózati támadások mintáit és egyebeket keresve monitorozza a bejövő és kimenő adatforgalmat. Ha támadást érzékel, azonnal megállítja.
* **ESA/WSA** \- Az e-mail biztonsági célberendezés (Email Security Appliance, ESA) kiszűri a kéretlen és gyanús leveleket. A webes biztonsági célberendezés (Web Security Appliance, WSA) kiszűri a kártevőket terjesztő, ismert vagy gyanús weboldalakat.
* **AAA Server** - Ez a szerver egy biztonságos adatbázisban tárolja a hálózati eszközök elérésére és kezelésére jogosult személyeket. A hálózati eszközök ezen adatbázis segítségével hitelesítik a rendszergazda felhasználókat.

16.3.2

## Biztonsági mentések

A konfigurációk és az adatok biztonsági mentése az adatvesztés elleni védelem egyik leghatékonyabb módja. Az adatmentés a számítógépen lévő információk egy példányát olyan cserélhető adathordozón tárolja, amelyet biztonságos helyen lehet tartani. Az infrastruktúra eszközök konfigurációs beállításairól és IOS-képfájljairól is mentést kell készíteni FTP- vagy hasonló fájlkiszolgálóra. Ha a számítógép vagy a router hardvere meghibásodik, az adatok és a konfiguráció visszaállítható a biztonsági másolatból.

Az adatok biztonsági mentését a házirendben meghatározott rendszeres időközönként el kell végezni. Az adatmentéseket általában külső helyszínen (offsite) tárolják, hogy megvédjék a biztonsági másolatot, ha bármi történne a fő létesítménnyel. A Windows operációs rendszert futtató számítógépek rendelkeznek biztonsági mentés és visszaállítás segédprogrammal. Ez fontos, mert a felhasználók másolatot készíthetnek adataikról egy másik meghajtóra vagy egy felhőalapú tárhelyre.

A táblázat a mentési szempontokat és azok leírásait mutatja be.

| Table caption | |
| --- | --- |
| **Szempont** | **Leírás** |
| Gyakoriság | * Az adatok biztonsági mentését a biztonsági házirendben meghatározott rendszeres időközönként el kell végezni. * A teljes biztonsági mentés időigényes lehet, ezért készítsünk havi vagy heti rendszerességű részleges mentéseket a megváltozott fájlokról. |
| Tárolás | * Mindig ellenőrizzük az adatok sértetlenségét és a fájlok visszaállíthatóságát a mentések biztonsága érdekében! |
| Biztonság | * A mentéseket el kell szállítani megfelelő tárolási helyre napi, heti vagy havi forgásban a biztonsági házirend előírásai szerint. |
| Érvényesség | * A biztonsági mentéseket erős jelszóval kell védeni. Az adatok visszaállítása csak a jelszó megadásával lehetséges. |

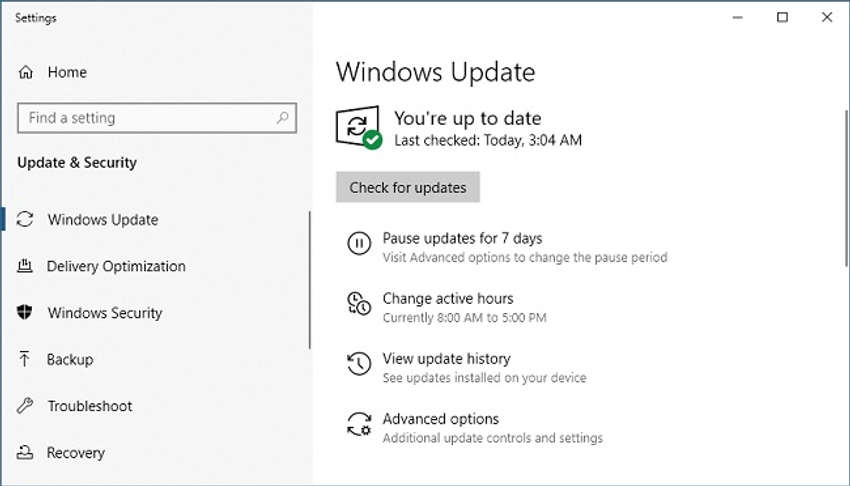
16.3.3

## Frissítés és hibajavítás

A legutóbbi fejlesztések eredményeinek folyamatos alkalmazása eredményesebb védekezést tesz lehetővé a támadások ellen. Amint egy új kártevő megjelenik, a vállalkozásoknak frissíteniük kell víruskereső szoftvereik adatbázisát.

A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch). A nagy számosságú rendszerek felügyelete maga után vonja egy általános szoftvercsomag (operációs rendszer és kliens alkalmazások) létrehozásának szükségességét, amely telepítéskor vagy frissítéskor használható. Amennyiben a biztonsági követelmények változnak, a már üzemelő rendszereken is szükség van a biztonsági frissítések telepítésére.

A kritikus biztonsági javítások kezelésének egyik megoldása annak, hogy az összes végberendezés automatikusan letölti a frissítéseket, amint az a Windows 10 példáján látható. A biztonsági javítások automatikusan letöltődnek és telepítésre kerülnek felhasználói beavatkozás nélkül.



16.3.4

## Hitelesítés, jogosultság kezelés és naplózás

Minden hálózati eszközt úgy kell konfigurálni, hogy csak az engedélyezett személyek férhessenek hozzá. A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, amelyek a hálózati eszközök hozzáférésszabályozásának 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 fogalma egy bankkártya használathoz hasonlítható. A kártya meghatározza, hogy ki használhatja, mennyit költhetnek el róla, és lekönyveli a felhasznált összeg sorsát (lásd ábra).

The figure shows two credit cards one on top of the other next to a credit card statement. There is a rectangle around the numbers on the top credit card with the text, Authentication Who are you? A second rectangle is around the credit limit on the credit card statement with text, Authorization How much can you spend? A third rectangle is around the transaction portion of the credit card summary with the text Accounting What did you spend on it?



**Authentication**  
  
Who are you?**Authorization**  
  
How much can you spend?**Accounting**  
  
What did you spend it on?

16.3.5

## Tűzfalak

A tűzfal az egyik leghatékonyabb biztonsági eszköz, amely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal úgy védi a számítógépeket és hálózatokat, hogy megakadályozza a belső hálózatba irányuló nem kívánt adatforgalmat.

A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is. A felső ábra azt mutatja be, hogy a tűzfal engedélyezi a belső hálózatból induló forgalom kilépését, majd visszatérését. Az alsó topológia pedig azt szemlélteti, hogy miként blokkolja a külső hálózatból (pl.: az internetről) a belső hálózat felé indított adatforgalmat.

The figure shows a rectangle, labeled Inside. Inside the rectangle there is a pc. Outside of and to the right of the rectangle, there is a firewall. To the right of the firewall, there is a cloud labeled, Internet. There are two arrows, one signifying traffic leaving the pc going through the firewall and out to the Internet. The second arrow signifies the firewall permitting traffic from the Internet to the pc. The figure shows another rectangle, labeled Inside. Inside the rectangle there is a pc. Outside of and to the right of the rectangle, there is a firewall. To the right of the firewall, there is a cloud labeled, Internet. There is an arrow pointing from the Internet to the firewall with an X signifying that traffic is being denied from the Internet to the internal network.

### Tűzfal műveletek

Firewall permits traffic from users in the inside network to exit and return.InsideInternetFirewallFirewall denies outside traffic access to the inside network.InsideInternetFirewall

A tűzfal bizonyos szolgáltatásokhoz ellenőrzött hozzáférést biztosíthat külső felhasználók számára. A külső felhasználók számára elérhető szerverek egy speciális hálózatban kapnak helyet, amelyet demilitarizált zónának (DMZ, demilitarized zone) neveznek (lásd ábra). A hálózati rendszergazdák speciális irányelveket alkalmazhatnak a DMZ-hálózathoz kapcsolódó állomásokra.

The figure shows a rectangle, labeled Inside. Inside the rectangle there is a pc. Outside of and to the right of the rectangle, there is a firewall. To the right of the firewall, there is a cloud labeled Internet. Above the firewall, theres a DMZ server inside of a rectangle. There are twos arrows, one going from the pc through the firewall to the DMZ server and another going from the Internet through the firewall to the DMZ sever.

### Tűzfal topológia DMZ-vel

DMZServerInsideInternet

16.3.6

## Tűzfalak típusai

A tűzfalaknak számos formája létezik. Ezek különféle technikákat használnak annak meghatározására, hogy mi számít engedélyezett és mi tiltott hálózati hozzáférésnek. Az alkalmazott módszerek a következők:

* **Csomagszűrés** - IP- vagy MAC-cím alapján akadályozza meg vagy engedélyezi a hozzáférést.
* **Alkalmazás szűrés** - Tiltja vagy engedélyezi a hozzáférést bizonyos alkalmazások számára portszámuk alapján.
* **URL-szűrés** - Tiltja vagy engedélyezi weboldalak elérését adott URL vagy kulcsszó alapján.
* **Állapotalapú csomagvizsgálat (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).

16.3.7

## Végpontok biztonsága

A végpont vagy állomás olyan egyedi számítógépes rendszer vagy eszköz, amely hálózati ügyfélként működik. Gyakori végpont típusok a laptopok, az asztali számítógépek, a szerverek, az okostelefonok és a tabletek. 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 tartalmazzák a víruskereső és behatolás megelőző szoftverek használatának módját. A minden részletre kiterjedő állomásbiztonsági megoldások a hálózati hozzáférés vezérlésén alapulnak.

16.3.8

## Tudáspróba - Hálózati támadások elkerülése

Az űrlap teteje

Check your understanding of network attack mitigation by choosing the BEST answer to the following questions.

1. Which device controls traffic between two or more networks to help prevent unauthorized access?

Az űrlap alja

Which device is used by other network devices to authenticate and authorize management access?

Which backup policy consideration is concerned with using strong passwords to protect the backups and for restoring data?

This zone is used to house servers that should be accessible to outside users.

Which is appropriate for providing endpoint security?

[16.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati támadások](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Eszközbiztonság](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 
* 

1. Hálózatbiztonsági alapok
2. Eszközbiztonság

# Eszközbiztonság

16.4.1

## Cisco AutoSecure

A hálózati területen működő eszközök biztonságának fenntartása kiemelt figyelmet kíván. Valószínűleg már rendelkezünk jelszóval a számítógépünkhöz, a mobiltelefonunkhoz vagy a táblagépünkhöz. Vajon ezek olyan erősek, mint lenniük kellene? Használunk más módszereket is eszközeink biztonságának fokozására? Ebben a témakörben megismerhetjük, hogyan tehetjük meg.

Egy új rendszer telepítése után az eszköz biztonsági beállításai az alapértelmezett értéket kapják. A legtöbb esetben ez a biztonsági szint nem elegendő. Cisco routerek esetében az AutoSecure szolgáltatás segít a rendszer biztonságossá tételében (lásd ábra).

Router# **auto secure**

--- AutoSecure Configuration ---

\*\*\* AutoSecure configuration enhances the security of

the router but it will not make router absolutely secure

from all security attacks \*\*\*

A beállítás néhány egyszerű lépésből áll, amelyek alkalmazhatók a legtöbb operációs rendszer esetében is:

* 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.

Mivel a gyártótól szállított berendezések hosszabb időt is tölthetnek raktárakban, nincsenek naprakész állapotban. Fontos, hogy beüzemelés előtt frissítsük a szoftvereket és telepítsük a biztonsági javításokat.

16.4.2

## Jelszavak

A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. Kövessük az alábbi szabványos irányelveket:

* Használjunk legalább 8, de inkább 10, vagy annál több karakterből álló jelszavakat. A hosszabb jelszó biztonságosabb.
* Alkalmazzunk 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 a születési dátumok, azonosító számok, szülők nevei, vagy bármely könnyen azonosítható információ.
* Írjuk szándékosan rosszul a kiválasztott szót. 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 írjuk le a jelszavakat és ne hagyjuk őket látható helyen, az asztalon vagy a monitoron.

A táblázatban példákat láthatunk erős és gyenge jelszavakra.

### Gyenge jelszavak

| Table caption | |
| --- | --- |
| **Gyenge jelszó** | **Miért gyenge?** |
| secret | Egyszerű, szótárban szereplő szó |
| smith | Az anya leánykori neve |
| toyota | Autómárka |
| bob1967 | A felhasználó neve és születésnapja |
| Blueleaf23 | Egyszerű szavak és számok |

### Erős jelszavak

| Table caption | |
| --- | --- |
| **Erős jelszó** | **Miért erős?** |
| b67n42d39c | Alfanumerikus karakterek kombinációja |
| 12^h u4 @1p7 | Alfanumerikus karakterek és szimbólumok kombinációja, és tartalmaz egy szóközt |

Cisco eszközökön a vezető szóközök törlődnek a jelszavakból, de az első karakter után begépeltek megmaradnak. Erős jelszót kapunk, ha a szóköz billentyű segítségével több szóból álló kifejezést hozunk létre. Ezt jelmondatnak (passphrase) is hívják. Egy jelmondatot könnyebb megjegyezni mint egy bonyolult jelszót. Hosszabb és nehezebb is kitalálni.

16.4.3

## További jelszóbiztonsági beállítások

Az erős jelszavak is csak akkor hasznosak, ha titokban maradnak. Cisco router és switch esetében a következő lépések segíthetik a jelszavak titokban tartását:

* A szöveges jelszavak titkosítása
* A minimális elfogadható jelszóhossz beállítása
* A jelszótalálgatás (brute-force) típusú támadások megakadályozása
* Az inaktív, EXEC módú hozzáférés kiléptetése meghatározott idő elteltével

A **service password-encryption** parancs megakadályozza a jogosulatlan személyeket abban, hogy megnézhessék a konfigurációs állományban lévő szöveges jelszavakat (lásd ábra). Ez a parancs titkosítja az összes egyszerű jelszót. Figyeljük meg a példában, hogy a „cisco” jelszó titkosított formája „03095A0F034F”.

A jelszavak minimális hosszának biztosítására használjuk a **security passwords min-length** length parancsot globális konfigurációs módban. A példában minden új jelszónak legalább nyolc karakterből kell állnia.

A támadók jelszótörő szoftvert használhatnak egy hálózati eszköz ellen történő brute-force támadására. Ez a támadás újra és újra megpróbálja kitalálni az érvényes jelszavakat, amíg az egyik be ne válik. Használjuk a **login block-for # attempts # within #** globális konfigurációs parancsot az ilyen típusú támadások megakadályozására. A példában a **login block-for 120 attempts 3 within 60** parancs letiltja a bejelentkezést 120 másodperc időtartamra, ha 3 sikertelen kísérletet érzékel 60 másodpercen belül.

A rendszergazdák figyelme is kihagyhat, és véletlenül egy EXEC módú munkamenetet hagyhatnak nyitva a terminálon. Ez lehetővé teszi egy belső támadó számára az eszköz konfigurációjának módosítását vagy törlését.

Alapértelmezés szerint a Cisco eszközök 10 perces inaktivitás után kijelentkeznek az EXEC munkamenetből. Ezt az értéket azonban az **exec-timeout** perc másodperc vonali konfigurációs paranccsal csökkenthetjük. A parancs alkalmazható konzol, aux és vty vonalakon is. A példában szereplő parancs automatikusan kilépteti a vty vonalon levő inaktív felhasználót 5 perc 30 másodperc tétlenség után.

R1(config)# **service password-encryption**

R1(config)# **security passwords min-length 8**

R1(config)# **login block-for 120 attempts 3 within 60**

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco123**

R1(config-line)# **exec-timeout 5 30**

R1(config-line)# **transport input ssh**

R1(config-line)# **end**

R1#

R1# **show running-config | section line vty**

line vty 0 4

password 7 094F471A1A0A

exec-timeout 5 30

login

transport input ssh

R1#

16.4.4

## Az SSH engedélyezése

A Telnet leegyszerűsíti a távoli eszközök elérését, de nem biztonságos. A Telnet csomagokban lévő adatok titkosítás nélkül kerülnek átvitelre. Éppen ezért a biztonságos távoli eléréshez nagyon ajánlott az SSH engedélyezése az eszközön.

Az SSH-támogatás Cisco eszközön való konfigurálásának négy lépése:

**1. lépés Konfiguráljunk egy egyedi eszköznevet**. Az eszköznek az alapértelmezettől eltérő, egyedi állomásnévvel kell rendelkeznie.

**2. lépés Az IP-tartománynév beállítása**. Konfiguráljuk a hálózat IP-tartománynevét az **ip-domain name** globális konfigurációs paranccsal.

**3. lépés Hozzunk létre kulcsot az SSH-forgalom titkosításához**. Az SSH titkosítja a forrás és a cél közötti forgalmat. Ehhez azonban egyedi hitelesítési kulcsot kell generálni a **crypto key generate rsa general-keys modulus** bitek száma globális konfigurációs parancs használatával. A bitek száma határozza meg a kulcs méretét, amely 360 és 2048 között érték lehet. Minél nagyobb a szám, annál biztonságosabb a kulcs. Nagyobb bitérték esetén azonban tovább tart az információk titkosítása és visszafejtése. Az ajánlott minimális modulus hossz 1024 bit.

**4. lépés Helyi adatbázis bejegyzés ellenőrzése vagy létrehozása**. Hozzunk létre helyi felhasználót. Erre szolgál a **username** globális konfigurációs parancs. A példában a **secret** paraméter szerepel, így a jelszó titkosítva lesz MD5 használatával.

**5. lépés Hitelesítés a helyi adatbázisban**. A **login local** vonali konfiguráció paranccsal a vty vonal használata a helyi adatbázisból történő hitelesítéssel történik.

**6. lépés Engedélyezzük a vty vonalon bejövő SSH-munkameneteket**. Alapértelmezés szerint a vty vonalakon nem engedélyezett a bejövő kapcsolat. A **transport input [ssh | telnet]** paranccsal több bemeneti protokollt is megadhatunk, beleértve a Telnetet és az SSH-t is.

A példában az R1 router a span.com tartományban van. Ez az információ a **crypto key generate rsa general-keys modulus** parancsban megadott bitértékkel együtt a titkosítási kulcs létrehozásához szükséges.

A következő parancsban létrejön egy Bob nevű felhasználó a helyi adatbázisban. Végül a vty vonalak konfigurációja következik, amely szerint a bejelentkezések a helyi adatbázisból kerülnek hitelesítésre, és csak SSH-munkamenetek jöhetnek létre.

Router# **configure terminal**

Router(config)# **hostname R1**

R1(config)# **ip domain name span.com**

R1(config)# **crypto key generate rsa general-keys modulus 1024**

The name for the keys will be: Rl.span.com % The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1(config)#

R1(config)# **username Bob secret cisco**

R1(config)# **line vty 0 4**

R1(config-line)# **login local**

R1(config-line)# **transport input ssh**

R1(config-line)# **exit**

R1(config)#

16.4.5

## Nem használt szolgáltatások letiltása

A Cisco routerek és switch-ek bekapcsolásakor sok olyan szolgáltatás is elindul, amelyekre esetleg nincs szükség a hálózatban. Tiltsuk le a nem használt szolgáltatásokat a rendszererőforrások (például a CPU és a RAM) megőrzése érdekében, egyúttal megakadályozva a támadókat ezen szolgáltatások kihasználásában. Az alapértelmezés szerint bekapcsolt szolgáltatások típusa az IOS verziójától függően változhat. Például az IOS-XE esetében csak HTTPS- és DHCP- portok lesznek nyitva. Ezt a **show ip ports all** paranccsal ellenőrizhetjük (lásd kimenet).

Router# **show ip ports all**

Proto Local Address Foreign Address State PID/Program Name

TCB Local Address Foreign Address (state)

tcp :::443 :::\* LISTEN 309/[IOS]HTTP CORE

tcp \*:443 \*:\* LISTEN 309/[IOS]HTTP CORE

udp \*:67 0.0.0.0:0 387/[IOS]DHCPD Receive

Router#

Az IOS-XE előtti IOS-verziók a **show control-plane host open-ports** parancsot használják. Ezt a parancsot azért említjük, mert régebbi eszközökkel is sokszor találkozhatunk. A kimenet hasonló. Figyeljük meg azonban, hogy ez a régebbi router HTTP-kiszolgálót és a Telnetet futtat, amelyek nem biztonságosak. Mindkét szolgáltatást le kell tiltani. A HTTP kikapcsolása a **no ip http server** globális konfigurációs paranccsal történik. A Telnet letiltása és csak az SSH engedélyezése a **transport input ssh** vonali konfigurációs paranccsal lehetséges.

Router# **show control-plane host open-ports**

Active internet connections (servers and established)

Prot Local Address Foreign Address Service State

tcp \*:23 \*:0 Telnet LISTEN

tcp \*:80 \*:0 HTTP CORE LISTEN

udp \*:67 \*:0 DHCPD Receive LISTEN

Router# configure terminal

Router(config)# **no ip http server**

Router(config)# **line vty 0 15**

Router(config-line)# **transport input ssh**

16.4.6

## Packet Tracer - Biztonságos jelszavak és SSH konfigurálása

A hálózati rendszergazda megbízott bennünket az RTA és az SW1 eszközök előkészítésével. A hálózathoz való csatlakoztatásuk előtt biztonsági beállításokat kell konfigurálnunk.

[Biztonságos jelszavak és SSH konfigurálása](https://contenthub.netacad.com/courses/itn/_common/16.4.6-packet-tracer---configure-secure-passwords-and-ssh_hu-HU.pka)

16.4.7

## Laborgyakorlat - SSH konfigurálása hálózati eszközökön

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Eszközök alapvető konfigurálása
* Bölüm 2: SSH-hozzáférés konfigurálása routeren
* Bölüm 3: SSH-hozzáférés konfigurálása switch-en
* Bölüm 4: SSH-belépés CLI-ből

[16.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózati támadások elkerülése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[16.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    

1. Hálózatbiztonsági alapok
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

16.5.1

## Packet Tracer feladat - Hálózati eszközök biztonsági beállításai

Ebben a feladatban egy routert és egy switch-et konfigurálunk egy követelménylista alapján.

[Hálózati eszközök biztonsági beállításai](https://contenthub.netacad.com/courses/itn/_common/16.5.1-packet-tracer---secure-network-devices_hu-HU.pka)

16.5.2

## Laborgyakorlat - Hálózati eszközök biztonsági beállításai

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Eszközök alapvető konfigurálása
* Bölüm 2: Alapvető biztonsági beállítások routeren
* Bölüm 3: Alapvető biztonsági beállítások switch-en

16.5.3

## Miről tanultunk ebben a fejezetben?

**Biztonsági fenyegetések és sebezhetőségek**

Egy hálózat elleni támadás végzetes lehet, a fontos információk és eszközök megrongálása vagy ellopása idő- és pénzveszteséget okoz. Azokat a behatolókat, akik a szoftver módosításával vagy a szoftver sebezhető pontjait kihasználva jutnak hozzáféréshez támadóknak (hacker) nevezzük. Miután a támadó hozzáfér a hálózathoz, négyféle fenyegetés merülhet fel: információlopás, adatvesztés és manipuláció, azonosító lopás és a szolgáltatás megzavarása. Három elsődleges biztonsági rés vagy gyengeség van: technológiai, konfigurációs és biztonsági házirendbeli. A fizikai fenyegetések négy típusa: hardver, környezet, elektromos és karbantartási.

**Hálózati támadások**

A "malware" a rosszindulatú szoftverek rövid neve (malicious software). Ez a kód vagy szoftver kifejezetten az adatok, számítógépek és hálózatok károsítására, megzavarására, ellopására, vagy törvénytelen műveletek végrehajtására készült. A rosszindulatú programok típusai: vírusok, férgek és trójaiak. A hálózati támadások három fő kategóriába sorolhatók: felderítéses, hozzáférési és szolgáltatásmegtagadás. A fizikai fenyegetések négy típusa: hardver, környezet, elektromos és karbantartási. A felderítéses támadások három típusa: internetes lekérdezések, ping pásztázás és port szkennelés. A hozzáférési támadások négy kategóriája: jelszó (brute-force, trójai, protokoll elemző), bizalom kihasználása, portátirányítás és közbeékelődés. A szolgáltatás megtagadás támadások két típusa: DoS és DDoS.

**Hálózati támadás elkerülése**

A hálózati támadások elkerülése érdekében először az eszközöket kell megvédeni: a routereket, a switch-eket, a kiszolgálókat és a munkaállomásokat. Sok szervezet alkalmaz mélységi védelmet (defense-in-depth), más néven a védelem rétegzésének stratégiáját. Ez a hálózati eszközök és szolgáltatások kötelékben való működését követeli meg. Számos biztonsági eszköz és szolgáltatás működik a felhasználók és a berendezések védelme érdekében: VPN, ASA-tűzfal, IPS, ESA/WSA és AAA-szerver. Az infrastruktúra eszközök konfigurációs beállításairól és IOS-képfájljairól mentést kell készíteni FTP- vagy hasonló fájlkiszolgálóra. Ha a számítógép vagy a router hardvere meghibásodik, az adatok és a konfiguráció visszaállítható a biztonsági másolatból. A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch). A kritikus biztonsági javítások kezeléséhez győződjünk meg arról, hogy az összes végberendezés automatikusan letölti a frissítéseket. 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 két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is. A külső felhasználók számára elérhető szerverek egy speciális hálózatban, a DMZ-ben kapnak helyet. A tűzfalak különböző technikákat alkalmaznak a hálózati hozzáférés engedélyezéséhez vagy megtagadásához: csomagszűrés, alkalmazásszűrés, URL-szűrés és állapottartó csomagvizsgálat (SPI). A végponti eszközök védelme kritikus fontosságú a hálózati biztonság szempontjából. Egy vállalatnak jól meghatározott szabályzatokkal kell rendelkeznie, amelyek magukban foglalhatják a víruskereső szoftverek alkalmazását és a behatolásmegelőző rendszerek használatát. A minden részletre kiterjedő állomásbiztonsági megoldások a hálózati hozzáférés vezérlésén alapulnak.

**Eszközbiztonság**

Egy új rendszer telepítése után az eszköz biztonsági beállításai az alapértelmezett értéket veszik fel. Ez a biztonsági szint nem elegendő. Cisco routerek esetében az AutoSecure szolgáltatás segít a rendszer biztonságossá tételében. A rendszerek alapértelmezett felhasználónevét és jelszavát azonnal módosítani kell. A rendszererőforrásokhoz való hozzáférést azokra a személyekre kell korlátozni, akik jogosultak ezek használatára. A szükségtelen szolgáltatásokat és alkalmazásokat ki kell kapcsolni vagy el kell távolítani, ha lehetséges. A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. Egy jelmondatot könnyebb megjegyezni mint egy bonyolult jelszót. Hosszabb és nehezebb is kitalálni. Routerek és switch-ek esetén titkosítsuk az összes egyszerű szöveges jelszót, állítsunk be a minimális jelszóhosszúságot, akadályozzuk meg jelszó feltörő támadásokat, és zárjuk be az inaktív, EXEC módú munkamenetet egy meghatározott tétlenségi idő után. Állítsuk be az eszközökön az SSH-támogatást, és tiltsuk le a nem használt szolgáltatásokat.

16.5.4

## Ellenőrző kvíz - Hálózatbiztonsági alapok

Az űrlap teteje

1. Melyik összetevőt tervezték arra, hogy megvédjen a számítógépre irányuló és onnan érkező illetéktelen kommunikációtól?

Az űrlap alja

Melyik parancs tiltja le a bejelentkezést a RouterA forgalomirányítón 30 másodperc időtartamra, ha 2 sikertelen bejelentkezési kísérletet érzékel 10 másodpercen belül?

What is the purpose of the network security accounting function?

Milyen típusú támadás járhat együtt olyan eszközök használatával, mint az nslookup és az fping?

Milyen előnyöket kínál az SSH a Telnet-hez képest a routerek távoli kezeléséhez?

Mi az egyik leghatékonyabb biztonsági eszköz, amely megvédi a felhasználókat a külső fenyegetések ellen?

Milyen típusú hálózati fenyegetés célja, hogy megakadályozza, hogy az arra jogosult felhasználók hozzáférjenek az erőforrásokhoz?

Melyik három szolgáltatást nyújtja az AAA-keretrendszer? (Három jó válasz van.)

Melyik rosszindulatú kódtámadás önálló, és próbál meg kihasználni egy adott biztonsági rést a megtámadott rendszerben?

Néhány router és switch meghibásodott a huzalozási központban, miután a légkondicionáló egység tönkrement. Milyen típusú fenyegetést ír le ez a helyzet?

Mit jelent a sebezhetőség kifejezés?

Melyik három konfigurációs beállítást kell megadni a routerhez való SSH-hozzáférés megvalósításához? (Három jó válasz van.)

Mi a célja egy hálózati felderítéses támadásnak?

Biztonsági okokból a hálózati rendszergazdának biztosítania kell, hogy a helyi számítógépek ne tudják pingelni egymást. Ennek eléréséhez mit kell módosítania?

A hálózati rendszergazda SSH-n keresztül kapcsolódik egy switch-hez. Milyen jellemző írja le egyértelműen az SSH-kapcsolatot?

[16.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Eszközbiztonság](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     

1. Kisméretű hálózat építése
2. Bevezetés

# Bevezetés

17.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Kisméretű hálózat építése című fejezetben!

Hurrá! Ez a Bevezetés a hálózatok világába v7.0 című tanfolyam utolsó fejezete. Már rendelkezünk azzal az alapvető tudással, amelyek szükséges egy saját hálózat létrehozásához. Hogyan tovább? Természetesen építünk egy hálózatot. Nem csak építünk, hanem ellenőrizzük a működését, és néhány gyakori hálózati problémát is elhárítunk. Ez a fejezet laborgyakorlatokat és Packet Tracer feladatokat is tartalmaz, amelyek segítenek elsajátítani a hálózati rendszergazda számára szükséges készségeket. Kezdjünk bele!

17.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Fejezet címe:** Kisméretű hálózat építése

**Fejezet célja:** Hálózati terv megvalósítása egy kisméretű hálózat számára, amely router-t, switch-et és végberendezéseket tartalmaz.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Kisméretű hálózatok eszközei** | A kisméretű hálózatokban használt készülékek azonosítása |
| **Kisméretű hálózatok alkalmazásai és protokolljai** | A kisméretű hálózatban használt protokollok és alkalmazások azonosítása. |
| **Átmenet a nagyobb hálózatok felé** | Annak ismertetése hogyan szolgál egy kisméretű hálózat a nagyobb hálózatok alapjául. |
| **Kapcsolatok ellenőrzése** | A ping és tracert parancsok kimenetének használata a kapcsolat ellenőrzéséhez és a relatív hálózati teljesítmény megállapításához. |
| **Számítógépes és IOS parancsok** | Információk begyűjtése a hálózatban működő eszközökkel kapcsolatban az állomás utasításai és IOS-parancsok segítségével. |
| **Hibaelhárítási módszerek** | Gyakori hálózati hibaelhárítási módszerek ismertetése. |
| **Hibaelhárítási forgatókönyvek** | A hálózat eszközeivel kapcsolatos problémák elhárítása. |

[16.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kisméretű hálózatok eszközei](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         

1. Kisméretű hálózat építése
2. Kisméretű hálózatok eszközei

# Kisméretű hálózatok eszközei

17.1.1

## Kisméretű hálózati topológiák

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

Egy kisméretű hálózat terve általában egyszerű. A benne lévő eszközök száma és típusa jelentősen kevesebb a nagyobb hálózatéhoz képest.

Lásd például az ábrán látható kisvállalkozás hálózatának mintáját.

small network topology with a printer, server, IP phone and attached host, access point and attached laptop, all connected to a switch connected to a router connected to the Internet cloud

Internet

Ez a kisméretű hálózat router-t, switch-et és vezeték nélküli hozzáférési pontot tartalmaz a vezetékes és vezeték nélküli felhasználók, az IP-telefon, a nyomtató és a kiszolgáló csatlakoztatásához. A kisméretű hálózatok internet kapcsolata általában egyetlen WAN-csatlakozás, amely DSL, kábel vagy Ethernet szolgáltatáson keresztül valósul meg.

A nagyméretű hálózatokban informatikai részleg szükséges a hálózati eszközök karbantartásához, hibaelhárításához és a biztonság megvalósításához, valamint a szervezet adatainak védelméhez. Egy kisméretű hálózat felügyelete nagyon hasonló képességeket igényel, mint egy nagyméretű hálózaté. A kisméretű hálózatokat helyi informatikai technikus vagy szerződéses szakember kezeli.

17.1.2

## Kisméretű hálózat eszközeinek kiválasztása

A nagyméretű hálózatokhoz hasonlóan a kisméretű hálózatok is tervezést igényelnek, hogy megfeleljenek a felhasználói elvárásoknak. Tervezéskor figyelembe kell venni az összes követelményt, költség tényezőt és fejlesztési igényt.

A tervezés egyik első lépése a közvetítő eszközök típusának kiválasztása.

Kattintsunk az egyes gombokra a hálózati eszközök kiválasztáshoz szükséges tényezők megismeréséhez!

**Költség**

A switch és a router 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 a hálózati eszközök csatlakoztatásához szükséges kábelezés költségét is. A költségeket befolyásoló másik kulcsfontosságú elem a hálózatba beépítendő redundancia mértéke.

17.1.3

## IP-címzés a kisméretű hálózatokban

A hálózat megvalósításakor hozzunk létre egy IP-címzési sémát és használjuk azt. Minden végberendezésnek és hálózati eszköznek egyedi címmel kell rendelkeznie.

Az IP-címzési sémába beszámító eszközök a következők:

* Végfelhasználói eszközök - A kapcsolatok száma és típusa (pl. vezetékes, vezeték nélküli, távoli hozzáférés)
* Kiszolgálók és perifériák (pl. nyomtatók és biztonsági kamerák)
* Közvetítő eszközök, beleértve a switch-eket és a hozzáférési pontokat (AP)

Tervezzünk meg, dokumentáljunk és tartsunk karban egy IP-címzési sémát az eszköztípusok alapján. Az IP-címzési rendszer használata megkönnyíti az eszköz azonosítását és a problémák elhárítását, például a hálózati protokoll-elemzővel történő hibajavítást.

Az ábrán egy kis- vagy közepes méretű szervezet hálózati topológiája látható.

network topology consisting of three LANs - 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 - with various end devices, connected to a router connected to the Internet cloud

192.168.1.0/24 192.168.2.0/24

192.168.3.0/24

Internet

A szervezetnek három felhasználói LAN-ra van szüksége (192.168.1.0/24, 192.168.2.0/24 és 192.168.3.0/24). A hálózati terv szerint minden 192.168.x.0/24 LAN esetében egységes IP-címzési séma kerül bevezetésre:

| Device Type Assignable IP Address Range Summarized as …Default gateway (Router)192.168.x.1 - 192.168.x.2192.168.x.0/30Switches (max 2)192.168.x.5 - 192.168.x.6192.168.x.4/30Access points (max 6)192.168.x.9 - 192.168.x.14192.168.x.8/29Servers (max 6)192.168.x.17 - 192.168.x.22192.168.x.16/29Printers (max 6)192.168.x.25 - 192.168.x.30192.168.x.24/29IP Phones (max 6)192.168.x.33 - 192.168.x.38192.168.x.32/29Wired devices (max 62)192.168.x.65 - 192.168.x.126192.168.x.64/26Wireless devices (max 62)192.168.x.193 - 192.168.x.254192.168.x.192/26 | | |
| --- | --- | --- |
| **Készülék típus** | **Hozzárendelhető IP-címtartomány** | **Hálózat** |
| Alapértelmezett átjáró (Router) | 192.168.x.**1** - 192.168.x.**2** | 192.168.x.**0/30** |
| Switch-ek (max. 2) | 192.168.x.**5** - 192.168.x.**6** | 192.168.x.**4/30** |
| Hozzáférési pontok (max. 6) | 192.168.x.**9** - 192.168.x.**14** | 192.168.x.**8/29** |
| Szerverek (max. 6) | 192.168.x.**17** - 192.168.x.**22** | 192.168.x.**16/29** |
| Nyomtatók (max. 6) | 192.168.x.**25** - 192.168.x.**30** | 192.168.x.**24/29** |
| IP telefonok (max. 6) | 192.168.x.**33** - 192.168.x.**38** | 192.168.x.**32/29** |
| Vezetékes eszközök (max. 62) | 192.168.x.**65** - 192.168.x.**126** | 192.168.x.**64/26** |
| Vezeték nélküli eszközök (max. 62) | 192.168.x.**193** - 192.168.x.**254** | 192.168.x.**192/26** |

Az ábrán egy példa látható a 192.168.2.0/24 hálózat címzésére, amelyben az eszközök IP-címei az előre definiált IP-címzési séma szerint vannak megadva.

The diagram is a small LAN topology with a network address of 192.168.2.0/24. It shows various end devices all connected to a switch, with address .5, connected to a router, at address .1, connected to the Internet cloud. All devices have been assigned an IP address. A printer has an address of .25; server has an address of .17; a PC has an address of .65 connected to an IP phone with an address of .33; and a laptop has an address of .193 connected to an access point with an address of .9.

.193 .9 .5 .33 .65 .25 .17 .1

192.168.2.0/24

Internet

Például az alapértelmezett átjáró IP-címe 192.168.2.1/24, a switch IP-címe 192.168.2.5/24, a kiszolgáló IP-címe 192.168.2.17/24 stb.

Figyeljük meg, hogy a hozzárendelhető IP-címtartományok szándékosan kerültek alhálózati határra a csoporttípus összegzésének egyszerűsítése érdekében. Tegyük fel, hogy egy 192.168.2.6 IP-címmel rendelkező switch-et adunk a hálózathoz. Egy hálózati házirendben az összes switch azonosításához a rendszergazda használhatja a 192.168.x.4/30 összesített hálózati címet.

17.1.4

## Redundancia a kisméretű hálózatban

A hálózattervezés másik fontos eleme a megbízhatóság. A kisvállalkozások üzleti folyamatai számára elengedhetetlen a hálózat megfelelő működése. Egy hálózati hiba jelentős anyagi veszteséget okozhat.

A magas szintű megbízhatóság fenntartása érdekében hálózati redundancia tervezésére van szükség. Amely segít az elsődleges meghibásodási pontok kiküszöbölésében.

A redundancia megvalósításának számos módja van egy hálózatban. Az egyik a berendezések másodpéldányainak telepítése, a másik a hálózati összeköttetések többszörözése, ahogy az ábrán is látható.

The diagram illustrates the use of redundant servers, links, switches, and routers in a network. Shown are four layers with an explanation of the redundancy achieved at each. The top layer has three servers and text reads: Redundant servers are available in case of server failure. The next layer shows that each server has two connections leading to two switches and text reads: Redundant links are present to provide alternate paths in case of a link failure. The next layer shows two switches connected to each other with each connected to all three servers above and text reads: Redundant switches are present in case of switch failure. The bottom layer shows two routers connected to each other with each connected to one of the switches and text reads: Redundant routers are available in case of router or route failure.

A redundáns kiszolgálók egy szerver meghibásodása esetén is elérhetők.A redundáns kapcsolatok alternatív útvonalakat biztosítsanak egy kapcsolat meghibásodása esetén.A redundáns switch-ek átveszik a meghibásodottak szerepét.A redundáns routerek rendelkezésre állnak egy router vagy útvonal meghibásodása esetén is.

A kisméretű hálózatoknak általában egy kijáratuk van az internet felé egy vagy több alapértelmezett átjárón keresztül. Ilyenkor a router meghibásodása a teljes hálózat internet kapcsolatának elvesztését eredményezi. Éppen ezért a kisvállalkozások számára is kifizetődő lehet egy olcsó másodlagos összeköttetés előfizetése (backup).

17.1.5

## Forgalomszabályozás

Egy jó hálózati terv célja kisméretű hálózatok esetén is a munka hatékonyságának növelése és a kiesési idő minimalizálása. A hálózati rendszergazdának a rendszer tervezésekor tekintetbe kell vennie a különféle forgalomtípusokat és azok kezelésének módját.

A kisméretű hálózatokban a routereket és switch-eket úgy kell konfigurálni, hogy a valós idejű forgalmat (például a hang- és a videó átvitel) az egyéb adatforgalomtól elválasztva kezeljék. Egy jó hálózati tervben a forgalom prioritás alapján kerül osztályozásra (QoS), ahogy az ábrán is látható.

The diagram shows how a router prioritizes network traffic. An arrow shows that traffic is sent to a router without any priority. The router then sends traffic to the backbone in order of priority. The router has layers of different traffic with varying levels of priority, the highest priority at the top. Voice is listed first with high priority, then SMTP with medium priority, then instant messaging with normal priority, and lastly FTP with low priority.

Traffic sent to router without any priorityBackbone NetworkTraffic sent to backbone in order of priorityVoiceHigh PrioritySMTPMedium PriorityInstant MessagingNormal PriorityFTPLow Priority

A várakozási lista négy sorból áll. A kiemelt prioritású várólista ürül ki először.

17.1.6

## Tudáspróba - Kisméretű hálózatok eszközei

Az űrlap teteje

Check your understanding of the devices in a small network by choosing the BEST answer to the following questions.

1. Which statement correctly relates to a small network?

Az űrlap alja

Which factor must be considered when selecting network devices?

What is necessary to plan and use when implementing a network?

What is required to maintain a high degree of reliability and eliminate single points of failure?

What is required to classify traffic according to priority?

[17.0](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Bevezetés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kisméretű hálózatok alkalmazásai és protokolljai](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           

1. Kisméretű hálózat építése
2. Kisméretű hálózatok alkalmazásai és protokolljai

# Kisméretű hálózatok alkalmazásai és protokolljai

17.2.1

## Gyakori alkalmazások

Az előző fejezetben egy kisméretű hálózat elemeit, valamint néhány tervezési megfontolást ismerhettünk meg. Ezek az elvek a hálózat összeállításához szükségesek. Összeállítás után a hálózat megfelelő működéséhez további alkalmazások és protokollok szükségesek.

Egy hálózat csak olyan mértékben hasznos, mint amennyire a benne lévő alkalmazások. Kétféle szoftver vagy folyamat van, ami hozzáférést biztosít a hálózathoz: a hálózati alkalmazások és az alkalmazási rétegbeli szolgáltatások.

**Hálózati alkalmazások**

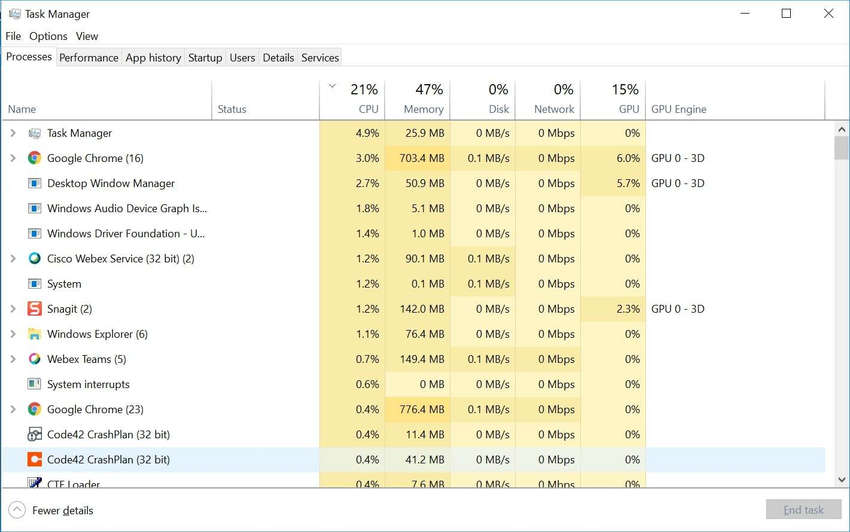
A hálózati alkalmazások olyan szoftverek, melyek alkalmasak a hálózaton keresztüli kommunikációra. Néhány felhasználói program hálózat-tudatos, azaz olyan alkalmazási rétegbeli protokollokat használ, amelyek képesek kommunikálni az alsóbb rétegekkel. Ilyen alkalmazások például az email kliensek és a 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.

A Feladatkezelő segítségével megtekinthetjük egy Windows számítógépen futó aktuális alkalmazásokat, folyamatokat és szolgáltatásokat (lásd ábra).



17.2.2

## Gyakori protokollok

Egy szakember legtöbb feladatában valamilyen módon megjelennek a hálózati protokollok, legyen szó akár egy kis- vagy nagyméretű hálózatról. A hálózati protokollok támogatják az alkalmazottak által használt programokat és szolgáltatásokat egy kisméretű hálózatban.

A hálózati rendszergazdáknak általában szükségük van a hálózati eszközökhöz és kiszolgálókhoz való hozzáférésre. A két leggyakoribb távelérési megoldás a Telnet és az SSH (Secure Shell). Az SSH-szolgáltatás a Telnet biztonságos alternatívája. Csatlakozáskor a rendszergazdák úgy érik el az SSH-kiszolgálót, mintha helyben lennének bejelentkezve.

Az SSH biztonságos távelérési kapcsolatot hoz létre az SSH kliens és az SSH-kompatibilis eszköz között:

* **Hálózati eszköz** — A hálózati eszköznek (pl. router, switch, hozzáférési pont stb.) támogatnia kell az SSH-t, hogy távoli hozzáférést biztosító SSH-kiszolgálói szolgáltatásokat nyújthasson az ügyfeleknek.
* **Kiszolgáló** — A szervernek (pl. webkiszolgáló, e-mail kiszolgáló stb.) támogatnia kell az SSH-kiszolgálói szolgáltatásokat az ügyfelek számára.

A hálózati rendszergazdáknak ismerniük kell a hálózati kiszolgálókat és az általuk használt hálózati protokollokat is (lásd ábra).

Web ServerEmail ServerFTP ServerDHCP ServerDNS Server

Kattintsunk az egyes gombokra a hálózati kiszolgálókkal és a hozzájuk kapcsolódó hálózati protokollokkal kapcsolatos további információkért!

**Webkiszolgáló**

* A webes ügyfelek és webkiszolgálók a HTTP-protokoll (Hypertext Transfer Protocol) használatával cserélnek információkat.
* A HTTPS (Hypertext Transfer Protocol Secure) a biztonságos webes kommunikációhoz használható.

**MEGJEGYZÉS**: Egy kiszolgáló több hálózati szolgáltatást is nyújthat. Például egy kiszolgáló lehet e-mail, FTP- és SSH-szerver is egyben.

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

* 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

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

17.2.3

## Hang és videó alkalmazások

A vállalkozások egyre inkább IP-telefónia és videó konferencia segítségével kommunikálnak az ügyfelekkel és az üzleti partnerekkel. Számos szervezet teszi lehetővé az alkalmazottaik számára, hogy távolról dolgozzanak. Amint azt az ábra mutatja, a felhasználóknak szükségük van a vállalati szoftverekhez és fájlokhoz való hozzáférésre, valamint a hang és videó alkalmazások használatára.



Ezért a hálózati rendszergazdának gondoskodnia kell a megfelelő berendezések telepítéséről és konfigurálásáról.

Kattintsunk az egyes gombokra, hogy további információkat kapjunk azokról a tényezőkről, amelyeket egy kisméretű hálózat rendszergazdájának figyelembe kell vennie a valós idejű alkalmazások támogatásakor!

**Infrastruktúra**

* A hálózati infrastruktúrának támogatnia kell a valós idejű alkalmazásokat.
* A meglévő eszközöket és kábeleket tesztelni és ellenőrizni kell.
* Újabb hálózati berendezésekre is szükség lehet.

17.2.4

## Tudáspróba - Kisméretű hálózat alkalmazásai és protokolljai

Az űrlap teteje

Check your understanding of small network applications and protocols by choosing the BEST answer to the following questions.

1. What are two forms of software programs or processes that provide access to the network? (Choose two.)

Az űrlap alja

Which two network protocols are used to establish a remote access network connection to a device? (Choose two.)

[17.1](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kisméretű hálózatok eszközei](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatok növekedése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             

1. Kisméretű hálózat építése
2. Hálózatok növekedése

# Hálózatok növekedése

17.3.1

## A kisméretű hálózat növekedése

Ha egy kisvállalkozás szeretné, hogy az üzlet növekedjen, akkor a hálózatnak is együtt kell növekednie vele. A folyamat neve a hálózat méretezése, és van néhány bevált módszer a megvalósítására.

A növekedés számos kisvállalkozás természetes folyamata, amelyet a hálózataiknak is követniük kell. Ideális esetben a rendszergazdának elegendő ideje van a hálózat növekedésével kapcsolatos döntések meghozatalára, amelyek illeszkednek a vállalat növekedési folyamatába.

A hálózat méretezéséhez szükséges elemek:

* **Hálózati dokumentáció** - Fizikai és logikai topológia
* **Eszközleltár** \- A hálózatot használó vagy működtető eszközök listája
* **Költségvetés** - Részletes IT-költségvetés, amely tartalmazza az üzleti év eszközbeszerzésre fordítandó kiadásait
* **Forgalom elemzés** - Protokollok, alkalmazások és szolgáltatások, valamint a hozzájuk tartozó forgalmi követelmények

Ezek az információk szükségesek a kisméretű hálózatok bővítésével kapcsolatos döntéshozatalban.

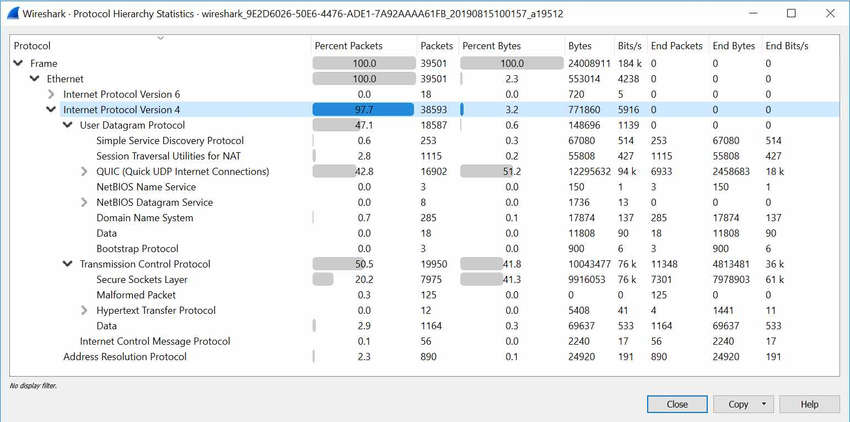
17.3.2

## Protokoll elemzés

A hálózat növekedéses során fontos meghatározni a hálózati forgalom kezelését. Fontos megismerni a hálózaton áthaladó forgalom típusát, valamint az aktuális forgalmi mutatókat. Számos hálózatkezelő eszköz használható erre a célra. Azonban egy egyszerű protokoll analizátor, például a Wireshark is alkalmas a vizsgálat lefolytatására.

A Wireshark futtatása több kulcsfontosságú állomáson felfedheti a hálózati forgalom típusát. A ábrán egy kisméretű hálózat Windows számítógépére vonatkozó protokoll statisztika látható.

screen capture of Wireshark protocol hierarchy statistics for traffic captured by a host



A számítógép IPv6- és IPv4-protokollokat használ. A kimenetből látható, hogy az állomás IPv4-en belül DNS, SSL, HTTP és ICMP és más protokollokat használ.

A hálózat forgalmi mintáinak meghatározása érdekében az alábbiak fontosak:

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

Ezután a begyűjtött adatok rendszerezhetők az üzenetek forrása, célja és típusa szerint is. Az elemzés alapján meghozhatók azok a döntések, amelyekkel 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 teljesítményt optimalizálni.

17.3.3

## Hálózathasználat

A forgalmi trendek változásának megértésén túl a hálózati rendszergazdának tisztában kell lennie a hálózat használatával kapcsolatos változásokkal is. Számos operációs rendszer beépített eszközöket biztosít az ilyen információk megjelenítéséhez. Egy Windows számítógép például a Feladatkezelőt, az Eseménynaplót és az Adatforgalom eszközöket.

Ezek a következő információk „pillanatfelvételének” rögzítésére használhatók:

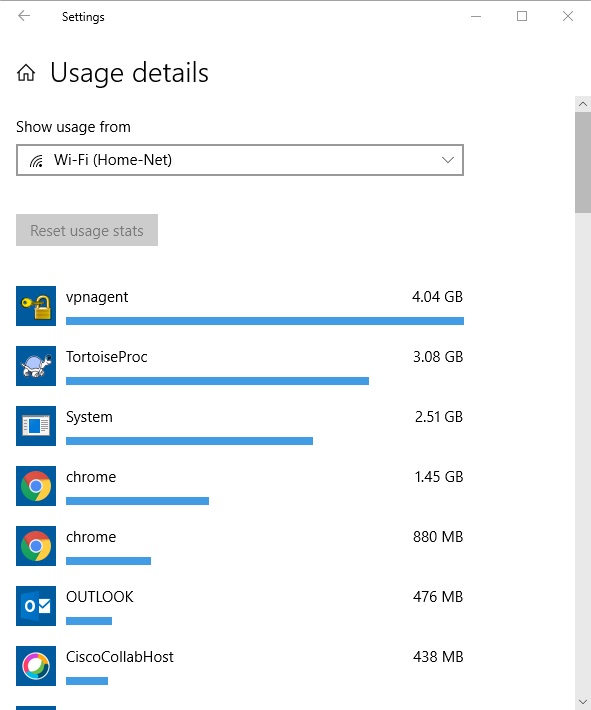
* Operációs rendszer és annak verziója
* CPU-használat
* Memória használat
* Meghajtók használata
* Lokális alkalmazások
* Hálózati alkalmazások

A kisméretű hálózat felhasználóiról rendszeresen készített pillanatfelvételek elemzése nagyon hasznos a protokollok azonosításában és a forgalmi követelmények meghatározásában. A felhasználói szokások megváltozása a hálózati erőforrások megfelelő átcsoportosítását igényli a rendszergazdától.

A Windows 10 Adatforgalom eszköz alkalmas annak meghatározására, hogy mely alkalmazások használnak hálózati szolgáltatásokat a számítógépen. Az Adatforgalom eszköz a következő módon érhető el: **Gépház > Hálózat és internet > Adatforgalom > hálózati interfész** (Az elmúlt 30 napból).

Az ábrán egy Windows 10 számítógép Wi-Fi hálózati kapcsolatát használó programok láthatók.

screen capture of the Windows 10 Data Usage Tool showing usage from a local Wi-Fi connection



17.3.4

## Tudáspróba - Hálózatok növekedése

Az űrlap teteje

Check your understanding of scaling to larger networks by choosing the BEST answer to the following questions.

1. Which elements are required to scale to a larger network? (Choose two.)

Az űrlap alja

Which software installed on key hosts can reveal the types of network traffic flowing through the network?

What Windows 10 tool is useful to determine which applications are using network services on a host?

[17.2](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kisméretű hálózatok alkalmazásai és protokolljai](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kapcsolatok ellenőrzése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 

1. Kisméretű hálózat építése
2. Kapcsolatok ellenőrzése

# Kapcsolatok ellenőrzése

17.4.1

## Kapcsolatok ellenőrzése a ping parancs használatával

Függetlenül attól, hogy a hálózat kisméretű és új vagy egy meglévő hálózat bővítése, mindig ellenőrizni kell, hogy a benne levő komponensek megfelelően csatlakoznak-e egymáshoz és az internethez. Ez a témakör azokat a segédprogramokat tárgyalja, amelyek segítségével megvizsgálhatjuk a hálózati eszközök csatlakozását.

A **ping** parancs a leghatékonyabb módja a 3. rétegbeli kapcsolatok tesztelésének a forrás és a cél IP-cím között. A parancs válaszidő statisztikákat is megjelenít.

A **ping** parancs az ICMP (Internet Control Message Protocol) protokoll a visszhang kérés (echo, ICMP Type 8) és a visszhang válasz (echo reply, ICMP Type 0) üzeneteket használja. A **ping** parancs elérhető a legtöbb operációs rendszerben, beleértve a Windows-t, a Linux-ot, macOS-t és Cisco IOS-t.

Egy Windows 10 számítógépen a **ping** parancs négy egymást követő ICMP visszhang üzenetet küld, és négy egymást követő ICMP visszhang választ vár a céltól.

Tegyük fel, hogy PC A megpingeli PC B-t. Amint az ábrán látható, a PC A számítógép négy egymást követő ICMP visszhang üzenetet küld a PC B felé (azaz 10.1.1.10-nek).

The diagram shows host PC A, at address 192.168.10.10, using the ping ping 203.0.113.8 command from the command prompt to send four ICMP echo messages with a source IP of 198.168.10.10 (should read 192.168.10.10) and a destination IP of ping 203.0.113.8, which is host PC B on another network.

192.168.10.10 PC A PC B C:\>ping 203.0.113.8

203.0.113.8

| **Source IP** | **Destination IP** | **ICMP** |
| --- | --- | --- |
| 192.168.10.10 | 10.1.1.10 | **Echo** |

Internet

A célállomás megkapja és feldolgozza az ICMP visszhang kérést. Az ábrán látható, hogy PC B úgy válaszol, hogy négy ICMP visszhang választ küld PC A-nak

The diagram shows host PC B, at address 203.0.113.8, sending four ICMP echo replies with source IP 203.0.113.8 and destination IP 198.168.10.10 (should read 192.168.10.10) in response to a ping from host PC A at address 192.168.10.10.

PC A PC B C:\>ping 203.0.113.8 203.0.113.8

192.168.10.10

| **SourceIP** | **Destination IP** | **ICMP** |
| --- | --- | --- |
| 10.1.1.10 | 192.168.10.10 | **Echo Replies** |

Internet

A parancs kimenetén látható, hogy PC A visszhang válaszokat kapott PC-B-től, ellenőrizve a 3. rétegbeli hálózati kapcsolatot.

C:\Users\PC-A> **ping 10.1.1.10**

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time=47ms TTL=51

Reply from 10.1.1.10: bytes=32 time=60ms TTL=51

Reply from 10.1.1.10: bytes=32 time=53ms TTL=51

Reply from 10.1.1.10: bytes=32 time=50ms TTL=51

Ping statistics for 10.1.1.10:

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

Approximate round trip times in milli-seconds:

Minimum = 47ms, Maximum = 60ms, Average = 52ms

C:\Users\PC-A>

A parancskimenet visszaigazolja a 3. rétegbeli kapcsolatot PC A és PC B között.

A Cisco IOS **ping** parancskimenete különbözik a Windows rendszerétől. Például az IOS ping utasítás öt ICMP echo üzenetet küld az ábrán látható módon.

R1# **ping 10.1.1.10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R1#

Figyeljük meg a **!!!!!** kimeneti karaktereket. Az IOS **ping** parancs minden beérkezett ICMP visszhang válaszhoz egy jelzőt jelenít meg. A táblázat felsorolja a **ping** parancs leggyakoribb kimeneti karaktereit.

### Az IOS ping utasítás jelei

| Table caption | |
| --- | --- |
| **Jel** | **Leírás** |
| **!** | * A felkiáltójel a visszhang válasz üzenet sikeres fogadását jelzi. * Nyugtázza a 3. rétegbeli kapcsolatot a forrás és a cél között. |
| **.** | * A pont azt jelenti, hogy a várakozási idő lejárt egy visszhang válaszra történő várakozás közben. * Ez kapcsolati problémát jelez az útvonalon. |
| **U** | * A nagybetűs **U** egy az útvonal mentén található router válaszát jelzi, amely a cél elérhetetlen (destination unreachable, ICMP Type 3) hibaüzenettel válaszolt. * A lehetséges okok közé tartozik, hogy a router nem ismeri a célhálózat irányát, vagy nem találta az állomást a célhálózaton. |

**MEGJEGYZÉS:** Egyéb lehetséges ping válaszok: Q, M, ?, vagy &. Ezek jelentésének magyarázata kívül esik a fejezet hatókörén.

17.4.2

## Kiterjesztett ping

A hagyományos **ping** a célhálózathoz legközelebb eső interfész IP-címét használja a **ping** forráscímeként. Az R1-en kiadott **ping 10.1.1.10** parancs forrás IP-címe a G0/0/0 interfész (209.165.200.225) lesz, amint az ábrán is látható.

The diagram shows how a router uses a standard ping to ping a host by sending four consecutive ICMP echo messages sourced from the interface closest to the destination. Router R1 is connected to two networks: on the left is 192.168.10.0/24 on interface G0/0/1 with address .1 and on the right is network 209.165.200.224/30 on interface G0/0/0 with address .225. The latter network is connected to R2 which is connected to network 10.1.1.0/24 on which host PC B is attached with address .10. R1 is sending PC B four ICMP echo messages with a source IP of 209.165.200.225 and a destination IP of 10.1.1.10.

R2 .10 .1 G0/0/0 .10 209.165.200.224 /30 192.168.10.0 /24 10.1.1.0/24 .225 G0/0/1 PC A PC B

R1

| **Source IP** | **Destination IP** | **ICMP** |
| --- | --- | --- |
| 209.165.200.225 | 10.1.1.10 | **Echo** |

A Cisco IOS-ban a **ping** parancs „kiterjesztett” (extended) módja is használható. Ez a mód lehetővé teszi a felhasználó számára, hogy speciális típusú pingeket hozzon létre a parancs paramétereinek beállításával.

Használatához EXEC módban gépeljük be a **ping** parancsot cél IP-cím nélkül. Ezután több kérdést is kapunk a kiterjesztett **ping** testreszabásához.

**MEGJEGYZÉS:** Az **Enter** billentyű leütésének hatására a []-ben lévő alapértelmezett értékek kerülnek elfogadásra.

Tegyük fel például, hogy tesztelni akarjuk a kapcsolatot az R1 LAN-ról (92.168.10.0/24) a 10.1.1.0 LAN-ra. Ez ellenőrizhető lenne a PC A-ról is. Azonban az R1 routeren konfigurálható egy kiterjesztett **ping** úgy, hogy más forráscímet adunk meg.

A példában látható, hogy az R1-en kiadott **ping** parancs forrás IP-címe konfigurálható a G0/0/1 interfész IP-címének használatára (192.168.10.1).

The diagram shows how a router uses an extended ping command to ping a host by sending four consecutive ICMP echo messages with a specified source IP address. Router R1 is connected to two networks: on the left is 192.168.10.0/24 on interface G0/0/1 with address .1 and on the right is network 209.165.200.224/30 on interface G0/0/0 with address .225. The latter network is connected to R2 which is connected to network 10.1.1.0/24 on which host PC B is attached with address .10. R1 is sending PC B four ICMP echo messages with a source IP of 192.168.10.1 and a destination IP of 10.1.1.10.

R2 .10 .1 G0/0/0 .10 209.165.200.224 /30 192.168.10.0 /24 10.1.1.0/24 .225 G0/0/1 PC A PC B

R1

| **Source IP** | **Destination IP** | **ICMP** |
| --- | --- | --- |
| 192.168.10.1 | 10.1.1.10 | **Echo** |

A következő parancskimenetben a kiterjesztett **ping** konfigurálása látható, amelyben a forrás IP-cím a G0/0/1 interfész (192.168.10.1) lesz.

R1# **ping**

Protocol [ip]:

Target IP address: **10.1.1.10**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Ingress ping [n]:

Source address or interface: **192.168.10.1**

DSCP Value [0]:

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0x0000ABCD]:

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

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.10.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#

**MEGJEGYÉS**: A **ping ipv6** parancs IPv6 kiterjesztett pingekhez használható.

17.4.3

## Kapcsolatok ellenőrzése Traceroute segítségével

A **ping** parancs segítségével gyorsan megállapítható, hogy van-e 3. rétegbeli csatlakozási probléma. Azt azonban nem azonosítja, hogy a probléma hol található az útvonal mentén.

A traceroute segíthet megtalálni a 3. rétegbeli problémás területeket a hálózatban. A nyomkövetés (trace) eredménye azon ugrások listája, amelyek a csomagtovábbítás során a hálózati útvonalon előfordulnak. Ezt fel lehet használni az útvonal problémás pontjának azonosításához.

Amint az ábrán is látható a nyomkövetés parancsának szintaxisa operációs rendszerenként változó.

The diagram shows the difference between the trace command as issued from a Windows host versus a Cisco IOS router. The network topology consists of a host PC A connected to a switch connected to router R1 connected to router R2 connected to router R3 connected to a switch connected to host PC B. PC A, at IP address 192.168.10.10, is issuing the following command from a Windows command prompt: C:>:tracert 10.1.1.10. R1 is issuing the following command from the Cisco IOS CLI: R#traceroute 10.1.1.10.

### Windows és Cisco IOS nyomkövetési parancsok

PC A PC B 10.1.1.10 192.168.10.10 .1 R3 R2

R1

Trace from Windows host

C:\ >:**tracert 10.1.1.10**

Trace from a Cisco IOS router

R# **traceroute 10.1.1.10**

A következő példában a **tracert** parancskimenete látható egy Windows 10 számítógépen.

C:\Users\PC-A> **tracert 10.1.1.10**

Tracing route to 10.1.10 over a maximum of 30 hops:

1 2 ms 2 ms 2 ms 192.168.10.1

2 \* \* \* Request timed out.

3 \* \* \* Request timed out.

4 \* \* \* Request timed out.

^C

C:\Users\PC-A>

**MEGJEGYZÉS:** Windowsban a **Ctrl-C** billentyűkombináció segítségével megszakíthatjuk a \*\*tracert\*\* működését.

Az egyetlen sikeres válasz az R1-en található átjáró volt. Nyomkövetés kérések időtúllépését egy csillag (\ \*) jelzi, ami azt jelenti, hogy a következő router nem válaszolt. Ez azt jelzi, hogy a hiba a helyi hálózaton túl található, vagy a következő útválasztók úgy vannak beállítva, hogy ne válaszoljanak a nyomkövetésben használt visszhang kérésekre. Ebben a példában úgy tűnik, hogy a probléma az R1 és R2 között van.

A Cisco IOS **traceroute** és a Windows **tracert** rendszerek parancskimenetei különböznek egymástól. Tekintsük meg az ábrán látható topológiát.

The diagram shows a network topology with the IP addressing of router interfaces and a traceroute command issued from a Cisco IOS router. The topology consists of the following devices and networks, from left to right. A switch on network 192.168.10.0/24 is connected to router R1 at an interface with an address of .1. R1 is connected to router R2 by network 209.165.200.224/30. The interface on R1 has an address of .225 and the interface on R2 has an address of .226. R2 is connected to router R3 by network 209.165.200.228/30. The interface on R2 has an address of .229 and the interface on R3 has an address of .230. R3 is connected to a switch which is connected to host PC B with address 10.1.1.10. R1 is issuing the following trace command from the CLI: R1# traceroute 10.1.1.10.

PC B 10.1.1.10 192.168.10.0 /24 .1 R3 R1 .225 .226 .229 R2 .230 209.165.200.224 /30 209.165.200.228 /30

R1

Trace from a Cisco IOS router

R1# **traceroute 10.1.1.10**

A következő ábrán az R1-en kiadott traceroute parancs kimenete látható.

R1# **traceroute 10.1.1.10**

Type escape sequence to abort.

Tracing the route to 10.1.1.10

VRF info: (vrf in name/id, vrf out name/id)

1 209.165.200.226 1 msec 0 msec 1 msec

2 209.165.200.230 1 msec 0 msec 1 msec

3 10.1.1.10 1 msec 0 msec

R1#

Ebben a példában a nyomkövetés igazolta, hogy a PC B sikeresen elérhető.

Az időtúllépések lehetséges problémát jeleznek. Ha például a 10.1.1.10 állomás nem lenne elérhető, a **traceroute** parancs a következő kimenetet jelenítené meg.

R1# **traceroute 10.1.1.10**

Type escape sequence to abort.

Tracing the route to 10.1.1.10

VRF info: (vrf in name/id, vrf out name/id)

1 209.165.200.226 1 msec 0 msec 1 msec

2 209.165.200.230 1 msec 0 msec 1 msec

3 \* \* \*

4 \* \* \*

5 \*

A **Ctrl-Shift-6** segítségével megszakíthatjuk **traceroute** parancs futását.

**MEGJEGYZÉS**: A traceroute Windows implementációja (tracert) ICMP Echo kéréseket küld ki. A Cisco IOS és Linux UDP-t használ érvénytelen portszámmal. A végső célállomás egy ICMP port elérhetetlen (port unreachable) üzenettel válaszol.

17.4.4

## Kiterjesztett Traceroute

A kiterjesztett **ping** parancshoz hasonlóan létezik kiterjesztett **traceroute** parancs is. Ez lehetővé teszi a rendszergazda számára a parancshoz kapcsolódó paraméterek beállítását. Ez hasznos az irányítási hurkok hibaelhárításakor, a következő router meghatározásakor, vagy annak eldöntésére, hogy egy router vagy tűzfal hol dobja el a csomagokat.

A Windows **tracert** parancs lehetővé teszi több paraméter bevitelét a parancssor opcióin keresztül. Azonban ez nem irányított, mint a kiterjesztett traceroute IOS parancs. A következő kimenetben a Windows **tracert** parancs lehetséges beállításai láthatók.

C:\Users\PC-A> **tracert /?**

Usage: tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout]

[-R] [-S srcaddr] [-4] [-6] target\_name

Options:

-d Do not resolve addresses to hostnames.

-h maximum\_hops Maximum number of hops to search for target.

-j host-list Loose source route along host-list (IPv4-only).

-w timeout Wait timeout milliseconds for each reply.

-R Trace round-trip path (IPv6-only).

-S srcaddr Source address to use (IPv6-only).

-4 Force using IPv4.

-6 Force using IPv6.

C:\Users\PC-A>

A Cisco IOS kiterjesztett **traceroute** lehetővé teszi a felhasználó számára, hogy speciális nyomkövetést végezzen a parancs paramétereinek beállításával. Használatához EXEC módban gépeljük be a **traceroute** parancsot cél IP-cím nélkül. Az IOS kérdések feltevésével vezet végig a parancs opcióin a különböző paraméterek beállításához.

**MEGJEGYZÉS**: Az **Enter** billentyű leütésének hatására a []-ben lévő alapértelmezett értékek kerülnek elfogadásra.

Tegyük fel például, hogy tesztelni akarjuk a PC B kapcsolatát az R1 LAN-ról. Ez ellenőrizhető lenne a PC A-ról is. Azonban az R1 routeren konfigurálható egy kiterjesztett **traceroute** úgy, hogy más forráscímet adunk meg.

The diagram shows a network topology with the IP addressing of router interfaces and an extended traceroute command issued from a Cisco IOS router. The topology consists of the following devices and networks, from left to right. A switch on network 192.168.10.0/24 is connected to router R1 at an interface with an address of .1. R1 is connected to router R2 by network 209.165.200.224/30. The interface on R1 has an address of .225 and the interface on R2 has an address of .226. R2 is connected to router R3 by network 209.165.200.228/30. The interface on R2 has an address of .229 and the interface on R3 has an address of .230. R3 is connected to a switch which is connected to host PC B with address 10.1.1.10. R1 is issuing the following trace command from the CLI: R1# traceroute.

PC B 192.168.10.0/24 209.165.200.224/30 209.165.200.228/30 10.1.1.10 R1 R3 R2 .1 .225 .226 .229

.230

Extended trace from a Cisco IOS router

R1# **traceroute**

A példában látható, hogy az R1-en kiadott **traceroute** parancs forrás IP-címe konfigurálható a LAN interfész IP-címének használatára (192.168.10.1).

R1# **traceroute**

Protocol [ip]:

Target IP address: **10.1.1.10**

Ingress traceroute [n]:

Source address: **192.168.10.1**

DSCP Value [0]:

Numeric display [n]:

Timeout in seconds [3]:

Probe count [3]:

Minimum Time to Live [1]:

Maximum Time to Live [30]:

Port Number [33434]:

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

Type escape sequence to abort.

Tracing the route to 192.168.10.10

VRF info: (vrf in name/id, vrf out name/id)

1 209.165.200.226 1 msec 1 msec 1 msec

2 209.165.200.230 0 msec 1 msec 0 msec

3 \*

10.1.1.10 2 msec 2 msec

R1#

17.4.5

## A hálózat alapállapota

Az egyik leghatékonyabb eszköz a teljesítmény figyelésére és a hibaelhárításra a hálózat alapállapotának, más néven viszonyítási alapjának meghatározása. Egy hatékony hálózati viszonyítási alap létrehozásához meghatározott időtartam szükséges. A különböző időpontokban történő mérések segítenek teljesebb képet alkotni a hálózat összteljesítményéről.

A hálózat viszonyítási alapjához különféle parancsok kimenetei szolgáltatják az adatokat. Az állapotfelmérés kezdőlépése a **ping**, **trace** és egyéb fontos parancsok eredményeinek elmentése egy szöveges állományba. Ezeket a szöveges fájlokat időbélyeggel lehet ellátni, és lementeni őket egy archívumba a későbbi visszakeresés és összehasonlítás céljából.

Figyelni kell a hibaüzeneteket és az állomások közötti válaszidőket. Ha a válaszidők jelentős növekedése tapasztalható, akkor a késleltetésekkel is foglalkozni kell.

Például a következő **ping** kimenetet rögzítettük és mentettük egy szövegfájlba.

**August 19, 2019 at 08:14:43**

C:\Users\PC-A> **ping 10.1.1.10**

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Reply from 10.1.1.10: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.1.10:

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

Approximate round trip times in milli-seconds:

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

C:\Users\PC-A>

Figyeljük meg, hogy a **ping** válaszidők értéke kevesebb mint 1 ms.

Egy hónappal később a pinget megismételjük és rögzítjük.

**September 19, 2019 at 10:18:21**

C:\Users\PC-A> **ping 10.1.1.10**

Pinging 10.1.1.10 with 32 bytes of data:

Reply from 10.1.1.10: bytes=32 time=50ms TTL=64

Reply from 10.1.1.10: bytes=32 time=49ms TTL=64

Reply from 10.1.1.10: bytes=32 time=46ms TTL=64

Reply from 10.1.1.10: bytes=32 time=47ms TTL=64

Ping statistics for 10.1.1.10:

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

Approximate round trip times in milli-seconds:

Minimum = 46ms, Maximum = 50ms, Average = 48ms

C:\Users\PC-A>

Figyeljük meg, hogy a **ping** válaszidők sokkal nagyobbak, ez potenciális problémát jelez.

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

A Cisco hálózati viszonyítási alap létrehozására vonatkozó bevált módszerei megtalálhatók az interneten a „Baseline Process Best Practices” kifejezésre való kereséssel.

17.4.6

## Laborgyakorlat - Hálózati késleltetés ellenőrzése ping és traceroute parancsok használatával

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Bölüm 1: Ping használata a hálózati késleltetés dokumentálására
* Bölüm 2: Traceroute használata a hálózati késleltetés dokumentálására

[17.3](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hálózatok növekedése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Számítógépes és IOS parancsok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        

1. Kisméretű hálózat építése
2. Számítógépes és IOS parancsok

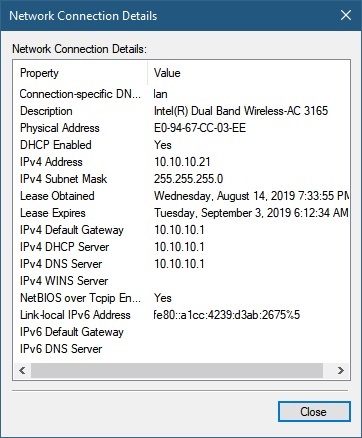
# Számítógépes és IOS parancsok

17.5.1

## IP-konfiguráció Windows számítógépen

Ha az előző témakörben említett eszközök valamelyikével leellenőriztük a kapcsolatot, és úgy találtuk, hogy a hálózat egy része nem működik megfelelően, akkor itt az ideje, hogy bizonyos parancsokat használva elvégezzük az eszközök hibaelhárítását. A számítógép és az IOS parancsai segítenek meghatározni, hogy a probléma az eszközök IP-címzésével van-e, mert ez egy gyakran előforduló hálózati probléma.

Az IP-címzés ellenőrzése gyakori feladat a hálózatépítés során a végpontok közötti kapcsolat ellenőrzéséhez és hibaelhárításához. A Windows 10 rendszerben az IP-címzés részletei a **Hálózati és megosztási központ** elemből kérhetők le, ahol gyorsan megtekinthető a négy legfontosabb beállítás: cím, maszk, alapértelmezett átjáró és DNS (lásd ábra).



Egy Windows számítógépen a hálózati rendszergazdák általában a **ipconfig** parancs használatával tekinthetik meg az IP-címzési információkat az ábra parancskimenetén látható módon.

C:\Users\PC-A> **ipconfig**

Windows IP Configuration

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16

IPv4 Address. . . . . . . . . . . : 192.168.10.10

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.10.1

(Output omitted)

Használjuk a **ipconfig /all** parancsot a MAC-cím, valamint a 3. rétegbeli címzéssel kapcsolatos részletetek megtekintéséhez a parancskimeneten látható módon.

C:\Users\PC-A> **ipconfig /all**

Windows IP Configuration

Host Name . . . . . . . . . . . . : PC-A-00H20

Primary Dns Suffix . . . . . . . : cisco.com

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

WINS Proxy Enabled. . . . . . . . : No

DNS Suffix Search List. . . . . . : cisco.com

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265

Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)

IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM

Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM

Default Gateway . . . . . . . . . : 192.168.10.1

DHCP Server . . . . . . . . . . . : 192.168.10.1

DHCPv6 IAID . . . . . . . . . . . : 100177090

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A

DNS Servers . . . . . . . . . . . : 192.168.10.1

NetBIOS over Tcpip. . . . . . . . : Enabled

Ha egy állomás DHCP-kliensnek van beállítva, az IP-cím konfigurációja megújítható a **ipconfig /release** és a **ipconfig /renew** parancsok használatával a parancskimeneten látható módon.

C:\Users\PC-A> **ipconfig /release**

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16

Default Gateway . . . . . . . . . :

(Output omitted)

C:\Users\PC-A> **ipconfig /renew**

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16

IPv4 Address. . . . . . . . . . . : 192.168.1.124

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

(Output omitted)

C:\Users\PC-A>

A Windows PC DNS-kliens szolgáltatása a memóriában tárolja a korábban már feloldott neveket és ezáltal javítja a névfeloldás teljesítményét. Az **ipconfig /displaydns** utasítás egy Windows számítógép gyorsítótárának DNS-bejegyzéseit mutatja meg a parancskimeneten is látható módon.

C:\Users\PC-A> **ipconfig /displaydns**

Windows IP Configuration

(Output omitted)

netacad.com

----------------------------------------

Record Name . . . . . : netacad.com

Record Type . . . . . : 1

Time To Live . . . . : 602

Data Length . . . . . : 4

Section . . . . . . . : Answer

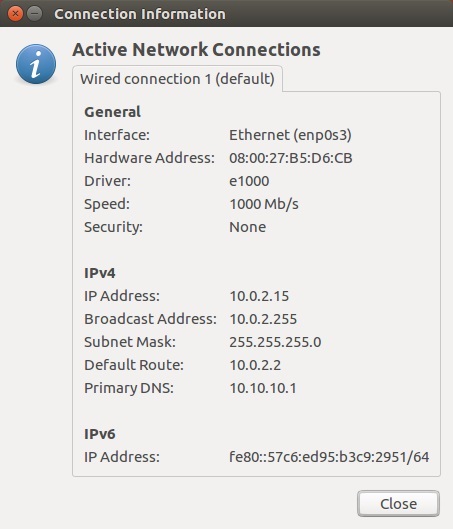
A (Host) Record . . . : 54.165.95.219

(Output omitted)

17.5.2

## IP-konfiguráció Linux számítógépen

Egy Linux számítógépen az IP-beállítások GUI használatával történő ellenőrzése a Linux disztribúciótól és az asztali felület típusától függ. Az ábrán egy Gnome asztalt futtató Ubuntu **Connection Information** párbeszédpanel látható.



Parancssorban a hálózati rendszergazdák az **ifconfig** utasítással jelenítik meg az aktív interfészek állapotát és IP-konfigurációját ahogy a parancskimeneten is látható.

[analyst@secOps ~]$ **ifconfig**

enp0s3 Link encap:Ethernet HWaddr 08:00:27:b5:d6:cb

inet addr: 10.0.2.15 Bcast:10.0.2.255 Mask: 255.255.255.0

inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0

TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:1855455014 (1.8 GB) TX bytes:13140139 (13.1 MB)

lo: flags=73 mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10

loop txqueuelen 1000 (Local Loopback)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

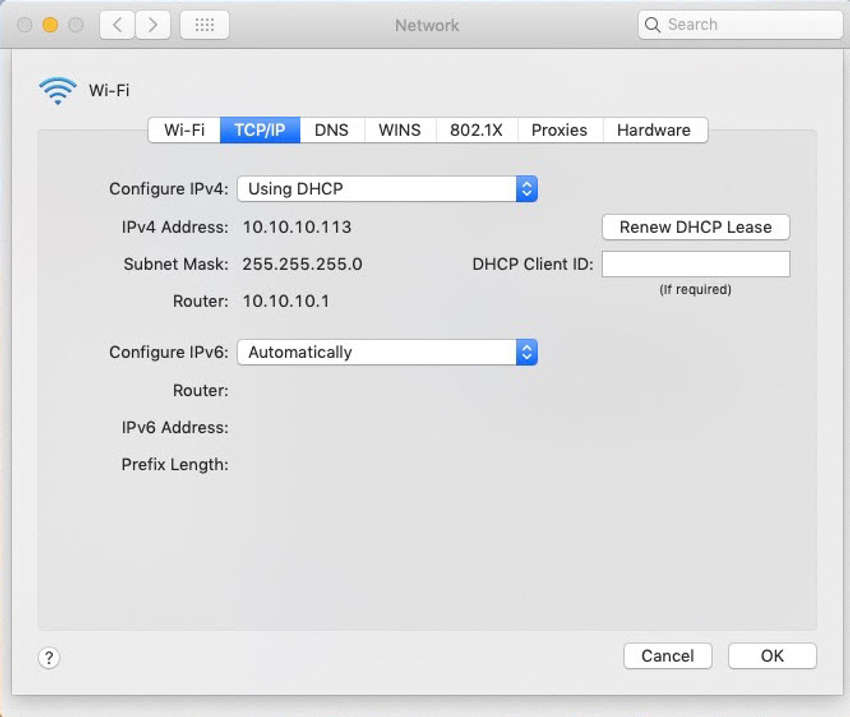
A Linux **ip address** parancs a címek és tulajdonságaik megjelenítésére szolgál. Használható még IP-címek megadására vagy törlésére is.

**MEGJEGYZÉS:** A megjelenített kimenet Linux disztribúciótól függően változhat.

17.5.3

## IP-konfiguráció macOS számítógépen

Egy Mac számítógép grafikus felületén nyissuk meg a **Network Preferences > Advanced** menüpontot az IP-címzési információk megjelenítéséhez az ábrán látható módon.



Az interfész IP-konfigurációjának ellenőrzéséhez használható még az **ifconfig** parancs is a parancskimeneten látható módon.

MacBook-Air:~ Admin$ **ifconfig en0**

en0: flags=8863 mtu 1500

ether c4:b3:01:a0:64:98

inet6 fe80::c0f:1bf4:60b1:3adb%en0 prefixlen 64 secured scopeid 0x5

inet 10.10.10.113 netmask 0xffffff00 broadcast 10.10.10.255

nd6 options=201

media: autoselect

status: active

MacBook-Air:~ Admin$

További hasznos macOS-parancsok az IP-beállítások ellenőrzésére a **networksetup -listallnetworkservices** és a **networksetup -getinfo <** network service**>,** ahogy a parancskimeneten is látható.

MacBook-Air:~ Admin$ **networksetup -listallnetworkservices**

An asterisk (\*) denotes that a network service is disabled.

iPhone USB

Wi-Fi

Bluetooth PAN

Thunderbolt Bridge

MacBook-Air:~ Admin$

MacBook-Air:~ Admin$ **networksetup -getinfo Wi-Fi**

DHCP Configuration

IP address: 10.10.10.113

Subnet mask: 255.255.255.0

Router: 10.10.10.1

Client ID:

IPv6: Automatic

IPv6 IP address: none

IPv6 Router: none

Wi-Fi ID: c4:b3:01:a0:64:98

MacBook-Air:~ Admin$

17.5.4

## Az arp parancs

Az **arp** parancs futtatható Windows, Linux és macOS parancssorban is. A parancs felsorolja az állomás ARP-gyorsítótárában lévő összes eszközt, beleértve azok IPv4-címét, fizikai címét és a cím típusát (statikus/dinamikus).

Tekintsük meg az ábrán látható minta topológiát.

five hosts with IP addresses 10.0.0.1/24, 10.0.0.2/24, 10.0.0.3/24, 10.0.0.4/24, and 10.0.0.5/24 are connected to a switch connected to a router with an IP address of 10.0.0.254/24

10.0.0.254/24 10.0.0.1/24 10.0.0.2/24 10.0.0.3/24 10.0.0.4/24 10.0.0.5/24

PC-A

Az ábra a PC-A Windows állomáson kiadott **arp -a** parancskimenetét mutatja.

C:\Users\PC-A> **arp -a**

Interface: 192.168.93.175 --- 0xc

Internet Address Physical Address Type

10.0.0.2 d0-67-e5-b6-56-4b dynamic

10.0.0.3 78-48-59-e3-b4-01 dynamic

10.0.0.4 00-21-b6-00-16-97 dynamic

10.0.0.254 00-15-99-cd-38-d9 dynamic

Az **arp -a** parancs megjeleníti az összes ismert IP-címet és a hozzájuk tartozó MAC-címet. Figyeljük meg, hogy a 10.0.0.5 IP-cím nem szerepel a listában. Az ARP-gyorsítótár csak azoknak az eszközöknek az információit tartalmazza, amelyekhez mostanában történt hozzáférés.

A cache feltöltéséhez **ping** eljük meg a kívánt eszközt, így biztosan lesz bejegyzés hozzá az ARP-táblában. Ha például PC-A megpingeli a 10.0.0.5 címet, akkor az ARP-gyorsítótár tartalmazni fog egy bejegyzést ehhez az IP-címhez.

A gyorsítótár a **netsh interface ip delete arpcache** paranccsal törölhető, ha a hálózati rendszergazda szeretné friss információkkal újratölteni azt.

**MEGJEGYZÉS**: Az **netsh interface ip delete arpcache** parancs használatához szükség lehet rendszergazdai hozzáférésre az állomáson.

17.5.5

## Gyakori show parancsok

Az állomások konfigurációjának vizsgálatához hasonlóan a közvetítő eszközök interfészeinek ellenőrzéséhez is rendelkezésre állnak utasítások és segédprogramok. A Cisco IOS-ben számos parancs szolgál a router és a switch interfészeinek ellenőrzésére.

A Cisco IOS parancssori felületén (CLI) a **show** parancsok használhatók az eszközök konfigurációjával és működésével kapcsolatos információk megjelenítésére. A hálózati szakemberek sokszor használják a **show** parancsokat a konfigurációs fájlok megtekintéséhez, az eszközök interfészeinek és folyamatainak állapotellenőrzéséhez és az eszköz működőképességének vizsgálatához. A router szinte minden folyamatának és funkciójának állapota megjeleníthető valamelyik **show** parancs segítségével.

A táblázatban a gyakran használt **show** parancsok és azok használatának célja szerepel.

| **Command** | **Useful for …** |
| --- | --- |
| **show running-config** | To verify the current configuration and settings |
| **show interfaces** | To verify the interface status and see if there are any error messages |
| **show ip interface** | To verify the Layer 3 information of an interface |
| **show arp** | To verify the list of known hosts on the local Ethernet LANs |
| **show ip route** | To verify the Layer 3 routing information |
| **show protocols** | To verify which protocols are operational |
| **show version** | To verify the memory, interfaces, and licences of the device |

Kattintsunk a gombokra az egyes parancsokhoz tartozó példák megtekintéséhez! MEGJEGYZÉS: Egyes parancsok kimenete rövidítésre került, hogy a megfelelő beállításokra fókuszáljon.

**show running-config**

Megjeleníti az aktuális konfigurációt és beállításokat

R1# **show running-config**

(Output omitted)

!

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname R1

!

interface GigabitEthernet0/0/0

description Link to R2

ip address 209.165.200.225 255.255.255.252

negotiation auto

!

interface GigabitEthernet0/0/1

description Link to LAN

ip address 192.168.10.1 255.255.255.0

negotiation auto

!

router ospf 10

network 192.168.10.0 0.0.0.255 area 0

network 209.165.200.224 0.0.0.3 area 0

!

banner motd ^C Authorized access only! ^C

!

line con 0

password 7 14141B180F0B

login

line vty 0 4

password 7 00071A150754

login

transport input telnet ssh

!

end

R1#

17.5.6

## A show cdp neighbors parancs

Számos más hasznos IOS-parancs is létezik. A CDP (Cisco Discovery Protocol) a Cisco saját gyári protokollja, amely az adatkapcsolati rétegben működik. Mivel a CDP az adatkapcsolati rétegben működik, így a Cisco hálózati eszközök (pl. routerek) képesek egymásról tudomást szerezni még akkor is, ha nincs közöttük 3. rétegbeli összeköttetés.

Amikor egy Cisco eszköz elindul, a CDP alapértelmezés szerint szintén betöltődik. Ezután felderíti a CDP-t futtató szomszédos Cisco berendezéseket, függetlenül attól, hogy milyen 3. rétegbeli protokoll vagy programcsomag fut rajtuk. A CDP az eszköz hardver és szoftver információit cseréli a közvetlenül csatlakozó szomszédok között.

A CDP által szolgáltatott információk:

* **Eszközazonosítók** — A switch, router vagy más eszköz konfigurált állomásneve
* **Címlista** - Hálózati rétegbeli cím, minden támogatott protokollhoz legfeljebb egy
* **Port azonosító** - A helyi és a távoli portok nevei ASCII formátumban (pl. FastEthernet 0/0)
* **Képességek listája** — Például, hogy az adott eszköz 2. rétegbeli switch vagy 3. rétegbeli router
* **Platform** - Az eszköz hardver típusa, például Cisco 1841 sorozatú router

Figyeljük meg a topológiát és a **show cdp neighbor** parancs kimenetét.

router R3 is connected via interface G0/0/1 to switch S3 at port F0/5 which is connected to switch S4

G0/0/1 F0/5 R3 S3

S4

R3# **show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,

D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID

S3 Gig 0/0/1 122 S I WS-C2960+ Fas 0/5

Total cdp entries displayed : 1

R3#

A kimenet azt mutatja, hogy R3 GigabitEthernet 0/0/1 interfésze csatlakozik S3 FastEthernet 0/5 interfészéhez, amely egy Cisco Catalyst 2960+ switch. Figyeljük meg, hogy R3 nem gyűjtött információt S4-ről. Ez azért van, mert a CDP csak a közvetlenül csatlakoztatott Cisco eszközöket tudja felderíteni. S4 nem kapcsolódik közvetlenül R3-hoz, ezért nem szerepel a parancskimenetben.

A **show cdp neighbors detail** parancs megmutatja a szomszéd eszköz IP-címét is (az ábrán ez nem szerepel). A CDP képes megmutatni a szomszédos eszköz IP-címét akkor is, ha az nem pingelhető. Ez akkor nagyon hasznos, amikor két Cisco forgalomirányító nem képes a forgalom továbbítására a közös adatkapcsolaton. A **show cdp neighbors detail** parancs segít meghatározni a szomszédos eszköz IP-cím konfigurációs hibáját.

Akármennyire is hasznos a CDP, biztonsági kockázatot is jelenthet, mivel a hálózati infrastruktúrával kapcsolatos információkat szolgáltathat bárki számára. Sok IOS-verzió alapértelmezés szerint CDP-hirdetéseket küld ki az összes engedélyezett portján. Ajánlott, hogy a CDP csak olyan interfészeken legyen engedélyezve, amelyek más Cisco eszközökhöz csatlakoznak. A CDP-hirdetéseket le kell tiltani a felhasználói portokon.

Mivel néhány IOS-verzió alapértelmezett beállítása a CDP-hirdetések küldése, így fontos ismerni a CDP kikapcsolásának módjait. A CDP egész eszközre kiterjedő tiltásához használjuk globális konfigurációs módban a **no cdp run** parancsot. A CDP egy adott interfészen történő tiltására a **no cdp enable** interfész konfigurációs parancs szolgál.

17.5.7

## A show ip interface brief parancs

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

A **show ip interface brief** kimenete felsorolja például a router interfészeit, a hozzájuk rendelt IP-címet és a működési állapotukat.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 209.165.200.225 YES manual up up

GigabitEthernet0/0/1 192.168.10.1 YES manual up up

Serial0/1/0 unassigned NO unset down down

Serial0/1/1 unassigned NO unset down down

GigabitEthernet0 unassigned YES unset administratively down down

R1#

**A switch interfészeinek ellenőrzése**

A **show ip interface brief** parancs a switch interfészeinek állapotáról is jelentést ad (lásd parancskimenet).

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlanl 192.168.254.250 YES manual up up

FastEthernet0/l unassigned YES unset down down

FastEthernet0/2 unassigned YES unset up up

FastEthernet0/3 unassigned YES unset up up

A VLAN1 interfész a 192.168.254.250 IPv4-címmel rendelkezik, engedélyezve van és működőképes.

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

Ezzel szemben a kimenet azt mutatja, hogy a FastEthernet0/2 és a FastEthernet0/3 interfészek működőképesek. Ezt a Status és a Protocol állapotok "up" értéke jelzi.

17.5.8

## Videó - A show version parancs

A **show version** parancs az indításnál szerepet játszó hardver- és szoftverkomponensek ellenőrzésére és az esetleges hibák megkeresésére szolgál. A **show version** parancs magyarázatát tartalmazó videó megtekintéséhez kattintsunk a Lejátszás gombra!

17.5.9

## Packet Tracer feladat - Show parancsok vizsgálata

A feladatban ismétlésre kerülnek az IOS-ben leggyakrabban használt **show** parancsok. Konfigurálásra nem lesz szükség, feladatunk inkább a show parancsok kimenetének elemzése lesz.

[A show parancs vizsgálata](https://contenthub.netacad.com/courses/itn/_common/17.5.9-packet-tracer---interpret-show-command-output_hu-HU.pka)

[17.4](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Kapcsolatok ellenőrzése](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hibaelhárítási módszerek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           

1. Kisméretű hálózat építése
2. Hibaelhárítási módszerek

# Hibaelhárítási módszerek

17.6.1

## Alapvető hibaelhárítási módszerek

Az előző két témakörben megismerkedtünk néhány segédprogrammal és paranccsal, amelyek segítségével azonosíthatjuk a hálózat problémás területeit. Ez a hibaelhárítás fontos részét jelenti. A hálózati problémák elhárításának számos módja van. Ebben a témakörben egy strukturált hibaelhárítási folyamatot ismerhetünk meg, amely segíti a hálózati rendszergazda munkáját. Ezenkívül néhány további parancsot is megismerünk, amelyek a problémák megoldásában nyújtanak segítséget. A hálózati hibák lehetnek egészen egyszerűek vagy nagyon összetettek is, és származhatnak különböző hardveres, szoftveres vagy konfigurációs problémák valamilyen kombinációjából. Szakemberként képesnek kell lennünk a problémák vizsgálatára és a rendellenesség okának meghatározására, annak kijavítása érdekében. Ezt a folyamatot nevezzük hibaelhárításnak.

A hatékony hibaelhárítás tudományos módszereken alapul.

A folyamat a táblázatban lévő hat fő lépésből áll:

| Table caption | |
| --- | --- |
| **Lépés** | **Leírás** |
| **1. A probléma azonosítása** | * A hibaelhárítási folyamat első lépése. * Bár segédeszközök is használhatók ebben a lépésben, de a felhasználóval folytatott beszélgetés nyújt gyakran nagyon hasznos információkat. |
| **2. A lehetséges okok meghatározása.** | * A probléma azonosítása után próbáljuk megállapítani a valószínű okokat. * Gyakran több lehetséges oka is lehet egy problémának. |
| **3. Az elmélet tesztelése a hiba okának meghatározásához** | * A valószínű okok alapján teszteljük az elméletet, hogy megállapíthassuk melyik okozza a hibát. * A technikus gyakran gyors eljárásokat alkalmaz a tesztelésre, majd megvizsgálja, hogy az megoldja-e a problémát. * Ha egy gyors eljárás nem oldja meg a problémát, előfordulhat, hogy további kutatást kell végezni a pontos ok megállapításának érdekében. |
| **4. A megoldás tervének elkészítése és megvalósítása** | Miután meghatároztuk a probléma pontos okát, készítsünk cselekvési tervet a megoldásához és a folyamat megvalósításához. |
| **5. Megoldás ellenőrzése és megelőző intézkedések végrehajtása** | * Miután kijavítottuk a problémát, ellenőrizzük a teljes működőképességet. * Ha szükséges, alkalmazzunk megelőző intézkedéseket. |
| **6. A probléma, a megoldási lépések és az eredmények dokumentálása** | * A hibaelhárítás utolsó szakasza a feltárt okok, az elvégzett tevékenységek és a következmények dokumentálása. * Ez nagyon fontos a jövőbeli tevékenységek szempontjából. |

A probléma felmérésekor először állapítsuk meg, hogy a hálózat hány eszközét érinti a hiba. Ha csak egyet, akkor kezdjük a hibaelhárítást azon az eszközön. Ha minden eszköz érintett, akkor kezdjük a hiba felderítését azon a berendezésen, ahová az összes többi csatlakozik. A hibák megállapításakor kövessünk mindig egy logikus és következetes eljárást, amelynek során lépésről lépésre, de egyszerre csak egy problémát hárítunk el.

17.6.2

## Megoldás vagy Továbbadás?

Bizonyos esetekben előfordulhat, hogy nem lehet azonnal megoldani a problémát. A problémát tovább kell adni, ha vezetői döntést, bizonyos speciális szakértelmet vagy hálózati hozzáférési szintet igényel a technikus számára.

Például, a hibaelhárítás során a technikus arra a következtetésre jut, hogy a router egy modulját ki kell cserélni. Ez a művelet vezetői jóváhagyást igényel. Előfordulhat, hogy a vezetőnek is tovább kell adnia az igényt, mivel az új modul megvásárlása előtt szükség lehet a pénzügyi részleg jóváhagyására.

A vállalati szabályozásnak pontosan meg kell határoznia, hogy a technikusnak mikor és hogyan kell továbbadnia egy problémát.

17.6.3

## A debug parancs

Az operációs rendszer folyamatai, a protokollok és az események üzeneteket generálnak állapotuk jelzésére. Ezek az üzenetek értékes információkat nyújthatnak a rendszer hibaelhárítása vagy ellenőrzése során. Az IOS **debug** parancsa lehetővé teszi a rendszergazda számára, hogy ezeket az üzeneteket valós időben jelenítse meg elemzés céljából. Ez egy nagyon fontos eszköz a rendszer működésének megfigyelésére Cisco IOS eszközökön.

Minden **debug** parancsot EXEC módban kell futtatni. A Cisco IOS lehetővé teszi a **debug** parancs kimenetének szűrését, hogy csak a releváns funkcióhoz tartozó információk jelenjenek meg. Ez fontos, mert a hibakereső folyamatokat a processzor magas prioritással futtatja, alkalmazásuk használhatatlanná teheti a rendszert. Emiatt csak speciális problémák elhárításához használjuk a **debug** parancsokat.

Cisco routeren az ICMP-üzenetek állapotának figyeléséhez használjuk a **debug ip icmp** parancsot a példában látható módon.

R1# **debug ip icmp**

ICMP packet debugging is on

R1#

R1# **ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R1#

\*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

R1#

A hibakeresési parancsok rövid leírásának megjelenítéséhez használjuk a **debug ?** parancsot EXEC módban.

A hibakeresés megszakításához használjuk a **no** kulcsszót a **debug** parancs előtt:

Router# **no debug ip icmp**

Alternatív megoldásként használhatjuk az **undebug** formát is:

Router# **undebug ip icmp**

Az összes aktív hibakeresési folyamat egyszerre történő kikapcsolásához használjuk az **undebug all** parancsot:

Router# **undebug all**

Legyünk óvatosak a **debug** parancs használatával. Például a **debug all** és a **debug ip packet** jelentős mennyiségű kimenet generál, és a rendszer erőforrásainak jelentős részét felhasználhatja. A routert annyira lefoglalhatja a **debug** üzenetek megjelenítése, hogy nem marad elegendő erőforrása a hálózati funkciók végrehajtásához, vagy akár a hibakeresési funkció kikapcsolásához. Ezért ezen paraméterek nem ajánlottak, használatukat kerülni kell.

17.6.4

## A terminal monitor parancs

Az IOS parancssori interfészéhez való hozzáférést biztosító kapcsolatok a következő két módon hozhatók létre:

* **Helyileg** - A helyi kapcsolat (pl. konzol kapcsolat) fizikai hozzáférést igényel a router vagy a switch konzol portjához egy speciális (rollover, konzol) kábellel.
* **Távolról** — A távoli kapcsolatokhoz Telnet vagy SSH használata szükséges az IP-címmel konfigurált eszközhöz való csatlakozáshoz.

Bizonyos IOS-üzenetek automatikusan megjelennek a konzol kapcsolaton, de a távoli elérésen nem. Például a **debug** parancs kimenete alapértelmezés szerint megjelenik a konzol kapcsolaton. Ugyanakkor a **debug** kimenete nem kerül kijelzésre automatikusan a távoli kapcsolatokon. Ez azért van, mert a **debug** üzenetek naplóüzenetek, amelyek nem jelennek meg a vty vonalakon.

A következő példában a felhasználó távoli kapcsolatot hozott létre Telnet segítségével R2-ről R1-re. Ezután kiadta a **debug ip icmp** parancsot. A parancs azonban nem jeleníti meg a **debug** kimenetét.

R2# **telnet 209.165.200.225**

Trying 209.165.200.225 ... Open

Authorized access only!

User Access Verification

Password:

R1> **enable**

Password:

R1# **debug ip icmp**

ICMP packet debugging is on

R1# **ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R1#

! No debug output displayed>

A naplóüzenetek terminálon (virtuális konzolon) történő megjelenítéséhez használjuk a **terminal monitor** EXEC parancsot. A terminálon megjelenő naplóüzenetek leállításához használjuk a **terminal no monitor** parancsot.

Figyeljük meg, hogy a **terminal monitor** parancs kiadása után a **ping** hatására a **debug** megjeleníti a kimenetet.

R1# **terminal monitor**

R1# **ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms

R1#

\*Aug 20 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*\*Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*\*Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*\*Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

\*\*Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0 topoid 0

R1# **no debug ip icmp**

ICMP packet debugging is off

R1#

**MEGJEGYZÉS**: A \*\*debug\*\* használatának célja a valós idejű megfigyelés rövid intervallumban (néhány másodperctől egy percig). Mindig tiltsuk le a \*\*debug\*\* parancsot, ha nincs szükség rá.

17.6.5

## Tudáspróba - Hibaelhárítási módszerek

Az űrlap teteje

Check your understanding of troubleshooting methodologies by choosing the BEST answer to the following questions.

1. A technician is troubleshooting a network problem and has just established a theory of probable causes. What would be the next step in the troubleshooting process?

Az űrlap alja

A technician is troubleshooting a network problem. After troubleshooting, the technician concludes that a switch should be replaced. What should the technician do next?

A technician is using the **debug ip icmp** privileged EXEC command to capture live router output. Which commands would stop this **debug** command on a Cisco router? (Choose two.)

A technician has established a remote connection to router R1 to observe **debug** output. The technician enters the **debug ip icmp** command then pings a remote destination. However, no output is displayed. Which command would the technician have to enter to display log messages on a remote connection?

[17.5](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Számítógépes és IOS parancsok](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hibaelhárítási forgatókönyvek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                

1. Kisméretű hálózat építése
2. Hibaelhárítási forgatókönyvek

# Hibaelhárítási forgatókönyvek

17.7.1

## A duplex működés és problémái

Számos gyakori hálózati probléma könnyen beazonosítható és megoldható. Most, hogy már ismerjük a hálózati hibaelhárítás eszközeit és folyamatát, ebben a témakörben megvizsgálunk néhány gyakori hálózati problémát, amelyekkel hálózati rendszergazdaként valószínűleg találkozni fogunk.

Az adatkommunikációban a duplex kifejezés a két eszköz közötti adatátvitel irányára utal.

Kétféle duplex kommunikációs mód létezik:

* **Félduplex** - A kommunikáció egyidejűleg csak egy irányban történik.
* **Full-duplex** - A kommunikációban egyszerre történik a küldés és a fogadás.

Az ábra azt szemlélteti, hogyan működnek az egyes duplex módszerek.

The figure is a comparison of half-duplex versus full-duplex communications. The top diagram shows half-duplex communication. Switch S1 is connected to switch S2 with an arrow flowing from S1 to S2 indicating a device can send or receive. The bottom diagram shows-full duplex communication. Switch S1 is connected to switch S2 with arrows pointing in both directions indicating a device can send AND receive simultaneously.

S2 S1 S2

S1

Full-Duplex CommunicationHalf-Duplex CommunicationSend **OR** receiveSend **AND** receive simultaneously

Az egymáshoz kapcsolódó Ethernet interfészeknek ugyanabban a duplex módban kell működniük a legjobb teljesítmény, valamint a kapcsolati problémák és késleltetések elkerülése érdekében.

Az Ethernet automatikus egyeztetés (autonegotiation) funkciója megkönnyíti a konfigurációt, minimalizálja a problémákat és maximalizálja a kapcsolat teljesítményét az összeköttetésen. A csatlakoztatott eszközök először bejelentik a támogatott képességeiket, majd kiválasztják a mindkét végen támogatott legmagasabb teljesítményű üzemmódot. Például az ábrán látható switch és router sikeresen egyeztette a teljes duplex módot.

S1

R1

I can operate in full-duplex ...I can operate in full-duplex ...F0/5G0/0/1

Ha két csatlakoztatott eszköz egyike teljes duplex, a másik pedig félduplex módban működik, duplexitás hiba következik be. Amíg az adatkommunikáció ilyen hibás kapcsolaton keresztül folyik, a hálózat sebessége nagyon alacsony lesz.

A duplexitás eltéréseket általában egy rosszul konfigurált interfész okozza, vagy ritkán egy sikertelen automatikus egyeztetés. Az ilyen hibák azonosítása nehézkes lehet, mivel az eszközök közötti kommunikáció továbbra is fennáll.

17.7.2

## IP-címzési problémák az IOS-ben

Az IP-címzéssel kapcsolatos hibák valószínűleg megakadályozzák a hálózati eszközök közötti kommunikációt. Mivel az IP-címek hierarchikusak, a hálózati berendezésekhez rendelt IP-címnek illeszkednie kell az adott hálózat címtartományához. A rosszul hozzárendelt IP-címek számos problémát okoznak, beleértve az IP-cím ütközéseket és a forgalomirányítási problémákat.

A helytelen IPv4-hozzárendelés két gyakori oka a kézi beállítás hibája vagy a DHCP-vel kapcsolatos problémák.

A hálózati rendszergazdáknak gyakran manuálisan kell IP-címeket hozzárendelniük eszközökhöz (pl a szerverekhez és routerekhez).. Ha hiba történik a hozzárendelés során, akkor valószínűleg kommunikációs problémák fognak jelentkezni.

IOS-eszközön a **show ip interface** vagy a **show ip interface brief** parancsokkal ellenőrizhetjük, hogy milyen IPv4-címek vannak hozzárendelve a hálózati interfészekhez. Például a **show ip interface** **brief** parancs kiadása után az ábrán látható módon jelenik meg az interfészek állapota az R1-en.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 209.165.200.225 YES manual up up

GigabitEthernet0/0/1 192.168.10.1 YES manual up up

Serial0/1/0 unassigned NO unset down down

Serial0/1/1 unassigned NO unset down down

GigabitEthernet0 unassigned YES unset administratively down down

R1#

17.7.3

## IP-címzési problémák végberendezéseken

Windows rendszerű számítógépeken, amikor az eszköz nem tud kapcsolatba lépni egyetlen DHCP-kiszolgálóval sem, a Windows automatikusan hozzárendel egy 169.254.0.0/16 tartományhoz tartozó címet. Ez a funkció az úgynevezett automatikus privát IP-címzés (APIPA), amelynek célja, hogy megkönnyítse a kommunikációt a helyi hálózaton belül. Képzeljük azt, mintha a Windows ezt mondaná: „A 169.254.0.0/16 tartománybeli címemet fogom használni, mert nem tudtam más címhez jutni”.

Gyakran előfordul, hogy az APIPA-címmel rendelkező számítógép nem tud kommunikálni a hálózat más eszközeivel, mivel ezek az eszközök valószínűleg nem tartoznak a 169.254.0.0/16 hálózathoz. Ez a helyzet egy automatikus címhozzárendelés problémát jelez, amelyet meg kell oldani.

**MEGJEGYZÉS**: Más operációs rendszerek, mint például a Linux vagy az OS X, nem rendelnek IPv4-címet a hálózati interfészhez, ha a DHCP-kiszolgálóval való kommunikáció sikertelen.

A legtöbb végberendezés úgy van konfigurálva, hogy egy DHCP-kiszolgálóra támaszkodjon az IPv4-cím automatikus hozzárendeléséhez. Ha az eszköz nem tud kommunikálni a DHCP-szerverrel, akkor a kiszolgáló nem tud IPv4-címet biztosítani az adott hálózathoz, így az eszköz nem tud kommunikálni.

Egy Windows számítógéphez rendelt IP-cím ellenőrzéséhez használjuk az **ipconfig** parancsot (lásd parancskimenet).

C:\Users\PC-A> **ipconfig**

Windows IP Configuration

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16

IPv4 Address. . . . . . . . . . . : 192.168.10.10

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.10.1

(Output omitted)

17.7.4

## Alapértelmezett átjáró hibák

Egy végberendezés alapértelmezett átjárója az a legközelebbi hálózati eszköz, amely továbbítja a forgalmat más hálózatokba. Ha egy eszköz hibás vagy nem létező alapértelmezett átjáró címmel rendelkezik, akkor nem lesz képes kommunikálni a távoli hálózatokban lévő berendezésekkel. Mivel az alapértelmezett átjáró a távoli hálózatok felé vezető útvonal első állomása, a címnek ugyanahhoz a hálózathoz kell tartoznia, mint amihez a végberendezés.

Az alapértelmezett átjáró címe beállítható manuálisan vagy beszerezhető egy DHCP-kiszolgálótól. Az IPv4-címzéssel kapcsolatos hibákhoz hasonlóan az alapértelmezett átjáró problémák is a helytelen konfigurációhoz (kézi hozzárendelés esetén) vagy DHCP-problémákhoz kapcsolódhatnak.

Az ilyen hibák megoldásához először győződjünk meg arról, hogy az eszköz rendelkezik-e a megfelelő alapértelmezett átjáróval. Ha a cím manuálisan lett beállítva, de helytelenül, akkor egyszerűen cseréljük ki a megfelelő címre. Ha a címhozzárendelés automatikus, győződjünk meg arról, hogy az eszköz képes-e kommunikálni a DHCP-kiszolgálóval. Fontos ellenőrizni azt is, hogy megfelelő IPv4-cím és alhálózati maszk van-e beállítva a router interfészén, és hogy az interfész aktív-e.

Windows alapú számítógépek alapértelmezett átjárójának ellenőrzéséhez használjuk az **ipconfig** parancsot.

C:\Users\PC-A> **ipconfig**

Windows IP Configuration

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16

IPv4 Address. . . . . . . . . . . : 192.168.10.10

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.10.1

(Output omitted)

Router esetén használjuk a **show ip route** parancsot az irányítótábla listázásához és ellenőrizzük, hogy az alapértelmezett átjáró, az úgynevezett alapértelmezett útvonal be van-e állítva. Ezt az útvonalat abban az esetben használják a routerek, ha az irányítótáblában egyetlen útvonal sem felel meg a csomag cél IP-címének.

A példában az látható, hogy R1 rendelkezik alapértelmezett útvonallal (Gateway of last resort, végső átjáró), amely a 209.168.200.226 IP-címre mutat.

R1# **show ip route | begin Gateway**

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

O\*E2 0.0.0.0/0 [110/1] via 209.165.200.226, 02:19:50, GigabitEthernet0/0/0

10.0.0.0/24 is subnetted, 1 subnets

O 10.1.1.0 [110/3] via 209.165.200.226, 02:05:42, GigabitEthernet0/0/0

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/1

209.165.200.0/24 is variably subnetted, 3 subnets, 2 masks

C 209.165.200.224/30 is directly connected, GigabitEthernet0/0/0

L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0

O 209.165.200.228/30

[110/2] via 209.165.200.226, 02:07:19, GigabitEthernet0/0/0

R1#

Az első sorban az látható, hogy bármely (azaz 0.0.0.0) célcímhez tartozó átjáró a 209.165.200.226 IP-cím. A második kiemelés azt mutatja, hogyan ismerte meg R1 az alapértelmezett útvonalat. Ebben az esetben R1 egy másik OSPF-routertől kapta az információt.

17.7.5

## DNS hibaelhárítás

A DNS (Domain Name System) egy olyan automatizált szolgáltatás, amely tartományneveket (például [www.cisco.com](http://www.cisco.com)) feleltet meg IP-címeknek. Bár a DNS-névfeloldás nem döntő jelentőségű az eszköz kommunikációjához, nagyon fontos a végfelhasználók számára.

Egy internetes link működését a felhasználók gyakran tévesen kapcsolják a DNS elérhetőségéhez. A „hálózat leállt” vagy „nincs internet” típusú panaszokat okozhatja egy elérhetetlen DNS-kiszolgáló is. Bár a forgalomirányítás és az összes többi hálózati szolgáltatás működőképes, DNS-hibák miatt gyakran téves következtetésre jutnak a felhasználók. Ha egy felhasználó beír a webböngészőbe egy tartománynevet (például [www.cisco.com](http://www.cisco.com)), de a DNS-kiszolgáló nem érhető el, a név nem lesz lefordítva IP-címre, így a weboldal nem jelenik meg.

A DNS-kiszolgálók címei manuálisan vagy automatikusan is megadhatók. Általában a hálózati rendszergazdák felelősek a DNS-kiszolgálók címeinek manuális hozzárendeléséért szerverek és más eszközök esetében. Míg az ügyfél számítógépekhez DHCP segítségével automatikusan hozzárendelhetők a DNS-kiszolgálói címek.

Bár a vállalatok és szervezetek gyakran saját DNS-kiszolgálókat üzemeltetnek, a nevek feloldására minden elérhető DNS-szerver használható. A kisméretű irodai és otthoni (SOHO) felhasználók az internetszolgáltató által fenntartott DNS-kiszolgálóra támaszkodnak a névfeloldáshoz. Az internetszolgáltató DHCP-n keresztül rendeli hozzá a SOHO-ügyfelekhez az általa karbantartott DNS-kiszolgálókat. Ezenkívül a Google nyilvános DNS-kiszolgálót tart fenn, amelyet bárki használhat, és nagyon hasznos a teszteléshez. A Google nyilvános DNS-kiszolgálójának IPv4-címe 8.8.8.8, IPv6-címe pedig 2001:4860:4860::8888.

A Cisco az OpenDNS-t kínálja, amely biztonságos DNS-szolgáltatást nyújt az adathalászat és néhány rosszindulatú webhely szűrésével. A 208.67.222.222 és 208.67.220.220 címeket használhatjuk az Elsődleges és Másodlagos DNS-kiszolgáló mezőkben. További speciális funkciók, például webes tartalomszűrés és biztonság, érhetők el a családok és a vállalkozások számára.

Az **ipconfig /all** parancs segítségével ellenőrizhetjük, hogy melyik DNS-kiszolgálót használja a Windows számítógép.

C:\Users\PC-A> **ipconfig /all**

(Output omitted)

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265

Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)

IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM

Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM

Default Gateway . . . . . . . . . : 192.168.10.1

DHCP Server . . . . . . . . . . . : 192.168.10.1

DHCPv6 IAID . . . . . . . . . . . : 100177090

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A

DNS Servers . . . . . . . . . . . : 208.67.222.222

NetBIOS over Tcpip. . . . . . . . : Enabled

(Output omitted)

Az **nslookup** parancs egy másik hasznos DNS-hibaelhárító eszköz a PC-ken. Az **nslookup** használatával a felhasználó DNS-lekérdezéseket indíthat, és elemezheti a DNS-választ. Az **nslookup** parancs kimenete megjeleníti a [www.cisco.com](http://www.cisco.com) lekérdezésének eredményét. Figyeljük meg, hogy IP-címet is megadhatunk, és az **nslookup** feloldja a nevet.

C:\Users\PC-A> **nslookup**

Default Server: Home-Net

Address: 192.168.1.1

> **cisco.com**

Server: Home-Net

Address: 192.168.1.1

Non-authoritative answer:

Name: cisco.com

Addresses: 2001:420:1101:1::185

72.163.4.185

> **8.8.8.8**

Server: Home-Net

Address: 192.168.1.1

Name: dns.google

Address: 8.8.8.8

>

> **208.67.222.222**

Server: Home-Net

Address: 192.168.1.1

Name: resolver1.opendns.com

Address: 208.67.222.222

>

17.7.6

## Laborgyakorlat - Kapcsolódási problémák elhárítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* A probléma azonosítása
* Hálózati változások végrehajtása
* A teljes működőképesség ellenőrzése
* Az eredmények és konfigurációs változások dokumentálása

17.7.7

## Packet Tracer feladat — Kapcsolódási problémák elhárítása

A Packet Tracer feladat célja a csatlakozási problémák felderítése és megoldása, ha lehetséges. Ellenkező esetben a hibajelenséget egyértelműen dokumentálni kell, így lehet további feldolgozásra átadni.

[Kapcsolati hibák elhárítása](https://contenthub.netacad.com/courses/itn/_common/17.7.7-packet-tracer---troubleshoot-connectivity-issues_hu-HU.pka)

[17.6](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hibaelhárítási módszerek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[17.8](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

# Introduction to Networks

v7.0

[Skip to content](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU#chunks-container)

1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     
2. Kisméretű hálózat építése
3. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

17.8.1

## Laborgyakorlat - Kisvállalati hálózat tervezése és kivitelezése

A laborgyakorlat során egy hálózatot fogunk megtervezni és kiépíteni.

17.8.2

## Packet Tracer – Komplex képességmérő feladat

Ebben a Packet Tracer feladatban minden olyan készséget használni fogunk, amelyet a kurzusben szereztünk.

[Komplex képességmérő feladat](https://contenthub.netacad.com/courses/itn/_common/17.8.2-packet-tracer---skills-integration-challenge_hu-HU.pka)

17.8.3

## Packet Tracer - Komplex hibaelhárítási feladat

Ebben a Packet Tracer feladatban számos hálózati problémát fogunk feltárni és megoldani.

[Hibaelhárítási feladat](https://contenthub.netacad.com/courses/itn/_common/17.8.3-packet-tracer---troubleshooting-challenge_hu-HU.pka)

17.8.4

## Miről tanultunk ebben a fejezetben?

**Kisméretű hálózatok eszközei**

A kisméretű hálózatok internet kapcsolata általában egyetlen WAN-csatlakozás, amely DSL, kábel vagy Ethernet szolgáltatáson keresztül valósul meg. A kisméretű hálózatokat helyi informatikai technikus vagy szerződéses szakember kezeli. A kisméretű hálózat hálózati eszközeinek kiválasztásakor figyelembe kell venni a költségeket, a sebességet és a portok/interfészek típusát, a bővíthetőséget és az operációs rendszer funkcióit és szolgáltatásait. A hálózat megvalósításához hozzunk létre egy IP-címzési sémát, és használjuk azt a végberendezéseken, a kiszolgálókon és a perifériákon, valamint a közvetítő eszközökön. A hálózati redundancia megvalósításának módja a berendezések másodpéldányainak telepítése és az összeköttetések többszörözése. A kisméretű hálózatokban a routereket és switch-eket úgy kell konfigurálni, hogy a valós idejű forgalmat (például a hang- és a videó átvitel) az egyéb adatforgalomtól elválasztva kezeljék. Egy jó hálózati tervben a forgalom prioritás alapján kerül osztályozásra (QoS).

**Kisméretű hálózatok alkalmazásai és protokolljai**

Kétféle szoftver vagy folyamat van, ami hozzáférést biztosít a hálózathoz: a hálózati alkalmazások és az alkalmazási rétegbeli szolgáltatások. Néhány felhasználói program olyan alkalmazási rétegbeli protokollokat használ, amelyek képesek kommunikálni az alsóbb rétegekkel. Ilyen alkalmazások például az email kliensek és a böngészőprogramok. Más programoknak az alkalmazási réteg szolgáltatásai nyújtanak segítséget az olyan hálózati erőforrások használatához, mint a fájl átvitel vagy a hálózati nyomtatás. Ezek a szolgáltatások teremtenek kapcsolatot a hálózattal és készítik elő az adatokat az átvitelre. A két leggyakoribb távelérési megoldás a Telnet és az SSH (Secure Shell). Az SSH-szolgáltatás a Telnet biztonságos alternatívája. A hálózati rendszergazdáknak ismerniük kell a hálózati kiszolgálókat és a kapcsolódó protokollokat, például a web-, az e-mail, az FTP-, a DHCP- és a DNS-szervert. A vállalkozások egyre inkább az IP-telefónia és videó konferencia segítségével kommunikálnak az ügyfelekkel és üzleti partnerekkel. Ezek valósidejű alkalmazások A hálózati infrastruktúrának támogatnia kell a VoIP, az IP-telefon és más valós idejű szolgáltatásokat.

**Hálózatok növekedése**

A hálózat továbbfejlesztéséhez több elemre van szükség: hálózati dokumentáció, eszközleltár, költségvetés és forgalomelemzés. Ismerjük meg a hálózaton áthaladó forgalom típusát, valamint az aktuális forgalmi mutatókat. Elemezzük a forgalmat a csúcs kihasználtsági időszak során, hogy képet kapjunk a különböző forgalmi típusokról. Végezzük el a műveletet különböző hálózati szegmenseken és eszközökön is a helyi jellegzetességek felderítéséhez. A hálózati rendszergazdáknak ismerniük kell miként változik a hálózat használata. A felhasználói számítógépek használati adatait „pillanatképben” rögzíthetjük olyan eszközökkel, mint a Windows Feladatkezelő, az Eseménynapló és az Adatforgalom.

**Kapcsolatok ellenőrzése**

A **ping** parancs a leghatékonyabb módja a 3. rétegbeli kapcsolatok tesztelésének a forrás és a cél IP-cím között. A parancs válaszidő statisztikákat is megjelenít. A Cisco kiterjesztett ping parancsa lehetővé teszi a felhasználó számára, hogy speciális típusú pingeket hozzon létre a parancs paramétereinek beállításával. A használathoz EXEC módban gépeljük be a ping parancsot cél IP-cím nélkül. A Traceroute segíthet megtalálni a 3. rétegbeli problémás területeket a hálózatban. A nyomkövetés (trace) eredménye azon ugrások listája, amelyek a csomagtovábbítás során a hálózati útvonalon előfordulnak. Ezt fel lehet használni az útvonal problémás pontjának azonosításához. Windows rendszerben a parancs a **tracert**. A Cisco IOS parancs pedig a **traceroute**. Van kiterjesztett **traceroute** parancs is. Ez lehetővé teszi a rendszergazda számára a parancshoz kapcsolódó paraméterek beállítását. A hálózat viszonyítási alapjához különféle parancsok kimenetei szolgáltatják az adatokat. Az állapotfelmérés kezdőlépése a ping, a traceroute és egyéb fontos parancsok eredményeinek elmentése egy szövegállományba. Ezeket a szöveges fájlokat időbélyeggel kell ellátni, és lementeni egy archívumba a későbbi visszakeresés és összehasonlítás céljából.

**Számítógépes és IOS parancsok**

A hálózati rendszergazdák az **ipconfig** parancs kiadásával tekinthetik meg az IP-címzési adatokat (cím, maszk, router és DNS) egy Windows számítógépen. Egyéb szükséges parancsok az **ipconfig /all**, az **ipconfig /release**, az **ipconfig /renew**, és az **ipconfig /displaydns**. Egy Linux számítógépen az IP-beállítások GUI használatával történő ellenőrzése a Linux disztribúciótól és az asztali felület típusától függ. A szükséges parancsok az **ifconfig**, és az **ip address**. Egy Mac számítógép grafikus felületén nyissuk meg a Network Preferences > Advanced menüpontot az IP-címzési információk megjelenítéséhez. További Mac IP-címzési parancsok az **ifconfig**, a **networksetup -listallnetworkservices** és a **networksetup -getinfo**<network service\ >. Az **arp** parancs futtatható a WIndows, Linux és macOS parancssorában is. A parancs felsorolja az állomás ARP-gyorsítótárában lévő összes eszközt, beleértve azok IPv4-címét, fizikai címét és a cím típusát (statikus/dinamikus). Az **arp -a** parancs megjeleníti az összes ismert IP-címet és a hozzájuk tartozó MAC-címet. Gyakori **show** parancsok: **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, és **show version**. A **show cdp neighbor** parancs a következő információkat tartalmazza a szomszédos CDP eszközökről: azonosító, címlista, portazonosító, képességek listája és platform. A **show cdp neighbors detail** parancs segít meghatározni a szomszédos CDP eszköz IP-cím konfigurációs hibáját. A **show ip interface brief** parancs kimenete felsorolja a router interfészeit, a hozzájuk rendelt IP-címet és a működési állapotukat.

**Hibaelhárítási módszerek**

1. A probléma azonosítása
2. A lehetséges okok meghatározása.
3. Az elmélet tesztelése a hiba okának meghatározásához
4. A megoldás tervének elkészítése és megvalósítása
5. Megoldás ellenőrzése és megelőző intézkedések végrehajtása
6. A probléma, a megoldási lépések és az eredmények dokumentálása

A problémát tovább kell adni, ha vezetői döntést, bizonyos speciális szakértelmet vagy hálózati hozzáférési szintet igényel a technikus számára. Az operációs rendszer folyamatai, a protokollok és az események üzeneteket generálnak állapotuk jelzésére. Az IOS **debug** parancsa lehetővé teszi a rendszergazda számára, hogy ezeket az üzeneteket valós időben jelenítse meg elemzés céljából. A naplóüzenetek terminálon (virtuális konzolon) történő megjelenítéséhez használjuk a **terminal monitor** EXEC parancsot.

**Hibaelhárítási forgatókönyvek**

Kétféle duplex kommunikációs mód létezik: félduplex és teljes duplex. Ha két csatlakoztatott eszköz egyike teljes duplex, a másik pedig félduplex módban működik, duplexitás hiba következik be. Amíg az adatkommunikáció ilyen hibás kapcsolaton keresztül folyik, a hálózat sebessége nagyon alacsony lesz.

A rosszul hozzárendelt IP-címek számos problémát okoznak, beleértve az IP-cím ütközéseket és a forgalomirányítási problémákat. A helytelen IPv4-hozzárendelés két gyakori oka a kézi beállítás hibája vagy a DHCP-vel kapcsolatos problémák. A legtöbb végberendezés úgy van konfigurálva, hogy egy DHCP-kiszolgálóra támaszkodjon az IPv4-cím automatikus hozzárendeléséhez. Ha az eszköz nem tud kommunikálni a DHCP-szerverrel, akkor a kiszolgáló nem tud IPv4-címet biztosítani az adott hálózathoz, így az eszköz nem tud kommunikálni.

Egy végberendezés alapértelmezett átjárója az a legközelebbi hálózati eszköz, amely továbbítja a forgalmat más hálózatokba. Ha egy eszköz hibás vagy nem létező alapértelmezett átjáró címmel rendelkezik, akkor nem lesz képes kommunikálni a távoli hálózatokban lévő berendezésekkel. Mivel az alapértelmezett átjáró a távoli hálózatok felé vezető útvonal első állomása, a címnek ugyanahhoz a hálózathoz kell tartoznia, mint amihez a végberendezés.

A DNS-hibák gyakran arra engedik következtetni a felhasználót, hogy a hálózat leállt. Ha egy felhasználó beír a webböngészőbe egy tartománynevet (például [www.cisco.com](http://www.cisco.com)), de a DNS-kiszolgáló nem érhető el, a név nem lesz lefordítva IP-címre, így a weboldal nem jelenik meg.

17.8.5

## Ellenőrző kvíz - Kisméretű hálózat építése

Az űrlap teteje

1. Melyik hálózattervezési szempont fontosabb egy nagy cég esetében, mint egy kisvállalkozásnál?

Az űrlap alja

Egy újonnan felvett hálózati technikus feladata, hogy új hardvert rendeljen egy kisvállalkozás számára, ami várhatóan nagy növekedést produkál a jövőben. Melyik szempontot kell a leginkább figyelembe vennie az eszközök kiválasztásakor?

Melyik a legnagyobb prioritású forgalomtípus a hálózaton?

Egy hálózati technikus vizsgálja a számítógép és a 10.1.1.5 címmel rendelkező állomás közötti hálózati kapcsolatot. Melyik parancs jeleníti meg a távoli állomáshoz vezető útvonalat, ha Windows PC-n adják ki?

A felhasználó nem tudja elérni a weboldalt, amikor beírja a **ht​tp://ww​w.cisco.com** címet egy webböngészőbe, de a **ht​tp://72.163.4.161**. Mi a probléma?

Hol jelenik meg alapértelmezés szerint a Cisco IOS hibakeresési üzeneteinek kimenete?

A hálózat méretezésének mely eleme foglalja magába a fizikai és logikai topológiák azonosítását?

Milyen mechanizmust lehet megvalósítani egy kis hálózatban a valós idejű adatfolyam-alkalmazások hálózati késleltetésének minimalizálása érdekében?

Melyik folyamat sikertelen, ha a számítógép nem tud hozzáférni az internethez, és a 169.254.142.5 IP-címet kapta?

Egy kisvállalkozás egyetlen forgalomirányítón keresztül csatlakozik az internetszolgáltatóhoz. Melyik megoldás alkalmas az összeköttetés fenntartására, ha a forgalomirányító vagy az ISP-kapcsolat meghibásodik?

Mikor kell a rendszergazdának elkészítenie a hálózat viszonyítási alapját?

Melyik két forgalomtípus igényel késleltetésre érzékeny kézbesítést? (Két jó válasz van.)

A hálózati technikus gyanítja, hogy egy adott, két Cisco switch közötti hálózati kapcsolatban duplexitás eltérés van. Melyik paranccsal nézheti meg a technikus a switchport 1. és 2. rétegbeli részletes információit?

Melyik állítás igaz a CDP-ről egy Cisco eszközön?​

Milyen szempontot kell figyelembe venni egy kis hálózat kialakításakor az eszközök kiválasztásánál?

[17.7](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)

[Hibaelhárítási forgatókönyvek](https://contenthub.netacad.com/itn/1.0.1?lng=hu-HU" \l "/itn/undefined.1)