Bevezetés a hálózatok világába

Hálózati réteg

A hálózati réteg, vagy más néven az OSI 3. rétege olyan szolgáltatásokat biztosít, amelyek lehetővé teszik a végberendezések közötti kommunikációt a hálózaton. A végponttól-végpontig történő szállításhoz a hálózati réteg négy alapvető folyamatot használ:

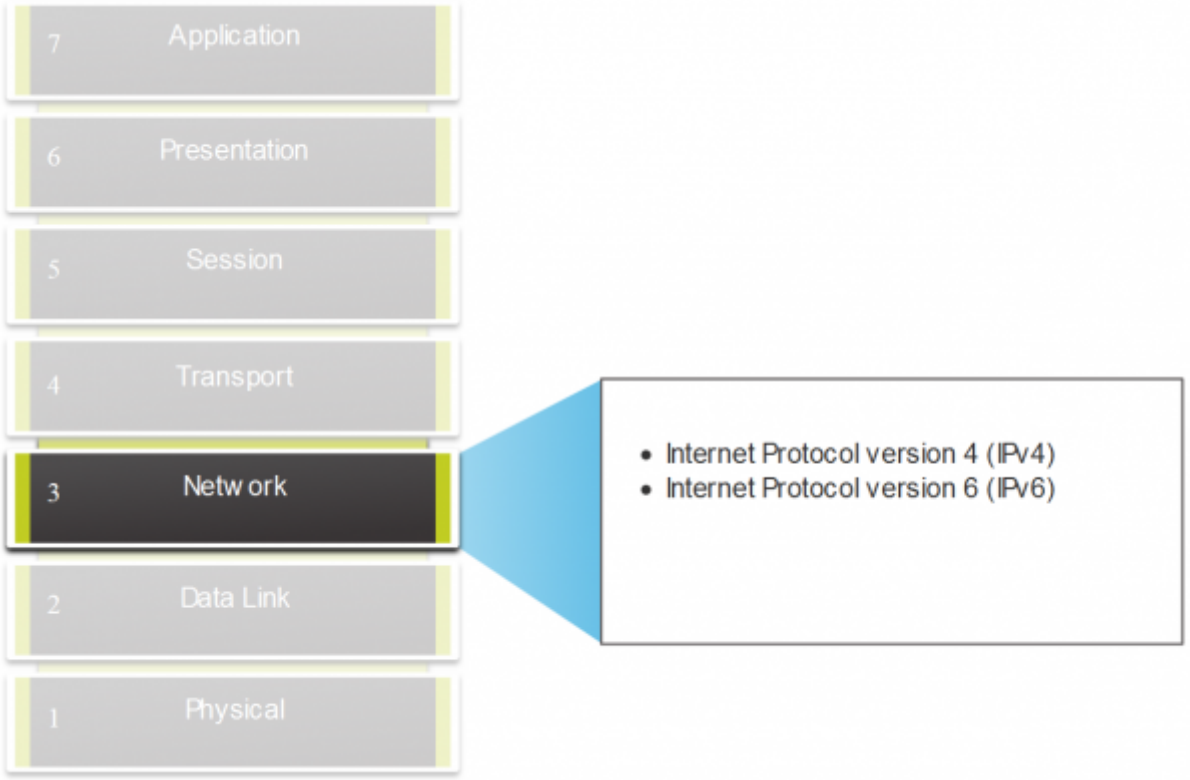
- **Végberendezések címzése** - Mint ahogy egy telefon egyedi telefonszámmal rendelkezik, úgy egy végberendezés is csak egyedi IP-címmel azonosítható a hálózaton. Egy adott IP-címmel rendelkező végberendezést állomásnak nevezünk.
- **Beágyazás** - A hálózati réteg a szállítási rétegtől fogad egy protokoll adategységet (PDU - protocol data unit). A beágyazás során a hálózati réteg ezt a PDU-t IP-fejléc információkkal egészíti ki, mint például a forrás- és a célállomás IP-címe. A fejléc információkkal kiegészített PDU-t nevezzük csomagnak.
- **Forgalomirányítás** - A hálózati réteg szolgáltatásainak segítségével a csomagok egy másik hálózaton lévő célállomáshoz irányíthatók. A csomag másik hálózatba történő továbbításához forgalomirányítóra van szükség. A forgalomirányító feladata a célállomás felé vezető út kiválasztása és a csomagok cél felé továbbítása. Ezt a folyamatot nevezzük forgalomirányításnak. A csomag számos közvetítő eszközön haladhat keresztül, mielőtt elérkezik a célállomáshoz. A célállomáshoz vezető útvonal egyes szakaszait ugrásnak nevezzük.
- **Kicsomagolás** - Amikor a csomag megérkezik a célállomás hálózati rétegéhez, az állomás ellenőrzi a csomag IP-fejlécét. Ha a fejlécben lévő cél IP-cím megegyezik a saját IP-címével, akkor eltávolítja a csomagról az IP-fejlécet. Az alacsonyabb rétegek fejlécének eltávolítását nevezzük kicsomagolásnak. A hálózati rétegben történő kicsomagolást követően a keletkezett 4. rétegbeli PDU a szállítási réteg megfelelő szolgáltatásához kerül.

Míg a szállítási réteg (OSI 4. réteg) az állomásokon futó folyamatok közötti adattovábbítást kezeli, addig a hálózati réteg a csomagok felépítését és feldolgozását definiálja, ami az adatok állomásról állomásra történő továbbításához szükséges. A csomagokban szállított adatoktól független működésnek köszönhetően, a hálózati réteg képes az állomások közötti különböző típusú kommunikáció továbbítására.

IP-beágyazás

Az IP egy fejléc hozzáadásával csomagolja be a szállítási réteg szegmenseit. Ez a fejléc teszi lehetővé a csomagok célállomáshoz továbbítását, és mindaddig szükség van rá, amíg a csomag a forrás hálózati rétegét elhagyva megérkezik a célállomás hálózati rétegéhez.

Az adatok rétegről rétegre történő becsomagolásának folyamata teszi lehetővé, hogy az egyes rétegek szolgáltatásai más rétegektől függetlenül fejlődjenek és bővüljenek. Mindez azt jelenti, hogy a szállítási réteg szegmensei becsomagolhatók IPv4, IPv6 vagy akár egy új, a jövőben kifejlesztett protokoll segítségével is.



A forgalomirányítók képesek a különböző hálózati rétegbeli protokollok egyidejű működtetésére, összekötve a hálózat különböző típusú állomásait. A közvetítő eszközök a forgalomirányítás során csak a csomag fejlécének tartalmát veszik figyelembe. A csomag adat része - a szállítási rétegbeli PDU - a hálózati rétegbeli feldolgozás során minden esetben változatlan marad.

Az IP-protokoll jellemzői

Az IP-t kis többletterhelésű protokollnak tervezték. Ennek megfelelően csak azokat a funkciókat tartalmazza, amelyek feltétlenül szükségesek ahhoz, hogy egy csomag összekapcsolt hálózatokon keresztül a forrástól a célig eljusson. A protokollnak nem feladata a csomagok nyomon követése és felügyelete. Ezeket a funkciókat szükség esetén más rétegbeli protokollok biztosítják.

Az IP legfőbb jellemzői:

- **Összeköttetés-mentes** - Az adatküldést megelőzően nem épül fel kapcsolat a küldő és a fogadó állomás között.
- **Legjobb szándékú (nem megbízható)** - A csomagok kézbesítése nem garantált.
- **Közegfüggetlen** - Működése független az adattovábbításhoz használt átviteli közegtől.

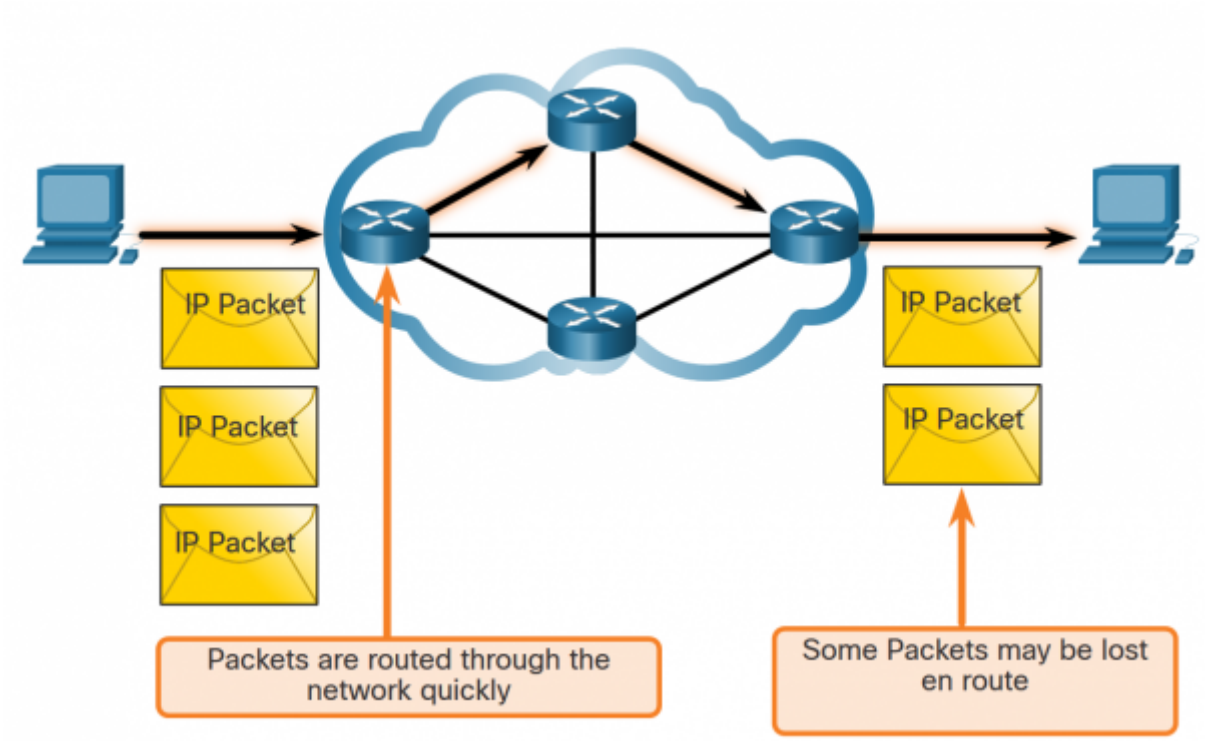
Összeköttetés-mentesség

A hálózati réteg feladata a csomagok állomások közötti továbbítása a hálózatra nézve a lehető legkisebb többletterheléssel. A hálózati réteg nem foglalkozik, vagy tudatában sincs a csomagban zajló kommunikáció típusával. Az IP összeköttetés-mentes, ami azt jelenti, hogy az adatküldést megelőzően a végpontok között nem épül ki kapcsolat. Az összeköttetés-mentes kommunikáció hasonló ahhoz, mint amikor egy levelet küldünk anélkül, hogy arról a címzettet előre értesítenénk.

Mivel az IP összeköttetés-mentes, így a csomagtovábbítás előtt nincs szükség a végpontok közötti kapcsolat kiépítéséhez fontos vezérlési információk cseréjére sem. Szintén nincs szükség a PDU-fejlécében olyan további információkra, amelyek a felépített kapcsolat kezelését segítenék. Mindezek nagy mértékben csökkentik az IP által okozott többletterhelését. Mivel nem épül fel kapcsolat a végpontok között, így a küldőnek nincs információja a megcímzett eszköz létezéséről vagy működéséről, illetve arról sem, hogy a csomagja megérkezik-e vagy hogy a címzett fel tudja-e azt dolgozni.

Legjobb szándékú kézbesítés

Az IP-t gyakran nevezik nem megbízható vagy legjobb szándékú kézbesítést (best-effort delivery) biztosító protokollnak. Ez nem azt jelenti, hogy az IP időnként megfelelően működik, máskor pedig nem, vagy hogy az IP gyenge adatkommunikációs protokoll. A nem megbízható mindössze annyit jelent, hogy az IP nem képes felügyelni és helyreállítani a nem kézbesített vagy hibás csomagokat. Ez amiatt van, hogy az IP-csomag a feladási helyen kívül semmilyen információt nem tartalmaz, ami alapján a küldőt értesíteni lehetne a sikeres kézbesítésről. Az IP fejléce nem tartalmaz szinkronizációs adatokat a csomagok kézbesítési sorrendjének nyomon követéséhez, nem nyugtázza a csomagok megérkezését, és nem tartalmaz hibajavítási adatot sem, amellyel ellenőrizhető a csomagok hibamentes kézbesítése. Előfordulhat, hogy a csomagok hibásan, rossz sorrendben vagy egyáltalán nem érkeznek meg a célállomáshoz. Az IP-fejlécben található információk alapján, egyik hiba esetében sincs mód a csomag újraküldésére.



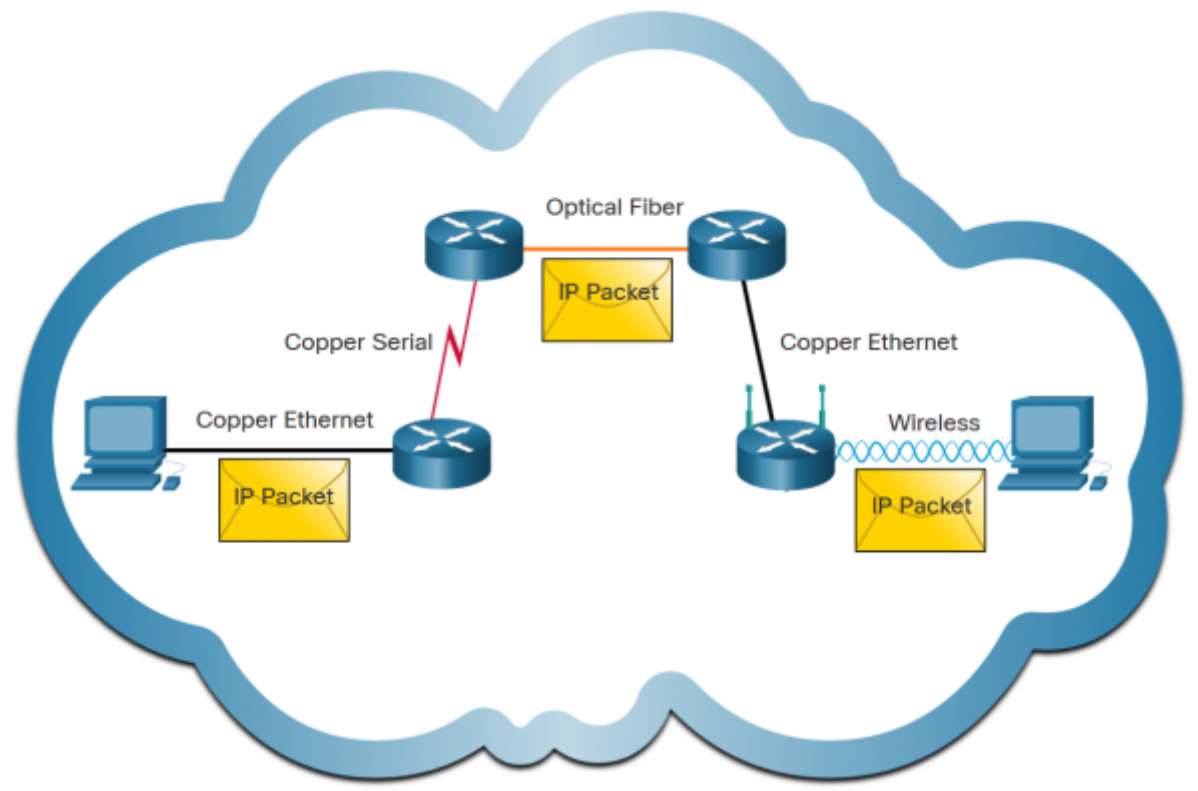
Rossz sorrendben érkező vagy elveszett csomagok esetén a magasabb rétegbeli szolgáltatások, mint például a TCP feladata a probléma kezelése. Mindezek eredményeképpen az IP nagyon hatékonyan képes működni. Ha az IP-fejléc a megbízhatósághoz szükséges többlet információkat is tartalmazná, akkor az összeköttetést vagy megbízhatóságot nem igénylő kommunikációk esetében sávszélesség felhasználási és késleltetési problémák merülnének fel. A TCP/IP-protokollkészletben a szállítási rétegbeli protokoll lehet TCP vagy UDP attól függően, hogy az adott kommunikáció esetében mennyire fontos a megbízhatóság. Annak köszönhetően, hogy az IP a megbízhatósági feladatokat a szállítási rétegre bízza, egy rugalmas és különböző típusú kommunikációk esetén is használható protokoll.

Közegfüggetlenség

A hálózati réteg nem foglalkozik a csomagok továbbításához használt átviteli közeg jellemzőivel sem. Az IP teljesen függetlenül működik az átviteli közegtől, ahol a protokollkészlet alacsonyabb rétegeiben zajló adatátvitel történik. Ahogy az ábrán is látható, az IP-csomagok továbbíthatók elektromos úton kábelen keresztül, optikai jelként üvegszálat használva, vagy vezeték nélküli környezetben rádió jelként.

Az IP-csomagok fogadása és felkészítése az átviteli közegen történő továbbításra az OSI adatkapcsolati rétegének feladata. Mindez azt jelenti, hogy az IP-csomagok továbbítása nincs korlátozva egyetlen átviteli közegre sem.

A hálózati réteg azonban figyelembe veszi az átviteli közeg egy fő jellemzőjét, a közegen átvihető maximális PDU méretét. Ezt nevezzük maximális átviteli egységnek (Maximum Transmission Unit, MTU). A csomagok maximális méretének meghatározása az adatkapcsolati és a hálózati réteg közötti kommunikáció során történik. Az adatkapcsolati réteg megadja a hálózati réteg számára az MTU értékét, a hálózati réteg pedig meghatározza a maximális csomagméretet.



Bizonyos esetekben egy közvetítő eszköznek, általában egy forgalomirányítónak át kell méreteznie a csomagokat ahhoz, hogy egy kisebb MTU-értékkel rendelkező közegen továbbítani tudja őket. Ezt a folyamatot nevezik tördelésnek vagy feldarabolásnak (fragmentation).

Az IPv4-csomag

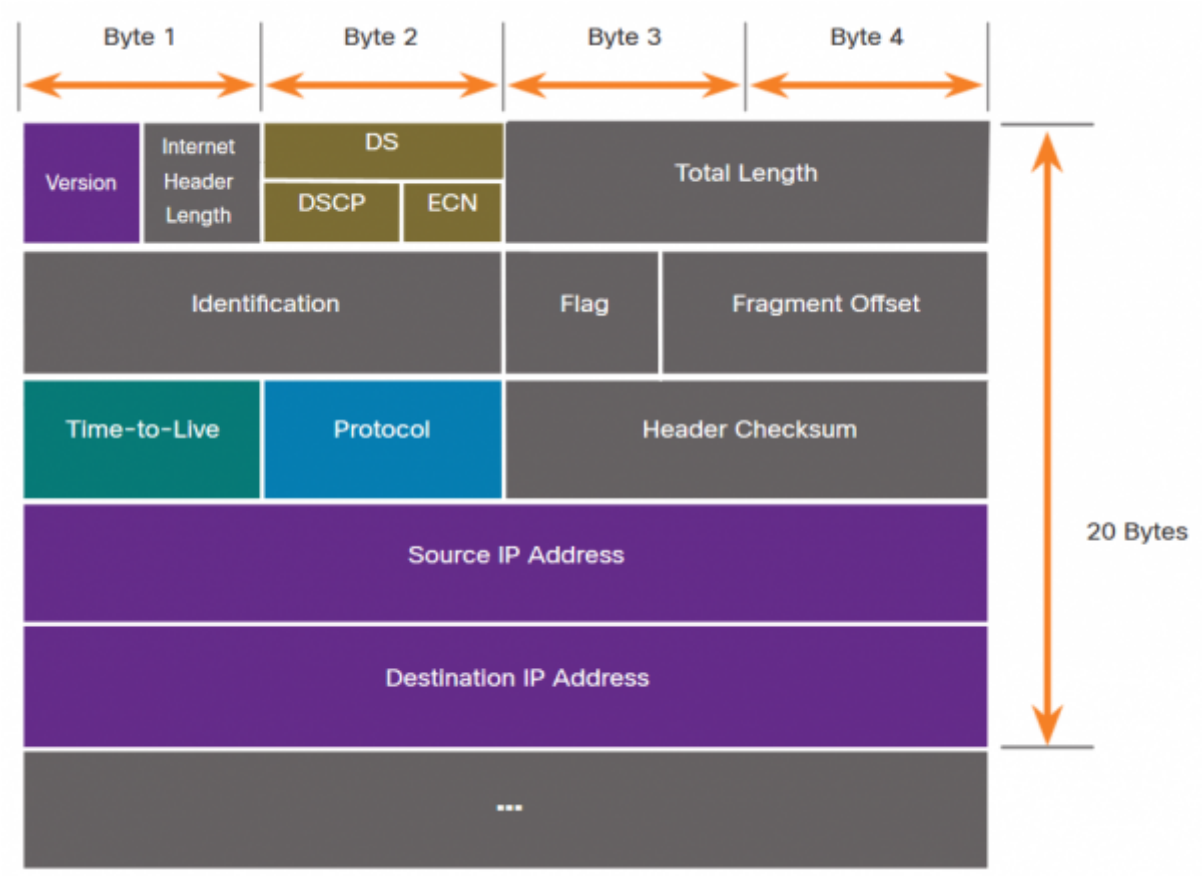
Az IPv4-csomag fejléce

Az IPv4-et 1983-ban fejlesztették ki az Internet elődjének tekinthető ARPANET (Advenced Tesarch Projects Agency Network) hálózat működéséhez. Az internet elsősorban az IPv4 protokollra épül, ami a legszélesebb körben használt hálózati rétegbeli protokoll.

Az IPv4 csomag két részből áll:

- **IP-fejléc** - A csomag jellemzőit határozza meg.
- **Adattartalom** - A 4. rétegbeli szegmens információkat és a tényleges adatokat tartalmazza.

Az IPv4-csomag fejléce olyan mezőkből áll, melyek a csomagról tartalmaznak fontos információkat. Ezek a mezők bináris számok, melyeket a 3. réteg dolgoz fel. Az egyes mezők bináris értékei az IP-csomag különböző tulajdonságait határozzák meg.



A legfontosabb IPv4-fejléc mezők:

- **Verzió** - Az IP-csomag verzióját határozza meg 4 biten. IPv4 esetén ez az érték mindig 0100.
- **Differenciált szolgáltatások (Differentiated Services, DS)** - A korábban ToS-nak (Type of Service, szolgáltatás típus) nevezett DS mező egy 8 bites érték, ami a csomagok prioritását adja meg. Az első 6 bit a DCSP (Differentiated Services Code Point, differenciált szolgáltatások kódpont) érték, amit a szolgáltatási minőség (Quality of Service, QOS) biztosításához használnak. Az utolsó 2 bit pedig az ECN (explicit congestion notification, explicit torlódásjelzés) érték, ami hálózati torlódás esetén a csomagvesztések elkerülésére szolgál.
- **Élettartam (Time-To-Live, TTL)** - A csomag élettartamát korlátozó 8 bites bináris szám. Értéke másodpercben van megadva, de rendszerint ugrásszámmal hivatkoznak rá. A csomag küldője beállít egy kezdeti TTL-értéket, amit a csomagot feldolgozó minden forgalomirányító vagy 3. rétegbeli továbbító eszköz eggyel csökkent. Ha a TTL értéke eléri a nullát, a forgalomirányító eldobja a csomagot és egy ICMP Time Exceeded üzenetet küld a forrás állomásnak. A traceroute parancs ezt a mezőt használja a forrás- és a célállomás közötti forgalomirányítók azonosításához.
- **Protokoll** - 8 bites érték, ami meghatározza a csomagban szállított adattartalom típusát. Ennek segítségével továbbítja a hálózati réteg az adatot a megfelelő felsőbb rétegbeli protokoll számára. A leggyakoribb értékei: 0x01 (ICMP), 0x06 (TCP), 0x11 (UDP).
- **Forrás IP-cím** - A csomag forrásállomásának címét megadó 32 bites bináris szám.
- **Cél IP-cím** - A csomag célállomásának címét megadó 32 bites bináris szám.

A két leggyakrabban hivatkozott mező a forrás és cél IP-cím. Ezek határozzák meg, hogy a csomag honnan indult és hová tart. Általában ezek a címek nem változnak a forrástól a célállomásig vezető út

során.

Az eddig nem említett mezők a csomag azonosításához és érvényesítéséhez, vagy a szétdarabolt csomag újbóli összeállításához szükségesek.

Az azonosításra és érvényesítésre használt mezők:

- **Internet fejléc hossz (Internet Header Length, IHL)** - Egy 4 bites érték, ami megadja a csomag fejlécében található 32 bites szavak számát. Az IHL értéke változhat az Options (opciók) és a Padding (kitöltés) mezők miatt. A mező legkisebb értéke 5 (5×32=160bit=20 bájt), legnagyobb értéke pedig 15 (15×32=480bit=60 bájt) lehet.
- **Teljes hossz (Total Lenght)** - Az időnként Packet Lenght-nek (csomaghossz) is nevezett 16 bites mező a teljes csomag (fejléc és adat) bájtokban mért hosszát adja meg. A minimális csomagméret 20 bájt (20 bájt fejléc + 0 bájt adat), a maximális pedig 65535 bájt.
- **Fejléc ellenőrző összeg (Header Checksum)** - 16 bites mező az IP-csomag sértetlenségének ellenőrzésére. Egy csomag megérkezésekor a fejléc ellenőrző összegét újraszámolják és összehasonlítják a mező értékével. Ha a kér érték nem egyezik, akkor a csomag eldobásra kerül.

Amikor egy forgalomirányító a csomagokat egy kisebb MTU-értékkel rendelkező átviteli közegre továbbítja, akkor a csomagokat kisebb egységekre kell feldarabolnia. Ezt a folyamatot nevezzük feldarabolásnak (fragmentation). A feldarabolt adategységek nyomon követéséhez az IPv4-csomag a következő mezőket használja:

- **Azonosítás (Identification)** - 16 bites szám, ami egyértelműen azonosítja az IP-csomag egy darabját.
- **Jelzők (Flags)** - A csomag feldarabolásának módját meghatározó 3 bit. A Fragment Offset (csomagdarab eltolás) és az Identification mezőkkel együtt elősegíti a csomagdarabokból az eredeti csomag visszaállítását.
- **Csomagdarab eltolás (Fragment Offset)** - 13 bites érték, ami a csomag darabokból történő összeállításánál megadja a csomagok sorrendjét.

Megjegyzés: Az Opciók és a Kitöltés mezők használata igen ritka, így a tananyag ezeket nem tárgyalja.

IPv6-csomag

Az IPv4 korlátai

Az elmúlt évek során az IPv4 protokollt a megjelenő újabb és újabb kihívásoknak köszönhetően számtalanszor frissítették. Mindezek ellenére az IPv4-nek maradt három alapvető problémája:

- **Elfogytak az IPv4-címek** - Az IPv4 korlátozott számú egyedi nyilvános címmel rendelkezik. Bár megközelítőleg 4 billió IPv4-cím létezik, az IP-alapú eszközök számának növekedése, a permanens kapcsolatok és a fejletlen országok várható igényei nagyban megnövelték a szükséges címek számát.
- **Megnövekedett irányítótábla méret az interneten** - Az irányítótáblát a forgalomirányítók a

legjobb útvonal kiválasztásához használják. Az internetre csatlakozó szerverek számának növekedésével növekszik a hálózati útvonalak száma is. Ezen IPv4-útvonalak kezelése rengeteg memóriát és processzorteljesítményt igényel az internet forgalomirányítóin.

- **Végponttól végpontig tartó kapcsolatok hiánya** - A hálózati címfordítás (Network Address Translation, NAT) az IPv4-hálózatokban gyakorta alkalmazott technológia. A NAT lehetővé teszi, hogy több eszköz egyetlen nyilvános IP-címet használjon. Mivel a nyilvános IP-címek a megosztottak, a belső állomások IP-címei rejtve maradnak. Ez problémát okozhat a végponti kapcsolatokat igénylő technológiák esetén.

Az IPv6 bemutatása

Az 1990-es évek elején az IETF (Internet Engineering Task Force) egyre nagyobb aggodalommal figyelte az IPv4 kapcsán felmerülő problémákat, és elkezdte keresni a megoldást. Ez vezetett aztán az IPv6 kifejlesztéséhez. Az IPv6 megoldja az IPv4 problémáit, és egy olyan robusztus megoldás biztosít, amely tulajdonságainak köszönhetően alkalmasabb a jelenlegi és a várható hálózati igények kielégítésére.

Az IPv6 kibővített tulajdonságai:

- **Megnövekedett címtér** - Az IPv6-címek, a 32 bites IPv4-címekkel ellentétben, 128 bites hierarchikus felépítésűek, melynek köszönhetően nagyságrendekkel több IP-címet biztosítanak.
- T**ovábbfejlesztett csomagkezelés** - Az IPv6-fejléc kevesebb mezőt tartalmaz. Ez növeli a csomagkezelés hatékonyságát a forgalomirányítókon és lehetővé teszi a skálázhatóságot biztosító kiterjesztések és opciók használatát.
- **Nincs szükség címfordításra** - A nagy számú nyilvános IPv6-címnek köszönhetően nincs szükség címfordításra (NAT). A legnagyobb vállalatok telephelyeitől a kis háztartásokig mindenhova kiosztható IPv6-os hálózati cím. Ez megoldja a NAT használatával keletkezett problémákat azoknál az alkalmazásoknál, amelyek végponti kapcsolatokat igényelnek.
- **Integrált biztonság** - Az IPv6 támogatja a hitelesítést és a titkosítást. IPv4 esetén ezekhez további kiegészítések szükségesek.

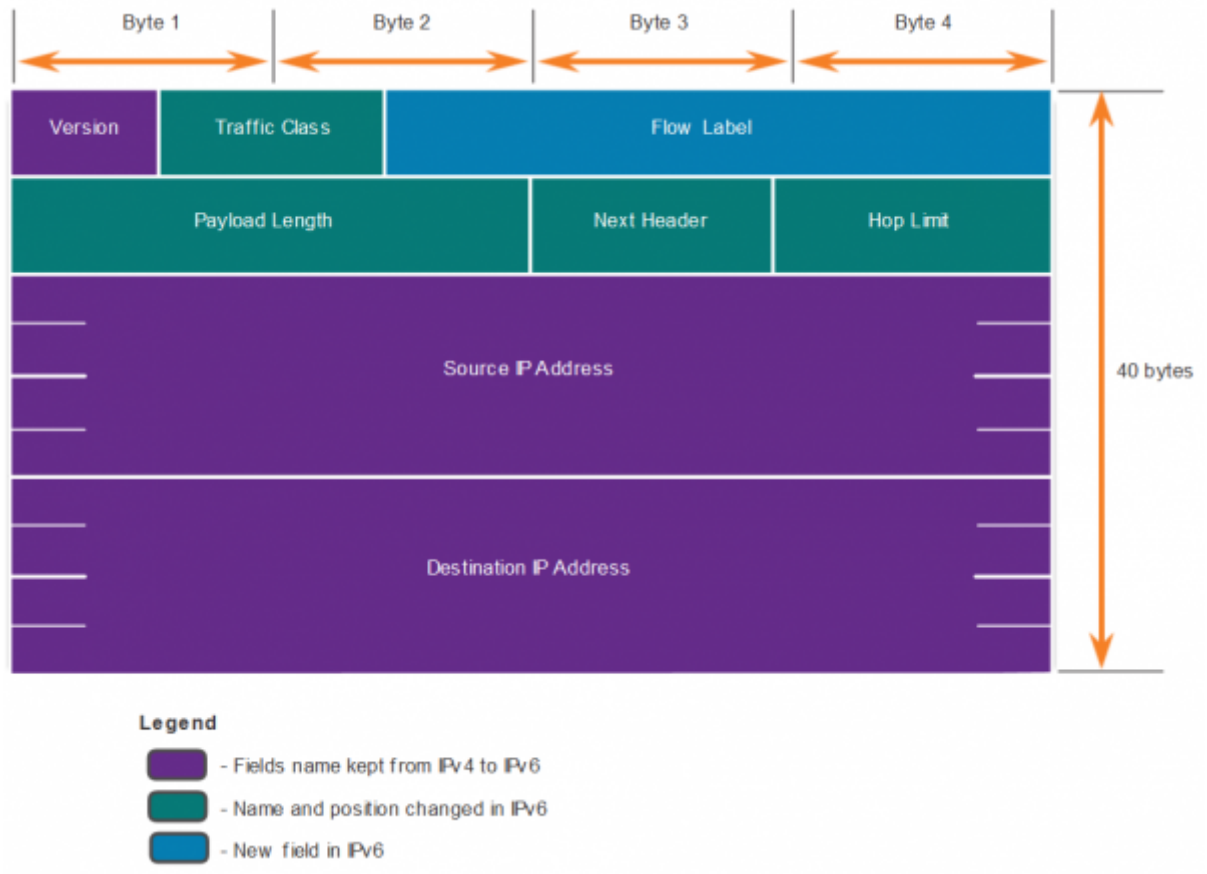
A 32 bites IPv4-címtér megközelítőleg 4.294.967.296 egyedi címet tartalmaz. Mivel az IPv4 a címeket osztályokba sorolja, valamint címeket tart fent a csoportos címzésre, a tesztelésre és egyéb felhasználás érdekében, így a teljes címtérből csak 3,7 milliárd a ténylegesen kiosztható.

Az IPv6 340.282.366.920.938.463.463.374.607.431.768.211.456 vagyis kb. 340 szextillió címet biztosít, ami megközelítőleg annyi, mint a Föld összes homokszeme.

Az IPv6 kapcsán az egyik legfőbb tervezési változás az IPv4-hez képest az egyszerűsített fejléc.

Az IPv4-fejléc 20 oktett (maximum 60 byte az Opciók mezővel együtt), ami az Opciók és a Kitöltés mezőket leszámítva 12 alapvető mezőből áll.

Az IPv6-fejléc ezzel szemben 40 oktett (a forrás- és célcím mérete miatt ilyen nagy), ami 3 IPv4 alap és 5 további mezőt, azaz összesen 8 mezőt tartalmaz.



IPv6-csomag fejléc

Az IPv6-csomag fejléc mezői:

- **Verzió** - Ez a 4 bit adja meg az IP-csomag verzióját, ami IPv6 esetén 0110.
- **Forgalom osztály (Traffic Class)** - Ez a 8 bit megegyezik az IPv4-fejléc differenciált szolgáltatások (Differentiated Services, DS) mezőjével. Szintén egy 6 bites DSCP (Differentiated Services Code Point) érték osztályozza a csomagokat és egy 2 bites ECN (Explicit Congedtion Notification) mező szolgál torlódásvezérlésre.
- **Folyamcimke (Flow Label)** - A 20 bites mező lehetővé teszi a valós idejű alkalmazások speciális kezelését. Segítségével értesíthetők a forgalomirányítók és a kapcsolók, hogy egy csomagfolyam esetén ugyanazt az útvonalat használják, így a csomagokat nem kell összerendezni.
- **Adatmező hossza (Payload Length)** - Ez a 16 bites mező megegyezik az IPv4-fejléc Total Length (Teljes hossz) mezőjével. A teljes csomag (töredék) méretét adja meg a fejrésszel és az opcionális kiegészítésekkel együtt.
- **Következő fejléc (Next Header)** - A 8 bites mező megegyezik az IPv4 Protokoll mezőjével. Ez adja meg a csomagban lévő adattartalom típusát, lehetővé téve ezzel a hálózati réteg számára, hogy az adatokat a megfelelő felsőbb rétegbeli protokollnak továbbítsa. A mezőt akkor is használják, ha az IPv6-csomagban opcionális kiterjesztések vannak.
- **Ugrás korlát (Hop Limit)** - Ez a 8 bit felel meg az IPv4 csomag TTL-mezőjének. Értéke mindig eggyel csökken, amikor egy forgalomirányító továbbítja a csomagot. Amikor a számláló eléri a 0 értéket, a csomagot az adott forgalomirányító eldobja és egy ICMPv6 üzenettel értesíti a küldő állomást arról, hogy a csomag nem érkezett meg a célhoz.

- **Forrás IP-cím (Source Address)** - Ez a 128 bites mező adja meg a küldő állomás IPv6 címét.
- **Cél IP-cím (Destination Address)** - Ez a 128 bites mező adja meg a fogadó állomás IPv6-címét.

Az IPv6-csomag kiterjesztett fejléct (Extension Header, EH) is tartalmazhat, ami további hálózati rétegbeli információkat biztosít. Ez a kiterjesztett fejléc opcionális és az IPv6-fejléc és az adat között helyezkedhet el. Használják például csomagok feldarabolása vagy biztonság és mobilitás támogatás esetén is.

Állomás csomagtovábbítási döntései

A hálózati réteg másik feladata a csomagok állomások közötti irányítása. Egy állomás által küldött csomag címzettje lehet:

- **Saját maga** - Ilyenkor egy speciális IP-címet, a 127.0.0.1-et használja, amit visszahurkolási (loopback) interfésznek nevezünk. Ez a loopback cím automatikusan hozzárendelődik minden állomáshoz, amint a TCP/IP futni kezd. Az, hogy egy állomás a hálózat segítségével saját magának is tud üzenetet küldeni tesztelési célból fontos. A 127.0.0.0/8 hálózat bármely IP-címe a helyi állomásra utal.
- **Helyi állomás** - A küldő állomással egy hálózatban lévő másik állomás. A két állomás hálózati címe azonos.
- **Távoli állomás** - Távoli hálózat egy állomása. A két állomás hálózati címe különböző.

Az, hogy egy csomagot helyi vagy távoli állomásnak címeztek, a forrásállomás IP-cím és hálózati maszk kombinációjának a célállomás IP-címével történő összevetése dönti el.

Otthoni vagy vállalati hálózatokban számos vezetékes és vezeték nélküli eszköz kapcsolódik össze közvetítő hálózati eszköz, mint például LAN-kapcsoló és/vagy vezeték nélküli hozzáférési pont (Wireless Access Point, WAP) segítségével. Ez a közvetítő eszköz biztosítja a kapcsolatot a helyi hálózat állomásai között. A helyi állomások további eszközök használata nélkül képesek egymást elérni és információt megosztani. Amikor egy állomás ugyanazon a hálózaton lévő állomásnak küld üzenetet, a csomag egyszerűen az állomás interfészéről a közvetítő eszközön keresztül a célállomáshoz kerül továbbításra.

Természetesen a legtöbb esetben szeretnénk, hogy eszközeink helyi hálózaton kívüli állomásokhoz, vállalatokhoz és az internethez is csatlakozni tudjanak. A helyi hálózaton kívüli berendezéseket távoli állomásoknak nevezzük. Amikor egy állomás egy távoli célállomásnak küld üzenetet, akkor forgalomirányítóra és irányításra van szükség. A forgalomirányítási folyamat feladata a legjobb útvonal megtalálása a célállomáshoz. A helyi hálózati szegmenshez csatlakozó forgalomirányítót nevezzük **alapértelmezett átjárónak**.

Alapértelmezett átjáró

Az alapértelmezett átjáró irányítja a forgalmat a helyi hálózatról a távoli hálózatok eszközeihez. Otthoni vagy kisvállalati környezetben gyakori, hogy az alapértelmezett átjárót az internethez való csatlakozáshoz használják.

Amikor egy állomás csomagot küld egy másik IP-hálózaton lévő eszköznek, akkor azt egy közvetítő eszközön keresztül az alapértelmezett átjárónak kell küldenie. Ez azért van így, mert a helyi állomás nem tárol irányítási információkat a helyi hálózaton kívül lévő, távoli célállomásokról, az alapértelmezett átjáró viszont rendelkezik a szükséges információkkal. Az alapértelmezett átjáró, ami leggyakrabban egy forgalomirányító, egy iránytótáblát tart fenn. Az irányítótábla egy RAM-ban tárolt adatfájl, amiben a közvetlenül csatlakozó és az eszköz által megtanult távoli hálózatok adatai szerepelnek. A forgalomirányító a táblában lévő információkat használja fel a célhoz vezető legjobb útvonal megtalálásához.

Állomások irányítótáblái

Hogyan tudja eldönteni az állomás, hogy a csomagokat az alapértelmezett átjáróhoz kell-e továbbítania? Az állomásnak saját, helyi irányítótáblát kell fenntartania ahhoz, hogy a hálózati rétegbeli csomagokat a megfelelő célhálózatba tudja küldeni. Ez a helyi tábla jellemzően az alábbiakat tartalmazza:

- **Közvetlen kapcsolat** - Út a visszahurkolási interfészhez (127.0.0.1).
- **Helyi hálózati útvonal** - Az állomáshoz csatlakozó hálózat automatikusan bekerülnek az állomás irányítótáblájába.
- **Helyi alapértelmezett útvonal** - Az alapértelmezett útvonal segítségével érhető el minden távoli hálózat. Az alapértelmezett útvonal akkor jön létre, amikor egy alapértelmezett átjáró beállításra kerül az állomáson. Az alapértelmezett átjáró címe a helyi hálózathoz csatlakozó forgalomirányító hálózati interfészének IP-címe. Ez a cím beállítható manuálisan vagy megtanulható dinamikusan.

Egy Windows állomáson a **route print** vagy a **netstat -r** parancs jeleníti meg az állomás irányítótábláját. A két parancs kimenete megegyezik. Bár a kimenet első ránézésre bonyolultnak tűnhet, mégis könnyen megérthető.

A **netstat -r** vagy a vele megegyező **route print** parancs az aktuális TCP/IP hálózati kapcsolatokra vonatkozóan az alábbi három információt tartalmazza:

- **Interfész lista** - Megadja az állomás minden hálózati interfészének (Ethernet, Wi-Fi és Bluetooth) MAC címét és hozzárendelt interfész azonosítóját.
- **IPv4-irányítótábla** - Tartalmazza az állomás által ismert összes IPv4-útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.
- **IPv6-irányítótábla** - Tartalmazza az állomás által ismert összes IPv6 útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.

Forgalomirányító csomagtovábbítási döntései

Amikor egy állomás csomagot küld egy másik állomásnak, akkor az irányítótáblája segítségével dönti el, hogy hova továbbítsa azt. Ha a célállomás egy távoli hálózaton van, akkor a csomagot egy átjárónak kell küldeni.

Mi történik, amikor egy csomag érkezik egy forgalomirányító interfészére? A forgalomirányító megnézi az irányítótábláját és annak segítségével dönti el, hogy a csomagot merre kell küldenie.

Egy forgalomirányító irányítótáblája az alábbiakról tárol információkat:

- **Közvetlenül csatlakozó útvonalak** - A forgalomirányító aktív interfészein lévő hálózatok. A forgalomirányító akkor jegyez be a táblájába egy közvetlenül csatlakozó útvonalat, ha a megfelelő interfésze aktív és van IP-címe. A forgalomirányító minden interfésze külön hálózathoz tartozik. Az irányítótáblában minden csatlakoztatott és aktív hálózati szegmens információi megtalálhatók.
- **Távoli útvonalak** - Más forgalomirányítókhoz csatlakozó hálózatokra mutató útvonalak. Konfigurálhatók kézzel a helyi forgalomirányítón a hálózati rendszergazda által, vagy dinamikusan a helyi és a távoli forgalomirányítók közötti irányító protokollok segítségével.

IPv4-irányítótábla

Egy állomás irányítótáblájában csak a közvetlenül csatlakozó hálózatok szerepelnek, így egy távoli célállomás eléréséhez alapértelmezett átjáróra van szüksége. Egy forgalomirányító irányítótáblája hasonló információkat tartalmaz azzal a különbséggel, hogy távoli hálózatok azonosítására is képes.

A forgalomirányító és az állomás irányítótáblája is tartalmazza a következőket:

- célhálózat
- célhálózathoz tartozó mérték (metrika)
- célhálózat eléréséhez szükséges átjáró

```
C:\Windows\System32> netstat -r
===========================================================================
Interface List
  8...90 fb a6 82 60 69 ......Realtek PCIe GBE Family Controller
  7...0a 00 27 00 00 07 ......VirtualBox Host-Only Ethernet Adapter
 13...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 15...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
  4...00 00 00 00 00 00 00 e0 Microsoft ISATAP adapter
  6...00 00 00 00 00 00 00 e0 Microsoft ISATAP adapter #2
 14...00 00 00 00 00 00 00 e0 Microsoft ISATAP adapter #3
 16...00 00 00 00 00 00 00 e0 Microsoft ISATAP adapter #4
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     172.22.220.1    172.22.220.17     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     172.22.220.0    255.255.255.0         On-link     172.22.220.17    266
    172.22.220.17  255.255.255.255         On-link     172.22.220.17    266
   172.22.220.255  255.255.255.255         On-link     172.22.220.17    266
```

```
     192.168.17.0    255.255.255.0         On-link      192.168.17.1    276
     192.168.17.1  255.255.255.255         On-link      192.168.17.1    276
   192.168.17.255  255.255.255.255         On-link      192.168.17.1    276
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    266
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    266
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    266
    192.168.175.0    255.255.255.0         On-link     192.168.175.1    276
    192.168.175.1  255.255.255.255         On-link     192.168.175.1    276
  192.168.175.255  255.255.255.255         On-link     192.168.175.1    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.175.1    276
        224.0.0.0        240.0.0.0         On-link      192.168.17.1    276
        224.0.0.0        240.0.0.0         On-link     172.22.220.17    266
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.175.1    276
  255.255.255.255  255.255.255.255         On-link      192.168.17.1    276
  255.255.255.255  255.255.255.255         On-link     172.22.220.17    266
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    266
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  8     26 ::/0                     fe80::32e4:dbff:fe27:8d3f
  1    306 ::1/128                  On-link
  8     26 2001:738:3000:24e4::/64  On-link
  8    266 2001:738:3000:24e4:288c:3137:802a:17f4/128
                                    On-link
  8    266 2001:738:3000:24e4:cd4e:a16d:e4f3:dcb6/128
                                    On-link
 13    276 fe80::/64                On-link
 15    276 fe80::/64                On-link
  8    266 fe80::/64                On-link
  7    266 fe80::/64                On-link
 13    276 fe80::815:8858:f633:7871/128
                                    On-link
  7    266 fe80::8d2b:8b3b:7bb4:1588/128
                                    On-link
 15    276 fe80::ad28:85e0:e13d:80c6/128
                                    On-link
  8    266 fe80::cd4e:a16d:e4f3:dcb6/128
                                    On-link
  1    306 ff00::/8                 On-link
 13    276 ff00::/8                 On-link
 15    276 ff00::/8                 On-link
  8    266 ff00::/8                 On-link
  7    266 ff00::/8                 On-link
```

```
===========================================================================
Persistent Routes:
  None

C:\Windows\System32>
```

Egy Cisco IOS forgalomirányítón a **show ip route** parancs jeleníti meg az irányítótáblát. Ebben további útvonal információk is találhatók arról, hogy milyen módon tanulta meg és mikor frissítette utoljára a forgalomirányító az adott útvonalat, és melyik interfészen keresztül érhető el a kívánt célhálózat.

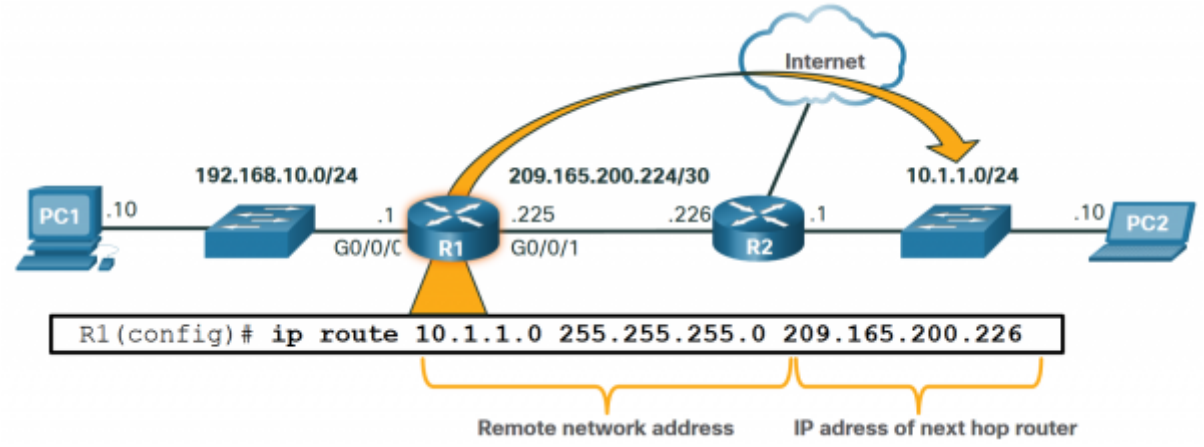
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45,
GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

A forgalomirányító az interfészére érkező csomag fejlécéből olvassa ki a célhálózat címét. Ha a célhálózat szerepel az irányítótábla útvonalai között, akkor a forgalomirányító a táblában szereplő információk alapján továbbítja a csomagot. Ha két vagy több útvonal is vezet ugyanahhoz a célhálózathoz, a mérték alapján dől el, hogy melyik kerül az irányítótáblába.

Egy forgalomirányító a távoli hálózatokat kétféleképpen ismerheti meg:

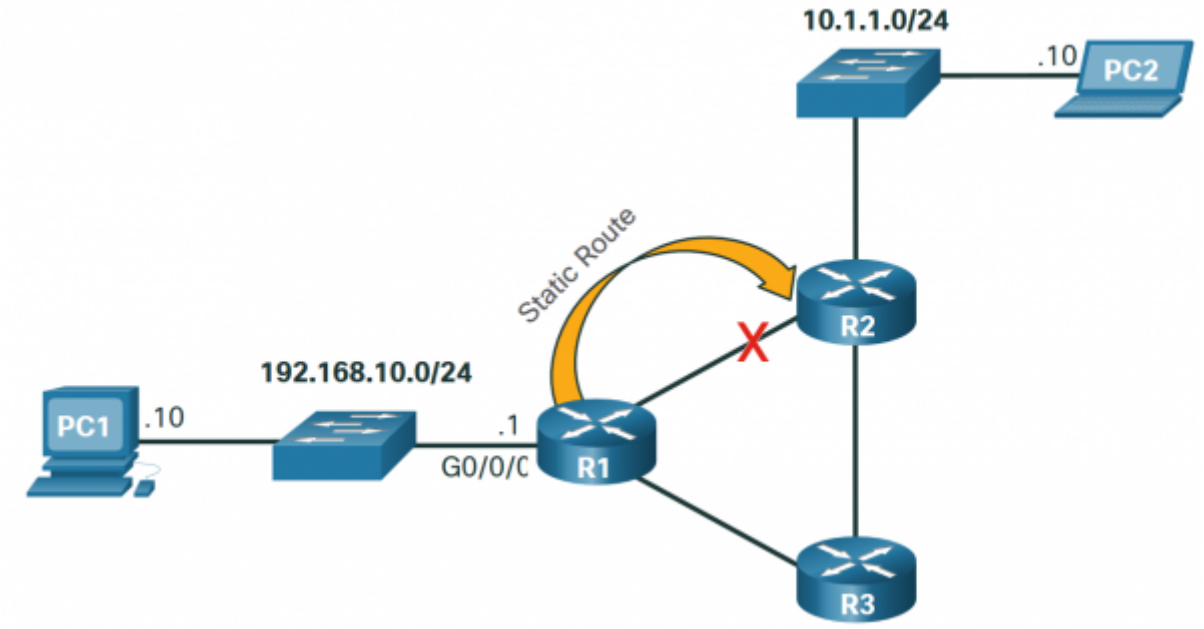
- **Kézzel megadva** - A távoli hálózatok statikus útvonalként, manuálisan megadva kerülnek az irányítótáblába.
- **Dinamikusan** - A távoli hálózatokról a forgalomirányító egy dinamikus irányító protokoll segítségével értesül.

Statikus forgalomirányítás



A statikus útválasztás a következő jellemzőkkel rendelkezik:

- A statikus útvonalat manuálisan kell konfigurálni.
- Az rendszergazdának újra kell konfigurálnia egy statikus útvonalat, amennyiben változás történik a hálózati topológiában, és a statikus útvonal már nem életképes.
- A statikus útvonal leginkább kis hálózatok esetén alkalmazható, illetve redundáns kapcsolatmentes hálózatokban.
- A statikus útvonalat általában egy dinamikus útválasztási protokollal együtt használják az alapértelmezett útvonal konfigurálásához.

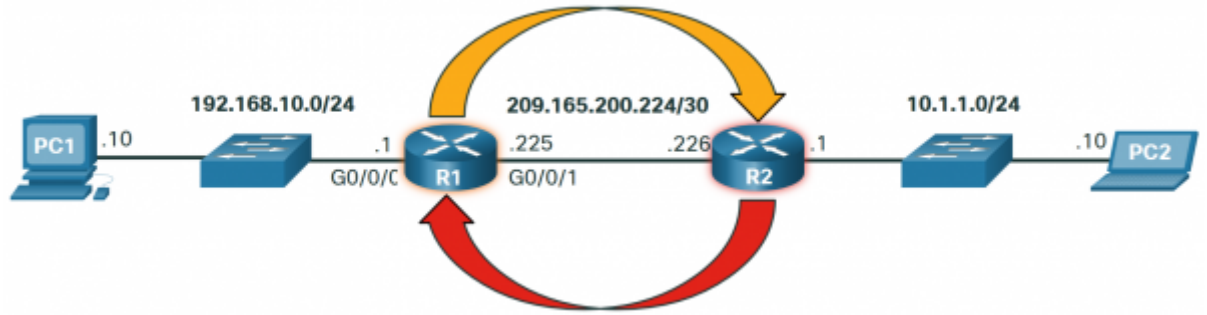


Dinamikus forgalomirányítás

A dinamikus útválasztási protokoll lehetővé teszi az útválasztók számára, hogy más útválasztóktól automatikusan megismerjék a távoli hálózatokat, beleértve az alapértelmezett útvonalat is. A dinamikus útválasztási protokollokat használó útválasztók automatikusan megosztják az útválasztási információkat más útválasztókkal, és kompenzálják az esetleges topológiai változásokat a hálózati rendszergazda bevonása nélkül. Ha változás történik a hálózati topológiában, az útválasztók megosztják ezeket az információkat a dinamikus útválasztási protokoll használatával, és

automatikusan frissítik útválasztási táblázataikat.

Dinamikus routing protokoll-példák: RIP, EIGRP, IS-IS, OSPF, BGP.



Az alapkonfigurációhoz a hálózati rendszergazdának kell megadnia a dinamikus útválasztási protokollon belül közvetlenül csatlakozó hálózatokat. A dinamikus útválasztási protokoll automatikusan a következőket fogja tenni:

- Felfedezi a távoli hálózatokat
- Naprakészen tartja az útválasztási információkat
- Kiválasztja a legjobb utat a célhálózatokhoz
- Amennyiben a jelenlegi útvonal már nem áll rendelkezésre, megpróbál egy új legjobb utat találni