Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/1.1.1#chunks-container)

Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

* [1Alapbeállítások](https://contenthub.netacad.com/srwe-dl/1.1.1#1)
  + [1.0Bevezetés](https://contenthub.netacad.com/srwe-dl/1.1.1#1.0)
    - [1.0.1Miért fontos ez a fejezet?](https://contenthub.netacad.com/srwe-dl/1.0.1)
    - [1.0.2Miről fogunk tanulni ebben a fejezetben?](https://contenthub.netacad.com/srwe-dl/1.0.2)
    - [1.0.3Videómagyarázat - A Packet Tracer letöltése és telepítése](https://contenthub.netacad.com/srwe-dl/1.0.3)
    - [1.0.4Videómagyarázat - Első lépések a Cisco Packet Tracerben](https://contenthub.netacad.com/srwe-dl/1.0.4)
    - [1.0.5Packet Tracer - Logikai és fizikai módok felfedezése](https://contenthub.netacad.com/srwe-dl/1.0.5)
  + [1.1A switch alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.1.1#1.1)
    - [1.1.1A switch rendszerindítási sorrendje](https://contenthub.netacad.com/srwe-dl/1.1.1)
    - [1.1.2Egy boot rendszer parancs](https://contenthub.netacad.com/srwe-dl/1.1.2)
    - [1.1.3A kapcsoló LED-jelzőfényei](https://contenthub.netacad.com/srwe-dl/1.1.3)
    - [1.1.4Helyreállítás egy rendszerösszeomlás után](https://contenthub.netacad.com/srwe-dl/1.1.4)
    - [1.1.5A switch felügyeleti hozzáférése](https://contenthub.netacad.com/srwe-dl/1.1.5)
    - [1.1.6Példa a switch virtuális interfészének (SVI) beállítására](https://contenthub.netacad.com/srwe-dl/1.1.6)
    - [1.1.7Laborgyakorlat - A switch alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.1.7)
  + [1.2Switchportok vezérlésja](https://contenthub.netacad.com/srwe-dl/1.1.1#1.2)
  + [1.3Biztonságos távoli hozzáférés](https://contenthub.netacad.com/srwe-dl/1.1.1#1.3)
  + [1.4A router alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.1.1#1.4)
  + [1.5Közvetlenül csatlakozó hálózatok ellenőrzése](https://contenthub.netacad.com/srwe-dl/1.1.1#1.5)
  + [1.6Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/1.1.1#1.6)
* [2Fogalmak váltása](https://contenthub.netacad.com/srwe-dl/1.1.1#2)
* [3VLAN-ok](https://contenthub.netacad.com/srwe-dl/1.1.1#3)
* [4Inter-VLAN Routing](https://contenthub.netacad.com/srwe-dl/1.1.1#4)
* [5STP fogalmak](https://contenthub.netacad.com/srwe-dl/1.1.1#5)
* [6EtherChannel](https://contenthub.netacad.com/srwe-dl/1.1.1#6)
* [7DHCPv4](https://contenthub.netacad.com/srwe-dl/1.1.1#7)
* [8SLAAC és DHCPv6](https://contenthub.netacad.com/srwe-dl/1.1.1#8)
* [9FHRP koncepciók](https://contenthub.netacad.com/srwe-dl/1.1.1#9)
* [10LAN biztonsági koncepciók](https://contenthub.netacad.com/srwe-dl/1.1.1#10)
* [11Switch biztonságának beállítása](https://contenthub.netacad.com/srwe-dl/1.1.1#11)
* [12WLAN fogalmak](https://contenthub.netacad.com/srwe-dl/1.1.1#12)
* [13WLAN konfiguráció](https://contenthub.netacad.com/srwe-dl/1.1.1#13)
* [14Útválasztási fogalmak](https://contenthub.netacad.com/srwe-dl/1.1.1#14)
* [15IP statikus útválasztás](https://contenthub.netacad.com/srwe-dl/1.1.1#15)
* [16Statikus és alapértelmezett útvonalak hibaelhárítása](https://contenthub.netacad.com/srwe-dl/1.1.1#16)

1. Alapbeállítások
2. A switch alapbeállításainak megadása

A switch alapbeállításainak megadása

1.1.1

A switch rendszerindítási sorrendje

Egy switch konfigurálása előtt azt be kell kapcsolni, és lehetővé tenni, hogy menjen az ötlépéses rendszerindítási sorrenden. Ez a témakör a switch konfigurálásának alapjait tárgyalja, a végén egy laborgyakorlattal.

Egy Cisco switch bekapcsolása után az alábbi öt rendszerindítási lépésen megy keresztül:

**1. lépés** : Először a kapcsoló betölti a ROM-ban tárolt bekapcsolási önteszt (POST) programot. A POST leellenőrzi a CPU alrendszert, azaz vizsgálja meg a CPU-t, a DRAM-ot, és a flash memóriában található fájlrendszert. **2. lépés** : Ezután a kapcsoló betölti a rendszertöltő szoftvert. A rendszerindító szoftver egy kicsi program a ROM-ban tárolva, közvetlenül a POST sikeres befejezése után fut le. **3. lépés** : A rendszertöltő alacsony szintű CPU inicializálást hajt végre. Beállítja a CPU-regisztereket, a fizikai memória felhasználását, a memória mennyiségét és sebességét vezérlik. **4. lépés** : A rendszertöltő inicializálja a flash fájlrendszert az alaplapon. **5. lépés**: Végül a rendszertöltő megkeresi és betölti az alapértelmezett IOS operációs rendszer szoftverképet a memóriába, és átadja az IOS-re való váltás vezérlését.

1.1.2

Egy boot rendszer parancs

A rendszert automatikusan megkísérli a indítást a BOOT változó információi alapján. Ha ez a változó nincs beállítva, a switch megpróbálja betölteni és végrehajtani az első futtatható fájlt, amit talál. A Catalyst 2960 sorozatú switch-ek esetében a képfájl általában egy olyan könyvtárban található, amely nem megegyezik a képfájl nevével (kivéve a .bin fájlkiterjesztést).

Az IOS rendszer ezután inicializálja az interfészeket az indítási beállításs (startup-config) fájlban található Cisco IOS parancsok alapján. Az indítási telepítéss fájl neve **config.text** , és a flash memóriában tárolódik.

A példában a BOOT környezeti változó a globális beállításs mód **boot system** parancsával állítható be. Figyeljük meg, hogy az IOS egy külön mappában található, és a térkép elérési útja is meg van adva. A **show boot** utasítással megnézhetjük, hogy az IOS rendszerindító fájl jelenleg mire van beállítva.

S1(config)# **boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin**

Az alábbi táblázat a **boot system** utasítás egyes részeinek jelentését értelmezi.

| Táblázat felirata | |
| --- | --- |
| **Parancs** | **Értelmezés** |
| **rendszerindító rendszer** | A fő parancs |
| **vaku:** | A tárolóeszköz |
| **c2960-lanbasek9-mz.150-2.SE/** | A fájlrendszer elérési útja |
| **c2960-lanbasek9-mz.150-2.SE.bin** | Az IOS fájlnév |

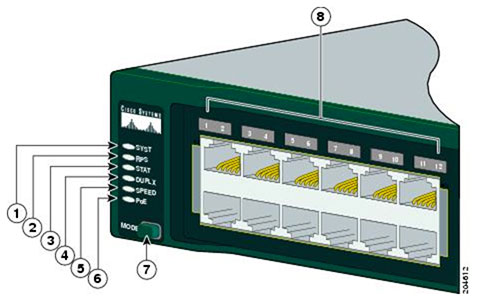
1.1.3

A kapcsoló LED-jelzőfényei

A Cisco Catalyst switch-en számos állapotjelző LED található. Az állapotjelző LED-ekkel gyorsan ellenőrizhető a switch működése és teljesítménye. A LED-ek jelentése és előlapi elrendezésük a switch modellje és felszereltsége szerint változhat.

Az ábrán egy Cisco Catalyst 2960 switch LED-jeit és Mode gombját láthatjuk.

Az ábrán a LED-ek, a Mode gomb és a switch bal elülső oldalán található portok láthatók. A 6 db LED kijelző fentről lefelé a következő: SYST, RPS, STAT, DUPLX, SPEED és PoE. A LED-kijelzők alatt, az ábrán 7-es jelzéssel a Mode gomb található. A switchportok felett, az ábrán 8-as jelzéssel ellátva a port LED-ek találhatók.



A Mode gomb (az ábrán 7-es jelzéssel ellátva) a portállapot, a duplexitást, a sebességet, és támogatja, akkor PoE (Power over Ethernet) állapot kijelzésének váltogatására szolgál a port LED-eken (az ábrán 8-as jelzéssel ellátva) .

A LED-indikátorok (az ábrán 1-6 között jelölt) céljának és színük jelentésének megismeréséhez kattintsunk az egyes gombokra:

1 SYST

2 RPS

3 STAT

4 DUPLX

5 SEBESSÉGES

6 PoE

**Rendszer LED**

Megmutatja, hogy a rendszer kap-e áramot, és megfelelően működik-e. Ha a LED nem világít, akkor a rendszer nincs bekapcsolt állapotban. Ha a LED zölden világít, a rendszer megfelelően működik. Ha a LED sárga, a rendszer áram alatt van, de nem működik megfelelően.

**Redundáns energiaellátó rendszer (RPS) LED**

Az RPS állapotát mutatja. Ha a LED nem világít, akkor az RPS ki van kapcsolva, vagy nincs megfelelően csatlakoztatva. Ha a LED zöld, az RPS csatlakoztatva van, és készen áll a tartalék tápfeszültség biztosítására. Ha a LED villogó zöld, akkor az RPS csatlakoztatva van, de nem elérhető, mivel más eszköz számára biztosított tápfeszültséget. Ha a LED sárgán világít, akkor az RPS készenléti üzemmódban van, vagy hibás. Ha a LED villogó sárga, akkor a switch belső tápegysége meghibásodott, és az RPS szolgáltató áramot a készüléknek.

**Port állapot LED**

Azt jelzi, hogy a portállapot mód van kiválasztva, ha a LED zöld. Ez az beállítás mód. Ekkor az egyes port LED-ek színei az üzemmódnak megfelelően világítanak. Ha a port LED nem világít, ha nincs kapcsolat vagy a port adminisztratívan le van tiltva. Ha a port LED zöld, a kapcsolat működik. Ha a port LED villogó zöld, akkor a port éppen adatokat küld vagy fogad. Ha a port LED felváltva zöld-sárga, akkor hibás a kapcsolat. Ha a port LED sárgán világít, akkor a port blokkolva van annak érdekében, hogy ne lehessenek hurkok az érintett tartományban, és ilyenkor nem továbbít adatokat (a portok ebben az állapotban jellemzően a bekapcsolásuk utáni 30 másodpercben vannak). Ha a port sárgán villog, a port le van tiltva, hogy egy adott lehetséges hurok kialakulását az esetleges szegmensen.

**Port Duplex LED**

Azt jelzi, hogy a port duplex mód van kiválasztva, ha a LED zöld. Ebben az esetben, ha az egyes port LED-ek nem világítanak, akkor azok félduplex (half-duplex) módban működnek. Ha a port LED zöld, a port teljes duplex (full-duplex) módban üzemel.

**Port sebesség LED**

Azt jelzi, hogy a port sebessége mód van kiválasztva. Ekkor az egyes port LED-ek színei az üzemmódnak megfelelően világítanak. Ha a LED nem világít, akkor a port 10 Mbps sebességen működik. Ha a LED zöld, akkor a port 100 Mbps sebességen működik. Ha a LED villogó zöld, akkor a port 1000 Mbps sebességen működik.

**Power over Ethernet (PoE) mód LED**

Ha a PoE támogatott, a PoE mód LED világít. Ha a LED nem világít, azt jelzi, hogy a PoE mód nincs ugyan kiválasztva, de egyik porton sincs tápellátáshiány vagy -meghibásodás. Ha a port sárgán villog, akkor a PoE mód ugyancsak nincs kiválasztva, de legalább az egyik porton tápellátáshiány PoE-hiba lépett fel. Ha a LED zöld, a PoE mód kiválasztása került, és az egyes port LED-ek színei ennek az üzemmódnak megfelelően világítanak. Ha a port LED nem világít, a PoE ki van kapcsolva az adott porton. Ha a port LED zöld, a PoE be van kapcsolva. Ha a port felváltva zöld-sárga, a PoE le van tiltva, mert nincs elegendő tápkapacitás a portra csatlakoztatott LED-es eszköz ellátására. Ha a LED sárgán villog, akkor a PoE egy hiba miatt ki van kapcsolva. Ha a LED sárga, a PoE a porton le van tiltva.

1.1.4

Helyreállítás egy rendszerösszeomlás után

Ha az operációs rendszer hiányzó vagy sérült fájlok miatt használhatatlanná válik, akkor a boot loader segítségével még hozzáférhetünk a switch-hez. A boot loader parancssorán keresztül elérhetők a flash memóriában tárolt fájlok.

Egy konzolkapcsolaton keresztül a boot loader parancssora az alábbi lépésekkel érhető el:

**1. lépés** . Konzolkábellel csatlakoztassunk egy PC-t a switch konzolportjához. Állítsunk be egy terminálemulációs szoftvert a switch-hez való csatlakozásra. **2. lépés** . Húzzuk ki a switch tápkábelét. **3. lépés** . Csatlakoztassa újra a tápkábelt a kapcsolóhoz, és 15 másodpercen belül nyomja meg és tartsa lenyomva a **Mode** gombot, amíg a rendszer LED továbbra is zölden villog. **4. lépés** . Továbbra is nyomja meg a **Mode** gombot, amíg a rendszer LED rövid időre borostyánsárgára, majd folyamatosan zöldre nem vált; majd engedje fel a **Mode** gombot. **5. lépés** . A boot loader **switch:** promptja a terminál emulációs szoftver ablakában.

Írjuk be a **help** vagy **?**parancsokat a boot loader parancsába az elérhető parancsok kiadványnak néznek.

Alap szerint a switch változó a BOOT környezeti értelmezésben található információk alapján automatikusan elindulni. A switch BOOT környezeti változójában lévő elérési út képernyő gépeljük be a **set** parancsot. segítségével a flash memória fájlrendszerét a **flash \_ init** parancs segítségével inicializálhatjuk, hogy az ábrán látható módon megtekinthessük az aktuálisan rajta tárolt fájlokat.

switch: **set**

BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin

(output omitted)

switch: **flash\_init**

Initializing Flash...

flashfs[0]: 2 files, 1 directories

flashfs[0]: 0 orphaned files, 0 orphaned directories

flashfs[0]: Total bytes: 32514048

flashfs[0]: Bytes used: 11838464

flashfs[0]: Bytes available: 20675584

flashfs[0]: flashfs fsck took 10 seconds.

...done Initializing Flash.

Miután a flash inicializálása befejeződött, írjuk be a **dir flash:** parancsot a flash-ben tárolja a könyvtárak és fájlok képéhez, az ábrán látható módon.

switch: **dir flash:**

Directory of flash:/

2 -rwx 11834846 c2960-lanbasek9-mz.150-2.SE8.bin

3 -rwx 2072 multiple-fs

Írjuk be a **BOOT=flash** parancsot a BOOT környezeti változóban lévő elérési út megváltoztatásához, amelyet a switch a flash-ben lévő új IOS betöltéséhez használhat. A BOOT környezeti változóba bekerült új elérési út ellenőrzéséhez adjuk ki ismét a **set** parancsot. Végül pedig az új IOS betöltéséhez a **boot** parancsot kell kiadnunk argumentumok nélkül, ahogy az ábrán is látható.

switch: **BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin**

switch: **set**

BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin

(output omitted)

switch: **boot**

A boot loader parancsai támogatják a flash memória inicializálását, formázását, új IOS telepítését, a BOOT környezeti változó megváltoztatását, valamint az elveszett vagy elfelejtett jelszavak helyreállítását is.

1.1.5

A switch felügyeleti hozzáférése

A kapcsoló távoli felügyeleti hozzáférésre való előkészítéséhez a kapcsolónak rendelkeznie kell egy kapcsoló virtuális interfésszel (SVI), amely IPv4-címmel és alhálózati maszkkal vagy IPv6-címmel és IPv6-előtaghosszal van konfigurálva. Az SVI egy virtuális interfész és nem a switch egyik fizikai portja. Ne felejtsük el, hogy a switch távoli hálózatról történő eléréséhez konfigurálni kell egy alapértelmezett átjárót is! Ez nagyban hasonlít a munkaállomások IP-beállításához.

switch with a network connection to a router and a console cable connection to a host PC

2001:db8:acad:99::1/64172.17.99.1VLAN 99172.17.99.11/242001:db8:acad:99::11/64S1R1PC1R1

Console Cable

1.1.6

Példa a switch virtuális interfészének (SVI) beállítására

Alapértelmezés szerint a switch felügyelete az 1-es VLAN-on keresztül történik. Kezdetben a switch minden portja az 1-es VLAN-hoz van hozzárendelve. Biztonsági okokból azonban nem ajánlott az 1-es VLAN felügyeleti célokra történő használata, bevált gyakorlat azt egy másik VLAN-nal helyettesíteni, mint amilyen az alábbi példában a 99-es.

A switchfelügyelet konfigurációs lépéseinek megismeréséhez kattintsunk az egyes gombokra!

1. lépés

2. lépés

3. lépés

**Step 1**

**Configure the Management Interface**

From VLAN interface configuration mode, an IPv4 address and subnet mask is applied to the management SVI of the switch. Pontosabban, az SVI VLAN 99 a 172.17.99.11/24 IPv4-címet és a 2001:db8:acad:99::1/64 IPv6-címet fogja hozzárendelni az ábrán látható módon.

**Note**: The SVI for VLAN 99 will not appear as “up/up” until VLAN 99 is created and there is a device connected to a switch port associated with VLAN 99.

**Note**: The switch may need to be configured for IPv6. For example, before you can configure IPv6 addressing on a Cisco Catalyst 2960 running IOS version 15.0, you will need to enter the global configuration command **sdm prefer dual-ipv4-and-ipv6 default** and then **reload** the switch.

| TaskIOS CommandsLépjen be a globális konfigurációs módba.S1# configure terminalLépjen be az SVI interfész konfigurációs módjába.S1(config)# interfész vlan 99A felügyeleti interfész IPv4-címének konfigurálása.S1(config-if)# ip address 172.17.99.11 255.255.255.0Configure the interface.0 IPv6 addressS1(config-if)# ipv6 address 2001:db8:acad:99::1/64A felügyeleti felület engedélyezése.S1(config-if)# no shutdown Visszatérés a privilegizált EXEC módba.S1(config-if)# end Mentse a futtató config az indítási config.S1# másolása running-config startup-config | |
| --- | --- |
| **Task** | **IOS Commands** |
| Lépjünk be a globális konfigurációs módba. | S1# **configure terminal** |
| Lépjünk be az SVI interfészkonfigurációs módjába. | S1(config)# **interface vlan 99** |
| Állítsuk be a felügyeleti interfész IPv4-es címét. | S1(config-if)# **ip address 172.17.99.11 255.255.255.0** |
| Állítsuk be a felügyeleti interfész IPv6-os címét. | S1(config-if)# **ipv6 address 2001:db8:acad:99::11/64** |
| Engedélyezzük a felügyeleti interfészt. | S1(config-if)# **no shutdown** |
| Lépjünk vissza a privilegizált EXEC módba. | S1(config-if)# **end** |
| Mentsük el az aktuális konfigurációt indítási konfigurációként. | S1# **copy running-config startup-config** |

1.1.7

Laborgyakorlat - A switch alapbeállításainak megadása

Készségek gyakorlási lehetőség

Lehetőséged van az alábbi készségek gyakorlására:

* Part 1: 1. rész: A hálózat kábelezése és a switch alapértelmezett beállításainak vizsgálata
* Part 2: 2. rész: A hálózati eszköz alapbeállításainak megadása
* Part 3: 3. rész: A hálózati kapcsolat ellenőrzése

Ezeket a készségeket gyakorolhatja a Packet Tracer vagy a laboratóriumi berendezés segítségével, ha áll rendelkezésre.

**Packet Tracer – Fizikai mód (PTPM)**

 Alapvető kapcsolókonfiguráció – Fizikai mód

[Alapvető kapcsolókonfiguráció – Fizikai mód](https://contenthub.netacad.com/courses/srwe-dl/_common/1.1.7-packet-tracer---basic-switch-configuration---physical-mode_hu-HU.pka)

**Laboratóriumi berendezések**

 Alap kapcsoló konfiguráció

[1.0](https://contenthub.netacad.com/srwe-dl/1.1.1" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/1.1.1" \l "/srwe-dl/undefined.1)

[1.2](https://contenthub.netacad.com/srwe-dl/1.1.1" \l "/srwe-dl/undefined.1)

[Switchportok vezérlésja](https://contenthub.netacad.com/srwe-dl/1.1.1" \l "/srwe-dl/undefined.1)

Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/1.2.1#chunks-container)

Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

* [1Alapbeállítások](https://contenthub.netacad.com/srwe-dl/1.2.1#1)
  + [1.0Bevezetés](https://contenthub.netacad.com/srwe-dl/1.2.1#1.0)
    - [1.0.1Miért fontos ez a fejezet?](https://contenthub.netacad.com/srwe-dl/1.0.1)
    - [1.0.2Miről fogunk tanulni ebben a fejezetben?](https://contenthub.netacad.com/srwe-dl/1.0.2)
    - [1.0.3Videómagyarázat - A Packet Tracer letöltése és telepítése](https://contenthub.netacad.com/srwe-dl/1.0.3)
    - [1.0.4Videómagyarázat - Első lépések a Cisco Packet Tracerben](https://contenthub.netacad.com/srwe-dl/1.0.4)
    - [1.0.5Packet Tracer - Logikai és fizikai módok felfedezése](https://contenthub.netacad.com/srwe-dl/1.0.5)
  + [1.1A switch alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.2.1#1.1)
    - [1.1.1A switch rendszerindítási sorrendje](https://contenthub.netacad.com/srwe-dl/1.1.1)
    - [1.1.2Egy boot rendszer parancs](https://contenthub.netacad.com/srwe-dl/1.1.2)
    - [1.1.3A kapcsoló LED-jelzőfényei](https://contenthub.netacad.com/srwe-dl/1.1.3)
    - [1.1.4Helyreállítás egy rendszerösszeomlás után](https://contenthub.netacad.com/srwe-dl/1.1.4)
    - [1.1.5A switch felügyeleti hozzáférése](https://contenthub.netacad.com/srwe-dl/1.1.5)
    - [1.1.6Példa a switch virtuális interfészének (SVI) beállítására](https://contenthub.netacad.com/srwe-dl/1.1.6)
    - [1.1.7Laborgyakorlat - A switch alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.1.7)
  + [1.2Switchportok vezérlésja](https://contenthub.netacad.com/srwe-dl/1.2.1#1.2)
    - [1.2.1Duplex kommunikáció](https://contenthub.netacad.com/srwe-dl/1.2.1)
    - [1.2.2Switchportok beállítása a fizikai rétegben](https://contenthub.netacad.com/srwe-dl/1.2.2)
    - [1.2.3Auto-MDIX](https://contenthub.netacad.com/srwe-dl/1.2.3)
    - [1.2.4A switch ellenőrzésére szolgáló parancsok](https://contenthub.netacad.com/srwe-dl/1.2.4)
    - [1.2.5A switchportok beállításainak ellenőrzése](https://contenthub.netacad.com/srwe-dl/1.2.5)
    - [1.2.6A hálózatelérési réteg problémái](https://contenthub.netacad.com/srwe-dl/1.2.6)
    - [1.2.7Az interfész bemeneti és kimeneti hibái](https://contenthub.netacad.com/srwe-dl/1.2.7)
    - [1.2.8A hálózatelérési réteg problémáinak hibaelhárítása](https://contenthub.netacad.com/srwe-dl/1.2.8)
    - [1.2.9Parancsszimulátor - Switchportok beállítása](https://contenthub.netacad.com/srwe-dl/1.2.9)
  + [1.3Biztonságos távoli hozzáférés](https://contenthub.netacad.com/srwe-dl/1.2.1#1.3)
  + [1.4A router alapbeállításainak megadása](https://contenthub.netacad.com/srwe-dl/1.2.1#1.4)
  + [1.5Közvetlenül csatlakozó hálózatok ellenőrzése](https://contenthub.netacad.com/srwe-dl/1.2.1#1.5)
  + [1.6Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/1.2.1#1.6)
* [2Fogalmak váltása](https://contenthub.netacad.com/srwe-dl/1.2.1#2)
* [3VLAN-ok](https://contenthub.netacad.com/srwe-dl/1.2.1#3)
* [4Inter-VLAN Routing](https://contenthub.netacad.com/srwe-dl/1.2.1#4)
* [5STP fogalmak](https://contenthub.netacad.com/srwe-dl/1.2.1#5)
* [6EtherChannel](https://contenthub.netacad.com/srwe-dl/1.2.1#6)
* [7DHCPv4](https://contenthub.netacad.com/srwe-dl/1.2.1#7)
* [8SLAAC és DHCPv6](https://contenthub.netacad.com/srwe-dl/1.2.1#8)
* [9FHRP koncepciók](https://contenthub.netacad.com/srwe-dl/1.2.1#9)
* [10LAN biztonsági koncepciók](https://contenthub.netacad.com/srwe-dl/1.2.1#10)
* [11Switch biztonságának beállítása](https://contenthub.netacad.com/srwe-dl/1.2.1#11)
* [12WLAN fogalmak](https://contenthub.netacad.com/srwe-dl/1.2.1#12)
* [13WLAN konfiguráció](https://contenthub.netacad.com/srwe-dl/1.2.1#13)
* [14Útválasztási fogalmak](https://contenthub.netacad.com/srwe-dl/1.2.1#14)
* [15IP statikus útválasztás](https://contenthub.netacad.com/srwe-dl/1.2.1#15)
* [16Statikus és alapértelmezett útvonalak hibaelhárítása](https://contenthub.netacad.com/srwe-dl/1.2.1#16)

1. Alapbeállítások
2. Switchportok konfigurációja

Switchportok vezérlésja

1.2.1

Duplex kommunikáció

A switch portjai független konfigurálhatók, a különböző igényeknek megfelelően. Ez a témakör a switchportok konfigurálását, ellenőrzését, a gyakori hibákat és a switch beállításával kapcsolatos problémák elhárítását ismerteti.

A teljes duplex (full-duplex) kommunikáció nem teszi lehetővé a sávszélesség kihasználását azáltal, hogy egy kapcsolat mindkét végén lehetővé teszi az adatok egyidejű küldését és fogadását. Ezt kétirányú kommunikációnak nevezik, és mikroszegmentációt igényel. Mikroszegmentált LAN akkor jön létre, amikor a switch minden portjára egyetlen eszköz csatlakozik, és a portok full-duplex módban üzemelnek. A teljes duplex üzemmódban működő switchporthoz nem tartozik ütközési tartomány.

A teljes duplex kommunikációval, a félduplex (half-duplex) kommunikáció egyirányú. A félplex kommunikáció teljesítményromlást okoz, mivel az adatok egyszerre csak egy irányban áramolhatnak, ami gyakori ütközéseket biztosít. A félduplex kapcsolatok jellemzően régebbi hardverekben (pl.: hub-okban) találhatók meg. A félduplex hubokat alapértelmezés szerint full-duplex kommunikációt használt kapcsolók váltották fel.

Az ábra a teljes és félduplex (full-duplex és half-duplex) kommunikációt szemlélteti.

Az ábra szemlélteti a két kapcsoló közötti full-duplex és félduplex kommunikáció közötti különbséget. A tetején látható diagram full-duplexet mutat, mindkét irányban nyilakkal a két kapcsoló közötti linken a következő szöveggel: Küldés ÉS fogadás, egyszerre. Az alsó diagram a félduplexet mutatja, és csak egy nyíl áramlik egyik kapcsolóról a másikra a következő szöveggel: Küldés VAGY fogadás.

PC4

**Full-duplex kommunikációFél-duplex kommunikáció**Küldés ÉS fogadás, egyszerreKüldés VAGY fogadás

A Gigabit Ethernet és a 10 Gb-es hálózati kártyák teljes duplex üzemmódot igényelnek a működésükhöz. Mivel teljes duplex módban az ütközést érzékelő áramkör a hálózati kártyán van tiltva, a full-duplex kapcsolat 10 százalékos hatékonyságot biztosít mindkét irányban (küldés és fogadás). Ez az sáv szélesség lehetséges felhasználásának megduplázódását adott módon.

1.2.2

Switchportok beállítása a fizikai rétegben

A kapcsoló portjait manuálisan be lehet állítani az egyedi duplexitás vagy sebességnek megfelelően. A switchport duplex üzemmódjának manuális megadásához használjuk a **duplex** interfészkonfigurációs parancsot. A sebesség manuális megadásához használjuk a **speed** interfészkonfigurációs parancsot. Például a topológiában látható mindkét switch-nek állandóan 100 Mbps sebességű full-duplex üzemmódban kell működni.

hálózati topológia, amely két, full-duplex módban 100/Mpbs sebességgel működő switch közötti kapcsolatot mutat

PC1PC2S1S2F0/18F0/1F0/1

Full-Duplex mód 100/Mbps.Full-Duplex mód 100/Mbps.

A táblázat az S1 parancsait mutatja. Ugyanazok a parancsok alkalmazhatók az S2 esetében is.

| TaskIOS CommandsEnter global configuration mode.S1# configure terminalEnter interface configuration mode.S1(config)# interface FastEthernet 0/1Configure az interfész duplex. duplex full Az interfész konfigurálásaS1(config-if)# sebesség. sebesség 100 Visszatérés a kiváltságos EXEC-hezS1(config-if)# mode.S1(config-if)# endSave the running config to the startup config.S1# copy running-config startup-config | |
| --- | --- |
| **Feladat** | **IOS parancsok** |
| Lépjünk be a globális konfigurációs módba. | S1# **configure terminal** |
| Lépjünk át interfészkonfigurációs módba. | S1(config)# **interface FastEthernet 0/1** |
| Állítsuk be az interfész duplexitását. | S1(config-if)# **duplex full** |
| Állítsuk be az interfész sebességét. | S1(config-if)# **speed 100** |
| Lépjünk vissza a privilegizált EXEC módba. | S1(config-if)# **end** |
| Mentsük el az aktuális konfigurációt indítási konfigurációként. | S1# **copy running-config startup-config** |

A Cisco Catalyst 2960 és 3560 switch-ek esetében a duplexitás és a sebesség automatikus felismerése az alapértelmezett beállítás. A 10/100/1000-es portok 10 vagy 100 Mbps sebességre állítva fél- vagy teljes duplex módban működnek, 1000 Mbps (1 Gbps) sebességre állítva pedig csak teljes duplex módban. Az automatikus egyeztetés akkor hasznos, ha a porthoz csatlakozó eszköz sebesség- és duplexbeállításai ismeretlenek vagy változhatnak. Ismert eszközök (pl.: szerverek, dedikált munkaállomások, hálózati eszközök) esetében célszerű a sebesség- és duplexbeállítások manuális megadása.

A switchportok hibaelhárításakor fontos, hogy ellenőrizzük a duplex- és sebességbeállításokat.

**Note**: Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues. Az automatikus egyeztetés hibája is okozhat ilyen nem megfelelő beállításokat.

All fiber-optic ports, such as 1000BASE-SX ports, operate only at one preset speed and are always full-duplex.

1.2.3

Auto-MDIX

Egészen a közelmúltig a készülékek egymáshoz csatlakoztatásához különböző típusú (egyenes- vagy keresztkötésű) kábelek voltak szükségesek. A switch-switch vagy a switch-router közötti kapcsolatokhoz másfajta Ethernet kábeleket kellett használni. Az auto-MDIX (automatic medium-dependent interface crossover, automatikus közegfüggő interfész fordítás) funkció kiküszöbölte ezt a problémát. Amikor az auto-MDIX engedélyezve van, az interfész automatikusan felismeri a szükséges kábeltípust (egyenes- vagy keresztkötés), majd a kapcsolatot ennek megfelelően konfigurálja. Az auto-MDIX funkcióval nem rendelkező kapcsolókhoz való csatlakozáskor egyeneskötésű (straight-through) kábelt kell alkalmaznunk az olyan eszközök esetében, mint a szerverek, a munkaállomások vagy a routerek. Keresztkötésű (crossover) kábelt kell alkalmazni másik switch-ek vagy repeaterek csatlakoztatásához.

Az auto-MDIX funkció engedélyezésével bármelyik kábeltípus használható más eszközökhöz való csatlakozáshoz, és az interfész automatikusan alkalmazkodik a sikeres kommunikációhoz. Az újabb Cisco switch-ek esetében az **mdix auto** interfészkonfigurációs parancs engedélyezi a funkciót. Ha egy interfészen az auto-MDIX engedélyezett, akkor a funkció megfelelő működéséhez az interfész sebességét és duplexitását **auto** értékre kell állítani.

Az auto-MDIX engedélyezésére szolgáló parancsot a switch interfészkonfigurációs módjában kell kiadni az ábrán látható módon:

S1(config-if)# **mdix auto**

**Note**: The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches but is not available on the older Catalyst 2950 and Catalyst 3550 switches.

Egy konkrét interfész auto-MDIX beállításainak vizsgálatához adjuk ki a **show controllers ethernet-controller** parancsot a **phy** kulcsszóval kiegészítve. A kimenet auto-MDIX vonatkozású sorainak a kiszűréséhez adjuk ki a **include MDIX** szűrőt. A kimenet az ábrán látható módon mutatja a funkció ki- vagy bekapcsolt állapotát.

S1# **show controllers ethernet-controller fa0/1 phy | include MDIX**

Auto-MDIX : On [AdminState=1 Flags=0x00052248]

1.2.4

A switch ellenőrzésére szolgáló parancsok

A táblázat a switch ellenőrzésére szolgáló hasznosabb parancsokat foglalja össze.

| TaskIOS CommandsDisplay interface status and configuration.S1# show interfészek [interface-id]Az aktuális indítási konfiguráció megjelenítése.S1 show# startup-configAz aktuális működési konfiguráció megjelenítése.S1 show# running-configDisplay information about flash file system.S1# show flashDisplay system hardware and software status.S1# show versionDisplay a beírt parancs előzményei.S1 előzmények megjelenítése IP információk megjelenítése egy# interface.S1 show ip interface [interface-id]A MAC cím megjelenítése# table.S1# show mac-address-tableORS1# show mac address-table | |
| --- | --- |
| **Feladat** | **IOS parancsok** |
| Az interfész állapotának és konfigurációjának megjelenítése. | S1# **show interfaces** [*interface-id*] |
| Az érvényben lévő indítási konfiguráció megjelenítése. | S1# **show startup-config** |
| Az érvényben lévő aktív konfiguráció megjelenítése. | S1# **show running-config** |
| A flash fájlrendszerrel kapcsolatos információk megjelenítése. | S1# **show flash** |
| A rendszer hardver- és szoftverállapotának megjelenítése. | S1# **show version** |
| A parancselőzmények megjelenítése. | S1# **show history** |
| Egy interfész IP-beállításainak megjelenítése. | S1# **show ip interface** [*interface-id*]  OR  S1# **show ipv6 interface** [*interface-id*] |
| A MAC-címtábla megjelenítése. | S1# **show mac-address-table**  OR  S1# **show mac address-table** |

1.2.5

A switchportok beállításainak ellenőrzése

A **show running-config** paranccsal ellenőrizhető, hogy a switch beállításai megfelelőek-e. Az alábbi ábrán a parancs kimenetének egy kivonata látható, amely a fontosabb információkat tartalmazza.

* A Fast Ethernet 0/18 interfész a 99-es felügyeleti VLAN-ra van beállítva.
* A 99-es VLAN a 172.17.99.11 255.255.255.255.255.0 IPv4-címmel van konfigurálva.
* Az alapértelmezett átjáró a 172.17.99.1 címre van beállítva.

S1# **show running-config**

Building configuration...

Current configuration : 1466 bytes

!

interface FastEthernet0/18

switchport access vlan 99

switchport mode access

!

(output omitted)

!

interface Vlan99

ip address 172.17.99.11 255.255.255.0

ipv6 address 2001:DB8:ACAD:99::1/64

!

ip default-gateway 172.17.99.1

A **show interfaces** egy másik gyakran használt parancs, amely a switch hálózati interfészeinek állapotára és statisztikáira vonatkozó információkat jeleníti meg. A **show interfaces** parancsot gyakran használjuk hálózati eszközök konfigurálása és megfigyelése során is.

A **show interfaces fastEthernet 0/18** parancs kimenetének első sora megmutatja, hogy a FastEthernet 0/18 interfész állapota "up/up", ami azt jelenti, hogy működik. Lejjebb az látható, hogy az interfész teljes duplex üzemmódban van, és a sebessége 100 Mbps.

S1# **show interfaces fastEthernet 0/18**

FastEthernet0/18 is up, line protocol is up (connected)

Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full-duplex, 100Mb/s, media type is 10/100BaseTX

1.2.6

A hálózatelérési réteg problémái

A **show interfaces** parancs hasznos az átviteli közeggel kapcsolatos gyakoribb problémák meghatározásához. Ennek a kimenetnek az egyik legfontosabb része a vonali és az adatkapcsolati protokoll állapotának megjelenítése, ahogy a példában is látható.

S1# **show interfaces fastEthernet 0/18**

FastEthernet0/18 is up, line protocol is up (connected)

Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

Az első paraméter (FastEthernet0/18 is up) a fizikai rétegre vonatkozik, és jelzi hogy az interfész megkapja-e a vivőérzékelő jelet. A második paraméter (line protocol is up) az adatkapcsolati rétegre vonatkozik, és azt jelzi, hogy az adatkapcsolati réteg protokollja fogad-e készenléti (keepalive) jeleket.

A **show interfaces** parancs kimenete alapján a lehetséges problémák a következőképpen javíthatók:

* Ha az interfész működik, de a vonali protokoll nem (up/down), akkor második rétegbeli hiba áll fenn. Lehetséges, hogy eltérő a beágyazás (encapsulation) típusa, a túloldal interfésze hiba miatt lekapcsolt (error-disabled) állapotban van, vagy hardveres probléma lépett fel.
* Ha sem a vonali protokoll, sem pedig az interfész nem működik (down/down), akkor a kábel nincs csatlakoztatva, vagy valamilyen más interfészprobléma áll fenn. Például, egy közvetlen (úgynevezett back-to-back) kapcsolat esetén a túloldali interfész adminisztratív úton lekapcsolt (administratively down) állapotban van. Ha az interfész leállítása adminisztratív úton történt (administratively down), akkor a \* If the interface is administratively down, it has been manually disabled (the **shutdown** utasítást adták ki az aktív konfigurációban.

A **show interfaces** parancs számlálókat és statisztikákat jelenít meg a FastEthernet 0/18 interfészről, amint az a példában is látható.

S1# **show interfaces fastEthernet 0/18**

FastEthernet0/18 is up, line protocol is up (connected)

Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full-duplex, 100Mb/s, media type is 10/100BaseTX

input flow-control is off, output flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00

Last input never, output 00:00:01, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

2295197 packets input, 305539992 bytes, 0 no buffer

Received 1925500 broadcasts (74 multicasts)

0 runts, 0 giants, 0 throttles

3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 74 multicast, 0 pause input

0 input packets with dribble condition detected

3594664 packets output, 436549843 bytes, 0 underruns

8 output errors, 1790 collisions, 10 interface resets

0 unknown protocol drops

0 babbles, 235 late collision, 0 deferred

Bizonyos közeghibák nem elég erősek, hogy az áramkör hibájához vezessenek, ugyanakkor okozhatnak hálózati teljesítménybeli problémákat. A táblázat néhány olyan gyakoribb hibát mutat be, amely a **show interfaces** parancs használatával felderíthető.

| Error TypeDescriptionInput ErrorsTotal number of errors. Ez magában foglalja a futást, giants, no buffer, CRC, frame, overrun, and ignored counts.RuntsPackets that are discarded because they are smaller than the minimum packet size for the átviteli közegbe. For instance, any Ethernet packet that is less than 64 bytes is futásnak tekinthető.GiantsPackets amiket eldobunk, mert meghaladják a maximális csomagméret a médiához. Például bármely Ethernet-csomag 1518 bájtnál nagyobb méret óriásinak számít.CRCCRC hibák keletkeznek amikor a számított ellenőrző összeg nem egyezik meg a kapott ellenőrzőösszeggel.Kimenet ErrorsSum of all errors that prevented the final transmission of datagrams ki a vizsgált felületről.Ütközések Üzenetek száma Ethernet-ütközés miatt újraküldve.Késői ütközésekEgyütközés that occurs after 512 bits of the frame have been transmitted. | |
| --- | --- |
| **Hibatípus** | **Leírás** |
| **Bemeneti hibák (Input Errors)** | A hibák összesített száma. Tartalmazza a futásokat, óriásokat, puffer nélküli, CRC-t, keret, túllépés és figyelmen kívül hagyott számok. |
| **Töredékek (runts)** | Frames that are discarded because they are smaller than the minimum keretméret a közepeshez. Például bármely Ethernet-keret 64 bájtnál kevesebbet futtatásnak tekintünk. |
| **Óriás keretek (giants)** | Keretek, amelyeket a rendszer eldob, mert meghaladja a maximális keretméretet a médium számára. Például bármely Ethernet-keret, amely nagyobb, mint 1518 bájt óriásinak számít. |
| **CRC** | CRC-hibák akkor keletkeznek, amikor a számított ellenőrző összeg nem egyezik meg a a kapott ellenőrző összeggel. |
| **Kimeneti hibák** | Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. |
| **Ütközések (collisions)** | Ethernet ütközés miatt újraküldött üzenetek száma. |
| **Késői ütközések (late collisions)** | A collision that occurs after 512 bits of the frame have been transmitted. |

1.2.7

Az interfész bemeneti és kimeneti hibái

A bejövő hibák (input errors) számláló az összes, a vizsgált interfészre darab hibás adatcsomagszámát adja meg. Ez magában foglalja a következő számlálókat: töredékek (runts), óriások (giants), CRC, nincs puffer (no buffer), keret (frame), túllépett (overrun), és mellőzött (ignored). A **show interfaces** parancs által jelzett bemeneti hibák a következők:

* **Runt Frames** – A 64 bájtos minimális megengedett hossznál rövidebb Ethernet-kereteket futtató kereteknek nevezzük. Számuk túlzott növekedését általában egy hibásan működő hálózati kártya okozza, de keletkezhetnek a gyakori ütközések eredményeképpen is.
* **Óriások** – A megengedett legnagyobb méretnél nagyobb Ethernet kereteket óriásoknak nevezzük.
* **CRC hibák** – Ethernet és soros interfészeken a CRC hibák általában adathordozó- vagy kábelhibára utalnak. A Gyakori okok közé tartozik az elektromos interferencia, a laza vagy sérült csatlakozások, valamint a nem megfelelő kábelezés. Ha sok CRC-hibát látunk, akkor túl sok a zaj a linken, és meg kell vizsgálni a kábelt. Meg kell keresni a lehetséges zajforrásokat is, és meg kell azokat szüntetni.

A kimeneti hibák (output errors) számláló összes olyan hiba összege, amely azt mondta, hogy a vizsgált interfészről az adatcsomagok végső kiküldését. A **show interfaces** által jelzett kimeneti hibák a következők:

* **Ütközések** – A félduplex műveletek ütközései normálisak. Teljes duplex kommunikációra beállított interfézen viszont soha nem szabad ütközéseket látni.
* **Késői ütközések** – A késői ütközés olyan ütközésre utal, amely a keret 512 bitjének átvitele után következik be. A késői ütközés egyik leggyakoribb előidézője a kábelezés túl hosszú méretet. Egy másik gyakori ok pedig a duplexitás hibás beállítása. Például, akkor lehet ilyen probléma, ha a kapcsolat egyik végén teljes duplex, míg a másikon félduplex beállítás található. Azon az interfészek láthatók a késői ütközések, amelyek félduplexek van konfigurálva. A hiba kijavítása érdekében mindkét oldalon ugyanazt a duplexitást kell beállítani. Egy helyesen megtervezett és kialakított hálózatban soha nem fordulhat elő késői ütközés.

1.2.8

A hálózatelérési réteg problémáinak hibaelhárítása

A kapcsolt hálózat teljesítményét a legtöbb probléma már a telepítés során felmerülhet. Elméletileg, a telepítés után egy hálózat gond nélkül működik tovább. Azonban sérülhet a kábelezés, változhat a vezérlő, és olyan új eszköz is csatlakozhat a switch-hez, amelyik beállítást igényel. Ezért szükséges a hálózat folyamatos karbantartása és hibaelhárítása.

Ha nincs vagy hibás egy csatlakozás a switch és egy másik eszköz között, akkor az elhárítás során kövessük az alábbi ábrán látható általános hibakeresési folyamatot.

Az ábra egy folyamatábra a rossz kapcsolat vagy a hálózati eszközök közötti kapcsolat hiánya hibaelhárításához. A legfelső lépés az interfészek megjelenítése. Ebből következik a kérdés, hogy az interfész fent van? Ha a válasz nem, akkor ez a következő lépésekből áll: ellenőrizze a megfelelő kábeleket; ellenőrizze a kábelek és csatlakozók sérülését; és ellenőrizze, hogy a sebesség mindkét végén megfelelően van-e beállítva. Ha a válasz igen, akkor ez a következő lépésekhez vezet: vannak-e jelek EMI-re/zajra? Ha igen, távolítsa el a forrásokat; és ellenőrizze, hogy a duplex beállítás mindkét végén megfelelően van-e beállítva. Ezek arra a kérdésre vezetnek, hogy megoldódott-e a probléma? Ha a válasz nem, akkor a következő lépés az elvégzett munka dokumentálása és a probléma eszkalálása. Ha a válasz igen, akkor kész.

Adjuk ki a **show interfaces** parancsot.Működik az interfész?Megoldódott a probléma?

* Van EMI- vagy zajforrás a közelben? Ha igen, akkor távolítsuk al a forrást.
* Ellenőrizzük, hogy a duplexitás beállítása megfelelő-e mindkét oldalon.

Dokumentáljuk az elvégzett munkákat, és eszkaláljuk a problémát.Kész

* Ellenőrizzük a kábelezés megfelelőségét.
* Ellenőrizzük a kábelek és csatlakozók sértetlenségét.
* Ellenőrizzük a sebesség megfelelő beállítását mindkét végén.

IgenIgenNemNem

Az interfészek állapotának ellenőrzéséhez használjuk a **show interfaces** parancsot.

Az interfés nem működik (down állapot):

* Győződjünk meg arról, hogy a kábeleket használjuk-e, valamint ellenőrizzük a kábel és a megfelelő csatlakozók épségét. Ha rossz vagy nem megfelelő a kábel, akkor cseréljük ki.
* akkor az interfés még mindig nem működik, akkor a probléma oka az eltérő sebességbeállítás lehet. Az interfés sebessége általában kerül konfigurálásra. Ha az egyik interfész mégis manuálisan beállítva, akkor ettől függetlenül egy másik oldalt használhatja az automatikusan beállítást. Ha sebességbeli eltérés lép fel hibás beállítás, esetleg valamilyen hardver- vagy szoftver probléma miatt, az okozhatja az interfész leállását. Ilyen jellegű probléma lehetséges, akkor állítsuk be kézzel ugyanazt a sebességet mindkét oldalon!

Az interfész működik, de a kapcsolat problémái továbbra is fennállnak:

Adjuk ki a \* A **show interfaces** segítségével parancsot a túlzottan zajos közeg ellenőrzésére. Ezt jelezheti a töredék-, óriás- és a CRC-hibák számlálóinak növekedése. Ha túl zajos az átviteli közeg, először találjuk meg és távolítsuk el a zaj forrását, amely lehetséges. Vizsgáljuk meg, hogy a kábelhossz nem haladja meg a maximálisan engedélyezett értéket, és ellenőrizzük a használt kábel típusát is.

* Ha nem a zaj okozza a problémát, akkor ellenőrizzük az ütközések mértékét. Ha ütközések, vagy késői ütközések, akkor nézzük meg a két végén a duplex beállításokat. A sebességbeállításhoz hasonlóan a duplexitás beállítása is rendszerint automatikus egyeztetésen alapul. Ez az eltérő duplexitás lehet a probléma, akkor manuálisan állítsuk be azt a kapcsolat mindkét oldalán.

## Parancsszimulátor - Switchportok beállítása

Állítsunk be egy switchportot a meghatározott követelmények alapján.

Lépjen be a konfigurációs módba, és állítsa a FastEthernet0/1 duplex, speed és MDIX paramétereket automatikusra, majd mentse a konfigurációt az NVRAM-ba.

S1#konfigurálja a terminált

Adja meg a konfigurációs parancsokat, soronként egyet. Vége a CNTL/Z-vel.

S1(config)#interfész FastEthernet0/1

S1(config-if)#duplex auto

S1(config-if)#sebességű automata

S1(config-if)#mdix auto

Lépjen ki az interfész konfigurációs módból, és mentse a konfigurációt NVRAM-ba.

S1(config-if)#vége

%SYS-5-CONFIG\_I: Konzolról konzolra konfigurálva

S1#másolja a running-config startup-config

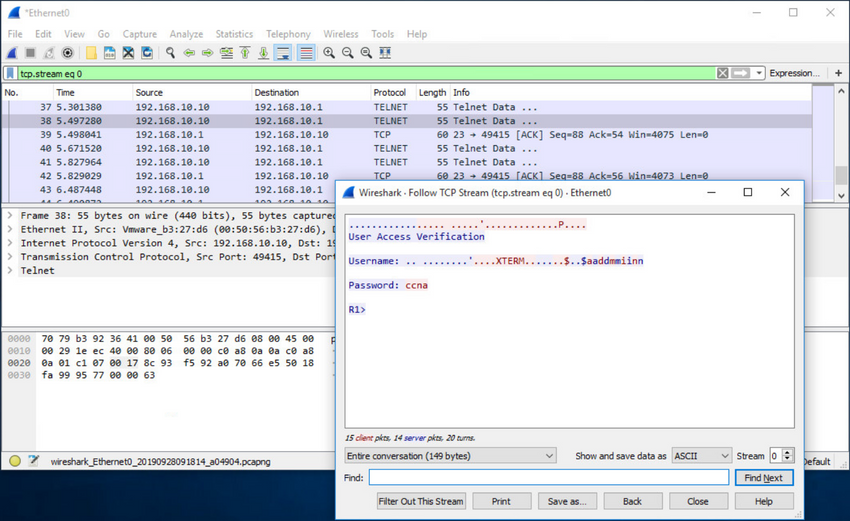
Sikeresen konfigurálta a duplex, a sebesség és az Auto-MDIX beállításokat egy kapcsolófelületen, és elmentette a konfigurációt az NVRAM-ba.

A Telnet működése

Előfordulhat, nem mindig van közvetlen hozzáférésünk ahhoz, hogy a switch-hez, hogy adott konfigurálnunk kell. Távolról is kell tudni férni és elengedhetetlen, hogy ez a hozzáférés biztonságos legyen. Ez a témakör a Secure Shell (SSH) alapú távoli hozzáférési beállításával foglalkozik. Egy Packet Tracer feladatai biztosítják arra, hogy ezt magunk is kipróbáljuk.

A Telnet a 23-as TCP-portot használja. Ez egy régebbi jegyzőkönyv, amely mind a kijelentkezés hitelesítését (felhasználónév és jelszó), mind pedig az adatokat egy nem biztonságos, titkosított formában továbbítja a kommunikáló eszközök között. Egy támadó képes így a csomagokat a Wireshark segítségével megfigyelni. Az ábrán például a támadó elfogja az **admin** felhasználónevet és a **ccna** jelszót egy Telnet kapcsolatból.

képernyőkép egy Telnet munkamenet WireShark-rögzítéséről, amely az egyszerű szövegben elküldött felhasználónevet és jelszót mutatja



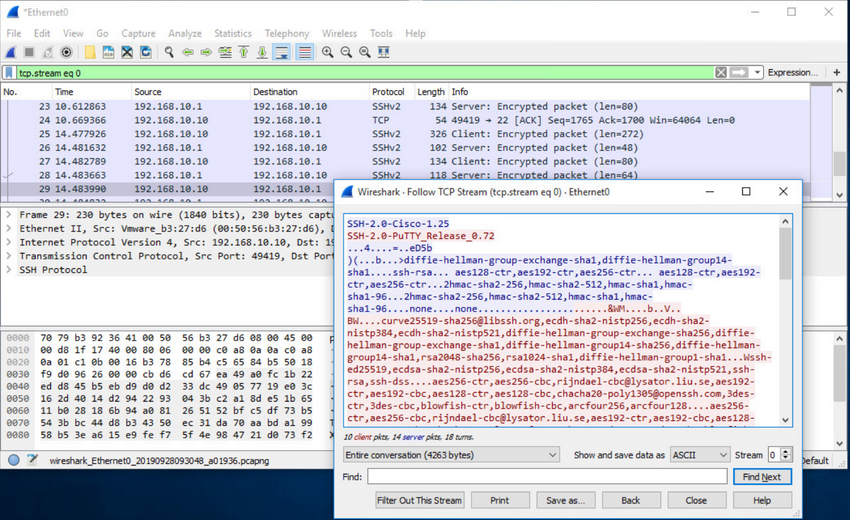
1.3.2

Az SSH működése

A Secure Shell (SSH) egy biztonságos protokoll, amely 22-es TCP-portot használ. Biztonságos (titkosított) felügyeleti biztosíték egy távoli eszközhöz. Az SSH-nak át kell vennie a Telnet szerepét a felügyeleti kapcsolatokban. Az SSH biztonságos távoli kapcsolatokat valósít meg, mert erős titkosítást használ mind a hiteleshez (felhasználónév és jelszó kezelése), mind pedig a kommunikáló eszközök közötti adatátvitelhez.

Az ábra például egy SSH-munkamenet Wireshark által történő elfogását mutatja. A támadó képes a felügyelt eszköz IP-címe alapján elfogni a munkamenetet. A Telnet megoldásával szemben viszont az SSH-ban a felhasználónév és a titkosított jelszó.

képernyőkép egy SSH-munkamenet WireShark-rögzítéséről, amelyen a felhasználónév és a jelszó titkosítva van



1.3.3

A switch SSH-támogatottságának ellenőrzése

Ahhoz, hogy engedélyezzük az SSH-t egy Catalyst 2960 switch esetében, az eszköznek kriptográfiai (titkosítási) funkciókkal és képességekkel rendelkező IOS-t kell futtatnia. Adjuk ki a **show version** parancsot a switch által éppen futtatott IOS képernyőt. Az IOS nevében szereplő "k9" szövegrészlet a kriptográfiai (titkosítási) funkciók és képességek támogatását jelenti. A példa a **show version** parancs kimenetét mutatja.

S1# **show version**

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE (fc1)

1.3.4

Az SSH beállítás

Az SSH konfigurálása előtt a switch-en legalább a megfelelő hálózati paramétereket kell beállítani.

Az SSHvezérlős lépéseinek megismeréséhez kattintsunk az egyes gombokra!

1. lépés

2. lépés

3. lépés

4. lépés

5. lépés

6. lépés

**1. lépés az SSH-támogatást.**A **show ipssh** paranccsal mondja, hogy a kapcsoló támogatja-e az SSH-t.

Ha a kapcsoló által futtatott IOS nem támogatja a titkosítási funkciókat, akkor az eszköz ezt a parancsot nem fogja felismerni.

S1# **show ip ssh**

1.3.5

Az SSH működésének ellenőrzése

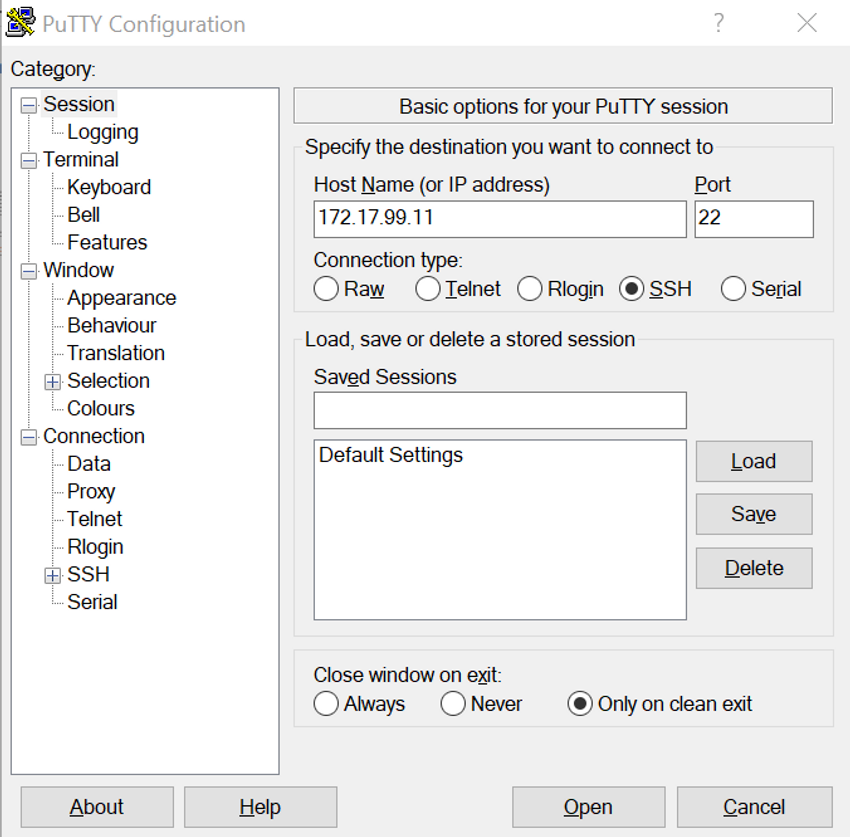
A számítógépen egy SSH-kliensprogram (pl.: PuTTY) segítségével lehet csatlakozni egy SSH-szerverhez. Tegyük fel például, hogy a következők vannak konfigurálva:

* Az SSH engedélyezve van az S1 switch-en.
* A VLAN 99 interfészhez (SVI) a 172.17.99.11 IPv4-es cím lett hozzárendelve az S1 switch-en.
* A PC1 IPv4-es címe: 172.17.99.21.

Az ábra a PC1 PuTTY beállításait mutatja az SSH-kapcsolat kezdeményezéséhez az S1 SVI VLAN IPv4-címéhez.

The figure shows a host connected to a switch and the PuTTY settings to initiate an SSH connection to the SVI of the switch. Host PC1, with address 172.17.99.21, has a network connection to a switch S1, with address 172.17.99.11. A screenshot of the PuTTY configuration on PC1 shows the address 172.17.99.11 entered in the box under Host Name (or IP address) and 22 entered in the box under Port. SSH has been selected as the connection type.

172.17.99.11172.17.99.21PC1S1



Csatlakozáskor a felhasználónak meg kell adni egy felhasználónevet és egy jelszót, a példában látható módon. Az előző példát használva az **admin** felhasználónevet és a **ccna** jelszót kell megadni. A helyes beállítás megadása után a felhasználó SSH-n keresztül csatlakozik a Catalyst 2960 switch parancssori felületéhez (CLI).

Login as: **admin**

Using keyboard-interactive

Authentication.

Password:

S1> **enable**

Password:

S1#

Az SSH verzió- és beállításs adatainak térképéhez az SSH-szerverként használt eszközön adjuk ki a **show ip ssh** parancsot. A példában az SSH 2-es verziója van engedélyezve.

S1# **show ip ssh**

SSH Enabled - version 2.0

Authentication timeout: 120 secs; Authentication retries: 3

To check the SSH connections to the device, use the show ssh command as shown.

S1# **show ssh**

%No SSHv1 server connections running.

Connection Version Mode Encryption Hmac State Username

0 2.0 IN aes256-cbc hmac-sha1 Session started admin

0 2.0 OUT aes256-cbc hmac-sha1 Session started admin

S1#

A router alapbeállításainak megadása

1.4.1

A router alapvető beállításainak megadása

Ez a fejezet eddig csak a switch-ekkel foglalkozott. Ha olyan eszközre van szükségünk, amely a hálózatunkon kívülre is képes adatot küldeni vagy onnan fogadni, akkor routert kell konfigurálnunk. Ez a témakör a router alapbeállításainak megadását mutatja be, és két parancsszimulátort, valamint egy Packet Tracer feladatot is tartalmaz, így gyakorolhatjuk is ezeket a készségeket.

A Cisco routerek és switch-ek sok hasonlóságot mutatnak. Hasonló operációs rendszert használnak, hasonló a parancsok szerkezete, sőt, számos parancsuk meg is van. csomag mindkét eszköztípus alapbeállítási lépései is hasonlóak. A következő suunnitelmas példája mindkettőnél el kell végezni. Nevezzük el az eszközt, hogy megkülönböztethető legyen a többi router-től, és állítsunk be jelszavakat is, ahogy az alábbi ábrán is látható.

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **hostname R1**

R1(config)# **enable secret class**

R1(config)# **line console 0**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)# **service password-encryption**

R1(config)#

Állítsunk be az ábrán látható módon egy bejelentkezési üzenetet, amely figyelmeztet egy esetleges jogosulatlan hozzáférésre.

R1(config)# **banner motd #Authorized Access Only!#**

R1(config)#

Mentsük el a változtatásokat az ábrán látható módon.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

1.4.2

Parancsszimulátor - A router alapbeállításainak megadása

Ebben a parancsszimulátorban az R2 alapbeállításait fogjuk megadni.

**Lépjen be a globális konfigurációs módba, és nevezze el az R2** útválasztót .

Az űrlap teteje

Router#



Az űrlap alja

VisszaállításMutasd meg nekemMutasd az összeset

1.4.3

Dual stack topológia

A switch-ek és a routerek közötti egyik megkülönböztető jellemző az általuk támogatott interfészek típusai. A második rétegbeli switch-ek például LAN-okat támogatnak, ezért több FastEthernet vagy Gigabit Ethernet porttal rendelkezik. Az ábrán látható dual stack (kettős verem) topológia a router interfészek IPv4-es és IPv6-os konfigurációjának bemutatására szolgál.

kettős veremű hálózati topológia, amely több gazdagépből, kapcsolóból és útválasztóból áll, IPv4 és IPv6 címekkel egyaránt konfigurált interfészekkel

PC1PC2PC3PC4S1S2S4R1R2.10.10.10.10::10::10::10::10192.168.10.0/24192.168.11.0/2410.1.1.0/2410.1.2.0/242001:db8:acad:1::/642001:db8:acad:2::/642001:db8:acad:4::/642001:db8:acad:5::/64G0/0/0G0/0/0G0/0/1G0/0/1209.165.200.224/302001:db8:acad:3::/64.1::1.1::1.1::1.1::1.225::225.226::226S0/1/0S0/1/0S3

1.4.4

Router interfészek konfigurálása

A routerek LAN-okat és WAN-okat támogatják és különböző típusú hálózatokat kötnek össze, ezért számos interfésztípust támogatnak. Például a G2 ISR-eknek egy vagy kettő beépített Gigabit Ethernet interfészük van, valamint nagy sebességű WAN kártyafoglalat is (High-Speed ​​WAN Interface Card, HWIC), amelyek más típusú hálózatokat is képesek kezelni, ilyenek a soros, a DSL és a kábeltévés kapcsolatok .

Egy interfész működéséhez a következől kellenek:

* **Legalább egy IP-címmel konfigurálva** – Használja az **ip***-cím ip-cím alhálózati maszk* és az **ipv6-cím***ipv6-cím/előtag* csatoló konfigurációs parancsait. Aktivált leállítás nincs leállítási parancs.\* \* **\* - Alapértelmezés szerint a LAN és a WAN interfészek nincsenek aktiválva (\*\*** ). Az interfész engedélyezéséhez a \*\*\*\* (Ez hasonló az interfészkapcsolásához.) segítségével kell aktiválni. Ahhoz, hogy egy interfészen valóban aktív legyen, azt egy másik eszközhöz (hub, switch vagy egy másik router) is csatlakoztatni kell.
* **Leírás** – Opcionálisan a felület konfigurálható egy legfeljebb 240 karakteres rövid leírással is. Célszerű minden egyes interfészhez leírást is megadni. Egy hálózatban működő interfészleírások előnye hamar nyilvánvalóvá válik, mivel a hibakeresést, valamint a harmadik féltől bejövő kapcsolatokat és azok kapcsolattartóinak beazonosítását.

Az alábbi példa az R1 router interfészeinek beállítását mutatja be.

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **ip address 192.168.10.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **description Link to LAN 1**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ip address 192.168.11.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:2::1/64**

R1(config-if)# **description Link to LAN 2**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **ip address 209.165.200.225 255.255.255.252**

R1(config-if)# **ipv6 address 2001:db8:acad:3::225/64**

R1(config-if)# **description Link to R2**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)#

1.4.5

Parancsszimulátor - Router interfészek konfigurálása

Ebben a parancsszimulátorban az R2 interfészeinek IPv4-es és IPv6-os beállításait adhatjuk meg.

A GigabitEthernet 0/0/0 konfigurálása.

* **A g0/0/0** gombbal lépjen be az interfész konfigurációs módba.
* Konfigurálja a **10.1.1.1** IPv4-címet és a **255.255.255.0** alhálózati maszkot .
* Állítsa be az IPv6-címet **2001:db8:acad:4::1/64** .
* A hivatkozás leírása: **Link a LAN-hoz 3** .
* Aktiválja a felületet.

Az űrlap teteje

Router(config)#



Az űrlap alja

VisszaállításMutasd meg nekemMutasd az összeset

1.4.6

IPv4-es loopback interfészek

A Cisco IOS routerek egy másik gyakori beállítása a loopback interfész engedélyezése.

A loopback interfész a router belső, logikai interfése. Egyetlen fizikai porthoz sincs hozzárendelve, ezért másik eszközzel sem csatlakoztatható hozzá. Ez egy szoftveres interfésznek, amely segítségével „up” állapotba kerül, amíg csak a router működik.

A loopback interfész hasznos segítség lehet a Cisco IOS eszközök tesztelése és felügyelete során, mert így biztosítható, hogy legalább egy interfész mindig elérhető legyen. Tesztelhetjük vele például a belső irányítási folyamatokat úgy, hogy a router mögött lévő hálózatokat emulálunk vele.

A loopback interfészeket gyakran használjuk laborkörnyezetben további interfészek létrehozására. Létrehozhatunk például több loopback interfészt egy routeren, hogy hálózatokat szimuláljunk telepítéss vagy tesztelési célból. Ebben a tananyagban gyakran használunk loopback interfészeket az internetes kapcsolat szimulálására.

Egy loopback cím engedélyezése és beállítása:

Router(config)# **csatoló visszahurkolási**  *száma*

Router(config-if)# **IP-cím**  *ip-cím alhálózati maszk*

Egy routeren több loopback interfész engedélyezhető. Egy loopback interfész IPv4-es címének egyedinek kell lenni, azt nem más interfész nem használhatja, mint ahogy az alábbi példakonfigurációban is látható az R1 router loopback 0 interfése esetén.

R1(config)# **interface loopback 0**

R1(config-if)# **ip address 10.0.0.1 255.255.255.0**

R1(config-if)# **exit**

R1(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

Közvetlenül csatlakozó hálózatok ellenőrzése

1.5.1

Interfészellenőrző parancsok

Nincs sok értelme routert konfigurálni, ha nem ellenőrizzük a beállításokat és a kapcsolatokat. Ez a témakör a közvetlenül csatlakoztatott hálózatok ellenőrzésére szolgáló parancsokat tárgyalja. Két parancsszimulátort és egy Packet Tracer feladatot tartalmaz.

Számos **show** parancs használható egy interfész működésének és beállításának ellenőrzésére. Az ábrán látható topológia a router interfész-beállításainak ellenőrzését szemlélteti.

PC1PC2PC3PC4S1S2S4R1R2.10.10.10.10::10::10::10::10192.168.10.0/24192.168.11.0/2410.1.1.0/2410.1.2.0/242001:db8:acad:1::/642001:db8:acad:2::/642001:db8:acad:4::/642001:db8:acad:5::/64G0/0/0G0/0/0G0/0/1G0/0/1209.165.200.224/302001:db8:acad:3::/64.1::1.1::1.1::1.1::1.225::225.226::226S0/1/0S0/1/0S3

A következő parancsok különösen hasznosak egy interfésznek gyors meghatározásához:

* **show ip interface brief** és **show ipv6 interface brief** - Ezek a parancsok minden interfésznek megjelenítése az összefoglalóba, az interfész IPv4-es és IPv6-os címét, valamint a pillanatnyi állapotát.
* **show running-config interface***interface-id* - Megmutatja az adott interfészre kiadott parancsokat.
* **show ip route** és **show ipv6 route** - Ezek a RAM-ban tárolt IPv4 vagy IPv6 útválasztási táblát jelenítenek meg. A Cisco IOS 15 rendszerben az aktív interfészeknek meg kell jelenniük az útválasztási táblázatban két kapcsolódó bejegyzéssel, amelyet a ' **C** ' (csatlakoztatva) vagy' **L** ' (helyi) kód azonosít. A korábbi IOS verziókban csak egyetlen bejegyzés jelenik meg a ' **C** ' kóddal.

1.5.2

Az interfész állapotának ellenőrzése

A **show ip interface brief** és **show ipv6 interface** shortokkal egy router minden interfészének állapotát gyorsan parancsolhatjuk. Ellenőrizhetjük, hogy az interfészek aktívak-e és működnek-e, ahogyan azt az ábrán a "Status/up" és a "Protocol/up" jelzi. Az ettől eltérő kimeneti beállításval vagy a kábelezéssel kapcsolatos problémára utal.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 192.168.10.1 YES manual up up

GigabitEthernet0/0/1 192.168.11.1 YES manual up up

Serial0/1/0 209.165.200.225 YES manual up up

Serial0/1/1 unassigned YES unset administratively down down

R1# **show ipv6 interface brief**

GigabitEthernet0/0/0 [up/up]

FE80::7279:B3FF:FE92:3130

2001:DB8:ACAD:1::1

GigabitEthernet0/0/1 [up/up]

FE80::7279:B3FF:FE92:3131

2001:DB8:ACAD:2::1

Serial0/1/0 [up/up]

FE80::7279:B3FF:FE92:3130

2001:DB8:ACAD:3::1

Serial0/1/1 [down/down] Unassigned

1.5.3

IPv6 link-local és multicast címek ellenőrzése

A **show ipv6 interface brief** parancs kimenete interfészenként két konfigurált IPv6-címet jelenít meg. Az egyik a kézzel beállított globális egyedi (unicast) IPv6-os cím. A másik, FE80-nal kezdődő cím pedig az interfész link-local egyedi címe. A link-local cím létrejön minden interfészhez, amely globális egyedi címet állítunk be. Egy IPv6 hálózati interfésznek kell lennie link-local címének, de globális egyedi cím nem szükséges.

A **show ipv6 interface gigabitethernet 0/0/0** parancs az interfész állapotát és az interfészhez tartozó összes IPv6-os címet jeleníti meg. A link-local és a globális egyedi cím mellett a kimenet még az interfészhez rendelt multicast címeket is, ezek az ábrán FF02 előtaggal kezdődnek.

R1# **show ipv6 interface gigabitethernet 0/0/0**

GigabitEthernet0/0/0 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64

Joined group address(es):

FF02::1

FF02::1:FF00:1

FF02::1:FF92:3130

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ICMP unreachables are sent

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

1.5.4

Az interfészszabályozás ellenőrzése

A **show running-config interface** parancs kimenete a megfelelően interfészre kiadott aktuális jeleníti meg az ábrának megfelelő parancsokat.

R1 **show running-config interface gigabitethernet 0/0/0**

Building configuration...

Current configuration : 158 bytes

!

interface GigabitEthernet0/0/0

description Link to LAN 1

ip address 192.168.10.1 255.255.255.0

negotiation auto

ipv6 address 2001:DB8:ACAD:1::1/64

end

R1#

A következő két parancs segítségével részletesebb információkat kaphatunk az interfészről:

* **show interfaces** -Az eszköz valamennyi interfészére jelenít meg rendelkezésre álló és adatforgalmi számlákat.
* **show ip interface** and **és show ipv6 interface** - Megjelenítik az IPv4-hez és IPv6-hoz kapcsolódó forgalmat a router összes interfészére adja meg.

1.5.5

Útvonalak ellenőrzése

A **show ip route** és **show ipv6 route** parancsok kimenete megmutatja a három elérhető hálózatot és a három helyi útvonal bejegyzését, ahogy az a példában látható. A helyi localhost útvonal adminisztratív távolsága 0. A maszkja IPv4 esetében /32, IPv6 esetében pedig /128. A helyi localhost útvonal a router IP-címet birtokló útvonalához tartozik. Ezt a router az adott IP-címre küldött csomagok feldolgozásához használja.

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.11.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.11.1/32 is directly connected, GigabitEthernet0/0/1

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/30 is directly connected, Serial0/1/0

L 209.165.200.225/32 is directly connected, Serial0/1/0

R1# **show ipv6 route**

IPv6 Routing Table - default - 7 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C 2001:DB8:ACAD:1::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via GigabitEthernet0/0/0, receive

C 2001:DB8:ACAD:2::/64 [0/0]

via GigabitEthernet0/0/1, directly connected

L 2001:DB8:ACAD:2::1/128 [0/0]

via GigabitEthernet0/0/1, receive

C 2001:DB8:ACAD:3::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:3::1/128 [0/0]

via Serial0/1/0, receive

L FF00::/8 [0/0]

via Null0, receive

R1#

Az irányítótáblában az útvonal előtti **C** azt jelzi, hogy ez egy közvetlenül csatlakoztatott hálózat. Ha a router interfése egyedi globális címmel van konfigurálva és "up/up" állapotban van, akkor az IPv6-os előtag (prefix) és a prefix hosszaott útvonalként kerül be az IPv6-os irányítótáblába.

Az interfészek konfigurációja IPv6-os globális egyedi cím szintén bekerül az irányítótáblába, mint helyi útvonalon. A helyi útvonal előtagja /128. A helyi útvonalakat a router arra használja, hogy kritikán dolgozza fel valamely saját interfészének címzett csomagokat.

A **ping** parancs IPv6 esetén is használható, mint IPv4-ben, csak itt IPv6-os címet adunk meg. Ahogy az ábrán is látható, a **ping** parancsot az R1 és a PC1 közötti harmadik rétegbeli kapcsolat ellenőrzésére használjuk.

R1# **ping 2001:db8:acad:1::10**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

1.5.6

A show parancsok kimenetének szűrése

A több képernyőnyi kép kimenetet kimenető parancsok alapértelmezésben 24 soronként megáll. A megállított szöveg végén a --More-- (--Több--) szöveg látszik. Az **Enter** billentyűre a következő sor, míg a szóköz billentyű lenyomására egy következő szakasz meg. A **terminál hossza** paranccsal beállíthatjuk a megjeleníteni kívánt sorok mennyiségét. Ha nullát (0) adunk meg, akkor a router nem fogja megállítani a kimeneti futását képernyőoldalanként.

Egy másik nagyon hasznos funkció, amely javítja CLI használhatóságát, a **show** parancsok kimenetének szűrése. A szűrőparancsok segítségével a kimenet meghatározott szakaszai jeleníthetők meg. Szűrési parancs létrehozásához gépeljük be a "cső" vagy "pipe" ( **|** ) karaktert a **show** parancs után, majd adjunk meg egy szűrési paramétert és egy kifejezést.

Négyféle szűrési paraméter van, amit a "cső" után beállíthatunk.

A szűrési parancsok megismeréséhez kattintsunk az egyes gombokra!

Rész

tartalmazza

kizárni

kezdődik

**szakasz**

Megjeleníti a teljes részt, amely a szűrőkifejezéssel kezdődik, ahogy a példában is látható.

R1# show running-config | szakasz vonal vty sor vty 0 4 jelszó 7 110A1016141D bejelentkezés szállítás bevitel összes

**Megjegyzés** : Kimeneti szűrőt minden **show** parancshoz használhatóunk.

1.5.7

Parancsszimulátor - A show parancsok kimenetének szűrése

Ebben a parancsszimulátoros feladatban show parancsok kimenetét fogjuk szűrni.

Írja be a parancsot a show running-config kimenetének szűréséhez a „line con” szakaszhoz.

R1#show running-config | szakasz vonal kon

vonal con 0

jelszó 7 05080F1C2243

szállítási bemenet nincs

Írja be a parancsot a "le" interfészek szűréséhez a rövid listában.

R1#ip interfész rövid megjelenítése | tartalmazza le

Serial0/1/1 unassigned NO unset down down

Írja be a parancsot a „fel” interfészek kizárásához a rövid listában.

R1#ip interfész rövid megjelenítése | kizárja fel

Az interfész IP-címe rendben van? Method Status Protocol

Serial0/1/1 unassigned NO unset down down

Írja be a parancsot, hogy a show running-config kimenetet a „sor” szóval kezdje.

R1#show running-config | kezdősor

vonal con 0

jelszó 7 05080F1C2243

szállítási bemenet nincs

stopbit 1

sor vty 0 4

jelszó 7 110A1016141D

Belépés

szállítási bemenet minden

Sikeresen végrehajtotta a szűrt show parancsokat.

VisszaállításMutasd meg nekemMutasd az összeset

1.5.8

Parancselőzmények

A parancselőzmények funkció hasznos, mert ideiglenesen tárolja a korábban végrehajtott parancsok utasításait, majd később elő lehet hívni.

Az előzménypufferben lévő utasítások előhívásához használjuk a **Ctrl** + **P** billentyűkombinációt vagy az **Up Arrow** billentyűt. A parancskimenet a legutóbb használt utasítással kezdődik. A gomb ismételt megnyomásával az egyre régebben használt parancsokat hozhatjuk elő. Az előzménypufferben lévő későbbi parancsok előhívására használjuk a **Ctrl** + **N** billentyűkombinációt vagy a **Down Arrow** billentyűt. Ismételt megnyomásra az egyre újabb parancsokat fogjuk kapni.

A parancselőzmények funkció alapértelmezés szerint engedélyezve van, és a rendszer a legutóbb használt 10 parancsot őrzi meg az átmeneti tárolójában. A privilegizált EXEC mód **show history** parancsával tudjuk az előzménypuffer tartalmát megjeleníteni.

Hasznos lehet megnövelni az aktuális munkamenet eltárolandó parancsainak számára vonatkozó értéket. Használjuk a felhasználói EXEC mód **termináltörténet mérete** parancsát a puffer méretének növeléséhez vagy csökkentéséhez.

Az ábrán a **terminál történelem mérete** és a **show történelem** parancsokra látható példát.

R1# **terminal history size 200**

R1# **show history**

show ip int brief

show interface g0/0/0

show ip route

show running-config

show history

terminal history size 200

1.5.9

Parancsszimulátor - Parancselőzmények

Ebben a parancsszimulátoros feladatban a parancselőzmények funkciót fogjuk használni.

Írja be a parancsot, hogy a parancselőzmények sorainak számát 200-ra állítsa.

R1>termináltörténet mérete 200

Írja be a parancsot a parancselőzmények megjelenítéséhez.

R1>mutasd meg a történelmet

show running-config | szakasz vonal kon

ip interfész rövid megjelenítése | tartalmazza le

ip interfész rövid megjelenítése | kizárja fel

show running-config | kezdősor

termináltörténet mérete 200

mutasd meg a történelmet

R1>

Sikeresen beállította és megjelenítette a parancselőzményeket.

## Miről tanultunk ebben a fejezetben?

**Konfiguráljon egy kapcsolót a kezdeti beállításokkal**

Egy Cisco switch bekapcsolása után öt rendszerindítási lépésen megy keresztül. A BOOT környezeti változó a globális szabályozáss mód **boot system**parancsával állítható be. Az IOS egy külön mappában található, és a térkép elérési útja is meg van adva. A switch LED-jeinek segítségével ellenőrizhetjük a switch aktivitását és teljesítményét: SYST, RPS, STAT, DUPLX, SPEED és PoE. Ha az operációs rendszer hiányzó vagy sérült fájlok miatt használhatatlanná válik, akkor a boot loader segítségével még hozzáférhetünk a switch-hez. A boot loader parancssorán keresztül elérhetők a flash memóriában tárolt fájlok. A switch-ek távoli felügyeletéhez be kell állítani egy IP-címet és egy alhálózati maszkot. A kapcsoló távoli hálózatról történő eléréséhez konfigurálni kell egy telepített átjárót is! A switch SVI-interfészének először be kell állítani a felügyeti interfészt, megadni az alap átjárót, végül pedig ellenőrizni a beállítást.

**Konfigurálja a kapcsolóportokat**

A teljes duplex (full-duplex) kommunikáció növeli a tényleges sávszélességet, mivel lehetővé teszi, hogy a kapcsolat mindkét végén egyidejűleg küldjön és fogadjon adatokat. A félduplex (half-duplex) kommunikáció adott pillanatban csak egyirányú lehet. A kapcsoló portjait manuálisan be lehet állítani az egyedi duplexitás vagy sebességnek megfelelően. Használjunk automatikus egyeztetést, ha a porthoz csatlakozó eszköz sebesség- és duplexbeállításai ismeretlenek vagy változhatnak. Amikor az auto-MDIX engedélyezi, az interfész típust felismeri a szükséges kábel (vagy keresztkötés), majd ezt megfelelően konfigurálja. Számos **show** parancs használható a switch beállításának ellenőrzéséhez. Használjuk a **show running-config** és a**show interfaces** parancsokat egy switchport beállításainak ellenőrzéséhez. A **show interfaces** parancs szintén hasznos a hálózatelérési réteg gyakoribb hibáinak észlelésére, mivel visszajelzi a vonal- és adatkapcsolati állapotot. A **show interfaces** által jelzett bemeneti hibák: töredék keretek (runts), óriás keretek (giants), CRC-hibák, valamint az ütközések és a késői ütközések. A **show interfaces** paranccsal megállapíthatjuk, ha a switch és egy másik eszköz között nics vagy hibás a kapcsolat.

**Biztonságos távoli hozzáférés**

A (23-as TCP-portot használó) Telnet egy régi protokoll, amely nem biztonságos módon, nyílt szövegként továbbítja mind a bejelentkezési hitelesítő adatokat (felhasználónév és jelszó), mind az eszközök közötti egyéb adatkommunikációt. A (22-es TCP-portot használó) SSH egy biztonságos protokoll, amely titkosított felügyeleti kapcsolatot biztosít egy távoli eszközhöz. Az SSH biztonságos távoli kapcsolatokat valósít meg, mert erős titkosítást használ mind a hiteleshez (felhasználónév és jelszó kezelése), mind pedig a kommunikáló eszközök közötti adatátvitelhez. Adjuk ki a **show verziót**parancsot a switch által éppen futtatott IOS néz. Az IOS nevében szereplő "k9" szövegrészlet a kriptográfiai funkciók és képességek támogatását jelenti. Az SSH beállításához ellenőrizni kell, hogy a switch-e, majd be kell állítanunk egy tartománynevet, generálni egy RSA-kulcspárt, beállítani a felhasználói hitelesítést, konfigurálni a VTY-vonalakat, majd ellenőrizni az SSH 2-es verzióját. Az SSH működésének ellenőrzéséhez használjuk a **show ip ssh** parancsot, amely megjeleníti az SSH verzióját és beállításának adatait az eszközön.

**Alapvető router konfiguráció**

Az alábbi beállításs kezdőlépéseket minden alkalommal el kell végezni: az eszköz elnevezése, hogy megkülönböztethető legyen más routerektől, jelszavak létrehozása, bejelentkezési üzenet beállítása, amely értesíti a jogosulatlanról, valamint a változások elmentése a routeren. A switch-ek és a routerek közötti egyik megkülönböztető jellemző az általuk támogatott interfészek típusai. A második rétegbeli kapcsolók például LAN-okat szolgálnak ki, ehhez számos FastEthernet vagy Gigabit Ethernet portot használnak. A dual stack (kettős verem) topológia a router interfészek IPv4-es és IPv6-os konfigurációjának bemutatására szolgál. A routerek LAN-okat és WAN-okat támogatják és különböző típusú hálózatokat kötnek össze, ezért számos interfésztípust támogatnak. Például a G2 ISR-eknek egy vagy kettő beépített Gigabit Ethernet interfészük van, valamint nagy sebességű WAN kártyafoglalat is (High-Speed ​​WAN Interface Card, HWIC), amelyek más típusú hálózatokat is képesek kezelni, ilyenek a soros, a DSL és a kábeltévés kapcsolatok. A loopback interfész a router belső, logikai interfése. Egyetlen fizikai porthoz sincs hozzárendelve, ezért másik eszközzel sem csatlakoztatható hozzá.

**Ellenőrizze a közvetlenül csatlakoztatott hálózatokat**

A következő parancsokkal gyorsan megállapítható egy interfész állapotát: a **show ip interface brief** és a **show ipv6 interface short** parancsokkal egy rövid összefoglalást kapunk az interfészekről (IPv4-es és IPv6-os címek, működési állapot), a **show running-config interface interface-id** paranccsal az egy adott interfészre kiadott utasításokat ellenőrizni tudja, a **show ip route** és a **show ipv6 route** parancsokkal a RAM-ban tárolt IPv4-es és IPv6-os irányítótáblákat tekinthetünk meg. A **show ip interface brief** és **show ipv6 interface** shortokkal egy router minden interfészének állapotát gyorsan parancsolhatjuk. A**show ipv6 interface gigabitethernet 0/0/0** parancs az interfész állapotát és az interfészhez tartozó összes IPv6-os címet jeleníti meg. A link-local és a globális egyedi cím mellett a kimenet még az interfészhez rendelt multicast címeket is. A **show running-config interface** parancs kimenete az egy meghatározott interfészre kiadott aktuális parancsokat jeleníti meg az ábrának megfelelően. A **show interfaces** parancs az eszköz valamennyi interfészére jelenít meg rendelkezésre és adatforgalmi számlálókat. Az interfész beállításait a **show ip interface** és a **show ipv6 interface**parancsokkal ellenőrizzük, egy router valamennyi interfészére jelenítenek meg IPv4 és IPv6 vonatkozású információkat. Az útvonalakat a **show ip route** és a **show ipv6 route** parancsokkal ellenőrizzük. A show parancs kimenetét a "cső" (|) karakterrel szűrhetjük. Használható szűrési kifejezések: section, include, exclude és begin. A parancselőzmények funkció alapértelmezés szerint engedélyezve van, és a rendszer a legutóbb használt 10 parancsot őrzi meg az átmeneti tárolójában. Az előzménypuffer tartalmát a privilegizált EXEC mód **show history** parancsa jeleníti meg.

# Bevezetés

2.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Kapcsolás elmélete fejezetben!

Switch-eket csatlakoztatunk és konfigurálunk, ez nagyszerű! De még a legújabb technológiával rendelkező hálózatban is előfordulhatnak problémák. Ha hálózati hibaelhárítást kell végezni, tudnunk kell hogyan működnek a switch-ek. Ez a fejezet ismerteti a switch-eket és működésük alapjait. Szerencsére a switch-ek működése könnyen érthető.

2.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe:** Fogalmak váltása

**Modul célja** : Magyarázza el, hogy a 2. réteg hogyan váltja át az adatokat.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Kerettovábbítás** | Magyarázza el, hogyan történik a keretek továbbítása kapcsolt hálózatban. |
| **Domain váltás** | Hasonlítsa össze az ütközési tartományt a broadcast tartományokkal. |

Kerettovábbítás

2.1.1

Hálózati kapcsolás

Az adatkeretek kapcsolásának és kiadásának általános érvényessége a hálózati működésben és a telekommunikációban. Sokféle típusú switch működik a különféle helyi (LAN) és nagytávolságú (WAN) hálózatokban, valamint a nyilvános kapcsolt telefonhálózatban (PSTN) is.

A switch a forgalom érkezéséhez szükséges döntést a beő adatfolyam alapján hozza meg. Az interfészre érdeklődők és onnan kiküldött keret két kifejezés kapcsolódik:

* **Belépés** – Ez a port leírása, ahol a keret belép az eszközbe.
* **Kilépés** – Ez a port leírása, amelyet a keretek használnak, amikor elhagyják az eszközt.

A LAN switch egy táblázatot tart fenn, amelyet a forgalom adásakor használ. Egyetlen képessége az, hogy képes használni ezt a táblát a forgalom áruára. A forgalmat a bejövő port és az Ethernet keretet cél MAC-címe alapján továbbítja. Mivel a switch-nek csak egyetlen kapcsolótáblája van - a főcím pontos hozzárendelései között találhatók portok és MAC-ek között -, ezért egy adott célcímű üzenet mindig ugyanazon a kimenő porton távozik, attól függetlenül, hogy melyik bejövő porton érkezett.

**Megjegyzés** : Az Ethernet keret soha nem lesz továbbítva ugyanazon a porton, amelyen fogadta.

A kapcsolás folyamatáról szóló animáció képernyő kattintsunk a Lejátszásba!

Az animáció egy téglalapot mutat be a kapcsoló azonosítására, 6 számozott négyzettel 6 kapcsolóporthoz. A MAC-cím táblázat az egyes portszámokhoz regisztrált Mac-címeket mutatja

Port táblázat

| Úticélok címei | Kikötő |
| --- | --- |
| EE | 1 |
| AA | 2 |
| BA | 3 |
| EA | 4 |
| AC | 5 |
| AB | 6 |

2.1.2

A kapcsoló MAC-címtáblája

A switch integrált áramkörökből és olyan szoftverekből épül fel, amelyek az adatáramlási útvonalat határozzák meg. A switch-ek a cél MAC-címeket használnak arra, hogy a hálózati kommunikációt a megfelelő porton a cél felé továbbítsák.

Ahhoz, hogy a switch tudja, melyik portját használhatja egy keretbe, először meg kell tanulnia, hogy mely eszközök kapcsolódnak a portjaihoz. Amint megtanulta az eszköz-port összefüggést, felépíti a MAC-címtáblának nevezett táblát. Ez a táblázat egy tartalom alapján címezhető memóriában (content addressable memory, CAM) tárolódik, amely egy speciális memória típus és nagy sebességű kereső alkalmazásnál van használatban. Emiatt a MAC-címtáblát néha CAM-táblának nevezik.

A LAN-switch-ek folyamatosan karbantartják a MAC-címtáblákat, hogy képesek legyenek a bejövő adatok kezelésére. A címtábla felépítésekor a switch feljegyzi az egyes portokhoz kapcsolódó eszközöket MAC-címét. A táblában tárolt tárolja úgy használja, hogy egy adott eszköznek címzett keretet azon a porton küldi ki, a címtáblában az eszközhöz van rendelve.

2.1.3

A switch tanulási és használati módszere

A következő kétlépéses folyamat minden olyan Ethernet kereten végrehajtásra kerül, amelyik beérkezik a switch-be.

**1. lépés: Tanulás – A forrás MAC-cím vizsgálata**

Minden keret, amely beérkezik egy switch-be ellenőrzésen esik át új információk megismerése érdekében. Ez úgy történik, hogy a kapcsolót megvizsgálja a keret forrás MAC-címét és azt a portot, amelyen a keret beérkezett:

* Ha a forrás MAC-címe nem található meg a MAC-címtáblában, a rendszer hozzáadja a MAC-címet és a bejövő port számát a táblázathoz.
* Ha a forrás MAC-címe létezik, akkor a switch frissíti a bejegyzés elévülési időzítőjét. Alapértelmezés szerint a legtöbb Ethernet switch 5 percig tart meg egy bejegyzést a táblázatban. Ha a forrás MAC-cím létezik a táblázatban, de egy másik porton, a switch ezt az új bejegyzésként kezeli. A bejegyzést ugyanazzal a MAC-címmel, de az aktuális portszámmal helyettesíti.

**2. lépés Továbbítás – A cél MAC-címének vizsgálata**

Ha a cél MAC-cím egyedi cím, a switch egyezést keres a keret cél-MAC-címe és a MAC-címtábla egy bejegyzése között:

* Ha a cél MAC-cím szerepel a táblázatban, akkor továbbítja a keretet a megfelelő porton.
* Ha a cél MAC-cím nem szerepel a táblázatban, a switch a bejövő port kivételével az összes portján keresztül kiküldi a keretet. Ezt hívják ismeretlen unicast-nek. Ha a cél MAC-cím szórásos vagy csoportos, akkor a keret a bejövő port kivételével az összes porton árura kerül.

2.1.4

Videó - Egymáshoz csatlakoztatott switch-ek MAC-címtáblái

Kattintsunk Lejátszást bemutató bemutató a saját két összekapcsolt switch építi MAC-címtábláit.

Play Video

2.1.5

Kapcsolási módok

A switchek nagyon gyorsan meghozzák a 2. rétegbeli döntéseiket. Ez az alkalmazásspecifikus integrált áramkörök (ASIC) szoftvere miatt van így. Az áramkörök lecsökkentik az eszközben a keretkezelésre fordított időt, és a teljesítmény gyengítését is egyszerre több port kezelést biztosítanak.

A 2. rétegbeli swich-ek két módszer egyikét használja a keretek kapcsolására

* **Tárolás és továbbítás váltás** – Ez a módszer továbbítási döntést hoz egy keretről, miután az megkapta a teljes keretet, és a ciklikus redundancia-ellenőrzés (CRC) néven ismert matematikai hibaellenőrző mechanizmus segítségével ellenőrizte a keretet hibákra. A Cisco által elsődlegesen alkalmazott LAN kapcsolási módszer a tárol-és-továbbít eljárás.
* **Átvágási kapcsolás** – Ez a módszer a bejövő keret MAC-címének és a kimenő portnak a meghatározása után indítja el a továbbítási folyamatot.

2.1.6

Tárol-és-továbbít kapcsolás

A tárol és továbbít kapcsolás a következő két alapvető (a közvetlen kapcsolástól eltérő) jellemzővel rendelkezik:

* **Hibaellenőrzés** – Miután megkapta a teljes keretet a bemeneti porton, a kapcsoló összehasonlítja a datagram utolsó mezőjében lévő keretellenőrzési sorozat (FCS) értékét saját FCS-számításaival. Az FCS művelet segítségével biztosítva van, hogy a keret mentes a fizikai és adatkapcsolati hibáktól. Ha a keret hibamentes, a switch továbbküldi, egyébként pedig eldobja.
* **Automatikus pufferelés** – A bemeneti port pufferelési folyamata, amelyet a tárolási és továbbítási kapcsolók használnak, rugalmasságot biztosít az Ethernet-sebesség bármilyen keverékének támogatásához. Például egy 100 Mbit/s sebességű porton aktív keret esetén, melyet egy 1 Gbit/s interfészen kell továbbítani, a tárol-és-tovább módszer használatára van szükség. Ha a bejövő és kimenő portok között sebességeltérés van, a switch az egész keretet az átmeneti tárba helyezi, végezi rajta a hibaellenőrzést, majd továbbítja a kimenő port pufferébe és kiküldi azt.

Az ábra azt szemlélteti, hogyan történik a tárolás és továbbkapcsolás az Ethernet keret alapján.

egy ethernet keret diagramját mutatja be, és kiemeli azt a tényt, hogy a tárolás és továbbítás váltáskor a kapcsoló beolvassa a teljes keretet, beleértve az összes fejlécet, az adatokat és a keretellenőrzési szekvenciát a továbbítás előtt

86624

Hálózati fejlécKeret fejlécPreambulumCél MAC-címForrás MAC-címTípusFCS ellenőrző összeg (CRC)Szállítási fejlécAdatBájtokA tárolási és továbbítási váltás magában foglalja a teljes keret fogadását (akár kb. 9200 bájtot a jumbo kereteknél), mielőtt a továbbítási döntés megszületik.

2.1.7

Közvetlen kapcsolás

Tárol továbbítkapcsolás esetén olyan keretek és eldobásra, amelyek nem felelnek meg az FCS-ellenőrzésen. Ezért ez a módszer nem továbbít érvénytelen kereteket.

Ezzel közvetlen kapcsoláskor a nem megfelelő keretek továbbítódnak, mivel itt nincs FCS hibaellenőrzés. A közvetlen kapcsolás viszont gyors keretet képes végrehajtani. Amint az ábrán is látható, közvetlen döntés a cél MAC-cím beérkezése és a MAC-címtáblában azonosítása után azonnal megállítható.

egy ethernet keret diagramját mutatja be, és kiemeli azt a tényt, hogy átkapcsoláskor a switch tovább tudja küldeni a keretet, miután beolvassa a cél MAC címet

86624

Hálózati fejlécKeret fejlécPreambulumCél MAC-címForrás MAC-címTípusFCS ellenőrző összeg (CRC)Szállítási fejlécAdatBájtokA keretek továbbítása azonnal megkezdhető, amint megérkezik a cél MAC.

A switch-nek megvárnia a keret további részeinek megérkezését a nem kell döntés meghozásához.

A töredékmentes kapcsolás az átvágó kapcsolás egy módosított formája, amelyben a kapcsoló csak a keret továbbítását kezdi meg. Jobb hibaellenőrzést biztosít, mint a közvetlen kapcsolást, és nem növeli a késleltetést.

A közvetlen kapcsolás kis késleltetési ideje előnyt jelent a szélsőséges igényeket támasztó, nagy számítási teljesítményű alkalmazások számára, amelyek 10 ms-nál kisebb késleltetést követelnek meg.

Közvetlen kapcsolási mód esetén előfordulhat hibás keretek szállítása. Ha túl magas a hibaarány a hálózatban (sok a rossz keret), a közvetlen kapcsolás negatív hatással lehet a sávszélességre, eldugítva azt sérült és hibás keretekkel.

Ütközés és sugárzási tartományok

2.2.1

Ütközési tartományok

Az előző részben alaposabban megismerhettük a switch-et és annak működését. Ez a témakör azzal foglalkozik, hogy a switchek hogyan működjenek együtt egymással és más eszközökkel az ütközések kiküszöbölése és a hálózati torlódások csökkentése érdekében. Az ütközés és torlódás kifejezések itt ugyanabban az értelemben használatosak, mint az utcai forgalomban.

A régi hub-alapú Ethernet szegmensekben a hálózati eszközök versenyeztek a megosztott átviteli közegért. Azokat a hálózatrészeket, ahol az eszközök azonos sávszélességen osztoznak egymás közt ütközési tartományoknak nevezzük. Ha ugyanazon az ütközési tartományon belül két vagy több eszköz egyszerre próbál kommunikálni ütközés következik be.

Ha egy Ethernet switchport fél-duplex módban működik, mindegyik szegmens a saját ütközési tartományában található. Nincsenek ütközések, ha a kapcsolóportok full-duplex üzemmódban működnek. Azonban ha a switchport fél-duplex módban működik, akkor létrejöhet az ütközési tartomány.

Alapértelmezés szerint az Ethernet switchportok teljes duplex módot fognak egyeztetni, ha a szomszédos eszköz szintén képes a teljes duplex módú működésre. Ha a switchport fél-duplex működő eszközhöz van csatlakoztatva, akkor egy régi duplex módban fog működni. Fél-duplex üzemmód esetén a switchport egy ütközési tartomány tagja lesz.

Ahogy az ábrán látható, a legnagyobb közös sávszélességgel működő full duplex mód kerül kiválasztásra, ha mindkét eszköz akkor támogatja azt.

ábra azt mutatja, hogy a számítógép és a kapcsoló automatikusan egyezteti a duplex beállításokat és sebességeket. Ebben az esetben full duplex és 100Mb/s

S2PC A

DuplexitásDuplexitásSebességSebességTeljesFélTeljesFél100 Mbps10 Mbps100 Mbps10 Mbps1000 Mbps1. portÖntárgyalás

2.2.2

Szórási tartományok

Az így egymáshoz csatlakoztatott switch-ek egy szórási tartományt (broadcast domain) alkotnak. A 2. rétegbeli szórási tartományokat csak egy hálózati rétegbeli eszköz (pl. router) tudja elválasztani egymástól. A routerek a szórási tartományok szegmentálására szolgálnak, de ütközési tartományokat is határolnak.

Ha egy eszköz 2. rétegbeli üzenetszórást küld, a keret cél MAC-címe csupa bináris 1-et tartalmaz.

A 2. rétegbeli szórási tartományt MAC szórási tartománynak is nevezik. A szórási tartomány tehát azon LAN-eszközök összessége, melyekhez eljut egy adott állomás üzenetszórása.

Ennek látható láthatósunk az ábrán Lejátszáshoz!

egy diagramanimációt mutat be egy broadcast üzenetről, amely eljut minden, a switch-hez csatlakoztatott gazdagéphez, valamint kapcsolóról kapcsolóra a broadcast tartományon vagy LAN-on belül

Ha a switch szórásos keret fogad, akkor minden portján továbbítja azt, kivéve azt a bejövő portot, amelyen az üzenetszórás érkezett. A switch-hez csatlakozó minden eszköz megkapja a szórásos keretet egy másolatot és feldolgozza azt.

Az üzenetszórás néha nélkülözhetetlen az eszközök és hálózati szolgáltatások kezdeti azonosítására, de csökkenti a hálózat hatékonyságát. A szórásos forgalom sávszélességet használ el. Erős hálózati forgalom esetén a túl sok üzenetszórás torlódást okozhat, amely lelassítja a hálózat teljesítőképességét.

Két egymáshoz második csatlakoztatott switch megnöveli a szórási tartomány méretét, ez látható az animáció felében. Ebben az esetben az S1 switch minden csatlakoztatott portján továbbküldi a szórásos keretet. Mivel S1 csatlakozik S2-höz, így a keret S2 minden kapcsolódó eszközéhez is eljut.

2.2.3

Hálózati túlterhelés enyhítése

A LAN switch-ek speciális tulajdonságai lehetővé teszik a hálózati túlterhelés csökkentését. Alapértelmezés szerint az összekapcsolt switchportok teljes módú kapcsolatot próbálnak létesíteni, így elkerülve az ütközési tartományok létrejöttét. Minden egyes teljes duplex switchport teljes sávszélességet biztosít a hozzá csatlakozó eszközök számára. Teljes duplex kapcsolat szükséges az 1 Gbit/s vagy annál nagyobb sebességekhez, melyek segítségével megnöveljük a LAN hálózati teljesítményét.

A switch-ek összekötik a LAN-szegmenseket, MAC-címeket használnak a kimenő port meghatározására, valamint csökkentik vagy teljesen kiküszöbölik az ütközéseket. Hálózati torlódást enyhítő kapcsoló jellemzők:

* **Gyors portsebesség** – Az Ethernet switch port sebessége típusonként és célonként változik. Például a legtöbb hozzáférési rétegben található switch 100 Mbps és 1 Gbps portsebességet támogat. Az elosztási rétegbeli switch-ek 100 Mbit/s, 1 Gbit/s és 10 Gbit/s portsebességet, a magrétegben és az adatközpontban lévő switch-ek pedig 100 Gbit/s, 40 Gbit/s és 10 Gbit/s portsebességet támogatnak. A gyorsabb portsebességű switch-ek többe több, de csökkenthetik a torlódást.
* **Gyors belső kapcsolás** – A kapcsolók gyors belső buszt vagy megosztott memóriát használnak a nagy teljesítmény érdekében.
* **Nagy keretpufferek** – A kapcsolók nagy memóriapuffereket használnak, hogy ideiglenesen több fogadott keretet tároljanak, mielőtt el kellene dobniuk őket. Ez lehetővé teszi a gyorsabb portból (pl. 1 Gbit/s) érdeklődő forgalom szállítását egy lassabban (pl. 100 Mbit/s) kimenő portra a keretek elvesztése nélkül.
* **Nagy portsűrűség** – A nagy portsűrűségű kapcsoló csökkenti az általános költségeket, mivel csökkenti a szükséges kapcsolók számát. Ha például 96 hozzáférési portra lenne szükség, akkor olcsóbb lenne két 48 portos switch-et vásárolni négy 24 portos switch helyett. A nagy portsűrűségű switch-ek elősegítik a forgalom helyi szinten tartását, ami lehetővé teszi a torlódás enyhítését.

## Miről tanultunk ebben a fejezetben?

**Kerettovábbítás**

A switch a forgalom érkezéséhez szükséges döntést a beő adatfolyam alapján hozza meg. A bemenő kifejezést használjuk, mikor egy keret belép az eszközbe annak valamelyik portján. A kimenő kifejezés azt a portot írja le, amelyet csak a keretek fognak használni az eszköz elhagyásakor. Az Ethernet keret soha nem kerül forgalomba azon a porton ahol beérkezett. Ahhoz, hogy a switch tudja, melyik portját használhatja egy keretbe, először meg kell tanulnia, hogy mely eszközök kapcsolódnak a portjaihoz. Amint megtanulta az eszköz-port összefüggést, felépíti a MAC-címtáblának nevezett táblát. Minden beérkező keret ellenőrzésen esik át, amikor a switch-et vizsgálja meg a keret MAC-címét és annak a portnak a számát, amelyen a keret beérkezett, így ismer meg új információt. Ha a cél MAC-cím egy unicast cím, a switch egyezést keres a keret cél-MAC-címe és a MAC-címtábla egy bejegyzése között. A switch váltó módszerei közé tartozik a tárol és továbbít, valamint a közvetlen kapcsolódási rendszer. A tárol és továbbít módszer hibaellenőrzést és automatikus pufferelést is végez. Közvetlen kapcsolás esetén nem történik hibaellenőrzés. Ehelyett gyorskeretkapcsolást hajt végre. Ez azt jelenti, hogy a switch a döntési döntést a cél MAC-cím beérkezése és a MAC-címtáblában azonosítása után azonnal meg tudja hozni.

**Domain váltás**

Ha egy Ethernet switchport fél-duplex módban működik, mindegyik szegmens a saját ütközési tartományában található. Ha a switchportok teljesen duplex módban működnek, akkor nincsenek ütközési tartományok. Alapértelmezés szerint az Ethernet switchportok teljes duplex módot fognak egyeztetni, ha a szomszédos eszköz szintén képes a teljes duplex módú működésre. Az így egymáshoz csatlakoztatott switch-ek egy szórási tartományt (broadcast domain) alkotnak. A 2. rétegbeli szórási tartományokat csak egy hálózati rétegbeli eszköz (pl. router) tudja elválasztani egymástól. A 2. rétegbeli szórási tartományt MAC szórási tartománynak is nevezik. A szórási tartomány tehát azon LAN-eszközök összessége, melyekhez eljut egy adott állomás üzenetszórása. Ha a switch szórásos keret fogad, akkor minden portján továbbítja azt, ki azt a bejövő portot, amelyen az üzenetszórás érkezett. A switch-hez csatlakozó minden eszköz megkapja a szórásos keretet egy másolatot és feldolgozza azt. A switch-ek összekötik a LAN-szegmenseket, MAC-címeket használnak a kimenő port meghatározására, valamint csökkentik vagy teljesen kiküszöbölik az ütközéseket. A hálózati torlódást enyhítő switch-ek jellemzői a gyors portsebesség, a gyors belső kapcsolás, a nagy keretpufferek és a nagy portsűrűség.

# Bevezetés

3.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a VLAN-okról szóló fejezetben!

Képzeljük el, hogy mi felelünk egy nagyon nagy konferencia megrendezéséért. Mindenhonnan érkeznek olyan emberek, akiknek közös az érdeklődési körük, és vannak olyanok is, akik különleges szakértelemmel rendelkeznek. Képzeljük el, ha minden szakértőnek, aki egy kisebb közönségnek szeretné bemutatni az információt, ugyanabban a nagy teremben kellene ezt megtenni az összes többi szakértővel és azok kisebb közönségével. Senki sem hallana semmit. Külön termeket kellene találni az összes szakértőnek és a kisebb közönségüknek. A virtuális LAN (VLAN) hasonló feladatot lát el a hálózatban. A VLAN-okat a 2. rétegben hozzák létre a szórásos forgalom csökkentését vagy megszüntetését. VLAN-ok segítségével a hálózatot kisebb hálózatokra bonthatjuk, hogy az azonos VLAN-on belüli eszközök és személyek kommunikálhassanak egymással, és ne kelljen más hálózatok forgalmát kezelni. A hálózati rendszergazda a VLAN-okat hely, a használt személy, az eszköz típusa vagy bármilyen más kategória szerint rendezheti. Ugye, hogy meg akarjuk tanulni, hogyan kell ezt csinálni? Akkor ne tétovázzunk!

3.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe: VLAN-ok**

**Modul célja** : VLAN-ok és trönkölés megvalósítása kapcsolt hálózatban.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A VLAN-ok áttekintése** | Elmagyarázzuk a VLAN-ok célját egy kapcsolt hálózatban. |
| **VLAN-ok több switch-et tartalmazó környezetben** | Elmagyarázzuk, hogy miként továbbítja a switch a kereteket a VLAN-konfiguráció alapján több switch-ből álló környezetben. |
| **VLAN konfiguráció** | Konfiguráljon egy kapcsolóportot a VLAN-hoz a követelmények alapján. |
| **VLAN trönkek** | Konfigurálja a fővonali portot a LAN-kapcsolón. |
| **Dynamic Trunking Protocol** | Állítsa be a Dynamic Trunking Protocol (DTP) protokollt. |

A VLAN-ok áttekintése

3.1.1

VLAN definíciók

Természetesen a hálózatot kisebb hálózatokba szervezni nem olyan egyszerű, mint szétválasztani a csavarokat és befőttesüvegekbe tenni őket. De ez kéri a hálózat kezelését. A VLAN-ok szegmentációt és szervezeti rugalmasságot biztosítanak egy kapcsolt hálózaton belül. Az eszközök egy VLAN- belül úgy kommunikálnak egymással, mintha ugyanarra a vezetékre csatlakoznának. A VLAN-ok fizikai kapcsolatok helyett logikai kapcsolatokra épülnek.

Amint az ábrán látható, a VLAN-ok egy kapcsolt hálózatban lehetővé teszik, hogy a különböző részlegek (pl.: IT, HR és értékesítés) felhasználói ugyanahhoz a hálózathoz csatlakozzanak, függetlenül a használt fizikai switch-től vagy a telephelyi LAN-on belüli elhelyezkedéstől .

Az ábrán egy 3 emeletes épület látható, emeletenként kapcsolóval. A kapcsolók egy másik kapcsolóhoz csatlakoznak, amely egy útválasztóhoz csatlakozik. Minden emelethez több host kapcsolódik. Három VLAN van, amelyek mindhárom emeletet átfogják, és minden emeleten több gazdagépet tartalmaznak. A VLAN-ok a következők: VLAN 2, IT, 10.0.2.0/24; VLAN 3, HR, 10.0.3.0/24; VLAN 4, Értékesítés, 10.0.4.0/24.

Harmadik emeletMásodik emeletElső emeletVLAN 2  
IT  
10.0.2.0/24VLAN 3  
HR  
10.0.3.0/24VLAN 4  
Értékesítés  
10.0.4.0/24

A VLAN-ok lehetővé teszik a rendszergazda számára, hogy olyan szempontok alapján szegmentálja a hálózatot, mint például a gépek szerepe, egy csapat vagy mondjuk egy alkalmazást, minden esetben egy felhasználó vagy egy készülék fizikai elhelyezkedésétől. Minden VLAN külön logikai hálózatnak megfelelő. Egy VLAN-on belül az eszközök úgy viselkednek, mintha egy saját független hálózatukon lennének, még akkor is, ha más VLAN-okkal együtt ugyanazt a közös infrastruktúrát használják. Bármely switchport tartozhat egy VLAN-hoz.

Az egyedi címzéses (unicast), a szórásos (broadcast) és a csoportcímzéses (multicast) csomagok kizárólag azon végberendezésekhez lesznek továbbítva, amelyek a csomagok forrásához tartozó VLAN-on belül vannak. Más VLAN-ba tartozó állomásoknak címzett csomagokat olyan eszközön keresztül kell továbbítani, amely a forgalomirányítást (routing) támogatja.

Egy kapcsolt hálózatban több IP-alhálózat is létezhet VLAN-ok használata nélkül. Az eszközök azonban ugyanabban a 2. rétegbeli szórási tartományban lesznek. Ez azt jelenti, hogy minden 2. rétegbeli szórást (pl.: az ARP-kéréseket) a kapcsolt hálózat összes eszköze megkapja, még azok is, akik nem kívánják a szórást fogadni.

Egy VLAN akár több fizikai LAN-szegmensre kiterjedő szórási tartományt is alkothat. A VLAN-ok javítják a hálózat teljesítményét, mivel a nagyméretű szórási tartományokat kisebbekre osztják fel. Ha a VLAN-hálózat egy eszköze szórásos Ethernet keretet küld, akkor azt a VLAN minden eszközét megkapja, de más VLAN-okban lévő eszközök már nem.

VLAN-ok segítségével a hálózati rendszergazda az adott csoportjaihoz illeszkedő hozzáférési- és biztonsági házirendeket valósíthat meg. Minden switchport csak egyetlen VLAN-hoz tartozhat (kivéve az olyan portot, amely egy IP-telefonhoz vagy egy másik switch-hez csatlakozik).

3.1.2

A VLAN kialakításának előnyei

Egy kapcsolt hálózatban minden egyes VLAN egy IP-hálózatnak felel meg. Ezért a VLAN-ok kialakítása során a hierarchikus hálózatcímzési terv megalkotását is figyelembe kell venni. A hierarchikus hálózatcímzés annyit jelent, hogy a hálózati szegmensekhez vagy VLAN-okhoz a hálózat egészét szem előtt tartva, rendezett módon, IP-alhálózatokat rendelünk. Ahogy az ábrán is látható, összefüggő hálózati címblokkokat foglalunk le és konfigurálunk be a hálózat egy meghatározott területén lévő eszközök számára.

The figure shows a network topology with multiple switches, multiple VLANs, and contiguous network addressing. At the top of the topology is a router R1 connected to a switch below. The switch is connected to two other switches. The switch on the left has three hosts connected to it, each assigned to a different VLAN. PC1 connected to port F0/11 has the following assignment: Faculty, VLAN 10, 172.17.10.21/24. PC2 connected to port F0/18 has the following assignment: Student, VLAN 20, 172.17.20.22/24. PC3 connected to port F0/6 has the following assignment: Guest, VLAN 30, 172.17.30.23/24. The switch on the right also has three hosts connected to it, each assigned to a different VLAN. PC4 connected to port F0/11 has the following assignment: Faculty, VLAN 10, 172.17.10.24/24. PC5 connected to port F0/18 has the following assignment: Student, VLAN 20, 172.17.20.25/24. PC6 connected to port F0/6 has the following assignment: Guest, VLAN 30, 172.1.7.20.26/24.

R1PC1PC2PC3PC6PC5PC4F0/18Fa0/1F0/3F0/11F0/11F0/18F0/6F0/6G0/0/1F0/3F0/5Fa0/1

Kari  
VLAN 10  
172.17.10.21/24Diák  
VLAN 20  
172.17.20.22/24Vendég  
VLAN 30  
172.17.30.23/24Vendég  
VLAN 30  
172.17.30.26/24Diák  
VLAN 20  
172.17.20.25/24Kari  
VLAN 10  
172.17.10.24/24

A táblázat felsorolja a VLAN-ok segítségével kialakított hálózat előnyeit.

| BenefitDescriptionSmaller broadcast domainsDividing a network into VLANs reduces the number of devices in the broadcast domain. In the figure, there are six computers in the network but only three broadcast domains (i.e., Faculty, Student, and Guest).Improved securityOnly users in the same VLAN can communicate together.In the figure, faculty network traffic on VLAN 10 is completely separated and secured from users on other VLANs.Improved IT efficiencyVLANs simplify network management because users with similar network requirements can be configured on the same VLAN. VLANs can be named to make them easier to identify. In the figure, VLAN 10 was named “Faculty”, VLAN 20 “Student”, and VLAN 30 “Guest.”Reduced costVLANs reduce the need for expensive network upgrades and use the existing bandwidth and uplinks more efficiently, resulting in cost savings.Better performanceSmaller broadcast domains reduce unnecessary traffic on the network and improve performance.Simpler project and application managementVLANs aggregate users and network devices to support business or geographic requirements. Having separate functions makes managing a project or working with a specialized application easier; an example of such an application is an e-learning development platform for faculty. | |
| --- | --- |
| **Előny** | **Leírás** |
| Kisebb méretű szórási tartományok | * - Egy hálózat VLAN-okra történő felosztása csökkenti a szórási tartományban broadcast domain. * Az ábrán hat számítógép van a hálózatban, de csak három szórási tartomány (azaz az oktatói, a hallgatói és a vendég). |
| Javított biztonság | * Csak az azonos VLAN-ba tartozó felhasználók kommunikálhatnak egymással. * Csak az ugyanabban a VLAN-ban lévő felhasználók tudnak kommunikálni az útválasztó szolgáltatásai nélkül. Az útválasztó rendelkezhet biztonsági funkcióval, például hozzáférés-vezérlési listával, amely korlátozza a VLAN-ok közötti kommunikációt. |
| Javított informatikai hatékonyság | * A VLAN-ok egyszerűsítik a hálózatkezelést, mivel a hasonló hálózati követelményekkel konfigurálhatók ugyanazon a VLAN-on. * A VLAN-okat el lehet nevezni, hogy könnyebb legyen azonosítani őket. * Az ábrán a VLAN 10 a 'Faculty', a VLAN 20 a 'Student', a VLAN 30 pedig a 'Guest' nevet kapta. |
| Alacsonyabb költségek | A VLAN-ok csökkentik a drága hálózati fejlesztések állapotát, és nem szükséges ki a minden sávszélességet és a felfelé irányuló kapcsolatokat (uplink), ami költségmegtakarítást eredményez. |
| Jobb teljesítmény | A kisebb szórási tartományok csökkentik a szükségtelen forgalmat a hálózaton, és javítják a teljesítményt. |
| Könnyebb projekt- és alkalmazásmenedzsment | * A VLAN-ok vállalati vagy földrajzi követelmény alapján csoportosítanak felhasználókat földrajzi követelmények. * A különálló funkciók egy projekt kezelését vagy speciális alkalmazással való munkát; ilyen alkalmazás például egy e-learning fejlesztési platform a tanárok számára. |

3.1.3

VLAN típusok

A VLAN-okat különböző okokból kínálja a modern hálózatokban. Egyes VLAN típusok a forgalmi osztályok alapján vannak meghatározva. Más típusú VLAN-ok meghatározása az általuk biztosított funkció alapján történik.

További információért kattintunk az egyes VLAN típusokra!

Alapértelmezett VLAN

Adat VLAN

Natív VLAN

Felügyeleti VLAN

Hangátviteli VLAN

**Alapértelmezett VLAN**

Az alapértelmezett VLAN egy Cisco switchen a VLAN 1. Ezért minden switchport a VLAN 1-ben van, ki, ha más VLAN-ra van konfigurálva. Alapértelmezés szerint minden második rétegbeli vezérlőforgalom is a VLAN 1-hez van hozzátársítva.

A VLAN 1-el kapcsolatos fontos tények a következők:

* Alapértelmezés szerint minden port a VLAN 1-hez van hozzárendelve.
* A natív VLAN alapértelmezés szerint VLAN 1.
* A felügyeleti VLAN alapértelmezés szerint VLAN 1.
* A VLAN 1 nem nevezhető át vagy törölhető.

Például a **show vlan short** kimenetben az összes port jelenleg az alapértelmezett VLAN 1-hez van hozzárendelve. Nincs konkrétan kijelölt natív VLAN és nincsenek egyéb aktív VLAN-ok, következésképpen a hálózat úgy van tervezve, hogy a natív VLAN egyben felügyeleti VLAN is legyen . Ez biztonsági szempontból kockázatot jelent.

**Adat VLAN**

Az adat-VLAN-ok olyan VLAN-ok, amelyek a felhasználó által generált forgalom elkülönítésére vannak konfigurálva. Az adat VLAN-okat a hálózat felhasználói vagy eszközcsoportok alapján szétválasztására használjuk. Egy modern hálózat a szervezeti követelményektől függően számos adat VLAN-t tartalmaz. Vegyük figyelembe, hogy a hang- és hálózatkezelési forgalom nem engedélyezhető az adat VLAN-okon.

**Natív VLAN**

A VLAN-ból érkező felhasználói forgalmat fel kell címkézni a VLAN azonosítójával, amikor egy másik switchre küldik. A trönk a kapcsolók portját hasznosítja a címkézett forgalom átvitelének támogatására. Pontosabban, egy 802.1Q trönkport egy 4 bájtos címkét helyez el az Ethernet keret fejlécébe, hogy azonosítsa azt a VLAN-t, amelyhez a keret tartozik.

Előfordulhat, hogy a switch-nek címkézetlen forgalmat kell küldenie a trönkvonalon keresztül. A címkézetlen forgalmat egy switch generálja, és származhat elavult eszközökből is. A 802.1Q trönkprotokoll a címkézetlen forgalmat a natív VLAN-hoz rendeli. A Cisco switch-ek natív VLAN-ja a VLAN 1 (vagyis az alapértelmezett VLAN).

A legjobb módszer a natív VLAN-t egy használaton, VLAN 1-től és a többi VLAN-tól eltérő VLAN-nak beállítható. Valójában nem szokatlan dolog egy meghatározott VLAN-t rászánni arra, hogy a natív VLAN szerepét töltse be a kapcsolt hálózati tartomány valamennyi trönkportja számára.

**Menedzsment VLAN**

A felügyeleti VLAN egy kifejezetten a hálózatfelügyeleti forgalomhoz konfigurált adat-VLAN, beleértve az SSH-t, Telnetet, HTTPS-t, HTTP-t és SNMP-t. Alapértelmezés szerint egy 2. rétegbeli switch-en a VLAN 1 felügyeleti VLAN-ként van konfigurálva.

**Hang VLAN**

A Voice over IP (VoIP) támogatásához külön VLAN szükséges. A VoIP forgalom a következőket igényli: *Biztos sávszélesség a hangminőség biztosítása* Az átviteli prioritás a többi hálózati forgalomhoz csatlakozó *Lehetőség a hálózat zsúfolt területei által meghatározott* követelményeknek megfelelően 150 ms-nál kisebb késleltetés a hálózaton Ezen teljesítése érdekében a teljes hálózatot kell megtervezni, hogy támogassa a VoIP-t.

Az ábrán a hangforgalom küldésére a VLAN 150 lett kijelölve. A PC hallgatói számítógép egy Cisco IP-telefonhoz van csatlakoztatva, a telefon pedig az S3 switch-hez. A PC5 a VLAN 20-hoz tartozik, amelyet a hallgatói adatok használnak.

Az ábrán egy IP-telefonhoz csatlakoztatott gazdagép látható, amely a hang- és adat-VLAN konfigurációját mutatja. A diagram tetején az R1 útválasztó található, amely a G0/0/1 interfészen keresztül kapcsolódik az S1 kapcsolóhoz az F0/5 porton. Az S1 úgy van beállítva, hogy támogassa a hangforgalmat a következőképpen: VLAN 150-et használ a hang VLAN-hoz, és előnyben részesíti a hangforgalmat. Az S1 az F0/3 porton keresztül csatlakozik az S3 kapcsolóhoz az F0/3 porton. Az S3 az F0/18-as porton keresztül csatlakozik egy IP-telefonhoz, amely azután csatlakozik a gazdagép PC5-höz. A PC5 a következő feladattal rendelkezik: Student, VLAN 20, 172.17.20.25. Az S3 F0/18-as portja úgy van konfigurálva, hogy támogassa a hangforgalmat: a port CDP-kereteket küld az IP-telefon által használt információk biztosítására, a port pedig továbbítja a VLAN 150-hez társított kereteket.

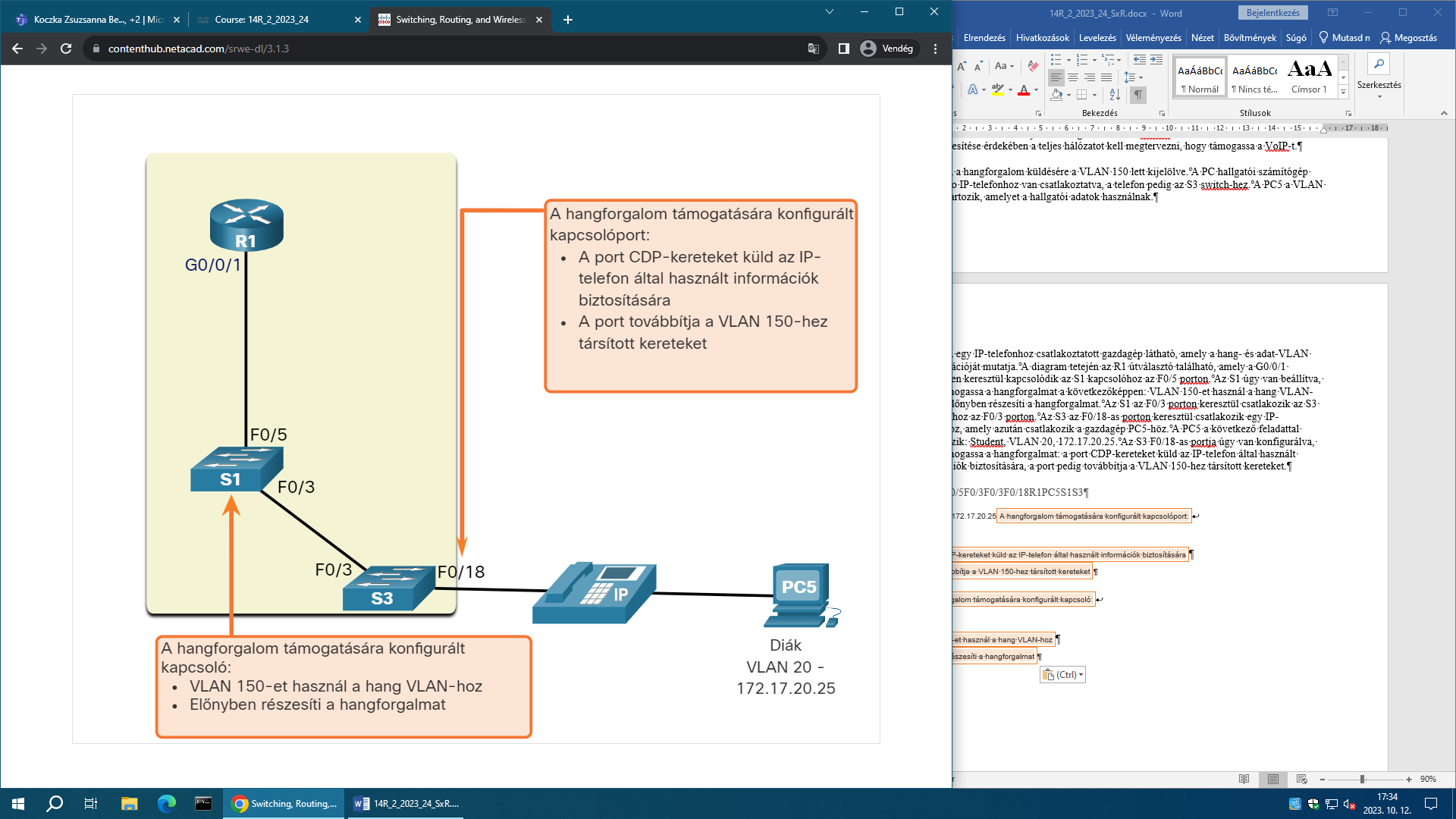
G0/0/1F0/5F0/3F0/3F0/18R1PC5S1S3

Diák  
VLAN 20 - 172.17.20.25A hangforgalom támogatására konfigurált kapcsolóport:

* A port CDP-kereteket küld az IP-telefon által használt információk biztosítására
* A port továbbítja a VLAN 150-hez társított kereteket

A hangforgalom támogatására konfigurált kapcsoló:

* VLAN 150-et használ a hang VLAN-hoz
* Előnyben részesíti a hangforgalmat



VLAN-ok több switch-et tartalmazó környezetben

3.2.1

VLAN-trönkök meghatározása

A VLAN-ok nem lennének jól használhatóak VLAN-trönkök nélkül. A VLAN-trönkök biztosítják az összes VLAN-forgalom terjedését a switch-ek között. Ez lehetővé teszi, hogy a különböző switch-ekhez csatlakoztatott, de ugyanabba a VLAN-ba tartozó eszközök routeren való áthaladás nélkül kommunikáljanak egymással.

A trönk egy pont-pont kapcsolat két olyan hálózati eszközzel, amely egynél több VLAN forgalmát is továbbítja. A VLAN-trönk kiterjeszti a VLAN-okat a hálózat egészére. A Cisco az IEEE 802.1Q szabványt támogatja a Fast Ethernet, a Gigabit Ethernet és a 10-Gigabit Ethernet interfészeken a trönkök összehangolására.

A VLAN-trönk nem tartozik egyetlen adott VLAN-hoz sem. Ehelyett switch-ek és routerek közötti csatornaként szolgálnak több VLAN számára. Trönk használható egy hálózati eszköz és egy szerver, vagy egyéb, 802.1Q kezelésére alkalmas hálózati kártyával felszerelt eszköz között is. Alapértelmezés szerint a Cisco Catalyst switch-eken egy trönkport valamennyi VLAN forgalmát továbbítja.

Az ábrán lévő S1 és S2, valamint az S1 és S3 switch-ek közötti kapcsolatok a 10-es, 20-as, 30-as és 99-es (natív) VLAN-okból eredő forgalom hálózaton keresztüli kapcsolókra vannak konfigurálva. Ez a hálózat nem működik VLAN-trönkök nélkül.

The figure is a network topology with multiple switches and multiple VLANs highlighting the VLAN trunk links between the switches. At the top of the topology is switch S1. S1 is connected via port F0/1 to switch S2 at port F0/1. This connection is highlighted. S1 is also connected via port F0/3 to switch S3 at port F0/3. This connection is also highlighted. Both S2 and S3 have three hosts connected to them, each assigned to a different VLAN. Connected to S2 are PC1, PC2, and PC3. PC1 is connected to port F0/11 has the following assignment: Faculty, VLAN 10, 172.17.10.21. PC2 is connected to port F0/18 has the following assignment: Student, VLAN 20, 172.17.20.22. PC3 is connected to port F0/6 has the following assignment: Guest, VLAN 30, 172.17.30.23. Connected to S3 are PC4, PC5, and PC6. PC4 is connected to port F0/11 has the following assignment: Faculty, VLAN 10, 172.17.10.24. PC5 is connected to port F0/18 has the following assignment: Student, VLAN 20, 172.17.20.25. PC6 is connected to port F0/6 has the following assignment: Guest, VLAN 30, 172.1.7.20.26.

PC2PC3PC6PC5PC4S2S3S1PC1F0/18F0/1F0/3F0/11F0/11F0/18F0/6F0/6F0/1F0/3

Vendég  
VLAN 30 -  
172.17.30.26Vendég  
VLAN 30 -  
172.17.30.23Kar  
VLAN 10 -  
172.17.10.21Kari  
VLAN 10 -  
172.17.10.24Diák  
VLAN 20 -  
172.17.20.22Diák  
VLAN 20 -  
172.17.20.25

3.2.2

VLAN-ok nélküli hálózat

Amikor egy switch az egyik portján szórásos keretet fogad, akkor azt minden portján továbbítja, ki azt, amelyen a szórás beérkezett. Az animációban az egész hálózat ugyanabba az alhálózatba (172.17.40.0/24) tartozik, és nincsenek VLAN-ok konfigurálva. Ennek eredményeként amikor az oktatói számítógép (PC1) egy szórásos keretet küld, akkor azt az S2 switch valamennyi portján kiküldi. Végül az egész hálózat megkapja a szórást, mivel a hálózat egyetlen szórási tartomány.

Adás

Adás

Adás

A PC1 helyi 2. rétegű adást küld. A kapcsolók továbbítják a broadcast keretet az összes elérhető porton.

Kar  
172.17.40.21/24

Diák  
172.17.40.22/24

Vendég  
172.17.40.23/24

Kar  
172.17.40.24/24

Diák  
172.17.40.25/24

Vendég  
172.17.40.26/24

3.2.3

VLAN-okat használó hálózat

A VLAN-ok az egyes kapcsolóportokhoz vannak társítva és azokon konfigurálva. Az ezekhez a portokhoz csatlakoztatott eszközöknek nincs fogalma a VLAN-ról. Ezek az eszközök azonban IP-címmel vannak konfigurálva, és egy adott IP-hálózat tagjai. Itt látszik a kapcsolat a VLAN és az IP hálózat között. A VLAN egy IP-hálózat (vagy alhálózat) egyenértékű. A VLAN-ok a kapcsolón, míg az IP-címzés az eszközön vannak konfigurálva.

Kattintsunk a Lejátszás az animációban, hogy láthassuk miként lett a hálózat most két VLAN segítségével szegmentálva. Az oktatói eszközök a 10-es VLAN-hoz, a hallgatói eszközök pedig a 20-as VLAN-hoz vannak rendelve. Amikor az oktatói PC1 számítógép szórásos keretet küld az S2 switch-nek, akkor a switch ezt a szórásos keretet csak azokon a portokon fogja továbbítani, hogy a VLAN 10 használatára lettek beállítva.

A PC1 helyi 2. rétegű adást küld. A kapcsolók csak a VLAN10-hez konfigurált portokon keresztül továbbítják a broadcast keretet.

A következő VLAN-trunkok támogatására konfigurálva: VLAN 10 és 20

Kari  
VLAN 10  
172.17.10.21/24

Diák  
VLAN 20  
172.17.20.22/24

Kari  
VLAN 10  
172.17.10.24/24

Diák  
VLAN 20  
172.17.20.25/24

Az S2 és S1 switch-ek közötti linkhez tartozó F0/1 port, valamint az S1 és S3 közötti linkhez tartozó F0/3 port trönk módban vannak, tehát úgy lettek konfigurálva, hogy a hálózat valamennyi VLAN-ját továbbítsák.

Amikor S1 az F0/1 porton fogadja a szórásos keretet, akkor az egyetlen VLAN 10-et támogató másik portján, az F0/3-on továbbítja azt. Amikor S3 az F0/3 porton megkapja a szórásos keretet, akkor ő is a VLAN 10-et támogató másik portján, az F0/11-en továbbítja azt. Ezek után a szórásos keret megérkezik a PC4 oktatói számítógéphez, amely az egyetlen másik, VLAN 10-re konfigurált számítógép a hálózatban.

Amikor egy switch-en VLAN-okat használunk, akkor egy meghatározott VLAN-ba tartozó állomás egyedi- és csoportos címzésű, valamint szórásos forgalmának a szállítása kizárólag azokra az eszközökre fog korlátozódni, amelyek ugyanabba a VLAN-ba tartoznak.

3.2.4

VLAN azonosítása címkével

A szabványos Ethernet keret fejléce nem tartalmazhat információt arról, hogy melyik keret melyik VLAN-hoz tartozik. Ezért, ha az Ethernet kereteket egy trönkvonalra helyezzük, az információkat kell hozzáadni azokról a VLAN-okról, amelyekhez tartoznak. Ez a címkézésnek (tagging) nevezett folyamat az IEEE 802.1Q szabványban meghatározott IEEE 802.1Q fejléc segítségével történik. A 802.1Q fejléc egy eredeti Ethernet keret fejlécébe illesztett 4 bájtos címkét tartalmaz, amely beazonosítja azt a VLAN-t, amelyhez a keret tartozik.

Amikor a switch egy VLAN-hoz rendelhető hozzáférési módú porton keretet fogad, akkor a keretfejlécbe egy VLAN-címkét szúr be, majd újraszámítja a keretellenőrző összeget (FCS), és a címkézett keretet egy trönkporton továbbküldi.

**VLAN címkemező részletei**

Amint az ábrán látható, a VLAN címkevezérlési információs mezője egy Típus (Type) mezőből, egy Prioritás (Priority) mezőből, egy Kanonikus formátumazonosító (Canonical Format Identifier) ​​mezőből és egy VLAN-azonosító (VLAN ID) mezőből áll:

* **Típus** – 2 bájtos érték, az úgynevezett címkeprotokoll-azonosító (TPID). Ethernet esetén az értéke hexadecimális 0x8100.
* **Felhasználói prioritás** – 3 bites érték, amely támogatja a szint vagy a szolgáltatás megvalósítását.
* **Canonical Format Identifier (CFI)** – 1 bites azonosító, amely lehetővé teszi a Token Ring keretek átvitelét Ethernet kapcsolatokon keresztül.
* **VLAN ID (VID)** – 12 bites VLAN azonosító szám, amely akár 4096 VLAN azonosítót is támogat.

Miután a switch beillesztette a címkevezérlési információs mezőket, újraszámolja az FCS-értéket, és elhelyezi azt a keret FCS-mezőjében.

Az ábrán egy VLAN címke látható a keret fejlécébe. Az ábra tetején van egy keret, amely a következő mezőket mutatja: Dst MAC, Src MAC, Type/Length, Data és FCS. Alatta ismét látható a keret, ezúttal az Src MAC és a Type/Length mezők közé beszúrt Címke mezővel. Alatta a címke alábbi almezői és azok hossza: Típus (0x8100), hossza 2 bájt; Pri, hossza 3 bit; CFI, hossza 1 bit; és VID, hossza 12 bit.

Dst MACSrc MACCímkeTípus/hosszúságAdatFCSTípus (0x8100)Dst MACSrc MACTípus/hosszúságAdatFCS2 bájt3 bit1 bit12 bitVIDPriCFI

3.2.5

Natív VLAN-ok és a 802.1Q címkézés

Az IEEE 802.1Q szabványa határozza meg a natív VLAN-t a trönkkapcsolatokon, amely alapértelmezés szerint a VLAN 1. Amikor a címkézetlen keret érkezik a trönkportra, azt a natív VLAN-hoz rendeli. A switch-ek között küldött felügyeleti keretek tipikus példa a címkézetlen forgalomra. Ha a két switch közötti kapcsolat trönk módban van, a switch a címkézetlen forgalmat a natív VLAN-ra küldi.

**Címkézett keretek a natív VLAN-on**

A trönkölést támogató egyes eszközök VLAN-címkét adnak a natív VLAN forgalomhoz. A natív VLAN-on küldött vezérlési forgalmat nem kell címkézni. Ha egy 802.1Q trönkport natív VLAN ID-vel megcímkézett keretet fogad, akkor eldobja azt. Következésképpen amikor switchportot konfigurálunk egy Cisco switch-en, akkor úgy kell az eszközöket beállítanunk, hogy azok ne küldjenek címkézett kereteket a natív VLAN-on. Egyéb gyártók natív VLAN-címkézést támogató eszközök közé tartoznak az IP-telefonok, a szerverek, a routerek és a nem Cisco switch-ek.

**Címkézetlen keretek a natív VLAN-on**

Amikor egy Cisco switch trönkportja címkézetlen kereteket fogad (ami egyébként szokatlan egy jól tervezett hálózatban), akkor azokat a natív VLAN-ra továbbítja. Ha nincsenek a natív VLAN-hoz társított eszközök (ami viszont nem szokatlan) és más trönkportok sincsenek (ami szintén nem szokatlan), akkor a keret eldobásra kerül. Alapértelmezés szerint az 1-es VLAN a natív VLAN. Egy 802.1Q trönkport konfigurálásakor a natív VLAN ID értéke az alapértelmezett port VLAN ID (PVID) lesz. Minden, 802.1Q portra beérkező vagy arról, hogy kimenő címkézetlen forgalom a PVDI érték alapján kerül termékre. Ha például natív VLAN-nak a VLAN 99 lett beállítva, akkor a PVID értéke 99 és minden címkézetlen forgalom a VLAN 99-be lesz továbbítva. Ha a natív VLAN nem lett újrakonfigurálva, akkor a PVID értéke a VLAN 1 lesz.

Az ábrán PC1 egy hub-on keresztül csatlakozik egy 802.1Q trönkkapcsolathoz.

Az ábra egy hálózati topológia, amely a címkézetlen forgalom áramlását mutatja a natív VLAN-on. Az ábra tetején egy kapcsoló található. A kapcsoló alább négy másik kapcsolóhoz csatlakozik egy 802.1Q fővonali kapcsolaton keresztül. A felső kapcsoló és a bal szélen lévő kapcsoló között van egy hub, amelyhez a PC1 állomás csatlakozik. A bal szélső kapcsolónak van egy portja a VLAN 1-ben és egy portja a VLAN 2-ben. A bal oldali második kapcsolónak a VLAN 3-ban van egy portja. A bal oldali harmadik kapcsolónak van egy portja a VLAN 1-ben. A jobb oldali kapcsolónak van egy portja. port a VLAN 2-ben és egy port a VLAN 3-ban. A narancssárga nyilak mutatják a PC1-ről a hub felé küldött forgalmat, amely mindkét csatlakoztatott switchre továbbítja. A bal szélső kapcsoló a VLAN 1 portját küldi ki. A felső kapcsoló a bal oldali harmadik kapcsolónak küldi ki, amely a VLAN 1-hez csatlakoztatott portot küldi ki.

PC1

VLAN 1VLAN 2VLAN 3VLAN 1VLAN 2VLAN 3802.1Q törzs802.1Q törzs802.1Q törzs802.1Q törzs

PC1 címkézetlen forgalmat küld, amit a switch-ek a trönkportokon konfigurált natív VLAN-hoz társítanak, és annak megfelelően továbbítanak. A trönkről érdeklődő címkézett forgalmat PC1 eldobja. Ez a több szempontból is gyenge hálózattervezést tükröz: hub-ot használ, állomást csatlakoztat egy trönkhöz, és ez maga után vonja, hogy a switch-eknek hozzáférési portjai a VLAN-hoz rendelve. Jól szemlélteti azonban az IEEE 802.1Q specifikáció azon szándékát is, hogy natív VLAN-ok segítségével kezeljék a hagyományos hálózati megvalósításokat.

3.2.6

Hangátviteli VLAN-ok címkézése

A VoIP (Voice over IP) adatforgalom egy különálló VLAN szükséges. Ez lehetővé teszi a szolgáltatásminőségi (QoS) és a biztonsági házirendek alkalmazását a hangforgalomra.

A Cisco IP-telefon közvetlenül csatlakozik egy switchporthoz. Egy IP-állomás is csatlakozhat az IP-telefonhoz, hogy hálózati csatlakozási lehetőségek kapjon. A Cisco IP-telefonhoz csatlakoztatható külön hozzáférési port két VLAN használatára konfigurálható. Az egyik VLAN a hangforgalomhoz, a másik pedig egy adat VLAN az állomásforgalom támogatására. A switch és az IP-telefon közötti kapcsolat egy trönkkapcsolatot szimulál, hogy mind a hang VLAN-forgalmat, mind az adat VLAN-forgalmat továbbítsa.

A Cisco IP-telefon konkrétan egy beépített, három portos 10/100-as switch-et tartalmaz. A portok meghatározott célú kapcsolatokat biztosítják az eszközöknek:

* Az 1-es port a switch-hez vagy egy másik VoIP-eszközhöz csatlakozik.
* A 2-es port egy belső 10/100-as interfész, amely az IP-telefon forgalmát továbbítja.
* A 3-as port (hozzáférési port) PC-hez vagy valamilyen más eszközhöz csatlakozik.

A switch hozzáférési portja CDP-csomagokat küld, hogy a csatlakoztatott IP-telefont arra használja, hogy a hangforgalmat a háromféle módon küldje el. Az alkalmazott módszer a forgalom típusától függ:

* A hang VLAN forgalmát megfelelő 2. rétegbeli szolgáltatási osztály (CoS) prioritási értékével kell ellátni.
* A hozzáférési VLAN forgalma szintén címkézhető a 2. rétegbeli CoS prioritási értékkel.
* A hozzáférési VLAN nincs címkézve (nincs 2. rétegbeli CoS prioritási értéke).

Az ábrán a PC5 hallgatói számítógép egy Cisco IP-telefonhoz van csatlakoztatva, a telefon pedig az S3 switch-hez. A 150-es VLAN a hangforgalom lebonyolítására szolgál, míg a PC5 a 20-as VLAN-ban van, amelyet a diákok adatforgalmára használnak.

host csatlakoztatva egy IP-telefonhoz, amely egy kapcsolóhoz van csatlakoztatva, amely a hang- és adat-VLAN konfigurációját mutatja

F0/18P1P2P3S3PC5

A hangforgalom támogatására konfigurált kapcsolóport:

* Utasítja a telefont, hogy hangkereteket jelöljön meg VLAN 150-el
* Előnyben részesíti a hangkereteket
* Továbbítja a VLAN 20 adatkeretét

A hangforgalmi keretek VLAN 150-el való címkézésére konfigurálva.Cisco IP telefon  
ASIC telefonHozzáférési port3 portos kapcsoló

3.2.7

Példa a hang VLAN ellenőrzésére

Az ábrán a **interface fa0/18 switchport** parancs példakimenete látható meg. A parancskimeneti példa kiemelt részei jól mutatják, hogy az F0/18 interfész egy, az adatok számára beállított VLAN-nal (VLAN 20) és egy hang számára beállított VLAN-nal (VLAN 150) lett konfigurálva.

S1# **show interfaces fa0/18 switchport**

Name: Fa0/18

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 20 (student)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: 150 (voice)

VLAN konfiguráció

3.3.1

VLAN-tartományok a Catalyst switch-eken

A VLAN-ok létrehozása a hálózatépítés legtöbb más aspektusához hasonlóan a megfelelő parancsok megadásával történik. Ez a témakör részletesen ismerteti a különböző típusú VLAN-ok konfigurációját és ellenőrzését.

A különböző Cisco Catalyst switch-ek eltérő számú VLAN-t támogatnak. A támogatott VLAN-ok elegendően nagy a legtöbb szervezetnek megfelelő kielégítésére. A Catalyst 2960 és 3650 sorozatú switch-ek például több mint 4000 VLAN-t kezelnek. A normál tartományú VLAN-ok ezeken a switch-eken 1-től 1005-ig számozottak, a kiterjesztett tartományú VLAN-ok pedig 1006 és 4094 között. Az ábra egy Cisco IOS Release 15.x-et futtató Catalyst 2960 switch alaphelyzetben VLAN-jait szemlélteti.

Switch# **show vlan brief**

VLAN Name Status Ports

---- ----------------- ------- --------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

**Normál hatótávolságú VLAN-ok**

A normál tartományú VLAN-ok jellemzői a következők:

* Kis- és közepes méretű vállalkozásokban és vállalati hálózatokban használtak.
* 1 és 1500 közötti VLAN ID-val vannak azonosítva.
* Az 1002 és 1005 közötti azonosítók az elavult hálózati technológiák (pl.: Token Ring és Fibre Distributed Data Interface) számára fenntartva.
* Az, valamint az 1002 és 1005 közötti ID-k jön 1 jönnek létre és nem lehet őket törölni sem.
* A konfigurációkat a switch flash memóriája tárolja a vlan.dat nevű VLAN-adatbázisfájlban.
* Ha be van állítva, a VLAN trönkprotokoll (VTP) segít a VLAN-adatbázis switch-ek közötti szinkronizálásában.

**Kiterjesztett hatótávolságú VLAN-ok**

A kiterjesztett tartományú VLAN-ok jellemzői az alábbiak:

* Ezeket a szolgáltatók több hasznos ügyfélszolgálatot, valamint a globális vállalatokat, elég nagyok ahhoz, hogy kiterjesztett tartományú VLAN-azonosítókra legyen szükségük.
* 1006 és 4094 közötti VLAN ID-val vannak azonosítva.
* A beállításk alapértelmezés szerint az aktívan kellő mentésre.
* A normál tartományú VLAN-oknál kevesebb VLAN-funkciót támogatnak.
* A kiterjesztett tartományú VLAN-ok támogatásához a VTP transzparens módú beállításja szükséges.

**Megjegyzés** : A 4096 a Catalyst kapcsolókon elérhető VLAN-ok számának felső határa, mivel az IEEE 802.1Q fejléc VLAN ID mezőjében 12 bit található.

3.3.2

VLAN létrehozási parancsok

Amikor tartományú VLAN-okat konfigurálunk, akkor a részletes beállítás egy kapcsoló flash memóriájában egy vlan.dat nevű fájlban tárolódik. A flash memória tartalma nem felejtős, és nincs szükség a **copy-config startup-config** parancsra. Mivel egy Cisco switch-en a VLAN-ok létrehozásával párhuzamosan gyakran más részletek is beállításra kerül, bevált gyakorlat az aktuális beállítást az indítási beállításba is elmenteni.

A táblázat egy VLAN switch-en létrehozásához és elnevezéséhez használt Cisco IOS utasítások szintaktikáját mutatja. A switch-ek konfigurálásakor bevált gyakorlatnak minden VLAN-nak nevet adni.

| TaskIOS CommandEnter globális konfigurációs mód.Switch# configure terminálHozzon létre egy VLAN-t érvényes azonosító számmal.Switch(config)# vlan vlan-id Adjon meg egy egyedi nevet a VLAN azonosításához.Switch(config-vlan)# név vlan-name Visszatérés a privilegizált EXEC-hez mode.Switch(config-vlan)# end | |
| --- | --- |
| **Feladat** | **IOS-parancs** |
| Lépjünk be a globális szabályozáss módba. | Switch# **konfiguráló terminál** |
| Hozzunk létre egy VLAN-t érvényes azonosítószámmal. | Switch(config)# **vlan**  *vlan-id* |
| Adjunk meg egy egyedi nevet a VLAN azonosításához. | Switch(config-vlan)# **név**  *vlan-név* |
| Térjünk vissza privilegizált EXEC módba. | Switch(config-vlan)# **vége** |

3.3.3

Példa VLAN létrehozására

A topológiában a hallgatói számítógép (PC2) még nem lett VLAN-hoz rendelve, de már rendelkezik a 172.17.20.22 IP-címmel, amely a 20-as VLAN-hoz tartozik.

diák PC, host PC2, a 172.17.20.22 címen az S1 kapcsolóhoz csatlakozik az F0/6 porton, amely az F0/1 porton keresztül csatlakozik az S2 kapcsolóhoz az F0/1 porton

S2S1PC2F0/06F0/1F0/1172.17.20.22

Diák PC

Az ábra azt szemlélteti, hogy miként kell az S1 switch-en a hallgatói VLAN-t (VLAN 20) beállítani.

S1# **configure terminal**

S1(config)# **vlan 20**

S1(config-vlan)# **name student**

S1(config-vlan)# **end**

**MEGJEGYZÉS:** Egyetlen VLAN ID bevitelén felül VLAN ID-k vesszővel elválasztott sorozatát, vagy kötőjellel elválasztott tartományát is megadhatjuk a **vlan***vlan-id* parancsban. Például a **vlan 100,102,105-107** blokkvezérlős parancs megadásával 100, 102, 105, 106 és 107-es VLAN-ok hozhatók létre.

3.3.4

A portok VLAN-hoz rendele

Egy VLAN létrehozása után a következő lépés a portok VLAN-hoz rendelése.

A táblázat egy port hozzáférési portként történő definiálásának és VLAN-hoz rendelésének szintaktikáját mutatja. A **switchport mode access** utasítás ugyan opcionális, de mint biztonsági gyakorlatot erősen ajánlott. Ezzel a paranccsal az interfész szigorú hozzáférési módra vált. A hozzáférési mód azt jelzi, hogy a port egyetlen VLAN-hoz tartozik, és nem tárgyalja, hogy fővonali kapcsolattá váljon.

| TaskIOS CommandAdja meg a globális konfigurációs módot.Switch# configure terminalBelépés interfész konfigurációs módba.Switch(config)# interfész interfész-id Állítsa be a portot hozzáférési módba.Switch(config-if)# switchport mode access A port hozzárendelése egy VLAN-hoz.Switch(config-if )# switchport access vlan vlan-idVissza a privilegizált EXEC módba.Switch(config-if)# end | |
| --- | --- |
| **Feladat** | **IOS-parancs** |
| Lépjünk be a globális szabályozáss módba. | Switch# **konfiguráló terminál** |
| Lépjünk át interfészkonfigurációs módba. | Switch(config)# **interface** *interface-id* |
| Állítsuk a portot hozzáférési módba. | Switch(config-if)# **switchport mód hozzáférés** |
| Rendeljük a portot egy VLAN-hoz. | Switch(config-if)# **switchport access vlan**  *vlan-id* |
| Térjünk vissza a privilegizált EXEC módba. | Switch(config-if)# **end** |

**MEGJEGYZÉS:** Használjuk az **interface range** utasítást több interfész párhuzamos beállításához.

3.3.5

Példa a portok VLAN-hoz hozzárendelésére

Az ábrán az S1 switch F0/6 portja hozzáférési portként van konfigurálva és a 20-as VLAN-hoz van hozzárendelve. Az adott porthoz csatlakoztatott összes eszközt a 20-as VLAN-hoz lesz társítva. Ezért példánkban PC2 a 20-as VLAN-hoz tartozik.

A topológia egy diák PC-t, a 172.17.20.22 címen lévő PC2 gazdaszámítógépet mutatja, amely az S1 kapcsolóhoz van csatlakoztatva az F0/6 porton, amely az F0/1 porton keresztül csatlakozik az S2 kapcsolóhoz az F0/1 porton. Az S1 alatt az 1. kapcsoló olvasható: F0/6 port és VLAN 20.

S2S1PC2172.17.20.22F0/06F0/1F0/1

S1 kapcsoló:  
F0/06  
VLAN 20 portDiák PC

A példa az S1 beállításját mutatja, ahogy az F0/6 portot a 20-as VLAN-hoz rendeli.

S1# **configure terminal**

S1(config)# **interface fa0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 20**

S1(config-if)# **end**

A VLAN-ok konfigurálása a switchporton történik, nem pedig a végberendezésen. PC2-t a switchporton beállított VLAN-hoz tartozó IPv4-címmel és alhálózati maszkkal konfiguráljuk. Ebben a példában ez a VLAN 20. A 20-as VLAN más switch-eken történő beállításával a hálózati rendszergazdának kell az egyéb hallgatói számítógépeket a PC2-vel egy alhálózaton (172.17.20.0/24) lévőnek beállítani.

3.3.6

Adat és hang VLAN-ok

Egy hozzáférési port egyszerre csak egy adat VLAN-hoz tartozhat. Egy port azonban egy hang VLAN-hoz is társítható. Például az a port, amely egy IP-telefonhoz és egy végberendezéshez is csatlakozik két VLAN-hoz is tartozhat: egy hang és egy adat VLAN-hoz.

Vegyük az ábra topológiáját. PC5 a Cisco IP-telefonhoz van csatlakoztatva, amely viszont az S3-on lévő FastEthernet 0/18 interfészhez csatlakozik. A megvalósításhoz egy adat VLAN és egy hang VLAN van létrehozása.

A Host PC5 a Student VLAN 20-on található a 172.17.20.25 címen. A PC5 egy IP-telefonhoz csatlakozik, amely az F0/18-as porton az S3 kapcsolóhoz csatlakozik. Az erre a portra mutató nyíllal ellátott szövegdobozban ez olvasható: A switchportnak támogatnia kell a VLAN-forgalmat az IP-telefonra irányuló hangforgalomhoz és az adatforgalmat a PC5-höz. Az S3 az F0/3 porton keresztül csatlakozik az S1 kapcsolóhoz az F0/3 porton.

F0/3F0/3F0/18S1S3PC5

A kapcsolóportnak támogatnia kell a VLAN-forgalmat:

* Hangforgalom az IP-telefonhoz
* Adatforgalom PC-re5

**Diák  
VLAN 20 - 172.17.20.25**

3.3.7

Példa adat és hang VLAN-okra

A **switchport voice vlan***vlan-id* interfészkonfigurációs paranccsal rendelhetünk hang VLAN-t egy porthoz.

A hangforgalmat támogató LAN-okban általában a szolgáltatásminőség (QoS) is engedélyezve van. A hangforgalmat megbízhatónak kell jelölni, amint belép a hálózatba. Az **mls qos trust [ cos | készülék cisco-phone | dscp | ip-precedence ]** interfészációs paranccsal beállíthatjuk egy interfész megbízható állapotát, és megadhatjuk, hogy a csomag mezőit használja a forgalom osztályozására.

A példában mutatkozó konfigurálás a két VLAN-t (azaz a VLAN 20-at és a VLAN 150-et), majd az S3 F0/18-as interfészét switchportként rendelhető hozzá a VLAN 20-hoz. Emelett hangforgalmat rendel a VLAN 150-hez, és engedélyezi a QoS-osztályozást az IP-telefon által kijelölt szolgáltatási osztály (CoS) alapján.

S3(config)# **vlan 20**

S3(config-vlan)# **name student**

S3(config-vlan)# **vlan 150**

S3(config-vlan)# **name VOICE**

S3(config-vlan)# **exit**

S3(config)# **interface fa0/18**

S3(config-if)# **switchport mode access**

S3(config-if)# **switchport access vlan 20**

S3(config-if)# **mls qos trust cos**

S3(config-if)# **switchport voice vlan 150**

S3(config-if)# **end**

S3#

**MEGJEGYZÉS:** A QoS megvalósítása nagy ennek a tanfolyamnak a kereteit.

A **switchport access vlan** parancs kikényszeríti egy VLAN létrehozását, hogy még nem létezik a switch-en. A VLAN 30 például nem jelenik meg a switch **show vlan short** parancsának kimenetében. Ha a **switchport access vlan 30** parancsot olyan interfészen adjuk ki, amelyen nincs korábbi beállítás, akkor a switch a következőket jeleníti meg:

% Access VLAN does not exist. Creating vlan 30

3.3.8

VLAN-információk ellenőrzése

A VLAN konfigurálása után a VLAN-beállításokat a Cisco IOS **show** parancsaival ellenőrizhetjük.

A **show vlan** parancs megjelenítési az összes konfigurált VLAN kijelzést. A **show vlan** parancs opciókkal is használható. A teljes szintaxis a **show vlan [ short** | **id***vlan-id* | **név***vlan-név* | **összefoglaló** ] .

A táblázat a **show vlan** parancs beállításait ismerteti.

| TaskCommand Option Megjeleníti a VLAN nevét, állapotát és portjait egy VLAN soronként.brief Információkat jelenít meg az azonosított VLAN azonosító számról. A vlan-id esetében a tartomány 1-től 4094-ig terjed. vlan-id Információkat jelenít meg az azonosított VLAN-névről. A vlan-név egy 1 és 32 karakter közötti ASCII karakterlánc.name vlan-name Megjeleníti a VLAN összefoglaló információit.summary | |
| --- | --- |
| **Feladat** | **Parancsbeállítás** |
| Megjeleníti a VLAN nevét, állapotát és portjait, soronként egy VLAN adataival. | **rövid** |
| Egy adott azonosítószámú VLAN-al kapcsolatos információk térképe. For *vlan-id* értéke 1 és 4094 közötti lehet. | **id**  *vlan-id* |
| Egy adott nevű VLAN-al kapcsolatos információk térképe. The *vlan-name* egy 1 és 32 karakter közötti ASCII-karakterlánc. | **név**  *vlan-név* |
| Összefoglaló VLAN információs térkép | **összefoglaló** |

A **show vlan summary** parancs a konfigurált VLAN-ok számát adja vissza.

S1# **show vlan summary**

Number of existing VLANs : 7

Number of existing VTP VLANs : 7

Number of existing extended VLANS : 0

További hasznos parancsok a **show interfaces***interface-id***switchport** és a **show interfaces vlan***vlan-id* parancsok. A **show interfaces fa0/18 switchport** parancs például annak megerősítésére használható, hogy a Fastethernet 0/18 port megfelelően van-e hozzárendelve az adatokhoz és a hang VLAN-okhoz.

S1# **show interfaces fa0/18 switchport**

Name: Fa0/18

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 20 (student)

Trunking Native Mode VLAN: 1 (default)

Voice VLAN: 150

Administrative private-vlan host-association: none

(Output omitted)

3.3.9

Port VLAN-tagságának megváltoztatása

Egy port VLAN-tagságának a megváltoztatására többféle módszer létezik.

Ha a switch hozzáférési portja helytelenül lett hozzárendelve egy VLAN-hoz, akkor egyszerűen adjuk meg újra a **switchport access vlan***vlan-id* interfészkonfigurációs parancsot a helyes VLAN-azonosítóval. Tegyük fel például, hogy a Fa0/18 úgy lett helytelenül konfigurálva, hogy a VLAN 20 helyett az alapértelmezett VLAN 1-hez tartozik A port 20-as VLAN-hoz rendelhető egyszerűen gépeljük be a switchport access vlan 20 **parancsot** .

Ha egy port tagságát szeretnénk visszaállítani az alapértelmezett VLAN 1 értékre, használjuk a **no switchport access vlan** interfészkonfigurációs parancsot az ábrán látható módon.

A kimenetben például a Fa0/18 port az alapértelmezett VLAN 1-hez van rendelve, amit a **show vlan short** parancs is megerősít.

S1(config)# **interface fa0/18**

S1(config-if)# **no switchport access vlan**

S1(config-if)# **end**

S1#

S1# **show vlan brief**

VLAN Name Status Ports

---- ------------------ --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

20 student active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Figyeljük meg, hogy a 20-as VLAN továbbra is aktív, annak ellenére, hogy nincs hozzá rendelve.

A **show interfaces f0/18 switchport** kimenete annak ellenőrzésére is használható, hogy a hozzáférési VLAN az F0/18-as porton vissza lett-e állítva az 1-es VLAN-ra, amint az a kimeneten látható.

S1# **show interfaces fa0/18 switchport**

Name: Fa0/18

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: negotiate

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

3.3.10

VLAN-ok törlése

A **no vlan***vlan-id* globális beállításs parancs egy VLAN eltávolítására szolgál a switch-en vlan.dat fájlból.

**Caution** : Egy VLAN törlése először győződjünk meg arról, hogy minden hozzá tartozó port át lett helyezve egy másik VLAN-ba. Bármely port, amely nem lett egy aktív VLAN-ba áthelyezve, a VLAN törlése után egészen addig nem lesz képes más állomásokkal kommunikálni, amíg a hozzárendelése egy aktív VLAN-hoz nem történik.

A teljes vlan.dat fájl egy privilegizált EXEC móddal **delete flash:vlan.dat** parancsával törölhető. A parancs rövidített változata ( **delete vlan.dat** ) akkor használható, ha a vlan.dat fájl nem lett áthelyezve az alapértelmezett helyéről. A parancs kiadása és a switch újraindítása után a korábban konfigurált VLAN-ok többé nem lesznek elérhetők. Ezzel a switch megfelelően a gyári állapotba kerül a VLAN-beállítások tekintetében.

**Megjegyzés** : A Catalyst switch gyári állapotának visszaállításához húzzuk ki az összes kábelt a konzol- és a tápkábel kivételével a switch-ből. ezt adjuk ki az **erase startup-config** privilegizált EXEC módú parancsot, majd a **delete vlan.dat** parancsot.

3.3.11

Parancsszimulátor - VLAN-konfiguráció

A parancsszimulátorban az előírt követelmények alapján megadhatjuk és ellenőrizhetjük a switch interfészeinek VLAN-konfigurációját.

Complete the following steps to create a data VLAN:

* Enter global configuration mode.
* Create VLAN 20.
* Nevezze el a VLAN-t **tanulónak**.
* Return to privileged EXEC mode.

S1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#vlan 20

S1(config-vlan)#name student

S1(config-vlan)#end

\*Mar 31, 08:55:14.5555: %SYS-5-CONFIG\_I: Configured from console by console

Display the brief VLAN information.

S1#show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

20 student active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to create a voice VLAN:

* Enter global configuration mode.
* Create VLAN 150.
* Nevezze el a VLAN-t **VOICE**-nak.
* Return to global configuration mode.

S1#configure terminal

S1(config)#vlan 150

S1(config-vlan)#name VOICE

S1(config-vlan)#exit

Complete the following steps to assign the data and voice VLANs to a port:

* Enter interface configuration mode. Use **fa0/18** as the interface designation.
* Configure the port as an access port.
* Assign the data VLAN 20 to the port.
* Engedélyezze a QoS beállításokat az **mls qos trust cos** paranccsal.
* Assign the voice VLAN 150 to the port.
* Return to privileged EXEC mode.

S1(config)#interface fa0/18

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#mls qos trust cos

S1(config-if)#switchport voice vlan 150

S1(config-if)#end

Display the brief vlan information.

S1#show vlan brief

LAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/19, Fa0/20, Fa0/21

Fa0/22, Fa0/23, Fa0/24, Gi0/1

Gi0/2

20 student active Fa0/18

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to delete and verify a deleted VLAN on a port:

* Enter global configuration mode.
* Enter interface configuration mode. Use **fa0/18** as the interface designation.
* Remove the data VLAN from the port.
* Use the **do** form of the command to display brief VLAN information.

S1#configure terminal

S1(config)#interface fa0/18

S1(config-if)#no switchport access vlan

S1(config-if)#do show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

Gi0/1, Gi0/2

20 student active

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Complete the following steps to assign VLAN 20 to another interface.

* Enter interface configuration mode. Use **fa0/11** as the interface designation.
* Assign VLAN 20 to the port.
* Return to privileged EXEC mode.

S1(config-if)#interface fa0/11

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#end

Display the brief VLAN information.

S1#show vlan brief

LAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gig0/1, Gig0/2

20 student active Fa0/11

150 VOICE active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

Display the VLAN information specifically for the student VLAN.

S1#show vlan name student

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

20 student active Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

20 enet 100020 1500 - - - - - 0 0

Display summary information for VLANs

S1#mutasd vlan összefoglalót

Meglévő VLAN-ok száma: 7

Meglévő VTP VLAN-ok száma: 7

Meglévő kiterjesztett VLAN-ok száma: 0

Jelenítse meg a kapcsolóport információit. Használja **a fa0/11-et** az interfész kijelölésére.

S1#mutasd az interfész fa0/11 switchportját

Név: Fa0/11

Kapcsolóport: Engedélyezve

Adminisztrációs mód: statikus hozzáférés

Üzemmód: lefelé

Adminisztratív trönk beágyazása: dot1q

Működési csatorna-beágyazás: natív

Tranking tárgyalása: Ki

VLAN hozzáférési mód: 20 (tanulók)

Tranking natív módú VLAN: 1 (alapértelmezett)

Voice VLAN: nincs

(kimenet kimaradt)

Sikeresen konfigurálta és ellenőrizte a VLAN-konfigurációt a kapcsolófelületeken.

# VLAN-trönkök

3.4.1

## Trönkkonfigurációs parancsok

Most, hogy a VLAN-okat konfiguráltuk és ellenőriztük, itt az ideje a VLAN-trönkök konfigurációjának és ellenőrzésének. A VLAN trönk egy második rétegbeli kapcsolat két switch között, amely minden VLAN forgalmát továbbítja (hacsak az engedélyezett VLAN-ok listája manuálisan vagy dinamikusan nem korlátozott).

A trönkkapcsolatok engedélyezéséhez állítsuk be az összekötött portokat a táblázatban látható interfészkonfigurációs parancsokkal.

| TaskIOS CommandEnter globális konfigurációs mód.Switch# configure terminalLépjen interfész konfigurációs módba.Switch(config)# interface interface-id Állítsa be a portot állandó trönkelési módba.Switch(config-if)# switchport mode trunk A natív VLAN-t a VLAN 1-től eltérőre állítja be. Switch(config-if)# switchport trunk natív vlan vlan-id Adja meg a fővonali linken engedélyezhető VLAN-ok listáját.Switch(config-if)# switchport trunk enabled vlan vlan-listVissza a privilegizált EXEC módba.Switch(config- if)# vége | |
| --- | --- |
| **Feladat** | **IOS-parancs** |
| Lépjünk be a globális szabályozáss módba. | Switch# **konfiguráló terminál** |
| Lépjünk át interfészkonfigurációs módba. | Switch(config)# **interface** interface-id |
| Állítsuk a portot állandó trönk üzemmódba. | Switch(config-if)# **switchport mód trönk** |
| Állítsuk be a natív VLAN-t a VLAN 1-től eltérő értékre. | Switch(config-if)# **switchport trunk natív vlan** vlan-id |
| Adjuk meg a trönkkapcsolaton az engedélyezett VLAN-ok beállítását. | Switch(config-if)# **switchport trunk engedélyezett vlan** vlan-list |
| Térjünk vissza a privilegizált EXEC módba. | Switch(config-if)# **end** |

3.4.2

## Trönkkonfigurációs példa

Az ábrán a VLAN 10, 20 és 30 lettek az oktatói (Faculty), a hallgatói (Student) és a vendég (Guest) számítógépek (PC1, PC2 és PC3) számára kialakítva. Az S1 switch F0/1 portja trönknek lett konfigurálva és a 10-es, 20-as and 30-as VLAN-ok forgalmát továbbítja. Natív VLAN-nak a VLAN 99 lett beállítva.

A hálózati topológia három gazdagépet mutat különböző VLAN-okban, amelyek ugyanahhoz az S2 kapcsolóhoz csatlakoznak. A PC1 a kari VLAN 10-en található, 172.17.10.21 címmel. A PC2 a Student VLAN 20-on található 172.17.20.22 címmel. A PC3 a Guest VLAN 30-on található 172.17.30.23 címmel. Az S2 az F0/1 porton keresztül csatlakozik az S1 kapcsolóhoz az F0/1-nél. Ez a kapcsolat trunk felirattal van ellátva.

PC2PC1PC3S2S1F0/1F0/1

TörzsKari  
VLAN 10  
172.17.10.21Diák  
VLAN 20  
172.17.20.22Vendég  
VLAN 30  
172.17.30.23

Az egyes VLAN-okhoz társított alhálózatok a következők: VLAN 10 - Kar/Személyzet - 172.17.10.0/24 VLAN 20 - Diákok - 172.17.20.0/24 VLAN 30 - Vendégek - 172.17.30.0/24 VLAN -717 -24 VLAN -717 . .99,0/24

A példa az S1 switch F0/1 portjának trönkportként való konfigurálását mutatja. A natív VLAN le lett cserélve VLAN 99-re, és a trönkön engedélyezett VLAN-ok listája pedig le lett korlátozva 10, 20, 30 és 99-re.

S1(config)# **interface fastEthernet 0/1**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk native vlan 99**

S1(config-if)# **switchport trunk allowed vlan 10,20,30,99**

S1(config-if)# **end**

**Megjegyzés** : Ez a konfiguráció feltételezi a Cisco Catalyst 2960 kapcsolók használatát, amelyek automatikusan 802.1Q tokozást használnak a fővonali kapcsolatokon. Más típusú switch-eken szükség lehet a beágyazás manuális beállítására. Egy trönkkapcsolat mindkét végét mindig ugyanazzal a natív VLAN-al konfiguráljuk. Ha a 802.1Q trönkkonfiguráció nem ugyanaz a két végen, akkor a Cisco IOS szoftver hibát jelez.

3.4.3

## Trönkbeállítások ellenőrzése

A parancskimenet az S1 switch F0/1 portjának beállítását mutatja. A kontrolle a **show interfaces**interface-id **switchport** paranccsal történik.

S1# **show interfaces fa0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 99 (VLAN0099)

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk associations: none

Administrative private-vlan trunk private VLANs: none

Operational private-vlan: none

Trunking VLANs Enabled: 10,20,30,99

Pruning VLANs Enabled: 2-1001

**(output omitted)**

A felső kiemelt rész megmutatja, hogy az F0/1 port adminisztrációs módnak (Administrative Mode) beállítás **trunk** . A port tehát trönk módban van. A következő kiemelt terület igazolja, hogy a VLAN 99 a natív VLAN. A parancskimenetben lejjebb látható kiemelt rész jelzi, hogy a trönkön valamennyi VLAN (10, 20, 30 és 99) engedélyezve van.

Egy másik hasznos parancs a veryfing trunk interfészek számára a parancs. **Megjegyzés** : **az interfész törzsének megjelenítése**

3.4.4

## A trönk visszaállítása alapértelmezett állapotra

A **no switchport trunk enabled vlan** és a **no switchport trunk native vlan** parancsokkal eltávolíthatjuk az engedélyezett VLAN-okat, és alaphelyzetbe állíthatjuk a trönk natív VLAN-ját. Az állapot visszaállítása után a trönk valamennyi VLAN-t engedélyezi, és a VLAN 1-et használja natív VLAN-ként. A példa egy trönkinterfész trönkölési alapbeállításainak a visszaállítására szolgáló parancsokat mutatja.

S1(config)# **interface fa0/1**

S1(config-if)# **no switchport trunk allowed vlan**

S1(config-if)# **no switchport trunk native vlan**

S1(config-if)# **end**

A **show interfaces f0/1 switchport** parancs megmutatja, hogy a fővonalat alapállapotba állítottuk át.

S1# **show interfaces fa0/1 switchport**

Name: Fa0/1

Switchport: Enabled

Administrative Mode: trunk

Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: dot1q

Negotiation of Trunking: On

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

Administrative private-vlan host-association: none

Administrative private-vlan mapping: none

Administrative private-vlan trunk native VLAN: none

Administrative private-vlan trunk Native VLAN tagging: enabled

Administrative private-vlan trunk encapsulation: dot1q

Administrative private-vlan trunk normal VLANs: none

Administrative private-vlan trunk associations: none

Administrative private-vlan trunk mappings: none

Operational private-vlan: none

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

**(output omitted)**

Az ábrán látható példa az S1 switch F0/1 portjáról a trönktulajdonság eltávolítására szolgáló utasításokat mutatja. A **show interfaces f0/1 switchport** utasítás igazolja, hogy az F0/1 interfész most valóban statikus hozzáférési módban van.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **end**

**S1# show interfaces fa0/1 switchport**

**Name: Fa0/1**

**Switchport: Enabled**

**Administrative Mode: static access**

**Operational Mode: static access**

**Administrative Trunking Encapsulation: dot1q**

**Operational Trunking Encapsulation: native**

**Negotiation of Trunking: Off**

**Access Mode VLAN: 1 (default)**

**Trunking Native Mode VLAN: 1 (default)**

**Administrative Native VLAN tagging: enabled**

**(output omitted)**

Dynamic Trunking Protocol

3.5.1

A DTP bemutatása

Egy C switch-ek olyan protokollal rendelkezik, amely lehetővé teszi a gyártónak, hogy a szomszédos eszközzel a trönkölésről. Ezt a protokollt Dynamic Trunking Protocol (DTP) néven ismerjük. A DTP felgyorsíthatja a hálózati rendszergazda számára a szabályozáss folyamatot. Az Ethernet trönkinterfészek különböző trönkölési módokat támogatnak. Egy interfész trönk (trunking) vagy nem trönk (nontrunking) módúra konfigurálható, illetve megadható az is, hogy a trönkölést egyeztesse a csatlakozó szomszédos interfésszel. A hálózati eszközök között a trönk egyeztetést a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP)kötött.

A DTP a Cisco szabadalmaztatott protokollja, amely a Catalyst 2960 és Catalyst 3650 sorozatú switch-eken automatikusan engedélyezve van. A DTP a trönk egyeztetést csak akkor hajtja végre, ha a szomszédos switch-en lévő port is olyan trönkmódra van beállítva, amely támogatja a DTP-t. Más gyártók switch-ei nem támogatják a DTP-t.

**Figyelem** : Egyes internetes eszközök hibásan továbbíthatják a DTP-kereteket, ami hibás konfigurációkat okozhat. Ennek elkerülése érdekében kapcsoljuk ki a DTP-t a Cisco switch-et azon interfésein, ami olyan eszközökhöz csatlakozik, amelyek nem támogatják a DTP-t.

A Cisco Catalyst 2960 és 3650 switch-ek beállított DTP-konfigurációja a dinamikus automatikus (dinamikus automatikus).

Egy Cisco switch és egy a DTP-t nem támogató eszköz, amely lehetővé teszi, hogy a **switchport mode trunk** és a **switchport nonegotiate** interfészkonfigurációs parancsokat használhassa. Ennek eredményeként az interfész trönk lesz, ezért nem generál DTP-kereteket.

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport nonegotiate**

A dinamikus trönkprotokoll újbóli engedélyezéséhez használjuk a **switchport mode dynamic auto** parancsot.

S1(config-if)# **switchport mode dynamic auto**

Ha a két switch-et összekötő portok úgy vannak beva, hogy a **switchport mode trunk** és a **switchport nonegotiate** parancsokkal figyelmen kívül hagyják az összes DTP-hirdetményt, a portok trönk módban maradnak. Ha az összekötő portok dinamikus automatikus beállítással rendelkezik, akkor nem egyeztetnek a trönkről, és hozzáférési módban maradnak, létesítve egy inaktív trönköt.

Amikor egy portot trönk üzemmódra konfigurálunk, használjuk a **switchport mode trunk** parancsot. Ilyenkor nem kétséges, hogy a trönk milyen állapotban van: mindig be van kapcsolva.

3.5.2

Egyeztetett interfészmódok

A **switchport mode** parancs további opciókkal rendelkezik az interfész üzemmódjának egyeztetéséhez. A parancs teljes szintaxisa a következő:

Switch(config-if)# **switchport mód** { **hozzáférés** | **dynamic** { **auto** | **kívánatos** } | **csomagtartó** }

Az opciók leírása a táblázatban található.

| OptionDescriptionaccessPuts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link.The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.dynamic autoMakes the interface able to convert the link to a trunk link.The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode.The default switchport mode for all Ethernet interfaces is dynamic auto.dynamic desirableMakes the interface actively attempt to convert the link to a trunk link.The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or dynamic auto mode. trunkPuts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link.The interface becomes a trunk interface even if the neighboring interface is not a trunk interface. | |
| --- | --- |
| **Beállítás** | **Leírás** |
| **hozzáférés** | * Az interfészt (szolgáltatási portot) állandó nem trönk módba helyezi, és egyeztet a kapcsolat nem trönkkapcsolattá alakításáról. * Az interfész hozzáférési (nem trönk) interfésszé válik, független attól, hogy a szomszédos interfész trönk interfész-e vagy sem. |
| **dinamikus automata** | * Képessé teszi az interfészt, hogy a kapcsolatot trönkkapcsolattá alakítsa. * Az interfész trönk interfésszé válik, ha a szomszédos interfész trönk (trunk) vagy induló (desirable) módra van beállítva. * Az összes Ethernet interfész alapértelmezett kapcsolóport-módja a **dinamikus automatikus** . |
| **dinamikus kívánatos** | * Az interfész aktívan megkísérli átalakítani a hivatkozást fővonali hivatkozássá. * Az interfész fővonali interfész lesz, ha a szomszédos interfész fővonali, kívánatos vagy dinamikus automatikus módra van állítva. |
| **törzs** | * Állandó trunking módba helyezi az interfészt, és egyezteti a szomszédos hivatkozás fővonali kapcsolattá alakítását. * Az interfész trönk interfésszé válik, attól függetlenül, hogy a szomszédos interfész esetleg nem trönk interfész. |

A **switchport nonegotiate** interfészkonfigurációs paranccsal leállíthatjuk a DTP-egyeztetést. A switch nem folytatja a DTP-egyeztetést ezen az interfészeken. Ez az utasítás csak akkor használható, ha a switchport beállítás **access** vagy **trunk** . Trönkkapcsolat kiépítéséhez a szomszédos interfészt manuálisan trönk interfésznek kell beállítani.

3.5.3

A DTP-konfiguráció eredményei

A táblázat a DTP-konfiguráció lehetséges kimeneteit mutatja egy Catalyst 2960 switchportokhoz csatlakozó trönkkapcsolat átellenes végeinek a függvényében. Amikor csak lehetséges, a trönkkapcsolatokat statikusan állítsuk be.

| Dynamic AutoDynamic DesirableTrunkAccessDynamic AutoAccessTrunkTrunkAccessDynamic DesirableTrunkTrunkTrunkAccessTrunkTrunkTrunkTrunkLimited connectivityAccessAccessAccessLimited connectivityAccess | | | | |
| --- | --- | --- | --- | --- |
|  | **Dynamic Auto** | **Dinamikus kívánatos** | **Törzs** | **Hozzáférés** |
| **Dynamic Auto** | Hozzáférés | Törzs | Törzs | Hozzáférés |
| **Dinamikus kívánatos** | Törzs | Törzs | Törzs | Hozzáférés |
| **Törzs** | Törzs | Törzs | Törzs | Korlátozott kapcsolat |
| **Hozzáférés** | Hozzáférés | Hozzáférés | Korlátozott kapcsolat | Hozzáférés |

3.5.4

A DTP-mód ellenőrzése

Az alapértelmezett DTP-mód függ a Cisco IOS szoftver verziójától és a platformtól. A DTP-mód látható adjuk ki a **show dtp interfész** parancsot a kimenetben látható módon.

S1# **show dtp interface fa0/1**

DTP information for FastEthernet0/1:

TOS/TAS/TNS: ACCESS/AUTO/ACCESS

TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE

Neighbor address 1: C80084AEF101

Neighbor address 2: 000000000000

Hello timer expiration (sec/state): 11/RUNNING

Access timer expiration (sec/state): never/STOPPED

Negotiation timer expiration (sec/state): never/STOPPED

Multidrop timer expiration (sec/state): never/STOPPED

FSM state: S2:ACCESS

# times multi & trunk 0

Enabled: yes

In STP: no

## Miről tanultunk ebben a fejezetben?

**A VLAN-ok áttekintése**

A virtuális LAN (VLAN) olyan eszközök csoportja, amelyek úgy kommunikálnak egymással, mintha ugyanarra a vezetékre csatlakoznának. A VLAN-ok a fizikai kapcsolatok helyett logikai kapcsolatokra épülnek. A rendszergazdák a VLAN-okat hálózatok szegmentálására hasznos olyan szempontok alapján, mint a funkció, a csapat vagy az alkalmazás. Minden VLAN külön logikai hálózatnak megfelelő. Bármely switchport tartozhat egy VLAN-hoz. Egy VLAN akár több fizikai LAN-szegmensre kiterjedő szórási tartományt is alkothat. A VLAN-ok javítják a hálózat teljesítményét, mivel a nagyméretű szórási tartományokat kisebbekre osztják fel. Egy kapcsolt hálózatban minden VLAN egy IP-alhálózatnak felel meg, ezért VLAN tervezéskor a hierarchikus hálózatcímzési tervet kell használni. A VLAN-ok típusai közé tartozik az alapértelmezett VLAN, az adat VLAN-ok,

**VLAN-ok többszörösen kapcsolt környezetben**

A VLAN-trönk nem tartozik egy adott VLAN-hoz. Ez egy csatorna több VLAN számára a switch-ek és routerek között. A VLAN-trönk egy pont-pont kapcsolat két olyan hálózati eszközzel, amely egynél több VLAN forgalmát is továbbítja. A VLAN-trönk kiterjeszti a VLAN-okat a hálózat egészére. Amikor egy switch-en VLAN-okat használunk, akkor egy meghatározott VLAN-ba tartozó állomás egyedi- és csoportos címzésű, valamint szórásos forgalmának a szállítása kizárólag azokra az eszközökre fog korlátozódni, amelyek ugyanabba a VLAN-ba tartoznak. A VLAN-címke mezői közé tartozik egy típus, a felhasználói prioritás, a CFI és a VID. Egyes eszközök VLAN-címkét adnak a natív VLAN forgalomhoz. Ha egy 802.1Q trönkport natív VLAN ID-vel megcímkézett keretet fogad, akkor eldobja azt. A VoIP (Voice over IP) adatforgalom egy különálló VLAN szükséges. A hangforgalomra QoS és biztonsági házirendek alkalmazhatók. A hang VLAN forgalmát megfelelő 2. rétegbeli CoS prioritási értékkel kell ellátni.

**VLAN konfiguráció**

A különböző Cisco Catalyst switch-ek eltérő számú VLAN-t támogatnak, amely egy normál tartományú VLAN-okat és egy kiterjesztett tartományú VLAN-okat. Amikor tartományú VLAN-okat konfigurálunk, akkor a részletes beállítás egy kapcsoló flash memóriájában egy vlan.dat nevű fájlban tárolódik. Bár nem kötelező, de jó gyakorlat az aktív beállításainak mentése az indítási beállításba. Egy VLAN létrehozása után a következő lépés a portok VLAN-hoz rendelése. Egy port hozzáférési portként történő meghatározáshoz és VLAN-hoz rendeléséhez több parancs is rendelkezésre áll. A VLAN-ok konfigurálása a switchporton történik, nem pedig a végberendezésen. Egy hozzáférési port egyszerre csak egy adat VLAN-hoz tartozhat. Egy port azonban egy hang VLAN-hoz is társítható. Például az a port, amely egy IP-telefonhoz és egy végberendezéshez is csatlakozik két VLAN-hoz is tartozhat: egy hang és egy adat VLAN-hoz. A VLAN konfigurálása után a VLAN-beállításokat a Cisco IOS**show** parancsaival ellenőrizhetjük. Ha a switch hozzáférési portja helytelenül lett hozzárendelve egy VLAN-hoz, akkor egyszerűen adjuk meg újra a **switchport access vlan**vlan-id interfészkonfigurációs parancsot a helyes VLAN-azonosítóval. A **no vlan**vlan-id globális beállításs parancs egy VLAN eltávolítására szolgál a switch-en vlan.dat fájlból.

**VLAN trönkek**

A VLAN trönk egy OSI második rétegbeli link két kapcsoló között, amely valamennyi VLAN forgalmát továbbítja. Az összekapcsolódó portok konfigurálásához több parancs is létezik. A VLAN-trönk beállításának ellenőrzéséhez használjuk a **show interfaces**Interface-ID **switchport** parancsot. A **no switchport trunk enabled vlan** és a **no switchport trunk native vlan** parancsokkal eltávolíthatjuk az engedélyezett VLAN-okat, és visszaállíthatja a trönk natív VLAN-ját.

**Dynamic Trunking Protocol**

Egy interfész trönk (trunking) vagy nem trönk (nontrunking) módúra konfigurálható, illetve megadható az is, hogy a trönkölést egyeztesse a csatlakozó szomszédos interfésszel. A hálózati eszközök között a trönk egyeztetését a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP)kötött. A DTP a Cisco saját protokollja, amely a trönk egyeztetését csak akkor hajtja végre, ha a szomszédos switch-en lévő port is olyan trönkmódra van beállítva, amely támogatja a DTP-t. Egy Cisco switch és egy a DTP-t nem támogató eszköz, amely lehetővé teszi, hogy a **switchport mode trunk** és a **switchport nonegotiate** interfészkonfigurációs parancsokat használhassa. Kapcsoló **mód**parancs további opciókkal rendelkezik az interfész üzemmódjának egyeztetéséhez, tartalmazza az access, dynamic auto, dynamic desirable és trunk beállításokat. Az aktuális DTP-mód ellenőrzéséhez adjuk ki a **show dtp interface** parancsot.

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. VLANs
2. Dynamic Trunking Protocol

# Dynamic Trunking Protocol

3.5.1

## A DTP bemutatása

Egyes Cisco switch-ek olyan gyártói protokollal rendelkeznek, amely lehetővé teszi számukra, hogy automatikusan egyeztessenek a szomszédos eszközzel a trönkölésről. Ezt a protokollt Dynamic Trunking Protocol (DTP) néven ismerjük. A DTP felgyorsíthatja a hálózati rendszergazda számára a konfigurációs folyamatot. Az Ethernet trönkinterfészek különböző trönkölési módokat támogatnak. Egy interfész trönk (trunking) vagy nem trönk (nontrunking) módúra konfigurálható, illetve megadható az is, hogy a trönkölést egyeztesse a hozzá csatlakozó szomszédos interfésszel. A hálózati eszközök között a trönk egyeztetést a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP) végzi.

A DTP a Cisco szabadalmaztatott protokollja, amely a Catalyst 2960 és Catalyst 3650 sorozatú switch-eken automatikusan engedélyezve van. A DTP a trönk egyeztetést csak akkor hajtja végre, ha a szomszédos switch-en lévő port is olyan trönkmódra van beállítva, amely támogatja a DTP-t. Más gyártók switch-ei nem támogatják a DTP-t.

**Caution**: Some internetworking devices might forward DTP frames improperly, which can cause misconfigurations. Ennek elkerülése érdekében kapcsoljuk ki a DTP-t a Cisco switch azon interfészein, amelyek olyan eszközökhöz csatlakoznak, amelyek nem támogatják a DTP-t.

A Cisco Catalyst 2960 és 3650 switch-ek alapértelmezett DTP-konfigurációja a dinamikus automatikus (dynamic auto).

Egy Cisco switch és egy a DTP-t nem támogató eszköz között a trönkölés engedélyezéséhez használjuk a **switchport mode trunk** és a **switchport nonegotiate** interfészkonfigurációs parancsokat. Ennek eredményeként az interfész trönk lesz, ugyanakkor nem generál DTP-kereteket.

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport nonegotiate**

A dinamikus trönkprotokoll újbóli engedélyezéséhez használjuk a **switchport mode dynamic** **auto** parancsot.

S1(config-if)# **switchport mode dynamic auto**

Ha a két switch-et összekötő portok úgy vannak beállítva, hogy a **switchport mode trunk** és a **switchport nonegotiate** parancsokkal figyelmen kívül hagyják az összes DTP-hirdetményt, a portok trönk módban maradnak. Ha az összekötő portok dinamikus automatikus beállítással rendelkeznek, akkor nem egyeztetnek a trönkről, és hozzáférési módban maradnak, létrehozva egy inaktív trönkkapcsolatot.

Amikor egy portot trönk üzemmódra konfigurálunk, használjuk a **switchport mode trunk** parancsot. Ilyenkor nem kétséges, hogy a trönk milyen állapotban van: mindig be van kapcsolva.

3.5.2

## Egyeztetett interfészmódok

A **switchport mode** parancs további opciókkal rendelkezik az interfész üzemmódjának egyeztetéséhez. A parancs teljes szintaxisa a következő:

Switch(config-if)# **switchport mode** { **access** | **dynamic** { **auto** | **desirable** } | **trunk** }

Az opciók leírása a táblázatban található.

| OptionDescriptionaccessPuts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link.The interface becomes a nontrunk interface, regardless of whether the neighboring interface is a trunk interface.dynamic autoMakes the interface able to convert the link to a trunk link.The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode.The default switchport mode for all Ethernet interfaces is dynamic auto.dynamic desirableMakes the interface actively attempt to convert the link to a trunk link.The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or dynamic auto mode. trunkPuts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link.The interface becomes a trunk interface even if the neighboring interface is not a trunk interface. | |
| --- | --- |
| **Beállítás** | **Leírás** |
| **access** | * Az interfészt (hozzáférési portot) állandó nem trönk módba helyezi, és egyeztet a kapcsolat nem trönkkapcsolattá alakításáról. * Az interfész hozzáférési (nem trönk) interfésszé válik, függetlenül attól, hogy a szomszédos interfész trönk interfész-e vagy sem. |
| **dynamic auto** | * Képessé teszi az interfészt, hogy a kapcsolatot trönkkapcsolattá alakítsa. * Az interfész trönk interfésszé válik, ha a szomszédos interfész trönk (trunk) vagy kezdeményező (desirable) módra van beállítva. * The default switchport mode for all Ethernet interfaces is **dynamic auto**. |
| **dynamic desirable** | * Makes the interface actively attempt to convert the link to a trunk link. * The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or dynamic auto mode. |
| **trunk** | * Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. * Az interfész trönk interfésszé válik, függetlenül attól, hogy a szomszédos interfész esetleg nem trönk interfész. |

A **switchport nonegotiate** interfészkonfigurációs paranccsal leállíthatjuk a DTP-egyeztetést. A switch nem folytat DTP-egyeztetést ezen az interfészen. Ez az utasítás csak akkor alkalmazható, ha a switchport beállítása **access** vagy **trunk**. Trönkkapcsolat kiépítéséhez a szomszédos interfészt manuálisan trönk interfésznek kell beállítani.

3.5.3

## A DTP-konfiguráció eredményei

A táblázat a DTP-konfiguráció lehetséges kimeneteit mutatja egy Catalyst 2960 switchportokhoz csatlakozó trönkkapcsolat átellenes végeinek a függvényében. Amikor csak lehetséges, a trönkkapcsolatokat statikusan állítsuk be.

| Dynamic AutoDynamic DesirableTrunkAccessDynamic AutoAccessTrunkTrunkAccessDynamic DesirableTrunkTrunkTrunkAccessTrunkTrunkTrunkTrunkLimited connectivityAccessAccessAccessLimited connectivityAccess | | | | |
| --- | --- | --- | --- | --- |
|  | **Dynamic Auto** | **Dinamikus kívánatos** | **Törzs** | **Hozzáférés** |
| **Dynamic Auto** | Hozzáférés | Törzs | Törzs | Hozzáférés |
| **Dinamikus kívánatos** | Törzs | Törzs | Törzs | Hozzáférés |
| **Törzs** | Törzs | Törzs | Törzs | Korlátozott kapcsolat |
| **Hozzáférés** | Hozzáférés | Hozzáférés | Korlátozott kapcsolat | Hozzáférés |

3.5.4

## A DTP-mód ellenőrzése

Az alapértelmezett DTP-mód függ a Cisco IOS szoftver verziójától és a platformtól. A DTP-mód megtekintéséhez adjuk ki a **show dtp interface** parancsot a kimenetben látható módon.

S1# **show dtp interface fa0/1**

DTP information for FastEthernet0/1:

TOS/TAS/TNS: ACCESS/AUTO/ACCESS

TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE

Neighbor address 1: C80084AEF101

Neighbor address 2: 000000000000

Hello timer expiration (sec/state): 11/RUNNING

Access timer expiration (sec/state): never/STOPPED

Negotiation timer expiration (sec/state): never/STOPPED

Multidrop timer expiration (sec/state): never/STOPPED

FSM state: S2:ACCESS

# times multi & trunk 0

Enabled: yes

In STP: no

**Note** : A general best practice is to set the interface to **trunk** and **nonegotiate** when a trunk link is required. Azokon az interfészeken, amelyeken nem akarunk trönkölni, a DTP-t ki kell kapcsolni.

3.5.5

## Packet Tracer - A DTP beállítása

A Packet Tracer feladat során beállítjuk, majd ellenőrizzük a DTP működését.

[DTP konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/3.5.5-packet-tracer---configure-dtp_hu-HU.pka)

3.5.6

## Tudáspróba - Dynamic Trunking Protocol

Az űrlap teteje

Ellenőrizze, hogy megértette-e a Dynamic Trunking Protocolt, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Igaz vagy hamis? A DTP egy nyílt szabványú IEEE protokoll, amely meghatározza a kapcsoló fővonali kapcsolatainak automatikus egyeztetését.

Az űrlap alja

Mi az alapértelmezett switchport mód a Cisco Catalyst kapcsolókhoz?

Igaz vagy hamis? Egy link két kapcsolóportja, amelyek mindegyike dinamikus automatikusként van konfigurálva, sikeresen egyeztet egy fővonalat.

Which two DTP modes will form a trunk with an interface that is configured as dynamic auto? (Két jó válasz van.)

[3.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-trönkök](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[3.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. VLANs
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

3.6.1

## Packet Tracer — A VLAN-ok és a trönkölés megvalósítása

A Packet Tracer feladat során a következőket fogjuk elvégezni:

* VLAN-ok konfigurálása
* Portok VLAN-okhoz rendelése
* Statikus trönkölés konfigurálása
* Dinamikus trönkölés konfigurálása

[VLAN-ok és trönkölés konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/3.6.1-packet-tracer---implement-vlans-and-trunking_hu-HU.pka)

3.6.2

## Laborgyakorlat — A VLAN-ok és a trönkölés megvalósítása

A laborgyakorlat során a következőket fogjuk elvégezni:

* Hálózat felépítése és az eszközök alapkonfigurációjának elvégzése
* VLAN-ok létrehozása és a switchportok hozzájuk rendelése
* 802.1Q trönk konfigurálása a switch-ek között

3.6.3

## Miről tanultunk ebben a fejezetben?

**A VLAN-ok áttekintése**

A virtuális LAN (VLAN) olyan eszközök csoportja, amelyek úgy kommunikálnak egymással, mintha ugyanarra a vezetékre csatlakoznának. A VLAN-ok a fizikai kapcsolatok helyett logikai kapcsolatokra épülnek. A rendszergazdák a VLAN-okat a hálózatok szegmentálására használják olyan szempontok alapján, mint a funkció, a csapat vagy az alkalmazás. Minden egyes VLAN külön logikai hálózatnak minősül. Bármely switchport tartozhat egy VLAN-hoz. Egy VLAN akár több fizikai LAN-szegmensre kiterjedő szórási tartományt is alkothat. A VLAN-ok javítják a hálózat teljesítményét, mivel a nagyméretű szórási tartományokat kisebbekre osztják fel. Egy kapcsolt hálózatban valamennyi VLAN egy IP-alhálózatnak felel meg, ezért VLAN tervezéskor a hierarchikus hálózatcímzési tervet kell használni. A VLAN-ok típusai közé tartozik az alapértelmezett VLAN, az adat VLAN-ok, a natív VLAN, a felügyeleti VLAN-ok és a hang VLAN-ok.

**VLAN-ok többszörösen kapcsolt környezetben**

A VLAN-trönk nem tartozik egy adott VLAN-hoz. Ez egy csatorna több VLAN számára a switch-ek és routerek között. A VLAN-trönk egy pont-pont kapcsolat két olyan hálózati eszköz között, amelyek egynél több VLAN forgalmát is továbbítják. A VLAN-trönk kiterjeszti a VLAN-okat a hálózat egészére. Amikor egy switch-en VLAN-okat használunk, akkor egy meghatározott VLAN-ba tartozó állomás egyedi- és csoportos címzésű, valamint szórásos forgalmának a továbbítása kizárólag azokra az eszközökre fog korlátozódni, amelyek ugyanabba a VLAN-ba tartoznak. A VLAN-címke mezői közé tartoznak a típus, a felhasználói prioritás, a CFI és a VID. Egyes eszközök VLAN-címkét adnak a natív VLAN forgalomhoz. Ha egy 802.1Q trönkport natív VLAN ID-vel megcímkézett keretet fogad, akkor eldobja azt. A VoIP (Voice over IP) adatforgalom továbbítására egy elkülönített VLAN szükséges. A hangforgalomra QoS és biztonsági házirendek alkalmazhatók. A hang VLAN forgalmát megfelelő 2. rétegbeli CoS prioritási értékkel kell ellátni.

**VLAN konfiguráció**

A különböző Cisco Catalyst switch-ek eltérő számú VLAN-t támogatnak, beleértve a normál tartományú VLAN-okat és a kiterjesztett tartományú VLAN-okat. Amikor normál tartományú VLAN-okat konfigurálunk, akkor a részletes konfiguráció a kapcsoló flash memóriájában egy vlan.dat nevű fájlban tárolódik. Bár nem kötelező, de jó gyakorlat az aktív konfiguráció módosításainak mentése az indítási konfigurációba. Egy VLAN létrehozása után a következő lépés a portok VLAN-hoz rendelése. Egy port hozzáférési portként történő definiálásához és VLAN-hoz rendeléséhez több parancs is rendelkezésre áll. A VLAN-ok konfigurálása a switchporton történik, nem pedig a végberendezésen. Egy hozzáférési port egyszerre csak egy adat VLAN-hoz tartozhat. Egy port azonban egy hang VLAN-hoz is társítható. Például az a port, amely egy IP-telefonhoz és egy végberendezéshez is csatlakozik két VLAN-hoz is tartozhat: egy hang és egy adat VLAN-hoz. A VLAN konfigurálása után a VLAN-beállításokat a Cisco IOS **show** parancsaival ellenőrizhetjük. Ha a switch hozzáférési portja helytelenül lett hozzárendelve egy VLAN-hoz, akkor egyszerűen adjuk meg újra a **switchport access vlan** vlan-id interfészkonfigurációs parancsot a helyes VLAN-azonosítóval. A **no vlan** vlan-id globális konfigurációs parancs egy VLAN eltávolítására szolgál a switch-en található vlan.dat fájlból.

**VLAN trönkek**

A VLAN trönk egy OSI második rétegbeli link két kapcsoló között, amely valamennyi VLAN forgalmát továbbítja. Az összekapcsolódó portok konfigurálásához több parancs is létezik. A VLAN-trönk konfigurációjának ellenőrzéséhez használjuk a **show interfaces** Interface-ID **switchport** parancsot. A **no switchport trunk allowed vlan** és a **no switchport trunk native vlan** parancsokkal eltávolíthatjuk az engedélyezett VLAN-okat, és visszaállíthatja a trönk natív VLAN-ját.

**Dynamic Trunking Protocol**

Egy interfész trönk (trunking) vagy nem trönk (nontrunking) módúra konfigurálható, illetve megadható az is, hogy a trönkölést egyeztesse a hozzá csatlakozó szomszédos interfésszel. A hálózati eszközök között a trönk egyeztetését a pont-pont alapon működő dinamikus trönkprotokoll (Dynamic Trunking Protocol, DTP) végzi. A DTP a Cisco saját protokollja, amely a trönk egyeztetését csak akkor hajtja végre, ha a szomszédos switch-en lévő port is olyan trönkmódra van beállítva, amely támogatja a DTP-t. Egy Cisco switch és egy a DTP-t nem támogató eszköz között a trönkölés engedélyezéséhez használjuk a **switchport mode trunk** és a **switchport nonegotiate** interfészkonfigurációs parancsokat. A **switchport mode** parancs további opciókkal rendelkezik az interfész üzemmódjának egyeztetéséhez, beleértve az access, dynamic auto, dynamic desirable és trunk beállításokat. Az aktuális DTP-mód ellenőrzéséhez adjuk ki a **show dtp interface** parancsot.

3.6.4

## Ellenőrző kvíz - VLAN-ok

Az űrlap teteje

1. Mi történik egy 10-es VLAN-hoz társított porttal, ha a VLAN-t eltávolítjuk a switch-ről?

Az űrlap alja

Egy Catalyst switch-en melyik memóriahelyen tárolódnak a VLAN beállítások normál tartományú VLAN-ok esetén?

A rendszergazda egy Cisco és egy másik gyártó switch-e közti trönk vonal hibáját próbálja felderíteni. After a few **show** commands, the administrator notices that the switches are not negotiating a trunk. Mi lehet a probléma oka?

Mi a vlan.dat fájl funkciója a switch-eken?

Miért különítjük el a natív VLAN-t az adat VLAN-októl?

Amikor egy Cisco switch 802.1Q trönk portja címkézetlen kereteket fogad, alapértelmezés szerint melyik VLAN felé továbbítja a forgalmat?

A hálózati rendszergazda a VLAN trönk kapcsolatok kiépítését tervezi. Melyik két pont-pont összeköttetést használhatja VLAN trönkvonalként​? (Két jó válasz van.)

Milyen három fő előnye van a VLAN-ok használatának? (Három jó válasz van.)

Hol tárolódnak a kiterjesztett tartományú VLAN információk a Cisco switch-eken?

Alapértelmezés szerint hol tárolódnak Cisco switch-eken a normál tartományú VLAN-ok?

Melyik VLAN típust használja a rendszergazda a switch eléréséhez és konfigurálásához?

Milyen okból használja a hálózati rendszergazda a **show interfaces trunk** parancsot egy switchen?

Hol található a vlan.dat fájl egy switch-en?

Ha egy szervezet olyan fejlesztést hajt végre, hogy Cisco IP-telefonokat is használni fog a hálózatában, milyen tervezési funkciót kell figyelembe venni a hangminőség biztosításához?

Egy Cisco switch-en jelenleg engedélyezett a 10-es és a 20-as VLAN forgalma az Fa0/5-ös trönk porton. What is the effect of issuing a **switchport trunk allowed vlan 30** command on Fa0/5?

[3.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Dynamic Trunking Protocol](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. Bevezetés

# Bevezetés

4.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a VLAN-ok közötti forgalomirányításról szóló fejezetben!

Most már tudjuk, hogyan szegmentálhatjuk és szervezhetjük a hálózatunkat VLAN-okba. Az állomások kommunikálni tudnak az ugyanabban a VLAN-ban lévő többi állomással, és többé nem lesznek olyan állomásaink, amelyek szórásos üzeneteket küldenek minden más eszköznek a hálózatban, felemésztve a szükséges sávszélességet. De mi van akkor, ha az egyik VLAN-ban lévő állomásnak egy másik VLAN-ban lévő állomással kell kommunikálnia? Ha hálózati rendszergazdák vagyunk, akkor tudjuk, hogy az emberek a saját hálózatukon kívül is szeretnének kommunikálni másokkal. Ebben segíthet a VLAN-ok közötti forgalomirányítás. A VLAN-ok közötti forgalomirányítás egy 3. rétegbeli eszközt, például egy routert vagy egy 3. rétegbeli switch-et használ. Vegyük a VLAN-szakértelmünket, kombináljuk a hálózati rétegbeli ismereteinkkel, és tegyük őket próbára!

4.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe: Inter-VLAN Routing**

**Modul célja** : VLAN-ok közötti útválasztás hibaelhárítása 3. rétegbeli eszközökön.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **A VLAN-ok közötti forgalomirányítás működése** | Ismertesse a VLAN-ok közötti útválasztás beállítási lehetőségeit. |
| **VLAN-ok közötti forgalomirányítás a router-on-a-stick módszerrel** | Állítsa be az útválasztót a VLAN-ok között. |
| **VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-ekkel** | Konfigurálja a VLAN-ok közötti útválasztást a 3. rétegbeli kapcsolás segítségével. |
| **VLAN-ok közötti forgalomirányítás hibaelhárítása** | A VLAN-ok közötti konfiguráció leggyakoribb problémáinak elhárítása |

[3.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A VLAN-ok közötti forgalomirányítás működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. A VLAN-ok közötti forgalomirányítás működése

# A VLAN-ok közötti forgalomirányítás működése

4.1.1

## Mit értünk VLAN-ok közötti forgalomirányításon?

A VLAN-okat különböző okokból használják a 2. rétegbeli kapcsolt hálózatok szegmentálására. Az okoktól függetlenül az egyik VLAN-ban lévő hosztok nem tudnak kommunikálni a másik VLAN-ban lévő hosztokkal, hacsak nincs egy router vagy 3. rétegbeli switch, amely forgalomirányítási szolgáltatásokat nyújt.

A VLAN-ok közötti forgalomirányítás a hálózati forgalom továbbítása egyik VLAN-ból egy másik VLAN-ba.

VLAN-ok közötti forgalomirányításra háromféle lehetőség van:

* **Legacy Inter-VLAN routing** - This is a legacy solution. Nem jól skálázható.
* **Router-on-a-Stick** – Ez egy elfogadható megoldás kis és közepes méretű hálózatok számára.
* **3. rétegbeli kapcsoló kapcsolt virtuális interfészek (SVI) használatával** – Ez a leginkább méretezhető megoldás közepes és nagy szervezetek számára.

4.1.2

## A VLAN-ok közti forgalomirányítás hagyományos módja

Az első VLAN-ok közötti forgalomirányítási megoldás egy több Ethernet interfésszel rendelkező router használatára támaszkodott. Minden egyes router interfész különböző VLAN-okban lévő switchporthoz volt csatlakoztatva. A router interfészei a VLAN-alhálózat helyi állomásainak alapértelmezett átjárójaként szolgáltak.

Nézzük meg például azt a topológiát, ahol R1 két interfésze csatlakozik az S1 switch-hez.

A fizikai hálózati topológia két PC-t, egy kapcsolót és egy útválasztót mutat. A bal oldali PC1 IP-címe 192.168.10.10, VLAN 10-ben van, és az F0/11-es portra van csatlakoztatva. A jobb oldali PC2 IP-címe 192.168.20.10, a VLAN 20-ban van, és az F0/24 porton lévő kapcsolóhoz csatlakozik. Az S1 kapcsolónak két kapcsolata van az R1 útválasztóval. Az F0/1 kapcsolóport az R1 G0/0/0 interfészéhez csatlakozik. Az F0/2 kapcsolóport az R1 G0/0/1 interfészére csatlakozik. A G0/0/0 útválasztó interfész IP-címe 192.168.10.1. A G0/0/1 útválasztó interfész IP-címe 192.168.20.1.

PC2 S1 PC1 G0/0/0 192.168.10.1/24 F0/11 F0/24 F0/12 F0/1 G0/0/1 192.168.20.1/24 R1

192.168.10.10   
VLAN 10 192.168.20.10   
VLAN 20

Vegyük észre, hogy a példában az S1 MAC-címtáblája a következőképpen van feltöltve:

* Az Fa0/1 port a VLAN 10-hez van rendelve, és az R1 G0/0/0 interfészéhez van csatlakoztatva.
* Az Fa0/11 port a VLAN 10-hez van rendelve, és PC1-hez van csatlakoztatva.
* Az Fa0/12 port a VLAN 20-hoz van hozzárendelve, és az R1 G0/0/1 interfészéhez csatlakozik.
* A Fa0/24 port a VLAN 20-hoz van hozzárendelve, és a PC2-höz csatlakozik.

### S1 MAC-cím táblája

| PortMAC-cím VLANF0/1R1 G0/0/0 MAC10F0/11PC1 MAC10F0/12R1 G0/0/1 MAC20F0/24PC2 MAC20 | | |
| --- | --- | --- |
| **Kikötő** | **Mac cím** | **VLAN** |
| F0/1 | R1 G0/0/0 MAC | 10 |
| F0/11 | PC1 MAC | 10 |
| F0/12 | R1 G0/0/1 MAC | 20 |
| F0/24 | PC2 MAC | 20 |

Amikor PC1 egy másik hálózaton lévő PC2-nek küld csomagot, a 192.168.10.1 alapértelmezett átjáró címre továbbítja azt. R1 a G0/0/0 interfészén fogadja a csomagot, és megvizsgálja a csomag célcímét. R1 ezután a csomagot a G0/0/1 interfészén keresztül S1 VLAN 20-ban lévő F0/12-es portjára irányítja. Végül S1 továbbítja a keretet PC2-nek.

A fizikai interfészeket használó hagyományos VLAN-ok közötti forgalomirányítás működik, de van egy jelentős korlátozása. Nem ésszerűen skálázható, mivel a routerek korlátozott számú fizikai interfésszel rendelkeznek. Ha minden egyes VLAN-hoz külön interfészt használunk, hamar elfogynak a rendelkezésre álló fizikai interfészek.

Példánkban R1-nek két külön Ethernet interfészre volt szüksége a VLAN 10 és a VLAN 20 közötti forgalomirányításhoz. Mi lenne, ha hat (vagy több) VLAN-t kellene összekapcsolni? Minden egyes VLAN-hoz külön interfészre lenne szükség. Nyilvánvaló, hogy ez a megoldás nem méretezhető.

**Megjegyzés** : Ezt a VLAN-ok közötti útválasztási módszert már nem alkalmazzák kapcsolt hálózatokban, és csak magyarázatként szerepel.

4.1.3

## VLAN-ok közötti forgalomirányítás router-on-a-stick módszerrel

A VLAN-ok közötti forgalomirányítás router-on-a-stick módszere kiküszöböli a hagyományos módszer korlátait. Csak egy fizikai Ethernet interfészre van szükség a hálózat több VLAN-ja közötti forgalom továbbításához.

Egy Cisco IOS router Ethernet interfésze 802.1Q trönkként van konfigurálva, és egy 2. rétegbeli switch trönkportjához van csatlakoztatva. Pontosabban, a router interfésze alinterfészek használatával van konfigurálva az forgalomirányításra alkalmas VLAN-ok azonosítására.

A konfigurált alinterfészek szoftveralapú virtuális interfészek. Mindegyikhez egyetlen fizikai Ethernet interfész tartozik. Az alinterfészek konfigurálása szoftveresen történik a routeren. Minden alinterfész önállóan van konfigurálva, IP-címmel és VLAN-hozzárendeléssel. Az alinterfészek a VLAN-hozzárendelésnek megfelelő alhálózatba tartozó IP-címet kapnak. Ez megkönnyíti a logikai forgalomirányítást.

Amikor a VLAN-címkével ellátott forgalom belép a router interfészre, továbbításra kerül a VLAN-alinterfészre. A hálózati cél IP-cím alapján hozott forgalomirányítási döntés után a router meghatározza a kimenő interfészt a forgalom számára. If the exit interface is configured as an 802.Q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface.

A router-on-a-stick forgalomirányítási folyamat megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

G0/0/0,10

G0/0/0,30

**R1 Alinterfészek**   
G0/0/0.10: 172.17.10.1 [VLAN 10]   
G0/0/0.20: 172.17.20.1 [VLAN 20]   
G0/0/0.30: 172.17.30.1 [VLAN 30]

**Kapcsolja az S1 portokat**   
F0/1-F0/3 = törzs   
  
**Kapcsolja az S2 portokat**   
F0/11 = VLAN 10   
F0/18 = VLAN 20   
F0/23 = VLAN 30   
F0/1-F0/2 = törzs

VLAN Tagged   
Keret

VLAN Tagged   
Keret

**Törzs**

**Törzs**

**Törzs**

Amint az animációban látható, a 10-es VLAN-on lévő PC1 kommunikál a 30-as VLAN-on lévő PC3-mal. Amikor R1 fogadja a VLAN 10 felcímkézett egyedi címzésű forgalmát, a konfigurált alinterfészeinek segítségével továbbítja azt a VLAN 30 felé. Az S2 switch eltávolítja a VLAN-címkét az egyedi címzésű forgalomról, majd továbbküldi az F0/23 interfészen a PC3 felé.

**Megjegyzés** : A VLAN-ok közötti útválasztás „router-on-a-stick” módszere nem skálázódik 50 VLAN fölé.

4.1.4

## VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-en

A VLAN-ok közötti forgalomirányítás modern módszere a 3. rétegbeli switch-ek és a kapcsolt virtuális interfészek (SVI) használata. Az SVI, ahogy az az ábrán is látható, egy 3. rétegbeli switch virtuális interfésze.

**Note** : A Layer 3 switch is also called a multilayer switch as it operates at Layer 2 and Layer 3. Ebben a kurzusban azonban a 3. rétegbeli switch kifejezést használjuk.

A fizikai hálózati topológia két PC-t, két Layer 2 switchet és egy Layer 3 switchet mutat. A bal oldali PC a VLAN 10-ben van, és egy Layer 2 kapcsolóhoz csatlakozik, amely viszont a Layer 3 kapcsolóhoz csatlakozik. A jobb oldali PC a VLAN 20-ban van, és egy Layer 2 kapcsolóhoz csatlakozik, amely viszont a Layer 3 kapcsolóhoz csatlakozik. A Layer 3 switch két SVI interfésszel rendelkezik. Az SVI1 a VLAN 10-ben van, és az IP-címe 10.1.10.1. Az SVI2 a VLAN 20-ban van, és az IP-címe 10.1.20.1.

VLAN 10

VLAN 20

**SVI interfész**   
VLAN 20   
10.1.20.1 **SVI interfész**   
VLAN 10   
10.1.10.1

A VLAN-ok közötti SVI-k ugyanúgy jönnek létre, mint ahogy a felügyeleti VLAN-interfészt konfiguráljuk. Az SVI egy olyan VLAN-hoz jön létre, amely létezik a switch-en. Bár virtuális, az SVI ugyanazokat a funkciókat látja el a VLAN számára, mint egy router interfész. Pontosabban, 3. rétegbeli feldolgozást biztosít az adott VLAN-hoz tartozó összes switchportra érkező vagy onnan küldött csomagok számára.

Az alábbiakban a 3. rétegbeli switch-ek VLAN-ok közötti forgalomirányításhoz való használatának előnyei szerepelnek:

* Sokkal gyorsabb, mint a router-on-a-stick megoldás, mert minden kapcsolási és forgalomirányítási művelet hardver alapú.
* A forgalomirányításhoz nem igényel külön switch és router közti vonalat.
* Nem korlátozódnak egy linkre, mert a sávszélesség növelése érdekében 2. rétegbeli EtherChannel-ek trönkkapcsolatként használhatók a switch-ek között.
* A késleltetési idő sokkal alacsonyabb, mivel az adatoknak nem kell elhagyniuk a switch-et ahhoz, hogy egy másik hálózatba irányítsák őket.
* Gyakrabban telepítik ezeket az egyetemi LAN-okban, mint a routereket.

Az egyetlen hátrányuk, hogy a 3. rétegbeli switch-ek drágábbak.

4.1.5

## Tudáspróba - A VLAN-ok közötti forgalomirányítás működése

Ebben a tudáspróba feladatban különböző esetek tartoznak minden egyes kérdéshez. Kattintsunk az egyes gombokra a kérdésekhez tartozó VLAN-ok közötti forgalomirányításról szóló esetek megtekintéséhez.

**A forgatókönyv**

A fizikai hálózati topológia két PC-t, egy kapcsolót és egy útválasztót mutat. A PC1 IP-címe 10.17.10.4/24, a VLAN 10-ben van, és az S2 kapcsolóhoz csatlakozik. A PC2 IP-címe 1.17.20.4/24, a VLAN 20-ban van, és az S3 kapcsolóhoz csatlakozik. Mind az S2, mind az S3 a Layer 3 kapcsolóhoz, az S1-hez csatlakozik. Az S1 rendelkezik egy SVI interfésszel a VLAN 10-ben 10.17.10.1/24 IP-címmel és egy SVI interfésszel a VLAN 20-ban 10.17.20.1/24 IP-címmel

S1 S1 S2 S3 PC1 PC2 10.17.10.4/24 10.17.20.4/24 SVI VLAN 10 - 10.17.10.1/24

SVI VLAN 20 - 10.17.20.1/24

VLAN 20 VLAN 10

Az űrlap teteje

1. **Tekintse meg az egyes forgatókönyv-topológiákat** . Mely állítások írják le legjobban a VLAN-ok közötti útválasztási megoldások különböző típusait? (Válassza ki az összes megfelelőt.)

Az űrlap alja

[4.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás router-on-a-stick módszerrel](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. VLAN-ok közötti forgalomirányítás router-on-a-stick módszerrel

# VLAN-ok közötti forgalomirányítás router-on-a-stick módszerrel

4.2.1

## Router-on-a-stick eset

Az előző témakörben a VLAN-ok közötti forgalomirányítás létrehozásának három különböző módját soroltuk fel, és részleteztük a hagyományos VLAN-ok közötti forgalomirányítást. Ez a témakör a router-on-a-stick VLAN-ok közötti forgalomirányítás beállítását részletezi. Az ábrán látható, hogy a router nem a topológia középpontjában áll, hanem úgy tűnik, mintha egy boton lenne az egyik végen, innen ered az elnevezés.

Az ábrán az R1 GigabitEthernet 0/0/1 interfésze az S1 FastEthernet 0/5 portjához csatlakozik. Az S1 FastEthernet 0/1 portja az S2 FastEthernet 0/1 portjához csatlakozik. Ezek olyan trönkkapcsolatok, amelyek a VLAN-okon belüli és a VLAN-ok közötti forgalom továbbításához szükségesek.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

192.168.10.10/24 G0/0/1 F0/5 192.168.99.2/24 F0/1 F0/1 192.168.99.3/24 F0/6 F0/18 192.168.20.10/24 S1 S2 R1 PC1

PC2

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

A VLAN-ok közötti forgalomirányításhoz az R1 GigabitEthernet 0/0/1 interfésze logikailag három alinterfészre van felosztva, ahogy a táblázatban látható. A táblázat a switch-eken konfigurálandó három VLAN-t is mutatja.

### Az R1 router alinterfészei

| Alinterfész VLANIP-cím G0/0/0.1010192.168.10.1/24G0/0/0.2020192.168.20.1/24G0/0/0.3099192.168.99.1/24 | | |
| --- | --- | --- |
| **Alinterfész** | **VLAN** | **IP-cím** |
| G0/0/1.10 | 10 | 192.168.10.1/24 |
| G0/0/1.20 | 20 | 192.168.20.1/24 |
| G0/0/1,99 | 99 | 192.168.99.1/24 |

Tegyük fel, hogy R1, S1 és S2 kezdeti alapkonfigurációkkal rendelkeznek. Jelenleg a PC1 és a PC2 nem tudja **ping** elni egymást, mert külön hálózatokon vannak. Csak az S1 és S2 tudja **ping** elni egymást, de ők sem a PC1, sem a PC2 számára nem elérhetőek, mert szintén különböző hálózatokon vannak.

Ahhoz, hogy az eszközök pingelni tudják egymást, a switch-eket VLAN-okkal és trönköléssel kell konfigurálni, a routert pedig VLAN-ok közötti forgalomirányításra kell beállítani.

4.2.2

## Az S1 VLAN- és trönkkonfigurációja

Végezzük el az alábbi lépéseket az S1 VLAN-okkal és trönköléssel történő konfigurálásához:

**Step 1** . Hozzuk létre és nevezzük el a VLAN-okat.

**Step 2** . Hozzuk létre a felügyeleti interfészt.

**Step 3** . Állítsuk be a hozzáférési portokat.

**Step 4** . Állítsuk be a trönkportokat.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24. A PC2 IP-címe 192.168.20.10/24. A PC1 az F0/6 kapcsolóporton lévő S1 kapcsolóhoz csatlakozik. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton vannak egymással összekötve. Az S1 kapcsoló az F0/5 kapcsolóporton lévő R1 útválasztóhoz csatlakozik, amely az R1 G0/0/1 interfészéhez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

192.168.10.10/24 G0/0/1 F0/5 192.168.99.2/24 F0/1 F0/1 192.168.99.3/24 F0/6 F0/18 192.168.20.10/24 S1 S2 R1 PC1

PC2

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

Kattintsunk az egyes gombokra a konfigurációs lépés részleteinek megtekintéséhez!

**1 . Hozza létre és nevezze el a VLAN-okat.**

First, the VLANs are created and named. A VLAN-ok csak a VLAN-alkonfigurációs módból való kilépés után jönnek létre.

S1(config)# vlan 10 S1(config-vlan)# név LAN10 S1(config-vlan)# kilépés S1(config)# vlan 20 S1(config-vlan)# név LAN20 S1(config-vlan)# kilépés S1( config)# vlan 99 S1(config-vlan)# név Kezelés S1(config-vlan)# kilépés S1(config)#

4.2.3

## Az S2 VLAN- és trönkkonfigurációja

Az S2 konfigurációja hasonló az S1-hez.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

192.168.10.10/24 G0/0/1 F0/5 192.168.99.2/24 F0/1 F0/1 192.168.99.3/24 F0/6 F0/18 192.168.20.10/24 S1 S2 R1 PC1

PC2

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

S2(config)# **vlan 10**

S2(config-vlan)# **name LAN10**

S2(config-vlan)# **exit**

S2(config)# **vlan 20**

S2(config-vlan)# **name LAN20**

S2(config-vlan)# **exit**

S2(config)# **vlan 99**

S2(config-vlan)# **name Management**

S2(config-vlan)# **exit**

S2(config)#

S2(config)# **interface vlan 99**

S2(config-if)# **ip add 192.168.99.3 255.255.255.0**

S2(config-if)# **no shut**

S2(config-if)# **exit**

S2(config)# **ip default-gateway 192.168.99.1**

S2(config)# **interface fa0/18**

S2(config-if)# **switchport mode access**

S2(config-if)# **switchport access vlan 20**

S2(config-if)# **no shut**

S2(config-if)# **exit**

S2(config)# **interface fa0/1**

S2(config-if)# **switchport mode trunk**

S2(config-if)# **no shut**

S2(config-if)# **exit**

S2(config-if)# **end**

\*Mar 1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

4.2.4

## Az R1 alinterfész-konfigurációs módja

A router-on-a-stick módszer megköveteli, hogy minden egyes VLAN-hoz létre kell hozni egy alinterfészt.

A subinterface is created using the **interface** interface \_ id.subinterface \_ id global configuration mode command. Az alinterfész szintaxisa a fizikai interfész, amelyet egy pont és az alinterfész száma követ. Bár nem kötelező, de szokás az alinterfész számát a VLAN-számmal egyeztetni.

Ezután minden alinterfész az alábbi két paranccsal konfigurálható:

* **encapsulation dot1q** vlan \_ id **\ [native ]** - Ez a parancs állítja be az alinterfészt az adott VLAN-id-vel érkező 802.1Q beágyazású keret fogadására. The **A native** kulcsszót csak akkor kell hozzáadni, ha a natív VLAN-t a VLAN 1-től eltérőre állítjuk be.
* **ip address** ip-address subnet-mask - Ez a parancs beállítja az alinterfész IPv4-címét. Ez a cím általában az azonosított VLAN alapértelmezett átjárójaként szolgál.

Ismételjük meg a folyamatot minden egyes irányítandó VLAN esetében. Forgalomirányítás csak akkor lehetséges, ha minden alinterfész külön alhálózathoz tartozó IP-címet kap.

Ha minden alinterfész létrejött, engedélyezzük a fizikai interfészt a **no shutdown** konfigurációs paranccsal. Hasonlóképpen, ha a fizikai interfészt letiltjuk, azzal az összes alinterfészt is letiltjuk.

A következő konfigurációban az R1 G0/0/1 alinterfészei a 10-es, 20-as és 99-es VLAN-okhoz vannak beállítva.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24. A PC2 IP-címe 192.168.20.10/24. A PC1 az F0/6 kapcsolóporton lévő S1 kapcsolóhoz csatlakozik. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton vannak egymással összekötve. Az S1 kapcsoló az F0/5 kapcsolóporton lévő R1 útválasztóhoz csatlakozik, amely az R1 G0/0/1 interfészéhez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

192.168.10.10/24 G0/0/1 F0/5 192.168.99.2/24 F0/1 F0/1 192.168.99.3/24 F0/6 F0/18 192.168.20.10/24 S1 S2 R1 PC1

PC2

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

R1(config)# **interface G0/0/1.10**

R1(config-subif)# **description Default Gateway for VLAN 10**

R1(config-subif)# **encapsulation dot1Q 10**

R1(config-subif)# **ip add 192.168.10.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)#

R1(config)# **interface G0/0/1.20**

R1(config-subif)# **description Default Gateway for VLAN 20**

R1(config-subif)# **encapsulation dot1Q 20**

R1(config-subif)# **ip add 192.168.20.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)#

R1(config)# **interface G0/0/1.99**

R1(config-subif)# **description Default Gateway for VLAN 99**

R1(config-subif)# **encapsulation dot1Q 99**

R1(config-subif)# **ip add 192.168.99.1 255.255.255.0**

R1(config-subif)# **exit**

R1(config)#

R1(config)# **interface G0/0/1**

R1(config-if)# **description Trunk link to S1**

R1(config-if)# **no shut**

R1(config-if)# **end**

R1#

\*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down

\*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up

\*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1#

4.2.5

## A PC1 és PC2 közötti kapcsolat ellenőrzése

A router-on-a-stick konfigurációja a switch trönkjének és a router alinterfészeinek beállítása után befejeződött. A konfiguráció ellenőrizhető a hosztokról, a routerről és a switch-ről.

Egy állomásról a **ping** parancs segítségével ellenőrizzük a kapcsolatot egy másik VLAN-ban lévő állomáshoz. Célszerű először az aktuális állomás IP-konfigurációját ellenőrizni az **ipconfig** paranccsal Windows alatt.

C:\Users\PC1> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::5c43:ee7c:2959:da68%6

IPv4 Address : 192.168.10.10

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.10.1

C:\Users\PC1>

A kimenet alapján megerősíthető a PC1 IPv4-címe és alapértelmezett átjárója. Ezután a **ping** segítségével ellenőrizzük a PC2 és az S1 kapcsolatát az ábrán látható módon. A **ping** kimenete sikeresen megerősíti, hogy a VLAN-ok közötti forgalomirányítás működik.

C:\Users\PC1> **ping 192.168.20.10**

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:

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

Approximate round trip times in milli-seconds:

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

C:\Users\PC1>

C:\Users\PC1> **ping 192.168.99.2**

Pinging 192.168.99.2 with 32 bytes of data:

Request timed out.

Request timed out.

Reply from 192.168.99.2: bytes=32 time=2ms TTL=254

Reply from 192.168.99.2: bytes=32 time=1ms TTL=254 |

Ping statistics for 192.168.99.2:

Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\PC1>

4.2.6

## A router-on-a-stick VLAN-ok közötti forgalomirányítás ellenőrzése

Az eszközök közötti **ping** használata mellett a következő **show** parancsok is használhatók a router-on-a-stick konfiguráció ellenőrzésére és hibaelhárítására.

* **mutasd az ip útvonalat**
* **ip interfész rövid megjelenítése**
* **interfészek megjelenítése**
* **interfészek törzsének megjelenítése**

Kattintsunk az egyes gombokra a parancsok példakimenetének megtekintéséhez.

Verify that the subinterfaces are appearing in the routing table of R1 by using the **show ip route** command. Vegyük észre, hogy minden egyes irányítható VLAN-hoz három csatlakoztatott útvonal (C) és a hozzájuk tartozó kimenő interfészek tartoznak. A kimenet megerősíti, hogy a megfelelő alhálózatok, VLAN-ok és alinterfészek aktívak.

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/1.10

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/1.10

192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.20.0/24 is directly connected, GigabitEthernet0/0/1.20

L 192.168.20.1/32 is directly connected, GigabitEthernet0/0/1.20

192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.99.0/24 is directly connected, GigabitEthernet0/0/1.99

L 192.168.99.1/32 is directly connected, GigabitEthernet0/0/1.99

R1#

4.2.7

## Packet Tracer - VLAN-ok közötti forgalomirányítás konfigurálása a router-on-a-stick módszerrel

A feladat során a VLAN-ok közötti forgalomirányítás beállítása előtt ellenőrizzük a kapcsolatot. Ezután beállítjuk a VLAN-okat és a VLAN-ok közötti forgalomirányítást. Végül engedélyezzük a trönköket és ellenőrizzük a VLAN-ok közti kapcsolatot.

[Router-on-a-stick forgalomirányító konfigurálása VLAN-ok közötti forgalomirányításra](https://contenthub.netacad.com/courses/srwe-dl/_common/4.2.7-packet-tracer---configure-router-on-a-stick-inter-vlan-routing_hu-HU.pka)

4.2.8

## Laborgyakorlat - VLAN-ok közötti forgalomirányítás konfigurálása a router-on-a-stick módszerrel

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: VLAN-ok és trönkök konfigurálása a switch-eken
* Part 3: Trönk alapú VLAN-ok közötti forgalomirányítás beállítása

[4.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A VLAN-ok közötti forgalomirányítás működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-ek használatával](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-ek használatával

# VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-ek használatával

4.3.1

## VLAN-ok közötti forgalomirányítás egy 3. rétegbeli switch-en

A modern, vállalati hálózatok ritkán használják a router-on-a-stick megoldást, mivel az nem skálázható könnyen az igényeknek megfelelően. Ezekben a rendkívül nagy hálózatokban a hálózati rendszergazdák 3. rétegbeli switch-eket használnak a VLAN-ok közötti forgalomirányítás konfigurálására.

A router-on-a-stick módszerrel történő VLAN-ok közötti forgalomirányítás egyszerűen megvalósítható egy kis- vagy közepes méretű szervezet számára. Egy nagyvállalatnak azonban gyorsabb, sokkal jobban skálázható módszerre van szüksége a VLAN-ok közötti forgalomirányítás biztosítására.

A vállalati telephelyek LAN-jai 3. rétegbeli switch-eket használnak a VLAN-ok közötti forgalomirányítás biztosítására. A 3. rétegbeli switch-ek hardveralapú kapcsolást használnak, hogy a routereknél nagyobb csomagfeldolgozási sebességet érjenek el. A 3. rétegbeli switch-eket gyakran alkalmazzák a vállalati elosztóréteg kábelrendező szekrényeiben is.

A 3. rétegbeli switch-ek többek között az alábbiakra képesek:

* Forgalomirányítás egyik VLAN-ból a másikba több kapcsolt virtuális interfész (SVI) használatával.
* Egy 2. rétegbeli switchport átalakítása 3. rétegbeli interfésszé (azaz irányított porttá). Az irányított port hasonló a Cisco IOS router fizikai interfészéhez.

A VLAN-ok közötti forgalomirányítás biztosításához a 3. rétegbeli switch-ek SVI-ket használnak. Az SVI-k konfigurálása ugyanazzal az **interface vlan** vlan-id paranccsal történik, mint amelyet a 2. rétegbeli switch-en a felügyeleti SVI létrehozásához használunk. A 3. rétegbeli SVI-t minden egyes irányítható VLAN-hoz létre kell hozni.

4.3.2

## A 3. rétegbeli switch esete

Az ábrán a D1 3. rétegbeli switch két, különböző VLAN-ban lévő állomáshoz van csatlakoztatva. A PC1 a VLAN 10-ben, a PC2 pedig a VLAN 20-ban van, ahogy az ábrán látható. A 3. rétegbeli switch a két hoszt számára VLAN-ok közötti forgalomirányítási szolgáltatásokat nyújt.

A fizikai hálózati topológia két PC-t, egy kapcsolót és egy útválasztót mutat. A bal oldali PC1 IP-címe 192.168.10.10, átjárócíme 192.168.10.1/24, a VLAN 10-ben van, és a G1/0/6 portra van csatlakoztatva. A jobb oldali PC2 IP-címe 192.168.20.10, átjárócíme 192.168.20.10/24, a VLAN 20-ban van, és a kapcsolóval a G1/0/18 portra van csatlakoztatva.

D1 PC1 PC2 G1/0/6 G1/0/18 192.168.10.10/24

192.168.20.10/24

(VLAN 10) (VLAN 20) Átjáró: 192.168.10.1 Átjáró: 192.168.20.1

A táblázat az egyes VLAN-okhoz tartozó IP-címeket mutatja.

### D1 VLAN IP-címek

| VLAN interfész IP-cím10192.168.10.1/2420192.168.20.1/24 | |
| --- | --- |
| **VLAN-interfész** | **IP-cím** |
| 10 | 192.168.10.1/24 |
| 20 | 192.168.20.1/24 |

4.3.3

## A 3. rétegbeli switch konfigurációja

Végezzük el az alábbi lépéseket az S1 VLAN-okkal és trönköléssel történő konfigurálásához:

**Step 1** . Hozzuk létre a VLAN-okat.

**Step 2** . Hozzuk létre az SVI VLAN-interfészeket.

**Step 3** . Állítsuk be a hozzáférési portokat.

**Step 4**. Engedélyezzük az IP-alapú forgalomirányítást.

Kattintsunk az egyes gombokra a konfigurációs lépés részleteinek megtekintéséhez!

**1. Create the VLANs.**

First, create the two VLANs as shown in the output.

D1(config)# vlan 10 D1(config-vlan)# név LAN10 D1(config-vlan)# vlan 20 D1(config-vlan)# név LAN20 D1(config-vlan)# kilépés D1(config)#

4.3.4

## A 3. rétegbeli switch VLAN-ok közötti forgalomirányításának ellenőrzése

A 3. rétegbeli switch használatával történő VLAN-ok közötti forgalomirányítás egyszerűbben konfigurálható, mint a router-on-a-stick módszer esetében. A konfiguráció befejezése után a beállítások ellenőrizhetők a hosztok közötti kapcsolat tesztelésével.

Egy állomásról a **ping** parancs segítségével ellenőrizzük a kapcsolatot egy másik VLAN-ban lévő állomáshoz. Célszerű először az aktuális állomás IP-konfigurációját ellenőrizni az **ipconfig** paranccsal Windows alatt. A kimenet alapján megerősíthető a PC1 IPv4-címe és alapértelmezett átjárója.

C:\Users\PC1> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

Link-local IPv6 Address : fe80::5c43:ee7c:2959:da68%6

IPv4 Address : 192.168.10.10

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.10.1

C:\Users\PC1>

Ezután ellenőrizzük a PC2-vel való kapcsolatot a Windows alatt kiadott **ping** parancs segítségével, a kimeneten látható módon. A **ping** kimenete sikeresen megerősíti, hogy a VLAN-ok közötti forgalomirányítás működik.

C:\Users\PC1> **ping 192.168.20.10**

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:

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

Approximate round trip times in milli-seconds:

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

C:\Users\PC1>

4.3.5

## Forgalomirányítás 3. rétegbeli switch-en

Ha a VLAN-okat más 3. rétegbeli eszközökkel is el akarjuk érni, akkor statikus vagy dinamikus forgalomirányítással kell hirdetni őket. A forgalomirányítás engedélyezéséhez egy 3. rétegbeli switch-en irányított portot kell konfigurálni.

Az irányított port egy 3. rétegbeli switch-en úgy jön létre, hogy egy másik 3. rétegbeli eszközhöz csatlakoztatott 2. rétegbeli porton letiltjuk a switchport funkciót. Konkrétan a **no switchport** interfészkonfigurációs parancs kiadásával egy 2. rétegbeli portot 3. rétegbeli interfésszé alakítunk. Ezután az interfész IPv4-konfigurációval beállítható, hogy csatlakozzon egy routerhez vagy egy másik 3. rétegbeli switch-hez.

4.3.6

## A forgalomirányítás esete 3. rétegbeli switch-en

Az ábrán a korábban konfigurált D1 3. rétegbeli switch most az R1-hez csatlakozik. Az R1 és D1 is egy OSPF (Open Shortest Path First) irányítóprotokoll tartományában vannak. Tegyük fel, hogy D1-en sikeresen megvalósult a VLAN-ok közötti kapcsolat. R1 G0/0/1 interfészét is konfiguráltuk és engedélyeztük. Ezenkívül R1 az OSPF-et használja a két hálózat (10.10.10.0/24 és 10.20.20.0/24) hirdetésére.

**Note**: OSPF routing configuration is covered in another course. Ebben a fejezetben az OSPF konfigurációs parancsokat minden feladat és számonkérés során megkapjuk. A konfiguráció megértéséhez nincs szükség az OSPF-forgalomirányítás engedélyezésére a 3. rétegbeli switch-en.

The physical network topology shows two PCs, a Layer 3 switch (D1), a router (R1), and a server. PC1 has IP address 192.168.10.10, gateway address of 192.168.10.1/24, is in VLAN 10, and is connected the switch on port G1/0/6. PC2 has IP address 192.168.20.10, gateway address of 192.168.20.10/24, is in VLAN 20, and is connected the switch on port G1/0/18. The switch, D1, interface G0/0/1 has IP address 10.10.10.2/24 and connects to the router, R1, G0/0/1 interface which has IP address 10.10.10.1/24. The router, R1, connects to the server over the 10.10.20.0/24 network with the R1 having the 10.10.10.1 ip address and the server having the 10.10.20.254 ip address. The router is also running OSPF.

PC1 PC2 G1/0/6 G1/0/18 192.168.10.10/24 192.168.20.10/24 D1 .2 G0/0/1 G0/0/1 .1 .1 .254 10.10.10.0/24 10.10.20.0/24 R1 Svr OSPF

G0/0/0

(VLAN 10)(VLAN 20)Gateway: 192.168.10.1Gateway: 192.168.20.1

4.3.7

## Forgalomirányítás konfigurálása 3. rétegbeli switch-en

Végezzük el az alábbi konfigurációs lépéseket, hogy D1 útvonallal rendelkezzen R1-hez:

**Step 1**. Állítsuk be az irányított portot.

**Step 2**. Engedélyezzük a forgalomirányítást.

**Step 3**. Állítsuk be a forgalomirányítást.

**Step 4**. Ellenőrizzük a forgalomirányítást.

**Step 5**. Ellenőrizzük az összeköttetéseket.

Kattintsunk az egyes gombokra a konfigurációs lépés részleteinek megtekintéséhez!

**1. Configure the routed port.**

Configure G0/0/1 to be a routed port, assign it an IPv4 address, and enable it.

D1(config)# interfész GigabitEthernet0/0/1 D1(config-if)# leírás irányítva Port Link az R1-hez D1(config-if)# nincs switchport D1(config-if)# IP-cím 10.10.10.2 255.255.255.0 D1( config-if)# no shut D1(config-if)# kilépés D1(config)#

4.3.8

## Packet Tracer - 3. rétegbeli kapcsolás és VLAN-ok közötti forgalomirányítás beállítása

A feladat során egy Cisco 3560-as switch-en konfigurálunk 3. rétegbeli kapcsolást és VLAN-ok közötti forgalomirányítást.

[3. rétegbeli kapcsolás és VLAN-ok közötti forgalomirányítás konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/4.3.8-packet-tracer---configure-layer-3-switching-and-inter-vlan-routing_hu-HU.pka)

[4.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás router-on-a-stick módszerrel](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás hibaelhárítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. VLAN-ok közötti forgalomirányítás hibaelhárítása

# VLAN-ok közötti forgalomirányítás hibaelhárítása

4.4.1

## A VLAN-ok közötti forgalomirányítás gyakori problémái

Mostanra már tudjuk, hogy a konfigurálás és ellenőrzés során a hibaelhárításra is képesnek kell lennünk. Ez a témakör néhány gyakori hálózati problémát tárgyal a VLAN-ok közötti forgalomirányítással kapcsolatban.

Számos oka lehet annak, hogy a VLAN-ok közötti forgalomirányítás konfigurációja nem működik. Mindegyik az összeköttetési problémákkal függ össze. Először is ellenőrizzük a fizikai réteget, hogy megoldjuk azokat a problémákat, amelyeknél előfordulhat, hogy egy kábel rossz porthoz van csatlakoztatva. Ha a csatlakozások megfelelőek, akkor a táblázatban található lista alapján keressük meg azokat az egyéb gyakori okokat, amelyek miatt a VLAN-ok közötti kapcsolat meghiúsulhat.

| Probléma típusaHogyan javítható a Hiányzó VLAN-ok ellenőrzése Hozzon létre (vagy hozza létre újra) a VLAN-t, ha az nem létezik.Győződjön meg arról, hogy a gazdagépport a megfelelő VLAN-hoz van hozzárendelve.show vlan [rövid] interfészek megjelenítése switchport pingSwitch fővonali portok ProblémákGyőződjön meg arról, hogy a fővonalak megfelelően vannak konfigurálva. egy fővonali port és engedélyezve van.show interface trunk show running-configSwitch Access Port IssuesA megfelelő VLAN hozzárendelése a hozzáférési porthoz. Győződjön meg róla, hogy a port hozzáférési port, és engedélyezve van.A gazdagép helytelenül van konfigurálva a rossz alhálózatban.show interfaces switchport show running-config interface ipconfigRouter Configuration IssuesRouter alinterface IPv4 address issues Helytelenül van beállítva a router alinterfésze.A router alinterfésze a VLAN interfész azonosítójához van rendelve show show.show interfészek | | |
| --- | --- | --- |
| **A probléma típusa** | **Hogyan javítható?** | **Hogyan ellenőrizhető?** |
| Hiányzó VLAN-ok | * Hozzuk létre (vagy hozzuk létre újra) a VLAN-t, ha az nem létezik. * Győződjünk meg arról, hogy a hoszt portja a megfelelő VLAN-hoz van rendelve. | **mutasd vlan [rövid]**  **interfészek switchport megjelenítése**  **ping** |
| Switch trönkportjával kapcsolatos problémák | * Győződjünk meg arról, hogy a trönkök megfelelően vannak konfigurálva. * Győződjünk meg róla, hogy a port trönkport, és engedélyezve van. | **interfészek törzsének megjelenítése**  **futó-konfig megjelenítése** |
| Switch hozzáférési portjával kapcsolatos problémák | * Rendeljük hozzá a megfelelő VLAN-t a hozzáférési porthoz. * Győződjünk meg róla, hogy a port hozzáférési port, és engedélyezve van. * Az állomás helytelenül, rossz alhálózatba van konfigurálva. | **interfészek switchport megjelenítése**  **futó-config felület megjelenítése**  **ipconfig** |
| A router konfigurálásával kapcsolatos kérdések | * A router alinterfészének IPv4-címe helytelenül van beállítva. * A router alinterfésze VLAN-azonosítóhoz van rendelve. | **ip interfész rövid megjelenítése**  **interfészek megjelenítése** |

4.4.2

## A VLAN-ok közötti forgalomirányítás hibaelhárításának esete

A következőkben néhány példát mutatunk be a VLAN-ok közötti forgalomirányítási problémákra.

Ezt a topológiát fogjuk használni mindegyik problémánál.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

R1 S1 S2 PC1 PC2 G0/0/1 192.168.99.2/24 F0/6 F0/18 F0/1 F0/1 192.168.99.3/24 192.168.10.10/24 192.168.20.10/24

F0/5

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

R1 VLAN és IPv4-címzési információi a táblázatban láthatók.

### Az R1 router alinterfészei

| Alinterfész VLANIP-cím G0/0/0.1010192.168.10.1/24G0/0/0.2020192.168.20.1/24G0/0/0.3099192.168.99.1/24 | | |
| --- | --- | --- |
| **Alinterfész** | **VLAN** | **IP-cím** |
| G0/0/0,10 | 10 | 192.168.10.1/24 |
| G0/0/0,20 | 20 | 192.168.20.1/24 |
| G0/0/0,30 | 99 | 192.168.99.1/24 |

4.4.3

## Hiányzó VLAN-ok

A VLAN-ok közötti kapcsolódási problémát okozhatja egy hiányzó VLAN. A VLAN hiányozhat, ha nem hozták létre, véletlenül törölték, vagy ha nem engedélyezett a trönk-kapcsolaton.

Például a PC1 jelenleg a 10-es VLAN-hoz van csatlakoztatva, amint azt a **show vlan brief** parancs kimenete mutatja.

S1# **show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

10 LAN10 active Fa0/6

20 LAN20 active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S1#

Most tegyük fel, hogy a VLAN 10 véletlenül törlölve lett, ahogy az a következő kimenetben látható.

S1(config)# **no vlan 10**

S1(config)# **do show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

20 LAN20 active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S1(config)#

Figyeljük meg, hogy a VLAN 10 most hiányzik a kimenetről. Vegyük észre azt is, hogy az Fa0/6 port nem lett újra hozzárendelve az alapértelmezett VLAN-hoz. Ennek oka az, hogy amikor törlünk egy VLAN-t, akkor a VLAN-hoz rendelt portok inaktívvá válnak. Mindaddig a VLAN-hoz társítva maradnak (és így inaktívak), amíg új VLAN-hoz nem rendeljük őket, vagy újra létre nem hozzuk a hiányzó VLAN-t.

A VLAN-tagság ellenőrzéséhez használjuk a **show interface** interface-id **switchport** parancsot.

S1(config)# **do show interface fa0/6 switchport**

Name: Fa0/6

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 10 (Inactive)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

(Output omitted)

A hiányzó VLAN újbóli létrehozása automatikusan újra hozzárendeli a hosztokat, ahogy az a következő kimeneten látható.

S1(config)# **vlan 10**

S1(config-vlan)# **do show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

20 LAN20 active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S1(config-vlan)#

Figyeljük meg, hogy a VLAN nem a várt módon jött létre. Ennek oka az, hogy a VLAN létrehozásához ki kell lépni a VLAN alkonfigurációs módból, ahogyan az a következő kimeneten látható.

S1(config-vlan)# **exit**

S1(config)# **vlan 10**

S1(config)# **do show vlan brief**

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gi0/1, Gi0/2

10 VLAN0010 active Fa0/6

20 LAN20 active

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S1(config)#

Most vegyük észre, hogy a VLAN szerepel a listában, és hogy az Fa0/6-hoz csatlakozó állomás a 10-es VLAN-hoz tartozik.

4.4.4

## Switch trönkportjával kapcsolatos problémák

A VLAN-ok közötti forgalomirányítás másik problémája a rosszul konfigurált switchportokra vezethető vissza. A VLAN-ok közötti forgalomirányítás hagyományos megvalósításakor ez akkor fordulhat elő, ha a csatlakozó router portja nem a megfelelő VLAN-hoz van hozzárendelve.

A router-on-a-stick megoldásnál azonban a leggyakoribb ok a rosszul konfigurált trönkport.

Tegyük fel például, hogy a PC1 egészen a közelmúltig képes volt más VLAN-okban lévő hosztokhoz csatlakozni. A karbantartási naplókra vetett gyors pillantás alapján megállapítható, hogy az S1 2. rétegbeli switch-hez nemrég rutinkarbantartás céljából hozzáfértek. Ezért azt gyanítjuk, hogy a probléma ezzel az eszközzel függhet össze.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

R1 S1 S2 PC1 PC2 G0/0/1 192.168.99.2/24 F0/6 F0/18 F0/1 F0/1 192.168.99.3/24 192.168.10.10/24 192.168.20.10/24

F0/5

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

Az ábrán látható módon a **show interfaces trunk** parancs segítségével ellenőrizzük az S1-en, hogy az R1-hez csatlakozó port (vagyis az F0/5) megfelelően van-e trönkkapcsolatként konfigurálva.

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20,99

S1#

Az R1-hez csatlakozó Fa0/5 port rejtélyes módon hiányzik a kimenetről. Ellenőrizzük az interfész konfigurációját a **show running-config interface fa0/5** paranccsal, az ábrán látható módon.

S1# **show running-config | include interface fa0/5**

Building configuration...

Current configuration : 96 bytes

!

interface FastEthernet0/5

description Trunk link to R1

switchport mode trunk

shutdown

end

S1#

Mint látható, a port véletlenül le lett kapcsolva. A probléma kijavításához kapcsoljuk fel újra a portot, és ellenőrizzük a trönkölés állapotát, a kimeneten látható módon.

S1(config)# **interface fa0/5**

S1(config-if)# **no shut**

S1(config-if)#

\*Mar 1 04:46:44.153: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up

S1(config-if)#

\*Mar 1 04:46:47.962: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

S1(config-if)# **do show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Fa0/5 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Fa0/5 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,99

Fa0/5 1,10,20,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20,99

Fa0/1 1,10,20,99

S1(config-if)#

Amennyiben szeretnénk annak a veszélyét csökkenteni, hogy a switch-ek között egy meghibásodott kapcsolat meghiúsítsa a VLAN-ok közötti forgalomirányítást is, már a hálózattervezéskor gondolnunk kell redundáns kapcsolatok és alternatív útvonalak kialakítására.

4.4.5

## A switch hozzáférési portjával kapcsolatos problémák

Ha a switch hozzáférési portjának konfigurációjával kapcsolatban probléma gyanúja merül fel, a konfiguráció vizsgálatához és a probléma azonosításához használjuk az ellenőrző parancsokat.

Tegyük fel, hogy PC1 a helyes IPv4-címmel és alapértelmezett átjáróval rendelkezik, de nem képes **ping** elni a saját alapértelmezett átjáróját. A PC1-et egy 10-es VLAN-ba tartozó porthoz kell csatlakoztatni.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

R1 S1 S2 PC1 PC2 G0/0/1 192.168.99.2/24 F0/6 F0/18 F0/1 F0/1 192.168.99.3/24 192.168.10.10/24 192.168.20.10/24

F0/5

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

Ellenőrizzük a port konfigurációját az S1-en a **show interfaces** interface-id **switchport** parancs segítségével.

S1# **show interface fa0/6 switchport**

Name: Fa0/6

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 1 (default)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

Az Fa0/6 port hozzáférési portként lett konfigurálva, ahogyan azt a "static access" jelzi. Úgy tűnik azonban, hogy nem lett hozzárendelve a 10-es VLAN-hoz. Ellenőrizzük az interfész konfigurációját.

S1# **show running-config interface fa0/6**

Building configuration...

Current configuration : 87 bytes

!

interface FastEthernet0/6

description PC-A access port

switchport mode access

end

S1#

Rendeljük hozzá az Fa0/6 portot a 10-es VLAN-hoz, és ellenőrizzük a port hozzárendelését.

S1# **configure terminal**

S1(config)# **interface fa0/6**

S1(config-if)# **switchport access vlan 10**

S1(config-if)#

S1(config-if)# **do show interface fa0/6 switchport**

Name: Fa0/6

Switchport: Enabled

Administrative Mode: static access

Operational Mode: static access

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 10 (VLAN0010)

Trunking Native Mode VLAN: 1 (default)

Administrative Native VLAN tagging: enabled

Voice VLAN: none

(Output omitted)

PC1 most már képes más VLAN-okban lévő hosztokkal kommunikálni.

4.4.6

## A router konfigurálásával kapcsolatos kérdések

A router-on-a-stick módszer konfigurációs problémái általában az alinterfészek hibás beállításához kapcsolódnak. Például helytelen IP-címet állítottak be, vagy rossz VLAN-azonosítót rendeltek hozzá az alinterfészhez.

R1-nek például VLAN-ok közötti forgalomirányítást kell biztosítania a 10, 20 és 99 VLAN-ok felhasználói számára. A 10-es VLAN felhasználói azonban nem érhetnek el más VLAN-t.

A fizikai hálózati topológia két PC-t, két kapcsolót és egy útválasztót mutat. A PC1 IP-címe 192.168.10.10/24, alapértelmezett átjárója 192.168.10.1, és a VLAN 10-ben van. A PC2 IP-címe 192.168.20.10/24, az alapértelmezett 192.168.10.10/20 átjáró pedig a connect PC1 VLAN20.2s-ban van. S1 az F0/6 kapcsoló porton. A PC2 az F0/18-as kapcsolóporton lévő S2 kapcsolóhoz csatlakozik. Az S1 kapcsoló és az S2 kapcsoló az F0/1 kapcsolóporton egy fővonalon keresztül kapcsolódnak egymáshoz. Az S1 kapcsoló az R1 útválasztóhoz csatlakozik az F0/5 kapcsolóporton lévő fővonalon keresztül, amely az R1 G0/0/1 interfészeihez csatlakozik. Az S1 kezelési IP-címe 192.168.99.2/24. Az S1 kezelési IP-címe 192.168.99.3/24

R1 S1 S2 PC1 PC2 G0/0/1 192.168.99.2/24 F0/6 F0/18 F0/1 F0/1 192.168.99.3/24 192.168.10.10/24 192.168.20.10/24

F0/5

Fővonali kapcsolatok Átjáró: 192.168.10.1   
VLAN 10 átjáró: 192.168.20.1   
VLAN 20

Ellenőriztük a switch trönkkapcsolatát, és úgy tűnik, minden rendben van vele. Ellenőrizzük az alinterfész állapotát a **show ip interface brief** paranccsal.

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 unassigned YES unset administratively down down

GigabitEthernet0/0/1 unassigned YES unset up up

Gi0/0/1.10 192.168.10.1 YES manual up up

Gi0/0/1.20 192.168.20.1 YES manual up up

Gi0/0/1.99 192.168.99.1 YES manual up up

Serial0/1/0 unassigned YES unset administratively down down

Serial0/1/1 unassigned YES unset administratively down down

R1#

Az alinterfészekhez a megfelelő IPv4-címeket rendelték, és működőképesek.

Ellenőrizzük, hogy az egyes alinterfészek melyik VLAN-okban vannak. Ehhez a **show interfaces** parancs lenne hasznos, de rengeteg további, nem szükséges kimenetet generál. A parancs kimenete csökkenthető az IOS-parancsszűrők segítségével, a kimeneten látható módon.

R1# **show interfaces | include Gig|802.1Q**

GigabitEthernet0/0/0 is administratively down, line protocol is down

GigabitEthernet0/0/1 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set

GigabitEthernet0/0/1.10 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 100.

GigabitEthernet0/0/1.20 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 20.

GigabitEthernet0/0/1.99 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 99.

R1#

A pipe szimbólum (|) néhány szűrő kulcsszóval együtt hasznos módszer a parancsok kimenetének szűrésére. Ebben a példában az **include** kulcsszóval azonosítottuk, hogy csak a "Gig" vagy a "802.1Q" betűket tartalmazó sorok jelenjenek meg. Mivel a **show interface** kimenete természetesen listázva van, e szűrők használata az interfészek és a hozzájuk rendelt VLAN-ok tömörített listáját eredményezi.

Vegyük észre, hogy a G0/0/1.10 interfész helytelenül a 100-as VLAN-hoz lett hozzárendelve a 10-es VLAN helyett. Ezt a képen látható módon az R1 GigabitEthernet 0/0/1.10 alinterfész konfigurációjának megtekintésével igazolhatjuk.

R1# **show running-config interface g0/0/1.10**

Building configuration...

Current configuration : 146 bytes

!

interface GigabitEthernet0/0/1.10

description Default Gateway for VLAN 10

encapsulation dot1Q 100

ip address 192.168.10.1 255.255.255.0

end

R1#

A probléma kijavításához állítsuk be a G0/0/1.10 alinterfészt úgy, hogy a helyes VLAN-hoz tartozzon az **encapsulation dot1q 10** alinterfész konfigurációs parancs segítségével.

R1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# **interface gigabitEthernet 0/0/1.10**

R1(config-subif)# **encapsulation dot1Q 10**

R1(config-subif)# **end**

R1#

R1# **show interfaces | include Gig|802.1Q**

GigabitEthernet0/0/0 is administratively down, line protocol is down

GigabitEthernet0/0/1 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 1., loopback not set

GigabitEthernet0/0/1.10 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 10.

GigabitEthernet0/0/1.20 is up, line protocol is up

Encapsulation 802.1Q Virtual LAN, Vlan ID 20.

GigabitEthernet0/0/1.99 is up, line protocol is up

R1#

Amint az alinterfész átkerül a megfelelő VLAN-ra, elérhető lesz az adott VLAN eszközei számára, és a VLAN-ok közti forgalomirányítás is működni fog.

Megfelelő diagnosztikai módszerekkel a router konfigurációs hibái könnyen azonosíthatóak, így a VLAN-ok közti forgalomirányítás is helyreállítható.

4.4.7

## Tudáspróba - A VLAN-ok közötti forgalomirányítás hibaelhárítása

Az űrlap teteje

Ellenőrizze, hogy megértette-e a VLAN-ok közötti útválasztási módszereket, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. VLAN-ok közötti probléma elhárítását végzi egy útválasztón, és ellenőriznie kell, hogy az alinterfészek benne vannak-e az útválasztási táblázatban. Melyik VLAN-ok közötti útválasztási hibaelhárítási parancsot használná ehhez?

Az űrlap alja

Egy VLAN-ok közötti probléma elhárítását végzi egy kapcsolón, és ellenőriznie kell a VLAN-ok listáját és a hozzájuk rendelt portokat. Melyik VLAN-ok közötti útválasztási hibaelhárítási parancsot használná ehhez?

Ön egy VLAN közötti probléma elhárítását végzi egy kapcsolón, és ellenőriznie kell a hozzáférési port állapotát és a hozzáférési mód VLAN-ját. Melyik hibaelhárítási parancsot használná ehhez?

Ön egy VLAN közötti probléma elhárítását végzi egy switchen, és tömörített formátumban kell ellenőriznie az összes interfész állapotát és IP-címét. Melyik VLAN-ok közötti útválasztási hibaelhárítási parancsot használná ehhez?

4.4.8

## Packet Tracer - VLAN-ok közötti forgalomirányítás hibaelhárítása

A Packet Tracer feladat során a következőket fogjuk elvégezni:

* Part 1: Hálózati problémák megkeresése
* Part 2: A megoldás megvalósítása
* Part 3: A hálózati kapcsolat ellenőrzése

[VLAN-ok közötti forgalomirányítás hibaelhárítása](https://contenthub.netacad.com/courses/srwe-dl/_common/4.4.8-packet-tracer---troubleshoot-inter-vlan-routing_hu-HU.pka)

4.4.9

## Laborgyakorlat - VLAN-ok közötti forgalomirányítás hibaelhárítása

##### Készségek gyakorlási lehetőség

Lehetőséged van az alábbi készségek gyakorlására:

* 1. rész: A hálózat működésének értékelése
* 2. rész: Információgyűjtés, cselekvési terv létrehozása és korrekciók végrehajtása

Ezeket a készségeket gyakorolhatja a Packet Tracer vagy a laborberendezés segítségével, ha rendelkezésre áll.

**Packet Tracer – Fizikai mód (PTPM)**

[VLAN-ok közötti útválasztás – fizikai mód hibaelhárítása](https://contenthub.netacad.com/courses/srwe-dl/_common/4.4.9-packet-tracer---troubleshoot-inter-vlan-routing---physical-mode_hu-HU.pka)

**Laboratóriumi berendezések**

[4.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás 3. rétegbeli switch-ek használatával](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[4.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Inter-VLAN Routing
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

4.5.1

## Packet Tracer - VLAN-ok közötti forgalomirányítási kihívás

A feladat során kipróbáljuk és begyakoroljuk a VLAN-ok közötti forgalomirányítás konfigurálását, beleértve az IP-címek, a VLAN-ok, a trönkök és az alinterfészek beállítását is.

[VLAN-ok közötti forgalomirányítás feladat](https://contenthub.netacad.com/courses/srwe-dl/_common/4.5.1-packet-tracer---inter-vlan-routing-challenge_hu-HU.pka)

4.5.2

## Laborgyakorlat - VLAN-ok közötti forgalomirányítás megvalósítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: VLAN-ok létrehozása és a switchportok hozzárendelése
* Part 3: 802.1Q trönk konfigurálása a switch-ek között
* Part 4: VLAN-ok közötti forgalomirányítás konfigurálása az S1 switch-en
* Part 5: A VLAN-ok közötti forgalomirányítás működésének ellenőrzése

4.5.3

## Miről tanultunk ebben a fejezetben?

**Inter-VLAN útválasztási művelet**

Az egyik VLAN-ban lévő hosztok nem tudnak kommunikálni egy másik VLAN-ban lévő hosztokkal, hacsak nincs router vagy 3. rétegbeli switch, amely forgalomirányítási szolgáltatásokat nyújt. A VLAN-ok közötti forgalomirányítás a hálózati forgalom továbbítása egyik VLAN-ból egy másik VLAN-ba. Három lehetőség van: a hagyományos, a router-on-a-stick és az SVI-ket használó 3. rétegbeli switch. A hagyományos megoldás több Ethernet-interfésszel rendelkező routert használt. Minden egyes router interfész különböző VLAN-okban lévő switchporthoz volt csatlakoztatva. Ha minden egyes VLAN-hoz külön interfészt használunk, hamar elfogynak a rendelkezésre álló fizikai interfészek. A router-on-a-stick VLAN-ok közötti forgalomirányítási módszer esetében csak egy fizikai Ethernet-interfészre van szükség a hálózat több VLAN-ja közötti forgalom továbbításához. Egy Cisco IOS router Ethernet interfésze 802.1Q trönkként van konfigurálva, és egy 2. rétegbeli switch trönkportjához van csatlakoztatva. A router interfésze alinterfészek használatával van konfigurálva a forgalomirányításra alkalmas VLAN-ok azonosítására. A konfigurált alinterfészek szoftveralapú virtuális interfészek, amelyek egyetlen fizikai Ethernet interfészhez tartoznak. A modern módszerrel a VLAN-ok közötti forgalomirányítás egy 3. rétegbeli switch-en történik, SVI-k segítségével. Az SVI-t egy, a switch-en létező VLAN-hoz hozzuk létre. Az SVI ugyanazokat a funkciókat látja el a VLAN számára, mint egy router interfész. 3. rétegbeli feldolgozást biztosít az adott VLAN-hoz tartozó összes switchportra érkező vagy onnan küldött csomagok számára.

**Router-on-a-Stick Inter-VLAN Routing**

A switch VLAN-okkal és trönköléssel történő konfigurálásához hajtsuk végre a következő lépéseket: hozzuk létre és nevezzük el a VLAN-okat, hozzuk létre a felügyeleti interfészt, állítsuk be a hozzáférési portokat, és konfiguráljuk a trönkportokat. A router-on-a-stick módszer megköveteli, hogy minden egyes VLAN-hoz létre kell hozni egy alinterfészt. Az alinterfész létrehozásához az **interface** interface \_ id subinterface \_ id globális konfigurációs parancsot kell használni. Forgalomirányítás csak akkor lehetséges, ha minden alinterfész külön alhálózathoz tartozó IP-címet kap. Ha minden alinterfész létrejött, a fizikai interfészt a **no shutdown** interfészkonfigurációs parancs segítségével engedélyezni kell. Egy állomásról a **ping** parancs segítségével ellenőrizzük a kapcsolatot egy másik VLAN-ban lévő állomáshoz. A **ping** paranccsal ellenőrizzük a kapcsolódást az állomáshoz és a switch-hez. Az ellenőrzéshez és a hibaelhárításhoz használjuk a **show ip route** , **show ip interface brief** , **show interfaces** , és **show interfaces trunk** parancsokat.

**VLAN-ok közötti útválasztás 3. rétegbeli kapcsolókkal**

A vállalati telephelyek LAN-jai 3. rétegbeli switch-eket használnak a VLAN-ok közötti forgalomirányítás biztosítására. A 3. rétegbeli switch-ek hardveralapú kapcsolást használnak, hogy a routereknél nagyobb csomagfeldolgozási sebességet érjenek el. A 3. rétegbeli switch képességei közé tartozik az egyik VLAN-ból a másikba történő forgalomirányítás több kapcsolt virtuális interfész (SVI) használatával, valamint a 2. rétegbeli switchport 3. rétegbeli interfésszé (azaz irányított porttá) alakítása. A VLAN-ok közötti forgalomirányítás biztosításához a 3. rétegbeli switch-ek SVI-ket használnak. Az SVI-k konfigurálása ugyanazzal az **interface vlan** vlan-id paranccsal történik, mint amelyet a 2. rétegbeli switch-en a felügyeleti SVI létrehozásához használunk. A 3. rétegbeli SVI-t minden egyes irányítható VLAN-hoz létre kell hozni. A switch VLAN-okkal és trönköléssel történő konfigurálásához a következő lépéseket kell elvégezni: hozzuk létre a VLAN-okat, hozzuk létre az SVI VLAN-interfészeket, állítsuk be a hozzáférési portokat, és engedélyezzük az IP-alapú forgalomirányítást. Egy állomásról a **ping** parancs segítségével ellenőrizzük a kapcsolatot egy másik VLAN-ban lévő állomáshoz. Ezután a Windows alatt kiadott **ping** paranccsal ellenőrizzük az állomáshoz való kapcsolódást. A VLAN-okat statikus vagy dinamikus forgalomirányítással kell hirdetni. A forgalomirányítás engedélyezéséhez egy 3. rétegbeli switch-en irányított portot kell konfigurálni. Az irányított port egy 3. rétegbeli switch-en úgy jön létre, hogy egy másik 3. rétegbeli eszközhöz csatlakoztatott 2. rétegbeli porton letiltjuk a switchport funkciót. Az interfészen IPv4-konfigurációval beállítható, hogy csatlakozzon egy routerhez vagy egy másik 3. rétegbeli switch-hez. Annak beállításához, hogy egy 3. rétegbeli switch egy routerrel együtt forgalomirányítást végezzen, kövessük a következő lépéseket: az irányított port konfigurálása, a forgalomirányítás engedélyezése, az forgalomirányítás konfigurálása, a forgalomirányítás és a kapcsolódás ellenőrzése.

**Az Inter-VLAN Routing hibaelhárítása**

Számos oka lehet annak, hogy egy VLAN-ok közötti konfiguráció nem működik. Mindegyik kapcsolódási problémákkal függ össze, például hiányzó VLAN-okkal, a switch trönk vagy hozzáférési portjával kapcsolatos, valamint a router konfigurációjával kapcsolatos problémával. Egy VLAN hiányozhat, ha nem hozták létre, véletlenül törölték, vagy ha nem engedélyezett a trönkkapcsolaton. A VLAN-ok közötti forgalomirányítás másik problémája a rosszul konfigurált switchportokra vezethető vissza. A VLAN-ok közötti forgalomirányítás hagyományos megoldásánál rosszul konfigurált switchportot eredményezhet, ha a csatlakozó router portja nem a megfelelő VLAN-hoz van hozzárendelve. A router-on-a-stick megoldásnál a leggyakoribb ok a rosszul konfigurált trönkport. Ha a switch hozzáférési portjának konfigurációjával kapcsolatos probléma gyanúja merül fel, használjuk a **ping** és **show interfaces** interface-id **switchport** parancsokat a probléma azonosítására. A router-on-a-stick módszer konfigurációs problémái általában az alinterfészek hibás beállításához kapcsolódnak. Ellenőrizzük az alinterfész állapotát a **show ip interface brief** paranccsal.

4.5.4

## Ellenőrző kvíz - VLAN-ok közötti forgalomirányítás

Az űrlap teteje

1. Egy PC egy másik hálózaton levő webszerverhez szeretne hozzáférni. Melyik VLAN-ok közti módszer biztosít a harmadik rétegben legnagyobb sávszélességet és emellett alapértelmezett átjárót is a PC számára?

Az űrlap alja

Milyen skálázható módszert kell használni, ha VLAN-ok közti forgalomirányítást kell megvalósítani egy több, mint 1000 VLAN-t használó kapcsolt hálózaton?

Ha egy routert úgy konfigurálunk, hogy része legyen egy router-on-a-stick VLAN-ok közötti forgalomirányítási topológiának, akkor hol kell beállítani az IP-címet?

Egy kisméretű főiskola a 10-es VLAN-t használja a tantermi, a 20-as VLAN-t pedig az irodai hálózathoz. Mi szükséges a két VLAN közötti kommunikáció engedélyezéséhez, ha hagyományos VLAN-ok közötti forgalomirányítást használunk?

Mi a hátránya a többrétegű switch-ek használatának VLAN-ok közti forgalomirányítás esetén?

Melyik VLAN-ok közti kommunikációs mód igényli több alinterfész beállítását?

Mi a hátránya a router-on-a-stick VLAN-ok közötti forgalomirányítási módszernek?

Mi a 10-es szám jelentése az **encapsulation dot1Q 10 native** router alinterfész konfigurációs módbeli parancsban?

A többrétegű kapcsolón a VLAN-ok közötti útválasztás konfigurálása közben a hálózati rendszergazda a **no switchport** parancsot adja ki egy másik kapcsolóhoz csatlakoztatott interfészen. Mi a parancs célja?

A hálózati rendszergazda a következő parancsokat adja ki egy Cisco 3560-as switch-en. Mi a parancsok célja? Switch(config)# **interfész gigabites-thernet 0/1** Switch(config-if)# **nincs kapcsolóport**

Milyen működési módot kell használni azon a switchporton, amelyik egy olyan routerhez csatlakozik, amelyen router-on-a-stick VLAN-ok közötti forgalomirányítást használnak?

Melyik állítás írja le helyesen az SVI-ket használó VLAN-ok közötti forgalomirányítási módszert?

Hogyan irányítják a forgalmat több VLAN között egy többrétegű switch-en?

Mire van szükség a router-on-a-stick VLAN-ok közötti forgalomirányítás működéséhez?

A rendszergazda hibaelhárítást végzett egy router-on-a-stick topológián és arra a következtetésre jutott, hogy a probléma a router alinterfészein található VLAN-ok konfigurációjával van kapcsolatban. Melyik két parancsot használhatja a rendszergazda a routeren a probléma azonosítására? (Két jó válasz van.)

[4.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-ok közötti forgalomirányítás hibaelhárítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[5.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. STP fogalmak
2. Bevezetés

# Bevezetés

5.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az STP alapjairól szóló fejezetben!

Egy jól megtervezett 2. rétegbeli hálózat redundáns switch-ekkel és útvonalakkal rendelkezik, amelyek biztosítják, hogy ha egy eszköz leáll, egy másik switch-hez vezető út továbbra is rendelkezésre áll az adatok továbbításához. A hálózat felhasználói nem tapasztalnak semmilyen szolgáltatás-kiesést. A redundancia a hierarchikus hálózattervezés során megoldja az "egyetlen meghibásodási pont" problémáját, viszont létrehozhat egy másfajta problémát, amit 2. rétegbeli huroknak nevezünk.

Mi az a hurok? Képzeljük el, hogy egy koncerten vagyunk. Az énekes mikrofonja és az erősített hangszóró - számos okból - visszacsatolási hurkot hozhat létre. Amit hallunk, az egy felerősített jel a mikrofonból, amely a hangszóróból jön ki, majd a mikrofon újra felveszi, tovább erősödik, és újra áthalad a hangszórón. A hang pillanatok alatt nagyon hangossá és kellemetlenné válik, és lehetetlenné teszi, hogy halljuk a tényleges zenét. Ez a "gerjedés" addig folytatódik, amíg a mikrofon és a hangszóró közötti kapcsolatot meg nem szakítjuk.

A 2. rétegbeli hurok hasonló káoszt okoz egy hálózatban. Nagyon gyorsan létrejöhet, és lehetetlenné teszi a hálózat használatát. 2. rétegbeli hurkot létrehozni és a hibát terjeszteni többféle módszerrel is lehet. A feszítőfa-protokollt (Spanning Tree Protocol, STP) kifejezetten arra tervezték, hogy megszüntesse a 2. rétegbeli hurkokat a hálózatban. Ez a fejezet a hurkok okait és az STP-protokollok különböző típusait tárgyalja. Tartalmaz egy videót és egy Packet Tracer feladatot is, ami segíti az STP-fogalmak megértését.

5.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe** : STP fogalmak

**Modul célja** : Magyarázza el, hogyan teszi lehetővé az STP a redundanciát a 2. rétegű hálózatban.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Az STP célja** | Ismertesse a gyakori problémákat egy redundáns, L2 kapcsolt hálózatban. |
| **Az STP működése** | El tudjuk magyarázni, hogyan működik az STP egy egyszerű kapcsolt hálózatban. |
| **Az STP fejlődése** | Ismertesse a Rapid PVST+ működését. |

[4.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[5.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP célja](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. STP fogalmak
2. Az STP célja

# Az STP célja

5.1.1

## Redundancia a 2. rétegbeli kapcsolt hálózatokban

Ez a témakör a 2. rétegbeli hálózatban fellépő hurkok kialakulásának okait ismerteti, és röviden azt is, hogy miként működik a feszítőfa-protokoll. A redundancia fontos része a hálózattervezésnek; a segítségével elérhető, hogy ne legyen olyan gyenge pontja a hálózatnak, mely önmagában komoly zavart okozna a hálózati szolgáltatásokban. A redundáns hálózatokhoz további fizikai útvonalak hozzáadása szükséges, de a tervezés során a logikai redundanciát is szem előtt kell tartani. A hálózaton áthaladó adatok számára biztosított alternatív útvonalak lehetővé teszik, hogy a felhasználók azok zavara esetén is hozzáférjenek az erőforrásokhoz. Ugyanakkor a kapcsolt Ethernet hálózatban a redundáns útvonalak egyaránt vezethetnek fizikai és logikai (2. rétegbeli) hurkok keletkezéséhez.

Az Ethernet LAN-ok hurok nélküli topológiát igényelnek, amelyben egyetlen útvonal van bármely két eszköz között. Egy Ethernet LAN-ban a hurok a keretek folyamatos továbbítását okozhatja mindaddig, míg a kapcsolat meg nem szakad és meg nem szűnik a hurok.

5.1.2

## Feszítőfa-protokoll (Spanning Tree Protocol)

A Spanning Tree Protocol (STP) egy hurok létrejöttét megelőző hálózati protokoll, amely redundanciát tesz lehetővé egy hurokmentes 2. rétegbeli topológia létrehozásakor. Az IEEE 802.1D az eredeti IEEE-féle MAC Bridging szabvány STP-hez.

Az animáció megtekintéséhez kattintsunk a Lejátszás gombra!

### Az STP normál működése

A PC1 szórásos keretet küld.

Az S2 továbbítja a szórást az összes portján, kivéve a bejövő és a blokkolt portot.

Az S1 továbbítja a szórást minden portján, kivéve a bejövő portot.

Az S3 megkapja a keretet, és továbbítja visszafelé az S2-nek.

Az S2 eldobja a keretet, mert blokkolt porton kapta.

2. csomagtartó

Csomagtartó 1

3. csomagtartó

5.1.3

## Az STP újraszámítása

A hiba esetén szükséges STP-újraszámításról szóló animáció megtekintéséhez kattintsunk az alábbi ábrán látható Lejátszás gombra!

Az ábra az előző animációval megegyező topológiájú animáció. Az animációban az S2 és S1 közötti fővonali kapcsolat meghibásodott. Az S2 feloldja a Trunk 2 portjának blokkolását. A PC1 broadcast keretet küld az S2-nek. Az S2 továbbítja a szórást az összes kapcsolóporton, kivéve a kiinduló portot és az 1. fővonal meghibásodott összeköttetését. Az S3 továbbítja a szórást az összes elérhető kapcsolóporton, kivéve a kiinduló portot. Az S1 csak az F0/3-ból továbbítja az adást.

### Az STP kompenzálja a hálózati hibát

Az S2 és S1 közötti trönkkapcsolat hiba miatt leáll.

Az S2 feloldja a blokkolást a Trunk2 porton.

A PC1 szórásos keretet küld az S2-nek.

Az S2 a szórásos keretet minden switchportján továbbítja, kivéve a bejövő, valamint a meghibásodott Trunk1 portot.

Az S3 továbbítja a szórást minden működő portján, kivéve a bejövő portot.

Az S1 csak az F0/3-ra továbbítja a szórást.

2. csomagtartó

Csomagtartó 1

3. csomagtartó

5.1.4

## A redundáns switch-kapcsolatok problémái

Az útvonal-redundancia több hálózati szolgáltatást nyújt azáltal, hogy kiküszöböli az egyetlen meghibásodási pont lehetőségét. Amikor két eszköz között több útvonal is létezik, és a switchek nem használnak feszítőfa-megoldásokat, 2. rétegbeli hurok jön létre. A 2. rétegbeli hurok a MAC-címtábla instabilitását, a kapcsolatok telítődését, valamint a switch-ek és a végberendezések nagy CPU-kihasználtságát eredményezheti, amitől a hálózat használhatatlanná válik.

A 3. rétegbeli IPv4 és az IPv6 protokollokkal ellentétben a 2. rétegbeli Ethernet nem tartalmaz olyan mechanizmust, amely lehetővé tenné a végtelen hurokba került keretek felismerését és eltávolítását. Az IPv4 és az IPv6 TTL-alapú (élettartam) módszerrel korlátozza le, hogy a 3. rétegbeli eszközök legfeljebb hányszor továbbíthassák a csomagot. Egy router minden IPv4-csomagban csökkenti a TTL (Time to Live) értékét, illetve minden IPv6-csomagban a Hop Limit mezőt. Ha ezek a mezők 0-ra csökkennek, a router eldobja a csomagot. Maga az Ethernet és az Ethernet switch-ek nem rendelkeznek ezzel összevethető mechanizmussal annak korlátozására, hogy egy switch hányszor továbbíthat egy 2. rétegbeli keretet. Az STP-t kifejezetten a 2. rétegbeli Ethernet hurok megelőzési mechanizmusaként fejlesztették ki.

5.1.5

## 2. rétegbeli hurkok

Az STP engedélyezése nélkül 2. rétegbeli hurkok keletkezhetnek, így a szórásos, a csoportos és az ismeretlen célú egyedi címzésű keretek a végtelenségig bolyonghatnak a hálózaton. Ez nagyon rövid időn belül, esetenként csupán néhány másodperc alatt leállíthatja a hálózatot. A szórásos kereteket (pl.: az ARP-kérést) például az összes switchport továbbítja, kivéve az eredeti bejövő portot. 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 switch MAC-címtáblázata a szórásos keretek alapján folyamatosan változni fog, ami a MAC-címtábla instabilitásához vezet. Ez nagy CPU-kihasználtságot okozhat, ami miatt a switch nem képes továbbítani a kereteket.

A hurkok nem csak a szórásos kereteket érintik. A hurkot tartalmazó hálózatba küldött ismeretlen célú egyedi címzésű keretek esetenként megkettőzve érnek a céljukhoz. Ismeretlen célú egyedi címzésű keret az, amikor a switch nem rendelkezik a cél MAC-címmel a címtáblájában, és a keretet ki kell küldenie az összes porton, kivéve a bejövő portot.

Az animáció megtekintéséhez kattintsunk a Lejátszás gombra! Amikor az animáció megáll, olvassuk el a műveletet leíró szöveget. Az animáció rövid szünet után folytatódik.

S3 MAC táblázat

S1 MAC táblázat

S2 MAC táblázat

S3 MAC táblázat

S1 MAC táblázat

S2 MAC táblázat   
PC1 = F0/11

S3 MAC táblázat   
PC1 = F0/2

S2 MAC táblázat   
PC1 = F0/11

S1 MAC táblázat   
PC1 = F0/1

S3 MAC táblázat   
PC1 = F0/1

S2 MAC táblázat   
PC1 = F0/11

S1 MAC táblázat   
PC1 = F0/2

S3 MAC táblázat   
PC1 = F0/1

S2 MAC táblázat   
PC1 = F0/1

S1 MAC táblázat   
PC1 = F0/2

Az S2 frissíti a MAC-címtáblázatot. A PC1 MAC-címe F0/11-re van leképezve.

Az S2 a vételi port kivételével minden porton továbbítja az adást.

Az S3 és az S1 frissíti a MAC-címtáblázatát a PC1 információkkal.

Az S3 és S1 a vételi port kivételével az összes porton továbbítja a sugárzást.

Az S1 és S3 csomagot kap a PC1-től egy új porton. Ennek megfelelően frissítik a MAC-címtáblázatukat.

Az S1 és S3 a vételi port kivételével az összes porton továbbítja a sugárzást.

Az S2 frissíti a MAC-címtábláját PC1-el kapcsolatban az utolsó porttal, amelyen megkapta a szórásos keretet.

S2 továbbítja a szórást kifelé minden portján, kivéve a bejövő portot. A ciklus újrakezdődik.

2. csomagtartó

1. csomagtartó

3. csomagtartó

5.1.6

## Szórási vihar

A szórási vihar abnormálisan nagy számú szórásos üzenet, amely egy adott idő alatt túlterheli a hálózatot. A szórási vihar másodpercek alatt leterhelheti a hálózatot alkotó switch-eket és végberendezéseket. A szórási viharokat hardveres probléma, például hibás hálózati kártya vagy a hálózatban lévő 2. rétegbeli hurok okozhatja.

A 2. rétegbeli szórások (pl.: az ARP-kérések) nagyon gyakoriak egy hálózatban. A 2. rétegbeli hurok valószínűleg azonnal kialakul és leállítja a hálózatot. A 2. rétegbeli csoportcímzésű üzeneteket általában ugyanúgy továbbítja a switch, mint a szórásokat. Bár az IPv6-os csomagokat soha nem továbbítjuk 2. rétegbeli szórásként, az ICMPv6 szomszédfelderítése (ND) a 2. rétegbeli csoportcímzést használja.

Kattintsunk az ábrán látható Lejátszás gombra egy olyan animáció megtekintéséhez, ami egy hurok egyre kedvezőtlenebb hatásait mutatja, mivel a szórás és az ismeretlen célú egyedi címzésű keretek továbbra is határozatlan ideig továbbítódnak egy szórási viharban.

A PC1 továbbít egy szórást, ami egy 2. rétegbeli hurokba kerül.

A PC4 egy újabb szórást küld, ami szintén hurokba kerül.

A PC3 továbbít egy másik szórást, ami ismét csak hurokba kerül.

A PC2 továbbítaná a szórásos keretet, de az a hálózat forgalmi túlterhelése miatt nem dolgozható fel.

2. csomagtartó

1. csomagtartó

3. csomagtartó

A hurokban érintett állomás nem képes elérni a hálózat többi állomását. Ezen felül a MAC-címtábla folyamatos változása miatt a switch nem tudja, hogy az egyedi kereteket melyik portjára kellene továbbítania. A fenti példában a switch-ek helytelen portot tárolnak a PC1-hez. Bármilyen, a PC1-nek szánt ismeretlen célú egyedi címzésű keret kering (körbe) a hálózaton, mint ahogy a szórásos keretek. Egyre több keret jön létre, ami végül létrehoz egy szórási vihart.

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

5.1.7

## A feszítőfa-algoritmus (STA)

Az STP egy Radia Perlman által kifejlesztett algoritmuson alapul, amelyet akkor alkotott meg, amikor a Digital Equipment Corporation-nél dolgozott. 1985-ös publikációjának eredeti címe "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN". A feszítőfa algoritmusa (Spanning Tree Algorithm, STA) hurokmentes topológiát hoz létre egy gyökérponti híd (root bridge) kiválasztásával, ami felé az összes többi switch egyetlen, legalacsonyabb költségű útvonalat határoz meg.

Enélkül a protokoll nélkül hurkok jönnének létre, ami a redundáns kapcsolt hálózatot működésképtelenné tenné.

Az egyes gombokra kattintva megtekinthetjük annak magyarázatát, hogy az STA miként hoz létre hurokmentes topológiát.

**STA forgatókönyv topológia**

Ez az STA forgatókönyv több kapcsoló között redundáns kapcsolatokkal rendelkező Ethernet LAN-t használ.

A fizikai hálózati topológia nyolc összekapcsolt kapcsolót mutat. Az S1 kapcsoló az S2, S3 és S5 kapcsolókhoz csatlakozik. Az S2 kapcsoló az S1 és S4 kapcsolókhoz csatlakozik. Az S3 kapcsoló az S1 és S5 kapcsolókhoz csatlakozik. Az S4 kapcsoló az S2 és S5 kapcsolókhoz csatlakozik. Az S5 kapcsoló az S1, S3, S4 és S6 kapcsolókhoz csatlakozik. Az S6 kapcsoló az S5 kapcsolóhoz csatlakozik. Az S7 kapcsoló az S8 kapcsolóhoz csatlakozik. Az S8 kapcsoló az S4, S5 és S7 kapcsolókhoz csatlakozik.

S1 S3 S2 S4 S5 S6 S7

S8

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

5.1.8

## Videó - Az STP működésének megfigyelése

Az STP bemutatójának megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

5.1.9

## Packet Tracer — Az STP hurokmegelőzésének vizsgálata

A Packet Tracer feladat során a következőket fogjuk elvégezni:

* Egy egyszerű, három switch-ből álló hálózat létrehozása és konfigurálása STP-vel
* Az STP működésének megfigyelése
* Az STP letiltása és a működés megtekintése újra

[STP-hurok megelőzésének vizsgálata](https://contenthub.netacad.com/courses/srwe-dl/_common/5.1.9-packet-tracer---investigate-stp-loop-prevention_hu-HU.pka)

5.1.10

## Tudáspróba - Az STP célja

Az űrlap teteje

Ellenőrizze, hogy megértette-e az STP célját, és válassza ki a megfelelő választ a következő kérdésekre.

1. Melyik állítás írja le legjobban az STP-t?

Az űrlap alja

Without STP on the Ethernet LAN, which three types of frames could cause a catastrophic loop in the network? (Három jó válasz van.)

Milyen eszközt választ a Spanning Tree Algorithm? Az összes többi kapcsoló egyetlen legalacsonyabb költségű utat határoz meg ehhez az eszközhöz.

[5.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[5.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. STP fogalmak
2. Az STP működése

# Az STP működése

5.2.1

## A hurokmentes topológia létrehozásának lépései

Most már tudjuk, hogyan jönnek létre a hurkok, és az STP alapjait is ismerjük, ami megakadályozza ezeket. Ez a témakör lépésről lépésre vezet végig az STP működésén. Az STP hurokmentes topológiát épít fel egy négy lépéses folyamat során:

1. A gyökérponti híd kiválasztása
2. Gyökérportok megválasztása
3. Kijelölt portok megválasztása
4. Alternatív (blokkolt) portok kiválasztása

Az STA és STP funkciók során a switchek a Bridge Protocol Data Unit-nak (BPDU) nevezett üzenetek (keretek) használatával osztják meg a magukról és kapcsolataikról szóló információkat. A BPDU-k a gyökérponti híd, a gyökérportok, a kijelölt portok és az alternatív portok kiválasztására szolgálnak. Minden BPDU tartalmaz egy hídazonosítót (Bridge Identifier, BID), amely azonosítja, hogy melyik switch küldte azt. A BID számos STA-döntés meghozatalában vesz részt, beleértve a gyökérponti híd és a portszerepek kiválasztását. As shown in the figure, the BID contains a priority value, an extended system ID, and the MAC address of the switch. A három mező egyesített értékét használják, így határozzák meg a legalacsonyabb értékű hídazonosítót.

A grafikon három négyzet látható, amelyek mindegyike a hídazonosító egy-egy összetevőjét képviseli. Balról jobbra az első doboz a Bridge Priority, amely 4 bit hosszú, a második doboz a kiterjesztett rendszerazonosító, amely 12 bit hosszú, a harmadik pedig a MAC-cím, amely 48 bit hosszú. A mezőktől jobbra található szöveg Hídazonosító a kiterjesztett rendszerazonosítóval. A grafika alján olvasható szöveg A BID tartalmazza a Bridge prioritást, a kiterjesztett rendszerazonosítót és a kapcsoló MAC-címét.

A híd prioritása kiterjesztve   
System ID MAC-cím Bridge ID a kiterjesztett rendszer-azonosítóval 4 bit 12 bit 48 bit

A BID tartalmazza a hídprioritást, a kiterjesztett rendszer-azonosítót és a switch MAC-címét.

**Híd prioritás**

A Cisco switch-ek alapértelmezett prioritása a decimális 32768. Az érték 0 és 61440 közé eshet, 4096-os lépésekben. A legalacsonyabb értékű prioritást részesítjük előnyben. A 0 érték minden más prioritás előtt elsőbbséget élvez.

**Kiterjesztett rendszerazonosító**

A kiterjesztett rendszer-azonosító a hídprioritás értékéhez adódik hozzá a BID-en belül és bekerül a BPDU-ba, meghatározva annak VLAN-ját.

Az IEEE 802.1D korai megvalósításai olyan hálózatokhoz készültek, amelyek nem használtak VLAN-okat, minden switch egy közös feszítőfába tartozott. Emiatt a régebbi switch-ekben a kiterjesztett rendszer-azonosító nem szerepelt a BPDU-kban. 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.

The extended system ID allows later implementations of STP to have different root bridges for different sets of VLANs. Ez lehetővé teszi, hogy egy adott VLAN-csoporthoz tartozó STP-topológiában a redundáns, nem-továbbító kapcsolatokat egy másik gyökérponti híddal rendelkező VLAN-csoport továbbítóként használjon.

**MAC address**

Amikor két switch ugyanazt a prioritást kapja, és a kiterjesztett rendszer-azonosítójuk is egyforma, akkor az alacsonyabb hexadecimális értékű MAC-címmel rendelkező switch-nek lesz kisebb a hídazonosítója.

5.2.2

## 1. A gyökérponti híd kiválasztása

Az STA kiválaszt egy switch-et, amelyet gyökérponti hídnak (root bridge) nevezünk, ez lesz minden útvonalszámítás kiindulási pontja. A switch-ek BPDU-kat cserélnek, hogy létrehozzák a hurokmentes topológiát, kezdve a gyökérponti híd kiválasztásával.

A gyökérponti híd meghatározása választási folyamat során történik. A szórási tartományban lévő minden switch részt vesz a választásban. Miután egy switch elindul, két másodpercenként BPDU-kereteket kezd küldeni. Ezek a BPDU-keretek tartalmazzák a küldő switch BID-jét és a gyökérponti híd BID-jét, amelyet Root ID néven ismerünk.

A legalacsonyabb BID-értékű switch lesz a gyökérponti híd. Először minden switch gyökérponti hídnak nyilvánítja magát, a saját BID-jét Root ID-ként beállítva. Végül a switch-ek megtanulják a BPDU-k cseréje révén, hogy melyik switch-nek a legalacsonyabb a BID-je, és megállapodnak abban, melyik lesz a gyökérponti híd.

Az ábrán az S1-et választják gyökérponti hídnak, mert ennek a legalacsonyabb a BID-je.

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint négy PC-t (PC1, PC2, PC3, PC4) mutat. S1 a gyökérhíd. Az S1 hídazonosítója prioritás = 24577 és MAC-cím = 000A00333333. Az S1 az S3 kapcsoló F0/2 portjához és az S2 F0/1 kapcsolóporthoz csatlakozik. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/3 kapcsolóporton keresztül. Az S2 hídazonosítója prioritás = 32769 és MAC-cím = 000A00111111. Az S2 az S3 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 az F0/11 kapcsolóporton keresztül csatlakozik a PC1-hez, az F0/18 kapcsolóporton keresztül csatlakozik a PC2-hez, és az F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S3 hídazonosítója prioritás = 32769 és MAC-cím = 000A00222222. Az S3 az S2 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. A PC4 IP-címe 172.17.10.27.

PC2 PC1 PC3 S3 S2 S1 PC4 F0/1 F0/2 F0/ 18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6 172.17.10.27 172.17.10.23 172.17.10.22 172.17.10.21

F0/3

Trunk3 Trunk1 Trunk2 gyökérhídhíd azonosítója:   
Prioritás = **32769**   
MAC-cím = 000A00222222 Hídazonosító:   
Prioritás = **24577**   
MAC-cím = 000A00333333 Hídazonosító:   
Prioritás = **32769**   
MAC-cím = 000A00111111

5.2.3

## Az alapértelmezett BID-ek hatása

Mivel az alapértelmezett BID 32768, lehetséges, hogy két vagy több switch azonos prioritással rendelkezik. Abban az esetben, ha minden switch prioritása azonos, a legalacsonyabb MAC-című lesz a gyökérponti híd. Ha a rendszergazda szeretné a gyökérponti híd kiválasztását a hálózat igényeihez igazítani, a gyökérponti hídnak szánt switch prioritását alacsonyabbra kell állítania.

Az ábrán az összes switch ugyanolyan értékű, 32769-es prioritással van konfigurálva. Tehát a gyökérponti híd kiválasztásának döntő tényezője a MAC-cím lesz. A legalacsonyabb hexadecimális MAC-című eszköz lesz a preferált gyökérponti híd. A példában az S2 MAC-címe a legalacsonyabb, tehát ez lesz az adott feszítőfa gyökérponti hídja.

**Note** : In the example, the priority of all the switches is 32769. Ez úgy áll elő, hogy az alapértelmezett 32768-as prioritáshoz hozzáadódik a kiterjesztett rendszer-azonosító, a switch-eken hozzárendelt 1-es VLAN-é (32768+1).

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint négy PC-t (PC1, PC2, PC3, PC4) mutat. S2 a gyökérhíd. Az S1 hídazonosítója prioritás = 32769 és MAC-cím = 000A00333333. Az S1 az S3 kapcsoló F0/2 portjához és az S2 F0/1 kapcsolóporthoz csatlakozik. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/3 kapcsolóporton keresztül. Az S2 hídazonosítója prioritás = 32769 és MAC-cím = 000A00111111. Az S2 az S3 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 az F0/11 kapcsolóporton keresztül csatlakozik a PC1-hez, az F0/18 kapcsolóporton keresztül csatlakozik a PC2-hez, és az F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S3 hídazonosítója prioritás = 32769 és MAC-cím = 000A00222222. Az S3 az S2 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. A PC4 IP-címe 172.17.10.27.

PC2 PC1 PC3 S3 S2 PC4 S1 F0/1 F0/2 F0/ 18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6 172.17.10.27 172.17.10.23 172.17.10.22 172.17.10.21

F0/3

Trunk3 Trunk1 Trunk2 gyökérhídhíd azonosítója:   
Prioritás = 32769   
MAC-cím = **000A00222222** Hídazonosító:   
Prioritás = 32769   
MAC-cím = **000A00333333** Hídazonosító:   
Priority = 32769  
MAC-cím = **000A00111111**

5.2.4

## A gyökérelérési útvonal költségének meghatározása

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 elérési útvonalat, amelyet belső gyökérelérési útvonalnak nevezünk, a switch-től a gyökérponti hídig vezető útvonal mentén felmerülő összes egyedi portköltség összege határozza meg.

**Note** : The BPDU includes the root path cost. Ez az útvonal költsége a küldő switch-től a gyökérponti hídig.

Amikor egy switch megkapja a BPDU-t, hozzáadja a szegmens belépési portjának költségét a gyökérelérési útvonal költségének meghatározásához.

Az alapértelmezett portköltség a port sebességéből adódik. A táblázat az IEEE által javasolt alapértelmezett portköltségeket mutatja. A Cisco switch-ek alapértelmezés szerint az IEEE 802.1D szabvány (más néven legrövidebb útvonalköltség) által meghatározott értékeket használják mind az STP, mind az RSTP esetében. Az IEEE szabvány azonban azt javasolja, hogy az IEEE-802.1w (más néven teljes útvonalköltség) által meghatározott értékeket használjuk 10 Gbit/s és annál gyorsabb kapcsolatok esetében.

**Megjegyzés** : Az RSTP-t a modul későbbi részében részletesebben tárgyaljuk.

| Link SpeedSTP költség: IEEE 802.1D-1998 RSTP költség: IEEE 802.1w-2004 10 Gb/s22,0001 Gb/s420,000100 Mb/s19200,00010 Mb/s10000,0 | | |
| --- | --- | --- |
| **Összeköttetés sebessége** | **STP-költség: IEEE 802.1D-1998** | **RSTP-költség: IEEE 802.1w-2004** |
| 10 Gbps | 2 | 2,000 |
| 1 Gbps | 4 | 20,000 |
| 100 Mbps | 19 | 200,000 |
| 10 Mbit/s | 100 | 2 000 000 |

Habár a switchportokhoz alapértelmezett költségértéket rendeltek, ez az érték átkonfigurálható. A rendszergazda az egyes portok költségének beállításával rugalmasan képes befolyásolni a gyökérponti hídhoz vezető feszítőfa-útvonalakat.

5.2.5

## 2. Gyökérportok megválasztása

A gyökérponti híd meghatározása után az STA-algoritmust használják a gyökérport kiválasztására. Minden, nem gyökérponti híd kiválaszt egy gyökérportot. A gyökérport a gyökérponti hídhoz legközelebb eső port, a hozzá vezető teljes költség (legjobb útvonal) szempontjából. Ez a teljes költség az úgynevezett belső gyökérelérési útvonalköltség.

Az útvonal költsége a gyökérponti hídhoz vezető útvonalon levő portok költségeinek összege. A legalacsonyabb költségű útvonal a legelőnyösebb, minden más redundáns útvonal pedig le lesz tiltva. A példában az S2 és az S1, mint gyökérponti híd közötti 1-es útvonal költsége 19 (az IEEE szerinti alapértelmezett költségekkel), a 2-es útvonal költsége pedig 38. Mivel az 1-es útvonalnak alacsonyabb a gyökérponti hídhoz vezető teljes költsége, ez az előnyben részesített útvonal, és az F0/1 lesz az S2 gyökérportja.

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint négy PC-t (PC1, PC2, PC3, PC4) mutat. S1 a gyökérhíd. Az S1 hídazonosítója prioritás = 32769 és MAC-cím = 000A00333333. Az S1 az S3 kapcsoló F0/2 portjához és az S2 F0/1 kapcsolóporthoz csatlakozik. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/3 kapcsolóporton keresztül. Az S2 hídazonosítója prioritás = 32769 és MAC-cím = 000A00111111. Az S2 az S3 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S2 F0/1 kapcsolóportja gyökérportként van jelölve. Az S2 és S3 közötti kapcsolat a 2. fővonal címkével van ellátva. Az S2-től S1-be vezető útvonal 1-es út. Az S2-től S3-ig tartó elérési út 2-es út. Az S2 a PC1 F0/11 kapcsolóporton keresztül, a PC2 F0/18 kapcsolóporton keresztül, és a PC3 F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S3 hídazonosítója prioritás = 32769 és MAC-cím = 000A00222222. Az S3 az S2 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S3 F0/1 kapcsolóportja gyökérportként van jelölve. Az S3-tól S1-ig tartó elérési út 2-es elérési út. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. A PC4 IP-címe 172.17.10.27. A grafika alján található szöveg: 1. útvonal költsége = 19x1=19. 2. útvonal költsége = 19x2=38. Az 1. útvonal a preferált útvonal.

PC2 PC1 PC3 S3 S2 S1 PC4 F0/1 F0/2 F0/ 18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6 172.17.10.27 172.17.10.23 172.17.10.22 172.17.10.21

F0/3

Trunk3 Trunk1 Trunk2 Root Bridge Root port 2-es útvonal 1-es útvonal 2-es útvonal Root port **1-es útvonal** költsége = 19 x 1 = **19**   
**2-es útvonal** költsége = 19 x 2 = **38**   
Az 1-es útvonal az előnyben részesített útvonal.

5.2.6

## 3. Kijelölt portok megválasztása

Az, hogy a feszítőfa miként akadályozza meg a hurok létrejöttét, nyilvánvalóvá válik a következő két lépés során. Miután minden switch kiválasztja a gyökérportot, megválasztják a kijelölt portokat.

Két adott switch között minden szegmensen egy kijelölt port lesz. A kijelölt port a szegmens (amit két switch alkot) egy portja, amelynek a gyökérponti hídhoz vezető gyökérelérési útvonalköltsége a legkisebb. Más szóval, a kijelölt port renelkezik a legjobb útvonallal a gyökérponti hídhoz vezető forgalom fogadásához.

Ami nem gyökérport vagy kijelölt port, alternatív vagy lezárt porttá válik. A végeredmény egyetlen útvonal minden switch-től a gyökérponti hídig.

Az egyes gombokra kattintva megtekinthejük a magyarázatokat, hogy miként választja ki az STA a kijelölt portokat.

**Kijelölt portok a Root Bridge-en**

All ports on the root bridge are designated ports, as shown in the figure. Ez azért van, mert a gyökérponti híd biztosítja a legalacsonyabb költséget saját magához.

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint négy PC-t (PC1, PC2, PC3, PC4) mutat. S1 a gyökérhíd. Az S1 az S3 kapcsoló F0/2 portjához és az S2 F0/1 kapcsolóporthoz csatlakozik. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/3 kapcsolóporton keresztül. Az S1 F0/3 kapcsolóportja egy kijelölt port. Az S1 F0/2 kapcsolóportja egy kijelölt port. Az S1 F0/1 kapcsolóportja egy kijelölt port. Az S2 az S3 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 az F0/11 kapcsolóporton keresztül csatlakozik a PC1-hez, az F0/18 kapcsolóporton keresztül csatlakozik a PC2-hez, és az F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S2-n lévő F0/1 kapcsoló port a root port. Az S3 az S2 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S3 F0/1 kapcsolóportja egy gyökérport. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. A PC4 IP-címe 172.17.10.27. Az ábra alján olvasható szöveg: A gyökérhíd összes portja kijelölt port.

PC2 PC1 PC3 S3 S2 S1 PC4 F0/1 F0/2 F0/ 18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6 172.17.10.27 172.17.10.23 172.17.10.22 172.17.10.21

F0/3

Trunk3 Trunk1 Trunk2 Root Bridge Root Port Kijelölt Port Kijelölt Port Root Port Kijelölt Port

Egy gyökérponti híd minden portja kijelölt port.

5.2.7

## 4. Alternatív (lezárt) portok kijelölése

Ha egy port nem gyökérport vagy kijelölt port, akkor alternatív (vagy tartalék) porttá válik. 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 portja lezárt állapotban van, és nem továbbít Ethernet kereteket. Minden más, switch-ek közti port továbbító állapotban van. Ez az STP hurokmegelőző eljárása.

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint négy PC-t (PC1, PC2, PC3, PC4) mutat. S1 a gyökérhíd. Az S1 az S3 kapcsoló F0/2 portjához és az S2 F0/1 kapcsolóporthoz csatlakozik. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/3 kapcsolóporton keresztül. Az S1 F0/3 kapcsolóportja egy kijelölt port. Az S1 F0/2 kapcsolóportja egy kijelölt port. Az S1 F0/1 kapcsolóportja egy kijelölt port. Az S2 az S3 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 az F0/11 kapcsolóporton keresztül csatlakozik a PC1-hez, az F0/18 kapcsolóporton keresztül csatlakozik a PC2-hez, és az F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S2-n lévő F0/1 kapcsoló port a root port. Az S2 kapcsoló F0/2 portja a kijelölt port. Az S3 az S2 kapcsoló F0/2 portjához és az S1 F0/1 kapcsolóporthoz csatlakozik. Az S3 F0/1 kapcsolóportja egy gyökérport. Az S3 F0/2 kapcsolóportja egy alternatív port. Egy piros kör alakú blokkoló szimbólum van elhelyezve a fővonalon az S3 és S2 között, az S3 F0/2 interfésze mellett. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. A PC4 IP-címe 172.17.10.27. Az ábra alján olvasható szöveg: Az S2 Fa0/2 interfésze az S3 szegmens kijelölt portja.

PC2 PC1 PC3 S3 S2 S1 PC4 F0/1 F0/2 F0/ 18 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6 172.17.10.27 172.17.10.23 172.17.10.22 172.17.10.21

F0/3

Trunk3 Trunk1 Trunk2 Root Bridge Root Port Kijelölt Port Kijelölt Port Gyökérport Kijelölt Port Alternatív Port Kijelölt Port

Az S3 Fa0/2 interfésze nem gyökérport vagy kijelölt port, így alternatív vagy blokkolt porttá válik.

5.2.8

## Gyökérport kijelölése több, egyenlő költségű útvonalon

A gyökérport és a kijelölt portok a gyökérponti hídhoz vezető legalacsonyabb költségű útvonalon alapulnak. De mi történik, ha egy switch több egyenlő költségű útvonallal rendelkezik a gyökérponti hídhoz? Hogyan jelöl ki a switch egy gyökérportot?

Ha egy switch több egyenlő költségű útvonalat is ismer a gyökérponti hídhoz, a következő feltételek alapján választja ki a portot:

1. A küldő legalacsonyabb BID-je
2. A küldő legalacsonyabb portprioritása
3. A küldő legalacsonyabb portazonosítója

A példákért és magyarázatokért kattintsunk az egyes kritériumokra!

**1 . Legalacsonyabb feladó BID**

The figure shows a topology with four switches, including switch S1 as the root bridge. Ha megnézzük a portszerepeket, akkor az S3 switch F0/1 és az S4 switch F0/3 portjai lesznek a gyökérportok, mert ezek gyökérponti híd felé vezető útvonalköltségei a legkisebbek. Az S2-nek két egyenlő költségű portja vezet a gyökérponti híd felé, az F0/1 és az F0/2. Ebben az esetben a szomszédos S3 és S4 switch-ek hídazonosítói fogják eldönteni a kérdést. Ezt a küldő hídazonosítójának nevezzük. Az S3 hídazonosítója 32769.5555.5555.5555, az S4-é pedig 32769.1111.1111.1111. Mivel az S4 hídazonosítója alacsonyabb, az S2 F0/1-es, S4-hez kapcsolódó portja lesz a gyökérport.

A fizikai hálózati topológia négy összekapcsolt kapcsolót mutat, S1, S2, S3 és S4. Az S1 a gyökérhíd, és az F0/1 kapcsolóporton keresztül csatlakozik az S4-hez és az F0/2 fővonali porton keresztül az S3-hoz. Az S1 és S4 közötti kapcsolatot Trunk 1-nek nevezik. Az S1 F0/1 interfésze egy kijelölt port. Az S1 hídazonosítója 24577.3333.3333.3333. Az S1 az F0/2 kapcsolóporton keresztül csatlakozik az S3-hoz. Az S1 és S3 közötti kapcsolat a Trunk 3 felirattal van ellátva. Az S1 F0/2 interfésze egy kijelölt port. Az S4 az S1 kapcsoló F0/3 portjához csatlakozik, amely egy gyökérport. Az S4 az S2 kapcsoló F0/1 portjához csatlakozik, amely egy kijelölt port. Az S4 és S2 közötti linket Trunk 4-nek nevezik. Az S4 Bridge ID 32769.1111.1111.1111. Az S2 az S4 F0/1 kapcsolóporthoz csatlakozik, amely egy gyökérport, és az S3 kapcsoló F0/2 portjához, amely egy alternatív port. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 F0/2 interfésze mellett egy piros X látható, jelezve, hogy blokkolja a forgalmat. Az S2 hídazonosítója 32769.AAAA.AAAA.AAAA. S3 csatlakozik az S2 over F0/2 kapcsolóporthoz, amely egy kijelölt port, és az S1 over switchporthoz, az F0/1 kapcsolóporthoz, amely egy gyökérport. Az S3 hídazonosítója: 32769.5555.5555.5555.

S3 S1 S2 S4 F0/1 F0/2 F0/3 F0/1 F0/1 F0/2 F0/1

F0/2

Trunk3 Trunk2 Trunk1 Root Bridge Trunk4 Bridge ID = 24577.3333.3333.3333 Root Port Kijelölt Port Alternatív Kijelölt Port Port Gyökérport Kijelölt Port Kijelölt Port Gyökér Port Bridge ID = 32769.5555.5555.5555 Bridge ID = 32769.5555.5555.5555 Bridge ID = 32769.5555.5555.5555 Bridge ID = 32769.5555.5555.5555 Bridge ID = 3277.5555.5555.5555 Bridge ID = 3277.5555.5555.5555 Bridge ID = 3277.5555.5555.5555 Bridge ID = 3277.3333.3333.3333. 1.1111

5.2.9

## STP-időzítők és -portállapotok

Az STP a konvergenciához három időzítőt használ, az alábbiak szerint:

* **Hello Timer** - The hello time is the interval between BPDUs. Az alapértelmezett érték 2 másodperc, de 1 és 10 másodperc közötti értékre módosítható.
* **Forward Delay Timer** - The forward delay is the time that is spent in the listening and learning state. Az alapértelmezett érték 15 másodperc, de 4 és 30 másodperc közötti értékre módosítható.
* **Max Age Timer** - The max age is the maximum length of time that a switch waits before attempting to change the STP topology. Az alapértelmezett érték 20 másodperc, de 6 és 40 másodperc közötti értékre módosítható.

**Megjegyzés** : Az alapértelmezett idők módosíthatók a gyökérhídon, amely meghatározza ezen időzítők értékét az STP tartomány számára.

Az STP a szórási tartományban logikai hurokmentes útvonalakat biztosít. A feszítőfa felépítése a csatlakoztatott kapcsolók közötti BPDU-keretek cseréje során tanult információn alapul. Ha egy switchport lezárt állapotból azonnal továbbító állapotba lépne anélkül, hogy a teljes topológiát megismerné, akkor ez a port hurkot képezhetne a hálózatban. Ezért az STP öt portállapottal rendelkezik, amelyek közül négy az ábrán látható működő portállapot. A letiltott állapot nem működőképes állapot.

**Note** : Az STP-vel kapcsolatos problémák elkerülése érdekében az IEEE legfeljebb hét kapcsoló átmérőjét javasolja az alapértelmezett STP időzítők használatakor.

Az ábra a négy STP működési állapotát ábrázoló folyamatábrát mutatja. A folyamatábra tetején a Blokkolás állapot látható. Blokkolás állapotban nem érkezik BPDU, és a Max Age = 20 másodperc. Egy nyíl mutat a Blokkolás állapotból a Hallgatás állapotba. A Listening állapot előrehaladási késleltetése 15 másodperc. Van egy nyíl, amely a Hallgatás állapotból a Tanulási állapotba mutat. A tanulási állapot előrehaladási delday = 15 másodperc. Van egy nyíl, amely a tanulási állapotból a továbbítási állapotba mutat. Létezik egy folyamatábra, amelynek címei. A hivatkozás egy nyíllal jelenik meg, amely egy második, Blokkolás című mezőre mutat. A Blokkolás mező szövege Blokkoló állapotban állapotú, amíg az SPT meg nem határozza, hogy a port gyökér vagy kijelölt port-e. Ebben a mezőben van egy nyíl, amely a hallgatási állapotra mutat.

**Blokkolás**

* Nem érkezett BPDU
* Max. életkor = 20 másodperc

**Listening (Figyelő)**

* Továbbítási késleltetés = 15 másodperc

**Learning (Tanuló)**

* Továbbítási késleltetés = 15 másodperc

**Forwarding (Továbbító) Blocking**

* Lezárt állapot, amíg az STP meg nem határozza, hogy a port gyökér- vagy kijelölt port-e

**Működni kezd az összeköttetés**

Az egyes portállapotok részleteit a táblázat tartalmazza.

| Táblázat felirata | |
| --- | --- |
| **Portállapot** | **Leírás** |
| Blokkolás | Alternatív port, nem vesz részt a keretek továbbításában. A port BPDU-kereteket fogad, hogy meghatározza a gyökérponti híd helyét és azonosítóját. A BPDU-keretek azt is meghatározzák, hogy mely portszerepköröket kell minden switchportnak felvennie a végső, aktív STP-topológiában. A max. életkor időzítő 20 másodpercének leteltével egy switchport, ami nem kapta meg a várt BPDU-t egy szomszéd switch-től, lezárt állapotba megy át. |
| Listening (Figyelő) | A blokkoló állapot után a port a figyelő állapotba kerül. The port fogadja a BPDU-kat a gyökérponti híd elérési útvonalának meghatározásához. A port emellett továbbítja saját BPDU-kereteit és tájékoztatja a szomszédos switch-eket arról, hogy a port az aktív topológiában való részvételre készül. |
| Learning (Tanuló) | A switchport a tanuló állapotba megy át a figyelő állapotból. A tanulási állapot során a switchport fogadja és feldolgozza a BPDU-kat és felkészül, hogy részt vegyen a keretek továbbításában. Ezen kívül elkezdi feltölteni a MAC-címtáblát. Viszont a tanuló állapotban a felhasználói kereteket még nem továbbítja a rendeltetési helyükre. |
| Forwarding (Továbbító) | A továbbítási állapotban a switchport a topológia aktív részének tekintendő. A port továbbítja a felhasználói forgalmat, illetve küldi és fogadja a BPDU-kereteket. |
| Letiltott | A letiltott állapotban lévő switchport nem vesz részt a feszítőfában és nem továbbít kereteket. A letiltott állapot akkor figyelhető meg, amikor a a port adminisztratív módon le van tiltva. |

5.2.10

## Az összes portállapot működési adatai

A táblázat összefoglalja az egyes portállapotok működési adatait.

| Port StateBPDUMAC Address TableForwarding Data FramesDisabledNone sent or receivedNo updateNoBlockingReceive onlyNo updateNoListeningReceive and sendNo updateNoLearningReceive and sendUpdating tableNoForwardingReceive and sendUpdating tableYes | | | |
| --- | --- | --- | --- |
| **Portállapot** | **BPDU** | **MAC-címtábla** | **Adatkeretek továbbítása** |
| Blocking | Csak fogadás | Nincs frissítés | Nem |
| Listening (Figyelő) | Fogadás és küldés | Nincs frissítés | Nem |
| Learning (Tanuló) | Fogadás és küldés | A címtáblázat frissítése | Nem |
| Forwarding (Továbbító) | Fogadás és küldés | A címtáblázat frissítése | Igen |
| Kikapcsolva | Nincs küldés vagy fogadás | Nincs frissítés | Nem |

5.2.11

## VLAN-onkénti feszítőfa-protokoll

Eddig az STP-t olyan környezetben tárgyaltuk, ahol csak egy VLAN van. Az STP azonban beállítható úgy, hogy több VLAN-nal rendelkező környezetben is működjön.

A VLAN-onkénti feszítőfa-protokoll (Per-VLAN Spanning Tree, PVST) esetében minden feszítőfában külön-külön választanak gyökérponti hidat. Ez lehetővé teszi, hogy különböző gyökérponti hidak legyenek különböző VLAN-okhoz. Az STP minden egyes VLAN esetében külön STP-példányt tart fenn. Ha minden switch minden portja a VLAN 1-be tartozik, akkor csak egyetlen feszítőfa létezik.

5.2.12

## Tudáspróba - Az STP működése

Az űrlap teteje

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

1. Alapértelmezés szerint (a kapcsolón lévő konfiguráció nélkül) mi határozza meg, hogy melyik kapcsoló a gyökérhíd?

Az űrlap alja

A gyökérhíd lesz a kapcsoló a következőkkel:

A legkevesebb összköltség (legjobb út) szempontjából a gyökérhídhoz legközelebbi port a következő:

A szegmens portja (két kapcsolóval), amelyiknek a legalacsonyabb az útköltsége a gyökérhídhoz, a következő:

Which of the following ports will forward Ethernet frames? (Két jó válasz van.)

A kapcsolótól a gyökérhídig tartó útvonalon az egyes portköltségek összege a következőképpen ismert:

Milyen gyakran küld egy kapcsoló BPDU-t?

[5.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP célja](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[5.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP fejlődése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. STP fogalmak
2. Az STP fejlődése

# Az STP fejlődése

5.3.1

## Az STP különböző változatai

Ez a témakör az STP több különböző verzióját és a hálózati hurkok megakadályozására szolgáló egyéb lehetőségeket ismerteti.

Mindeddig a feszítőfa-protokoll kifejezést és angol rövidítését, az STP-t használtuk, ami félrevezető lehet. A szakemberek ezt a rövidítést a feszítőfa különböző megvalósításainak megemlítésekor is 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 legújabb szabványát az IEEE-802-1D-2004 tartalmazza, az IEEE szabvány eredeti címe: Local and metropolitan area networks:Media Access Control (MAC) Bridges. A szabvány ezen verziója kimondja, hogy az ennek megfelelő switch-ek és bridge-ek a gyors feszítőfa-protokollt (Rapid Spanning Tree Protocol, RSTP) használják az eredeti 802.1d szabványban meghatározott régebbi STP protokoll helyett. 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, valamint az STP és az RSTP Cisco általi megvalósításaira fogunk koncentrálni.

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

| Táblázat felirata | |
| --- | --- |
| **STP típusa** | **Leírás** |
| STP | Ez az eredeti IEEE 802.1D verzió (802.1D-1998 és korábbi). Hurok nélküli topológiát biztosít egy redundáns kapcsolatokkal rendelkező hálózatban. Nevezik Common Spanning Tree-nek (CST) is, ez feltételezi, hogy egyetlen feszítőfapéldány létezik a teljes kapcsolt hálózatban, függetlenül a VLAN-ok számától. |
| PVST+ | A Per-VLAN Spanning Tree (PVST+) egy Cisco-féle továbbfejlesztése az STP-nek, ami egy külön 802.1D feeszítőfapéldányt biztosít minden VLAN számára, ami csak létezik a hálózatban. A PVST+ támogatja a PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, és loop guard elnevezésű kiegészítéseket. |
| RSTP | A gyors feszítőfa-protokoll (Rapid Spanning Tree Protocol, RSTP) vagy IEEE 802.1w egy továbbfejlesztése az STP-nek, ami gyorsabb konvergenciát biztosít, mint az STP. |
| 802.1D-2004 | Ez az STP-szabvány módosítása, amely tartalmazza az IEEE 802.1w szabványt. |
| Gyors PVST+ | Az RSTP Cisco általi, PVST+-t használó továbbfejlesztése, ami VLAN-onként biztosít egy külön 802.1w példányt. Minden egyes példány támogatja a PortFast, BPDU guard, BPDU filter, root guard, és loop guard kiegészítéseket. |
| MSTP | A Multiple Spanning Tree Protocol (MSTP) egy IEEE-szabvány, amit a korábbi, Cisco által szabadalmaztatott Multiple Instance STP (MISTP) megvalósítás ihletett. Az MSTP több VLAN-t ugyanabba a feszítőfapéldányba képez le. |
| MST | A Multiple Spanning Tree (MST) a Cisco-féle MSTP-megvalósítás, ami akár 16 RSTP-példányt is biztosít, és számos, ugyanolyan fizikai és logikai topológiával rendelkező VLAN-t képezhet le egy közös RSTP-példányba. Minden példány támogatja a PortFast, BPDU guard, BPDU filter, root guard és loop guard funkciókat. |

A switch-ek üzemeltetéséért felelős hálózati szakembernek kell döntenie a használni kívánt feszítőfa-protokoll változatáról.

A Cisco IOS 15.0 vagy újabb verzióját futtató switch-ek alapértelmezés szerint a PVST+ verziót futtatják. Ez a verzió tartalmazza az IEEE 802.1D-2004 számos specifikációját, például alternatív portokat említ a korábbi, nem kijelölt portok helyett. A switch-eket külön kell konfigurálni a gyors feszítőfa módhoz, ha azt szeretnénk használni.

5.3.2

## Az RSTP alapjai

Az RSTP (802.1w) felváltja az eredeti 802.1D-t, de visszafelé kompatibilis vele. A 802.1w STP terminológiája megegyezik az eredeti IEEE 802.1D STP-vel. A legtöbb paraméter változatlan maradt. Az eredeti STP-szabványt ismerő felhasználók egyszerűen konfigurálhatják az RSTP-t is. A portszerepkörök és a topológia meghatározásához az STP és az RSTP is ugyanazt az algoritmust használja.

Az RSTP felgyorsítja a feszítőfa újraszámítását a 2. rétegbeli topológia megváltozásakor. Sokkal gyorsabb konvergenciát lehet vele elérni egy megfelelően konfigurált hálózatban, néha mindössze néhány száz milliszekundumon belül. Ha egy portot alternatív portként konfiguráltak, akkor azonnal továbbító állapotba válthat anélkül, hogy megvárná a hálózat konvergálását.

**Note** : Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. A Rapid PVST+ esetében minden VLAN-ban független RSTP-példány fut.

5.3.3

## RSTP portállapotok és portszerepkörök

Az STP és az RSTP portállapotok és portszerepkörök hasonlóak.

Az STP és RSTP portállapotok és portszerepek összehasonlításához kattintsunk az egyes gombokra!

**STP és RSTP kikötőállamok**

As shown in the figure, there are only three port states in RSTP that correspond to the three possible operational states in STP. A 802.1D letiltott, lezárt és figyelő állapotok egy közös, 802.1w szerinti eldobó állapotban egyesültek.

Az ábra összehasonlítás céljából egymás mellett mutatja az STP és az RSTP portállapotokat. A bal oldalon az STP portállapotok fentről lefelé sorrendben vannak felsorolva: Letiltva, Blokkolás, Figyelés, Tanulás, Továbbítás. A jobb oldalon az RSTP portállapotok fentről lefelé sorrendben vannak felsorolva: Discarding, Learning, Forwarding.

Kikapcsolva Blocking Listening Learning Forwarding RSTP Discarding Learning Forwarding STP

5.3.4

## PortFast és BPDU Guard

Amikor egy eszköz switchporthoz van csatlakoztatva, vagy amikor egy switch bekapcsol, a port mind a figyelő, mind a tanuló állapotokon minden alkalommal keresztülmegy, megvárva, míg a továbbítási késleltetés időzítője le nem jár. Ez a késleltetés 15 másodperc minden állapotra, a figyelőre és tanulóra is, összesen tehát 30 másodperc. Ez problémát jelenthet a DHCP-szervert kereső DHCP-kliensek számára. A csatlakoztatott állomás DHCP-üzeneteit a rendszer nem továbbítja a továbbítási késleltetés 30 másodperce alatt, és előfordulhat, hogy a DHCP-folyamat időtúllépéssel leáll. Ennek eredményeként az IPv4-kliens nem kap érvényes IPv4-címet.

**Megjegyzés** : Bár ez előfordulhat az ICMPv6 Router Solicitation üzeneteket küldő klienseknél, az útválasztó továbbra is küld ICMPv6 Router Advertisement üzeneteket, így az eszköz tudni fogja, hogyan szerezheti be a címinformációit.

A PortFast beállítás a switchportot lezárt állapotból azonnal továbbító állapotba váltja, amellyel megkerüli a szokásos 802.1D STP-állapotátmeneteket (a figyelő és a tanuló állapotokat jelentő 30 másodperces késleltetést). A PortFast használható a hozzáférési portokon, hogy az ezekhez a portokhoz csatlakoztatott eszközök, például a DHCP-kliensek azonnal hozzáférhessenek a hálózathoz, ahelyett, hogy megvárnák az IEEE 802.1D STP konvergálását az egyes VLAN-okon. Mivel a PortFast célja, hogy a hozzáférési portoknak a lehető legkevesebbet kelljen a feszítőfa konvergálására várakozniuk, a beállítást csak ezeken a portokon szabad használni. Másik switch-hez csatlakozó porton használva feszítőfahurok létrejöttét kockáztatjuk. A PortFast csak a végberendezésekhez csatlakozó switchportokon használható!

A fizikai hálózati topológia három összekapcsolt kapcsolót (S1, S2 és S3), valamint három PC-t, PC1-et, PC2-t és PC3-at mutat. Az S1 az S3 kapcsoló F0/2 portjához csatlakozik, és az S2 F0/1 kapcsolóporthoz, amely mellett a D betű látható. Az S1 és S2 közötti összeköttetést Trunk 1-nek nevezik. Az S1 és S3 közötti kapcsolatot Trunk 3-nak nevezik. Az S1 a PC4-hez csatlakozik az F0/2 kapcsolóporton keresztül, amely mellett a D betű látható. S2 csatlakozik az S3 over kapcsoló F0/2 portjához, amely mellett a D betű van, és az S1 over switch porthoz, az F0/1 kapcsolóhoz, amely mellett az R betű van. Az S2 és S3 közötti kapcsolat a Trunk 2 felirattal van ellátva. Az S2 az F0/11 kapcsolóporton keresztül csatlakozik a PC1-hez, az F0/18 kapcsolóporton keresztül csatlakozik a PC2-hez, és az F0/6 kapcsolóporton keresztül csatlakozik a PC3-hoz. Az S3 csatlakozik az S2 kapcsoló F0/2 portjához, amely mellett A betű, és az S1 F0/1 kapcsolóporthoz, amely mellett az R betű látható. Egy piros X szimbólum van elhelyezve a fővonalon az S3 és S2 között. A PC1 IP-címe 172.17.10.21. A PC2 IP-címe 172.17.10.22. A PC3 IP-címe 172.17.10.23. Egy szövegdobozban a PortFast és a BPDU Guard felirat olvasható, és a nyilak az S2, F0/11, F0/18 és F0/6 három kapcsolóportjára mutatnak.

PC2 PC1 PC3 S3 S1 S2 F0/1 172.17.10.21 172.17.10.23 172.17.10.22 F0/2 F0/2 F0/1 F0/2 F0/1 F0/11 F0/6

F0/18

Trunk 3 Trunk 1 Trunk 2 PortFast és BPDU Guard D D D R R A

Szabályos PortFast beállítások esetén sosem érkezhetnek BPDU-k az erre konfigurált portokon, mert ez azt jelentené, hogy a portra másik bridge vagy switch csatlakozik. Ez potenciálisan egy feszítőfahurkot okozna. Az ilyen esetek elkerülése érdekében a Cisco switch-ek támogatják a BPDU guard nevű funkciót. Ha engedélyeztük, a BPDU guard azonnal hiba miatt letiltott állapotba helyezi a portot bármilyen BPDU érkezésekor. Ez védelmet nyújt a potenciális hurkok ellen a port leállításával. A BPDU guard biztonságos megoldás a hibás konfigurációk ellen, mert az interfészt csak manuálisan lehet újból üzembe helyezni.

5.3.5

## Az STP alternatívái

Az STP régen is egy Ethernet hurokmegelőzési protokoll volt, és máig az maradt. Az évek során a szervezetek nagyobb rugalmasságot és rendelkezésre állást igényeltek a LAN-okban. Az Ethernet LAN-ok az egyetlen routerhez csatlakoztatott, pár összekapcsolt switch-ből álló topológiákról áttértek egy kifinomult hierarchikus hálózati tervezési modellre, beleértve a hozzáférési, az elosztási és a magrétegbeli switch-eket, ahogy az ábrán is látható.

Két fizikai hálózati topológia, amelyek hierarchikus hálózattervet és összeomlott magtervezést mutatnak

**Összecsukott Core** Internet Internet Internet Internet **Core Layer Elosztási réteg hozzáférési réteg**

A megvalósítástól függően a 2. réteg nemcsak a hozzáférési réteget, hanem az elosztási vagy akár a magréteget is magában foglalhatja. Ezek a kialakítások több száz switch-et tartalmazhatnak, több száz vagy akár több ezer VLAN-nal. Az STP alkalmazkodott a hozzáadott redundancia- és komplexitásbeli fejlesztésekhez, az RSTP és MSTP részeként.

A hálózattervezés fontos szempontja a gyors és kiszámítható konvergencia, ha a topológiában hiba vagy változás következik be. Az STP nem kínálja ugyanazt a hatékonyságot és kiszámíthatóságot, amelyet a 3. rétegben az irányító protokollok nyújtanak. Az ábra egy hagyományos hierarchikus hálózati tervet mutat be az elosztási és a magréteg 3. rétegbeli switch-eivel, amelyek forgalomirányítást is végeznek.

A fizikai hálózati topológia négy 3. rétegbeli kapcsolót, három 2. rétegbeli kapcsolót és hat PC-t tartalmaz. Két Layer 3 kapcsoló a topológia tetején található a magban. Két 3. rétegbeli kapcsoló található az elosztási rétegben. A három Layer 2 kapcsoló és a hat PC az Access rétegben található.

Core Distribution Access Layer 3 Routing Layer 2 Switching

A 3. rétegbeli forgalomirányítás a portok blokkolása nélkül teszi lehetővé, hogy a topológiában redundáns útvonalak és hurkok legyenek. Emiatt egyes környezetekben mindenhol áttérnek a 3. rétegre, kivéve, ahol az eszközök a hozzáférési réteg switch-éhez csatlakoznak. Más szóval, a hozzáférési rétegbeli és az elosztási rétegbeli switch-ek közötti kapcsolatok 2. rétegbeliek helyett 3. rétegbeliek lehetnek, ahogy azt a következő ábra mutatja.

A fizikai hálózati topológia hét Layer 3 switchet és hat PC-t mutat. Két Layer 3 kapcsoló a topológia tetején található a magban. Két 3. rétegbeli kapcsoló található az elosztási rétegben. Három 3. rétegbeli kapcsoló köti össze az elosztási és hozzáférési réteget. A hat PC teljes mértékben az Access rétegben van.

Core Distribution Access Layer 3 Routing Layer 2 Switching

Bár az STP valószínűleg továbbra is hurokmegelőzési mechanizmusként fog működni a vállalatoknál, a hozzáférési rétegbeli switch-eken más technológiákat is alkalmaznak, beleértve a következőket:

* Multi System Link Aggregation (MLAG)
* Legrövidebb út híd (SPB)
* Sok link átlátszó összekapcsolása (TRILL)

**Megjegyzés** : Ezek a technológiák túlmutatnak a tanfolyamon.

5.3.6

## Tudsápróba - Az STP evolúciója

Az űrlap teteje

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

1. Which three STP port states are merged into the RSTP discarding port state? (Három jó válasz van.)

Az űrlap alja

Melyik protokollt tervezték az STP gyorsabb konvergenciájához?

Melyik technológia oldja meg azt a problémát, hogy egy eszköz nem tud IPv4-címet kapni a DHCP-kiszolgálótól az STP továbbítási késleltetési időzítők miatt?

[5.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[5.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. STP fogalmak
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

5.4.1

## Miről tanultunk ebben a fejezetben?

**Purpose of STP**

A kapcsolt Ethernet hálózatban a redundáns útvonalak egyaránt vezethetnek fizikai és logikai (2. rétegbeli) hurkok keletkezéséhez. A 2. rétegbeli hurok a MAC-címtábla instabilitását, a kapcsolatok telítődését, valamint a switch-ek és a végberendezések nagy CPU-kihasználtságát eredményezheti, amelytől a hálózat használhatatlanná válik. A 3. rétegbeli IPv4 és az IPv6 protokollokkal ellentétben a 2. rétegbeli Ethernet nem tartalmaz olyan mechanizmust, amely lehetővé tenné a végtelen hurokba került keretek felismerését és eltávolítását. Az Ethernet LAN-ok hurok nélküli topológiát igényelnek, amelyben csak egyetlen útvonal van bármely két eszköz között. Az STP egy hurokmegelőzési hálózati protokoll, amely lehetővé teszi a redundanciát egy hurokmentes 2. rétegbeli topológia létrehozásakor. Az STP engedélyezése nélkül 2. rétegbeli hurkok keletkezhetnek, így a szórásos, a csoportos és az ismeretlen célú egyedi címzésű keretek a végtelenségig bolyonghatnak a hálózaton, amitől egy hálózat le is állhat. A szórási vihar abnormálisan nagy számú szórásos üzenet, amely egy adott idő alatt túlterheli a hálózatot. A szórási vihar másodpercek alatt leterhelheti a hálózatot alkotó switch-eket és végberendezéseket. Az STP egy Radia Perlman által feltalált algoritmuson alapul. A feszítőfa algoritmusa (Spanning Tree Algorithm, STA) hurokmentes topológiát hoz létre egy gyökérponti híd (root bridge) kiválasztásával, ami felé az összes többi switch egyetlen, legalacsonyabb költségű útvonalat határoz meg.

**STP Operations**

Az STP hurok nélküli topológiát épít egy négylépcsős folyamat során: kiválasztja a gyökérponti hidat, kiválasztja a gyökérportokat, kiválasztja a kijelölt portokat, végül pedig az alternatív (lezárt) portokat. Az STA és STP funkciók során a switchek a BPDU-nak nevezett üzenetek (keretek) használatával osztják meg a magukról és kapcsolataikról szóló információkat. A BPDU-k a gyökérponti híd, a gyökérportok, a kijelölt portok és az alternatív portok kiválasztására szolgálnak. Minden BPDU tartalmazza a küldő switch hídazonosítóját (BID). A BID számos STA-döntés meghozatalában vesz részt, beleértve a gyökérponti híd és a portszerepek kiválasztását. A BID egy prioritás értékből, a küldő switch MAC-címéből és egy kiterjesztett rendszer-azonosítóból (extended system ID) áll. A három mező egyesített értékét használják, így határozzák meg a legalacsonyabb értékű hídazonosítót. A legalacsonyabb BID-értékű switch lesz a gyökérponti híd. Mivel az alapértelmezett BID 32768, lehetséges, hogy két vagy több switch azonos prioritással rendelkezik. Abban az esetben, ha minden switch prioritása azonos, a legalacsonyabb MAC-című lesz a gyökérponti híd. Amint egy feszítőfapéldány kiválasztotta a gyökérponti hídját, az STA megkezdi a szórási tartomány minden eszközétől a gyökérponti híd felé vezető legjobb útvonalak meghatározását. Az elérési útvonalat, amelyet belső gyökérelérési útvonalnak nevezünk, a switch-től a gyökérponti hídig vezető útvonal mentén felmerülő összes egyedi portköltség összege határozza meg. A gyökérponti híd meghatározása után az STA-algoritmust használják a gyökérport kiválasztására. A gyökérport a gyökérponti hídhoz legközelebb eső port, a hozzá vezető teljes költség (legjobb útvonal) szempontjából. Miután minden switch kiválasztja a gyökérportot, kiválasztják a kijelölt portokat is. A kijelölt port a szegmens (amit két switch alkot) egy portja, amelynek a gyökérponti hídhoz vezető gyökérelérési útvonalköltsége a legkisebb. Ha egy port nem gyökérport vagy kijelölt port, akkor alternatív (vagy tartalék) porttá válik. Az alternatív és a tartalék portok a hurkok megelőzése céljából lezárt állapotban vannak. Ha egy switch több egyenlő költségű elérési utat is ismer a gyökérponti hídhoz, akkor a következő feltételek alapján határozza meg a portot: a küldő legalacsonyabb BID-je, majd a küldő legalacsonyabb portprioritása, végül a küldő legalacsonyabb portazonosítója. Az STP konvergenciájához három időzítő szükséges: a hello időzítő, a továbbítási késleltés időzítője és a maximális életkor időzítő. A portállapotok: lezárt, figyelő, tanuló, továbbító és letiltott. A PVST esetében minden feszítőfában külön-külön választanak gyökérponti hidat. Ez lehetővé teszi, hogy különböző gyökérponti hidak legyenek különböző VLAN-okhoz.

**Az STP evolúciója.**

Az STP kifejezés és rövidítés használata bizonyos esetekben félrevezető lehet. Az STP-t gyakran használják az feszítőfa különböző implementációira is, mint például az RSTP és az MSTP. Az RSTP az STP továbbfejlesztése, ami gyorsabb konvergenciát biztosít, mint az STP. Az RSTP portállapotok: eldobó, tanuló és továbbító. A PVST+ az STP Cisco-féle továbbfejlesztése, amely külön feszítőfapéldányt biztosít a hálózatban konfigurált minden VLAN számára. A PVST+ támogatja a PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard és loop guard kiegészítéseket. A Cisco IOS 15.0 vagy újabb verzióját futtató switch-ek alapértelmezés szerint a PVST+ verziót futtatják. A Rapid PVST+ az RSTP Cisco általi továbbfejlesztése, amely a PVST+-t használja, és minden VLAN-hoz külön 802.1w példányt biztosít. A PortFast beállítás a switchportot lezárt állapotból azonnal továbbító állapotba váltja, amellyel megkerüli az STP figyelő és a tanuló állapotokat jelentő 30 másodperces késleltetést. A PortFast használható a hozzáférési portokon, hogy az ezekhez a portokhoz csatlakoztatott eszközök, például a DHCP-kliensek azonnal hozzáférhessenek a hálózathoz, ahelyett, hogy megvárnák az STP konvergálását az egyes VLAN-okon. A Cisco switch-ek támogatják a BPDU guard nevű funkciót, amely azonnal hiba miatt letiltott állapotba helyezi a switchportot bármely BPDU beérkezése után, hogy megvédje azt a potenciális hurkok ellen. Az Ethernet LAN-ok az egyetlen routerhez csatlakoztatott, pár összekapcsolt switch-ből álló topológiákról áttértek egy kifinomult hierarchikus hálózati tervezési modellre. A megvalósítástól függően a 2. réteg nemcsak a hozzáférési réteget, hanem az elosztási vagy akár a magréteget is magában foglalhatja. Ezek a kialakítások több száz switch-et tartalmazhatnak, több száz vagy akár több ezer VLAN-nal. Az STP alkalmazkodott a hozzáadott redundancia- és komplexitásbeli fejlesztésekhez, az RSTP és MSTP részeként. A 3. rétegbeli forgalomirányítás a portok blokkolása nélkül teszi lehetővé, hogy a topológiában redundáns útvonalak és hurkok legyenek. Emiatt egyes környezetekben mindenhol áttérnek a 3. rétegre, kivéve, ahol az eszközök a hozzáférési réteg switch-éhez csatlakoznak.

5.4.2

## Ellenőrző kvíz - STP

Az űrlap teteje

1. Melyik portállapot váltja át a portokat azonnal a PortFast beállításakor?

Az űrlap alja

A gyökérponti híd megválasztása után a switch-ek miként határozzák meg a gyökérponti híd felé vezető legjobb útvonalat?

Melyik az alapértelmezett STP-mód a Cisco Catalyst kapcsolókon?

Melyik érték határozza meg a gyökérponti hidat, ha az összes switch trönkvonalon csatlakozik egymáshoz, alapértelmezett STP-beállításokkal?

A feszítőfa-protokoll futása közben a hálózati rendszergazda minden switch-et újraindított. Mi a feszítőfa választási folyamatának első lépése?

Melyik két fogalom köthető ahhoz a kapcsolóporthoz, amelyhez csak végberendezések kapcsolódnak és amely soha nem csatlakozik másik kapcsolóhoz? (Két jó válasz van.)

Melyik portállapotot használja a Rapid PVSTP+? (Három jó válasz van.)

Egy PVST-t futtató kapcsolt hálózatban melyik portállapotra igaz, hogy a fogadott BPDU-k alapján BPDU-kereteket továbbít, de nem továbbít adatkeretet?

Melyik STP-portszerepet veszi fel a switchport, ha nincs nála alacsonyabb költségű port a gyökérponti híd felé?

Melyik két állítás jellemzi a PortFast üzemmódú switchportot? (Két jó válasz van.)

Hogyan javítható ki egy feszítőfa hiba?

Milyen kiegészítő információ található a BPDU 12 bites kiterjesztett rendszerazonosítójában (extended system ID)?

A rendszergazda egy switch-et vizsgál, és szeretné ellenőrizni, hogy a switch-e a gyökérponti híd. Melyik paranccsal tudja ezt megtenni?

Melyik a redundancia definíciója?

[5.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az STP fejlődése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[6.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. EtherChannel
2. Bevezetés

# Bevezetés

6.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az EtherChannel-ről szóló fejezetben.

A hálózatunk redundáns switch-eket és kapcsolatokat tartalmaz. Az STP valamelyik verzióját úgy állítottuk be, hogy megakadályozza a 2. rétegbeli hurkot. De most, mint a legtöbb hálózati rendszergazda, rájövünk, hogy több sávszélességet és redundanciát használhatnánk a hálózatban. Nem kell aggódni, az EtherChannel segít! Az EtherChannel egyesíti az eszközök közötti kapcsolatokat úgynevezett kötegekbe (bundle). Ezek a kötegek redundáns linkeket tartalmaznak. Az STP blokkolhatja az egyik ilyen köteget, de nem fogja mindet. Az EtherChannel segítségével a hálózat redundanciával, hurokmegelőzéssel és nagyobb sávszélességgel rendelkezhet!

Két protokollról kell szót ejteni: a PAgP-ről és az LACP-ről. Ez a fejezet mindkettőt elmagyarázza, és azt is megmutatja, hogyan konfigurálhatjuk, ellenőrizhetjük és háríthatjuk el a hibáikat! Egy parancsszimulátor és két Packet Tracer feladat segít a protokollok jobb megértésében. Gyerünk, fogjunk bele!

6.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: EtherChannel

**Module Objective**: Troubleshoot EtherChannel on switched links.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **EtherChannel Operation** | Describe EtherChannel technology. |
| **Az EtherChannel konfigurálása** | Configure EtherChannel. |
| **Az EtherChannel ellenőrzése és hibajavítása** | Troubleshoot EtherChannel. |

[5.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[6.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[EtherChannel Operation](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. EtherChannel
2. EtherChannel Operation

# EtherChannel Operation

6.1.1

## Portok összefogása (Link Aggregation)

Vannak olyan helyzetek, amelyekben több sávszélességre vagy redundanciára van szükség az eszközök között, mint amit egyetlen kapcsolat biztosíthat. Több kapcsolat is használható az eszközök között a sávszélesség növelése érdekében. Viszont a Spanning Tree Protocol (STP), amely alapértelmezés szerint engedélyezve van a 2. rétegbeli eszközökön (pl.: a Cisco switch-eken), blokkolja a redundáns kapcsolatokat, hogy megakadályozza a kapcsolási hurkok kialakulását, ahogy az ábrán is látható.

Olyan technológiára van tehát szükség, amely lehetővé teszi az STP által nem blokkolt eszközök közötti redundáns kapcsolatot. Ezt a technológiát EtherChannel néven emlegetik.

Az EtherChannel egy kapcsolatokat összefogó (aggregáló) technológia, amely több fizikai Ethernet kapcsolatot egyetlen logikai kapcsolatba fog össze. Hibatűrést, terhelésmegosztást, nagyobb sávszélességet és redundanciát biztosít a switch-ek, routerek és szerverek között.

Az EtherChannel segítségével lehetőség van a switch-ek közötti fizikai összeköttetések többszörözésére a köztük lévő sebesség növelése érdekében.

két többrétegű kapcsoló, amelyek egy-egy LAN-kapcsolóhoz csatlakoznak két fizikai hálózati kapcsolaton keresztül; a két kapcsolat egyike az STP által blokkoltként jelenik meg

Zárolt

Alapértelmezés szerint az STP blokkolja a redundáns kapcsolatokat.

6.1.2

## EtherChannel

Az EtherChannel technológiát a Cisco fejlesztette ki, amely a LAN-kapcsolók közötti FastEthernet vagy Gigabit Ethernet portok egyetlen logikai csatornába való rendezésére szolgál. Az EtherChannel konfigurálása után létrejövő virtuális interfészt portcsatornának (port channel) nevezzük. A fizikai interfészek kötegelve egy portcsatorna-interfészt alkotnak, ahogy az ábrán is látható.

két többrétegű kapcsoló, amelyek egy-egy LAN-kapcsolóhoz csatlakoznak két fizikai hálózati kapcsolaton keresztül; mindkét kapcsolat egy EtherChannel-be lett egyesítve

EtherChannel EtherChannel

6.1.3

## Az EtherChannel előnyei

Az EtherChannel technológia számos előnnyel rendelkezik:

* A legtöbb konfigurációs feladat elvégezhető az EtherChannel (portcsatorna) interfészen, így nincs szükség a portok egyedi kezelésére, ezzel biztosítható azok következetes beállítása.
* Az EtherChannel a meglévő switchportokat 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. These methods include source MAC and destination MAC load balancing, or source IP and destination IP load balancing, across the physical links.
* Az EtherChannel-be rendezett portcsoport egyetlen logikai kapcsolatként működik. Ha két switch között több EtherChannel köteg 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 hozzá tartozó portot. 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 köteg egy logikai kapcsolatot alkot. Továbbá a csatorna valamely fizikai portjának kiesése nem okoz változást a topológiában. Ezért nem szükséges az STP újraszámítása. Amíg legalább egy fizikai port jelen van, addig az EtherChannel is működőképes marad, de a kiesett portok miatt a teljes átbocsátóképesség lecsökken.

6.1.4

## A megvalósítás korlátai

Az EtherChannel megvalósítása bizonyos korlátozásokkal bír, beleértve a következőket:

* Az interfésztípusok nem keverhetők össze. Például FastEthernet és Gigabit Ethernet típusok nem kerülhetnek vegyesen egy EtherChannel-be.
* Minden csatorna legfeljebb nyolc, azonosan konfigurált Ethernet portból állhat. Az EtherChannel legfeljebb 800 Mb/s (Fast EtherChannel) vagy 8 Gb/s (Gigabit EtherChannel) teljes duplex sávszélességet biztosít switch-switch vagy switch-szerver viszonylatban.
* Jelenleg egy Cisco IOS-t futtató 2960-as switch-en egyidejűleg hat EtherChannel létezhet. Azonban új IOS-verziók megjelenésével néhány eszközön és bővítőkártyán nagyobb portszámú EtherChannel kapcsolat is konfigurálható, illetve a csatornák száma is több lehet.
* A csatorna egyedi portjainak konfigurációja mindkét eszközön azonos kell, hogy legyen. Ha az egyik oldalon a fizikai portok trönkmódban vannak, akkor a másik oldal portjainak is trönkmódban kell lenniük, azonos natív VLAN-nal. Továbbá, az EtherChannel kapcsolat összes portját kötelezően 2. rétegbeli portnak kell beállítani.
* Minden EtherChannel-höz tartozik egy logikai portcsatorna-interfész, ahogy az ábrán is látható. A portcsatorna-interfészen elvégzett beállítások minden olyan fizikai portra érvényesek, ami tagja a csatornának.

Az ábra egy 2960-as kapcsoló elölnézetét mutatja, amely több fizikai 10/100/1000-es port csatornacsoport-összerendelését mutatja logikai portcsatorna-interfészekhez. Az egyik logikai portcsatorna interfész az 1–6. fizikai portokat, a másik pedig a 9–12. portokat köti össze.

Catalyst 2960 SERIES MODE SYS T S T R T U T I L D U P L X S P E E D RPS 1 2 3 4 5 6 7 8 9 10 1 1

12

Logikai port   
Csatorna interfész logikai port   
Csatorna interfész Csatornacsoport   
Binding 10/100/1000 portok Fizikai portok

6.1.5

## Automatikus egyeztető protokollok

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

**Megjegyzés** : Statikus vagy feltétel nélküli EtherChannel konfigurálása PAgP vagy LACP nélkül is lehetséges.

6.1.6

## A PagP működése

A PAgP a Cisco saját fejlesztésű protokollja, amely segít az EtherChannel kapcsolatok automatikus létrehozásában. 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 a csatorna felügyeletét is elvégzi. A PAgP-csomagok 30 másodpercenként kerülnek elküldésre. A protokoll ezekkel ellenőrzi a konfiguráció egyezőségét, valamint felügyeli a kapcsolatok hozzáadását és hibáit a switch-ek között. Biztosítja azt is, hogy az EtherChannel létrehozása során a résztvevő portok beállításai azonosak legyenek.

**Megjegyzés** : Az EtherChannelben kötelező, hogy minden portnak azonos sebességgel, duplex beállítással és VLAN-információkkal rendelkezzen. A csatorna létrehozása utáni minden port-csatorna módosítás az összesített csatornaportokat is megváltoztatja.

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. A PagP üzemmódjai az alábbiak:

* **On** - This mode forces the interface to channel without PAgP. Az ilyen módra konfigurált interfészek nem cserélnek PAgP-csomagokat egymással.
* **PAgP kívánatos** – Ez a PAgP mód egy interfészt aktív tárgyalási állapotba helyez, amelyben az interfész PAgP-csomagok küldésével tárgyalásokat kezdeményez más interfészekkel.
* **PAgP auto** - Ez a PAgP mód egy interfészt passzív egyeztető állapotba helyez, amelyben az interfész válaszol a kapott PAgP csomagokra, de nem kezdeményez PAgP egyeztetést.

A két oldalon beállított módoknak kompatibilisnek kell lenniük egymással. Ha az egyik oldal auto módban van, az passzív állapotot jelent, vagyis 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 minden üzemmódot letiltunk a **no** paranccsal, vagy nem állítunk be semmilyen módot sem, akkor az EtherChannel le lesz tiltva.

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 lévő interfész nem képes az egyeztetésre.

A két switch közötti egyeztetés hiánya azt jelenti, hogy nem ellenőrizzük, hogy az EtherChannel összes linkje a másik oldalon megfelelően van-e végződtetve, vagy hogy PagP kompatibilis-e a másik switch.

6.1.7

## Példa a PagP-módok beállításaira

Tekintsük az ábrán látható két switch-et. Az, hogy az S1 és az S2 létrehoznak-e EtherChannel-t PagP használatával, a csatorna két oldalán található módbeállításoktól függ.

két LAN-kapcsoló, amelyek két fizikai hálózati kapcsolaton keresztül kapcsolódnak egymáshoz, amelyek PAgP használatával EtherChannel-t alkottak

S1

S2

PagP

A táblázat bemutatja az S1 és S2 switch-eken beállítható PagP-módok különböző kombinációit, valamint a csatorna létrehozásának eredményét.

### PAgP-módok

| S1S2 Channel Establishment On On YesOn Desirable/AutoNo Desirable Desirable Yes DesirableAutomatikus igen AutoKívánatos Igen AutoAuto.Nem | | |
| --- | --- | --- |
| **S1** | **S2** | **Csatorna létrehozása** |
| Tovább | Tovább | Igen |
| Tovább | Kívánatos/Automatikus | Nem |
| Kívánatos | Kívánatos | Igen |
| Kívánatos | Auto | Igen |
| Auto | Kívánatos | Igen |
| Auto | Auto | Nem |

6.1.8

## Az LACP működése

Az LACP az IEEE 802.3ad szabvány része, amely lehetővé teszi fizikai portok összefogását egyetlen logikai csatornába. A protokoll LACP-csomagokkal egyeztet a switch-ek 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-ök kialakítását. Cisco eszközökön mindkét protokoll támogatott.

**Note** : LACP was originally defined as IEEE 802.3ad. Jelenleg viszont az újabb, helyi és városi hálózatokat leíró IEEE 802.1AX szabványban dokumentálták.

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 LACP üzemmódjai a következők:

* **On** - This mode forces the interface to channel without LACP. Az ilyen módra konfigurált interfészek nem cserélnek LACP-csomagokat egymással.
* **LACP active** - This LACP mode places a port in an active negotiating state. amely így LACP-csomagokat küld kezdeti egyeztetés céljából más interfészeknek.
* **LACP passive** - This LACP mode places a port in a passive negotiating state. 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.

Az LACP nyolc aktív és nyolc készenléti kapcsolatot tesz lehetővé. A készenléti kapcsolat aktívvá válik, ha az egyik jelenlegi aktív kapcsolat meghibásodik.

6.1.9

## Példa az LACP-módok beállításaira

Tekintsük az ábrán látható két switch-et. Az, hogy az S1 és az S2 között létrejön-e EtherChannel az LACP használatával, függ a mód beállításaitól a csatorna mindkét oldalán.

két LAN-kapcsoló, amelyek két fizikai hálózati kapcsolaton keresztül kapcsolódnak egymáshoz, amelyek LACP használatával EtherChannel-t alkottak

S1

S2

LACP

A táblázat bemutatja az S1 és S2 switch-eken beállítható LACP-módok különböző kombinációit, valamint a csatorna létrehozásának eredményét.

| S1S2Channel Establishment On On Igen Aktív/PasszívNemAktívAktívIgenAktívPasszívIgenPasszívAktívIgenPasszívPasszívNem | | |
| --- | --- | --- |
| **S1** | **S2** | **Csatorna létrehozása** |
| Tovább | Tovább | Igen |
| Tovább | Aktív Passzív | Nem |
| Aktív | Aktív | Igen |
| Aktív | Passzív | Igen |
| Passzív | Aktív | Igen |
| Passzív | Passzív | Nem |

6.1.10

## Tudáspróba - Az EtherChannel működése

Az űrlap teteje

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

1. Melyek az EtherChannel technológia előnyei? (Válassza ki az összes megfelelőt.)

Az űrlap alja

Igaz vagy hamis? A FastEthernet és a GigabitEthernet hivatkozások egyetlen EtherChannel-ba kombinálhatók.

Igaz vagy hamis? A PAgP és a LACP egyaránt Cisco által védett kapcsolat-összesítési protokoll.

Which three are PAgP interface modes? (Három jó válasz van.)

Melyik PAgP interfész mód kezdeményezi az egyeztetést más interfészekkel?

A PAgP módok mely kombinációi alkotnak EtherChannel-t? (Válassza ki az összes megfelelőt.)

[6.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[6.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az EtherChannel konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. EtherChannel
2. Az EtherChannel konfigurálása

# Az EtherChannel konfigurálása

6.2.1

## Konfigurálási útmutató

Most, hogy már tudjuk, mi az EtherChannel, ez a témakör bemutatja, hogyan is kell konfigurálni. Az alábbi irányelvek és korlátozások hasznosak lehetnek az EtherChannel beállításakor:

* **EtherChannel támogatás** – Minden Ethernet interfésznek támogatnia kell az EtherChannel-t anélkül, hogy az interfészeknek fizikailag szomszédosnak kell lenniük.
* **Sebesség és duplex** – Konfigurálja az EtherChannel összes interfészét, hogy azonos sebességgel és ugyanabban a duplex módban működjenek.
* **VLAN egyezés** – Az EtherChannel kötegben lévő összes interfészt ugyanahhoz a VLAN-hoz kell hozzárendelni, vagy fővonalként kell beállítani (az ábrán látható). VLAN-ok automatikus kívánatos üzemmódja.\* \* **\* - Az EtherChannel a VLAN-ok ugyanazt a megengedett tartományát támogatja a trönkölő EtherChannel összes interfészén. Ha a VLAN-ok megengedett tartománya nem azonos, az interfészek nem alkotnak EtherChannel-t, még akkor sem, ha \*\*** vagy \*\*\*\* értékre vannak állítva.

Az ábrán egy olyan konfiguráció látható, amely lehetővé teszi, hogy egy EtherChannel jöjjön létre az S1 és az S2 között.

Az ábra két LAN-kapcsolót mutat, amelyek két fizikai hálózati kapcsolaton keresztül kapcsolódnak egymáshoz, amelyek portkonfigurációjuk alapján EtherChannel-t alkottak. Mind az S1, mind az S2 port konfigurációk; sebesség 1 Gbps, duplex full és VLAN 10.

|  |  |
| --- | --- |
| Az S1 portbeállításai | |
| Sebesség | 1 Gbps |
| Duplexitás | Teljes |
| VLAN | 10 |

|  |  |
| --- | --- |
| Az S2 portbeállításai | |
| Sebesség | 1 Gbps |
| Duplexitás | Teljes |
| VLAN | 10 |

Az EtherChannel létrejött.

Az EtherChannel akkor jön létre, ha a konfigurációs beállítások megegyeznek mindkét switch-en.

A következő ábrán az S1 portjai fél duplex módban vannak. Ezért az EtherChannel nem jön létre az S1 és az S2 között.

A diagram két olyan LAN-kapcsolót mutat, amelyek két fizikai hálózati kapcsolaton keresztül kapcsolódnak egymáshoz, amelyek portkonfigurációjuk alapján nem alkottak EtherChannel-t. Az S1 port konfigurációk; sebesség 1 Gbps, duplex fél és VLAN 10. Az S2 port konfigurációk a következők; sebesség 1 Gbps, duplex full és VLAN 10.

|  |  |
| --- | --- |
| Az S1 portbeállításai | |
| Sebesség | 1 Gbps |
| Duplexitás | Fél |
| VLAN | 20 |

|  |  |
| --- | --- |
| Az S2 portbeállításai | |
| Sebesség | 1 Gbps |
| Duplexitás | Teljes |
| VLAN | 20 |

Az EtherChannel nem jön létre.

Az EtherChannel nem jön létre, ha a konfigurációs beállítások eltérőek az egyes switch-eken.

A fenti beállítások megváltoztatását portcsatorna-interfész konfigurációs módjában lehet elvégezni. A portcsatorna-interfészen végrehajtott bármely módosítás az összes egyedi fizikai interfészen is érvényesítésre kerül. Ugyanakkor az egyedi interfészeken végzett módosítások nem érvényesülnek a portcsatorna-interfészen. Ezért az EtherChannel kapcsolathoz tartozó egyedi portokon végrehajtott konfigurációs módosítások kompatibilitási problémákat is okozhatnak.

A portcsatorna hozzáférési módban, trönkmódban (leggyakoribb) vagy irányított porton is konfigurálható.

6.2.2

## LACP konfigurációs példa

Az EtherChannel alapértelmezés szerint nincs engedélyezve, ezért be kell állítani. Az ábrán látható topológia egy EtherChannel konfigurációs példát mutat be LACP használatával.

két kapcsoló, az S1 és az S2, két fizikai hálózati kapcsolaton keresztül van összekötve, amelyek EtherChannel-t alkottak; Az S1 F0/1 portja az S2 F0/1 portjához csatlakozik; Az S1 F0/2 portja az S2 F0/2 portjához csatlakozik

S2 S1 Fa0/1 Fa0/1 Fa0/2

Fa0/2

Az EtherChannel LACP-vel történő konfigurálása a következő három lépésből áll:

**Step 1.** Specify the interfaces that compose the EtherChannel group using the **interface range** interface global configuration mode command. A **range** kulcsszó lehetővé teszi, hogy több interfészt tudjunk egyszerre konfigurálni.

**Step 2.** Create the port channel interface with the **channel-group** identifier **mode active** command in interface range configuration mode. Az azonosító a csatorna sorszámát határozza meg. A **mode active** kulcsszavak azt mutatják, hogy ez egy LACP EtherChannel beállítás.

**Step 3.** To change Layer 2 settings on the port channel interface, enter port channel interface configuration mode using the **interface port-channel** command, followed by the interface identifier. A példában az S1-en egy LACP EtherChannel van beállítva. A portcsatornát trönk interfészként konfiguráltuk az engedélyezett VLAN-ok megadásával.

S1(config)# **interface range FastEthernet 0/1 - 2**

S1(config-if-range)# **channel-group 1 mode active**

Creating a port-channel interface Port-channel 1

S1(config-if-range)# **exit**

S1(config)# **interface port-channel 1**

S1(config-if)# **switchport mode trunk**

S1(config-if)# **switchport trunk allowed vlan 1,2,20**

6.2.3

## Parancsszimulátor - Az EtherChannel konfigurálása

Konfiguráljuk az EtherChannel-t az S2-n a megadott követelmények alapján!

két kapcsoló, az S1 és az S2, két fizikai hálózati kapcsolaton keresztül van összekötve, amelyek EtherChannel-t alkottak; Az S1 F0/1 portja az S2 F0/1 portjához csatlakozik; Az S1 F0/2 portja az S2 F0/2 portjához csatlakozik

S2 S1 Fa0/1 Fa0/1 Fa0/2

Fa0/2

Lépjen be a FastEthernet0/1 és FastEthernet0/2 interfész tartomány üzemmódjába. Használja **a fa 0/1 - 2-t** interfész jelölésként.

Az űrlap teteje

S1(config)#

Az űrlap alja

6.2.4

## Packet Tracer - Az EtherChannel konfigurálása

Három olyan switch-et helyeztek mostanában üzembe, 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 akár nyolc redundáns kapcsolatot is tartalmazhat. A feladat során 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.

[EtherChannel konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/6.2.4-packet-tracer---configure-etherchannel_hu-HU.pka)

[6.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[EtherChannel Operation](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[6.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az EtherChannel ellenőrzése és hibajavítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. EtherChannel
2. Az EtherChannel ellenőrzése és hibajavítása

# Az EtherChannel ellenőrzése és hibajavítása

6.3.1

## Az EtherChannel ellenőrzése

Mint mindig, amikor konfiguráljuk az eszközöket a hálózatban, ellenőrizni kell a beállításokat. Ha problémák merülnek fel, akkor is képesnek kell lennünk a hibák elhárítására és javítására. Ez a témakör az ellenőrzéshez használható parancsokat, valamint néhány gyakori EtherChannel hálózati problémát és azok megoldásait mutatja be.

Az ellenőrző parancsok példáiban az ábrán látható topológiát fogjuk használni.

két kapcsoló, az S1 és az S2, két fizikai hálózati kapcsolaton keresztül van összekötve, amelyek EtherChannel-t alkottak; Az S1 F0/1 portja az S2 F0/1 portjához csatlakozik; Az S1 F0/2 portja az S2 F0/2 portjához csatlakozik

S2 S1 Fa0/1 Fa0/2 Fa0/2

Fa0/1

Számos parancs létezik az EtherChannel konfigurációjának ellenőrzésére. A magyarázatok és parancskimenetek megtekintéséhez kattintsunk az egyes gombokra!

The **show interfaces port-channel** command displays the general status of the port channel interface. Az ábrán a Port-channel1 interfész működő (up) állapotban van.

S1# interfészek megjelenítése port-channel 1 Az 1-es port-csatorna fent van, a vonali protokoll fel van kapcsolva (csatlakozva) A hardver EtherChannel, a cím c07b.bcc4.a981 (bia c07b.bcc4.a981) MTU 1500 bájt, BW 200000 Kbit/sec, DLY 100 usec, megbízhatóság 255/255, txload 1/255, rxload 1/255 (kimenet kimaradt)

6.3.2

## Gyakori problémák az EtherChannel konfigurációjával

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. Ezeknek a beállításoknak a megadása jelentősen csökkenti az EtherChannel-lel kapcsolatos hálózati problémákat. Az EtherChannel gyakori problémái a következők:

* Az EtherChannel-hez hozzárendelt portok nem ugyanannak a VLAN-nak a tagjai vagy nincsenek trönkként konfigurálva. Az eltérő natív VLAN-hoz tartozó portok nem alkothatnak EtherChannel-t.
* A trönközést az EtherChannel-t alkotó egyes portokon konfigurálták, de nem mindegyiken. Nem ajánlott beállítani a trönkmódot az EtherChannel-t alkotó egyedi portokon. Amikor egy trönköt konfigurálunk az EtherChannel-ön, ellenőrizzük a csatornán beállított trönkmódot. Ha az engedélyezett VLAN-ok tartománya nem egyezik, a portok nem fognak Etherchannel-t kialakítani akkor sem, ha a PAgP szerinti\* If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the **auto vagy** or **desirable** módban vannak.
* A PAgP és LACP dinamikus egyeztetési beállításai nem egyező módon lettek konfigurálva az EtherChannel mindkét végén.

**Note** : It is easy to confuse PAgP or LACP with DTP, because they are all protocols used to automate behavior on trunk links. A PAgP és az LACP portok összefogására szolgál (EtherChannel), míg a DTP a trönkvonalak kialakításának automatizálására használható. Egy EtherChannel trönk létrehozásakor jellemzően először az EtherChannel (PAgP vagy LACP) konfigurálását kell elvégezni és csak azután a DTP-ét.

6.3.3

## EtherChannel hibaelhárítási példa

Az ábrán az S1 és az S2 switch-ek F0/1 és F0/2 portjain létrehozott EtherChannel látható. Az EtherChannel azonban nem működik.

két kapcsoló, az S1 és az S2, két fizikai hálózati kapcsolaton keresztül van összekötve, amelyek EtherChannel-t alkottak; Az S1 F0/1 portja az S2 F0/1 portjához csatlakozik; Az S1 F0/2 portja az S2 F0/2 portjához csatlakozik

S2 S1 Fa0/1 Fa0/2 Fa0/2

Fa0/1

Az EtherChannel hibaelhárításához kattintsunk az egyes gombokra.

**Step 1. Az EtherChannel összefoglaló információinak megtekintése** A **show etherchannel summary** parancs kimenete azt jelzi, hogy az EtherChannel nem működik.

S1# ethercsatorna összefoglaló megjelenítése Jelzők: D - le P - az I port-csatornába kötve - önálló s - felfüggesztett H - Hot-standby (csak LACP) R - Layer3 S - Layer2 U - használatban N - nincs használatban, nincs aggregáció f - nem sikerült kiosztani az M aggregátort - nincs használatban, a minimális hivatkozások nem teljesülnek m - nincs használatban, a port nem aggregált a minimális hivatkozások miatt u - nem alkalmas a kötegelésre w - aggregálásra vár d - az alapértelmezett A port - Auto LAG alkotta Használt csatornacsoportok száma: 1 Aggregátorok száma: 1 Csoport Port-csatorna Protokoll Portok ------+-------------+----- ------+-------------------------------------------- ---- 1 Po1(SD) - Fa0/1(D) Fa0/2(D)

6.3.4

## Packet Tracer - Az EtherChannel hibaelhárítása

Egy kezdő szakember nemrégiben négy switch-et helyezett üzembe. A felhasználók a hálózat lassúságára panaszkodnak, és bennünket kértek meg a felülvizsgálatra.

[EtherChannel hibaelhárítása](https://contenthub.netacad.com/courses/srwe-dl/_common/6.3.4-packet-tracer---troubleshoot-etherchannel_hu-HU.pka)

[6.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az EtherChannel konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[6.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. EtherChannel
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

6.4.1

## Packet Tracer - EtherChannel megvalósítása

Feladatul kaptuk egy EtherChannel megvalósítás megtervezését egy olyan vállalat számára, ami javítani kívánja a switch-ek trönkkapcsolatainak teljesítményét. Az EtherChannel megvalósításának több különböző módját is kipróbálhatjuk annak érdekében, hogy kiértékelhessük, melyik a legjobb a vállalat számára. Meg fogjuk építeni a topológiát, konfiguráljuk a trönkportokat, és megvalósítjuk az LACP és PagP EtherChannel-t.

[EtherChannel megvalósítása](https://contenthub.netacad.com/courses/srwe-dl/_common/6.4.1-packet-tracer---implement-etherchannel_hu-HU.pka)

6.4.2

## Laborgyakorlat - Az EtherChannel megvalósítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: VLAN-ok létrehozása és a switchportok hozzárendelése
* Part 3: 802.1Q trönkök konfigurálása a switch-ek között
* Part 4: EtherChannel megvalósítása és ellenőrzése a switch-ek között

6.4.3

## Miről tanultunk ebben a fejezetben?

**EtherChannel működés**

A sávszélesség vagy redundancia növelése érdekében több kapcsolat is létrehozható az eszközök között. Viszont az STP protokoll blokkolni fogja a redundáns kapcsolatokat a hurkok létrejöttének megakadályozására. Az EtherChannel egy kapcsolatokat összefogó technológia, amely lehetővé teszi az STP által nem blokkolt eszközök közötti redundáns kapcsolatokat. Az EtherChannel több fizikai Ethernet kapcsolatot egyetlen logikai kapcsolatba csoportosít. Hibatűrést, terhelésmegosztást, nagyobb sávszélességet és redundanciát biztosít a switch-ek, routerek és szerverek között. Az EtherChannel konfigurálása után létrejövő virtuális interfészt portcsatornának (port channel) nevezzük. Az EtherChannel számos előnnyel rendelkezik, viszont a megvalósítása bizonyos korlátozásokkal is jár. EtherChannel-ök automatikus egyeztetés útján is létrehozhatók két protokoll segítségével, ezek a PAgP és az LACP. A két protokoll a szomszédos switch-ek hasonló jellemzőkkel bíró portjai között dinamikusan alakít ki csatornákat. Ha egy EtherChannel-t a Cisco által kifejlesztett PAgP használatával konfigurálnak, a PAgP-csomagokat az EtherChannel-t támogató portok között küldik el a csatorna kialakításának egyeztetése érdekében. A PAgP-módok közé a bekapcsolt (on), a kezdeményező (desirable) és az automatikus (auto) módok tartoznak. Az LACP a Cisco-féle PAgP-hez hasonló funkciót valósít meg. Mivel az LACP egy IEEE-szabvány, ezért különböző gyártók berendezései között is lehetővé teszi az EtherChannel-ök kialakítását. Az LACP-módok közé a bekapcsolt (on), az aktív (active) és a passzív (passive) módok tartoznak.

**Az EtherChannel konfigurálása**

Az alábbi irányelvek és korlátozások hasznosak lehetnek az EtherChannel beállításakor:

* **EtherChannel támogatás** – Az összes modul minden Ethernet interfészének támogatnia kell az EtherChannel-t anélkül, hogy az interfészeknek fizikailag szomszédosnak kell lenniük, vagy ugyanazon a modulon.
* **Speed and duplex** Sebesség és duplexitás - Az EtherChannel összes interfészét azonos sebességre és egyforma duplexitásra kell beállítani.
* **VLAN egyezés** – Az EtherChannel kötegben lévő összes interfészt ugyanahhoz a VLAN-hoz kell hozzárendelni, vagy fővonalként kell konfigurálni.
* **VLAN-ok tartománya** – Az EtherChannel a VLAN-ok ugyanazt a megengedett tartományát támogatja a trönkölő EtherChannel összes interfészén.

Az EtherChannel LACP-vel történő konfigurálása a következő három lépésből áll:

**1. lépés:** Adja meg az EtherChannel csoportot alkotó interfészeket az interfész tartomány interfész globális konfigurációs mód parancsával.

**2. lépés:** Hozza létre a portcsatorna interfészt a csatornacsoport azonosító mód aktív paranccsal interfész tartomány konfigurációs módban.

**3. lépés:** A 2. réteg beállításainak módosításához a portcsatorna interfészen, lépjen be a portcsatorna interfész konfigurációs módba az interfész port-channel paranccsal, majd adja meg az interfész azonosítóját.

**Az EtherChannel ellenőrzése és hibaelhárítása.**

Számos parancs létezik az EtherChannel konfigurációjának ellenőrzésére, mint például a **show interfaces port-channel** , a **show etherchannel summary** , a **show etherchannel port-channel** és a **show interfaces etherchannel** . Az EtherChannel gyakori problémái a következők:

* Az EtherChannel-hez hozzárendelt portok nem ugyanannak a VLAN-nak a tagjai vagy nincsenek trönkként konfigurálva. Az eltérő natív VLAN-hoz tartozó portok nem alkothatnak EtherChannel-t.
* A trönközést az EtherChannel-t alkotó egyes portokon konfigurálták, de nem mindegyiken.
* Ha az engedélyezett VLAN-tartományok között eltérés van, akkor az interfészek nem kerülnek be a csatornába még akkor sem, ha auto vagy desirable módra vannak beállítva.
* A PAgP és LACP dinamikus egyeztetési beállításai nem egyező módon lettek konfigurálva az EtherChannel mindkét végén.

6.4.4

## Ellenőrző kvíz - Etherchannel

Az űrlap teteje

1. LACP-t használó EtherChannel összeköttetést alakítottak ki az S1 és az S2 kapcsolók között. Milyen mód kombinációt használhattak a switch-eken?

Az űrlap alja

EtherChannel konfigurálása esetén melyik PAgP-mód állítja be a portot úgy, hogy kezdeményezze a csatorna létrehozását?

Melyik három interfész paraméternek kell megegyezni egy EtherChannel létrejöttéhez? (Három jó válasz van.)

Mik az EtherChannel használatának előnyei? (Három jó válasz van.)

A hálózati rendszergazda EtherChannel-t konfigurál egy kapcsoló két fizikai portján. Melyik állítás igaz arra az esetre, ha az egyik port leáll?

Milyen típusú logikai kapcsolatba van több fizikai interfész összevonva az EtherChannel megvalósításakor?

EtherChannel konfigurálása esetén melyik PAgP-mód állítja be a portot úgy, hogy csak akkor jöjjön létre a csatorna, ha a port PAgP-üzenetet fogad más eszköztől?

Melyik két terheléselosztási módszer használható az EtherChannel technológiában? (Két jó válasz van.)

Melyik funkciót biztosítja az EtherChannel?

Melyik állítás igaz az EtherChannel technológiára?

Melyik két mód kombinációja eredményezné az EtherChannel sikeres egyeztetését? (Két jó válasz van.)

Melyik két protokoll alkalmas fizikai vonalak összefogására (link aggregation protocol)? (Két jó válasz van.)

EtherChannel konfigurálása esetén melyik LACP-mód állítja be a portot úgy, hogy kezdeményezze a csatorna létrehozását?

Mi történik, ha egy hálózati rendszergazda egy EtherChannel-hez tartozó portot az EtherChannel többi portjától különböző VLAN-ba tesz át?

EtherChannel konfigurálása esetén melyik LACP-mód hatására fog a port csak akkor LACP-módban aktiválódni, ha másik eszköztől LACP-csomag érkezik?

[6.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az EtherChannel ellenőrzése és hibajavítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[7.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. DHCPv4
2. Bevezetés

# Bevezetés

7.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a DHCPv4 fejezetben!

A DHCP (Dynamic Host Configuration Protocol) az IP-címek dinamikus hozzárendelésére szolgál a hálózati állomások számára. A DHCPv4 IPv4-címeket használó hálózathoz való. (A DHCPv6-ot egy másik fejezet fogja tárgyalni.) Ez azt jelenti, hogy nekünk, hálózati rendszergazdáknak, nem kell a hálózat minden eszközére vonatkozó IP-címek konfigurálásával töltenünk a napunkat. Egy otthoni vagy irodai hálózatban ez még nem is lenne nehéz, de egy nagyobb hálózatban több száz vagy ezer eszköz is lehet.

Ebben a fejezetben egy Cisco IOS routert fogunk DHCPv4-szerverként konfigurálni. Ezután pedig kliensként is be fogjuk állítani. A fejezet tartalmaz néhány parancsszimulátor és Packet Tracer feladatot, amelyekkel ki is próbálhatjuk az újonnan megtanultakat. A DHCPv4 konfigurációs tudás jelentősen lecsökkenti a rendszergazda terhelését, ki ne szeretné ezt?

7.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe** : DHCPv4

**Modul célja** : A DHCPv4 megvalósítása több LAN-on keresztül történő működéshez.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **DHCPv4-alapfogalmak** | A DHCPv4 működése egy kis- és közepes vállalat hálózatában. |
| **Cisco IOS DHCPv4-kiszolgáló konfigurálása** | Router konfigurálása DHCPv4-kiszolgálóként. |
| **DHCPv4-ügyfél konfigurálása** | Router konfigurálása DHCPv4-ügyfélként. |

[6.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[7.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv4 alapfogalmak](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. DHCPv4
2. DHCPv4 alapfogalmak

# DHCPv4 alapfogalmak

7.1.1

## DHCPv4-kiszolgáló és ügyfél

A DHCPv4 (Dynamic Host Configuration Protocol v4) az IP-címek és egyéb hálózati beállítások dinamikus kiosztására szolgál. Mivel egy hálózatban a csomópontok túlnyomó részét asztali számítógépek képezik, a DHCPv4 rendkívül fontos eszköz a hálózati rendszergazdák számára, amellyel rengeteg időt takaríthatnak meg.

Egy dedikált DHCPv4-szerver jól skálázható és viszonylag könnyen felügyelhető. Ha egy kisebb fiókirodáról vagy otthoni környezetről van szó, nincs szükség dedikált szerverre, a DHCPv4-szolgáltatás egy Cisco routerrel is biztosítható. A Cisco IOS szoftver egy teljes funkcionalitású DHCPv4-szervert is tartalmaz.

A DHCPv4-szerver dinamikusan hozzárendel (bérbe ad) a klienshez egy címet a rendelkezésre álló készletből a szerver által meghatározott időre, vagy ameddig a kliensnek szüksége van rá.

Az ügyfél a címet a megadott ideig használja (bérbe veszi). A rendszergazdák beállíthatják a DHCPv4-szervereken, hogy a bérleti idő milyen időközönként járjon le. Ez jellemzően 24 óra és egy hét között alakul, néha ennél több is lehet. Amikor a bérlet lejár, az ügyfélnek új címet kell kérnie, de általában újra ugyanazt a címet kapja meg.

DHCPv4-kiszolgáló egy DHCPv4-ügyfélhez csatlakoztatott kapcsolóhoz csatlakozik; az első lépésben a DHCPv4 kliens üzenetet küld; a második lépésben a DHCPv6 szerver üzenettel válaszol

1

2

DHCPv4 szerver DHCPv4 kliens

1. A DHCPv4 bérleti folyamat azzal kezdődik, hogy az ügyfél egy DHCP-kiszolgáló szolgáltatásait kérő üzenetet küld.
2. Ha van olyan DHCPv4-kiszolgáló, amely megkapja az üzenetet, az IPv4-címmel és egyéb hálózati konfigurációs információkkal fog válaszolni.

7.1.2

## A DHCPv4 működése

A DHCPv4 ügyfél-kiszolgáló módban működik. Ha egy kliens kommunikációt folytat egy DHCPv4-szerverrel, a szerver egy IPv4-címet oszt ki vagy ad bérbe a kliensnek. A kliens ezzel a bérelt IP-címmel kapcsolódik a hálózatra, amíg a bérleti idő le nem jár. A bérleti idő meghosszabbításához a kliensnek rendszeres időközönként fel kell keresnie a DHCP-szervert. Ez a bérleti mechanizmus garantálja, hogy az áthelyezett vagy kikapcsolt kliensek ne tartsák meg azokat a címeket, amelyekre már nincs szükségük a továbbiakban. A bérleti idő lejárta után a DHCP-szerver gondoskodik arról, hogy a cím visszakerüljön az ismételten kiosztható címek készletébe.

7.1.3

## A bérlet megszerzésének lépései

Amikor a kliens elindul (vagy más módon kapcsolódik a hálózathoz), egy négy lépésből álló folyamattal kezdeményezi a bérleti jog megszerzését.

1. DHCP-felfedezés (DHCPDISCOVER)
2. DHCP-ajánlat (DHCPOFFER)
3. DHCP-kérés (DHCPREQUEST)
4. DHCP-nyugtázás (DHCPACK)

Kattintsunk a gombokra a DHCP-bérlet megszerzéséhez szükséges négylépéses folyamat megismeréséhez.

**1. lépés. DHCP Discover (DHCPDISCOVER)**

The client starts the process using a broadcast DHCPDISCOVER message with its own MAC address to discover available DHCPv4 servers. Mivel a kliens nem rendelkezik érvényes IPv4-információval induláskor, a szerverrel való kommunikációhoz 2. rétegbeli és 3. rétegbeli szórási címeket használ. A DHCPDISCOVER üzenettel deríthetők fel a hálózatban működő DHCPv4-szerverek.

a DHCPv4 folyamat 1. lépése a DHCPv4 klienstől a DHCPv6 szerver felé küldött DHCPDISCOVER üzenettel kezdődik, amely lényegében azt mondja, hogy címet szeretnék kérni.

1

DHCPREQUEST   
Adás "Szeretnék címet kérni." DHCPv4 szerver DHCPv4 kliens

7.1.4

## A bérlet megújítása

A bérleti idő lejárta előtt a kliens a megújítást két lépésből álló folyamattal kísérli meg a DHCPv4-szerver felé, amint az ábrán is láthatjuk:

**1 . DHCP-kérés (DHCPREQUEST)**

A bérleti idő lejárta előtt a kliens DHCPREQUEST üzenetet küld közvetlenül annak a DHCPv4-szervernek, amelytől a címét korábban kapta. Amennyiben a DHCPACK bizonyos időn belül nem érkezik meg, a kliens szórással egy újabb DHCPREQUEST-et indít, hogy valamelyik másik DHCPv4-szerver meghosszabbítsa a bérleti idejét.

**2 . DHCP nyugtázás (DHCPACK)**

A DHCPREQUEST üzenet megérkezése után a szerver egy DHCPACK visszaküldésével erősíti meg a bérleti adatokat.

**Megjegyzés** : Ezek az üzenetek (elsősorban a DHCPOFFER és a DHCPACK) az IETF RFC 2131 szerint unicastként vagy sugárzottként küldhetők.

A diagram bemutatja a kétlépéses folyamatot és üzenetváltást a DHCPv4 kliens és a DHCPv4 szerver között, amikor az ügyfél meg akarja hosszabbítani a bérletet. Az első lépésben a kliens egy DCHPREQUEST unicast üzenetet küld a szervernek, amelyben azt mondja, hogy lényegében szeretném megújítani a bérletemet. A 2. lépésben a szerver egy DHCPACK unicast üzenettel válaszol, amely lényegében az Ön kérésének nyugtázását jelenti.

1

2

– Kérését nyugtázták. DHCPACK   
Unicast DHCPREQUEST   
Unicast "Szeretném megújítani a bérletemet." DHCPv4 szerver DHCPv4 kliens

7.1.5

## Tudáspróba - A DHCPv4 alapjai

Az űrlap teteje

Ellenőrizze, hogy megértette-e a DHCPv4 fogalmait, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik üzenetet küldi a DHCPv4 kliens a bérletszerzési folyamat elindításához?

Az űrlap alja

Which two DHCPv4 messages are sent by the server in the lease obtaining process? (Két jó válasz van.)

Which two DHCPv4 messages are used in the lease renewal process? (Két jó válasz van.)

[7.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[7.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Cisco IOS DHCPv4-kiszolgáló konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Ugrás a tartalomra](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. DHCPv4
2. Cisco IOS DHCPv4-kiszolgáló konfigurálása

# Cisco IOS DHCPv4-kiszolgáló konfigurálása

7.2.1

## Cisco IOS DHCPv4-kiszolgáló

Mostanra már értjük a DHCPv4 alapvető működését és azt, hogy hogyan teszi könnyebbé a dolgunkat. Ez a fejezet bemutatja, hogyan használhatunk egy Cisco IOS router-t DHCPv4-kiszolgálóként, ha nincs erre külön szerverünk. Egy Cisco IOS operációs rendszert futtató router is beállítható DHCPv4-szervernek. A Cisco IOS DHCPv4-szervere képes a routeren megadott IPv4-címkészletek DHCPv4-kliensek felé történő kiosztására és kezelésére.

A hálózati topológia egy útválasztót mutat, amely DHCPv4 szerverként működik, és két LAN-t köt össze. A bal oldalon a 192.168.10.0/24-es hálózat látható, amely az S1 kapcsolóhoz csatlakoztatott PC1-ből áll, amely a G0/0/0-s R1 útválasztóhoz csatlakozik .1 címmel. A jobb oldalon a 192.168.11.0/24-es hálózat látható, amely a PC2-ből és a 192.168.11.6/24 címen található DNS-kiszolgálóból áll, amely az S2 kapcsolóhoz csatlakozik, amely a G0/0/1-es R1-hez csatlakozik .1 címmel.

PC2 S1 PC1 S2 R1 G0/0/0.1 192.168.11.0/24 192.168.10.0/24

G0/0/1.1

DNS-kiszolgáló 192.168.11.6/24 DHCPv4-kiszolgáló

7.2.2

## A Cisco IOS DHCPv4 kiszolgáló konfigurálásának lépései

A Cisco IOS DHCPv4-kiszolgáló konfigurálásához az alábbi lépések szükségesek:

**Step 1** . Címek kizárása.   
**Step 2** . A DHCPv4-készlet nevének megadása.   
**Step 3** . A készlet konfigurálása.

**1. lépés: zárja ki az IPv4-címeket**

A DHCPv4-szerverként üzemelő router a címkészlet összes címét kiadja, ha nem zárunk ki belőle bizonyos címeket. A készlet néhány IPv4-címe jellemzően a statikus címet igénylő hálózati eszközöknek van kiosztva. Következésképpen ezeket a címeket nem szabad más eszközöknek kiosztani. Az IPv4-címek kizárásának parancsszintaxisa a következő:

Router(config)#  **ip dhcp kizárt-cím**  alacsony-cím [ high-address ]

Egy cím vagy címtartomány kizárása az első és utolsó cím megadásával lehetséges. Azokat a címeket zárjuk ki, amelyeket routereknek, szervereknek, nyomtatóknak vagy egyéb eszközöknek manuálisan adtunk vagy fogunk adni. A parancsot többször is használhatjuk.

**2. lépés: Adjon meg egy DHCPv4-készletnevet**

A DHCPv4-szerverek beállítása magában foglalja a kiosztható címkészlet megadását.

Az ábrán láthatjuk, hogy a **ip dhcp pool** készlet-neve parancs a megadott névvel létrehoz egy készletet, és a router DHCPv4 konfigurációs módba lép, amit a Router(dhcp-config)# prompt jelez.

A készlet definiálásának parancsa:

Router(config)#  **ip dhcp pool**  pool\_name   
Router(dhcp-config)#

**3. lépés: Konfigurálja a DHCPv4-készletet**

Táblázatban soroltuk fel a DHCPv4-készlet konfigurálásának feladatait.

Be kell állítani a címtartományt és az alapértelmezett átjárót. A **network** paranccsal megadjuk az elérhető címtartományt. A **default-router** paranccsal megadjuk az alapértelmezett átjárót. Az átjáró jellemzően a klienseszközökhöz legközelebb található router LAN-interfésze. Egy átjáró megadása kötelező, de akár nyolc cím is megadható, ha több is van belőlük.

A többi DHCPv4-címkészletre vonatkozó parancs megadása nem kötelező. Például, a DHCPv4-klliens számára elérhető DNS-szerver IP-címét a **dns-server** paranccsal adhatjuk meg. A **domain-name** paranccsal adhatjuk meg a domain nevet. A bérleti idő hosszát pedig a **lease** paranccsal állíthatjuk be. Az alapértelmezett bérleti idő egy nap. A **netbios-name-server** paranccsal állítható be a NetBIOS WINS-szerver.

| TaskIOS CommandHatározza meg a címet pool.network network-number [maszk | /prefix-length]Határozza meg az alapértelmezett útválasztót vagy gateway.default-router címet [cím2….cím8]DNS szerver.dns-szerver cím meghatározása [cím2…cím8]Domain name.domain-name tartomány meghatározása Határozza meg a a DHCP bérlet időtartama.bérlet {nap[óra[perc]] | végtelen} Define the NetBIOS WINS server.netbios-name-server address [address2…address8] | |
| --- | --- |
| **Feladat** | **IOS-parancs** |
| A címkészlet megadása. | **hálózati**  hálózati szám [ maszk | / előtag-hossz ] |
| Alapértelmezett átjáró megadása. | **alapértelmezett útválasztó**  címe [ cím2….cím8 ] |
| DNS-szerver megadása. | **dns-szerver**  címe [ cím2…cím8 ] |
| Domain név megadása. | **domain név**  domain |
| A bérleti idő megadása. | **bérlet**  { nap [ óra [ perc ]] |  **végtelen**  } |
| NetBIOS WINS-szerver megadása. | **netbios-névszerver**  címe [ cím2…cím8 ] |

**MEGJEGYZÉS** : A Microsoft nem javasolja a WINS használatát, ehelyett DNS-t használjunk névfeloldásra.

7.2.3

## Konfigurációs példa

A példában használt topológiát az ábrán láthatjuk.

A hálózati topológia egy útválasztót mutat, amely DHCPv4 szerverként működik, és két LAN-t köt össze. A bal oldalon a 192.168.10.0/24-es hálózat látható, amely az S1 kapcsolóhoz csatlakoztatott PC1-ből áll, amely a G0/0/0-s R1 útválasztóhoz csatlakozik .1 címmel. A jobb oldalon a 192.168.11.0/24-es hálózat található, amely a PC2-ből és a 192.168.11.5/24 címen található DNS-kiszolgálóból áll, amely az S2 kapcsolóhoz csatlakozik, amely a G0/0/1-es R1-hez csatlakozik .1 címmel.

PC2 S1 PC1 S2 R1 G0/0/0.1 192.168.11.0/24 192.168.10.0/24 G0/0/1.1

192.168.11.5/24

DNS-kiszolgáló DHCPv4 Server

A példán az R1-et állítjuk be, hogy DHCPv4-kiszolgáló legyen a 192.168.10.0/24 LAN számára.

R1(config)# **ip dhcp excluded-address 192.168.10.1 192.168.10.9**

R1(config)# **ip dhcp excluded-address 192.168.10.254**

R1(config)# **ip dhcp pool LAN-POOL-1**

R1(dhcp-config)# **network 192.168.10.0 255.255.255.0**

R1(dhcp-config)# **default-router 192.168.10.1**

R1(dhcp-config)# **dns-server 192.168.11.5**

R1(dhcp-config)# **domain-name example.com**

R1(dhcp-config)# **end**

R1#

7.2.4

## A DHCPv4 működését ellenőrző parancsok

A táblázatban található parancsok segítségével ellenőrizhetjük a Cisco IOS DHCPv4-kiszolgáló működését.

| CommandDescriptionshow running-config | section dhcpDisplays the DHCPv4 az útválasztón konfigurált parancsok.show ip dhcp kötés Megjeleníti az összes listát A DHCPv4 szolgáltatás által biztosított IPv4-cím és MAC-cím összerendelés.show ip dhcp server statistics Számadatokat jelenít meg a számra vonatkozóan A küldött és fogadott DHCPv4 üzenetek. | |
| --- | --- |
| **Parancs** | **Leírás** |
| **show running-config | szakasz dhcp** | A routeren beállított DHCPv4-parancsokat mutatja meg. |
| **ip dhcp kötés megjelenítése** | Megmutatja a DHCPv4-szolgáltatás által kiadott IPv4-címek és MAC-címek listáját. |
| **ip dhcp szerver statisztikák megjelenítése** | Displays count information regarding the number of DHCPv4 messages that elküldték és fogadták. |

7.2.5

## A DHCPv4 működésének ellenőrzése

A példában szereplő kimenetek az ábrán látható topológiája alapján készültek. Az R1 router beállítása a DHCPv4-szolgáltatások nyújtására már megtörtént. A PC1 elindítására még nem került sor, ezért IP-címmel sem rendelkezik.

A hálózati topológia egy útválasztót mutat, amely DHCPv4 szerverként működik, és két LAN-t köt össze. A bal oldalon a 192.168.10.0/24-es hálózat látható, amely az S1 kapcsolóhoz csatlakoztatott PC1 gazdaszámítógépből áll, amely az R1 útválasztóhoz csatlakozik a G0/0/0 helyen .1 címmel. A jobb oldalon a 192.168.11.0/24-es hálózat található, amely a PC2-ből és a 192.168.11.5/24 címen található DNS-kiszolgálóból áll, amely az S2 kapcsolóhoz csatlakozik, amely a G0/0/1-es R1-hez csatlakozik .1 címmel.

PC2 S1 PC1 S2 R1 G0/0/0.1 192.168.11.0/24 192.168.10.0/24 G0/0/1.1

192.168.11.5/24

DNS-kiszolgáló DHCPv4 Server

A következő parancsok kimenete feltételezi, hogy a PC1 megkapta az IPv4 címzési információkat a DHCPv4 szervertől. Előfordulhat, hogy Windows PC-n be kell írnia az ipconfig /renew parancsot, hogy DHCPDISCOVER üzenetet küldjön. Kattintson az egyes gombra a DHCPv4 működését igazoló parancs kimenetének megtekintéséhez.

**Ellenőrizze a DHCPv4 konfigurációt** Ahogy a példában is látható, a **show running-config | szakasz dhcp** parancskimenete megjeleníti az R1-en konfigurált DHCPv4 parancsokat.

A **| szakasz** paraméter csak a DHCPv4 konfigurációhoz tartozó parancsokat jeleníti meg.

R1# show running-config | A DHCP IP DHCP szakasz kizárva-címe 192.168.10.1 192.168.10.9 IP DHCP Kizárt cím 192.168.10.254 IP DHCP POOL LAN-POOL-1 NETHÁZ 192.168.10.0 255.255.255.0 alapértelmezett 192.168.10,10,10,10,10,10,10,10,10,10,10.10.10.1688. neve example.com

7.2.6

## Parancsszimulátor - DHCPv4 konfigurálása

Ebben a feladatban az R1-et konfiguráljuk a 192.168.11.0/24 hálózat DHCPv4-szerverként.

A hálózati topológia egy útválasztót mutat, amely DHCPv4 szerverként működik, és két LAN-t köt össze. A bal oldalon a 192.168.10.0/24-es hálózat látható, amely az S1 kapcsolóhoz csatlakoztatott PC1 gazdaszámítógépből áll, amely az R1 útválasztóhoz csatlakozik a G0/0/0 helyen .1 címmel. A jobb oldalon a 192.168.11.0/24-es hálózat található, amely a PC2-ből és a 192.168.11.5/24 címen található DNS-kiszolgálóból áll, amely az S2 kapcsolóhoz csatlakozik, amely a G0/0/1-es R1-hez csatlakozik .1 címmel.

PC2 S1 PC1 S2 R1 G0/0/0.1 192.168.11.0/24 192.168.10.0/24

G0/0/1.1

DNS-kiszolgáló 192.168.11.6/24 DHCPv4-kiszolgáló

Exclude the following addresses from the 192.168.11.0/24 address range:

* Exclude the .1 through the .9 address.
* Exclude the .254 address.

R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.9

R1(config)#ip dhcp excluded-address 192.168.11.254

Configure the DHCPv4 pool with the following requirements:

* Define the pool name of **LAN-POOL-2**.
* Configure the network address.
* Configure the default gateway address.
* Configure the DNS server address.
* Configure **example.com** as the domain name.
* Return to privileged EXEC mode.

R1(config)#ip dhcp pool LAN-POOL-2

R1(dhcp-config)#network 192.168.11.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.11.1

R1(dhcp-config)#dns-server 192.168.11.6

R1(dhcp-config)#domain-name example.com

R1(dhcp-config)#end

You have successfully configured DHCPv4 server and relay agent

7.2.7

## A Cisco IOS DHCPv4-kiszolgáló letiltása

A DHCPv4-szolgáltatás alapértelmezés szerint engedélyezve van. A szolgáltatást a **no service dhcp** globális konfigurációs paranccsal tudjuk kikapcsolni. A **service dhcp** globális konfigurációs parancs újra engedélyezi a DHCPv4-szerver szolgáltatást (lásd ábra). Ha a paraméterek nincsenek beállítva, a szolgáltatás engedélyezésének nincs semmilyen hatása.

**Megjegyzés** : A DHCP-összerendelések törlése vagy a DHCP-szolgáltatás leállítása és újraindítása ideiglenesen duplikált IP-címek kiosztását eredményezheti a hálózaton.

R1(config)# **no service dhcp**

R1(config)# **service dhcp**

R1(config)#

7.2.8

## DHCPv4 relé

Összetett, hierarchikus vállalati hálózatokban a szerverek a hálózat központjában kapnak helyet. Ezek a szerverek DHCP-, DNS-, TFTP- és FTP-szolgáltatásokat nyújthatnak a hálózat számára. A hálózati kliensek jellemzően nincsenek egy alhálózaton ezekkel a szerverekkel. A kliensek gyakran szórásos üzenetek segítségével találják meg a szervereket, hogy igénybe vegyék az általuk kínált szolgáltatásokat.

Az ábrán PC1 szórásos üzenet segítségével próbál IPv4-címet szerezni egy DHCPv4-szervertől. Ebben a példában R1 router nincs beállítva, hogy DHCPv4-szerverként működjön és a szórást sem továbbítja. Mivel a DHCPv4-szerver egy másik hálózaton van, ezért a PC1 nem kap IP-címet DHCP segítségével. R1-et úgy kell konfigurálni, hogy a DHCPv4-üzeneteket továbbítsa a DHCPv4-kiszolgálónak.

A hálózati topológia egy útválasztót mutat, amely két LAN-t köt össze. A bal oldalon a 192.168.10.0/24-es hálózat látható, amely az S1 kapcsolóhoz csatlakoztatott PC1 gazdaszámítógépből áll, amely az R1 útválasztóhoz csatlakozik a G0/0/0 helyen .1 címmel. A PC1 alatti szöveg olvasható; DHCPv4 szervert keresek. A router alatti szöveg olvasható; Nem tudom továbbítani az adásokat a hálózatok között. A jobb oldalon található a 192.168.11.0/24-es hálózat, amely a PC2-ből, a 192.168.11.5/24-es DNS-kiszolgálóból és a 192.168.11.6/24-es DHCPv4-szerverből áll, amelyek mindegyike az S2 kapcsolóhoz csatlakozik, amely az R1-hez csatlakozik a G0/ helyen. 0/1 .1 címmel.

PC2 S1 PC1 S2 R1 G0/0/0.1 192.168.11.0/24 192.168.10.0/24

G0/0/1.1

DHCPv4-kiszolgáló 192.168.11.6/24 DNS-kiszolgáló 192.168.11.5/24 DHCPv4-kiszolgálót keresek. Nem tudom továbbítani az adásokat a hálózatok között.

Ebben a példában a hálózati rendszergazda megpróbálja megújítani a PC1 IPv4-címzési adatait. Kattintsunk az egyes gombokra a parancsok kimenetének megtekintéséhez, amelyekben a hálózati rendszergazda megoldja ezt a problémát.

**ipconfig /release** A PC1 egy Windows számítógép.

The network administrator releases all current IPv4 addressing information using the **ipconfig /release** command. Figyeljük meg, hogy az IPv4-cím eltűnik, nem látunk címet.

C:\Users\Student> ipconfig /release Windows IP-konfiguráció Ethernet adapter Ethernet0: Kapcsolat-specifikus DNS-utótag.

:

Default Gateway . . . . . . . . . :

7.2.9

## Egyéb továbbított szórásos szolgáltatások

Nem csak a DHCPv4-szolgáltatást képes a router továbbítani. Alapesetben az **ip helper-address** parancs hatására a routerek a következő nyolc UDP alapú szolgáltatás forgalmát közvetítik:

* 37-es port: Idő
* 49-es port: TACACS
* 53-as port: DNS
* Port 67: DHCP-/BOOTP-kiszolgáló
* Port 68: DHCP-/BOOTP-kliens
* 69-es port: TFTP
* Port 137: NetBIOS névszolgáltatás
* Port 138: NetBIOS datagram szolgáltatás

7.2.10

## Packet Tracer - A DHCPv4 konfigurálása

A Packet Tracer feladat során a következőket fogjuk elvégezni:

* Part 1: Router konfigurálása DHCP-szerverként
* Part 2: DHCP-továbbítás konfigurálása
* Part 3: Router konfigurálása DHCP-kliensként
* Part 4: A DHCP és a kapcsolatok ellenőrzése

[DHCPv4 konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/7.2.10-packet-tracer---configure-dhcpv4_hu-HU.pka)

[7.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv4 alapfogalmak](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[7.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv4-ügyfél konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. DHCPv4
2. DHCPv4-ügyfél konfigurálása

# DHCPv4-ügyfél konfigurálása

7.3.1

## A Cisco Router, mint DHCPv4-kliens

Vannak olyan esetek, amikor az internetszolgáltatónk DHCP-szerverét kell használnunk. Ekkor a Cisco IOS routerünket DHCPv4-ügyfélként kell beállítanunk. Most ezen a folyamaton fogunk végigmenni.

Időnként egy otthoni vagy kisvállalati hálózatban vagy külső telephelyen a Cisco routert kell DHCPv4-kliensként konfigurálnunk, mintha kliens számítógép lenne. A használandó módszer az internetszolgáltatótól függ. A kábel- vagy DSL-modemhez a legegyszerűbb esetekben Ethernet-interfész használatával lehet kapcsolódni.

Az Ethernet interfészt DHCP-kliensként az **ip address dhcp** interfész konfigurációs paranccsal tudjuk beállítani.

Tegyük fel, hogy az ábrán szereplő ISP-routert úgy konfigurálták, hogy az ügyfelek számára a 209.165.201.0/27 hálózatból adjon címet, miután az ügyfél routerének G0/0/1 interfészén kiadták az **ip address dhcp** parancsot.

a router configured as a DHCPv4 client is connected via G0/0/1 to a cable or DSL modem which is then connected to the cloud which is then connected to an ISP router functioning as a DHCPv4 server

G0/0/1 SOHO

ISP

DHCPv4 ClientCable or DSL  
ModemDHCPv4 Server

7.3.2

## Konfigurációs példa

Az Ethernet interfészt DHCP-kliensként az **ip address dhcp** interfész konfigurációs paranccsal tudjuk beállítani (lásd ábra). Feltételezzük, hogy az internetszolgáltató úgy lett beállítva, hogy IPv4-címzési információkat biztosítson az ügyfelek számára.

SOHO(config)# **interface G0/0/1**

SOHO(config-if)# **ip address dhcp**

SOHO(config-if)# **no shutdown**

Sep 12 10:01:25.773: %DHCP-6-ADDRESS\_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO

A **show ip interface g0/0/1** parancs kimenetéből látjuk, hogy az interfész aktív és címinformációkat kapott a DHCPv4-szervertől.

SOHO# **show ip interface g0/0/1**

GigabitEthernet0/0/1 is up, line protocol is up

Internet address is 209.165.201.12/27

Broadcast address is 255.255.255.255

Address determined by DHCP

(output omitted)

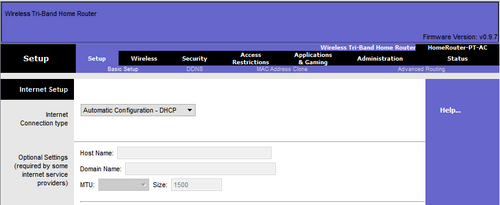
7.3.3

## Otthoni router DHCPv4-kliensként

Az otthoni routerek alapbeállítása általában olyan, hogy az IPv4-címinformációkat a szolgáltatótól kérjék. Így a vásárló nagyon könnyen be tudja üzemelni a routert és kapcsolódni tud a szolgáltatójához.

A példában a Packet Tracerben található vezeték nélküli router alapértelmezett WAN-beállításait látjuk. Figyeljük meg, hogy az internetkapcsolat típusa **Automatic Configuration - DHCP**. Ha a router DSL- vagy kábelmodemhez kapcsolódik, DHCPv4-klienssé válik, és az internetszolgáltatótól kér IPv4-címet.

Az otthoni routerek nagy része hasonló alapbeállításokkal rendelkezik.



7.3.4

## Parancsszimulátor - Cisco router konfigurálása DHCP-ügyfélként

Ebben a feladatban Cisco routert konfigurálunk DHCP-ügyfélként.

a router configured as a DHCPv4 client is connected via G0/0/1 to a cable or DSL modem which is then connected to the cloud which is then connected to an ISP router functioning as a DHCPv4 server

G0/0/1 SOHO

ISP

DHCPv4 ClientDHCPv4 ServerCable or DSL  
Modem

Lépjünk át interfészkonfigurációs módba. Use **g0/0/1** as the interface name.

SOHO(config)#interface g0/0/1

Configure the interface to acquire IPv4 addressing information from the ISP.

SOHO(config-if)#ip address dhcp

Activate the interface.

SOHO(config-if)#no shutdown

Sep 12 10:01:25.773: %DHCP-6-ADDRESS\_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO

Return to privileged EXEC mode.

SOHO(config-if)#end

Use the **show ip interface g0/0/1** command to verify the IPv4 information.

SOHO#show ip interface g0/0/1

GigabitEthernet0/0/1 is up, line protocol is up

Internet address is 209.165.201.12/27

Broadcast address is 255.255.255.255

Address determined by DHCP

(output omitted)

You have successfully configured the router as a DHCP client.

[7.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Cisco IOS DHCPv4-kiszolgáló konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[7.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. DHCPv4
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

7.4.1

## Packet Tracer - A DHCPv4 megvalósítása

Egy vállalat hálózati szakembereként azt a feladatot kapjuk, hogy állítsunk be egy Cisco routert úgy, hogy DHCP-szerverként dinamikusan osszon címeket a hálózaton lévő klienseknek. Ezen felül feladatunk, hogy a hálózat szélén levő router DHCP-kliensként IP-címet kapjon az internetszolgáltatótól. Mivel a DHCP-szerver a központban van, a két LAN-routeren be kell állítani azt is, hogy a LAN-ok DHCP-forgalmát a DHCP-szerverként üzemelő router felé továbbítása.

[DHCPv4 megvalósítása](https://contenthub.netacad.com/courses/srwe-dl/_common/7.4.1-packet-tracer---implement-dhcpv4_hu-HU.pka)

7.4.2

## Laborgyakorlat - A DHCPv4 megvalósítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: Két DHCPv4-kiszolgáló konfigurálása és ellenőrzése az R1-en
* Part 3: DHCP Relay konfigurálása és ellenőrzése az R2-n

7.4.3

## Miről tanultunk ebben a fejezetben?

**DHCPv4 Concepts**

A DHCPv4-szerver dinamikusan hozzárendel (bérbe ad) a klienshez egy címet a rendelkezésre álló készletből a szerver által meghatározott időre, vagy ameddig a kliensnek szüksége van rá. A DHCPv4 bérleti folyamat azzal kezdődik, hogy az ügyfél egy DHCP-kiszolgáló szolgáltatásait kérő üzenetet küld. Ha van olyan DHCPv4-kiszolgáló, amely megkapja az üzenetet, az IPv4-címmel és egyéb hálózati konfigurációs információkkal fog válaszolni. A bérleti idő meghosszabbításához a kliensnek rendszeres időközönként fel kell keresnie a DHCP-szervert. Ez a bérleti mechanizmus garantálja, hogy az áthelyezett vagy kikapcsolt kliensek ne tartsák meg azokat a címeket, amelyekre már nincs szükségük a továbbiakban. Amikor a kliens elindul (vagy más módon kapcsolódik a hálózathoz), egy négy lépésből álló folyamattal kezdeményezi a bérleti jog megszerzését: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, végül pedig DHCPACK. A bérleti idő lejárta előtt a kliens a megújítást két lépésből álló folyamattal kísérli meg a DHCPv4-szerver felé: DHCPREQUEST és DHCPACK.

**Configure a Cisco IOS DHCPv4 Server**

Egy Cisco IOS operációs rendszert futtató router beállítható DHCPv4-szerverként. A következő lépésekkel konfigurálhatjuk a Cisco IOS DHCPv4-kiszolgálót: címek kizárása, DHCPv4-készlet nevének megadása, majd a készlet címtartományának megadása. A konfigurációt a **show running-config | section dhcp**, a **show ip dhcp binding** és a **show ip dhcp server statistics** parancsokkal ellenőrizhetjük. A DHCPv4-szolgáltatás alapértelmezés szerint engedélyezve van. A szolgáltatást a **no service dhcp** globális konfigurációs paranccsal tudjuk kikapcsolni. Összetett, hierarchikus vállalati hálózatokban a szerverek a hálózat központjában kapnak helyet. Ezek a szerverek DHCP-, DNS-, TFTP- és FTP-szolgáltatásokat nyújthatnak a hálózat számára. A hálózati kliensek jellemzően nincsenek egy alhálózaton ezekkel a szerverekkel. A kliensek gyakran szórásos üzenetek segítségével találják meg a szervereket, hogy igénybe vegyék az általuk kínált szolgáltatásokat. A PC-k szórásos üzenetek segítségével próbálnak IPv4-címet szerezni DHCPv4-szervertől. Ha a router nincs beállítva DHCPv4-szerverként, nem továbbítja a szórásokat. Ha a DHCPv4-szerver egy másáik hálózaton van, a PC nem tud IP-cím információt kapni DHCP-vel. A routert úgy kell konfigurálni, hogy a DHCPv- üzeneteket továbbítsa a DHCPv4-kiszolgálónak. A hálózati rendszergazda a **ipconfig /release** parancs használatával eldobja az aktuális IPv4-cím konfigurációt. Ezután a hálózati rendszergazda megpróbálja megújítani az IPv4 címzési információkat az **ipconfig /renew** paranccsal. Jobb megoldás a router konfigurálása az **ip helper-address** cím interfész konfigurációs paranccsal. A rendszergazda a **show ip interface** paranccsal ellenőrizheti a konfigurációt. A számítógép most már képes IPv4-címet szerezni a DHCPv4-kiszolgálóról, ami a **ipconfig /all** paranccsal ellenőrizhető. Alapesetben az **ip helper-address** parancs hatására a routerek a következő nyolc UDP alapú szolgáltatás forgalmát közvetítik:

* Port 37: Time
* Port 49: TACACS
* Port 53: DNS
* Port 67: DHCP-/BOOTP-kiszolgáló
* Port 68: DHCP-/BOOTP-kliens
* Port 69: TFTP
* Port 137: NetBIOS névszolgáltatás
* Port 138: NetBIOS datagram szolgáltatás

**Configure a DHCPv4 Client**

Kábel- vagy DSL-modemhez Ethernet interfész használatával kapcsolódunk. Az Ethernet interfészt DHCP-kliensként az **ip address dhcp interface** interfész konfigurációs paranccsal tudjuk beállítani. Az otthoni routerek alapbeállítása általában olyan, hogy az IPv4-címinformációkat a szolgáltatótól kérjék. Az internetkapcsolat típusa automatikus DHCP-konfigurációra (Automatic Configuration - DHCP) van beállítva. Ez azt jelenti, hogy ha a router DSL- vagy kábelmodemhez kapcsolódik, DHCPv4-klienssé válik, és az internetszolgáltatótól kér IPv4-címet.

7.4.4

## Ellenőrző kvíz - DHCPv4

Az űrlap teteje

1. Egy DHCP-kliens PC most indult el. A DHCP-szerverrel való kommunikáció során melyik két lépésben használ a kliens PC szórásos üzeneteket? (Két jó válasz van.)

Az űrlap alja

A rendszergazda kiadja a következő parancsokat: Router(config)# **interfész g0/1** Router(config-if)# **ip-cím dhcp** Mit akar elérni a rendszergazda?

Amikor egy kliens először igényel címet a DHCP-szervertől, akkor a DHCPREQUEST üzenetet miért üzenetszórással küldi?

Melyik DHCP-üzenet tartalmazza a következő információkat? Cél címe: 255.255.255.255 Kliens IPv4-címe: 0.0.0.0 Alapértelmezett átjáró címe: 0.0.0.0 Alhálózati maszk: 0.0.0.0

Milyen üzenetet küld egy DHCPv4-ügyfél, amikor IP-címet kér?

Milyen üzenetet küld a kliens a DHCP-szervernek, amikor egy DHCPv4-bérlet a lejárati idejéhez közeledik?

Mi a cél IP-címe egy IPv4-állomás által küldött DHCPDISCOVER üzenetnek?

Ha a helyi hálózaton több DHCP-szerver is elérhető, milyen sorrendben haladnak az üzenetek az állomás és a DHCP-szerver között?

Melyik egy tipikus eset arra, amikor egy router WAN-interfésze DHCP-kliensként dinamikus IP-címet kap az internetszolgáltatótól?

Melyik az a DHCPv4 címkiosztási mód, amikor az IPv4-címek hozzárendelése egy adott bérleti időre szól?

Miért szórással kerül kiküldésre a DHCPREQUEST üzenet a DHCPv4-folyamat során?

Hogyan továbbítódik a DHCPDISCOVER üzenet a hálózaton a DHCP-szerver felé?

Melyik cél IPv4-címet használja egy DHCPv4-ügyfél a kezdeti DHCP-felderítő csomag elküldésére, amikor DHCP-kiszolgálót keres?

Melyik két helyzetben konfigurálnánk egy routert DHCPv4-kliensként? (Két jó válasz van.)

Melyik célcímet használja a DHCPv4-kiszolgáló, amikor DHCPOFFER üzenetet küld egy ügyfélnek, amely címkérelmet nyújtott be?

[7.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv4-ügyfél konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. Bevezetés

# Bevezetés

8.0.1

## Üdvözöljük

Üdvözöljük a SLAAC és DHCPv6-ról szóló fejezetben!

A SLAAC és a DHCPv6 dinamikus címzési protokollok IPv6 hálózatban. Egy kis konfigurálásért cserébe megkönnyíti hálózati rendszergazdaként a napunkat. Ebben a fejezetben megtudhatjuk, hogyan használjuk a SLAAC módszert arra, hogy az állomások saját IPv6 globális unicast címüket létrehozzák, valamint beállíthatunk egy Cisco IOS routert DHCPv6-kiszolgálónak, DHCPv6-ügyfélnek vagy DHCPv6 továbbító ügynöknek. A fejezet egy laborfeladatot is tartalmaz, amelyben DHCPv6-ot konfigurálhatunk valós eszközökön.

8.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: SLAAC and DHCPv6

**Module Objective**: Configure dynamic address allocation in IPv6 networks.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **IPv6 globális egyedi címek kiosztása** | Explain how an IPv6 host can acquire its IPv6 configuration. |
| **Állapotmentes automatikus címkonfiguráció (SLAAC)** | Explain the operation of SLAAC. |
| **DHCPv6** | Explain the operation of DHCPv6. |
| **DHCPv6-kiszolgáló konfigurálása** | Configure a stateful and stateless DHCPv6 server. |

[7.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IPv6 GUA hozzárendelés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. IPv6 GUA hozzárendelés

# IPv6 GUA hozzárendelés

8.1.1

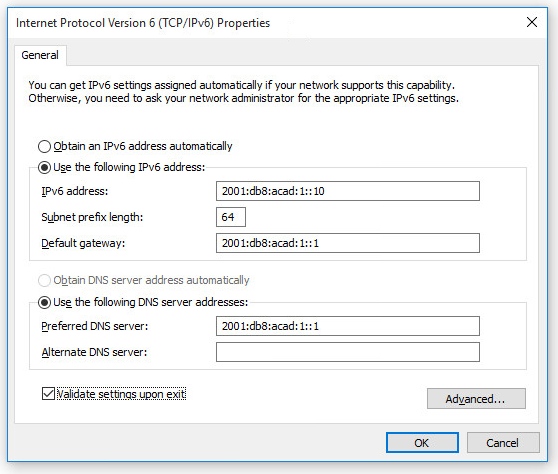
## IPv6 állomás konfiguráció

Kezdjük az elején! Az állapotmentes automatikus címkonfiguráció (stateless address autoconfiguration, SLAAC) vagy a DHCPv6 használatához át kell tekintenünk a globális egyedi címeket (global unicast address, GUA) és a link-local címeket (link-local address, LLA). Ez a témakör mindkettőt lefedi.

Routeren az IPv6 globális egyedi cím (GUA) kézzel beállítható az **ipv6 address** ipv6-address**/**prefix-length interfész konfigurációs paranccsal.

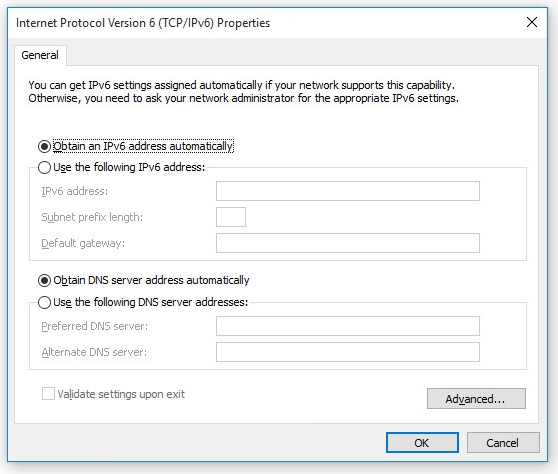
Windows állomáson a GUA-cím konfiguráció szintén beállítható manuálisan az ábrán látható módon.

shows the Internet Protocol Version 6 properties window and static IPv6 address and DNS server settings



Az IPv6 GUA kézi megadása időigényes lehet és hibák is előfordulhatnak a bevitel során. Ezért a legtöbb Windows állomáson engedélyezve van az IPv6 GUA konfiguráció dinamikus beállítása az ábrán látható módon.

shows the Internet Protocol Version 6 properties window and automatic DHCP IPv6 address and DNS server settings



8.1.2

## IPv6 állomás link-local cím

Ha automatikus IPv6-címzés van kiválasztva, az állomás megpróbálja automatikusan megszerezni és beállítani az IPv6-címadatokat az interfészen. Az állomás az interfészen kapott ICMPv6 (Internet Control Message Protocol version 6) protokoll router hirdetés (Router Advertisement, RA) üzenetben meghatározott három módszer egyikét fogja használni. Az állomással közös hálózaton található IPv6-router olyan RA üzeneteket küld, amelyek azt közlik az állomásokkal hogyan szerezhetik be IPv6-címzési információikat. Az állomás automatikusan létrehozza az IPv6 link-local címet az elindulásakor, amikor az Ethernet interfész aktívvá válik. A példa **ipconfig** parancskimenetében egy automatikusan generált link-local cím (LLA) van kiemelve.

In the figure, notice that the interface does not have an IPv6 GUA. The reason is because, in this example, the network segment does not have a router to provide network configuration instructions for the host or the host has not been configured with at static IPv6 address.

**Note:** Host operating systems will at times show a link-local address appended with a "%" and a number. Ezt Zóna-azonosítónak (Zone ID) vagy hatókör-azonosítónak (Scope ID) nevezik. Az operációs rendszer ezt használja az LLA adott interfészhez társításához.

C:\PC1> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . :

Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21

IPv4 Address. . . . . . . . . . . : 169.254.202.140

Subnet Mask . . . . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . . . :

C:\PC1>

8.1.3

## IPv6 GUA hozzárendelés

Az IPv6-ot úgy tervezték, hogy egyszerűsítse az IPv6-konfiguráció beállítását az állomáson. Alapértelmezés szerint egy IPv6 router hirdeti a saját IPv6-információit. Ez lehetővé teszi az állomás számára, hogy dinamikusan hozzon létre vagy szerezzen be IPv6-konfigurációt.

Amint az ábrán is látható az IPv6 GUA dinamikusan kiosztható állapottartó és állapotmentes szolgáltatások használatával.

Az ebben a fejezetben található állapottartó és állapotmentes módszerek mindegyike ICMPv6 RA üzeneteket használ, hogy ajánlatot küldjön az állomásnak az IPv6 konfiguráció megszerzésére vonatkozóan. Bár az operációs rendszerek követik az RA üzenet ajánlatát, a tényleges döntést végső soron az állomás hozza meg.

an inverted tree diagram starts with Dynamic GUA Assignment, splits into two: stateless and stateful. Stateless splits into SLAAC and SLAAC with DHCPv6 server and stateful leades to a DHCPv6 stateful server

**Dinamikus GUA címhozzárendelésÁllapotmentes**

* Egyetlen eszköz sem követi nyomon az IPv6-címek hozzárendelését.

**Állapottartó**

* A DHCPv6 server is managing the assignment of IPv6 addresses.

**Csak SLAAC**

* Router sends Router Advertisement (RA) messages providing all IPv6 addressing information (i.e., network prefix, prefix-length, and default gateway information).
* A állomások kizárólag az RA üzenet információit használják az összes címzési beállításhoz, beleértve a saját GUA létrehozását is.

**SLAAC DHCP-kiszolgálóval**  
**(Állapotmentes DHCPv6)**

* A router RA üzenetei információt szolgáltatnak az IPv6 konfigurációról az állomásoknak, és tájékoztatják őket, hogy további konfigurációs információért lépjenek kapcsolatba egy állapotmentes DHCPv6 kiszolgálóval.
* Az állomások az RA üzenet információit használják a saját egyedi GUA létrehozására és, hogy további információkat kapjanak a DHCPv6 szervertől.

**DHCPv6 kiszolgáló**  
**(Állapottartó DHCPv6)**

* A router RA üzenetei arról tájékoztatják az állomásokat, hogy az IPv6 konfigurációs adatok (az alapértelmezett átjáró címét kivéve) megszerzéséhez lépjenek kapcsolatba egy állapottartó DHCPv6-kiszolgálóval vagy DHCPv6-ot futtató routerrel.
* Az állomások felveszik a kapcsolatot egy DHCPv6-kiszolgálóval, hogy hozzájussanak az összes IPv6-címzési információhoz.
* Az állomás az alapértelmezett átjáró címéhez a router RA üzeneteiből jut hozzá.

8.1.4

## Az RA üzenetek három jelzőbitje

A kliens az RA üzenet beállításaitól függően dönti el, hogy milyen módon jusson hozzá az IPv6 globális egyedi címhez.

Az ICMPv6 RA üzenet három jelzőbitet tartalmaz, amelyek a következők szerint azonosítják az állomás számára elérhető dinamikus beállításokat:

* **A flag** - This is the Address Autoconfiguration flag. SLAAC használatával hozható létre az IPv6 globális egyedi cím.
* **O flag** - This is the Other Configuration flag. Egyéb információk az állapotmentes DHCPv6 szervertől érhetők el.
* **M flag** - This is the Managed Address Configuration flag. Állapottartó DHCPv6-szerver használatával állítható be az IPv6 GUA.

Az RA üzenetekben az A, O és M jelzőbitek különböző kombinációit használva megadhatók az állomás részére a rendelkezésre álló dinamikus címkiosztási lehetőségek.

Az ábra ezt a három módszert szemlélteti.

diagram shows R1 sending an RA message in response to an RS from PC1. The RA option fields can specify three different options: SLAAC only, stateless SLAAC with DHCPv6 server, and stateful DHCPv6 server only

R1 PC1

G0/0/1

ÜgyfélRS"Only use this RA."RA Options"I need an RA from R1."SLAAC Only (Default)"Use this RA and a DHCPv6 server."Stateless DHCP: SLAAC and DHCPv6"Use a DHCPv6 server."Stateful DHCPv6: DHCPv6 OnlyA flag=1O flag=0M flag=0A flag=1O flag=1M flag=0A flag=0M flag=1

8.1.5

## Tudáspróba - IPv6 GUA hozzárendelés

Az űrlap teteje

Check your understanding of IPv6 global unicast address assignment methods by choosing the BEST answer to the following questions.

1. Which address type is automatically created by default on a host interface when no RAs are received?

Az űrlap alja

Which method best describes stateless DHCP?

[8.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[SLAAC](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. SLAAC

# SLAAC

8.2.1

## A SLAAC áttekintése

Not every network has or needs access to a DHCPv6 server. Azonban egy IPv6 hálózat minden eszközének szüksége van globális egyedi címre. A SLAAC módszer lehetővé teszi az állomások számára, hogy létrehozzák saját IPv6 globális egyedi címüket DHCPv6-szerver nélkül.

A SLAAC egy állapotmentes szolgálatás. Ez azt jelenti, hogy nincs olyan kiszolgáló, amely a hálózati címadatok megőrzésével tudná, hogy mely IPv6-címek vannak használatban és melyek állnak rendelkezésre.

A SLAAC az ICMPv6 protokoll router keresés (RA) üzenet segítségével kínál címzési és egyéb konfigurációs adatokat, amelyeket normál esetben egy DHCP-szerver biztosítana. Az állomás az RA üzenetben kiküldött információk alapján állítja be a saját IPv6-címét. Egy IPv6 router 200 másodpercenként küld ki RA-üzeneteket.

Az állomás egy router keresés (RS) üzenet elküldésével is kérheti, hogy egy IPv6 router RA-üzenetet küldjön neki.

A SLAAC egymagában vagy DHCPv6-al kiegészítve alkalmazható.

8.2.2

## A SLAAC engedélyezése

A következő topológiában megtekinthetjük, hogy milyen módon van engedélyezve a SLAAC az állapotmentes dinamikus GUA kiosztáshoz.

shows a topology with a router connected to a switch connected to a host PC

PC1 R1 G0/0/1 fe80::1 2001:db8:acad:1::1/64

2001:db8:acad:1::/64

Tegyük fel, hogy R1 Gigabitethernet 0/0/1 interfésze a jelzett IPv6 GUA-val és link-local címekkel van konfigurálva. Kattintsunk az egyes gombokra, hogy ismertetőt kapjunk a SLAAC engedélyezéséről R1-en.

Az IPv6 minden-router csoport az FF02::2 csoportcímre küld választ. You can use the **show ipv6 interface** command to verify if a router is enabled as shown, in the output.

Az IPv6-os Cisco routerek minden 200. másodpercben kiküldik az RA üzeneteiket az IPv6 ff02::1 minden állomás csoportcímre.

R1# mutatja az ipv6 interfészt G0/0/1 | szakasz Csatlakozott Csatlakozott csoport címe(i): FF02::1 FF02::2 FF02::1:FF00:1 R1#

8.2.3

## A SLAAC kizárólagos használata

A **ipv6 unicast-routing** parancs használatakor a kizárólag SLAAC-ot használó módszer alapértelmezés szerint engedélyezve van. Ahogy az ábrán látható, az összes olyan Ethernet-interfész, amely IPv6 globális egyedi címmel van konfigurálva RA-üzeneteket küldésébe kezd, amelyekben az A jelzőbit 1-re, az O és M jelzőbitek pedig 0-ra vannak állítva.

Az **A = 1** jelzőbit azt javasolja a kliensnek, hogy saját IPv6 globális egyedi címet hozzon létre az RA-üzenetben hirdetett előtag használatával. Az ügyfél saját interfész azonosítót hozhat létre az EUI-64 (Extended Unique Identifier) módszerrel vagy véletlenszerű generálással.

Az **O =0** és **M=0**jelzőbitek arra utasítják a klienst, hogy kizárólag az RA-üzenet információit használja. Az RA-üzenet tartalmazza az előtagra, az előtag hosszára, a DNS-szerverre, az MTU-ra, valamint az alapértelmezett átjáróra vonatkozó adatokat. További információt DHCPv6-szervertől sem fog kapni.

diagram shows that with SLAAC only the router has the A flag set to 1 in the RA

R1 PC1 G0/0/1 fe80::1 2001:db8:acad:1::1/64

2001:db8:acad:1::/64

RA Message

| **Flag** | **value** |
| --- | --- |
| A | 1 |
| O | 0 |
| M | 0 |

A példában PC1-en engedélyezve van az IPv6-címzési információk automatikus beszerzése. Az A, O és M jelzőbitek értékei miatt PC1 csak a SLAAC-ot hajtja végre az R1 által küldött RA-üzenetben szereplő információk felhasználásával.

Az alapértelmezett átjáró címe az RA-üzenetben szereplő forrás IPv6-cím, amely az R1 link-local címe. Az alapértelmezett átjáró címe csak az RA-üzenetből érhető el automatikusan. A DHCPv6-kiszolgáló ezt az információt nem szolgáltatja.

C:\PC1> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c

Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21

IPv4 Address. . . . . . . . . . . : 169.254.202.140

Subnet Mask . . . . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . . . : fe80::1%21

C:\PC1>

8.2.4

## ICMPv6 RS üzenetek

A router 200 másodpercenként küld ki RA-üzeneteket. Viszont akkor is küld RA-üzenetet, ha RS-üzenetet kap egy állomástól.

Ha egy kliens úgy van beállítva, hogy a címzési adatait automatikusan kapja meg, akkor egy RS-üzenetet küld az IPv6 ff02::2 minden-router csoportcímre.

Az ábra azt szemlélteti, hogy az állomás miként kezdeményezi a SLAAC módszert.

show the PC sending an RS message to the all routers multicast address and getting an RA in response

1 2 PC1 R1 G0/0/1 fe80::1 2001:db8:acad:1::1/64

2001:db8:acad:1::/64

RA MessageRS Message

1. A PC1 éppen elindult, és még nem kapott RA üzenetet. Ezért RS üzenetet küld az IPv6 ff02::2 minden router csoportcímre amelyben RA-t kér.
2. R1 tagja az IPv6 minden router csoportnak és megkapja az RS üzenetet. Előállítja a helyi hálózati előtagot és az előtag hosszát tartalmazó RA-t (pl. 2001:db8:acad:1::/64) Majd elküldi az RA-üzenetet az IPv6 minden állomás csoportcímre (ff02::1). PC1 ezt az információt használja fel az egyedi IPv6 GUA létrehozásához.

8.2.5

## Interfész azonosító előállításának folyamata az állomáson

SLAAC használatakor az állomás az IPv6 alhálózat 64 bites adatait általában a router RA-üzenetéből állapítja meg. Azonban a fennmaradó 64 bites interfész azonosítót (ID) két módszer egyikével kell létrehoznia:

* **Randomly generated** - The 64-bit interface ID is randomly generated by the client operating system. Ezt a módszert használják a Windows 10 állomások.
* **EUI-64** - The host creates an interface ID using its 48-bit MAC address. A gazdagép beszúrja az fffe hexadecimális értékét a cím közepére, és megfordítja az interfészazonosító hetedik bitjét. Ez megváltoztatja az interfészazonosító második hexadecimális számjegyének értékét. Egyes operációs rendszerek adatvédelmi problémák miatt az EUI-64 módszer helyett véletlenszerűen generált interfész azonosítót használnak. Ennek az az oka, hogy az EUI-64 az állomás Ethernet MAC-címét használja az interfész azonosító létrehozásához.

**Note**: Windows, Linux, and Mac OS allow for the user to modify the generation of the interface ID to be either randomly generated or to use EUI-64.

Például a következő **ipconfig** parancskimeneten kiemelve látható, hogy a Windows 10-et futtató PC1 állomás az R1-től érkezett RA-üzenetben található IPv6 alhálózati információkat használta, és véletlenszerű 64 bites interfészazonosítót generált.

C:\PC1> **ipconfig**

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c

Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21

IPv4 Address. . . . . . . . . . . : 169.254.202.140

Subnet Mask . . . . . . . . . . . : 255.255.0.0

Default Gateway . . . . . . . . . : fe80::1%6

C:\PC1>

8.2.6

## Duplikált cím felderítés

A fenti folyamat lehetővé teszi az állomásnak, hogy létrehozzon egy IPv6-címet. Azonban arra nincs garancia, hogy a cím egyedi a hálózaton.

A SLAAC egy állapotmentes folyamat, ezért az állomásnak lehetősége van ellenőrizni az újonnan létrehozott IPv6-cím egyediségét, mielőtt használatba vehetné azt. A duplikált cím felderítés (Duplicate Address Detection, DAD) folyamatot arra használja egy állomás, hogy megbizonyosodjon az IPv6 globális egyedi címe egyediségéről.

A DAD az ICMPv6 használatával valósul meg. A végrehajtásához az állomás egy ICMPv6 szomszéd keresés (NS) üzenetet küld egy speciálisan kialakított multicast címre, amelyet solicited-node csoportcímnek hívnak. Ez a cím átmásolja az állomás IPv6-címének utolsó 24 bitjét.

Ha semmilyen másik eszköz nem válaszol egy szomszéd hirdetés (NA) üzenettel, akkor a cím virtuálisan egyedinek minősíthető és PC1 használatba veheti. Ha egy NA üzenet érkezik válaszként PC1-nek, akkor a cím nem egyedi, így az operációs rendszernek kell meghatároznia az új interfészazonosítót.

Az IETF (Internet Engineering Task Force) azt ajánlja, hogy DAD-ot végezze el az állomás minden IPv6 egyedi cím esetén, függetlenül attól, hogy azt kizárólag SLAAC használatával hozták létre, állapottartó DHCPv6 használatával vagy kézzel konfigurálva. A DAD ettől még nem kötelező, mert a 64 bites interfész azonosító 18 kvintillió lehetőséget biztosít és kicsi a duplikáció esélye. Azonban a legtöbb operációs rendszer minden IPv6 unicast címen elvégzi a DAD műveletet függetlenül attól, hogy a cím hogyan van konfigurálva.

8.2.7

## Tudáspróba - SLAAC

Az űrlap teteje

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

1. Which two ICMPv6 messages are used in the SLAAC process? (Choose two.)

Az űrlap alja

Which command must be configured on a router to enable it to join the IPv6 all-routers multicast address ff02::2?

What are the flag settings when a host should use the SLAAC only option?

Which ICMPv6 message is sent by a host in an attempt to locate an online IPv6enabled router to obtain IPv6 addressing information?

What method is used by a host to verify an IPv6 address is unique on the local network before assigning that address to an interface?

[8.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IPv6 GUA hozzárendelés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. DHCPv6

# DHCPv6

8.3.1

## A DHCPv6 működésének lépései

Ez a témakör az állapotmentes és állapottartó DHCPv6-ot ismerteti. Az állapotmentes DHCPv6 a SLAAC egyes részeit használja annak biztosítására, hogy az összes szükséges információ eljusson az állomáshoz. Az állapottartó DHCPv6 nem igényel SLAAC-ot.

Habár a DHCPv6 a kínált szolgáltatások tekintetében sokban hasonlít a DHCPv4-hez, a két protokoll egymástól teljesen független.

**Note**: DHCPv6 is defined in RFC 3315.

Az eszköz DHCPv6 kliens/szerver kommunikációt kezdeményez, ha az RA-üzenet állapotmentes vagy állapottartó DHCPv6-ot ír elő.

A kiszolgáló kliensnek küldött DHCPv6 üzenetei az 546-os UDP célportot, míg a kliens DHCPv6-kiszolgálónak küldött üzenetei az 547-es UDP célportot használják.

A DHCPv6 működésének lépései a következők:

1. Az állomás RS-üzenetet küld.
2. A router RA-üzenettel válaszol.
3. Az állomás DHCPv6 SOLICIT üzenetet küld.
4. A DHCPv6-kiszolgáló egy ADVERTISE üzenettel válaszol.
5. Az állomás választ küld a DHCPv6-kiszolgálónak.
6. A DHCPv6-kiszolgáló REPLY üzenetet küld.

A DHCPv6 működési lépéseinek magyarázatáért és illusztrációjáért kattintsunk az egyes gombokra.

**Step 1. Host sends an RS message.**

PC1 sends an RS message to all IPv6-enabled routers.

R1 PC1 G0/0/1

1

SLAAC OperationsRouter SolicitationDHCPv6 Server

8.3.2

## Az állapotmentes DHCPv6 működése

Az állapot nélküli DHCPv6-kiszolgáló csak olyan információkat szolgáltat, amelyek azonosak a hálózaton lévő összes eszközről, például egy DNS-kiszolgáló IPv6-címét.

Ezt a folyamatot állapotmentes DHCPv6-nak nevezzük, mivel a szerver semmilyen, a kliens állapotára vonatkozó információt (pl.: a kiosztott és a még rendelkezésre álló IPv6-címek listáját) nem tart karban. Az állapotmentes DHCPv6-szerver kizárólag konfigurációs beállításokat kínál a kliensek számára, IPv6-címet nem.

Az ábra az állapotmentes DHCPv6 működését szemlélteti.

shows a diagram in which the PC gets its stateless DHCPv6 server information from router R1

2001:db8:acad:1::1/64 fe80::1 G0/0/1 1 2 R1

PC1

|  |  |
| --- | --- |
| **Flag** | **Value** |
| A | 1 |
| O | 1 |
| M | 0 |

Stateless DHCPv6 ServerRA Message

1. PC1 egy állapotmentes DHCP RA-üzenetet kap. Az RA-üzenet tartalmazza a hálózati előtagot és az előtag hosszát. Az állapottartó DHCP M jelzőbitje az alapértelmezett 0 értékre van állítva. Az A=1 jelzőbit érték jelzi a kliensnek, hogy használjon SLAAC-ot. Az O=1 jelzőbit érték tudatja a klienssel, hogy további konfigurációs beállítások állnak rendelkezésre egy állapotmentes DHCPv6-szerveren.
2. A kliens DHCPv6 SOLICIT üzenetet küld, amely egy állapotmentes DHCPv6-szervert keres további információk (pl. DNS-kiszolgálócímek) megszerzéséhez.

8.3.3

## Állapotmentes DHCPv6 engedélyezése egy interfészen

Az állapotmentes DHCPv6 engedélyezése egy router interfészen az **ipv6 nd other-config-flag** interfész konfigurációs paranccsal lehetséges. Ez 1-re állítja az O jelzőbit értékét.

A parancskimenet kiemelt részén látható, hogy az RA-üzenet közli a fogadó állomásokkal, hogy használjanak állapotmentes automatikus konfigurációt (A = 1), és lépjenek kapcsolatba egy DHCPv6-szerverrel további konfigurációs információkért (O = 1).

**Note:** You can use the **no ipv6 nd other-config-flag** to reset the interface to the default SLAAC only option (O flag = 0).

R1(config-if)# **ipv6 nd other-config-flag**

R1(config-if)# **end**

R1#

R1# **show ipv6 interface g0/0/1 | begin ND**

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

Hosts use DHCP to obtain other configuration.

R1#

8.3.4

## Az állapottartó DHCPv6 működése

Ez a lehetőség hasonlít legjobban a DHCPv4-hez. Ebben az esetben az RA-üzenet azt jelzi az ügyfélnek, hogy szerezzen be minden címzési információt egy állapottartó DHCPv6-szervertől, az alapértelmezett átjáró címének kivételével, amely az RA-üzenetben található forrás-IPv6 link-local cím.

Ezt állapottartó DHCPv6-nak nevezzük, mivel a DHCPv6-szerver tartja karban az IPv6-os állapotinformációkat. Ez hasonlít arra, ahogy a DHCPv4-szerver osztja ki az IPv4-címeket.

Az ábra az állapottartó DHCPv6 működését szemlélteti.

shows a diagram with a stateful DHCPv6 server, connected to a switch, connected to a client PC and a DHCPv6 client router

2001:db8:acad:1::1/64 fe80::1 G0/0/1 1 2 R1

PC1

|  |  |
| --- | --- |
| **Flag** | **Value** |
| A | 0 |
| O | 0 |
| M | 1 |

Stateful DHCPv6 ServerRA Message

1. PC1 DHCPv6 RA-üzenetet kap, amelyben az O jelzőbit 0-ra, az M jelzőbit pedig 1-re van állítva, ez jelzi PC1-nek, hogy az összes IPv6-címzési információt egy állapottartó DHCPv6-szervertől fogja megkapni.
2. PC1 egy DHCPv6 SOLICIT üzenet elküldésével keres állapottartó DHCPv6-kiszolgálót.

**Note**: If A=1 and M=1, some operating systems such as Windows will create an IPv6 address using SLAAC and obtain a different address from the stateful DHCPv6 server. A legtöbb esetben ajánlott manuálisan beállítani az A jelzőbitet 0-ra.

8.3.5

## Állapottartó DHCPv6 engedélyezése interfészen

Az állapottartó DHCPv6 az **ipv6 nd managed-config-flag** interfész konfigurációs paranccsal engedélyezhető egy router interfészen. Ez 1-re állítja az M jelzőbit értékét. Az interfész parancs letiltja a SLAAC-t az A jelző 0-ra állításával.**ipv6 nd prefix default no-autoconfig**

A példa parancskimenetében kiemelve látható, hogy az RA-üzenet értesíti az állomást, hogy minden IPv6 konfigurációs információt egy DHCPv6-kiszolgálótól szerezzen be (M = 1).

R1(config)# **int g0/0/1**

R1(config-if)# **ipv6 nd managed-config-flag**

R1(config-if)# **ipv6 nd prefix default no-autoconfig**

R1(config-if)# **end**

R1#

R1# **show ipv6 interface g0/0/1 | begin ND**

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds (using 30000)

ND advertised reachable time is 0 (unspecified)

ND advertised retransmit interval is 0 (unspecified)

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

ND advertised default router preference is Medium

Hosts use DHCP to obtain routable addresses.

R1#

8.3.6

## Tudáspróba - DHCPv6

Az űrlap teteje

Check your understanding of DHCPv6 by choosing the BEST answer to the following questions.

1. What UDP port do DHCPv6 clients use to send DHCPv6 messages?

Az űrlap alja

What DHCPv6 message does a host send to look for a DHCPv6 server?

What DHCPv6 message does a host send to the DHCPv6 server if it is using stateful DHCPv6?

What flag settings combination is used for stateless DHCP?

What M flag setting indicates that stateful DHCPv6 is used?

[8.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[SLAAC](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv6-kiszolgáló konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. DHCPv6-kiszolgáló konfigurálása

# DHCPv6-kiszolgáló konfigurálása

8.4.1

## DHCPv6 router szerepek

A Cisco IOS routerek nagy teljesítményű eszközök. Kisebb hálózatokban nem szükségesek külön eszközök ahhoz, hogy DHCPv6-kiszolgálóval, ügyféllel vagy DHCP-közvetítővel rendelkezzünk. Egy Cisco IOS router konfigurálható DHCPv6-szerver működésre.

Vagyis beállítható úgy, hogy az alábbiak egyike legyen:

* **DHCPv6 Server** - Router provides stateless or stateful DHCPv6 services.
* **DHCPv6 Client** - Router interface acquires an IPv6 IP configuration from a DHCPv6 server.
* **DHCPv6 Relay Agent** - Router provides DHCPv6 forwarding services when the client and the server are located on different networks.

8.4.2

## Állapotmentes DHCPv6-szerver konfigurálása

Állapotmentes DHCPv6-szerver opció esetén a router az IPv6-hálózat címzési információit RA-üzenetekben hirdeti. Az ügyfélnek azonban további információért egy DHCPv6-kiszolgálóval kell kapcsolatba lépnie.

A minta topológiáról megismerhetjük az állapotmentes DHCPv6-kiszolgáló konfigurálásának módját.

shows a diagram in which a client router gets its stateless DHCPv6 server information from router R1

G0/0/1 G0/0/1 fe80::1 2001:db8:acad:1::1/64 R1 R3

PC1

Stateless DHCPv6 ServerÜgyfél

Ebben a példában R1 SLAAC-szolgáltatásokat nyújt az állomás IPv6-konfigurációjához és a DHCPv6-szolgáltatásokhoz.

Öt lépésben konfigurálhatjuk és ellenőrizhetjük a routert állapotmentes DHCPv6 kiszolgálóként.

**Step 1**. Engedélyezzük az IPv6-forgalomirányítást. **Step 2**. Adjuk meg a DHCPv6-készlet nevét. **Step 3**. Állítsuk be a DHCPv6 készletet. **Step 4**. Csatoljuk a DHCPv6-készletet egy interfészhez. **Step 5**. Ellenőrizzük, hogy az állomások megkapták-e az IPv6-címzési információkat.

Kattintsunk az egyes gombokra a lépésekhez tartozó példák megtekintéséhez.

**Step 1. Enable IPv6 routing.**

The **ipv6 unicast-routing** command is required to enable IPv6 routing. Ez nem szükséges ahhoz, hogy a router állapottartó DHCPv6-szerver legyen, viszont az ICMPv6 RA-üzenetek küldéséhez nélkülözhetetlen.

R1(config)# **ipv6 unicast-routing**

R1(config)#

8.4.3

## Állapotmentes DHCPv6-kliens konfigurálása

A router DHCPv6-kliens is lehet és IPv6-konfigurációt kaphat egy DHCPv6-kiszolgálótól, például egy DHCPv6-kiszolgálóként működő routertől. Az ábrán R1 egy állapotmentes DHCPv6-szerver.

G0/0/1 G0/0/1 fe80::1 2001:db8:acad:1::1/64 R1 R3

PC1

Stateless DHCPv6 ServerÜgyfél

There are five steps to configure and verify a router as a stateless DHCPv6 client.

**Step 1**. Engedélyezzük az IPv6-forgalomirányítást. **Step 2**. Állítsuk be a kliens routert LLA létrehozásához. **Step 3**. Állítsuk be a kliens routert SLAAC használatára. **Step 4**. Győződjünk meg arról, hogy az routerhez hozzá lett rendelve GUA. **Step 5**. Ellenőrizzük, hogy a kliens router megkapta-e a szükséges DHCPv6-információkat.

Kattintsunk az egyes gombokra a lépésekhez tartozó példák megtekintéséhez.

**Step 1. Engedélyezze az IPv6-útválasztást.** A DHCPv6-kliens útválasztónak engedélyeznie kell az **ipv6 unicast-routing** funkciót.

R3(config)# ipv6 unicast-routing R3(config)#

8.4.4

## Állapottartó DHCPv6-kiszolgáló konfigurálása

Az állapottartó DHCP-kiszolgáló opcióhoz az kell, hogy az IPv6 router utasítsa az állomást a kapcsolat felvételére egy DHCPv6-kiszolgálóval az összes szükséges IPv6-hálózati címzési információ beszerzése érdekében.

Az ábrán R1 állapottartó DHCPv6 szolgáltatásokat nyújt a helyi hálózat minden állomásának. Egy állapottartó DHCPv6-szerver beállítása nem sokban különbözik egy állapotmentes szerver beállításától. A legjelentősebb eltérés az, hogy egy állapottartó DHCPv6-szerver IPv6-címadatokat is tartalmaza a DHCPv4-szerverekhez hasonlóan.

R1 R3 PC1 G0/0/1 fe80::1 2001:db8:acad:1::1/64

G0/0/1

Stateful DHCPv6 ServerDHCPv6 Client

There are five steps to configure and verify a router as a stateful DHCPv6 server:

**Step 1**. Engedélyezzük az IPv6-forgalomirányítást. **Step 2**. Adjuk meg a DHCPv6-készlet nevét. **Step 3**. Állítsuk be a DHCPv6 készletet. **Step 4**. Csatoljuk a DHCPv6-készletet egy interfészhez. **Step 5**. Ellenőrizzük, hogy az állomások megkapták-e az IPv6-címzési információkat.

Kattintsunk az egyes gombokra a lépésekhez tartozó példák megtekintéséhez.

**Step 1. Enable IPv6 routing.**

The **ipv6 unicast-routing** command is required to enable IPv6 routing.

R1(config)# **ipv6 unicast-routing**

R1(config)#

8.4.5

## Állapottartó DHCPv6-kliens konfigurálása

Egy router DHCPv6 kliens is lehet. A kliens routeren az **ipv6 unicast-routing** paranccsal engedélyezni kell az IPv6-forgalomirányítást, valamint a routernek IPv6-link-local címmel kell rendelkeznie az IPv6 üzenetek küldéséhez és fogadásához.

A minta topológiáról megismerhetjük az állapottartó DHCPv6-kliens konfigurálásának módját.

PC1 R3 2001:db8:acad:1::1/64fe80::1 G0/0/1 G0/0/1

R1

Stateful DHCPv6 ServerDHCPv6  
Client

There are five steps to configure and verify a router as a stateful DHCPv6 client.

**Step 1**. Engedélyezzük az IPv6-forgalomirányítást. **Step 2**. Állítsuk be a kliens routert LLA létrehozásához. **Step 3**. Állítsuk be a kliens routert DHCPv6 használatára. **Step 4**. Győződjünk meg arról, hogy az routerhez hozzá lett rendelve GUA. **Step 5**. Ellenőrizzük, hogy a kliens router megkapta-e a szükséges DHCPv6-információkat.

Kattintsunk az egyes gombokra a lépésekhez tartozó példák megtekintéséhez.

**Step 1. Enable IPv6 routing.**

The DHCPv6 client router needs to have **ipv6 unicast-routing** enabled.

R3(config)# **ipv6 unicast-routing**

R3(config)#

8.4.6

## DHCPv6-kiszolgáló ellenőrzésének parancsai

A **show ipv6 dhcp pool** és **show ipv6 dhcp binding** parancsok segítségével ellenőrizhetjük a DHCPv6 működését egy routeren.

Kattintsunk az egyes gombokra a parancsok példakimenetének megtekintéséhez.

Use the **show ipv6 dhcp binding** command output to display the IPv6 link-local address of the client and the global unicast address assigned by the server.

A parancskimenet R1 aktuális állapottartó címbérleteit jeleníti meg. Az első kliens PC1, a második pedig R3.

Ezen adatokat egy állapottartó DHCPv6-szerver tartja karban. Egy állapotmentes DHCPv6-kiszolgáló nem őrizné meg ezt az információt.

R1# ipv6 dhcp kötés megjelenítése Kliens: FE80::192F:6FBC:9DB:B749 DUID: 0001000125148183005056B327D6 Felhasználónév : hozzárendeletlen VRF : alapértelmezett IA NA: IA NA: IA azonosító 0x23091:2AC01:2AC091:2AC091:2AC091:2AC091:2AC091:2AC091:2AC091:2AC091:2AC091:2AC091:2AC01:22090 :FD28:9D79:9E42 előnyben részesített élettartam 86400, érvényes élettartam 172800 lejár: 2019. szeptember 27. 09:10 (171192 másodperc) Kliens: FE80::2FC:BAFF:FE94:29B1 Alapértelmezett felhasználói név univerzális név: FE94:29B1 Username un VBANAIAB0:090100 IA ID 0x00060001, T1 43200, T2 69120 Cím: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C előnyben részesített élettartam 86400, érvényes élettartam 172800 lejár: szeptember 27 19s219219219

8.4.7

## DHCPv6-közvetítő beállítása

Ha a DHCPv6-szerver és a kliens eltérő hálózaton vannak, akkor az IPv6-forgalomirányítót beállíthatjuk DHCPv6-közvetítőként. Egy DHCPv6-közvetítő beállítása nem sokban különbözik egy IPv4-forgalomirányító DHCPv4-közvetítőként történő beállításától.

Az ábrán R3 állapottartó DHCPv6-kiszolgálóként van konfigurálva. PC1 a 2001:db8:acad:2::/64 hálózaton található és az IPv6-konfiguráció megszerzéséhez egy állapottartó DHCPv6-kiszolgáló szolgáltatásaira van szüksége. R1-et DHCPv6-közvetítőként kell konfigurálni.

PC1 R1 R3 2001:db8:acad:2::/64 2001:db8:acad:1::/64 :1fe80::1 :1fe80::1 :2fe80::3 G0/0/1 G0/0/0

G0/0/0

DHCPv6  
ClientDHCPv6  
Relay AgentStateful DHCPv6  
Server

A router DHCPv6-közvetítőként történő konfigurálásának parancs szintaxisa a következő:

Router(config-if)# **ipv6 dhcp relay destination** ipv6-address [interface-type interface-number]

Ahogy az ábrán is látható a parancs a DHCPv6-kliensekhez kapcsolódó interfészen van konfigurálva, és megadja a DHCPv6-kiszolgáló címét, valamint a kiszolgáló eléréséhez szükséges kimenő interfészt. Kimenő interfész csak akkor szükséges, ha a következő ugrás címe link-local cím.

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0**

R1(config-if)# **exit**

R1(config)#

8.4.8

## DHCPv6-közvetítő ellenőrzése

A DHCPv6-közvetítő működését a **show ipv6 dhcp interface** és a **show ipv6 dhcp binding** parancsokkal ellenőrizhetjük. Az **ipconfig /all** paranccsal pedig azt, hogy a Windows állomások megkapták-e az IPv6-címzési információkat.

Kattintsunk az egyes gombokra a parancsok példakimenetének megtekintéséhez.

On R3, use the **show ipv6 dhcp binding command** to verify if any hosts have been assigned an IPv6 configuration.

Figyeljük meg, hogy az adott link-local című klienshez egy IPv6 GUA lett hozzárendelve. Feltételezhetjük, hogy ez PC1.

R3# ipv6 dhcp kötés megjelenítése Kliens: FE80::5C43:EE7C:2959:DA68 DUID: 0001000124F5CEA2005056B3636D Felhasználónév : hozzárendeletlen VRF : alapértelmezett IA NA : IA NA: DBC0,2AC01,2AC03:2AC01,2AC03:2AC01,2AC091,2AC091,2AC091,2AC091,2AC091,2AC091,2AC091,2AC091:2AC091:2AC091:2AC09 :64DE:AADA:7857 preferált élettartam 86400, érvényes élettartam 172800 lejár: 2019. szeptember 29. 20:26 (172710 másodperc) R3#

8.4.9

## Tudáspróba - DHCPv6-kiszolgáló konfigurálása

Az űrlap teteje

Check your understanding of DHCPv6 server configuration by choosing the BEST answer to the following questions.

1. Which three DHCPv6 roles can a router perform? (Choose all that apply.)

Az űrlap alja

Which command is not configured in stateless DHCPv6?

An IPv6-enabled router is to acquire its IPv6 GUA from another IPv6 router using SLAAC. Which interface configuration command should be configured on the client router?

A router is to provide DHCPv6 server services. Which command should be configured on the client facing interface?

An IPv6-enabled router is to acquire its IPv6 GUA from a DHCPv6 server. Which interface configuration command should be configured on client router?

Which DHCPv6 verification command would display the link-local and GUA assigned address for each active client?

Which command is configured on the client LAN interface of the DHCPv6 relay agent?

[8.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[8.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. SLAAC and DHCPv6
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

8.5.1

## Laborgyakorlat - DHCPv6 konfigurálása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: SLAAC-cím hozzárendelésének ellenőrzése R1-ről
* Part 3: Állapotmentes DHCPv6-kiszolgáló konfigurálása és ellenőrzése R1-en
* Part 4: Állapottartó DHCPv6-kiszolgáló konfigurálása és ellenőrzése R1-en
* Part 5: DHCPv6-közvetítő konfigurálása és ellenőrzése R2-n

8.5.2

## Miről tanultunk ebben a fejezetben?

**IPv6 GUA Assignment**

Egy routeren az IPv6 globális egyedi címek (GUA) az **ipv6 address** ipv6-address/prefix-length interfész konfigurációs paranccsal állíthatók be manuálisan. Ha automatikus IPv6-címzés van kiválasztva az állomás megpróbálja automatikusan megszerezni és beállítani az IPv6-címadatokat az interfészen. Az állomás automatikusan létrehozza az IPv6 link-local címet az elindulásakor, amikor az Ethernet interfész aktívvá válik. Alapértelmezés szerint az IPv6-router hirdeti az IPv6-adatait, amely lehetővé teszi az állomás számára, hogy dinamikusan létrehozza vagy beszerezze az IPv6-konfigurációját. Az IPv6 GUA dinamikusan kiosztható állapottartó és állapotmentes szolgáltatások használatával. A kliens az RA-üzenet beállításaitól függően dönti el, hogy milyen módon jusson hozzá az IPv6 globális egyedi címhez. Az ICMPv6 RA-üzenet három jelzőbitet tartalmaz, amelyek az állomás számára elérhető dinamikus beállításokat azonosítják:

* **A flag** – This is the Address Autoconfiguration flag. IPv6 GUA létrehozásához használjunk SLAAC-ot.
* **O jelzőbit** - Egyéb (Other) beállításokat jelző bit. Egyéb információk az állapotmentes DHCPv6-szervertől érhetők el.
* **M flag** – This is the Managed Address Configuration flag. Állapottartó DHCPv6-szerver használatával állítható be az IPv6 GUA.

**SLAAC**

A SLAAC módszer lehetővé teszi az állomások számára, hogy létrehozzák saját IPv6 globális egyedi címüket DHCPv6-szerver nélkül. A SLAAC, amely egy állapotmentes szolgáltatás, az ICMPv6 protokoll router keresés (RA) üzenet segítségével kínál címzési és egyéb konfigurációs adatokat, amelyeket normál esetben egy DHCP-szerver biztosítana. A SLAAC önállóan vagy DHCPv6-al kiegészítve alkalmazható. Ahhoz, hogy az RA-üzenetek küldése engedélyezve legyen a routernek csatlakoznia kell az IPv6 minden-router csoporthoz a **ipv6 unicast-routing** globális konfigurációs parancs használatával. A **show ipv6 interface** paranccsal ellenőrizhetjük, hogy ez engedélyezve van-e a routeren. Az ipv6 unicast-routing parancs használatakor a SLAAC módszer alapértelmezés szerint engedélyezve van. Az összes olyan Ethernet-interfész, amely IPv6 globális egyedi címmel van konfigurálva RA-üzeneteket küldésébe kezd, amelyekben az A jelzőbit 1-re, az O és M jelzőbitek pedig 0-ra vannak állítva. Az A = 1 jelzőbit azt javasolja a kliensnek, hogy saját IPv6 globális egyedi címet hozzon létre az RA-üzenetben hirdetett előtag használatával. Az O = 0 és M = 0 jelzőbitek pedig arra utasítják a klienst, hogy kizárólag az RA-üzenet információit használja. A router 200 másodpercenként küld ki RA-üzeneteket. Viszont akkor is küld RA-üzenetet, ha RS-üzenetet kap egy állomástól. SLAAC használatakor az állomás az IPv6 alhálózat 64 bites adatait általában a router RA-üzenetéből állapítja meg. Azonban a fennmaradó 64 bites interfész azonosítót (ID) két módszer egyikével kell létrehoznia: véletlenszerűen generált vagy EUI-64. A DAD (duplikált cím felderítés) folyamatot arra használja egy állomás, hogy megbizonyosodjon az IPv6 globális egyedi címe egyediségéről. A DAD az ICMPv6 használatával valósul meg. A végrehajtásához az állomás egy ICMPv6 NS (szomszéd hirdetés) üzenetet küld egy speciálisan kialakított multicast címre, amelyet solicited-node csoportcímnek hívnak. Ez a cím megduplázza az állomás IPv6-címének utolsó 24 bitjét.

**DHCPv6**

Az eszköz DHCPv6 kliens/szerver kommunikációt kezdeményez, ha az RA-üzenet állapotmentes vagy állapottartó DHCPv6-ot jelez. A kiszolgáló kliensnek küldött DHCPv6 üzenetei az 546-os UDP célportot, míg a kliens DHCPv6-kiszolgálónak küldött üzenetei az 547-es UDP célportot használják. Az állapotmentes DHCPv6 opció értesíti a klienst, hogy az RA-üzenet információit kell használnia a címzéshez, de a többi konfigurációs beállítást a DHCPv6-szerver bocsátja a rendelkezésére. Ez az úgynevezett állapotmentes DHCPv6, mert a kiszolgáló nem tart fenn semmilyen ügyfélállapot-információt. Az állapotmentes DHCPv6 engedélyezése egy router interfészen az **ipv6 nd other-config-flag** interfész konfigurációs paranccsal lehetséges. Ez 1-re állítja az O jelzőbit értékét. Állapottartó DHCPv6 esetén az RA-üzenet azt jelzi az ügyfélnek, hogy szerezzen be minden címzési információt egy állapottartó DHCPv6-szervertől, az alapértelmezett átjáró címének kivételével, amely az RA-üzenetben található forrás-IPv6 link-local cím. Ezt állapottartó módszernek nevezzük, mivel a DHCPv6-szerver tartja karban az IPv6-os állapotinformációkat. Az állapottartó DHCPv6 az **ipv6 nd managed-config-flag** interfész konfigurációs paranccsal engedélyezhető egy router interfészen. Ez 1-re állítja az M jelzőbit értékét.

**Configure DHCPv6 Server**

Egy Cisco IOS router konfigurálható úgy, hogy DHCPv6-kiszolgáló szolgáltatásokat nyújtson a következő három típus egyikében: DHCPv6-kiszolgáló, DHCPv6-ügyfél vagy DHCPv6-közvetítő. Állapotmentes DHCPv6-szerver opció esetén a router az IPv6-hálózat címzési információit RA-üzenetekben hirdeti. A router DHCPv6-kliens is lehet és IPv6-konfigurációt kaphat egy DHCPv6-kiszolgálótól. Az állapottartó DHCP-kiszolgáló opció előírja, hogy az IPv6-router utasítsa az állomást a kapcsolat felvételére egy DHCPv6-kiszolgálóval az összes szükséges IPv6-hálózati címzési információ beszerzése érdekében. Ahhoz, hogy a kliens router DHCPv6-router lehessen a **have ipv6 unicast-routing** paranccsal engedélyezni kell az IPv6-forgalomirányítást, valamint a routernek IPv6-link-local címmel kell rendelkeznie az IPv6 üzenetek küldéséhez és fogadásához. A **show ipv6 dhcp pool** és **show ipv6 dhcp binding** parancsok segítségével ellenőrizhetjük a DHCPv6 működését egy routeren. Ha a DHCPv6-szerver és a kliens eltérő hálózaton vannak, akkor az IPv6-forgalomirányítót beállíthatjuk DHCPv6-közvetítőként az **ipv6 dhcp relay destination** ipv6-address [interface-type interface-number] paranccsal. A parancs a DHCPv6-kliensekhez kapcsolódó interfészen van kiadva, és megadja a DHCPv6-kiszolgáló címét, valamint a kiszolgáló eléréséhez szükséges kimenő interfészt. Kimenő interfész csak akkor szükséges, ha a következő ugrás címe link-local cím. A DHCPv6-közvetítő működését a **show ipv6 dhcp interface** és a **show ipv6 dhcp binding** parancsokkal ellenőrizhetjük.

8.5.3

## Ellenőrző kvíz - SLAAC és DHCPv6

Az űrlap teteje

1. Hogyan győződik meg az IPv6-kliens a saját címe egyediségéről, miután az IPv6-címét SLAAC módszerrel állította be?

Az űrlap alja

Egy IPv6-állomás melyik módszert alkalmazza az alapértelmezett átjáró címének SLAAC használatával történő megismerésére?

Milyen két módszerrel hozható létre interfészazonosító egy SLAAC-ot használó IPv6-állomáson? (Két jó válasz van.)

Egy kliens állapotmentes automatikus címkonfigurációt (SLAAC) használ egy interfész IPv6-címzésére. A cím generálása és interfészhez rendelése után mit kell a kliensnek tenni, mielőtt használatba venné ezt az IPv6-címet?

Melyik parancsot kell kiadni egy router interfészén ahhoz, hogy az eszközt állapottartó DHCPv6-kliensként állítsuk be?

Milyen üzenet tájékoztatja az IPv6-interfészeket arról, hogy használjanak állapottartó DHCPv6-ot az IPv6-cím megszerzéséhez?

Melyik cél IP-cím van abban az üzenetben, amelyben egy IPv6-állomás DHCPv6 SOLICIT-üzenetet küld DHCPv6-kiszolgáló kereséséhez?

A DHCPv6 melyik megoldása esetén nyújt egy router dinamikus IPv6-konfigurációs információkat az állomásoknak?

Egy vállalat állapotmentes DHCPv6-módszerrel ad IPv6-címeket a dolgozói munkaállomásoknak. Miután az állomás több DHCPv6-szervertől is kapott a szolgáltatás elérhetőségére vonatkozó értesítést, milyen üzenetet küld a szervernek a konfigurációs információk megszerzése céljából?

Az ICMPv6 melyik eljárását használja az állomás annak ellenőrzésére, hogy egy interfészen használni kívánt cím egyedi-e?

Melyik két jellemző vonatkozik az IPv6-cím konfiguráláshoz használt SLAAC módszerre? (Két jó válasz van.)

Egy kliens indulást követően egy ICMPv6 RA üzenetet kap, amelyben az M jelzőbit értéke 0, az O jelzőbité pedig 1. Mit jelent ez?

A network administrator is entering the command **ipv6 unicast-routing** to start configuring DHCPv6 operation on a router. Melyik állítás jellemzi helyesen a parancs funkcióját?

[8.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCPv6-kiszolgáló konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[9.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. FHRP Concepts
2. Bevezetés

# Bevezetés

9.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az FHRP alapjairól szóló fejezetben!

A hálózatunk működőképes. Elértük a 2. rétegbeli redundanciát hurkok létrejötte nélkül. Minden eszköz dinamikusan kapja meg a címét. Nagyon jók vagyunk a hálózat konfigurálásában! De várjunk csak. Az egyik router, ami történetesen az alapértelmezett átjárónk, leállt. Egyik állomás sem küldhet üzenetet a közvetlen hálózatán kívülre. Eltart egy ideig, amíg újra működni fog ez az alapértelmezett átjárót biztosító router. Egy csomó dühös ember jön megkérdezni, hogy milyen hamar lesz kész a hálózat.

Ezt a problémát könnyen elkerülhetjük. Az "első ugrás", vagyis az alapértelmeztt átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols, FHRP) adják azt a megoldást, amire szükségünk van. Ez a fejezet az FHRP működését és a rendelkezésre álló összes FHRP-típust tárgyalja. Az egyik ilyen típus a Cisco saját fejlesztésű FHRP-je, a Hot Standby Router Protocol (HSRP) nevű protokoll. Megtudjuk, hogyan működik a HSRP, majd elvégzünk egy Packet Tracer feladatot, ahol konfiguráljuk és ellenőrizzük azt. Ne is várjunk, kezdjük el!

9.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title:** FHRP Concepts

**Module Objective**: Explain how FHRPs provide default gateway services in a redundant network.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Az alapértelmezett átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols)** | Explain the purpose and operation of first hop redundancy protocols. |
| **HSRP** | Explain how HSRP operates. |

[8.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[9.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az alapértelmezett átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols)](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. FHRP Concepts
2. Az alapértelmezett átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols)

# Az alapértelmezett átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols)

9.1.1

## Az alapértelmezett átjáró korlátai

Ha egy router 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 két vagy több router is tagja ugyanannak a VLAN-nak. Ezt a mechanizmust az FHRP biztosítja.

Egy kapcsolt hálózatban minden kliens egyetlen alapértelmezett átjáróval rendelkezik. Nincs lehetőség másodlagos átjáró használatára, 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 keresztülhaladó csomagokat a külső hálózatok felé irányítani. Azonban az a forgalom, amely a belső hálózatról az R1-hez irányult (munkaállomásoktól, szerverektől és nyomtatóktól, amelyeknek az R1 volt az alapértelmezett átjárója) még most is az R1-nek lesz címezve és emiatt eldobásra kerül.

**Note**: For the purposes of the discussion on router redundancy, there is no functional difference between a Layer 3 switch and a router at the distribution layer. A gyakorlatban leginkább egy többrétegű switch adja az alapértelmezett átjárót a kapcsolt hálózat minden VLAN-jának. Ez a tananyag a forgalomirányításra összpontosít, függetlenül a használt fizikai eszköztől.

The physcial network topology shows two switches, router, a PC, and a server. The PC, PC1, is sending a packet through the network. The graphic shows the packet being dropped at the interface of R1.

R1 R2

PC1

10.1.10.3/24  
0014.a866.289810.1.10.2/24  
0014.a855.1788Szerver  
10.9.1.50/24

A PC1 nem tudja elérni az alapértelmezett átjárót.

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

**Note**: IPv6 devices receive their default gateway address dynamically from the ICMPv6 Router Advertisement. Az IPv6-os eszközök is jobban járnak az új alapértelmezett átjáróra való gyorsabb átállással az FHRP használata esetén.

9.1.2

## Routerek redundanciája

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

The physcial network topology shows four PCs, three routers and an Internet or ISP backbone cloud. The four PCs and the three routers are connected to a LAN. The three routers also each have a link going up to the Ineternet or IPS backbone. There is a forwarding router with IP address 192.0.2.1/24. There is a virtual router with IP address 192.0.2.100/24. There is a standby router with IP address 192.0.2.2/24. An arrow representing a packet sent from PC2 goes to the virtual router at IP address 192.0.2.100 then to the forwarding router with IP address 192.0.2.1 and then to the Internet or ISP backbone.

PC1 PC3 PC4 PC2 192.0.2.2/24 192.0.2.1/24

192.0.2.3/24

Forwarding  
RouterStandby  
RouterVirtual  
RouterInternet or ISP backboneLAN

Az IP-alhálózat munkaállomásainak alapértelmezett átjárója a virtuális router 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 router MAC-címét fogja visszaadni. A virtuális router MAC-címére küldött kereteket a virtuális routercsoport éppen aktív routere fogja fizikailag feldolgozni. A csoport tagjainak azonosítását és szinkronizálását külön protokoll végzi. Az állomások a forgalmat a virtuális router IP-címére küldik. A valódi router, amely a forgalmat ténylegesen továbbítja, az állomások számára láthatatlan.

A redundancia-protokoll biztosítja a mechanizmust annak meghatározásához, hogy melyik router vegye át az aktív szerepet a forgalom továbbításában. Szintén ez határozza meg, hogy a továbbító szerepet mikor vegye át egy készenléti router. A végberendezések számára a továbbító szerep átadása nem érzékelhető.

A hálózat azon adottságát, hogy képes legyen dinamikusan helyrehozni az alapértelmezett átjárót biztosító eszköz meghibásodását, az "első ugrás" vagy alapértelmezett átjáró redundanciájának (first-hop redundancy) nevezzük.

9.1.3

## A router feladatátvételének lépései

Az aktív router meghibásodásakor a redundancia protokoll a készenléti routert aktívvá teszi, ahogy az ábrán látható. melynek lépései a következők:

1. A készenléti (standby) router nem kap az aktív, továbbító routertől Hello üzeneteket.
2. A tartalék átveszi a továbbító router szerepét.
3. Mivel az új továbbító router a virtuális router IP- és MAC-címét is átveszi, az állomások kiszolgálása nem szakad meg.

The physcial network topology shows four PCs, three routers and an Internet or ISP backbone cloud. The four PCs and the three routers are connected to a LAN. The three routers also each have a link going up to the Ineternet or IPS backbone. There is a forwarding router with IP address 192.0.2.1/24. There is a virtual router with IP address 192.0.2.100/24. There is a standby router with IP address 192.0.2.2/24. There is an X through the LAN link to the router with IP address 192.0.2.1 that was previously a forwarding router. An arrow representing a packet sent from PC2 goes to the virtual router at IP address 192.0.2.100 then to the new forwarding router with IP address 192.0.2.2 and then to the Internet or ISP backbone.

PC1 PC3 PC4 PC2 192.0.2.1/24 192.0.2.100/24

192.0.2.2/24

Virtual RouterNew Forwarding  
RouterInternet or ISP backboneLANLink vagy eszköz meghibásodása: A készenléti router lesz a továbbító router.

9.1.4

## FHRP-verziók

A vállalati környezetben használt FHRP-verzió nagymértékben függ a hálózat berendezéseitől és igényeitől. A táblázat felsorolja az FHRP-k összes verzióját.

| Table caption | |
| --- | --- |
| **FHRP-verziók** | **Leírás** |
| HSRP (Hot Standby Router Protocol) | A HRSP egy Cisco által védett FHRP, amelyet úgy terveztek, hogy lehetővé tegye egy első ugrású IPv4-eszköz átlátható feladatátvétele. HSRP magas a hálózat elérhetősége az első ugrásos útválasztási redundancia biztosításával az IPv4 számára állomások IPv4 alapértelmezett átjárócímmel konfigurált hálózatokon. HSRP is used in a group of routers for selecting an active device and a készenléti eszköz. Az eszköz interfészek egy csoportjában az aktív eszköz az a csomagok útválasztására használt eszköz; a készenléti eszköz a eszköz, amely átveszi az irányítást, ha az aktív eszköz meghibásodik, vagy ha előre be van állítva conditions are met. A HSRP készenléti útválasztó funkciója az figyelemmel kíséri a HSRP csoport működési állapotát és gyorsan feltételezi csomagtovábbítási felelősség, ha az aktív útválasztó meghibásodik. |
| HSRP for IPv6 | This is a Cisco-proprietary FHRP that provides the same functionality of HSRP, de IPv6 környezetben. A HSRP IPv6 csoport virtuális MAC-vel rendelkezik a HSRP csoportszámból és egy virtuális IPv6 link-localból származó cím a HSRP virtuális MAC-címből származó cím. Periodikusan router advertisements (RAs) are sent for the HSRP virtual IPv6 link-local címet, ha a HSRP csoport aktív. Amikor a csoport inaktívvá válik, ezek az RA-k leállnak a végső RA elküldése után. |
| Virtual Router Redundancy Protocol 2-es verziója (VRRPv2) | Ez egy nem védett választási protokoll, amely dinamikusan hozzárendel felelősség egy vagy több virtuális útválasztóért a VRRP útválasztók felé IPv4 LAN. This allows several routers on a multiaccess link to use the ugyanaz a virtuális IPv4-cím. A VRRP útválasztó konfigurálva van a VRRP futtatására protokollt egy vagy több másik útválasztóval együtt, amely a LAN. VRRP konfigurációban egy router van kiválasztva virtuálisnak router master, a többi útválasztó pedig biztonsági másolatként működik, abban az esetben, ha a virtuális router master meghibásodik. |
| VRRPV3 | IPv4-es és IPv6-os címzést is támogató protokoll. VRRPV3 works in multi-vendor environments and is more scalable than VRRPv2. |
| Gateway Load Balancing Protocol (GLBP ) | Ez egy CISCO által szabadalmaztatott FHRP, amely védelmet biztosít meghibásodott útválasztó vagy áramkör, például HSRP és VRRP, ugyanakkor lehetővé teszi a terhelést is kiegyensúlyozás (más néven terhelésmegosztás) a redundánsok csoportja között routers. |
| GLBP for IPv6 | This is a Cisco-proprietary FHRP that provides the same functionality of GLBP, de IPv6 környezetben. A GLBP for IPv6 automatikus router backup for IPv6 hosts configured with a single default gateway on a LAN. A LAN-on több első ugrású router együttesen kínál egyetlen útválasztót virtuális első ugrású IPv6 útválasztó, miközben megosztja az IPv6 csomagtovábbítást load. |
| ICMP Router Discovery Protocol (IRDP) | Az RFC 1256-ban definiált, elavultnak tekinthető FHRP-megoldás. Az IRDP lehetővé teszi az IPv4-et hosts to locate routers that provide IPv4 connectivity to other (nem helyi) IP-hálózatok. |

9.1.5

## Tudáspróba - Az alapértelmezett átjáró redundanciáját biztosító protokollok

Az űrlap teteje

Check your understanding of first hop redundancy protocols by choosing the BEST answer to the following questions.

1. What type of device routes traffic destined to network segments beyond the source network segment for which the sending node may not have explicit routing information?

Az űrlap alja

What device presents the illusion of a single router to hosts on a LAN segment but actually represents a set of routers working together?

What device is part of a virtual router group assigned the role of alternate default gateway?

What device that is part of a virtual router group assigned to the role of default gateway?

Which FHRPs are Cisco-proprietary? (Két jó válasz van.)

[9.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[9.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[HSRP](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. FHRP Concepts
2. HSRP

# HSRP

9.2.1

## A HSRP áttekintése

A Cisco biztosítja a HSRP és a HSRP for IPv6 protokollokat, hogy kivédhessük a külső hálózati hozzáférés elvesztését, ha az alapértelmezett átjáró meghibásodik.

A HSRP a Cisco saját fejlesztésű FHRP-je, az alapértelmezett átjárót biztosító IPv4-eszköz hibatűrő működtetésére.

A HSRP magas szintű hálózati elérhetőséget biztosít, az IPv4-es alapértelmezett átjárót használó állomások számára ad "első ugrás" router redundanciát. A HSRP a routerek egy csoportjából választ ki aktív és készenléti (standby) 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 routerének feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibája esetén.

9.2.2

## HSRP-prioritás és elővételi jog

Az aktív és készenléti routerek szerepe a HSRP választási folyamata során dől el. Alapértelmezés szerint a legmagasabb értékű IPv4-címmel rendelkező routert választják ki aktív routerként. Azonban mindig jobb kézben tartanunk, hogy a hálózat miként fog működni normál körülmények között, ahelyett, hogy a véletlenre hagynánk.

**HSRP Priority**

A HSRP-prioritás használható az aktív router meghatározására. A legmagasabb HSRP-prioritású eszköz lesz az aktív router. Alapértelmezés szerint a HSRP-prioritás értéke100. Ha a prioritások egyformák, a legmagasabb értékű IPv4-címmel rendelkező router lesz aktív.

Ahhoz, hogy egy router aktív legyen, használjuk a **standby priority** interfész-konfigurációs parancsot. A HSRP-prioritás értéke 0 és 255 közé eshet.

**HSRP Preemption**

Alapértelmezés szerint, miután egy eszköz aktív routerré válik, akkor is aktív szerepkörben marad, ha egy másik router magasabb HSRP-prioritással lép működésbe.

Ahhoz, hogy egy új HSRP választási folyamatot kényszerítsünk ki egy magasabb prioritású router elindulásakor, az elővételi jogot engedélyezni kell a **standby preempt** interfész konfigurációs módbeli paranccsal. Az elővételi jog (preemption) az a képesség, hogy egy HSRP-router elindíthatja az újraválasztási folyamatot. Amikor engedélyezve van, a magasabb HSRP-prioritással rendelkező router fogja viselni az aktív router szerepét.

Az elővételi jog csak akkor teszi lehetővé, hogy a router aktívvá váljon, ha magasabb prioritással rendelkezik. Az olyan router, amely azonos prioritású, de magasabb értékű IPv4-címmel rendelkezik, nem váltja ki az aktív routert. Vegyük az ábra topológiáját.

The physcial network topology shows three PCs connected to a switch. The switch in turn is connected to two routers, router R1 with IP address 172.16.10.2/24 which is the currect active router with a priority of 150, and router R2 with IP address 172.16.10.3/24 which is the current standby router with a priority of 100. R1 and R2 both connect to a backbone cloud. There is a virtual router with a virtual IP address of 172.16.10.1/24 and a virtual MAC address of 0000.0C07.AC01.

172.16.10.2/24 172.16.10.3/24 R2 R1 G0/0/1

G0/0/1

Virtual RouterVirtuális IPv4-cím  
172.16.10.1/24  
Virtuális MAC-cím  
0000.0C07.AC01Active router  
Priority 150Standby router  
Priority 100

Az R1 150-es HSRP-prioritással lett konfigurálva, míg az R2 alapértelmezett HSRP-prioritása 100. Az elővételi jog engedélyezve van az R1-en. Nagyobb prioritásával az R1 az aktív router, az R2 pedig a készenléti. A csak R1-et érintő áramkimaradás miatt az aktív router már nem áll rendelkezésre, és az eddig készenléti R2 vállalja át az aktív szerepet. A tápellátás helyreállítása után az R1 újra működőképes lesz. Mivel az R1-nek magasabb prioritása van, és az elővételi jog engedélyezve van rajta, új választási folyamatot fog kikényszeríteni. Az R1 újra átveszi az aktív router szerepét, míg az R2 visszatér a készenléti szerepbe.

**Note**: With preemption disabled, the router that boots up first will become the active router if there are no other routers online during the election process.

9.2.3

## HSRP-állapotok és -időzítők

A router lehet aktív HSRP-router, amely felelős a szegmens forgalmának továbbításáért, vagy lehet passzív, készenléti állapotban, készen arra, hogy vállalja az aktív szerepet, ha az aktív eszköz meghibásodik. Amikor egy interfészt HSRP-re konfiguráltak, vagy először aktiválódik egy meglévő HSRP-konfigurációval, a router HSRP hello csomagokat küld és fogad, hogy megkezdje annak meghatározását, hogy melyik állapotot fogja felvállalni a HSRP-csoportban.

A táblázat összefoglalja a HSRP-állapotokat.

| Table caption | |
| --- | --- |
| **HSRP-állapot** | **Leírás** |
| Kezdeti | Ez az állapot konfiguráció változásakor jön létre, vagy ha egy interfész először válik elérhetővé. |
| Tanuló | A router nem határozta meg a virtuális IP-címet, és még nem látott bejönni egy hello üzenetet sem az aktív routertől. Ebben az állapotban a router várja, hogy halljon az aktív router felől. |
| Figyelő | A router ismeri a virtuális IP-címet, de még se nem aktív, se nem készenléti router. Hallgatja az azoktól az eszközöktől érkező hello üzeneteket. |
| Beszélő | A router rendszeres hello üzeneteket küld, és aktívan részt vesz az aktív és/vagy készenléti router megválasztásában. |
| Készenléti | A router jelölve lesz a következő aktív eszköz szerepére, és küldi a periodikus hello üzeneteket. |
| Aktív | A router nyerte a választást. |

Az aktív és készenléti HSRP-routerek alapértelmezés szerint 3 másodpercenként küldenek hello csomagokat a HSRP-csoport multicast célcímére. A készenléti router aktívvá válik, ha 10 másodperc után nem kap hello üzenetet az aktív routertől. A feladatátvétel vagy az elővétel felgyorsítása érdekében csökkenthetjük ezeket az időzítő beállításokat. Viszont a megnövekedett CPU-használat és a szükségtelen készenléti állapotváltozások elkerülése érdekében ne állítsuk a hello időzítőt 1 másodperc, illetve a megtartási időzítőt 4 másodperc alá.

9.2.4

## Tudáspróba - HSRP

Az űrlap teteje

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

1. What is the default HSRP priority?

Az űrlap alja

True or False? If a router with a higher HSRP priority joins the network, it will take over the active router roll from an existing active router which has a lower priority.

During which HSRP state does an interface begin sending periodic hello messages?

Which is a characteristic of the HSRP learn state?

[9.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Az alapértelmezett átjáró redundanciáját biztosító protokollok (First Hop Redundancy Protocols)](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[9.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. FHRP Concepts
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

9.3.1

## Miről tanultunk ebben a fejezetben?

**First Hop Redundancy Protocols**

Ha egy router vagy egyik interfésze (amelyik az alapértelmezett átjáró szerepét játssza) meghibásodik, az átjárót használó állomások nem érik el a távoli hálózatokat. Az FHRP olyan mechanizmus, amely alternatív alapértelmezett átjárót biztosít olyan kapcsolt hálózatokban, ahol két vagy több forgalomirányító is tagja ugyanannak a VLAN-nak. Az egyik módszer arra, hogy megszüntessük a router, mint egyetlen meghibásodási pont szerepét az, hogy virtuális routert valósítunk meg. Ekkor több routert olyan módon konfigurálunk, hogy együttesen egyetlen router látszatát keltsék a LAN állomásainak számára. Az aktív router meghibásodásakor a redundancia-protokoll a készenléti routert aktívvá teszi, melynek lépései a következők:

1. A készenléti (standby) router nem kap az aktív, továbbító routertől Hello üzeneteket.
2. A tartalék átveszi a továbbító router szerepét.
3. Mivel az új továbbító router a virtuális router IP- és MAC-címét is átveszi, az állomások kiszolgálása nem szakad meg.

A vállalati környezetben használt FHRP-verzió nagymértékben függ a hálózat berendezéseitől és igényeitől. A következő lehetőségek állnak rendelkezésre az FHRP-k esetében:

* HSRP és HSRP for IPv6
* VRRPv2 és VRRPV3
* GLBP és GLBP for IPv6
* IRDP

**HSRP**

A HSRP a Cisco saját fejlesztésű FHRP-je, az alapértelmezett átjárót biztosító IPv4-eszköz hibatűrő működtetésére. A HSRP a routerek egy csoportjából választ ki aktív és készenléti (standby) 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 routerének feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibája esetén. A legmagasabb HSRP-prioritású eszköz lesz az aktív router. Az elővételi jog (preemption) az a képesség, hogy egy HSRP-router elindíthatja az újraválasztási folyamatot. Amikor engedélyezve van, a magasabb HSRP-prioritással rendelkező router fogja viselni az aktív router szerepét. A HSRP-állapotok közé tartozik a kezdeti, tanuló, figyelő, beszélő és készenléti állapot.

9.3.2

## Ellenőrző kvíz - Az FHRP alapjai

Az űrlap teteje

1. Mi a HSRP célja?

Az űrlap alja

Melyik gyártófüggetlen protokoll nyújt router redundanciát az IPv4-es LAN-ban működő routereknek?

A hálózati rendszergazda az alapértelmezett átjáró redundanciáját biztosító (FHRP) protokollok elemzését végzi. Melyik a VRRPv3 jellemzője?

Mi a lehetséges hátránya a HSRP megvalósításának a GLBP-vel szemben?

Egy hálózati mérnök redundáns alapértelmezett átjárót szeretne beállítani úgy, hogy a legjobban kihasználja a rendelkezésre álló hálózati erőforrásokat. Melyik protokollt válassza?

FHRP-protokoll használatakor milyen információkat osztanak meg egymással a routerek, hogy egyetlen eszköz benyomását keltsék? (Két jó válasz van.)

Az FHRP-terminológiában mi jelenti a routerek olyan csoportját, amely egyetlen router illúzióját kelti az állomások számára?

Egy felhasználónak növelnie kell a vállalati routerek redundanciáját. Milyen három lehetőséget használhat a felhasználó? (Három jó válasz van.)

Melyik két protokoll biztosítja az átjáró redundanciáját a 3. rétegben? (Két jó válasz van.)

A hálózati rendszegazda az FHRP-protokollok felügyeletét végzi. Melyik két protokoll a Cisco saját protokollja? (Két jó válasz van.)

Melyik állítás írja le a GLBP egyik jellemzőjét?

Egy hálózati rendszergazda elemzi a különböző FHRP-protokollok által támogatott funkciókat. Melyik tulajdonság jellemző a GLBP-re?

9.3.3

## Packet Tracer - A HSRP konfigurációja

**Note**: HSRP configuration is not a required skill for this module, course, or for the CCNA certification. Úgy gondoltuk azonban, hogy a HSRP implementálása a Packet Tracerben tetszeni fog. A feladat elvégzése segít jobban megérteni az FHRP-k, és különösen a HSRP működését.

A Packet Tracer feladat során megtudhatjuk, hogyan konfigurálható a Hot Standby Router Protocol (HSRP), hogy redundáns alapértelmezett átjáróeszközöket biztosítsunk a LAN-okon lévő állomásoknak. A HSRP konfigurálása után tesztelhetjük a konfigurációt, hogy ellenőrizzük, vajon az állomások tudják-e használni a redundáns alapértelmezett átjárót, ha az aktuális átjáróeszköz nem lesz elérhető.

* Állítsuk be a HSRP aktív routert.
* Állítsuk be a HSRP készenléti routert.
* Ellenőrizzük a HSRP működését.

[A HSRP konfigurációja](https://contenthub.netacad.com/courses/srwe-dl/_common/9.3.3-packet-tracer---hsrp-configuration-guide_hu-HU.pka)

9.3.4

### Packet Tracer - Data Center Exploration

Az adatközpontokat gyakran egy olyan szervezet agyának nevezik, amely adatokat tároló és elemző, belső és ügyfelek közötti kommunikációt biztosít, és biztosítja a kutatási és fejlesztési tevékenységekhez szükséges eszközöket. Az adatközpontot úgy kell megépíteni, hogy a katasztrófától függetlenül biztonságosan és hatékonyan tudja kiaknázni teljes potenciálját. Az adatközpont felépítéséhez sokféle rendszer jár, de ennél a tevékenységnél csak a hálózati komponensekkel foglalkozunk.

Az adatközpontok mérete néhány szervertől a több száz vagy akár több ezer szerverig terjedhet. Bármi legyen is a méret, az adatközpontot rendkívül szervezett módon kell felépíteni, hogy leegyszerűsítsék az összetett környezet kezelését és hibaelhárítását. Egy másik tervezési jellemző az adatközpont robusztusabbá tétele a redundancia használatával, hogy kiküszöbölje az egyetlen hibapontot. Ez magában foglalhatja további eszközök hozzáadását a fizikai redundancia biztosításához és/vagy olyan technológiák alkalmazását, mint a First Hop Redundancy Protocols (FHRP) és a logikai redundanciát biztosító link-aggregáció.

Ebben a Packet Tracer Physical Mode (PTPM) tevékenységben a torontói és seattle-i adatközpontok legtöbb eszköze már üzembe helyezve és konfigurálva van. Önt most vették fel a jelenlegi telepítés áttekintésére és a torontói Data Center 1 kapacitásának bővítésére.

**Note**: Kérjük várjon. A PTPM-tevékenység betöltése több percig is eltarthat.

[Data Center Exploration - Physical Mode](https://contenthub.netacad.com/courses/srwe-dl/_common/9.3.4-packet-tracer---data-center-exploration---physical-mode_hu-HU.pka)

[9.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[HSRP](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. Bevezetés

# Bevezetés

10.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a LAN biztonsággal kapcsolatos fogalmakat bemutató fejezetben!

Ha pályafutásunkat az IT területén képzeljük el, akkor hálózatokat nem csak építeni vagy karbantartani fogunk, hanem mi felelünk a hálózat biztonságáért is. A mai hálózattervezők és rendszergazdák számára a biztonság nem másodlagos szempont. Ez a legfontosabb a számukra! Sokan az informatikában már ma is kizárólag hálózatbiztonsággal foglalkoznak.

Tisztában vagyunk azzal, hogy mitől lesz biztonságos egy LAN? Tudjuk, hogy mit tehetnek a támadók, hogy feltörjék a hálózatunk védelmét? Tudjuk, hogy mit tehetünk azért, hogy megállítsuk őket? Ez a fejezet bevezet minket a hálózatbiztonság világába, ezért ne is késlekedjünk! Kattintsunk a Tovább gombra!

10.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: LAN Security Concepts

**Module Objective**: Explain how vulnerabilities compromise LAN security.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Endpoint Security** | Explain how to use endpoint security to mitigate attacks. |
| **Hozzáférés-szabályozás** | Elmagyarázza, hogy miként használható az AAA és a 802.1X egy LAN végpontjainak és eszközeinek a hitelesítésére. |
| **2. rétegbeli biztonsági fenyegetések** | Identify Layer 2 vulnerabilities. |
| **MAC-címtábla elleni támadások** | Explain how a MAC address table attack compromises LAN security. |
| **LAN-támadások** | Explain how LAN attacks compromise LAN security. |

[9.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Endpoint Security](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. Endpoint Security

# Endpoint Security

10.1.1

## Hálózati támadások napjainkban

A hírmédia gyakran foglalkozik a vállalati hálózatok elleni támadásokkal. Csak keressünk rá az interneten a "legújabb hálózati támadások" kifejezésre, és máris naprakész információkat találunk az aktuális támadásokról. Valószínűleg ezek a támadások az alábbiak közül egyet vagy többet tartalmaznak:

* **Distributed Denial of Service (DDoS)** – This is a coordinated attack from many devices, called zombies, with the intention of degrading or halting public access to an organization’s website and resources.
* **Data Breach** – This is an attack in which an organization’s data servers or hosts are compromised to steal confidential information.
* **Malware** – This is an attack in which an organization’s hosts are infected with malicious software that cause a variety of problems. Például, az ábrán látható WannaCry-hoz hasonló zsarolóvírusok titkosítják az adatokat egy állomáson, és a váltságdíj kifizetéséig blokkolják a hozzáférést.



10.1.2

## Hálózatbiztonsági eszközök

Különböző hálózatbiztonsági eszközökre van szükség ahhoz, hogy a hálózat peremét megvédjük a külső hozzáférésektől. Ezen eszközök közé tartozhat egy virtuális magánhálózatot (VPN) támogató router, egy újgenerációs tűzfal (NGFW) és egy hálózati hozzáférés-ellenőrző (NAC) eszköz.

Bővebb információért kattintsunk az egyes hálózatbiztonsági eszközökre!

Egy NGFW állapottartó csomagellenőrzést, az alkalmazások követhetőségét és ellenőrzését, új generációs behatolásmegelőző rendszert (NGIPS), fejlett kártevők elleni védelmet (AMP) és URL-szűrést biztosít.

10.1.3

## Végpontok védelme

A LAN-eszközök, például a switch-ek, a vezeték nélküli LAN-vezérlők (WLC-k) és más hozzáférési pontok (AP) összekapcsolják a végpontokat. Ezen eszközök többsége ki van téve az ebben a fejezetben tárgyalt, a LAN-hoz kapcsolódó támadásoknak.

Sok támadás azonban a hálózaton belülről is indulhat. Ha egy belső munkaállomásra behatolnak, akkor azt kiindulópontként használhatja egy támadó, hogy hozzáférjen a kritikus rendszereszközökhöz, például a szerverekhez és az érzékeny adatokhoz.

A végpontok olyan állomások, amelyek általában laptopokból, asztali számítógépekből, szerverekből és IP-telefonokból, valamint a munkavállalók tulajdonában lévő eszközökből állnak, amelyekre jellemzően saját eszközökként (BYOD, Bring Your Own Device) hivatkozunk. A végpontok különösen érzékenyek az e-mailben vagy webböngészés során érkező, kártevők okozta támadásokra. Ezek a végpontok jellemzően a hagyományos állomás-alapú biztonsági funkciókat használják, mint amilyen például a vírus- és kártevőellenes program, kliens-oldali tűzfal és a hoszt-alapú behatolás-megelőző rendszer (HIPS). Manapság azonban a végpontokat a legjobban a NAC, a hoszt-alapú AMP-szoftver, az e-mail biztonsági berendezés (ESA) és a webes biztonsági berendezés (WSA) kombinációja védi. A fejlett kártevők elleni védelmet (AMP) nyújtó termékek közé tartoznak a végponti megoldások, például a Cisco AMP for Endpoints.

Az ábrán egy egyszerű topológia látható, amely a fejezetben tárgyalt összes hálózatbiztonsági eszközt és végponti megoldást ábrázolja.

The figure is a network topology showing network security devices and endpoint solutions. At the upper left is the Internet cloud. Attached to the Internet cloud is a remote user with VPN client. Connected to the cloud on the internal network is a VPN-enabled router which is connected to an NGFW. The NGFW is connected to a multilayer switch which has two connections to another multilayer switch. Connected to the first switch is a NAC AAA/ISE device. Connected to the second switch isn ESA/WSA device. The two multilayer switches are both connected to a secured LAN switch and a WLC. Several wired and wireless endpoints secured with AMP are also shown including a desktop, laptop, IP phone, and smartphone.

internetRemote User with VPN ClientNAC   
AAA/ISEESA/WSAVPN-Enabled   
RouterNGFWWLCWired and Wireless   
Endpoints Secured with AMP

10.1.4

## Cisco Email Security Appliance (ESA)

A tartalombiztonsági készülékek a szervezet felhasználói számára az e-mail és a webböngészés finomított ellenőrzését tartalmazzák.

A Cisco Talos Intelligence Group szerint 2019 júniusában az összes elküldött e-mail 85%-a levélszemét volt. Az adathalász támadások a levélszemét különösen virulens formája. Emlékezzünk vissza, hogy egy adathalász támadás ráveszi a felhasználót, hogy kattintson egy linkre vagy nyisson meg egy mellékletet. A célzott adathalászat olyan magas rangú alkalmazottakat vagy vezetőket vesz célba, akik esetleg emelt szintű hozzáféréssel rendelkeznek. Ez különösen fontos a mai környezetben, ahol a SANS Institute szerint a vállalati hálózatok elleni támadások 95%-a sikeres célzott adathalász támadás eredménye.

A Cisco ESA egy olyan eszköz, amelyet az SMTP protokoll felügyeletére terveztek. A Cisco ESA folyamatosan frissül a Cisco Talos valós idejű adataival, amely egy világméretű adatbázis-figyelő rendszer segítségével észleli és korrelálja a fenyegetéseket és a megoldásokat. Ezeket a fenyegetés felderítési adatokat a Cisco ESA három-öt percenként hívja le. A Cisco ESA néhány funkciója:

* Az ismert fenyegetések blokkolása.
* A kezdeti észlelést elkerülő lopakodó kártevők elleni helyreállítás.
* A rossz linkeket tartalmazó e-mailek elvetése (az ábrán látható módon).
* Az újonnan fertőzött webhelyekhez való hozzáférés blokkolása.
* A kimenő e-mailek tartalmának titkosítása az adatvesztés megelőzése érdekében.

Az ábrán a Cisco ESA egy rossz hivatkozást tartalmazó adathalász e-mailt dob el.

a threat actor sends a phishing email from the cloud intended for a company executive; the firewall forwards it to the ESA which discards it

1 2

3

ESACompany  
Executive

1. Threat actor sends a phishing attack to an important host on the network.
2. The firewall forwards all email to the ESA.
3. The ESA analyzes the email, logs it, and if it is malware discards it.

10.1.5

## Cisco Web Security Appliance (WSA)

A Cisco WSA a web-alapú fenyegetések elhárítására szolgáló technológia. Segít a szervezeteknek a webes forgalom védelmével és ellenőrzésével kapcsolatos kihívások kezelésében. A Cisco WSA egyesíti a fejlett kártevők elleni védelmet, az alkalmazások követhetőségét és ellenőrzését, valamint a házirend szabályozók betartásának és a jelentéseknek a kezelését.

A Cisco WSA teljes körű ellenőrzést biztosít a felhasználók internet-hozzáférése felett. Bizonyos funkciók és alkalmazások, például a csevegés, az üzenetküldés, a videó és a hang, a szervezet követelményeinek megfelelően engedélyezhetők, korlátozhatók időben és sávszélességben, vagy letilthatók. A WSA képes az URL-ek feketelistázására, URL-szűrésre, kártevők vizsgálatára, URL-kategorizálásra, webalkalmazások szűrésére, valamint a webes forgalom titkosítására és visszafejtésére.

Az ábrán egy belső vállalati alkalmazott próbál meg csatlakozni az okostelefonjával egy ismert feketelistán szereplő webhelyhez.

an internal user attempts to connect to a blacklisted website; the firewall forwards it to the WSA which discards it

3 1

2

WSAinternethttp://example.com/bad

1. A user attempts to connect to a website.
2. The firewall forwards the website request to the WSA.
3. The WSA evaluates the URL and determines it is a known blacklisted site. The WSA discards the packet and sends an access denied message to the user.

10.1.6

## Check Your Understanding - Endpoint Security

Az űrlap teteje

Check your understanding of endpoint security by choosing the BEST option to the following questions.

1. Which attack encrypts the data on hosts in an attempt to extract a monetary payment from the victim?

Az űrlap alja

Which devices are specifically designed for network security? (Choose three)

Which device monitors SMTP traffic to block threats and encrypt outgoing messages to prevent data loss?

Which device monitors HTTP traffic to block access to risky sites and encrypt outgoing messages?

[10.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Hozzáférés-szabályozás](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. Hozzáférés-szabályozás

# Hozzáférés-szabályozás

10.2.1

## Hitelesítés helyi jelszóval

Az előző témakörben megtanultuk, hogy a NAC-eszköz AAA-szolgáltatásokat is nyújt. Ebben a témakörben többet fogunk megtudni az AAA-ról és a hozzáférés ellenőrzésének módjairól.

A hálózati eszközökön sokféle hitelesítés végezhető, és mindegyik módszer különböző szintű biztonságot nyújt. A távoli hozzáférés hitelesítésének legegyszerűbb módja a felhasználónév és jelszó kombinációjának beállítása a konzol- és VTY-vonalakon, valamint az AUX-porton, ahogyan az a következő példában a VTY-vonalakon látható. Ez a módszer a legkönnyebben megvalósítható, de egyben a leggyengébb és legkevésbé biztonságos is, mivel nem naplózható, és a jelszó egyszerű szöveges formában kerül továbbításra. Bárki, aki ismeri a jelszót, bejuthat az eszközre.

R1(config)# **line vty 0 4**

R1(config-line)# **password ci5c0**

R1(config-line)# **login**

Az SSH a távoli hozzáférés biztonságosabb formája:

* Felhasználónevet és jelszót igényel, amelyek az átvitel során titkosítva vannak.
* A felhasználónevet és a jelszót a helyi adatbázis alapján lehet hitelesíteni.
* Nagyobb elszámoltathatóságot is biztosít, mivel bejelentkezéskor a felhasználónév rögzítésre kerül.

Az alábbi példa a távoli hozzáférés SSH-val és helyi adatbázissal történő használatát szemlélteti.

R1(config)# **ip domain-name example.com**

R1(config)# **crypto key generate rsa general-keys modulus 2048**

R1(config)# **username Admin secret Str0ng3rPa55w0rd**

R1(config)# **ip ssh version 2**

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

R1(config-line)# **login local**

A helyi adatbázis alapú hitelesítésnek is vannak bizonyos korlátai:

* A felhasználói fiókokat minden eszközön helyben kell konfigurálni. Egy nagyvállalati környezetben, ahol számos router és switch kezelendő, időigényes lehet a helyi adatbázisok bevezetése és módosítása minden egyes eszközön.
* A helyi adatbázis konfigurációja nem biztosít tartalék hitelesítési módszert. Mi történik például, ha a rendszergazda elfelejti az adott eszköz felhasználónevét és jelszavát? Mivel a hitelesítéshez nem áll rendelkezésre tartalék módszer, a jelszó helyreállítása marad az egyetlen lehetőség.

Jobb megoldás, ha minden eszköz ugyanarra a központi szerverről származó felhasználónév- és jelszó adatbázisra hivatkozik.

10.2.2

## Az AAA összetevői

Az AAA a hitelesítés (Authentication), jogosultságkezelés (Authorization) és a naplózás (Accounting) rövidítése. Az AAA koncepciója a hitelkártya használatához hasonló, ahogy az ábrán is látható. A hitelkártya meghatározza, hogy ki használhatja, mennyit költhet az adott felhasználó, és nyilvántartást vezet arról, hogy a felhasználó milyen termékeket vagy szolgáltatásokat vásárolt.

AAA vagy tripla A néven hivatkozunk azokra a szolgáltatásokra, amelyek a hozzáférés-szabályozás alapját biztosítják a hálózati eszközökön. Az AAA szabályozza, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultságkezelés), és nyomon követi a használat során végrehajtott műveleteket (naplózás).

Authentication-Authorization-and-Accounting--transcript--UUID



**Authentication**  
  
Who are you?**Authorization**  
  
How much can you spend?**Accounting**  
  
What did you spend it on?

10.2.3

## Hitelesítés

Az AAA-hitelesítés megvalósításának két gyakori módja a helyi- és a szerver alapú.

**Local AAA Authentication**

A lokális AAA helyben tárolja a felhasználóneveket és jelszavakat a hálózati eszközökön, például egy Cisco routeren. A felhasználók hitelesítése a helyi adatbázis alapján történik, ahogy az ábrán is látható. A lokális AAA ideális a kis hálózatok számára.

a remote client connects to a AAA router, is prompted for a username and password, the router checks its local database before allowing access into the corporate network

1 2

3

Remote ClientAAA RouterCorporate Network

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is provided access to the network based on information in the local database.

**Server-Based AAA Authentication**

A szerver alapú módszer esetében a router egy központi AAA-szervert használ, az ábrán látható módon. The AAA server contains the usernames and passwords for all users. A router a RADIUS (Remote Authentication Dial-In User Service) vagy a TACACS+ (Terminal Access Controller Access Control System) protokollt használja az AAA-szerverrel való kommunikációhoz. Több router és switch esetén a szerver alapú AAA a megfelelőbb.

a remote client connects to a AAA router, is prompted for a username and password, the router authenticates the credentials using a AAA server, and the user is provided access to the network

1 2 3

4

Remote ClientAAA RouterAAA-kiszolgáló

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a AAA server.
4. The user is provided access to the network based on information in the remote AAA server.

10.2.4

## Jogosultságkezelés

Az AAA jogosultságkezelése automatikus, és a felhasználóknak a hitelesítés után nem kell további lépéseket tenniük. A jogosultságkezelés szabályozza, hogy a felhasználók a hitelesítés után mit tehetnek és mit nem tehetnek a hálózaton.

A jogosultságkezelés egy attribútumkészletet használ, amely leírja a felhasználó hálózathoz való hozzáférését. Ezeket az attribútumokat az használja az adott felhasználó jogosultságainak és korlátozásainak meghatározásához, az ábrán látható módon.

1 2

3

Remote ClientAAA-kiszolgáló

1. When a user has been authenticated, a session is established between the router and the AAA server.
2. The router requests authorization from the AAA server for the client's requested service.
3. The AAA server returns a PASS/FAIL response for authorization.

10.2.5

## Accounting

Az AAA naplózás összegyűjti és regisztrálja a használati adatokat. Ezek az adatok aztán olyan célokra használhatók fel, mint az auditálás vagy a számlázás. Az összegyűjtött adatok közé tartozhatnak a kapcsolat megkezdésének és befejezésének időpontjai, a végrehajtott parancsok, a csomagok és a bájtok száma.

A naplózás elsődleges felhasználási módja az AAA-hitelesítéssel való kombinálás. Az részletes naplót vezet arról, hogy egy hitelesített felhasználó pontosan mit csinál az eszközön, ahogy az ábrán is látható. Ez magában foglalja a felhasználó által kiadott összes EXEC módú és konfigurációs parancsot. A napló számos adatmezőt tartalmaz, többek között a felhasználónevet, a dátumot és az időt, valamint a felhasználó által beírt tényleges parancsot. Ezek az információk hasznosak az eszközök hibaelhárításakor. Emellett bizonyítékot szolgáltat arra az esetre is, ha valaki rosszindulatú cselekményeket hajt végre.

1

2

Remote ClientAAA-kiszolgáló

1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

10.2.6

## 802.1X

Az IEEE 802.1X szabvány egy portalapú hozzáférés-szabályozási és hitelesítési protokoll. Ez a protokoll megakadályozza, hogy illetéktelen munkaállomások a nyilvánosan elérhető switchportokon keresztül csatlakozzanak a LAN-hoz. A hitelesítési szerver minden egyes csatlakozó munkaállomást hitelesít, mielőtt a switch vagy a LAN által nyújtott szolgáltatásokat elérhetővé tenné.

A 802.1X portalapú hitelesítés esetén a hálózatban lévő eszközök meghatározott szerepkörökkel rendelkeznek, ahogy az ábrán is látható.

The diagram shows the devices involved in 802.1x port-based authentication. On the left is the supplicant, in this case a desktop, which requires access and responds to requests from a switch. The supplicant is connected to the authenticator, in this case a switch, which controls physical access to the network based on client authentication status. The authenticator is connected to the authentication server which performs client authentication.

**Supplicant**Requires access and responds to requests from switch**Authenticator**Controls physical access to the network based on client authentication status**Authentication**Performs client authentication

* **Client (Supplicant)** - This is a device running 802.1X-compliant client software, which is available for wired or wireless devices.
* **Switch (Authenticator)** –The switch acts as an intermediary between the client and the authentication server. Azonosítási információkat kér a klienstől, ellenőrzteti ezeket a hitelesítési szerverrel, majd a választ továbbítja a kliensnek. Egy másik eszköz, amely hitelesítőként működhet, a vezeték nélküli hozzáférési pont.
* **Authentication server** –The server validates the identity of the client and notifies the switch or wireless access point that the client is or is not authorized to access the LAN and switch services.

10.2.7

## Check Your Understanding - Access Control

Az űrlap teteje

Check your understanding of access control by choosing the BEST answer to the following questions.

1. Which AAA component is responsible for collecting and reporting usage data for auditing and billing purposes?

Az űrlap alja

Which AAA component is responsible for controlling who is permitted to access the network?

Which AAA component is responsible for determining what the user can access?

In an 802.1X implementation, which device is responsible for relaying responses?

[10.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Endpoint Security](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A 2. rétegbeli fenyegetések](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. A 2. rétegbeli fenyegetések

# A 2. rétegbeli fenyegetések

10.3.1

## A 2. réteg sebezhetőségei

Az előző két témakör a végpontok védelmét tárgyalta. Ebben a témakörben a LAN védelmének módjaival folytatjuk, az adatkapcsolati rétegben (2. réteg) található keretekre és a switch-re összpontosítva.

Emlékezzünk vissza, hogy az OSI referenciamodell hét rétegre van felosztva, amelyek egymástól függetlenül működnek. Az ábra mutatja az egyes rétegek működését és a meghatározó alapelemeket.

A hálózati rendszergazdák rutinszerűen alkalmaznak védelmi megoldásokat a 3. rétegtől a 7. rétegig. VPN-eket, tűzfalakat és IPS-eszközöket használnak ezen elemek védelmére. Ha azonban a 2. réteg veszélyeztetett, akkor bizony a felette lévő összes réteg is érintett. Ha például egy, a belső hálózathoz hozzáféréssel rendelkező támadó a 2. rétegbeli kereteket elfogná, akkor a fenti rétegekben megvalósított összes védelmi intézkedés haszontalan lenne. A támadó nagy károkat okozhatna a LAN 2. rétegbeli hálózati infrastruktúrájában.

The diagram shows the number, name, and other information related to the OSI layers from top to bottom: 7 - application, 6- presentation, 5 - session, 4 - transport, 3 - Network, 2 - data link, and 1 - physical. It shows an initial compromise of Ethernet frames at layer 2 with an arrow indicating all the layers above have also been compromised.

HTTP, HTTPS, POP3, IMAP, SSL, SSH,...Protocols/PortsIP-címekEthernet FramesPhysical LinksInitial CompromiseCompromised7654321AlkalmazásPresentationSessionTransportHálózatData LinkPhysical

10.3.2

## A switch elleni támadások kategóriái

A biztonság csak annyira erős, mint a rendszer leggyengébb láncszeme, ami jelen esetben a 2. réteget jelenti. Ennek oka, hogy a LAN-ok hagyományosan egyetlen szervezet felügyelete alatt álltak. A LAN-hoz kapcsolódó minden személyben és eszközben eredendően megbíztunk. Manapság a BYOD és a kifinomultabb támadások miatt a LAN-ok sokkal sebezhetőbbé váltak a behatolásokkal szemben. Ezért a hálózatbiztonsági szakembereknek a 3. rétegtől a 7. rétegig terjedő réteg védelmén túlmenően a LAN 2. rétegbeli infrastruktúráját érő támadásokat is el kell hárítaniuk.

A 2. rétegbeli infrastruktúrát érő támadások elhárításának első lépése a 2. réteg alapvető működésének és a 2. rétegbeli infrastruktúra által jelentett fenyegetések megértése.

A 2. rétegbeli LAN-infrastruktúra elleni támadásokat az alábbi táblázat tartalmazza, és a fejezet későbbi részeiben részletesebben is tárgyaljuk.

### A 2. rétegbeli támadások

| Table caption | |
| --- | --- |
| **Kategória** | **Példák** |
| **MAC-címtábla elleni támadások** | Tartalmazza a MAC-címek történő elárasztásos támadásokat. |
| **VLAN támadások** | Tartalmazza a VLAN-ugrásos (VLAN hopping) és a kettős címkézéses (double-tagging) VLAN-támadásokat. Ez is magában foglalja attacks between devices on a common VLAN. |
| **DHCP támadások** | Tartalmazza a DHCP-kiéheztetést (DHCP starvation) és a DHCP hamisításos (DHCP-spoofing) támadásokat. |
| **ARP támadások** | Tartalmazza az ARP hamisítást (ARP spoofing) és az ARP mérgezést (ARP poisoning). |
| **Címhamisításos támadások** | Tartalmazza a MAC-címet és az IP-címet hamisító támadásokat. |
| **STP támadások** | Tartalmazza az STP-manipulációs támadásokat. |

10.3.3

## A switch-ek elleni támadások elhárítási technikái

A táblázat áttekintést nyújt a 2. rétegbeli támadások megelőzését segítő Cisco megoldásokról.

### A 2. rétegbeli támadások elhárítása

| Table caption | |
| --- | --- |
| **Megoldás** | **Leírás** |
| **Port Security** | Prevents many types of attacks including MAC address flooding attacks and DHCP starvation attacks. |
| **DHCP Snooping** | Megakadályozza a DHCP-kiéheztetést és a DHCP hamisítással kapcsolatos támadásokat. |
| **Dinamikus ARP ellenőrzés (DAI)** | Megakadályozza az ARP-hamisítást és az ARP-mérgezést. |
| **IP Source Guard (IPSG)** | Megakadályozza a MAC- és IP-címeket hamisító támadásokat. |

Ezek a 2. rétegbeli megoldások nem lesznek hatékonyak, ha a felügyeleti protokollok nincsenek biztonságban. Például a Syslog, az SNMP (Simple Network Management Protocol), a TFTP (Trivial File Transfer Protocol), a Telnet, az FTP (File Transfer Protocol) és a legtöbb más elterjedt protokoll nem biztonságos, ezért a következő stratégiák használata ajánlott:

* Mindig használjuk e protokollok biztonságos változatait, mint amilyen például az SSH, a Secure Copy Protocol (SCP), a Secure FTP (SFTP) és a Secure Socket Layer/Transport Layer Security (SSL/TLS).
* Fontoljuk meg a sávon kívüli felügyeleti hálózat használatát az eszközök kezeléséhez.
* Használjunk dedikált felügyeleti VLAN-t, ami kizárólag a felügyeleti forgalat továbbítja.
* Használjunk ACL-eket a nem kívánatos hozzáférések szűrésére.

10.3.4

## Check Your Understanding - Layer 2 Security Threats

Az űrlap teteje

Check your understanding of Layer 2 security threats by choosing the BEST answer to the following questions.

1. Which of the following mitigation techniques are used to protect Layer 3 through Layer 7 of the OSI Model? (Három jó válasz van.)

Az űrlap alja

Which of the following mitigation techniques prevents many types of attacks including MAC address table overflow and DHCP starvation attacks?

Which of the following mitigation techniques prevents MAC and IP address spoofing?

Which of the following mitigation techniques prevents ARP spoofing and ARP poisoning attacks?

Which of the following mitigation techniques prevents DHCP starvation and DHCP spoofing attacks?

[10.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Hozzáférés-szabályozás](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A MAC-címtábla elleni támadások](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. A MAC-címtábla elleni támadások

# A MAC-címtábla elleni támadások

10.4.1

## A switch működésének áttekintése

Ebben a témakörben a hangsúly továbbra is a switch-eken van, különösen a MAC-címtáblákon, és hogy ezek a táblák mennyire sebezhetőek a támadásokkal szemben.

Emlékezzünk vissza, hogy a továbbítási döntések meghozatalához a 2. rétegbeli LAN-switch a fogadott keretekben lévő forrás MAC-címek alapján épít fel egy táblázatot, amelyet MAC-címtáblának nevezünk. (lásd az ábrán). A MAC-címtábla tárolása a memóriában történik, a keretek hatékonyabb továbbítása céljából.

S1# **show mac address-table dynamic**

Mac Address Table

-------------------------------------------

Vlan Mac Address Type Ports

---- ----------- -------- -----

1 0001.9717.22e0 DYNAMIC Fa0/4

1 000a.f38e.74b3 DYNAMIC Fa0/1

1 0090.0c23.ceca DYNAMIC Fa0/3

1 00d0.ba07.8499 DYNAMIC Fa0/2

S1#

10.4.2

## A MAC-címtábla elárasztása

Minden MAC-címtáblának meghatározott mérete van, és ennek következtében a switch kifogyhat a MAC-címek tárolására szolgáló erőforrásokból. A MAC-címek elárasztását célzó támadások kihasználják ezt a korlátozást, és addig bombázzák a switch-et hamis forrás MAC-címekkel, amíg a MAC-címtábla meg nem telik.

Amikor ez bekövetkezik, a switch a keretet ismeretlen egyedi címként kezeli, és elkezdi elárasztani az összes bejövő forgalmat az azonos VLAN-on lévő összes portján anélkül, hogy a MAC-címtáblára hivatkozna. Ez a pillanatnyi állapot lehetővé teszi egy támadó számára, hogy a helyi LAN-on vagy a helyi VLAN-on az egyik állomásról a másikra küldött összes keretet elfogja.

**Note**: Traffic is flooded only within the local LAN or VLAN. A támadó csak azon a helyi LAN-on vagy VLAN-on belüli forgalmat tudja elfogni, amelyhez kapcsolódik.

Az ábra azt mutatja, hogy egy támadó miként használhatja könnyen a **macof** nevű hálózati támadóeszközt a MAC-címtábla elárasztására.

1 2 3

4

Threat ActorVLAN 10

1. The threat actor is connected to VLAN 10 and uses **macof** to rapidly generate many random source and destination MAC and IP addresses.
2. Over a short period of time, the switch’s MAC table fills up.
3. When the MAC table is full, the switch begins to flood all frames that it receives. As long as **macof** continues to run, the MAC table remains full and the switch continues to flood all incoming frames out every port associated with VLAN 10.
4. The threat actor then uses packet sniffing software to capture frames from any and all devices connected to VLAN 10.

Ha a támadó leállítja a **macof** futtatását, vagy felfedezik és leállítják, a switch végül kiüríti a MAC-címtábla régebbi bejegyzéseit, és ismét switch-ként kezd viselkedni.

10.4.3

## A MAC-címtáblák elleni támadás elhárítása

Az olyan eszközöket, mint a **macof**, az teszi olyan veszélyessé, hogy a támadó nagyon gyorsan létrehozhat egy MAC-címtábla elárasztásos támadást. Egy Catalyst 6500-as switch például 132.000 MAC-címet tárolhat a MAC-címtáblájában. Egy eszköz, mint a **macof**, másodpercenként akár 8.000 hamis kerettel is eláraszthatja a switch-et; néhány másodperc alatt létrehozhat egy MAC-címtábla elárasztásos támadást. A példa a **macof** parancs kimenetét mutatja egy Linux állomáson.

# **macof -i eth1**

36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512

16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512

18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512

e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512

62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512

c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512

88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512

b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512

e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512

A másik ok, amiért ezek a támadási eszközök veszélyesek, hogy nem csak a helyi switch-et érintik, hanem más csatlakoztatott 2. rétegbeli switch-eket is. Amikor egy switch MAC-címtáblája megtelt, elárasztja az összes portot, beleértve azokat is, amelyek más 2. rétegbeli switch-ekhez vannak csatlakoztatva.

A MAC-címtábla elárasztásos támadások elhárítása érdekében a hálózati rendszergazdáknak portbiztonságot kell alkalmazniuk. A portbiztonság csak meghatározott számú forrás MAC-cím megtanulását engedélyezi az adott porton. A portbiztonságot egy másik fejezetben tárgyaljuk.

10.4.4

## Check Your Understanding - MAC Address Table Attacks

Az űrlap teteje

Check your understanding of MAC address table attacks by choosing the BEST answer to the following questions.

1. What is the behavior of a switch as a result of a successful MAC address table attack?

Az űrlap alja

What would be the primary reason a threat actor would launch a MAC address overflow attack?

What mitigation technique must be implemented to prevent MAC address overflow attacks?

[10.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A 2. rétegbeli fenyegetések](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[LAN-támadások](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. LAN-támadások

# LAN-támadások

10.5.1

## Videómagyarázat - VLAN- és DHCP-támadások

Ez a téma a LAN-támadások számos különböző típusát és azok elhárítási technikáit vizsgálja. Az előző témákhoz hasonlóan ezek a támadások általában a switch-ekre és a 2. rétegre jellemzőek.

A VLAN- és DHCP-támadásokról szóló videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

10.5.2

## VLAN-ugrásos támadás

A VLAN-ugrásos támadás lehetővé teszi, hogy az egyik VLAN-ból érkező forgalom router segítsége nélkül megjelenjen egy másik VLAN-on. Az alapvető VLAN-ugrásos támadás során a támadó úgy konfigurál egy állomást, hogy az switch-ként viselkedjen, és kihasználja a legtöbb switchporton alapértelmezés szerint engedélyezett automatikus trönkport funkciót.

A támadó úgy konfigurálja az állomást, hogy az meghamisítsa a 802.1Q és a Cisco saját DTP (Dynamic Trunking Protocol) protokolljának csomagjait, hogy a csatlakozó switch felé trönkkapcsolatot létesítsen. Ha ez sikerül, a switch trönkkapcsolatot hoz létre az állomással, az ábrán látható módon. Ekkor a támadó hozzáférhet a switch összes VLAN-jához. A támadó bármelyik VLAN-on küldhet és fogadhat forgalmat, gyakorlatilag a VLAN-ok között ugrálva.

An attacker is connected to a switch which is connected to another switch via an 802.1Q trunk. The second switch has a connection to Server 1 on V LAN 10 and a connection to Server 2 at V LAN 20. A támadó jogosulatlan 802.1Q fővonali kapcsolatot hozott létre a kapcsolóhoz, hogy hozzáférjen a szerver V LAN-jához. egy nyíl a támadóról a kapcsolóra mutat, és jogosulatlan trunk felirattal van ellátva.

802.1QTrunk802.1QVLAN 20Server1VLAN 10Server 2Attacker gains access to the server VLANUnauthorized Trunk

10.5.3

## Kettős címkézéses támadás

A támadó bizonyos helyzetekben beágyazhat egy rejtett 802.1Q címkét egy olyan keretbe, amely már rendelkezik 802.1Q címkével. Ez a címke lehetővé teszi a keretnek egy olyan VLAN-ba történő továbbítását, amely az eredeti 802.1Q címkében nem volt megadva.

A kettős címkézéses támadás példájának és magyarázatának megtekintéséhez kattintsunk az egyes lépésekre!

A támadó egy kettős címkével ellátott 802.1Q keretet küld a switch-nek. A külső fejléc a támadó VLAN-címkéjét tartalmazza, amely megegyezik a trönkport natív VLAN-jával. A példa kedvéért tegyük fel, hogy ez a VLAN 10. A belső címke pedig a megtámadott VLAN, amely ebben az estben a VLAN 20.

An attacker is connected to a switch which has a trunk link to another switch that is set to native VLAN 10. The second switch has an attached target host in VLAN 20. The attacker sends a frame to the first switch that consists of the following fields: Ethernet, VLAN 10, VLAN 20, and data.

1

EthernetVLAN 10VLAN 20DataTrunk Native VLAN = 10Target (VLAN 20)

Ez a támadástípus egyirányú, és csak abban az esetben működik, amikor a támadó a trönkport natív VLAN-jához tartozó portra csatlakozik. Az ötlet lényege, hogy a kettős címkézés lehetővé teszi a támadó számára, hogy adatokat küldjön olyan VLAN-ban lévő állomásoknak vagy szervereknek, amelyeket egyébként valamilyen hozzáférés-szabályozási konfiguráció blokkolna. Feltehetően a válaszforgalom is engedélyezett lesz, így a támadó képes lesz kommunikálni az egyébként blokkolt VLAN-ban lévő eszközökkel.

**VLAN Attack Mitigation**

A VLAN-ugrásos és a kettős címkézéses VLAN-támadások megelőzhetők az alábbi trönkbiztonsági irányelvek alkalmazásával, amint azt egy korábbi fejezetben tárgyaltuk:

* Tiltsuk le a trönkkapcsolat létesítését minden hozzáférési porton.
* Tiltsuk le a trönkkapcsolat automatikus létesítését a trönkvonalakon, így a trönköket manuálisan kell engedélyezni.
* Győződjünk meg arról, hogy a natív VLAN csak a trönkkapcsolatoknál használatos.

10.5.4

## DHCP-üzenetek

A DHCP-szerverek a kliensek IP-konfigurációs információinak dinamikus beállítását biztosítják, beleértve az IP-címet, az alhálózati maszkot, az alapértelmezett átjárót, a DNS-szervereket és egyebeket. Az ábrán a kliens és a szerver közötti DHCP-üzenetváltás folyamata látható.

The diagram shows the sequence of DHCP messages exchanged between a client and a server. The server is shown on the left and the client on the right. From top to bottom, what follows is the sequence of messages. First, the client sends a DHCPDISCOVER broadcast to the server indicating, I would like to request an address. Next, the server responds with a DHCPOFFER unicast indicating, I am DHCPsvr1, here is an address I can offer. The message includes an IP address of 192.168.10.15, a subnet mask of 255.255.255.0, a default gateway of 192.168.10.1, and a lease time of 3 days. The client responds with a DHCPREQUEST broadcast indicating, I accept the IP address offer. Lastly, the server responds with a DHCPACK unicast indicating, your acceptance is acknowledged.

IP address: 192.168.10.15Subnet mask: 255.255.255.0Default Gateway: 192.168.10.1Lease time: 3 days

KiszolgálóÜgyfélDHCPOFFERDHCPACKDHCPDISCOVERDHCPREQUEST"I would like to request an address.""I am DHCPsvr1. Here is an address I can offer.""I accept the IP address offer.""Your acceptance is acknowledged."Broadcast vagy UnicastBoradcast vagy UnicastBroadcastBroadcast

10.5.5

## DHCP-támadások

A DHCP-támadások két típusa a DHCP-kiéheztetés és a DHCP-hamisítás. Mindkét támadás elhárítható a DHCP snooping alkalmazásával.

**DHCP Starvation Attack**

A DHCP-kiéheztetés célja, hogy szolgáltatás megtagadást (DoS) okozzon a kapcsolódó ügyfelek számára. A DHCP-kiéheztetéshez olyan támadóeszközre van szükség, mint a például a Gobbler.

A Gobbler képes átnézni a kiosztható IP-címek teljes körét, és megpróbálja azokat mind kiosztatni. Konkrétan hamis MAC-címeket tartalmazó DHCP-felderítési üzeneteket hoz létre.

**DHCP Spoofing Attack**

DHCP-hamisítás akkor következik be, amikor támadó szándékkal egy hamis, egy ál DHCP-szervert csatlakoztatnak a hálózatra, és az téves IP-konfigurációs paramétereket oszt ki a gyanútlan ügyfeleknek. Ez a támadó szerver számos félrevezető információt adhat át:

* **Wrong default gateway** - The rogue server provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. Ez a tevékenység akár teljesen észrevétlen is maradhat, hiszen a támadó csupán elfogja a hálózaton áthaladó adatforgalmat.
* **Wrong DNS server** - The rogue server provides an incorrect DNS server address pointing the user to a nefarious website.
* **Wrong IP address** - The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

A DHCP-hamisítás példájának és magyarázatának megtekintéséhez kattintsunk az egyes lépésekre!

**Threat Actor Connects Rogue DHCP Server**

A threat actor successfully connects a rogue DHCP server to a switch port on the same subnet and VLANs as the target clients. A támadó szerver célja, hogy a klienseket hamis IP-beállításokkal lássa el.

a rogue DHCP server is connected to a switch on a network

DHCP-kiszolgálóRogue DHCP Server

10.5.6

## Videómagyarázat - ARP-támadások, STP-támadások és CDP-felderítés

A VLAN- és DHCP-támadásokról szóló videó megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra!

10.5.7

## ARP-támadások

Recall that hosts broadcast ARP Requests to determine the MAC address of a host with a particular IPv4 address. Ez általában az alapértelmezett átjáró MAC-címének felderítésére szolgál. Az alhálózaton lévő összes állomás megkapja és feldolgozza az ARP-kérést. The host with the matching IPv4 address in the ARP Request sends an ARP Reply.

According to the ARP RFC, a client is allowed to send an unsolicited ARP Request called a “gratuitous ARP.” When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IPv4 address contained in the gratuitous ARP in their ARP tables.

A probléma az, hogy egy támadó hamisított MAC-címet tartalmazó gratuitous ARP-üzenetet küldhet egy switch-nek, és a switch ennek megfelelően frissíti a MAC-címtábláját. Ezért bármelyik állomás azt állíthatja magáról, hogy ő a tulajdonosa bármelyik tetszőleges IP- és MAC-cím kombinációjának. In a typical attack, a threat actor can send unsolicited ARP Replies to other hosts on the subnet with the MAC Address of the threat actor and the IPv4 address of the default gateway.

Az interneten számos eszköz áll rendelkezésre a közbeékelődéses ARP-támadások létrehozásához, ilyen például a dsniff, a Cain & Abel, az ettercap, a Yersinia és mások. Az IPv6 az ICMPv6 Neighbor Discovery Protocol protokollját használja a 2. rétegbeli címfeloldáshoz. Az IPv6 tartalmaz módszereket a Neighbor Advertisement spoofing (szomszédhirdetés hamisítása) elhárítására, hasonlóan ahhoz, ahogy az IPv6 megakadályozza a hamisított ARP-válaszokat is.

Az ARP-hamisítás és az ARP-mérgezés a DAI (Dynamic ARP Inspection) alkalmazásával elhárítható.

Az ARP-hamisítás és ARP-mérgezés példájának és magyarázatának megtekintéséhez kattintsunk az egyes lépésekre!

**Normál állapot konvergált MAC-címtáblákkal**

Minden eszköz pontos MAC-címtáblával rendelkezik, amely tartalmazza a LAN-on lévő többi eszköz helyes IPv4- és MAC-címét.

PC1 PC2

R1

MEGJEGYZÉS: A MAC-címek az egyszerűség kedvéért 24 bitesek.R1 ARP CachePC1 ARP CachePC2 ARP CacheMAC: CC:CC:CCIP: 10.0.0.12MAC: BB:BB:BBIP: 10.0.0.11MAC: AA:AA:AAIP: 10.0.0.1

|  |  |
| --- | --- |
| **IP Address** | **MAC Address** |
| 10.0.0.1 | AA:AA:AA |
| 10.0.0.11 | BB:BB:BB |

|  |  |
| --- | --- |
| **IP Address** | **MAC Address** |
| 10.0.0.11 | BB:BB:BB |
| 10.0.0.12 | CC:CC:CC |

|  |  |
| --- | --- |
| **IP Address** | **MAC Address** |
| 10.0.0.1 | AA:AA:AA |
| 10.0.0.12 | CC:CC:CC |

10.5.8

## Címhamisításos támadás

Az IP-címek és MAC-címek többféle okból is hamisíthatók. IP-cím meghamisításáról akkor beszélünk, amikor a támadó eltéríti egy másik eszköz érvényes IP-címét az alhálózaton, vagy véletlenszerű IP-címeket használ. Az IP-cím meghamisítását nehéz elhárítani, különösen akkor, ha egy olyan alhálózaton belül használják, amelyhez az IP tartozik.

A MAC-cím meghamisításával kapcsolatos támadások akkor fordulnak elő, amikor a támadók megváltoztatják a saját állomásuk MAC-címét, hogy az egyezzen a célállomás egy másik ismert MAC-címével. A támadó állomás ezután az újonnan konfigurált MAC-címmel keretet küld a hálózaton keresztül. Amikor a switch megkapja a keretet, megvizsgálja a forrás MAC-címét. A switch felülírja a MAC-címtábla aktuális bejegyzését, és az ábrán látható módon hozzárendeli a MAC-címet az új porthoz. Ezután nem szándékosan ugyan, de továbbítja a célállomásnak szánt kereteket a támadó állomásnak.

A threat agent on PC2 is connected to a switch at port Fa0/2. Connected to the switch at port Fa0/1 is PC1 with MAC BB:BB:BB. The threat agent is sending a message to the switch that says, my MAC is BB:BB:BB. The switch MAC address table now shows no MAC address mapped to port Fa0/1 but MAC BB:BB:BB mapped to port Fa0/1

PC2 PC1 Fa0/2

Fa0/1

MAC Address Table

|  |  |
| --- | --- |
| **Port** | **MAC Address** |
| Fa0/1 |  |
| Fa0/2 | BB:BB:BB |

Note:"My MAC is BB:BB:BB"MAC: BB:BB:BB

Amikor a célállomás valamilyen forgalmat küld, a switch kijavítja a hibát, és a MAC-címet újra az eredeti porthoz rendeli. Annak érdekében, hogy a switch ne tudja visszaállítani a port hozzárendelését a helyes állapotba, a támadó létrehozhat egy olyan programot vagy szkriptet, amely folyamatosan kereteket küld a switch-nek, így az fenntartja a hibás vagy hamisított információt. A 2. rétegben nincs olyan biztonsági mechanizmus, amely lehetővé tenné a switch számára, hogy ellenőrizze a MAC-címek forrását, és ez teszi azt annyira sebezhetővé a hamisítással szemben.

Az IP- és MAC-cím hamisítása az IPSG (IP Source Guard) alkalmazásával mérsékelhető.

10.5.9

## STP-támadás

A hálózati támadók manipulálhatják a Spanning Tree Protocol (STP) protokollt, hogy támadást hajtsanak végre a root bridge meghamisításával és ezáltal a hálózat topológiájának megváltoztatásával. A támadók a saját állomásaikat root bridge-ként jeleníthetik meg, és így a közvetlen kapcsolási tartomány teljes forgalmát elfoghatják.

Az STP-manipulációs támadás végrehajtásához a támadó állomás olyan konfigurációs és topológiai változásokat tartalmazó BPDU-kat (Bridge Protocol Data Unit) küld ki szórással, amelyek a feszítőfa újraszámítását kényszerítik ki, az ábrán látható módon. A támadó állomás által küldött BPDU-k alacsonyabb prioritást jelentenek be, hogy megpróbáljanak root bridge szerepkört megszerezni.

**Note**: Ezek a problémák akkor fordulhatnak elő, ha valaki rosszindulatú szándék nélkül Ethernet-kapcsolót ad hozzá a hálózathoz.

The diagram shows a threat agent and two switches connected together in a triangle, with the attacker at the bottom. Both ports between the attacker and the upper left switch are forwarding. Both ports on the connection between the switches are forwarding. On the link between the attacker and the upper right switch, the port on the attacker is blocking and the port on the switch is forwarding. The upper left switch is currently the root bridge with a priority of 8192. The attacker has sent STP BPDUs to both switches with a priority of 0.

STP BDPU Priority = 0Root BridgeSTP BDPU Priority = 0TovábbBlockPriority = 8192

Ha sikerrel jár, a támadó állomás lesz a root bridge, ahogy az ábrán is látható, és ekkor már számos olyan keretet is képes elfogni, amelyek egyébként nem lennének számára elérhetőek.

The diagram shows a threat agent and two switches connected together in a triangle, with the attacker at the bottom. The attacker has become the root bridge. Both ports between the attacker and the upper left switch are forwarding. Both ports on the link between the attacker and the upper right switch are also forwarding. On the connection between the upper switches, the switchport on the left is forwarding and the switchport on the right is blocking.

TovábbBlockRoot Bridge

Ezt az STP-támadást úgy lehet elhárítani, hogy az összes hozzáférési porton BPDU Guard-ot állítunk be. A BPDU Guard-ot a tanfolyam későbbi részében részletesebben tárgyaljuk.

10.5.10

## CDP-felderítés

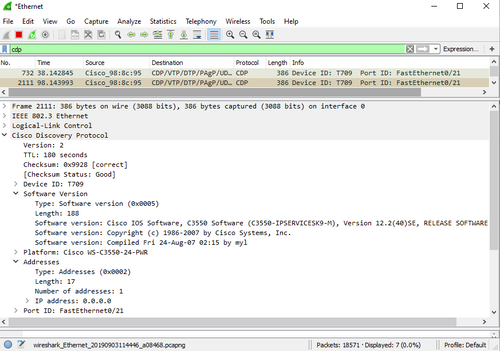
A CDP (Cisco Discovery Protocol) a Cisco saját protokollja, amely az adatkapcsolati rétegben működik. Alapértelmezés szerint minden Cisco eszközön engedélyezve van. A CDP képes automatikusan felderíteni más CDP-kompatibilis eszközöket, és segít a kapcsolat automatikus konfigurálásában. A hálózati rendszergazdák a CDP-t a hálózati eszközök konfigurálásához és hibaelhárításához is használják.

CDP information is sent out CDP-enabled ports in a periodic, unencrypted multicast. amelyek tartalmazzák az eszköz IP-címét, az IOS szoftververzióját, a platformot, a képességeket és a natív VLAN-t. A CDP-üzenetet fogadó eszköz frissíti a CDP-adatbázisát.

A CDP-információk rendkívül hasznosak a hálózati hibaelhárításban. Használható például az 1. és 2. rétegbeli kapcsolatok ellenőrzésére. Ha a rendszergazda nem tud pingelni egy közvetlenül csatlakoztatott interfészt, de mégis kap CDP-információt, akkor a probléma valószínűleg a 3. réteg konfigurációjával kapcsolatos.

A CDP által szolgáltatott információkat azonban egy támadó arra is felhasználhatja, hogy felfedezze a hálózati infrastruktúra sebezhetőségeit.

Az ábrán a Wireshark által elfogott csomagok között látható egy CDP-csomag tartalma. A támadó képes azonosítani az eszköz által használt Cisco IOS szoftververzióját. Ez különösen veszélyes, mert így megállapítható, hogy van-e a szoftverváltozatnak valamilyen támadható sérülékenysége.



A CDP-szórások küldése titkosítatlanul és hitelesítés nélkül történik. Ezért a támadó zavarhatja a hálózati infrastruktúrát azáltal, hogy hamis eszközinformációkat tartalmazó, manipulált CDP-kereteket küld a közvetlenül csatlakoztatott Cisco eszközöknek.

A CDP támadások megakadályozása érdekében korlátozzuk a CDP használatát az eszközökön vagy portokon. A CDP letiltható például a nem megbízható eszközökhöz kapcsolódó portokon.

A CDP egész eszközre kiterjedő tiltásához használjuk globális konfigurációs módban a **no cdp run** parancsot. A CDP engedélyezéséhez adjuk ki a **cdp run** globális konfigurációs parancsot.

A CDP egy adott porton történő letiltásához használjuk a **no cdp enable** interfészkonfigurációs parancsot. A CDP egy adott porton történő engedélyezéséhez használjuk a **cdp enable** interfészkonfigurációs parancsot.

**Note**: Link Layer Discovery Protocol (LLDP) is also vulnerable to reconnaissance attacks. Az LLDP globális letiltásához adjuk ki a **no lldp run** parancsot. Az LLDP egy adott interfészen történő letiltásához a **no lldp transmit** és **no lldp receive** parancsokat kell kiadni.

10.5.11

## Check Your Understanding - LAN Attacks

Az űrlap teteje

Check your understanding of LAN attacks by choosing the BEST answer to the following questions.

1. A threat actor changes the MAC address of the threat actor's device to the MAC address of the default gateway. What type of attack is this?

Az űrlap alja

A threat actor sends a BPDU message with priority 0. What type of attack is this?

A threat actor leases all the available IP addresses on a subnet. What type of attack is this?

A threat actor sends a message that causes all other devices to believe the MAC address of the threat actor's device is the default gateway. What type of attack is this?

A threat actor configures a host with the 802.1Q protocol and forms a trunk with the connected switch. What type of attack is this?

A threat actor discovers the IOS version and IP addresses of the local switch. What type of attack is this?

[10.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A MAC-címtábla elleni támadások](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[10.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. LAN Security Concepts
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

10.6.1

## Miről tanultunk ebben a fejezetben?

A végpontok különösen érzékenyek az e-mailben vagy webböngészés során érkező támadásokra, mint amilyen a DDoS, az adatlopás vagy a kártevő programok (malware). Ezek a végpontok jellemzően a hagyományos hoszt alapú biztonsági funkciókat használják, mint amilyen például a vírus- és kártevőellenes program, kliensoldali tűzfal és a hoszt alapú behatolásmegelőző rendszer (HIPS). A végpontokat a legjobban a NAC, a hoszt alapú AMP-szoftver, az e-mail biztonsági berendezés (ESA) és a webes biztonsági berendezés (WSA) kombinációja védi. A WSA képes az URL-ek feketelistázására és szűrésére, kártevők vizsgálatára, URL-ek kategorizálására, webalkalmazások szűrésére, valamint a webes forgalom titkosítására és visszafejtésére.

Az AAA szabályozza, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultságkezelés), és nyomon követi a használat során végrehajtott műveleteket (naplózás). A jogosultságkezelés egy attribútumkészletet használ, amely leírja a felhasználó hálózathoz való hozzáférését. A naplózás az AAA-hitelesítéssel kombinálva történik. Az AAA szerver részletes naplót vezet arról, hogy egy hitelesített felhasználó pontosan mit is csinál egy adott eszközön. Az IEEE 802.1X szabvány olyan port-alapú hozzáférés-szabályozási és hitelesítési protokollt definiál, amely megakadályozza, hogy jogosulatlan munkaállomások nyilvánosan elérhető portokon keresztül csatlakozzanak egy helyi hálózathoz (LAN-hoz).

Ha a 2. réteg veszélyeztetett, akkor a felette lévő összes réteg is érintett. A 2. rétegbeli infrastruktúrát érő támadások elhárításának első lépése a 2. réteg alapvető működésének és a 2. rétegbeli megoldások (pl.: portbiztonság, DHCP snooping, DAI és IPSG) megértése. Ezek nem fognak működni, ha a felügyeleti protokollok védelme nem biztosított.

A MAC-címek elárasztását célzó támadások addig bombázzák a switch-et hamis forrás MAC-címekkel, amíg a MAC-címtábla meg nem telik. Amikor ez bekövetkezik, a switch a keretet ismeretlen egyedi címként kezeli, és elkezdi elárasztani az összes bejövő forgalmat az azonos VLAN-on lévő összes portján anélkül, hogy a MAC-címtáblára hivatkozna. Ez a pillanatnyi állapot lehetővé teszi egy támadó számára, hogy a helyi LAN-on vagy a helyi VLAN-on az egyik állomásról a másikra küldött összes keretet elfogja. A támadó a **macof** segítségével gyorsan sok véletlenszerű forrás- és célcímet generál (MAC- és IP-címet egyaránt). A MAC-címtábla elárasztásos támadások elhárítása érdekében a hálózati rendszergazdáknak portbiztonságot kell alkalmazniuk.

A VLAN-ugrásos támadás lehetővé teszi, hogy az egyik VLAN-ból érkező forgalmat router segítsége nélkül lássa egy másik VLAN. A támadó úgy konfigurál egy állomást, hogy az switch-ként viselkedjen, és kihasználja a legtöbb switchporton alapértelmezés szerint engedélyezett automatikus trönkport funkciót.

Ez a támadástípus egyirányú, és csak abban az esetben működik, amikor a támadó a trönkport natív VLAN-jához tartozó portra csatlakozik. A kettős címkézés lehetővé teszi a támadó számára, hogy adatokat küldjön olyan VLAN-ban lévő állomásoknak vagy szervereknek, amelyeket egyébként valamilyen hozzáférés-szabályozási konfiguráció blokkolna. A válaszforgalom is engedélyezett lesz, így a támadó képes lesz kommunikálni az egyébként blokkolt VLAN-ban lévő eszközökkel.

A VLAN-ugrásos és a kettős címkézéses VLAN-támadások megelőzhetők az alábbi trönkbiztonsági irányelvek alkalmazásával:

* Tiltsuk le a trönkkapcsolat létesítését minden hozzáférési porton.
* Tiltsuk le a trönkkapcsolat automatikus létesítését a trönkvonalakon, így a trönköket manuálisan kell engedélyezni.
* Győződjünk meg arról, hogy a natív VLAN csak a trönkkapcsolatoknál használatos.

DHCP-támadás: A DHCP-szerverek dinamikusan biztosítják az IP-konfigurációs beállításokat a kliensek számára, beleértve az IP-címet, az alhálózati maszkot, az alapértelmezett átjárót, a DNS-szervereket és egyebeket. A DHCP-támadások két típusa a DHCP-kiéheztetés és a DHCP-hamisítás. Mindkét támadás elhárítható a DHCP snooping alkalmazásával.

ARP-támadás: Egy támadó hamisított MAC-címet tartalmazó gratuitous ARP-üzenetet küldhet egy switch-nek, és a switch ennek megfelelően frissíti a MAC-címtábláját. Now the threat actor sends unsolicited ARP Requests to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. Az ARP-hamisítás és az ARP-mérgezés a DAI alkalmazásával elhárítható.

Címhamisításos támadás: IP-cím meghamisításáról akkor beszélünk, amikor a támadó eltéríti egy másik eszköz érvényes IP-címét az alhálózaton, vagy véletlenszerű IP-címet használ. A MAC-cím meghamisításával kapcsolatos támadások akkor fordulnak elő, amikor a támadók megváltoztatják a saját állomásuk MAC-címét, hogy az egyezzen a célállomás egy másik ismert MAC-címével. Az IP- és MAC-cím hamisítása az IPSG alkalmazásával mérsékelhető.

STP-támadás: A támadók manipulálhatják az STP protokollt, hogy támadást hajtsanak végre a root bridge meghamisításával és a hálózat topológiájának megváltoztatásával. A támadók a saját állomásaikat root bridge-ként jeleníthetik meg, és így a közvetlen kapcsolási tartomány teljes forgalmát elfoghatják. Ezt az STP-támadást úgy lehet elhárítani, hogy az összes hozzáférési porton BPDU Guard-ot állítunk be.

CDP Reconnaissance: CDP information is sent out CDP-enabled ports in a periodic, unencrypted multicast. amelyek tartalmazzák az eszköz IP-címét, az IOS szoftververzióját, a platformot, a képességeket és a natív VLAN-t. A CDP-üzenetet fogadó eszköz frissíti a CDP-adatbázisát, de a CDP által szolgáltatott információkat egy támadó arra is felhasználhatja, hogy felfedezze a hálózati infrastruktúra sebezhetőségeit. A CDP kiaknázásának megakadályozása érdekében korlátozzuk a CDP használatát az eszközökön vagy portokon.

10.6.2

## Ellenőrző kvíz - LAN biztonsági fogalmak

Az űrlap teteje

1. Milyen két protokollt támogatják a Cisco eszközök az AAA kommunikációhoz? (Két jó válasz van.)

Az űrlap alja

Melyik szolgáltatás engedélyezett alapértelmezés szerint egy Cisco routeren, amely fontos információkat árulhat el a routerről, és potenciálisan sebezhetőbbé teheti a támadásokkal szemben?

Melyik OSI réteg tekinthető a hálózati rendszer leggyengébb láncszemének biztonsági szempontból?​

Melyik 2. rétegbeli támadás eredményezi azt, hogy egy switch elárasztja a bejövő keretekkel valamennyi portját?

Miért részesítjük előnyben az AAA-val történő hitelesítést a helyi adatbázison alapuló módszerrel szemben?

Szerver alapú AAA esetén melyik protokoll teszi lehetővé, hogy a router sikeresen kommunikáljon az AAA-szerverrel?

Melyik Cisco megoldás segíti megelőzni a MAC- és IP-címek hamisítási támadásait?

Mi a célja az AAA naplózásnak?

Melyik 2. rétegbeli támadás eredményezi azt, hogy a jogos felhasználók nem kapnak érvényes IP-címet?

Melyik három Cisco termék fókuszál a végpontok biztonsági megoldásaira? (Három jó válasz van.)

Igaz vagy hamis?  
A 802.1X szabványban a hálózathoz csatlakozni próbáló klienst kérelmezőnek (supplicant) nevezik.

Miből áll egy IP-cím hamisításos támadás?

Melyik három szolgáltatást biztosítja az AAA keretrendszer? (Három jó válasz van.)

Az érvényesített biztonsági szabályozások miatt a felhasználó csak FTP-vel férhet hozzá egy szerverhez. Melyik AAA összetevő valósítja meg ezt?

Melyik védekezési módszer a legjobb a MAC-címtábla túlterhelésére irányuló DoS támadások meghiúsítására?

[10.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[LAN-támadások](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. Bevezetés

# Bevezetés

11.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a switch biztonsági beállítások című fejezetben!

Hálózati szakemberként munkánk fontos része a hálózat biztonságának megőrzése. Legtöbbször csak a kívülről érkező biztonsági támadásokra gondolunk, de a fenyegetések a hálózaton belülről is jöhetnek. A fenyegetések széles skálán mozognak, kezdve például, ha egy alkalmazott saját elhatározásából csatlakoztat egy switch-et a vállalati hálózathoz, hogy több szabad portja legyen, egészen addig, ha egy elégedetlen munkavállaló szándékosan rosszindulatú támadást hajt végre. Feladatunk a hálózat biztonságos működtetése az üzleti folyamatok kompromisszumok nélküli biztosítása céljából.

Hogyan tarthatjuk biztonságosan és stabilan a hálózatot? Hogyan védjük meg a hálózaton belüli rosszindulatú támadásoktól? Hogyan biztosíthatjuk, hogy az alkalmazottak ne csatlakoztassanak switch-et, kiszolgálókat és egyéb eszközöket, amelyek veszélyeztethetik a hálózati működést?

Ez a fejezet bemutatja a hálózat belső biztonságának megőrzését.

11.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: Switch Security Configuration

**Module Objective**: Configure switch security to mitigate LAN attacks.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| Implement Port Security | Implement port security to mitigate MAC address table attacks. |
| Mitigate VLAN Attacks | Explain how to configure DTP and native VLAN to mitigate VLAN attacks. |
| Mitigate DHCP Attacks | Explain how to configure DHCP snooping to mitigate DHCP attacks. |
| Mitigate ARP Attacks | Explain how to configure ARP inspection to mitigate ARP attacks. |
| Mitigate STP Attacks | A PortFast és a BPDU Guard konfigurálása az STP-támadások kiküszöbölésére. |

[10.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Portbiztonság megvalósítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. Portbiztonság megvalósítása

# Portbiztonság megvalósítása

11.1.1

## Használaton kívüli portok védelme

A 2. rétegbeli eszközök a vállalati infrastruktúra biztonsági szempontból leggyengébb láncszemei. A 2. rétegbeli támadások a legkönnyebben megvalósíthatók a hackerek számára, de ezek a fenyegetések néhány egyszerű megoldással kivédhetők.

Minden portot (interfészt) védeni kell, mielőtt a switch a végleges környezetébe kerülne. A port védelmének módja függ annak funkciójától.

A legegyszerűbb módszer, melyet sok rendszergazda alkalmaz az illetéktelen hozzáférés megakadályozására, a nem használt portok letiltása. Például, ha egy Catalyst 2960 switch 24 portja közül csak háromhoz van eszköz csatlakoztatva, akkor ajánlott a nem használt 21 portot letiltani. Keressük meg az összes használaton kívüli portot, és mindegyiknél adjuk ki a **shutdown** parancsot! Ha egy portot később újra aktiválni kell, az engedélyezhető a **no shutdown** paranccsal.

Egy porttartomány konfigurálásához használjuk az **interface range** parancsot.

Switch(config)# **interface range** type module/first-number – last-number

Például, a Fa0/8 és a Fa0/24 közötti portok leállításához a következő parancsot kell kiadni.

S1(config)# **interface range fa0/8 - 24**

S1(config-if-range)# **shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

(output omitted)

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S1(config-if-range)#

11.1.2

## A MAC-címtábla támadások enyhítése

A legegyszerűbb és leghatékonyabb módszer a MAC-címtábla túlcsordulási támadások megakadályozására a portbiztonság engedélyezése.

A portbiztonság fizikai interfészenként korlátozza az engedélyezett MAC-címek számát. Ez lehetővé teszi a rendszergazda számára, hogy manuálisan konfiguráljon a MAC-címeket egy porthoz, vagy engedélyezze a switch számára, hogy dinamikusan tanuljon meg korlátozott számú MAC-címet. Amikor egy portbiztonsággal konfigurált port keretet fogad, a forrás MAC-címet összehasonlítja a biztonságos MAC-címek listájával, amelyeket vagy manuálisan konfiguráltak vagy dinamikusan tanult meg a port.

A portokon engedélyezett MAC-címek számának korlátozásával a portbiztonság a hálózathoz való jogosulatlan hozzáférés szabályozására használható (lásd ábra).

The graphic shows a switch connected to three devices. Above the switch is a MAC address table with port 0/1 with allowed MAC AA:AA:AA, port 0/2 allowed MAC BB:BB:BB, and port 0/2 allowed MAC CC:CC:CC. The switch shows that port 0/1 that is connected to a P C with a MAC address of AA:AA:AA. This link has a green check. Then port 0/2 off of the switch is connected to a rogue laptop with the MAC address of BA:AD:01. The link has a red circle with a line through it. Port 0/3 off of the switch is also connected to a rogue laptop with the MAC address of BA:AD:02. This link also has a red circle with a line through it.

MAC: AA:AA:AAMAC: BA:AD:01MAC: BA:AD:020/10/20/3PortAllowed MAC0/10/20/3AA:AA:AABB:BB:BBCC:CC:CC

**MEGJEGYZÉS**: A MAC-címek az egyszerűség kedvéért 24 bitesek.

11.1.3

## Portbiztonság engedélyezése

Figyeljük meg, hogy a **switchport port-security** parancs elutasításra került. Ennek az az oka, hogy a portbiztonság csak manuálisan beállított hozzáférési vagy trönk portokon konfigurálható. Alapértelmezés szerint a switch portok dynamic auto (trunking on) értékre vannak állítva. Ezért a példában a port a **switchport mode access** interfész konfigurációs paranccsal van konfigurálva.

**Note**: Trunk port security is beyond the scope of this course.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security**

Command rejected: FastEthernet0/1 is a dynamic port.

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport port-security**

S1(config-if)# **end**

S1#

A **show port-security interface** paranccsal jeleníthetjük meg a Fastethernet 0/1 aktuális portbiztonsági beállításait (lásd ábra). Figyelje meg, hogyan van engedélyezve a portbiztonság, a port állapota Biztonságos leállítás, ami azt jelenti, hogy nincsenek csatlakoztatva eszközök, és nem történt megsértés, a szabálysértési mód a Leállítás, és hogy a MAC-címek maximális száma 1. If a device is connected to the port, the switch port status would display Secure-up and the switch will automatically add the device’s MAC address as a secure MAC. Ebben a példában egyetlen eszköz sem csatlakozik a porthoz.

S1# **show port-security interface f0/1**

Port Security : Enabled

Port Status : Secure-down

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 0

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0

Security Violation Count : 0

S1#

**Note**: If an active port is configured with the **switchport port-security** command and more than one device is connected to that port, the port will transition to the error-disabled state. Ezt a feltételt később tárgyaljuk részletesen.

A portbiztonság engedélyezése után más specifikációk is konfigurálhatók, amint az a példában látható.

S1(config-if)# **switchport port-security ?**

aging Port-security aging commands

mac-address Secure mac address

maximum Max secure addresses

violation Security violation mode

S1(config-if)# **switchport port-security**

11.1.4

## MAC-címek tanulása és számuk korlátozása

A porton engedélyezett MAC-címek maximális számának beállításához használjuk a következő parancsot:

Switch(config-if)# **switchport port-security maximum** value

Az alapértelmezett portbiztonsági érték 1. A konfigurálható biztonságos MAC-címek maximális száma a switch-től és az IOS-tól függ. Ebben a példában a maximális érték 8192.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security maximum ?**

<1-8192> Maximum addresses

S1(config-if)# **switchport port-security maximum**

A switch háromféle módon konfigurálható a biztonságos MAC-címek megtanulása szempontjából:

**1. Manually Configured**

A rendszergazda manuálisan konfigurál egy biztonságos MAC-címet a porthoz a következő paranccsal:

Switch(config-if)# **switchport port-security mac-address** mac-address

**2. Dynamically Learned**

A **switchport port-security** parancs beírásakor a porthoz csatlakoztatott eszköz MAC-címe automatikusan biztonságosnak minősül, de nem kerül hozzáadásra az indító konfigurációhoz. Ha a switch újraindul, a portnak újra meg kell tanulnia az eszköz MAC-címét.

**3. Dynamically Learned – Sticky**

A rendszergazda a következő paranccsal engedélyezheti, hogy a switch dinamikusan megtanulja a MAC-címet, és hozzáadja azt az aktív konfigurációhoz:

Switch(config-if)# **switchport port-security mac-address sticky**

Az aktív konfiguráció mentése a dinamikusan tanult MAC-címet az NVRAM-ba helyezi.

The following example demonstrates a complete port security configuration for FastEthernet 0/1 with a host connected to port Fa0/1. The administrator specifies a maximum of 2 MAC addresses, manually configures one secure MAC address, and then configures the port to dynamically learn additional secure MAC addresses up to the 2 secure MAC address maximum. A konfiguráció ellenőrzéséhez használjuk a **show port-security interface** és a **show port-security address** parancsokat.

\*Mar 1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#**conf t**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport port-security**

S1(config-if)# **switchport port-security maximum 2**

S1(config-if)# **switchport port-security mac-address aaaa.bbbb.1234**

S1(config-if)# **switchport port-security mac-address sticky**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 a41f.7272.676a SecureSticky Fa0/1 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

A parancs kimenete ellenőrzi, hogy a portbiztonság engedélyezve van-e, van-e egy gazdagép csatlakoztatva a porthoz (azaz biztonságos-e), összesen 2 MAC-cím engedélyezett, és az S1 statikusan megtanult egy MAC-címet és egy MAC-címet. dinamikusan (azaz ragadósan).**show port-security interface**

A parancs kimenete felsorolja a két tanult MAC-címet.**show port-security address**

11.1.5

## Portbiztonság lejárati idő

A lejárati idő segítségével beállíthatjuk a porton lévő statikus és dinamikus biztonságos címek elévülési idejét. Portonként kétféle lejárati módszer támogatott:

* **Absolute** - The secure addresses on the port are deleted after the specified aging time.
* **Inactivity** - The secure addresses on the port are deleted only if they are inactive for the specified aging time.

A lejárati idő használatával anélkül távolíthatjuk el a MAC-címeket, hogy manuálisan kellene törölnünk azokat. A lejárati idők megnövelhetők annak érdekében, hogy a korábbi biztonságos MAC-címek megmaradjanak, még akkor is, ha új MAC-címeket adunk hozzá. A statikusan konfigurált biztonságos címek elévülése portonként engedélyezhető vagy letiltható.

A **switchport port-security aging** paranccsal engedélyezhetjük vagy tilthatjuk a statikus MAC-címek elévülését, illetve beállíthatjuk a lejárati időt vagy típust.

Switch(config-if)# **switchport port-security aging** { **static** | **time** time | **type** {**absolute** | **inactivity**}}

A parancs paramétereit a táblázat tartalmazza.

| Paraméter Leírás staticEngedélyezi az öregedést a statikusan konfigurált biztonságos használathoz címek ezen a porton.time time Adja meg a port öregedési idejét. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.type absoluteSet the absolute aging time. Az összes biztonságos cím bekapcsolva this port age out exactly after the time (in minutes) specified and are removed from the secure address list.type inactivitySet the inactivity aging type. A porton található biztonságos címek csak akkor évülnek el, ha nincs adatforgalom a biztonságos forráscím felől a megadott időtartamon belül. | |
| --- | --- |
| **Parameter** | **Description** |
| **static** | Engedélyezi a stikusan konfigurált MAC-címek elévülését. |
| **time** time | Megadja az elévülési időt. Az érték 0 és 1440 perc között lehet. Ha the time is 0, aging is disabled for this port. |
| **type absolute** | Abszolút lejárati időt határoz meg. Az összes biztonságos cím ezen a portkoron pontosan a megadott idő (percben) letelte után kerül ki, és eltávolításra kerülnek a biztonságos címlistát. |
| **type inactivity** | Inaktivitás lejárati időt határoz meg. The secure addresses on this port age out csak akkor, ha nincs adatforgalom a biztonságos forráscímről meghatározott időtartam. |

**MEGJEGYZÉS**: A MAC-címek az egyszerűség kedvéért 24 bitesek.

A példában a rendszergazda 10 perces inaktivitásra konfigurálja az elévülési típust, és a **show port-security interface** parancs segítségével ellenőrzi a konfigurációt.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport port-security aging time 10**

S1(config-if)# **switchport port-security aging type inactivity**

S1(config-if)# **end**

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1#

11.1.6

## Porbiztonság megsértési módok

Ha a porthoz csatlakozó eszköz MAC-címe nincs benne a biztonságos címek listájában, akkor portbiztonság sértés következik be. Alapértelmezés szerint a port "error-disabled" (hiba miatt letiltott) állapotba kerül.

A portbiztonság megsértési módjának beállításához használjuk a következő parancsot:

Switch(config-if)# **switchport port-security violation** { **protect** | **restrict** | **shutdown**}

Az alábbi táblázat azt mutatja be, hogy a switch hogyan reagál a bekonfigurált szabálysértési mód alapján.

### Porbiztonság megsértési módok leírása

| ModeDescriptionshutdown (alapértelmezett) A port átvált a hiba miatt letiltottra state immediately, turns off the port LED, and sends a syslog message. Ez increments the violation counter. Ha egy biztonságos port található a error-disabled state, an administrator must re-enable it by entering the leállítás és nincs leállítási parancs. limitA port eldobja a csomagokat ismeretlen forráscímeket, amíg el nem távolít elegendő számú biztonságos MAC-t hogy a maximálisan megengedett érték alá kerüljünk, vagy meg nem növeljük a maximális értéket. This mode causes the Security Violation counter to increment and generates a syslog message.protectThis is the least secure of the security violation üzemmód. A port eldobja az ismeretlen MAC-forráscímű csomagokat, amíg Ön távolítson el elegendő számú biztonságos MAC-címet, hogy a maximum alá csökkenjen vagy meg nem növeljük a maximális értéket. Nem küld syslog üzenetet. | |
| --- | --- |
| **Mód** | **Leírás** |
| **shutdown**  (default) | A port azonnal hiba miatt letiltott állapotba kerül, kikapcsolja a port LED-jét, és küld egy syslog üzenetet. Megnöveli a hibaszámláló értékét. Ha egy biztonságos port hiba miatt letiltott állapotban van, egy a rendszergazdának újra engedélyeznie kell a(z) **shutdown** and **no shutdown** commands. |
| **restrict** | A port eldobja az ismeretlen forráscímű csomagokat, amíg el nem távolítja a elegendő számú biztonságos MAC-cím ahhoz, hogy a maximum alá csökkenjen vagy meg nem növeljük a maximális értéket. Ez a mód a Biztonságot okozza Violation counter to increment and generates a syslog message. |
| **protect** | Ez a legkevésbé biztonságos az üzemmódok között. A port leesik ismeretlen MAC-forráscímű csomagokat, amíg el nem távolítja a megfelelőt biztonságos MAC-címek száma, hogy a maximális érték alá csökkenjen, vagy increase the maximum value. Nem küld syslog üzenetet. |

### Portbiztonság megsértési módok összehasonlítása

| Violation Mode Discards Offending Traffic Sends Syslog MessageIncrease Violation CounterShuts Down PortProtect Yes No No NoRestrict YesYes Yes NoShutdown YesYes Yes Yes | | | | |
| --- | --- | --- | --- | --- |
| **Mód** | **Forgalom tiltás** | **Syslog üzenet** | **Hibaszámláló növelés** | **Port letiltás** |
| Védelem (Protect) | Igen | Nem | Nem | Nem |
| Korlátozás (Restrict) | Igen | Igen | Igen | Nem |
| Letiltás (Shutdown) | Igen | Igen | Igen | Igen |

A következő példában a rendszergazda a biztonsági üzemmódot „restrict” beállításra módosítja. A **show port-security interface** parancs kimenete megerősíti, hogy a módosítás megtörtént.

S1(config)# **interface f0/1**

S1(config-if)# **switchport port-security violation restrict**

S1(config-if)# **end**

S1#

S1# **show port-security interface f0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Restrict

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7272.676a:1

Security Violation Count : 0

S1#

11.1.7

## Hiba miatt letiltott portok

Mi történik, ha a port biztonságának megsértése leáll, és port megsértése történik? The port is physically shutdown and placed in the error-disabled state, and no traffic is sent or received on that port.

Az ábrán a portbiztonság megsértése visszaállt az alapértelmezett leállítási beállításra. Ezután az a41f.7272.676a MAC-című gazdagépet leválasztják, és egy új gazdagépet csatlakoztatnak a Fa0/1-hez.

Figyelje meg, hogyan jön létre a portbiztonsággal kapcsolatos üzenetek sorozata a konzolon.

S1(config)# **int fa0/1**

S1(config-if)# **switchport port-security violation shutdown**

S1(config-if)# **end**

S1#

\*Mar 1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1#

\*Mar 1 00:24:32.829: %PM-4-ERR\_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state

\*Mar 1 00:24:32.838: %PORT\_SECURITY-2-PSECURE\_VIOLATION: Security violation occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.

\*Mar 1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar 1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

S1#

**Note**: The port protocol and link status are changed to down and the port LED is turned off.

A példában a **show interface** parancs megmutatja, hogy a port állapota "**err-disabled**". Az interfész parancs kimenete mostantól a port állapotát Biztonságos leállításként mutatja a Biztonságos leállítás helyett.**show port-security** A portbiztonság hibaszámlálója 1-gyel növekszik.

S1# **show interface fa0/1 | include down**

FastEthernet0/18 is down, line protocol is down (err-disabled)

(output omitted)

S1# **show port-security interface fa0/1**

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7273.018c:1

Security Violation Count : 1

S1#

A rendszergazdának meg kell határoznia, hogy mi okozta a portbiztonság megsértését. Ha egy nem engedélyezett eszköz csatlakozik a porthoz, a port újbóli engedélyezése előtt meg szüntetni a biztonsági fenyegetést.

A következő példában az első gazdagép újracsatlakozik a Fa0/1-hez. A port újbóli engedélyezéséhez először használjuk a **shutdown** parancsot, majd a port működőképessé tételéhez a **no shutdown** parancsot, amint az a példában látható.

S1(config)# **interface fa0/1**

S1(config-if)# **shutdown**

S1(config-if)#

\*Mar 1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

S1(config-if)# **no shutdown**

S1(config-if)#

\*Mar 1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up

\*Mar 1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#

11.1.8

## Portbiztonság ellenőrzése

Egy switch portbiztonsági beállítása után ellenőrizzük, hogy megfelelően lettek-e konfigurálva az egyes opciók és a statikusan beírt MAC-címek is helyesek-e.

**Portbiztonság minden interfészhez**

Egy switch portbiztonsági beállításainak megjelenítéséhez használjuk a **show port-security** parancsot. A példában mind a 24 interfész konfigurálva van a **switchport port-security** paranccsal, a megengedett maximális érték 1, a szabálysértési mód pedig lekapcsolás. Nincs csatlakoztatott eszköz. Ezért a CurrentAddr (Count) értéke 0 minden egyes interfész esetén.

S1# **show port-security**

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

---------------------------------------------------------------------------

Fa0/1 2 2 0 Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

**Portbiztonság egy adott interfészen**

A **show port-security interface** paranccsal megtekinthetjük egy adott interfész beállításait, ahogy a korábbi példákban és ebben is látható.

S1# **show port-security interface fastethernet 0/1**

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 10 mins

Aging Type : Inactivity

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 2

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : a41f.7273.018c:1

Security Violation Count : 0

S1#

**A megtanult MAC-címek ellenőrzése**

A MAC-címek konfigurációban való jelenlétének ellenőrzésére használjuk a **show run** parancsot a példában látható módon.

S1# **show run interface fa0/1**

Building configuration...

Current configuration : 365 bytes

!

interface FastEthernet0/1

switchport mode access

switchport port-security maximum 2

switchport port-security mac-address sticky

switchport port-security mac-address sticky a41f.7272.676a

switchport port-security mac-address aaaa.bbbb.1234

switchport port-security aging time 10

switchport port-security aging type inactivity

switchport port-security

end

S1#

**Biztonságos MAC-címek ellenőrzése**

Az összes kézzel konfigurált vagy dinamikusan megtanult biztonságos MAC-cím megjelenítéséhez használjuk a példában látható **show port-security address** parancsot.

S1# **show port-security address**

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 a41f.7272.676a SecureSticky Fa0/1 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/1 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 1

Max Addresses limit in System (excluding one mac per port) : 8192

S1#

11.1.9

## Parancsszimulátor - Portbiztonság megvalósítása

Switch portbiztonságának megvalósítása a megadott követelmények alapján

You are currently logged into S1. Állítsa be a FastEthernet 0/5 portbiztonságot a következő követelményekkel: \* Használja a **fa0/5** interfész nevet az interfész konfigurációs módba való belépéshez.

* Enable the port for access mode.
* Enable port security.
* Set the maximum number of MAC address to 3.
* Statically configure the MAC address aaaa.bbbb.1234.
* Configure the port to dynamically learn additional MAC addresses and dynamically add them to the running configuration.
* Return to privileged EXEC mode.

S1(config)#interface fa0/5

S1(config-if)#switchport mode access

S1(config-if)#switchport port-security

S1(config-if)#switchport port-security maximum 3

S1(config-if)#switchport port-security mac-address aaaa.bbbb.1234

S1(config-if)#switchport port-security mac-address sticky

S1(config-if)#end

Enter the command to verify port security for all interfaces.

S1#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

---------------------------------------------------------------------------

Fa0/5 3 2 0 Shutdown

---------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

Enter the command to verify port security on FastEthernet 0/5. Használja a **fa0/5** értéket az interfész nevéhez.

S1#show port-security interface fa0/5

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 2

Configured MAC Addresses : 1

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0090.2135.6B8C:1

Security Violation Count : 0

Enter the command that will display all of the addresses to verify that the manually configured and dynamically learned MAC addresses are in the running configuration.

S1#show port-security address

Secure Mac Address Table

-----------------------------------------------------------------------------

Vlan Mac Address Type Ports Remaining Age

(mins)

---- ----------- ---- ----- -------------

1 0090.2135.6b8c SecureSticky Fa0/5 -

1 aaaa.bbbb.1234 SecureConfigured Fa0/5 -

-----------------------------------------------------------------------------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

You have successfully configured and verified port security for the interface.

11.1.10

## Packet Tracer - Portbiztonság megvalósítása

Ebben a feladatban beállítjuk egy switch portbiztonságát majd teszteljük azt. A portbiztonság lehetővé teszi, hogy korlátozzuk a portok használatát, és csak bizonyos MAC-című eszközökről engedjünk forgalmat az adott portra.

[Implement Port Security](https://contenthub.netacad.com/courses/srwe-dl/_common/11.1.10-packet-tracer---implement-port-security_hu-HU.pka)

[11.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. VLAN-támadások kiküszöbölése

# VLAN-támadások kiküszöbölése

11.2.1

## VLAN-támadások áttekintése

Áttekintésként, egy VLAN-ugrásos (VLAN hopping) támadás háromféle módon következhet be:

* A támadó állomás hamis DTP-üzeneteinek hatására a switch trönk üzemmódba lép. Ekkor a támadó a cél VLAN címkéjével elküldött forgalmát a switch továbbítani fogja a célállomásnak.
* Illegális switch bekötése a hálózatba trönk üzemmódban. A támadó ezután hozzáférhet a megtámadott switch-en lévő összes VLAN-hoz az illegális switch-ről.
* A VLAN-ok támadásának egy másik típusa a kettős címkézéssel (vagy kettős beágyazással) végrehajtott VLAN-ugrás. Ez a támadástípus azt a módot használja ki, ahogyan a legtöbb switch hardvere működik.

11.2.2

## A VLAN-ugrásos támadások enyhítésének lépései

A VLAN-ugrásos támadások enyhítéséhez kövessük az alábbi lépéseket:

**Step 1**: Disable DTP (auto trunking) negotiations on non-trunking ports by using the **switchport mode access** interface configuration command.

**Step 2**: Disable unused ports and put them in an unused VLAN.

**Step 3**: Manually enable the trunk link on a trunking port by using the **switchport mode trunk** command.

**Step 4**:4. A DTP automatikus egyeztetés letiltása a trönk portokon a**switchport nonegotiate** parancs használatával.

**Step 5**: Set the native VLAN to a VLAN other than VLAN 1 by using the **switchport trunk native vlan** vlan\_number command.

Tegyük fel például a következőket:

* A FastEthernet 0/1 - 0/16 aktív hozzáférési portok
* FastEthernet ports 0/17 through 0/20 are not currently in use
* A FastEthernet 0/21 - 0/24 közötti portok trönk portok.

A VLAN-ugrásos támadás a következő konfiguráció végrehajtásával csökkenthető.

S1(config)# **interface range fa0/1 - 16**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **exit**

S1(config)#

S1(config)# **interface range fa0/17 - 20**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 1000**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **exit**

S1(config)#

S1(config)# **interface range fa0/21 - 24**

S1(config-if-range)# **switchport mode trunk**

S1(config-if-range)# **switchport nonegotiate**

S1(config-if-range)# **switchport trunk native vlan 999**

S1(config-if-range)# **end**

S1#

* A FastEthernet 0/1—0/16 portok hozzáférési portok, emiatt a trönkölés le van tiltva.
* A FastEthernet 0/17-0/20 portok nem használt portok, le vannak tiltva és egy nem használt VLAN-hoz vannak rendelve.
* A FastEthernet 0/21 és 0/24 közötti portok manuálisan beállított trönk kapcsolatok, és ki van kapcsolva a DTP egyeztetés. A natív VLAN is meg van változtatva az alapértelmezett VLAN 1-ről a nem használt VLAN 999-re.

11.2.3

## Parancsszimulátor - A VLAN-ugrásos támadások enyhítése

Küszöböljük ki a VLAN-ugrásos támadásokat a megadott követelmények alapján.

You are currently logged into S1. The ports status of the ports are as follows:

* FastEthernet ports 0/1 through 0/4 are used for trunking with other switches.
* FastEthernet ports 0/5 through 0/10 are unused.
* FastEthernet ports 0/11 through 0/24 are active ports currently in use.

Use **range fa0/1 - 4** to enter interface configuration mode for the trunks.

S1(config)#interface range fa0/1 - 4

Configure the interfaces as nonnegotiating trunks assigned to default VLAN 99.

S1(config-if-range)#switchport mode trunk

S1(config-if-range)#switchport nonegotiate

S1(config-if-range)#switchport trunk native vlan 99

S1(config-if-range)# exit

Használja a **fa0/5 - 10** tartományt, hogy belépjen a nem használt portok interfész konfigurációs módjába.

S1(config)#interface range fa0/5 - 10

Configure the unused ports as access ports, assign them to VLAN 86, and shutdown the ports.

S1(config-if-range)#switchport mode access

S1(config-if-range)#switchport access vlan 86

% Access VLAN does not exist. Creating vlan 86

S1(config-if-range)#shutdown

\*Mar 1 00:28:48.883: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

\*Mar 1 00:28:48.900: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

\*Mar 1 00:28:48.908: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

\*Mar 1 00:28:48.917: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

\*Mar 1 00:28:48.942: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

\*Mar 1 00:28:48.950: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

\*Mar 1 00:28:49.890: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

\*Mar 1 00:28:49.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to down

S1(config-if-range)# exit

Use range **fa0/11 - 24** to enter interface configuration mode for the active ports and then configure them to prevent trunking.

S1(config)#interface range fa0/11 - 24

S1(config-if-range)#switchport mode access

S1(config-if-range)# end

S1#

You have successfully mitigated VLAN hopping attacks on this switch.

[11.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Portbiztonság megvalósítása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. DHCP-támadások kiküszöbölése

# DHCP-támadások kiküszöbölése

11.3.1

## DHCP-támadás áttekintése

A DHCP-kiéheztetés (starvation) támadás célja egy szolgáltatásmegtagadás (DoS) létrehozása a kapcsolódni szándékozó ügyfelek felé. A DHCP-kiéheztetés támadásokhoz olyan támadási eszközre van szükség, amilyen például a Gobbler. Emlékezzünk vissza, hogy a DHCP-kiéheztetési támadások hatékonyan mérsékelhetők a portbiztonság használatával, mivel a Gobbler minden elküldött DHCP-kéréshez egyedi forráskódú MAC-címet használ.

A DHCP-hamisítás (spoofing) elleni támadások enyhítése azonban fokozottabb védelmet igényel. A Gobbler beállítható úgy, hogy a tényleges interfész MAC-címét használja forrásként, de a DHCP-üzenet belsejében egy másik Ethernet-címet adjon meg. Ez hatástalanítja a portbiztonságot, mert a forrás MAC-cím biztonságosnak tekintett.

A DHCP-hamisítási támadások megbízható (trusted) portokon DHCP snooping használatával mérsékelhetők.

11.3.2

## DHCP Snooping

A DHCP snooping (szaglászás) nem a forrás MAC-címeken alapul. Azt határozza meg, hogy a DHCP-üzenetek megbízható vagy nem megbízható forrásból származnak-e. Ennek alapján szűri a DHCP-üzeneteket és korlátozza a nem megbízható forrásokból érkező DHCP-forgalmat.

A felügyelet alatt álló eszközök, például a switch-ek, router-ek és a szerverek megbízható források. A tűzfalon vagy a hálózaton kívüli bármely más eszköz nem megbízható forrás. Továbbá az összes hozzáférési port általában nem megbízható forrás. Az ábrán egy példa látható a megbízható és a nem megbízható portokra.

The diagram shows a DHCP server at the upper right side of topology that is connected to a distribution switch below it. The distribution switch is connected to another distribution switch to the left of the diagram and access switch below it. The other distribution switch has an access switch connected below it. Both access switches have a connection to both distribution switches, but to each other. The access switch on the right has a PC below it and the other access switch has a PC with a rogue character under it. The diagram shows a purple square for trusted ports and a red circle for untrusted ports. There is are purple squares between the DHCP server and the distribution switch, as well as between each link between all of the switches. However, there is a red circle between the two PCs and the access switches.

DHCP ClientDHCP-kiszolgálóRogue DHCP ServerTrusted portUntrusted port

Notice that the rogue DHCP server would be on an untrusted port after enabling DHCP snooping. Alapértelmezés szerint minden interfész nem megbízhatóként van beállítva. A megbízható interfészek jellemzően trönk kapcsolatok, vagy olyan portok, amelyek közvetlenül kapcsolódnak egy saját DHCP-kiszolgálóhoz. Ezeket az interfészeket manuálisan kell megbízhatónak konfigurálni.

Ilyenkor egy DHCP-tábla épül fel, amely tartalmazza a nem megbízható porton lévő eszköz MAC-címét és a DHCP-kiszolgáló által adott IP-címet. A MAC-cím és az IP-cím egymáshoz van rendelve. Ezt a táblázatot DHCP snooping kötési táblának nevezik.

11.3.3

## A DHCP snooping megvalósításának lépései

A DHCP snooping engedélyezéséhez kövessük az alábbi lépéseket:

**1**. Engedélyezzük a DHCP snooping-ot az **ip dhcp snooping** globális konfigurációs paranccsal.

**2**. A megbízható portokon használjuk az **ip dhcp snooping trust** parancsot.

**3**. Korlátozza a nem megbízható portokon másodpercenként fogadható DHCP-felderítési üzenetek számát az **ip dhcp snooping limit rate** csatolókonfigurációs paranccsal.

**4**. Engedélyezzük a DHCP snooping-ot VLAN-onként a **ip dhcp snooping** paranccsal.

11.3.4

## DHCP snooping konfigurációs példa

A DHCP snooping példához tartozó referencia topológia az ábrán látható. Figyeljük meg, hogy az F0/5 nem megbízható port, mert egy számítógéphez csatlakozik. Az F0/1 megbízható port, mivel a DHCP-kiszolgálóhoz csatlakozik.

The graphic has a legend with a Purple square Trusted Port and a red circle Untrusted Port below the topology diagram. Then the graphic shows a LAN network with a switch with trusted and untrusted ports. A kapcsoló bal oldalán egy PC, a jobb oldalon pedig egy DHCP van csatlakoztatva. A PC-hez csatlakozó interfészen piros kör látható a nem megbízható interfésznél, a DHCP szerverhez csatlakoztatott interfészen pedig a megbízható portot jelölő lila négyzet.

192.168.10.10 F0/5 S1

F0/1

DHCP-kiszolgálóTrusted PortUntrusted Port

Az alábbiakban egy példa látható a DHCP snooping konfigurálására. Figyeljük meg, hogy az első parancs a DHCP snooping engedélyezése. Ezután a DHCP-kiszolgáló interfésze megbízhatónak lesz beállítva. Az F0/5 - F0/24 portok tartománya alapértelmezés szerint nem megbízható, ezért az üzenetfogadás másodpercenként hat csomagra van beállítva. Végül a DHCP snooping engedélyezve van a VLAN 5, 10, 50, 51 és 52-n.

S1(config)# **ip dhcp snooping**

S1(config)# **interface f0/1**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **exit**

S1(config)# **interface range f0/5 - 24**

S1(config-if-range)# **ip dhcp snooping limit rate 6**

S1(config-if-range)# **exit**

S1(config)# **ip dhcp snooping vlan 5,10,50-52**

S1(config)# **end**

S1#

A **show ip dhcp snooping** paranccsal ellenőrizhető a DHCP snooping, a **show ip dhcp snooping binding** paranccsal pedig megtekinthetők azok az ügyfelek, amelyek DHCP-információkat kaptak (lásd ábra).

**MEGJEGYZÉS**: DHCP snooping szükséges a DAI számára (Dynamic ARP Inspection), amely a következő témakörben kerül tárgyalásra.

S1# **show ip dhcp snooping**

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

5,10,50-52

DHCP snooping is operational on following VLANs:

none

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

FastEthernet0/1 yes yes unlimited

Custom circuit-ids:

FastEthernet0/5 no no 6

Custom circuit-ids:

FastEthernet0/6 no no 6

Custom circuit-ids:

S1# **show ip dhcp snooping binding**

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD 192.168.10.11 193185 dhcp-snooping 5 FastEthernet0/5

11.3.5

## Parancsszimulátor - DHCP-támadások enyhítése

Végezzük el a DHCP snooping beállítását egy switch-en a következő topológia és a megadott követelmények alapján.

The syntax checker has a topology that has a distribution switch connected to an access switch G0/1 interface. The access switch F0/1 interface connects to P C to the left and on the right side the switch G0/2 interface is connected to a server.

S1 F0/1 G0/1

G0/2

DHCP-kiszolgáló

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for **g0/1 - 2**, trust the interfaces, and return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#exit

Enter interface configuration mode for **f0/1 - 24**, limit the DHCP messages to no more than 10 per second, and return to global configuration mode.

S1(config)#interface range f0/1 - 24

S1(config-if-range)#ip dhcp snooping limit rate 10

S1(config-if-range)#exit

Enable DHCP snooping for VLANs **10,20,30-49**.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)# exit

Enter the command to verify DHCP snooping.

S1#show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

10,20,30-49

DHCP snooping is operational on following VLANs:

none

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)

----------------------- ------- ------------ ----------------

GigabitEthernet0/1 yes yes unlimited

Custom circuit-ids:

GigabitEthernet0/2 yes yes unlimited

Custom circuit-ids:

FastEthernet0/1 no no 10

Custom circuit-ids:

Enter the command to verify the current DHCP bindings logged by DHCP snooping

S1#show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

------------------ --------------- ---------- ------------- ---- --------------------

00:03:47:B5:9F:AD 10.0.0.10 193185 dhcp-snooping 5 FastEthernet0/1

S1#

You have successfully configured and verified DHCP snooping for the switch.

[11.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[VLAN-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[ARP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. ARP-támadások kiküszöbölése

# ARP-támadások kiküszöbölése

11.4.1

## Dinamikus ARP-ellenőrzés

In a typical ARP attack, a threat actor can send unsolicited ARP requests to other hosts on the subnet with the MAC Address of the threat actor and the IP address of the default gateway. Az ARP-hamisítás és az ebből eredő ARP-mérgezés megelőzése érdekében a switch-nek biztosítania kell, hogy csak érvényes ARP-kérések és válaszok legyenek továbbítva.

A dinamikus ARP-ellenőrzés (Dynamic ARP inspection, DAI) működéséhez DHCP snooping szükséges, és ezáltal segít megelőzni az ARP-támadásokat:

* Not relaying invalid or gratuitous ARP Requests out to other ports in the same VLAN.
* Elfogja az ARP-kérelmeket és válaszokat a nem megbízható portokon.
* Minden elfogott csomagot ellenőriz egy érvényes IP-MAC összerendelés végett.
* Dropping and logging ARP Requests coming from invalid sources to prevent ARP poisoning.
* Hiba miatt letiltott állapotba helyezi az interfészt, ha az ARP-csomagok száma túllépi a DAI-ban konfigurált értéket.

11.4.2

## A DAI megvalósításának irányelvei

Az ARP-hamisítás és az ARP-mérgezés elkerülése érdekében kövessük az alábbi irányelveket:

* Engedélyezzük globálisan a DHCP snooping szolgáltatást.
* Engedélyezzük a DHCP snooping szolgáltatást a kijelölt VLAN-okon.
* Engedélyezzük a DAI-t a kiválasztott VLAN-okon.
* Konfiguráljunk megbízható interfészeket a DHCP snooping és az ARP-ellenőrzés szolgáltatásokhoz.

Ajánlatos az összes hozzáférési switch portot nem megbízhatóként konfigurálni, a többi switch felé vezető uplink portokat pedig megbízhatóként beállítani.

A minta topológiában megbízható és nem megbízható portok láthatók.

The graphic shows a legend with a Purple square Trusted Port and a red circle Untrusted Port, above that is a LAN diagram showing Dynamic ARP Inspection Trust. The diagram illustrates a LAN network with trusted and untrusted ports. Az egyik interfészen a bal alsó sarokban egy támadó található az egyik számítógépen, a bal felső sarokban pedig egy hagyományos PC. Mindkét eszköz csatlakozik a switch-hez, és mindkettő kapcsolóportján piros kör látható, amely nem megbízható portot jelöl. To the right of the switch is a router that is also connected to the switch. The router connection has a purple square on the switch that symbolizes a trusted connection for ARP.

PC-A S1 R1 F0/1 F0/2

F0/24

Untrusted PortTrusted PortVLAN 10

11.4.3

## DAI konfigurációs példa

Az előző topológiában az S1-hez két felhasználó csatlakozik a VLAN 10-en. A DAI úgy lesz beállítva, hogy enyhítse az ARP-hamisítás és az ARP-mérgezés támadásokat.

Amint az a példában látható, a DHCP snooping engedélyezve van, mert a DAI megköveteli a DHCP snooping kötési táblázat működését. A DHCP snooping és az ARP-ellenőrzés engedélyezett a VLAN10-ben. A router felé irányuló port megbízhatóként van konfigurálva a DHCP snooping és az ARP-ellenőrzés végrehajtásához.

S1(config)# **ip dhcp snooping**

S1(config)# **ip dhcp snooping vlan 10**

S1(config)# **ip arp inspection vlan 10**

S1(config)# **interface fa0/24**

S1(config-if)# **ip dhcp snooping trust**

S1(config-if)# **ip arp inspection trust**

A DAI úgy is konfigurálható, hogy ellenőrizze a cél- vagy a forrás MAC-címeket és IP-címeket:

* **Destination MAC** - Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body.
* **Source MAC** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
* **IP address** - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Az **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** globális konfigurációs paranccsal konfigurálhatjuk a DAI-t az ARP-csomagok eldobására, ha az IP-címek érvénytelenek. Ez akkor lép működésbe, ha az ARP-csomagokban lévő MAC-címek nem egyeznek meg az Ethernet fejlécben szereplő címekkel. A következő példában megfigyelhetjük hogyan lehet egyetlen parancsban elvégezni a beállítást. Mivel több **ip arp inspection validate** parancs beírása felülírja az előzőt. Ha egynél több érvényesítési módszert szeretnénk használni, írjuk be őket ugyanabba a parancsba az alább látható módon.

S1(config)# **ip arp inspection validate ?**

dst-mac Validate destination MAC address

ip Validate IP addresses

src-mac Validate source MAC address

S1(config)# **ip arp inspection validate src-mac**

S1(config)# **ip arp inspection validate dst-mac**

S1(config)# **ip arp inspection validate ip**

S1(config)# **do show run | include validate**

ip arp inspection validate ip

S1(config)# **ip arp inspection validate src-mac dst-mac ip**

S1(config)# **do show run | include validate**

ip arp inspection validate src-mac dst-mac ip

S1(config)#

11.4.4

## Parancsszimulátor - ARP-támadások enyhítése

Állítsuk be a DAI-t a topológia és meghatározott követelményeken alapján.

The syntax checker has a topology that has a distribution switch connected to an access switchs G0/1 interface. The access switchs F0/1 interface connects to PC to the left and on the right side the switch G0/2 interface is connected to a server.

S1 F0/1 G0/1

G0/2

DHCP-kiszolgáló

You are currently logged into S1. Enable DHCP snooping globally for the switch.

S1(config)#ip dhcp snooping

Enter interface configuration mode for **g0/1 - 2**, trust the interfaces for both DHCP snooping and DAI, and then return to global configuration mode.

S1(config)#interface range g0/1 - 2

S1(config-if-range)#ip dhcp snooping trust

S1(config-if-range)#ip arp inspection trust

S1(config-if-range)#exit

Enable DHCP snooping and DAI for VLANs **10,20,30-49**.

S1(config)#ip dhcp snooping vlan 10,20,30-49

S1(config)#ip arp inspection vlan 10,20,30-49

S1(config)#

You have successfully configured DAI for the switch.

[11.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[DHCP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[STP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. STP-támadások kiküszöbölése

# STP-támadások kiküszöbölése

11.5.1

## PortFast és BPDU Guard

Emlékezzünk vissza, hogy a támadók manipulálhatják az STP-protokollt (Spanning Tree Protocol) a gyökérponti híd meghamisításával és a hálózat topológiájának megváltoztatásával. Az STP-protokoll ellen irányuló manipulációs támadások enyhítésére használjuk a PortFast és a BPDU Guard (Bridge Protocol Data Unit) eszköket:

* **PortFast** - PortFast immediately brings an interface configured as an access port to the forwarding state from a blocking state, bypassing the listening and learning states. Az összes végfelhasználói portra alkalmazzuk. A PortFast beállítást csak a végberendezéseket csatlakoztató portokon konfiguráljunk.
* **BPDU Guard** - BPDU guard immediately error disables a port that receives a BPDU. A PortFasthoz hasonlóan a BPDU-t is csak a végberendezésekhez csatlakoztatott interfészeken konfiguráljunk.

Az ábrán az S1 hozzáférési portjait a PortFast és a BPDU Guard segítségével kell konfigurálni.

There are two distribution layer 3 switches at the top of the diagram that are connected by a trunk.  
Both layer 3 switches have a trunk link that are connected to the same access layer 2 switch below. This named S1 and is connected on int G0/1 and G0/2. Below S1 are several PCs and to the side of the switch it states Access Ports F0/1 - F0/24.

G0/1 G0/2 F0/1 - F0/24

S1

TrunkTrunkTrunkAccess Ports

11.5.2

## PortFast konfigurálása

A PortFast kihagyja az STP figyelési és tanulási állapotait, így minimálisra csökkenti az STP-konvergenciára fordított időt. Ha a PortFast-ot egy másik switch-hez csatlakozó porton használjuk kockáztatjuk egy feszítőfa hurok létrejöttét.

A PortFast a **spanning-tree portfast** interfész konfigurációs paranccsal engedélyezhető egy interfészen. Alternatív megoldásként a Portfast globálisan is konfigurálható az összes hozzáférési porton a **spanning-tree portfast default** globális konfigurációs paranccsal.

A PortFast globális ellenőrzéséhez a **show running-config | begin span** vagy a **show spanning-tree summary** parancsokat használhatjuk. A PortFast interfészen történő engedélyezését a **show running-config interface** type/number paranccsal ellenőrizhetjük az ábrán látható módon. A **show** **spanning-tree interface** type/number **detail** parancs is használható az ellenőrzéshez.

Figyeljük meg, ha a PortFast engedélyezve van, figyelmeztető üzenetek jelennek meg.

S1(config)# **interface fa0/1**

S1(config-if)# **switchport mode access**

S1(config-if)# **spanning-tree portfast**

%Warning: portfast should only be enabled on ports connected to a single

host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when portfast is enabled, can cause temporary bridging loops.

Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only

have effect when the interface is in a non-trunking mode.

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast default**

%Warning: this command enables portfast by default on all interfaces. You

should now disable portfast explicitly on switched ports leading to hubs,

switches and bridges as they may create temporary bridging loops.

S1(config)# **exit**

S1# **show running-config | begin span**

spanning-tree mode pvst

spanning-tree portfast default

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport mode access

spanning-tree portfast

!

interface FastEthernet0/2

!

interface FastEthernet0/3

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

(output omitted)

S1#

11.5.3

## A BPDU Guard konfigurálása

Annak ellenére, hogy a PortFast engedélyezve van, az interfész továbbra is figyeli a BPDU-üzeneteket. Egy nem várt BPDU lehet a véletlen műve, vagy egy jogosulatlan kísérlet része, amelyben egy switch-et adnak a hálózathoz.

Ha egy BPDU Guard szolgáltatással engedélyezett porton BPDU-k érkeznek, akkor a port hiba miatt letiltott állapotba kerül. Ez azt jelenti, hogy a port lekapcsol, és manuálisan kell újra engedélyezni, vagy automatikusan lehet visszaállítani a **errdisable recovery cause bpduguard** globális paranccsal.

A BPDU Guard a **spanning-tree bpduguard enable** interfész konfigurációs paranccsal engedélyezhető egy porton. A **spanning-tree portfast bpduguard default** globális konfigurációs parancs a BPDU-védelmet az összes PortFast-tal konfigurált porton bekapcsolja.

A feszítőfa állapotára vonatkozó információk megjelenítéséhez használjuk a **show spanning-tree summary** parancsot. A példában a PortFast és a BPDU Guard egyaránt alapértelmezetten engedélyezett a hozzáférési portokon.

**Note**: Always enable BPDU Guard on all PortFast-enabled ports.

S1(config)# **interface fa0/1**

S1(config-if)# **spanning-tree bpduguard enable**

S1(config-if)# **exit**

S1(config)# **spanning-tree portfast bpduguard default**

S1(config)# **end**

S1# **show spanning-tree summary**

Switch is in pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

(output omitted)

S1#

11.5.4

## Parancsszimulátor - STP-támadások enyhítése

Állítsuk be a PortFast és a BPDU Guard szolgáltatásokat a topológia és a megadott követelmények alapján.

The syntax checker has a topology that is the same as the diagram in 11.5.1; where there are two distribution layer 3 switches at the top of the diagram that are connected by a trunk. Both layer 3 switches have a trunk link that are connected to the same access layer 2 switch below. This named S1 and is connected on int G0/1 and G0/2. Below S1 are several PCs and to the side of the switch it states Access Ports F0/1 - F0/24.12.1.5 The diagram shows where various technologies operate within the electromagnetic spectrum. Types of waves from left to right are; radio waves, infrared, ultraviolet, X-rays, and gamma rays. The wave frequency increases from left to right. Wireless devices including radio towers, radios, TVs, microwave ovens and satellite dishes, are listed under the left side.

G0/1 G0/2 F0/1 - F0/24

S1

TrunkTrunkTrunkAccess Ports

You are currently logged into S1. Complete the following steps to implement PortFast and BPDU Guard on all access ports:

* Enter interface configuration mode for **fa0/1 - 24**.
* Configure the ports for access mode.
* Return to global configuration mode.
* Enable PortFast by default for all access ports.
* Enable BPDU Guard by default for all access ports.

S1(config)#interface range fa0/1 - 24

S1(config-if-range)#switchport mode access

S1(config-if-range)#exit

S1(config)#spanning-tree portfast default

S1(config)#spanning-tree portfast bpduguard default

S1(config)# exit

Verify that PortFast and BPDU Guard is enabled by default by viewing STP summary information.

S1#show spanning-tree summary

Switch is in pvst mode

Root bridge for: none

Extended system ID is enabled

Portfast Default is enabled

PortFast BPDU Guard Default is enabled

Portfast BPDU Filter Default is disabled

Loopguard Default is disabled

EtherChannel misconfig guard is enabled

UplinkFast is disabled

BackboneFast is disabled

Configured Pathcost method used is short

(output omitted)

S1#

You have successfully configured and verified PortFast and BPDU Guard for the switch.

[11.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[ARP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[11.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Switch biztonságának beállítása
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

11.6.1

## Packet Tracer - Switch biztonságának beállítása

A Packet Tracer feladat során a következőket fogjuk elvégezni:

* Használaton kívüli portok védelme
* Portbiztonság megvalósítása
* VLAN-ugrásos támadások enyhítése
* DHCP-támadások enyhítése
* ARP-támadások enyhítése
* STP-támadások enyhítése
* Switch biztonsági beállításainak ellenőrzése

[Switch biztonságának beállítása](https://contenthub.netacad.com/courses/srwe-dl/_common/11.6.1-packet-tracer---switch-security-configuration_hu-HU.pka)

11.6.2

## Laborgyakorlat - Switch biztonságának beállítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Használaton kívüli portok védelme
* Portbiztonság megvalósítása
* VLAN-ugrásos támadások enyhítése
* DHCP-támadások enyhítése
* ARP-támadások enyhítése
* STP-támadások enyhítése
* Switch biztonsági beállításainak ellenőrzése

11.6.3

## Miről tanultunk ebben a fejezetben?

Minden portot (interfészt) védeni kell, mielőtt a switch a végleges környezetébe kerül. A legegyszerűbb és leghatékonyabb módszer a MAC-címtábla túlcsordulási támadások megakadályozására a portbiztonság engedélyezése. Alapértelmezés szerint a switch portok dynamic auto (trunking on) értékre vannak állítva. A switch egy biztonságos porton háromféle módon ismerhet meg MAC-címeket: manuálisan konfigurált, dinamikusan tanult és dinamikusan tanult sticky opcióval. A lejárati idő segítségével beállíthatjuk a porton lévő statikus és dinamikus biztonságos címek elévülési idejét. Portonként kétféle elévülés támogatott: abszolút és inaktivitás alapú. Ha a porthoz csatlakozó eszköz MAC-címe nincs benne a biztonságos címek listájában, akkor portbiztonság sértés következik be. Alapértelmezés szerint a port "error-disabled" (hiba miatt letiltott) állapotba kerül. Az "error-disabled" állapotban levő port ténylegesen lekapcsolódik, vagyis nem küldhet és nem fogadhat adatokat. Egy switch portbiztonsági beállításainak megjelenítéséhez használjuk a **show port-security** parancsot.

A VLAN-ugrásos támadások enyhítése érdekében:

**Step 1.** Disable DTP negotiations on non-trunking ports. **Step 2.** Disable unused ports. **Step 3.** Manually enable the trunk link on a trunking port. **Step 4.** Disable DTP negotiations on trunking ports. **Step 5.** Set the native VLAN to a VLAN other than VLAN 1.

A DHCP-kiéheztetés (starvation) támadás célja egy szolgáltatásmegtagadás (DoS) létrehozása a kapcsolódni szándékozó ügyfelek felé. A DHCP-hamisítási támadások megbízható (trusted) portokon DHCP snooping használatával mérsékelhetők. A DHCP snooping azt határozza meg, hogy a DHCP-üzenetek megbízható vagy nem megbízható forrásból származnak-e. Ennek alapján szűri a DHCP-üzeneteket és korlátozza a nem megbízható forrásokból érkező DHCP-forgalmat. A DHCP snooping engedélyezéséhez kövessük az alábbi lépéseket:

**Step 1.** Enable DHCP snooping. **Step 2.** On trusted ports, use the **ip dhcp snooping trust** interface configuration command. **Step 3.** Limit the number of DHCP discovery messages that can be received per second on untrusted ports. **Step 4.** Enable DHCP snooping by VLAN, or by a range of VLANs.

A dinamikus ARP-ellenőrzés (Dynamic ARP inspection, DAI) működéséhez DHCP snooping szükséges, és ezáltal segít megelőzni az ARP-támadásokat:

* Nem továbbítja az érvénytelen ARP-válaszokat a VLAN-ban levő többi portra.
* Elfogja az ARP-kérelmeket és válaszokat a nem megbízható portokon.
* Minden elfogott csomagot ellenőriz egy érvényes IP-MAC összerendelés végett.
* Eldobja és naplózza az érvénytelen ARP-válaszokat az ARP-mérgezés megelőzésére.
* Hiba miatt letiltott állapotba helyezi az interfészt, ha az ARP-csomagok száma túllépi a DAI-ban konfigurált értéket.

Az ARP-hamisítás és az ARP-mérgezés elkerülése érdekében kövessük az alábbi irányelveket:

* Engedélyezzük globálisan a DHCP snooping szolgáltatást.
* Engedélyezzük a DHCP snooping szolgáltatást a kijelölt VLAN-okon.
* Engedélyezzük a DAI-t a kiválasztott VLAN-okon.
* Konfiguráljunk megbízható interfészeket a DHCP snooping és az ARP-ellenőrzés szolgáltatásokhoz.

Ajánlatos az összes hozzáférési switch portot nem megbízhatóként konfigurálni, a többi switch felé vezető uplink portokat pedig megbízhatóként beállítani.

A DAI úgy is konfigurálható, hogy ellenőrizze a cél- vagy a forrás MAC-címeket és IP-címeket:

* **Destination MAC** - Checks the destination MAC address in the Ethernet header against the target MAC address in ARP body.
* **Source MAC** - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
* **IP address** - Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Az STP-protokoll ellen irányuló manipulációs támadások enyhítésére használjuk a PortFast és a BPDU Guard (Bridge Protocol Data Unit) eszköket:

* **PortFast** - PortFast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. Az összes végfelhasználói portra alkalmazzuk. A PortFast beállítást csak a végberendezéseket csatlakoztató portokon konfiguráljunk. A PortFast kihagyja az STP figyelési és tanulási állapotait, így minimálisra csökkenti az STP-konvergenciára fordított időt. Ha a PortFast-ot egy másik switch-hez csatlakozó porton használjuk kockáztatjuk egy feszítőfa hurok létrejöttét.
* **BPDU Guard** - BPDU guard immediately error disables a port that receives a BPDU. Like PortFast, BPDU guard should only be configured on interfaces attached to end devices. BPDU Guard can be enabled on a port by using the **spanning-tree bpduguard enable** interface configuration command. Alternatively, Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on all PortFast-enabled ports.

11.6.4

## Ellenőrző kvíz - Switch biztonsági konfiguráció

Az űrlap teteje

1. Mi a bevált gyakorlat a natív VLAN-ok használata során?

Az űrlap alja

Melyik switch portokon kell engedélyezni a PortFast funkciót az STP stabilitásának növelése érdekében?

Melyik parancs alkalmazása a legcélszerűbb egy használaton kívüli switchport esetében, ha a vállalat betartja a Cisco által javasolt bevált gyakorlatot?

Egy Cisco Catalyst switch melyik két funkciója használható a DHCP-kiéheztetés és a DHCP-hamisítás elleni támadások enyhítésére? (Két jó válasz van.)

Melyik a legjobb módszer a VLAN-ugrásos támadások megelőzésére?

Melyik eljárás ajánlott az ARP-hamisítás hatásainak enyhítésére?

Melyik két porttípus használható a Cisco switch-eken a DHCP-hamisítási támadások elleni védelem részeként? (Két jó válasz van.)

Melyik két parancs használható a PortFast funkció bekapcsolásához egy switch-en? (Két jó válasz van.)

A rendszergazda egy switch kapcsolódási problémájának hibaelhárítása során észreveszi, hogy a portbiztonságra konfigurált port hiba miatt letiltott (err-disabled) állapotban van. Miután ellenőrizte a letiltás okát, hogyan kell újra engedélyeznie a portot anélkül, hogy megzavarná a hálózat működését?

A hálózati rendszergazda DHCP snooping szolgáltatás konfigurálását végzi egy switch-en. Melyik konfigurációs parancsot kell használnia először?

A network administrator is configuring DAI on a switch with the command **ip arp inspection validate dst-mac**. Mi a célja ennek a parancsnak?

Melyik biztonsági funkciót kell engedélyezni annak megakadályozásához, hogy a támadó túlterhelje a switch MAC-címtábláját?

Melyik 2. rétegbeli támadás mérsékelhető a DTP letiltásával?

A hálózati rendszergazda DAI-t (Dynamic ARP Inspection) konfigurál egy switch-en. Melyik parancsot használja a routerhez csatlakozó uplink interfészen?

Hol tárolódnak a dinamikusan tanult MAC-címek, ha a sticky tanulás engedélyezve van a **switchport port-security mac-address sticky** paranccsal?

[11.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[STP-támadások kiküszöbölése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. Bevezetés

# Bevezetés

12.0.1

## Miért fontos ez a fejezet?

Üdvözlünk a vezeték nélküli hálózatokban!

Használt már valaki vezeték nélküli kapcsolatot otthon, a munkahelyen vagy az iskolában? Elondolkozott már azon, hogyan működik?

Számos mód van a vezeték nélküli csatlakozásra. Bizonyos helyzetekben ezek a kapcsolattípusok a legalkalmasabbak a hálózati csatlakozásra. Speciális eszközöket igényelnek, és érzékenyek különféle típusú támadásokra is. Természetesen vannak megoldások a támadások kiküszöbölésére. Szeretnénk többet megtudni? A WLAN-alapok modul tartalmazza a vezeték nélküli LAN-ok működésére, használatára és védelmére vonatkozó alapvető ismereteket.

Kezdjük el még ma!

12.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: WLAN Concepts

**Module Objective**: Explain how WLANs enable network connectivity.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| Introduction to Wireless | Describe WLAN technology and standards. |
| Components of WLANs | Describe the components of a WLAN infrastructure. |
| WLAN Operation | Explain how wireless technology enables WLAN operation. |
| CAPWAP Operation | Explain how a WLC uses CAPWAP to manage multiple APs. |
| Channel Management | Describe channel management in a WLAN. |
| WLAN Threats | Describe threats to WLANs. |
| Secure WLANs | Describe WLAN security mechanisms. |

[11.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Introduction to Wireless](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. Introduction to Wireless

# Introduction to Wireless

12.1.1

## A vezeték nélküli hálózat előnyei

WLAN (Wireless LAN) alatt az otthonokban, irodákban és telephelyeken használt vezeték nélküli hálózatokat értjük. A hálózatoknak támogatniuk kell a mozgásban lévő embereket, akik különféle számítógépeket, laptopokat, tableteket és okostelefonokat használnak. Számos különböző infrastruktúra létezik, amelyek hálózati hozzáférést biztosítanak, például vezetékes LAN-ok, szolgáltatói hálózatok és mobiltelefon-hálózatok. A WLAN mobilitást biztosít az otthoni és üzleti környezetekben.

Egy vezeték nélküli hálózattal rendelkező cég számára sokkal olcsóbb az eszközöket, dolgozókat más helyre költöztetni, laboratóriumot átrendezni, vagy ideiglenes helyre, például kihelyezett projekt helyszínekre települni. Egy vezeték nélküli infrastruktúra képes alkalmazkodni a gyorsan változó igényekhez és technológiákhoz.



12.1.2

## Vezetéknélküli hálózatok típusai

A vezeték nélküli hálózatok az IEEE (Institute of Electrical and Electronics Engineers) szabványain alapulnak, és négy fő típusba sorolhatók: WPAN, WLAN, WMAN és WWAN.

Kattintsunk az egyes vezeték nélküli típusokra a további információért!

**Wireless Wide-Area Networks (WWANs)** - Uses transmitters to provide coverage over an extensive geographic area. A WWAN-ok alkalmasak országos és globális kommunikációra. A WWAN-ok speciális engedélyezett frekvenciákat használnak.

WWAN showing a map of the world with radio towers and satellites scattered throughout the continents

12.1.3

## Vezeték nélküli technológiák

A vezeték nélküli technológiák a rádiófrekvenciás spektrum szabadon használható sávjait használják adattovábbításra. A szabadon használható rádiófrekvenciákat bárki használhatja, akinek rendelkezésére áll egy vezeték nélküli eszköz.

Kattintsunk az egyes vezeték nélküli technológiákra a további információért!

**Satellite Broadband** - Provides network access to remote sites through the use of a directional satellite dish that is aligned with a specific geostationary Earth orbit satellite. Rendszerint nagyon drága és tiszta rálátást igényel. Tipikusan olyan távoli területeken használják, ahol nincs sem DSL, sem kábeles szolgáltatás.



12.1.4

## 802.11 szabványok

A vezeték nélküli kommunikáció világa hatalmas. A gyakorlati készségek megszerzésének érdekében a WiFi bizonyos elemeire fogunk összpontosítani. A legjobb kiindulópont az IEEE 802.11 WLAN-szabványok területe. Ezek határozzák meg, hogyan használhatók a rádiófrekvenciák a vezeték nélküli kapcsolatokhoz. A legtöbb szabvány úgy rendelkezik, hogy a vezeték nélküli eszközök egyazon antennával végzik a jelek továbbítását és fogadását a megadott rádiófrekvencián (2,4 GHz vagy 5 GHz). A nagyobb sebesség megvalósításához a hozzáférési pontok (AP) és a kliensek több antennával rendelkeznek a MIMO (multiple-input multiple-output) technológia használatával. A MIMO több antennát használ mind az adáshoz, mind a vételhez, ezzel növeli a kommunikáció teljesítményét Maxiumum 8 adó- és vevő antenna építhető be az átvitel növelése érdekében.

Az IEEE 802.11 szabványon belül számos megvalósítás jött létre az idők folyamán, amelyek az alábbi táblázatban találhatók.

| Table caption | | |
| --- | --- | --- |
| **IEEE WLAN-szabvány** | **Rádiófrekvencia** | **Leírás** |
| 802.11 | 2,4 GHz | * max. 2 Mb/s sebesség |
| 802.11a | 5 GHz | * max. 54 Mb/s sebesség * kis lefedettségi terület * gyenge áthatolóképesség az épületszerkezeteken * nem kompatibilis a 802.11b és 802.11g szabványokkal |
| 802.11b | 2,4 GHz | * max. 11 Mb/s sebesség * nagyobb hatótávolság, mint a 802.11a esetén * jobban képes áthatolni épületszerkezeteken |
| 802.11g | 2,4 GHz | * max. 54 Mb/s sebesség * visszafelé kompatibilis a 802.11b-vel, de csökkentett sávszélességgel |
| 802.11n | 2,4 GHz és 5 GHz | * adatátviteli sebessége 150 - 600 Mb/s, hatótávolsága max. 70 m * a hozzáférési pontok és a vezeték nélküli ügyfelek több antennát igényelnek a MIMO használatához * visszafelé kompatibilis a 802.11a/b/g eszközökkel, de csökkentett sávszélességgel |
| 802.11ac | 5 GHz | * 450 Mb/s és 1,3 Gb/s közötti adatátviteli sebességet biztosít MIMO technológia használatával * max. 8 antennát támogat * visszafelé kompatibilis a 802.11a/n eszközökkel, de csökkentett sávszélességgel |
| 802.11ax | 2,4 GHz és 5 GHz | * latest standard released in 2019 * also known as Wi-Fi 6 or High-Efficiency Wireless (HEW) * jobb energiahatékonyságot, nagyobb adatátviteli sebességet, nagyobb kapacitást biztosít, és számos csatlakoztatott eszközt kezel * jelenleg 2,4 GHz-en és 5 GHz-en működik, de 1 GHz-et és 7 GHz-et fog használni, amikor ezek a frekvenciák elérhetővé válnak * További információért keressünk rá az interneten "Wi-Fi Generation 6" kifejezésre! |

12.1.5

## Rádiófrekvenciák

Minden vezeték nélküli eszköz az elektromágneses spektrum rádióhullámú (RF) tartományában üzemel. A WLAN-hálózatok a 2,4 GHz és az 5 GHz tartományokban működnek. A vezeték nélküli LAN-eszközök adó- és vevőáramkörei megadott frekvenciákra vannak hangolva, amelyek a 802.11 szabvány szerint a következők:

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

wireless devices, and other technologies, and where they operate on the electromagnetic spectrum

### Az elektromágneses spektrum

Wireless Devices

12.1.6

## Vezeték nélküli szabványügyi szervezetek

A szabványok lehetővé teszik a különböző gyártók eszközei közötti együttműködést. A WLAN-szabványokat három nemzetközi szervezet kezeli: ITU-R, IEEE, és Wi-Fi Alliance.

Kattintsunk az egyes gombokra a szabványügyi szervezettel kapcsolatos további információkért!

Az ITU (International Telecommunication Union, Nemzetközi Távközlési Unió) szabályozza a rádiófrekvenciás spektrum és a műholdas pályák elosztását az ITU-R-en keresztül. Az ITU-R az ITU rádiókommunikációs szektorát jelenti.

12.1.7

## Tudáspróba - Bevezetés a vezeték nélküli hálózatokba

Az űrlap teteje

Check your understanding of wireless networks, technologies, and standards by choosing the BEST answer to the following questions.

1. Which of the following wireless networks typically uses lower powered transmitters for short ranges?

Az űrlap alja

Which of the following wireless networks are specified in the IEEE 802.11 standards for the 2.4 GHz and 5 GHz radio frequencies?

Which of the following is an IEEE 802.15 WPAN standard that uses a device-pairing process to communicate?

Which 802.11 standards exclusively use the 5 GHz radio frequency? (Choose 2)

Which standards organization is responsible for allocating radio frequencies?

[12.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-összetevők](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. WLAN-összetevők

# WLAN-összetevők

12.2.1

## Videó - WLAN-összetevők

Az előző témakörben megismerkedtünk a vezeték nélküli hálózatok előnyeivel és típusaival, a 802.11 szabványokkal és a rádiófrekvenciák használatával. Most a WLAN felépítésével foglalkozunk.

Kattintsunk a Lejátszás gombra a WLAN összetevőiről szóló videó megtekintéséhez!

12.2.2

## Vezeték nélküli hálózati kártyák

Egy vezeték nélküli hálózat megvalósításához legalább két olyan eszközre van szükség, amely ugyanarra a rádiófrekvenciára hangolt rádióadóval és vevővel rendelkezik:

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

A vezeték nélküli kommunikációhoz a laptopok, a táblagépek, az okostelefonok és a legújabb autók beépített vezeték nélküli hálózati csatlakozót tartalmaznak, amely magában foglal egy rádió adó-vevő egységet is. Ha egy eszközben nincs ilyen NIC, akkor használhatunk USB vezeték nélküli adaptert (lásd ábra)

**Note**: Many wireless devices you are familiar with do not have visible antennas. Ilyenek az okostelefonok, a laptopok és a vezeték nélküli otthoni routerek.

### USB vezeték nélküli adapter



12.2.3

## Vezeték nélküli otthoni router

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

Például egy otthoni felhasználó rendszerint egy kis méretű vezeték nélküli routerhez csatlakoztatja eszközeit (lásd ábra). A vezeték nélküli router egyben:

* **Access point** - This provides 802.11a/b/g/n/ac wireless access.
* **Switch** - This provides a four-port, full-duplex, 10/100/1000 Ethernet switch to interconnect wired devices.
* **Router** - This provides a default gateway for connecting to other network infrastructures, such as the internet.



Egy vezeték nélküli router kisvállalati vagy otthoni környezetben gyakran hozzáférési pontként működik. A router "jelzőtűz" keretekkel (beacon) hirdeti vezeték nélküli szolgáltatásait, amelyek tartalmazzák saját azonosítóját is (service set identifier, SSID). A vezeték nélküli kliens eszközök felismerik az SSID-t, megpróbálnak csatlakozni hozzá és hitelesíteni magukat, hogy elérjék a helyi hálózatot és az internetet.

A legtöbb vezeték nélküli router további funkciókkal is rendelkezik, például nagy sebességű hozzáférés, videofolyam támogatás, IPv6-címzés, QoS, konfigurációs segédprogram és USB-portok nyomtatók vagy hordozható meghajtók csatlakoztatására.

Emellett, azok az otthoni felhasználók, akik ki szeretnék bővíteni hálózati szolgáltatásaikat, beüzemelhetnek Wi-Fi hatótávolság növelő berendezéseket (extender). Egy vezeték nélkül kliens csatlakozhat ehhez, ilyenkor az extender jelismétlőként működik és továbbítja a kommunikációt a router felé.

12.2.4

## Vezeték nélküli hozzáférési pontok

Bár a hatótávolság-növelők egyszerűen telepíthetők és konfigurálhatók, de a legjobb megoldás egy másik vezeték nélküli hozzáférési pont beüzemelése, amely dedikált hozzáférést biztosít a felhasználói eszközök számára. A vezeték nélküli kliensek hálózati adaptere felderíti a közelben levő AP-ket SSID-jük alapján. Ezután a kliensek megpróbálnak kapcsolódni az AP-hez és hitelesíteni magukat. A sikeres hitelesítést követően hozzáférnek a hálózati erőforrásokhoz. A képen Cisco Meraki Go AP-k láthatók.



12.2.5

## AP-kategóriák

A hozzáférési pontok két kategóriába sorolhatók: önálló AP-k és vezérlő alapú AP-k.

Kattintsunk a gombokra az egyes típusokkal és a topológiával való megismerkedéshez!

**Autonomous APs**

These are standalone devices configured using a command line interface or a GUI, as shown in the figure. Használatuk akkor indokolt, ha a hálózatban csak néhány elérési pontra van szükség. Egy otthoni router jó példa az önálló AP-re, mivel a teljes konfiguráció az eszközön található. Ha újabb vezeték nélküli igények merülnek fel, akkor további AP-kat kell telepíteni. Az AP-k egymástól függetlenül működnek, és mindegyik egyedi konfigurációt és felügyeletet igényel. Ez kezelhetetlen, ha sok AP-re van szükség.

several wireless devices connected to an autonomous AP which has a wired connection to a switch on a wired network

Autonomous AP

12.2.6

## Vezeték nélküli antennák

A legtöbb üzleti célú AP-hez külső antennát kell használni, hogy teljes értékű eszközként működjön.

Kattintsunk az egyes antennákra további információért!

A körsugárzó 360 fokos szögben szórja a jeleket, ezért ideális nyílt légterű irodákban, konferenciatermekben és kültéren.



12.2.7

## Tudáspróba - WLAN-összetevők

Az űrlap teteje

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

1. True or False: Laptops that do not have an integrated wireless NIC can only be attached to the network through a wired connection.

Az űrlap alja

Which of the following components are integrated in a wireless home router? (Három jó válasz van.)

True or False: When you need to expand the coverage of a small network, the best solution is to use a range extender.

Which of the following is a standalone device, like a home router, where the entire WLAN configuration resides on the device?

Which of the following antennas provide 360 degrees of coverage?

[12.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Introduction to Wireless](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-működés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. WLAN-működés

# WLAN-működés

12.3.1

## Videó - WLAN-működés

Az előző témakör a WLAN-komponenseket tárgyalta. Ebben a témakörben a WLAN működésével foglalkozunk.

Kattintsunk a Lejátszás gombra a WLAN működéséről szóló videó megtekintéséhez!

12.3.2

## 802.11 WLAN topológia módok

A vezeték nélküli LAN-oknak többféle hálózati topológiájuk lehet. A 802.11 szabvány kétféle alapvető módot határoz meg: Ad hoc és Infrastruktúra mód. A tethering (pányvázás) egy olyan további mód, amely gyorsan létrehozható vezeték nélküli hozzáférést biztosít.

Kattintsunk az egyes vezeték nélküli topológiákra a további információért!

**Ad hoc mode -** This is when two devices connect wirelessly in a peer-to-peer (P2P) manner without using APs or wireless routers. Ilyen például a Bluetooth vagy a Wi-Fi Direct használatával közvetlenül egymáshoz csatlakozó két vezeték nélküli ügyfél. Az IEEE 802.11 szabvány az ad hoc hálózatot IBSS-nek (independent basic service set, független alap szolgáltatáskészlet) hívja.

two laptops communicating directly with each other via wireless signals

12.3.3

## BSS és ESS

A szabvány kétféle infrastruktúra mód topológiát határoz meg: alap szolgáltatás-készlet (BSS) és kiterjesztett szolgáltatás-készlet (ESS).

Kattintsunk a gombokra a további információk megtekintéséhez!

**Basic Service Set**

A BSS consists of a single AP interconnecting all associated wireless clients. Az ábrán két BSS látható. A körök a BSS lefedettségi területét ábrázolják, amelyet BSA-nak (Basic Service Area) neveznek. Ha egy kliens kilép a cellából, többé nem képes kommunikálni a BSA más ügyfeleivel.

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

The figure shows two BSAs. One is identified by the BSSID 00d0:bc80:dd07 and consists of a laptop with a wireless connection to an AP. The second BSA is identified by the BSSID 00d0:afdb:e0fc and consists of two laptops each with a wireless connection to an AP.

BSABSA**BSSID:**  
00d0:bc80.dd07**BSSID**  
00d0:afdb.e0fc10–15%-os átfedés, hogy a kapcsolat elvesztése nélkül biztosítható legyen a barangolás a BSA-k között

12.3.4

## A 802.11 keretek szerkezete

Emlékezzünk vissza, hogy az összes 2. rétegbeli keret fejléc, adat és keretellenőrző összeg (Frame Check Sequence, FCS) szakaszból áll. A 802.11 keretformátum hasonlít az Ethernet-hez, de több mezőt tartalmaz.

Az ábrán egy 802.11 keret mezői láthatók. A fejléc balról jobbra a következő mezőket tartalmazza: keretvezérlés, időtartam, cím 1, cím 2, cím 3, szekvencia-vezérlés és cím 4. Ezeket követi az adat, az utolsó pedig az FCS-mező.

HeaderPayloadFCSFrame ControlIdőtartamAddress1Address2Address3Sequence ControlAddress4

A 802.11 keretek a következő mezőkből épülnek fel:

* **Frame Control** - This identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
* **Duration** - This is typically used to indicate the remaining duration needed to receive the next frame transmission.

Vezeték nélküli eszközről: Cím 1 Vevő címe - Az AP MAC címe. \*\*\*\* Address 2 Address Address – a küldő MAC-címe. \* **3. cím SA/DA/BSSID - A cél MAC-címe, amely lehet vezeték nélküli eszköz vagy vezetékes eszköz. \*\***

Az AP-ból: Address 1 Receiver Address - a küldő MAC-címe. \*\*\*\* Address 2 Address Address – az AP MAC-címe. \* **3. cím SA/DA/BSSID - A vezeték nélküli célállomás MAC-címe. \*\***

* **Sequence Control** - This contains information to control sequencing and fragmented frames.
* **Address4** - This usually missing because it is used only in ad hoc mode.
* **Payload** - This contains the data for transmission.
* **FCS** - This is used for Layer 2 error control.

12.3.5

## CSMA/CA

A WLAN-ok fél-duplex működésűek, az átviteli közeget megosztott módon használják. A fél-duplex azt jelenti, hogy egy adott pillanatban csak egyetlen ügyfél tud továbbítani vagy fogadni. A megosztott média pedig azt jelenti, hogy minden vezeték nélküli ügyfél ugyan azon a rádiócsatornán keresztül tud továbbítani és fogadni. Ez problémát okoz, mert adás közben a kliens nem hall semmit, így az ütközést sem tudja érzékelni.

A probléma megoldásához a WLAN CSMA/CA-t (Carrier Sense Multiple Access with Collosion Avoidance, vivőjelérzékeléses többes elérés ütközés elkerüléssel) használ annak meghatározására, hogyan és mikor küldjenek adatokat a hálózaton. A vezeték nélküli ügyfél a következőket teszi:

1. Belehallgat a csatornába, hogy üresjáratban van-e, ami azt jelenti, hogy nincs más forgalom a közegben. A csatornát hordozónak (carrier) is nevezik.
2. Sends a request to send (RTS) message to the AP to request dedicated access to the network.
3. Az AP-tól egy hozzáférést biztosító CTS-üzenetet (Clear To Send, szabad a küldés) kap.
4. Ha a vezeték nélküli ügyfél nem kap CTS-üzenetet, a folyamat újraindítása előtt véletlenszerűen várakozik.
5. Miután megkapta a CTS-t, továbbítja az adatokat.
6. Minden adás nyugtázásra kerül. Ha egy vezeték nélküli ügyfél nem kap visszaigazolást, azt feltételezi, hogy ütközés történt, és újraindítja a folyamatot.

12.3.6

## A vezeték nélküli kliens és az AP társítása

A vezeték nélküli klienseknek csatlakozniuk kell egy AP-hoz vagy egy vezeték nélküli routerhez, hogy kommunikálni tudjanak a hálózaton. A 802.11 folyamat fontos része a WLAN felderítése, majd a hozzákapcsolódás. A vezeték nélküli eszközök a következő három lépéses folyamatot hajtják végre (lásd ábra):

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

The figure shows the three-stage process used by a wireless client to associate with an AP. A laptop represents a wireless client that is communicating wirelessly with an AP. An arrow flowing from the client to the AP represents stage one in which the client discovers the AP. Below that, a double arrow between the devices represents the authentication stage. Below that, another double arrow between the devices represents the association stage.

Wireless ClientAPDiscover APHitelesítésAssociate

A vezeték nélküli kliens és az AP társításához egyeztetni kell bizonyos paramétereket, amelyeket mindkét eszközön konfigurálni kell.

* **SSID** -The SSID name appears in the list of available wireless networks on a client. Azoknál a nagyobb szervezeteknél, amelyek több VLAN-t használnak a forgalom szétválasztásához, mindegyik SSID egy adott VLAN-hoz van hozzárendelve. A hálózati konfigurációtól függően több AP is használhatja ugyanazt az SSID-t.
* **Password** - This is required from the wireless client to authenticate to the AP.
* **Network mode** - This refers to the 802.11a/b/g/n/ac/ad WLAN standards. Az AP-k és a vezeték nélküli routerek működhetnek Mixed (vegyes) módban is, azaz egyidejűleg használhatnak többféle szabványt.
* **Security mode** - This refers to the security parameter settings, such as WEP, WPA, or WPA2. Mindig a legmagasabb elérhető biztonsági szintet válasszuk!
* **Channel settings** - This refers to the frequency bands used to transmit wireless data. A vezeték nélküli routerek és hozzáférési pontok megvizsgálják a rádiófrekvenciás csatornákat, és automatikusan kiválasztják a megfelelő beállítást. A csatornák beállíthatók manuálisan is más AP-k zavaró hatásának (interferencia) kiküszöbölése érdekében.

12.3.7

## Passzív és aktív felderítési mód

A csatlakozás érdekében a vezeték nélküli eszközöknek fel kell kutatniuk az AP-t vagy a routert, amelyhez egy pásztázási (probe) folyamatot alkalmaznak. Ez a folyamat lehet passzív vagy aktív.

További információért kattintsunk az egyes módokra!

Passzív módban az AP nyíltan hirdeti szolgáltatását szórásos beacon keretek rendszeres küldésével, amik az SSID-t, a támogatott szabványokat és a biztonsági beállításokat tartalmazzák. A beacon keretek elsődleges feladata a vezeték nélküli kliensek értesítése arról, hogy milyen hálózatok és AP-k vannak az adott területen. Ez lehetővé teszi az ügyfelek számára a kívánt hálózat és hozzáférési pont kiválasztását.

an AP sending three beacon frames containing SSID, supported standards, and security settings which are received by a wireless client

Wireless ClientAPBeaconBeaconBeacon

* SSID
* Supported standards
* Security settings
* SSID
* Supported standards
* Security settings
* SSID
* Supported standards
* Security settings

12.3.8

## Tudáspróba - WLAN-működés

Az űrlap teteje

Check your understanding of WLAN operation by choosing the BEST answer to the following questions.

1. Which wireless topology mode is used by two devices to connect in a peer-to-peer network?

Az űrlap alja

True or False: An ESS is created when two or more BSSs need to be joined to support roaming clients.

How many address fields are in the 802.11 wireless frame?

What is the term for an AP that openly advertises its service periodically?

What is the term for an AP that does not send a beacon, but waits for clients to send probes?

[12.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-összetevők](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A CAPWAP működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. A CAPWAP működése

# A CAPWAP működése

12.4.1

## Videó - CAPWAP

Az előző témakörben megismerkedtünk a WLAN működésével. Most a CAPWAP (Control and Provisioning of Wireless Access Points, vezeték nélküli hozzáférési pontok kiépítése és vezérlése) működésével foglalkozunk.

Kattintsunk a Lejátszás gombra a CAPWAP-ről szóló videó megtekintéséhez!

12.4.2

## Bevezetés a CAPWAP-ba

A CAPWAP egy szabványos IEEE-protokoll, amely lehetővé teszi a WLC számára több hozzáférési pont és WLAN kezelését. A CAPWAP felelős a hozzáférési pont és a WLC közötti WLAN-ügyfélforgalom beágyazásáért és továbbításáért.

A CAPWAP az LWAPP-n alapul, de fejlettebb biztonságot nyújt a DTLS (Datagram Transport Layer Security) szolgáltatás használatával. A CAPWAP alagutakat (tunnel) hoz létre UDP-portokon keresztül. IPv4- vagy IPv6-protokollon is működhet, de alapértelmezés szerint IPv4-et használ (lásd ábra).

Az IPv4 és az IPv6 egyaránt az 5246-os és az 5247-es UDP-portot használja. Az 5246-os port a WLC által az AP kezelésére használt CAPWAP vezérlőüzenetekhez való. Az 5247-es portot a CAPWAP használja a vezeték nélküli kliensek felé és onnan érkező adatcsomagok beágyazására. A CAPWAP alagutak azonban különböző IP-protokollokat használnak a csomagfejlécben. Az IPv4 a 17-es, az IPv6 pedig a 136-os IP-protokollt használja.

The figure shows a small IPv4 or IPv6 network in the cloud. A WLC connects to three APs using CAPWAP.

IPv4 or IPv6 NetworkAPAPWLCCAPWAPCAPWAPAPCAPWAP

12.4.3

## Split MAC architektúra

A CAPWAP egyik legfontosabb összetevője a megosztott közeghozzáférés-vezérlés (split Media Access Control, MAC) fogalma. A CAPWAP split MAC koncepció elvégzi az önálló AP-k által általában végrehajtott összes funkciót, és elosztja azokat két összetevő között:

* AP MAC-funkciók
* WLC MAC-funkciók

A táblázat az egyes MAC-funkciókat mutatja be.

| Table caption | |
| --- | --- |
| **AP MAC-funkciók** | **WLC MAC-funkciók** |
| Beaconok és szondaválaszok | Hitelesítés |
| Csomag nyugtázás és újraküldés | Barangoló ügyfelek társítása és újratársítása |
| Keret várólisták és csomagprioritások kezelése | Keretek konvertálása más protokollokra |
| MAC-réteg adattitkosítás és dekódolás | A 802.11 forgalom végződtetése vezetékes interfészen |

12.4.4

## DTLS-titkosítás

A DTLS egy olyan protokoll, amely biztonságos kommunikációt nyújt az AP és a WLC között. Lehetővé teszi számukra, hogy titkosítva kommunikáljanak, és megakadályozza a lehallgatást vagy a hamisítást.

A DTLS alapértelmezés szerint engedélyezve van a CAPWAP vezérlő csatornán, de tiltott az adatcsatorna esetében (lásd ábra). Az AP és a WLC közötti CAPWAP menedzsment forgalom alapértelmezés szerint titkosított, hogy biztosítsa a vezérlés adatvédelmét és megakadályozza a beékelődéses (Man-in-the-Middle, MITM) támadásokat.

A CAPWAP-adattitkosítás opcionális, és hozzáférési pontonként engedélyezhető. Az adattitkosításhoz DTLS-licencet kell telepíteni a WLC-re, mielőtt engedélyeznék egy hozzáférési ponton. Ha engedélyezve van, az összes WLAN-ügyfélforgalom titkosításra kerül az AP-n, mielőtt továbbítódik a WLC-re, és fordítva.

The figure shows a WLC connected to an AP using CAPWAP encapsulation. The control channel encapsulation is enabled by default while the data encryption is optional and enabled on each AP.

CAPWAP EncapsulationCAPWAP ControlDTLS Encryption (disabled by default)CAPWAP DataDTLS Encryption (enabled by default)APWLC

12.4.5

## FlexConnect AP-k

A FlexConnect egy vezeték nélküli megoldás fiókirodai és távoli telephelyen történő telepítésekhez. Lehetővé teszi a távoli AP-k konfigurálását és ellenőrzését a vállalati központból egy WAN-összeköttetésen keresztül, anélkül, hogy minden helyszínen telepíteni kellene egy vezérlőt.

A FlexConnect AP-nak két üzemmódja van.

* **Connected mode** - The WLC is reachable. Ebben a módban a FlexConnect AP CAPWAP-kapcsolattal rendelkezik a WLC felé, és forgalmat tud küldeni a CAPWAP-alagúton keresztül (lásd ábra). A WLC minden CAPWAP-funkcióját ellátja.
* **Standalone mode** - The WLC is unreachable. A FlexConnect elvesztette, vagy nem tudja létrehozni a CAPWAP-kapcsolatot a WLC felé. Ebben a módban a FlexConnect hozzáférési pont elvégezhet bizonyos WLC-funkciókat, mint például az ügyféladatforgalom helyi irányítása és az ügyfél hitelesítésének helyi végrehajtása.

The figure shows a CAPWAP tunnel formed between a FlexConnect AP at a branch office and a WLC at a corporate office. The branch office equipment consists of a laptop with a wireless connection to a FlexConnect AP which is connected to a switch which is connected to a router. The router is then connected to another router in the corporate office to which the WLC is connected. The WLC provides access into the corporate network and the Internet.

internetFlexconnect APCorporate NetworkCAPWAPBranch OfficeWLCCorporate Office

12.4.6

## Tudáspróba - CAPWAP-működés

Az űrlap teteje

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

1. What IP versions does CAPWAP support?

Az űrlap alja

What UDP ports and IP protocols are used by CAPWAP for IPv4? (Három jó válasz van.)

What UDP ports and IP protocols are used by CAPWAP for IPv6? (Három jó válasz van.)

In the split MAC architecture for CAPWAP, which of the following are the responsibility of the AP? (Choose four.)

In the split MAC architecture for CAPWAP, which of the following are the responsibility of the WLC? (Choose four.)

True or False: DTLS is enabled by default on the control and data CAPWAP tunnels.

Which of the following statements are true about modes of operation for a FlexConnect AP? (Két jó válasz van.)

[12.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-működés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Csatorna kezelés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. Csatorna kezelés

# Csatorna kezelés

12.5.1

## Frekvenciacsatornák telítettsége

A vezeték nélküli LAN-eszközök adó- és vevőáramkörei megadott frekvenciákra vannak hangolva a kommunikáció végrehajtásához. 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.

Kattintsunk az egyes technikákra további információért!

**Direct-Sequence Spread Spectrum (DSSS)** - This is a modulation technique designed to spread a signal over a larger frequency band. Háborús időkben fejlesztették ki, hogy nehezebbé tegyék az ellenség számára a kommunikációs jel elfogását vagy megszakítását. Azáltal, hogy a jelet szélesebb frekvenciára terjeszti ki, hatékonyan elrejti a jel észrevehető csúcsértékét (lásd ábra). Egy megfelelően beállított vevőkészülék visszafordítja a DSSS-modulációt, és újraépíti az eredeti jelet. A DSSS-t a 802.11b eszközök használják, hogy elkerüljék az azonos 2,4 GHz-es frekvencián működő más eszközök interferenciáját.

PowerDSSS SignalOriginal SignalGyakoriság

12.5.2

## Csatorna kiválasztása

A több AP-t használó WLAN-ok esetében bevált gyakorlat a nem-átlapolódó csatornák használata. For example, the 802.11b/g/n standards operate in the 2.4 GHz to 2.5 GHz spectrum. A 2,4 GHz-es sávot is több csatornára osztották. Minden csatorna 20 MHz-el van eltolva a következő csatornától. A 802.11b szabvány 13 csatornát határoz meg az Európában történő használatra (USA - 11, Japán - 14) (lásd ábra).

**Megjegyzés**: Keressen az interneten 2,4 GHz-es csatornákat, ha többet szeretne megtudni a különböző országok változatairól.

The figure shows 11 channels that are 22MHz wide and 5MHz between each. The spectrum is between 2.2GHz and 2.5GHz.

### 2,4 GHz-es átfedő csatornák Észak-Amerikában

Channels2,4 GHz2.5 GHz5 MHz22 MHz

Interferencia akkor alakul ki, ha egy nemkívánatos jel átfedésbe kerül a csatorna jelével és eltorzítja azt. The best practice for 2.4 GHz WLANs that require multiple APs is to use non-overlapping channels, although most modern APs will do this automatically. Ha három szomszédos AP van, használjuk az 1, 6 és 11 csatornákat (lásd ábra).

The figure shows three APs using channels 1, 6, and 11.

### 802.11b/g/n 2,4 GHz-es, nem átfedő csatornák

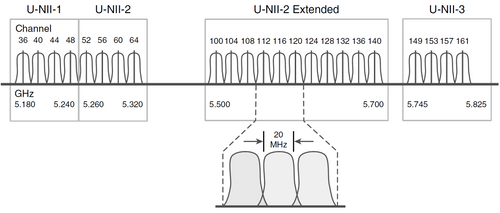
Channel 1Channel 6Channel 11

A 802.11a/n/ac 5 GHz-es szabványoknál 24 csatorna van. Az 5 GHz-es sáv három részre oszlik. Minden csatorna 20 MHz-el van eltolva a következő csatornától. Az ábra az 5 GHz-es sáv 24 U-NNI (Unlicensed National Information Infrastructure) csatornáját mutatja be. Bár van egy kis átfedés, a csatornák nem zavarják egymást. Az 5 GHz-es rendszer gyorsabb adatátvitelt biztosít a kliensek számára a sok vezeték nélküli hálózatot tartalmazó területeken a nagyszámú, nem átfedő csatorna miatt.

**MEGJEGYZÉS**: Keressünk rá az interneten a \"5 GHz channels\" kifejezésre, ha többet szeretnénk megtudni a különböző országok változatairól.

The figure shows 8 channels that have 20MHz between each. The spectrum is between 5150 MHz and 5350 MHz.

### Az első nyolc 5 GHz-es, nem átfedő csatorna



A 2,4 GHz-es WLAN-okhoz hasonlóan válasszunk nem átfedő csatornákat, ha több, egymással szomszédos 5 GHz-es hozzáférési pontot telepítünk (lásd ábra).

The figure shows three APs using channels 36, 48, and 60.

12.5.3

the figure shows a map of a venue with different areas, entrances, and exits. There are circles in different areas to limit the area of coverage.

### 802.11a/n/ac 5 GHz-es, nem átfedő csatornák

Channel 3640-es csatorna44-es csatorna

12.5.3

## WLAN-bevezetés tervezése

A WLAN-kliensek számának meghatározásakor számít a földrajzi elhelyezkedés (beleértve a tereptárgyakat és mesterséges szerkezeteket), az elvárt sávszélesség, a nem-átlapolódó csatornák használata több AP esetén, valamint az adóteljesítmény.

Az AP helyének megtervezésekor a legfontosabb tényező a lefedettségi terület meghatározása, de más feltételeket is figyelembe kell venni:

* Rajzoljuk be a meglévő vezetékes hálózatot, valamint jelöljük be azokat a helyeket, ahová nem telepíthetjük az AP-kat.
* Keressünk meg minden lehetséges interferenciaforrást, amely magában foglalhatja a mikrohullámú sütőket, a vezeték nélküli videokamerákat, a fénycsöveket, a mozgásérzékelőket vagy a 2,4 GHz-es tartományt használó bármely más eszközt.
* 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.
* Ha egy IEEE 802.11 hálózat vegyes üzemmódra van konfigurálva, akkor a vezeték nélküli ügyfelek a szokásosnál kisebb sebességet tapasztalhatnak a régebbi szabványok támogatása miatt.

Az AP lefedettségi területének becslésénél vegyük figyelembe, hogy ez az érték függhet még az alkalmazott WLAN-szabvány(ok)tól, a környezeti tényezőktől, az AP-n konfigurált adóteljesítménytől és még sok egyébtől. Tanulmányozzuk át az AP műszaki leírását is a lefedettség kiszámításához.

EntranceConcessionsFreightExitExitExitExitExitExitExitExitExit

12.5.4

## Tudáspróba - Csatorna kezelés

Az űrlap teteje

Check your understanding of channel management by choosing the BEST answer to the following questions.

1. Which of the following modulation techniques rapidly switches a signal among frequency channels?

Az űrlap alja

Which of the following modulation techniques spreads a signal over a larger frequency band?

Which of the following modulation techniques is used in the new 802.11ax standard?

How many channels are available for the 2.4 GHz band in Europe?

How many channels are available for the 5 GHz band?

[12.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A CAPWAP működése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-fenyegetések](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. WLAN-fenyegetések

# WLAN-fenyegetések

12.6.1

## Videó - WLAN-fenyegetések

Az előző témakörökben a WLAN komponenseivel és konfigurációjával foglalkoztunk. Most a WLAN-ra leselkedő fenyegetéseket ismerjük meg.

Kattintsunk a Lejátszás gombra a WLAN-ok fenyegetéseiről szóló videó megtekintéséhez!

12.6.2

## A vezeték nélküli biztonság áttekintése

A WLAN nyitott bárki számára az AP hatókörén belül, akinek birtokában vannak a csatlakozáshoz szükséges engedélyek. 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 támadások származhatnak kívülállóktól, elégedetlen munkavállalóktól, rosszhiszeműségből vagy akaratlanul. A vezeték nélküli hálózatok különösen érzékenyek a következő fenyegetésekre:

* **Interception of data** - Wireless data should be encrypted to prevent it from being read by eavesdroppers.
* **Wireless intruders** - Unauthorized users attempting to access network resources can be deterred through effective authentication techniques.
* **Denial of Service (DoS) Attacks** - Access to WLAN services can be compromised either accidentally or maliciously. A DoS-támadás forrásától függően különböző védelmi megoldások léteznek.
* **Rogue APs** - Unauthorized APs installed by a well-intentioned user or for malicious purposes can be detected using management software.

12.6.3

## DoS-támadások

A vezeték nélküli DoS-támadások származási helye lehet:

* **Improperly configured devices** - Configuration errors can disable the WLAN. Például egy rendszergazda véletlenül módosítja a beállításokat és letiltja a hálózatot, vagy egy adminisztrátori jogokkal rendelkező behatoló szándékosan teszi ugyanezt.
* **A malicious user intentionally interfering with the wireless communication** - Their goal is to disable the wireless network completely or to the point where no legitimate device can access the medium.
* **Accidental interference** - WLANs are prone to interference from other wireless devices including microwave ovens, cordless phones, baby monitors, and more, as shown in the figure. A 2,4 GHz-es tartomány érzékenyebb az interferenciára, mint az 5 GHz-es sáv.

signals radiating from a cordless phone and a microwave are interfering with signals on a wireless network

S3

WR

this is the image’s alt text

A rosszindulatú és a félrekonfigurált eszközök miatti DoS-támadások minimalizálása érdekében védjük fizikailag az eszközöket, tartsuk a jelszavakat biztonságban, készítsünk biztonsági mentéseket és a konfigurációs módosításokat munkaidőn kívül végezzük.

Legjobb megoldás a WLAN interferencia-hibáinak folyamatos figyelése és az azonnali beavatkozás. Mivel a 2,4 GHz-es sávot sok más eszköz is használja, alkalmazzunk inkább 5 GHz-es AP-kat a zavaró hatásnak kitett területeken.

12.6.4

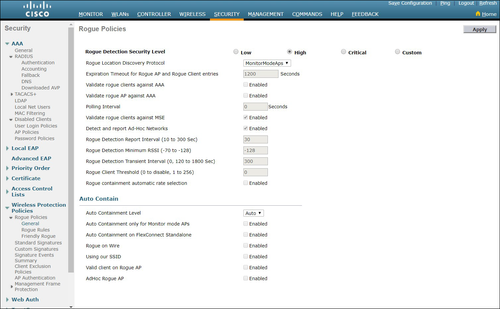
## Csaló (rouge) AP-k

Egy csaló AP olyan hozzáférési pont, amely engedély nélkül és a vállalati házirendet megsértve csatlakozik a szervezet vezetékes hálózatához. Egy személy, akinek hozzáférése van az infrastruktúrához, beüzemelhet egy olcsó WiFi-routert (rossz szándékkal vagy tudatlanságból), amely alkalmas a védett hálózat elérésére.

Miután csatlakozott, a támadó használhatja azt MAC-címek és adatcsomagok rögzítésére, hálózati erőforrásokhoz való hozzáférésre, vagy közbeékelődéses támadás indítására.

Egy személyes hotspot is használható csaló AP-ként. 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 WLC-t kell használni olyan szoftverrel, amely folyamatosan figyeli a rádiótartományt és kiszűri a jogosulatlan elérési pontokat.



12.6.5

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

Közbeékelődéses támadás során a hacker a kommunikáló felek között helyezkedik el, hogy elolvassa vagy módosítsa az átadott adatokat. Ez többféle módon is végrehajtható.

Az egyik népszerű vezeték nélküli MITM-támadás az “evil twin AP” (gonosz iker) nevet viseli. Ilyenkor a támadó beüzemel egy csaló AP-t és ugyanazt 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 threat actor at Bobs Latte has used their laptop to set up an evil twin using an SSID of Bob latte, open authentication, and channel 6

Bob's LatteSSID: Bob latte Authentication: Open Channel: 6Felhasználóinternet

A felcsatlakozó vezeték nélküli kliens két működő AP-t lát ugyan azzal az SSID-vel. 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 (lásd ábra). A visszajövő forgalom a valódi AP-ról a csaló AP-ra kerül, az befogja, majd továbbítja a gyanútlan állomás felé. A támadó megszerezheti a felhasználó jelszavát, személyes információit, hálózati hozzáférését és megrongálhatja a rendszerét.

a user at Bobs Latte is sending wireless traffic to a laptop set up by a threat actor as an evil twin which forwards the traffic to a router within the Internet cloud

Bob's LatteFelhasználóinternet

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

12.6.6

## Tudáspróba - WLAN-fenyegetések

Az űrlap teteje

Check your understanding of WLAN threats by choosing the BEST answer to the following questions.

1. Which of the following is most likely NOT the source of a wireless DoS attack?

Az űrlap alja

True or False: A rogue AP is a misconfigured AP connected to the network and a possible source of DoS attacks.

What type of attack is an “evil twin AP” attack?

[12.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Csatorna kezelés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.7](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-ok biztonsága](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. WLAN-ok biztonsága

# WLAN-ok biztonsága

12.7.1

## Videó - WLAN-ok biztonsága

Az előző témakörben megismertük a WLAN-fenyegetéseket. Mit tehetünk a WLAN védelme érdekében?

Kattintsunk a Lejátszás gombra a WLAN biztonsági technikáiról szóló videó megtekintéséhez!

12.7.2

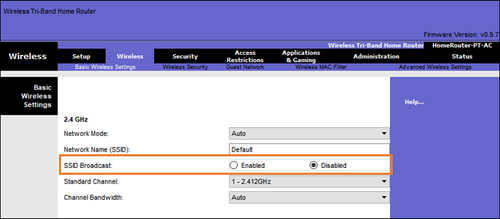
## SSID-rejtés és MAC-cím szűrés

A vezeték nélküli jelek áthatolnak a szilárd anyagokon, például a mennyezeten, a padlón, a falakon, elhagyják a lakás vagy az iroda területét. Szigorú szabályok nélkül WLAN-t telepíteni olyan, mintha mindenhová Ethernet csatlakozókat szerelnénk, még az épületen kívülre is.

A vezeték nélküli behatolók okozta fenyegetés távol tartására és az adatok védelmére két biztonsági szolgáltatás használható, amelyek megtalálhatók a legtöbb routeren és AP-n: az SSID-rejtés és a MAC-cím szűrés

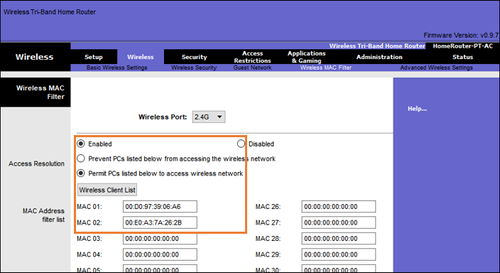
**SSID Cloaking**

Az AP-k és a vezeték nélküli routerek lehetővé teszik az SSID-szórás (beacon keret) letiltását (lásd ábra). A klienseknek manuálisan kell beállítaniuk az SSID-t, ha kapcsolódni szeretnének a hálózathoz.



**MAC Addresses Filtering**

Egy rendszergazda engedélyezheti vagy tilthatja a vezeték nélküli kliensek csatlakozását fizikai címük (MAC) alapján. Az ábrán látható routeren két MAC-cím van engedélyezve. Az ezektől különböző MAC-című eszközök nem tudnak csatlakozni a 2,4 GHz-es WLAN-hoz.



12.7.3

## 802.11 hitelesítési módok

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

Az eredeti 802.11 szabvány kétféle hitelesítést határoz meg:

* **Open system authentication** - Any wireless client should easily be able to connect and should only be used in situations where security is of no concern, such as those providing free internet access like cafes, hotels, and in remote areas. A vezeték nélküli ügyfél felelős a biztonságért, például virtuális magánhálózat (VPN) használatával. A VPN-ek hitelesítési és titkosítási szolgáltatásokat nyújtanak, tárgyalásuk túlmutat a fejezet témakörén.
* **Shared key authentication** - Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. A jelszót viszont előre meg kell osztani a kliensekkel.

Az alábbi ábra összefoglalja ezeket a hitelesítési módszereket.

HitelesítésNyíltOsztott kulcsosWEPWPAWPAWPA3

* Nincs szükség jelszó megadására.
* Bármely kliens csatlakozhat, ha akar.
* Általában ingyenes internet-hozzáférést biztosító helyeken használják.
* Az ügyfél teljes felelősséget vállal a biztonságért.

12.7.4

## Megosztott kulcsú hitelesítési módok

Négy megosztott kulcsú hitelesítési módszer áll rendelkezésre, a táblázatban leírtak szerint. Amíg a WPA3-eszközök mindenütt elterjednek, addig a vezeték nélküli hálózatokban a WPA2-szabványt kell használni.

| Table caption | |
| --- | --- |
| **Hitelesítési mód** | **Leírás** |
| **WEP (Wired Equivalent Privacy)** | Az eredeti 802.11 specifikáció az adatokat RC4 (Rivest Cipher 4) módszerrel titkosítja, amelyhez statikus kulcsot használ. Ekkor a kulcs soha nem változik meg a csomagok cseréje során. Ez megkönnyíti a feltörését. A WEP már nem ajánlott, soha nem szabad használni. |
| **WPA** | Wi-Fi Alliance szabvány, amely a WEP protokollját használja, de az adatokat a sokkal erősebb TKIP (Temporal Key Integrity Protocol) algoritmussal titkosítja. A TKIP minden csomag esetében megváltoztatja a kulcsot, így sokkal nehezebben törhető fel. |
| **WPA2** | A WPA2 egy ipari szabvány a vezeték nélküli hálózatok biztonságossá tételére. Ez AES-t (Advanced Encryption Standard) használ a titkosításhoz. Az AES a jelenlegi legerősebb titkosítási protokoll. |
| **WPA3** | A Wi-Fi biztonság következő generációja. Minden WPA3-kompatibilis eszköz a legújabb biztonsági módszereket alkalmazza, tiltja az elavult protokollokat, és szüksége van a PMF (Protected Management Frames) használatára. Azonban a WPA3-képes eszközök még nem állnak nagy számban rendelkezésre. |

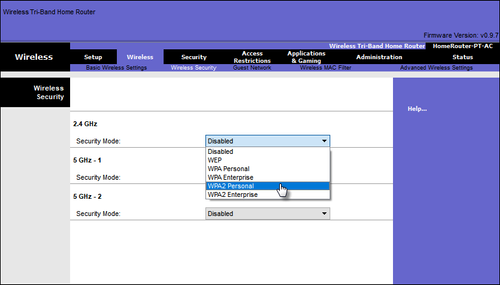
12.7.5

## Otthoni felhasználó hitelesítése

Az otthoni routerek általában két választási lehetőséget kínálnak a hitelesítéshez: a WPA-t és a WPA2-t. A WPA2 az erősebb. Két WPA2 hitelesítési módszer létezik:

* **Personal** - Intended for home or small office networks, users authenticate using a pre-shared key (PSK). amelyet megosztott jelszónak is neveznek. Nincs szükség különálló hitelesítő szerverre.
* **Enterprise** - Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. 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.

Az ábrán egy rendszergazda konfigurálja a vezeték nélküli routert WPA2-Personal hitelesítéssel a 2,4 GHz-es sávon.



12.7.6

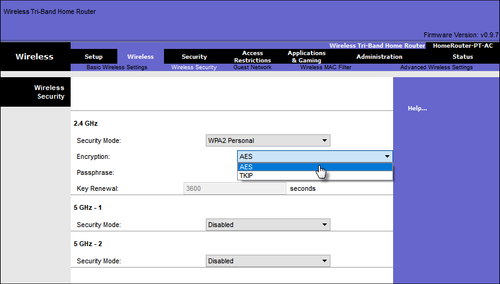
## Titkosítási módok

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

A WPA- és WPA2-szabvány a következő titkosítási protokollokat használja:

* **Temporal Key Integrity Protocol (TKIP)** - TKIP is the encryption method used by WPA. Régebbi WLAN-berendezések támogatására szolgál, a 802.11 WEP-titkosítás hibáit próbálja kijavítani. A 2. rétegbeli adatokat TKIP-vel titkosítja, és ellenőrző összeget (Message Integrity Check, MIC) továbbít a titkosított csomagban az adatok sértetlenségének biztosítására.
* **Advanced Encryption Standard (AES)** - AES is the encryption method used by WPA2. Ez a javasolt módszer, mert egy sokkal erősebb titkosítást használ. 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.

Az ábrán egy rendszergazda konfigurálja a vezeték nélküli routert a WPA2 AES titkosítás használatára a 2,4 GHz-es sávon.



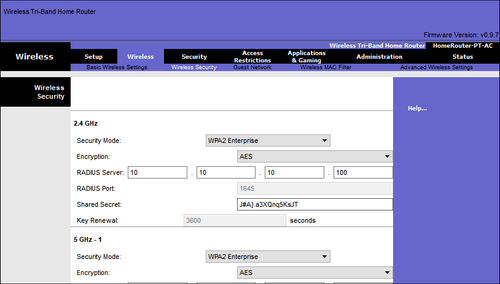
12.7.7

## Vállalati felhasználó hitelesítése

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

* **RADIUS Server IP address** - This is the reachable address of the RADIUS server.
* **UDP port numbers** - Officially assigned UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646, as shown in the figure.
* **Shared key** - Used to authenticate the AP with the RADIUS server.

Az ábrán a rendszergazda konfigurálja a vezeték nélküli routert WPA2 Enterprise hitelesítéssel, AES-titkosítással. Látható a RADIUS-kiszolgáló IPv4-címe és az erős jelszó a vezeték nélküli router és a RADIUS-kiszolgáló közötti kommunikációhoz.



Ez nem az a megosztott kulcs (jelszó), amit a vezeték nélküli kliensen kell konfigurálni. Ez csupán az AP-n szükséges, hogy hitelesítse magát a RADIUS-szerveren. A felhasználók hitelesítését és a jogosultságokat a 802.1X szabvány kezeli, amely központi, szerver alapú végfelhasználói hitelesítést nyújt.

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, amelyet ezután a TKIP és az AES a vezeték nélküli titkosítási folyamatban használ.

12.7.8

## WPA3

A tananyag írásásának idején a WPA3-hitelesítést támogató eszközök még nincsenek kereskedelmi forgalomban. A WPA2 azonban már nem tekinthető biztonságosnak. Ha a WPA3 rendelkezésre áll, akkor ez az ajánlott 802.11 hitelesítési módszer. A WPA3 négyféle hálózati funkciót tartalmaz:

* WPA3-Personal (személyes)
* WPA3-Enterprise (vállalati)
* Open Networks
* Internet of Things Onboarding (IoT-kapcsolatok)

**WPA3-Personal**

A WPA2-Personal esetében a támadók lehallgatják a vezeték nélküli kliens és az AP közötti „kézfogást”, és a nyers erő (brute force) módszer alkalmazásával próbálják megfejteni a PSK-t. A WPA3-Personal meghiúsítja ezt a támadást a SAE (Simultaneous Authentication of Equals) használatával, amely az IEEE 802.11-2016 szabványban meghatározott szolgáltatás. A PSK nem kerül átadásra, ami lehetetlenné teszi, hogy a támadó megfejthesse azt.

**WPA3-Enterprise**

A WPA3-Enterprise továbbra is 802.1X/EAP hitelesítést használ. Szüksége van viszont egy 192 bites titkosítási csomag használatára, és kiküszöböli a biztonsági protokollok vegyes használatát a korábbi 802.11 szabványokhoz képest. A WPA3-Enterprise alkalmazza a CNSA-készletet (Commercial National Security Algoritm), amelyet általánosan használnak a magas biztonságú Wi-Fi hálózatokban.

**Open Networks**

A WPA2 nyílt hálózatai titkosítás nélkül, nyílt szövegben továbbítják a felhasználói forgalmat. A WPA3-ban a nyilvános Wi-Fi hálózatok továbbra sem használnak hitelesítést, azonban az OWH (Opportunistic Wireless Encryption) használatával titkosítják az összes vezeték nélküli forgalmat.

**IoT Onboarding**

Bár a WPA2 WPS-szolgáltatása (Wi-Fi Protected Setup) alkalmas az intelligens (IoT) eszközök konfigurálás nélküli csatlakoztatására, de számos támadással szemben sebezhető, ezért nem ajánlott. Emellett az IoT-eszközökön jellemzően nincs beépített grafikus felhasználói felület a konfiguráláshoz, viszont igényelnek valamilyen egyszerű módot a vezeték nélküli hálózathoz való csatlakozáshoz. A DPP (Device Provisioning Protocol) célja ennek az igénynek a kezelése. Minden ilyen egyszerű eszköznek van egy kódolt nyilvános kulcsa. A kulcs általában a berendezés külső oldalára vagy csomagolására van nyomtatva QR-kódként. A hálózati rendszergazda beolvashatja a QR-kódot, és gyorsan telepítheti az eszközt. Bár a DPP szigorúan véve nem része a WPA3-szabványnak, idővel felváltja a WPS-t.

12.7.9

## Tudáspróba - WLAN-biztonság

Az űrlap teteje

Check your understanding of techniques for securing WLANs by choosing the BEST answer to the following questions.

1. What are the best ways to secure WLANs? (Két jó válasz van.)

Az űrlap alja

Which of the following authentication methods does not use a password shared between the wireless client and the AP?

Which encryption method is used by the original 802.11 specification?

Which of the following encryption methods uses CCMP to recognize if the encrypted and non-encrypted bits have been altered?

Which of the following authentication methods has the user enter a pre-shared password? (Choose two)

[12.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-fenyegetések](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[12.8](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Concepts
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

12.8.1

## Miről tanultunk ebben a fejezetben?

WLAN (Wireless LAN) alatt az otthonokban, irodákban és épületekben használt vezeték nélküli hálózatokat értjük. A vezeték nélküli hálózatok IEEE-szabványokon alapulnak, és négy fő típusba sorolhatók: WPAN, WLAN, WMAN és WWAN. A vezeték nélküli technológiák a rádiófrekvenciás spektrum szabadon használható sávjait használják adattovábbításra. Ilyen technológia például a Bluetooth, a WiMAX, a mobil és a műholdas szélessávú szolgáltatás. Az IEEE 802.11 WLAN szabványok határozzák meg, hogyan használhatók a rádiófrekvenciák a vezeték nélküli kapcsolatokhoz. A WLAN-hálózatok a 2,4 GHz és az 5 GHz tartományokban működnek. A szabványok lehetővé teszik a különböző gyártók eszközei közötti együttműködést. A WLAN-szabványokat három nemzetközi szervezet kezeli: ITU-R, IEEE, és Wi-Fi Alliance.

A vezeték nélküli kommunikációhoz a legtöbb eszköz olyan vezeték nélküli hálózati csatlakozót tartalmaz, amely magában foglal egy rádió adó-vevő egységet is. A vezeték nélküli router átjáróként, hozzáférési pontként és switch-ként is működik. A vezeték nélküli kliensek hálózati adaptere felderíti a közelben levő AP-ket SSID-jük alapján. Ezután a kliensek megpróbálnak kapcsolódni az AP-hez és hitelesíteni magukat. A sikeres hitelesítést követően hozzáférnek a hálózati erőforrásokhoz. A hozzáférési pontok két kategóriába sorolhatók: önálló AP-k és vezérlő alapú AP-k. A vállalti környezetben használt AP-k háromféle antennával rendelkezhetnek: körsugárzó, irányított és MIMO.

A 802.11 szabvány kétféle alapvető módot határoz meg: Ad hoc és Infrastruktúra mód. A tethering gyors vezeték nélküli hozzáférést biztosít. A szabvány kétféle infrastruktúra mód topológiát határoz meg: alap szolgáltatás-készlet (BSS) és kiterjesztett szolgáltatás-készlet (ESS). Minden vezeték nélküli keret fejléce a következő mezőket tartalmazza: keretvezérlés, időtartam, cím 1, cím 2, cím 3, szekvencia-vezérlés, cím 4, adat és keretellenőrző összeg. A WLAN a CSMA/CA-módszert használja annak meghatározására, hogy hogyan és mikor küldjenek adatokat a hálózatba. A 802.11 folyamat fontos része a WLAN felderítése, majd a hozzákapcsolódás. A vezeték nélküli eszközök felderítenek egy AP-t, hitelesítik magukat rajta, majd társulnak hozzá. Ezt a folyamatot végezhetik aktív vagy passzív módon.

A CAPWAP egy szabványos IEEE-protokoll, amely lehetővé teszi egy WLC számára több hozzáférési pont és WLAN kezelését. A CAPWAP split MAC koncepció elvégzi az egyes AP-k által általában végrehajtott összes feladatot, és elosztja azokat két funkcionális összetevő között: AP MAC és WLC MAC funkciók. A DTLS egy olyan protokoll, amely biztonságos kommunikációt nyújt az AP és a WLC között. A FlexConnect egy vezeték nélküli megoldás fiókirodai és távoli telephelyen történő telepítésekhez. Lehetővé teszi a távoli AP-k konfigurálását és ellenőrzését a vállalati központból egy WAN-összeköttetésen keresztül, anélkül, hogy minden helyszínen telepíteni kellene egy vezérlőt. A FlexConnect AP-nak két üzemmódja van: csatlakoztatott és önálló.

A vezeték nélküli LAN-eszközök adó- és vevőáramkörei megadott frekvenciákra vannak hangolva a kommunikáció végrehajtásához. A frekvenciák tartományokra oszlanak, amelyeket tovább darabolnak, a kapott egységet pedig csatornának nevezik. A 802.11b/g/n szabványok a 2,4 GHz-től 2,5 GHz-ig működnek. A 2,4 GHz-es sávot is több csatornára osztották. Minden csatorna 20 MHz-el van eltolva a következő csatornától. Az AP-k helyének megtervezésekor fontos a körkörös lefedettségi terület hozzávetőleges meghatározása.

A vezeték nélküli hálózatok fogékonyak a fenyegetésekre, ilyenek például a csaló AP-k, az üzenet eltérítés és a DoS-támadások. A vezeték nélküli DoS-támadások okai a következők lehetnek: helytelenül konfigurált eszközök, egy rosszindulatú felhasználó szándékos zavarása és véletlen interferencia. A csaló AP egy olyan hozzáférési pont vagy vezeték nélküli router, amely engedély nélkül csatlakozik egy vállalati hálózathoz. Miután kapcsolódott, a támadó használhatja azt MAC-címek és adatcsomagok rögzítésére, hálózati erőforrásokhoz való hozzáférésre, vagy közbeékelődéses támadás indítására. Egy MITM-támadás során a hacker a kommunikáló felek között helyezkedik el, hogy elolvassa vagy módosítsa az átadott adatokat. Az egyik népszerű vezeték nélküli MITM-támadás az “evil twin AP” (gonosz iker) nevet viseli. Ilyenkor a támadó beüzemel egy csaló AP-t és ugyanazt az SSID-t állítja be rajta, mint ami a valódi AP-n van. A csaló hozzáférési pontok telepítésének megakadályozása érdekében a szervezeteknek a WLC-ket megfelelő házirendekkel kell konfigurálniuk.

A vezeték nélküli behatolók okozta fenyegetés távol tartására és az adatok védelmére két biztonsági szolgáltatás használható, amelyek megtalálhatók a legtöbb routeren és AP-n: az SSID-rejtés és a MAC-cím szűrés. Négy megosztott kulcsú hitelesítési módszer létezik: a WEP, a WPA, a WPA2 és a WPA3 (a WPA3-eszközök még nem terjedtek el). Az otthoni routerek általában két választási lehetőséget kínálnak a hitelesítéshez: a WPA-t és a WPA2-t. A WPA2 az erősebb. A titkosítás az adatvédelmet szolgálja. A WPA- és WPA2-szabvány a következő titkosítási protokollokat használja: TKIP és AES. A szigorúbb biztonságú hálózatokban fejlettebb hitelesítés vagy bejelentkezés szükséges a vezeték nélküli kliensek hozzáférésének engedélyezésére. Az Enterprise mód használatához AAA (Authentication, Authorization, Accounting; hitelesítés, jogosultság, naplózás) RADIUS-szerver kell.

12.8.2

## Ellenőrző kvíz - WLAN-alapok

Az űrlap teteje

1. Mobil eszközök kérdéskörében mit jelent a pányvázás (tethering)?

Az űrlap alja

A 802.11n szabványú vezeték nélküli hozzáférési pontok melyik tulajdonsága teszi lehetővé, hogy nagyobb adatátviteli sebesség legyen elérhető a korábbi 802.11 Wi-Fi szabványokhoz képest?

Melyik vezeték nélküli hitelesítési mód a legerősebb?

Melyik paramétert használják gyakran egy vezeték nélküli hálózat nevének azonosítására otthoni AP konfigurálásakor?

Melyik jellemző írja le az aktív üzemmódban működő vezeték nélküli klienst?

Melyik IEEE-szabvány működik mind az 5 GHz, mind a 2,4 GHz vezeték nélküli frekvenciatartományban?

Melyik álítás írja le az autonóm hozzáférési pontot?

Általában melyik két szerepet látja el az olyan vezeték nélküli router, amelyet otthoni vagy kisvállalati környezetben használnak? (Két jó válasz van.)

Milyen protokollt és portszámokat használnak mind az IPv4, mind az IPv6 CAPWAP alagutak? (Két jó válasz van.)

Ha három 802.11b szabványú hozzáférési pontot egymáshoz közel kell elhelyezni, akkor melyik három csatornát kell használni? (Három jó válasz van.)

Milyen típusú távközlési technológiát alkalmaznak a tengeri hajók internet-hozzáférésének biztosítására?

Melyik vezeték nélküli hálózati topológiát konfigurálja az a szakember, aki Bluetooth kapcsolatot használó billentyűzetet, egeret és fejhallgatót telepít?

Milyen típusú vezeték nélküli topológia jön létre, ha két vagy több BSS összekapcsolódik Etherneten keresztül?

Milyen Wi-Fi felügyeleti keret rendszeres küldésével hirdeti magát egy AP?

[12.7](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[WLAN-ok biztonsága](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Bevezetés

# Bevezetés

13.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a WLAN-konfigurációról szóló fejezetben!

Néhányan még emlékeznek a betárcsázós internet-elérésre. A tárcsázás vezetékes telefon használatával történt. Az internet használata közben a telefon nem volt használható. Az ilyen internetkapcsolat nagyon lassú volt. Ez alapvetően azt jelentette, hogy a legtöbb ember számára a számítógép mindig egy adott helyen volt, vagy az otthonában, vagy az iskolában.

Később a telefonvonal használata nélkül is tudtunk csatlakozni az internethez. A számítógépeink viszont még mindig erősen kötődtek az őket az internethez csatlakoztató eszközökhöz. Manapság vezeték nélküli eszközökkel kapcsolódhatunk az internethez, szinte bárhová elvihetjük telefonunkat, laptopjainkat és táblagépeinket. Jó a mozgás szabadsága, de speciális vég- és közvetítő eszközöket igényel, valamint a vezeték nélküli protokollok megfelelő ismeretét. Szeretnénk többet tudni? Akkor ez a modul kell nekünk!

13.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: WLAN Configuration

**Module Objective**: Implement a WLAN using a wireless router and WLC.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| Remote Site WLAN Configuration | Configure a WLAN to support a remote site. |
| Alapvető WLAN-beállítások a WLC-n | WLC WLAN konfigurálása a felügyeleti interfész és a WPA2 PSK hitelesítés használatához. |
| Vállalati WLAN-beállítások a WLC-n | WLC WLAN konfigurálása VLAN-interfész, DHCP-kiszolgáló és WPA2 vállalati hitelesítés használatára. |
| Troubleshoot WLAN Issues | Troubleshoot common wireless configuration issues. |

[12.8](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Külső telephelyi WLAN konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Külső telephelyi WLAN konfigurálása

# Külső telephelyi WLAN konfigurálása

13.1.1

## Videó - Vezeték nélküli hálózat konfigurálása

A vezeték nélküli hálózatról szóló videó megtekintéséhez kattintsunk az ábrán lévő Lejátszás gombra!

13.1.2

## Vezeték nélküli router

A távmunkásoknál, a kis irodai és az otthoni hálózatokban gyakan előfordulnak a SOHO-routerek (Small Office and HOme). Ezeket integrált routernek is nevezik, mert általában tartalmaznak egy switch-et a vezetékes kliensek számára, egy portot az internet-kapcsolat számára (néha „WAN”felirattal), és összetevőket a vezeték nélküli kliensek számára is (például az ábrán látható Cisco Meraki MX64W). A továbbiakban a kis irodai és otthoni routereket vezeték nélküli routernek nevezzük.

The figure shows the back of a small office or home router. The router has two antennas, one on each side. On the left, there is a reset button. Next to the reset button there are four ports for LAN devices to connect. Then theres a port for the WAN connection and finally the the power button and the port for the power cord.

### Cisco Meraki MX64W



A következő ábrán egy topológia látható, amelyen egy vezetékes laptop csatlakozik egy vezeték nélküli routerhez, majd az egy kábel- vagy DSL-modemen keresztül az internethez.

The figure depicts the physical connection of a wired laptop to the wireless router, which is then connected to a cable or DSL modem for internet connectivity. It shows a person sitting at a computer desk. Connected to the back of the desktop computer is a link going to a wireless router and from the wireless router theres a link going to the broadband modem. The broadband modem has a serial connection to the Internet depicted by a cloud.

Wireless routerBroadband ModemInternet

Ezek a vezeték nélküli routerek jellemzően WLAN-biztonságot, DHCP-szolgáltatásokat, címfordítást (NAT), szolgáltatásminőséget (QoS), valamint számos egyéb funkciót biztosítanak. A szolgáltatáskészlet a modelltől függően változhat.

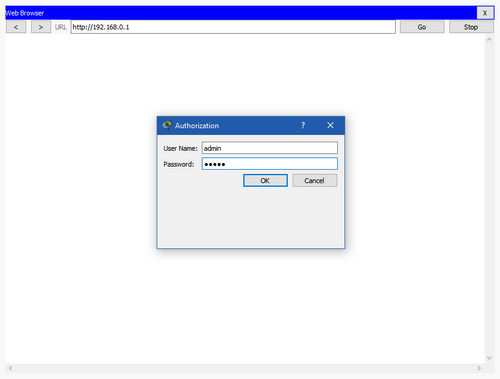
**Note**: Cable or DSL modem configuration is usually done by the service provider’s representative either on-site or remotely through a walkthrough with you on the phone. Modem vásárlásakor kapunk egy dokumentációt arról, hogyan csatlakoztassuk az eszközt a szolgáltatóhoz, amely valószínűleg tartalmazza, hogy további információkért lépjünk kapcsolatba az ügyfélszolgálattal.

13.1.3

## Bejelentkezés a vezeték nélküli routerre

A vezeték nélküli router kicsomagolás után rögtön használatra kész. A hálózati csatlakozás és bizonyos szolgáltatások már előre be vannak rajta állítva. Például a vezeték nélküli router DHCP-t használ, hogy automatikusan címzési információkat biztosítson a csatlakoztatott eszközöknek. A router alapértelmezett IP-címe, felhasználóneve és jelszava könnyedén fellelhető az interneten. Csak be kell írni a keresőbe a "wireless router default IP address" vagy a "wireless router default passwords" kifejezést, és számos weboldal jelenik meg a találati listában, megadva a keresett információt. Például, az ábrán látható router felhasználóneve és jelszava „admin”. Ezért biztonsági okokból elsődlegesen fontos az alapértelmezett beállítások megváltoztatása!

A vezeték nélküli router grafikus konfigurációs felületének eléréséhez nyissunk meg egy webböngészőt. A címmezőbe írjuk be a router alapértelmezett IP-címét. Ezt a címet az eszközhöz mellékelt dokumentációban találhatjuk meg, vagy megkereshetjük az interneten is. Az ábrán a 192.168.0.1 IP-cím látható, amely gyakori alapértelmezett érték számos gyártó esetében. Egy felugró ablak hitelesítési adatokat kér a router grafikus felületének eléréséhez. Alapértelmezett felhasználónévként és jelszóként általában az "admin" szót használjuk. Ezek az információk ugyancsak benne vannak a dokumentációban vagy megkereshetők az interneten.



13.1.4

## Alapvető hálózatbeállítás

Az alapszintű hálózati beállítás a következő lépéseket tartalmazza:

1. Bejelentkezés a routerre egy webböngészőből.
2. Az alapértelmezett jelszó megváltoztatása.
3. Bejelentkezés az új jelszóval.
4. A DHCP IPv4-címek módosítása.
5. Az IP-cím megújítása.
6. Bejelentkezés az új IP-címmel.

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. Jelentkezzen be az útválasztóba egy webböngészőből.** A bejelentkezés után megnyílik egy grafikus felhasználói felület.

A grafikus felhasználói felületen fülek vagy menük találhatók, amelyek segítenek eligazodni a különböző konfigurációs feladatokban. Az ablakban szükség van a megváltoztatott beállítások mentésére, mielőtt továbbmennénk egy másik ablakra. Lehetőség van a beállításoknak az alapértelmezett értékre történő visszaállítására is.

Kattintsunk a következő lépésre!

The figure depicts logging into a router from a web browser. There are seven tabs on the main menu: Setup, Wireless, Access Restrictions, Applications & Gaming, Administration and Status. The Setup tab has been selected and shows Internet
and Network setup options. Under Internet Setup it shows that DHCP has been selected as the Internet connection type and there are also optional settings to enter Hostname and Domain information, if required by the ISP. Under Network Setup,
The router IP is 192.168.0.1 with the subnet mask 255.255.255.0 and the DCHP server settings have been enabled on the router. The starting IP address to give to hosts is 192.168.0.100 and the maximum number of users is set to 50.

13.1.5

## Alapvető vezeték nélküli beállítások

Az alapszintű vezeték nélküli beállítás a következő lépéseket tartalmazza:

1. Az alapértelmezett WLAN-beállítások megtekintése.
2. Hálózati mód megváltoztatása.
3. Az SSID beállítása.
4. A vezeték nélküli csatorna beállítása.
5. A biztonsági mód kiválasztása.
6. A jelszó beállítása.

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. View the WLAN defaults.**

Out of the box, a wireless router provides wireless access to devices using a default wireless network name and password. A hálózat nevét szolgáltatáskészlet-azonosítónak (Service Set Identified, SSID) nevezzük. Ezeket az alapértelmezett értékeket a Basic Wireless Settings (alapvető vezeték nélküli beállítások) menüben lehet megváltoztatni.

Kattintsunk a következő lépésre!

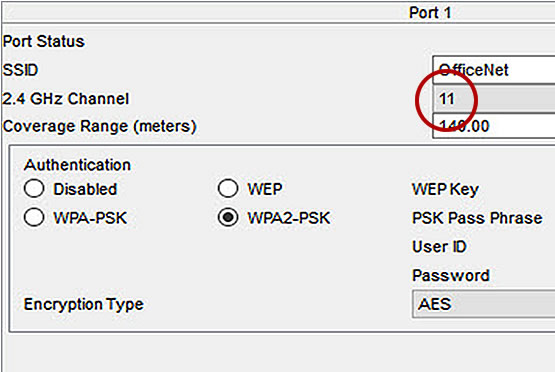
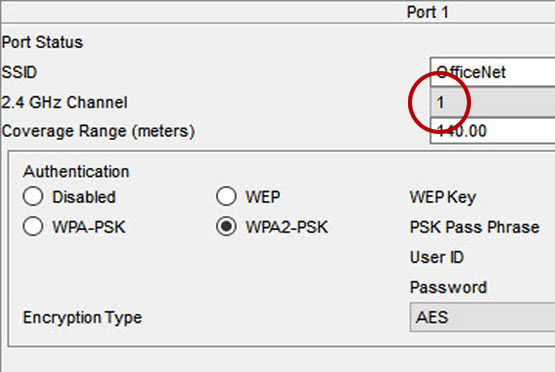
The figure depicts viewing the WLAN defaults on a router GUI. The Wireless tab has been selected and displays basic wireless settings. Under 2.4 GHz the network mode is auto, the network name (SSID) is Default, SSID broadcast is enabled, standard channel
is 2.412GHZ and the channel bandwidth is auto. Under 5 GHz the network mode is auto, the network name (SSID) is Default, SSID broadcast is enabled, standard channel is auto and the channel bandwidth is auto.

13.1.6

## A vezeték nélküli hálózat kiterjesztése

Egy kisvállalati vagy otthoni hálózatban egyetlen vezeték nélküli router is képes hozzáférést biztosítani az összes felhasználó számára. Ha szeretnénk kiterjeszteni a hatósugarat (beltéren körülbelül 45 méterrel és kültéren 90 méterrel), akkor további vezeték nélküli hozzáférési pontokkal bővíthetjük a hálózatot. Az ábrán látható kiterjesztett vezeték nélküli hálózatban két hozzáférési pont van ugyanolyan WLAN-beállításokkal konfigurálva. Vegyük észre, hogy az 1-es és 11-es csatornák lettek kiválasztva, így a hozzáférési pontok nem zavarják a korábban a 6-os csatornára beállított vezeték nélküli routert.

The figure depicts two wireless access points in a small office or home network. The wireless access points connect wirelessly to a router. The router is connected to a broadband modem. The broadband modem is connected to a cloud depicting the Internet. There are arrows pointing from the wireless access points showing the configuration settings. One wireless access point is on channel 1 on 2.4GHz and the other is on channel 11 on 2.4GHz.



internet

Egy kisvállalati vagy otthoni WLAN kiterjesztése egyre egyszerűbben megvalósítható. A gyártók okostelefon alkalmazásokon keresztül lehetővé teszik a kiterjesztett vezeték nélküli hálózat (Wireless Mesh Network, WMN) létrehozását. Megvásároljuk a rendszert, szétosztjuk és csatlakoztatjuk a hozzáférési pontokat, letöltjük az alkalmazást, majd néhány lépésben beállítjuk a WMN-t. Keressünk rá az interneten a "best wi-fi mesh network system" kifejezésre az aktuális ajánlatok megtekintéséhez!

13.1.7

## IPv4-címfordítás (NAT)

Ha megnézzük egy router "Status" oldalát, megtekinthetjük azon IPv4 címzési információkat, amelyeket a router használ az internetre történő adatküldéshez. Vegyük észre, hogy a 209.165.201.11 IPv4 -cím eltérő hálózatban van, mint a router LAN-interfészéhez rendelt 10.10.10.1 cím. A LAN-interfészéhez csatlakozó összes eszköz 10.10.10 előtaggal rendelkező címet fog kapni.

The figure depicts a the Status information of a small office/home office router. The Router tab under Status on the main menu is selected and displays router information as well as information on Internet connection. Under router information, it lists the
Firmware version: v0.93.3, Current time: not available, Internet MAC address: 000D.BDA6.3001, Host Name and Domain. Under Internet connection, it lists the connection type: DHCP, Internet IP Address: 209.165.201.11, Subnet mask: 255.255.255.0, Default gateway:
209.165.201.1, DNS: 64.100.0.100, MTU: 1500, and DHCP Lease time: 1 day.

A 209.165.201.11 IPv4-cím nyilvános és irányítható az interneten. Viszont, bármely olyan cím, amelynek első oktettjében a 10 szerepel, magán IPv4-címnek minősül és nem továbbítható az interneten. Ezért a router egy hálózati címfordításnak (Network Address Translation, NAT) nevezett folyamatot használ, hogy a privát IPv4-címeket interneten is továbbítható IPv4-címekké alakítsa. A NAT használatával egy privát (helyi) forrás IPv4-cím átfordítható egy publikus (nyilvános) címre. Bejövő csomagoknál a folyamat fordított irányban zajlik le. A router a NAT segítségével több belső IPv4-címet is képes nyilvános IP-címekre fordítani.

Néhány szolgáltató magán IP-címeket használ az előfizetői készülékek csatlakozásához is. Ettől függetlenül a forgalom elhagyhatja a szolgáltatói hálózatot és továbbítva lesz az interneten. Eszközünk IP-címének megtekintéséhez keressünk rá az interneten a "what is my IP address" kifejezésre! Tegyük meg ezt a többi eszközről is ugyanebből a hálózatból, és azt fogjuk látni, hogy mindegyikük ugyanazt a publikus IPv4-címet használja. A NAT ezt úgy teszi lehetővé, hogy nyomon követi a forrás portszámokat minden egyes, az eszköz által indított munkamenetre vonatkozóan. Amennyiben az ISP támogatja az IPv6-ot, minden egyes eszköznél egyedi IPv6-címet fogunk látni.

13.1.8

## Szolgáltatás minőség (QoS)

Számos vezeték nélküli router rendelkezik szolgáltatásminőségre (Quality of Service, QoS) vonatkozó beállítási lehetőséggel. A QoS beállításával biztosíthatjuk, hogy bizonyos forgalomtípusok, mint például a hang és a videó, magasabb prioritással rendelkezzenek a nem időérzékeny forgalomhoz, például az elektronikus levelezéshez és a webböngészéshez képest. Bizonyos vezeték nélküli routereken a forgalmat meghatározott portok alapján lehet rangsorolni.

Az ábrán egy QoS-felület egyszerűsített modellje látható, Netgear grafikus felhasználói felületen. A QoS-beállításokat általában az Advanced menüben találhatjuk. Amennyiben van vezeték nélküli routerünk, vizsgáljuk meg a QoS-beállításokat! Néha ezt a "sávszélesség-szabályozás" vagy hasonló menüpont alatt találhatjuk meg. Nézzünk utána a vezeték nélküli router dokumentációjában, vagy keressünk rá az interneten a "qos settings" kulcsszóra a gyártó és a modellszám alapján!

| **#** | **Qos Policy** | **Priority** | **Description** |
| --- | --- | --- | --- |
| 1 | IP Phone | High | IP Phone applications |
| 2 | Counter Strike | High | Online Gaming Counter Strike |
| 3 | Netflix | High | Online Video Streaming Netflix |
| 4 | FTP | Medium | FTP Applications |
| 5 | WWW | Medium | WWW Applications |
| 6 | Gnutella | Low | Gnutella Applications |
| 7 | SMTP | Medium | SMTP Applications |

Add Priority RoleAdvanced SetupAdminisztrációBiztonságStorageBeállításAdvanced HomeBasicSpeciálisÖsszes törléseSzerkesztésTörlésMégsemapplyQoS SetupInternet SetupWireless SetupLAN SetupQoS Setup

13.1.9

## Port továbbítás

A vezeték nélküli routerek általában blokkolják a TCP- és UDP-portokat, így megakadályozható a jogosulatlan hozzáférés egy helyi hálózatba bemenő és kimenő irányban is. Vannak azonban helyzetek, amikor bizonyos portokat meg kell nyitni, hogy a programok és az alkalmazások kommunikálni tudjanak a más hálózatokban található eszközökkel. A porttovábbítás (port forwarding) egy szabály alapú módszer a különböző hálózatokon lévő eszközök közötti forgalom engedélyezéséhez.

Amikor a forgalom eléri a routert, az meghatározza, hogy a forgalmat továbbítani kell-e egy adott készülékre a csomagokban látott portszám alapján. Például egy router konfigurálható a HTTP-hez társított 80-as port továbbítására. Amikor a router kap egy csomagot 80-as célporttal, akkor továbbítja a forgalmat a belső hálózati szervernek, amely a weboldalakat szolgáltatja. Az ábrán a porttovábbítás a 80-as port számára van engedélyezve és a webkiszolgáló 10.10.10.50 IPv4-címéhez van hozzárendelve.

The figure depicts the Port Forward options on a small office/home office router GUI. The Applications & Gaming tab on the main menu is selected and displays port forwarding information.
Under application name for a single port, is the name Web Server. The external and internal port are set to 80. The protocol is TCP and the address to forward is set to 10.10.10.50.

A portkioldás (port triggering) lehetővé teszi, hogy a router ideiglenesen adatokat továbbítson a bejövő portokon át egy adott eszköz számára. Használhatjuk arra, hogy csak akkor továbbítsuk az adatokat egy számítógépnek, ha egy kijelölt porttartományt használunk egy kimenő kéréshez. Például, egy videojáték használhatja a 27000 és 27100 közötti portokat a többi játékossal való összekapcsolódáshoz. Ezek a trigger (kioldó) portok. A csevegőkliens az 56-os portot használja ugyanazon játékosok összekapcsolására, hogy beszélgetni tudjanak egymással. Ebben az esetben, ha kimenő forgalom van a trigger porttartományon belül, akkor az 56-os porton a bejövő csevegőforgalom továbbítva lesz a videojátékok lejátszására használt számítógépre. Amikor a játéknak vége, és a trigger portok már nincsenek használatban, az 56-os porton már nem lesz engedélyezett a forgalom továbbítása erre a számítógépre.

13.1.10

## Packet Tracer - Vezeték nélküli hálózat konfigurálása

Ebben a feladatban egy vezeték nélküli routert és egy hozzáférési pontot konfigurálunk az ügyfelek csatlakoztatásához és az IP-csomagok továbbításához.

[Vezetéknélküli hálózat beállítása](https://contenthub.netacad.com/courses/srwe-dl/_common/13.1.10-packet-tracer---configure-a-wireless-network_hu-HU.pka)

13.1.11

## Laborgyakorlat - Vezeték nélküli hálózat konfigurálása

A laborgyakorlat során alapvető beállításokat fogunk elvégezni egy vezeték nélküli routeren, majd vezeték nélkül fogunk csatlakoztatni hozzá egy PC-t.

[13.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Alapvető WLAN-beállítások a WLC-n](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Alapvető WLAN-beállítások a WLC-n

# Alapvető WLAN-beállítások a WLC-n

13.2.1

## Videó - Alapvető WLAN-beállítások a WLC-n

Az előző témakörben megismerkedtünk az egyedi WLAN konfigurációjával. Ez a témakör egy WLAN alapvető konfigurálásáról szól a WLC-n.

Kattintsunk a Lejátszás gombra a Cisco 3504 WLC alapvető WLAN-kapcsolatának beállításáról szóló videó megtekintéséhez.

13.2.2

## WLC-topológia

A videókhoz és a témához használt topológia és címzési séma az ábrán és a táblázatban látható. Ez a hozzáférési pont egy vezérlő alapú AP, szemben az eddigi egyedi (autonóm) hozzáférési ponttal. Emlékezzünk vissza, hogy a vezérlő alapú hozzáférési pontok nem igényelnek kezdeti konfigurációt, és gyakran nevezik őket LAP-nek. A LAP-ok az LWAPP (Lightweight Access Point Protocol) segítségével kommunikálnak a WLAN-vezérlővel. 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.

The figure shows a wireless LAN controller (WLC) topology. PC-A is a RADIUS/SNMP Server connected to R1 on R1s F0/0 interface. PC-B is connected to S1 on S1s F0/6 port. R1 and S1 are connected together on R1s F0/1 interface and on S1s F0/5 interface. S1 is connected to a WLC on its F0/18 port. On S1s F0/1 port its connected to an access point, AP1. A laptop is wirelessly connected to AP1.

### Topológia

PC-A PC-B R1 S1 AP1 WLC F0/0 F0/1 F0/5 F0/18 G1 F0/6

F0/1

RADIUS/SNMP ServerAdminPoE802.1q trunk802.1q trunk

Az AP PoE-képes, ami azt jelenti, hogy a switch-hez csatlakoztatott Ethernet kábelen keresztül kap tápellátást.

### Címzési táblázat

| DeviceInterfaceIP AddressSubnet MaskR1F0/0172.16.1.1255.255.255.0R1F0/1.1192.168.200.1255.255.255.0S1VLAN 1DHCPWLCManagement192.168.200.254255.255.255.0AP1Wired 0192.168.200.3255.255.255.0PC-ANIC172.16.1.254255.255.255.0PC-BNICDHCPWireless LaptopNICDHCP | | | |
| --- | --- | --- | --- |
| **Eszköz** | **Interfész** | **IP-cím** | **Alhálózati maszk** |
| R1 | F0/0 | 172.16.1.1 | 255.255.255.0 |
| R1 | F0/1.1 | 192.168.200.1 | 255.255.255.0 |
| S1 | VLAN 1 | DHCP | |
| WLC | Management | 192.168.200.254 | 255.255.255.0 |
| AP1 | Wired 0 | 192.168.200.3 | 255.255.255.0 |
| PC-A | NIC | 172.16.1.254 | 255.255.255.0 |
| PC-B | NIC | DHCP | |
| Wireless Laptop | NIC | DHCP | |

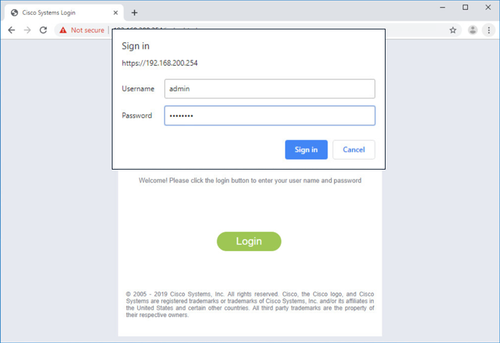
13.2.3

## Bejelentkezés a WLC-be

Egy vezeték nélküli LAN-vezérlő (WLC) konfigurálása nem sokban különbözik egy vezeték nélküli router konfigurálásától. A nagy különbség az, hogy a WLC vezérli az AP-ket, és több szolgáltatást és felügyeleti lehetőséget nyújt, amelyek közül sok túlmutat a modul hatókörén.

**Note**: The figures in this topic that show the graphical user interface (GUI) and menus are from a Cisco 3504 Wireless Controller. Más WLC-modellekben is hasonló menüket és jellemzőket találhatunk.

Az ábrán az látható, amint a felhasználó bejelentkezik a WLC-be az alapértelmezett hitelesítő adatokkal.



The **Network Summary** page is a dashboard that provides a quick overview of the number of configured wireless networks, associated access points (APs), and active clients. Iitt látható a nem hitelesített (rouge, csaló) hozzáférési pontok és ügyfelek száma is.

The figure depicts the Network Summary page on a WLC GUI. The Network summary tab is selected showing the number of wireless networks: 0, access points: 1, Active clients on 2.4 GHz and 5 GHz: 0, Rogue APs: 51, Rogue Clients: 5 and
Interferers on 2.4 GHz and 5 GHz: 0. It also shows the access points usage in a doughnut chart and operating systems.

13.2.4

## AP-információk megtekintése

Click **Access Points** from the left menu to view an overall picture of the AP’s system information and performance, as shown in the next figure. Az AP a 192.168.200.3 IP-címet használja. Mivel a CDP (Cisco Discovery Protocol) aktív ezen a hálózaton, a WLC tudja, hogy a hozzáférési pont a switch Fastethernet 0/1 portjához van csatlakoztatva.

The figure depicts information about Access Points on a WLC GUI. The Access points tab is selected showing information about the access point. It lists the AP name, Location, Mac Address, IP address, CDP/LLDP, Ethernet Speed, Model/Domain, Power status,
Serial Number, Groups, Mode/sub-mode, Max capabilities, Fabric. There is also a Performance Summary which lists the number of Clients, Channels, Configured Rate, Usage Traffic, Throughput, Transmit Power, Noise, Channel Utilization, Interference,
Traffic, Air Quality, Admin Status, and Clean Air Status for both 2.4 GHz and 5GHz. 

Ez az AP egy Cisco Aironet 1815i, ami azt jelenti, hogy használhatjuk a parancssort és bizonyos ismerős IOS-parancsokat. A példában a hálózati rendszergazda pingeli az alapértelmezett átjárót és a WLC-t, valamint ellenőrzi a vezetékes interfészt.

AP1# **ping 192.168.200.1**

Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1069812.242/1071814.785/1073817.215 ms

AP1# **ping 192.168.200.254**

Sending 5, 100-byte ICMP Echos to 192.168.200.254, timeout is 2 seconds

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1055820.953/1057820.738/1059819.928 ms

AP1# **show interface wired 0**

wired0 Link encap:Ethernet HWaddr 2C:4F:52:60:37:E8

inet addr:192.168.200.3 Bcast:192.168.200.255 Mask:255.255.255.255

UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1

RX packets:2478 errors:0 dropped:3 overruns:0 frame:0

TX packets:1494 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:80

RX bytes:207632 (202.7 KiB) TX bytes:300872 (293.8 KiB)

AP1#

13.2.5

## Haladó beállítások

A legtöbb WLC kezdőoldala csak alapvető beállításokat és menüket tartalmaz, amelyben a felhasználók gyorsan megvalósíthatják a különféle konfigurációkat. Hálózati rendszergazdaként azonban hozzáférhetünk a speciális beállításokhoz. For the Cisco 3504 Wireless Controller, click **Advanced** in the upper right-hand corner to access the advanced **Summary** page, as shown in the figure. Innen elérhetjük a WLC összes funkcióját.

The figure depicts the Summary page on a WLC GUI. The Monitor tab is selected showing the Summary page for a Cisco 3504 Wireless controller. It shows the front of a Cisco 3504 Wireless controller and information about the controller such as
Management address, Software version, System name, Uptime, Active rogue APs, Active Rogue Clients, ADhoc Rogues and Rogues on Wired Network.

13.2.6

## WLAN konfigurálása

A vezeték nélküli LAN-vezérlők portokkal és interfészekkel rendelkeznek. A portok a vezetékes hálózathoz való fizikai csatlakozásra szolgálnak. Hasonlítanak a switch portokra. Az interfészek virtuálisak. Szoftveresen hozhatók létre, és nagyon hasonlítanak a VLAN-interfészekhez. Valójában minden olyan interfész, amely egy adott WLAN forgalmát hordozza, a WLC-n más-más VLAN-ként van konfigurálva. A Cisco 3504 WLC 150 hozzáférési pontot és 4096 VLAN-t támogat, azonban csak öt fizikai portja van (lásd ábra). Ez azt jelenti, hogy minden fizikai porthoz számos AP és WLAN csatlakozhat . A WLC portjai lényegében trönk portok, amelyek képesek átadni több VLAN forgalmát egy switch-en keresztül az AP-k felé. Minden hozzáférési pont több WLAN-t is kezelhet.

The figure shows the front of a Cisco 3504 Wireless Controller. It has 2 service ports for out-of-band management, a console port, a mini-usb console port, 3.0 USB port, a 5G port, and four gigabit ports.



A WLC alapvető WLAN-konfigurációja a következő lépéseket tartalmazza:

1. WLAN létrehozása
2. WLAN alkalmazása és engedélyezése
3. Interfész kiválasztása
4. WLAN-biztonság beállítása
5. A WLAN működésének ellenőrzése
6. A WLAN felügyelete
7. Vezeték nélküli ügyféladatok megtekintése

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. Create the WLAN**

In the figure, the administrator is creating a new WLAN that will use **Wireless\_LAN** as the name and service set identifier (SSID). Az ID egy tetszőleges érték, amely a WLC-n a WLAN azonosítására szolgál.

The figure depicts the creation of a new WLAN on a WLC GUI. The WLANs New tab is selected with options for the Type, Profile Name, SSID and ID. The type is WLAN, the profile name is Wireless_LAN,
the SSID is Wireless_LAN and the ID is 1. 

13.2.7

## Packet Tracer - Alapvető WLAN-beállítások a WLC-n

Ebben a feladatban megismerjük egy vezeték nélküli LAN-vezérlő néhány funkcióját. Létrehozunk egy új WLAN-t a vezérlőn, és biztonsági beállításokat adunk meg hozzá. Ezután konfigurálunk egy vezeték nélküli állomást, amely a WLC irányítása alatt álló AP-n keresztül csatlakozik az új WLAN-hoz. Végül ellenőrizni fogjuk a kapcsolatokat.

[Alapvető WLAN-beállítások a WLC-n](https://contenthub.netacad.com/courses/srwe-dl/_common/13.2.7-packet-tracer---configure-a-basic-wlan-on-the-wlc_hu-HU.pka)

[13.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Külső telephelyi WLAN konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Vállalati WLAN-beállítások a WLC-n](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Vállalati WLAN-beállítások a WLC-n

# Vállalati WLAN-beállítások a WLC-n

13.3.1

## Videó — SNMP- és RADIUS-kiszolgáló beállítása a WLC-n

Az előző témakör egy WLAN alapvető konfigurálásáról szólt a WLC-n. Most megismerkedünk egy vállalati WPA2 WLAN konfigurálásával.

Kattintsunk a Lejátszás gombra az SNMP- és a RADIUS-szolgáltatások WLC-n történő konfigurálásának megtekintéséhez.

13.3.2

## SNMP és RADIUS

Az ábrán látható PC-A számítógép SNMP (Simple Network Management Protocol) és RADIUS (Remote Authentication Dial-In User Service) kiszolgáló szoftvert futtat. Az SNMP a hálózat megfigyelésére szolgál. A hálózati rendszergazda azt szeretné, hogy a WLC továbbítsa az összes SNMP-naplóüzenetet, amelyet "trap"-nek hívnak, az SNMP-kiszolgálónak.

Emellett a WLAN felhasználói hitelesítéshez a rendszergazda RADIUS-kiszolgálót szeretne használni a hitelesítési, az engedélyezési és a naplózási szolgáltatásokhoz (AAA). Ahelyett, hogy egy többek által ismert, előre megosztott kulcsot írnának be a hitelesítéshez, mint a WPA2-PSK esetében, a felhasználók saját felhasználónevüket és jelszavukat adják meg. A hitelesítő adatokat a RADIUS-kiszolgáló ellenőrzi. Így szükség esetén nyomon követhető és naplózható az egyéni felhasználói hozzáférés, és a fiókok központi helyről adhatók hozzá vagy módosíthatók. A WPA2 Enterprise hitelesítést használó WLAN-ok esetében RADIUS-kiszolgáló szükséges.

**Note**: SNMP server and RADIUS server configuration is beyond the scope of this module.

The figure depicts a network topology. PC-A is a RADIUS/SNMP Server connected to R1 on R1s F0/0 interface. PC-B is connected to S1 on S1s F0/6 port. R1 and S1 are connected together on R1s F0/1 interface and on S1s F0/5 interface. S1 is connected to a WLC on its F0/18 port. On S1s F0/1 port its connected to an access point, AP1. A laptop is wirelessly connected to AP1.

### Topológia

PC-A PC-B R1 S1 AP1 WLC F0/0 F0/1 F0/5 F0/18 G1 F0/6

F0/1

RADIUS/SNMP ServerAdminPoE802.1q trunk802.1q trunk802.1q trunk

13.3.3

## SNMP-kiszolgáló adatainak beállítása

Click the **MANAGEMENT** tab to access a variety of management features. Az SNMP a bal oldali menü tetején található. Click **SNMP** to expand the sub-menus, and then click **Trap Receivers**. Click **New...** to configure a new SNMP trap receiver, as shown in the figure.

The figure depicts three steps to creating a new SNMP server configuration on a WLC GUI. The Management tab on the main menu is selected and outlined with a rectangle and the number 1. SNMP on the sub-menu is selected and outlined with a rectangle and the
number 2. Trap Receivers is selected and outlined with a rectangle and the number 3. The New... button is outlined with a rectangle and the number 4.

1. Click **MANAGEMENT**
2. Click **SNMP**
3. Click **Trap Receivers**
4. Click **New...**

Adjuk meg az SNMP-kiszolgáló Community nevét és IP-címét (IPv4 vagy IPv6). Kattintson a **Apply** gombra. A WLC továbbítani fogja az SNMP-naplóüzeneteket az SNMP-kiszolgálónak.

The figure depicts entering the SNMP Trap Receiver information and applying the configuration. The Management tab on the main menu is selected and under SNMP Trap Receiver> New, the Community Name is CCNAv7, the IP address is 172.16.1.254 and the status has
been enabled. The Apply button is outlined with a rectangle indicating to click.

13.3.4

## RADIUS-kiszolgáló adatainak beállítása

A példa konfigurációban a rendszergazda WPA2 Enterprise (vállalati) használatával szeretne WLAN-t konfigurálni, a WPA2 Personal (személyes, WPA2 PSK) szolgáltatás helyett. A hitelesítést a PC-A számítógépen futó RADIUS-kiszolgáló kezeli.

To configure the WLC with the RADIUS server information, click the **SECURITY** tab > **RADIUS** > **Authentication**. Jelenleg nincs konfigurálva RADIUS-kiszolgáló. Click **New...** to add PC-A as the RADIUS server.

The figure depicts four steps to creating a new RADIUS Authentication server configuration on a WLC GUI. The Security tab on the main menu is selected and outlined with a rectangle and the number 1. RADIUS on the sub-menu is selected and outlined with a
rectangle and the number 2. Authentication is selected and outlined with a rectangle and the number 3. The New... button is outlined with a rectangle and the number 4.

1. Click **SECURITY**
2. Click **RADIUS**
3. Click **Authentication**
4. Click **New...**

Adjuk meg a PC-A IPv4-címét és a megosztott titkos kulcsot. Ez a jelszó a WLC és a RADIUS-kiszolgáló között működik. Nem a felhasználóknak szól. Click **Apply**, as shown in the figure.

The figure depicts device information and options for creating a new RADIUS Authentication server configuration on the WLC GUI. The Security tab on the main menu is selected and under RADIUS Authentication Servers> New, the Server IP Address is 172.16.1.254
and a shared secret has been typed and confirmed. The Apply button is outlined with a rectangle indicating to click.

Az **Apply** gombra való kattintás után a **RADIUS Authentication Servers** lista az ábrán látható új kiszolgálóval frissül.



13.3.5

## Videó - VLAN konfigurálása egy új WLAN-hoz

Kattintsunk a Lejátszás gombra egy VLAN WLC-n történő konfigurálásának megtekintéséhez.

13.3.6

## Topológia (VLAN 5 címzéssel)

A WLC-n konfigurált minden WLAN-nak saját virtuális interfészre van szüksége. A WLC öt fizikai porttal rendelkezik az adatforgalom számára. Minden fizikai port konfigurálható több WLAN fogadására a saját virtuális interfészén keresztül. Lehetséges a fizikai portok összefogása is, nagy sávszélességű kapcsolatok létrehozásához.

A rendszergazda úgy döntött, hogy az új WLAN a VLAN 5 interfészt és a 192.168.5.0/24 hálózatot használja. Az R1 már rendelkezik egy VLAN 5-höz konfigurált és aktív alinterfésszel, amint azt a topológia és a **show ip interface brief** kimenet is mutatja.

The figure depicts a network topology. PC-A is a RADIUS/SNMP Server connected to R1 on R1s F0/0 interface. R1 has a sub-interface configured on VLAN 5 with the IP address 192.168.5.1. PC-B is connected to S1 on S1s F0/6 port. R1 and S1 are connected together on R1s F0/1 interface and on S1s F0/5 interface. S1 is connected to a WLC on its F0/18 port. The WLC has the management IP address of 192.168.200.254 and an interface on VLAN 5 with an IP address of 192.168.5.254. On S1s F0/1 port its connected to an access point, AP1. A laptop is wirelessly connected to AP1.

### Topológia

PC-A PC-B R1 S1 AP1 F0/0 F0/18 F0/6 F0/5 F0/1 G1

F0/1

RADIUS/SNMP ServerPoEWLCManagement: 192.168.200.254  
Interface VLAN5: 192.168.5.254802.1q trunk802.1q trunk802.1q trunkVLAN5:192.168.5.1

R1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 172.16.1.1 YES manual up up

FastEthernet0/1 unassigned YES unset up up

FastEthernet0/1.1 192.168.200.1 YES manual up up

FastEthernet0/1.5 192.168.5.1 YES manual up up

(output omitted)

R1#

13.3.7

## Új interfész konfigurálása

A VLAN-interfész konfigurációja a WLC-n a következő lépésekből áll:

1. Új interfész konfigurálása.
2. VLAN-név és azonosító beállítása.
3. Port és interfész cím beállítása.
4. DHCP-kiszolgáló címének beállítása.
5. Alkalmazás és megerősítés.
6. Interfész beállítások ellenőrzése.

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. Create a new interface.**

To add a new interface, click **CONTROLLER > Interfaces > New...**, as shown in the figure.

The figure depicts the creation of a new interface on a WLC GUI. The Controller tab on the main menu is selected and outlined with a rectangle and the number 1. Interfaces on the sub-menu is selected and outlined with a rectangle and the number 2. The New...
button is outlined with a rectangle and the number 3.

1. Click **CONTROLLER**
2. Click **Interfaces**
3. Click **New...**

13.3.8

## Videó - DHCP-hatókör konfigurálása

Kattintsunk a Lejátszás gombra a DHCP-szolgáltatások konfigurálásának megtekintéséhez!

13.3.9

## DHCP-hatókör konfigurálása

A DHCP-hatókör konfigurációja a következő lépéseket tartalmazza:

1. Új DHCP-hatókör létrehozása.
2. A DHCP-hatókör elnevezése.
3. A DHCP-hatókör ellenőrzése.
4. Az új DHCP-hatókör beállítása és engedélyezése.
5. A DHCP-hatókör működésének ellenőrzése.

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. Create a new DHCP scope.**

A DHCP scope is very similar to a DHCP pool on a router. Számos információt tartalmazhat, többek között az ügyfelekhez rendelhető címkészletet, a DNS-kiszolgáló adatait, a bérleti időket stb. To configure a new DHCP scope, click **Internal DHCP Server > DHCP Scope > New...**, as shown in the figure.

The figure depicts the creation of a new DHCP Scope on a WLC GUI. The Controller tab on the main menu is selected. The Internal DHCP Server sub-menu is selected and outlined with a rectangle and the number 1. DHCP Scope is selected and outlined with a rectangle
and the number 2. The New... button is outlined with a rectangle and the number 3.

1. Click **Internal DHCP Server**.
2. Click **DHCP Scope**.
3. Click **New...**

13.3.10

## Videó - WPA2 Enterprise WLAN konfigurálása

Kattintsunk a Lejátszás gombra a WPA2 Enterprise WLC-n történő konfigurálásának megtekintéséhez.

13.3.11

## WPA2 Enterprise WLAN konfigurálása

Alapértelmezés szerint a WLC-n minden újonnan létrehozott WLAN a WPA2 AES-t (Advanced Encryption System) fogja használni. A 802.1X az alapértelmezett kulcskezelési protokoll a RADIUS-kiszolgálóval történő kommunikációhoz. Mivel a hálózati rendszergazda már konfigurálta a WLC-n a RADIUS-kiszolgálót a PC-A IPv4-címével, egyetlen beállítás maradt hátra, egy új WLAN létrehozása a **vlan5** interfész használatával.

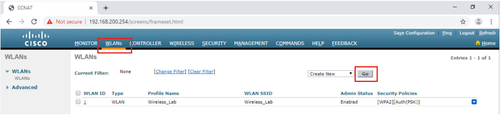
Az új WLAN konfigurálása a WLC-n a következő lépéseket tartalmazza:

1. Új WLAN létrehozása.
2. WLAN-név és SSID konfigurálása.
3. A WLAN engedélyezése a VLAN 5 számára.
4. Az AES és a 802.1X beállítások ellenőrzése.
5. A WLAN-biztonság beállítása a RADIUS-kiszolgáló használatához.
6. Az új WLAN elérhetőségének ellenőrzése.

További információért és GUI példákért kattintsunk az egyes lépésekre!

**1. Create a new WLAN.**

Click the **WLANs** tab and then **Go** to create a new WLAN, as shown in the figure.



13.3.12

## Packet Tracer - WPA2 Enterprise WLAN konfigurálása a WLC-n

Ebben a feladatban új WLAN-t hozunk létre egy vezeték nélküli LAN-vezérlőn (WLC), beleértve a használni kívánt VLAN-interfészt is. A WLAN-t úgy konfiguráljuk, hogy RADIUS-kiszolgálót és WPA2-Enterprise biztonságot használjon a felhasználók hitelesítéséhez. Továbbá beállítjuk a WLC-t SNMP-kiszolgáló használatára is.

[WPA2 vállalati WLAN konfigurálása a WLC-n](https://contenthub.netacad.com/courses/srwe-dl/_common/13.3.12-packet-tracer---configure-a-wpa2-enterprise-wlan-on-the-wlc_hu-HU.pka)

[13.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Alapvető WLAN-beállítások a WLC-n](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Troubleshoot WLAN Issues](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Troubleshoot WLAN Issues

# Troubleshoot WLAN Issues

13.4.1

## Hibaelhárítási szemléletmódok

Az előző témakörökben megismerkedtünk a WLAN konfigurációjával. Most megvitatjuk a WLAN-problémák elhárítását.

A hálózati hibák lehetnek egészen egyszerűek vagy nagyon összetettek is, és származhatnak különböző hardveres, szoftveres vagy konfigurációs problémák valamilyen kombinációjából. Szakemberként képesnek kell lennünk a problémák vizsgálatára és a rendellenesség okának meghatározására, annak kijavítása érdekében. Ezt a folyamatot nevezzük hibaelhárításnak.

Mindenféle hálózati probléma elhárítása szisztematikus megközelítést igényel. A hatékony hibaelhárítás tudományos módszereken alapul, és hat lépésre bontható (lásd táblázat).

| StepTitleDescription1A probléma azonosításaAz első lépés a troubleshooting process is to identify the problem. Miközben az eszközök használhatók in this step, a conversation with the user is often very helpful.2Establish a Theory of Probable CausesAfter you have talked to the user and identified the problem, you can try and establish a theory of probable causes. Lehetővé teszi továbbá, hogy a meglévő ügyfeleknél új jövedelemforrásra találjon, új ügyfeleket szólítson meg, valamint kiépítse, és tovább bővítse szolgáltatásértékesítési hálózatát. step often yields more than a few probable causes to the problem.3Test the Theory to Determine CauseBased on the probable causes, test your theories to határozza meg, melyik a probléma oka. A technician will often apply a quick procedure to test and see if it solves the problem. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause.4Establish a Plan of Action to Resolve the Problem and Implement the SolutionAfter you have determined the exact cause of the problem, establish a plan of action to resolve the problem and implement the solution.5Verify Full System Functionality and Implement Preventive MeasuresAfter you have corrected the problem, verify full functionality and, if applicable, implement preventive intézkedések.6 Dokumentum megállapítások, cselekvések és eredményekAz utolsó lépésben a troubleshooting process, document your findings, actions, and outcomes. Lehetővé teszi továbbá, hogy a meglévő ügyfeleknél új jövedelemforrásra találjon, új ügyfeleket szólítson meg, valamint kiépítse, és tovább bővítse szolgáltatásértékesítési hálózatát. is very important for future reference. | | |
| --- | --- | --- |
| **Lépés** | **Megszólítás** | **Leírás** |
| 1 | A probléma azonosítása | The first step in the troubleshooting process is to identify the problem. While tools can be used in this step, a conversation with the a felhasználó gyakran nagyon segítőkész. |
| 2 | A lehetséges okok meghatározása. | After you have talked to the user and identified the problem, you can try and establish a theory of probable causes. Ez a lépés gyakran meghozza az eredményt more than a few probable causes to the problem. |
| 3 | Az elmélet tesztelése a hiba okának meghatározásához | Based on the probable causes, test your theories to determine which az egyik a probléma oka. Egy technikus gyakran alkalmaz egy gyors procedure to test and see if it solves the problem. If a quick procedure does not correct the problem, you might need to research the problem further to establish the exact cause. |
| 4 | Establish a Plan of Action to Resolve the Problem and Implement the Solution | Miután meghatározta a probléma pontos okát, állapítsa meg a plan of action to resolve the problem and implement the solution. |
| 5 | A rendszer teljes működésének ellenőrzése és megelőző intézkedések alkalmazása | After you have corrected the problem, verify full functionality and, if applicable, implement preventive measures. |
| 6 | A probléma, a megoldási lépések és az eredmények dokumentálása | In the final step of the troubleshooting process, document your findings, actions, and outcomes. This is very important for future reference. |

A probléma felmérésekor először állapítsuk meg, hogy a hálózat hány eszközét érinti a hiba. Ha csak egyet, akkor kezdjük a hibaelhárítást azon az eszközön. Ha minden eszköz érintett, akkor kezdjük a hiba felderítését azon a berendezésen, ahová az összes többi csatlakozik. A hibák megállapításakor kövessünk mindig egy logikus és következetes eljárást, amelynek során lépésről lépésre, de egyszerre csak egy problémát hárítunk el.

13.4.2

## A vezeték nélküli kliens nem csatlakozik

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

Az ábrán látható vezeték nélküli kliens nem tud a WLAN-hoz csatlakozni.

The figure shows a network topology with a wireless client not able to connect to the AP. The figure has a router connected to a switch. The switch is connected to a second switch. The second switch is connected to a WLC, 2 PCs and the AP. The AP is wirelessly connected to a Cell phone, Tablet and Laptop. However the Laptop connection to the AP has an X indicating no connection has been formed.

AP

WLC

Ha nincs kapcsolat, vizsgáljuk meg a következőket:

Ellenőrizzük a PC hálózati konfigurációját az \* Confirm the network configuration on the PC using the **ipconfig** paranccsal. 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 pingeljünk 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 NIC 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 egy 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. Nézzük meg az áramellátás állapotát.

13.4.3

## Lassú hálózat hibaelhárítása

A 802.11 kétnormás routerek és AP-k sávszélességének optimalizálása és növelése:

* **Upgrade your wireless clients** - Older 802.11b, 802.11g, and even 802.11n devices can slow the entire WLAN. A legjobb teljesítmény eléréséhez az összes vezeték nélküli berendezésnek ugyanazt a legmagasabb szabványt kell támogatnia. Bár 2019-ben megjelent a 802.11ax, de valószínűleg a 802.11ac az a legmagasabb szint, amelyet a vállalatok jelenleg érvényesíthetnek.
* **Split the traffic** - The easiest way to improve wireless performance is to split the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band. 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).

The figure depicts a home network splitting the traffic between 2.4GHz and 5GHz. The WLC is connected to a television, cell phone and tablet using 5GHz. It is also connected to two laptops using 2.4 GHz.

Home-Net5 5 GHzHome-Net2.4 2.4 GHz

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 sávszélesség viszont még mindig megosztva használható 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.

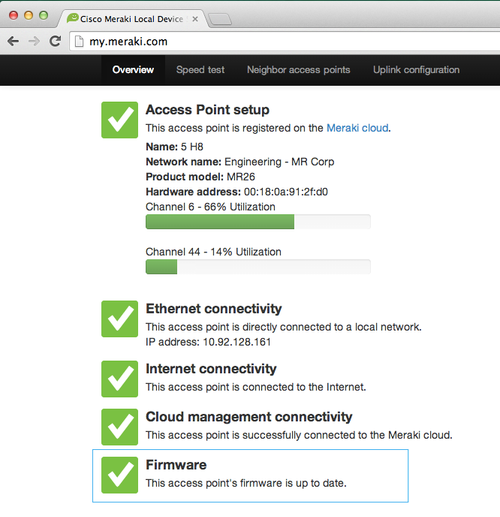
Alapértelmezés szerint a kétnormás routerek ugyanazt a hálózati nevet használják a 2,4 GHz-es és az 5 GHz-es sávban is. A forgalom szétválasztásának legegyszerűbb módja az egyik hálózat átnevezése. Különböző nevek segítségével könnyebb a megfelelő hálózathoz való csatlakozás.

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

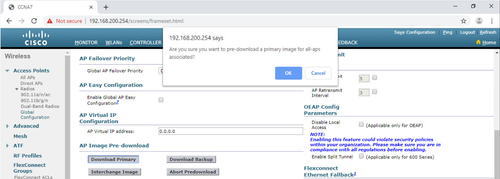
13.4.4

## Firmware frissítés

A legtöbb routeren és AP-n frissíthető a működtető szoftver (firmware). A firmware kiadások javításokat tartalmaznak, egyrészt az ügyfelek által jelzett hibákhoz, másrészt a biztonsági sebezhetőségekre. Rendszeresen ellenőrizzük az eszközökhöz kiadott frissítéseket! Az ábrán egy rendszergazda ellenőrzi, hogy a firmware naprakész-e egy Cisco Meraki AP-n.



Egy WLC valószínűleg képes frissíteni a firmware-t minden olyan AP-n, amelyet felügyel. A következő ábrán a rendszergazda letölti a firmware-t, amelyet az AP-k frissítésére használ.



On a Cisco 3504 Wireless Controller, Click the **WIRELESS** tab > **Access Points** from the left menu > **Global Configuration** submenu. Ezután görgessünk az oldal aljára az AP Image Pre-download részhez.

A frissítés idejére a felhasználók kapcsolata megszakad a WLAN-nal és az internettel. A vezeték nélküli router néhányszor újraindulhat, amíg a normális hálózati működés végleg helyreáll.

13.4.5

## Packet Tracer — WLAN kapcsolódási problémák elhárítása

Most, hogy megtanultuk a vezeték nélküli hálózatok konfigurálását az otthoni és a vállalati hálózatokban, meg kell ismerjük a vezeték nélküli környezetben történő hibaelhárítást is. A cél az, hogy IP- és URL-cím alapján engedélyezzük a hálózatban lévő állomások és a webkiszolgáló közötti kapcsolatot. Az otthoni és nagyvállalati hálózatok közötti kapcsolat létrehozása nem szükséges.

[WLAN-problémák hibaelhárítása](https://contenthub.netacad.com/courses/srwe-dl/_common/13.4.5-packet-tracer---troubleshoot-wlan-issues_hu-HU.pka)

[13.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Vállalati WLAN-beállítások a WLC-n](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[13.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. WLAN Configuration
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

13.5.1

## Packet Tracer - WLAN-konfiguráció

Ebben a feladatban egy vezeték nélküli otthoni routert és egy WLC-alapú hálózatot is konfigurálunk. Mind a WPA2-PSK, mind a WPA2-Enterprise biztonságot megvalósítjuk.

[WLAN beállítása](https://contenthub.netacad.com/courses/srwe-dl/_common/13.5.1-packet-tracer---wlan-configuration_hu-HU.pka)

13.5.2

### Packet Tracer – Vezeték nélküli technológia felfedezése

Az XYZ Corporation kibővíti hálózati képességeit, hogy jobb kapcsolatot tegyen lehetővé helyi irodáikban, valamint a távolról dolgozni vágyók számára. Ebben a Packet Tracer Physical Mode (PTPM) tevékenységben arra kérték Önt, hogy segítse ezt a tervet a jelenlegi hálózati képességek áttekintésével és szükség szerint vezeték nélküli funkciók hozzáadásával.

**Note**: Please be patient. It may take several minutes for this PTPM activity to load.

[Wireless Technology Exploration - Physical Mode](https://contenthub.netacad.com/courses/srwe-dl/_common/13.5.2-packet-tracer---wireless-technology-exploration---physical-mode_hu-HU.pka)

13.5.3

## Miről tanultunk ebben a fejezetben?

A távmunkások, a kis irodák és az otthoni hálózatok gyakran használnak vezeték nélküli routert, amely tartalmaz egy switch-et a vezetékes ügyfelek számára, egy internetkapcsolathoz való portot (néha „WAN” felirattal), és vezeték nélküli összetevőket a vezeték nélküli ügyfelek kapcsolódásához. A legtöbb ilyen eszközön a hálózati csatlakozás és bizonyos szolgáltatások már előre be vannak állítva. Például a vezeték nélküli router DHCP-t használ, hogy automatikusan címzési információkat biztosítson a csatlakoztatott eszközöknek. Első feladatunk a router felhasználónevének és jelszavának módosítása. Használjuk a router konfigurációs felületét az alapvető hálózati és vezeték nélküli beállítások véglegesítéséhez. Ha szeretnénk kiterjeszteni a hatósugarat (beltéren körülbelül 45 méterrel és kültéren 90 méterrel), akkor további vezeték nélküli hozzáférési pontokkal bővíthetjük a hálózatot. A router egy hálózati címfordításnak (Network Address Translation, NAT) nevezett folyamatot használ, hogy a privát IPv4-címeket interneten is továbbítható IPv4-címekké alakítsa. A QoS beállításával biztosíthatjuk, hogy bizonyos forgalomtípusok, mint például a hang és a videó, magasabb prioritással rendelkezzenek a nem időérzékeny forgalomhoz, például az elektronikus levelezéshez és a webböngészéshez képest.

Az LAP-k az LWAPP (Lightweight Access Point Protocol) segítségével kommunikálnak a WLAN-vezérlővel. Egy vezeték nélküli LAN-vezérlő (WLC) konfigurálása hasonlít egy vezeték nélküli router konfigurálásához, kivéve, hogy a WLC vezérli az AP-eket, és több szolgáltatást és felügyeleti lehetőséget biztosít. A WLC konfigurációs felületén megtekinthetjük a hozzáférési pontok információit és teljesítményét, hozzáférhetünk a speciális beállításokhoz és konfigurálhatjuk a WLAN-t.

Az SNMP a hálózat megfigyelésére szolgál. A WLC továbbítja az összes SNMP-naplóüzenetet (trap) az SNMP-kiszolgálónak. A WLAN a felhasználói hitelesítéshez RADIUS-kiszolgálót használ a hitelesítési, engedélyezési és naplózási szolgáltatásokhoz (AAA). Az egyéni felhasználói hozzáférés nyomon követhető és auditálható. A WLC konfigurációs felületén beállíthatjuk az SNMP- és RADIUS-kiszolgálót, a VLAN-interfészeket, a DHCP-hatókört és a WPA2 Enterprise WLAN-t.

A hibaelhárítási folyamat hat lépésből áll. Egy WLAN-hiba elhárítása során a kizárásos módszer használata javasolt. Gyakori problémák: nincs vagy rossz teljesítményű a vezeték nélküli kapcsolat, amikor a számítógép működik. A 802.11 kétnormás routerek és hozzáférési pontok sávszélességének optimalizálása és növelésének módja: vezeték nélküli kliensek frissítése vagy a forgalom megosztása. A legtöbb routeren és AP-n frissíthető a működtető szoftver (firmware). A firmware kiadások javításokat tartalmaznak, egyrészt az ügyfelek által jelzett hibákhoz, másrészt a biztonsági sebezhetőségekre. Rendszeresen ellenőrizzük az eszközökhöz kiadott frissítéseket!

13.5.4

## Ellenőrző kvíz - WLAN-konfiguráció

Az űrlap teteje

1. Egy felhasználó vezeték nélküli hozzáférési pontot konfigurál, és meg akarja akadályozni, hogy a szomszédok felfedezzék a hálózatot. Milyen lépéseket kell tennie?

Az űrlap alja

Egy kis irodai vezeték nélküli hálózatban általában milyen típusú IP-címzést használnak?

A felhasználó nemrég vásárolt egy átlagos otthoni routert, és szeretné biztonságossá tenni. Mit kell tennie a vezeték nélküli router biztonsága érdekében?

Melyik protokollt használhatja egy vállalat olyan eszközök megfigyelésére, mint a vezeték nélküli LAN vezérlő (WLC)?

Amikor egy Cisco 3500 sorozatú vezeték nélküli LAN vezérlőt (WLC) WPA2 Enterprise WLAN-hoz konfigurálunk, mit kell létrehozni a WLC-n az új WLAN létrehozása előtt?

Mi az a DHCP-hatókör, amely a WLC-vezérlőn konfigurált WLAN-ra vonatkozik?

Miért állít be a technikus egy WLAN-hoz jelszót egy vezeték nélküli routeren?

Az ügyfél otthoni vezeték nélküli hozzáférési pontot telepít a konyha melletti szekrénybe. Az ügyfél megemlíti, hogy a vezeték nélküli kommunikációs teljesítmény leromlik, ha a vezeték nélküli telefon vagy a mikrohullámú sütő használatban van. Mi lehet az oka ennek?

Milyen funkciókra van szükség a routereken ahhoz, hogy a távmunkások VoIP és videokonferencia-képességekkel rendelkezzenek?

Egy vezeték nélküli router a 192.168.0.1 IP-címen érhető el. Ez vajon mit jelent?

Egy laptop nem tud csatlakozni egy vezeték nélküli hozzáférési ponthoz. Melyik két hibaelhárítási műveletet kell alkalmazni először? (Két jó válasz van.)

Egy kis iroda hálózatának létrehozásakor a rendszergazda úgy határoz, hogy dinamikusan rendel hozzá privát IP-címeket a munkaállomásokhoz és a mobileszközökhöz. Melyik funkciót kell engedélyezni a vállalati routeren, hogy az irodai eszközök hozzáférjenek az internethez?

Mi a különbség az otthoni környezetben működő autonóm hozzáférési pontok és a vállalati környezetben működő vezérlő-alapú hozzáférési pontok között?

A hálózati rendszergazda általában melyik WLC lapot használja a leggyakrabban használt WLAN-ok összefoglaló nézetének megtekintéséhez, beleértve az adott WLAN-t használó ügyfelek számát is?

Egy IEEE 802.11n hálózat felhasználói alacsony sebességre panaszkodnak. A hálózati rendszergazda ellenőrzi a hozzáférési pontot és megállapítja, hogy az rendben működik. Mit tehet a hálózati teljesítmény növelése érdekében?

[13.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Troubleshoot WLAN Issues](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Routing Concepts
2. Bevezetés

# Bevezetés

14.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Forgalomirányítás elmélete című fejezetben.

Nem számít, mennyire hatékonyan állítjuk be a hálózatot, a dolgok néha elromlanak, hibásan, vagy egyáltalán nem működnek. Ez egy alapvető igazság a hálózatokról. Annak ellenére, hogy már elég sokat tudunk a forgalomirányításról, még meg kell ismernünk, hogy hogyan működnek valójában a routerek. Ez a tudás kritikus fontosságú, ha azt szeretnénk, hogy képesek legyünk a hálózat hibaelhárítására. Ez a fejezet részletesen bemutatja a router működését. Vágjunk bele!

14.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Module Title**: Routing Concepts

**Module Objective**: Explain how routers use information in packets to make forwarding decisions.

| Table caption | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Útvonalak meghatározása** | Explain how routers determine the best path. |
| **Csomagtovábbítás** | Explain how routers forward packets to the destination. |
| **A router alapbeállításainak áttekintése** | A router alapbeállításainak konfigurálása |
| **IP Routing Table** | Describe the structure of a routing table. |
| **Static and Dynamic Routing** | Compare static and dynamic routing concepts. |

[13.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Útvonalak meghatározása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Routing Concepts
2. Útvonalak meghatározása

# Útvonalak meghatározása

14.1.1

## A router két funkciója

Mielőtt egy router bárhova is továbbítana egy csomagot, meg kell határoznia a csomag számára a legjobb utat. Ez a témakör azt mutatja be, hogyan határozzák meg a routerek ezt az útvonalat.

Az Ethernet switch-ek végberendezések és más közvetítő eszközök (pl. más Ethernet kapcsolók) ugyanazon hálózathoz történő csatlakoztatására szolgálnak. A router több hálózatot kapcsol össze, tehát több, különböző IP-hálózatokhoz tartozó interfésze van.

Miután egy router valamelyik interfészén fogad egy IP-csomagot, meg kell határoznia, hogy melyik interfészén kell azt a célja felé továbbítania. Ezt hívjuk forgalomirányításnak. Lehet, hogy az az interfész, amelyen a csomagot továbbítja már a csomag végső célja, de lehet egy olyan hálózat is, amely egy következő routerhez vezet, és amely a csomagot megint csak továbbítja a cél felé. Minden hálózathoz, melyekhez a router csatlakozik általában külön interfész szükséges, de ez nem minden esetben van így.

A router elsődleges funkciói a csomagtovábbítás legjobb útvonalának meghatározása az irányítótáblában szereplő információk alapján, valamint a csomagok célállomás felé történő továbbítása.

14.1.2

## Példák a router funkcióira

A router az irányítótáblája segítségével határozza meg a csomag továbbításához a legjobb útvonalat. Egy csomag forrás PC-től a cél PC-ig történő nyomkövetésének megtekintéséhez kattintsunk az ábrán látható Lejátszás gombra! Figyeljük meg, hogy R1 és R2 hogyan használják a megfelelő IP-irányítótábláikat a legjobb elérési útvonal meghatározásához, majd a csomag továbbításához.

The animation depicts two LAN networks with hosts connected by two routers R1 and R2. A packet is animated traversing the connection from one LAN to the other LAN. The router screens appear FOR R! and R2 showing the matching IP v.4 addresses in the router passing from one network to another.

192.168.3.0/24

LAN

LAN

192.168.1.0/24

R2 follows the same process.

Routers use the routing table like a map to discover the best path for a given network.

14.1.3

## A legjobb útvonal egyenlő a leghosszabb egyezéssel

Mit értünk azalatt, hogy a routernek a legjobb egyezést kell megtalálnia az irányítótáblában? Az a legjobb útvonal az irányítótáblában, amelyik a leghosszabban ráillik a keresett címre. A leghosszabb egyezés keresése egy olyan folyamat, amelyet a router használ a csomag cél IP-címe és az irányítótábla útvonal bejegyzése közötti egyezés megtalálására.

Az irányítótábla egy előtagból (hálózati cím) és az előtag hosszúságából álló útvonalbejegyzéseket tartalmaz. Ahhoz, hogy egy csomag cél IP-címe és az irányítótábla egy útvonala között egyezés legyen, bal oldalról nézve bizonyos számú bitnek meg kell egyeznie bennük. Az egyező bitek minimális számának meghatározásához az útvonalhoz megadott előtag hosszot használják. Ne feledjük, hogy az IP-csomag csak a cél IP-címét tartalmazza, az előtag hosszát nem.

Leghosszabb egyezésnek az irányítótábla azon útvonalát tekintjük, amelynek bal oldalról nézve a legtöbb bitje egyezik meg a csomag cél IP-címével. Legjobb útvonalnak mindig azt az útvonalat tekintjük, amely balról kezdve a legtöbb egyező bittel vagy leghosszabb egyezéssel rendelkezik.

**Note**: The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.

14.1.4

## Példa IPv4-cím leghosszabb egyezésre

A táblázatban egy IPv4-csomag a 172.16.0.10 cél IPv4-címmel rendelkezik. A router IPv4 irányítótáblájában három lehetséges útvonal található a megadott célhoz: 172.16.0.0/12, 172.16.0.0/18 és 172.16.0.0/26. Mivel a három útvonal közül a 172.16.0.0/26 mutatja a leghosszabb egyezést, így a forgalomirányító ezt választja a csomag továbbításához. Ne feledjük, hogy egyezésről csak akkor beszélhetünk, ha legalább az alhálózati maszkban jelzett bitszámig megegyezik binárisan a célcím és az adott útvonal.

| Cél IPv4-cím A cím bináris alakja 172.16.0.10 10101100.00010000.00000000.000000.001010 | | | |
| --- | --- | --- | --- |
| **Cél IPv4-cím** | | | **A cím bináris alakja** |
| 172.16.0.10 | | | **10101100.00010000.00000000.00**001010 |
| Útvonal-bejegyzés előtagja/Előtag hossz A cím bináris alakja 1 172.16.0.0/12 10101100.00010000.0000000000.000000.00000000.00000000.0000000000.0000000000.0000000000.0000000000.00000000000000.0000001010 | | | | |
| **Útvonal-bejegyzés** | **Előtag/Előtag hossz** | **A cím bináris alakja** | | |
| 1 | 172.16.0.0**/12** | **10101100.0001**0000.00000000.00001010 | | |
| 2 | 172.16.0.0**/18** | **10101100.00010000.00**000000.00001010 | | |
| 3 | 172.16.0.0**/26** | **10101100.00010000.00000000.00**001010 | | |

14.1.5

## Példa IPv6-cím leghosszabb egyezésre

A táblázatban egy IPv6-csomag a 2001:db8:c000።99 cél IPv6-címmel rendelkezik. Ez a példa három útvonalbejegyzést mutat, de közülük csak kettő érvényes egyezés, és egyikük a leghosszabb egyezés. Az első két útvonalbejegyzés rendelkezik olyan előtag-hosszal, mint az előtag hossz által jelzett szükséges bitszám. Az első /40 előtagú útvonalbejegyzés megegyezik az IPv6-cím bal szélső 40 bitjével. A második útvonalbejegyzés előtag-hossza /48, és mind a 48 bit megegyezik a cél IPv6-címével, és ez a leghosszabb egyezés. A harmadik útvonalbejegyzés nem egyező, mert a /64 előtaghoz 64 egyező bit szükséges. Ahhoz, hogy a 2001:db8:c000:5555።/64 előtag egyezzen, az első 64 bitnek a csomag cél IPv6-címének kellene lennie. Csak az első 48 bit egyezik meg, így ez az útvonalbejegyzés nem tekinthető egyezésnek.

A **2001:db8:c000**። 99 célcímmel rendelkező IPv6-csomag esetén a következő három útvonalbejegyzést vegyük figyelembe:

| Útvonal-bejegyzés előtagja/Előtag hossz Egyezés 12001:db8:c000። /40 40 egyező bit 22001:db8:c000።/48 egyező bit (leghosszabb egyezés) 32001:db8:c 000:5555።/64 Nincs 64 egyező bit | | |
| --- | --- | --- |
| **Útvonal-bejegyzés** | **Előtag/Előtag hossz** | **Egyezés** |
| 1 | **2001:db8:c0**00።**/40** | 40 egyező bit |
| 2 | **2001:db8:c000**።**/48** | 48 egyező bit (leghosszabb egyezés) |
| 3 | **2001:db8:c000:5555**። /64 | Nincs 64 egyező bit |

14.1.6

## Az irányítótábla létrehozása

Az irányítótábla előtagokat és az előtagok hosszát tartalmazza. De hogyan térképezi fel a router a hálózatokat? Hogyan tölti fel az ábrán lévő R1 az irányítótábláját?

The figure depicts three types of networks Directed Connected Network, Remote Network, and Default Route. Router1 (R1) is the directly connected network with two switches S1 and S2 connected to two PCs PC1 and PC2. Each switch is connected to router R1. R1 and Router2(R2) are connected directly via point to point connection. R2 is connected two two switches S# and S4 with each switch having a PC PC3 and P4 connected to them. R2 forms the remoted network. R2 has an additional remote connection to the ISP by a point to point connection which is the Internet connection. The number scheme for each device is dual stack IPv4 and IPv6 addressees.

### Hálózatok R1 szemszögéből

PC1 PC2 PC3 PC4 S1 S2 S4 R1 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2

S0/1/1

internetDirectly Connected NetworkDirectly Connected NetworkTávoli hálózatokRemote NetworkRemote NetworkRemote NetworkDirectly Connected Network

A topológiában található hálózatok R1 szemszögéből vannak kiemelve és címkézve. Minden sárga színnel kiemelt IPv4- és IPv6-hálózat közvetlenül kapcsolódik. Az összes kék színnel kiemelt IPv4- és IPv6-hálózat távoli hálózat.

A router különböző útvonal tanulási módszereiről szóló további információkért kattintsunk az alábbi gombokra!

**Directly Connected Networks**

Directly connected networks are networks that are configured on the active interfaces of a router. Egy közvetlenül csatlakozó hálózat akkor adódik hozzá az irányítótáblához, ha egy interfész IP-címmel és alhálózati maszkkal (előtag hossz) van konfigurálva és aktív (felkapcsolt állapotú).

14.1.7

## Tudáspróba - Útvonalak meghatározása

Az űrlap teteje

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

1. What table does a router use to determine how to forward an IP packet?

Az űrlap alja

What action will a router take on a packet with a destination IP address that is on a remote network?

Which of the following routes may be found in a routing table? (Choose all that apply.)

What is used to determine the minimum number of far-left bits that must match between the prefix in the route entry and the destination IP address.

[14.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Csomagtovábbítás](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Routing Concepts
2. Csomagtovábbítás

# Csomagtovábbítás

14.2.1

## A csomagtovábbítás döntési folyamata

Miután a router a leghosszabb egyezés alapján meghatározta a csomaghoz a legjobb útvonalat, meg kell határoznia, hogyan ágyazza be a csomagot és továbbítsa azt a megfelelő kimenő interfészen.

Az ábra azt mutatja be, hogy a router milyen módon határozza meg először a legjobb útvonalat, majd továbbítja a csomagot.

The figure depicts how a router first determines the best path, and then forwards the packet. There are 5 steps depicted with these steps:

1. Az adatkapcsolati keretbe ágyazott IP-csomag érkezik a bejövő interfészre.

2. A router megvizsgálja a csomag fejrészében található cél IP-címet és keresést indít az IP-irányítótáblában.

3. Megtalálja benne a leghosszabb egyezést mutató előtagot.

4. Beágyazza a csomagot egy adatkapcsolati keretbe és továbbítja azt a kimenő interfészen. A cél egy olyan eszköz lehet, amely a hálózathoz vagy egy követező ugrás routerhez csatlakozik.

5. Azonban, ha nincs egyező bejegyzés az irányítótáblában a csomag eldobásra kerül.

1 1 2 3 3 4

5

Data Link HeaderDestination IP AddressRest of IP PacketData Link TrailerFind the longest match between destination IP address and the entries in the routing tableNo matching route entry in the routing table, including no default routeRoute entry shows destination IP address is on a directly connected networkData Link HeaderDestination IP AddressRest of IP PacketData Link TrailerForward packet directly to destination deviceRoute entry shows destination IP address is on a remote networkData Link HeaderDestination IP AddressRest of IP PacketData Link TrailerForward packet to next-hop routerIP Routing TableRoute entries:  
Prefix/Prefix Length  
Prefix/Prefix Length  
Prefix/Prefix Length  
Prefix/Prefix Length  
...

The following steps describe the packet forwarding process shown in the figure:

1. Az adatkapcsolati keretbe ágyazott IP-csomag érkezik a bejövő interfészre.
2. A router megvizsgálja a csomag fejrészében található cél IP-címet és keresést indít az IP-irányítótáblában.
3. Megtalálja benne a leghosszabb egyezést mutató előtagot.
4. Beágyazza a csomagot egy adatkapcsolati keretbe és továbbítja azt a kimenő interfészen. A cél egy olyan eszköz lehet, amely a hálózathoz vagy egy követező ugrás routerhez csatlakozik.
5. Azonban, ha nincs egyező bejegyzés az irányítótáblában a csomag eldobásra kerül.

A legjobb útvonal meghatározása után a router által a csomaggal végrehajtható három dologról szóló leírásért kattintsunk az alábbi gombokra!

**Forwards the Packet to a Device on a Directly Connected Network**

If the route entry indicates that the egress interface is a directly connected network, this means that the destination IP address of the packet belongs to a device on the directly connected network. Ezért a csomag közvetlenül a céleszköznek továbbítható. A céleszköz általában egy Ethernet LAN végberendezése, ami azt jelenti, hogy a csomagot Ethernet keretbe kell ágyazni.

A csomag Ethernet keretbe történő beágyazásához a routernek meg kell határoznia a csomag cél IP-címéhez társított MAC-címet. The process varies based on whether the packet is an IPv4 or IPv6 packet:

* **IPv4 packet** - The router checks its ARP table for the destination IPv4 address and an associated Ethernet MAC address. Ha nincs találat, a router egy ARP-kérést küld ki. A céleszköz ARP-választ küld, amelybe a saját MAC-címét teszi bele. A router most már továbbíthatja az IPv4-csomagot egy Ethernet keretbe ágyazva a megfelelő cél MAC-címmel.
* **IPv6 packet** - The router checks its neighbor cache for the destination IPv6 address and an associated Ethernet MAC address. Ha nincs találat, a router egy ICMPv6 szomszéd keresés (Neighbor Solicitation, NS) üzenetet küld ki. A céleszköz egy ICMPv6 szomszéd hirdetés (Neighbor Advertisement, NA) üzenetet küld a saját MAC-címével. A router most már továbbíthatja az IPv6-csomagot egy Ethernet keretbe ágyazva a megfelelő cél MAC-címmel.

14.2.2

## Végpontok közötti csomagtovábbítás

A csomagtovábbítás elsődleges fontosságú művelete a csomag beágyazása a megfelelő adatkapcsolati keretbe a kimenő interfész számára. Például egy soros összeköttetés adatkapcsolati keretformátuma lehet pont-pont (Point-to-Point, PPP) protokoll, High-Level Data Link Control (HDLC) protokoll vagy más 2. rétegbeli protokoll is.

Kattintsunk az egyes gombokra és játsszuk le az animációt, amelyben PC1 csomagot küld PC2-nek. Figyeljük meg, hogyan változik az adatkapcsolati keret tartalma és formátuma minden ugrásnál.

**PC1 Sends Packet to PC2**

In the first animation, PC1 sends a packet to PC2. Mivel a PC2 egy másik hálózaton van, a PC1 továbbítja a csomagot az alapértelmezett átjárónak. A PC1 megkeresi az ARP-gyorsítótárában az alapértelmezett átjáró MAC-címét, és hozzáadja a jelzett keretinformációkat.

**Note**: If an ARP entry does not exist in the ARP table for the default gateway of 192.168.1.1, PC1 sends an ARP request. Router R1 would then return an ARP reply with its MAC address.

The network diagram is PC1 connected to PC2 thru routers R1, R2, and R3. PC1 is 192.168.1.10 on network 192.168.1.0/24 connected to R1. R1 is connected to R2 on network 192.168.2.0/14 with Gigabit connections R1 G0/0/1 192.168.2.1 connected to R2 G/0/0 192.168.2.2. R2 connects to R3 on network 192.168.3.0/24. R2 S0/1/0 102.168.3.1 connects to R3 S0/1/0 192.168.3.2 on serial interfaces.. R3 connects to PC2 on network 192.168.4.0/24. The interface connection for R3 G0/0/0 192.168.4.1 connects directly to PC2 192.168.4.10. There are four different animations. The first animation depicts PC1s arp cache and decision to send the packet to R1 its gateway

What path does it need to take?

14.2.3

## Csomagtovábbító módszerek

Ahogy korábban említettük, a csomagtovábbítás elsődleges fontosságú művelete a csomag beágyazása a megfelelő adatkapcsolati keretbe a kimenő interfész számára. Minél hatékonyabban tudja végrehajtani ezt a feladatot a router, annál gyorsabb képes a csomagok továbbítására. A routerek az alábbi háromféle csomagtovábbító módszert támogatják:

* Folyamatkapcsolás (Process switching)
* Gyorskapcsolás (Fast switching)
* Cisco Expressz Továbbítás (Cisco Express Forwarding, CEF)

Tegyük fel, hogy van egy adatfolyam, amely öt csomagból áll. Mind ugyanarra a célállomásra mennek. Kattintsunk az egyes gombokra a csomagtovábbítási módszerekkel kapcsolatos további információkért!

**Process Switching**

An older packet forwarding mechanism still available for Cisco routers. Amikor csomag érkezik egy interfészre, a vezérlési szintre (control plane) kerül, ahol a processzor a célcímet összeveti a forgalomirányító táblával, majd meghatározza a kimenő interfészt és továbbítja a csomagot. Fontos megérteni, hogy a forgalomirányító ezt minden egyes csomagra végrehajtja, még akkor is, ha egy sor csomagnak ugyanaz a célja. Ez a módszer nagyon lassú, modern hálózatokban alig használják. Vessük össze a gyorskapcsolással.

The figure separates the control plane which is the CPU from the Data Plane. There are 5 packets labeled 1 thru 5 entering the Ingress Interface thru the data plane to the control plane. The control plane then forwards the packets thru the Data plane out the Egress Interface.

**Control PlaneIngress  
InterfaceData PlaneEgress  
Interface**1st Packet2nd Packet3rd Packet4th Packet5th PacketCPU

A három különöző módszer összehasonlítását a következő analógiával szoktuk illusztrálni:

* A folyamatkapcsolás minden problémát végigszámol matematikailag, még akkor is, ha ugyanaz a probléma már meg lett oldva.
* A gyorskapcsolás egyszer számolja végig a problémát, de emlékszik a válaszra és a következő ugyanilyen problémákhoz már ezt használja.
* A CEF minden lehetséges problémát előre kiszámol és az eredményeket egy táblázatban tárolja.

14.2.4

## Tudáspróba - Csomagtovábbítás

Az űrlap teteje

Check your understanding of forwarding packets from source to destination by choosing the BEST answer to the following questions.

1. If a router needs to send an ARP Request for the destination IPv4 address of the packet, this means the packet will be forwarded:

Az űrlap alja

If a router needs to send an ARP Request for the IPv4 address in one of its route entries, this means the packet will be forwarded:

Which packet forwarding method is used by default on Cisco routers?

[14.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Útvonalak meghatározása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A router alapbeállításainak áttekintése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Switching, Routing, and Wireless Essentials

v7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Routing Concepts
2. A router alapbeállításainak áttekintése

# A router alapbeállításainak áttekintése

14.3.1

## Topológia

A router irányítótáblát hoz létre, amely segít meghatározni, hogy hova továbbítsa a csomagokat. De mielőtt belemerülnénk az IP-irányítótábla részleteibe, ez a témakör áttekinti az alapvető router konfigurációs és ellenőrzési feladatokat. Egy Packet Tracer feladatot is elvégezhetünk, hogy felfrissítsük a tudásunkat.

Az ábrán látható topológiát konfigurációs és ellenőrzési példákra fogjuk használni. Ez a következő témakörben is felhasználható lesz az IP-irányítótábla vizsgálatakor.

The figure depicts a diagram of 3 routers R1,R2,and R3 connected to 4 switches S1,S2,S3 and S4. R1 connects to switches S1 and S2 using two gigabit connections G/0/0 and G0/0/1. PC1 is connected to switch 1 (S1)on network 10.0.1.0/24 and 2001:db8:acad:1::/64 with a dual stack ip address of .10 and ::10. PC2 is connected to switch 2 (S2) on network 10.0.2.0/24 and 2001:db8:acad:2::/64 with a dual stack ip address of .10 and ::10. R1 has a point to point network to R2 and the ISP networks. The serial connection to R2 is S0/1/01 and S0/1/0. The ISP connection is S0/1/1. The R1 to R2 network is network 10.0.3.0/22 and 2001:db8:acad:3::/64. The R2 network is 209.165.200.224/30 and 2001:db8:feed:224::/64 to the ISP. R2 has two gigabit connections to switches 3 (S3) and switch (S4) G0/0/0 and G/0/0/1. S3 is network 10.0.4.0/24 and 2001:db8:acad:4::/64 connected to the R2 interface G0/0/0. S4 is network 10.0.5.0/24 and 2001:db8:acad:5::/64 connected to R2 interface G0/0/1. PC3 connects to S3 with an address of .10 and ::10. PC4 connects to S4 with an address of .10 and ::10. R1 and R2 gateway addresses end with .1 and ::1. The serial interface between R1 and R2 have addresses of R1 .1 ans ::1 and R2 .2 and ::2. The R2 to ISP connection is .225 and .1 to ISP .226 and ::2.

PC1 PC2 PC3 PC4 S1 S2 S4 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2 S0/1/1

R1

internet

14.3.2

## Konfigurációs parancsok

A következő példák R1 teljes konfigurációját mutatják be.

Router> **enable**

Router# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# **hostname R1**

R1(config)# **enable secret class**

R1(config)# **line console 0**

R1(config-line)# **logging synchronous**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **exit**

R1(config)# **line vty 0 4**

R1(config-line)# **password cisco**

R1(config-line)# **login**

R1(config-line)# **transport input ssh telnet**

R1(config-line)# **exit**

R1(config)# **service password-encryption**

R1(config)# **banner motd #**

Enter TEXT message. End with a new line and the #

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**WARNING: Unauthorized access is prohibited!**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**#**

R1(config)# **ipv6 unicast-routing**

R1(config)# **interface gigabitethernet 0/0/0**

R1(config-if)# **description Link to LAN 1**

R1(config-if)# **ip address 10.0.1.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:1::1/64**

R1(config-if)# **ipv6 address fe80::1:a link-local**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface gigabitethernet 0/0/1**

R1(config-if)# **description Link to LAN 2**

R1(config-if)# **ip address 10.0.2.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:2::1/64**

R1(config-if)# **ipv6 address fe80::1:b link-local**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1(config)# **interface serial 0/1/1**

R1(config-if)# **description Link to R2**

R1(config-if)# **ip address 10.0.3.1 255.255.255.0**

R1(config-if)# **ipv6 address 2001:db8:acad:3::1/64**

R1(config-if)# **ipv6 address fe80::1:c link-local**

R1(config-if)# **no shutdown**

R1(config-if)# **exit**

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

14.3.3

## Ellenőrző parancsok

A gyakran használt ellenőrző parancsok a következők:

* **show ip interface brief**
* **show running-config interface** interface-type number
* **show interfaces**
* **show ip interface**
* **show ip route**
* **ping**

A parancs IPv6 verziójához minden esetben cseréljük le az **ip**-t **ipv6**-ra. Az ábrán ismét megmutatjuk a topológiát az egyszerűség kedvéért.

The figure depicts a diagram of 3 routers R1,R2,and R3 connected to 4 switches S1,S2,S3 and S4. R1 connects to switches S1 and S2 using two gigabit connections G/0/0 and G0/0/1. PC1 is connected to switch 1 (S1)on network 10.0.1.0/24 and 2001:db8:acad:1::/64 with a dual stack ip address of .10 and ::10. PC2 is connected to switch 2 (S2) on network 10.0.2.0/24 and 2001:db8:acad:2::/64 with a dual stack ip address of .10 and ::10. R1 has a point to point network to R2 and the ISP networks. The serial connection to R2 is S0/1/01 and S0/1/0. The ISP connection is S0/1/1. The R1 to R2 network is network 10.0.3.0/22 and 2001:db8:acad:3::/64. The R2 network is 209.165.200.224/30 and 2001:db8:feed:224::/64 to the ISP. R2 has two gigabit connections to switches 3 (S3) and switch (S4) G0/0/0 and G/0/0/1. S3 is network 10.0.4.0/24 and 2001:db8:acad:4::/64 connected to the R2 interface G0/0/0. S4 is network 10.0.5.0/24 and 2001:db8:acad:5::/64 connected to R2 interface G0/0/1. PC3 connects to S3 with an address of .10 and ::10. PC4 connects to S4 with an address of .10 and ::10. R1 and R2 gateway addresses end with .1 and ::1. The serial interface between R1 and R2 have addresses of R1 .1 ans ::1 and R2 .2 and ::2. The R2 to ISP connection is .225 and .1 to ISP .226 and ::2.

PC1 PC2 PC3 PC4 S1 S2 S4 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2 S0/1/1

R1

internet

R1 parancskimenetének megtekintéséhez kattintsunk az egyes gombokra!

R1# **show ip interface brief**

Interface IP-Address OK? Módszer Állapot Protokoll GigabitEthernet0/0/0 10.0.1.1 IGEN kézi fel fel GigabitEthernet0/0/1 10.0.2.1 IGEN manuális fel fel Serial0/1/0 nincs hozzárendelve IGEN unset adminisztratívan le Serial0/1/1 10.0.3.1 IGEN kézi fel GigabitEthernet0 nincs hozzárendelve IGEN kikapcsolva R1#

14.3.4

## Parancsok kimenetének szűrése

A parancssori felület (CLI) egy másik nagyon hasznos funkciója, amely nagyban megkönnyíti a felhasználó munkáját a **show** parancsok kimenetének szűrése. A szűrőparancsok segítségével a kimenet meghatározott szakaszai jeleníthetők meg. Szűrési parancs létrehozásához gépeljük be a "cső" vagy "pipe" (**|**) karaktert a **show** parancs után, majd adjunk meg egy szűrési paramétert és egy kifejezést.

A függőleges vonal után a következő paramétereket használhatjuk szűrésre:

* **section** - A szűrő kifejezéssel kezdődő egész szakaszt mutatja meg.
* **include** - Minden olyan sort megkapunk, amely a szűrő kifejezésre illik.
* **exclude** - Minden olyan sort megkapunk, amely nem illik a szűrő kifejezésre.
* **begin** - A kimenetet egy bizonyos helytől a végéig listázza ki a szűrő kifejezésre illő sortól kezdődően.

**Note**: Kimeneti szűrőt bármelyik **show** parancshoz használhatunk.

Az ábra ismét a topológiát mutatja a kényelmünk érdekében

The figure depicts a diagram of 3 routers R1,R2,and R3 connected to 4 switches S1,S2,S3 and S4. R1 connects to switches S1 and S2 using two gigabit connections G/0/0 and G0/0/1. PC1 is connected to switch 1 (S1)on network 10.0.1.0/24 and 2001:db8:acad:1::/64 with a dual stack ip address of .10 and ::10. PC2 is connected to switch 2 (S2) on network 10.0.2.0/24 and 2001:db8:acad:2::/64 with a dual stack ip address of .10 and ::10. R1 has a point to point network to R2 and the ISP networks. The serial connection to R2 is S0/1/01 and S0/1/0. The ISP connection is S0/1/1. The R1 to R2 network is network 10.0.3.0/22 and 2001:db8:acad:3::/64. The R2 network is 209.165.200.224/30 and 2001:db8:feed:224::/64 to the ISP. R2 has two gigabit connections to switches 3 (S3) and switch (S4) G0/0/0 and G/0/0/1. S3 is network 10.0.4.0/24 and 2001:db8:acad:4::/64 connected to the R2 interface G0/0/0. S4 is network 10.0.5.0/24 and 2001:db8:acad:5::/64 connected to R2 interface G0/0/1. PC3 connects to S3 with an address of .10 and ::10. PC4 connects to S4 with an address of .10 and ::10. R1 and R2 gateway addresses end with .1 and ::1. The serial interface between R1 and R2 have addresses of R1 .1 ans ::1 and R2 .2 and ::2. The R2 to ISP connection is .225 and .1 to ISP .226 and ::2.

PC1 PC2 PC3 PC4 S1 S2 S4 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2 S0/1/1

R1

internet

A példák a szűrő paraméterek gyakori használatát mutatják be.

R1# **show running-config | section line vty**

line vty 0 4

password 7 121A0C0411044C

login

transport input telnet ssh

R1#

R1# **show ipv6 interface brief | include up**

GigabitEthernet0/0/0 [up/up]

GigabitEthernet0/0/1 [up/up]

Serial0/1/1 [up/up]

R1#

R1# **show ip interface brief | exclude unassigned**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0/0 192.168.10.1 YES manual up up

GigabitEthernet0/0/1 192.168.11.1 YES manual up up

Serial0/1/1 209.165.200.225 YES manual up up

R1#

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.10.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.10.1/32 is directly connected, GigabitEthernet0/0/0

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.11.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.11.1/32 is directly connected, GigabitEthernet0/0/1

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks

C 209.165.200.224/30 is directly connected, Serial0/1/1

L 209.165.200.225/32 is directly connected, Serial0/1/1

R1#

14.3.5

## Packet Tracer - A router alapvető konfigurációjának áttekintése

R1 és R2 routerek 2-2 LAN hálózattal rendelkeznek. R1 már konfigurálva van. Feladatunk a megfelelő címzés beállítása R2-n, majd a LAN-ok közti kapcsolat ellenőrzése.

[A router alapbeállításainak áttekintése](https://contenthub.netacad.com/courses/srwe-dl/_common/14.3.5-packet-tracer---basic-router-configuration-review_hu-HU.pka)

[14.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Csomagtovábbítás](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP Routing Table](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Útválasztási fogalmak
2. IP-útválasztó táblázat

# IP-útválasztó táblázat

14.4.1

## Az útvonal forrásai

Honnan tudja a router, hogy hova küldhet csomagokat? Létrehoz egy irányítótáblát, amely azon a hálózaton alapul, amelyben található.

Az irányítótábla az ismert hálózatokhoz vezető útvonalak listáját (előtagok és előtag-hosszok) tartalmazza. Ezen információ forrása a következőkből származik:

* Közvetlenül kapcsolódó hálózatok
* Statikus útvonalak
* Dinamikus forgalomirányító protokollok

Az ábrán R1 és R2 OSPF dinamikus forgalomirányító protokollt használ az útvonal információk megosztására. Továbbá R2-n egy alapértelmezett statikus útvonal is konfigurálva van az ISP-hez.

Az ábra 3 R1, R2 és R3 routert ábrázol, amelyek 4 S1, S2, S3 és S4 kapcsolóhoz vannak csatlakoztatva. Az R1 két gigabites G/0/0 és G0/0/1 kapcsolaton keresztül csatlakozik az S1 és S2 kapcsolókhoz. A PC1 a 10.0.1.0/24 és 2001:db8:acad:1::/64 hálózat 1. kapcsolójához (S1) csatlakozik, .10 és ::10 kettős verem IP-címmel. A PC2 a 10.0.2.0/24 és 2001:db8:acad:2::/64 hálózat 2. kapcsolójához (S2) csatlakozik .10 és ::10 kettős verem IP-címmel. Az R1-nek van egy pont-pont hálózata az R2-vel és az ISP-hálózatokkal. Az R2 soros csatlakozása S0/1/01 és S0/1/0. Az internetszolgáltató kapcsolata S0/1/1. Az R1–R2 hálózat 10.0.3.0/22 ​​és 2001:db8:acad:3::/64. Az R2 hálózat 209.165.200.224/30 és 2001:db8:feed:224::/64 az internetszolgáltatónak. Az R2 két gigabites csatlakozással rendelkezik a 3. (S3) és a kapcsoló (S4) G0/0/0 és G/0/0/1 kapcsolókhoz. Az S3 a 10.0.4.0/24 hálózat és a 2001:db8:acad:4::/64, amely a G0/0/0 R2 interfészhez csatlakozik. Az S4 a 10.0.5.0/24 hálózat és a 2001:db8:acad:5::/64, amely a G0/0/1 R2 interfészhez csatlakozik. A PC3 .10 és ::10 címmel csatlakozik az S3-hoz. A PC4 .10 és ::10 címmel csatlakozik az S4-hez. Az R1 és R2 átjárócímek .1-re és ::1-re végződnek. Az R1 és R2 közötti soros interfész R1 .1 és ::1 és R2 .2 és ::2 címekkel rendelkezik. Az R2 és az ISP közötti kapcsolat .225 és .1 az ISP .226 és ::2 között. Az R1 router kiemelve van az ábrán

PC1 PC2 PC3 PC4 S1 S2 S4 R1 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2

S0/1/1

Internet

Kattintsunk az egyes gombokra a routerek irányítótáblájának megtekintéséhez miután a közvetlenül csatlakozó hálózatok, a statikus és dinamikus forgalomirányítás konfigurálva lettek. A témakör többi részében bemutatásra kerül, hogyan épülnek fel ezek a táblázatok.

R1# ip útvonal megjelenítése Kódok: L - helyi, C - csatlakoztatott, S - statikus, R - RIP, M - mobil, B - BGP D - EIGRP, EX - EIGRP külső, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA külső típus 1, N2 - OSPF NSSA külső típus 2 E1 - OSPF külső típus 1, E2 - OSPF külső típus 2 i - IS-IS, su - IS-IS összefoglaló, L1 - IS-IS level-1, L2 - IS-IS szint-2 ia - IS-IS inter area, \* - jelölt alapértelmezett, U - felhasználónkénti statikus útvonal o - ODR, P - periodikusan letöltött statikus útvonal, H - NHRP, l - LISP a - alkalmazás útvonala + - replikált útvonal, % - következő ugrás felülírása, p - felülbírálások a PfR átjáróról az utolsó lehetőségről 10.0.3.2 hálózatra 0.0.0.0 O\*E2 0.0.0.0/0 [110/1] keresztül 10.0.3.2, 00:51:34 , Serial0/1/1 10.0.0.0/8 változó alhálózat, 8 alhálózat, 2 maszk C 10.0.1.0/24 közvetlenül kapcsolódik, GigabitEthernet0/0/0 L 10.0.1.1/32 közvetlenül kapcsolódik, GigabitEthernet0/0/0 A C 10.0.2.0/24 közvetlenül csatlakozik, a GigabitEthernet0/0/1 L 10.0.2.1/32 közvetlenül, a GigabitEthernet0/0/1 C 10.0.3.0/24 közvetlenül csatlakozik ed, Serial0/1/1 L 10.0.3.1/32 közvetlenül csatlakoztatva, Serial0/1/1 O 10.0.4.0/24 [110/50] a 10.0.3.2-n keresztül, 00:24:22, Serial0/1/1 O 10.0.5.0/24 [110/50] keresztül 10.0.3.2, 00:24:15, Serial0/1/1 R1#

Figyeljük meg, hogy R1 és R2 irányítótábláiban az egyes útvonalak forrásait kóddal azonosítják. A kód mutatja meg, hogy a router honnan tanulta meg az útvonalat. Példák gyakori kódokra:

* **L** - A router interfészéhez rendelt címet jelenti. Ennek segítségével tudja a router hatékonyan megállapítani, hogy a csomagot nem kell továbbítani, hanem neki kell elfogadnia.
* **C** - Közvetlenül csatlakozó hálózatot jelöl.
* **S** - Egy bizonyos hálózat eléréséhez létrehozott statikus útvonal.
* **O** - Dinamikusan megtanult hálózatot jelöl, amelyet OSPF protokollal kaptunk egy másik forgalomirányítótól.
* **\*** - Az útvonal egy alapértelmezettnek kijelölt útvonal.

14.4.2

## Az irányítótábla alapelvei

A táblázatban leírtak szerint három irányítótábla alapelv létezik. Ezeket a dinamikus forgalomirányító protokollok vagy statikus útvonalak megfelelő konfigurációja kezeli a forrás- és céleszközök közötti összes routeren.

| Útválasztási táblázat elvePéldaMinden útválasztó egyedül hozza meg döntését, a saját útválasztási táblájában található információk alapján. Az R1 csak a saját útválasztási táblája segítségével tudja továbbítani a csomagokat. Az R1 nem tudja, hogy milyen útvonalak vannak a többi útválasztó (pl. R2) útválasztási táblázatában. Amit egy útválasztó tartalmaz az útválasztási táblázatában, az nem jelenti azt, hogy más útválasztók is rendelkeznek ugyanazokkal az információkkal. Csak azért, mert az R1 útválasztónak az útválasztási táblázatában van útvonal egy hálózat az interneten az R2 útválasztón keresztül, ez nem jelenti azt, hogy R2 tud ugyanarról a hálózatról. Az útvonalra vonatkozó útválasztási információk nem adnak vissza útválasztási információkat. Az R1 egy csomagot kap a PC1 cél IP-címével és a PC3 forrás IP-címével . Csak azért, mert az R1 tudja továbbítani a csomagot a G0/0/0 interfészén, nem feltétlenül jelenti azt, hogy tudja, hogyan kell a PC1-ről származó csomagokat visszaküldeni a PC3 távoli hálózatába. | |
| --- | --- |
| **Irányítótábla alapelv** | **Példa** |
| Minden router egyedül hozza meg a döntését a rendelkezésére álló információk alapján, amelyek az irányítótáblájában találhatók. | * R1 csak a saját irányítótáblája segítségével továbbíthatja a csomagokat. * R1 nem tudja milyen útvonalak vannak más routerek (pl. R2) irányítótáblájában. |
| Egy router irányítótáblájában szereplő információk nem feltétlenül egyeznek meg egy másik router irányítótáblájában lévőkkel. | Csak azért, mert R1 útvonallal rendelkezik az irányítótáblájában egy a világhálón található hálózathoz R2-n keresztül, ez nem jelenti azt, hogy R2 ismeri ugyanazt a hálózatot. |
| Az irányítási információk egy útvonalról nem biztosítanak visszirányú útvonal információt. | R1 kap egy csomagot PC1 cél IP-címével és PC3 forrás IP-címével. Csak azért mert R1 tudja, hogy a csomagot a G0/0/0 interfészen kell továbbítani, az nem feltétlenül jelenti azt, hogy ismeri hogyan továbbítsa a PC1-től származó csomagokat a távoli hálózatba PC3-nak. |

14.4.3

## Az irányítótábla bejegyzései

Elengedhetetlen, hogy a hálózat rendszergazdája értelmezni tudja az IPv4 és IPv6-irányítótábla tartalmát. Az ábra R1 irányítótáblájának IPv4 és IPv6 bejegyzéseit tartalmazza a 10.0.4.0/24 és 2001:db8:acad:4::/64 távoli hálózatokról. Mindkét útvonal dinamikusan lett megtanulva az OSPF irányító protokolltól.

Az ábra bemutatja, hogyan kell beolvasni az IPv4 útválasztási bejegyzést és az IPV6 útválasztási bejegyzést. Az IPv4 útválasztási táblázatának bejegyzése a 0 útválasztási forrással kezdődik, majd a célhálózattal (előtag és előtag hossza) 10.0.4.0/24, a 110-es adminisztratív távolság és az 50-es metrika után a következő ugrás a 10.0.3.2-n keresztül és az útvonal időbélyege 00:13;29, amely egy Serial 0/1/1 kilépési interfésszel végződik. A bejegyzés összeállítása a következő: 0 10.0.0.0/24 110/50 via 10.0.3.2 00:13:29 Sorozat 0/1/1. Az ipv6 bejegyzés ugyanúgy kezdődik a 0 útválasztási forrással, majd a 2001:DB8:ACAD:4::/64 célhálózata, az adminisztratív távolság 110 és a metrika 50, a következő ugrás után az FE80::2:C-n keresztül. nincs Útvonal időbélyegzője, és a Serial 0/1/1 Exit interfészével végződik

O 10.0.4.0/24 O 2001:DB8:ACAD:4::/64 via FE80::2:C, [110/50] via 10.0.3.2, Serial0/1/1 Serial0/1/1 00:13:29, [110/50] 1 2 3 4 5 6 7 1 2 3 4 5

7

IPv4 Routing Table IPv6 Routing Table

14.4.4

## Közvetlenül csatlakozó hálózatok

Mielőtt egy router megismerhetne távoli hálózatokat, legalább egy aktív interfésznek rendelkeznie kell IP-címmel és alhálózati maszkkal (előtag hossz). Ezt közvetlenül csatlakozó hálózatnak vagy közvetlenül csatlakozó útvonalnak nevezzük. A router akkor jegyez be az irányítótáblájába közvetlenül csatlakozó útvonalat, amikor egy interfésze aktívvá válik és van IP-címe.

A közvetlenül csatlakozó hálózatot a **C** állapotkódja jelöli az irányítótáblában. Az útvonal hálózati előtagot és előtag hosszot tartalmaz.

Az irányítótábla minden közvetlenül csatlakozó hálózatához tartalmaz egy helyi útvonalat is, amelyet az **L** állapotkód jelez. Ez az az IP-cím, amely a közvetlenül csatlakozó hálózaton található interfészhez van hozzárendelve. IPv4 helyi útvonalak esetén az előtag hossz /32, IPv6 helyi útvonalaknál pedig /128. Ez azt jelenti, hogy a csomag cél IP-címének meg kell egyeznie a helyi útvonal összes bitjével ahhoz, hogy ezzel az útvonallal egyezést mutasson. A helyi útvonal célja, hogy a router hatékonyan meg tudja állapítani, hogy a csomagot neki kell elfogadnia és nem kell továbbküldeni.

A következő kimeneten közvetlenül csatlakozó hálózatok és helyi útvonalak vannak megjelenítve.

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

(Output omitted)

C 10.0.1.0/24 is directly connected, GigabitEthernet0/0/0

L 10.0.1.1/32 is directly connected, GigabitEthernet0/0/0

R1#

R1# **show ipv6 route**

IPv6 Routing Table - default - 10 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

(Output omitted)

C 2001:DB8:ACAD:1::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via GigabitEthernet0/0/0, receive

R1#

14.4.5

## Statikus útvonalak

Miután bekonfiguráltuk a közvetlenül csatlakozó interfészeket és azok bekerültek a forgalomirányító táblába, sor kerülhet a statikus vagy a dinamikus forgalomirányítás megvalósítására is a távoli hálózatok eléréséhez.

A statikus útvonalakat a hálózati rendszergazda manuálisan konfigurálja. Egyértelmű utat írnak le két hálózati eszköz között. Ellentétben a dinamikus forgalomirányító protokollok használatával, a statikus útvonalak nem frissülnek automatikusan, a topológia változásakor kézzel kell őket újra beállítani. A statikus útvonalak használatának előnye, hogy biztonságosabbak, és velük hatékonyabban használhatjuk az erőforrásokat. A statikus útvonalak kevesebb sávszélességet használnak el, mint a dinamikus forgalomirányító protokollok, és az útvonalak számolásához és terjesztéséhez sem kell processzoridő. A legnagyobb hátrányuk, hogy a topológia változásakor nem fognak automatikusan újra konfigurálódni.

A statikus forgalomirányítás három alapvető felhasználási területe:

* Olyan kisméretű hálózatok esetén, amelyek várhatóan nem növekednek meg jelentősen, így az irányítótáblák karbantartása egyszerűen elvégezhető.
* Olyan hálózatok irányába vezető egyszerű alapértelmezett útvonal használatakor, amely nem egyezik meg az irányítótábla egyetlen másik útvonalával sem. Alapértelmezett útvonalak segítségével a forgalom bármilyen, a szomszédos forgalomirányítón túli célhálózat felé továbbítható.
* Forgalomirányítás egy véghálózat (stub network) irányába és vissza. A véghálózat olyan hálózat, ahonnan csak egy út vezet az egyetlen szomszéd hálózat felé.

Az ábrán véghálózatokra látható példa. Figyeljük meg, hogy bármely R1-hez csatlakozó hálózat egyetlen kijárattal rendelkezik más hálózatok, így az R2-höz kapcsolódó vagy még távolabbi hálózatok felé is. Ez azt jelenti, hogy a 10.0.1.0/24 és a 10.0.2.0/24 hálózatok véghálózatok és R1 a véghálózati router.

Az ábra két csonkhálózatot ábrázol, amelyek egy PC1-ből állnak a 10.0.1.0/24-es hálózaton és a 2001:db8:acad:1::/64-ből, amely az S1 kapcsolóhoz van csatlakoztatva, amelyhez egy gigabites G0/0/0 van csatlakoztatva az R1 útválasztóhoz. A PC2 a 10.0.2.4-es hálózaton, a 2001:db8:acad:2::/64 pedig S2 kapcsolóhoz csatlakozik, amely az R1 G0/0/1 gigabites interfészéhez csatlakozik. Az R1 útválasztót csonk útválasztónak nevezik. Az R1 az R2 útválasztóhoz 10.0.3.0/24 hálózati című R1 S0/1/1-S0/1/0 soros kapcsolaton keresztül csatlakozik az R2-n. Az R2 más hálózatokhoz csatlakozik. A PC-k kettős egymásra vannak rakva, .10 és ::10 címekkel. Az R1 interfészek .1 és ::1. Az R2 soros csatlakozási címe .2 és ::2

.10 ::10 10.0.2.0/24 2001:db8:acad:2::/64 .1 ::1 ::2 .2 S0/1/1 S0/1/0 10.0.3.0/24 .10 ::10 10.0.1.0/24 2001:db8:acad:1::/64 G0/0/0 G0/0/1 .1 ::1 .1 ::1 PC1 PC2 S1 S2 R1

R2

Internet és egyéb hálózatok csonk Hálózati csonk Hálózati csonk útválasztó

R1 helyi hálózata ebben a példában az R2 routeren konfigurált statikus útvonallal érhető el. Mivel R1 csak egyetlen irányba tudja a nem helyi forgalmat továbbítani, így rajta egy olyan alapértelmezett statikus útvonal adható meg, amely minden más hálózat felé az R2-t adja meg következő ugrásnak.

14.4.6

## Statikus útvonalak az IP-irányítótáblában

A statikus forgalomirányítás bemutatásához az ábrán látható topológia le van egyszerűsítve úgy, hogy mindegyik routerhez csak egy LAN kapcsolódik. Az ábra IPv4 és IPv6 statikus útvonalakat mutat, amelyek R1-en vannak beállítva, az R2 router 10.0.4.0/24 és 2001:db8:acad:4። /64 hálózatai elérésére. A konfigurációs parancsok csak illusztrációként szolgálnak, és egy másik fejezetben kerülnek bemutatásra.

A diagram az R1 konfigurációs parancsait mutatja be, amelyek az IPv4 és IPv6 statikus útvonalait állítják be a PC3 eléréséhez a 14.3.1. ábrán leírt topológiából. Az IPv4 parancs R1 (config)#ip route 10.0.4.0 255.255.255.0 10.0.3.2. A távoli IPv4 hálózati cím 10.0.4.0 255.255.255.0. A következő ugrású útválasztó IPv4-címe 10.0.3.2. Az IPv6 parancs R1 (config)# ipv6 route 2001.db8.acad.4::/64 2001.db8.acad3::2 formában van írva. A távoli IPv6-hálózat címe 2001.db8.acad.4::/64, a következő ugrású útválasztó IPv6-ja pedig 2001.db8.acad3::2.

ip route 10.0.4.0 255.255.255.0 10.0.3.2 ipv6 route 2001.db8.acad.4::/64 2001.db8.acad.3::2 .10 .1 .1 ::1 .2 .10 10.0.3.0/24 10.0.1.0/24 .1 G0/0/0 R2 R1 PC1 S1 S3 ::2 2001:db8:acad:1::/64 10.0.4.0/24 ::1 S0/1/1 ::10 ::10 PC3 ::1 2001:db8:acad:3::/64 2001:db8:acad:4::/64 S0/1/0 G0/0/0 R1 (config)#

R1 (config)#

Távoli IPv6 hálózati cím A következő ugrású útválasztó IPv6-címe Távoli IPv4-hálózati cím A következő ugrású útválasztó IPv4-címe

A kimenet az IPv4 és IPv6 statikus útvonal bejegyzéseket mutatja az R1 routeren, amelyről elérhetők az R2 10.0.4.0/24 és 2001:db8:acad:4::/64 hálózatai. Figyeljük meg, hogy mindkét útvonal bejegyzés az **S** állapotkódot használja, amely azt jelzi, hogy az útvonalak statikus módon lettek megtanulva. Mindkét bejegyzés tartalmazza a következő ugrás router IP-címét is (via IP-cím ). A parancs végén lévő **static** paraméter csak a statikus útvonalakat jeleníti meg.

R1# **show ip route static**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

(output omitted)

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

S 10.0.4.0/24 [1/0] via 10.0.3.2

R1# **show ipv6 route static**

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

(output omitted)

S 2001:DB8:ACAD:4::/64 [1/0]

via 2001:DB8:ACAD:3::2

14.4.7

## Dinamikus forgalomirányító protokollok

A dinamikus forgalomirányító protokollok segítségével a routerek távoli hálózatok elérhetőségét és állapotát tudják automatikusan megosztani egymással. A dinamikus forgalomirányító protokollok többféle tevékenységet is végeznek, mint például a hálózatok felderítése és a forgalomirányító táblák karbantartása.

A dinamikus forgalomirányító protokollok fontos előnyei, hogy automatiusan képesek kiválasztani a legjobb útvonalat és felfedezni az új legjobb útvonalat, ha a topológiában változás történik.

Hálózatok felderítésének azt nevezzük, amikor a forgalomirányító protokoll az általa ismert hálózatok információit megosztja az ugyanilyen protokollt használó más forgalomirányítókkal. Ahelyett, hogy minden forgalomirányítón kézzel konfigurálnánk be statikus útvonalakat valamennyi távoli hálózat felé, a dinamikus forgalomirányító protokoll segítségével a forgalomirányítók automatikusan megtanulják ezeket az útvonalakat egymástól. Ezeket a hálózatokat és a feléjük vezető legjobb útvonalat hozzáadják a forgalomirányító táblájukhoz és megjelölik, mint egy konkrét dinamikus protokoll által tanult útvonalat.

Az ábra az R1 és R2 routereket mutatja, amelyek közös forgalomirányító protokollt használnak a hálózati információk megosztására.

Az ábra 3 R 1, R 2 és R3 routert ábrázol, amelyek 4 S 1, S 2, S 3 és S4 kapcsolóhoz vannak csatlakoztatva. Az R 1 két gigabites G/0/0 és G0/0/1 kapcsolaton keresztül csatlakozik az S 1 és S 2 kapcsolókhoz. A P C1 a 10.0.1.0/24 és a 2001:db8:acad:1::/64 hálózat 1. kapcsolójához (S 1) csatlakozik, .10 és ::10 kettős verem IP-címmel. A P C2 a 10.0.2.0/24 és 2001:db8:acad:2::/64 hálózaton a 2. kapcsolóhoz (S 2) csatlakozik, .10 és ::10 kettős verem IP-címmel. Az R1-nek pont-pont hálózata van R2-vel és az ISP-hálózatokkal. Az R2 soros csatlakozása S0/1/01 és S0/1/0. Az internetszolgáltató kapcsolata S0/1/1. Az R 1 - R 2 hálózat 10.0.3.0/22 ​​és 2001:db8:acad:3::/64. Az R 2 hálózat 209.165.200.224/30 és 2001:db8:feed:224::/64 az internetszolgáltatónak. Az R 2 két gigabites csatlakozással rendelkezik a 3. (S 3) és a kapcsoló (S4) G0/0/0 és G/0/0/1 kapcsolójához. Az S 3 a 10.0.4.0/24 hálózat és a 2001:db8:acad:4::/64, amely a G0/0/0 R 2 interfészhez csatlakozik. Az S4 hálózat 10.0.5.0/24 és 2001:db8:acad:5::/64, amely a G0/0/1 R 2 interfészhez csatlakozik. A P C3 .10 és ::10 címmel csatlakozik az S 3-hoz. A P C4 0,10 és ::10 címmel csatlakozik az S4-hez. Az R1 és R2 átjárócímek .1-re és ::1-re végződnek. Az R1 és R2 közötti soros interfész R 1 .1 és ::1 és R 2 .2 és ::2 címekkel rendelkezik. Az R 2 és az ISP közötti kapcsolat .225 és .1 az ISP .226 és ::2 között. Az R1 és R2 útválasztók dinamikus útválasztási protokollon keresztül osztanak meg minden változást a hálózaton, az R1-ből kiemelt négyzetekkel, amelyek azt jelzik, hogy megosztom R2-vel az összes hálózatot, amelyről tudok, és értesítem R2-t, ha bármilyen változás történik. Ugyanez vonatkozik az R2-re, amely az R1-et tájékoztatja.

PC1 PC2 PC3 PC4 S1 S2 S4 R1 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2

S0/1/1

Megosztom R2-vel az összes hálózatot, amelyről tudok, és szólok R2-nek, ha bármilyen változás történik. Megosztom R1-el az összes hálózatot, amelyről tudok, és szólok R1-nek, ha bármilyen változás történik. Internet

14.4.8

## Dinamikus útvonalak az IP-irányítótáblában

Az előző példa statikus útvonalakat használt a 10.0.4.0/24 és a 2001:db8:acad:4::/64 hálózatokhoz. Ezek a statikus útvonalak már nincsenek beállítva, most az OSPF szolgál az R1-hez és R2-höz csatlakozó összes hálózat dinamikus megismerésére. A következő példák IPv4 és IPv6 OSPF útvonal bejegyzéseket mutatnak be az R1-en, amely eléri R2 ezen hálózatait. Figyeljük meg, hogy mindkét útvonal bejegyzés az **O** állapotkódot használja annak jelzésére, hogy az útvonal OSPF irányító protokolltól lett megtanulva. Mindkét bejegyzés tartalmazza a következő ugrás router IP-címét is (via IP-cím).

**Note**: IPv6 routing protocols use the link-local address of the next-hop router.

**Note**: OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

R1# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

(output omitted for brevity)

O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1

O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1

R1# **show ipv6 route**

IPv6 Routing Table - default - 10 entries

(Output omitted)

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

O 2001:DB8:ACAD:4::/64 [110/50]

via FE80::2:C, Serial0/1/1

O 2001:DB8:ACAD:5::/64 [110/50]

via FE80::2:C, Serial0/1/1

14.4.9

## Alapértelmezett útvonal

Az alapértelmezett útvonal az állomások alapértelmezett átjárójához hasonló. Az alapértelmezett útvonal egy következő ugrás routert határoz meg, amelyet akkor kell használni, ha az irányítótábla nem tartalmaz olyan útvonalat, amely megfelel a cél IP-címének.

Az alapértelmezett útvonal lehet statikus útvonal, vagy automatikusan megtanulható egy dinamikus irányító protokolltól. Az alapértelmezett útvonal IPv4 bejegyzése a 0.0.0.0/0, vagy IPv6 bejegyzése a ::/0. Ez azt jelenti, hogy nulla vagyis egyetlen bitnek sem kell megfelelnie a cél IP-címe és az alapértelmezett útvonal között.

A legtöbb vállalati router irányítótáblájában van alapértelmezett útvonal. Ez csökkenti a bejegyzések számát az irányítótáblában.

Egy otthoni vagy kisvállalati környezetben használt router, amely csak egyetlen helyi hálózattal rendelkezik, alapértelmezett útvonalon keresztül elérheti az összes távoli hálózatát. Ez akkor hasznos, ha a routernek csak közvetlenül csatlakozó hálózatai vannak és csak egy kilépési pontot tartalmaz a szolgáltatói routerhez.

Az ábrán az R1 és R2 routerek OSPF-et használnak a saját hálózataikról szóló útvonal információk megosztására (10.0.x.x/24 és 2001:db8:acad:x::/64 hálózatok). R2 statikus alapértelmezett útvonallal rendelkezik az ISP routerhez. R2 minden olyan csomagot továbbít az ISP routernek, amelynek cél IP-címe nem egyezik meg az irányítótáblája egyik hálózatával sem. Ebbe az internetre szánt összes csomag beletartozhat.

The figure depicts a diagram of 3 routers R1,R2,and R3 connected to 4 switches S1,S2,S3 and S4. R1 connects to switches S1 and S2 using two gigabit connections G/0/0 and G0/0/1. PC1 is connected to switch 1 (S1)on network 10.0.1.0/24 and 2001:db8:acad:1::/64 with a dual stack ip address of .10 and ::10. PC2 is connected to switch 2 (S2) on network 10.0.2.0/24 and 2001:db8:acad:2::/64 with a dual stack ip address of .10 and ::10. R1 has a point to point network to R2 and the ISP networks. The serial connection to R2 is S0/1/01 and S0/1/0. The ISP connection is S0/1/1. The R1 to R2 network is network 10.0.3.0/22 and 2001:db8:acad:3::/64. The R2 network is 209.165.200.224/30 and 2001:db8:feed:224::/64 to the ISP. R2 has two gigabit connections to switches 3 (S3) and switch (S4) G0/0/0 and G/0/0/1. S3 is network 10.0.4.0/24 and 2001:db8:acad:4::/64 connected to the R2 interface G0/0/0. S4 is network 10.0.5.0/24 and 2001:db8:acad:5::/64 connected to R2 interface G0/0/1. PC3 connects to S3 with an address of .10 and ::10. PC4 connects to S4 with an address of .10 and ::10. R1 and R2 gateway addresses end with .1 and ::1. The serial interface between R1 and R2 have addresses of R1 .1 ans ::1 and R2 .2 and ::2. The R2 to ISP connection is .225 and .1 to ISP .226 and ::2. The diagram shows R2 has a static default route to the ISP router. The default route is advertised by R2 to R1 using the dynamic routing protocol OSPF. There is an arrow showing the route to the ISP.

PC1 PC2 PC3 PC4 S1 S2 S4 R2 .10 .10 .10 .10 ::10 ::10 ::10 ::10 10.0.1.0/24 10.0.2.0/24 10.0.4.0/24 10.0.5.0/24 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:4::/64 2001:db8:acad:5::/64 G0/0/0 G0/0/1 209.165.200.224/30 2001:db8:feed:224::/64 .1 ::1 .1 ::1 .225 ::1 .1 ::1 S0/1/1 S0/1/1 S3 ::2 10.0.3.0/24 S0/1/0 .2 G0/0/0 G0/0/1 .1 ::1 .1 ::1 ISP 2001:db8:acad:3::/64 .226 ::2 S0/1/1 R1 1

2

Internet

1. R2 statikus alapértelmezett útvonallal rendelkezik az ISP routerhez.
2. Az alapértelmezett útvonalat R2 az OSPF dinamikus irányító protokoll használatával hirdeti R1-nek.

R2 OSPF használatával osztotta meg az alapértelmezett útvonalat R1-el. R1 most már rendelkezik egy alapértelmezett útvonallal az irányító táblájában, amelyet dinamikusan tanult meg OSPF-el. R1 minden olyan csomagot továbbít az R2 routernek, amelynek cél IP-címe nem egyezik meg az irányítótáblája egyik hálózatával sem.

A következő példák az R2-n konfigurált IPv4 és IPv6 statikus alapértelmezett útvonal bejegyzéseket mutatják az irányítótáblában.

R2# **show ip route**

(Output omitted)

S\* 0.0.0.0/0 [1/0] via 209.165.200.226

R2#

R2# **show ipv6 route**

(Output omitted)

S ::/0 [1/0]

via 2001:DB8:FEED:224::2

R2#

14.4.10

## Az IPv4-irányítótábla szerkezete

Az IPv4-et az 1980-as évek elején szabványosították a mára elavult osztály alapú címzési architektúrával. Az IPv4-irányítótábla ugyanezen osztály alapú szerkezetre épül. A **show ip route** kimeneten figyeljük meg, hogy egyes útvonalbejegyzések balra igazítottak, míg mások behúzással rendelkeznek. Ez azon alapul, hogy a forgalomirányítási folyamat milyen módon keresi az IPv4-irányítótáblában a leghosszabb egyezést. Mindez az osztály alapú címzés miatt lett ilyen. Bár a keresési folyamat már nem használ osztályokat, az IPv4-irányítótábla szerkezete továbbra is ebben a formátumban maradt.

Router# **show ip route**

(Output omitted)

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0

L 192.168.1.1/32 is directly connected, GigabitEthernet0/0

O 192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0

O 192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1

192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.12.0/30 is directly connected, Serial0/0/0

L 192.168.12.1/32 is directly connected, Serial0/0/0

192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.13.0/30 is directly connected, Serial0/0/1

L 192.168.13.1/32 is directly connected, Serial0/0/1

192.168.23.0/30 is subnetted, 1 subnets

O 192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0

Router#

**Note**: The IPv4 routing table in the example is not from any router in the topology used in this module.

Habár a szerkezet részletei túlmutatnak a fejezet hatókörén, a tábla szerkezetének ismerete hasznos lehet. A behúzott bejegyzést gyermek útvonalnak nevezik. Az útvonalbejegyzés behúzásra kerül, ha az egy osztály alapú cím (A, B vagy C osztályú hálózat) alhálózata. A közvetlenül csatlakozó hálózatok mindig be vannak húzva (gyerek útvonalak), mert az interfész helyi címe mindig /32 alakban kerül beírásra az irányítótáblába. A gyermek útvonal tartalmazza az útvonal forrását és az összes továbbítási információt, például a következő ugrás címét. Ennek az alhálózatnak az osztály alapú hálózati címe az útvonalbejegyzés felett jelenik meg, kisebb behúzással, a forrás kódja nélkül. Ezt hívjuk szülő útvonalnak.

**Megjegyzés** : Ez csak egy rövid bevezetés az IPv4 útválasztási tábla szerkezetébe, és nem tér ki az architektúra részleteire vagy sajátosságaira.

A következő példa a topológiában lévő R1 IPv4-irányítótábláját mutatja be. Figyeljük meg, hogy a topológia összes hálózata alhálózat, melyek gyermek útvonalak, és az A osztályú 10.0.0.0/8 hálózathoz, a szülő útvonalhoz tartoznak.

R1# **show ip route**

(output omitted for brevity)

O\*E2 0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

C 10.0.1.0/24 is directly connected, GigabitEthernet0/0/0

L 10.0.1.1/32 is directly connected, GigabitEthernet0/0/0

C 10.0.2.0/24 is directly connected, GigabitEthernet0/0/1

L 10.0.2.1/32 is directly connected, GigabitEthernet0/0/1

C 10.0.3.0/24 is directly connected, Serial0/1/1

L 10.0.3.1/32 is directly connected, Serial0/1/1

O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1

O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1

R1#

14.4.11

## Az IPv6-irányítótábla szerkezete

Az osztály alapú címzés fogalma soha nem volt része az IPv6-nak, így az IPv6-irányítótábla szerkezete nagyon egyértelmű. Minden IPv6-útvonalbejegyzés ugyanúgy van formázva és igazítva.

R1# **show ipv6 route**

(output omitted for brevity)

OE2 ::/0 [110/1], tag 2

via FE80::2:C, Serial0/0/1

C 2001:DB8:ACAD:1::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via GigabitEthernet0/0/0, receive

C 2001:DB8:ACAD:2::/64 [0/0]

via GigabitEthernet0/0/1, directly connected

L 2001:DB8:ACAD:2::1/128 [0/0]

via GigabitEthernet0/0/1, receive

C 2001:DB8:ACAD:3::/64 [0/0]

via Serial0/1/1, directly connected

L 2001:DB8:ACAD:3::1/128 [0/0]

via Serial0/1/1, receive

O 2001:DB8:ACAD:4::/64 [110/50]

via FE80::2:C, Serial0/1/1

O 2001:DB8:ACAD:5::/64 [110/50]

via FE80::2:C, Serial0/1/1

L FF00::/8 [0/0]

via Null0, receive

R1#

14.4.12

## Adminisztratív távolság

Egy adott hálózati cím útvonalbejegyzése (előtag és előtag hossz) csak egyszer jelenhet meg az irányítótáblában. Lehetséges azonban, hogy az irányítótábla egynél több forrásból is megismeri ugyanazt a hálózati címet.

A nagyon különleges körülményektől eltekintve egyetlen dinamikus forgalomirányító protokollt használunk egy routeren. Viszont bekonfigurálhatunk OSPF-et és EIGRP-t is ugyanazon a routeren, és így mindkét forgalomirányító protokoll tudomást szerezhet ugyanarról a célhálózatról. Mindegyik forgalomirányító protokoll dönthet különböző útvonal mellett is a cél elérésére, a protokollok különböző mértékei alapján.

Ez felvet néhány kérdést, például a következőket:

* Honnan tudja a router, hogy melyik forrást használja?
* Melyik útvonal kerüljön be az irányítótáblába? Az OSPF-től tanult útvonal, vagy az EIGRP-től tanult útvonal?

A Cisco IOS az adminisztratív távolságnak (administrative distance, AD) nevezett értéket használja annak eldöntésére, hogy melyik útvonal kerüljön be az IP forgalomirányító táblába. Az adminisztratív távolság az útvonal "megbízhatóságának" mértéke. Minél kisebb az adminisztratív távolság, annál megbízhatóbb forrásból származik az útvonal. Mivel az adminisztratív távolsága értéke EIGRP esetén 90, OSPF esetén pedig 110, ezért az EIGRP útvonalbejegyzés kerülne be az irányítótáblába.

**Megjegyzés** : Az AD nem feltétlenül jelzi, hogy melyik dinamikus útválasztási protokoll a legjobb.

Hétköznapibb példa egy olyan router lehet, amely statikus útvonal és dinamikus irányító protokoll (például OSPF) forrásokból is megismeri ugyanazt a hálózati címet. Egy statikus útvonal adminisztratív távolsága 1, míg egy OSPF által feltárt útvonalé 110. Ugyanahhoz a célhálózathoz tartozó két különböző útvonal forrás esetén a router a kisebb adminisztratív távolságút választja. Ha a forgalomirányítónak egy statikus és egy OSPF útvonal között kell választania, a statikus élvez elsőbbséget.

**Note** : Directly connected networks have the lowest AD of 0. Csak közvetlenül csatlakozó hálózat adminisztratív távolság értéke lehet 0.

A táblázatban különböző forgalomirányító protokollok és a hozzájuk tartozó adminisztratív távolság értékek vannak felsorolva.

| Útvonalforrás Adminisztratív távolság Közvetlenül csatlakoztatva0 Statikus útvonal1 EIGRP összefoglaló útvonal5 Külső BGP20Belső EIGRP90OSPF 110IS-IS115RIP120Külső EIGRP170Belső BGP200 | |
| --- | --- |
| **Útvonal forrása** | **Adminisztratív távolság** |
| Közvetlenül csatlakozó | 0 |
| Statikus útvonal | 1 |
| EIGRP összevont útvonal | 5 |
| Külső BGP | 20 |
| Belső EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| NYUGODJ BÉKÉBEN | 120 |
| Külső EIGRP | 170 |
| Belső BGP | 200 |

14.4.13

## Tudáspróba - IP-irányítótábla

Az űrlap teteje

Ellenőrizze, hogy megértette-e az IP-útválasztási táblázatot, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Melyik útválasztási tábla elve nem megfelelő?

Az űrlap alja

Which route entry would be used for a packet with a destination IP address that matches an IP address of one of the router interfaces?

What type of network is accessed by a single route and the router has only one neighbor?

Which two route sources have the ability to automatically discover a new best path when there is a change in the topology? (Két jó válasz van.)

Igaz vagy hamis? Az alapértelmezett útvonal csak statikus útvonal lehet.

A hálózati rendszergazda statikus útvonalat konfigurál ugyanahhoz a célhálózathoz, amelyet az útválasztó automatikusan megtanult az OSPF használatával. Melyik útvonal kerül telepítésre és miért?

[14.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[A router alapbeállításainak áttekintése](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Statikus és dinamikus útválasztás](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Útválasztási fogalmak
2. Static and Dynamic Routing

# Statikus és dinamikus útválasztás

14.5.1

## Statikus vagy dinamikus?

Az előző témakör azt ismertette, hogy a router milyen módon hozza létre az irányítótáblát. Most már tudjuk, hogy a forgalomirányítás az IP-címzéshez hasonlóan lehet statikus vagy dinamikus. Statikus vagy dinamikus forgalomirányítást kell inkább használnunk? A válasz: mindkettőt! A statikus és dinamikus forgalomirányítás nem zárják ki egymást. Sőt a legtöbb esetben a hálózatok egyszerre mindkettőt alkalmazzák.

**Statikus útvonalak**

A statikus útvonalakat általában a következő esetekben használjuk:

* Alapértelmezett útvonalként csomagok továbbítására a szolgáltatónak
* Az irányítási tartományon kívüli és dinamikus irányító protokoll által meg nem ismert útvonalak esetén
* Amikor a hálózati rendszergazda saját maga akarja megadni egy adott hálózat elérési útját
* A véghálózatok közötti forgalomirányításhoz

A statikus útvonalak olyan kisebb hálózatok esetén alkalmazhatók hatékonyan, amelyek egyetlen kijárattal rendelkeznek egy külső hálózat felé. Ezen felül nagyobb hálózatokban is biztonságosan alkalmazhatók fokozott biztonságot igénylő forgalom vagy összeköttetés esetén.

**Dinamikus útválasztási protokollok**

A dinamikus irányító protokollok a statikus útvonalak megadásának és karbantartásának időigényes és fárasztó munkájában segítik a hálózati rendszergazdát. A dinamikus irányító protokollok minden hálózattípusban beállíthatók, amely néhánynál több routerből áll. Skálázhatóak és automatikusan meghatározzák a jobb útvonalakat, ha változás történik a topológiában.

A dinamikus irányító protokollokat általában a következő esetekben használjuk:

* Néhánynál több routert tartalmazó hálózatokban
* Ha a hálózati topológia megváltozásakor szükség van egy másik útvonal automatikus meghatározására
* A skálázhatóság miatt. A hálózat növekedésével a dinamikus irányító protokoll automatikusan megismeri az új hálózatokat.

A táblázat a dinamikus és statikus forgalomirányítás közötti különbségek összehasonlítását mutatja.

| Dinamikus útválasztásStatikus útválasztásKonfiguráció összetettsége Független a hálózat méretétől A hálózat méretével növekszik a topológia változásaihoz Automatikusan alkalmazkodik a topológia változásaihoz Adminisztrátori beavatkozás szükséges Skálázhatóság Egyszerű és összetett hálózati topológiákhoz Alkalmas Egyszerű topológiákhoz Biztonság A biztonságot konfigurálni kell A biztonság inherens. Kifejezetten használt ting protokoll az adminisztrátor határozza meg | | |
| --- | --- | --- |
| **Funkció** | **Dinamikus forgalomirányítás** | **Statikus forgalomirányítás** |
| Konfigurálás bonyolultsága | Független a hálózat méretétől | A hálózat méretével növekszik |
| Topológia változások | Automatikusan alkalmazkodik a topológia változásokhoz | Rendszergazda beavatkozása szükséges |
| Skálázhatóság | Egyszerű és bonyolult topológiák esetén is alkalmas | Egyszerűbb topológiák esetén alkalmas |
| Biztonság | A biztonságra külön oda kell figyelni | Alapjaiban biztonságos |
| Erőforrás használat | CPU-t, memóriát és sávszélességet használ | Nincs szükség további erőforrásra |
| Az útvonal kiszámíthatósága | Az útvonal a használt topológiától és az irányító protokolltól függ | A rendszergazda által egyértelműen meghatározott |

14.5.2

## A dinamikus forgalomirányítás fejlődése

A dinamikus forgalomirányító protokollokat az 1980-as évek végétől kezdődően használják a hálózatokban. Az első irányító protokollok egyike a RIP (Routing Information Protocol) volt. A RIPv1-et 1998-ban adták ki, viszont a protokoll által használt alap algoritmusok közül néhányat már 1969-ben is használtak az ARPANET-nél (Advanced Research Projects Agency Network, Speciális Kutatási Programok Hivatalának hálózata).

Ahogy a hálózatok fejlődtek és egyre összetettebbé váltak, úgy alakultak ki az újabb irányító protokollok is. A RIP protokollt a megnövekedett hálózati igényeknek megfelelően RIPv2-vé fejlesztették tovább. Azonban a RIPv2 még mindig nem megfelelő a mai nagyméretű hálózati megvalósításokhoz. A nagyobb méretű hálózati igények kielégítésére két fejlett irányító protokollt fejlesztettek ki: a legrövidebb út (Open Shortest Path First, OSPF) és a közbülső rendszerből közbülső rendszerbe (Intermediate System-to-Intermediate System, IS-IS) protokollokat. A Cisco a belső átjáró irányító protokollt (Interior Gateway Routing Protocol, IGRP) hozta létre, amelyet később felváltott a továbbfejlesztett IGRP (Enhanced IGRP, EIGRP), amely szintén jól illeszkedik a nagyméretű hálózati megvalósításokra.

Ezen felül szükség volt a különböző szervezetek irányítási tartományaiak összekapcsolására és a köztük lévő forgalomirányítás megvalósítására is. Az internetszolgáltatók (ISP) között erre a célra a külső átjáró protokoll ( Exterior Gateway Protocol, EGP) utódja a határátjáró-protokoll (Border Gateway Protocol, BGP) használható. A BGP-t az ISP-k és számos egyéni szervezet közötti irányítási információk cseréjére is használják.

Az ábra idővonalán a különböző protokollok bevezetésének időpontjai láthatók.

Az ábra idővonalán a különböző protokollok bevezetésének időpontjai láthatók. Starting with 1982 EGP, 1985 IGRP, 1988 RIPv1, 1990 IS-IS, 1991 OSPFv2, 1992 EIGRP, 1994 RIPv2, 1995 BGP, 1997 RIPng, 1998 BGP-MP, 1999 OSPFv3, 2000 IS-ISv6.

IS-ISv6 2008 EGP IGRP 1982 1985 RIPv1 1988 IS-IS OSPFv2 EIGRP 1990s 1990 1991 1992 BGP RIPv2 1994 1995 RIPng BGP-MP 1997 1998 OSPFv3 1999

2000s

Az IPv6 kommunikáció támogatása érdekében az IP alapú irányító protokollok újabb változatai jöttek létre, ezek a táblázat IPv6 sorában láthatók.

A táblázat az aktuális irányító protokollokat csoportosítja. A belső átjáróprotokollok (IGP) olyan irányító protokollok, amelyek egy adott szervezet által felügyelt irányítási tartományon belüli irányítási információk cseréjére szolgálnak. Csak egyetlen EGP létezik, és ez a BGP. A BGP az irányítási információk különböző szervezetek, az úgynevezett autonóm rendszerek (AS) közötti cseréjére szolgál. A BGP-t az internetszolgáltatók használják a csomagok interneten történő továbbítására. A távolságvektor, a kapcsolatállapot és az útvonalvektor alapú irányító protokollok irányítási algoritmust használnak a legjobb útvonal meghatározásához.

| Belső átjáróprotokollokKülső átjáró protokollok Távolság VectorLink-StatePath VectorIPv4RIPv2EIGRPOSPFv2IS-ISBGP-4IPv6RIPngEIGRP az IPv6OSPFv3IS-IS-hez IPv6BGP-MP-hez | | | | | |
| --- | --- | --- | --- | --- | --- |
|  | **Belső átjáró protokollok** | | | | **Külső átjáró protokollok** |
|  | **Távolságvektor alapú** | | **Kapcsolatállapot alapú** | | **Útvonal vektor alapú** |
| **IPv4** | RIPv2 | EIGRP | OSPFv2 | IS-IS | BGP-4 |
| **IPv6** | RIPNG | IPv6-os EIGRP | OSPFv3 | IPv6-os IS-IS | BGP-MP |

14.5.3

## Dinamikus forgalomirányító protokollok elmélete

A forgalomirányító protokoll olyan folyamatok, algoritmusok és üzenetek összessége, amelynek használatával lehetővé válik az irányítási információk cseréje és az irányítótábla legjobb útvonalakkal történő feltöltése. A dinamikus forgalomirányító protokollok céljai a következők:

* Távoli hálózatok felderítése.
* Az aktuális irányítási információk karbantartása.
* A célhálózatokhoz vezető legjobb útvonal kiválasztása.
* Az aktuális útvonal elérhetetlenné válása esetén egy újabb legjobb útvonal kiválasztásának képessége.

A dinamikus forgalomirányító protokollok fő összetevői a következők:

* **Data structures -** Routing protocols typically use tables or databases for their operations. Ezeket az információkat a RAM-ban tárolják.
* **Útválasztási protokoll üzenetek –** Az útválasztási protokollok különféle típusú üzeneteket használnak a szomszédos útválasztók felderítésére, az útválasztási információk cseréjére és egyéb feladatokra a hálózattal kapcsolatos pontos információk megismerésére és karbantartására.
* **Algorithm -** An algorithm is a finite list of steps used to accomplish a task. Az irányító protokollok algoritmusokat használnak a forgalomirányítási információk cseréjéhez és a legjobb útvonal meghatározásához.

Az irányító protokollok teszik lehetővé a routerek számára, hogy dinamikusan információkat osszanak meg távoli hálózatokról és automatikusan hozzáadják ezt az információt a saját irányító táblájukhoz. A folyamat animációjának megtekintéséhez kattintsunk a Lejátszás gombra!

Az ábra egy animáció három R1, R2 és R3 routerrel, amelyek háromszög mintázatban vannak összekapcsolva. Az animáció azt szemlélteti, hogy amikor frissítés történik bármelyik útválasztón, azt kiküldi a többieknek.

Frissítés

Az irányító protokollok a legjobb útvonalat határozzák meg a hálózatok felé. Ez az útvonal ezután felajánlásra kerül az irányítótáblának. Az útvonal telepítve lesz az irányítótáblába, ha nem található egy másik, alacsonyabb AD-vel rendelkező útvonalforrás. A dinamikus forgalomirányító protokollok legfontosabb előnye, hogy a topológiában bekövetkezett változáskor a routerek információt cserélnek egymással. Ez az információcsere teszi lehetővé a számukra, hogy automatikusan értesüljenek az új hálózatokról vagy egy meglévő hálózathoz vezető kapcsolat hibája esetén alternatív útvonalat találjanak.

14.5.4

## Legjobb útvonal

Mielőtt egy távoli hálózat elérési útja felajánlásra kerülne az irányítótáblának, a dinamikus forgalomirányító protokollnak meg kell határoznia a legjobb útvonalat a hálózathoz. A legjobb útvonal meghatározása több olyan útvonal vizsgálatát is magába foglalhatja, amelyek ugyanahhoz a célhálózathoz vezetnek, majd közülük kell kiválasztani az optimális vagy legrövidebb útvonalat a hálózat felé. Amikor ugyanahhoz a hálózathoz több útvonal is vezet, akkor mindegyik útvonal másik kimenő interfészen fogja elhagyni a routert a hálózat felé.

A legjobb útvonalat egy forgalomirányító protokoll választja ki, egy a hálózat távolságát tükröző érték vagy mérték alapján. A mérték a hálózat távolságának mérőszáma. Az a legjobb útvonal, amelyhez a legkisebb mérték tartozik.

A dinamikus forgalomirányító protokollok jellemzően a saját szabályaikat és mértékeiket használják az irányítótáblák felépítéséhez és frissítéséhez. A forgalomirányító algoritmus minden útvonalhoz egy értéket, vagy más néven mértéket társít. A mérték az útvonal egy vagy több jellemző tulajdonsága alapján állhat elő. Néhány forgalomirányító protokoll több mérték kombinációjából állít elő egyetlen mértéket, ami alapján a választást végzi majd.

Az alábbi táblázat a gyakori dinamikus protokollokat és azok mértékeit tartalmazza.

| Routing ProtocolMetricRouting Information Protocol (RIP)A metrika az „ugrásszám”.Az útvonalon lévő minden útválasztó hozzáad egy ugrást az ugrások számához.Legfeljebb 15 ugrás megengedett.Open Shortest Path First (OSPF) A mérőszám a „költség”, amely a forrástól a célállomásig terjedő kumulált sávszélességen alapul.A gyorsabb kapcsolatokhoz alacsonyabb költségek tartoznak, mint a lassabb (magasabb költségű) kapcsolatokhoz.Enhanced Interior Gateway Routing Protocol (EIGRP) A leglassabb sávszélesség és késleltetési értékek alapján számítja ki a mérőszámot. a terhelést és a megbízhatóságot is bele kell foglalni a metrika számításába. | |
| --- | --- |
| **Irányító protokoll** | **Mérték** |
| **Routing Information Protocol (RIP)** | * A mérték az "ugrásszám". * Az útvonal mentén minden router hozzáad egy ugrást az ugrásszámhoz. * Legfeljebb 15 ugrás a megengedett. |
| **Először nyissa meg a legrövidebb utat (OSPF)** | * A mérték a "költség", amely a forrástól célig összegzett sávszélességen alapul. * Gyorsabb kapcsolatokhoz alacsonyabb költségek vannak rendelve, mint a lassabbakhoz (magasabb költség). |
| **Enhanced Interior Gateway Routing Protocol (EIGRP)** | * A mértéket a legkisebb sávszélesség és késleltetés értéke alapján számolja ki. * A mérték kiszámítása magában foglalhatja a terhelést és a megbízhatóságot is. |

Az animáció megmutatja, hogy a használt mértéktől függően hogyan változhat az útvonal. Ha a legjobb útvonal elérhetetlenné válik, a dinamikus irányító protokoll automatikusan kiválaszt egy új legjobb útvonalat, ha létezik ilyen.

Az ábra egy animáció egy PC1 feliratú PC-vel, amely egy R1 útválasztóhoz van csatlakoztatva. R1 csatlakozik az R2-höz 1 Gbps-os kapcsolattal, és R2 csatlakozik az R3-hoz 1 Gbps-os kapcsolattal. Az R3 100 Mbps-os kapcsolattal csatlakozik az R1-hez. Az útválasztók derékszögű háromszöghöz hasonlóan vannak ábrázolva. Egy másik PC2 feliratú PC csatlakozik az R3-hoz. Az animáció az ugrásszámon vagy a sávszélességen alapuló útválasztási döntéseket ábrázolja.

14.5.5

## Terheléselosztás

Mi történik akkor, ha az irányítótábla kettő vagy még több útvonalat is tartalmaz azonos mértékkel ugyanazon célhálózat felé?

Ha a routernek egy cél felé kettő vagy több azonos mértékű útvonala van, mindkét útvonalat azonos arányban fogja használni. Ezt hívják egyenlő vagy azonos költségű terhelésmegosztásnak. Az irányítótábla egyetlen célhálózatot tartalmaz, de több kimenő interfésszel, minden azonos költségű úthoz egyet-egyet. A router ezeket a kimenő interfészeket fogja használni a csomagok továbbításához.

Ha helyesen van beállítva, a terhelésmegosztás növelheti a hálózat hatékonyságát és teljesítményét.

A dinamikus forgalomirányító protokollok automatikusan végrehajtják az azonos költségű terheléselosztást. Ez a statikus útvonalaknál is engedélyezve van, ha több statikus útvonal létezik ugyanahhoz a célhálózathoz különböző következő ugrás routerekkel.

**Megjegyzés** : Csak az EIGRP támogatja az egyenlőtlen költség terheléselosztást.

Az animáción példát láthatunk egyenlő költségű terhelésmegosztásra.

Az ábra egy animáció négy R1, R2, R3 és R4 routerrel, amelyek 52 Mbps-os kapcsolattal vannak összekapcsolva. Egy PC1 jelzésű PC csatlakozik az R1-hez, és egy második PC2 feliratú PC csatlakozik az R3-hoz. Amikor az animáció fut, a PC1-ről érkező csomagok különböző utakat visznek az útválasztókon keresztül a PC2-re, ami az egyenlő költségterhelés-kiegyenlítést szemlélteti, mivel minden útválasztó azonos sebességgel rendelkezik.

14.5.6

## Tudáspróba - Dinamikus és statikus forgalomirányítás

Az űrlap teteje

Ellenőrizze, hogy megértette-e a dinamikus és statikus útválasztást, ha kiválasztja a LEGJOBB választ a következő kérdésekre.

1. Melyik típusú útválasztás alkalmazkodik automatikusan a topológia változásaihoz?

Az űrlap alja

Milyen típusú útválasztást használnak általában egy csonkhálózatnál?

Milyen mérőszámot használ az OSPF a legjobb útvonal meghatározásához?

Milyen kifejezést használnak a célhoz vezető két vagy több útvonalon történő útvonalak leírására azonos költségmutatókkal?

[14.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP Routing Table](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[14.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Útválasztási fogalmak
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

14.6.1

## Miről tanultunk ebben a fejezetben?

**Útvonal meghatározása**

A router elsődleges funkciói a csomagtovábbítás legjobb útvonalának meghatározása az irányítótáblában szereplő információk alapján, valamint a csomagok célállomás felé történő továbbítása. A legjobb útvonal az irányítótáblában a leghosszabb egyezésként is ismert. Leghosszabb egyezésnek az irányítótábla azon útvonalát tekintjük, amelynek bal oldalról nézve a legtöbb bitje egyezik meg a csomag cél IP-címével. A közvetlenül csatlakozó hálózatok olyan hálózatok, amelyek a router aktív interfészein vannak konfigurálva. Egy közvetlenül csatlakozó hálózat akkor adódik hozzá az irányítótáblához, ha egy interfész IP-címmel és alhálózati maszkkal (előtag hossz) van konfigurálva és aktív (felkapcsolt állapotú). A routerek kétféleképpen ismerhetik meg a távoli hálózatokat: kézi konfigurálással statikus útvonalak kerülnek az irányítótáblába, vagy dinamikus irányító protokollokkal. Dinamikus forgalomirányító protokollok (például EIGRP és OSPF) használatakor az útvonalak akkor vannak hozzáadva az irányítótáblához, amikor az irányító protokollok dinamikusan megismerik a távoli hálózatot.

**Csomagtovábbítás**

Miután a router meghatározta a helyes útvonalat, továbbíthatja a csomagot egy közvetlenül csatlakozó hálózaton, vagy egy következő ugrás routernek, vagy el is dobhatja a csomagot. A csomagtovábbítás elsődleges fontosságú művelete a csomag beágyazása a megfelelő adatkapcsolati keretbe a kimenő interfész számára. A routerek három csomagtovábbítási mechanizmust támogatnak: folyamatkapcsolást, gyors kapcsolást és a CEF-et. Az alábbi lépések a csomagtovábbítási folyamatot írják le:

1. Az adatkapcsolati keretbe ágyazott IP-csomag érkezik a bejövő interfészre.
2. A router megvizsgálja a csomag fejrészében található cél IP-címet és keresést indít az IP-irányítótáblában.
3. Megtalálja benne a leghosszabb egyezést mutató előtagot.
4. Beágyazza a csomagot egy adatkapcsolati keretbe és továbbítja azt a kimenő interfészen. A cél egy olyan eszköz lehet, amely a hálózathoz vagy egy követező ugrás routerhez csatlakozik.
5. Azonban, ha nincs egyező bejegyzés az irányítótáblában a csomag eldobásra kerül.

**Az útválasztó alapvető konfigurációjának áttekintése**

Számos konfigurációs és ellenőrző parancs létezik a routereken: **show ip route** , **show ip interface** , **show ip interface brief** és **show running-config** . A parancskimenet mennyiségének csökkentéséhez használjunk szűrőt. A szűrőparancsok segítségével a kimenet meghatározott szakaszai jeleníthetők meg. A szűrő parancsok engedélyezéséhez, üssük le a függőleges vonal (|) karaktert a **show** parancs után, majd adjuk meg a szűrő paramétert és a szűrési kifejezést. A függőleges vonal után a következő szűrő paramétereket használhatjuk:

* **section** - A szűrő kifejezéssel kezdődő egész szakaszt mutatja meg
* **include** - Minden olyan sort megkapunk, amely a szűrő kifejezésre illik.
* **exclude** - Minden olyan sort megkapunk, amely nem illik a szűrő kifejezésre.
* **begin** - A kimenetet egy bizonyos helytől a végéig listázza ki, mégpedig a szűrő kifejezésre illő sorral kezdődően.

**IP-útválasztó táblázat**

Az irányítótábla az ismert hálózatokhoz vezető útvonalak listáját (előtagok és előtag-hosszok) tartalmazza. Ezen információ forrásait közvetlenül csatlakozó hálózatok, statikus útvonalak és dinamikus irányító protokollok jelentik. Az irányítótábla gyakori kódjai a következők:

* **L** - A router interfészéhez rendelt címet jelenti. Ennek segítségével tudja a router hatékonyan megállapítani, hogy a csomagot nem kell továbbítani, hanem neki kell elfogadnia.
* **C** - Közvetlenül csatlakozó hálózatot jelöl.
* **S** - Egy bizonyos hálózat eléréséhez létrehozott statikus útvonal.
* **O** - Dinamikusan megtanult hálózatot jelöl, amelyet OSPF protokollal kaptunk egy másik forgalomirányítótól.
* **\*** - Az útvonal egy alapértelmezettnek kijelölt útvonal.

Minden router önállóan hozza meg a döntését az irányítótáblájában rendelkezésére álló információk alapján. Egy router irányítótáblájában szereplő információk nem feltétlenül egyeznek meg egy másik router irányítótáblájában lévő információkkal. Egy útvonal irányítási információi nem biztosítanak a vissza irányú útvonalról információkat. Az irányítótábla bejegyzései közé tartozik az útvonal forrása, a célhálózat, az adminisztratív távolság, a mérték, a következő ugrás, az útvonal-időbélyeg és a kimenő interfész. A távoli hálózatok megismeréséhez a routernek rendelkeznie kell legalább egy aktív interfésszel, amely IP-címmel és alhálózati maszkkal (előtag hosszal) van konfigurálva, ezt közvetlenül csatlakozó hálózatnak nevezik. A statikus útvonalak kézzel vannak megadva, és egyértelmű útvonalat határoznak meg két hálózati eszköz között. A dinamikus forgalomirányító protokollok felfedezhetik a hálózatot, kezelhetik az irányítótáblákat, kiválaszthatják a legjobb útvonalat, és automatikusan felfedezhetik az új legjobb útvonalat, ha a topológia megváltozik. Az alapértelmezett útvonal egy következő ugrás routert határoz meg, amelyet akkor kell használni, ha az irányítótábla nem tartalmaz olyan útvonalat, amely megfelel a cél IP-címének. Az alapértelmezett útvonal lehet statikus útvonal, vagy automatikusan megtanulható egy dinamikus irányító protokolltól. Az alapértelmezett útvonal IPv4 bejegyzése a 0.0.0.0/0, vagy IPv6 bejegyzése a ::/0. Az IPv4-irányítótábláknak továbbra is osztály alapú felépítése van, amelyet a behúzás szintjei jelölnek. Az IPv6-irányítótáblák nem használják az IPv4-irányítótábla szerkezetet. A Cisco IOS az adminisztratív távolságnak (administrative distance, AD) nevezett értéket használja annak eldöntésére, hogy melyik útvonal kerüljön be az IP forgalomirányító táblába. Az adminisztratív távolság az útvonal "megbízhatóságának" mértéke. Minél kisebb az adminisztratív távolság, annál megbízhatóbb forrásból származik az útvonal.

**Statikus és dinamikus útválasztás**

A statikus útvonalak gyakori használata:

* Alapértelmezett útvonalként csomagok továbbítására a szolgáltatónak.
* Az irányítási tartományon kívüli és dinamikus irányító protokoll által meg nem ismert útvonalak esetén.
* Amikor a hálózati rendszergazda saját maga akarja megadni egy adott hálózat elérési útját.
* A véghálózatok közötti forgalomirányításhoz.

A dinamikus forgalomirányító protokollok gyakori használata:

* Néhánynál több routert tartalmazó hálózatokban
* Ha a hálózati topológia megváltozásakor szükség van egy másik útvonal automatikus meghatározására
* A skálázhatóság miatt. A hálózat növekedésével a dinamikus irányító protokoll automatikusan megismeri az új hálózatokat.

Az aktuális irányító protokollok közé az IGP-k és az EGP-k tartoznak. Az IGP-k egy adott szervezet által felügyelt irányítási tartományon belüli irányítási információk cseréjét végzik. Az egyetlen EGP a BGP. A BGP különböző szervezetek között osztja meg az irányítási információkat. A BGP-t az internetszolgáltatók használják a csomagok interneten történő továbbítására. A távolságvektor, a kapcsolatállapot és az útvonalvektor alapú irányító protokollok irányítási algoritmust használnak a legjobb útvonal meghatározásához. A dinamikus irányító protokollok fő összetevői az adatstruktúrák, az irányító protokoll üzenetek és az algoritmusok. A legjobb útvonalat egy forgalomirányító protokoll választja ki, egy a hálózat távolságát tükröző érték vagy mérték alapján. A mérték a hálózat távolságának mérőszáma. Az a legjobb útvonal, amelyhez a legkisebb mérték tartozik. Ha a routernek egy cél felé kettő vagy több azonos mértékű útvonala van, mindkét útvonalat azonos arányban fogja használni. Ezt hívják egyenlő vagy azonos költségű terhelésmegosztásnak.

14.6.2

## Ellenőrző kvíz - Forgalomirányítás elmélete

Az űrlap teteje

1. A Cisco forgalomirányítók melyik beállítása teszi lehetővé a forgalom továbbítását, ha nincs meghatározva konkrét útvonal?

Az űrlap alja

Melyik három előnyt nyújtja a statikus forgalomirányítás? (Három jó válasz van.)

Melyik két feladatot látják el az irányító protokollok? (Két jó válasz van.)

Mi az előnye a dinamikus irányítóprotokolloknak a statikus forgalomirányítással szemben?

Az irányítótábla melyik értéke jelöli a megbízhatóságot, amely alapján a router meghatározza, hogy melyik útvonalat kell elhelyezni a routing táblázatba, ha több útvonal is létezik ugyanahhoz a célhálózathoz?

Melyik csomagtovábbítási módszert használja a router a kapcsolási döntések meghozatalához, ha továbbítási információs bázist és szomszédsági táblát használ?

Milyen típusú útvonalat használnának egy határponti (border) routeren, hogy a cégen belüli eszközök hozzáférhessenek az internethez?

Mi a router két funkciója? (Két jó válasz van.)

Amikor egy forgalomirányító egy adott célhálózathoz több útvonalat tanul meg ugyanazon forgalomirányító protokoll által, melyik tényező alapján fogja kiválasztani a legjobb útvonalat a csomagok továbbításához?

Melyik két forrás kód jelenik meg automatikusan az irányítótáblában, amikor egy router interfész IP-címet kap és aktiváljuk? (Két jó válasz van.)

Az **show ip route** parancs kimenete a következő bejegyzést tartalmazza: S 10.2.0.0 [1/0] via 172.16.2.2.

Milyen értéket jelez az 1 [1/0] részében? a kimenet

Melyik statikus útvonal hoz létre végső átjárót?

Melyik a két gyakori statikus útvonal típus az irányítótáblában? (Két jó válasz van.)

Mi a két oka annak, hogy a rendszergazda a dinamikus helyett a statikus forgalomirányítást választja? (Két jó válasz van.)

Milyen címet és előtag hosszt használunk IPv6 alapértelmezett statikus útvonal konfigurálásakor?

[14.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Static and Dynamic Routing](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. Bevezetés

# Bevezetés

15.0.1

## Miért fontos ez a fejezet?

Üdvözöljük az IP statikus routing fejezetben!

Annyiféle módon lehet az IP-csomagokat dinamikusan irányítani, elgondolkodtató, hogy miért vesződne bárki statikus útvonalak manuális konfigurálásával. Olyan, mintha kézzel mosnánk a ruháinkat, miközben egy tökéletesen működő mosógépünk is van. De vannak olyan ruhák, amelyeket nem lehet géppel mosni. Másoknak jót tesz, ha kézzel mossák őket. Egy kicsit hasonlít a hálózatokhoz. Mint kiderült, sok olyan helyzet van, amikor a kézzel beállított statikus útvonal a legjobb megoldás.

A statikus útvonalaknak különböző típusai vannak, mindegyik egy-egy tipikus hálózati probléma megoldására vagy elkerülésére jó. Számos hálózat dinamikus és statikus útvonalakat is használ, így a rendszergazdáknak ismerniük kell a statikus útvonalak konfigurálását, ellenőrzését és hibaelhárítását is. Aki ezt a tananyagot tanulja, valószínűleg hálózati rendszergazda szeretne lenni, tehát tovább mélyítjük adminisztrátori tudásunkat. Ennek a fejezetnek az anyagát sokat fogjuk alkalmazni a későbbiekben! Mivel a fejezet statikus útvonalak konfigurálásáról szól, több parancsszimulátort, Packet Tracer feladatot és laborgyakorlatot is találunk benne.

15.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe** : IP statikus útválasztás

**Modul célja** : Az IPv4 és IPv6 statikus útvonalak konfigurálása.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Statikus útvonalak** | Ismertesse a statikus útvonalak parancs szintaxisát. |
| **IP statikus útvonalak** | Állítsa be az IPv4 és IPv6 statikus útvonalakat. |
| **Állítsa be az alapértelmezett statikus IP-útvonalakat** | Konfigurálja az IPv4 és IPv6 alapértelmezett statikus útvonalait. |
| **Lebegő statikus útvonalak** | Állítson be egy lebegő statikus útvonalat a tartalék kapcsolat biztosításához. |
| **Statikus állomás útvonalak konfigurálása** | Állítson be olyan IPv4 és IPv6 statikus gazdagépútvonalakat, amelyek a forgalmat egy adott gazdagépre irányítják. |

[14.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. Static Routes

# Static Routes

15.1.1

## A statikus útvonalak típusai

Statikus útvonalakat gyakran használnak különféle hálózatokban. Még akkor is, ha dinamikus routing protokollt is használnak. Például, egy szervezet használhat alapértelmezett statikus útvonalat a szolgáltató irányába, majd ezt az útvonalat más vállalati routerek felé hirdetheti dinamikus routing protokoll használatával.

Statikus útvonalak konfigurálhatók IPv4 és IPv6 esetén egyaránt. Mindkét protokoll támogatja a következő statikus útvonal fajtákat:

* Hagyományos statikus útvonal
* Alapértelmezett statikus útvonal
* Lebegő statikus útvonal
* Összevont statikus útvonal

A statikus útvonalak konfigurálására az **ip route** és az **ipv6 route** globális konfigurációs parancsok használhatók.

15.1.2

## A következő ugrás beállítása

Statikus útvonal konfigurálásakor a következő ugrás megadható IP-címmel, kimenő interfésszel vagy mindkettővel. A cél meghatározásától függően az alábbi három statikus útvonal típus egyike jön létre:

* **Következő ugrás útvonal** - Csak a következő ugrás IP-címe van megadva
* **Közvetlenül csatlakoztatott statikus útvonal** – Csak a router kilépési interfésze van megadva
* **Teljesen meghatározott statikus útvonal** – Meg van adva a következő ugrás IP-címe és a kilépési interfész

15.1.3

## IPv4 statikus útvonal parancs

Az IPv4 statikus útvonalakat a következő globális konfigurációs paranccsal konfiguráljuk:

Router(config)# **ip route** network-address subnet-mask { ip-address | exit-intf [ip-address]} [distance]

**Megjegyzés:** Vagy az ip-address , exit-intf vagy az ip-address és exit-intf paramétereket kell konfigurálni.

A táblázat bemutatja az **ip route** parancs paramétereit.

| ParameterDescriptionnetwork-addressA távoli hálózat cél IPv4 hálózati címét határozza meg, amelyet az útválasztási táblához kell hozzáadni.subnet-maskA távoli hálózat alhálózati maszkját azonosítja. Az alhálózati maszk módosítható hálózatok csoportjának összegzéséhez és egy összefoglaló statikus route.ip létrehozásához. -address Azonosítja a következő ugrású útválasztó IPv4-címét.Általában broadcast hálózatokhoz (pl. Ethernet) használják. Rekurzív statikus útvonalat hozhat létre, ahol az útválasztó további keresést hajt végre a kilépési interfész megtalálásához.exit-intfA csomagok továbbításához szükséges kilépési interfészt azonosítja. Közvetlenül csatlakoztatott statikus útvonalat hoz létre.Általában pont-pont konfigurációban használatos.exit-intf ip-address Teljesen meghatározott statikus útvonalat hoz létre, mert meghatározza a kilépési interfészt és a következő ugrású IPv4-címet.distance Opcionális parancsot, amellyel hozzá lehet rendelni adminisztratív távolság értéke 1 és 255 között. Jellemzően lebegő statikus útvonal konfigurálására használják olyan adminisztratív távolság beállításával, amely nagyobb, mint egy dinamikusan tanult útvonal. | |
| --- | --- |
| **Paraméter** | **Leírás** |
| hálózati cím | Annak a távoli hálózatnak az IPv4-hálózatcíme, amelyet a routing táblához szeretnénk hozzáadni. |
| alhálózati maszk | * A távoli hálózat alhálózati maszkja. * Az alhálózati maszk módosítható a hálózatok egy csoportjának összegzésére és egy összefoglaló statikus útvonal létrehozására. |
| IP-cím | * A következő ugrás (next-hop) router IPv4-címe. * Általában szórásos hálózatokban használjuk (pl. Ethernet). * Rekurzív statikus útvonal jön létre, ahol a routernek a kimenő interfész meghatározásához még egy keresést le kell futtatnia. |
| exit-intf | * A csomagok továbbításához használandó kimenő interfész. * Közvetlenül csatlakoztatott statikus útvonalat hoz létre. * Általában pont-pont hálózatokban használjuk. |
| exit-intf ip-cím | Teljesen meghatározott statikus útvonalat hoz létre, amikor a következő ugrás IP-címét interface and next-hop IPv4 address. |
| távolság | * Opcióként megadhatjuk az útvonal adminisztratív távolságát 1 és 255 közötti értékkel. * Általában lebegő statikus útvonal konfigurálásához használjuk, ilyenkor magasabb adminisztratív távolságot adunk meg, mint a dinamikusan megtanult útvonalé. |

15.1.4

## IPv6 statikus útvonal parancs

Az IPv6 statikus útvonalakat a következő globális konfigurációs paranccsal konfiguráljuk:

Router(config)# **ipv6 route** ipv6-prefix/prefix-length {ipv6-address | exit-intf [ipv6-address]} [distance]

A paraméterek többsége megegyezik az IPv4-parancsnál használtakkal.

A táblázat bemutatja az **ipv6 route** parancs paramétereit és leírását.

| ParameterDescriptionipv6-prefix Azonosítja a távoli hálózat cél IPv6 hálózati címét, amelyet az útválasztási táblához kell hozzáadni./prefix-lengthA távoli hálózat előtag hosszát határozza meg.ipv6-addressA következő ugrású útválasztó IPv6-címét jelöli. Jellemzően üzenetszórási hálózatokhoz használják (pl. Ethernet)Létrehozhat egy rekurzív statikus útvonalat, ahol az útválasztó további keresést végez a kilépési interfész megtalálásához.exit-intfA kilépési interfészt azonosítja a csomagok továbbításához.Közvetlenül csatlakoztatott statikus útvonalat hoz létre.Általában pont-pont konfigurációban használatos.exit -intf ipv6-address Teljesen meghatározott statikus útvonalat hoz létre, mert meghatározza a kilépési felületet és a következő ugrású IPv6 address.distance parancsot, amellyel beperelhető egy 1 és 255 közötti adminisztratív távolság érték hozzárendelése. Általában lebegő statikus útvonal konfigurálására használják beállítással adminisztratív távolság, amely nagyobb, mint egy dinamikusan tanult útvonal. | |
| --- | --- |
| **Paraméter** | **Leírás** |
| ipv6-előtag | Annak a távoli hálózatnak az IPv6-hálózatcíme, amelyet a routing táblához szeretnénk hozzáadni. |
| /előtag-hossz | A távoli hálózat előtagjának hossza. |
| ipv6-cím | * A következő ugrás router IPv6-címe. * Általában szórásos hálózatokban használjuk (pl. Ethernet). * Rekurzív statikus útvonal jön létre, ahol a routernek a kimenő interfész meghatározásához még egy keresést le kell futtatnia. |
| exit-intf | * A csomagok továbbításához használandó kimenő interfész. * Közvetlenül csatlakoztatott statikus útvonalat hoz létre. * Általában pont-pont hálózatokban használjuk. |
| exit-intf ipv6-cím | Teljesen meghatározott statikus útvonalat hoz létre, amikor a következő ugrás IP-címét és a kimenő interfészt is megadjuk. |
| távolság | * Opcióként megadhatjuk az útvonal adminisztratív távolságát 1 és 255 közötti értékkel. * Általában lebegő statikus útvonal konfigurálásához használjuk, ilyenkor magasabb adminisztratív távolságot adunk meg, mint a dinamikusan megtanult útvonalé. |

**MEGJEGYZÉS** : Az **ipv6 unicast-routing** globális konfigurációs paranccsal engedélyeznünk kell a router számára az IPv6-csomagok továbbítását.

15.1.5

## Dual-stack topológia

Az ábrán egy dual-stack topológia látható. Jelenleg sem IPv4 sem IPv6 statikus útvonalak nincsenek konfigurálva.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/242001:db8:acad:1::/64 172.16.2.0/242001:db8:acad:2::/64 192.168.1.0/242001:db8:cafe:1::/64 172.16.3.0/242001:db8:acad:3::/64 192.168.2.0/242001:db8:cafe:2::/64 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1

.1

15.1.6

## A kiinduló IPv4 routing táblák

A gombokra kattintva megnézhetjük a routerek IPv4 routing tábláját és a ping parancs kimeneteket. Figyeljük meg, hogy minden routernek csak a közvetlenül csatlakoztatott hálózatokhoz és a hozzárendelt helyi címekhez van bejegyzése a routing táblában.

**R1 IPv4 routing tábla**

R1# mutat ip útvonalat | begin Gateway Az utolsó lehetőség átjárója nincs beállítva 172.16.0.0/16 változóan alhálózatos, 4 alhálózat, 2 maszk C 172.16.2.0/24 közvetlenül kapcsolódik, Serial0/1/0 L 172.16.2.1/32 közvetlenül kapcsolódik, Serial0/ 1/0 C 172.16.3.0/24 közvetlenül csatlakozik, GigabitEthernet0/0/0 L 172.16.3.1/32 közvetlenül csatlakozik, GigabitEthernet0/0/0 R1#

15.1.7

## A kiinduló IPv6 routing táblák

A gombokra kattintva megnézhetjük a routerek IPv6 routing tábláját és a ping parancs kimeneteket. Figyeljük meg, hogy minden routernek csak a közvetlenül csatlakoztatott hálózatokhoz és a hozzárendelt helyi címekhez van bejegyzése a routing táblában.

**R1 IPv6 routing tábla**

R1# ipv6 útvonal megjelenítése | kezdődik CC 2001:DB8:ACAD:2::/64 [0/0] Serial0/1/0-n keresztül, közvetlenül L 2001:DB8:ACAD:2::1/128 [0/0] Serial0/1/ 0, fogadja a C 2001:DB8:ACAD:3::/64 [0/0] GigabitEthernet0/0/0-n keresztül, közvetlenül csatlakoztatva L 2001:DB8:ACAD:3::1/128 [0/0] GigabitEthernet0/-en keresztül 0/0, L FF00::/8 [0/0] fogadása Null0-n keresztül, R1# fogadása

15.1.8

## Tudáspróba - Statikus útvonalak

Az űrlap teteje

Ellenőrizze, hogy megértette-e a statikus útvonalakat, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. Which two methods can be used to identify the next hop in a static route? (Két jó válasz van.)

Az űrlap alja

Melyik IPv4 statikus útvonal állítás igaz?

Hogyan azonosítható a célhálózat egy statikus IPv6 útvonalon?

[15.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP statikus útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. IP statikus útvonalak konfigurálása

# IP statikus útvonalak konfigurálása

15.2.1

## Next-hop IPv4 statikus útvonal

A normál statikus útvonalak konfigurálásához szükséges parancsok kissé eltérnek az IPv4 és az IPv6 esetében. Ez a témakör bemutatja, hogyan konfiguráljunk következő ugrással megadott, közvetlenül csatlakoztatott és teljesen megadott statikus útvonalakat mind az IPv4, mind az IPv6 esetében.

Next-hop címmel megadott statikus útvonal esetében csak a következő ugrás IP-címe van meghatározva. A kimenő interfészt a router a next-hop címből határozza meg. A példában három next-hop IPv4 statikus útvonal van konfigurálva R1-en a következő ugrás (ami itt R2) megadásával.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:cafe:1::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64

2001:db8:acad:3::/64

A három távoli hálózat felé mutató IPv4 statikus útvonal létrehozásának parancsai az R1-en a következők:

R1(config)# **ip route 172.16.1.0 255.255.255.0 172.16.2.2**

R1(config)# **ip route 192.168.1.0 255.255.255.0 172.16.2.2**

R1(config)# **ip route 192.168.2.0 255.255.255.0 172.16.2.2**

Az R1 routing táblája most már rendelkezik a három távoli IPv4-hálózathoz vezető útvonallal.

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

S 172.16.1.0/24 [1/0] via 172.16.2.2

C 172.16.2.0/24 is directly connected, Serial0/1/0

L 172.16.2.1/32 is directly connected, Serial0/1/0

C 172.16.3.0/24 is directly connected, GigabitEthernet0/0/0

L 172.16.3.1/32 is directly connected, GigabitEthernet0/0/0

S 192.168.1.0/24 [1/0] via 172.16.2.2

S 192.168.2.0/24 [1/0] via 172.16.2.2

R1#

15.2.2

## Next-hop IPv6 statikus útvonal

A három távoli hálózat felé mutató IPv6 statikus útvonalak parancsai R1-en a következők:

R1(config)# **ipv6 unicast-routing**

R1(config)# **ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:2::2**

R1(config)# **ipv6 route 2001:db8:cafe:1::/64 2001:db8:acad:2::2**

R1(config)# **ipv6 route 2001:db8:cafe:2::/64 2001:db8:acad:2::2**

R1 routing táblája most már rendelkezik a három távoli IPv6-hálózathoz vezető útvonalakkal.

R1# **show ipv6 route**

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations

ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy

a - Application

S 2001:DB8:ACAD:1::/64 [1/0]

via 2001:DB8:ACAD:2::2

C 2001:DB8:ACAD:2::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:2::1/128 [0/0]

via Serial0/1/0, receive

C 2001:DB8:ACAD:3::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:ACAD:3::1/128 [0/0]

via GigabitEthernet0/0/0, receive

S 2001:DB8:CAFE:1::/64 [1/0]

via 2001:DB8:ACAD:2::2

S 2001:DB8:CAFE:2::/64 [1/0]

via 2001:DB8:ACAD:2::2

L FF00::/8 [0/0]

via Null0, receive

15.2.3

## Közvetlenül csatlakozó IPv4 statikus útvonal

Statikus útvonal létrehozásakor a következő ugrás címe helyett lehetőség van a kimenő interfész megadására is. Az ábrán a korábbi topológia látható.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:cafe:1::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64

2001:db8:acad:3::/64

R1-en három közvetlenül csatlakozó IPv4 statikus útvonal van beállítva kimenő interfésszel.

R1(config)# **ip route 172.16.1.0 255.255.255.0 s0/1/0**

R1(config)# **ip route 192.168.1.0 255.255.255.0 s0/1/0**

R1(config)# **ip route 192.168.2.0 255.255.255.0 s0/1/0**

Az R1 routing táblája azt mutatja, hogy egy 192.168.2.0/24 hálózat felé küldött csomag esetében az R1 egyezést keres az irányítótáblában, majd ebből meghatározza, hogy a csomagot a Serial 0/1/0 interfészén kell kiküldeni.

**Note** : Using a next-hop address is generally recommended. Közvetlenül csatlakoztatott statikus útvonalakat pont-pont soros interfészekkel kell használni, mint ebben a példában.

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

S 172.16.1.0/24 is directly connected, Serial0/1/0

C 172.16.2.0/24 is directly connected, Serial0/1/0

L 172.16.2.1/32 is directly connected, Serial0/1/0

C 172.16.3.0/24 is directly connected, GigabitEthernet0/0/0

L 172.16.3.1/32 is directly connected, GigabitEthernet0/0/0

S 192.168.1.0/24 is directly connected, Serial0/1/0

S 192.168.2.0/24 is directly connected, Serial0/1/0

15.2.4

## Közvetlenül csatlakozó IPv6 statikus útvonal

A minta hálózatban R1-en három közvetlenül csatlakozó IPv6 statikus útvonal van beállítva kimenő interfésszel.

R1(config)# **ipv6 route 2001:db8:acad:1::/64 s0/1/0**

R1(config)# **ipv6 route 2001:db8:cafe:1::/64 s0/1/0**

R1(config)# **ipv6 route 2001:db8:cafe:2::/64 s0/1/0**

Az R1 IPv6 routing táblája azt mutatja, hogy egy 2001:db8:cafe:2::/64 hálózat felé küldött csomag esetében az R1 egyezést keres az irányítótáblájában, majd ebből meghatározza, hogy a csomagot a Serial 0/1/0 interfészén kell kiküldeni.

**Note** : Using a next-hop address is generally recommended. Közvetlenül csatlakoztatott statikus útvonalakat pont-pont soros interfészekkel kell használni, mint ebben a példában.

R1# **show ipv6 route**

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations

ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy

a - Application

S 2001:DB8:ACAD:1::/64 [1/0]

via Serial0/1/0, directly connected

C 2001:DB8:ACAD:2::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:2::1/128 [0/0]

via Serial0/1/0, receive

C 2001:DB8:ACAD:3::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:ACAD:3::1/128 [0/0]

via GigabitEthernet0/0/0, receive

S 2001:DB8:CAFE:1::/64 [1/0]

via Serial0/1/0, directly connected

S 2001:DB8:CAFE:2::/64 [1/0]

via Serial0/1/0, directly connected

L FF00::/8 [0/0]

via Null0, receive

R1#

15.2.5

## Teljesen meghatározott IPv4 statikus útvonal

Egy teljesen meghatározott statikus útvonal esetében mind a következő ugrás IP-címe, mind a kimenő interfész meg van adva. Akkor használjuk ezt a fajta megadási formát, ha a kimenő interfész többes hozzáférésű (multi-access) és emiatt a next-hop címet egyértelműen meg kell adnunk. Ilyenkor a next-hop címnek közvetlenül csatlakoznia kell a megadott kimenő interfészhez. A kimenő interfész megadása opcionális, de a következő ugrás címe kötelező paraméter.

Tegyük fel, hogy az R1 és az R2 közötti kapcsolat Ethernet, és az R1 router GigabitEthernet 0/0/1 interfésze csatlakozik ide (lásd ábra).

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy keresztirányú Ethernet kábel az R1s G0/0/1 interfésztől az R2s G0/0/1 interfészig és egy soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek .1 címet kapnak az összes LAN és WAN interfészhez, kivéve az R2s interfészek mindkét csatlakozását, amelyek a többi útválasztóhoz csatlakoznak. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1-et veszik a hivatkozásnak. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1 link-local címe FE80::1 az interfészeken, az R2 pedig FE80::2 az interfészeken. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti Ethernet IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 G0/0/1 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 G0/0/1 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:cafe:1::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64 2001:db8:acad:3::/64 fe80::2

fe80::1

A különbség egy többes hozzáférésű Ethernet és egy pont-pont soros hálózat között az, hogy pont-pont hálózat esetében csak egyetlen további eszköz van a hálózaton, mégpedig az összeköttetés másik végén lévő router. Ethernet esetén azonban különböző eszközök, köztük állomások és akár routerek is osztozhatnak ugyanazon a többes hozzáférésű hálózaton.

Ethernet kimenő interfész esetén ajánlott a next-hop statikus útvonalak használata. Teljesen meghatározott statikus útvonalat is használhatunk, amely tartalmazza mind a kimenő interfészt, mind a következő ugrás címet.

R1(config)# **ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2**

R1(config)# **ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2**

R1(config)# **ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2**

A csomagok R2 felé történő továbbításakor a kimenő interfész a GigabitEthernet 0/0/1, a következő ugrás IPv4-címe pedig 172.16.2.2, amint az R1 **show ip route** parancskimenetéből is látszik.

R1# **show ip route | begin Gateway**

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

S 172.16.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1

C 172.16.2.0/24 is directly connected, GigabitEthernet0/0/1

L 172.16.2.1/32 is directly connected, GigabitEthernet0/0/1

C 172.16.3.0/24 is directly connected, GigabitEthernet0/0/0

L 172.16.3.1/32 is directly connected, GigabitEthernet0/0/0

S 192.168.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1

S 192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1

15.2.6

## Teljesen meghatározott IPv6 statikus útvonal

Egy teljesen meghatározott IPv6 statikus útvonal esetében mind a next-hop IP-cím, mind a kimenő interfész meg van adva. IPv6-nál van olyan eset, amikor kötelező teljesen meghatározott útvonalat használnunk. Ha az IPv6 statikus útvonala IPv6 link-local címet tartalmaz next-hop címként, akkor teljesen meghatározott útvonalat kell használnunk. Az ábrán egy ilyen teljesen meghatározott IPv6 statikus útvonal látható, ahol a következő ugrás címe egy IPv6 link-local cím.

A grafika egy egyszerű hálózatot jelenít meg két routerrel, az R1 a bal oldalon és az R2 a jobb oldalon.   
Az útválasztók soros kábellel vannak összekötve; mindkettő az S0/1/0 interfészt használja. Minden útválasztónak van egy LAN-ja, amelyen nem jelennek meg konkrét berendezések. Az R1-en lévő LAN IPv6-címe 2001:db8:acad:3::/64, az R2-n lévő LAN IPv6-címe pedig 2001:db8:acad:1::/64. A soros hivatkozás címe 2001:db8:acad:2::/64, az R1 a ::1-et és az FE80::1-et, az R2 pedig a ::2-t és az FE80::2-t használja. A soros hivatkozás alatt egy narancssárga mező található, benne az IPv6 Link-Local Addresses utasítással. A mező mindkét végén két narancssárga nyíl található, amelyek mindkét útválasztón a soros interfészen található link-local címre mutatnak.

fe80::1 fe80::2 :1 S0/1/0 2001:db8:acad:3::/64 2001:db8:acad:1::/64 2001:db8:acad:2::/64 S0/1/0 :2 R1

R2

IPv6 Link-helyi címek

R1(config)# **ipv6 route 2001:db8:acad:1::/64 fe80::2**

%Interface has to be specified for a link-local nexthop

R1(config)# **ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2**

Az ábrán egy teljesen meghatározott IPv6 statikus útvonal létrehozása látható, ahol a next-hop cím az R2 link-local címe. Figyeljük meg az IOS-hibaüzenetet, amely szerint a kimenő interfészt is meg kell adni.

Ebben az esetben azért van szükség egy teljesen meghatározott statikus útvonalra, mert az IPv6 link-local címek nem szerepelnek a router IPv6-irányítótáblájában. A link-local címek csak egy adott összeköttetésen vagy hálózaton egyediek. Egy link-local címmel megadott next-hop cím szerepelhet több, a router-hez csatlakozó hálózatban is, így mindenképpen szükséges a kimenő interfész megadása.

A következő ábrán az útvonal bejegyzése látható az IPv6 routing táblában. Figyeljük meg, hogy mind a next-hop link-local cím, mind pedig a kimenő interfész szerepel benne.

R1# **show ipv6 route static | begin 2001:db8:acad:1::/64**

S 2001:DB8:ACAD:1::/64 [1/0]

via FE80::2, Seria0/1/0

15.2.7

## Statikus útvonalak ellenőrzése

A **show ip route**, **show ipv6 route**, **ping** és **traceroute** mellett a statikus útvonalak ellenőrzésére használatos parancsok a következők:

* \*\*show ip route static
* **show ip route** hálózat
* \*\*show running-config | section ip route

IPv6 esetén cseréljük az **ip** kulcsszót **ipv6**-ra.

A parancsok áttekintésekor a következő topológiát használjuk.

The graphic shows a network of three routers. The topology has R1 is at the bottom left, R2 is at the middle top, and R3 is at the bottom right. There is a serial cable from R1s S0/1/0 interface to R2s S0/1/0 interface and another serial cable from R2s S0/1/1 interface to R3s S0/1/1 interface. All three LANs are using the G0/0/0 interface of their router. There is a switch connected to the router and a PC connected to the switch. PC1 is on the LAN for R1, PC2 is on the LAN for R2, and PC3 is on the LAN for R3. Router interfaces will be given .1 address for all LAN and WAN interfaces, except for both serial (WAN) interfaces on R2. These interfaces on R2 are given .2 since .1 is taken the WAN link. None the switches or the PCs were assigned IP addresses. The addressing on the LAN on R1 has the IPv4 address of 172.16.3.0/24 and the IPv6 addressing of 2001:db8:acad:3::/64. The WAN between R1 and R2 has the IPv4 address of 172.16.2.0/24 and the IPv6 addressing of 2001:db8:acad:2::/64. The addressing on the LAN on R2 has the IPv4 address of 172.16.1.0/24 and the IPv6 addressing of 2001:db8:acad:1::/64. The WAN between R2 and R3 has the IPv4 address of 192.168.1.0/24 and the IPv6 addressing of 2001:db8:cafe:1::/64. The addressing on the LAN on R3 has the IPv4 address of 192.168.2.0/24 and the IPv6 addressing of 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:cafe:1::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64

2001:db8:acad:3::/64

Kattintsunk a gombokra az IPv4 és az IPv6 statikus útvonalakra vonatkozó parancsok kimeneteinek megtekintéséhez!

A kimenet csak az IPv4 statikus útvonalakat jeleníti meg a routing táblából. Figyeljük meg, hogy a szűrő hatására a routing kódok kimaradnak a megjelenítésből.

R1# ip útvonal statikus | begin Gateway A végső átjáró nincs beállítva 172.16.0.0/16 változóan alhálózatos, 5 alhálózat, 2 maszk S 172.16.1.0/24 [1/0] via 172.16.2.2 S 192.168.1.0/24 via [1/0] 172.16.2.2 S 192.168.2.0/24 [1/0] keresztül 172.16.2.2 R1#

15.2.8

## Parancsszimulátor - Statikus útvonalak beállítása

Konfiguráljuk a statikus útvonalakat a megadott követelmények alapján.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy keresztirányú Ethernet kábel az R1s G0/0/1 interfésztől az R2s G0/0/1 interfészig és egy soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek .1 címet kapnak az összes LAN és WAN interfészhez, kivéve az R2s interfészek mindkét csatlakozását, amelyek a többi útválasztóhoz csatlakoznak. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1-et veszik a hivatkozásnak. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1 link-local címe FE80::1 az interfészeken, az R2 pedig FE80::2 az interfészeken. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti Ethernet IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 G0/0/1 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 G0/0/1 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:cafe:1::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64 2001:db8:acad:3::/64 fe80::2

fe80::1

Configure an IPv4 next-hop static route on R2 to the 192.168.2.0/24 network using the next-hop address 192.168.1.1.

R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1

Configure a fully specified IPv4 static route on R2 to the 172.16.3.0/24 network using the exit interface/next-hop pair: **g0/0/1 172.16.2.1**

R2(config)#ip route 172.16.3.0 255.255.255.0 g0/0/1 172.16.2.1

Configure an IPv6 next-hop static route on R2 to the 2001:db8:cafe:2::/64 network using the next-hop address 2001:db8:cafe:1::1.

R2(config)#ipv6 route 2001:db8:cafe:2::/64 2001:db8:cafe:1::1

Configure a fully specified IPv6 static route on R2 to the 2001:db8:acad:3::/64 network using the exit interface/next-hop pair: **g0/0/1 / fe80::1**

R2(config)#ipv6 route 2001:db8:acad:3::/64 g0/0/1 fe80::1

Exit configuration mode and issue the command to display only the IPv4 static routes in the routing table of R2.

R2(config)#exit

\*Sep 18 21:44:32.910: %SYS-5-CONFIG\_I: Configured from console by console

R2#show ip route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

S 172.16.3.0/24 [1/0] via 172.16.2.1, GigabitEthernet0/0/1

S 192.168.2.0/24 [1/0] via 192.168.1.1

Issue the command to display only the IPv6 static routes in the routing table of R2.

R2#show ipv6 route static

IPv6 Routing Table - default - 9 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Application

S 2001:DB8:ACAD:3::/64 [1/0]

via FE80::1, GigabitEthernet0/0/1

S 2001:DB8:CAFE:2::/64 [1/0]

via 2001:DB8:CAFE:1::1

==============================================================

**You are now logged into R3:**

Configure a directly connected IPv4 static route on R3 to the 172.16.3.0/24 network using exit interface S0/1/1.

R3(config)#ip route 172.16.3.0 255.255.255.0 s0/1/1

Configure a directly connected IPv4 static route on R3 to the 172.16.1.0/24 network using exit interface S0/1/1.

R3(config)#ip route 172.16.1.0 255.255.255.0 s0/1/1

Configure a directly connected IPv4 static route on R3 to the 172.16.2.0/24 network using exit interface S0/1/1.

R3(config)#ip route 172.16.2.0 255.255.255.0 s0/1/1

Configure a directly connected IPv6 static route on R3 to the 2001:db8:acad:1::/64 network using exit interface S0/1/1.

R3(config)#ipv6 route 2001:db8:acad:1::/64 s0/1/1

Configure a directly connected IPv6 static route on R3 to the 2001:db8:acad:3::/64 network using exit interface S0/1/1.

R3(config)#ipv6 route 2001:db8:acad:3::/64 s0/1/1

Configure a directly connected IPv6 static route on R3 to the 2001:db8:acad:2::/64 network using exit interface S0/1/1.

R3(config)#ipv6 route 2001:db8:acad:2::/64 s0/1/1

Exit configuration mode and issue the command to display only the IPv4 static routes in the routing table of R3.

R3(config)#exit

Sep 18 21:47:57.894: %SYS-5-CONFIG\_I: Configured from console by console

R3#show ip route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

S 172.16.1.0 is directly connected, Serial0/1/1

S 172.16.2.0 is directly connected, Serial0/1/1

S 172.16.3.0 is directly connected, Serial0/1/1

Issue the command to display only the IPv6 static routes in the routing table of R3.

R3#show ipv6 route static

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Application

S 2001:DB8:ACAD:1::/64 [1/0]

via Serial0/1/1, directly connected

S 2001:DB8:ACAD:2::/64 [1/0]

via Serial0/1/1, directly connected

S 2001:DB8:ACAD:3::/64 [1/0]

via Serial0/1/1, directly connected

You have successfully configured and verified IPv4 and IPv6 static routes.

[15.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP alapértelmezett statikus útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. IP alapértelmezett statikus útvonalak konfigurálása

# IP alapértelmezett statikus útvonalak konfigurálása

15.3.1

## Alapértelmezett statikus útvonal

Ez a témakör bemutatja az IPv4 és az IPv6 alapértelmezett útvonalak konfigurálását. Azt is elmagyarázza, hogy mikor használunk alapértelmezett útvonalakat. Az alapértelmezett útvonal egy olyan statikus útvonal, amely minden csomagra illeszkedik. A router nem tárol külön-külön útvonalakat a világ összes hálózatához a routing táblában, helyette egyetlen alapértelmezett útvonalat használ, amely az irányítótáblában nem szereplő hálózatokat jelöli.

A routerek vagy helyben konfigurált, vagy dinamikus irányító protokoll által megtanult alapértelmezett útvonalakat alkalmaznak. Az alapértelmezett útvonal és a cél IP-cím közötti egyezéshez nem szükséges a bal szélső biteket azonos értéke. Ezeket az útvonalakat abban az esetben használják a routerek, ha a routing táblában egyetlen útvonal sem felelt meg a csomag cél IP-címének. Más szóval, ha a router nem talál jobb egyezést, akkor az alapértelmezett útvonalat használja végső átjáróként (Gateway of Last Resort).

Akkor használunk alapértelmezett útvonalat, ha a hálózatunk szélső (edge, perem-) routerét konfiguráljuk, amely a szolgáltató hálózatához csatlakozik, vagy ha a routernek csak egyetlen felfelé irányú szomszédja van (stub router).

Az ábrán egy tipikus eset látható az alapértelmezett statikus útvonal használatára.

Az ábrán két router látható, az R1 a bal alsó sarokban, a jobb felső sarokban pedig soros kapcsolat található az R2-vel. Mindkét útválasztó S0/1/0 interfészt használ. Az R2 egy felhőhöz csatlakozik, amelynek közepén a Network felirat olvasható. Az R1 egy S1 kapcsolóval rendelkező LAN-hoz csatlakozik, és az S1-hez csatlakoztatott PC1 feliratú PC. R1 G0/0/0-t használ a LAN-hoz; amelynek IPv4-címe 172.16.3.0/24. A soros linken a 172.16.2.0/24 IPv4-cím szerepel. A LAN körül sárga mező látható. A LAN mező felett a következő felirat látható: Stub Network narancssárga mezőben, és egy nyíllal a LAN-ra mutat. A LAN alatt a következő szavak láthatók: Stub Router egy másik narancssárga mezőben, és az R1-re mutat. A diagram alatt a következő kijelentés található: R1-nek csak a közvetlenül kapcsolódó hálózatokról kell tudnia. Az összes többi hálózatnál használhat egy alapértelmezett statikus útvonalat, amely R2-re mutat.

PC1 S1 R1 R2 G0/0/0 S0/1/0 172.16.2.0/24 172.16.3.0/24

S0/1/0

Stub Network Stub Router Hálózat

Az R1-nek csak a közvetlenül csatlakoztatott hálózatokról kell tudnia. A többi hálózat felé egy alapértelmezett statikus útvonalat használ, amely az R2 felé mutat.

**IPv4 Default Static Route**

Az alapértelmezett statikus útvonal parancsának szintaxisa hasonló bármely más statikus útvonaléhoz, a különbség csak annyi, hogy a hálózat cím **0.0.0.0** és az alhálózati maszk **0.0.0.0** . A 0.0.0.0 0.0.0.0 minden hálózattal megegyezik.

**Megjegyzés** : Az IPv4 alapértelmezett statikus útvonalát általában négynulla útvonalnak nevezik.

Az alapértelmezett IPv4 statikus útvonal parancsának szintaxisa:

Router(config)# **ip route 0.0.0.0 0.0.0.0** {ip-address | exit-intf}

**IPv6 alapértelmezett statikus útvonal**

Az alapértelmezett IPv6 statikus útvonal parancsának szintaxisa hasonló bármely más statikus útvonaléhoz, a különbség csak annyi, hogy az ipv6-előtag/előtag-hossz **::/0** , ami minden útvonalra ráillik.

Az alapértelmezett IPv6 statikus útvonal parancsának szintaxisa:

Router(config)# **ipv6 route ::/0** {ipv6-address | exit-intf}

15.3.2

## Alapértelmezett statikus útvonal létrehozása

Az ábrán levő R1 routeren beállíthatnánk három statikus útvonalat, egyet-egyet a topológia távoli három hálózatához. Az R1 azonban egy véghálózati (stub) router, mert csak R2-höz csatlakozik. Emiatt hatékonyabb, ha egy alapértelmezett statikus útvonalat definiálunk rajta.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1DCE S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 DCE .1 .1 .2 .2 .1 .1 .1 2001:db8:cafe:1::/64 2001:db8:cafe:2::/64 2001:db8:acad:3::/64 2001:db8:acad:1::/64

2001:db8:acad:2::/64

Az ábrán az R1 routeren alapértelmezett IPv4 statikus útvonalat konfiguráltak. Ezzel a beállítással minden olyan csomag, ami nem egyezik egyetlen más routing tábla bejegyzéssel sem, az R2 router 172.16.2.2 IP-címére kerül továbbításra.

R1(config)# **ip route 0.0.0.0 0.0.0.0 172.16.2.2**

Az IPv6 alapértelmezett statikus útvonal hasonló módon van konfigurálva. Ezzel a beállítással minden olyan csomag, ami nem egyezik egyetlen más IPv6 routing tábla bejegyzéssel sem, az R2 router 2001:db8:acad:2::2 címére kerül továbbításra.

R1(config)# **ipv6 route ::/0 2001:db8:acad:2::2**

15.3.3

## Alapértelmezett statikus útvonal ellenőrzése

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/0/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/0/0 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:1::/64 2001:db8:acad:2::/64 2001:db8:acad:3::/64 2001:db8:cafe:2::/64

2001:db8:cafe:1::/64

**Ellenőrizze az IPv4 alapértelmezett statikus útvonalát**

Az R1-en kiadott **show ip route static** parancs megmutatja a routing táblában levő statikus útvonalakat. Figyeljük meg a " " jelet a ) next to the route with code ‘S’. As displayed in the codes table in the **show ip route** kimenetében, ami az alapértelmezett statikus útvonalat jelöli, jelen esetben ez lesz a végső átjáró is (Gateway of Last Resort).

R1# **show ip route static**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP   
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area   
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2   
E1 - OSPF external type 1, E2 - OSPF external type 2   
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2   
ia - IS-IS inter area, \* - candidate default, U - per-user static route   
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP   
+ - replicated route, % - next hop override   
  
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 172.16.2.2

R1#

**Ellenőrizze az IPv6 alapértelmezett statikus útvonalát**

A példában a **show ipv6 route static** parancs kimenetét látjuk, amely arouting táblát jeleníti meg.

R1# **show ipv6 route static**

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations

ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy

a - Application

S ::/0 [1/0]

via 2001:DB8:ACAD:2::2

R1#

Figyeljük meg, hogy a statikus alapértelmezett útvonal konfigurációja a /0 maszkot használja az IPv4-hez és a ::/0 előtagot az IPv6-hoz. Emlékezzünk vissza, hogy a routing táblában az IPv4 alhálózati maszk és az IPv6 előtag hossz határozza meg, hogy hány bitnek kell egyeznie egy csomag cél IP-címe és a tábla útvonala között. A /0 maszk vagy ::/0 előtag hossz azt jelenti, hogy egyetlen bitnek sem kell megegyezni. Ha nincs pontosabb egyezés, az alapértelmezett statikus útvonal minden csomagra ráillik.

15.3.4

## Parancsszimulátor - Alapértelmezett statikus útvonalak beállítása

Konfiguráljunk és ellenőrizzünk az alapértelmezett statikus útvonalakat a követelményeknek megfelelően.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1 .1 2001:db8:acad:3::/64 2001:db8:acad:2::/64 2001:db8:acad:1::/64 2001:db8:cafe:1::/64

2001:db8:cafe:2::/64

Configure an IPv4 default static route on R3 to reach all remote networks. Use the next-hop IPv4 address argument.

R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2

Configure an IPv6 default static route on R3 to reach all remote networks. Use the next-hop IPv6 address argument.

R3(config)#ipv6 route ::/0 2001:db8:cafe:1::2

Exit configuration mode and display only the static routes in the IPv4 routing table.

R3(config)#exit

\*Sep 16 10:11:43.767: %SYS-5-CONFIG\_I: Configured from console by console

R3#show ip route static

Kódok: L - helyi, C - csatlakoztatott, S - statikus, R - RIP, M - mobil, B - BGP

D - EIGRP, EX - EIGRP külső, O - OSPF, IA - OSPF inter area

N1 – OSPF NSSA külső típus 1, N2 – OSPF NSSA külső típus 2

E1 - OSPF külső típus 1, E2 - OSPF külső típus 2

i - IS-IS, su - IS-IS összefoglaló, L1 - IS-IS szint-1, L2 - IS-IS szint-2

ia - IS-IS inter area, \* - jelölt alapértelmezett, U - felhasználónkénti statikus útvonal

o - ODR, P - periodikusan letöltött statikus útvonal, H - NHRP, l - LISP

a - alkalmazási útvonal

+ - replikált útvonal, % - következő ugrás felülírása

Az utolsó lehetőség átjárója nincs beállítva

Csak a statikus útvonalakat jelenítse meg az IPv6 útválasztási táblázatban.

R3# statikus ipv6 útvonal megjelenítése

IPv6 Routing Table – alapértelmezett – 1 bejegyzés

Kódok: C - Csatlakoztatott, L - Helyi, S - Statikus, U - Felhasználónkénti Statikus útvonal

B – BGP, R – RIP, H – NHRP, I1 – ISIS L1

I2 – ISIS L2, IA – ISIS interarea, IS – ISIS összefoglaló, D – EIGRP

EX - EIGRP külső, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Alkalmazás

Sikeresen konfigurálta és ellenőrizte az alapértelmezett statikus útvonalakat.

[15.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP statikus útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Configure Floating Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. Configure Floating Static Routes

# Állítsa be a lebegő statikus útvonalakat

15.4.1

## Lebegő statikus útvonalak

A fejezet többi témaköréhez hasonlóan most megtanuljuk IPv4 és IPv6 lebegő statikus útvonalak konfigurálását és használatát.

A statikus útvonalak egy másik típusa a lebegő statikus útvonal. Ezek olyan statikus útvonalak, amelyek egy elsődleges statikus vagy dinamikus útvonal kapcsolatának kiesése esetén tartalék útvonalakat biztosítanak. A lebegő statikus útvonalat a router csak az elsődleges útvonal kiesése esetén használja.

Az előbb említettek miatt a lebegő statikus útvonal nagyobb adminisztratív távolsággal rendelkezik, mint az elsődleges útvonal. Az adminisztratív távolság egy útvonal megbízhatóságát mutatja. Ha egy célállomáshoz több útvonal is vezet, akkor a router a legkisebb adminisztratív távolsággal rendelkező utat választja.

Példaként tegyük fel, hogy a rendszergazda lebegő statikus útvonalat szeretne konfigurálni egy EIGRP által megtanult útvonal tartalékaként. Ebben az esetben a lebegő statikus útvonalat az EIGRP-nél nagyobb adminisztratív távolsággal kell konfigurálni. Az EIGRP adminisztratív távolsága 90. Ha a lebegő statikus útvonalat 95-ös adminisztratív távolsággal konfiguráljuk, akkor a hálózat az EIGRP által dinamikusan megtanult útvonalat részesíti előnyben. Ha az EIGRP-útvonal kiesik, akkor helyette a lebegő statikus útvonal kerül használatba.

Az ábrán látható Branch router normál esetben minden forgalmat a privát WAN-hálózaton keresztül továbbít a HQ routerhez. A routerek az irányítási információikat EIGRP-protokoll segítségével cserélik ki. Egy 91 vagy nagyobb adminisztratív távolsággal létrehozott lebegő statikus útvonal tartalék útvonalként működik. Ha a privát WAN-kapcsolat kiesik és az EIGRP-útvonal eltűnik a routing táblából, akkor a lebegő statikus útvonal válik a legjobb úttá a HQ LAN eléréséhez.

Az ábrán két útválasztó látható, amelyek két soros kapcsolattal rendelkeznek két különböző felhőhöz, amelyek lehetővé teszik a kommunikációt az útválasztók között. A bal oldalon az első útválasztó neve Branch, a második útválasztó pedig HQ, és a jobb oldalon található. Mindkét útválasztó S0/1/0-t használ a felhőhöz való csatlakozáshoz a topológia tetején. Ennek a felhőnek a közepén a Private WAN szavak találhatók 172.16.1.0/30 címmel. Mindkét útválasztó S0/1/1-et használ az alsó felhőhöz való csatlakozáshoz. Ennek a felhőnek van egy ISP nevű útválasztója. A felhőben benne van az Internet szó. A Branch router kapcsolata az internetszolgáltatóval 209.165.200.240/29, .242 a Branch oldalon és .241 az ISP oldalon. A HQ router kapcsolata az internetszolgáltatóval a 209.165.200.224/29 .226 a HQ oldalon és .225 az ISP oldalon. Van egy lila ívelt vonal, amely a Branch útválasztótól a Private WAN felhőn át nyúlik, és a HQ útválasztóra mutat. Az ág oldalán egy körben az 1-es szám található. A Branch útválasztó lila mezőjében ez áll: Jobban szeretem elérni a HQ útválasztót a privát WAN-kapcsolaton keresztül. Alul van egy másik ívelt vonal, amely szürke, és a Branch útválasztótól indul az internetes felhő alatt, és a HQ útválasztóra mutat. A 2-es szám van egy körben az ág oldalán. A Branch útválasztó szürke mezőjében ez áll: Ha azonban ez a kapcsolat meghibásodik, tartalékként használhatok egy lebegő statikus útvonalat, amely az internethez csatlakozik. A topológiai diagram alján két számozott utasítás található: 1. A dinamikus útválasztással megtanult útvonalat részesítjük előnyben. és 2. Ha a dinamikus útvonal elérhetetlen, a lebegő statikus kerülő használatba.

172.16.1.0/30 209.165.200.224/29 209.165.200.240/29 .225 .241 S0/1/1.242 S0/1/0 .2 .1 S0/1/1.226 S0/1/0 1

2

Inkább a privát WAN-kapcsolaton keresztül érem el a HQ routert. Ha azonban ez a kapcsolat meghibásodik, tartalékként használhatok egy lebegő statikus útvonalat, amely az internethez csatlakozik. Fiók Privát WAN internet ISP HQ

1. A dinamikus útvonal az elsődleges.
2. Ha a dinamikus útvonal elérhetetlen, a lebegő statikus kerül használatba.

A statikus útvonalak adminisztratív távolsága alapértelmezés szerint 1, ezzel előnyt élveznek a dinamikus routing protokollok által megtanult útvonalakkal szemben. Példaként néhány gyakran használt belső routing protokoll adminisztratív távolsága:

* EIGRP = 90
* OSPF = 110
* IS-IS = 115

Egy statikus útvonal adminisztratív távolságának megnövelésével olyan útvonal hozható létre, amely bármely más statikus vagy dinamikusan megtanult útvonalnál kedvezőtlenebb. Ilyen módon a statikus útvonal "lebeg", és mindaddig nem kerül használatba, amíg egy kisebb adminisztratív távolságú útvonal aktív. Ha az előnyben részesített útvonal eltűnik, a lebegő statikus útvonal veszi át a helyét és a forgalom ezen az alternatív útvonalon keresztül továbbítható.

15.4.2

## IPv4 és IPv6 lebegő statikus útvonalak konfigurálása

Az IP lebegő statikus útvonalakhoz a **distance** paraméterrel adhatunk meg adminisztratív távolságot. Ha nincs megadva adminisztratív távolság, akkor az alapértelmezett érték 1.

Nézzük meg az ábrán szereplő topológiát és az R1-en kiadott **ip route** és **ipv6 route** parancsokat. Ebben a hálózatban az R1 alapértelmezett útvonala elsődlegesen az R2 felé mutat. Az R1 és az R3 közötti kapcsolat pedig tartalék útvonalként szolgál.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Az immár egy harmadik soros kapcsolat az R1s S0/1/1 interfész .1 címmel és az R3s S0/1/0 interfész .2 címmel. Ennek a hivatkozásnak az IPv4-címe 10.10.10.0/24, az IPv6-címe pedig a 2001:db8:feed:10::/64. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 .1 PC2 PC1 PC3 R2 .1 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 G0/0/0 G0/0/0 .2 .2 .1 .1 .1 S0/1/0 S0/1/1 10.10.10.0/24 .1 .2 R1 S0/1/0 S0/1/1 2001:db8:acad:1::/64 2001:db8:feed:10::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64 2001:db8:cafe:1::/64

2001:db8:acad:3::/64

R1(config)# **ip route 0.0.0.0 0.0.0.0 172.16.2.2**

R1(config)# **ip route 0.0.0.0 0.0.0.0 10.10.10.2 5**

R1(config)# **ipv6 route ::/0 2001:db8:acad:2::2**

R1(config)# **ipv6 route ::/0 2001:db8:feed:10::2 5**

Az R1-en az IPv4 és az IPv6 alapértelmezett statikus útvonalak az R2 felé mutatnak. Mivel adminisztratív távolságot nem adtak meg, így a statikus útvonalakhoz az alapértelmezett 1-es érték tartozik. Az R1-en IPv4 és IPv6 lebegő statikus útvonalak is létre lettek hozva, amelyek R3 felé mutatnak 5-ös adminisztratív távolsággal. Ez az érték nagyobb, mint az alapértelmezett 1-es érték, így az útvonal lebeg és nem kerül be a routing táblába mindaddig, amíg az elsődleges útvonal aktív.

A **show ip route** és a **show ipv6 route** kimenetből látszik, hogy jelenleg az R2 felé mutató alapértelmezett útvonalak vannak a routing táblában. Figyeljük meg, hogy az R3 felé mutató IPv4 lebegő statikus útvonal nincs közöttük.

R1# **show ip route static | begin Gateway**

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 172.16.2.2

R1# **show ipv6 route static | begin S :**

S ::/0 [1/0]

via 2001:DB8:ACAD:2::2

R1#

A **show run** parancs segítségével ellenőrizhetjük, hogy a lebegő statikus útvonalak jelen vannak a konfigurációban. A példában szereplő parancskimenet azt mutatja, hogy mindkét IPv6 statikus alapértelmezett útvonal benne van az aktív konfigurációban.

R1# **show run | include ipv6 route**

ipv6 route ::/0 2001:db8:feed:10::2 5

ipv6 route ::/0 2001:db8:acad:2::2

R1#

15.4.3

## Lebegő statikus útvonal működésének ellenőrzése

Mi történik az ábrán látható hálózatban, ha R2 meghibásodik?

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Az immár egy harmadik soros kapcsolat az R1s S0/1/1 interfész .1 címmel és az R3s S0/1/0 interfész .2 címmel. Ennek a hivatkozásnak az IPv4-címe 10.10.10.0/24, az IPv6-címe pedig a 2001:db8:feed:10::/64. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 .1 PC2 PC1 PC3 R2 .1 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 G0/0/0 G0/0/0 .2 .2 .1 .1 .1 S0/1/1 S0/1/0 S0/1/1 10.10.10.0/24 .1 .2 R1 S0/1/0 2001:db8:acad:1::/64 2001:db8:feed:10::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64 2001:db8:cafe:1::/64

2001:db8:acad:3::/64

A hibajelenséget úgy szimuláljuk, hogy R2 mindkét soros interfészét leállítjuk, amint láthatjuk is az ábrán.

R2(config)# **interface s0/1/0**

R2(config-if)# **shut**

\*Sep 18 23:36:27.000: %LINK-5-CHANGED: Interface Serial0/1/0, changed state to administratively down

\*Sep 18 23:36:28.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

R2(config-if)# **interface s0/1/1**

R2(config-if)# **shut**

\*Sep 18 23:36:41.598: %LINK-5-CHANGED: Interface Serial0/1/1, changed state to administratively down

\*Sep 18 23:36:42.598: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down

Figyeljük meg az R1 automatikus üzeneteit az R2 felé vezető soros interfész letiltott (down) állapotáról.

R1#

\*Sep 18 23:35:48.810: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to down

R1#

\*Sep 18 23:35:49.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

R1#

Ha megnézzük az R1 routing tábláit, akkor láthatjuk, hogy a lebegő statikus alapértelmezett útvonalakból alapértelmezett útvonalak lettek, amelyeknek következő ugrása az R3.

R1# **show ip route static | begin Gateway**

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

S\* 0.0.0.0/0 [5/0] via 10.10.10.2

R1# **show ipv6 route static | begin ::**

S ::/0 [5/0]

via 2001:DB8:FEED:10::2

R1#

15.4.4

## Parancsszimulátor - Lebegő statikus útvonalak beállítása

Konfiguráljunk és ellenőrizzünk a lebegő statikus útvonalakat a követelményeknek megfelelően.

A grafikon három útválasztóból álló hálózat látható. A topológiában az R1 a bal alsó sarokban, az R2 a középső felső, az R3 pedig a jobb alsó sarokban található. Van egy soros kábel az R1s S0/1/0 interfésztől az R2s S0/1/0 interfészig, és egy másik soros kábel az R2s S0/1/1 interfésztől az R3s S0/1/1 interfészig. Az immár egy harmadik soros kapcsolat az R1s S0/1/1 interfész .1 címmel és az R3s S0/1/0 interfész .2 címmel. Ennek a hivatkozásnak az IPv4-címe 10.10.10.0/24, az IPv6-címe pedig a 2001:db8:feed:10::/64. Mindhárom LAN az útválasztó G0/0/0 interfészét használja. Az útválasztóhoz egy kapcsoló, a kapcsolóhoz pedig egy PC csatlakozik. A PC1 az R1 LAN-on, a PC2 az R2 LAN-on, a PC3 pedig az R3 LAN-on van. Az útválasztó interfészek 0,1 címet kapnak minden LAN és WAN interfészhez, kivéve mindkét soros (WAN) interfészt az R2-n. Ezek az interfészek az R2-n .2-t kapnak, mivel a .1 a WAN kapcsolat. Egyik kapcsolóhoz vagy számítógéphez sem volt hozzárendelve IP-cím. Az R1-en lévő LAN-címzés IPv4-címe 172.16.3.0/24, IPv6-címe pedig 2001:db8:acad:3::/64. Az R1 és R2 közötti WAN IPv4-címe 172.16.2.0/24, IPv6-címe pedig 2001:db8:acad:2::/64. Az R2-n lévő LAN-címzés IPv4-címe 172.16.1.0/24, IPv6-címe pedig 2001:db8:acad:1::/64. Az R2 és R3 közötti WAN IPv4-címe 192.168.1.0/24, IPv6-címe pedig 2001:db8:cafe:1::/64. Az R3-on a LAN-címzés IPv4-címe 192.168.2.0/24, IPv6-címe pedig 2001:db8:cafe:2::/64.

R3 .1 PC2 PC1 PC3 R2 .1 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 G0/0/0 G0/0/0 .2 .2 .1 .1 .1 S0/1/1 S0/1/0 S0/1/1 10.10.10.0/24 .1 .2 R1 S0/1/0 2001:db8:acad:1::/64 2001:db8:feed:10::/64 2001:db8:acad:2::/64 2001:db8:cafe:2::/64 2001:db8:cafe:1::/64

2001:db8:acad:3::/64

Configure an IPv4 default static route on R3 using the next-hop address 192.168.1.2.

R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2

Configure an IPv4 default static route on R3 using the next-hop address 10.10.10.1 with an administrative distance of 5.

R3(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1 5

Configure an IPv6 default static route on R3 using the next-hop address 2001:db8:cafe:1::2

R3(config)#ipv6 route ::/0 2001:db8:cafe:1::2

Configure an IPv6 default route on R3 using the next-hop address 2001:db8:feed:10::1 with an administrative distance of 5.

R3(config)#ipv6 route ::/0 2001:db8:feed:10::1 5

Exit configuration mode and display the IPv4 routing table.

R3(config)#exit

\*Sep 20 02:55:53.327: %SYS-5-CONFIG\_I: Configured from console by console

R3#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 192.168.1.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.10.10.0/24 is directly connected, Serial0/1/0

L 10.10.10.2/32 is directly connected, Serial0/1/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Serial0/1/1

L 192.168.1.1/32 is directly connected, Serial0/1/1

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.2.1/32 is directly connected, GigabitEthernet0/0/0

Display the IPv6 routing table.

R3#show ipv6 route

IPv6 Routing Table - default - 8 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Application

S ::/0 [1/0]

via 2001:DB8:CAFE:1::2

C 2001:DB8:CAFE:1::/64 [0/0]

via Serial0/1/1, directly connected

L 2001:DB8:CAFE:1::1/128 [0/0]

via Serial0/1/1, receive

C 2001:DB8:CAFE:2::/64 [0/0]

via GigabitEthernet0/0/0, directly connected

L 2001:DB8:CAFE:2::1/128 [0/0]

via GigabitEthernet0/0/0, receive

C 2001:DB8:FEED:10::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:FEED:10::2/128 [0/0]

via Serial0/1/0, receive

L FF00::/8 [0/0]

via Null0, receive

You have successfully configured and verified floating static routes.

[15.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[IP alapértelmezett statikus útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Statikus állomás útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. Statikus állomás útvonalak konfigurálása

# Statikus állomás útvonalak konfigurálása

15.5.1

## Állomás útvonalak

Ez a témakör bemutatja, hogyan konfigurálunk és mikor használunk IPv4 és IPv6 statikus állomás útvonalakat.

Az állomás útvonal egy 32 bites maszkkal rendelkező IPv4-cím vagy 128 bites maszkkal rendelkező IPv6-cím. Állomás útvonalak három módon adhatók hozzá a routing táblához:

* Automatikusan belekerül, ha IP-címet állítunk be a routeren (lásd ábra)
* Statikus állomás útvonalként konfigurálva
* Az állomás útvonalat egyéb módszerekkel kapjuk meg (a későbbi tanfolyamokban tárgyaljuk)

15.5.2

## Automatikusan létrejött állomás útvonalak

A Cisco IOS automatikusan létrehoz egy állomás útvonalat, más néven helyi útvonalat, amikor egy interfész IP-címet kap a routeren. Az állomás útvonal segítségével a közvetlenül a routernek címzett (tehát nem továbbításra hozzá küldött) csomagok feldolgozása sokkal hatékonyabb. Ezt a közvetlenül csatlakoztatott útvonallal együtt jön létre, amelyet egy **C** betű jelöl és az interfész hálózatcímét tartalmazza.

Amikor egy router aktív interfészének IP-címet állítunk be, egy helyi állomás útvonal is bekerül a routing táblába. A helyi útvonalakat az **L** betű jelöli a routing táblában.

Tekintsük meg az ábrán látható minta topológiát.

Az ábra két útválasztó topológiáját mutatja. A bal oldalon az ISP router látható, amely soros kábellel csatlakozik a jobb oldali Branch routerhez. Az internetszolgáltatónak van kapcsolata a bal oldalon található Szerver nevű eszközzel. A szerver IPv4-címe 209.165.200.238/27 és IPv6-címe 2001:db8:acad:2::238/64. A két útválasztó közötti soros kapcsolat IPv6-címe 2001:db8:acad:1::/64, IPv4-címe pedig 198.51.100.0/30. Az internetszolgáltató router interfészéhez a .2, ::2 és fe80::2 IP-címek vannak hozzárendelve. A Branch útválasztóhoz a .1, ::1 és fe80::1 IP-címek vannak hozzárendelve.

209.165.200.238/272001:db8:acad:2::238/64 S0/1/0 fe80::2 2001:db8:acad:1:/64198.51.100.0/30 .2::2 .1::1

ISP

Kiszolgáló Branch

A Branch Serial0/1/0 interfészhez rendelt IP-címek: 198.51.100.1/30 és 2001:db8:acad:1::1/64. Az interfész helyi útvonalait az IOS hozza létre az IPv4 és IPv6 irányítótáblában, ahogy az ábrán is látható.

Branch# **show ip route | begin Gateway**

Gateway of last resort is not set

198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 198.51.100.0/30 is directly connected, Serial0/1/0

L 198.51.100.1/32 is directly connected, Serial0/1/0

Branch# **show ipv6 route | begin ::**

C 2001:DB8:ACAD:1::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via Serial0/1/0, receive

L FF00::/8 [0/0]

via Null0, receive

15.5.3

## Statikus állomás útvonalak

Egy állomás útvonal lehet manuálisan beállított statikus útvonal, amely egy adott céleszközre, például az ábrán látható kiszolgálóra irányítja a forgalmat. A statikus útvonal a cél IP-cím mellett 255.255.255.255 (/32) maszkot használja az IPv4 állomás útvonalakhoz, és /128-as előtag-hosszt az IPv6 állomás útvonalakhoz.

Az ábra két útválasztó topológiáját mutatja. A bal oldalon az ISP router látható, amely soros kábellel csatlakozik a jobb oldali Branch routerhez. Az internetszolgáltatónak van kapcsolata a bal oldalon található Szerver nevű eszközzel. A szerver IPv4-címe 209.165.200.238/27 és IPv6-címe 2001:db8:acad:2::238/64. A két útválasztó közötti soros kapcsolat IPv6-címe 2001:db8:acad:1::/64, IPv4-címe pedig 198.51.100.0/30. Az internetszolgáltató router interfészéhez a .2, ::2 és fe80::2 IP-címek vannak hozzárendelve. A Branch útválasztóhoz a .1, ::1 és fe80::1 IP-címek vannak hozzárendelve.

209.165.200.238/272001:db8:acad:2::238/64 .2::2 S0/1/0 fe80::2 2001:db8:acad:1::/64198.51.100.0/30 .1::1

ISP

Kiszolgáló Branch

15.5.4

## Statikus állomás útvonalak konfigurálása

A példa az IPv4 és IPv6 statikus állomásútvonal konfigurálását mutatja be a Branch routeren a kiszolgáló eléréséhez.

Branch(config)# **ip route 209.165.200.238 255.255.255.255 198.51.100.2**

Branch(config)# **ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2**

Branch(config)# **exit**

Branch#

15.5.5

## Statikus állomás útvonalak ellenőrzése

Az IPv4 és IPv6 routing táblákban láthatjuk, hogy az útvonalak aktívak.

Branch# **show ip route | begin Gateway**

Gateway of last resort is not set

198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 198.51.100.0/30 is directly connected, Serial0/1/0

L 198.51.100.1/32 is directly connected, Serial0/1/0

209.165.200.0/32 is subnetted, 1 subnets

S 209.165.200.238 [1/0] via 198.51.100.2

Branch# **show ipv6 route**

(Output omitted)

C 2001:DB8:ACAD:1::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via Serial0/1/0, receive

S 2001:DB8:ACAD:2::238/128 [1/0]

via 2001:DB8:ACAD:1::2

Branch#

15.5.6

## IPv6 statikus állomás útvonal konfigurálása link-local next-hop címmel

Az IPv6 statikus útvonalak esetén a next-hop cím lehet a szomszédos router link-local címe. Azonban link-local címek használata esetén kötelező megadni az interfész típusát és számát is (lásd ábra). Először eltávolítjuk az eredeti IPv6 statikus állomás útvonalat, majd egy teljesen meghatározott útvonalat konfigurálunk a szerver IPv6-címével és az ISP-router link-local címével.

Branch(config)# **no ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2**

Branch(config)# **ipv6 route 2001:db8:acad:2::238/128 serial 0/1/0 fe80::2**

Branch# show ipv6 route | begin ::

C 2001:DB8:ACAD:1::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via Serial0/1/0, receive

S 2001:DB8:ACAD:2::238/128 [1/0]

via FE80::2, Serial0/1/0

Branch#

15.5.7

## Parancsszimulátor - Statikus állomás útvonalak beállítása

Konfiguráljunk és ellenőrizzünk a statikus állomás útvonalakat a követelményeknek megfelelően.

Az ábra két útválasztó topológiáját mutatja. A bal oldalon az ISP router látható, amely soros kábellel csatlakozik a jobb oldali Branch routerhez. Az internetszolgáltatónak van kapcsolata a bal oldalon található Szerver nevű eszközzel. A szerver IPv4-címe 209.165.200.238/27 és IPv6-címe 2001:db8:acad:2::238/64. A két útválasztó közötti soros kapcsolat IPv6-címe 2001:db8:acad:1::/64, IPv4-címe pedig 198.51.100.0/30. Az internetszolgáltató router interfészéhez a .2, ::2 és fe80::2 IP-címek vannak hozzárendelve. A Branch útválasztóhoz a .1, ::1 és fe80::1 IP-címek vannak hozzárendelve.

209.165.200.238/272001:db8:acad:2::238/64 S0/1/0 fe80::2 2001:db8:acad:1::/64198.51.100.0/30 .2::2 .1::1

ISP

Kiszolgáló Branch

Display the routing tables on the Branch router.

* Issue the command to view the IPv4 routing table.
* Issue the command to view the IPv6 routing table.

Branch#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 198.51.100.0/30 is directly connected, Serial0/1/0

L 198.51.100.1/32 is directly connected, Serial0/1/0

Branch#show ipv6 route

IPv6 Routing Table - default - 3 entries

Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

B - BGP, R - RIP, H - NHRP, I1 - ISIS L1

I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP

EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination

NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Application

C 2001:DB8:ACAD:1::/64 [0/0]

via Serial0/1/0, directly connected

L 2001:DB8:ACAD:1::1/128 [0/0]

via Serial0/1/0, receive

L FF00::/8 [0/0]

via Null0, receive

Lépjen be a Globális konfigurációs módba a következők konfigurálásához: \* Statikus IPv4-útvonal a 209.165.200.238-as címen lévő gazdagéphez és egy **s0/1/0** kilépési interfész.

* Statikus IPv6-útvonal a 2001:db8:acad::2/128 címen lévő gazdagéphez és **s0/1/0** kilépési interfész.

**Note**: Be sure to use **s0/1/0** as the interface designation.

Branch#configure terminal

Branch(config)#ip route 209.165.200.238 255.255.255.255 s0/1/0

Branch(config)#ipv6 route 2001:db8:acad::2/128 s0/1/0

Exit configuration mode and display the IPv4 and IPv6 routing tables.

Branch(config)#exit

\*Sep 19 19:06:47.301: %SYS-5-CONFIG\_I: Configured from console by console

Branch#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks

C 198.51.100.0/30 is directly connected, Serial0/1/0

L 198.51.100.1/32 is directly connected, Serial0/1/0

209.165.200.0/32 is subnetted, 1 subnets

S 209.165.200.238 is directly connected, Serial0/1/0

Branch# ipv6 útvonalat mutat

IPv6 Routing Table - alapértelmezett - 4 bejegyzés

Kódok: C - Csatlakoztatott, L - Helyi, S - Statikus, U - Felhasználónkénti Statikus útvonal

B – BGP, R – RIP, H – NHRP, I1 – ISIS L1

I2 – ISIS L2, IA – ISIS interarea, IS – ISIS összefoglaló, D – EIGRP

EX - EIGRP külső, ND - ND alapértelmezett, NDp - ND előtag, DCE - Cél

NDr – Átirányítás, RL – RPL, O – OSPF Intra, OI – OSPF Inter

OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1

ON2 - OSPF NSSA ext 2, a - Alkalmazás

C 2001:DB8:ACAD:1::/64 [0/0]

Serial0/1/0-n keresztül, közvetlenül csatlakoztatva

L 2001:DB8:ACAD:1::1/128 [0/0]

Serial0/1/0-n keresztül, fogad

S 2001:DB8:ACAD:2::/128 [1/0]

Serial0/1/0-n keresztül, közvetlenül csatlakoztatva

L FF00::/8 [0/0]

Null0-n keresztül, fogad

Sikeresen konfigurálta a statikus gazdagép útvonalakat.

[15.4](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Configure Floating Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[15.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. IP statikus útválasztás
2. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

15.6.1

## Packet Tracer - IPv4 és IPv6 statikus és alapértelmezett útvonal beállítása

Ebben a Packet Tracer feladatban statikus, alapértelmezett és lebegő statikus útvonalakat állítunk be az IPv4- és az IPv6-protokoll számára.

[IPv4 és IPv6 statikus és alapértelmezett útvonalak konfigurálása](https://contenthub.netacad.com/courses/srwe-dl/_common/15.6.1-packet-tracer---configure-ipv4-and-ipv6-static-and-default-routes_hu-HU.pka)

15.6.2

## Laborgyakorlat - IPv4 és IPv6 statikus és alapértelmezett útvonal beállítása

A laborgyakorlat során az alábbi feladatokat végezzük el:

* Part 1: A hálózat felépítése és az eszközök alapbeállításainak megadása
* Part 2: IP- és IPv6-címzés konfigurálása és ellenőrzése az R1 és az R2 eszközökön.
* Part 3: Statikus és alapértelmezett IPv4-útvonal konfigurálása és ellenőrzése az R1 és az R2 eszközökön
* Part 4: Statikus és alapértelmezett IPv6-útvonal konfigurálása és ellenőrzése az R1 és az R2 eszközökön

15.6.3

## Miről tanultunk ebben a fejezetben?

**Statikus útvonalak**

Statikus útvonalak konfigurálhatók IPv4 és IPv6 esetén egyaránt. Mindkét protokoll támogatja a következő statikus útvonalakat: normál statikus útvonal, alapértelmezett statikus útvonal, lebegő statikus útvonal és összevont statikus útvonal. A statikus útvonalakat az ip route és az ipv6 route globális konfigurációs parancsok segítségével konfiguráljuk. Statikus útvonal konfigurálásakor a következő ugrás megadható IP-címmel, kimenő interfésszel vagy mindkettővel. A cél megadásának módja alapján a következő három statikus útvonal egyike jön létre: következő ugrással megadott (next-hop), közvetlenül csatlakoztatott és teljesen meghatározott. Az IPv4 statikus útvonalakat a következő globális konfigurációs paranccsal konfiguráljuk: **ip route** network-address subnet-mask { ip-address s | exit-intf \ [ ip=address ] }\ [ **distance** ] . Az IPv6 statikus útvonalakat a következő globális konfigurációs paranccsal konfiguráljuk: **ipv6 route** ipv6-prefix/prefix-length { ipv6-address | exit-intf \ [ ipv6-address ] }\ [ **distance** ] . Az IPv4 routing tábla megtekintésének parancsa: **show ip route** | **begin Gateway** . Az IPv6 routing tábla megtekintésének parancsa: **show ipv6 route** | **begin C.** .

**Állítsa be a statikus IP-útvonalakat**

Next-hop címmel megadott statikus útvonal esetében csak a következő ugrás IP-címe van meghatározva. A kimenő interfészt a router a next-hop címből határozza meg. Statikus útvonal létrehozásakor a következő ugrás címe helyett lehetőség van a kimenő interfész megadására is. Közvetlenül csatlakoztatott statikus útvonalakat pont-pont soros interfészekkel kell használni. Egy teljesen meghatározott statikus útvonal esetében mind a következő ugrás IP-címe, mind a kimenő interfész meg van adva. Akkor használjuk ezt a fajta megadási formát, ha a kimenő interfész többes hozzáférésű (multi-access) és emiatt a next-hop címet egyértelműen meg kell adnunk. Ilyenkor a next-hop címnek közvetlenül csatlakoznia kell a megadott kimenő interfészhez. Egy teljesen meghatározott IPv6 statikus útvonal esetében mind a következő ugrás IP-címe, mind a kimenő interfész meg van adva. A **show ip route** , a **show ipv6 route** , a **ping** és a **traceroute** parancsok mellett további hasznos parancsok a statikus útvonalak ellenőrzésére: **show ip route static** , **show ip route** hálózat , és **show running-config | section ip route** . IPv6 esetén cseréljük ki az "ip" kulcsszót "ipv6"-ra.

**Állítsa be az alapértelmezett statikus IP-útvonalakat**

Az alapértelmezett útvonal egy olyan statikus útvonal, amely minden csomagra illeszkedik. Az alapértelmezett útvonal és a cél IP-cím közötti egyezéshez nem szükséges a bal szélső biteket azonos értéke. Akkor használunk alapértelmezett útvonalat, ha a hálózatunk szélső (edge, perem-) routerét konfiguráljuk, amely a szolgáltató hálózatához csatlakozik, vagy ha a routernek csak egyetlen szomszédja van (stub router). Az alapértelmezett statikus útvonal parancsának szintaxisa hasonló bármely más statikus útvonaléhoz, a különbség csak annyi, hogy a hálózat cím 0.0.0.0 és az alhálózati maszk 0.0.0.0. A 0.0.0.0 0.0.0.0 minden hálózattal megegyezik. Az alapértelmezett IPv6 statikus útvonal parancsának szintaxisa hasonló bármely más statikus útvonaléhoz, a különbség csak annyi, hogy az ipv6-előtag/előtag-hossz ::/0 , ami minden útvonalra ráillik. Az IPv4 alapértelmezett statikus útvonal ellenőrzéséhez a **show ip route static** parancsot használjuk. IPV6 esetén pedig a **show ipv6 route static** parancsot.

**Állítsa be a lebegő statikus útvonalakat**

A lebegő statikus útvonalak olyan statikus útvonalak, amelyek egy elsődleges statikus vagy dinamikus útvonal kapcsolatának kiesése esetén tartalék útvonalakat biztosítanak. A lebegő statikus útvonalakat nagyobb adminisztratív távolsággal konfiguráljuk, mint az elsődleges útvonalat. A statikus útvonalak adminisztratív távolsága alapértelmezés szerint 1, ezzel előnyt élveznek a dinamikus routing protokollok által megtanult útvonalakkal szemben. Néhány gyakori belső routing protokoll adminisztratív távolsága: EIGRP = 90, OSPF = 110 és IS-IS = 115. Az IP lebegő statikus útvonalakhoz a **distance** paraméterrel adhatunk meg adminisztratív távolságot. Ha nincs megadva adminisztratív távolság, akkor az alapértelmezett érték 1. A **show ip route** és a **show ipv6 route** kimenetében nézhetjük meg a routing táblában levő alapértelmezett útvonalakat.

**Állítsa be a statikus gazdagép-útvonalakat**

Az állomás útvonal egy 32 bites maszkkal rendelkező IPv4-cím vagy 128 bites maszkkal rendelkező IPv6-cím. Háromféleképpen lehet állomás útvonalat hozzáadni a routing táblához: automatikusan bekerül, amikor egy IP-címet állítunk be a routeren, statikus állomás útvonalként konfiguráljuk, vagy automatikusan más módon, amelyeket ebben a fejezetben nem tárgyalunk. A Cisco IOS automatikusan létrehoz egy állomás útvonalat, más néven helyi útvonalat, amikor egy interfész IP-címet kap a routeren. Az állomás útvonal lehet manuálisan beállított statikus útvonal, amely egy adott céleszközre irányítja a forgalmat. IPv6 statikus útvonalak esetén a next-hop cím lehet a szomszédos router link-local címe, de ebben az esetben interfész típust és számot is meg kell adni. Először eltávolítjuk az eredeti IPv6 statikus állomás útvonalat, majd egy teljesen meghatározott útvonalat konfigurálunk a szerver IPv6-címével és az ISP-router link-local címével.

15.6.4

## Ellenőrző kvíz - IP statikus routing

Az űrlap teteje

1. A hálózati rendszergazda az **ip route 0.0.0.0 0.0.0.0 209.165.200.226** paranccsal konfigurálja az útválasztót. Mi a parancs célja?

Az űrlap alja

Milyen típusú statikus útvonal az, amelyet csak kimenő interfésszel adunk meg?

A network administrator uses the command **ip route 172.18.0.0 255.255.0.0 S0/0/1** to configure a floating static route on a router. Ez az útvonal tartalék útvonalként fog működni az EIGRP protokolltól megismert 172.18.0.0/16 hálózat eléréséhez. A konfiguráció után az EIGRP útvonal eltávolításra kerül az irányítótáblából annak ellenére, hogy az EIGRP továbbra is megfelelően működik. Miért nem úgy működik a statikus útvonal, ahogy elvárható volna?

Milyen statikus útvonalat állítunk be, amikor next-hop IP-címet és a kimenő interfészt is megadunk?

Mi a lebegő statikus útvonal helyes szintaxisa?

Melyik statikus útvonal utasítás jelent rekurzív IPv6 statikus útvonalat?

Egy hálózati rendszergazda olyan útvonalat konfigurál, amely a csomagokat egy adott webkiszolgálóra továbbítja. Milyen típusú útvonalat állít be?

Melyik parancs hoz létre egy működő IPv6 alapértelmezett útvonalat?

Melyik egy alapértelmezett statikus útvonal jellemzője?

Mi a célja a lebegő statikus útvonalnak?

Melyik IPv6 statikus útvonal szolgál tartalék útvonalként egy OSPF-en keresztül tanult dinamikus útvonalhoz?

Mely parancs vagy parancsok segítségével állapítható meg, hogy a HQ router konfigurációja a tervezettnek megfelelő-e?

**ip útvonal 0.0.0.0 0.0.0.0 soros 0/0/0 10   
ip útvonal 0.0.0.0 0.0.0.0 soros 0/1/0**

A statikus útvonalak melyik típusa használja a **ip route** globális konfigurációs parancs distance paraméterét?

Miért kell a lebegő statikus útvonal adminisztratív távolságát magasabbra állítani a routeren használt dinamikus routing protokoll értékénél?

Milyen hálózati cím és alhálózati maszk kombinációval lehet létrehozni olyan alapértelmezett statikus útvonalat, amely illeszkedik bármely IPv4-célcímre?

[15.5](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Statikus állomás útvonalak konfigurálása](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[16.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Troubleshoot Static and Default Routes
2. Bevezetés

# Bevezetés

16.0.1

## Miért fontos ez a fejezet?

Üdvözöljük a Statikus és alapértelmezett útvonalak hibaelhárítása fejezetben!

Gratulálunk! A Switching, Routing és Wireless Essentials v7.0 (SRWE) tanfolyam utolsó fejezetéhez érkeztünk! Ez a tanfolyam egyre növekvő hálózatunkban switch-ek, routerek, vezeték nélküli eszközök beüzemeléséhez szükséges mélyreható ismereteket adott át. Egész jó rendszergazdák kezdünk lenni!

De mi teszi a jó hálózati rendszergazdát nagyszerűvé? A hatékony hibaelhárítás képessége. A hálózati hibaelhárítás elsajátításának a legjobb módja egyszerű: csinálni kell... Ebben a fejezetben statikus és alapértelmezett útvonalak hibáival foglalkozunk. Lesz parancsszimulátor, Packet Tracer feladat és gyakorlati labor is, melyekben tovább fejlesztjük képességeinket. Kezdjük is el!

16.0.2

## Miről fogunk tanulni ebben a fejezetben?

**Modul címe** : Statikus és alapértelmezett útvonalak hibaelhárítása

**Modul célja** : A statikus és alapértelmezett útvonalkonfigurációk hibaelhárítása.

| Táblázat felirata | |
| --- | --- |
| **Témakör címe** | **Témakör célja** |
| **Csomagfeldolgozás statikus útvonalakkal** | Magyarázza el, hogyan dolgozza fel az útválasztó a csomagokat, ha statikus útvonal van konfigurálva. |
| **Hibaelhárítás az IPv4 statikus és alapértelmezett útvonal konfigurációjával** | A gyakori statikus és alapértelmezett útvonalkonfigurációs problémák elhárítása. |

[15.6](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[16.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Packet Processing with Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Troubleshoot Static and Default Routes
2. Packet Processing with Static Routes

# Csomagfeldolgozás statikus útvonalakkal

16.1.1

## Statikus útvonalak és csomagtovábbítás

Mielőtt a fejezet hibaelhárítással foglalkozó részébe belevágnánk, tekintsük át azt, hogyan történik a csomagok továbbítása statikus útvonalak használatával. Kattintsunk az ábra Lejátszás gombjára az animáció megtekintéséhez, amelyben PC1 egy csomagot küld PC3-nak.

Az ábra egy animáció, amely a 172.16.1.0/24 hálózatra kapcsolt PC2-t ábrázolja. A kapcsolót ezután a G0/0/0 Gigabit interfészen lévő útválasztóhoz (R2) csatlakozik, amelynek Gateway címe .1. Az R2-nek két soros S0/1/0 és S0/1/1 csatlakozója van, amelyek az S0/1/0 routerhez (R1) és az S0/1/1 csatlakozón lévő routerhez (R3) csatlakoznak. A hálózati cím R1-től R2-ig 172.16.2.0/14, R2-től R3-ig pedig 192.181.1.0/24. Az R2 soros csatlakozási címe .2, míg az R1 és R3 .1. Az R1 a G0/0/0 Gigabites interfészen keresztül csatlakozik egy 172.16.3.0/24-es hálózati kapcsolóhoz, amelyhez a PC1 csatlakozik. Az R3-nak Gigabites kapcsolata van a 192.168.2.0/24-es hálózaton lévő switch-hez, a PC3 pedig a switch-hez van csatlakoztatva.

Amint az animáción is követhető, a statikus útvonalakkal történő csomagtovábbítás lépései a következők:

1. A csomag megérkezik R1 GigabitEthernet 0/0/0 interfészére.
2. R1-nek nincs külön útvonala a cél hálózat, vagyis 192.168.2.0/24 felé. Ezért R1 az alapértelmezett statikus útvonalat használja.
3. R1 beágyazza a csomagot egy új keretbe. Mivel R2 felé a kapcsolat pont-pont jellegű, a második rétegbeli célcím csupa 1-es lesz.
4. A keret kimegy a 0/1/0-s Serial interfészen. A csomag megérkezik R2 Serial 0/1/0 interfészére.
5. R2 kicsomagolja a keretet és útvonalat keres a cél felé. R2-nek van a 192.168.2.0/24 hálózat felé vezető statikus útvonala a Serial 0/1/1 interfészén kifelé.
6. R2 beágyazza a csomagot egy új keretbe. Mivel R3 felé a kapcsolat pont-pont jellegű, a második rétegbeli célcím csupa 1-es lesz.
7. A keret kimegy a Serial 0/1/1 interfészen. A csomag megérkezik R3 Serial 0/1/1 interfészére.
8. R3 kicsomagolja a keretet és útvonalat keres a cél felé. R3-nak a 192.168.2.0/24 közvetlenül csatlakozó hálózat a GigabitEthernet 0/0/0 interfészén.
9. R3 bejegyzést keres az ARP-táblában a 192.168.2.10 IP-címhez, hogy megtalálja a PC3 2. rétegbeli MAC-címét. Ha nem talál bejegyzést, akkor egy ARP kérést küld ki a GigabitEthernet 0/0/0 interfészén, amire PC3 ARP-választ küld, benne a saját MAC-címével.
10. R3 beágyazza a csomagot egy új keretbe, amelyben a 2. rétegbeli forráscím a GigabitEthernet 0/0/0 interfész MAC-címe, a célcím pedig PC3 MAC-címe.
11. A keret kimegy a 0/0/0-s GigabitEthernet interfészen. A csomag megérkezik PC3 hálózati kártyájára.

16.1.2

## Tudáspróba - Csomagfeldoltozás statikus útvonalakkal

A kiállítás a 172.16.1.0/24 hálózatra kapcsolt PC2-t ábrázolja. A kapcsolót ezután a G0/0/0 Gigabit interfészen lévő útválasztóhoz (R2) csatlakozik, amelynek Gateway címe .1. Az R2-nek két soros S0/1/0 és S0/1/1 csatlakozója van, amelyek az S0/1/0 routerhez (R1) és az S0/1/1 csatlakozón lévő routerhez (R3) csatlakoznak. A hálózati cím R1-től R2-ig 172.16.2.0/14, R2-től R3-ig pedig 192.181.1.0/24. Az R2 soros csatlakozási címe .2, míg az R1 és R3 .1. Az R1 a G0/0/0 Gigabites interfészen keresztül csatlakozik egy 172.16.3.0/24-es hálózati kapcsolóhoz, amelyhez a PC1 csatlakozik. Az R3-nak Gigabites kapcsolata van a 192.168.2.0/24-es hálózaton lévő switch-hez, a PC3 pedig a switch-hez van csatlakoztatva.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1

.1

Az űrlap teteje

Ellenőrizze, hogy megértette-e a statikus útvonalakkal végzett csomagfeldolgozást, és válassza ki a LEGJOBB választ a következő kérdésekre.

1. **Lásd a kiállítást.** Igaz vagy hamis? R1 must encapsulate received packets into new frames before forwarding them to R2.

Az űrlap alja

**Hivatkozz a kiállításra.** Igaz vagy hamis? Az R2 továbbítja a kereteket az R3-nak, mind az 1s Layer 2 címmel.

**Hivatkozz a kiállításra.** Milyen műveletet hajt végre az R3 egy keret továbbítására, ha nincs bejegyzése az ARP táblában a cél MAC-cím feloldásához?

[16.0](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Bevezetés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[16.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Troubleshoot IPv4 Static and Default Route Configuration](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1. Troubleshoot Static and Default Routes
2. Troubleshoot IPv4 Static and Default Route Configuration

# Hibaelhárítás az IPv4 statikus és alapértelmezett útvonal konfigurációjával

16.2.1

## Változások a hálózatban

Bármennyire jól konfigurálunk egy hálózatot, a hibaelhárításra mindig készen kell állnunk. Számos olyan dolog történhet a hálózatunkban, amely megváltoztatja a működését. Például meghibásodhat egy interfész, vagy a szolgáltató felé megszakad egy összeköttetés. Túlterhelődhet egy kapcsolat, vagy valaki beírhat egy hibás konfigurációs parancsot.

Bármely változás eredményezheti az összeköttetések megszakadását. A rendszergazda feladata a problémák pontos meghatározása és megoldása. Ehhez ismernie kell azokat az eszközöket, amelyekkel a forgalomirányítási problémák gyorsan behatárolhatók.

16.2.2

## A hibakeresés szokásos parancsai

A hibakereséshez többek közöt az IOS következő parancsait használhatjuk:

* **ping**
* **traceroute**
* **mutasd az ip útvonalat**
* **ip interfész rövid megjelenítése**
* **cdp szomszédok részletének megjelenítése**

A parancsok bemutatásához az ábrán látható topológiát használjuk.

Az ábra a 172.16.1.0/24 hálózati kapcsolóhoz csatlakoztatott PC2-t ábrázolja. A kapcsolót ezután a G0/0/0 Gigabit interfészen lévő útválasztóhoz (R2) csatlakozik, amelynek Gateway címe .1. Az R2-nek két soros S0/1/0 és S0/1/1 csatlakozója van, amelyek az S0/1/0 routerhez (R1) és az S0/1/1 csatlakozón lévő routerhez (R3) csatlakoznak. A hálózati cím R1-től R2-ig 172.16.2.0/14, R2-től R3-ig pedig 192.181.1.0/24. Az R2 soros csatlakozási címe .2, míg az R1 és R3 .1. Az R1 a G0/0/0 Gigabites interfészen keresztül csatlakozik egy 172.16.3.0/24-es hálózati kapcsolóhoz, amelyhez a PC1 csatlakozik. Az R3-nak Gigabites kapcsolata van a 192.168.2.0/24-es hálózaton lévő switch-hez, a PC3 pedig a switch-hez van csatlakoztatva.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1

.1

Kattintsunk az egyes gombokra a gyakori hibaelhárítási parancsok példájáért és magyarázatáért.

**ping**

The example displays the result of an extended ping from the source interface of R1 to the LAN interface of R3. A kiterjesztett ping a ping segédprogram továbbfejlesztett verziója. A kiterjesztett ping lehetővé teszi a ping csomagok forrás-IP-címének megadását.

R1# ping 192.168.2.1 forrás 172.16.3.1 Írja be az escape szekvenciát a megszakításhoz.

5, 100 bájtos ICMP visszhang küldése a 192.168.2.1-re, időtúllépés 2 másodperc: A csomag 172.16.3.1 forráscímmel lett elküldve !!!!! A sikerességi arány 100 százalék (5/5), oda-vissza min/átl./max = 3/3/5 ms R1#

16.2.3

## Kapcsolódási problémák megoldása

Egy hiányzó vagy hibás útvonal megtalálása aránylag egyszerű, ha a segédeszközöket módszeresen használjuk.

Például PC1 felhasználója azt jelenti, hogy nem éri el az R3 helyi hálózatán lévő erőforrásokat. Ez megerősíthető azzal, ha R1 LAN interfészéről megpingeljük R3 LAN interfészét. Ismét az ábrán látható topológiát fogjuk használni annak bemutatására, hogyan lehet megoldani ezt a csatlakozási problémát.

Az ábra a 172.16.1.0/24 hálózati kapcsolóhoz csatlakoztatott PC2-t ábrázolja. A kapcsolót ezután a G0/0/0 Gigabit interfészen lévő útválasztóhoz (R2) csatlakozik, amelynek Gateway címe .1. Az R2-nek két soros S0/1/0 és S0/1/1 csatlakozója van, amelyek az S0/1/0 routerhez (R1) és az S0/1/1 csatlakozón lévő routerhez (R3) csatlakoznak. A hálózati cím R1-től R2-ig 172.16.2.0/14, R2-től R3-ig pedig 192.181.1.0/24. Az R2 soros csatlakozási címe .2, míg az R1 és R3 .1. Az R1 a G0/0/0 Gigabites interfészen keresztül csatlakozik egy 172.16.3.0/24-es hálózati kapcsolóhoz, amelyhez a PC1 csatlakozik. Az R3-nak Gigabites kapcsolata van a 192.168.2.0/24-es hálózaton lévő switch-hez, a PC3 pedig a switch-hez van csatlakoztatva.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1

.1

Az egyes gombokra kattintva megtudhatjuk, hogyan segítenek a hibaelhárításra szolgáló parancsok a kapcsolódási probléma megoldásában.

**Pingelje a távoli LAN-t**

The network administrator can test connectivity between the two LANs from R1 instead of PC1. A pinget R1 G0/0/0 interfészéről indítjuk R3 G0/0/0 interfészére, amint az ábra is mutatja. Az eredmény azt mutatja, hogy a hálózatok között nincs kapcsolat.

R1# ping 192.168.2.1 forrás g0/0/0 Írja be az escape szekvenciát a megszakításhoz.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.3.1

.....

Success rate is 0 percent (0/5)

16.2.4

## Parancsszimulátor - IPv4 statikus és alapértelmezett útvonalak hibáinak elhárítása

IPv4 statikus és alapértelmezett útvonalak hibáinak elhárítása a megadott követelmények alapján

Az ábra a 172.16.1.0/24 hálózati kapcsolóhoz csatlakoztatott PC2-t ábrázolja. A kapcsolót ezután a G0/0/0 Gigabit interfészen lévő útválasztóhoz (R2) csatlakozik, amelynek Gateway címe .1. Az R2-nek két soros S0/1/0 és S0/1/1 csatlakozója van, amelyek az S0/1/0 routerhez (R1) és az S0/1/1 csatlakozón lévő routerhez (R3) csatlakoznak. A hálózati cím R1-től R2-ig 172.16.2.0/14, R2-től R3-ig pedig 192.181.1.0/24. Az R2 soros csatlakozási címe .2, míg az R1 és R3 .1. Az R1 a G0/0/0 Gigabites interfészen keresztül csatlakozik egy 172.16.3.0/24-es hálózati kapcsolóhoz, amelyhez a PC1 csatlakozik. Az R3-nak Gigabites kapcsolata van a 192.168.2.0/24-es hálózaton lévő switch-hez, a PC3 pedig a switch-hez van csatlakoztatva.

R3 172.16.1.0/24 172.16.2.0/24 192.168.1.0/24 172.16.3.0/24 192.168.2.0/24 G0/0/0 S0/1/1 S0/1/0 S0/1/1 G0/0/0 G0/0/0 PC2 PC1 PC3 R1 R2 S0/1/0 .1 .1 .2 .2 .1 .1

.1

Pingeljük az R1-ről az R3 G0/0/0 interfészét.

R1#ping 192.168.2.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:

U.U.U

Success rate is 0 percent (0/5)

Teszteljük a következő ugrást úgy, hogy pingeljük az R1-ről az R2 S0/1/0 interfészét.

R1#ping 172.16.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms

Nézzük át az irányítótáblát az R1-en.

R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

S 172.16.1.0/24 [1/0] via 172.16.2.2

C 172.16.2.0/24 is directly connected, Serial0/1/0

L 172.16.2.1/32 is directly connected, Serial0/1/0

C 172.16.3.0/24 is directly connected, GigabitEthernet0/0/0

L 172.16.3.1/32 is directly connected, GigabitEthernet0/0/0

S 192.168.1.0/24 [1/0] via 172.16.2.2

S 192.168.2.0/24 [1/0] via 172.16.2.2

Nézzük át az irányítótáblát az R2-n.

R2#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/0/0

L 172.16.1.1/32 is directly connected, GigabitEthernet0/0/0

C 172.16.2.0/24 is directly connected, Serial0/1/0

L 172.16.2.2/32 is directly connected, Serial0/1/0

S 172.16.3.0/24 [1/0] via 172.16.2.1

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, Serial0/1/1

L 192.168.1.2/32 is directly connected, Serial0/1/1

Enter configuration mode and configure a static route on R2 to reach the R3 LAN.

R2#configure terminal

R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1

Lépjünk ki a konfigurációs módból, és tekintsük át az R2 irányítótábláját.

R2(config)#exit

\*Sep 20 03:10:34.913: %SYS-5-CONFIG\_I: Configured from console by console

R2#show ip route

Kódok: L - helyi, C - csatlakoztatott, S - statikus, R - RIP, M - mobil, B - BGP

D - EIGRP, EX - EIGRP külső, O - OSPF, IA - OSPF inter area

N1 – OSPF NSSA külső típus 1, N2 – OSPF NSSA külső típus 2

E1 - OSPF külső típus 1, E2 - OSPF külső típus 2

i - IS-IS, su - IS-IS összefoglaló, L1 - IS-IS szint-1, L2 - IS-IS szint-2

ia - IS-IS inter area, \* - jelölt alapértelmezett, U - felhasználónkénti statikus útvonal

o - ODR, P - periodikusan letöltött statikus útvonal, H - NHRP, l - LISP

a - alkalmazási útvonal

+ - replikált útvonal, % - következő ugrás felülírása, p - felülírások PfR-ből

Az utolsó lehetőség átjárója nincs beállítva

A 172.16.0.0/16 változó alhálózattal rendelkezik, 5 alhálózat, 2 maszk

A C 172.16.1.0/24 közvetlenül kapcsolódik, GigabitEthernet0/0/0

Az L 172.16.1.1/32 közvetlenül kapcsolódik, GigabitEthernet0/0/0

A C 172.16.2.0/24 közvetlenül csatlakozik, Serial0/1/0

Az L 172.16.2.2/32 közvetlenül kapcsolódik, Serial0/1/0

S 172.16.3.0/24 [1/0] – 172.16.2.1

A 192.168.1.0/24 változó alhálózattal rendelkezik, 2 alhálózat, 2 maszk

A C 192.168.1.0/24 közvetlenül csatlakozik, Serial0/1/1

Az L 192.168.1.2/32 közvetlenül kapcsolódik, Serial0/1/1

S 192.168.2.0/24 [1/0] – 192.168.1.1

Pingeljük az R1-ről az R3 G0/0/0 interfészét.

R1# ping 192.168.2.1

Írja be az escape szekvenciát a megszakításhoz.

5, 100 bájtos ICMP visszhang küldése a 192.168.2.1-nek, az időtúllépés 2 másodperc:

!!!!!

A sikerességi arány 100 százalék (5/5), oda-vissza út min/átl./max = 3/3/4 ms

Sikeresen elvégezte a hibaelhárítást az IPv4 statikus és alapértelmezett útvonalakon.

[16.1](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Packet Processing with Static Routes](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[16.3](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Gyakorlás és ellenőrzés](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

# Kapcsolás, útválasztás és vezeték nélküli alapvető szolgáltatások

v 7.02

[Skip to content](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU#chunks-container)

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

1.                                                                                                                                                                                                                                                                                                                                                                                                                                                    
2. Troubleshoot Static and Default Routes
3. Gyakorlás és ellenőrzés

# Gyakorlás és ellenőrzés

16.3.1

## Packet Tracer - Statikus és alapértelmezett útvonalak hibaelhárítása

Ebben a feladatban statikus és alapértelmezett útvonalak hibakeresését végezzük el, majd kijavítjuk a megtalált hibákat.

* IPv4 statikus útvonalak hibaelhárítása
* IPv6 statikus útvonalak hibaelhárítása
* IPv4 statikus útvonalak konfigurálása
* IPv4 alapértelmezett útvonalak konfigurálása
* IPv6 statikus útvonalak konfigurálása

[Statikus és alapértelmezett útvonalak hibaelhárítása](https://contenthub.netacad.com/courses/srwe-dl/_common/16.3.1-packet-tracer---troubleshoot-static-and-default-routes_hu-HU.pka)

16.3.2

## Lab – Az IPv4 és IPv6 statikus és alapértelmezett útvonalak hibaelhárítása

##### Készségek gyakorlási lehetőség

Lehetőséged van az alábbi készségek gyakorlására:

* 1. rész: A hálózat működésének értékelése
* 2. rész: Információgyűjtés, cselekvési terv létrehozása és korrekciók végrehajtása

Ezeket a készségeket gyakorolhatja a Packet Tracer vagy a laborberendezés segítségével, ha rendelkezésre áll.

**Packet Tracer – Fizikai mód (PTPM)**

[Az IPv4 és IPv6 statikus és alapértelmezett útvonalak hibaelhárítása – Fizikai mód](https://contenthub.netacad.com/courses/srwe-dl/_common/16.3.2-packet-tracer---troubleshoot-ipv4-and-ipv6-static-and-default-routes---physical-mode_hu-HU.pka)

**Laboratóriumi berendezések**

16.3.3

## Miről tanultunk ebben a fejezetben?

**Csomagfeldolgozás statikus útvonalakkal**

1. A csomag megérkezik R1-re.
2. R1 nem rendelkezik a célhálózat felé útvonallal, így az alapértelmezett statikus útvonalat használja.
3. R1 beágyazza a csomagot egy új keretbe. Mivel R2 felé a kapcsolat pont-pont jellegű, a második rétegbeli célcím csupa 1-es lesz.
4. A keret kimegy a megfelelő interfészen. A csomag megérkezik R2-re.
5. R2 kicsomagolja a keretet és útvonalat keres a cél felé. R2-nek van egy statikus útvonala a célhálózat felé.
6. R2 beágyazza a csomagot egy új keretbe. Mivel R3 felé a kapcsolat pont-pont jellegű, a második rétegbeli célcím csupa 1-es lesz.
7. A keret kimegy a megfelelő interfészen. A csomag megérkezik R3-ra.
8. R3 kicsomagolja a keretet és útvonalat keres a cél felé. R3-nak közvetlenül csatlakozó útvonala van a célhálózathoz.
9. Az R3 megkeresi a célhálózat ARP bejegyzését, hogy megtalálja a PC3 2. rétegbeli MAC-címét. Ha nem talál bejegyzést, akkor egy ARP kérést küld ki, amire PC3 ARP-választ küld benne a saját MAC-címével.
10. R3 beágyazza a csomagot egy új keretbe, amelyben a 2. rétegbeli forráscím a megfelelő interfészének MAC-címe, a célcím pedig PC3 MAC-címe.
11. A keret kimegy a megfelelő interfészen. A csomag megérkezik PC3 hálózati kártyájára.

**Hibaelhárítás az IPv4 statikus és alapértelmezett útvonal konfigurációjával**

Számos olyan dolog történhet a hálózatunkban, amely megváltoztatja a működését. Meghibásodhat egy interfész, vagy a szolgáltató felé megszakad egy kapcsolat. Túlterhelődhet egy összeköttetés, vagy valaki beírhat egy hibás konfigurációs parancsot. A hibakereséshez többek közöt az IOS következő parancsait használhatjuk:

* **ping**
* **traceroute**
* **mutasd az ip útvonalat**
* **ip interfész rövid megjelenítése**
* **cdp szomszédok részletének megjelenítése**

16.3.4

## Ellenőrző kvíz - Statikus és alapértelmezett útvonalak hibaelhárítása

Az űrlap teteje

1. Melyik sorrend határozza meg helyesen a router által végrehajtandó lépések sorrendjét, amikor egy csomagot kap egy Ethernet interfészen?

Az űrlap alja

Az IOS melyik három hibaelhárító parancsa segíthet a statikus forgalomirányítás hibáinak felderítésében? (Három jó válasz van.)

A hálózati rendszergazda statikus útvonalat adott meg egy szomszédos routerhez csatlakoztatott Ethernet LAN-hoz. Az útvonal azonban nem jelenik meg az irányítótáblában. Melyik parancsot használja a rendszergazda annak ellenőrzésére, hogy a kimenő interfész működik-e?

A routeren manuálisan hoztak létre egy statikus útvonalat. A célhálózat azonban már nem létezik. Mit tegyen a rendszergazda, hogy eltávolítsa a statikus útvonalat az irányítótáblából?

Melyik utasítás írja le a router által végrehajtott folyamatok sorrendjét, amikor egy géptől egy másik hálózaton lévő géphez szállítandó csomagot kap?

A network engineer issues the **show cdp neighbor** command on several network devices during the process of network documentation. Mi a parancs célja?

A hálózati rendszergazda észreveszi, hogy a helyesen megadott statikus útvonal nincs az irányítótáblában. Melyik két parancsot használja a rendszergazda annak megállapítására, hogy a kimenő interfész fel van-e kapcsolva, és a következő ugrás cím elérhető? (Két jó válasz van.)

Egy hálózati rendszergazda a következő parancsot adta be:

**ip útvonal 192.168.10.64 255.255.255.192 serial0/0/1**

When the network administrator enters the command **show ip route** , the route is not in the routing table. Mi legyen a következő lépése?

Mit tesz a router, ha nincs beállítva alapértelmezett útvonal, és egy csomagot olyan célhálózathoz kell továbbítani, amely nem szerepel az irányítótáblában?

Mit jelent a C betű a **show ip route** parancs kimenetében lévő bejegyzés mellett?

[16.2](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)

[Troubleshoot IPv4 Static and Default Route Configuration](https://contenthub.netacad.com/srwe-dl/10.0.1?lng=hu-HU" \l "/srwe-dl/undefined.1)