* [Fejezet száma 1 Bevezetés a hálózatok méretezésébe](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html" \l "1)
* [1.0 Bevezetés a hálózatok méretezésébe](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#1.0)
* [1.0.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#1.0.1)
* [1.0.1.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#1.0.1.1)

**Bevezetés**

Ahogy egy vállalkozás növekszik, úgy nőnek a hálózattal szemben támasztott követelményei is. A működés szempontjából kritikus szolgáltatásokban a vállalkozások a hálózati infrastruktúrára támaszkodnak. A hálózati leállások bevételkiesést és az ügyfelek elvesztését eredményezhetik. A hálózat tervezőinek úgy kell egy vállalati hálózatot megtervezni és felépíteni, hogy az méretezhető és nagy rendelkezésre állású legyen.

A fejezet olyan, a magas funkcionalitású hálózatok tervezéséhez használható stratégiákat mutat be, mint a hierarchikus hálózattervezési modell, a Cisco vállalati architektúra (Cisco Enterprise Architecture), és az eszközök megfelelő kiválasztása. A hálózattervezés célja, hogy korlátozza azoknak az eszközöknek a számát, amelyek funkcionalitását egyetlen hálózati eszköz meghibásodása befolyásolhatja, tervezett növekedési pályát biztosítson, és egy megbízható hálózatot hozzon létre.

# Csoportos feladat - Hálózat tervezése

**Hálózat tervezése**

Az egyik ügyfelünk új fiókirodát nyit.

Minket jelöltek ki az új telephelyre hálózati rendszergazdának, ahol feladatunk az új fiókiroda hálózatának megtervezése és üzemeltetése.

A többi fiókiroda rednszergazdája a hálózat megtervezésekor a Cisco háromrétegű tervezési modelljét használta. Úgy döntünk, hogy mi is ezt a megközelítést alkalmazzuk.

Szeretnénk megérteni, hogy miként segítheti a tervezési folyamotot a hierarchikus modell használata, ezért utána olvasunk.

[Csoportos feladat - Network by Design](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.0.1.2%20Network%20by%20Design%20Instructions.pdf)

**Miért jó a méretezhető hálózat?**

A vállalatok a működésük szempontjából kritikus szolgáltatások terén egyre nagyobb mértékben támaszkodnak a hálózati infrastruktúrájukra. Ahogy a vállalkozások növekednek, egyre több munkavállalót alkalmaznak, fiókirodákat nyitnak és globális piacok felé terjeszkednek. Ezek a változások közvetlenül hatnak a hálózattal szemben támasztott követelményekre. Vállalatinak nevezzük a nagyszámú felhasználóval, helyszínnel és rendszerrel rendelkező üzleti környezeteket. Az üzleti vállalkozások támogatására használt hálózatokat pedig vállalati hálózatoknak.

Kattintsunk a lejátszás gombra az animáció megtekintéséhez, melyen megfigyelhetjük, hogyan növekszik egy kis hálózat vállalati hálózattá.

Egy nagyvállalati hálózatnak képesnek kell lennie az egyes üzletrészek közötti olyan, egymástól eltérő hálózati forgalomtipusok lebonyolítására, mint például az adatállományok átvitele, elektronikus levelezés, IP telefónia vagy a videó alapú alkalmazások. A vállalati hálózatok

* támogatják az üzleti szempontból kritikus alkalmazásokat,
* támogatják a konvergált hálózati forgalmat,
* szerteágazó üzleti igényeket elégítenek ki és
* központosított felügyeletet biztosítanak.

# Vállalati szintű eszközök

A felhasználók elvárják a vállalati hálózatoktól - mint amilyen például az ábrán látható -, hogy az idő 99,999 százalékában rendelkezésre álljanak. A vállalati hálózat leállásai ellehetetlenítik az üzleti folymatokat, amely bevételkieséshez, illetve ügyfelek, adatok és lehetőségek elvesztéséhez vezethet.

Az elvárt megbízhatóság teljesítésének érdekében a vállalati hálózatokban magas minőségi kategóriájú eszközöket alkalmaznak. Mivel a nagyvállalati piacra szánt eszközök általában jelentős forgalmat bonyolítanak le, ezért tervezésüket és gyártásukat szigorúbb szabványok szabályozzák, mint az alacsonyabb kategóriájú eszközökét.

A vállalati piacra szánt eszközöknél elsődleges szempont a megbízhatóság, ezért ezeknek az eszközöknek olyan jellemzőik vannak, mint például a redundáns áramellátás és automatikus hibakezelési képesség. Egy eszköz automatikus hibakezelési képessége annyit jelent, hogy egy nem működő modul, szolgáltatás vagy eszköz működőre cserélése egyáltalán nem, vagy csak kis mértékben okoz kiesést a szolgáltatásban.

A professzionális eszközök beszerzése és telepítése ugyanakkor nem helyettesítheti a körültekintő hálózati tervezést.

# Hierarchikus hálózattervezés

Egy vállalati hálózatban a sávszélesség optimalizálásához a hálózatot úgy kell kialakítani, hogy a forgalom maradjon helyi, és szükségtelenül ne terjedjen át a hálózat többi részére. A háromrétegű hierarchikus tervezési modell segít a hálózat megfelelő kialakításában.

Ez a modell a hálózati funkciókat három elkülönülő rétegre osztja (lásd 1. ábra):

* hozzáférési réteg,
* elosztási réteg,
* központi réteg.

Mindegyik rétegnek jól meghatározott feladata van.

A hozzáférési réteg a felhasználók számára nyújt hálózati kapcsolatot. Az elosztási réteg a helyi hálózatok közötti adatáramlást biztosítja. Végül, a központi réteg nagysebességű gerincréteget jelent a szétszórt hálózatok között. A felhasználói forgalom a hozzáférési rétegben keletkezik, és amennyiben szükség van rá, áthaladhat a többi rétegen is.

Bár a hierarchikus modell háromrétegű, egyes kisebb vállalati hálózatok kétszintű hierarchikus tervezést is alkalmazhatnak. A kétszintű hierarchikus tervezés egy rétegbe egyesíti a központi és az elosztási rétegeket, csökkentve ezáltal a költségeket és a komplexitást (lásd 2. ábra).

**Cisco nagyvállalati architektúra (Cisco Enterprise Architecture)**

A Cisco nagyvállalati architektúra a hálózatot funkcionális összetevőkre osztja, míg ugyanakkor megtartja a központi, elosztási és hozzáférési rétegeket. Amint az ábra mutatja, a Cisco nagyvállalati architektúra moduljai a következők:

* Vállalati kampusz (Enterprise Campus)
* Vállalati határvonal (Enterprise Edge)
* Szolgáltatói határvonal (Service Provider Edge)
* Távoli hálózatrészek (Remote)

**Vállalati kampusz (Enterprise Campus)**

A vállalati kampusz tartalmazza a teljes kampusz infrastruktúrát, beleértve a hozzáférési-, elosztási- és gerincrétegeket. A hozzáférési réteg modul 2. vagy 3. rétegbeli kapcsolókat tartalmaz a szükséges portsűrűség biztosításához. Itt kerülnek megvalósításra a VLAN-ok és az épület elosztási rétege felé vezető trönkvonalak. Fontos az épület elosztási rétegbeli kapcsolói felé a redundancia. Az elosztási rétegbeli modul 3. rétegbeli eszközökkel valósítja meg az épület szintű hozzáférést. Ebben az elosztási rétegbeli modulban kerül megvalósításra a forgalomirányítás, a hozzáférés-vezérlés és a szolgáltatásminőség (QoS). A gerincrétegbeli modul nagy sebességű kapcsolatot biztosít az elosztási réteg modulja, az adatközpont kiszolgálófarmja és a vállalati határvonal között. Ebben a modulban a redundancia, a gyors konvergencia és a hibatűrés áll a tervezés középpontjában.

Ezeken kívül a vállalati telephely a következő almodulokat is tartalmazhatja:

* **Kiszolgálófarm és adatközpont modul** - Ez a terület biztosítja a nagysebességű csatlakoztathatóságot és a védelmet a kiszolgálóknak. Kritikus a biztonság, a redundancia és a hibatűrés biztosítása. A hálózatfelügyeleti rendszerek követik nyomon a teljesítményt az eszközök és a hálózat rendelkezésre állásának a figyelésével.
* **Szolgáltatómodul** - Ez a terület biztosítja a szolgáltatásokhoz való hozzáférést, mint amilyenek az IP-telefónia, a vezeték nélküli vezérlő szolgáltatások és az egyesített szolgáltatások.

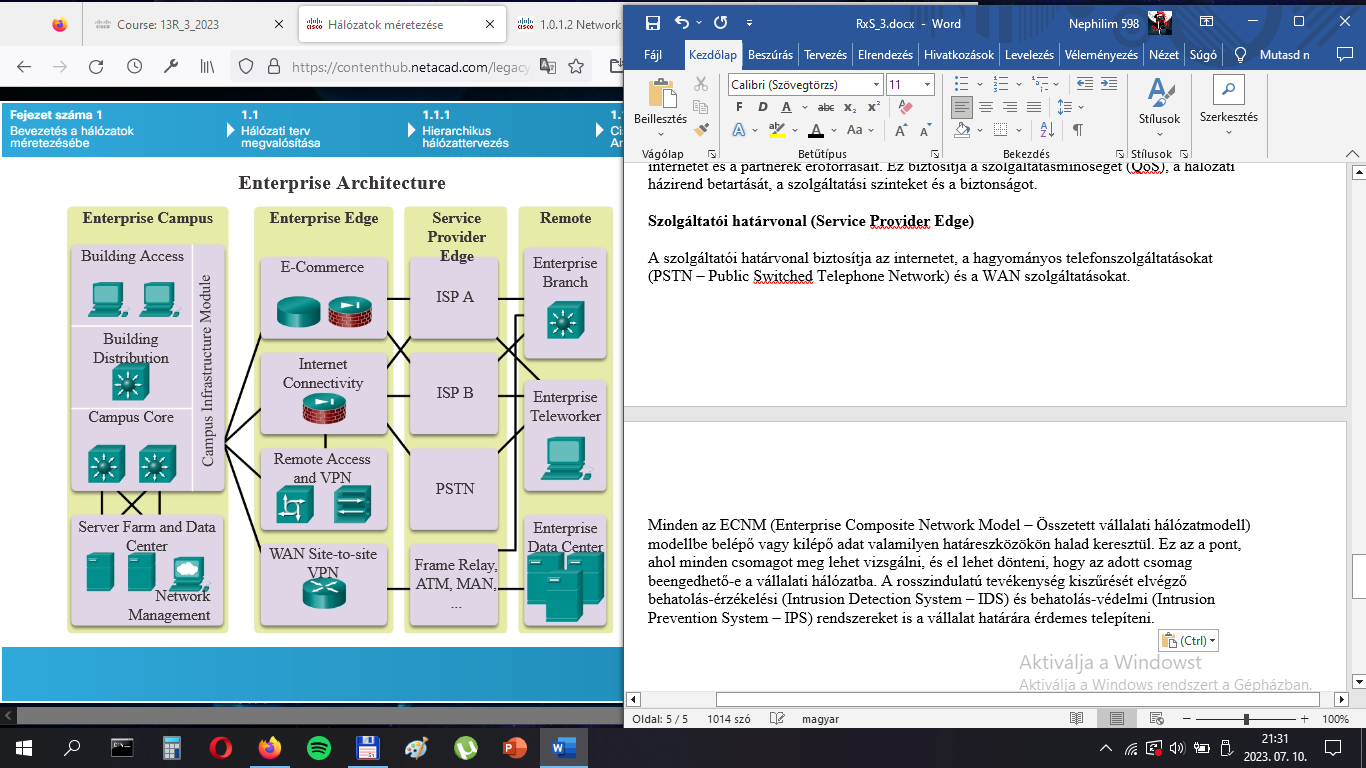
**Vállalati határvonal (Enterprise Edge)**

A vállalati határvonal (Enterprise Edge) az internet, a VPN és a WAN modulok összessége, melyek a vállalat hálózatát kapcsolják össze a szolgáltató hálózatával. Ez a modul terjeszti ki a vállalati szolgáltatásokat a távoli telephelyek felé és teszi lehetővé, hogy a vállalat elérje az internetet és a partnerek erőforrásait. Ez biztosítja a szolgáltatásminőséget (QoS), a hálózati házirend betartását, a szolgáltatási szinteket és a biztonságot.

**Szolgáltatói határvonal (Service Provider Edge)**

A szolgáltatói határvonal biztosítja az internetet, a hagyományos telefonszolgáltatásokat (PSTN – Public Switched Telephone Network) és a WAN szolgáltatásokat.

Minden az ECNM (Enterprise Composite Network Model – Összetett vállalati hálózatmodell) modellbe belépő vagy kilépő adat valamilyen határeszközökön halad keresztül. Ez az a pont, ahol minden csomagot meg lehet vizsgálni, és el lehet dönteni, hogy az adott csomag beengedhető-e a vállalati hálózatba. A rosszindulatú tevékenység kiszűrését elvégző behatolás-érzékelési (Intrusion Detection System – IDS) és behatolás-védelmi (Intrusion Prevention System – IPS) rendszereket is a vállalat határára érdemes telepíteni.



# Meghibásodási tartományok

Egy jól megtervezett hálózat a forgalom megfelelő szabályozása mellett korlátozza a meghibásodási tartományok méretét is. A meghibásodási tartomány az a hálózatrész, melyet közvetlenül érint egy kulcsfontosságú hálózati eszköz vagy szolgáltatás meghibásodása.

Az elsőként meghibásodó összetevő nagyban meghatározza, hogy mekkora tartományra lesz hatással a hiba. Például, ha egy adott szegmens kapcsolója hibásodik meg, akkor általában csak az adott szegmens állomásai érintettek. Ugyanakkor, ha az adott szegmenst a többihez kapcsoló forgalomirányító hibásodik meg, akkor a hatás sokkal nagyobb mértékű lehet.

A hálózati károk csökkenthetők redundáns kapcsolatok és megfelelő minőségű, professzionális eszközök használatával. A kisméretű meghibásodási tartományok csökkentik a hibák vállalati termelékenységére gyakorolt hatását. Ugyanakkor egyszerűsítik a hibaelhárítást, ezáltal csökkentik az egyes felhasználók által tapasztalt leállási időt.

Kattintson az egyes hálózati eszközökre a meghibásodási tartományuk megtekintéséhez!

**A meghibásodási tartományok méretének csökkentése**

Mivel egy meghibásodásnak a hálózat gerincrétegében potenciálisan nagyobb hatása lehet, ezért a hálózattervezők gyakran koncentrálnak ezen hibák megelőzésére. Ez azt eredményezi, hogy jelentősen megnőhet a hálózat megvalósításának a költsége. A hierarchikus tervezési modellben a legegyszerűbb - és általában a legolcsóbb is - az elosztási rétegbeli meghibásodási tartományok méretének szabályozása. A hozzáférési rétegben előforduló hálózati hibák kisebb területet érintenek, ezért kevesebb felhasználóra vannak hatással. Amikor 3. rétegbeli eszközt használunk az elosztási rétegben, akkor minden forgalomirányító korlátozott számú felhasználó számára lesz az alapértelmezett átjáró.

**Kapcsolóblokk kiépítés**

Forgalomirányítókat és 3. rétegbeli kapcsolókat általában egyenlő arányban elosztva, párban telepítik a hozzáférési rétegbeli kapcsolókhoz. Ezt a konfigurációt egy épületre vagy részlegre vonatkozó kapcsolóblokknak nevezik. Minden kapcsolóblokk független a többitől. Ennek eredményeként egyetlen eszköz meghibásodása nem okozza a hálózat teljes leállását. Egy teljes kapcsolóblokk meghibásodása is a végfelhasználóknak csak egy kevésbé jelentős hányadára van hatással.

# A méretezhetőség tervezése

Vállalati hálózatok esetében a hálózattervezőnek stratégiát kell kidolgozni a hálózat rendelkezésre állásának, valamint a növekedés egyszerű és hatékony megvalósításának biztosítására. Egy általános hálózattervezési stratégia az alábbi ajánlásokat tartalmazza:

* Használjunk bővíthető, moduláris vagy fürtözhető eszközöket, amelyeknek könnyen növelhetők a képességeik. Modulokkal egy meglévő eszköz funkciói bővíthetők anélkül, hogy jelentősebb eszközfejlesztést kellene végrehajtani. Egyes eszközök fürtbe szervezhetők, amelyek így egy eszközként funkcionálnak, megkönnyítve ezáltal a felügyeletet és a konfigurációt.
* Egy hierarchikusra tervezett hálózat esetében a modulok igény szerint hozzáadhatók, továbbfejleszthetők és cserélhetők, anélkül, hogy az hatással lenne a hálózat egyéb funkcionális részeinek tervezésére. Például egy különálló hozzáférési réteg anélkül is bővíthető, hogy az hatással lenne a vállalati hálózat elosztási- vatgy gerincrétegeire.
* Hozzunk létre egy hierarchikus IPv4 vagy IPv6 címzési stratégiát. Egy előrelátó IPv4 címzési terv szükségtelenné teszi a hálózat újracímzését, további felhasználók és szolgáltatások hozzáadásakor.
* Válasszunk forgalomirányítókat és többrétegű kapcsolókat a szórások korlátozására, valamint az egyéb nemkívánatos forgalmak kiszűrésére a hálózatból. Használjunk 3. rétegbeli kapcsolókat a hálózati gerinc forgalmának szűrésére és csökkentésére.

Az ábrán még további, fejlettebb hálózattervezési elvárások láthatók:

* Hozzunk létre redundáns hálózati kapcsolatokat a kritikus eszközök, és a hozzáférési- és gerincrétegbeli eszközök között.
* Az eszközök között hozzunk létre többszörös kapcsolatokat akár link aggregációval (EtherChannel), akár egyenlő költségű terhelés-elosztással a sávszélesség növelésére. Fogjunk össze több Ethernet kapcsolatot egyetlen terhelés-elosztást használó EtherChannel konfigurációba a rendelkezésre álló sávszélesség növelésére. EtherChannel megvalósítások abban az esetben is használhatók, ha költségvetési megszorítások nem teszik lehetővé nagysebességű interfészek és optikai kapcsolatok megvásárlását.
* Használjunk vezeték nélküli kapcsolatokat, amelyek lehetővé teszik a mobilitás és a hálózat kiterjesztését.
* Használjunk méretezhető irányító protokollokat és azokon belül olyan funkciókat, amelyek elszigetelik az irányítási frissítéseket és minimalizálják az irányítótábla méretét.

# Redundancia tervezése

**Redundancia megvalósítása**

Számos szervezet számára a hálózat elérhetősége elengedhetetlen a megfelelő működés biztosításához. A redundancia fontos része a hálózattervezésnek, általa elérhető, hogy ne legyen olyan gyenge pontja a hálózatnak, mely önmagában komoly zavart okozna a hálózati szolgáltatásokban. Egyik módszer a redundancia megvalósítására a duplikált eszközök üzembe helyezése és tartalék szolgáltatások biztosítása a kritikus eszközök számára.

A redundancia megvalósításának egy másik módszere a redundáns útvonalak alkalmazása, ahogyan azt az ábra is mutatja. A redundáns útvonalak alternatív fizikai kapcsolatok biztosítanak a hálózaton áthaladó forgalom számára. A redundáns kapcsolatok nagyobb rendelkezésre állást biztosítanak a kapcsolt hálózatban . Ugyanakkor a kapcsolók működésének következményeként, a redundáns kapcsolatok Ethernet hálózatban 2. rétegbeli logikai hurkokat okozhatnak. Emiatt vált szükségessé a feszítőfa-protokoll (Spanning Tree Protocol, STP).

Az STP kiküszöböli a 2. rétegbeli hurkokat abban az esetben, ha a kapcsolók között redundáns kapcsolatokat hozunk létre. Ezt egy olyan mechanizmus segítségével éri el, amely letiltja egy kapcsolt hálózatban a redundáns kapcsolatokat egészen addig, amíg azok nem válnak szükségessé, például, amikor hiba lép fel. Az STP egy nyílt szabványú protokoll, melyet kapcsolt környezetben, hurokmentes logikai topológia létrehozására használnak.

További részletek a LAN redundanciáról és az STP protokoll működéséről a "LAN redundancia" című fejezetben találhatók.

# Sávszélesség növelése

**EtherChannel megvalósítása**

A hierarchikus hálózattervezésben a hozzáférési- és elosztási rétegbeli kapcsolók közötti bizonyos kapcsolatoknak nagyobb mennyiségű forgalmat kell feldolgozniuk, mint a többinek. Amikor több kapcsolat forgalma zúdul rá egyetlen kimenő kapcsolatra, akkor előfordulhat, hogy az a kapcsolat válik a szűk keresztmetszetté. A portok összefogása (link aggregation) lehetővé teszi arendszergazda számára, hogy több fizikai kapcsolat egyetlen logikai kapcsolattá történő összefogásával megnövelje az eszközök közötti sávszélességet. Az ábrán is látható EtherChannel használata az egyik módja a kapcsolt hálózatokban a portok összefogásának.

Az EtherChannel a meglévő kapcsolóportokat használja, ezért többletköltség nélkül lehet a kapcsolatot egy gyorsabb kapcsolattá fejleszteni, és drágább kapcsolat nem szükséges. Az EtherChannel egyetlen, EtherChannel interfészt használó logikai kapcsolatnak tekinthető. A legtöbb konfigurációs feladatot az EtherChannel interfészen kell végrehajtani, így nincs szükség a portok egyedi kezelésére, és biztosítható azok következetes beállítása. Végül, az EtherChannel kihasználja az egyazon EtherChannel-hez tartozó portok közötti terheléselosztás lehetőségét, és a hardvertől függően egy vagy két terheléselosztási módszert alkalmaz.

Az EtherChannel működését és konfigurációját részletesen a "Portösszefogás" fejezet tárgyalja.

# A hozzáférési réteg bővítése

**Vezeték nélküli csatlakozás biztosítása**

A hálózatot úgy kell megtervezni, hogy képes legyen a felhasználók és eszközök csatlakozási igényeihez illeszkedő bővülésre. Egyre fontosabb szempont a hozzáférési rétegbeli csatlakoztathatóság kiterjesztése a vezeték nélküli kapcsolatokra. A vezeték nélküli csatlakozási lehetőség számos előnnyel jár, mint amilyen a rugalmasság, az alacsony költségek, és az a képesség, hogy a hálózat megváltoztatása nélkül képes az üzleti igényekhez illeszkedő növekedésre.

A vezeték nélküli kommunikációt a végberendezésben lévő NIC végzi, mely tartalmazza rádiós adó/vevő áramkört is. Működtetéséhez pedig megfelelő meghajtóprogram szükséges. Továbbá a felhasználók csatlakozásához egy vezeték nélküli forgalomirányító vagy hozzáférési pont (Access Point, AP) szükséges, ahogy azt az ábra is mutatja.

Számos megfontolási szempont van a vezeték nélküli hálózatok üzembe helyezésekor, mint amilyen a használt vezeték nélküli eszközök típusa, a lefedettségi követelmények, az interferencia- és biztonsági megfontolások.

A vezeték nélküli rendszerek működését és telepítését részletesen a "Vezeték nélküli LAN-ok" fejezet tárgyalja.

# Irányító protokollok finomhangolása

**Az irányított hálózat felügyelete**

A vállalati hálózatok és az internetszolgáltatók a hierarchikus felépítés és a bővíthetőség miatt gyakran alkalmaznak olyan fejlettebb protokollokat, mint a kapcsolatállapot alapú protokollok.

A kapcsolatállapot alapú irányító protokollok, mint az OSPF (Open Shortest Path First) is, kiválóan alkalmazhatók nagyobb, hierarchikus hálózatokban, ahol a gyors konvergencia fontos (lásd 1. ábra). Az OSPF forgalomirányítók szomszédsági kapcsolatokat építenek ki és tartanak fenn más csatlakozó OSPF forgalomirányítókkal. A szomszédsági viszony kialakítását követően a két forgalomirányító elkezdi a kapcsolatállapot frissítések küldését egymásnak. A teljes értékű (full state) szomszédsági viszonyt akkor érik el, ha kapcsolatállapot-adatbázisuk már összhangban van egymással. OSPF esetén a kapcsolatállapot frissítéseket változások esetén küldik ki a forgalomirányítók.

Az OSPF egy gyakran alkalmazott kapcsolatállapot alapú irányító protokoll, amely többféle módon finomhangolható. Az "Egyterületű OSPF beállítása és hibakeresése" című fejezet majd részletesen foglalkozik az OSPF haladó konfigurációjával és hibakeresésével.

Ezen felül, ahogy a 2. ábra is mutatja, az OSPF a területek használatával támogatja a kétrétegű hierarchikus tervezést. Minden OSPF hálózat kiindulási pontja a 0-s terület, melyet gerinchálózatnak is neveznek. A hálózat növekedésével más, a 0-s területtől eltérő területek is létrehozhatók. Minden területnek, mely nem gerinchálózat, közvetlenül a 0-s területhez kell kapcsolódnia. A "Többterületű OSPF" című fejezet mutatja be a többterületű OSPF előnyeit, működését és konfigurációját.

A nagyobb hálózatok egy másik népszerű irányító protokollja az EIGRP (Enhanced Interior Gateway Routing Protocol). Az EIGRP egy Cisco fejlesztésű távolságvektor alapú irányító protokoll számos továbbfejlesztett képességgel. Bár az EIGRP konfigurálása viszonylag egyszerű, a mögöttes funkciói és opciói kiterjedtek és robusztusak. Az EIGRP például több táblát is használ az irányítási folyamat kezeléséhez (lásd 3. ábra). Az EIGRP számos olyan tulajdonsággal rendelkezik, amely egyetlen irányító protokollban sem található meg. Jó választás a nagy, több protokollt és elsősorban Cisco eszközöket használó hálózatok esetén.

Az "EIGRP" című fejezet foglalkozik az EIGRP protokoll működésével és konfigurációjával, míg a "Haladó EIGRP konfiguráció és hibakeresés" című az EIGRP haladó konfigurációjával és hibakeresésével.

**Kapcsoló platformok**

Hálózat tervezésekor fontos annak a megfelelő hardvernek a kiválasztása, amely illeszkedik a meglévő hálózati követelményekhez, ugyanakkor lehetővé teszi a hálózat növekedését is. Egy vállalati hálózatban mind a kapcsolók, mind a forgalomirányítók kritikus szerepet töltenek be a hálózati kommunikációban.

A vállalati hálózatokban alkalmazott kapcsolóknak öt kategóriája létezik (lásd 1. ábra):

* **Telephelyi LAN kapcsolók** - Egy vállalati LAN hálózatban a hálózati teljesítmény méretezéséhez gerinc-, elosztási-, hozzáférési és kompakt kapcsolókat használnak. Ezek a kapcsoló platformok a fix 8-portos, ventillátor nélküli kapcsolótól a több száz portot támogató, 13-modulos kapcsolóig változhatnak. A telephelyi kapcsolókhoz tartoznak a Cisco 2960, 3560, 3750, 3850, 4500, 6500 és 6800 sorozatú eszközök.
* **Felhőből felügyelhető (Cloud-Managed) kapcsolók** - A Cisco Meraki felhőből felügyelhető kapcsolók lehetővé teszik a kapcsolók virtuális stack-elését . A helyi IT személyzet beavatkozása nélkül, a weben keresztül kapcsolóportok ezreit monitorozzák és konfigurálják.
* **Adatközponti kapcsolók** - Egy adatközpontnak olyan kapcsolókra kell épülnie, amelyek elősegítik az infrastruktúra méretezhetőségét, a működés folytonosságát és a továbbítás rugalmasságát. Az adatközponti kapcsoló platformok a Cisco Nexus és a Cisco Catalyst 6500 sorozatú kapcsolókat tartalmazzák.
* **Szolgáltatói kapcsolók** - A szolgáltatói kapcsolók két kategóriára oszthatók: aggregációs kapcsolók és Ethernet hozzáférési kapcsolók. Az aggregációs kapcsolók olyan speciális Ethernet kapcsolók, amelyek a hálózat határán egyesítik a forgalmat. A szolgáltatói Ethernet hozzáférési kapcsolók jellemzői az alkalmazási intelligencia, az egyesített szolgáltatások, a virtualizáció, az integrált biztonság és az egyszerű felügyelet.
* **Virtuális hálózatok** - A hálózatok egyre inkább virtualizálttá válnak. A Cisco Nexus virtuális hálózati kapcsoló platformok az adatközpontokhoz való virtualizációs intelligencia hozzáadásával biztonságos, több bérlős szolgáltatásokat biztosítanak.

Kapcsolók kiválasztásakor a rendszergazdának meg kell határoznia az alaki tényezőket. Ez magába foglalja a fix konfigurációt (2. ábra), a moduláris konfigurációt (3. ábra), vagy a stack-be szervezés lehetőségét (4. ábra) vagy annak hiányát. A kapcsoló vastagsága, amelyet a rack egységek (unit) száma fejez ki, szintén fontos a rack-be szerelhető kapcsolók esetében. Például a 2. ábrán látható fix kiépítésű kapcsolók mindegyike egy egység (1U) magas.

Ezen megfontolásokon felül az 5. ábra a kapcsoló kiválasztásának más, általános üzleti szempontjaira világít rá.

# Portsűrűség

Egy kapcsoló portsűrűsége az egyetlen kapcsolón rendelkezésre álló portok száma. Az ábra három különböző kapcsoló portsűrűségét szemlélteti.

A fix kiépítésű kapcsolók általában 48 portig biztosítanak hozzáférést egyetlen eszközön. Opcionálisan további legfeljebb négy portnak biztosíthatnak helyet az SFP (small form-factor pluggable) eszközök számára. A nagy portsűrűség lehetővé teszi a rendelkezésre álló hely jobb kihasználását és az áramfogyasztás korlátok közt tartását. Ha két 24-portos kapcsolónk van, akkor azok legfeljebb 46 port kiosztását támogatják, mivel kapcsolónként legalább egy port elveszik a hálózat többi részéhez történő csatlakoztatással. Ráadásul két elektromos csatlakozó szükséges hozzájuk. Ha ehelyett egyetlen 48-portos kapcsolót használunk, akkor egyetlen port elvesztése mellett 47 eszköz csatlakoztatása lehetséges, és csak egyetlen elektromos csatlakozásra van szükség.

A moduláris kapcsolók a kapcsoló modulok hozzáadásával nagyon nagy portsűrűséget is támogathatnak. Egyes Catalyst 6500 kapcsolók például 1,000 feletti kapcsolóport számot is támogatnak.

Nagyméretű, több ezer hálózati eszközt tartalmazó vállalati hálózatok nagy portsűrűséget igényelnek, amelyeknél a moduláris kapcsolók kínálják a legelőnyösebb helykihasználást és elektromos fogyasztást. Nagy portsűrűségű, moduláris kapcsolók használata nélkül a hálózatnak sok, fix kiépítésű kapcsolóra lenne szüksége a nagyszámú, hálózati hozzáférést igénylő hálózati eszköz elhelyezéséhez. Ez a megközelítés számos elektromos csatlakozást és a rack szekrényben sok helyet igényel.

A hálózattervezőnek foglalkozni kell a felfelé menő kapcsolatok szűk keresztmetszetének a problémájával: fix kiépítésű kapcsolók sorba kötésekor a megfelelő teljesítmény eléréséhez számos portot fel kell használni a sávszélesség aggregációjához. Egyetlen moduláris kapcsoló esetében a sávszélesség összefogása kevésbé jelent problémát, mivel a készülék háttérrendszere képes biztosítani a kapcsoló modulkártyáihoz csatlakozó eszközök elhelyezéséhez szükséges sávszélességet.

# Adattovábbítási sebesség

A továbbítási sebesség határozza meg egy kapcsoló feldolgozási képességeit, meghatározva hogy mennyi adatot képes továbbítani másodpercenként. A kapcsolók termékcsaládjait a továbbítási ráták alapján sorolják be, ahogy az az ábrán is látható. A belépő szintű kapcsolók alacsonyabb továbbítási sebességgel rendelkeznek, mint a vállalati szintű kapcsolók. A továbbítási sebesség fontos szempont egy kapcsoló kiválasztásakor. Ha a kapcsoló továbbítási sebessége túl alacsony, akkor nem képes valamennyi portján biztosítani a vezetéksebességű (wire-speed) kommunikációt. A vezetéksebesség az az adatráta, amelyre az adott kapcsoló valamennyi Ethernet portja képes. Ez az adatráta 100 Mb/s, 1 Gb/s, 10 Gb/s vagy 100 Gb/s lehet.

Egy általános 48-portos gigabites kapcsoló például teljes terhelésen 48 Gb/s forgalmat generál. Ha a kapcsoló csak 32 Gb/s továbbítási sebességet tesz lehetővé, akkor nem képes valamennyi portján párhuzamosan biztosítani a teljes vezetéksebességet. Szerencsére a hozzáférési rétegbeli kapcsolóknak nem kell teljes vezetéksebességen működniük, mivel az elosztási réteg felé menő kapcsolat (uplink) miatt fizikailag le vannak korlátozva. Ez azt jelenti, hogy az olcsóbb, alacsonyabb teljesítményű kapcsolókat használhatjuk a hozzáférési rétegben, míg a sokkal drágább, nagyteljesítményű kapcsolókat pedig az elosztási- és gerincrétegekben, ahol a továbbítási sebesség jobban befolyásolja a hálózat teljesítményét.

# Áramellátás Ethernet felett (PoE, Power over Ethernet)

PoE lehetővé teszi, hogy a kapcsoló egy meglévő Ethernet kábelezésen keresztül tápellátást biztosítson egy másik eszköz számára. Ez a funkció IP-telefonok és egyes vezeték nélküli hozzáférési pontok esetében alkalmazható. Kattintson az 1. ábra kiemelt ikonjaira az eszközök PoE portjainak a megtekintéséhez.

A PoE nagyobb rugalmasságot biztosít a vezeték nélküli hozzáférési pontok és a IP-telefonok telepítéséhez, mivel azok így bárhol felszerelhetők, ahol már van kiépített Ethernet kábel. A hálózati rendszergazdának azonban meg kell bizonyosodnia a PoE funkció szükségességéről, mivel a PoE-t támogató kapcsolók drágák.

A viszonylag új Cisco Catalyst 2960-C és 3560-C sorozatú kapcsolók támogatják a PoE áteresztést. A PoE áteresztést azt teszi lehetővé, hogy a hálózati rendszergazda mind a kapcsolóra csatlakoztatott PoE eszközöknek, mind pedig magának a kapcsolónak is biztosítsa a tápellátását a felettük lévő kapcsolókon keresztül. Kattintson a 2. ábra kiemelt ikonjára a Cisco Catalyst 2960-C megtekintéséhez.

# Többrétegű kapcsolás

A többrétegű kapcsolókat jellemzően egy kapcsolt szervezeti hálózat gerinc- és elosztási rétegében alkalmazzák. A többrétegű kapcsolók jellemzője, hogy képesek egy irányítótáblát felépíteni, több irányító protokollt támogatni, és 2. rétegbeli kapcsoláshoz közeli sebességgel IP-csomagokat továbbítani. A többrétegű kapcsolók gyakran olyan speciális hardverelemekkel rendelkeznek, mint például az alkalmazásspecifikus integrált áramkörök (ASIC, Application-specific Integrated Circuit). Az ASICS egy dedikált szoftveres adatszerkezettel együtt a CPU-tól függetlenül képes az IP-csomagokat továbbítani.

A trend a hálózatok területén a kizárólag 3. rétegbeli eszközöket tartalmazó kapcsolt környezet felé mutat. Amikor először használtak kapcsolókat, azok nem támogatták az irányítást. Ma már szinte valamennyi kapcsoló támogatja azt. Valószínű, hogy hamarosan minden kapcsoló tartalmazni fog egy irányítási processzort, mivel ennek a költsége így viszonylag lecsökkenti az egyéb korlátozásokat. Végül pedig maga a többrétegű kapcsoló kifejezés is szükségtelenné fog válni.

Az ábrán látható Catalyst 2960 kapcsolók is azt szemléltetik, hogy haladunk a tisztán 3. rétegbeli eszközöket tartalmazó környezetek felé. A 15.x IOS verzió előtti kapcsolók kizárólag egy virtuális kapcsolóinterfészt (SVI, Switched Virtual Interface) támogattak. Az IOS 15.x verziótól kezdve ezek a kapcsolók már több SVI-t támogatnak. Ezt azt jelenti, hogy így a kapcsoló távolról több, különböző hálózathoz tartozó IP-címről is elérhető.

# Packet Tracer - 2960 és 3560 kapcsolók összehasonlítása

**Háttér / esetleírás**

Ebben a feladatban különböző parancsokat fogunk használni három különböző kapcsolt topológia megvizsgálására, valamint a 2960 és 3650 kapcsoló hasonlóságainak és különbségeinek összehasonlítására. Össze fogjuk hasonlítani továbbá a 1941 forgalomirányító, valamint a 3560 kapcsoló irányítótábláját.

[Packet Tracer - Comparing 2960 and 3560 Switches Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.2.1.7%20Packet%20Tracer%20-%20Comparing%202960%20and%203560%20Switches%20Instructions.pdf)

[Packet Tracer - Comparing 2960 and 3560 Switches - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.2.1.7%20Packet%20Tracer%20-%20Comparing%202960%20and%203560%20Switches.pka)

 [1.2.1.8 Laborgyakorlat - Kapcsoló hardver kiválasztása](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#1.2.1.8)

**Laborgyakorlat - Kapcsoló hardver kiválasztása**

**Ebben a gyakorlatban a következő feladatokat végezzük el:**

* 1. rész: Cisco kapcsolók felkutatása.
* 2. rész: Egy hozzáférési kapcsoló kiválasztása.
* 3. rész: Egy elosztási-/gerincrétegbeli kapcsoló kiválasztása.

[Lab - Selecting Switching Hardware](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.2.1.8%20Lab%20-%20Selecting%20Switching%20Hardware.pdf)

**Forgalomirányító követelmények**

Egy vállalat elosztási rétegében irányításra van szükség. Irányítási folyamat nélkül a csomagok nem hagyhatják el a helyi hálózatot.

A forgalomirányítók szerepe a hálózatban kulcsfontosságú, mivel összeköttetést biztosítanak egy vállalati hálózat több telephelye között, redundáns útvonalakat kínálnak, és biztosítják az ISP-k felé a kapcsolatot az interneten keresztül. A forgalomirányítók betölthetik a tolmács szerepét is a különböző átviteli közegtípusok és protokollok között. Egy forgalomirányító például fogadhat csomagokat egy Ethernet hálózatról, majd újra beágyazva egy soros vonalon továbbítják azokat.

A forgalomirányító a cél IP-cím hálózati részét használja, hogy a csomagokat a megfelelő cél felé irányítsa. Ha megszűnik egy összeköttetés vagy torlódás alakul ki, akkor tartalékútvonalat jelöl ki. A forgalomirányító helyi interfészének IP-címét meg kell adni a helyi hálózat összes állomásának IP-beállításainál. A forgalomirányító ezen interfészét alapértelmezett átjárónak nevezzük.

A forgalomirányítók más hasznos funkciókat is ellátnak:

* A szórások kézben tartása
* Összeköttetés biztosítása távoli helyek között
* A felhasználók alkalmazási terület vagy szervezeti egység szerinti logikai csoportosítása
* Fokozott biztonság nyújtása

Az ábra kiemelt területeire kattintva további információt kaphatunk a forgalomirányítók funkcióiról.

A vállalatok és az internetszolgáltatók számára egyaránt kulcsfontosságú a csomagok célba juttatásához a hatékony forgalomirányítás és a meghibásodott hálózati kapcsolatok helyreállítása.

# Cisco forgalomirányítók

Fontos, hogy a hálózat növekedésével a követelményeknek megfelelő forgalomirányítót válasszunk. Amint az ábrán látható, a forgalomirányítóknak három kategóriája van:

* **Telephelyi forgalomirányítók (Branch Routers)** - A telephelyi forgalomirányítók egységes platformon optimalizálják a telephelyi szolgáltatásokat, miközben optimális alkalmazási élményt közvetítenek a helyi és a WAN infrastruktúrán keresztül. A telephelyi szolgáltatások rendelkezésre állásának maximalizálásához a 24x7x365 üzemidejű hálózat tervezése szükséges. Egy nagy rendelkezésre állású helyi hálózatnak biztosítania kell a tipikus hibákból történő gyors helyreállíthatóságot, miközben minimalizálja vagy megszünteti azok szolgáltatásokra gyakorolt kihatását, valamint lehetővé teszi az egyszerű hálózati konfigurációt és felügyeletet.
* **Határforgalomirányítók** - A határforgalomirányítók lehetővé teszik a szolgáltatások hálózati határon át történő nagyteljesítményű, nagybiztonságú és megbízható továbbítását, egységesen kampusz-, adatközponti- és telephelyi hálózatok esetében egyaránt. Az ügyfelek manapság a magas minőségű multimédiás élményt várnak el és több tartalomtípust, mint bármikor korábban. Interaktivitást, személyre szabottságot, mobilitást szeretnének, valamit szeretnék az összes tartalom felett az irányítást is gyakorolni. Elvárják azt is, hogy a tartalmakhoz bármikor és bárhonnan hozzáférjenek, bármilyen eszközről, függetlenül attól, hogy otthon vagy a munkahelyen vannak, vagy esetleg valahol útközben. A határforgalomirányítóknak fokozott szolgáltatási minőséget (QoS) kell biztosítaniuk, valamint non-stop videó és mobil képességekkel kell rendelkezniük.
* **Szolgáltatói forgalomirányítók** - A szolgáltatói forgalomirányítók megkülönböztetik a szolgáltatási csomagokat és méretezhető, végponttól-végpontig terjedő megoldások és szolgáltatások továbbításával növelik meg a bevételeket. Az üzemeltetőknek optimalizálniuk kell a műveleteket, csökkenteni a költségeket, valamint javítani a méretezhetőséget és a rugalmasságot, hogy következő generációs internetes élményeket továbbítsanak különböző eszközökön és helyszíneken keresztül. Ezeket a rendszereket arra tervezték, hogy egyszerűsítsék és fokozzák a szolgáltatás-továbbító hálózatok működését és üzembe helyezését.

# A forgalomirányító

Ahogy az ábrán is látható, a forgalomirányítók is különböző formákban kerülnek forgalomba. A hálózati rendszergazdáknak számos forgalomirányítót kell tudniuk kezelni, a kis asztali eszköztől egészen a rackbe szerelhető blade modellekig.

A forgalomirányítók az alapján is csoportosíthatók, hogy a hardverkonfigurációjuk rögzített vagy moduláris. A rögzített konfiguráció esetében a forgalomirányító interfészei fixen beépítettek. A moduláris forgalomirányítókat több bővítőhellyel szállítják, melyek lehetővé teszik a hálózati rendszergazdák számára a forgalomirányító interfészeinek cseréjét. A Cisco 1841-es forgalomirányítót például két beépített Fast Ethernet RJ-45 interfésszel szállítják, és van két – számos különböző típusú hálózati csatlakozómodul fogadására alkalmas – bővítő foglalata is. A forgalomirányítókat a legkülönfélébb (pl. Fast Ethernet, Gigabit Ethernet, soros, száloptikai) interfészekkel szállítják.

# Az IOS fájlok kezelése és licencelés

A Cisco termékvonalához tartozó hálózati eszközök széles skálájából egy szervezet gondosan meg tudja határozni azt az ideális kombinációt, amely a megfelel az alkalmazottak és az ügyfelek igényeinek.

Amikor egy Cisco IOS eszközt kiválasztunk vagy korszerűsítünk, akkor fontos, hogy hozzá a megfelelő IOS képfájt a megfelelő szolgáltatáskészlettel és verzióval válasszuk ki. Az IOS egyetlen többfeladatos operációs rendszerbe integrálja az irányítási, a kapcsolási, a biztonsági és az egyéb hálózati technológiákat. Egy új eszköz előre telepített képfájllal és az ügyfél által meghatározott csomagokhoz és funkciókhoz illeszkedő állandó licencel kerül leszállításra.

A Cisco IOS 15.0 verzió kiadásával a Cisco megváltoztatta a forgalomirányítók esetében az új technológiák IOS funkciók közé történő beépítésének folyamatát (lásd ábra).

Az "IOS képfájlok és licencelésük" című fejezet részletesen foglalkozik a Cisco IOS licencek menedzselésével és karbantartásával.

# Sávon belüli és sávon kívüli felügyelet

Függetlenül a használt Cisco IOS hálózati eszköztől, két módszer van arra, hogy konfigurációs vagy felügyeleti feladatok ellátására PC-t csatlakoztathassunk hozzá. Ahogy az ábra is mutatja, ez a két módszer a sávon kívüli (out-of-band) és a sávon belüli (in-band) felügyelet.

A sávon kívüli felügyelet a kezdeti konfiguráció megadásához vagy hálózati kapcsolat hiánya esetén használható. A sávon kívüli konfigurációhoz az alábbiak szükségesek:

* közvetlen összeköttetés a konzol- vagy AUX-porttal,
* terminálemulációs kliensprogram.

Sávon-belüli felügyeletet általában a hálózati eszközök monitorozásához, illetve a konfigurációjuk megváltoztatásához használjuk. A sávon belüli konfigurációhoz az alábbiak szükségesek:

* legalább egy csatlakoztatott és működőképes hálózati interfész az eszközön,
* Telnet, SSH vagy HTTP hozzáférés a Cisco eszközhöz.

# Alapvető forgalomirányító parancsok

A forgalomirányító alapkonfigurációjához az azonosító hosztnév beállítása, a biztonsági jelszavak megadása, az interfészekhez egy IP-cím hozzárendelése, valamint az alapvető irányítási beállítások tartoznak. Az 1. ábra az OSPF forgalomirányítón történő engedélyezésének utasításait mutatja. Ellenőrizzük és mentsük a konfiguráció változásait a **copy running-config startup-config** parancs segítségével. A 2. ábra az 1. ábrán kiadott konfigurációs parancsok eredményét mutatja. A forgalomirányító konfigurációjának törléséhez használjuk az **erase startup-config** és a **reload** utasításokat.

Használjuk a 3. ábra parancsszimulátorát a forgalomirányító konfigurációjának ellenőrzésére a benne szereplő **show** parancsokkal.

**Forgalomirányítók alapvető show parancsai**

Az alábbiakban a forgalomirányító működési állapotának és hálózati funkcionalitásának megjelenítéséhez, illetve ellenőrzéséhez használható leggyakoribb IOS parancsok közül következik néhány. Az alábbi parancsok több kategóriába sorolhatók.

Forgalomirányítással kapcsolatos parancsok:

* **show ip protocols** - A konfigurált irányító protokollokról jelenít meg információkat. Amennyiben OSPF lett konfigurálva, ez magába foglalja az OSPF folyamat azonosítóját, a forgalomirányító azonosítóját, a forgalomirányító által hirdetett hálózatokat, a szomszédokat, amelyektől a forgalomirányító frissítéseket kap, és az adminisztratív távolságot, amely az OSPF esetében 110 (lásd 1. ábra).
* **show ip route** - Megjeleníti az irányítótábla információit, mint az irányítási protokoll kódok, az ismert hálózatok, az adminisztratív távolság és a metrika, hogyan került az útvonal megtanulásra, a következő ugrás, a statikus útvonalak és az alapértelmezett útvonalak (lásd 2. ábra).
* **show ip ospf neighbor** - Információkat jelenít meg a megismert OSPF szomszédokról, mint a szomszéd forgalomirányító azonosítója, a prioritása, az állapota (FULL = kialakult a szomszédság), az IP-címe és a helyi interfész, amelyen keresztül megismerte az adott szomszédot (lásd 3. ábra).

Interfésszel kapcsolatos parancsok:

* **show interfaces** - Megjeleníti az interfészek vonali (protokoll) állapotát, a sávszélességet, a késleltetést, a megbízhatóságot, a beágyazást, a duplexitást és az I/O statisztikákat. Ha az interfész megnevezése nélkül adjuk ki, akkor valamennyi interfészt megjeleníti. Ha megadunk egy meghatározott interfészt a parancs után, akkor csak annak az interfésznek az információit mutatja (lásd 4. ábra).
* **show ip interfaces** - Olyan interfész információkat jelenít meg, mint a protokoll állapot, az IP-cím, lett-e beállítva kisegítő cím (helper address) és ha ACL van hozzárendelve az interfészhez. Ha az interfész megnevezése nélkül adjuk ki, akkor valamennyi interfészt megjeleníti. Ha megadunk egy meghatározott interfészt a parancs után, akkor csak annak az interfésznek az információit mutatja (lásd 5. ábra).
* **show ip interface brief** - Valamennyi interfésznek megjeleníti az IP-címét és a vonali protokoll állapotát (lásd 6. ábra).
* **show protocols** - Információkat jelenít meg az engedélyezett irányított protokollról és az interfészek protokoll állapotáról (lásd 7. ábra).

Egyéb, a kapcsolatok vizsgálatához tartozó parancsok: **show cdp neighbors** parancs (lásd 8. ábra). Ez a parancs a közvetlenül csatlakozó eszközökről jelenít meg olyan információkat, mint az eszköz azonosítója (Device ID), az eszközhöz csatlakozó helyi interfész, a képességek (R=router, S=switch), a platform és a távoli eszköz interfész azonosítója (Port ID). A "details" opció tartalmazza még az IP-címzési információkat és az IOS verziót.

Használjuk a 9. ábra parancsszimulátorát a forgalomirányító konfigurációjának ellenőrzésére a benne szereplő **show** parancsokkal.

# Alapvető kapcsoló parancsok

A kapcsoló alapbeállításainak részét képezi az azonosítás céljából megadott állomásnév, a biztonsági jelszavak beállítása, valamint a felügyelhetőség miatt hozzárendelt IP-cím. A sávon belüli hozzáféréshez a kapcsolónak IP-címmel kell rendelkeznie. Az 1. ábra egy kapcsoló alapkonfigurációjának utasításait mutatja.

A 2. ábra az 1. ábrán kiadott konfigurációs parancsok eredményét mutatja. Ellenőrizzük és mentsük a kapcsoló konfigurációját a **copy running-config startup-config** parancs segítségével. A kapcsoló konfigurációjának törléséhez használjuk az **erase startup-config** és a **reload** utasításokat. Előfordulhat, hogy a VLAN információkat is törölni kell a **delete flash:vlan.dat** parancs segítségével. Amikor már rendben van a kapcsoló konfigurációja, nézzük meg a beállításokat a **show running-config** parancs segítségével.

**Kapcsolók alapvető show parancsai**

A kapcsolón a beállítások megadása, az összeköttetés ellenőrzése és a kapcsoló jelenlegi állapotának megjelenítése IOS parancsok segítségével történik. Kattintsunk az 1-4 gombokra a példák parancskimeneteinek, valamint a rendszergazdák által belőlük kinyerhető fontos információknak a megjelenítéséért.

Interfésszel / porttal kapcsolatos parancsok:

* **show port-security** - Megjeleníti az aktív portbiztonsággal rendelkező portokat. Egy meghatározott interfész vizsgálatához adjuk meg annak azonosítóját is. A parancs kimenetében lévő információk: a maximálisan engedélyezett címszám, a pillanatnyi címszám, a portbiztonsági sértések száma és az ezekre tett intézkedések (lásd 1. ábra).
* **show port-security address** - Megjeleníti a kapcsoló interfészein konfigurált megbízható MAC-címeket (lásd 2. ábra).
* **show interfaces** - Megjeleníti egy vagy az összes interfész vonali (protokoll) állapotát, sávszélességét, megbízhatóságát, beágyazását, duplexitását és I/O statisztikáit (lásd 3. ábra).
* **show mac-address-table** - Megjeleníti a kapcsoló által megtanult MAC-címeket, a megtanulás módját (dinamikus/statikus), a hozzá tartozó portszámot, valamint hogy a port melyik VLAN-ba tartozik (lásd 4. ábra).

Ahogy a forgalomirányító, úgy a kapcsoló is támogatja a **show cdp neighbors** parancsot.

A forgalomirányítóknál alkalmazott sávon belüli és sávon kívüli konfigurálási technikák a kapcsoló beállításánál is ugyanúgy használhatók.

**Csoportos feladat - Többrétegű hálózattervezési szimuláció**

**Többrétegű hálózattervezési szimuláció**

Mint egy egészen kis hálózat rendszergazdája, szeretnénk készíteni egy hálózatszimulációs prezentációt a helyi vezetőnknek annak bemutatására, hogy a hálózat jelen pillanatban hogyan működik.

A kis hálózat az alábbi eszközöket tartalmazza:

* egy 2911 sorozatú forgalomirányító.
* egy 3560 kapcsoló
* egy 2960 kapcsoló
* négy felhasználói munkaállomás (PC-k vagy laptopok)
* egy nyomtató

[Class Activity - Layered Network Design Simulation](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.3.1.1%20Layered%20Network%20Design%20Simulation%20Instructions.pdf)

# Packet Tracer – Komplex képességmérő feladat

**Háttér / esetleírás**

A hálózatmenedzser megkért - mint frissen felvett technikust -, hogy mutassuk be képességeinket egy kis méretű helyi hálózat konfigurálásán keresztül. Feladatunk két Cisco IOS kapcsoló alapbeállításainak konfigurálása, valamint a munkaállomások IP-címzési beállításainak elvégzése a végponttól végpontig terjedő összeköttetés biztosítása érdekében. A két kapcsoló és a két PC bekapcsolt és összekötött állapotban vannak.

[Packet Tracer - Skills Integration Challenge Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.3.1.3%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer - Skills Integration Challenge - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/1.3.1.3%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge.pka)

# Összefoglalás

A hierarchikus tervezési modell a hálózati funkciókat hozzáférési-, elosztási- és gerincrétegre bontja. A Cisco nagyvállalati architektúra további funkcionális összetevőkre bontja a hálózatot.

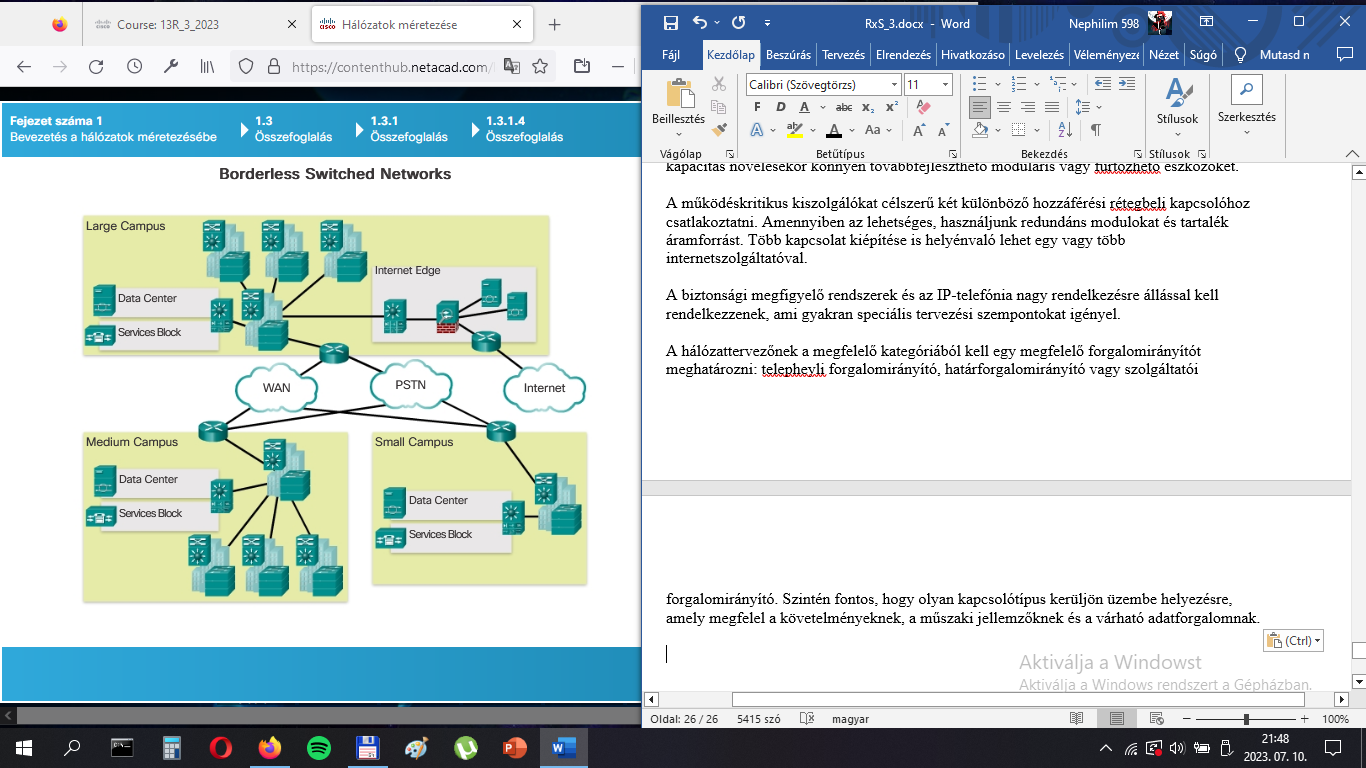
Egy jól megtervezett hálózat szabályozza a forgalmat és korlátozza a hibatartományok méretét. A forgalomirányítókat és a többrétegű kapcsolókat érdemes párosával telepíteni, hogy egyetlen eszköz meghibásodása ne okozhasson szolgáltatás-kimaradásokat.

A hálózati tervnek tartalmaznia kell egy IP-címzési tervet, a méretezhetőséget, az irányító protokollok gyors konvergenciáját, a megfelelő 2. rétegbeli protokollokat, valamint a kapacitás növelésekor könnyen továbbfejleszthető moduláris vagy fürtözhető eszközöket.

A működéskritikus kiszolgálókat célszerű két különböző hozzáférési rétegbeli kapcsolóhoz csatlakoztatni. Amennyiben az lehetséges, használjunk redundáns modulokat és tartalék áramforrást. Több kapcsolat kiépítése is helyénvaló lehet egy vagy több internetszolgáltatóval.

A biztonsági megfigyelő rendszerek és az IP-telefónia nagy rendelkezésre állással kell rendelkezzenek, ami gyakran speciális tervezési szempontokat igényel.

A hálózattervezőnek a megfelelő kategóriából kell egy megfelelő forgalomirányítót meghatározni: telepheyli forgalomirányító, határforgalomirányító vagy szolgáltatói forgalomirányító. Szintén fontos, hogy olyan kapcsolótípus kerüljön üzembe helyezésre, amely megfelel a követelményeknek, a műszaki jellemzőknek és a várható adatforgalomnak.



* [Fejezet száma 2 LAN redundancia](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#2)
* [2.0 LAN redundancia](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#2.0)
* [2.0.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#2.0.1)
* [2.0.1.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#2.0.1.1)

# Bevezetés

A hálózat megbízhatóságának kulcsa a redundancia. Az eszközök közti többszörös fizikai kapcsolatok alternatív útvonalakat biztosítanak, így a hálózat egy kapcsolat vagy port meghibásodása esetén még mindig működőképes marad. A redundáns útvonalak ezen felül a forgalmat is képesek megosztani és növelik a hálózat terhelhetőségét.

A többszörös kapcsolatokat úgy kell megvalósítani, hogy második rétegbeli hurkok ne képződhessenek. Ki kell választani a legjobb útvonalakat, és meghibásodásuk esetén az azonnal elérhető alternatív utakat is. A második rétegbeli redundancia kezeléséért a feszítőfa protokollok (Spanning Tree Protocol, STP) felelnek.

A többrétegű kapcsolók vagy forgalomirányítók redundáns megoldást biztosíthatnak a kliens számára, és alternatív alapértelmezett átjárót szolgáltatnak abban az esetben, ha az elsődleges meghibásodik. Így a kliens az alapértelmezett átjárókat több útvonalon is elérheti. Az alapértelmezett átjárók hozzárendeléséért az első ugrás redundancia protokollok (First Hop Redundancy Protocols, FHRP) felelősek, és az elsődleges alapértelmezett átjáró meghibásodása esetén alternatív megoldást biztosíthatnak.

Ez a fejezet a redundancia előzőekben említett formáihoz kapcsolódó protokollokkal foglalkozik. Áttekinti továbbá a redundanciához kapcsolódó lehetséges problémákat és tüneteiket is.

**Csoportos feladat - Viharos forgalom**

**Viharos forgalom**

Ez az első napunk hálózati rendszergazdaként egy kis vagy közepes méretű vállalatnál. Az előző rendszergazda egy hálózatfejlesztés után hirtelen távozott.

A fejlesztés során egy kapcsolóval bővült a hálózat, de azóta több kolléga panaszkodott az internet és a hálózat szerverei elérésének nehézségeire. Tulajdonképpen nagyrészüknek egyáltalán nincs hálózati kapcsolata. A főnökünk megkért, hogy azonnal vizsgáljuk ki a kapcsolódási problémák okait.

Először megnézzük a hálózatot alkotó berendezéseket az épület fő elosztóközpontjában. Azt tapasztaljuk, hogy a hálózati topológia látszólag helyes, a kábeleket megfelelően csatlakoztatták, a forgalomirányítók és kapcsolók áramellátása jó és működnek is, a kapcsolókat pedig a biztonsági és a redundancia megfontolások szerint telepítették.

Egyvalamit viszont azonnal észreveszünk: a kapcsolók állapotjelzői állandóan villognak, de olyan gyorsan, hogy szinte folyamatos világításnak tűnik. Úgy gondoljuk, megtaláltuk az alkalmazottak kapcsolódási problémáinak forrását.

Keressünk információkat az STP-ről az interneten! A keresés során jegyzeteljünk és magyarázzuk meg az alábbiakat:

* Szórási vihar (broadcast storm)
* Kapcsolási hurkok (switching loops)
* Az STP célja
* Az STP változatai

Válaszoljuk meg a feladathoz tartozó PDF-ben levő kérdéseket! Mentsük el a munkánkat és készüljünk fel arra, hogy a csoporttal megosszuk a válaszainkat!

[Csoportos feladat - Viharos forgalom](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.0.1.2%20Stormy%20Traffic%20Instructions.pdf)

**Redundancia az OSI modell 1. és 2. rétegeiben**

A központi, elosztási és hozzáférési rétegekből álló háromszintű hierarchikus hálózattervezési módszer redundancia használatával segíti a hálózat sérülékeny pontjainak kiküszöbölését. A kapcsolók közt megvalósított többszörös kábelezés biztosítja a kapcsolt hálózat fizikai redundanciáját. Ez növeli a megbízhatóságot és a hálózat rendelkezésre állását. A hálózaton áthaladó adatok számára biztosított alternatív útvonalak lehetővé teszik, hogy a felhasználók azok zavara esetén is hozzáférjenek az erőforrásokhoz.

Kattintsunk az első ábrán a **Play** gombra a redundanciáról szóló animáció megtekintéséhez.

* A PC1 a PC4-gyel redundáns hálózati topológián keresztül kommunikál.
* Amikor az S1 és az S2 között megszakad a hálózati kapcsolat, a PC1 és a PC4 közötti útvonal a szakadás kiküszöbölésére automatikusan átállítódik.
* Amikor az S1 és az S2 között ismét helyreáll a kapcsolat, az útvonal is helyreáll a PC4 irányába az S1-S2 közvetlen útra.

Sok szervezet számára a hálózat elérhetősége a céges munkamenet alapszükséglete, tehát a hálózati infrastruktúra helyes tervezése létfontosságú. Redundáns útvonalak segítségével megszüntethetők a hálózat kritikus pontjai.

**Megjegyzés**: Az 1. rétegbeli redundanciát általában többszörözött kapcsolatokkal és eszközökkel illusztráljuk, de a hálózat teljes megvalósításához nem csak a fizikai réteg figyelembe vétele szükséges. Ahhoz, hogy a redundancia elérje a célját, 2. rétegbeli protokollok is szükségesek, például a feszítőfa protokoll (Spanning Tree Protocol, STP).

A redundancia a hierarchikus tervezés fontos eszköze a hálózati szolgáltatások zavarainak megelőzésére. A redundáns hálózatokhoz további fizikai útvonalak hozzáadása szükséges, de a tervezés során a logikai redundanciát is szem előtt kell tartani. Ugyanakkor a kapcsolt Ethernet hálózatban a redundáns útvonalak egyaránt vezethetnek fizikai és 2. rétegbeli hurkok keletkezéséhez.

A 2. rétegbeli logikai hurkok a kapcsolók természetes működése miatt jönnek létre, konkrétan az automatikus tanulás és továbbítás módszer miatt. Amikor két eszköz között több út is létezik és a kapcsolók nem használnak feszítőfa megoldásokat, 2. rétegbeli hurok jön létre. Ez három fő problémát okoz, melyeket a 2. ábrán láthatunk.

**Az 1. rétegbeli redundancia problémái: MAC-adatbázis instabilitás**

Az Ethernet kereteknek nincs élettartam (time to live, TTL) tulajdonságuk. Emiatt nincs beépített megoldás az ellen, hogy a kapcsolók a kereteket végtelenségig, vagy valamelyik kapcsolat megszakadásáig (és ezzel a hurok megszűnéséig) továbbítsák egymás között. A szórásos keretek ezen folytonos továbbítása okozza a MAC-adatbázis instabilitást.

A szórásos keretek minden kapcsolóporton továbbítódnak az eredeti beérkező portot kivéve. Ez biztosítja azt, hogy a szórási tartomány minden eszköze megkapja a keretet. Ha több úton lehet a keretet a cél felé továbbítani, végtelen hurok jöhet létre. Amikor a hurok létrejön, a kapcsoló MAC-cím táblázata a szórásos keretek alapján folyamatosan változni fog, ami MAC-adatbázis instabilitáshoz vezet.

Kattintsunk a **Play** gombra az animáció megtekintéséhez. Amikor az animáció megáll, olvassuk el a topológiától balra levő szöveget. Az animáció rövid szünet után folytatódik.

Az animációban:

* A PC1 szórásos keretet küld az S2-nek. Az S2 a szórásos keretet az F0/11-es portján fogadja. A szórásos keret megérkezésekor az S2 módosítja a MAC-táblázatát, beleírja, hogy a PC1 az F0/11-es portján érhető el.
* Mivel a keret szórásos, az S2 azt minden portján továbbítja, így a Trunk1 és a Trunk2 portjain is. Amikor a szórásos keret az S3-ra és az S1-re megérkezik, a kapcsolók frissítik a MAC-táblázatukat, miszerint a PC1 az S1 F0/1-es portján, az S3 F0/2-es portján érhető el.
* Mivel a keret szórt, az S3 és az S1 is továbbítja minden portján a bejövőt kivéve. Az S3 a PC1-től érkező szórásos keretet az S1-nek is továbbítja. Ugyanígy az S1 a PC1-től érkező szórásos keretet az S3-nak is továbbítja. Minden kapcsoló frissíti a MAC-táblázatát a PC1-ről, csak már helytelen portokkal.
* Mindkét kapcsoló minden portján (kivéve a bejövőt) továbbítja a szórásos keretet, ami így kétfelől is megérkezik az S2-be.
* Amikor az S2 megkapja az S3-tól és az S1-től a szórásos keretet, frissíti a MAC-tábláját, mindig a legutolsóként fogadott keret információjával.

Ez a folyamat ismétlődik újra és újra mindaddig, amíg a hurkot alkotó valamelyik kapcsolatot fizikailag meg nem szüntetjük, vagy a hurokban részt vevő valamelyik kapcsolót le nem kapcsoljuk. Ez a hurokban szereplő minden kapcsolón magas processzorhasználatot okoz, mivel a kapcsolók ugyanazt a keretet továbbítják folyamatosan oda-vissza. A valódi forgalom feldolgozása emiatt lelassul.

A hurokban érintett állomás nem képes elérni a hálózat többi állomását, mivel a MAC-táblázat folyamatos változása miatt a kapcsoló nem tudja, hogy az egyedi kereteket melyik portjára kellene továbbítania. A fenti példában a kapcsolók helytelen portot tárolnak a PC1-hez. Minden a PC1-nek címzett egyedi keret szintén belekerül a hurokba a szórásos keretek mellé, így egyre több keret szorul be, a hálózat szórási vihart generál.

# Az 1. rétegbeli redundancia problémái: szórási viharok

Szórási viharnak (broadcast storm) nevezzük, amikor olyan sok szórásos keret kerül bele a 2. rétegbeli hurokba, hogy ez a teljes sávszélességet felemészti. Következésképpen a valódi forgalom számára nem marad elérhető sávszélesség, a hálózat elérhetetlenné válik. Ez tulajdonképpen egyfajta szolgáltatásmegtagadás (Denial of Service, DoS).

Hurkot tartalmazó hálózatban a szórási vihar elkerülhetetlen. Ahogy egyre több eszköz küld szórásos forgalmat, egyre több keret kerül bele a hurokba és emészti fel az erőforrásokat. Ez végül szórási viharhoz vezet és a hálózat nem működik többé.

A szórási viharoknak vannak egyéb következményei is. Mivel a szórásos forgalmat minden kapcsoló minden portján továbbítja, minden hozzá csatlakoztatott eszköznek szintén fel kell dolgoznia a hurokban végtelenségig továbbított szórásos kereteket. Ez a végberendezések hibás működéséhez is vezethet, mivel a nagy forgalom leterheli a hálózati kártya feldolgozóegységét.

Kattintsunk az ábrán a **Play** gombra a szórási viharról szóló animáció megtekintéséhez. Amikor az animáció megáll, olvassuk el a topológiától jobbra levő szöveget. Az animáció rövid szünet után folytatódik.

Az animációban:

* A PC1 szórásos keretet küld a hurkot tartalmazó hálózatba.
* A szórásos forgalom a kapcsolási hurokba kerül.
* A PC4 szintén küld egy szórásos keretet ugyanebbe a hálózatba.
* A PC4 kerete ugyanúgy belekerül a kapcsolók által alkotott hurokba, ahol már a PC1 kerete is kering.
* Ahogy egyre több eszköz küld szórásos forgalmat, egyre több keret kerül bele a hurokba és emészti fel az erőforrásokat. Ez végül szórási viharhoz és a hálózat leállásához vezet.
* Amikor a hálózat teljesen telített a hurokban keringő szórásos forgalommal, a kapcsolók az új kereteket eldobják, mert képtelenek feldolgozni.

Szórási vihar akár másodpercek alatt is kialakulhat, mert a hálózat eszközei rendszeresen küldenek szórásos kereteket, ilyenek például az ARP-kérések is. Emiatt egy hurok kialakulása után a kapcsolt hálózat nagyon gyorsan összeomlik.

# Az 1. rétegbeli redundancia problémái: duplikált egyedi keretek

A hurkok nem csak a szórásos kereteket érintik. A hurkot tartalmazó hálózatba küldött egyedi keretek esetenként megkettőzve érnek a céljukhoz.

Kattintsunk az ábrán a **Play** gombra a problémáról szóló animáció megtekintéséhez. Amikor az animáció megáll, olvassuk el a topológiától jobbra levő szöveget. Az animáció rövid szünet után folytatódik.

Az animációban:

* A PC1 egyedi keretet küld a PC4-nek.
* Az S2-nek nincs a MAC-táblában a PC4-hez tartozó bejegyzése, ezért a PC4 megtalálásának érdekében a beérkezőt kivéve minden portját elárasztja az egyedi kerettel.
* A keret megérkezik az S1 és az S3 kapcsolókra.
* Az S1-nek van bejegyzése a PC4-ről, ezért kiküldi neki a keretet.
* Az S3-nak szintén van bejegyzése a PC4-hez, ezért az egyedi keretet a Trunk3 kapcsolatán átküldi az S1-nek.
* Az S1-hez megérkezik a keret másolata is, ezt is továbbítja a PC4-nek.
* A PC4 kétszer kapja meg ugyan azt a keretet.

A legtöbb felsőbb rétegbeli protokoll nincs felkészítve arra, hogy felismerje a duplikált üzeneteket. Általában véve a sorszámozást használó protokollok azt feltételezik, hogy az átvitel sikertelen volt és a sorszámot újra felhasználták egy másik kommunikációs munkamenetben. Más protokollok a duplikált forgalmat továbbítják a megfelelő felsőbb protokoll számára, hogy feldolgozza, esetleg eldobja azt.

A 2. rétegbeli LAN-protokollok, amilyen az Ethernet is, nem tartalmaznak mechanizmust a végtelenségig keringő üzenetek felismerésére. Bizonyos 3. rétegbeli protokollok TTL-alapú (élettartam) módszerrel korlátozzák le, hogy a Layer 3 eszközök legfeljebb hányszor továbbíthassák a csomagot. A 2. rétegbeli eszközök nem használnak ilyet, a hurokba került forgalmat végtelenségig továbbítják. A probléma kiküszöbölésére az STP-t, a 2. rétegbeli hurok elkerülésére szolgáló módszert fejlesztették ki.

Az ilyen problémák megelőzésére a redundáns hálózatokban valamilyen feszítőfa protokollt kell engedélyeznünk a kapcsolókon. A 2. rétegbeli hurkok megelőzésének érdekében a feszítőfa a Cisco kapcsolókon alapértelmezés szerint engedélyezve van.

# Packet Tracer - Egy redundancia-terv vizsgálata

**Esetleírás**

Ebben a feladatban az STP alapértelmezés szerinti viselkedését fogjuk megfigyelni, valamint azt, hogy hogyan reagál a hibákra. A kapcsolókat gyári állapotukban kötöttük hálózatba. A Cisco kapcsolók a rendszergazda beavatkozása (konfigurálás) nélkül csatlakoztathatók a hálózathoz. A feladat kedvéért mindössze a hídprioritást változtattuk meg.

[Packet Tracer - Examining a Redundant Design Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.1.1.5%20Packet%20Tracer%20-%20Examining%20a%20Redundant%20Design%20Instructions.pdf)

[Packet Tracer - Examining a Redundant Design - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.1.1.5%20Packet%20Tracer%20-%20Examining%20a%20Redundant%20Design.pka)

**STP algoritmus: bevezetés**

A redundancia úgy növeli a hálózat rendelkezésre állását, hogy megvédi a hálózatot a kritikus pontok (egyetlen kábel vagy kapcsoló) meghibásodásának hatásaitól. Amikor egy hálózatba fizikai redundanciát építünk, hurkok keletkezhetnek és duplikált keretek jöhetnek létre. Mindkettő súlyos következményekkel járhat a kapcsolt hálózat működésére nézve. A probléma megoldására fejlesztették ki a feszítőfa protokollt (Spanning Tree Protocol, STP).

Az STP biztosítja, hogy a hálózat bármely két eszköze között csak egy logikai útvonal létezzen, mivel a hurok keletkezéséhez vezető redundáns utakat lezárja. A lezárt porton nem érkezik és nem távozik felhasználói adat. Ez nem érinti az STP által használt BPDU-kereteket (Bridge Protocol Data Unit, hídprotokoll adategység). A redundáns útvonalak lezárása a hurkok megelőzésének legfontosabb eleme. A fizikai útvonalak a redundancia érdekében továbbra is léteznek, de a hurkok megelőzése miatt letiltottak. Ha hálózati kábel vagy kapcsoló hibája miatt ismét szükség lenne az útvonalra, az STP újratervezi azokat és szükség szerint engedélyezi a korábban lezárt portokat.

Kattintsunk az 1. ábrán a **Play** gombra az STP-t működésének megtekintéséhez.

Ebben a példában minden kapcsolón aktív az STP:

* A PC1 szórást küld a hálózatba.
* Az S2-n az STP a Trunk2 portot lezárt módba állította. Lezárt módban a port felhasználói adatokat nem továbbít, így akadályozza meg hurok kialakulását. Az S2 a szórásos keretet minden kapcsolóportján továbbítja, kivéve a PC1 felé esőt (onnan érkezett), valamint a Trunk2 irányában levőt.
* Az S1 megkapja a szórásos keretet és továbbítja minden kapcsolóportján, így megérkezik a PC4-hez és az S3-hoz. Az S3 továbbítja a keretet a Trunk2 felé vezető portján, az S2 pedig eldobja. Nem alakul ki 2. rétegbeli hurok.

Kattintsunk a 2. ábrán a **Play** gombra, hogy megnézzük az STP újraszámítási műveletét hiba esetén.

Az STP hurokmentes útvonalakat hoz létre portok lezárásával a hálózat megfelelő pontjain. Az STP a hálózat hibáit úgy javítja, hogy a korábban lezárt portokat újra aktiválja és így a forgalom egy alternatív útvonalon továbbhaladhat.

A módszerre eddig a feszítőfa protokoll kifejezést és angol rövidítését, az STP-t használtuk. Azonban a kifejezés és a rövidítés használata bizonyos esetekben félrevezető lehet. A szakemberek ezt a rövidítést a feszítőfa különböző megvalósításainak közös említésekor használják, ilyenek például a Rapid Spanning Tree Protocol (RSTP) és a Multiple Spanning Tree Protocol (MSTP). Ha helyesen szeretnénk a feszítőfa módszerek elveiről beszélni, fontos, hogy a megfelelő konkrét megvalósítási módot vagy szabványt említsük. A feszítőfa legutolsó IEEE dokumentuma (IEEE-802-1D-2004) szerint "az STP-t mostanra leváltotta az RSTP". Az IEEE az STP alatt a feszítőfa eredeti megvalósítását érti, az RSTP alatt pedig az IEEE-802-1D-2004-ben leírt változatot. Ebben a tananyagban, amikor az eredeti feszítőfa protokollt tárgyaljuk, a félreértések elkerülése végett úgy hivatkozunk rá, hogy "az eredeti 802.1D feszítőfa". Mivel a két protokoll nagy része ugyanazt a terminológiát és módszereket használja, elsősorban a jelenlegi szabványokra és az STP és az RSTP Cisco általi megvalósításaira fogunk koncentrálni.

**Megjegyzés**: Az STP egy Radia Perlman által kifejlesztett algoritmuson alapul, amelyet akkor alkotott meg, amikor a Digital Equipment Corporationnál dolgozott. 1985-ös publikációjának eredeti címe "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN"

.

**Feszítőfa algoritmus: port szerepek**

Az IEEE 802.1D az STP és az RSTP feszítőfa algoritmust (Spanning Tree Algorithm, STA) használja annak a meghatározására, hogy a hálózat melyik portjait kell lezárni a hurkok megakadályozásának érdekében. Az STA kiválaszt egy kapcsolót, amelyet gyökérponti hídnak (root bridge) nevezünk, ez lesz minden útvonalszámítás referencia pontja. Az ábrán látható gyökérponti hidat (S1 kapcsoló) egy választási folyamat jelöli ki. Az STP-ben részt vevő összes kapcsoló BPDU-kereteket vált egymással, hogy meghatározzák, melyiküknek a legalacsonyabb a hídazonosítója (bridge ID, BID) a hálózatban. A legalacsonyabb hídazonosítójú kapcsoló lesz automatikusan az STA-számítások gyökérponti hídja.

**Megjegyzés**: Az egyszerűség kedvéért ott, ahol nincs külön feltüntetve, minden kapcsoló minden portja a VLAN 1-hez van rendelve. Minden kapcsoló egyedi MAC-címmel vesz részt a VLAN 1-ben.

A BPDU a kapcsolók között használt STP-üzenetváltásás kerete, mely tartalmazza a küldő kapcsoló hídazonosítóját (BID). A BID egy prioritás értékből, a küldő kapcsoló MAC-címéből és egy opcionális kiterjesztett rendszer azonosítóból (extended system ID) áll. A három mező egyesített értékét használják, így határozzák meg a legalacsonyabb hídazonosítót.

Miután megvan a gyökérponti híd, az STA meghatározza a gyökérponti híd felé vezető legrövidebb utat. Minden kapcsoló STA-val eldönti, hogy melyik portokat kell lezárni. Amíg az STA a kapcsolókon a gyökérponti híd felé vezető legrövidebb utakat számolja, a hálózat forgalmát a kapcsolók nem továbbítják. Az STA a lezárandó portok meghatározásánál az utak és a portok költségével is számol. A gyökérponti hídig vezető útvonal összköltsége az útvonal kapcsolói portsebességeihez tartozó költségek összege. Több lehetséges útvonal közül az STA a legalacsonyabb költségűt választja.

Amikor az STA minden kapcsolóhoz viszonyítva megállapította a legelőnyösebb utakat, a kapcsolók portjahoz szerepeket rendel. A port szerepek a gyökérponti hídhoz viszonyított kapcsolatot és a forgalom továbbíthatóságát mutatják meg.

* **Gyökérportok (root ports)** - A gyökérponti hídhoz legközelebbi kapcsolóportok. Az ábrán az S2 gyökérportja az F0/1, mely az S2 és az S1 közti trönkvonalon van (itt trönk a kapcsolók közötti gerincvonalat jelenti). Az S3 gyökérportja az F0/1, az S3 és az S1 közötti trönkön. Kapcsolónként csak egy gyökérport van.
* **Kijelölt portok (designated ports)** - Minden olyan, a hálózatba forgalmat továbbító port, amely nem gyökérport. Az ábrán az S1 F0/1 és F0/2 portjai kijelölt portok. Az S2 F0/2-es portja szintén kijelölt port. A kijelölt portok a trönk kapcsolaton (gerincvonalon) találhatók. Ha egy trönk egyik vége gyökérport, a másik vége kijelölt port lesz. Egy gyökérponti híd minden portja kijelölt port.
* **Alternatív és tartalék portok (alternate and bacup ports)** - Az alternatív és a tartalék portok a hurkok megelőzése céljából lezárt állapotban vannak. Az ábrán az STA az S3 F0/2 portját alternatív porttá tette. Az S3 F0/2-es portja tehát le van zárva. Azokon a trönkvonalakon jönnek létre alternatív portok, amelyeknek egyik vége sem gyökérport. Figyeljük meg az ábrán, hogy a gerincvonal egyik vége van csak lezárva. Ez teszi lehetővé, hogy szükség esetén gyorsabban továbbító állapotba kerüljön. (A portok lezárása akkor történik meg, amikor azonos kapcsolón két port redundáns kapcsolatot képezne.)
* **Letiltott portok (disabled ports)** - Olyan kapcsoló port, amely le van kapcsolva (shut down).

**Megjegyzés:** Ezek az RSTP-nél definált port szerepek. A 802.1D STP eredetileg úgy hívta az**alternatív és tartalék portokat,** hogy**nem kijelölt.**

# Feszítőfa algoritmus: gyökérponti híd

Amint az 1. ábrán látható, minden feszítőfában (kapcsolt LAN vagy szórási tartomány) van egy gyökérponti hídnak nevezett kapcsoló. A gyökérponti híd az alapja minden olyan feszítőfa számításnak, amely a redundáns útvonalak letiltását célozza.

A gyökérponti híd meghatározása választási folyamat során történik.

A 2. ábra a BID (bridge ID, hídazonosító) mezőit mutatja. A BID egy prioritás értékből, egy kiterjesztett rendszerazonosítóból és a kapcsoló MAC-címéből áll.

A szórási tartomány minden kapcsolója részt vesz a választásban. Miután egy kapcsoló elindul, két másodpercenként BPDU-kereteket kezd küldeni, melyek a kapcsoló hídazonosítóját és a gyökér azonosítóját (root ID) tartalmazzák.

Amikor a kapcsolók elküldik BPDU-keretüket, a szomszéd kapcsolóik megnézik a BPDU-keret gyökér azonosító mezőjét. Ha az érkezett BPDU gyökér azonosítója alacsonyabb, mint a fogadó kapcsoló root ID-je, a kapcsoló frissíti a gyökér azonosítóját és a szomszéd kapcsolót fogja gyökérponti hídként elismerni. Ez nem mindig a tényleges szomszédot jelenti, lehet a szórási tartomány bármelyik kapcsolója is. Ezután a kapcsoló továbbküldi az új BPDU-kereteket az alacsonyabb gyökér azonosítóval a szomszédainak. A folyamat végére a legalacsonyabb hídazonosítójú kapcsolót fogja gyökérponti hídként ismerni az egész feszítőfa.

Minden feszítőfában külön-külön választanak gyökérponti hidat. Így egy hálózatban több különböző gyökérponti híd is létezhet. Ha minden kapcsoló minden portja a VLAN 1-be tartozik, akkor csak egyetlen feszítőfa létezik. A különböző feszítőfa példányok kialakításában a kiterjesztett rendszerazonosító játszik fontos szerepet.

# Feszítőfa algoritmus: útvonalak költsége

Amint egy feszítőfa példány kiválasztotta a gyökérponti hídját, az STA megkezdi a szórási tartomány minden eszközétől a gyökérponti híd felé vezető legjobb útvonalak meghatározását. Az útvonal minőségének jelzője a céltól a gyökérponti híd felé vezető út egyes portjaihoz rendelt költségek összege. Cél alatt egy kapcsolóportot értünk.

Az alapértelmezett port költség a port sebességéből adódik. Az 1. ábrán látható, hogy a 10 Gb/s Ethernet portok költsége 2, az 1 Gb/s Ethernet portoké 4, a 100 Mb/s Fast Ethernet portok költsége 19, a 10 Mb/s Ethernet portoké pedig 100.

**Megjegyzés**: Ahogy egyre újabb és gyorsabb Ethernet technológiák terjednek el, a költség értékek az új sebességeknek megfelelően változhatnak. A táblázat nem lineáris számai is a régebbi Ethernet szabványokhoz képesti fejlődést mutatják, mivel az értékeket már a 10 Gb/s Ethernethez igazították. Például a nagy sebességű hálózatokban található Catalyst 4500 és 6500 kapcsolók más költségszámítási módszert használnak, ott a 10 Gb/s költsége 2000, a 100 Gb/s útvonalé 200, az 1 Tb/s költsége pedig 20.

Habár a kapcsolóportokhoz alapértelmezett költség értéket rendeltek, az érték konfigurálható. A rendszergazda az egyes portok költségének beállításával rugalmasan képes befolyásolni a gyökérponti hídhoz vezető feszítőfa utakat.

Egy interfész port költségének beállításához a "spanning-tree cost <érték>" parancsot használhatjuk interfész konfigurációs módban (lásd 2. ábra). Az érték 1 és 200 000 000 közé eshet.

A példában az F0/1 kapcsolóport költségét 25-re állítottuk a "spanning-tree cost 25" interfész konfigurációs paranccsal.

Az alapértelmezett 19-es költséget visszaállíthatjuk a "no spanning-tree cost" interfész konfigurációs paranccsal.

Egy útvonal össszköltsége a gyökérponti híd felé vezető útvonalon levő portok költségeinek összege (lásd 3. ábra). A legalacsonyabb költségű útvonal a legelőnyösebb, minden más redundáns útvonal pedig le lesz tiltva. Az példában az S2 és az S1 gyökérponti híd közötti 1-es útvonal költsége 19 (az IEEE szerinti alapértelmezett költségekkel), a 2-es útvonal költsége pedig 38. Mivel az 1-es útvonal költsége alacsonyabb, ez az előnyösebb, a redundáns útvonalat az STP letiltja, így nem jön létre hurok.

A port és útvonal költségek lekérdezése a "show spanning-tree" paranccsal lehetséges (lásd 4. ábra). A parancskimenet felső részén található "Cost" mező értéke a gyökérponti hídig vezető útvonal teljes költsége. Ez függ attól is, hogy hány kapcsolóporton keresztül vezet út a gyökérponti hídig. A parancskimenetben látható, hogy minden interfészhez külön port költség tartozik, jelen esetben ez 19.

# Az RSTP portszerepi

A példában az S1 a gyökérponti híd. Az S2 és az S3 kapcsolók S1 felé mutató portjai a gyökérportok (R).

Miután a kapcsoló meghatározta a gyökérportokat, meg kell állapítania, hogy melyek lesznek a kijelölt és az alternatív portok.

A gyökérponti híd automatikusan minden portját kijelölt porttá teszi (D). A többi kapcsoló nem gyökérportjai kijelölt vagy alternatív portok lesznek.

Minden LAN-szegmensen (összeköttetésen) van kijelölt port. Két azonos szegmensen levő kapcsoló a gyökérportok meghatározása után eldönti, hogy melyik port legyen kijelölt port és melyik marad alternatív port.

A LAN-szegmens kapcsolói BPDU-kereteket cserélnek egymással, mely tartalmazza a kapcsoló hídazonosítóját. Általában az alacsonyabb hídazonosítójú kapcsoló portja lesz kijelölt port, a magasabbé pedig alternatív port. Azonban emlékezzünk, hogy az első szempont a gyökérponti híd felé vezető alacsonyabb útvonalköltség, a küldő hídazonosítója csak akkor dönt, ha a költségek egyenlőek.

Minden kapcsoló meghatározza portjainak szerepét, hogy végül hurokmentes feszítőfa jöjjön létre.

Az 1-7-ig számozott ábrák bemutatják a port szerepek meghatározásának műveletsorát.

# Kijelölt és alternatív portok

Amikor egy kapcsoló a gyökérportját próbálja meghatározni, összehasonlítja az összes, a feszítőfában részt vevő portjának útvonal költségeit. A legalacsonyabb összköltségű útvonallal rendelkező port automatikusan gyökérport lesz, hiszen ő van a legközelebb a gyökérponti hídhoz. Egy kapcsolt hálózatban minden olyan kapcsolónak, amely nem gyökérponti híd, egyetlen gyökérportja lesz, az amelyik a gyökérponti híd felé a legalacsonyabb költségű utat biztosítja.

**Megjegyzés**: A hálózati topológiában minden olyan kapcsolónak, amely nem gyökérponti híd csak egy gyökérportja van.

Az ábrán egy négy kapcsolóból álló topológia látható. Ha megnézzük a port szerepeket, akkor az S3 kapcsoló F0/1 és az S4 kapcsoló F0/3 portjai lesznek a gyökérportok, mert ezek gyökérponti híd felé vezető útvonal költségei a legjobbak.

Az S2-nek két egyenlő költségű portja vezet a gyökérponti híd felé, az F0/1 és az F0/2. Ebben az esetben a szomszédos kapcsolók, S3 és S4 hídazonosítói fogják eldönteni a kérdést. Ezt a küldő hídazonosítójának hívjuk. Az S3 hídazonosítója 24577.5555.5555.5555, az S4-é pedig 24577.1111.1111.1111. Mivel az S4 hídazonosítója alacsonyabb, az S2 F0/1-es, S4-hez kapcsolódó portja lesz a gyökérport.

**Megjegyzés**: A hídazonosítók az ábrán nem szerepelnek.

Ezután a közös kapcsolatokon (szegmens, trönk) ki kell választani a kijelölt portokat. Az S2 és az S3 ugyanazon a LAN-kapcsolaton vannak, BPDU-kat cserélnek egymással. Az STP eldönti, hogy S2 F0/2-es vagy S3 F0/2-es portja lesz-e a szegmens kijelölt portja. A gyökérponti híd felé vezető alacsonyabb költségű útvonallal (gyökér útvonal) rendelkező kapcsoló portja lesz a kijelölt port. Az S3 F0/2-es portjának a gyökérponti híd felé vezető útvonala alacsonyabb költségű, tehát ez lesz a kijelölt port.

Az S2 és az S4 ugyanezt a gondolatmenetet hajtja végre a közös szegmensükön. Az S4 F0/1-es portjának költsége alacsonyabb, tehát ő lesz a kijelölt port.

Minden port megkapta STP port szerepét, kivéve az S2 F0/2-es portja. Az S2 F0/1-es portja már a kapcsoló gyökérportja. Mivel az S3 F0/2-es portja a szegmens kijelölt portja, az S2 F0/2-es portja alternatív port lesz.

A kijelölt port küld és fogad forgalmat a szegmensről, mivel rajta keresztül vezet a legjobb útvonal a gyökérponti hídhoz. Az alternatív port nem fogad és nem is küld forgalmat. Ez az STP hurokmegelőző eljárása.

# 802.1D BPDU keretformátum

A feszítőfa algoritmus a gyökérponti híd meghatározását BPDU-k küldésével végzi. A BPDU-keret 12 különböző mezőt tartalmaz, amelyek útvonal és prioritás információt hordoznak, segítségükkel határozható meg a gyökérponti híd és a felé vezető útvonal.

További információért kattintsunk az 1. ábrán a BPDU-mezőkre!

* Az első négy mező a protokoll, a verzió, az üzenet típus és a státusz jelző.
* A következő négy mező azonosítja a gyökponti hidat és a felé vezető útvonal költségét.
* Az utolsó négy mező időzítésre szolgál, hogy milyen gyakran kell BPDU-üzeneteket küldeni és mennyi ideig kell a BPDU-folyamat által kapott információkat megtartani.

A 2. ábrán egy a Wireshark által elfogott BPDU látható. A példában szereplő BPDU több mezőt tartalmaz, mint amit az előbb leírtunk. A BPDU-üzenet a hálózaton Ethernet keretbe ágyazva halad. A 802.3 fejlécben szerepel a BPDU-keret forrás- és célcíme. A keret cél MAC-címe a 01:80:C2:00:00:00, ez a feszítőfa csoportcíme. Amikor ilyen célcímű keret érkezik, a feszítőfát futtató összes kapcsoló elfogadja a keretet és megnézi a benne szereplő információkat. A hálózat többi eszköze eldobja a keretet.

A példában szereplő BPDU gyökérazonosítója és hídazonosítója ugyanaz. Ez azt jelenti, hogy a keretet a gyökérponti hídtól fogtuk el. Az időzítők az alapértelmezett értéken állnak.

**802.1D BPDU működése**

A szórási tartomány minden kapcsolója úgy indítja az algoritmust, hogy saját magát képzeli gyökérponti hídnak, a kiküldött BPDU-keretekben saját hídazonosítója lesz a gyökér azonosító. Alapértelmezés szerint a kapcsoló elindulása után két másodpercenként küld BPDU-kereteket. A BPDU-keretben meghatározott "hello" időzítő értéke 2 másodperc. Minden kapcsoló helyileg nyilvántartja a saját hídazonosítóját, a gyökér azonosítóját és a gyökér felé vezető útvonal költségét.

Amikor a szomszédos kapcsolók megkapják a BPDU-keretet, összehasonlítják a keretben szereplő gyökér azonosítót a saját gyökér azonosítójukkal. Ha a BPDU-keretben alacsonyabb gyökér azonosító érkezett, mint a saját magunk által nyilvántartott, a kapcsoló felülírja a saját gyökér azonosítóját és ezt küldi ki a BPDU-üzeneteiben is. Ezek a hálózat számára új gyökérponti hidat jeleznek. A gyökérponti híd felé vezető távolságot az útvonal költség frissítés jelzi. Például, ha a BPDU-t Fast Ethernet porton fogadta a kapcsoló, az útvonal költsége 19-cel növekszik. Ha a helyi gyökér azonosító alacsonyabb, mint ami érkezett, a kapcsoló eldobja a BPDU-keretet.

Miután a gyökér azonosító frissült az új gyökérponti hídnak megfelelően, minden további kiküldött BPDU-keret az új gyökér azonosítót és a módosított útvonal költséget fogja tartalmazni. Így az összes szomszédos kapcsoló látja a mindenkori legalacsonyabb gyökér azonosítót. Ahogy a BPDU keresztülhalad a kapcsolókon, azok az útvonal költségét folyamatosan frissítik, hogy a gyökérponti hídig vezető összköltséget mutassa. A feszítőfa összes kapcsolója ezeket az útvonal költségeket használja arra, hogy meghatározza a gyökérponti hídig vezető lehetséges legjobb útvonalat.

A BPDU-folyamat összefoglalása:

**Megjegyzés**: A gyökérponti híd kiválasztásának alap szempontja a prioritás. Ha minden kapcsoló prioritása azonos, a legalacsonyabb MAC-című lesz a gyökérponti híd.

* Kezdetben minden kapcsoló saját magát tartja gyökérponti hídnak. Az S2 BPDU-kereteket küld ki minden portján. (1. ábra)
* Amikor az S3 BPDU-t kap az S2-től, összehasonlítja a saját gyökér azonosítóját a BPDU-ban levővel. Mivel a prioritások azonosak, meg kell vizsgálni a MAC-cím részt, hogy melyik cím alacsonyabb. Az S2 MAC-címe alacsonyabb, tehát S3 felülírja a gyökér azonosítóját az S2 gyökér azonosítójával. Jelenleg az S3 az S2-t tartja gyökérponti hídnak. (2. ábra)
* Az S1 összehasonlítja a gyökér azonosítóját a BPDU-ban levővel, azt látja, hogy a sajátja alacsonyabb, tehát az S2 BPDU-ját nem veszi figyelembe. (3. ábra)
* Az S3 kiküldi BPDU-kereteit, amelyben a gyökér azonosító az S2 BID-je. (4. ábra)
* Az S2 megkapja a BPDU-t, de eldobja, mert látja, hogy a benne szereplő gyökér azonosító ugyanaz, mint a sajátja. (5. ábra)
* Az S1 szintén eldobja az S3-tól érkező BPDU-t, mert neki alacsonyabb gyökér azonosítója van eltárolva, mint ami érkezett. (6. ábra)
* Az S1 kiküldi BPDU-kereteit. (7. ábra)
* Az S3 észleli, hogy a keretben levő gyökér azonosító alacsonyabb, mint az övé, frissíti a sajátját, ezzel elismeri az S1-et gyökérponti hídként. (8. ábra)
* Az S2 szintén azt látja, hogy a BPDU-ban levő gyökér azonosító alacsonyabb, mint az ő eltárolt értéke, ezért frissíti azt és az S1-et könyveli el gyökérponti hídként. (9. ábra)

**Kiterjesztett rendszer azonosító**

A hálózat gyökérponti hídja a hídazonosító (BID) segítségével határozható meg. A BPDU-keret BID-mezője három külön részből áll:

* hídprioritás (bridge priority)
* kiterjesztett rendszer azonosító (Extended system ID)
* MAC-cím

Mindegyik mezőnek szerepe van a gyökérponti híd választásakor.

**Hídprioritás**

A hídprioritás olyan módosítható számérték, amelyet a gyökérponti híd választásának befolyásolásához használhatunk. A legalacsonyabb prioritással, tehát a legkisebb hídazonosítóval rendelkező kapcsoló lesz a gyökérponti híd, mivel az alacsonyabb számérték az erősebb. Például, ha egy bizonyos kapcsolót szeretnénk mindig gyökérponti hídként látni, állítsuk a prioritását a többi kapcsolóénál alacsonyabb értékre. A Cisco kapcsolók alapértelmezett prioritása 32768. Az érték 0 és 61440 közé eshet 4096-os lépésekben. Az érvényes prioritások tehát 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, és 61440. Más értékek nem használhatók. A 0 érték minden más prioritás előtt elsőbbséget élvez.

**kiterjesztett rendszer azonosító**

Az IEEE 802.1D korai megvalósításai olyan hálózatokhoz készültek, amelyek nem használtak VLAN-okat, minden kapcsoló egy közös feszítőfába tartozott. Emiatt a régebbi Cisco kapcsolók esetén a kiterjesztett rendszer azonosító a BPDU-ból elhagyható. Ahogy a VLAN-ok egyre szélesebb körben elterjedtek, a 802.1D szabványt továbbfejlesztették, hogy a BPDU-keretben a VLAN-azonosító is szerepelhessen. A VLAN sorszáma a BPDU-keretben a kiterjesztett rendszer azonosítóban szerepel. Az újabb kapcsolók már alapértelmezés szerint használják a kiterjesztett rendszer azonosítót.

Az 1. ábrán láthatjuk, hogy a hídprioritás mező 2 byte, azaz 16 bit hosszú. Ebből 4 bit a hídprioritás, 12 bit pedig a kiterjesztett rendszer azonosító, amely az STP-folyamatban részt vevő VLAN azonosítója. Ez a 12 bites kiterjesztett rendszer azonosító csökkenti le a hídprioritást 4 bitesre. Tehát a jobb oldali 12 bit a VLAN azonosító, a bal oldali 4 bit pedig a hídprioritás. Ezért lehet a hídprioritás csak a 4096 (2^12) többszöröse. Ha a bal szélső bitek értéke 0001, a hídprioritás 4096. Ha pedig 1111, akkor a hídprioritás 61440 (15x4096). A Catalyst 2960 és 3560 sorozatú kapcsolók nem engedélyezik a hídprioritás 65536-os (16x4096) értékét, mert ahhoz már ötödik bit is kellene, ami a kiterjesztett rendszer azonosító miatt nem használható.

A kiterjesztett rendszer azonosító a hídprioritás értékéhez adódik hozzá a hídazonosítóban, és kerül be a BPDU-ba meghatározva a prioritást és a VLAN-t.

Amikor két kapcsoló ugyan azt a prioritást kapja és kiterjesztett rendszer azonosítójuk is egyforma, akkor az alacsonyabb hexadecimális értékű MAC-címmel rendelkező kapcsolónak lesz kisebb a hídazonosítója. Kezdetben minden kapcsoló prioritása ugyanaz az alapértelmezett számérték. Tehát a gyökérponti híd választásának döntő tényezője a MAC-cím lesz. Ha a rendszergazda szeretné a gyökérponti híd választását a hálózat igényeihez igazítani, a gyökérponti hídnak szánt kapcsoló prioritását alacsonyabbra kell állítania. Ezzel azt is biztosítja, hogy a hálózathoz csatlakoztatott új kapcsolók nem kezdeményeznek új feszítőfa választást, amely a gyökérponti híd megválasztásáig akadályozná a hálózati kommunikációt.

A 2. ábrán az S1 prioritása alacsonyabb, mint a többi kapcsolóé. Ezért ő az előnyben részesített az adott feszítőfa gyökérponti hídjaként.

Amikor minden kapcsoló prioritása azonos, jelen esetben mindegyiké az alapértelmezett 32768, akkor a MAC-cím fogja eldönteni azt, hogy melyikük lesz a gyökérponti híd (lásd 3. ábra).

**Megjegyzés**: A példában minden kapcsoló prioritása 32769. Ez úgy áll elő, hogy az alapértelmezett 32768-as prioritáshoz hozzáadódik a kapcsolókon hozzárendelt 1-es VLAN (32768+1).

A legalacsonyabb hexadecimális MAC-című lesz a preferált gyökérponti híd. A példában az S2 MAC-címe a legalacsonyabb, tehát ő lesz az adott feszítőfa gyökérponti hídja.

# Laborgyakorlat - Redundáns kapcsolt hálózat építése

**Ezen a laborgyakorlaton az alábbi feladatokat végezzük el:**

* 1. rész: A hálózat felépítése és az eszközök alapvető konfigurálása
* 2. rész: A gyökérponti híd meghatározása
* 3. rész: A port költségen alapuló STP port kiválasztás megfigyelése
* 4. rész: A port prioritáson alapuló STP port kiválasztás megfigyelése.

[Lab - Building a Switched Network with Redundant Links](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.1.2.12%20Lab%20-%20Building%20a%20Switched%20Network%20with%20Redundant%20Links.pdf)

**A feszítőfa protokollok típusai**

Az eredeti IEEE 802.1D óta a feszítőfa protokolloknak számos változata jelent meg.

Ezek közül néhány:

* **STP** - Ez az eredeti IEEE 802.1D változat (802.1D-1998 és korábbi), amely hurokmentes topológiát biztosít redundáns kapcsolatokat tartalmazó hálózatban. A közös feszítőfa (Common Spanning Tree, CST) azt jelenti, hogy az egész kapcsolt hálózat egyetlen feszítőfát használ a VLAN-ok számától függetlenül.
* **PVST+** - Az STP Cisco által továbbfejlesztett változata, a hálózat minden VLAN-jához külön 802.1D feszítőfa példányt épít. A példányok támogatják a PortFast, UplinkFast, BackboneFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat.
* **802.1D-2004** - Ez az STP-szabvány módosítása, amely tartalmazza az IEEE 802.1w-t.
* **Rapid Spanning Tree Protocol (RSTP, gyors feszítőfa protokoll) vagy IEEE 802.1w** - Az STP gyorsabb konvergenciát biztosító fejlesztése.
* **Rapid PVST+** - Az RSTP Cisco általi PVST+-ot használó továbbfejlesztése. A Rapid PVST+ VLAN-onként biztosít 802.1w példányt. A példányok támogatják a PortFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat.
* **MSTP (Multiple Spanning Tree Protocol, több feszítőfa protokoll)** - A korábbi Cisco saját fejlesztésű több példányos feszítőfa (Multiple Instance STP, MISTP) nyomán készített IEEE szabvány. Az MSTP több VLAN-t ugyanabba a feszítőfa példányba képez le. Az MSTP Cisco megvalósítása az MST, amely legfeljebb 16 RSTP példányt használhat, és több, azonos fizikai és logikai topológiájú VLAN-t egyesít egy közös RSTP-példányba. Minden példány támogatja a PortFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat.

A kapcsolók üzemeltetéséért felelős hálózati szakembernek kell döntenie a használni kívánt feszítőfa protokoll változatról.

**A feszítőfa protokollok jellemzői**

Az ábrán a különféle feszítőfa protokollok jellemzői láthatók. A Cisco implementációk és IEEE-szabványok a következők:

* **STP** - A VLAN-ok számától függetlenül egyetlen IEEE 802.1D feszítőfa példány jön létre az egész kapcsolt hálózatban. Mivel csak egy példány van, ennek a változatnak alacsonyabb a processzor és memóriaigénye, mint a többié, viszont csak egy gyökérponti híd és egy fa létezik. Minden VLAN forgalma azonos útvonalakat használ, a hálózat forgalma nem mindig optimális. A 802.1D korlátai miatt ez a változat lassan konvergál.
* **PVST+** - Az STP Cisco általi továbbfejlesztése, amely külön-külön 802.1D példányt biztosít minden konfigurált VLAN-hoz. A konvergencia sebessége az eredeti STP-hez hasonló. A példányok támogatják a PortFast, UplinkFast, BackboneFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat. A port szerepek megegyeznek az RSTP-vel. A VLAN-onkénti külön példány több processzoridőt és memóriát igényel, de lehetővé teszi a VLAN-onkénti gyökérponti hidakat, valamint a hozzájuk tartozó optimalizált feszítőfát. A konvergencia a 802.1D-hez hasonló, de fontos különbség, hogy VLAN-onként külön konvergál.
* **RSTP (vagy IEEE 802.1w)** - A feszítőfa olyan továbbfejlesztése, amely az eredeti 802.1D-nél gyorsabb konvergenciát biztosít. Ez a változat sok konvergenciával kapcsolatos kérdést megold, de mivel egyetlen STP-t használ, a forgalom nem feltétlenül optimális. A gyorsabb konvergencia érdekében a processzor- és memóriaigénye magasabb az STP-nél, de a Rapid PVST+-nál alacsonyabb.
* **Rapid PVST+** - Az RSTP Cisco által továbbfejlesztett változata, PVST+-t használ. VLAN-onként biztosít külön 802.1w példányt, melyek támogatják a PortFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat. Ez a változat a konvergenciával és a nem optimális forgalommal kapcsolatos kérdéseket is megpróbálja megoldani. Azonban ennek a legmagasabb a processzor- és memóriaigénye.
* **MSTP** - Az IEEE 802.1s szabványa, a korábbi Cisco MISTP megvalósítás mintájára készült.. Az STP-példányok számának csökkentése érdekében az azonos forgalmi igényekkel rendelkező VLAN-okat közös feszítőfába építi be.
* **MST** - Az MSTP Cisco megvalósítása, legfeljebb 16 RSTP (802.1w) példányt használ, több, azonos fizikai és logikai topológiájú VLAN-t egyesít közös RSTP-példányba. Minden példány támogatja a PortFast, BPDU-védelem, BPDU-szűrő, gyökér védelem és hurokvédelem funkciókat. Ennek a változatnak a processzor- és memóriaigénye alacsonyabb a Rapid PVST+-nál, de magasabb az RSTP-nél.

A Cisco Catalyst kapcsolók alapértelmezett feszítőfa módja a PVST+, minden porton engedélyezve van. A PVST+ topológiaváltozás esetén lassabban konvergál, mint a Rapid PVST+.

**Megjegyzés**: Az újabb IOS-verziót futtató Cisco kapcsolók, mint a 15.0-s IOS-sal rendelkező Catalyst 2960, alapértelmezés szerint PVST+-t futtatnak. Az újabb kapcsolók az IEEE 802.1D-2004 specifikáció több összetevőjét megvalósítják, ilyen az alternatív port szerep a korábbi nem kijelölt port helyett. Azonban, ha a gyors feszítőfa protokollt szeretnénk használni, még az újabb kapcsolókon is kifejezetten be kell ezt állítanunk.

# A PVST+ áttekintése

Az eredeti IEEE 802.1D szabvány közös feszítőfát definiál, tehát a VLAN-ok számától függetlenül egyetlen feszítőfa példányt használ. A közös feszítőfát használó hálózatok jellemzői:

* Nem lehetséges a terheléselosztás. Az összekötő (uplink) kapcsolatok blokkolása minden VLAN-ra egyszerre érvényes.
* Processzorkímélő. Csak egyetlen feszítőfa példányt kell kiszámítani.

A Cisco kidolgozta a PVST+-t, amelynek segítségével a hálózat az IEEE 802.1D Cisco változatát minden VLAN-ra független példányként futtatja. A PVST+ esetében lehetséges, hogy egy kapcsoló valamely trönk portja az egyik VLAN-t blokkolja, egy másikon pedig továbbít. A PVST+ 2. rétegbeli terheléselosztásra is használható. A PVST+ kapcsolói több processzoridőt és több sávszélességet használnak a BPDU-k továbbításra, mint a hagyományos CST megvalósítások, mert minden VLAN külön STP-példányt futtat.

PVST+ környezetben a feszítőfa paramétereket hangolhatjuk olyan módon, hogy az összekötő (uplink v. trönk) kapcsolatok a VLAN-ok forgalmát elosztva továbbítsák. Az ábrán az S2 F0/3 portja a VLAN 20-at, az S2 F0/2 portja pedig a VLAN 10-et továbbítja. Ez úgy érhető el, hogy a VLAN-ok felének az egyik kapcsoló lesz a gyökérponti hídja, a többi VLAN-nak pedig egy másik kapcsolót választunk gyökérponti hídnak. Az ábrán az S2 a VLAN 20 gyökérponti hídja, az S1 pedig a VLAN 10-é. A VLAN-onkénti STP gyökérponti hidak növelik a hálózat redundanciáját.

A PVST+-t használó hálózatok jellemzői:

* Optimális terheléselosztás érhető el.
* A VLAN-onkénti külön-külön feszítőfa példány karbantartása jelentős mértékű processzoridő pazarlást jelent a hálózat összes kapcsolóján (ehhez adódik még a példányok saját BPDU-cseréjének sávszélesség használata). Azonban ez csak sok VLAN használata esetén okoz problémát.

# Port állapotok és a PVST+ működése

Az STP a szórási tartományban logikai hurokmentes útvonalakat biztosít. A feszítőfa felépítése a csatlakoztatott kapcsolók közötti BPDU-keretek cseréje során tanult információn alapul. A logikai feszítőfa kialakításához a kapcsolóportok öt lehetséges port állapotot és három BPDU-időzítőt használnak.

A feszítőfa a kapcsoló elindulása után azonnal kiépül. Ha egy kapcsoló port lezárt állapotból azonnal továbbító állapotba lépne anélkül, hogy a teljes topológiát megismerné, akkor ez a port hurkot képezhetne a hálózatban. Ezért az STP öt port állapotot használ. A PVST+ ugyanezeket az állapotokat valósítja meg. Az ábra bemutatja a feszítőfa hurokmegelőzést szolgáló állapotait:

* **Lezárt** - Alternatív port, nem vesz részt a keretek továbbításában. A port fogadja a BPDU-kereteket, hogy megtudja a gyökérponti híd helyét és azonosítóját, valamint, hogy melyik porthoz milyen szerepet rendeljen a végleges aktív STP-topológiában.
* **Figyelő** - A gyökér felé vezető utat figyeli. Ez a port részt vehet a keretek továbbításában a fogadott BPDU-keretek STP általi feldolgozása alapján. A port fogadja a BPDU-kat, küldi a sajátjait és tájékoztatja a szomszédait, hogy a port részt fog venni az aktív topológiában.
* **Tanuló** - MAC-címeket tanul. A port felkészül a keretek továbbítására és megkezdi MAC-cím táblázatának felépítését.
* **Továbbító** - A port az aktív topológia része. Továbbítja az adatkereteket, küld és fogad BPDU-kereteket.
* **Letiltott** - A port nem vesz részt a feszítőfában és nem továbbít kereteket. Ez az az állapot, amikor a portot a rendszergazda letiltotta (shut down).

Jegyezzük meg, hogy az egyes állapotokba (lezárt, figyelő, tanuló vagy továbbító) tartozó portok számát a show spanning-tree summary paranccsal jeleníthetjük meg.

A kapcsolt hálózat minden VLAN-jára a PVST+ a következő négy lépést hajtja végre a hurokmentes logikai hálózati topológia elérése érdekében:

* **Választ egy gyökérponti hidat** - Csak egy kapcsoló lehet gyökérponti híd (az adott VLAN-ban). A "root bridge" az a kapcsoló, amelynek a legalacsonyabb a hídazonosítója. A gyökérponti híd minden portja kijelölt port (nincs gyökér portja).
* **Minden nem gyökérponti hídon kiválasztja a gyökér portot** - A PVST+ minden kapcsolón (kivéve a gyökérponti hidat) minden VLAN-hoz meghatároz egy gyökér portot. A gyökér port az, amelynek a gyökérponti hídig a legalacsonyabb a költsége, tehát a gyökérponti híd felé vezető legjobb út felé irányul. A gyökér portok normál esetben továbbító állapotban vannak.
* **Minden szegmensen (tönk, uplink) kiválasztja a kijelölt portot** - A PVST+ minden kapcsolaton minden VLAN-hoz kiválaszt egy kijelölt portot. A kijelölt portot azon a kapcsolón választja ki, amelynek a gyökérponti híd felé a legalacsonyabb költségű útja van. A kijelölt portok normál esetben továbbító állapotban vannak, a forgalom engedélyezett a szegmensen.
* **A kapcsolt hálózat többi portja alternatív port** - Az alternatív portok normál esetben lezárt állapotban maradnak, így szakítják meg logikailag a hurkokat. A lezárt állapotban levő port nem továbbít forgalmat, de a beérkező BPDU-kereteket feldolgozza.

# A kiterjesztett rendszer azonosító és a PVST+

PVST+ környezetben a kiterjesztett rendszer azonosító biztosítja, hogy minden kapcsolónak VLAN-onként egyedi hídazonosítója legyen.

Például a VLAN 2-ben az alapértelmezett hídazonosító 32770 (a 32768-as prioritáshoz adódik hozzá 2, mint kiterjesztett rendszer azonosító). Ha a rendszergazda nem állít be prioritásokat, akkor minden kapcsoló az alapértelmezett értéket használja és a VLAN-ok gyökereinek választása MAC-cím alapján zajlik. Ez a módszer a gyökérponti hidat bizonyos szempontból véletlenszerűen jelöli ki.

Vannak olyan helyzetek, amikor a rendszergazda szeretne egy bizonyos kapcsolót gyökérponti hídnak látni. Ez különböző okok miatt történhet: a kapcsoló a LAN-topológia középpontjában van, nagyobb a feldolgozási sebessége, vagy egyszerűen ezt a legkönnyebb elérni és távolról felügyelni. A gyökérponti híd választásának befolyásolása úgy történik, hogy az adott VLAN-okban gyökérnek szánt kapcsoló prioritását alacsonyabbra állítjuk.

# A Rapid PVST+ áttekintése

Az RSTP (IEEE 802.1w) az eredeti 802.1D továbbfejlesztése, amelyet beépítettek az IEEE 802.1D-2004 szabványba. A 802.1w STP terminológiája megegyezik az eredeti IEEE 802.1D STP-vel. A legtöbb paraméter változatlan maradt, az STP-t ismerő szakemberek könnyen be tudják konfigurálni az új protokollt is. A Rapid PVST+ az RSTP VLAN-onkénti Cisco megvalósítása. Minden VLAN-hoz független RSTP-példány fut.

Az ábra egy RSTP-t futtató hálózatot mutat be. Az S1 a gyökérponti híd, két kijelölt portja továbbító állapotban van. Az RSTP egy új port típust is támogat. Az S2 F0/3-as portja egy eldobó (discarding) állapotban levő alternatív port. Figyeljük meg, hogy lezárt portok viszont nincsenek, mivel az RSTP-ben nincs ilyen port állapot. Az RSTP eldobó, tanuló és továbbító állapotokat ismer.

Az RSTP felgyorsítja a feszítőfa újraszámítását a 2. rétegbeli topológia változásakor. Sokkal gyorsabb konvergenciát lehet vele elérni egy megfelelően konfigurált hálózatban, néha mindössze néhány száz milliszekundumon belül. Az RSTP újradefiniálja a port típusokat és állapotaikat. Egy alternatív vagy tartalék port azonnal továbbító állapotba léphet, nem kell megvárni a hálózat konvergálását. Az RSTP jellemzői a következők:

* Az RSTP a 2. rétegbeli hurkok megelőzésének preferált protokollja. Az eredeti 802.1D-hez viszonyított továbbfejlesztés számos eleme Cisco általi módosításként született. Ilyen fejlesztések például: a BPDU-k a port szerepekről csak a szomszédos kapcsolókhoz szállítanak információt, a kiegészítő konfigurációs igények megszüntetése, valamint általános teljesítmény növelés. Mindezek beépültek a protokoll működésébe.
* Az eredeti 802.1D-hez készült Cisco saját fejlesztések nem kompatibilisek az RSTP-vel, ilyenek az UplinkFast és a BackboneFast funkciók.
* Az RSTP (802.1w) felváltja az eredeti 802.1D-t, de visszafelé kompatibilis vele, így legtöbb terminológia és paraméter is változatlan. Emellett a 802.1w a régebbi kapcsolókkal való együttműködés érdekében portonként képes visszaváltani az eredeti 802.1D módba. Például az RSTP feszítőfa-algoritmus pontosan olyan módon választ gyökérponti hidat, mint az eredeti 802.1D.
* Az RSTP megtartja az eredeti IEEE 802.1D BPDU-formátumát, kivéve, hogy a verzió mezőt 2-re állítja az RSTP jelzéseként és a flag mező mind a 8 bitjét használja.
* Az RSTP aktívan képes megerősíteni, hogy egy port biztonságosan továbbító állapotba kerülhet, nem hagyatkozik időzítőkre.

# RSTP BPDU-k

Az RSPT 2-es típusú, 2-es verziójú, míg az eredeti 802.1D STP 0-s típusú, 0-s verziójú BPDU-kat használ. Azonban egy RSTP-t alkalmazó kapcsoló közvetlenül képes kommunikálni egy eredeti 802.1D STP-t futtató kapcsolóval. Az RSTP az eredeti 802.1D-től kissé eltérő módon küldi a BPDU-kat és használja a flag bájtot:

* A protokoll információ azonnal elévül, ha a porton nem érkezik "Hello" üzenet három egymás utáni "Hello" idő lejárta alatt (alapértelmezés szerint 3x2= 6 másodperc), vagy amikor az elévülési időzítő lejár.
* A BPDU-kat életben tartó (keep-alive) mechanizmusként használják. Ezért három egymás utáni BPDU kimaradása a szomszéddal való kapcsolat megszakadását jelenti. Az információ viszonylag gyors elévülése miatt a hibák nagyon hamar észlelhetők.

**Megjegyzés**: Ahogy az STP, úgy az RSTP is küld BPDU-t aktuális információkkal "Hello" időközönként (alapértelmezés szerint 2 másodperc), még akkor is, ha az RSTP-kapcsoló a gyökérponti hídtól nem kap BPDU-kat.

Az RSTP a 2-es verziójú BPDU flag-formátumát használja (lásd az ábrán is):

* A 0. és 7. bit a topológiaváltozás és a nyugtázás. Ezek az eredeti 802.1D részei.
* Az 1. és 6. bitek a gyors konvergenciát segítő (Proposal Agreement) folyamathoz használatosak.
* A 2-5. bitek a port szerep és állapot jelzői.
* A 4-es és 5-ös bit két bites kóddal jelöli a port szerepét.

# Szélső portok (edge port)

Az RSTP szélső port egy kapcsoló olyan portja, amelyet soha nem szándékozunk másik kapcsolóhoz csatlakoztatni. Aktiválása után azonnal továbbító állapotba vált.

Az RSTP edge port fogalma megegyezik a PVST+ PortFast funkciójával. A szélső port végberendezéshez csatlakozik, feltételezhetjük, hogy kapcsoló nem fog csatlakozni hozzá. Az RSTP edge portok azonnal továbbító állapotba váltanak, kihagyva az eredeti 802.1D időigényes figyelő és tanuló állapotait.

A Cisco RSTP-megvalósítása (Rapid PVST+) megtartotta a PortFast kulcsszót, a szélső portokat a spanning-tree portfast paranccsal állíthatjuk be. Ez zökkenőmentessé teszi az STP-ről az RSTP-re váltást.

Az 1. ábrán edge portként konfigurálható portokat láthatunk. A 2. ábra olyan portokat mutat, amelyek nem szélső portok.

**Megjegyzés**: Edge portként konfigurált portot másik kapcsolóhoz csatlakoztatni nem ajánlott. Negatív hatással lehet az RSTP-re, mert átmenetileg hurok jöhet létre, ami lelassítja az RSTP konvergálását.

**Kapcsolat típusok**

A kapcsolat típus az RSTP-ben részt vevő portok osztályozása a port duplexitása alapján. Attól függően, hogy mi csatlakozik a portokhoz, két különböző kapcsolat típus lehet (link type):

* **Pont-pont (point-to-point)** - Egy teljes duplex módban üzemelő port tipikusan kapcsolót kapcsolóval köt össze és jó eséllyel gyorsan továbbító módba váltható.
* **Megosztott (shared)** - Egy félduplex módban üzemelő port kapcsolót hubhoz csatlakoztat, amelyre több eszköz kapcsolódik.

Kattintsunk az ábrán a kapcsolatokra típusuk megjelenítéséhez!

A kapcsolat típus azt határozza meg, hogy a port azonnal továbbító állapotba léphet-e, amennyiben annak feltételei teljesülnek. A feltételek szélső és nem szélső portok esetén különbözőek. A nem szélső portok két kapcsolat típusba sorolhatóak: pont-pont és megosztott. A kapcsolat típus meghatározása automatikus, de a "spanning-tree link-type " port konfigurációs paranccsal közvetlenül is beállítható. A port szerepek jellemzői a kapcsolat típusok tekintetében a következők:

* Az edge portok és a pont-pont kapcsolatra konfigurált portok alkalmasak a továbbító állapotba való gyors átváltásra. Azonban a kapcsolat típus paraméter figyelembe vétele előtt az RSTP-nek meg kell határoznia a port szerepét.
* A gyökér portok nem használják a kapcsolat típus paramétert. A gyökér portok gyorsan továbbító állapotba válthatók, amint a port szinkronizál.
* Az alternatív és a tartalék portok a legtöbb esetben nem használják a kapcsolat típus paramétert.
* Kijelölt portok esetében a leghasznosabb a kapcsolat típus, mivel ezek gyorsan továbbító állapotba válthatók, ha a paraméter pont-pont.

# A Catalyst 2960 alapbeállításai

A táblázat egy Cisco Catalyst 2960 sorozatú kapcsoló alapértelmezett feszítőfa beállításait mutatja be. Figyeljük meg, hogy az alapértelmezett STP-mód a PVST+.

# A hídazonosító (Bridge ID) beállítása és ellenőrzése

Amikor a rendszergazda egy bizonyos kapcsolót szeretne gyökérponti híddá tenni, a hídprioritását úgy kell beállítania, hogy a hálózat összes többi kapcsolójáénál alacsonyabb legyen. Cisco Catalyst kapcsolón két módszert használhatunk a hídprioritás beállítására.

**1. módszer**

Állítsuk a kapcsoló prioritását a legalacsonyabb értékre a **spanning-tree vlan** *vlan-azonosító* **root primary** globális konfigurációs paranccsal. A kapcsoló prioritása az előre meghatározott 24576 érték lesz, vagy a hálózatban érzékelt legalacsonyabb hídprioritásnál kisebb olyan szám, amely a legnagyobb 4096 többszörös.

Ha másodlagos gyökérponti hidat is szeretnénk beállítani, használhatjuk a **spanning-tree vlan** *vlan-azonosító* **root secondary** globális konfigurációs parancsot. Ez a parancs a kapcsoló prioritását az előre meghatározott 28672-re állítja. Így az elsődleges gyökérponti híd meghibásodása esetén ez lesz a gyökérponti híd. Feltételezzük, hogy a hálózat többi kapcsolójának a prioritása az alapértelmezett 32768.

Az 1. ábrán az S1-et elsődleges gyökérponti híddá tesszük a **spanning-tree vlan 1 root primary** paranccsal, az S2 pedig a másodlagos gyökérponti híd lesz a **spanning-tree vlan 1 root secondary** parancs segítségével.

**2. módszer**

A hídprioritás konfigurálásának egy másik módszere, ha a **spanning-tree vlan** *vlan-azonosító* **priority** *érték* globális konfigurációs parancsot használjuk. Ez a hídprioritás finomabb szabályozását teszi lehetővé. A prioritás értéke 0 és 61440 közé eshet 4096-os lépésekben.

A példában az S3 kapcsolóhoz a 24576 hídprioritást rendeltük a **spanning-tree vlan 1 priority 24576** parancs segítségével.

Egy kapcsoló hídprioritását a **show spanning-tree** paranccsal ellenőrizhetjük. A 2. ábrán a kapcsoló prioritása 24576. Figyeljük meg azt is, hogy a kapcsoló az adott feszítőfa példány gyökérponti hídja.

Használjuk a 3. ábrán lévő parancsszimulátort az S1, S2 és S3 kapcsolók beállítására! Alkalmazzuk a fent leírt 2. módszert, az S3-nak manuálisan adjuk meg a 24576-os hídprioritást a VLAN 1-re. Majd az 1. módszert használva állítsuk be, hogy az S2 a VLAN 1 másodlagos gyökere, az S1 pedig VLAN 1 elsődleges gyökere legyen. Ellenőrizzük a beállításokat az S1-en a **show spanning-tree** parancs kiadásával.

# PortFast és BPDU Guard

A PortFast a Cisco PVST+ környezetben használt funkciója. A PortFast beállítás a kapcsolóportot lezárt állapotból azonnal továbbító állapotba váltja, amellyel megkerüli a szokásos 802.1D STP állapotátmeneteket (a figyelő és a tanuló állapotokat). A PortFast arra szolgál, hogy a hozzáférési portok eszközei azonnal elérjék a hálózatot, ne kelljen megvárniuk az IEEE 802.1D STP konvergálását minden egyes VLAN-on. Hozzáférési porton az egyetlen munkaállomást vagy szervert csatlakoztató portot értjük.

Szabályos PortFast beállítások esetén sosem érkezhetnek BPDU-k, mert ez azt jelentené, hogy a portra másik híd vagy kapcsoló csatlakozik, ami feszítőfa hurokhoz vezethetne. A Cisco kapcsolók egy BPDU-védelemnek (BPDU guard) nevezett funkciót is támogatnak. Ha engedélyezzük, a BPDU-védelem a portot *error-disabled* állapotba helyezi, ha azon BPDU érkezik. Ez gyakorlatilag leállítja (shutdown) a portot. A BPDU-védelem biztonságos megoldás a hibás konfigurációk ellen, mert az interfészt csak manuálisan lehet újból üzembe helyezni.

A Cisco PortFast technológia DHCP használata esetén is hasznos. PortFast nélkül egy PC még azelőtt küldhetne DHCP-kérést, hogy a port továbbító állapotba kerülne, így nem kapna használható IP-címet és konfigurációt. A PortFast azonnal továbbító módba állítja a portot, így a PC mindig kap IP-címet.

**Megjegyzés**: Mivel a PortFast célja, hogy a hozzáférési portoknak a lehető legkevesebbet kelljen a feszítőfa konvergálására várakozniuk, a beállítást csak azokon szabad használni. Másik kapcsolóhoz csatlakozó porton használva feszítőfa hurok létrejöttét kockáztatjuk.

A PortFast beállításához használjuk a **spanning-tree portfast** interfész konfigurációs parancsot. Ezt minden interfészen ki kell adnunk, amelyen szeretnénk PortFast-ot használni (2. ábra). A **spanning-tree portfast default** globális konfigurációs parancs minden nem trönk interfészen engedélyezi a PortFast-ot.

Egy 2. rétegbeli porton a BPDU-védelmet a **spanning-tree bpduguard enable** interfész konfigurációs paranccsal kapcsolhatjuk be. A **spanning-tree portfast bpduguard default** globális konfigurációs parancs a BPDU-védelmet az összes PortFast-tal konfigurált porton bekapcsolja.

A PortFast és a BPDU-védelem állapotát megtudhatjuk a **show running-config** parancs kimenetéből (lásd 3. ábra). A PortFast és a BPDU-védelem alapértelmezés szerint minden interfészen ki van kapcsolva.

Használjuk a 4. ábrán lévő parancsszimulátort az S1 és az S2 kapcsolók PortFast és BPDU-védelem beállításához és ellenőrzéséhez!

# PVST+ terhelésmegosztás

Az 1. ábra topológiáján három kapcsoló van egymáshoz 802.1Q trönkön csatlakoztatva, amelyeken a VLAN 10 és VLAN 20 forgalmat továbbítják. Az a cél, hogy az S3 legyen VLAN 20 gyökérponti hídja, az S1 pedig VLAN 10-é. Ebben az esetben az S2 F0/3-as portja a VLAN 10-et blokkolja, a VLAN 20-at pedig továbbítja. Szimmetrikusan az S2 F0/2-es portja a VLAN 10-et továbbítja, a VLAN 20-at pedig nem.

A gyökérponti híd meghatározásán túl beállíthatunk másodlagos gyökérponti hidat is. Másodlagos gyökérponti híd az a kapcsoló, amely a VLAN elsődleges gyökerének meghibásodásakor az új gyökérponti híd lesz, ha a VLAN többi kapcsolója az alapértelmezett STP-prioritást használja.

A példa topológián levő PVST+ beállításának lépései:

**1.** Válasszuk ki az elsődleges és másodlagos gyökérponti hidakat minden VLAN-hoz. Például az 1. ábrán az S3 a VLAN 20 elsődleges hídja, az S1 pedig a másodlagos hídja.

**2.** Állítsuk be a VLAN elsődleges hídjának szánt kapcsolót a **spanning-tree vlan** *szám* **root primary** paranccsal (2. ábra).

**3.** Állítsuk be a VLAN másodlagos hídját a **spanning-tree vlan** *szám* **root secondary** paranccsal.

A gyökérponti híd meghatározásának másik módja az, hogy az általunk elsődlegesnek kiválasztott kapcsoló feszítőfa prioritását az összes többi kapcsolóénál alacsonyabbra állítjuk az adott VLAN-ra nézve.

Figyeljük meg, hogy a 2. ábrán az S3 a VLAN 20 elsődleges gyökérponti hídja, az S1 pedig a VLAN 10 elsődleges gyökérponti hídja. Az S2 STP-prioritása az alapértelmezett érték maradt.

Az ábrán azt is látható, hogy az S3 a VLAN 10 másodlagos gyökérponti hídja, az S1 pedig a VLAN 20 másodlagos gyökérponti hídja. Ez a konfiguráció terhelésmegosztást tesz lehetővé a feszítőfában, VLAN 10 forgalma az S1-en, VLAN 20 forgalma pedig az S3 kapcsolón halad keresztül.

A gyökérponti híd meghatározásának további módja, hogy az általunk elsődlegesnek kiválasztott kapcsoló feszítőfa prioritását a lehető legalacsonyabbra állítjuk a saját VLAN-jában (3. ábra). A kapcsoló prioritás minden feszítőfa példányhoz beállítható. Ez a beállítás befolyásolja azt, hogy egy kapcsoló gyökérponti híddá válik-e. Az alacsonyabb értékkel rendelkező kapcsoló nagyobb valószínűséggel lesz kiválasztott. Az érték 0 és 61440 közé eshet 4096-os lépésekben, egyéb számokat nem fogad el a kapcsoló. Egy érvényes prioritás érték lehet például a 4096\*2=8192.

Amint a 4. ábrán látható, a **show spanning-tree active** parancs megmutatja az aktív interfészek feszítőfa konfigurációjának részleteit. A bemutatott kimenet a PVST+-t használó S1 kapcsolóé. A Cisco IOS-ben a **show spanning-tree** parancsnak még számos paramétere van.

Az 5. ábrán látható parancskimenet szerint a VLAN 10 prioritása 4096, a három érintett VLAN közül a legalacsonyabb.

A 6. ábrán található parancsszimulátor segítségével konfiguráljuk és ellenőrizzük az S1 és az S3 feszítőfájának beállításait.

# Packet Tracer - A PVST+ konfigurálása

**Esetleírás**

Ebben a feladatban VLAN-okat és trönköket fogunk konfigurálni, valamint megvizsgáljuk és beállítjuk a feszítőfa protokoll elsődleges és másodlagos gyökérponti hídjait. Továbbá optimalizálni fogjuk a kapcsolt topológiát PVST+, PortFast és BPDU-védelem használatával.

[Packet Tracer - Configuring PVST+ Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.3.1.5%20Packet%20Tracer%20-%20Configuring%20PVST%20Instructions.pdf)

[Packet Tracer - Configuring PVST+ - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.3.1.5%20Packet%20Tracer%20-%20Configuring%20PVST.pka)

# Feszítőfa mód

A Rapid PVST+ az RSTP Cisco általi megvalósítása VLAN-onkénti támogatással. Az 1. ábra topológiáján két VLAN van: 10 és 20.

**Megjegyzés**: A Catalyst 2960 sorozatú kapcsolók alapértelmezett feszítőfa konfigurációja a PVST+, ezenkívül támogatják a PVST+, a Rapid PVST+ és az MST módokat, de egyszerre csak egy lehet aktív az összes VLAN számára.

A Rapid PVST+ parancsok az adott VLAN-hoz tartozó feszítőfa példányok konfigurációját vezérlik. Feszítőfa példány akkor jön létre, amikor egy interfészt VLAN-hoz rendelünk és akkor szűnik meg, amikor az utolsó interfészt is másik VLAN-hoz soroljuk át. A feszítőfa példány létrejötte előtt is beállíthatjuk az STP-re vonatkozó kapcsoló és port paramétereket, amelyek az STP-példány létrejöttekor válnak aktívvá.

A 2. ábra a Rapid PVST+ konfingurációjának Cisco IOS-szintaxisát mutatja be egy kapcsolón. A **spanning-tree mode rapid-pvst** globális konfigurációs parancs az egyetlen, amire szükségünk van a Rapid PVST+ konfigurálásához. Interfész megadásakor használhatunk fizikai portot, VLAN-t vagy port csatornákat is. A VLAN-azonosító 1 és 4094 közé eshet továbbfejlesztett szoftvert (enhanced software image, EI) esetén, és 1 és 1005 közé standard szoftvert (standard software image, SI) használatakor. A port csatorna száma 1-től 6-ig terjedhet.

A 3. ábrán az S1 kapcsoló Rapid PVST+ konfigurálásának parancsai láthatók.

A 4. ábrán a **show spanning-tree vlan 10** parancs megmutatja az S1 kapcsoló VLAN 10 feszítőfa konfigurációját. Figyeljük meg, hogy a hídprioritás 4096. A kimenetben a “Spanning tree enabled protocol rstp” azt jelenti, hogy az S1 Rapid PVST+-t futtat. Mivel az S1 a VLAN 10 gyökérponti hídja, minden interfésze kijelölt port.

Az 5. ábrán a **show running-config** paranccsal ellenőrizzük az S1 Rapid PVST+ beállításait.

**Megjegyzés**: Általában nem szükséges a *link-type* parancs paraméterének megadása Rapid PVST+ esetén, mert a megosztott kapcsolat típus nagyon ritka *.*. A legtöbb esetben a PVST+ és a Rapid PVST+ konfigurálása között az egyetlen különbség a **spanning-tree mode rapid-pvst** parancs.

**Laborgyakorlat - Rapid PVST+, PortFast és BPDU-védelem konfigurálása**

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

* 1. rész: A hálózat felépítése és az eszközök alapvető konfigurálása.
* 2. rész: VLAN-ok, natív VLAN-ok és trönkök konfigurálása.
* 3. rész: A gyökérponti híd konfigurálása, a PVST+ konvergenciájának megfigyelése.
* 4. rész: Rapid PVST+, PortFast és BPDU-védelem konfigurálása, majd a konvergencia megfigyelése.

[Lab - Configuring Rapid PVST+, PortFast, and BPDU Guard](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.3.2.3%20Lab%20-%20Configuring%20Rapid%20PVST,%20PortFast,%20and%20BPDU%20Guard.pdf)

# Az STP-topológia elemzése

Az STP-topológiát a következő lépéseken keresztül elemezhetjük:

**1.** Térképezzük fel a 2. rétegbeli topológiát. Nézzük meg a hálózat dokumentációját, ha létezik, vagy használjuk a **show cdp neighbors** parancsot a topológia felderítéséhez.

**2.** A 2. rétegbeli topológia felderítése után, az STP ismeretében határozzuk meg az elvárt útvonalat. Tudjuk meg, hogy melyik kapcsoló a gyökérponti híd.

**3.** A **show spanning-tree vlan** parancsot használva keressük meg a gyökérponti hidat.

**4.** Használjuk a **show spanning-tree vlan** parancsot minden kapcsolón, így megtudjuk, mely portok vannak lezárt vagy továbbító állapotban, és ezt összehasonlíthatjuk az elvárásainkkal.

# Elvárt kontra tényleges topológia

Sok hálózatban az optimális STP-topológiát a már a hálózat tervezésekor meghatározták, majd az STP prioritás és költség értékeinek változtatásával valósították meg. Vannak olyan esetek, amikor a hálózat tervezésekor nem vették figyelembe az STP-t, vagy figyelembe vették, meg is valósították, de a hálózat azóta jelentős növekedésen és változáson ment keresztül. Ilyen esetekben fontos tudnunk, hogyan elemezzük a működő hálózat aktuális STP-topológiáját.

A hibaelhárítás legnagyobb része abból áll, hogy a hálózat jelenlegi állapotát összehasonlítjuk az általunk elvárt állapottal és megkeressük a különbségeket és a problémára utaló jeleket. Hálózati szakemberként meg kell vizsgálnunk a kapcsolókat és fel kell derítenünk a jelenlegi topológiát, valamint elképzelésünk kell legyen arról, hogy milyen lenne a jó feszítőfa topológia.

# A feszítőfa állapotának áttekintése

A **show spanning-tree** parancs további opciók nélkül gyors áttekintést ad a kapcsoló összes VLAN-ján futó STP állapotáról. Ha csak egy bizonyos VLAN érdekel, a parancs kimenetét annak megadásával leszűkíthetjük.

A **show spanning-tree vlan** *vlan-azonosító* parancs csak egy VLAN-ról ad vissza STP-információkat. Ezzel a paranccsal a kapcsoló egyes portjainak szerepét és állapotát kérdezhetjük le. Az ábrán az S1 parancskimenetében látható, hogy mindhárom portja továbbító (FWD) állapotban van és a portok vagy kijelölt, vagy gyökér portok. A lezárt portok "BLK" (blocked) jelölést kapnak.

A kimenetből megtudhatjuk még saját kapcsolónk hídazonosítóját és a gyökér azonosítót is, amely nem más, mint a gyökérponti híd hídazonosítója.

# Feszítőfa hibák következményei

Egy protokoll hibás működése azt eredményezi, hogy elveszítjük az adott protokoll által biztosított funkciókat. Például, ha az OSPF rosszul működik egy forgalomirányítón, akkor a rajta keresztül elérhető hálózatokkal elveszítjük a kapcsolatot. Ez általában az OSPF-hálózat többi részét nem befolyásolja. Ha a forgalomirányítót még mindig elérjük, megkereshetjük a hiba okát és kijavíthatjuk azt.

STP-nél kétféle típusú hiba adódhat. Az első az OSPF-hibához hasonló; az STP hibásan lezár olyan portokat, amelyeknek továbbítaniuk kellene. A forgalom, amelynek ezen a kapcsolón keresztül kellene haladnia elvész, de a hiba a hálózat többi részét nem érinti. A másik típusú hiba sokkal rosszabb, lásd 1.ábra. Ez akkor történik, amikor az STP hibásan helyez egy vagy több portot továbbító állapotba.

Emlékezzünk rá, hogy az Ethernet keret fejlécében nincs TTL-mező, ami azt jelenti, hogy a hurokba bekerült keretet a kapcsolók végtelenségig továbbítják. Az kivételt csak az a keret képez, amelynek célcíme a kapcsolók MAC-cím táblájában már szerepel. Ezeket a kereteket a kapcsolók a MAC-címhez tartozó portra továbbítják, ezért nem lépnek be a hurokba. Azonban a hurokba minden elárasztott keret belekerül (2. ábra). Ilyenek a szórás és csoportos címzésű keretek, valamint az ismeretlen célcímmel rendelkező egyedi keretek.

Melyek az STP-hiba következményei és kapcsolódó tünetei (3. ábra)?

A kapcsolt LAN minden összeköttetésének terhelése egyre nő, ahogy egyre több keret lép be a hurokba. A probléma nem csak a hurkot alkotó kapcsolatokra korlátozódik, hanem a hálózat többi összeköttetésére is, mert az elárasztott keretek ezeket is érintik. Ha a feszítőfa hiba csak egy VLAN-ra korlátozódik, akkor csak a VLAN-t továbbító kapcsolatok érintettek. Azok a kapcsolók és trönkök, amelyek a hibás VLAN-t nem továbbítják, normálisan működnek tovább.

Ha a feszítőfa hiba továbbítási hurkot eredményezett, a forgalom exponenciálisan fog nőni. A kapcsolók a szórásokkal minden portjukat elárasztják. Ez minden egyes továbbításkor újabb másolatokat eredményez ugyanarról a keretről.

Amikor vezérlési forgalom is kerül a hurokba (például OSPF vagy EIGRP hello üzenetek), akkor az ezeket a protokollokat futtató eszközök is gyorsan elkezdenek túlterhelődni. Processzoruk kihasználtsága eléri a 100 százalékot, miközben az egyre növekvő vezérlési forgalmat próbálják feldolgozni. Sok esetben a szórási vihar legelső jele az, hogy forgalomirányítók vagy 3. rétegbeli kapcsolók vezérlési hibákat jeleznek és magas processzorterheléssel üzemelnek.

A kapcsolók gyakori MAC-cím tábla változásokat regisztrálnak. Amikor hurok van a hálózatban, a kapcsoló egy keretet érzékel egy bizonyos MAC-címmel egyik portján, majd egy másik keretet ugyanezzel a forrás MAC-címmel másik portján, mindezt a másodperc töredékén belül. Ennek határása a kapcsoló a MAC-cím tábláját egyazon MAC-cím miatt kétszer is frissíti.

A kapcsolatok leterheltsége és a magas processzorhasználat együttes hatása miatt az eszközök elérhetetlenné válnak. Ez rendkívül módon megnehezíti a probléma menet közbeni diagnosztizálását.

# A feszítőfa probléma javítása

A hibás feszítőfa egyik megoldása az, ha manuálisan megszüntetjük a kapcsolt hálózat redundáns összeköttetéseit, fizikailag vagy konfiguráció útján egészen addig, amíg a topológiából minden hurok eltűnik. Ahogy a hurkokat szétbontjuk, a forgalom és a processzor terhelés gyorsan visszatér a normális szintre és az eszközök újra elérik a hálózatot.

Habár a művelet helyreállítja a hálózat működőképességét, a hibaelhárítási folyamatnak ez még csak a kezdete. Mivel a kapcsolt hálózat redundanciáját megszüntettük, ezeket helyre kell majd állítanunk.

Ha a feszítőfa hiba oka még mindig fennáll, a redundáns kapcsolatok visszacsatlakoztatása ismét szórási viharhoz fog vezetni. A redundáns kapcsolatok helyreállítása előtt keressük meg és javítsuk ki a feszítőfa hiba okát! Figyeljük gondosan a hálózat forgalmát, hogy lássuk, a problémát tényleg megoldottuk.

# Az alapértelmezett átjáró korlátai

A feszítőfa protokollok fizikai redundanciát tesznek lehetővé a kapcsolt hálózatokban. Ugyanakkor a hierarchikus hálózat hozzáférési rétegében levő állomás számára hasznosak lehetnek az alternatív alapértelmezett átjárók is. Ha egy forgalomirányító vagy egyik interfésze (amelyik az alapértelmezett átjáró szerepét játssza) meghibásodik, az átjárót használó állomások nem érik el a távoli hálózatokat. Egy olyan mechanizmusra lenne szükség, amely alternatív alapértelmezett átjárót biztosít olyan kapcsolt hálózatokban, ahol kettő vagy több forgalomirányító is tagja ugyanannak a VLAN-nak.

**Megjegyzés**: A forgalomirányítók redundanciájának itt tárgyalt esetében nincs jelentős különbség aközött, hogy forgalomirányító vagy többrétegű kapcsoló van az elosztási rétegben. A gyakorlatban legtöbbször többrétegű kapcsoló adja az alapértelmezett átjárót a kapcsolt hálózat minden VLAN-jának. Ennek a fejezetnek a témája a *forgalomirányítás*, a konkrét fizikai eszköz típusától függetlenül.

Egy kapcsolt hálózatban minden kliens egyetlen alapértelmezett átjáróval rendelkezik. Nincs másodlagos átjáróra lehetőség, még akkor sem, ha a helyi hálózatról van második útvonal, amelyen a csomagok távozhatnak.

Az ábrán az R1 felel a PC1-től kapott csomagok irányításáért. Ha az R1 elérhetetlenné válik, a forgalomirányító protokollok dinamikusan konvergálnak. Az R2 fogja az eddig az R1-en keresztül haladó csomagokat a külső hálózatok felé irányítani. Azonban az a forgalom, amely a belső hálózatról az R1-hez irányult (munkaállomások, szerverek és nyomtatók, amelyeknek R1 volt az alapértelmezett átjárója) még most is R1-nek lesz címezve és emiatt eldobásra kerül.

A végberendezések alapértelmezett átjárója tipikusan egyetlen IP-cím, amely nem változik a topológia változásával. Ha az alapértelmezett átjáró IP-címe nem érhető el, a helyi eszköz nem tud a helyi hálózatról kifelé adatot küldeni, tulajdonképpen a hálózat többi részétől leválasztódik. Nincs dinamikus módszer arra, hogy az eszközök megtalálják az új alapértelmezett átjáró címét, még akkor sem, ha létezik redundáns forgalomirányító, amely a szegmens alapértelmezett átjárója lehetne.

# Forgalomirányító redundancia

Az egyik módszer arra, hogy megszüntessük a forgalomirányító kritikus meghibásodási pont szerepét az, hogy virtuális forgalomirányítót valósítunk meg. Ekkor több forgalomirányítót olyan módon konfigurálunk, hogy együttesen egyetlen forgalomirányító látszatát keltsék a LAN állomásainak számára. Egy IP-cím és egy MAC-cím közös használatával kettő vagy több forgalomirányító egyetlen virtuális forgalomirányítóként működhet.

Az IP-alhálózat munkaállomásainak alapértelmezett átjárója a virtuális forgalomirányító IP-címe lesz. Amikor egy állomás az alapértelmezett átjárónak küld kereteket, ARP-vel keresi meg az átjáró IP-címéhez tartozó MAC-címet. Az ARP-címfeloldás a virtuális forgalomirányító MAC-címét fogja visszaadni. A virtuális forgalomirányító MAC-címére küldött kereteket a virtuális forgalomirányító csoport éppen aktív forgalomirányítója fogja fizikailag feldolgozni. A csoport tagjainak azonosítását és szinkronizálását külön protokoll végzi. Az állomások a forgalmat a virtuális forgalomirányító IP-címére küldik. A valódi forgalomirányító, amely a forgalmat ténylegesen továbbítja, az állomások számára láthatatlan.

Redundancia protokoll biztosít mechanizmust annak a meghatározására, hogy a forgalom továbbítását melyik valódi forgalomirányító végezze. Szintén ez határozza meg, hogy a továbbító szerepet mikor vegye át egy készenléti forgalomirányító. A végberendezések számára a továbbító szerep átadása nem érzékelhető.

A hálózat azon adottságát, hogy képes legyen dinamikusan helyrehozni az alapértelmezett átjáró eszköz meghibásodását, első ugrás redundanciának hívjuk (first-hop redundancy). A protokollok összefoglaló neve FHRP (First Hop Redundancy Protocol, első ugrás redundancia protokoll).

# A hibatűrő forgalomirányító működése

Az aktív forgalomirányító meghibásodásakor a redundancia protokoll a készenléti forgalomirányítót aktívvá teszi, melynek lépései a következők:

1. A készenléti (standby) forgalomirányító nem kap az aktív továbbító forgalomirányítótól Hello üzeneteket.

2. A tartalék forgalomirányító átveszi a továbbító forgalomirányító szerepét.

3. Mivel az új továbbító forgalomirányító a virtuális forgalomirányító IP- és MAC-címét is átveszi, az állomások kiszolgáltatása nem szakad meg.

# First Hop Redundancy Protocols

Az FHRP (First Hop Redundancy Protocol, első ugrás redundancia protokoll) összefoglaló névbe tartozó protokollok és tulajdonságaik a következők (lásd ábra is):

* **HSRP (Hot Standby Router Protocol)** - A Cisco saját feljesztésű FHRP-je, az alapátjáró IPv4-eszköz hibatűrő működtetésére. A HSRP magas szintű hálózati elérhetőséget biztosít, az IPv4 alapértelmezett átjárót használó állomások számára ad első ugrás forgalomirányító redundanciát. A HSRP a forgalomirányítók egy csoportjából választ ki aktív és készenléti (standby, tartalék) eszközt. Az aktív eszköz végzi a csomagok továbbítását, a készenléti vagy tartalék eszköz pedig, megfelelő feltételek teljesülése esetén, átveszi a kiesett aktív eszköz szerepét. A HSRP tartalék forgalomirányítójának feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibájakor.
* **HSRP IPv6-verzió** - A Cisco saját fejlesztésű FHRP-je, ugyanaz a feladata, mint a HSRP-nek, csak IPv6 környezetben. Egy HSRP IPv6 csoport virtuális MAC-címe a HSRP-csoport számából, virtuális IPv6 link-local címe pedig a HSRP virtuális MAC-címből képződik. Amíg aktív a HSRP-csoport, tagjai rendszeresen küldenek forgalomirányító hirdetés (RA) üzeneteket a HSRP virtuális IPv6 link-local címére. Amikor a csoport inaktívvá válik, nem érkezik több ilyen hirdetés.
* **VRRPv2 (Virtual Router Redundancy Protocol version 2, )** - Nyílt fejlesztésű protokoll, egy vagy több virtuális forgalomirányító szerepét osztja ki dinamikusan a VRRP-ben részt vevő IPv4 forgalomirányítóknak. Lehetővé teszi, hogy egy többes hozzáférésű hálózaton több forgalomirányító használhassa ugyanazt a virtuális IPv4-címet. Egy VRRP-forgalomirányító konfigurálásakor a LAN-hoz kapcsolódó egy vagy több további forgalomirányítóval közös VRRP-konfigurációt hoznak létre. VRRP-nél egy forgalomirányító lesz mester szerepben (virtual router master), a többiek tartalék eszközök a mester hibája esetére.
* **VRRPv3** - IPv4 és IPv6 címeket is támogató protokoll. A VRRPv3 különböző gyártók eszközeit tartalmazó környezetben is használható és jobban skálázható, mint a VRRPv2.
* **GLBP (Gateway Load Balancing Protocol)** - A Cisco saját fejlesztésű FHRP-je, a HSRP-hez és a VRRP-hez hasonlóan védelmet biztosít meghibásodott átjáró vagy interfész esetére, de emellett terhelésmegosztásra is képes a redundáns forgalomirányítók csoportján belül.
* **GLBP IPv6** - A Cisco saját FHRP-protokollja, a GLBP-vel egyenértékű, csak IPv6 környezetben. A GLBP IPv6-os változata automatikus tartalék forgalomirányítót biztosít az egyetlen alapértelmezett átjáróval konfigurált IPv6-állomások számára. Több forgalomirányítót von össze egyetlen virtuális IPv6-forgalomirányítóvá, emellett a csoport tagjai a csomagtovábbítás terheléselosztását is elvégezik egymás között.
* **IRDP (ICMP Router Discovery Protocol, ICMP forgalomirányító felderítő protokoll)** - Az RFC 1256-ban definiált FHRP-megoldás. Az IRDP segítségével az állomások meg tudják keresni a távoli hálózatok felé továbbítást biztosító forgalomirányítókat.

# A HSRP ellenőrzése

Egy HSRP aktív forgalomirányító jellemzői a következők:

* Az alapértelmezett átjáróra vonatkozó ARP-kérésekre a virtuális forgalomirányító MAC-címével válaszol.
* Elvégzi a virtuális forgalomirányítónak címzett csomagok továbbítását.
* Hello üzeneteket küld.
* Ismeri a virtuális forgalomirányító IP-címét.

Egy HSRP készenléti forgalomirányító jellemzői:

* Figyeli a Hello üzeneteket.
* Átveszi a csomagok továbbítását, ha nem hall az aktív forgalomirányítótól semmit.

A **show standby** paranccsal kérdezhetjük le a HSRP állapotát. Az ábra parancskimenetében az látható, hogy ez a forgalomirányító az aktív.

# A GLBP ellenőrzése

Habár a HSRP és a VRRP is biztosítja a megfelelő rugalmasságot az átjáró szerephez, a redundancia csoport készenléti tagjainak a hálózatból kifelé irányuló sávszélességét nem használja.

HSRP és VRRP esetén csak a csoportok aktív forgalomirányítója végez csomagtovábbítást. A készenléti forgalomirányító erőforrásai nincsenek teljes mértékben kihasználva. Valamilyen mértékű terhelésmegosztást megvalósíthatunk ezekkel a protokollokkal is, létrehozhatunk több csoportot, több alapértelmezett átjárót oszthatunk ki az eszközöknek, de ez elég nagy adminisztrációs teher.

A GLBP a Cisco saját fejlesztésű protokollja, a meghibásodáskori automatikus átvételen kívül automatikus kiválasztást és több elérhető átjáró egyidejű használatát is lehetővé teszi. Amint az 1. ábrán is látható, a kliensek szemszögéből egyetlen alapértelmezett átjáró cím látszik, de a keretek továbbítása több forgalomirányító között oszlik meg.

A GLBP több csoport létrehozásának és több alapértelmezett átjáró konfigurálásának adminisztrációs terhe nélkül képes az erőforrásokat teljes mértékben kihasználni. A GLBP jellemzői:

* Több csoport létrehozásának adminisztrációs terhe nélkül képes minden eszköz erőforrásait teljes mértékben kihasználni.
* Egyetlen virtuális IP-címet és több virtuális MAC-címet használ.
* A forgalom egyetlen alapértelmezett átjárón keresztül halad, de eloszlik a forgalomirányítók között.
* Hiba esetén automatikusan átirányítja a forgalmat.

A **show glbp** paranccsal kérdezhetjük le a GLBP állapotát. A 2. ábrán látható, hogy az 1-es GLBP csoport állapota aktív, virtuális IP-címe 192.168.2.100.

# Parancsszimulátor - HSRP és GLBP

A HSRP és a GLBP konfigurációja nem része a tanfolyam anyagának, azonban a protokollok parancsainak ismerete nagyban segíti azok megértését. A parancsszimulátor és az azt követő laborgyakorlat nem kötelező feladat.

# Laborgyakorlat - HSRP és GLBP konfigurálása

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

* 1. rész: A hálózat felépítése és a kapcsolatok ellenőrzése
* 2. rész: Redundancia konfigurálása HSRP-vel
* 3. rész: Redundancia konfigurálása GLBP-vel

[Lab - Configuring HSRP and GLBP](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.4.3.4%20Lab%20-%20Configuring%20HSRP%20and%20GLBP.pdf)

# Csoportos feladat - STP-dokumentáció

**STP-dokumentáció**

Az épület dolgozóinak nehézségei támadtak a hálózat webszerverének elérésével kapcsolatban. Meg szeretnénk nézi az előző hálózati szakember által készített dokumentációt, de semmit nem találunk.

Ezért úgy döntünk, hogy megalkotjuk a saját dokumentációs rendszerünket. A hálózati hierarchia hozzáférési rétegénél kezdjük el a munkát. Itt találhatók a redundáns kapcsolók, valamint a cég szerverei, nyomtatói és helyi kiszolgálói.

Táblázatot készítünk, amely tartalmazza a hozzáférési réteg kapcsolóit. Dokumentálni fogjuk a kapcsolók neveit, a használt portokat, a kábeles kapcsolatokat, a gyökér portokat, valamint a kijelölt és alternatív portokat.

[Class Activity - Documentation Tree](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/2.5.1.1%20Documentation%20Tree%20Instructions.pdf)

# Összefoglalás

Egy 2. rétegbeli redundáns hálózat olyan problémákhoz vezethet, mint a szórási viharok, a MAC-adatbázis instabilitás és a duplikált egyedi keretek. Az STP egy olyan 2. rétegbeli protokoll, amely biztosítja, hogy a hálózat bármely két eszköze között csak egy logikai útvonal létezzen, ezért a hurkot okozó redundáns útvonalakat szándékosan lezárja.

Az STP a kapcsolók között BPDU-keretekkel kommunikál. Minden feszítőfa példány egy-egy kapcsolóját gyökérponti hídnak választja. A rendszergazda a választásba a hídprioritás megváltoztatásával tud beleavatkozni. A gyökérponti hidak konfigurálhatók oly módon, hogy a feszítőfa protokolltól függően VLAN-onként vagy VLAN-csoportonként terhelésmegosztás jöjjön létre. Az STP minden résztvevő porthoz szerepet rendel, ehhez az útvonal költséget veszi figyelembe. Az útvonal költsége a gyökérponti hídhoz vezető útvonalon levő portok költségeinek összege. Minden portnak van automatikus költsége, de manuálisan is konfigurálható. A legalacsonyabb költségű útvonal a legelőnyösebb, minden más redundáns útvonal pedig le lesz tiltva.

A Cisco kapcsolókon az IEEE 802.1D alapértelmezés szerint a PVST+ algoritmust használja. Ez VLAN-onként külön-külön STP-t futtat. Az RSTP egy újabb, gyorsabban konvergáló feszítőfa protokoll, a Cisco kapcsolókon ennek VLAN-onkénti változata, a Rapid PVST+ használható. A Multiple Spanning Tree (MST) a Multiple Spanning Tree Protocol (MSTP) Cisco megvalósítása, ahol egy feszítőfa példány egy meghatározott VLAN-csoport számára fut. A PortFast és a BPDU-védelem (BPDU guard) funkciók biztosítják, hogy a kapcsolt hálózat állomásai azonnal hozzáférjenek a hálózat erőforrásaihoz.

Az FHRP-protokollok - ilyen a HSRP, a VRRP vagy a GLBP - alternatív alapértelmezett átjárót biztosítanak a redundáns forgalomirányítókat vagy többrétegű kapcsolókat tartalmazó hálózat állomásainak számára. Ilyenkor több forgalomirányító használ közös virtuális IP- és MAC-címet, ez lesz a kliensek alapértelmezett átjárója. A virtuális forgalomirányító biztosítja, hogy az állomások az alapértelmezett átjáró meghibásodása esetén is elérjék a távoli hálózatokat. HSRP vagy VRRP használatakor a csoport egy forgalomirányítója aktív (továbbító) szerepben működik, a többiek pedig készenléti (tartalék) módban vannak. A GLBP az automatikus szerep átvétel mellett több átjáró egyidejű használatát is lehetővé teszi terheléselosztás céljából.

# 

* [Fejezet száma 3 Portok összefogása (Link Aggregation)](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#3)
* [3.0 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#3.0)
* [3.0.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#3.0.1)
* [3.0.1.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#3.0.1.1)

# Bevezetés

A portok összefogásával (link aggregation) az eszközök közötti fizikai kapcsolatok egyetlen logikai összeköttetéssé egyesíthetők. Így terheléselosztás alkalmazható a fizikai kapcsolatokon anélkül, hogy az STP egyet vagy többet blokkolna közülük. A kapcsolt hálózatokban a portegyesítés egyik módja az EtherChannel.

A fejezetben az EtherChannel tulajdonságaival és létrehozásának módjaival foglalkozunk. Az EtherChannel konfigurálható manuálisan, vagy a Cisco fejlesztésű PAgP (Port Aggregation Protocol), illetve az IEEE 802.3ad szabványban definiált LACP (Link Aggregation Control Protocol) protokollok használatával. A fejezetben szó esik még az EtherChannel beállításáról, ellenőrzéséről és hibaelhárításáról is.

# Csoportos feladat - Képzeljük el!

**Képzeljük el!**

Vége van a munkanapnak. Vállalatunknál megpróbáljuk elmagyarázni a hálózati mérnököknek, hogyan működik az EtherChannel és hogyan néz ki a fizikai megvalósításban. A mérnökök nehezen tudják elképzelni a két kapcsolót összekötő vezetékeket egyetlen közös csatornaként. Pedig a vállalatnál határozott cél az EtherChannel bevezetése.

Ezért azzal zárjuk a megbeszélést, hogy egy feladatot adunk a mérnököknek. A másnapi értekezletre készülve végezzenek némi kutatást az EtherChannel hálózati kapcsolatokról, és hozzák el annak egy grafikai ábráját. Majd ez alapján ismertessék az EtherChannel hálózatok működését a többi mérnökkel.

Az EtherChannel utáni kutatáskor érdemes rákeresni a "Hogyan néz ki az EtherChannel?" kérdésre. A kutatás alapján pedig egy néhány diából álló bemutatót ajánlott készíteni, amelyet be lehet mutatni a hálózati mérnökök csoportjának. Prezentáció használatával biztosítható a könnyű érthetősége annak, hogy miként kerül megvalósításra az EtherChannel egy hálózati topológiában. Célunk, hogy a másnapi megbeszélés végén mindenki jó gondolatnak tartsa az EtherChannel felvételét a hálózatfejlesztési tervek közé.

[Csoportos feladat - Képzeljük el!](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/3.0.1.2%20Imagine%20This%20Instructions.pdf)

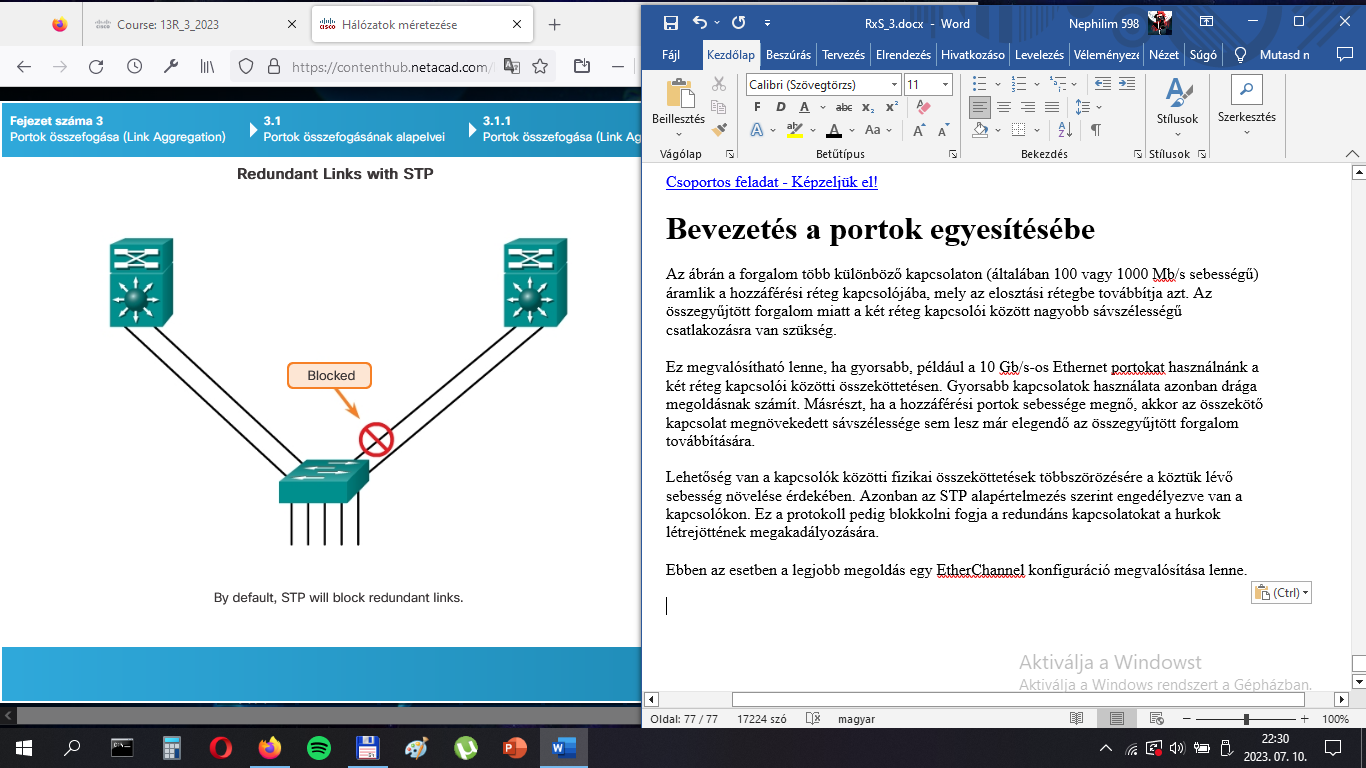
# Bevezetés a portok egyesítésébe

Az ábrán a forgalom több különböző kapcsolaton (általában 100 vagy 1000 Mb/s sebességű) áramlik a hozzáférési réteg kapcsolójába, mely az elosztási rétegbe továbbítja azt. Az összegyűjtött forgalom miatt a két réteg kapcsolói között nagyobb sávszélességű csatlakozásra van szükség.

Ez megvalósítható lenne, ha gyorsabb, például a 10 Gb/s-os Ethernet portokat használnánk a két réteg kapcsolói közötti összeköttetésen. Gyorsabb kapcsolatok használata azonban drága megoldásnak számít. Másrészt, ha a hozzáférési portok sebessége megnő, akkor az összekötő kapcsolat megnövekedett sávszélessége sem lesz már elegendő az összegyűjtött forgalom továbbítására.

Lehetőség van a kapcsolók közötti fizikai összeköttetések többszörözésére a köztük lévő sebesség növelése érdekében. Azonban az STP alapértelmezés szerint engedélyezve van a kapcsolókon. Ez a protokoll pedig blokkolni fogja a redundáns kapcsolatokat a hurkok létrejöttének megakadályozására.

Ebben az esetben a legjobb megoldás egy EtherChannel konfiguráció megvalósítása lenne.



**Az EtherChannel előnyei**

Az EtherChannel technológia Cisco fejlesztésű, amely a LAN-kapcsolók közötti Fast Ethernet vagy Gigabit Ethernet portok egyetlen logikai csatornába rendezésére szolgál. Az EtherChannel konfigurálása után létrejövő virtuális interfész neve port-csatorna. A fizikai interfészek egymáshoz kötegelve egy port-csatorna interfészt alkotnak.

Az EtherChannel technológia számos előnnyel rendelkezik:

* A legtöbb konfigurációs feladat elvégezhető az EtherChannel interfészen, így nincs szükség a portok egyedi kezelésére, ezzel biztosítható azok következetes beállítása.
* Az EtherChannel a létező kapcsolóportokat használja, így nincs szükség gyorsabb és jóval drágább összeköttetésre a nagyobb sávszélesség eléréséhez.
* Ugyanahhoz az EtherChannel-hez tartozó portok között terheléselosztás valósul meg. Hardvertől függően egy vagy több terheléselosztási mód is alkalmazható. Ez alapján beszélhetünk forrás és cél MAC közötti, illetve forrás és cél IP közötti terheléselosztásról a fizikai kapcsolaton.
* Az EtherChannel-be rendezett portcsoport egyetlen logikai kapcsolatként látszik. Ha két kapcsoló között több EtherChannel nyaláb is van, akkor az STP blokkolhat közülük néhányat a hurkok kialakulásának elkerülése érdekében. Ha az STP blokkol egy redundáns kapcsolatot, akkor zárolja az egész EtherChannel-t. Vagyis letiltja az összes portot, amely hozzá tartozik. Amikor csak egy EtherChannel kapcsolat létezik, akkor az összes benne levő fizikai port aktív marad, mivel az STP csak egy (logikai) kapcsolatot lát.
* Az EtherChannel redundanciát biztosít, mert a teljes összerendezett nyaláb egy logikai kapcsolatot alkot. Továbbá a csatorna valamely fizikai portjának kiesése sem okoz változást a topológiában, ezért a feszítőfa (spanning tree) újraszámolása sem szükséges. Amíg legalább egy fizikai port jelen van, addig az EtherChannel is működőképes marad, de a kiesett portok miatt a teljes átbocsátóképesség lecsökken.

# A megvalósítás korlátai

Az EtherChannel megvalósítása a fizikai portok egy vagy több logikai csatornába rendezését (összefogását) jelenti.

**MEGJEGYZÉS**: Az interfészek típusai nem keverhetők, például Fast Ethernet és Gigabit Ethernet típusok nem kerülhetnek vegyesen egy EtherChannel-be.

Az EtherChannel legfeljebb 800 Mb/s (Fast EtherChannel) vagy 8 Gb/s (Gigabit EtherChannel) teljes duplex sávszélességet biztosít kapcsoló-kapcsoló vagy kapcsoló-kiszolgáló viszonylatban. Minden csatorna legfeljebb nyolc, azonosan konfigurált Ethernet portból állhat. Jelenleg egy Cisco IOS-t futtató kapcsolón egyidejűleg hat EtherChannel lehet. Azonban új IOS-verziók megjelenésével néhány eszközön és bővítőkártyán nagyobb portszámú EtherChannel link is konfigurálható, illetve a csatornák száma is több lehet. Az elv változatlan, legyen szó bármekkora sebességről vagy a részt vevő kapcsolatok számáról. Az EtherChannel konfigurálásakor vegyük figyelembe a hardverekre vonatkozó előírásokat és korlátozásokat!

Az EtherChannel eredeti célja, hogy megnövelje a kapcsolók közötti összevont kapcsolatokon a sebességet. Az EtherChannel technológia népszerűvé válásával azonban az elv is megváltozott, és manapság már számos szerver támogatja a portok összevonását EtherChannel használatával. Az EtherChannel egy-az-egyhez típusú kapcsolat, azaz egy csatorna mindössze két eszközt köt össze. A csatorna létrejöhet két kapcsoló vagy egy EtherChannel-kompatibilis szerver és egy kapcsoló között. Tehát a forgalom nem küldhető azonos EtherChannel-en keresztül két különböző kapcsolóhoz.

A csatorna egyedi portjainak konfigurációja mindkét eszközön azonos kell legyen. Ha az egyik oldalon a fizikai portok trönk módban vannak, akkor a másik oldal portjainak is trönk módban kell lenniük azonos natív VLAN-nal. Továbbá, az EtherChannel kapcsolat összes portját kötelezően 2. rétegbeli portnak kell beállítani.

**MEGJEGYZÉS**: 3. rétegbeli EtherChannel konfigurálható a Cisco Catalyst többrétegű kapcsolókon, például a Catalyst 3560 típuson, ez viszont nem képezi részét a tananyagnak. 3. rétegbeli EtherChannel esetén a logikailag összerendelt kapcsolóportokhoz egy egyedi IP-cím társul.

Minden EtherChannel-hez tartozik egy logikai port-csatorna interfész, ahogy ez az ábrán is látható. A port-csatorna interfészen elvégzett beállítások minden olyan fizikai portra alkalmazódnak, amely tagja a csatornának.

# Port egyesítő protokoll (Port Aggregation Protocol, PAgP)

EtherChannel-ek automatikus egyeztetés útján is létrehozhatók két protokoll segítségével, ezek a PAgP és az LACP. A két protokoll a szomszédos kapcsolók hasonló jellemzőkkel bíró portjai között dinamikusan alakít ki csatornákat.

**MEGJEGYZÉS**: EtherChannel statikusan is konfigurálható, ekkor nincs szükség PAgP-re vagy LACP-re.

**PAgP**

A PAgP a Cisco saját fejlesztésű protokollja, mely az EtherChannel kapcsolatok automatikus létrehozását segíti. Használata esetén a kapcsolók PAgP-csomagokkal egyeztetnek a portok között az EtherChannel kialakításához. Ha a PAgP megfelelő Ethernet portokat talál, összefogja azokat egy EtherChannel-be, amely ezután egyedi portként vesz részt a feszítőfában.

Ha engedélyezett, a PAgP csatornafelügyelet is végez. A PAgP-csomagok 30 másodpercenként kerülnek elküldésre. A protokoll ezekkel ellenőrzi a konfiguráció egyezőségét, valamint vezérli a kapcsolatok hozzáadását és hibáit a kapcsolók között. Biztosítja azt is, hogy az EtherChannel létrehozása során a résztvevő portok beállításai azonosak legyenek.

**MEGJEGYZÉS**: EtherChannel esetén előírás, hogy minden port azonos sebességgel, duplexitással és VLAN-tagsággal rendelkezzen. A csatorna létrehozása után végrehajtott bármilyen port módosítás maga után vonja a csatorna összes portjának megváltozását.

A PAgP azzal segíti az EtherChannel kapcsolat létrehozását, hogy felismeri mindkét oldal konfigurációját és biztosítja a portok kompatibilitását, így szükség esetén a csatorna azonnal engedélyezhetővé válik. Az ábra a PAgP-re vonatkozó csatorna módokat mutatja be.

* **Bekapcsolt (On)** - Ebben a módban az interfész direkt módon kerül a csatornába PAgP használata nélkül. Az ilyen módra konfigurált interfészek nem cserélnek PAgP-csomagokat egymással.
* **Kezdeményező (PAgP desirable)** - Ez a PAgP-mód aktív egyeztető állapotba helyezi az interfészt, amely így PAgP-csomagokat küld kezdeti egyeztetés céljából más interfészeknek.
* **Automatikus (PAgP auto)** - Ez a PAgP-mód passzív egyeztető állapotba helyezi az interfészt, amely válaszol a beérkező PAgP-csomagokra, de nem kezdeményez egyeztetést.

A két oldalon beállított módoknak kompatibilisnek kell lenniük egymással. Ha az egyik oldal "auto" módban van, az passzív állapotot jelenet, várakozni fog a másik oldal által kezdeményezett EtherChannel egyeztetésre. Ha a másik oldal is "auto" módban van, akkor soha nem kezdődik egyeztetés és nem jön létre a csatorna. Ha mindenféle módot kikapcsolunk a **no** paranccsal, vagy nem állítunk be semmilyen módot sem, akkor az EtherChannel tiltva lesz.

Az "on" módra beállított interfész mindenféle egyeztetés nélkül, manuálisan kerül be egy csatornába. Ez csak akkor működik, ha a másik oldal is "on" módban van. Ha a másik oldal PAgP-egyeztetést használ, akkor sem jön létre a csatorna, mivel az "on" módban levő interfész nem képes az egyeztetésre.

# Port egyesítő vezérlési protokoll (Link Aggregation Control Protocol, LACP)

**LACP**

Az LACP az IEEE 802.3ad szabvány része, amely lehetővé teszi fizikai portok összefogását egyetlen logikai csatornába. A protokoll LACP-csomagokkal egyeztet a kapcsolók között a csatorna automatikus létrehozásához. Rendeltetése azonos a Cisco PAgP-jével. Mivel az LACP egy IEEE-szabvány, ezért különböző gyártók berendezései között is lehetővé teszi az EtherChannel-ek kialakítását. Cisco eszközökön mindkét protokoll támogatott.

**MEGJEGYZÉS**: Az LACP eredeti leírása az IEEE 802.3ad szabványban található. A jelenleg viszont az újabb, helyi és városi hálózatokat leíró IEEE 802.1AX szabványban van dokumentálva.

A PAgP-hez hasonlóan, az LACP is azzal segíti az EtherChannel kapcsolat létrehozását, hogy felismeri mindkét oldal konfigurációját és biztosítja a portok kompatibilitását, így szükség esetén a csatorna azonnal engedélyezhetővé válik. Az ábra az LACP-re vonatkozó csatorna módokat mutatja be.

* **Bekapcsolt (On)** - Ebben a módban az interfész direkt módon kerül a csatornába LACP használata nélkül. Az ilyen módra konfigurált interfészek nem cserélnek LACP-csomagokat egymással.
* **Aktív (LACP active)** - Ez az LACP-mód aktív egyeztető állapotba helyezi az interfészt, amely így LACP-csomagokat küld kezdeti egyeztetés céljából más interfészeknek.
* **Passzív (LACP passive)** - Ez az LACP-mód passzív egyeztető állapotba helyezi az interfészt, amely válaszol a beérkező LACP-csomagokra, de nem kezdeményez egyeztetést.

Csakúgy, mint a PAgP-nél itt is ügyelni kell arra, hogy a két oldalon beállított módok kompatibilisek legyenek egymással, különben az EtherChannel kapcsolat nem jön létre. Az "on" mód ismételten szerepel, mert az így beállított interfész manuálisan kerül bele egy csatornába, PAgP vagy LACP dinamikus egyeztetés nélkül.

# Konfigurálási útmutató

Az alábbi irányelvek és korlátozások hasznosak lehetnek az EtherChannel beállításakor:

* **EtherChannel támogatás** - Minden modulon az összes Ethernet interfésznek támogatnia kell az EtherChannel technológiát. A portoknak viszont nem kell fizikailag egymás mellett lenniük, sőt lehetnek különböző modulokban is.
* **Sebesség és duplexitás** - Az EtherChannel összes interfészét azonos sebességre és egyforma duplexitásra kell beállítani, ahogy az ábrán is látható.
* **VLAN-tagság** - Az EtherChannel összes interfészét azonos VLAN-hoz kell hozzárendelni vagy trönk módúra kell állítani, (ez szintén látható az ábrán is).
* **VLAN-tartomány** - Ha az EtherChannel interfészek trönk módban vannak, akkor az engedélyezett VLAN-tartománynak mindegyiken egyezni kell. Ha a tartományok között eltérés van, akkor az interfészek nem kerülnek be a csatornába még akkor sem, ha **auto** vagy **desirable** módban vannak.

A fenti beállítások megváltoztatását port-csatorna interfész konfigurációs módban lehet megtenni. A port-csatorna interfész beállítása után, a csatornán végrehajtott bármely módosítás az összes egyedi fizikai interfészen is érvényesítésre kerül. Ugyanakkor az egyedi interfészeken végzett módosítások nem érvényesülnek a port-csatorna interfészen. Ezért az EtherChannel kapcsolathoz tartozó egyedi portokon végrehajtott konfigurációs módosítások kompatibilitási problémákat is okozhatnak.

# Interfészek konfigurálása

Az EtherChannel konfigurálását LACP-vel két lépésben lehet elvégezni:

**1. lépés** Adjuk meg az EtherChannel csoportot alkotó interfészeket az **interface range** *interfész-név* globális konfigurációs paranccsal. A **range** kulcsszó lehetővé teszi, hogy több interfészt együtt tudjunk konfigurálni. Bevált gyakorlat a portok lekapcsolásával kezdeni abból a célból, hogy egy hiányos konfiguráció ne okozzon felesleges tevékenységet a kapcsolaton.

**2. lépés** Hozzuk létre a port-csatorna interfészt a **channel-group** *azonosító* **mode active** paranccsal interfész tartomány konfigurációs módban. Az azonosító a csatorna sorszámát határozza meg. A **mode active** kulcsszavak azt mutatják, hogy ez egy LACP EtherChannel beállítás.

**MEGJEGYZÉS**: Az EtherChannel alapértelmezés szerint nincs engedélyezve.

Az 1. ábrán a FastEthernet0/1 és a FastEthernet0/2 portok kerültek bele az 1-es sorszámú port-csatorna EtherChannel interfészbe.

A port-csatorna interfész 2.rétegbeli beállításainak megváltoztatásához lépjünk be port-csatorna interfész konfigurációs módba az interface port-channel parancs és az ezt követő azonosító szám használatával. A példában az EtherChannel trönk interfészként van konfigurálva engedélyezett VLAN-ok megadásával. Az 1. ábrán szintén látható, hogy az 1-es sorszámú port-csatorna trönk módra van beállítva, az engedélyezett VLAN-jai pedig az 1, 2 és 20.

Használjuk a 2. ábrán található parancsszimulátort az EtherChannel beállítására az S1 kapcsolón.

# Packet Tracer - EtherChannel konfigurálása

**Esetleírás**

Három olyan kapcsoló került mostanában üzembe helyezésre, amelyek között redundáns összeköttetések találhatók. Az összeköttetések közül azonban csak egy lehet aktív, különben kapcsolási hurok jönne létre. Kizárólag egy összeköttetés használatával viszont az elérhető sávszélességnek csak a fele használható ki. EtherChannel alkalmazásával azonban kialakítható egy olyan logikai csatorna, amely legfeljebb nyolc redundáns kapcsolatot tartalmazhat. Ebben a feladatban a Cisco saját fejlesztésű PAgP (Port Aggregation Protocol) illetve az IEEE 802.3ad nyílt szabványú LACP (Link Aggregation Control Protocol) EtherChannel protokollok konfigurálását fogjuk elvégezni.

[Packet Tracer - Configuring EtherChannel Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/3.2.1.3%20Packet%20Tracer%20-%20Configuring%20EtherChannel%20Instructions.pdf)

[Packet Tracer - Configuring EtherChannel - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/3.2.1.3%20Packet%20Tracer%20-%20Configuring%20EtherChannel.pka)

# Az EtherChannel ellenőrzése

Számos parancs létezik az EtherChannel konfigurációjának ellenőrzésére. A **show interface port-channel** parancs a port-csatorna interfész általános állapotát jeleníti meg. Az 1. ábrán a Port-channel1 interfész működő (up) állapotban van.

Ha egy eszközön több port-csatorna interfész is található, használjuk a **show etherchannel summary** parancsot, melynek kimenete minden port-csatornáról egy rövid, egysoros információt jelenít meg. A 2. ábrán látható, hogy a kapcsolón egy EtherChannel lett létrehozva, amely 1-es sorszámmal rendelkezik és LACP használatára van beállítva.

A csatorna a FastEthernet0/1 és a FastEthernet0/2 portokat tartalmazza. 2. rétegbeli EtherChannel-ként van konfigurálva és használatban van, ahogy ezt a port-csatorna neve utáni SU betűk is jelzik.

Használjuk a **show etherchannel port-channel** parancsot egy adott port-csatorna interfész részletes információinak megjelenítéséhez a 3. ábrán látható módon. A példában szereplő Port-channel1 interfész két fizikai portot tartalmaz, a FastEthernet0/1 és a FastEthernet0/2 portokat. A csatorna LACP-t használ aktív módban. Megfelelően csatlakozik egy másik kapcsolóhoz, a konfigurációjuk kompatibilis egymással, ezért is mondhatjuk azt, hogy a port-csatorna használatban van (in use).

Az EtherChannel csatorna bármely fizikai portjának csatornán belüli szerepéről a **show interfaces etherchannel** parancs nyújt információkat, a 4. ábrán látható módon. A FastEthernet 0/1 interfész az 1-es EtherChannel csatorna tagja. Ez a csatorna az LACP protokollt használja.

Használjuk az 5. ábrán található parancsszimulátort az EtherChannel ellenőrzésére az S1 kapcsolón.

**Az EtherChannel hibaelhárítása**

Az EtherChannel összes interfészének azonos konfigurációval kell rendelkeznie a sebesség, a duplexitás, a trönkportokon engedélyezett és natív VLAN-ok, valamint a hozzáférési portok VLAN-tagsága tekintetében:

* Az EtherChannel összes portját azonos VLAN-hoz kell hozzárendelni vagy trönk módba kell állítani őket. Az eltérő natív VLAN-hoz tartozó portok nem alkothatnak EtherChannel-t.
* Ha az EtherChannel-t trönk portokból hozzuk létre, ellenőriznünk kell, hogy mindegyiken azonos trönk mód legyen beállítva. A nem egységes trönk módok megakadályozhatják az EtherChannel működését és a portok lekapcsolódását eredményezhetik (errdisable state).
* Az EtherChannel-be csak azok a trönk portok kerülhetnek bele, amelyek engedélyezett VLAN-tartománya egyező. Ha ez a tartomány nem azonos, a portok akkor sem alkothatnak EtherChannel-t, ha PAgP-beállításuk **auto** vagy **desirable** módú.
* PAgP vagy LACP használata esetén az egyeztetési beállításoknak kompatibilisnek kell lenniük egymással az EtherChannel mindkét végén.

**MEGJEGYZÉS**: A PAgP-t és az LACP-t könnyű összekeverni a DTP-vel, mivel mindegyik protokoll automatizmusokat alkalmaz a trönk vonalakon. A PAgP és az LACP portok összefogására szolgál (EtherChannel), míg a DTP a trönk vonalak kialakításának automatizálására használható. Egy EtherChannel trönk létrehozásakor jellemzően először az EtherChannel (PAgP vagy LACP) konfigurálását kell elvégezni és csak azután a DTP-ét.

Az 1. ábrán az S1 és az S2 kapcsolók F0/1 és F0/2 portjain létrehozott EtherChannel látható. A parancskimenet szerint az EtherChannel üzemen kívüli állapotban van (down).

A 2. ábrán lévő részletes parancskimenetből kiderül, hogy az S1-en és az S2-n konfigurált PAgP-módok nem kompatibilisek egymással.

A 3. ábrán az EtherChannel PAgP-módja "desirable" értékre változott, így a csatorna működésbe lépett.

**MEGJEGYZÉS**: Az EtherChannel-nek és a feszítőfának szoros együttműködésben kell lenniük egymással. Emiatt fontos az EtherChannel parancsok használatának sorrendje, erre a 3. ábrán is látható egy példa, ahol a Port-channel1 először eltávolításra került, majd utána újra létre lett hozva a **channel-group** paranccsal, pedig közvetlenül is módosítani lehetett volna. Viszont, ha valaki közvetlenül próbálja meg a konfigurációt megváltoztatni, feszítőfa hibák léphetnek fel és az érintett portok blokkolt vagy hiba miatt lekapcsolt állapotba kerülhetnek.

#  [3.2.2.4 Laborgyakorlat - Az EtherChannel hibaelhárítása](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#3.2.2.4) Csoportos feladat - Kapcsolatépítés

**Kapcsolatépítés**

Vállalatunk hálózatában torlódások alakultak ki, annak ellenére is, hogy a céges kapcsolókon VLAN-okat, STP-t és más forgalomszervezési beállításokat alkalmaztunk.

A jelenlegi állapot nem tartható tovább, ezért szeretnénk kipróbálni az EtherChannel-t legalább a hálózat egy részén, hogy lássuk csökkenti-e a túlterhelést a hozzáférési és az elosztási réteg kapcsolói között.

A vállalati hálózat elosztási rétegében Catalyst 3560 típusú, a hozzáférési rétegben pedig Catalyst 2960 és 2950 típusú kapcsolók üzemelnek. Látogassuk meg a [System Requirements to Implement EtherChannel on Catalyst Switches](http://www.cisco.com/en/US/tech/tk389/tk213/technologies_tech_note09186a0080094646.shtml)weboldalt, ahol ellenőrizhető, hogy ezek a kapcsolók támogatják-e az EtherChannel-t. Az oldalon további információk is találhatók annak eldöntéséhez, hogy jó választás-e az EtherChannel a jelenlegi hálózati berendezéseinkhez.

A modellek vizsgálata után úgy döntöttünk, hogy a valós hálózatba történő telepítés előtt egy szimulációs programban fogjuk gyakorolni az EtherChannel konfigurálását. Ennek keretében megbizonyosodtunk róla, hogy a Packet Tracer szimulációs eszközei megfelelőek a gyakorló konfigurálásra.

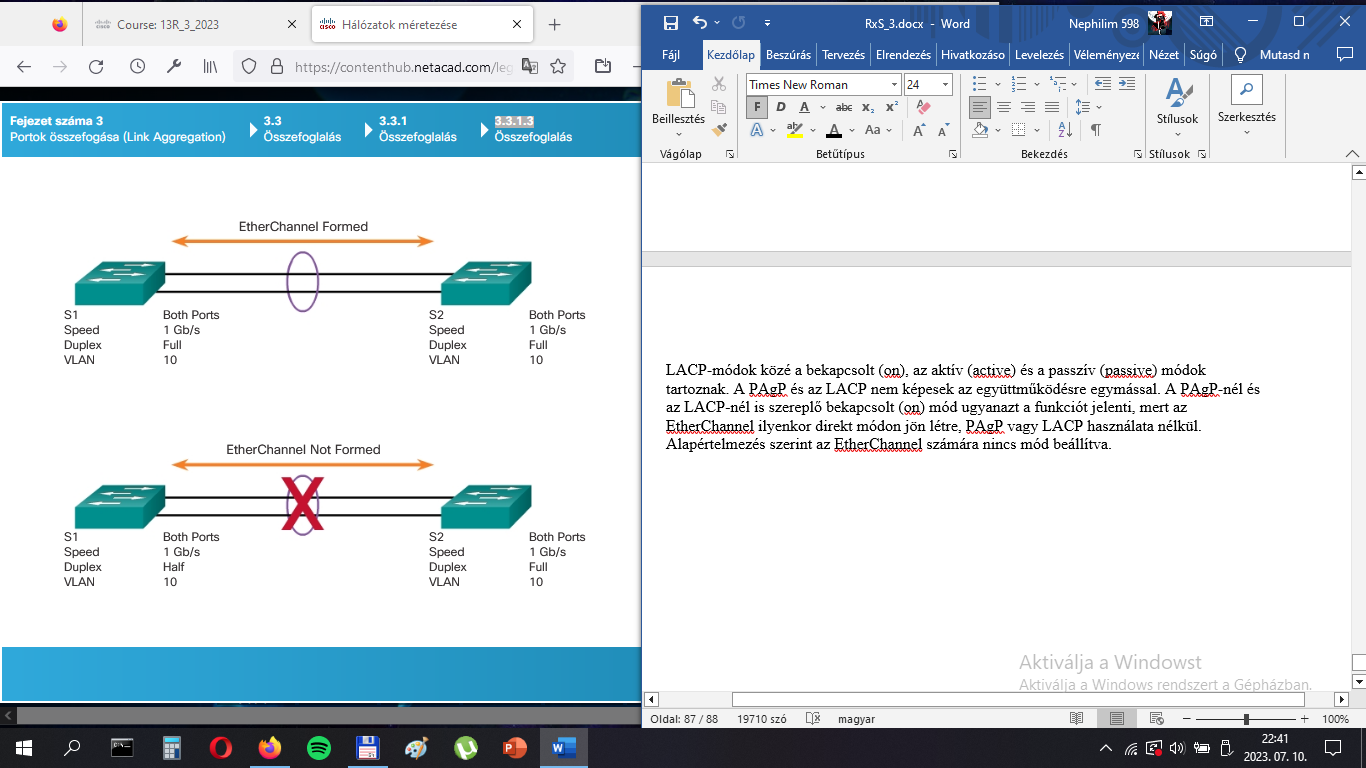
[Csoportos feladat - Kapcsolatépítés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/3.3.1.1%20Linking%20%20Up%20Instructions.pdf)

# <https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12025-49.html>

# Összefoglalás

Az EtherChannel kapcsolóportokat egyesít redundáns összeköttetéssé két eszköz közötti forgalom terheléselosztásának céljából. Az EtherChannel mindkét végpontján az összes fizikai portnak azonos sebesség és duplexitás beállítással, valamint egyező VLAN információkkal kell rendelkeznie. A port-csatorna interfészen végrehajtott módosítások érvényre jutnak a csatorna összes egyedi interfészén is. Az egyedi interfészeken végzett módosítások viszont nem érvényesülnek sem az EtherChannel interfészen, sem a csatorna többi fizikai portján.

A PAgP a Cisco saját fejlesztésű protokollja, amely segít az EtherChannel kapcsolatok automatikus létrehozásában. A PAgP-módok közé a bekapcsolt (on), a kezdeményező (desirable) és az automatikus (auto) módok tartoznak. Az LACP egy IEEE szabvány, amely szintén lehetővé teszi fizikai portok automatikus összefogását egyetlen logikai csatornába. Az LACP-módok közé a bekapcsolt (on), az aktív (active) és a passzív (passive) módok tartoznak. A PAgP és az LACP nem képesek az együttműködésre egymással. A PAgP-nél és az LACP-nél is szereplő bekapcsolt (on) mód ugyanazt a funkciót jelenti, mert az EtherChannel ilyenkor direkt módon jön létre, PAgP vagy LACP használata nélkül. Alapértelmezés szerint az EtherChannel számára nincs mód beállítva.



* [Fejezet száma 4 Vezeték nélküli hálózatok](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#4)
* [4.0 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#4.0)
* [4.0.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#4.0.1)
* [4.0.1.1 Bevezetés](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/index.html#4.0.1.1)

# Bevezetés

A vezeték nélküli hálózatok mobilitást biztosítanak a kliensek számára, hogy bárhonnan és bármikor csatlakozni tudjanak a hálózathoz, utazás, barangolás közben is. Vezeték nélküli helyi hálózat (Wireless LAN, WLAN) alatt az otthonokban, irodákban és épületekben használt vezeték nélküli hálózatokat értjük. Bár kábelek helyett rádiófrekvenciás hullámokat használ, de a kapcsolt hálózat részét képezi és az Ethernethez hasonló keretformátumot alkalmaz.

Ebben a fejezetben a WLAN technológiájáról, összetevőiről, biztonságáról, tervezéséről, megvalósításáról és hibaelhárításáról lesz szó. Különös tekintettel a hálózatok elleni támadásokra, melyre a vezeték nélküli rendszerek fölöttébb érzékenyek.

# Csoportos feladat - Kutassunk fel vezeték nélküli megoldásokat!

**Csoportos feladat - Kutassunk fel vezeték nélküli megoldásokat!**

Hálózati rendszergazdaként azt a feladatot kaptuk, hogy fejlesszük tovább a vállalat épületen belüli és kívüli vezeték nélküli hálózatát. Ebben segítségünkre lehet, ha megismerjük más vállalatok és intézmények WLAN csatlakozási megoldásait.

Keressük fel a "[Customer Case Studies and Research](http://www.cisco.com/c/en/us/products/wireless/customer-case-study.html" \t "_blank)" weboldalt és vizsgáljuk meg a használt vezeték nélküli technológiákat. Néhány videó megtekintése és esettanulmányok átolvasása után a csoport két tagja mutassa be a vezeték nélküli hálózat fejlesztésére vonatkozó javaslatokat.

A feladatra vonatkozó részletes utasítások a melléklet PDF-dokumentumban találhatók.

[Csoportos feladat - Kutassunk fel vezeték nélküli megoldásokat!](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/4.0.1.2%20Make%20Mine%20Wireless%20Instructions.pdf)

<https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-architecture-customer-success-stories.html?flt1_general-table0=Wireless&flt2_general-table0=null#~case-studies>

# Mobilitás

Napjaink vállalati hálózatai támogatják a mozgásban lévő munkavállalókat, akik eközben különféle számítógépeket, laptopokat, tableteket és okostelefonokat használnak. A mobilitás azt jelenti számukra, hogy utazás közben is kapcsolatban tudnak maradni a hálózattal.

Több különféle megoldás is létezik a mobilitás biztosítására, de vállalati környezetben a legfontosabb a vezeték nélküli helyi hálózat (WLAN).

A termelékenység többé nem kötődik meghatározott helyhez vagy időtartamhoz. Az emberek elvárják, hogy bárhol és bármikor kapcsolódni tudjanak hálózathoz a munkahelytől kezdve a repülőtéren keresztül egészen otthonukig. Régebben a munkavállalók utazás közben csak korlátozottan tudták üzeneteiket és hívásaikat fogadni, míg manapság okostelefonon váltanak hangüzenetet vagy email-t.

A felhasználók elvárják a szolgáltatástól a barangolás lehetőségét, mely a mozgásban lévő vezeték nélküli eszközök számára biztosítja a folyamatos hálózati kapcsolatot.

A videó a vezeték nélküli hálózat mobilitását mutatja be. Kattintsunk a lejátszás gombra!

# A vezeték nélküli hálózat előnyei

A vezeték nélküli hálózatnak számos előnye van mind otthoni, mind vállalati környezetben. Ilyenek a nagyobb rugalmasság és termelékenység, az alacsonyabb költségek, valamint a változó szükségletekhez való igazodás.

Az 1. ábra a vezeték nélküliség rugalmasságára mutat példát a mobilis munkavállalók esetére.

A legtöbb vállalat kapcsolt helyi hálózatot használ napi tevékenységéhez. Azonban az emberek egyre mozgékonyabbak és a munkaasztaluktól távolabb is szeretnének kapcsolatban maradni a vállalati erőforrásokkal. A dolgozók szeretnék magukkal vinni mobil eszközeiket a megbeszélésekre, a szomszéd irodába, a konferenciaterembe vagy akár az ügyfélhez is, mindeközben megtartva az irodához való csatlakozást. A vezeték nélküli hálózat biztosítja ezt a fajta rugalmasságot, így nincs szükség többé hatalmas iratcsomók cipelésére, sem vezetékes hálózat kiépítésére.

Bár nehéz mérni, de a vezeték nélküli elérés eredményezhet megnövekedett termelékenységet, valamint elégedettebb dolgozót is, mivel lehetősége van ott és akkor végezni a munkáját, ahol akarja. Egyaránt reagálhat egy ügyfél kérésére akár az irodában tartózkodik, akár ebédelni ment. Könnyedén elérheti e-mail-jeit és egyéb munkaeszközeit, javítva a gazdálkodást, az ügyfél elégedettségét és a profitot.

Vezeték nélküli hálózat használata költségcsökkenést is jelenthet. Egy vezeték nélküli hálózattal rendelkező cég számára sokkal olcsóbb az eszközöket, dolgozókat más helyre költöztetni, laboratóriumot átrendezni, vagy ideiglenes helyre, kihelyezett projekt helyszínekre költözni.

A vezeték nélküli hálózat másik fontos előnye a változó szükségletekhez és technológiákhoz való alkalmazkodás. Egy új eszköz bekapcsolása a hálózatba sokkal zökkenőmentesebben végezhető vezetékek nélkül. Gondoljunk csak egy otthoni vezeték nélküli csatlakozásra. Internetezhetünk a konyhában, a nappaliban, de akár a kertben is, legyen a készülékünk okostelefon, tablet vagy televízió.

Amint a 2. ábrán látható, egy otthoni vezeték nélküli forgalomirányítóval ezeket az eszközöket többletköltség nélkül csatlakoztathatjuk, ráadásul a kábelezés kényelmetlenségétől is mentesülünk.

# Vezeték nélküli technológiákRádiófrekvenciák

Minden vezeték nélküli eszköz az elektromágneses spektrum rádióhullámú (RF) tartományában üzemel, melynek szétosztásáért az International Telecommunication Union - Radiocommunication Sector (ITU-R) felel. Bizonyos frekvenciatartományokat vagy sávokat különféle célokra használnak. Néhány sáv szigorúan szabályozott felhasználású, ilyen például a légiforgalom-irányítás és a katasztrófavédelmi kommunikáció. Más sávok szabad felhasználásúak, például az ISM (Industrial, Scientific, and Medical, ipari-, tudományos- és egészségügyi) és az UNII (unlicensed national information infrastructure) frekvenciasávok.

**Megjegyzés**: a WLAN hálózatok az ISM 2,4 GHz és az UNII 5 GHz tartományokban működnek.

Az ábrán a vezeték nélküli kommunikációt is tartalmazó rádióhullám tartomány (3kHz - 300 GHz) látható, mely két részből áll: rádiófrekvenciás tartomány és mikrohullámú tartomány. A WLAN, a Bluetooth, a mobil és a műholdas kommunikáció egyaránt a mikrohullámú UHF, SHF és EHF tartományokban folyik.

A vezeték nélküli LAN-eszközök adó- és vevőáramkörei adott frekvenciatartományra vannak hangolva, melyek a 802.11 szabvány szerint a következők:

* **2,4 GHz (UHF)** - 802.11b/g/n/ad
* **5 GHz (SHF)** - 802.11a/n/ac/ad
* **60 GHz** **(EHF)** - 802.11ad

Vezeték nélküli kommunikációt számos területen használnak.

Bár a vezeték nélküli technológiák folyamatosan fejlőnek, ebben kurzusban a felhasználók mobilitását biztosító vezeték nélküli hálózatok állnak a fókuszban. A vezeték nélküli hálózatok a következő osztályokba sorolhatók:

* **Vezeték nélküli személyi hálózat (Wireless Personal-Area Network, WPAN)** - Hatótávolsága néhány méter. A Bluetooth vagy a Wi-Fi Direct készülékek használnak WPAN-t.
* **Vezeték nélküli helyi hálózat (WLAN)** - Hatótávolsága néhány 10 méter, jellemzően szobában, lakásban, irodában és épületen belül használják.
* **Vezeték nélküli nagytávolságú hálózat (Wireless Wide-Area Network, WWAN)** - Hatótávolsága néhány kilométer, nagyvárosi környezetben, mobilcellák és települések közötti mikrohullámú összeköttetésre használják.

Az ábrákra kattintva további információk jeleníthetők meg az alábbi vezeték nélküli kapcsolódási módokról:

* **Bluetooth** - IEEE 802.15 WPAN szabvány eszközpárok közötti kommunikációra, maximum 100 méterig. Az újabb Bluetooth verzió a Bluetooth Special Interest Group szabványa (<https://www.bluetooth.org/>).
* **Wi-Fi** - IEEE 802.11 WLAN szabvány, otthoni és vállalati felhasználók számára, adat-, hang- és videokommunikációhoz, körülbelül 300 méterig.
* **WiMAX (Worldwide Interoperability for Microwave Access)** - IEEE 802.16 WWAN szabvány, szélessávú vezeték nélküli kapcsolathoz, legfeljebb 50 km-ig. A kábeltévés és DSL kapcsolatok alternatívája. 2005 óta a szolgáltatók is használhatják mobil szélessávú hálózati hozzáférés biztosítására.
* **Mobil szélessávú szolgáltatás** - Különböző nemzeti és nemzetközi társaságok által használt technológia mobil szélessávú hálózati összeköttetés biztosítására. Először a 2. generációs mobiltelefonoknál jelent meg 1991-ben (2G), majd nagyobb sebességeken 2001-ben (3G) és 2006-ban (4G).
* **Műholdas szélessávú szolgáltatás** - A hálózati hozzáférést irányított parabola antennával biztosítja, mely egy Föld körüli geostacionárius pályán keringő műholdra néz. Rendszerint nagyon drága és tiszta rálátást igényel.

Sokféle vezeték nélküli technológia létezik, ebben a fejezetben a 802.11 WLAN-okról lesz szó.

# 802.11 szabványok

Az IEEE 802.11 WLAN szabvány határozza meg, hogy a vezeték nélküli kapcsolatok fizikai rétege és MAC alrétege hogyan használja az adott frekvenciatartományt.

Az IEEE 802.11szabványon belül számos megvalósítás jött létre az idők folyamán, melyek közül a jelentősebbek a következők:

* **802.11** - 1997-ben jelent meg, mára már elavult, ez az eredeti WLAN-specifikáció, a 2,4 GHz-es frekvenciatartományban működik, max. sebessége 2 Mb/s. Akkoriban a vezetékes hálózatok sebessége 10 Mb/s volt, így az új technológiát nem övezte lelkesedés. A vezeték nélküli eszközökben egyetlen antenna küldi és fogadja a jeleket.
* **IEEE 802.11a** - 1999-ben jelent meg, a kevésbé zsúfolt 5 GHz-es frekvenciatartományban működik max. 54 Mb/s sebességgel. A magasabb üzemelési frekvenciák miatt kisebb a lefedettségi területe, és kevésbé hatékony az épületfalakon keresztül történő továbbításban. A vezeték nélküli eszközökben egyetlen antenna küldi és fogadja a jeleket. A készülékek nem kompatibilisek a 802.11b és 802.11g szabványokkal.
* **IEEE 802.11b** - 1999-ben jelent meg, a 2,4 GHz-es frekvenciatartományban működik max. 11 Mb/s sebességgel. A szabvány alapján működő eszközök a 802.11a-hoz hasonlítva nagyobb hatótávolsággal rendelkeznek, és a jeleik hatékonyabban tudnak áthatolni az épületfalakon. A vezeték nélküli eszközökben egyetlen antenna küldi és fogadja a jeleket.
* **IEEE 802.11g** - 2003-ban jelent meg, a 2,4 GHz-es frekvenciatartományban működik max. 54 Mb/s sebességgel. A 802.11g nagyobb lefedettségét biztosít a 802.11a sebességén, de a 802.11b frekvenciasávján. A vezeték nélküli eszközökben egyetlen antenna küldi és fogadja a jeleket. A szabvány visszafelé kompatibilis a 802.11b-vel, de egy 802.11b kliens csatlakozásakor az összes kliens sávszélessége lecsökken.
* **IEEE 802.11n** - 2009-ban jelent meg, a 2,4 GHz-es és az 5 GHz-es frekvenciatartományban működik, ezért kétcsatornás eszköznek is nevezik. Adatátviteli sebessége 150 - 600 Mb/s, hatótávolsága max. 70 m. A nagyobb sebesség megvalósításához a hozzáférési pontok (AP) és a kliensek több antennával rendelkeznek a MIMO (multiple-input multiple-output) technológia miatt. A MIMO több antennát használ mind az adáshoz, mind a vételhez, ezzel növeli a kommunikáció teljesítményét (max. 4 antenna támogatott). A 802.11n szabvány visszafelé kompatibilis a 802.11a/b/g eszközökkel, de vegyes kliensekkel az átviteli sebesség alacsonyabb.
* **IEEE 802.11ac** - 2013-ban jelent meg, az 5 GHz-es frekvenciatartományban működik 450 Mb/s - 1,3 Gb/s sebességgel. MIMO technológiát használ, ezzel növeli a kommunikáció teljesítményét, max. 8 antennát támogat. A 802.11ac szabvány visszafelé kompatbilis a 802.11a/n eszközökkel, de vegyes kliensekkel alacsonyabb sávszélesség érhető el.
* **IEEE 802.11ad** - Várható megjelenése 2014, "WiGig" néven is ismert, 3-csatornás megoldás a 2,4 GHz, a 5 GHz és a 60 GHz használatával, max. sebessége 7 Gb/s. A 60 GHz-es sáv közvetlen rálátást igényel, ezért képtelen az épületfalakon való áthatolásra. Ha a felhasználó mozogni kezd, a készülék átvált az alacsonyabb 2,4 GHz és 5 GHz frekvenciákra. A szabvány kompatibilis az összes létező WiFi-eszközzel, de vegyes kliensekkel az átviteli sebesség alacsonyabb.

Az ábrán a 802.11 szabványok összesítve láthatók.

# Wi-Fi tanúsítvány

A szabványok lehetővé teszik a különböző gyártók eszközei közötti együttműködést. A WLAN-szabványokat három nemzetközi szervezet kezeli:

* **ITU-R** - Felügyeli a frekvenciatartományok kiosztását és a műholdak elhelyezését.
* **IEEE** - Meghatározza, hogyan kell a rádióhullámokat modulálni az információ átviteléhez. Karbantartja az IEEE 802 LAN/MAN szabványcsaládot, mely a helyi (LAN) és a nagyvárosi (MAN) hálózatokat írja le. Az IEEE 802 család két legjelentősebb tagja a 802.3 Ethernet és a 802.11 WLAN. Bár az IEEE szabályozza az RF modulációt végző eszközöket, de ipari szabványt nem ír elő, így a különböző gyártók 802.11 implementációi együttműködési problémákat okozhatnak a berendezések között.
* **Wi-Fi Szövetség** - A Wi-Fi Alliance® ([http://www.wi-fi.org](http://www.wi-fi.org/)) egy globális, non-profit, ipari szervezet, mely elkötelezett támogatója a WLAN-ok elterjesztésének. Tagjai olyan kereskedelmi szervezetek, akik jobbá kívánják tenni a 802.11 szabványú eszközök közötti együttműködést. Ezért minősítik a gyártókat az ipari normák és szabványok betartása alapján.

A Wi-Fi Alliance a következő termék-kompatibilitási tényezők szerint tanúsít:

* IEEE 802.11a/b/g/n/ac/ad kompatibilitás
* IEEE 802.11i biztonság, WPA2™ és EAP (Extensible Authentication Protocol) használat
* WPS (Wi-Fi Protected Setup), az eszközök egyszerű összekapcsolása
* Wi-Fi Direct, az eszközök adatátviteli közegének megosztása
* Wi-Fi Passpoint, a Wi-Fi hotspot-okhoz való egyszerű és biztonságos csatlakozás
* Wi-Fi Miracast, videojelek folyamatos továbbítása az eszközök között

**Megjegyzés**: További Wi-Fi tanúsított termékek is léteznek, például: WMM® (Wi-Fi Multimedia™), Tunneled Direct Link Setup (TDLS) és WMM-Power Save.

Az 1. ábrán a Wi-Fi Szövetség emblémái láthatók, melyek az adott eszköz különféle kompatibilitási tulajdonságait jelzik. Egy készüléken többféle logó is lehet.

Kattintsunk a 2-4. ábrákon a lejátszás gombra a Wi-Fi Direct, a Wi-Fi Passpoint és a Wi-Fi Miracast tulajdonságok megtekintéséhez!

**A WLAN és a LAN összehasonlítása**

A WLAN-ok és az Ethernet LAN-ok azonos alapokon nyugszanak, mindkettő az IEEE által alkotott 802 LAN/MAN számítógépes hálózati architektúra szabványba tartozik. A szabványcsalád két legjelentősebb tagja a 802.3 Ethernet és a 802.11 WLAN, de köztük jelentős különbség van.

A WLAN rádióhullámokat (RF) használ kábelek helyett a fizikai rétegben és az adatkapcsolati réteg MAC-alrétegében. A kábellel összevetve az RF-t a következők jellemzik:

* Az RF-nek nincs olyan fajta határa, mint a kábel burkolata. A rádióhullámon továbbított adatok mindazok számára elérhetők, akik képesek fogadni a rádiójeleket.
* Az RF védtelen a külső behatások ellen, míg a kábelt burkolat szigeteli el ezektől. Egyazon helyen lévő adók egymástól nem függnek, de ha azonos vagy közeli frekvenciát használnak, interferencia alakulhat ki közöttük.
* Az RF-átvitel is hasonló kihívásokkal küzd, mint bármely elektromágneses hullám alapú technológia, amilyen a hagyományos rádióadás is. Például, ha a vevő készülék távolodik az adótól, a rádióállomások között áthallás keletkezik és növekszik a statikus zaj, végül a jel teljesen elvész. Megfelelő hosszúságú kábelt használva a vezetékes hálózat jelminősége állandó.
* Az RF-tartományok országonként különböző módon szabályozottak. A WLAN-ok használata olyan kiegészítő előírások betartásával lehetséges, melyek a vezetékes hálózatokra nem vonatkoznak.

További különbségek:

* WLAN-ok esetében a kliensek csatlakozásához Ethernet kapcsoló helyett hálózati elérési pont (access point, AP) vagy vezeték nélküli forgalomirányító szükséges.
* A WLAN-okhoz gyakran akkumulátoros táplálású mobil eszközök kapcsolódnak, ellentétben a LAN-ok vezetékes energiaellátású berendezéseivel. A vezeték nélküli hálózati adapterek növelik a mobil eszközök fogyasztását, csökkentve ezzel az akku élettartamát.
* A WLAN-hoz csatlakozni kívánó állomásoknak le kell foglalniuk egy hullámsávot az RF-közegben. A 802.11 szabvány ütközés elkerülést (collision-avoidance, CSMA/CA) ír elő ütközés érzékelés (collision-detection, CSMA/CD) helyett, így előzetesen biztosítja az ütközésmentességet az átviteli közegben.
* A WLAN-ok más keretformátumot használnak, mint az Ethernet LAN-ok, az L2 fejrészbe további információk kerülnek.
* WLAN-ok esetén nagyobb a biztonsági kockázat, mivel a rádióhullámok az épület falain kívülre is eljutnak.

# Vezeték nélküli hálózati kártyák

A legegyszerűbb vezeték nélküli hálózathoz legalább két eszköz szükséges. Mindegyik berendezésben lenni kell egy adó- és egy vevőegységnek, melyek azonos frekvencián működnek.

Általában azonban egy vezeték nélküli hálózat telepítéséhez szükséges:

* Vezeték nélküli hálózati kártyával (wireless NIC) ellátott végberendezés
* Kiszolgáló eszköz, például vezeték nélküli forgalomirányító vagy elérési pont (AP)

A vezeték nélküli kommunikációt a végberendezésben lévő NIC végzi, mely tartalmazza adó/vevő áramkört is. Működtetéséhez pedig megfelelő szoftver meghajtó szükséges. A laptopok, tabletek és okostelefonok általában beépített vezeték nélküli hálózati kártyával rendelkeznek. Ha egy eszközben nincs ilyen NIC, akkor használhatunk USB vezeték nélküli adaptert.

Az ábrán kétféle vezeték nélküli hálózati adapter látható. A bal oldali egy mini USB adapter, a jobb oldali pedig egy másik USB-s változat.

**Vezeték nélküli otthoni forgalomirányító**

A végberendezéseket a hálózathoz kapcsoló hálózati kiszolgáló eszköz típusa többféle lehet a WLAN méretétől és követelményeitől függően.

Például egy otthoni felhasználó rendszerint egy kis méretű vezeték nélküli forgalomirányítóhoz csatlakoztatja eszközeit. A vezeték nélküli forgalomirányító egyben:

* **Hozzáférési pont (AP)** - 802.11a/b/g/n/ac vezeték nélküli elérést biztosít
* **Kapcsoló** - 4 portos, teljes duplex, 10/100/1000 Ethernet kapcsolóként üzemel
* **Forgalomirányító** - Alapátjáróként funkcionál más hálózatok eléréséhez

Amint az ábrán is látható, a vezeték nélküli forgalomirányító kisvállalati vagy otthoni környezetben gyakran elérési pontként működik. A forgalomirányító az internet szolgáltató (ISP) DSL-modemjéhez kapcsolódik, és alapjelzésekkel (beacon) hirdeti saját szolgáltatásait, melyek tartalmazzák saját azonosítóját is (shared service set identifier, SSID). A vezeték nélküli kliens eszközök felismerik a forgalomirányító SSID-t, megpróbálnak csatlakozni hozzá és hitelesíteni magukat, hogy internet eléréshez jussanak.

Ilyen feltételekkel egy vezeték nélküli forgalomirányító teljesítménye elegendő arra, hogy kiszolgálja a WLAN-t, a 802.3 Ethernet-et és az ISP-hez való kapcsolódást. A legtöbb vezeték nélküli forgalomirányító további funkciókkal is rendelkezik, például nagy sebességű hozzáférés, videofolyam támogatás, IPv6-címzés, QoS, konfigurációs segédprogram és USB-portok nyomtatók vagy hordozható meghajtók csatlakoztatására.

Ezen felül azok az otthoni felhasználók, akik szeretnék kibővíteni vezetékes és vezeték nélküli hálózatuk hatótávolságát, Poweline adaptert is telepíthetnek. Ez az eszköz elektromos vezetéken nyújt olyan hálózati összeköttetést, mely alkalmas HD videó adatfolyamok továbbítására és online játékokhoz is. Beüzemelésük egyszerű: be kell dugni a fali aljzatba vagy a hosszabbítóba, és egy gombnyomással csatlakoztatni az eszközt.

# Üzleti vezeték nélküli megoldások

Nagyobb szervezetek esetén WLAN-infrastruktúra kiépítése szükséges a vezeték nélküli kliensek további csatlakozási igényeinek kielégítésére.

**Megjegyzés**: az IEEE 802.11 a vezeték nélküli klienst állomásnak (station, STA) nevezi. Ebben a fejezetben a vezeték nélküli kliens bármely vezeték nélkül csatlakoztatható eszközt jelenti.

Az 1. ábrán látható kisvállalati hálózat alapja egy 802.3 Ethernet LAN. A kliensek (PC1 és PC2) hálózati kábellel csatlakoznak a kapcsolóhoz, mely a számukra a hálózat elérési pontja. Vegyük észre, hogy a vezeték nélküli AP is a kapcsolóhoz csatlakozik. Ebben a példában Cisco WAP4410N AP vagy WAP131 AP gondoskodik a vezeték nélküli kapcsolatról.

A vezeték nélküli kliensek hálózati adaptere deríti fel a közelben levő AP-ket SSID-jük alapján. Ezután a kliensek megpróbálnak kapcsolódni az AP-hez és hitelesíteni magukat, lásd 2. ábra. A sikeres hitelesítés után a vezeték nélküli kliensek hozzáférnek a hálózati erőforrásokhoz.

**Megjegyzés**: Egy kisvállalat vezeték nélküli kívánalmai jelentősen eltérnek egy nagy szervezetétől. A nagy vezeték nélküli rendszerekhez kiegészítő hardver szükséges, amely egyszerűsíti a kliensek telepítését és felügyeletét.

# Vezeték nélküli hozzáférési pontok

Az elérési pontok két kategóriába sorolhatók: önálló AP-k és vezérlő alapú AP-k (controller-based).

**Önálló AP-k**

Az önálló AP-k más eszközökkel nincsenek kapcsolatban, konfigurálásuk parancssorból vagy grafikus felületen történik. Használatuk akkor indokolt, ha a hálózatban csak néhány elérési pontra van szükség. Ha igény van rá, több AP vezérelhető együtt vezeték nélküli tartományi szolgáltatással (wireless domain services, WDS) a CiscoWorks Wireless LAN Solution Engine (WLSE) segítségével.

**Megjegyzés**: Egy otthoni forgalomirányító jó példa az önálló AP-re, mivel a teljes konfiguráció az eszközön található.

Az 1. ábrán egy kis hálózatban levő önálló AP látható. Ha újabb vezeték nélküli igények merülnek fel, további AP-kat kell telepíteni. Az AP-k egymástól függetlenül működnek, és mindegyik egyedi konfigurációt és felügyeletet igényel.

**Vezérlő alapú AP-k**

A vezérlő alapú AP-k szerverfüggő eszközök, melyek nem igényelnek kezdeti konfigurálást. A Cisco kétféle vezérlő alapú megoldást kínál. A vezérlő alapú AP-k akkor hasznosak, ha a hálózatban sok elérési pontra van szükség. Bármennyi AP kerül is a hálózatba, mindegyik konfigurálását és felügyeletét a WLAN-vezérlő végzi.

A 2. ábrán egy kis hálózatban levő vezérlő alapú AP látható. Vegyük észre, hogy az AP-k felügyeletéhez WLAN-vezérlő szükséges, melynek előnye, hogy sok AP irányítható vele.

**Megjegyzés**: Néhány AP típus képes mind önálló módban, mind vezérlő alapú módban működni.

**Kisméretű vezeték nélküli megoldások**

A kis vezeték nélküli igények kielégítésére a Cisco a következő önálló AP megoldásokat kínálja:

* **Cisco WAP4410N AP** - Ez az AP olyan kis szervezetek számára ideális, melyek két elérési pontot igényelnek csekély számú felhasználói csoport részére.
* **Cisco WAP121 és WAP321 AP-k** - Ezek az AP-k olyan szervezetek számára megfelelők, ahol több AP-t szeretnének egyszerűen kezelni.
* **Cisco AP541N AP** - Ez az AP olyan kis- és közepes szervezetek számára ideális, ahol klaszterbe, más néven fürtbe szervezett AP-kat szeretnének egyszerűen kezelni.

**Megjegyzés**: A legtöbb nagyvállalati szintű AP támogatja a PoE-t.

Az 1. ábrán a Cisco kisvállalati AP-k rövid leírása látható.

A 2. ábrán egy kisvállalati hálózati topológia látható WAP4410N AP-kkal. Minden AP-t egyedileg kell konfigurálni és felügyelni, ami több elérési pont esetén problémákat okozhat.

Emiatt a WAP121, a WAP321 és az AP541N AP-k klaszterbe szervezhetők vezérlő használata nélkül. A fürt biztosítja az egyetlen helyen történő felügyeletet, a rendszergazda az AP-kat egyetlen vezeték nélküli hálózatként láthatja, nem pedig önálló eszközökként. A fürtözés megkönnyíti a telepítést, konfigurálást és a felügyeletet a vezeték nélküli hálózat növekedése esetén is. Több AP telepíthető egyszerre és a konfiguráció egyidejűleg tölthető fel a klaszter összes eszközére. A vezeték nélküli hálózat egyetlen rendszerként felügyelhető, nem kell foglalkozni az AP-k egymásra hatásával, sem pedig külön-külön az AP-k beállításával.

Pontosabban a WAP121 és a WAP321 támogatja az egyetlen pontból történő beállítást (Single Point Setup, SPS), mely egyszerűsíti és gyorsítja a bevezetést (lásd 3. ábra). SPS-sel max. négy WAP121 illetve max. nyolc WAP321 telepíthető a vezeték nélküli LAN-ba, így kiterjeszthető a hálózat lefedettségi területe és további felhasználók csatlakoztathatók a vállalat változó igényei, növekedése szerint. Cisco AP541N AP-kből 10 kapcsolható össze és belőlük több klaszter is szervezhető.

Két AP fürtbe kapcsolható, ha teljesülnek az alábbi feltételek:

* A klaszter mód engedélyezve van az AP-n.
* A fürthöz csatlakozó AP-k klaszter neve azonos.
* Az AP-k azonos hálózati szegmensbe tartoznak.
* Az AP-k azonos vezeték nélküli szabványt használnak (pl.: 802.11n).

A következő linken elérhető egy online AP541N [emulátor](https://www.cisco.com/assets/sol/sb/AP541N_GUI/AP541N_1_9_2/Getting_Started.htm).

<https://www.cisco.com/assets/sol/sb/AP541N_GUI/AP541N_1_9_2/Getting_Started.htm>

**Nagyvállalati vezeték nélküli megoldások**

A nagy szervezetek fürtözött AP-kból álló nagy teljesítményű és méretezhető megoldást igényelnek. A Cisco számukra kínálja vezérlő alapú rendszereit, ilyenek például a Cisco Meraki Cloud Managed Architecture és a Cisco Unified Wireless Network Architecture.

**Megjegyzés**: További vezérlő alapú megoldások is léteznek, például a Flex módú vezérlők. Látogassunk el a [http://www.cisco.com](http://www.cisco.com/) oldalra további információkért.

**Cisco Meraki Cloud Managed Architecture**

A Cisco Meraki felhő architektúra egy felügyeleti megoldás, mely egyszerűbbé teszi a vezeték nélküli hálózat telepítését. Az AP-k a felhőben levő vezérlőről menedzselhetők (lásd 1. ábra). A felhőtechnológia központosított felügyeletet biztosít a helyi vezérlőberendezések és speciális szoftverek plusz költsége nélkül.

Ez a módszer csökkenti a költségeket és egyszerűbbé teszi a rendszert. A felhőben levő vezérlő tölti fel a Meraki AP-kre a szoftver frissítéseket, biztonsági beállításokat, hálózati paramétereket és az SSID adatait.

**Megjegyzés**: Csak felügyeleti adatok kerülnek be a Meraki felhőbe, a felhasználói adatforgalom nem halad át a Meraki adatközponton. Tehát, ha a felhő elérhetetlen, a hálózat akkor is rendben működik tovább. A felhasználók hitelesíthetik magukat, a tűzfal szabályok élnek, és a forgalom teljes sebességgel folyhat. Csak a felügyeleti funkciók szünetelnek, ilyenek például a jelentések és a konfigurációs segédprogramok.

A Cisco Meraki felhő alapú felügyeleti rendszerhez az alábbiak szükségesek:

* **Cisco MR Cloud Managed Wireless AP-k** - Többféle modell létezik a vezeték nélküli igények széles skálájának megfelelően.
* **Meraki Cloud Controller (MCC)** - A felhőben levő vezérlő biztosítja a Meraki WLAN-rendszer számára a felügyeletet, az optimalizálást és az ellenőrzést. Az MMC-t nem kell megvásárolni és telepíteni, mert egy felhő alapú szolgáltatás, amely folyamatosan végzi a hálózat karbantartását és jelentéseket készít annak állapotáról.
* **Web-alapú vezérlőpult (dashboard)** - A Meraki web-alapú vezérlőpultja biztosítja a távoli hozzáférést (konfigurálás és hibaelhárítás).

Kattintsunk a 2. ábra elemeire a Cisco Meraki rendszer további információiért.

**Nagyvállalati vezeték nélküli megoldások (folyt.)**

**Cisco Unified Wireless Network Architecture**

A Cisco egyesített vezeték nélküli hálózati architektúra egy split-MAC (szétosztott funkciók) rendszerű megoldás, mely WLAN-vezérlőt alkalmaz és menedzselhető WCS (Cisco Wireless Control System) segítségével is. A lecsupaszított elérési pontok (lightweight AP) LWAPP-n (Lightweight Access Control Point Protocol) kommunikálnak a WLAN-vezérlővel. A vezérlőben található az összes intelligencia, az AP csak egy "buta terminál", amely a csomagokat feldolgozza.

A Cisco egyesített vezeték nélküli hálózati architektúra eszközei:

* **Lightweight AP-k** - A Cisco Aironet 1600, 2600, 3600 vezeték nélküli elérési pontok megbízható és nagy teljesítményű hozzáférést nyújtanak a klienseknek.
* **Vezérlők kis- és közepes vállalkozásoknak** - Cisco 2500 Series Wireless Controller, Cisco Virtual Wireless Controller, Cisco Wireless Controller Module for Cisco ISR G2. Mindhárom eszköz képes kiszolgálni egy telephely vagy egy kisebb szervezet WLAN igényeit belépő szintű (entry-level) vezeték nélküli adatkapcsolattal.

Nagyobb teljesítményű WLAN-vezérlők is kaphatók, például a Cisco 5760 Wireless Controller vagy a Cisco 8500 Series Controller. Mindkettő költséghatékony módon felügyeli, teszi biztonságossá és optimalizálja a terjedelmes vezeték nélküli hálózatokat, amilyenek például a szolgáltatóknál vagy a nagy kiterjedésű telephelyeken találhatók.

Az 1. ábrán egy összegzés látható a lightweight AP-król.

A 2. ábra elemire kattintva a kis- és középvállalati vezérlők információi jelennek meg.

**Vezeték nélküli antennák**

A legtöbb üzleti célú AP-hez külső antennát kell használni, hogy teljes értékű eszközként működjön. A Cisco által a 802.11 AP-khez fejlesztett antennák illeszkednek a megkívánt telepítési feltételekhez, beleértve a fizikai szerkezetet, a hatótávolságot és a kivitelt.

A Cisco Aironet AP-khez csatlakoztatható:

* **Körsugárzó (omnidirectional) Wi-Fi antennák** - A Wi-Fi készülékeket gyárilag általában egyszerű dipólantennával szerelik fel, hasonlóan, mint a hordozható rádió adó-vevőket ("gumikacsa" dizájn). A körsugárzó 360 fokos szögben szórja a jeleket, ezért ideális nyílt légterű irodákban, előcsarnokokban, konferencia termekben és kültéren.
* **Irányított (directional) Wi-Fi antennák** - Az irányított antennák egy megadott irányba fókuszálják a rádiójeleket. Ez felerősíti az AP bejövő és kimenő jeleit abba az irányba, amerre az antenna mutat, így nagyobb jelerősséget eredményez, míg az összes többi irányba jelentősen lecsökkenti.
* **Yagi antennák** - Az irányított antennák speciális típusa nagy távolságú Wi-Fi-kapcsolatokhoz. Rendszerint kültéri elérési pontok hatótávolságának bizonyos irányba történő kiterjesztéséhez, vagy távoli épületek eléréséhez használják.

Az ábrán különféle beltéri és kültéri antennák láthatók.

Az IEEE 802.11n/ac/ad szabvány által használt MIMO-technológia megnöveli az elérhető sávszélességet. A MIMO több antennát (legfeljebb 4 ill. 8) alkalmaz, így nagyobb adatforgalomra képes, mint ami egy antennával lehetséges.

**Megjegyzés**: A vezeték nélküli forgalomirányítók sem egyformák. A belépő szintű 802.11n forgalomirányítók sebessége 150 Mb/s, egy WI-Fi adó-vevőjük és egy antennájuk van. A nagyobb sebességű 802.11n forgalomirányítók több adó-vevőt és több antennát használnak, így több adatcsatornát kezelhetnek egyszerre. Például, a két adó-vevővel és két antennával felszerelt 802.11n router legfeljebb 300 Mb/s sebességre képes, míg 450 és 600 Mb/s-hoz már négy adó-vevő és antenna kell.

**802.11 WLAN topológia módok**

A vezeték nélküli LAN-oknak többféle hálózati topológiájuk lehet. A 802.11 szabvány kétféle módot határoz meg:

* **Ad hoc mód** - Két berendezés vezeték nélkül közvetlenül kapcsolódik egymáshoz, hálózati eszköz (vezeték nélküli forgalomirányító vagy AP) segítsége nélkül. Ilyen például a Bluetooth és a Wi-Fi Direct.
* **Infrastruktúra mód** - A vezeték nélküli kliensek forgalomirányítón vagy AP-n keresztül kapcsolódnak egymáshoz, mint a WLAN-ban. Az AP-k pedig vezetéken csatlakoznak a hálózati infrastruktúrához, ami lehet például Ethernet.

Az 1. ábrán az ad hoc módra, a 2. ábrán az infrastruktúra módra láthatunk példát.

# Ad hoc mód

Ad hoc vezeték nélküli mód, amikor két kliens egyenrangú félként (peer-to-peer, P2P) kommunikál, AP vagy forgalomirányító használata nélkül. Egy vezeték nélküli munkaállomáson beállítható ad hoc mód, ami engedélyezi más eszközök becsatlakozását. A Bluetooth és a Wi-Fi Direct példák az ad hoc módra.

**Megjegyzés**Az IEEE 802.11 szabvány az ad hoc hálózatot független alap szolgáltatás készletnek (independent basic service set, IBSS) hívja.

Az ábrán az ad hoc mód összegzése látható.

Az ad hoc topológia másik változata, mikor egy mobil internet eléréssel rendelkező okostelefon vagy tablet személyes hotspotként üzemel (hotspot = vezeték nélküli internet-elérési pont). Ezt a tulajdonságot néha pányvázásnak (Tethering) nevezik. A hotspot beállítása egy okostelefonon általában azt jelenti, hogy az ideiglenesen Wi-Fi routerként üzemel. Ekkor más eszközök kapcsolódhatnak hozzá és hitelesíthetik magukat, hogy internet eléréshez jussanak. Az Apple iPhone esetében ennek neve Personal Hotspot, míg Android eszközökön Tethering vagy Portable Hotspot.

# Infrastruktúra mód

Az IEEE 802.11 architektúra elemei egymással együttműködve szolgálják ki a WLAN-klienseket. A szabvány kétféle infrastruktúra topológiát határoz meg: alap szolgáltatás-készlet (Basic Service Set, BSS) és kiterjesztett szolgáltatás-készlet (Extended Service Set, ESS).

**Basic Service Set**

A BSS egyetlen AP-ből és a hozzá kapcsolódott vezeték nélküli kliensekből áll. Az 1. ábrán két BSS látható. A körök jelölik azt a területet, amelyen belül a vezeték nélküli kliensek kommunikálni képesek. Ez a terület a cella (Basic Service Area, BSA). Ha a kliens kilép a cellából, többé nem képes kommunikálni a BSA más ügyfeleivel. A BSS topológiai építőelem, a BSA a valós lefedett terület (a két fogalmat gyakran vegyesen használják).

A BSS-t a hozzáférési pont (AP) MAC-címe egyedileg azonosítja, neve: Basic Service Set Identifier (BSSID). Tehát a BSSID a BSS formális neve és csak egyetlen egy AP-hez tartozhat.

**Extended Service Set**

Ha egyetlen BSS lefedettsége már nem elég, akkor több BSS-t kell egymáshoz csatlakoztatni közös elosztórendszeren (distribution system, DS) keresztül. A 2. ábrán egy ESS látható, mely két BBS-ből és az azokat összekapcsoló vezetékes elosztórendszerből áll. Az egyik cella (BSA) kliensei képesek kommunikálni a másik cella ügyfeleivel, feltéve ha mindketten ugyan abban az ESS-ben vannak. A mobil kliensek kapcsolatvesztés nélkül barangolhatnak a cellák között.

A téglalap jelöli azt a területet, amelyen belül az ESS tagjai kommunikálni tudnak egymással, a neve: Extended Service Area (ESA). Egy ESA általában több, egymást átfedő cellából épül fel.

Az ESS-t egy SSID azonosítja, a benne levő BSS-eket pedig a saját BSSID-jük. Biztonsági okokból további SSID-k rendelhetők az ESS-hez, így szétválaszthatók a különböző szintű hálózati hozzáférések.

**Megjegyzés**: A 802.11 szabvány az ad hoc módot IBSS-nek nevezi.

**Vezeték nélküli 802.11 keret**

Minden 2. rétegbeli (Layer2) keret fejrészből, adatrészből és ellenőrző összegből (FCS) áll (lásd 1. ábra). A 802.11 keretformátum hasonlít az Ethernet-hez, de több mezőt tartalmaz.

A 802.11 keretek a következő mezőkből épülnek fel (lásd 2. ábra):

* **Frame Control** - Keretvezérlés; azonosítja a vezeték nélküli keretet, almezői pedig a protokoll verziót, a kerettípust, a címtípust, energiaellátási és biztonsági beállításokat tartalmaznak.
* **Duration** - Időtartam; megadja, hogy mennyi idő telhet el a következő keret fogadásáig.
* **Address1** - Cím1; rendszerint a cél (fogadó) vezeték nélküli eszköz vagy az AP MAC-címe.
* **Address2** - Cím2; rendszerint a forrás (küldő) vezeték nélküli eszköz vagy AP MAC-címe.
* **Address3** - Cím3; egy cél MAC-címet tartalmazhat, például a forgalomirányító interfészét (default gateway), amelyhez az AP csatlakozik.
* **Sequence Control** - Sorrend vezérlés; a Sequence Number és a Fragment Number almezőkből áll. A Sequence Number a keret sorszámát tartalmazza, a Fragment Number pedig a töredék keret sorszámát jelenti az eredeti kereten belül.
* **Address4** - Cím4; általában üres, mert csak ad hoc módban használják.
* **Payload** - Hasznos teher; az átvitelre kerülő adatokat tartalmazza.
* **FCS** - Keretellenőrző összeg (Frame Check Sequence); a 2. rétegbeli hibák jelzésére szolgál.

A 3. ábrán egy Whireshark által elfogott WLAN beacon frame (jelzőkeret) látható. Figyeljük meg, hogy a Frame Control mező almezői is látszódnak.

**Megjegyzés**: A címmezők tartalma változhat a Frame Control mező beállításaitól függően.

**Frame Control mező**

A Frame Control mező több almezőből épül fel (lásd 1. ábra).

A Frame Control mező almezői a következők:

* **Protocol Version** - Protokoll verzió; a 802.11 aktuálisan használt verzióját tartalmazza. A fogadó állomások ebből az értékből tudják meghatározni, hogy az érkező keret támogatott-e általuk.
* **Frame Type** és **Frame Subtype** - Kerettípus; meghatározza a keret feladatát. Egy vezeték nélküli keret lehet vezérlőkeret (control frame), adatkeret (data frame) vagy felügyeleti keret (management frame). Minden kerettípushoz megfelelő altípusú mezők tartoznak, melyek a kerethez illeszkedő sajátos szerepet látnak el.
* **ToDS** és **FromDS** - Jelzi, ha a keret az elosztórendszerből származik vagy oda tart (distribution system, DS), csak AP-hoz csatlakozott kliensek esetén használatos.
* **More Fragments** - Azt jelzi, hogy a keret további töredékei (darabjai) fognak még érkezni, ezek lehetnek adat vagy felügyeleti típusúak is.
* **Retry** - Jelzi, hogy ez egy újraküldött keret, lehet adat vagy felügyeleti típusú is.
* **Power Management** - Jelzi, hogy a küldő eszköz aktív vagy energiatakarékos (alvó) módban van.
* **More Data** - Jelzi az energiatakarékos módban levő eszköznek, hogy az AP további kereteket fog küldeni. Másik szerepe, hogy jelzi az AP-nak a további broadcast/multicast keretek érkezését.
* **Security** - Jelzi, hogy a keret titkosított és hitelesítéssel védett. Beállítható minden adat- és felügyeleti keretre, amelyeknek az altípusa autentikációra van állítva.
* **Reserved** - Azt jelezheti, hogy a fogadott adatkereteket sorrendben kell feldolgozni.

A 2. ábrán egy Whireshark által elfogott WLAN beacon frame (jelzőkeret) látható. Emlékezzünk, hogy a Frame Type és a Frame Subtype mezők azonosítják, hogy a keret felügyeleti, vezérlő vagy adatkeret. Ebben a példában a Frame Type '0x0' értéke jelzi, hogy felügyeleti keretről van szó. Az altípus '8' értéke a beacon keretet jelenti. A kerettípust tehát a '0x08' azonosítja.

**Vezeték nélküli kerettípusok**

**Megjegyzés**A Frame Type és a Frame Subtype mezők azonosítják, hogy a vezeték nélküli átvitel milyen típusú. Amint az ábrán is látható, a keret háromféle lehet:

* **Management Frame** - Felügyeleti keret; a kommunikáció kezelésére használják, például AP keresés, kapcsolódás és hitelesítés.
* **Control Frame** - Vezérlőkeret; feladata, hogy elősegítse a vezeték nélküli kliensek között az adatkeretek cseréjét.
* **Data Frame** - Adatkeret; feladata a hasznos információk szállítása, ilyenek például a weboldalak és az állományok.

# Management keretek

A felügyeleti keretetek kizárólagos feladata az AP keresés, kapcsolódás és hitelesítés.

Az 1. ábrán a gyakori felügyeleti kerettípusok láthatók, úgymint:

* **Association request frame (0x00)** - Kapcsolódás kezdeményezés; a vezeték nélküli kliens küldi, hatására az AP erőforrásokat foglal le és egyeztet. A keretben a vezeték nélküli kapcsolat paraméterei vannak, többek közt a támogatott átviteli sebesség és társítani kívánt hálózat SSID-je. Ha az AP elfogadja a kérést, akkor létrehoz egy csatlakozási azonosítót és memóriát foglal a kliensnek.
* **Association response frame (0x01)** - Kapcsolódás válasz; az AP küldi a kliensnek, tartalma elfogadás vagy elutasítás egy kapcsolódási kérésre. Ha a válasz elfogadás, a keret tartalma a kapcsolati azonosító és a támogatott sebesség.
* **Reassociation request frame (0x02)** Újrakapcsolódási kérés; a kliens küldi, amikor kikerül a társított AP hatóköréből és egy erősebb jellel rendelkező AP-t talál. Az új AP összehangolja azokat a küldött információkat, amelyek esetleg a régi AP pufferében maradtak.
* **Reassociation response frame (0x03)** - Újrakapcsolódás válasz; az AP küldi, tartalma elfogadás vagy elutasítás egy újrakapcsolódási kérésre. A keret tartalma a társításhoz szükséges kapcsolati azonosító és a támogatott sebesség.
* **Probe request frame (0x04)** - Szondakérés; a vezeték nélküli kliens küldi, amikor információt kér egy másik klienstől.
* **Probe response frame (0x05)** - Szondaválasz; az AP válasza egy szondakérésre, például információt tartalmaz a támogatott átviteli sebességről.
* **Beacon frame (0x08)** - Jelzőtűzkeret; az AP küldi periodikusan, hirdeti saját jelenlétét és közzéteszi az SSID-t, valamint egyéb konfigurált paramétereit.
* **Disassociation frame (0x0A)** - Szétkapcsolás; az eszköz küldi, hogy befejezzen egy kapcsolatot. Hatására az AP felszabadíthatja a lefoglalt memóriát és törölheti az eszközt a társítási táblából.
* **Authentication frame (0x0B)** Hitelesítés; az eszköz küldi az AP-nek, tartalma a saját azonosítója.
* **Deauthentication frame (0x0C)** - Hitelesítés törlés; egy vezeték nélküli kliens küldi egy másik ügyfélnek a kapcsolat megszakítása céljából.

Egyedül a beacon kereteket szórja rendszeresen az AP, minden más felügyeleti keretet (probing, authentication, association) csak a kapcsolatfelvétel (vagy újrakapcsolódás) esetén.

A 2. ábrán egy Whireshark által elfogott felügyeleti keret látható. A mezőértékek a keret rendeltetését mutatják.

**Megjegyzés**: A példában Wireshark által gyűjtött adatokat láthatunk, ehhez azonban a WLAN-forgalom elfogásához szükséges beállítás kell. Ez operációs rendszerenként változó és speciális vezeték nélküli hálózati kártyát igényelhet.

# CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

A közegelérés az a módszer, amellyel az eszköz meghatározza, hogyan és mikor fér hozzá az átviteli közeghez, ha adatokat kell továbbítani a hálózaton. Az IEEE 802.11 WLAN-ok a CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, vivőérzékeléses többszörös hozzáférés ütközés elkerüléssel) MAC-protokollt használják. Bár az elnevezés hasonlít az Ethernet CSMA/CD-re, a működési elv azonban egészen más.

A Wi-Fi rendszerek fél-duplex, megosztott közegben működnek, ezért a vezeték nélküli kliensek ugyanazt a rádiócsatornát használhatják adásra és vételre egyaránt. Ez problémát okoz, mert adás közben a kliens nem hall semmit, így az ütközést sem tudja érzékelni. Megoldásként az IEEE kifejlesztett egy kiegészítő ütközés-elkerülési módszert, melyet DCF-nek (Distributed Coordination Function) hívnak. DCF használata esetén a kliens csak akkor kezdeményez adást, ha a csatorna szabad. Minden átvitel nyugtázott; ha kliens nem kap visszaigazolást, feltételezi, hogy ütközés történt, és újra próbálkozik egy véletlen időtartam után.

A vezeték nélküli kliensek és az AP-k RTS és CTS vezérlőkereteket használnak a tényleges adatforgalom elősegítéséhez.

Mielőtt a vezeték nélküli kliens adatküldésbe kezdene, először megvizsgálja a közeget, hogy más eszközök adásban vannak-e (lásd 1. ábra). Ha nincsenek, akkor egy RTS-keretet küld az AP-nak. Ez a keret egy kizárólagos hozzáférési kérelem az RF-közeghez egy meghatározott időtartamra. Az AP fogadja a keretet és ha az RF rendelkezésre áll, megadja a hozzáférést a kliensnek a kért időtartamra egy CTS-keret küldésével. Az összes többi vezeték nélküli eszköz is észleli a CTS-keretet, amely lefoglalta a közeget az adó számára.

A CTS vezérlőkeret tartalmazza azt az időintervallumot, amíg az állomás átvitelt végezhet. A többi kliens szünetelteti az adást legalább a megadott időtartamra.

A 2. ábrán a CSMA/CA folyamatábrája látható.

**A vezeték nélküli kliens és az AP társítása**

A vezeték nélküli klienseknek csatlakozniuk kell egy AP-hoz vagy egy vezeték nélküli forgalomirányítóhoz, hogy kommunikálni tudjanak a hálózaton. A 802.11 folyamat fontos része a WLAN felderítése, majd a hozzákapcsolódás.

A vezeték nélküli kliensek által használt felügyeleti keretek végzik a következő 3 lépéses műveletsort:

* Új AP felderítése.
* Hitelesítés az AP-n.
* Társulás az AP-vel.

# Csatlakozási paraméterek

A vezeték nélküli kliens és az AP társításához egyeztetni kell bizonyos paramétereket, melyeket mindkét eszközön konfigurálni kell. A leggyakoribb vezeték nélküli paraméterek:

* **Network mode (hálózati mód)** - A 802.11 WLAN-szabványt jelöli. Az AP-k és a vezeték nélküli forgalomirányítók működhetnek Mixed (vegyes) módban is, azaz egyidejűleg használhatnak többféle szabványt (lásd 1. ábra).
* **SSID** - Az SSID egy egyedi azonosító, mely a vezeték nélküli kliens számára a közelben levő hálózatok megkülönböztetésére szolgál. Ha az SSID-szórás engedélyezett, akkor az azonosító megjelenik az elérhető vezeték nélküli hálózatok listáján. A hálózati konfigurációtól függően több AP is használhatja ugyanazt az SSID-t. Az azonosító rendszerint 2-32 karakter hosszú. Az 1. ábrán az SSID értéke **Home-Net** és a szórása engedélyezve van.
* **Csatorna beállítások** - Azonosítja a vezeték nélküli adattovábbításhoz használt frekvenciasávokat. A vezeték nélküli forgalomirányítók és az AP-k képesek automatikus csatorna használatra, vagy beállíthatók manuálisan is más AP-k zavaró hatásának kiküszöbölése érdekében (interferencia). Az 1. ábrán kézzel beállították a 6-os csatornát, ami a 2,437 GHz frekvenciát jelenti.
* **Security mode (biztonság)** - A biztonsági beállításokat jelenti, például WEP, WPA és WPA2. Mindig a legmagasabb elérhető biztonsági szintet válasszuk! Otthoni vagy kisvállalati környezetben ez a **WPA2 Personal**mód (lásd 2. ábra).
* **Encryption (titkosítás)** - A WPA2-höz titkosítást is választani kell, használjuk az AES-t, amennyiben lehetséges.
* **Password (jelszó)** - A klienstől várt jelszó az AP-n történő hitelesítés során, időnként biztonsági kulcsnak (security key) is nevezik. Meggátolja a behatolók és a kéretlen felhasználók csatlakozását a hálózathoz.

**AP-k felkutatása**

A csatlakozás érdekében a vezeték nélküli eszközöknek fel kell kutatniuk az AP-t vagy a forgalomirányítót, melyhez egy pásztázási (probe) folyamatot alkalmaznak. Ez lehet:

* **Passive mode (passzív mód)** - Az AP nyíltan hirdeti szolgáltatásait szórással periodikusan küldött beacon (jelzőtűz) keretekkel, melyek tartalmazzák az SSID-t, a támogatott szabványokat és a biztonsági beállításokat. A beacon keretek elsődleges feladata a vezeték nélküli kliensek értesítése arról, hogy milyen hálózatok és AP-k vannak az adott területen, amelyekhez csatlakozni lehet.
* **Active mode (aktív mód)** - A vezeték nélküli klienseknek ismerniük kell az SSID-t. Majd el kell indítaniuk a csatlakozási folyamatot különböző csatornákon kiküldött szondakérési (probe request) keretekkel, melyek tartalmazzák az SSID-t és a támogatott szabványokat. Aktív mód akkor szükséges, ha az AP-n vagy a forgalomirányítón tiltott az SSID-szórás (beacon frames).

Az 1. ábra bemutatja, hogyan működik a passzív mód az AP által időközönként szórt beacon keretekkel.

A 2. ábra bemutatja, hogyan működik az aktív mód a kliens által küldött szondakéréssel (probe request) egy adott SSID felé. Az SSID-t birtokló AP szondaválasz (probe response) kerettel felel.

A vezeték nélküli kliens küldhet szondakérést SSID nélkül is a közelben található WLAN-ok felderítésére. Az SSID-szórással konfigurált AP-k válaszolnak és elküldik azonosítójukat. Ahol az SSID-szórás tiltott, az AP nem válaszol a kérésre.

**Authentication (hitelesítés)**

A 802.11 szabványba eredetileg kétféle hitelesítési mechanizmust építettek:

* **Open authentication (nyílt)** - Lényegében itt NINCS hitelesítés, a kliens azt mondja - "hitelesíts engem", mire az AP válaszol - "igen". A nyílt hitelesítés bármely vezeték nélküli kliens számára biztosítja a csatlakozást, csak olyan esetekben alkalmazható, ha a biztonságnak nincs jelentősége.
* **Shared key authentication (megosztott kulcs)** - A módszer alapja egy előre megosztott kulcs (jelszó) a kliens és az AP között.

Az 1. ábrán a hitelesítési folyamat látható. A legtöbb osztott kulcsú hitelesítés esetében a következőképpen zajlik:

1. A vezeték nélküli kliens egy hitelesítő keretet küld az AP-nak.

2. Az AP egy "kihívás" szöveggel (challenge text) válaszol.

3. A kliens titkosítja a kapott szöveget a megosztott kulccsal, és visszaküldi az AP-nak.

4. Az AP visszafejti a titkosított szöveget a megosztott kulccsal.

5. Ha a visszafejtett szöveg megegyezik az eredetileg kiküldöttel, az AP hitelesíti a klienst. Ha a két szöveg nem egyezik meg, a kliens elutasításra kerül és a vezeték nélküli hozzáférés nem jön létre.

A sikeres hitelesítés után az AP a társítási szakaszba lép (association). A csatlakozási folyamat véglegesíti a beállításokat és kiépíti az adatkapcsolatot a vezeték nélküli kliens és az AP között (2. ábra).

A folyamat lépései:

* A kliens küld egy Association Request (csatlakozás kérés) keretet saját MAC-címével.
* Az AP egy Associate Response kerettel válaszol, benne a BSSID-vel, ami az AP MAC-címe.
* Az AP hozzárendel egy logikai portot a klienshez, ez lesz a csatlakozási azonosító (association identifier, AID). Az AID egyenértékű egy kapcsoló porttal, lehetővé teszi a kapcsoló számára a vezeték nélküli klienseknek küldött keretek követését.

Az AP-hoz való társulás után elindulhat a kliens forgalom.

**Frekvenciacsatornák telítettsége**

A vezeték nélküli LAN-eszközök adó- és vevőáramkörei megadott frekvenciákra vannak hangolva. A gyakorlatban a frekvenciákat tartományokra osztják, majd tovább darabolják, a kapott egységet pedig csatornának nevezik.

Ha egy adott csatorna iránt túl nagy az igény, a csatorna túltelítetté válhat. A vezeték nélküli átviteli közeg telítettsége a kommunikáció minőségének romlásához vezet. Az évek során számos módszer jelent meg a vezeték nélküli kommunikáció javítására és a telítettség csillapítására. Az alábbi technológiák a csatornák hatékonyabb kihasználásával segítik a telítettség csökkentését:

* **DSSS (Direct-sequence spread spectrum, közvetlen sorrendű szórt spektrum)** - A DSSS egy spektrum-kiterjesztéses modulációs technológia. Ez annyit jelent, hogy a jelet egy szélesebb frekvenciatartományban sugározzák, csökkentve ezzel az interferenciára való érzékenységet. A jelet megszorozzák egy "ügyes zajnak" vagy "cseles zajnak" nevezett jellel (spreading code). Mivel a vevő is ismeri a kódot, matematikai módszerrel el tudja távolítani és vissza tudja állítani az eredeti jelet. Következésképpen redundancia keletkezik az átvitt jelekben, ami csökkenti a minőségromlást a vezeték nélküli közegben. A DSSS-t a 802.11b szabvány használja. Megtalálható még a 900 MHz, 2,4 GHZ, 5,8 GHz frekvenciát használó hordozható telefonokban, a CDMA- és GPS-hálózatokban (lásd 1. ábra).
* **FHSS (Frequency-hopping spread spectrum, frekvenciaugrásos szórt spektrum)** - Az FHSS is spektrum-kiterjesztéses modulációs technológia. Hasonlít a DSSS-hez, de az átvitelhez használt vivőjelet gyorsan kapcsolgatja sok frekvenciasáv között. FHSS alkalmazásakor az adó és a vevő szinkronban kell működjön, hogy tudják melyik csatornára kell ugrani. A frekvenciaugrásos módszer hatékonyabb csatornahasználatot eredményez, csökkentve ezzel túlterhelésüket. A hordozható rádió adó-vevők és a 900 MHz-es zsinór nélküli telefonok FHSS-t, a Bluetooh pedig annak egy változatát használja. Az eredeti 802.11 szabvány tartalmazza az FHSS-t (lásd 2. ábra).
* **OFDM (Orthogonal frequency-division multiplexing, ortogonális frekvenciaosztásos multiplexelés)** - Az OFDM esetében a csatornát több egymás melletti alcsatornára osztják, melyeket egyszerre használnak. A szomszédos alcsatornák jelei ortogonálisak (egymásra merőlegesek), így átfedés esetén sem jön létre közöttük interferencia. Ennek eredményeképpen az OFDM-rendszer képes a rendelkezésre álló frekvenciatartomány maximális kihasználására. A több párhuzamos csatorna alkalmazása azzal a járulékos előnnyel is jár, hogy egy keskenysávú zavar nem teszi lehetetlenné a kommunikációt, csak csökkenti az összesített sebességet. Az 802.11a/g/n/ac rendszerek OFDM-t használnak (lásd 3. ábra).

# Csatorna választás

Az IEEE 802.11/b/g/n szabványok mindegyike a rádiótartomány mikrohullámú frekvenciáin működik. Az IEEE 802.11b/g/n a 2,4 - 2,5 GHz-en, míg a 802.11a/n/ac a szigorúbban szabályozott 5 GHz-en. Az 1. ábrán a 802.11 szabványok működési tartományai láthatók. A teljes spektrum csatornákra van osztva, melyeket a középfrekvencia és a sávszélesség határoz meg.

A 2,4 GHz-es sáv is több csatornára van osztva, melyek 5 MHz eltolással követik egymást és sávszélességük 22 MHz. A 802.11b szabvány szerint 13 csatorna van (Európa). A 22 MHz sávszélesség 5 MHz-es eltolásokkal átfedést okoz a csatornák között (lásd 2. ábra).

**Megjegyzés**: Észak-Amerikában 11 csatorna van a 802.11b szabvány szerint.

Interferencia akkor alakul ki, ha egy nemkívánatos jel átfedésbe kerül a csatorna jelével és eltorzítja azt. Az interferencia elkerülhető átfedésben nem levő csatornák használatával, ezek a 802.11b esetében az 1, 6 és 11-es csatornák (lásd 3. ábra).

A több AP-t használó WLAN-ok esetében bevált gyakorlat a nem-átlapolódó csatornák használata. Ha három szomszédos AP van, használjuk az 1, 6 és 11 csatornákat, ha csak kettő, akkor használhatjuk bármelyik egymástól 5 csatornára levőket, pl.: 5 és 10. A legtöbb AP automatikusan is tud csatornát választani, a szomszédos eszközök csatornahasználatától függően. Néhány eszköz folyamatosan figyeli a rádiótartományt és dinamikusan igazítja a csatornabeállítást a környezet változásának megfelelően.

A 802.11n szabványú WLAN-ok a szélesebb, kevésbé zsúfolt 5 MHz-es tartományban is működnek, ezzel is csökkentve a "véletlen szolgáltatás-megtagadás (DoS)" esélyét. Például a 802.11n szabvány, amely OFDM-t használ, négy nem-átlapolódó csatornát támogat (lásd 4. ábra).

A 802.11n ezen kívül képes a csatornák kötegelésére, azaz összefog két 20 MHz-es csatornát egy 40 MHz szélességűvé (lásd 5. ábra). A csatornák összekötése növeli a hasznos átviteli sebességet azáltal, hogy két csatornán egyidejűleg szállít adatokat.

A legmodernebb AP-k automatikus csatorna hangolással kerülik el az interferenciát.

**Megjegyzés**: Az IEEE 802.11ac is OFDM-t használ, a csatornák szélessége 80, 160 illetve 80+80.

**WLAN bevezetés tervezése**

Költséghatékony és magas szintű szolgáltatást nyújtó WLAN megvalósításához gondos tervezés szükséges, legyen szó akár egyszerű telepítésről, akár bonyolult konstrukcióról. Mindenképpen szükséges egy jól dokumentált terv, mielőtt a hálózat megépítése elkezdődne.

Egy WLAN által kezelhető felhasználók számát nem egyszerű kiszámolni, mert több tényező befolyásolja. Számít a földrajzi elhelyezkedés, beleértve a tereptárgyakat és mesterséges szerkezeteket, az elvárt sávszélesség, a nem-átlapolódó csatornák használata több AP esetén, valamint az adóteljesítmény.

Tekintsük át az 1. ábrán látható alaprajzot! Az AP-k helyének tervezésekor nem elegendő csak a hatókört jelző körök elhelyezése a rajzon, más feltételeket is figyelembe kell venni:

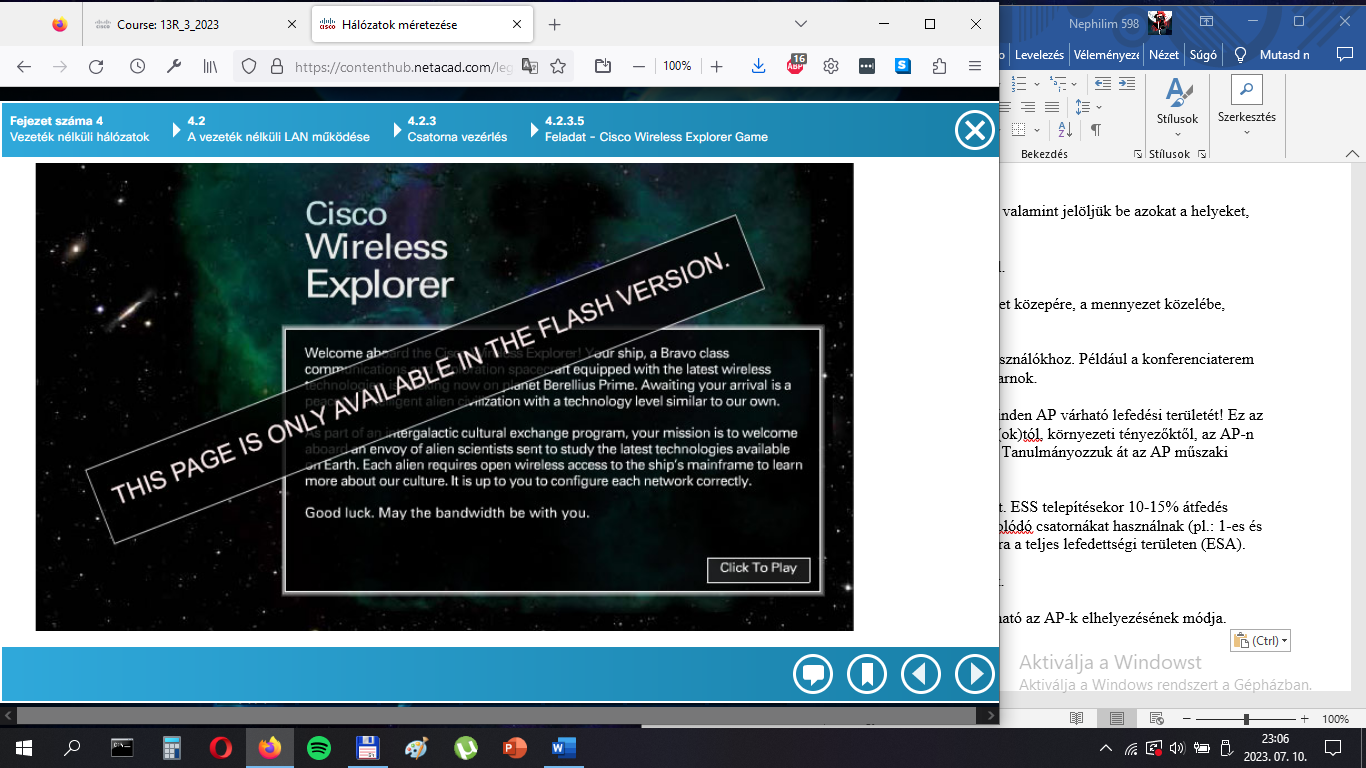
* Rajzoljuk be a meglévő vezetékes hálózatot, valamint jelöljük be azokat a helyeket, ahová nem telepíthetjük az AP-kat.
* Az AP-kat hozzáférhető módon helyezzük el.
* Ha lehetséges, szereljük az AP-kat a célterület közepére, a mennyezet közelébe, függőleges pozícióban.
* Helyezzük az AP-kat minél közelebb a felhasználókhoz. Például a konferenciaterem alkalmasabb hely az AP-knak, mint az előcsarnok.

A fenti elvek figyelembevételével becsüljük meg minden AP várható lefedési területét! Ez az érték függhet még az alkalmazott WLAN-szabvány(ok)tól, környezeti tényezőktől, az AP-n konfigurált adóteljesítménytől és még sok egyébtől. Tanulmányozzuk át az AP műszaki leírását is a lefedettség kiszámításához.

A cella (BSA) jelöli a csatorna által lefedett területet. ESS telepítésekor 10-15% átfedés szükséges az elemi cellák között, melyek nem átlapolódó csatornákat használnak (pl.: 1-es és 6-os). Így közös SSID-vel lehetőség van barangolásra a teljes lefedettségi területen (ESA).

A 2. ábrán a cellák (BSA) közötti átfedések láthatók.

Fontos még a helyszíni szemle, melyen megvizsgálható az AP-k elhelyezésének módja.



<https://serious.gameclassification.com/EN/games/43566-Wireless-Explorer/index.html>

**Vezeték nélküli biztonság megvalósítása**

Egy vezeték nélküli hálózat biztonságossá tétele bonyolultabb feladat, mint egy vezetékesé. A felhasználók és a hálózatot felügyelők számára egyaránt elsődleges cél legyen a biztonság.

A WLAN nyitott bárki számára az AP hatókörén belül, aki rendelkezik a csatlakozáshoz szükséges engedélyekkel. Ha a támadó rendelkezik vezeték nélküli hálózati kártyával és a védelem feltörésére vonatkozó ismeretekkel, akkor nem kell fizikailag behatolnia a munkahelyre, hogy WLAN-hozzáféréshez jusson.

A biztonsági megfontolások még fontosabbak vállalati hálózatok esetében, mivel az üzleti információk védelme megélhetési kérdés. Az adatbiztonság megsértésének jelentős következményei lehetnek, főképp ha a vállalat az ügyfél pénzügyeit is kezeli. A vezeték nélküliség egyre elterjedtebbek a nagyvállalatok körében is, de sok esetben kényelmi szerepből a teljes hálózatuk kritikus részévé vált. A WLAN-ok korábban is a behatolók célpontjai voltak, de népszerűségük növekedésével most elsődleges támadási felületté váltak.

A támadások származhatnak kívülről, munkavállalóktól rosszhiszeműségből vagy akaratlanul. A vezeték nélküli hálózatok különösen fogékonyak a következő fenyegetésekre:

* Vezeték nélküli behatolók
* Hamis AP-k
* Adateltérítés
* DoS támadások

Kattintsunk az ábrán az egyes típusok részletes információinak megtekintéséhez!

**Megjegyzés**: Más fenyegetések, mint például az AP MAC spoofing, a kódtörés, és a különféle infrastruktúra elleni támadások kívül esnek a fejezet hatókörén.

# DoS támadás felügyeleti keretekkel

Bár ritka, de egy rosszakaratú felhasználó szándékosan is elő tud idézni DoS-támadást olyan eszközzel, amely RF-zajt kelt és véletlen interferenciát okoz. Ez olyan, mintha a felügyeleti kereteket manipulálná, elfogyasztva az AP erőforrásait és foglattá téve a csatornát, így akadályozva a jogosult felhasználók adatforgalmát.

A felügyeleti keretek manipulálásával többféle típusú DoS-támadás indítható. A két leggyakoribb a következő:

* **Spoofed disconnect (átveréses szétkapcsolás) támadás** - Akkor történik, ha a támadó sorozatos "szétkapcsolás" (disassociate) parancsokat küld a cella vezeték nélküli klienseinek. A parancs hatására az összes ügyfél bontja a kapcsolatot. Ezután a kliensek megpróbálnak újrakapcsolódni, ami forgalmi csúcsterhelést okoz (burst). A támadó folytatja a disassociate keretek küldést és folyamat kezdődik elölről.
* **CTS flood (elárasztás)** - Akkor következik be, ha a támadó kihasználva a CSMA/CA kapcsolódási módot, lefoglalja a teljes sávszélességet és megakadályozza a többi vezeték nélküli kliens csatlakozását az AP-hoz. Ezt úgy éri el, hogy folyamatosan CTS (Clear to Send) kereteket küld egy nem létező állomásnak. A közegeben levő többi vezeték nélküli kliens megkapja a CTS-üzenetet, látja, hogy nem neki szól, ezért visszatartja a saját forgalmát mindaddig, míg a támadó be nem fejezi a CTS-keretek küldését.

Az 1.ábrán egy vezeték nélküli kliens és egy AP látható CSMA/CA szerinti szabályos közegeléréssel.

A 2. ábrán a CTS-elárasztás látható, amelyet a támadó küld egy hamis vezeték nélküli kliensnek. Az összes többi kliensnek várakozni kell a CTS-keretben meghatározott ideig. Ha a támadó folytatja a CTS-keretek küldését, a többiek határozatlan ideig várakozhatnak. A behatoló mostantól teljes felügyelet alatt tartja a közeget.

**Megjegyzés**: Ez csak egyetlen példa a felügyeleti kerettel végrehajtott támadásra, de sok más fajta is létezik.

Az ilyen típusú támadások elkerülésére a Cisco változatos megoldásokat fejlesztett ki, például a felügyeleti keret védelmet (Cisco Management Frame Protection, MFP), amely proaktív módon véd a keret és eszköz alapú átverésés támadások ellen is. A Cisco Adaptive Wireless IPS kiegészíti ezt egy korai érzékelő rendszerrel, mely a támadások mintázata alapján ismeri fel a behatolási kísérletet.

Az IEEE 802.11 két szabványt tartalmaz a vezeték nélküli biztonságra vonatkozóan. Az 802.11i szabvány, mely a Cisco MFP-n alapul, biztonsági elveket határoz meg a vezeték nélküli hálózatok számára, a 802.11w pedig a felügyeleti keretek védelmét szabályozza.

**Rogue Access Points (csaló AP-k)**

A csaló (rouge) AP olyan elérési pont vagy vezeték nélküli forgalomirányító, amely:

* Engedély nélkül és a vállalati házirendet megsértve csatlakozik a szervezet vezetékes hálózatához. Például az épületben jogosultan tartózkodó személy beüzemelhet egy olcsó WiFi-routert (rossz szándékkal vagy tudatlanságból), mely alkalmas a védett hálózat elérésére.
* A támadó által csatlakoztatott vagy engedélyezett eszköz kliens adatokat gyűjt, például a MAC-címeket (vezetékest és vezeték nélkülit egyaránt), vagy adatcsomagokat fog el hálózati erőforrások eléréséhez és man-in-the-middle támadáshoz.

Egy másik tényező, hogy egyszerűen lehet személyi hotspot-ot készíteni. Például a biztonságos hálózat egyik felhasználója a hitelesített Windows-munkaállomáson engedélyezi a WiFi AP-t. Ezáltal megkerüli a biztonsági óvintézkedéseket, hiszen jogosulatlan eszközöknek nyújt hálózati elérést a megosztáson keresztül.

A csaló AP-k telepítésének megakadályozására olyan szoftvert kell használni, amely folyamatosan figyeli a rádiótartományt és kiszűri a jogosulatlan elérési pontokat. Például ilyen az ábrán látható Cisco Prime Infrastructure hálózatfelügyeleti szoftver, amely éppen azonosított egy behatolót a hamisított MAC-címe alapján.

**Megjegyzés**: A Cisco Prime együttműködik más felügyeleti programokkal, központilag tárolja és jeleníti meg a hálózati információkat. Általában nagy szervezeteknél alkalmazzák.

# Man-in-the-Middle (közbeékelődéses) támadás

Az egyik legbonyolultabb rosszindulatú támadási módszer a közbeékelődéses (man-in-the-middle, MITM) támadás, mely többféle módon is végrehajtható.

Egyik népszerű vezeték nélküli MITM-támadás az "evil twin AP" (gonosz iker) nevet viseli; ilyenkor a támadó beüzemel egy csaló AP-t és ugyan azt az SSID-t állítja be rajta, mint ami a valódi AP-n van. A szabad WiFi-használatot nyújtó helyek, például a repülőterek, kávézók és éttermek, melegágyai az ilyen támadásoknak a nyílt hitelesítés miatt.

A felcsatlakozó vezeték nélküli kliens két működő AP-t lát, valószínűleg a közelebb levő csaló AP-val társul, mert annak erősebbek a jelei. A felhasználói forgalom így először a csaló AP-ra kerül, amely begyűjti az adatokat és továbbítja a valódi AP-nak. A visszajövő forgalom a valódi AP-ról a csaló AP-ra kerül, az befogja, majd továbbítja a gyanútlan állomásnak. A támadó megszerezheti a felhasználó jelszavát, személyes információit, hálózati hozzáférését és megrongálhatja rendszerét.

Például, a rosszindulatú felhasználó a “Bob’s Latte” kávézóban van és várja a begyűjtött adatokat a gyanútlan vezeték nélküli kliensektől (lásd 1. ábra). A támadó egy szoftvert használ, amely egy "gonosz iker" AP-t hoz létre azonos SSID-vel és csatornával, mint a valódi AP-n.

A felhasználó látja mindkét vezeték nélküli lehetőséget, de a csaló AP-t választja és ahhoz csatlakozik (lásd 2. ábra). A támadó begyűjti a felhasználói adatokat és továbbítja a valódi AP-nak, amely pedig a visszafelé tartó forgalmat a csaló AP-hoz irányítja. Az iker AP elfogja a visszatérő adatokat, majd továbbítja azokat a gyanútlan felhasználóhoz.

Az MITM-támadások meghiúsítása függ a WLAN-infrastruktúra kifinomultságától és a hálózatfigyelés éberségétől. A folyamat a WLAN jogosult eszközeinek azonosításával kezdődik, ehhez a felhasználóknak hitelesíteni kell magukat. Miután a valódi eszközök ismertek, elindulhat a hálózatfigyelés a szokatlan berendezések és forgalom kiszűrésére.

A legkorszerűbb eszközöket használó nagyvállalati WLAN-ok rendelkeznek olyan adminisztrátori segédeszközökkel, melyek behatolásvédelmi rendszerként működnek (intrusion prevention system, IPS). Figyelik a csaló AP-kat és ad-hoc hálózatokat, erőforrás-gazdálkodást folytatnak a rádiótartományban, amely elemzi az RF-sávot és az AP-k terhelését. Egy AP szokásosnál nagyobb kihasználtsága figyelmezteti a rendszergazdát, hogy valószínűleg jogosulatlan forgalmazás történik.

**A vezeték nélküli biztonság áttekintése**

A biztonság mindig kulcskérdés volt a WiFi-vel kapcsolatban a hálózat határának áthelyeződése miatt. A vezeték nélküli jelek áthatolnak a szilárd anyagokon, például a mennyezeten, a padlón, a falakon, elhagyják a lakás vagy az iroda területét. Szigorú helyi szabályok nélkül WLAN-t telepíteni olyan, mintha mindenhová Ethernet csatlakozókat szerelnénk, még kívülre is.

A vezeték nélküli behatolók okozta fenyegetés távol tartására és az adatok védelmére két biztonsági szolgáltatás használható:

* **SSID-rejtés (cloaking)** - Az AP-k és a vezeték nélküli forgalomirányítók lehetővé teszik az SSID-szórás (beacon keret) letiltását. A klienseknek manuálisan kell beállítaniuk az SSID-t, ha kapcsolódni szeretnének a hálózathoz.
* **MAC-cím szűrés** - A rendszergazda engedélyezheti vagy tilthatja a vezeték nélküli kliensek csatlakozását fizikai címük (MAC) alapján.

Bár a két szolgáltatás távol tartja a legtöbb illetéktelen felhasználót, de sem az SSID-rejtés, sem a MAC-cím szűrés nem rettenti el profi támadót. Az SSID könnyen kideríthető még akkor is, ha az AP nem szórja, A MAC-cím pedig becsapható (spoofing). A legjobb módszer a vezeték nélküli hálózat biztonságossá tételére a hitelesítés és a titkosítás (lásd 1. ábra).

Az eredeti 802.11 szabvány kétféle hitelesítést határoz meg:

* **Nyílt hitelesítés (open authentication)** - Minden vezeték nélküli kliens egyszerűen csatlakozhat; csak olyan esetekben alkalmazható, ha a biztonságnak nincs jelentősége, például szabad internet elérést biztosító helyeken (kávézók, szállodák, félreeső helyek).
* **Osztott kulcsú hitelesítés (shared key authentication)** - A hitelesítéshez és a kliens-AP adatforgalom titkosításához biztosít módszereket, pl.: WEP, WPA, és WPA2. A jelszót viszont előre meg kell osztani a kliensekkel.

A 2. ábrán a különféle hitelesítési módokat tartalmazó diagram látható.

**Megosztott kulcsú hitelesítési módok**

Háromféle megosztott kulcsú hitelesítési eljárás van (lásd 1. ábra).

* **WEP (Wired Equivalent Privacy)** - Vezetékessel egyenértékű titkosság; az eredeti 802.11 szabvány a vezetékes hálózati kapcsolattal azonos biztonságot határoz meg. Az adatokat RC4-titkosítással és statikus kulccsal védi. Mivel a kulcs az adatforgalom alatt nem változik, könnyen feltörhető.
* **WPA (Wi-Fi Protected Access)** - Wi-Fi védett hozzáférés; Wi-Fi Alliance szabvány, WEP-et használ, de az adattitkosítást az erősebb TKIP (Temporal Key Integrity Protocol) algoritmussal végzi. A TKIP minden csomag esetében megváltoztatja kulcsot, így sokkal nehezebben törhető fel.
* **WPA2 (IEEE 802.11i)** - Az IEEE 802.11i egy ipari szabvány a vezeték nélküli hálózatok biztonságossá tételére, a Wi-Fi Alliance változatát hívják WPA2-nek. Mindkettő AES-t (Advanced Encryption Standard) használ a titkosításhoz, mely jelenleg a legerősebb titkosítási protokoll.

A WEP használata már nem ajánlott, mert az általa használt kulcs bizonyítottan feltörhető. A WEP-kulcs gyengeségét ellensúlyozandó az első időkben a vállalatok bevezették az SSID-rejtés és a MAC-cím szűrés technológiákat. Az összes ilyen módszer túl gyengének bizonyult.

A WEP gyenge adatbiztonságát kiegészítő elemekkel igyekeztek pótolni. Azok a gyártók, akik nagyobb biztonságot igényeltek, mint például a Cisco, saját rendszereket fejlesztettek, elősegítve ezzel a 802.11i szabvány kialakítását. A 802.11i szabványig vezető úton alakult ki a TKIP titkosítási eljárás, amely később bekerült a Wi-Fi Alliance WPA-szabványba.

A korszerű vezeték nélküli hálózatokban a 802.11i/WPA2 szabványt kell használni. A WPA2 a 802.11i Wi-Fi változata, ezért a két szakkifejezés felcserélhető.

2006 óta a Wi-Fi Certified emblémával ellátott eszközök WPA2 igazolással is rendelkeznek.

**Megjegyzés**: Az N-es vezeték nélküli hálózatok WPA2-Personal módban nyújtják a legjobb teljesítményt.

A 2. ábrán az osztott kulcsú hitelesítési módok összefoglaló táblázata látható.

**Titkosítási módok**

A titkosítás az adatvédelmet szolgálja. Ha egy támadó titkosított adatokat gyűjt be, akkor azokat nem tudja értelmes időn belül visszafejteni.

Az IEEE 802.11i és a Wi-Fi Alliance WPA és WPA2 szabványai a következő titkosítási protokollokat használják:

* **TKIP (Temporal Key Integrity Protocol)** - A TKIP a WPA által használt titkosítási mód. Régebbi WLAN-berendezések támogatására szolgál, a 802.11 WEP titkosítás eredeti hibáit próbálja kijavítani. A 2. rétegbeli adatokat TKIP-val titkosítja, és ellenőrző összeget (Message Integrity Check, MIC) továbbít a titkosított csomagban az adatok sértetlenségének biztosítására.
* **AES (Advanced Encryption Standard)** - Az AES a WPA2 által használt titkosítási mód. Ez a preferált mód, mert igazodik a IEEE 802.11i szabványhoz. Az AES hasonlóan működik, mint a TKIP, de sokkal erősebb titkosítási módszert alkalmaz. CCMP-t (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) használ, hogy a célállomás érzékelni tudja a titkosított és titkosítatlan adatokban menet közben történt változásokat.

**Megjegyzés**: Válasszunk a WPA2/AES-t, amennyiben lehetséges.

**Otthoni felhasználó hitelesítése**

Az ábrán egy vezeték nélküli forgalomirányító biztonsági módjai láthatók. A lista a leggyengébbtől (Disabled, Nincs hitelesítés) a legerősebbig (WPA2 Personal vagy Enterprise) tart.

A WPA és a WPA2 kétféle hitelesítést támogat:

* **Personal (személyi)** - Otthoni vagy kisvállalati hálózatokba való mód, a felhasználók az AP-n előre megosztott kulccsal (PSK) hitelesítik magukat, melyet megosztott jelszónak is neveznek. Nincs szükség különálló hitelesítő szerverre.
* **Enterprise (vállalati)** - Vállalatok számára ajánlott, de szükség van egy RADIUS (Remote Authentication Dial-In User Service) hitelesítő szerverre. Bár beállítása bonyolultabb, cserébe több kiegészítő biztonsági elemet is tartalmaz. Először az eszköz hitelesít a RADIUS-szerveren, majd a felhasználói hitelesítés következik 802.1X szabvány szerint, mely EAP-ot (Extensible Authentication Protocol) használ.

A 802.1X bejelentkezési folyamat EAP-pal kommunikál az AP-val és a RADIUS-szerverrel. Ez a protokoll a hitelesített hálózati elérés keretrendszere. Biztonságos hitelesítési módot nyújt és egyezteti a titkos privát kulcsot, melyet ezután a TKIP és az AES a titkosítási folyamatban használ.

**Vállalati felhasználó hitelesítése**

A szigorúbb biztonságú hálózatokban további hitelesítés vagy bejelentkezés szükséges a vezeték nélküli kliensek hozzáférésének engedélyezésére. Az Enterprise mód használatához AAA (Authentication, Authorization, Accounting; hitelesítés, jogosultság, naplózás) RADIUS-szerver kell.

Az ábrán az Enterprise mód (WPA vagy WPA2) beállítására szolgáló mezők láthatók. Csak a megfelelő adatok bevitele után tud az AP az AAA-szerverrel kommunikálni:

* **RADIUS-szerver IP-címe** - Ez a RADIUS-szerver hálózatból elérhető címe.
* **RADIUS portszám** - Hivatalosan az UDP 1812 port van a RADIUS-hitelesítés, a 1813 port pedig a RADIUS-jogosultság számára, de képesek az UDP 1645-1646 portokon is működni (lásd ábra).
* **Megosztott kulcs** - Az AP hitelesítésére szolgál a RADIUS-szerveren.

Ez nem az a megosztott kulcs (jelszó), amit a vezeték nélküli kliensen kell konfigurálni. Ez csupán az AP-n szükséges, hogy hitelesíthesse magát a RADIUS-szerveren.

**Megjegyzés**: Azért nincs Password mező a listában, mert a felhasználói hitelesítést és jogosultságokat a 802.1X szabvány kezeli, mely központi, szerver-alapú végfelhasználói hitelesítést nyújt.

# Vezeték nélküli forgalomirányító beüzemelésének tervezése

A legtöbb otthoni vezeték nélküli forgalomirányító (köznapi nevén Wi-Fi router) kicsomagolás után használatra kész, nem igényel további konfigurálást. Viszont a forgalomirányító alapértelmezett IP-címe, felhasználóneve és jelszava könnyedén fellelhető az interneten. Csak be kell írni a keresőbe a "default router IP address" vagy a "default router password" kifejezést, és számos weboldal jelenik meg a találati listában. Ezért biztonsági okokból elsődlegesen fontos az alapértelmezett beállítások megváltoztatáa.

Üzembe helyezés előtt módosítsuk a következő beállításokat:

* **Internet connection (internet kapcsolat)** - Az internet kapcsolat IP-címét rendszerint az ISP adja DHCP segítségével (lásd ábra). Azomban a fejezet Packet Tracer feladataiban és laborgyakorlataiban statikusan fogjuk a címet beállítani.
* **DHCP Settings (DHCP-beállítások)** - A vezeték nélküli forgalomirányító konfigurált DHCP-beállításokkal érkezik mind a vezetékes, mind a vezeték nélküli hálózat kiszolgálására. Bevált biztonsági eljárás az alapértelmezett DHCP-értékek lecserélése, melyek az ábrán a **Network Setup** részben láthatók.
* **SSID Name (SSID név)** - A WLAN-hálózat alapértemezett neve, meg kell változtatni.
* **WLAN Security (WLAN biztonság)** - Gyárilag az otthoni forgalomirányítón nincs beállítva titlosítás és biztonsági jelszó. A WLAN nyílt és bármely vezeték nélküli kliens szabadon csatlakozhat hozzá. WPA2-hitelesítést, AES-titkosítást és egy erős jelszót kell beállítani.
* **Management Access (felügyeleti hozzáférés)** - A felügyeleti hozzáférés alapértelmezett jelszava bármely gyártó vezeték nélküli forgalomirányítójához megtalálható az interneten. Ezért a jelszót le kell cserélni, hogy megakadályozzuk az illetéktelen hozzáférést a forgalomirányító konfigurációs interfészéhez.

# Vezeték nélküli forgalomirányító csatlakoztatása az internethez

A forgalomirányítónak több portja van vezetékes eszközök számára. Például az ábrán látható eszköznek van egy USB-portja, egy internet portja és négy LAN-portja. Az **Internet** port olyan Ethernet csatlakozó, mely a forgalomirányítót a szolgáltatóval köti össze, például DSL- vagy kábelmodemen.

Az eszközök összeköttetését tartalmazó topológia a 2. ábrán látható. A vezeték nélküli forgalomirányító és a szélessávú modem összekapcsolásának lépései:

**1. lépés** Csatlakoztassunk egy egyenes kötésű Ethernet kábelt a forgalomirányító **Internet**feliratú portjába. A port neve lehet még **WAN**is. Az eszköz működési elve szerint minden adatforgalmat ezen a porton keresztül továbbít, mely az internet és a csatlakozó számítógépek között zajlik.

**2. lépés** A kábel másik végét csatlakoztassuk a szolgáltató szélessávú modemjének megfelelő portjába. A port felirata általában **Ethernet**, **Internet**vagy **WAN**.

**3. lépés**. Kapcsoljuk be a szélessávú modemet és csatlakoztassuk a forgalomirányító tápkábelét. Miután a modem kapcsolatba lépett az ISP-vel, elkezdi a kommunikációt a forgalomirányítóval. A forgalomirányító Internet ledje kigyullad, ez jelzi a kapcsolatot. A modemen keresztül a forgalomirányító hozzájut az internetcsatlakozáshoz szükséges hálózati információkhoz, beleértve a publikus IP-címet, az alhálózati maszkot és a DNS-szerver címét.

# Bejelentkezés a forgalomirányítóba

A vezeték nélküli forgalomirányító konfigurációs felületének eléréséhez kössük számítógépünket a forgalomirányító valamelyik LAN-portjába, majd nyissunk meg egy webböngészőt. A címmezőbe írjuk be a forgalomirányító alapértelmezett privát IP-címét. A címet a dokumentációban találjuk vagy megkereshetjük az interneten is. Az ábrán a 192.168.0.1 IP-cím látható, mely gyakori néhány gyártó esetében. Egy azonosító ablak jelenik meg a forgalomirányító grafikus felületének eléréséhez. Gyakran használt alapértelmezett felhasználó név és jelszó az **admin** . Ezek az információk is benne vannak a dokumentációban vagy megkereshetők az interneten.

# IP-címzés konfigurálása

Egy otthoni vagy kisvállalati forgalomirányító internet kapcsolati beállítását általában automatikus módban kell hagyni. De a fejezet Packet Tracer feladataiban és laborgyakorlataiban a vezeték nélküli forgalomirányítót egy szimulált hálózathoz fogjuk csatlakoztatni, ahol nincsenek internet szolgáltatások. Ezért ott az internet kapcsolatot kézzel kell konfigurálnunk.

Az 1. ábrán a statikus beállítás látható, a címadatok kézzel kerültek beírásra. A 2. ábrán az alapértelmezett DHCP-címzés megváltozott, helyette a 10.10.10.0/24 alhálózat került be. A DNS-cím azonos az 1. ábrán beállítottal.

A konfiguráció mentése után megszakad a kapcsolat a vezeték nélküli forgalomirányítóval. A hozzáférés visszaállításához újítsuk meg az IP-címünket, majd írjuk be a böngésző címsorába a forgalomirányító új címét, 10.10.10.1.

**Vezeték nélküli beállítások**

A forgalomirányítóba való sikeres belépés után bevált gyakorlat néhány alapbeállítást megtenni a vezeték nélküli hálózat biztonsága érdekében:

* **Network Mode (hálózati mód)** - Sok vezeték nélküli forgalomirányítón megválaszthatjuk, hogy melyik 802.11 szabványt kívánjuk használni. Az 1. ábrán "Mixed" beállítást láthatunk. Ez azt jelenti, hogy a forgalomirányítóhoz kapcsolódó vezeték nélküli eszköz használhatja a 802.11a, b, g, és n szabványt is.
* **SSID (hálózat név)** - Hálózati azonosítót rendel a WLAN-hoz. Az 1. ábrán a "Home-Net" beállítás látható. Ha az SSID-szórás tiltott, akkor a vezeték nélküli kliensen kézzel kell ezt a nevet megadni.
* **Standard Channel (standard csatorna)** - 802.11b és 802.11g szabványok legtöbbször az 1, 6 vagy 11 csatorna beállítást alkalmazzák az interferencia elkerülése céljából. Az 1. ábrán a 6-os kézi beállítás látható.
* **Wireless Security (vezeték nélküli biztonság)** - Konfiguráljuk a legerősebb biztonsági módot, amely a WPA2 AES-titkosítással (lásd 2. ábra).

# Felügyeleti hozzáférés konfigurálása

Bár megváltoztattuk a forgalomirányító felügyeleti címét (10.10.10.1), de a jelszó az alapértelmezett maradt. A Packet Tracer forgalomirányítóban a felügyeleti jelszót az "Administration" fül alatt lehet megváltoztatni (lásd 1. ábra).

Ugyan ezen a lapon, alul találhatók a "BackUp Configuration" és "Restore Configuration" (konfiguráció mentése, helyreállítása) nyomógombok (lásd 2. ábra).

# Vezeték nélküli kliens csatlakoztatása

Az AP vagy vezeték nélküli forgalomirányító beállítása után teszteljük le a kapcsolatot egy vezeték nélküli klienssel (lásd ábra). Ellenőrizzük le, hogy a kliens a megfelelő hálózathoz csatlakozott, különösen akkor, ha sok WLAN elérhető a közelben.

# Packet Tracer - Vezeték nélküli LAN konfigurálása

**Háttér / esetleírás**

Ebben a feladatban egy vezeték nélküli forgalomirányítót fogunk konfigurálni, mellyel távoli eléréshez juttatjuk a PC-ket, valamint vezeték nélküli kapcsolódást engedélyezünk WPA2 használatával. A PC vezeték nélküli kapcsolatát manuálisan konfiguráljuk az SSID és a jelszó begépelésével.

[Packet Tracer - Configuring Wireless LAN Access Instructions](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/4.4.2.2%20Packet%20Tracer%20-%20Configuring%20Wireless%20LAN%20Access%20Instructions.pdf)

[Packet Tracer - Configuring Wireless LAN Access - PKA](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/4.4.2.2%20Packet%20Tracer%20-%20Configuring%20Wireless%20LAN%20Access.pka)

**Hibaelhárítási szemléletmódok**

Mindenféle hálózati probléma elhárítása szisztematikus megközelítést igényel. A logikai hálózati modellek, mint például az OSI és a TCP/IP-modell a hálózati működést különálló szintekre bontják.

Hibaelhárítás során ezeket a réteges modelleket a fizikai hálózatra alkalmazva tudjuk elkülöníteni a hálózati problémákat. Például ha a jelenség fizikai kapcsolati hibára utal, akkor a hálózati szakember a hibaelhárítás során az áramkörökre tud összpontosítani, mivel azok működnek a fizikai rétegben. Ha az áramkör rendben üzemel, a technikus egy másik réteget fog megvizsgálni a hiba azonosításának céljából.

Három fő hibaelhárítási szemlélet van a hálózati problémák megoldására:

* **Lentről felfelé (bottom-up)** - Induljunk el az 1. rétegtől és haladjunk felfelé. Lásd 1. ábra.
* **Fentről lefelé (top-down)** - Induljunk el a legfelső rétegtől és haladjunk lefelé. Lásd 2. ábra.
* **Oszd meg és uralkodj (divide-and-conquer)** - Pingeld meg a célállomást. Ha ping sikertelen, ellenőrizd az alsóbb rétegeket. Ha a ping sikeres, ellenőrizd a felsőbb rétegeket. Lásd 3. ábra.

**A vezeték nélküli kliens nem csatlakozik**

A WLAN-hiba elhárítása során a kizárásos módszer használata javasolt.

Az ábrán látható vezeték nélküli kliens nem tud a WLAN-hoz csatlakozni. Ha nincs kapcsolat, vizsgáljuk meg a következőket:

* Ellenőrizzük a hálózati beállításokat a PC-n az **ipconfig** parancs segítségével! Nézzük meg, hogy kapott-e a PC IP-címet a DHCP-szervertől, vagy statikus IP-címmel van-e konfigurálva.
* Győződjünk meg róla, hogy az eszköz képes a vezetékes hálózathoz kapcsolódni. Csatlakoztassuk kábellel a LAN-hoz és **ping** -eljünk meg egy ismert IP-címet.
* Ha szükséges, töltsük be újra a megfelelő illesztőprogramokat. Esetleg próbáljunk ki egy másik vezeték nélküli hálózati kártyát.
* Ha a kliens vezeték nélküli illesztője működik, ellenőrizzük a biztonsági módot és a titkosítási beállításokat. Ha a biztonsági beállítások nem egyeznek a hálózatéval, a kliens nem tud csatlakozni a WLAN-hoz.

Ha a PC működik, de a vezeték nélküli kapcsolat gyenge, vizsgáljuk meg a következőket:

* Milyen messze van a PC az AP-től? Kívül esik a PC a cellán (BSA)?
* Ellenőrizzük a kliensen a csatornabeállításokat. Ha az SSID jó, a kliens szoftver fel kell ismerje a helyes csatornát.
* Ellenőrizzük, hogy nincs-e a területen egyéb berendezés, amely interferenciát okozhat a 2,4 GHz tartományban. Ilyenek lehetnek például a hordozható telefonok, a baba őrzők, a mikrohullámú sütők, a vezeték nélküli biztonsági rendszerek (kamerák) és a csaló AP-k. A berendezések által kibocsájtott jel interferenciát okozhat a WLAN-ban, ami rendszertelen kapcsolódási problémákhoz vezet a kliens és az AP között.

Továbbá, ellenőrizzük, hogy minden eszköz a helyén van-e. Gondoljunk a fizikai tényezőkre is. Minden eszköz kap áramot és be is vannak kapcsolva?

Végül ellenőrizzük a vezetékes eszközök közötti csatlakozásokat, keressünk rossz aljzatokat, sérült vagy hiányzó kábeleket. Ha a fizikai üzemvitelben nincs hiba, teszteljük pinggel a LAN-eszközöket, beleértve az AP-t is. Ha a kapcsolat megszakad ennél a pontnál, akkor valószínűleg az AP vagy annak beállításai hibásak.

Ha a kliens PC-t kizártuk a hibaforrások közül, és az eszközök fizikai állapota is megfelelő, akkor megkezdhetjük az AP teljesítményének vizsgálatát. Először nézzük meg az áramellátás állapotát.

# Lassú hálózat hibaelhárítása

802.11n/ac kétsávos forgalomirányítók (dual-band routers) sávszélességének optimalizálása és növelése:

* **Korszerűsítsük a vezeték nélküli klienseket** - A régebbi, 802.11b és 802.11g eszközök lelassíthatják a teljes WLAN-t. A legjobb teljesítmény eléréséhez az összes vezeték nélküli berendezésnek ugyan azt a legmagasabb szabványt kell támogatnia.
* **Válasszuk szét a forgalmat** - A vezeték nélküli teljesítmény növelésének legegyszerűbb módja a forgalom szétosztása a 802.11n 2,4 GHz-es és 5 GHz-es sávja között. A 802.11n (vagy annál jobb) eszközök képesek a két sávot két különálló hálózatként használni, így segíthetik a forgalom szabályozását. Például használjuk a 2,4 GHz-es hálózatot az alap internetes műveletekhez, mint a böngészés, az e-mail és a letöltés, az 5 GHz-es sávot pedig multimédiás adatfolyamokhoz (lásd ábra).

Különböző érvek szólnak a forgalom-szétválasztás használata mellett:

* A 2,4 GHz-es sáv megfelelő az alap internetes forgalom számára, ha az nem késleltetés-érzékeny.
* A sávszélességet megosztva kell használni más közeli WLAN-okkal.
* Az 5 GHz-es sáv sokkal kevésbé zsúfolt, mint a 2,4 GHz-es, tökéletes a multimédiás adatfolyamok számára.
* Az 5 GHz-es sávban több csatorna van, így a csatornaválasztás valószínűleg interferenciamentes.

Alapértelmezés szerint a kétsávos forgalomirányítók ugyanazt a hálózati nevet használják a 2,4 GHz-es és az 5 GHz-es sávban is. A forgalom szétválasztásának legegyszerűbb módja az egyik hálózat átnevezése. Különböző nevek segítségével könnyebb a megfelelő hálózathoz csatlakozás.

A vezeték nélküli hálózat hatótávolságának növeléséhez a forgalomirányítót akadálymentes területen kell elhelyezni, azaz távol a bútoroktól, berendezési tárgyaktól és magas szerkezetektől, melyek elnyelik a jeleket. Ha mindez nem oldja meg a problémát, akkor jelerősítőt (Wi-Fi Range Extender) vagy Powerline technológiát kell használni.

# Firmware frissítés

A legtöbb vezeték nélküli forgalomirányítón frissíthető a működtető szoftver (firmware). A firmware kiadások javításokat tartalmaznak, egyrészt az ügyfelek által jelezett hibákhoz, másrészt a biztonsági sebezhetőségekre. Rendszeresen ellenőrizzük a kiadott frissítésekért a gyártók honlapját! Letöltés után a forgalomirányító grafikus felületén tölthetjük fel firmware-t (lásd ábra). A frissítés idejére a felhasználók kapcsolata megszakad a WLAN-nal és az internettel. A vezeték nélküli forgalomirányító néhányszor újraindulhat, amíg a normális hálózati működés végleg helyreáll.

**Figyelem!**: Ne frissítsük a firmware-t, ha nincs probléma az AP-val vagy ha nem kívánunk új szolgáltatást igénybe venni.

**Csoportos feladat - Belső és külső vizsgálat**

**Belső és külső vizsgálat**

Készült egy értékelés annak igazolására, hogy vállalatunk vezeték nélküli hálózata fejlesztésre szorul. A jóváhagyott beszerzésben beltéri és kültéri elérési pontok és egy vezeték nélküli vezérlő van. Megrendelés előtt össze kell hasonlítanunk a különféle modelleket és azok műszaki leírását.

Ezért keressük fel a "[Wireless Compare Products and Services](http://www.cisco.com/en/US/products/hw/wireless/products_category_buyers_guide.html" \t "_blank)" weboldalt és tekintsük át a beltéri és kültéri AP-k, valamint a vezérlő eszközök összehasonlító táblázatát. Az információk között felbukkan néhány ismeretlen szakkifejezés, úgymint:

* FIPS (Federal Information Processing Standard)
* MIMO
* Cisco CleanAir Technology
* Cisco FlexConnect
* Band Select

Nézzünk utána a fenti szakkifejezéseknek! Készítsük el saját táblázatunkat vállalatunk legfontosabb igényeinek felsorolásával, melyek a bel- és kültéri AP-k és a vezérlők beszerzésére vonatkoznak. Ez a táblázat segítségünkre lesz, mikor a megrendelést jóváhagyatjuk a gazdasági vezetővel és a vezérigazgatóval (chief executive officer, CEO).

[Csoportos feladat - Belső és külső vizsgálat](https://contenthub.netacad.com/legacy/CCNA/ScaN/5.03/hu/course/files/4.5.1.1%20Inside%20and%20Outside%20Control%20Instructions.pdf)

# Összefoglalás

Gyakran használnak WLAN-ok otthonokban, irodákban, egyetemi épületekben. A 802.11 szabvány szerinti vezeték nélküli hálózatok a 2,4 GHz-es, az 5 GHz-es és 60 GHz-es frekvenciákat használják. Az ITU-R felügyeli az RF-tartomány kiosztását, az IEEE pedig a 802.11 szabványokban írja le, hogyan kell ezeket a frekvenciákat a vezeték nélküli hálózatok fizikai és MAC-alrétegében használni. A Wi-Fi Alliance minősíti a termékeket, hogy megfelelnek-e a szabványoknak.

A kliens vezeték nélküli hálózati kártyával csatlakozik egy infrastruktúrát biztosító eszközhöz, amely lehet vezeték nélküli forgalomirányító vagy AP. A kapcsolódáshoz SSID-t használ. Az AP-k működhetnek kis területet kiszolgáló önálló eszközként, vagy egy nagy, vezérlő alapú hálózat részeként.

A Cisco Aironet AP-hoz csatlakoztatható körsugárzó, irányított vagy Yagi-antenna is. Az IEEE 802.11n/ac/ad MIMO-technológiát alkalmaz a hasznos átvitel növelésére és négy antenna egyidejű használatát teszi lehetővé.

Ad-hoc módban (IBSS) két vezeték nélküli eszköz csatlakozik egymáshoz egyenrangú félként (P2P).

Infrastruktúra módban az AP-k vezetékkel kapcsolódnak a hálózathoz. Minden AP egy BSS-t alkot, melyet a BSSID (MAC-cím) egyedileg azonosít. Több BSS együtt ESS-t hozhat létre. Az ESS közös SSID-je zökkenőmentes barangolást tesz lehetővé a BSS-ek között. További SSID-k használatával elkülöníthetők egymástól a hálózati hozzáférési szintek és azok forgalma.

A vezeték nélküli kliens először hitelesíti magát az AP-n, majd társul vele (csatlakozik). A 802.11i/WPA2 hitelesítési szabvány használata ajánlott AES-titkosításal.

Vezeték nélküli hálózat tervezésekor, ha több AP is lefed azonos területet, használjunk nem-átlapolódó csatornákat. A cellák (BSA) között legyen 10-15% átfedés. A telepítés könnyítésére a Cisco AP-k támogatják a PoE-t is.

A vezeték nélküli hálózatok különösen fogékonyak bizonyos fenyegetésekre, ilyenek például a vezeték nélküli behatolók, a csaló AP-k, az üzenet eltérítés (MITM) és a DoS-támadások. A Cisco számos megoldást kínál ezen fenyegetések elhárítására.

