# Fejezet 10: DHCP 10.0.1.1 Bevezetés

# Bevezetés

## Bevezetés

Minden hálózatba kötött eszköznek egyedi címmel kell rendelkeznie. A hálózati rendszergazdák statikus IP-címet rendelnek az olyan forgalomirányítókhoz, szerverekhez, nyomtatókhoz és más eszközökhöz, amelyek (fizikai vagy logikai) helye várhatóan nem változik a későbbiekben. Ezek általában olyan berendezések, amelyek szolgáltatást nyújtanak a hálózatra csatlakozó felhasználóknak és eszközöknek, így a hozzájuk rendelt címeknek sem célszerű változnia. A statikus címek ezen felül lehetővé teszik a rendszergazdák számára az ilyen berendezések távoli felügyeletét. Ha egy berendezés IP-címe könnyen meghatározható, az leegyszerűsíti az eszköz elérését a hálózati rendszergazdák számára.

Egy szervezeten belül azonban a számítógépek és felhasználók helye gyakran változik, fizikai és logikai szempontból egyaránt. Nehézkes és időrabló lenne, ha a rendszergazdáknak új IP-címet kellene kiosztani minden egyes alkalommal, amikor egy dolgozó átköltözik. Nem beszélve arról, hogy a távoli helyekről dolgozó távmunkások megfelelő hálózati paramétereinek manuális beállítása további kihívásokat jelentene. Az IP-címek és egyéb címzési adatok kézzel történő megadása még az asztali kliensek esetében is adminisztratív terhet jelent, különösen a hálózat növekedése esetén.

A DHCP (Dynamic Host Configuration Protocol) szerver helyi hálózaton történő alkalmazása leegyszerűsíti az IP-címek kiosztását az asztali és a mobil eszközök számára egyaránt. Egy központi DHCP-szerver használatával lehetővé válik, hogy a szervezetek egyetlen szerverről adminisztrálják az összes IP-cím dinamikus kiosztását. Ez a gyakorlat hatékonyabbá teszi az IP-címek kezelését, valamint biztosítja a szervezet egészére vonatkozó következetességet, beleértve a fiókirodákat is.

A DHCP IPv4 (DHCPv4) és IPv6 (DHCPv6) esetén is rendelkezésre áll. Ez a fejezet a DHCPv4 és a DHCPv6 működésével, beállításával és hibaelhárításával egyaránt foglalkozik.

# Bevezetés

## Bevezetés

**Feladat - Saját vagy bérelt?**

A fejezet a kis- és középvállalatok hálózataiban használt DHCP-folyamat fogalmát mutatja be. Ez a modellezési feladat leírja, hogy miként működnek a DHCP-folyamatot használó, egészen egyszerű vezeték nélküli ISR eszközök.

Látogassunk el a <http://ui.linksys.com/WRT54GL/4.30.0/Setup.htm> oldalra, ahol egy web-alapú szimulátor segítségével tanulhatjuk meg a Linksys 54GL forgalomirányító DHCP-beállításait. A szimulátortól jobb oldalán (a leírást tartalmazó, kék hátterű oszlopban) rákattinthatunk a **More** feliratra, ahol további információkat olvashatunk a DHCP beállításáról ezen a konkrét szimulátoros integrált szolgáltatású forgalomirányítón (Integrated Service Router, ISR).

Gyakoroljuk az ISR konfigurációját az alábbiakkal:

* állomásnév
* helyi IP-cím és alhálózati maszk
* DHCP (engedélyezés vagy letiltás)
* kezdő IP-cím
* DHCP-vel kiosztott IP-címet kapható felhasználók maximális száma
* bérleti idő
* időzóna (használhatjuk a sajátunkat, vagy egy általunk kedveltet)

Amennyiben végeztünk a felsorolt beállítások megadásával, készítsünk egy képernyőképet a **PrtScrn** billentyűparanccsal. A készített képernyőképet illesszük be egy szövegszerkesztő dokumentumába. Mentsük el a dokumentumot, majd az általunk választott beállítások megvitatására az osztály többi tagjával!

[Csoportos feladat - Own or Lease? Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/10.0.1.2%20Own%20or%20Lease%20Instructions.pdf)

# DHCP v4

## A DHCPv4 működése

A DHCPv4 az IPv4-címek és az egyéb hálózati beállítások dinamikus kiosztásáért felel. 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 viszont egy kisebb fiókirodáról vagy otthoni/kisirodai környezetről van szó, nincs szükség dedikált szerverre. A DHCPv4-szolgáltatás egy Cisco forgalomirányító megfelelő beállításával is biztosítható. A Cisco IOS funkciókészletének Easy IP funkciója szükség esetén teljes értékű DHCPv4-szervert kínál.

A DHCPv4 három különböző kiosztási módot támogat, hogy megfelelő rugalmasságot biztosítson az IP-címek kiosztásánál:

* **Manuális kiosztás** - A rendszergazda egy előre meghatározott IPv4-címet rendel a klienshez, és a DHCPv4 csak átadja ezt az IPv4-címet az eszköznek.
* **Automatikus kiosztás** - A DHCPv4 automatikusan és maradandóan rendel hozzá egy statikus IPv4-címet az eszközhöz, amelyet a rendelkezésre álló címkészletből választ ki. Nincs szó bérletről, a számítógéphez mindig ez a cím lesz hozzárendelve.
* **Dinamikus kiosztás** - A rendelkezésre álló címkészletből a DHCPv4 dinamikusan oszt ki vagy ad bérbe egy IPv4-címet a szerver által meghatározott ideig, vagy addig, ameddig a kliensnek szüksége van a címre.

Ebben a fejezetben a legelterjedtebb DHCPv4 kiosztási móddal, a dinamikus kiosztással foglalkozunk. Amikor dinamikus kiosztásról beszélünk, az ügyfelek a címeket meghatározott időtartamra bérlik, az ábrán látható módon. A rendszergazdák úgy állítják be a DHCPv4-szervereket, hogy a bérleti idő különböző időközönként járjon le. A bérleti idő jellemzően 24 óra és egy (vagy több) hét között alakul. Amikor a bérlet lejár, az ügyfélnek új címet kell kérelmeznie, bár általában ugyanazt a címet kapja vissza.

# DHCP v4

## A DHCPv4 működése

Ahogy az 1. ábrán is látható, a DHCPv4 kliens/szerver 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 elköltöztetett 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 a szükség szerint ismételten kiosztható címek készletébe.

**A bérlet indítása**

Amikor a kliens elindul (vagy más módon kapcsolódik a hálózathoz), egy négy lépésből álló folyamattal kezdeményezi a bérleti jog megszerzését. Ahogy a 2. ábrán is látható, a kliens egy szórásos DHCP-felfedező (DHCPDISCOVER) üzenet szétküldésével kezdi meg a folyamatot, amelyben szerepel a saját MAC-címe. Ennek célja, hogy megtalálja a hálózaton elérhető DHCPv4-szervereket.

**DHCP-felfedezés (DHCPDISCOVER)**

A DHCPDISCOVER üzenettel deríthetők fel a hálózatban működő DHCPv4-szerverek. Mivel a kliens nem rendelkezik érvényes IPv4-információval induláskor, a szerverrel való kommunikációhoz 2. rétegbeli és 3. rétegbeli szórási címeket használ.

**DHCP-ajánlás (DHCPOFFER)**

Amikor a DHCPv4-szerver DHCPDISCOVER üzenetet kap, lefoglal egy rendelkezésre álló IPv4-címet, hogy bérbe adja a kliensnek. A szerver egy olyan ARP-bejegyzést is létrehoz, amely a kérést intéző kliens MAC-címéből, valamint a kliens által bérelt IPv4-címből áll. Ahogy a 3. ábrán is látható, a DHCPv4-szerver elküldi a foglalás tényét rögzítő DHCPOFFER üzenetet a kérést intéző kliensnek. A DHCPOFFER üzenet elküldése egyedi címzéssel történik,ahol a forráscím a szerver L2-es MAC-címe, a célcím pedig a kliens L2-es MAC-címe.

**DHCP-kérés (DHCPREQUEST)**

Ha a kliens DHCPOFFER üzenetet kap a szervertől, akkor egy DHCPREQUEST üzenetet küld vissza a 4. ábrán látható módon. Ez az üzenet használatos a bérlet indításához, illetve megújításához egyaránt. Amennyiben a bérlet indításához használjuk, a DHCPREQUEST egyfajta kötelező érvényű elfogadási értesítésként szolgál a kiválasztott szerver felé, míg az összes többi, foglalást rögzítő szerver felé értelemszerűen elutasítást jelent.

Sok vállalati hálózatban egyszerre több DHCPv4-szervert használnak. A DHCPREQUEST üzenet elküldése szórással történik, amely tájékoztatja a kiválasztott és az összes többi DHCPv4-szervert az ajánlat elfogadásáról.

**DHCP-nyugtázás (DHCPACK)**

A DHCPREQUEST üzenet megérkezése után a szerver egy, az adott címre küldött ICMP ping segítségével ellenőrzi, hogy az nincs-e már használatban, majd létrehoz egy új ARP-bejegyzést a bérlet tényéről, végül pedig egy egyedi címzésű DHCPACK üzenettel válaszol, az 5. ábrán látható módon. A DHCPACK üzenet tulajdonképpen a DHCPOFFER másolata, különbség csupán az üzenettípus mező értékében van. Amikor a kliens megkapja a DHCPACK üzenetet, naplózza a beállításokat, majd egy ARP-keresést végez a kiosztott címre vonatkozóan. Amennyiben az ARP-kérésre nem érkezik válasz, a kliens tudni fogja, hogy az IPv4-cím érvényes, és sajátjaként kezdi használni.

**A bérlet megújítása**

**DHCP-kérés (DHCPREQUEST)**

Ahogy a 6. ábrán is látszik, a bérleti idő lejártával a kliens egy DHCPREQUEST üzenetet küld közvetlenül annak a DHCPv4-szervernek, amely eredetileg kínálta fel az IPv4-címet. Amennyiben egy DHCPACK bizonyos időn belül nem érkezik meg, a kliens szórással egy újabb DHCPREQUEST-et indít, hogy valamelyik másik DHCPv4-szerver meghosszabbítsa a bérleti idejét.

**DHCP-nyugtázás (DHCPACK)**

A DHCPREQUEST üzenet megérkezése után a szerver egy DHCPACK visszaküldésével erősíti meg a bérleti adatokat, a 7. ábrán látható módon.

# DHCP v4

## A DHCPv4 működése

Az összes DHCPv4-tranzakcióhoz a DHCPv4-üzenet formátuma használatos. A DHCPv4-üzenetek beágyazása az UDP szállítási protokollon belül történik. A kliens által küldött DHCPv4-üzenetek az UDP 68-as forrásportját, illetve 67-es célportját használják. A szerver által a kliensnek küldött DHCPv4-üzenetek pedig az UDP 67-es forrásportját, illetve 68-as célportját használják.

Az ábrán egy DHCPv4-üzenet formátuma látható. A mezők nevei az alábbiak:

* **Műveleti (OP) kód -** Meghatározza az üzenet általános típusát. Az 1-es érték a kérést, míg a 2-es érték a választ jelöli.
* **Hardver típusa** - Felismeri a hálózaton használt hardver típusát. Az 1-es például az Ethernetet, a 15-ös a Frame Relay-t, a 20-as pedig a soros vonalat jelöli. Ezek megegyeznek az ARP-üzenetekben is használatos kódokkal.
* **Hardvercím hossza** - A cím hosszát határozza meg.
* **Ugrásszám** - Az üzenetek továbbítását szabályozza. Kérések továbbítása előtt a kliens 0-ra állítja az értékét.
* **Tranzakciós azonosító** - Arra használja a kliens, hogy a kérést összevesse a DHCPv4-szerverektől kapott válaszokkal.
* **Másodperc** - Meghatározza a kliens bérletindítási vagy -megújítási kísérlete óta eltelt másodpercek számát. A DHCPv4-szerverek a válaszok prioritási sorrendjének megadására használják, ha a klienskérések száma kimagaslóan nagy.
* **Jelzőbitek** - Olyan kliensek használják, amelyek nem ismerik a saját IPv4-címüket a kérés elküldésekor. A 16 bitből csupán az egyik van használatban; ez a szórási jelzőbit. Amennyiben ennek a mezőnek az értéke 1, az a kérést fogadó DHCPv4-szervernek vagy -közvetítőnek azt jelenti, hogy a választ szórással kell elküldeni.
* **Kliens IP-címe** - A kliens által használható érvényes cím, amelyet a bérlet megújításakor használ, nem pedig a cím megszerzése során. A kliens akkor és csak akkor helyezi a saját IPv4-címét ebbe a mezőbe, amennyiben érvényes IPv4-címmel rendelkezik lekötött állapotban. Ellenkező esetben a mező értékét 0-ra állítja.
* **Saját IP-cím** - A szerver használja, hogy IPv4-címet osszon ki a kliensnek.
* **Szerver IP-címe** Arra használja a szerver, hogy meghatározza annak a szervernek a címét, amelyet a kliensnek használni kell a rendszerindítási folyamat következő lépése során. Lehet ugyanaz vagy más is, mint az eredeti küldő szerver címe. A küldő szerver saját IPv4-címe mindig szerepel egy különleges mezőben, amelyet szerverazonosító (Server Identifier) DHCPv4-opciónak neveznek.
* **Átjáró IP-címe** - Útbaigazítja a DHCPv4-üzeneteket, amennyiben DHCPv4-közvetítők is érintettek a folyamatban. Az átjáró címe megkönnyíti a kliens és a szerverek közötti, DHCPv4 kérésekből és válaszokból álló DHCPv4-kommunikációt, amennyiben azok különböző alhálózaton vagy hálózatokon találhatóak.
* **Kliens hardveres címe** - Meghatározza a kliens fizikai rétegét.
* **Szerver neve:** - A DHCPOFFER és DHCPACK üzeneteket küldő szerver használja. Ebben a mezőben opcionálisan szerepelhet a saját neve. A név lehet egy egyszerű szöveges becenév vagy egy DNS-tartománynév, mint például a dhcpserver.netacad.net.
* **Indítófájl neve** - A kliens opcionálisan használhatja a DHCPDISCOVER üzenetet egy konkrét betöltőfájl-típus kéréséhez. A szerver egy DHCPOFFER üzenetben adja meg az indítófájl teljes könyvtár- és fájlnevét.
* **DHCP-opciók** - Tartalmazza a DHCP-opciókat, beleértve a DHCP alapvető működéséhez szükséges különféle paramétereket. A mező hosszúsága változó. Kliens és szerver egyaránt használhatja ezt a mezőt.

# DHCP v4

## A DHCPv4 működése

Amennyiben egy kliens úgy van beállítva, hogy az IPv4-beállításokat dinamikusan kapja, és kapcsolódni kíván a hálózathoz, a DHCPv4-szerverhez fordul a címzési információkért. Indításkor vagy aktív hálózati kapcsolat érzékelésekor a kliens egy DHCPDISCOVER üzenetet küld szét. Mivel a kliens semmilyen ismerettel nem rendelkezik arról az alhálózatról, amelyhez kapcsolódott, ezért a DHCPDISCOVER egy IPv4 szórásos üzenet (a 255.255.255.255 IPv4-célcímmel). Mivel a kliens még nem rendelkezik beállított IPv4-címmel, ezért IPv4-forráscímként a 0.0.0.0 szerepel.

Ahogy az 1. ábrán is látható, a kliens IPv4-címe (CIADDR), az alapértelmezett átjáró címe (GIADDR), valamint az alhálózati maszk mind a 0.0.0.0 cím használatát jelzik.

**MEGJEGYZÉS**: Ismeretlen információk küldése a 0.0.0.0 cím használatával történik.

Amikor a DHCPv4-szerver DHCPDISCOVER üzenetet kap, válaszként egy DHCPOFFER üzenetet küld el. Ez az üzenet tartalmazza a kliens kezdőbeállításait, beleértve a szerver által kínált IPv4-címet és alhálózati maszkot, a bérleti időt, valamint az adatokat kínáló DHCPv4-szerver címét.

Beállítható, hogy a DHCPOFFER üzenet tartalmazzon egyéb információkat is, mint például a bérletmegújítási időt, valamint a DNS-szerver címét.

Ahogy a 2. ábrán is látható, a DHCP-szerver a DHCPDISCOVER üzenetre küldött válaszában értéket rendel a kliens címéhez (CIADDR), valamint az alhálózati maszkhoz. A keret összeállításánál és a kérést intéző klienshez történő elküldésénél a kliens hardveres címét (CHADDR) használja.

A folyamat a kliens és a szerver nyugtázó üzeneteinek elküldésével zárul.

# DHCP v4

## A DHCPv4-szerver alapbeállításainak megadása

Egy Cisco IOS operációs rendszert futtató forgalomirányító is beállítható DHCPv4 szervernek. A Cisco IOS DHCPv4-szervere képes a forgalomirányítón belül megadott címkészletek IPv4-címeinek a DHCPv4-kliensek felé történő kiosztására és kezelésére. Ezt illusztrálja az 1. ábrán látható topológia.

**1. lépés: IPv4-címek kizárása**

A DHCPv4-szerverként működő forgalomirányító egy DHCPv4-címkészlet összes IPv4-címét kiosztja, hacsak nincs beállítva bizonyos címek kizárása. A készlet néhány IPv4-címe jellemzően a statikus címet igénylő hálózati eszközöknek van kiosztva. Ezért ezen címeket nem szabad más eszközöknek kiosztani! Bizonyos címek kizárásához használjuk az **ip dhcp excluded-address** parancsot a 2. ábrán látható módon.

Cím vagy címtartomány kizárása az első és utolsó cím megadásával lehetséges. Érdemes a kizárt címek közé felvenni a forgalomirányítók, szerverek, hálózati nyomtatók és más manuálisan konfigurált eszközök címeit.

**2. lépés: DHCPv4-készlet beállítása**

A DHCPv4-szerverek beállítása magában foglalja a kiosztható címkészlet megadását. Ahogy a 3. ábrán is látható, az **ip dhcp pool** *készlet-neve* parancs egy készletet hoz létre a megadott névvel, majd DHCPv4 konfigurációs módba lépteti a forgalomirányítót, amelyet az alábbi prompt is jelez: Router(dhcp-config)#.

**3. lépés: Konkrét feladatok beállítása**

A 4. ábrán egy lista látható a DHCPv4-címkészlet beállításához szükséges feladatokról. Ezek egy része opcionális, míg a többi beállítás megadása kötelező.

A címkészletet, valamint az alapértelmezett átjáró szerepét betöltő forgalomirányítót be kell állítani. A **network** utasítással adhatjuk meg a bérelhető címek tartományát.

A **default-router** paranccsal adható meg az alapértelmezett átjáró. Az átjáró jellemzően a klienseszközökhöz legközelebb található forgalomirányító 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. A DHCPv4-kliens számára elérhető DNS-szerver IPv4-címét például a **dns-server** paranccsal lehet beállítani. A **domain-name** *tartománynév* használatával adható meg a tartomány neve. A DHCPv4-bérlet időtartama módosítható a **lease** paranccsal. Az alapértelmezett bérleti idő egy nap. A **netbios-name-server** parancs használatával megadható a NetBIOS WINS szerver.

**DHCPv4 példa**

Az 5. ábrán látható a 192.168.10.0/24 LAN számára DHCPv4-szerverként szolgáló R1 forgalomirányítón megadott DHCPv4-alapbeállítások mintakonfigurációja, amely az 1. ábra topológiáját veszi alapul.

**A DHCPv4 letiltása**

A DHCPv4-szolgáltatás alapesetben engedélyezve van, amennyiben a Cisco IOS adott változata képes ilyen szolgáltatást nyújtani. A szolgáltatást a **no service dhcp** globális konfigurációs paranccsal tilthatjuk le. A **service dhcp** globális konfigurációs parancs kiadásával később újra engedélyezhetjük a szolgáltatást. Ha a paraméterek nincsenek beállítva, a szolgáltatás engedélyezésének nincs semmilyen hatása.

A 6. ábrán található parancsszimulátor segítségével a fentiekhez hasonló paraméterek állíthatók be az R1 forgalomirányítón a 192.168.10.0/24 LAN számára.

# DHCP v4

## A DHCPv4-szerver alapbeállításainak megadása

A példában szereplő kimenet az 1. ábra topológiája alapján készült. Az R1 forgalomirányító beállítása DHCPv4-szolgáltatások nyújtására már megtörtént. A PC1 elindítására még nem került sor, ezért IP-címmel sem rendelkezik.

A 2. ábrán látható **show running-config | section dhcp** parancs kimenete megjeleníti az R1 forgalomirányítón kiadott DHCPv4-parancsokat. A **| section** paraméter kizárólag a DHCPv4-beállításokhoz kapcsolódó parancsokat jeleníti meg.

A DHCPv4 működése a 3. ábrán látható **show ip dhcp binding** paranccsal ellenőrizhető. Ez megjeleníti a DHCPv4-szolgáltatás által kiosztott összes IPv4-cím, valamint hozzárendelt MAC-cím listáját. A 3. ábrán látható **show ip dhcp server statistics** paranccsal ellenőrizhetők a forgalomirányító által fogadott és küldött DHCPv4-üzenetek. A parancs segítségével a fogadott és küldött DHCPv4-üzenetek számát is meg lehet jeleníteni.

Ahogy a fenti parancsok kimenetéből is látszik, jelenleg nincs aktív hozzárendelés, és a statisztikák szerint sem történt üzenetküldés vagy -fogadás. Eddig a pillanatig egyetlen eszköz sem igényelt DHCPv4-szolgáltatásokat az R1 forgalomirányítótól.

A 4. ábrán ugyanazon parancsok kimenete látszik, de már a PC1 és a PC2 bekapcsolása és elindítása után.

Vegyük észre, hogy a megjelenő információk szerint a kiosztott 192.168.10.10 és 192.168.11.10 IPv4-címek MAC-címhez való hozzárendelése megtörtént! A statisztikák között megjelenik a DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, valamint a DHCPACK tevékenység.

Az 5. ábrán látható **ipconfig /all** parancs PC1 számítógépen történő kiadásával megjelennek a TCP/IP paraméterek. Mivel a PC1 a 192.168.10.0/24 hálózati szegmensre kapcsolódik, ezért automatikusan megkapja a DNS-utótagot, az IPv4-címet, az alhálózati maszkot, az alapértelmezett átjárót, valamint a DNS-szerver címét is. A forgalomirányító interfészeinek beállítására nincs szükség. Amennyiben egy PC olyan hálózati szegmensre kapcsolódik, ahol van rendelkezésre álló DHCPv4-címkészlet, a PC automatikusan a megfelelő címkészletből kaphat IPv4-címet.

# DHCP v4

## A DHCPv4-szerver alapbeállításainak megadása

**Mi a DHCP-közvetítő?**

Az összetett, hierarchikus hálózatokban a vállalati szerverek általában egy szerverfarmon találhatók. 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, és veszik igénybe az általuk kínált szolgáltatásokat.

Az 1. ábrán a PC1 szórásos üzenet segítségével próbál IPv4-címet szerezni egy DHCP-szervertől. Ebben a példában az R1 forgalomirányító nincs beállítva, hogy DHCPv4-szerverként működjön, így a szórást sem továbbítja. Mivel a DHCPv4-szerver egy másik hálózaton van, ezért a PC1 nem kaphat IP-címet a DHCP segítségével.

A 2. ábrán a PC1 megpróbálja megújítani az IPv4-címét. Ezt az **ipconfig /release** parancs kiadása teszi lehetővé. Vegyük észre, hogy az IPv4-cím felszabadítása után a 0.0.0.0 cím jelenik meg. Ezután az **ipconfig /renew** parancs kiadása következik. Ennek következtében a PC1 egy szórásos DHCPDISCOVER üzenetet küld szét. A parancs kimenetéből látszik, hogy a PC1 nem képes megtalálni a DHCPv4-szervert. Mivel a forgalomirányítók nem továbbítják a szórásos üzeneteket, ezért a kérés sikertelen.

A probléma megoldására a rendszergazdák DHCPv4-szervereket adhatnak az összes alhálózathoz. Ugyanakkor ezen szolgáltatások több számítógépen történő futtatása többletköltséget és adminisztratív többletmunkát eredményez.

Ennél jobb megoldás lehet egy Cisco IOS segédcím (helper address) beállítása. Ez lehetővé teszi, hogy egy forgalomirányító DHCPv4-szórásokat továbbítson a DHCPv4-szerver felé. Amikor a forgalomirányító továbbküldi a címkéréseket, DHCPv4-közvetítőként működik. A példában szereplő topológiában a PC1 egy szórásos kéréssel próbál egy DHCPv4-szervert találni. Ha az R1 forgalomirányító DHCPv4-közvetítőként lenne beállítva, a kérést a 192.168.11.0 alhálózaton található DHCPv4-szerver felé továbbítaná.

Az R1 forgalomirányító szórást fogadó interfészének beállítása a 3. ábrán látható **ip helper-address** interfész konfigurációs paranccsal történik. Az egyetlen beállítható paraméter a DHCPv4-szerver címe.

Amikor az R1 forgalomirányító DHCPv4-közvetítőként van beállítva, elfogadja a DHCPv4-szolgáltatásra vonatkozó szórásos kéréseket, majd egyedi címzéssel továbbküldi azokat a 192.168.11.6 IPv4-címre. A **show ip interface** paranccsal ellenőrizhető a konfiguráció.

Ahogy a 4. ábrán is látszik, a PC1 így már kaphat IPv4-címet a DHCPv4-szervertől.

Nem csupán a DHCPv4-szolgáltatás esetében állítható be, hogy a forgalomirányító közvetítsen. Alapesetben az **ip helper-address** parancs hatására a készülékek a következő nyolc UDP alapú szolgáltatás forgalmát közvetítik:

* 37-es port: idő
* 49-es port: TACACS
* 53-as port: DNS
* 67-es port: DHCP/BOOTP kliens
* 68-as port: DHCP/BOOTP szerver
* 69-es port: TFTP
* 137-es port: NetBIOS névszolgáltatás
* 138-as port: NetBIOS datagram szolgáltatás

Az 5. ábrán található parancsszimulátor segítségével a megfelelő forgalomirányítón beállíthatók a DHCPv4-közvetítő parancsok, így a PC3 kaphat IPv4-címet a DHCPv4-szervertől. Vegyük alapul az 1. ábrán látható hálózat topológiáját!

# DHCP v4

## DHCPv4 kliens beállítása

Előfordul, hogy a kisirodai/otthoni környezetben, esetleg fiókirodában működő Cisco forgalomirányítókat DHCPv4-kliensként kell beállítani, hasonlóan az egyszerű számítógépekhez. A megfelelő módszer kiválasztása az internetszolgáltatótól függ. A kábel- vagy DSL-modemhez a legegyszerűbb esetekben az Ethernet-interfész használatával lehet kapcsolódni. Egy Ethernet-interfész DHCP-kliensként történő beállításához használjuk az **ip address dhcp** interfész konfigurációs parancsot.

Az 1. ábrán feltételezzük, hogy az internetszolgáltatót úgy konfigurálták, hogy a kiválasztott ügyfelek számára a 209.165.201.0/27 hálózati tartományból biztosítson IP-címeket. Miután a G0/1 interfészt konfiguráltuk az **ip address dhcp** paranccsal, a **show ip interface g0/1** paranccsal ellenőrizhetjük, hogy az interfész felkapcsolt állapotban van, címet pedig egy DHCPv4-szervertől kapott.

A 2. ábrán található parancsszimulátorral beállítható, hogy az internetszolgáltatóhoz kapcsolódó interfész a DHCP-szervertől kapjon címet.

# DHCP v4

## DHCPv4 kliens beállítása

A kisebb, otthoni használatra készült szélessávú forgalomirányítók jellemzően beállíthatók úgy, hogy DSL- vagy kábelmodemen keresztül kapcsolódjanak az internetszolgáltatóhoz. A legtöbb esetben a kisirodai/otthoni forgalomirányítókat úgy állítják be, hogy a szolgáltatótól automatikusan kapjanak IPv4-címet.

Az ábrán például egy Linksys EA6500-as forgalomirányító alapértelmezés szerinti, WAN-beállításokat tartalmazó oldala látható. Figyeljük meg, hogy az internetkapcsolat típusa automatikus DHCP-konfigurációra (Automatic Configuration - DHCP) van beállítva. Ez azt jelenti, hogy ha a forgalomirányító például egy kábelmodemhez kapcsolódik, DHCPv4-klienssé válik, és az internetszolgáltatótól kér IPv4-címet.

**MEGJEGYZÉS**: A MAC-cím klónozása (MAC Address Clone) egy olyan funkció, amelynek segítségével egy konkrét címet adhatunk meg a forgalomirányító szolgáltató felőli interfészének MAC-forráscímeként. Számos internetszolgáltató az első beüzemeléshez használt eszköz MAC-címe alapján oszt IPv4-címet. Ha később egy másik eszközt, mint például egy kisirodai/otthoni forgalomirányítót csatlakoztatunk a szolgáltatóhoz, a szolgáltató megkövetelheti, hogy a WAN-interfészen az eredeti eszköz MAC-címe legyen beállítva.

# DHCP v4

## A DHCPv4 hibaelhárítása

A DHCPv4 problémáknak számos oka lehet. Okozhatják az operációs rendszerek szoftverhibái, a hálózati kártyák, a DHCP-közvetítők, de leggyakrabban konfigurációs hibákra vezethetők vissza. A potenciálisan problémás területek számából kifolyólag a hibaelhárítást módszeresen kell elvégeznünk, ahogy az ábrán is látható.

**1. hibaelhárítási feladat: Az IPv4-címek ütközésének feloldása**

Egy IPv4-cím bérlete lejárhat úgy is, hogy a kliens még a hálózatra kapcsolódik. Amennyiben a kliens nem újítja meg a bérletet, a DHCPv4-szerver kioszthatja ezt az IPv4-címet egy másik kliensnek. Amikor a kliens újraindul, IPv4-címet fog igényelni. Ha a DHCPv4-szerver nem válaszol elég gyorsan, a kliens az utolsó IPv4-címet veszi használatba. Ekkor fordul elő az a helyzet, amikor két kliens ugyanazt az IPv4-címet használja, vagyis ütközés lép fel.

A **show ip dhcp conflict** paranccsal kilistáztatható az összes olyan címütközés, amelyet a DHCP-szerver regisztrált. A szerver a **ping** parancs segítségével érzékeli a klienseket. A kliens az ARP címmeghatározó protokoll használatával érzékeli az ütközéseket. Címütközés esetén az érintett cím kikerül a kiosztható címek készletéből, és mindaddig vissza sem kerül, amíg a rendszergazda fel nem oldja az ütközést.

Az alábbi parancskimenet megjeleníti a problémás IP-címeket. Megmutatja a DHCP-szerver által kiosztott, ütközésben részt vevő IP-címek érzékelésének módját és idejét.

R1# **show ip dhcp conflict**

IP address Detection Method Detection time

192.168.10.32 Ping Feb 16 2013 12:28 PM

192.168.10.64 Gratuitous ARP Feb 23 2013 08:12 AM

**2. hibaelhárítási feladat: A fizikai kapcsolat ellenőrzése**

Először a **show interface** *interfész* parancs segítségével igazoljuk, hogy a kliens számára alapértelmezett átjáróként megadott forgalomirányító interfésze működőképes. Ha az interfész nincs működő állapotban, a forgalom - beleértve a DHCP-kliens kéréseit is - nem halad át a porton.

**3. hibaelhárítási feladat: A kapcsolat statikus IP-címmel történő ellenőrzése**

Ha bármilyen DHCPv4 problémába ütközünk, ellenőrizzük a hálózati kapcsolatot a kliensszámítógépen beállított statikus IPv4-címmel. Ha az állomás a statikusan beállított IPv4-címmel sem fér hozzá a hálózat erőforrásaihoz, akkor minden bizonnyal nem a DHCPv4-szolgáltatás felelős a hibáért. Ezen a ponton a hálózati kapcsolat hibaelhárítására van szükség.

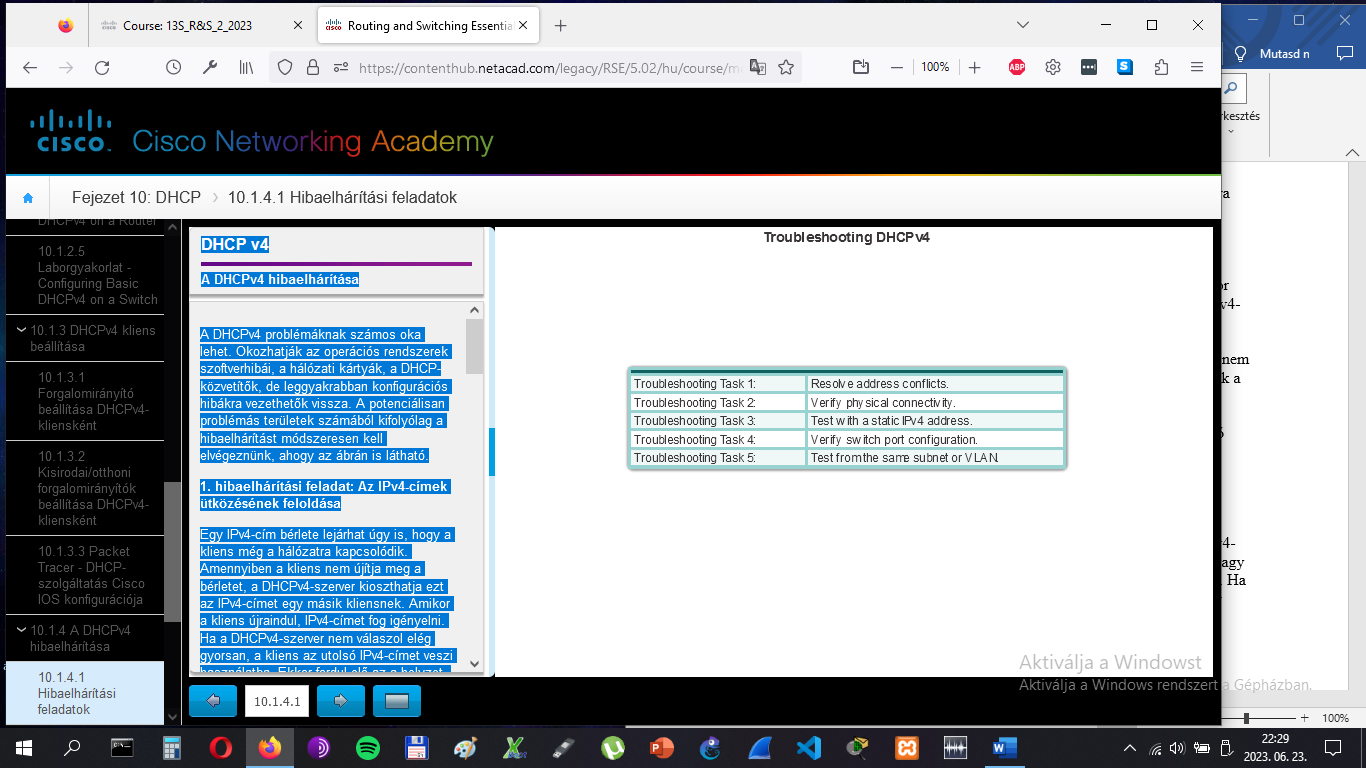
**4. hibaelhárítási feladat: A kapcsolóportok beállításainak ellenőrzése**

Ha a DHCPv4-kliens induláskor sem képes IPv4-címet kapni a DHCPv4-szervertől, akkor próbáljuk meg a klienst manuálisan egy DHCPv4-kérés küldésére kényszeríteni, hogy IPv4-címet szerezzen a DHCPv4-szervertől.

**MEGJEGYZÉS**: Ha a kliens és a DHCPv4-szerver között van egy kapcsoló, és a kliens nem kapja meg a DHCP-beállításokat, a kapcsolóportok beállításaival lehet gond. Ide tartoznak a trönkölésből, az összefogott csatornák kialakításából, valamint az STP és az RSTP használatából eredő problémák. A PortFast konfiguráció, valamint az élportok beállítása megoldja a DHCPv4-kliensek leggyakoribb problémáit, amelyek egy Cisco kapcsoló első üzembe helyezésénél fordulnak elő.

**5. hibaelhárítási feladat: A DHCPv4 egy alhálózaton vagy VLAN-on belüli működésének ellenőrzése**

Fontos felismerni, hogy a DHCPv4 megfelelően működik-e, amikor a kliens és a DHCPv4-szerver egy alhálózaton vagy VLAN-ban van. Amennyiben a DHCPv4 egy alhálózaton vagy VLAN-on belüli működése megfelelő, akkor a probléma forrása a DHCP-közvetítő lehet. Ha a probléma még azután is fennáll, hogy a DHCPv4 működését a szerver alhálózatán vagy VLAN-ján belül ellenőriztük, akkor magával a DHCPv4-szerverrel lehet gond.



# DHCP v4

## A DHCPv4 hibaelhárítása

Ha a DHCPv4-szerver és a kliens nem azonos szegmensen található, akkor a forgalomirányító kliens felőli interfészén engedélyezni kell a DHCPv4-kérések közvetítését az IPv4-segédcím megadásával. Amennyiben az IPv4-segédcím nincs megfelelően beállítva, a kliens DHCPv4-kérései nem lesznek továbbítva a DHCPv4-szerver felé.

A forgalomirányító beállításainak ellenőrzéséhez végezzük el az alábbi lépéseket:

**1. lépés** Ellenőrizzük, hogy az **ip helper-address** parancs kadása a megfelelő interfészen megtörtént. A DHCPv4-klienseket tartalmazó LAN bejövő interfészén kell megjelennie, és a megfelelő DHCPv4-szerver irányába kell mutatnia. Az ábrán látható a **show running-config** parancs kimenete, amellyel ellenőrizhető, hogy a DHCPv4-közvetítő IPv4-címe a 192.168.11.6 címen elérhető DHCPv4-szerverre hivatkozik-e.

A **show ip interface** paranccsal is ellenőrizhető, hogy egy interfészen be van-e állítva a DHCPv4-közvetítő.

**2. lépés** Ellenőrizzük, hogy a **no service dhcp** globális konfigurációs parancs nem lett-e kiadva. Ez a parancs letilt minden DHCP-szerver és -közvetítő funkciót a forgalomirányítón. A **service dhcp** parancs nem jelenik meg az aktív konfigurációban, mivel ez az alapértelmezés szerinti beállítás.

Az ábrán látható **show running-config | include no service dhcp** paranccsal ellenőrizhető, hogy a DHCPv4-szerver engedélyezve van, mivel nem ad találatot a **show running-config | include no service dhcp** parancsra. Ha a szolgáltatást letiltották volna, a **no service dhcp** parancs megjelenne a kimeneten.

# DHCP v4

## A DHCPv4 hibaelhárítása

A DHCPv4-szerverként beállított forgalomirányítókon a DHCPv4-folyamat sikertelen, ha a forgalomirányítóhoz nem érkeznek DHCP-kérések a klienstől. A hibaelhárítás részeként ellenőrizzük, hogy a forgalomirányítóhoz valóban érkeznek-e DHCPv4-kérések. Ez a lépés egy ACL beállítását is magában foglalja, hibakeresés céljából.

Az ábrán egy kiterjesztett ACL szerepel, amely kizárólag a 67-es és 68-as UDP-portra érkező csomagokat engedélyezi. Ezek jellemzően a DHCPv4-kliensek és -szerverek által DHCPv4-üzenetek küldésére használt portok. A kiterjesztett ACL a **debug ip packet** paranccsal együtt használva kizárólag a DHCPv4-üzeneteket jeleníti meg.

Az ábrán megjelenő parancskimenetből látszik, hogy a forgalomirányítóhoz érkeznek DHCP-kérések a klienstől. A forráscím 0.0.0.0, mivel a kliens még nem rendelkezik IP-címmel. A célcím 255.255.255.255, mivel a kliens által küldött DHCP-felfedezés szórásos üzenet. A kimenet csupán a csomag összegfoglalóját jeleníti meg, nem magát a DHCPv4-üzenetet. Ennek ellenére a forgalomirányító megkapta a DHCPv4-hez tartozó IP és UDP forrás- és célportokra érkező szórásos csomagokat. A teljes hibakeresési kimenet megjeleníti a DHCPv4-szerver és -kliens között zajló DHCPv4 kommunikáció összes csomagját.

Egy másik hasznos utasítás a DHCPv4 működésével kapcsolatos hibakereséshez a **debug ip dhcp server events** parancs. A fenti utasítás beszámol a címkiosztásokhoz és adatbázis-frissítésekhez hasonló szervereseményekről. Ezen felül a DHCPv4 küldések és fogadások dekódolására is használatos.

# DHCP v6

## SLAAC és DHCPv6

Az IPv4-hez hasonlóan az IPv6 globális egyedi címek beállítása történhet manuálisan és dinamikusan egyaránt. Az IPv6 globális egyedi címek dinamikus kiosztására viszont két módszer is létezik:

* SLAAC (az ábrán látható módon)
* Állapottartó DHCPv6

**A SLAAC bemutatása**

A SLAAC egy olyan módszer, amellyel egy DHCPv6-szerver szolgáltatásai nélkül szerezhetnek az eszközök IPv6 globális egyedi címet. A SLAAC működése az ICMPv6 protokollon alapul. Az ICMPv6 az ICMPv4-hez hasonló, de annál sokkal robusztusabb protokoll, amely további funkcionalitást kínál. A SLAAC az ICMPv6 protokoll forgalomirányító-keresés és forgalomirányító-hirdetés üzeneteinek segítségével kínál címzési és egyéb konfigurációs adatokat, amelyeket normál esetben egy DHCP-szerver biztosítana.

* **Forgalomirányító-keresés (Router Solicitation, RS) üzenet** - Ha egy kliens úgy van beállítva, hogy a címzési adatokat automatikusan a SLAAC-tól kapja, akkor egy RS-üzenetet küld a forgalomirányítónak. Az RS-üzenetet az IPv6 összes forgalomirányítót magába foglaló (all-routers nevű) FF02::2 csoportcímére küldik el.
* **Forgalomirányító-hirdetés (Router Advertisement, RA) üzenet** Az RA-üzeneteket a forgalomirányítók küldik, hogy címzési információt biztosítsanak azon klienseknek, amelyeket az IPv6-címük automatikus megszerzésére állítottak be. Az RA-üzenet tartalmazza a helyi szegmens előtagját és az előtag hosszát. A kliens ezen információk segítségével hozza létre a saját IPv6 globális egyedi címét. A forgalomirányító rendszeres időközönként, vagy egy RS-üzenetre válaszolva küld ki RA-üzeneteket. Alapértelmezés szerint a Cisco forgalomirányítók 200 másodpercenként küldenek RA-üzenetet. Az RA-üzeneteket mindig az IPv6 összes állomást tartalmazó (all-nodes nevű) FF02::1 csoportcímére küldik.

A SLAAC a nevéből eredően nem állapottartó. Az állapotmentes szolgáltatás azt jelenti, hogy nincs olyan szerver, amely karbantartja a hálózati címadatokat. A DHCP-vel ellentétben nincs olyan SLAAC-szerver, amely tudja, hogy melyek a használatban lévő, és melyek a rendelkezésre álló IPv6-címek.

# DHCP v6

## SLAAC és DHCPv6

Mielőtt egy forgalomirányító RA-üzeneteket küldhetne, engedélyezni kell rajta az IPv6-irányítást. Ennek engedélyezéséhez használjuk az alábbi parancsot:

Router(config)# **ipv6 unicast-routing**

1. Az 1. ábrán látható topológia szerint a PC1 úgy van beállítva, hogy automatikusan szerezzen magának IPv6-címet. Mivel a PC1 nem kapott RA-üzenetet az elindítása óta, ezért egy RS-üzenetet küld az összes forgalomirányítót tartalmazó (all-routers) csoportcímre, amelyben jelzi a helyi IPv6-forgalomirányító felé, hogy szüksége van egy RA-üzenetre.

2. Ahogy a 2. ábrán is látszik, az R1 megkapja az RS-üzenetet, amelyre egy RA-üzenettel válaszol. Az RA üzenet tartalmazza a hálózat előtagját, valamint az előtag hosszát. Az RA-üzenet elküldése az IPv6 összes állomást tartalmazó (all-nodes) FF02::1 csoportcímére történik, amelyben a forgalomirányító link-local címe van megadva IPv6-forráscímként.

3. A PC1 megkapja a helyi hálózat előtagját és az előtag hosszát tartalmazó RA-üzenetet. A PC1 ezen információk alapján létrehozza a saját IPv6 globális egyedi címét. A PC1 már rendelkezik egy 64-bites hálózati előtaggal, de egy globális egyedi cím létrehozásához szüksége van egy 64-bites interfészazonosítóra (Interface ID, IID) is.

Annak, hogy a PC1 létrehozhassa a saját, egyedi IID-jét, két módja van:

* **EUI-64** - Az EUI-64 folyamat segítségével a PC1 a 48-bites MAC-címe alapján hoz létre egy IID-t.
* **Véletlenszerűen generált** - A 64-bites IID lehet egy, a kliens operációs rendszere által generált véletlen szám.

A PC1 a 64-bites előtag és a 64-bites interfészazonosító kombinálásával létrehozhat egy 128-bites IPv6 globális egyedi címet a 3. ábrán látható módon. A PC1 a forgalomirányító link-local címét használja az alapértelmezett átjáró címeként.

4. Mivel a SLAAC protokoll állapotmentes, ezért a PC1-nek használat előtt ellenőriznie kell az újonnan létrehozott IPv6-cím egyediségét. Ahogy a 4. ábrán is látszik, a PC1 egy ICMPv6 szomszédkeresés (Neighbor Solicitation) üzenetet küld ki, amelyben a saját címe van megadva IPv6-célcímként. Ha semmilyen másik eszköz nem válaszol a szomszédkeresés üzenetre, akkor a cím egyedi és a PC1 használatba veheti. Ha egy szomszédhirdetés (Neighbor Advertisement) üzenet érkezik válaszként a PC1-nek, akkor a cím mégsem egyedi, így az operációs rendszernek kell meghatározni az új interfészazonosítót.

Ez a folyamat az ICMPv6 szomszédfelderítő (Neighbor Discovery) protokolljának részét képezi, és címütközés-érzékelés (Duplicate Address Detection, DAD) néven is ismert.

# DHCP v6

## SLAAC és DHCPv6

Az, hogy egy kliens az IPv6-címadatait a SLAAC vagy a DHCPv6 használatával, esetleg a kettő kombinációjával szerezze meg, az RA-üzenetben lévő beállításokon múlik. Az ICMPv6 RA-üzenetei két jelzőbitet tartalmaznak, annak jelölésére, hogy a kliensnek melyik lehetőséget kellene választania.

Az egyik a felügyelt címkonfigurációs jelzőbit (Managed Address Configuration flag, M jelzőbit), a másik az egyéb konfigurációs jelzőbit (Other Configuration flag, O jelzőbit).

Az M és az O jelzőbit különböző kombinációjával, az RA-üzenetek három címzési lehetőség egyikét kínálják az IPv6 eszköz számára az ábrán látható módon:

* SLAAC (csak forgalomirányító-hirdetéssel)
* Állapotmentes DHCPv6 (forgalomirányító-hirdetéssel és DHCPv6-tal)
* Állapottartó DHCPv6 (csak DHCPv6-tal)

Függetlenül a használt módtól az RFC 4861 azt javasolja, hogy minden IPv6 eszköz végezze el a címütközés-érzékelést bármely egyedi címre vonatkozóan, beleértve a SLAAC és DHCPv6 együttes használatával beállított címeket is.

**MEGJEGYZÉS**: Habár az RA-üzenet meghatározza a kliens IPv6-címének dinamikus megszerzéséhez javasolt folyamatot, a kliens operációs rendszere mégis dönthet úgy, hogy figyelmen kívül hagyja az RA-üzenetet, és kizárólag egy DHCPv6-szerver szolgáltatásait veszi igénybe.

# DHCP v6

## SLAAC és DHCPv6

**A SLAAC opció (csak forgalomirányító-hirdetéssel)**

A Cisco forgalomirányítókon a SLAAC az alapértelmezett lehetőség. Ahogy az ábrán is látszik, ilyenkor az M és az O jelzőbit értéke egyaránt 0 az RA-üzenetben.

Ez a lehetőség arra utasítja a klienst, hogy kizárólag az RA-üzenet információit használja. Ebbe beletartoznak az előtagra, az előtag hosszára, a DNS-szerverre, az MTU-ra, valamint az alapértelmezett átjáróra vonatkozó adatok. További információt a DHCPv6-szervertől sem fog kapni. Az IPv6 globális egyedi cím létrehozása úgy történik, hogy az RA-üzenet előtagját kombináljuk az EUI-64 folyamat során vagy véletlenszerűen generált interfészazonosítóval.

Az RA-üzenetek beállítása a forgalomirányítók egyes interfészein történik. Ahhoz, hogy egy másik opcióra állított interfészen ismételten engedélyezzük a SLAAC működését, az M és az O jelzőbitek kezdőértékét vissza kell állítani 0-ra. Ezt az alábbi, globális konfigurációs parancsokkal tehetjük meg:

Router(config-if)# **no** **ipv6 nd managed-config-flag**

Router(config-if)# **no ipv6 nd other-config-flag**

# DHCP v6

## SLAAC és DHCPv6

Habár a DHCPv6 a kínált szolgáltatások tekintetében sokban hasonlít a DHCPv4-hez, a két protokoll egymástól teljesen független. Az DHCPv6-ot az RFC 3315 definiálja. A specifikáció nagyon komoly munka eredménye, amit jól mutat az a tény, hogy az összes internetes szabványtervezet közül a DHCPv6 RFC-jét dolgozták át a legtöbbször.

**Az állapotmentes DHCPv6 opció (forgalomirányító-hirdetéssel és DHCPv6-tal)**

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.

Az RA-üzenetben szereplő előtaggal és az előtag hosszával, valamint az EUI-64 segítségével vagy véletlenszerűen generált interfészazonosítóval, a kliens létrehozza a saját IPv6 globális egyedi címét.

A kliens ezután kommunikálni kezd egy állapotmentes DHCPv6-szerverrel, hogy megszerezze az RA-üzenetben nem szereplő további adatokat. Ez lehet például egy DNS-szerverek IPv6-címeit tartalmazó lista. 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 állapotmentes DHCPv6 esetében az O jelzőbit értékét 1-re kell állítani, az M jelzőbit értéke pedig maradjon az alapértelmezés szerinti 0. Az O jelzőbit 1-es értéke jelzi a kliens számára, hogy további konfigurációs beállítások állnak rendelkezésre egy állapotmentes DHCPv6-szerveren.

Ahhoz, hogy egy forgalomirányító interfészén kiküldött RA-üzenetet úgy módosítsunk, hogy az állapotmentes DHCPv6-ot jelöljön, használjuk az alábbi parancsot:

Router(config-if)# **ipv6 nd other-config-flag**

# DHCP v6

## SLAAC és DHCPv6

**Állapottartó DHCPv6 (csak DHCPv6-tal)**

Ez a lehetőség hasonlít legjobban a DHCPv4-hez. Ebben az esetben az RA-üzenet azt jelzi a kliensnek, hogy ne használja az RA-üzenet információit. Így minden címzési és konfigurációs adatot egy DHCPv6-szervertől kell megszereznie. 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 M jelzőbit mutatja, hogy szükség van-e az állapottartó DHCPv6 használatára. Az O jelzőbitnek ebben nincs szerepe. Az állapottartó DHCPv6 kifejezhető azzal, ha az alábbi parancs segítségével átállítjuk az M jelzőbit értékét 0-ról 1-re:

Router(config-if)# **ipv6 nd managed-config-flag**

# DHCP v6

## SLAAC és DHCPv6

Ahogy az 1. ábrán is látszik, mindegy, hogy állapotmentes vagy állapottartó DHCPv6-ról van szó, minden a forgalomirányítótól érkező ICMPv6-üzenettel kezdődik. Az RA-üzenet lehet periodikus, de kérelmezheti egy RS-üzenetet küldő eszköz is.

Ha az RA-üzenet állapotmentes vagy állapottartó DHCPv6-ot jelez, akkor az eszköz DHCPv6 kliens/szerver kommunikációt kezdeményez.

**DHCPv6 kommunikáció**

Ha az RA-üzenet állapotmentes vagy állapottartó DHCPv6-ot jelez, a DHCPv6 műveleteket hívjuk segítségül. A DHCPv6-üzenetek küldése UDP-n keresztül történik. A szerver által a kliensnek küldött DHCPv6-üzenetek az UDP 546-os célportját használják. A kliens által a szervernek küldött DHCPv6-üzenetek pedig az UDP 547-es célportját használják.

A kliensnek, amely jelen esetben egy DHCPv6-kliens, találnia kell egy DHCPv6-szervert. A 2. ábrán a kliens egy DHCPv6 SOLICIT üzenetet küld az IPv6 összes DHCPv6-szervert tartalmazó (all-DHCPv6-servers nevű) FF02::1:2 csoportcímére. Ez a csoportcím link-local hatókörrel rendelkezik, ami azt jelenti, hogy a forgalomirányítók nem továbbítják az üzeneteket más hálózatokba.

Ahogy a 3. ábrán is látszik, egy vagy több DHCPv6-szerver DHCPv6 ADVERTISE üzenet küldésével válaszol. Az ADVERTISE üzenet jelzi a DHCPv6-kliens számára, hogy a szerver elérhető DHCPv6-szolgáltatással rendelkezik.

A 4. ábrán a kliens válaszként egy DHCPv6 REQUEST vagy INFORMATION-REQUEST üzenetet küld a szervernek, attól függően, hogy állapottartó vagy állapotmentes DHCPv6-ról van szó.

* **Állapotmentes DHCPv6-kliens** - A kliens egy olyan DHCPv6 INFORMATION-REQUEST üzenetet küld a DHCPv6-szervernek, amely kizárólag a konfigurációs beállításokat kéri. (Ilyen például a DNS-szerver címe.) A kliens úgy generálta a saját IPv6-címét, hogy az RA-üzenetben szereplő előtagot, valamint egy önmaga által generált interfészazonosítót használt.
* **Állapottartó DHCPv6-kliens** - A kliens egy DHCPv6 REQUEST üzenetet küld a szervernek, hogy az IPv6-címet az összes egyéb konfigurációs beállítással együtt a szervertől szerezze meg.

Ahogy az 5. ábrán is látszik, a szerver válaszként egy DHCPv6 REPLY üzenetet küld a kliensnek, amely tartalmazza a REQUEST vagy INFORMATION-REQUEST üzenetben kért adatokat.

# DHCP v6

## Állapotmentes DHCPv6

Ahogy az 1. ábrán is látszik, egy forgalomirányító négy lépésben állítható be DHCPv6-szervernek.

**1. lépés: Az IPv6-irányítás engedélyezése**

Az **ipv6 unicast-routing** paranccsal engedélyezhető az IPv6-irányítás. Ez a parancs nem szükséges ahhoz, hogy a forgalomirányító állapotmentes DHCPv6-szerver legyen, de az ICMPv6 RA-üzeneteinek küldéséhez nélkülözhetetlen.

**2. lépés: DHCPv6 készlet beállítása**

Az **ipv6 dhcp pool** *készlet-neve* parancs egy címkészletet hoz létre a megadott néven, majd DHCPv6 konfigurációs módba lépteti a forgalomirányítót, amelyet a Router(config-dhcpv6)# prompt jelez.

**3. lépés: A készlet paramétereinek beállítása**

A SLAAC folyamat során a kliens megkapta a saját IPv6 globális egyedi címének létrehozásához szükséges információkat. A kliens az alapértelmezett átjáró adatait is megkapta az RA-üzenetben szereplő IPv6-forráscím alapján, amely a forgalomirányító link-local címe. Az állapotmentes DHCPv6-szerver azonban úgy is beállítható, hogy egyéb információkat is biztosítson, amelyek nem feltétlenül szerepeltek az RA-üzenetben. (Ilyen például a DNS-szerver címe, valamint a tartomány neve.)

**4. lépés: A DHCPv6-interfész beállítása**

Az **ipv6 dhcp server** *készlet-neve* interfészkonfigurációs parancs a DHCPv6-készletet hozzárendeli az interfészhez. Az állapotmentes DHCPv6-kérésekre a forgalomirányító válaszként a készletben szereplő információkat küldi ki a fenti interfészen. Az O jelzőbit értékét át kell állítani 0-ról 1-re, az **ipv6 nd other-config-flag** interfészkonfigurációs parancs segítségével. A fenti interfészen küldött RA-üzenetek azt jelzik, hogy további információ áll rendelkezésre az állapotmentes DHCPv6-szerveren.

**Példa egy állapotmentes DHCPv6-szerverre**

A 2. ábrán egy forgalomirányító állapotmentes DHCPv6-szerverként történő beállítására láthatunk példát. Vegyük észre, hogy az R3 forgalomirányító DHCPv6-kliensként szerepel benne! Az R3 forgalomirányító kliensként történő beállítása segít az állapotmentes DHCPv6-műveletek ellenőrzésében.

# DHCP v6

## Állapotmentes DHCPv6

Az ábrán látható példában egy Cisco forgalomirányító tölti be a DHCPv6-kliens szerepét. Ez nem egy szokványos eset, kizárólag szemléltetés céljából használjuk. Az állapotmentes DHCPv6-kliens jellemzően valamilyen eszköz. Lehet például számítógép, táblagép, mobil eszköz vagy webkamera.

A kliens szerepét betöltő forgalomirányító interfészének szüksége van egy IPv6 link-local címre az olyan IPv6-címek küldésére és fogadására, mint amilyenek az RS-üzenetek és a DHCPv6-üzenetek. Az interfész link-local címe automatikusan létrejön, ha az interfészen engedélyezett az IPv6-protokoll. Ez akkor fordulhat elő, amikor beállítunk az interfészen egy globális egyedi címet az **ipv6 enable** paranccsal. Miután a forgalomirányító megkapja a link-local címét, küldhet RS-üzeneteket és részt vehet a DHCPv6-folyamatban is.

Ebben a példában az **ipv6 enable** parancsot használjuk, mivel a forgalomirányító még nem rendelkezik globális egyedi címmel.

Az **ipv6 address autoconfig** paranccsal engedélyezhető az IPv6-címadatok SLAAC használatával történő automatikus beállítása. Ezután a kliens szerepét betöltő forgalomirányító egy RA-üzenet segítségével értesül, hogy az állapotmentes DHCPv6-ot kell használnia.

# DHCP v6

## Állapotmentes DHCPv6

**Az állapotmentes DHCPv6-szerver ellenőrzése**

Az 1. ábrán látható **show ipv6 dhcp pool** paranccsal ellenőrizhető a DHCPv6-készlet neve és beállításai. Az aktív kliensek száma 0, mivel nincs olyan állapot, amelyet karbantartana a szerver.

A **show running-config** paranccsal szintén ellenőrizhető az összes korábban beállított utasítás.

**Az állapotmentes DHCPv6-kliens ellenőrzése**

Az ábrán látható példában egy forgalomirányító tölti be az állapotmentes DHCPv6-kliens szerepét. A 2. ábrán a **show ipv6 interface** parancs kimenetéből látszik, hogy a forgalomirányítón engedélyezve van az állapotmentes cím automatikus konfigurációja: "Stateless address autoconfig enabled", valamint az, hogy a forgalomirányító rendelkezik globális egyedi IPv6 címmel. Az IPv6 globális egyedi cím létrehozása a SLAAC használatával történt, amely tartalmazza az RA-üzenetben szereplő előtagot. Az interfészazonosító generálása az EUI-64 segítségével történt. Az IPv6-cím kiosztása nem a DHCPv6 segítségével valósult meg.

Az alapértelmezett forgalomirányító adatai szintén az RA-üzenetből származnak. Ez annak a csomagnak az IPv6-forráscíme, amely az RA-üzenetet és a forgalomirányító link-local címét tartalmazta.

A 3. ábrán a **debug ipv6 dhcp detail** parancs kimenete megjeleníti a kliens és a szerver között váltott DHCPv6-üzeneteket. Ebben a példában a parancsbevitel a kliensen történt. Az INFORMATION-REQUEST üzenet azért látszik, mert egy állapotmentes DHCPv6-kliensről küldték. Figyeljük meg, hogy a kliens szerepét betöltő R3 forgalomirányító a DHCPv6-üzeneteket a link-local címéről küldi az összes DHCPv6-közvetítőt és -szervert tartalmazó (All\_DHCPv6\_Relay\_Agents\_and\_Servers nevű) FF02::1:2 címre.

A hibakeresési kimenet megjeleníti a kliens és a szerver között váltott összes DHCPv6-üzenetet, beleértve a DNS-szervert és a szerveren megadott tartománynév-beállításokat.

A 4. ábrán található parancsszimulátor segítségével állítsuk be és ellenőrizzük a forgalomirányítón az állapotmentes DHCPv6-ot!

# DHCP v6

## Állapottartó DHCPv6-szerver

Egy állapottartó DHCPv6-szerver beállítása nem sokban különbözik egy állapotmentes szerver beállításától. A legjelentősebb eltérés az, hogy egy állapottartó szerver a DHCPv4-szerverekhez hasonlóan IPv6-címadatokat is tartalmaz.

**1. lépés: Az IPv6-irányítás engedélyezése**

Az ábrán látható módon használjuk az **ipv6 unicast-routing** parancsot az IPv6-irányítás engedélyezéséhez. Ez a parancs nem szükséges ahhoz, hogy a forgalomirányító állapottartó DHCPv6-szerver legyen, de az ICMPv6 RA-üzeneteinek küldéséhez nélkülözhetetlen.

**2. lépés:** **DHCPv6 készlet beállítása**

Az **ipv6 dhcp pool** *készlet-neve* parancs egy címkészletet hoz létre a megadott névvel, majd DHCPv6 konfigurációs módba lépteti a forgalomirányítót, amelyet a Router(config-dhcpv6)# prompt jelez.

**3. lépés:** **A készlet paramétereinek beállítása**

Az állapottartó DHCPv6 esetében minden címzési és konfigurációs adatot a DHCPv6-szervernek kell kiosztania. Az **address** *prefix/hossz* parancs kiadásával jelezhetjük, hogy a címkészletet a szerver osztja ki. A **lifetime** paraméter mutatja az érvényben lévő, valamint az előnyben részesített bérleti időt, másodpercben megadva. Csakúgy, mint az állapotmentes DHCPv6 esetében, a kliens annak a csomagnak az IPv6-forráscímét használja, amely tartalmazta az RA-üzenetet.

Az állapottartó DHCPv6-szerver által biztosított egyéb információk között jellemzően szerepel a DNS-szerver címe, valamint a tartomány neve.

**4. lépés: Az interfészkonfigurációs parancsok**

Az **ipv6 dhcp server** *készlet-neve* interfészkonfigurációs parancs a DHCPv6-készletet hozzárendeli az interfészhez. Az állapotmentes DHCPv6-kérésekre a forgalomirányító válaszként a készletben szereplő információkat küldi ki a fenti interfészen. Az M jelzőbit értékét át kell állítani 0-ról 1-re, az **ipv6 nd managed-config-flag** interfészkonfigurációs paranccsal. Ez értesíti az eszközt, hogy ne a SLAAC-t használja, hanem egy állapottartó DHCPv6-szervertől szerezze meg a címadatokat és az összes konfigurációs beállítást.

**Példa egy állapottartó DHCPv6-szerverre**

A 2. ábrán az R1 forgalomirányító állapottartó DHCPv6-szerverként történő beállítására láthatunk példát. Vegyük észre, hogy az alapértelmezett átjáró nincs megadva, mivel a forgalomirányító automatikusan a saját link-local címét küldi el alapértelmezett átjáróként! Az R3 forgalomirányító kliensként történő beállítása segít az állapottartó DHCPv6-műveletek ellenőrzésében.

# DHCP v6

## Állapottartó DHCPv6-szerver

Az ábrán látható módon használjuk az **ipv6 enable** interfészkonfigurációs parancsot, hogy a forgalomirányító megkapja a link-local címét, küldhessen RS-üzeneteket és részt vehessen a DHCPv6-folyamatban is.

Az **ipv6 address dhcp** interfészkonfigurációs paranccsal engedélyezhetjük, hogy a forgalomirányító DHCPv6-kliensként viselkedjen ezen az interfészen.

# DHCP v6

## Állapottartó DHCPv6-szerver

**Az állapottartó DHCPv6-szerver ellenőrzése**

Az 1. ábrán a **show ipv6 dhcp pool** paranccsal ellenőrizhető a DHCPv6-készlet neve és beállításai. Az aktív kliensek száma 1, amely azt tükrözi, hogy az R3 kliens a szervertől kapja meg az IPv6 globális egyedi címét.

A **show ipv6 dhcp binding** parancs megjeleníti a kliens link-local címének a szerver által kiosztott címhez történő automatikus hozzárendelését a 2. ábrán látható módon. A kliens link-local címe az FE80::32F7:DFF:FE25:2DE1. Ebben a példában ez az R3 forgalomirányító G0/1 interfésze. Ez a cím hozzá van rendelve a 2001:DB8:CAFE:1:5844:47B2:2603:C171 IPv6 globális egyedi címhez, amelyet a DHCPv6-szerver szerepét betöltő R1 forgalomirányító osztott ki. Ezen adatokat egy állapottartó, nem pedig egy állapotmentes DHCPv6-szerver tartja karban.

**Az állapottartó DHCPv6-kliens ellenőrzése**

A **show ipv6 interface** parancs ellenőrzi, hogy a DHCPv6-kliens szerepét betöltő R3 forgalomirányító IPv6 globális egyedi címét a DHCPv6-szerver osztotta-e ki. Az alapértelmezett forgalomirányító adatai nem a DHCPv6-szervertől származnak, hanem az RA-üzenetben szereplő IPv6-forráscím alapján kerültek meghatározásra. Habár a kliens nem veszi figyelembe az RA-üzenetben szereplő adatokat, így is használhatja az IPv6-forráscímet alapértelmezett átjáróként.

A 4. ábrán található parancsszimulátor segítségével állítsuk be és ellenőrizzük a forgalomirányítón az állapottartó DHCPv6-ot!

# DHCP v6

## Állapottartó DHCPv6-szerver

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.

**MEGJEGYZÉS**: Habár egy DHCP-közvetítő beállítása nem sokban különbözik DHCPv6 és DHCPv4 esetén, az IPv6-forgalomirányítók és -közvetítők kissé eltérő módon továbbítják a DHCPv6-üzeneteket, mint a DHCPv4-közvetítők. Ezek az üzenetek és a folyamat túlmutatnak a jelen tananyag keretein.

Az 1. ábrán látható topológia szerint a 2001:DB8:CAFE:1::/64 hálózaton található egy DHCPv6-szerver. A hálózati rendszergazda ezt egy központi, állapottartó DHCPv6-szerverként kívánja használni, amely az összes kliens IPv6-címének kiosztásáért felel. Ennek következtében a más hálózatra kapcsolódó klienseknek.(például a 2001:DB8:CAFE:A::/64 hálózaton lévő PC1-nek) kommunikálniuk kell a DHCPv6-szerverrel.

A kliensektől származó DHCPv6-üzenetek kiküldése az összes DHCPv6-közvetítőt és -szervert tartalmazó (All\_DHCPv6\_Relay\_Agents\_and\_Servers nevű) FF02::1:2 címre történik. Ez a cím link-local hatókörrel rendelkezik, ami azt jelenti, hogy a forgalomirányítók nem továbbítják az üzeneteket más hálózatokba. Ahhoz, hogy a DHCPv6-szerver és -kliens képes legyen egymással kommunikálni, az IPv6-forgalomirányítót DHCPv6-közvetítőként kell beállítanunk.

**A DHCPv6-közvetítő beállítása**

Ahogy a 3. ábrán is látszik, egy DHCPv6-közvetítő beállítása az **ipv6 dhcp relay destination** paranccsal történik. Ezt a parancsot a DHCPv6-kliens felőli interfészen kell kiadni, célként pedig a DHCPv6-szerver címe legyen megadva.

A **show ipv6 dhcp interface** paranccsal ellenőrizhető, hogy a G0/0 interfész közvetítő módban van-e, valamint a 2001:DB8:CAFE:1::6 cím van-e DHCPv6-szerverként megadva.

Az 3. ábrán található parancsszimulátor segítségével a megfelelő forgalomirányítón beállíthatók a DHCPv6 közvetítő parancsok, így a PC3 kaphat IPv6-címet a DHCPv6-szervertől. Vegyük alapul az 1. ábrán látható hálózat topológiáját!

# DHCP v6

## A DHCPv6 hibaelhárítása

A DHCPv6 hibaelhárítása nem sokban különbözik a DHCPv4 hibaelhárításától.

**1. hibaelhárítási feladat: Címütközések feloldása**

Az IPv4-címekhez hasonlóan egy IPv6-cím bérlete is lejárhat úgy, hogy a kliens még a hálózatra kapcsolódik. A **show ipv6 dhcp conflict** parancs megjeleníti az állapottartó DHCPv6-szerver által naplózott címütközéseket. IPv6-címütközés esetén a kliens jellemzően eltávolítja a címet, majd új címet generál a SLAAC vagy az állapottartó DHCPv6 használatával.

**2. hibaelhárítási feladat: A címkiosztási mód ellenőrzése**

A **show ipv6 interface** *interfész* parancs használatával ellenőrizhető, hogy az RA-üzenetben szereplő címkiosztás módja megfelel-e az M és az O jelzőbitek beállításainak. Ez az információ a parancskimenet utolsó soraiban szerepel. Amennyiben valamely eszköz nem kap IPv6-címadatokat egy állapottartó DHCPv6-szervertől, ez lehet az RA-üzenetben szereplő M és O jelzőbitek nem megfelelő beállítása miatt.

**3. hibaelhárítási feladat: A kapcsolat statikus IP-címmel történő ellenőrzése**

Ha bármilyen DHCP problémába ütközünk (akár DHCPv4-ről, akár DHCPv6-ról van szó), ellenőrizzük a hálózati kapcsolatot a kliensszámítógépen beállított statikus IP-címmel. IPv6 esetében, ha az állomás a statikusan beállított IPv6-címmel sem fér hozzá a hálózat erőforrásaihoz, akkor minden bizonnyal nem a SLAAC vagy a DHCPv6-szolgáltatás felelős a hibáért. Ezen a ponton a hálózati kapcsolat hibaelhárítására van szükség.

**4. hibaelhárítási feladat: A kapcsolóportok beállításainak ellenőrzése**

Ha a DHCPv6-kliens nem képes címadatokat szerezni egy DHCPv6-szervertől, akkor ellenőrizzük, hogy a kapcsolóport engedélyezve van-e és megfelelően működik-e.

**MEGJEGYZÉS**: Ha a kliens és a DHCPv6-szerver között van egy kapcsoló, valamint a kliens nem kapja meg a DHCP-beállításokat, a kapcsolóportok beállításaival lehet gond. Ide tartoznak a trönkölésből, az összefogott csatornák kialakításából, valamint az STP és az RSTP használatából eredő problémák. A PortFast konfiguráció, valamint az élportok beállítása megoldja a DHCPv6-kliensek leggyakoribb problémáit, amelyek egy Cisco kapcsoló első üzembe helyezésénél fordulnak elő.

**5. hibaelhárítási feladat: A DHCPv6 egy alhálózaton vagy VLAN-on belüli működésének ellenőrzése**

Ha az állapotmentes vagy állapottartó DHCPv6-szerver megfelelően működik, de a klienstől eltérő hálózaton van, akkor az IPv6-forgalomirányítót beállíthatjuk DHCPv6-közvetítőként. Ehhez a forgalomirányító kliens felőli interfészén engedélyezni kell az **ipv6 dhcp relay destination** parancsot.

# DHCP v6

## A DHCPv6 hibaelhárítása

Az állapotmentes és az állapottartó DHCPv6-szolgáltatások forgalomirányítón történő beállításában sok a hasonlóság, de jelentős különbségek is felfedezhetők. Az 1. ábrán mindkét DHCPv6-szolgáltatástípus konfigurációs parancsai megtalálhatók.

**Állapottartó DHCPv6**

Egy állapottartó DHCPv6-szolgáltatások nyújtására konfigurált forgalomirányítón az **address prefix** paranccsal történik a címadatok biztosítása.

Az állapottartó DHCPv6-szolgáltatások beállítása az **ipv6 nd managed-config-flag** interfészkonfigurációs paranccsal történik. Ebben a példában a kliens figyelmen kívül hagyja az RA-üzenetben szereplő információkat, és a címadatokat és egyéb beállításokat egyaránt egy DHCPv6-szervertől kéri.

**Állapotmentes DHCPv6**

Az állapotmentes DHCPv6-szolgáltatások beállítása az **ipv6 nd other-config-flag** interfészkonfigurációs paranccsal történik. Ez értesíti az eszközt, hogy a címadatokat a SLAAC-tól, a többi konfigurációs beállítást pedig a DHCPv6-szervertől kell igényelnie.

A **show ipv6 interface** parancs használható a címkiosztási mód jelenlegi beállításainak megtekintésére. Ahogy a 2. ábrán is látszik, a parancskimenet utolsó sora megjeleníti, hogy a kliensek milyen módon szerzik meg a címüket és a többi beállítást.

# DHCP v6

## A DHCPv6 hibaelhárítása

Ha a forgalomirányító állapotmentes vagy állapottartó DHCPv6-szerverként van beállítva, a **debug ipv6 dhcp detail** parancs segítségével ellenőrizhető a DHCPv6-üzenetek küldése és fogadása. Ahogy az ábrán is látszik, az állapottartó DHCPv6-forgalomirányító SOLICIT üzenetet kapott egy klienstől. A hozzárendeléseknél a forgalomirányító az IPV6-STATEFUL nevű készletében szereplő címadatokat fogja használni.

# Összefoglalás

## Összefoglalás

**Feladat - A "minden a hálón" és a DHCP**

Ez a fejezet a kis- és középvállalatok hálózataiban használt DHCP-folyamat fogalmát mutatja be. De a DHCP nem csak erre használható!

A "minden a hálón" (Internet of Everything, IoE) megjelenésével a vezetékes vagy vezeték nélküli hálózati kapcsolódásra képes otthoni eszközeink bármelyike elérhető lesz szinte bárhonnan.

A modellezési feladat Packet Tracer-ben történő megoldásához végezzük el az alábbi lépéseket:

* Az IPv4 és az IPv6 alapú címzéshez állítsunk be egy Cisco 1941-es forgalomirányítót, vagy egy DHCP-szerverképes integrált eszközt.
* Gondoljunk öt olyan otthoni eszközre, amelynek IP-címet szeretnénk kérni (és kapni) a forgalomirányító DHCP-szolgáltatásától. Állítsuk be a végberendezéseket úgy, hogy a DHCP-szervertől igényeljenek DHCP-címet.
* Jelenítsük meg azt a kimenetet, amely igazolja, hogy minden egyes végberendezés IP-címet kapott a szervertől. A parancskimenetről készítsünk képernyőmentést egy külső program segítségével vagy a **PrtScrn** billentyűparanccsal.
* Mutassuk be a meglátásainkat egy csoporttársunknak vagy az egész osztálynak.

[Csoportos feladat - IoE and DHCP Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/10.3.1.1%20IoE%20and%20DHCP%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

Minden hálózatba kötött állomásnak egyedi IP-címmel kell rendelkeznie, hogy más eszközökkel kommunikálhasson. Az IP-címek statikus kiosztása nagyméretű hálózatok esetében adminisztratív terhet jelent, de ez kiküszöbölhető, ha az IPv4- és IPv6-címek kiosztása dinamikusan történik, a DHCPv4 és a DHCPv6 segítségével.

A DHCPv4 három különböző kiosztási módot támogat, hogy megfelelő rugalmasságot biztosítson az IP-címek kiosztásánál:

* **Manuális kiosztás** - A rendszergazda egy előre kiosztott IPv4-címet rendel a klienshez, a DHCPv4 kizárólag az IPv4-címet kommunikálja az eszköz felé.
* **Automatikus kiosztás** - A DHCPv4 automatikusan hozzárendel egy statikus IPv4-címet az eszközhöz, amelyet a rendelkezésre álló címkészletből választ ki, méghozzá állandó jelleggel. Nincs szó bérletről, a számítógéphez mindig ez a cím lesz hozzárendelve.
* **Dinamikus kiosztás** - A rendelkezésre álló címkészletből a DHCPv4 dinamikusan kioszt vagy bérbe ad egy IPv4-címet a szerver által meghatározott, vagy a kliens által igényelt ideig.

A dinamikus kiosztás a legelterjedtebb DHCPv4-eljárás, amely számos különböző csomag cseréjét foglalja magában a DHCPv4-szerver és a DHCPv4-kliens között. Ennek eredményeként a kliens érvényes címadatokhoz jut, amelyeket egy előre meghatározott időszakra bérel.

A klienstől származó (DHCPDISCOVER, DHCPREQUEST) üzenetek elküldése szórással történik, hogy a hálózaton lévő összes DHCPv4-szerver értesüljön a címadatok igényléséről és fogadásáról. A DHCPv4-szerverről származó (DHCPOFFER, DHCPACK) üzenetek elküldése egyedi címzéssel történik, közvetlenül az adatokat kérő kliens felé.

Az IPv6 globális egyedi címek dinamikus kiosztására viszont két módszer is létezik:

* SLAAC
* Állapottartó DHCPv6

Állapotmentes automatikus konfiguráció esetén a kliens az RA-üzenetben szereplő információk segítségével automatikusan kiválasztja és beállítja az egyedi IPv6-címét. 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.

Az állapottartó DHCPv6 nem sokban különbözik a DHCPv4-től. Ebben az esetben az RA-üzenet jelzi a kliensnek, hogy ne használja az RA-üzenet információit. Így minden címzési és konfigurációs adatot egy DHCPv6-szervertől kell megszereznie. A DHCPv6-szerver gondoskodik az IPv6 állapotinformációik karbantartásáról. Ez hasonlít arra, ahogy a DHCPv4-szerver osztja ki az IPv4-címeket.

Ha a DHCP-szerver és a kliens eltérő hálózaton vannak, akkor szükség van egy DHCPv6-közvetítő beállítására. A közvetítő az egy LAN-szegmensből származó konkrét szórásos üzeneteket küldi tovább egy másik LAN-szegmensen található konkrét szerver felé. (Ebben az esetben a DHCP-üzenet továbbküldése történne meg egy DHCP-szerver felé.)

A DHCPv4-hez és a DHCPv6-hoz kapcsolódó problémák hibaelhárítása ugyanazokat a feladatokat foglalja magában:

* A címütközések feloldása.
* A fizikai kapcsolat ellenőrzése.
* A kapcsolat statikus IP-címmel történő ellenőrzése.
* A kapcsolóportok beállításainak ellenőrzése.
* Az egy alhálózaton vagy VLAN-on belüli működés ellenőrzése.

