Bevezetés a hálózatok világába

Címfeloldás

MAC és IP

Két fő címet rendelünk egy állomáshoz:

- fizikai címet (MAC-címet)
- logikai címet (IP-címet)

A MAC- és IP-cím közösen azonosítják be a készüléket a hálózaton. A folyamat, amelynek során a MAC-cím és az IP-cím segítségével megtalálunk egy számítógépet, hasonló ahhoz, mint amikor egy egyén nevét és címét használjuk levélküldés céljából.

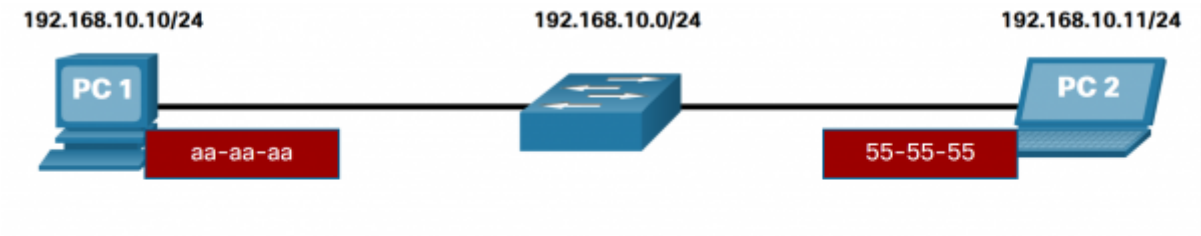
Egy személy neve általában nem változik. Másrészről a személy címe lakóhelyéhez kötődik és változhat is.

Egy adott személy nevéhez hasonlóan az állomás MAC-címe sem változik, fizikailag rendelik hozzá a gép hálózati kártyájához és fizikai címként ismeretes. A fizikai cím nem változik, függetlenül attól, hogy a gép hova kerül.

Az IP-cím hasonló egy személy címéhez. Ez a cím azon alapul, hogy az állomás ténylegesen hol található. Ezt a címet felhasználva lehetséges az, hogy egy keret meghatározza azt a helyet, ahova a keretet el kell küldeni. Az IP-cím vagy hálózati cím úgynevezett logikai cím, mert logikailag rendeljük hozzá az állomáshoz. Minden állomáshoz aszerint rendeli hozzá a hálózati rendszergazda, hogy az állomás melyik helyi hálózatra csatlakozik. Az ábra annak a hierarchikus jellegét mutatja be, ahogyan egy egyént keresünk meg egy „logikai” címre alapozva. Kattintsunk az egyes csoportosításokra, hogy lássuk, a cím hogyan tevődik össze.

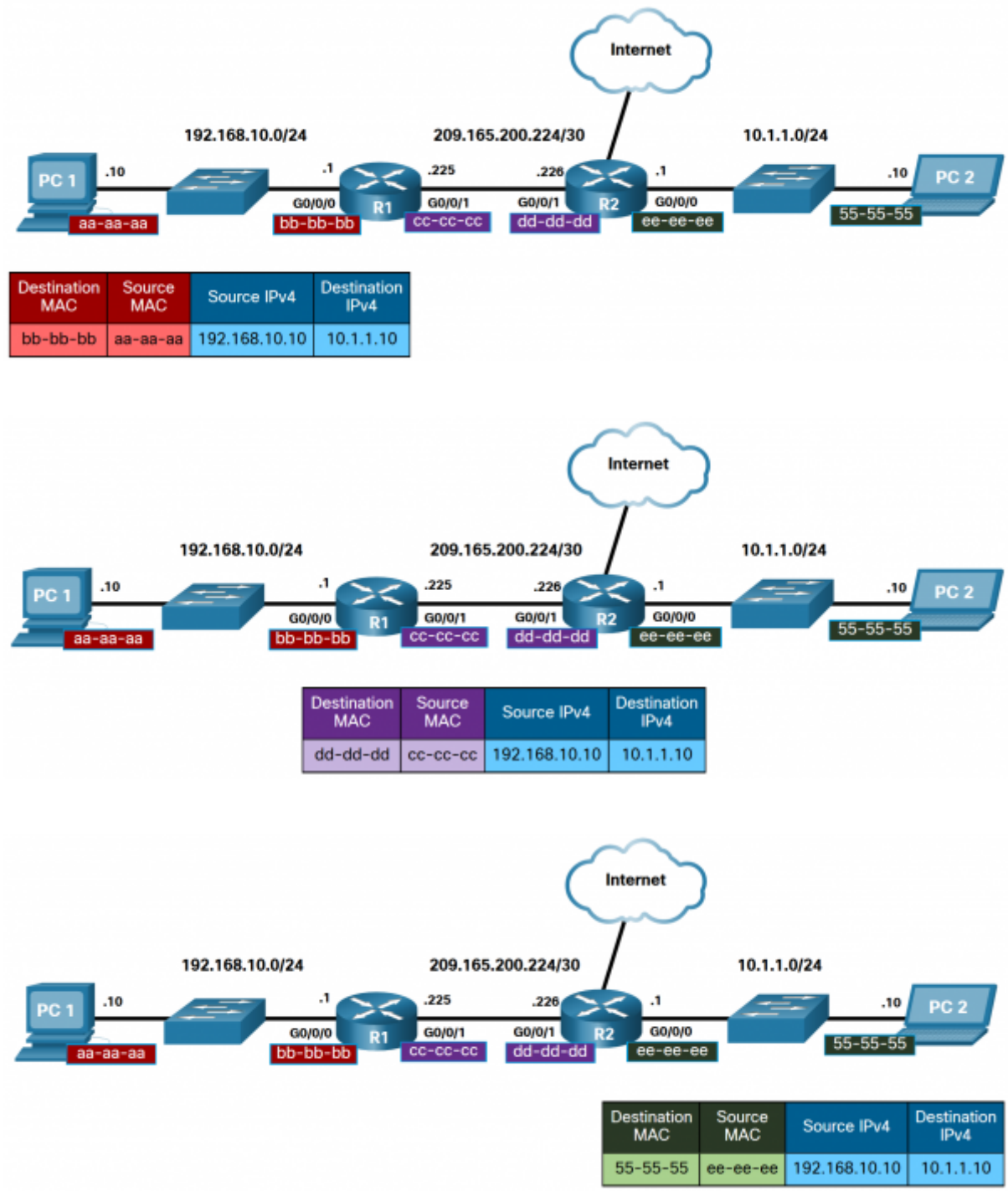
Mind a fizikai MAC-, mind pedig a logikai IP-cím szükséges a számítógép számára ahhoz, hogy egy hierarchikus hálózaton kommunikálni tudjon, mint ahogy egy személyről is szükséges tudni a nevét és a címét, hogy levelet tudjunk küldeni neki.

Amikor a címzett a helyi hálózaton található



Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Amikor a címzett egy távoli elérésű hálózaton található



A forrás eszköz a csomagot egy IP-cím alapján küldi el. Az egyik leggyakoribb módja annak, hogy a forrás eszköz meghatározza a cél eszköz IP-címét a DNS-szolgáltaatás (Domain Name Service), amelyben az IP-címhez egy tartománynevet társítunk.

Mindamellett egy IP-csomag az útvonal mentén minden kapcsolatszakaszon külön-külön beágyazódik az arra a szakaszra jellemző keretbe, mint például amilyen az Ethernet is. Egy Ethernet hálózaton a végberendezések a kapott kereteket nem az IP-cím, hanem a MAC-cím alapján fogadják és dolgozzák fel.

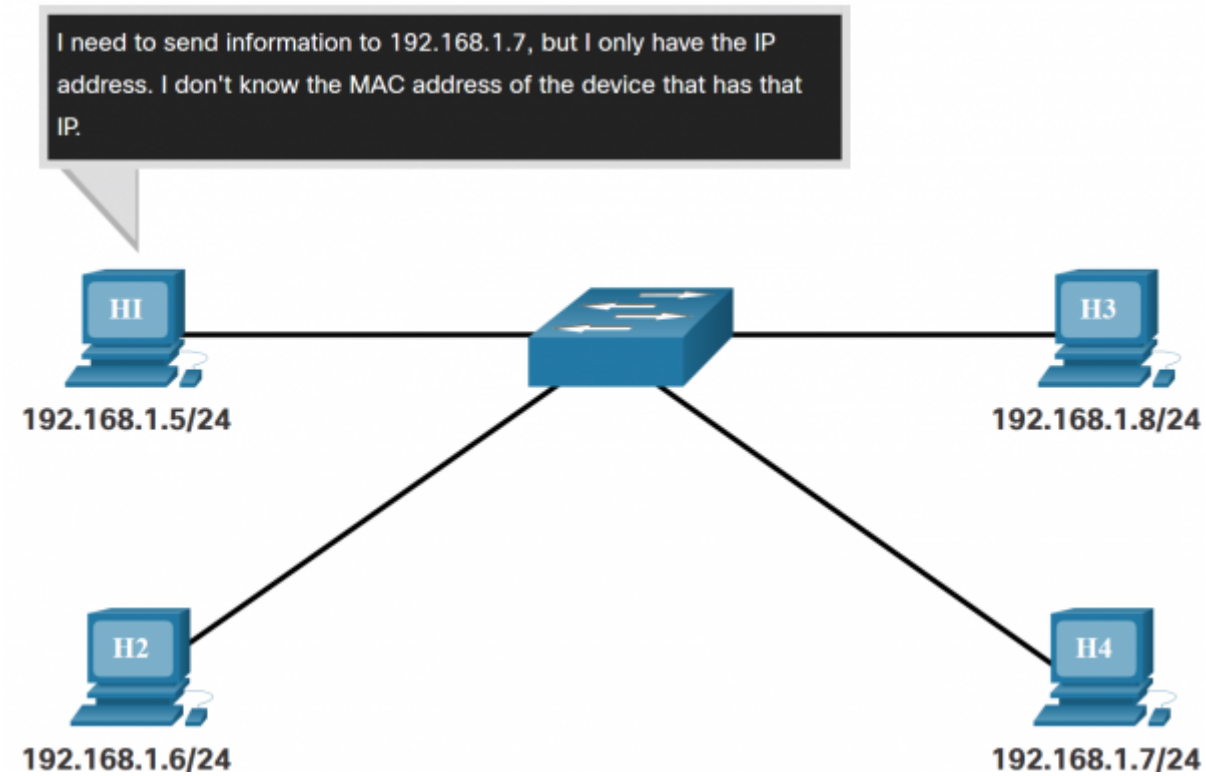
Az Ethernet hálózatok a MAC-címeket használják a forrás és a cél állomások azonosítására. Amikor

egy Ethernet hálózaton lévő állomás kommunikál, akkor olyan kereteket küld ki, amelyekben a saját MAC-címe a forráscím, és a kívánt címzett MAC-címe a célcím. Minden eszköz, amely a keretet megkapja kiolvassa belőle a cél MAC-címét. Az állomás kizárólag abban az esetben fogja a teljes üzenetet feldolgozni, amennyiben a cél MAC-cím megegyezik az állomás hálózati kártyáján beállított MAC-címmel.

Hogyan társítjuk azonban a célhoz vezető valamennyi kapcsolaton egy adatfolyam csomagjaiban lévő IP-címeket a MAC-címekhez? Ezt a folyamatot az úgynevezett címfeloldási vagy címmeghatározó protokoll (Address Resolution Protocol, ARP) végzi.

Címmeghatározó protokoll (Address Resolution Protocol, ARP)

Egy IP-hálózaton minden egyes csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Mindkét cím használata szükséges annak érdekében, hogy egy állomás adatokat küldhessen. Az állomásnak a saját MAC- és IP-címét kell használnia a forrás mezőkben, valamint meg kell adnia a célállomás MAC- és IP-címét is. Míg a cél IP-címet egy magasabb OSI-réteg fogja biztosítani, a küldő csomópontnak szüksége van egy módszerre ahhoz, hogy egy adott Ethernet kapcsolaton megtalálja a cél MAC-címét. Ez az ARP feladata.



Az ARP az Ethernet bizonyos szórásos és egyedi címzésű üzeneteire támaszkodik, az úgynevezett ARP-kérésekre és az ARP-válaszokra.

ARP funkciók

Az ARP-protokoll két alapvető funkciót biztosít:

- IPv4-címek összerendelése MAC-címekkel.

- Az összerendelési táblázat kialakítása.

IPv4-címek összerendelése MAC-címekkel

Ahhoz, hogy egy keretet a LAN átviteli közegére helyezhessünk, annak minimum egy cél MAC-címmel kell rendelkeznie. Amikor egy csomagot egy adatkapcsolati keretbe ágyazva elküldünk, az állomás a memóriájában lévő táblázatra támaszkodik, hogy megtalálja a cél IPv4-címhez tartozó adatkapcsolati rétegbeli címet. Ez a táblázat az úgynevezett ARP-táblázat vagy ARP-gyorsítótár (cache). Az ARP-táblázatot a készülék RAM-ja tárolja.

Az ARP-tábla minden bejegyzése vagy sora egy IP-címet köt össze egy MAC-címmel. A két érték közti kapcsolatot összerendelésnek vagy leképezésnek hívjuk - ez egyszerűen azt jelenti, hogy megkeresve az IP-címet a táblában megtalálhatjuk a megfelelő MAC-címet is. Az ARP-tábla csak ideiglenesen tárolja (cache-eli) a helyi LAN-eszközökhöz tartozó összerendeléseket.

A folyamat indításához a továbbító állomás megpróbálja megtalálni a cél IPv4-címhez társított MAC-címet. Ha ez az összerendelés megtalálható a táblázatban, akkor az állomás azt a MAC-címet fogja használni cél MAC-címként a keretben. A keretet ezután rákódolják a hálózati közegre.

Az ARP-táblázat karbantartása

Az ARP-táblázatot dinamikusan kezelik az eszközök. Két módja van, hogy egy készülék összegyűjthesse a MAC-címeket. Az egyik módszer az, hogy figyelemmel kíséri a helyi hálózati szegmensen előforduló forgalmat. Ahogy az állomás kereteket kap a közegen, a keret forrás IP- és MAC-címeit rögzíti az ARP-táblázatában. Miközben a keretek továbbításra kerülnek, addig a készülék folyamatosan fel is tölti az ARP-tábláját a megfelelő címpárokkal.

A készülék címpárokhoz jutásának egy másik módja, ha ARP-kéréseket küld ki, ahogy ezt az ábra is mutatja. Az ARP-kérés egy 2. rétegbeli szórás az Ethernet LAN minden eszközének . Az ARP-kérés tartalmazza a célállomás IP-címét és a szórásos MAC-címet, ami FFFF.FFFF.FFFF. Mivel ez egy szórás, minden állomás az Ethernet LAN-on megkapja és megnézi a tartalmát. Az az állomás fog válaszolni, amelynek az IP-címe megegyezik a kérésben lévő IP-címmel. A válasz egy egyedi címzésű keret lesz, amely magában foglalja a kérdéses IP-címhez tartozó MAC-címet is. Ezt a választ a küldő fél egy új tételként hozzá tudja majd adni ARP-táblájához.

Az ARP-táblázatban lévő bejegyzést hasonló időbélyeggel látják el, mint ahogy a kapcsolók kezelik a MAC-címtáblájuk bejegyzéseit. Ha a készülék nem kap keretet egy adott eszköztől az időbélyeg lejárta előtt, az eszközhöz tatozó bejegyzés kikerül az ARP-táblázatból.

Emellett statikus bejegyzéseket is lehet írni az ARP-táblába, de ez elég ritkán történik meg. A statikus ARP-bejegyzések nem járnak le az idő múlásával, és így kézzel kell őket eltávolítani.

Az ARP működése

A keret létrehozása

Mit tehet egy csomópont, ha egy keretet kell létrehoznia, és az ARP-cache nem tartalmaz bejegyzést

a cél MAC-címhez tartozó IP-címről? Létrehoz egy ARP-kérést!

Amikor az ARP-nek meg kell állapítania egy IPv4-címhez tartozó MAC-címet, azt először az ARP-táblázatban keresi. Ha a bejegyzés nem található, az IPv4 csomag beágyazása nem sikerül és a 2. rétegbeli folyamatok értesítik az ARP-t, hogy szükség van egy új összerendelésre. Az ARP folyamat ekkor kiküld egy ARP-kérést, hogy felderítse a helyi hálózaton a cél eszköz MAC-címét. Amennyiben egy eszköz a kérésben kapott cél IP-címmel rendelkezik, akkor egy ARP-választ küld vissza. Így létrejön az összerendelés az ARP-táblázatban. Az erre az IPv4-címre szóló csomagokat immár be lehet ágyazni a keretekbe.

Ha egyetlen eszköz sem válaszol az ARP-kérésre, a csomagot eldobják, mivel a keret nem hozható létre. Ezt a beágyazási hibát jelenteni kell az eszköz felsőbb rétegei felé. Ha az eszköz egy közvetítő eszköz, például egy forgalomirányító, a felső rétegek dönthetnek úgy, hogy a forrás állomásnak egy hibát jelző ICMPv4-csomaggal válaszolnak.

Az ARP szerepe a távoli kommunikációban

Minden keretet egy a helyi hálózati szegmensen lévő állomás felé kell továbbítani. Amennyiben a cél IPv4-állomás a helyi hálózaton van, a keret ennek a készüléknek a MAC-címét fogja használni mint cél MAC-címet.

Ha a cél IPv4-állomás nem a helyi hálózaton található, abban az esetben a forrás csomópontnak a keretet ahhoz a forgalomirányító interfészhez kell továbbítani, amelyet ezen cél eléréséhez átjáróként vagy más néven a következő ugrásként (next hop) használunk. A forrás csomópont az átjáró MAC-címét fogja használni a célállomás címeként minden olyan keret esetében, amely olyan IPv4-csomagot tartalmaz, amelyet másik hálózaton lévő állomásnak címeznek.

Az átjárónak, azaz a forgalomirányító interfészének a címét az állomások az IPv4-konfigurációjukban tárolják. Amikor az állomás létrehoz egy csomagot egy célállomásnak, összehasonlítja a cél IP-címet és a saját IP-címét annak meghatározására, hogy a két IP-cím ugyanazon a 3. rétegbeli hálózaton található-e. Ha a fogadó gép nem ugyanazon a hálózaton van, a forrás az ARP folyamatot az átjáró MAC-címének meghatározására használja.

Abban az esetben, ha az átjáró bejegyzés nem szerepel a táblázatban, a normál ARP folyamat kiküld egy ARP-kérést, hogy megszerezze a forgalomirányító interfész IP-címéhez társított MAC-címet.

Bejegyzések eltávolítása egy ARP-táblázatból

Egy ARP-cache időzítő távolítja el minden eszközön azokat az ARP-bejegyzéseket, amelyeket egy meghatározott idő óta nem használtak. Az időzítő függ a készüléktől és annak operációs rendszerétől. Egyes Windows operációs rendszerek például 2 percig tárolják az ARP-cache bejegyzéseket. Ha ez idő alatt a bejegyzést ismételten használják, a hozzá tartozó ARP-időzítő 10 percre meghosszabbodik.

Parancsokat is használhatunk, hogy az ARP-táblából manuálisan távolítsunk el bizonyos bejegyzéseket, vagy akár az összeset. Egy bejegyzés eltávolítása után, az ARP-kérés küldés és ARP-válasz fogadás folyamatának ismét meg kell történnie, hogy az összerendelés az ARP-táblázatba újból bekerülhessen.

Minden készülék egyedi, az operációs rendszertől függő paranccsal rendelkezik az ARP-cache

tartalmának törlésére. Ezek a parancsok semmilyen módon nem eredményezik az ARP végrehajtását. Egyszerűen csak eltávolítják a bejegyzéseket az ARP-táblából. Az ARP-szolgáltatást az IPv4-protokollba integrálják és maga a készülék hajtja végre. Működése észrevehetetlen mind a felső rétegbeli alkalmazások, mind a felhasználók számára.

ARP-táblázat a hálózati eszközökön

Egy Cisco forgalomirányítón a **show ip arp** parancsot használjuk az ARP-táblázat megjelenítéséhez:

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA
GigabitEthernet0/0/0
Internet  209.165.200.225        -   a0e0.af0d.e141  ARPA
GigabitEthernet0/0/1
Internet  209.165.200.226        1   a03d.6fe1.9d91  ARPA
GigabitEthernet0/0/1
R1#
```

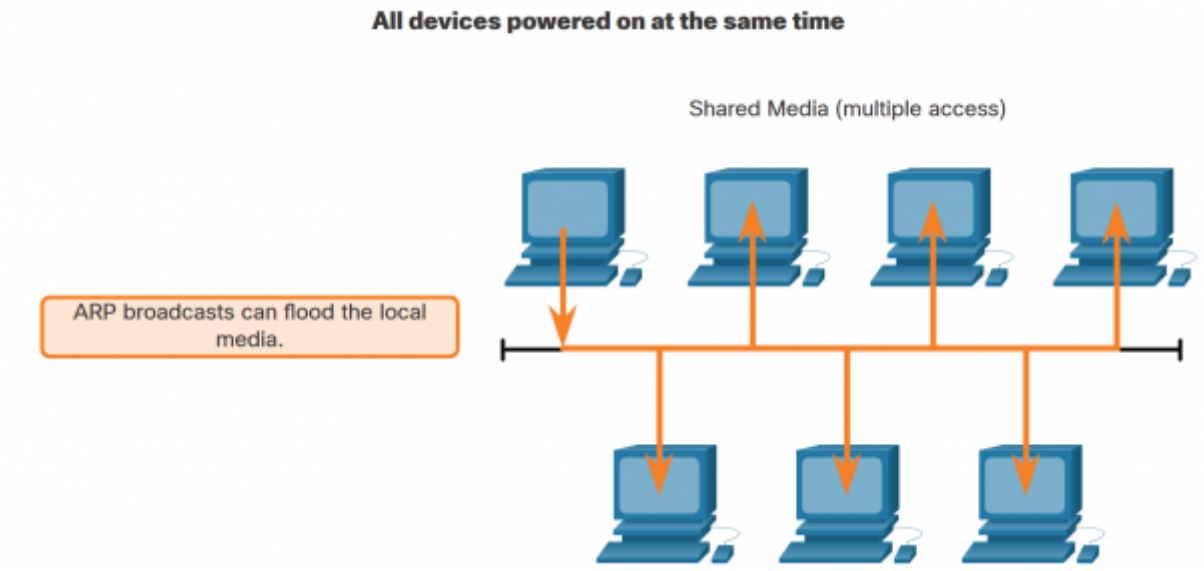
Egy Windows PC-n az **arp -a** parancsot használjuk az ARP-táblázat megjelenítéséhez:

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

ARP problémák

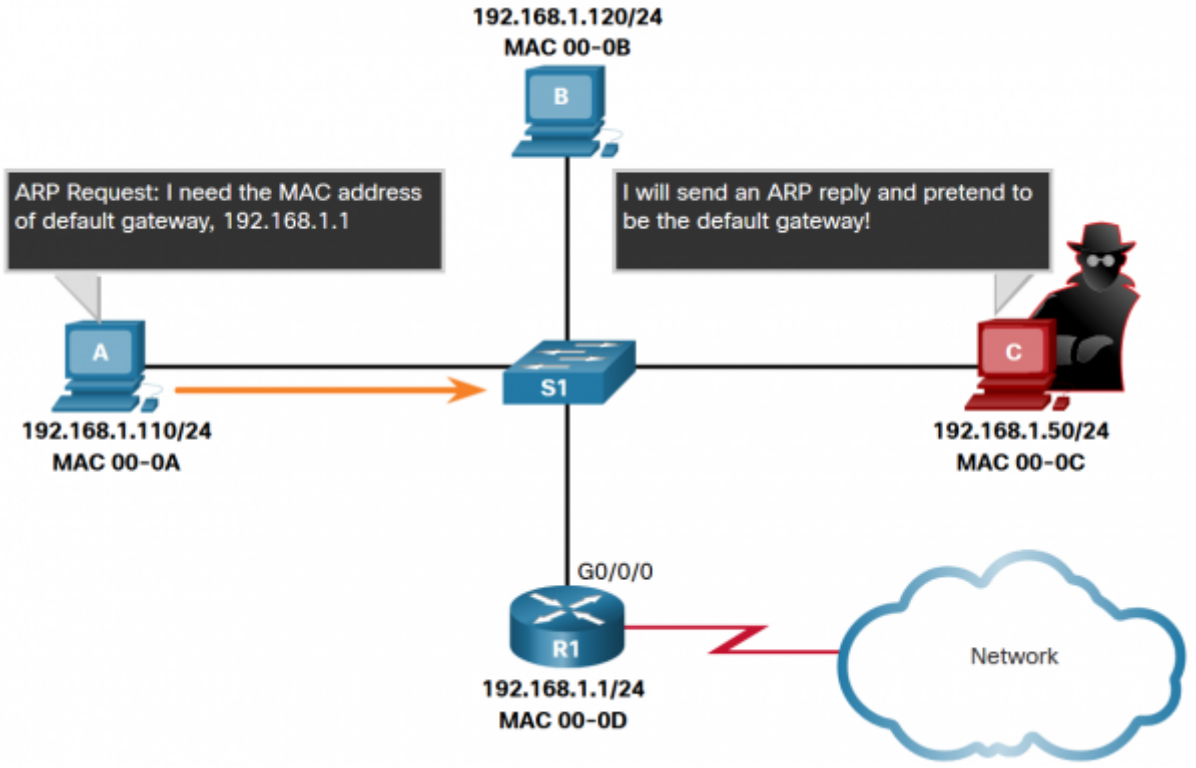
- A közeg túlterhelése
- Biztonsági problémák

A közeg túlterhelése



Szórásos keret lévén egy ARP-kérést a helyi hálózaton minden eszköz megkap és feldolgoz. Egy általános üzleti hálózaton ezek a szórások valószínűleg minimális hatással vannak a hálózati teljesítményre. Ugyanakkor ha nagy számú készüléket kapcsolnak be egyszerre és az összes hálózati szolgáltatás elérése ugyanabban az időben kezdődik, a teljesítmény egy kis időre csökkenhet. Ha például a laborban minden diák egyszerre jelentkezik be a tantermi számítógépekre és próbálja meg elérni az internetet, előfordulhatnak késések. Azonban miután a készülékek kiküldték az első ARP-szórásokat és megtanulták a szükséges MAC-címeket, a későbbi tanulási folyamatok hatása már csak minimális terhelést fog jelenteni.

Biztonsági problémák



Bizonyos esetekben az ARP használata potenciális biztonsági kockázatot jelenthet. Az ARP-spoofing (hamisítás) vagy az ARP-mérgezés egy-egy olyan technika, amely által a támadó hamis MAC-cím

összerendeléseket juttat a hálózatra hamis ARP-kérések segítségével. Ha a támadó meghamisítja egy eszköz MAC-címét, akkor azután a kereteket már nem a megfelelő helyre fogják küldeni.

Az ARP-hamisítás megakadályozásának egyik módja a manuálisan beállított statikus ARP-bejegyzések. Bizonyos hálózati eszközökön hitelesített MAC-címeket lehet beállítani, hogy a hálózati hozzáférést csak ezekre a listán szereplő eszközökre korlátozzuk.

ARP problémák enyhítése

Az ARP-vel kapcsolatos szórási és biztonsági kérdések enyhíthetők a modern kapcsolókkal. A Cisco kapcsolók számos általános, de kifejezetten ARP jellegű biztonsági technológiát is alkalmaznak, hogy enyhítsék az Ethernet szórásokkal kapcsolatos problémákat.

A kapcsolók szegmentálást biztosítanak a LAN-on, felosztva a LAN-t önálló ütközési tartományokra. A kapcsolón minden port egy külön ütközési tartományt jelent, és biztosítja a közeg teljes sávszélességét a portra csatlakozó állomás vagy állomások számára. Bár a kapcsolók alapértelmezés szerint nem akadályozzák a szórások továbbítását, de elkülönítik az egyedi címzésű Ethernet kommunikációt, hogy azt csak a forrás és a cél eszközök „hallhassák”. Tehát lehet akár nagyszámú ARP-kérés is, az ARP-válaszok mindegyike már csak két eszköz között fog létrejönni.

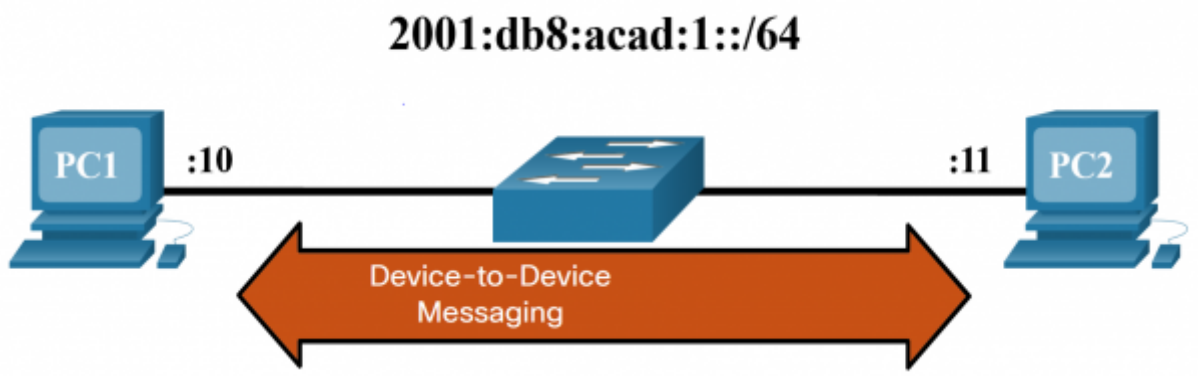
Tekintettel az Ethernet hálózatokon gyakori különféle szórásos támadások enyhítésére, a hálózati mérnökök különböző biztonsági beállításokkal védekezhetnek ezek ellen. Ilyenek lehetnek például a speciális hozzáférési listák és a portbiztonság alkalmazása.

Szomszédsági felderítés IPv6 felett (IPv6 Neighbor Discovery)

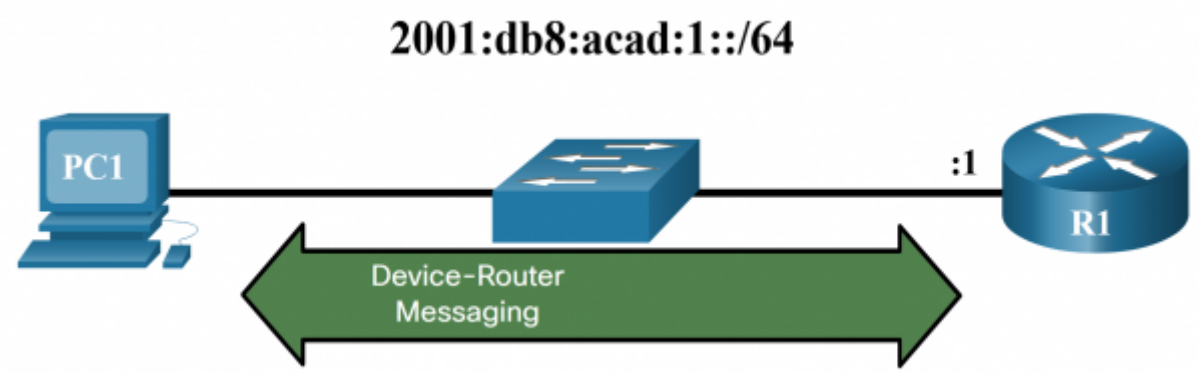
Az IPv6 Neighbor Discovery protokollt néha ND-nek vagy NDP-nek nevezik. Jelen tananyagban ND-ként fogunk rá hivatkozni. Az ND címfeloldási, útválasztási felfedezési és átirányítási szolgáltatásokat nyújt az IPv6 számára az ICMPv6 segítségével. Az ICMPv6 ND öt féle ICMPv6 üzenetet használ a szolgáltatások teljesítéséhez:

- ICMPv6 szomszédkeresés (Neighbor Solicitation) üzenetet
- ICMPv6 szomszédhirdetés (Neighbor Advertisement)
- Forgalomirányító-keresés (Router Solicitation, RS) üzenet
- Forgalomirányító-hirdetés (Router Advertisement, RA) üzenet
- Átirányítási üzenet

A szomszédkereséses és a szomszédhirdetéses üzeneteket az eszközök közötti üzenetküldéshez, például a címfelbontáshoz használják (hasonlóan az IPv4 feletti ARP-hez). Eszközök alatt úgy gazdagépeket, mint útválasztókat értünk.



A forgalomirányító-keresése és a forgalomirányító-hirdetési üzenetei az eszközök és a forgalomirányítók közötti üzenetküldésre szolgálnak. Az útválasztó felfedezését általában a dinamikus címosztáshoz és az állapotmentes (stateless) címek automatikus konfigurálásához (SLAAC) használják.



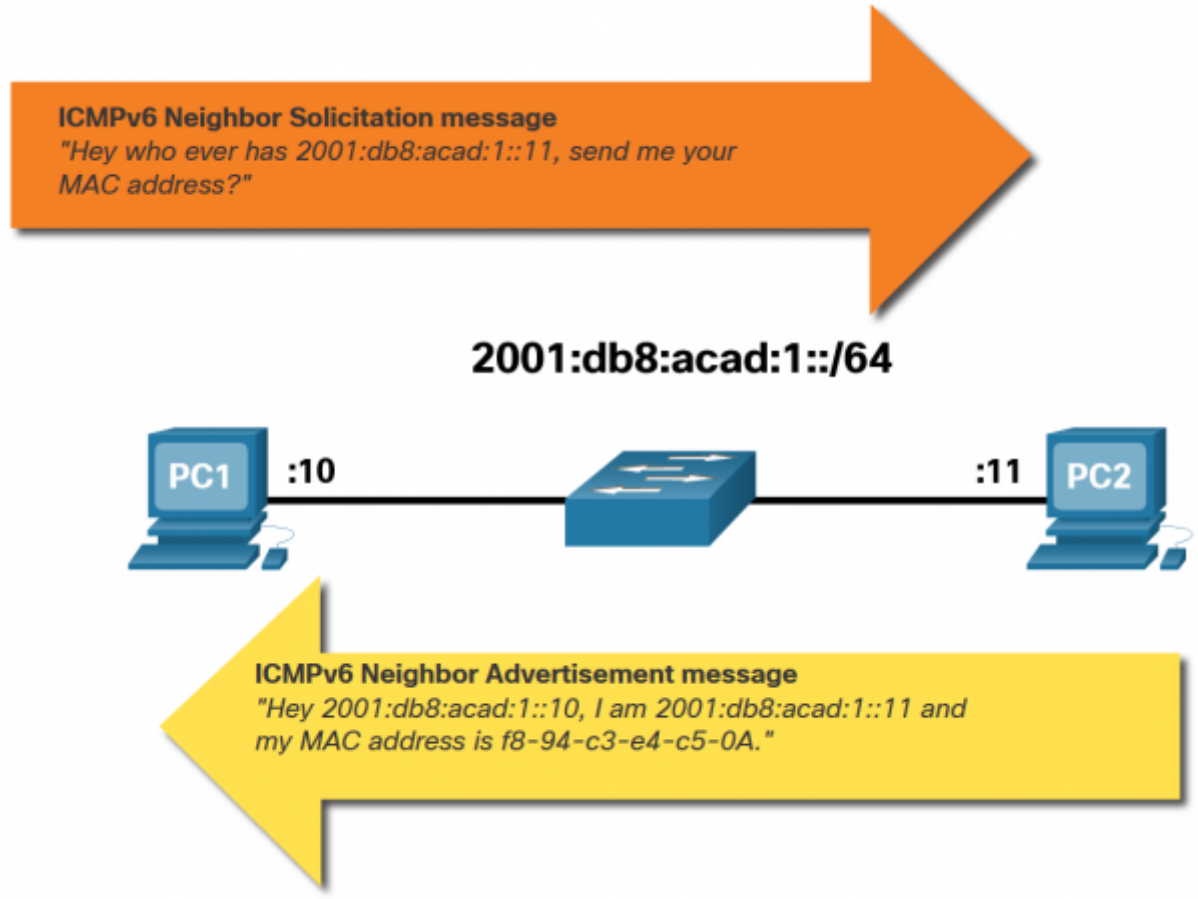
Megjegyzés:

Az ötödik ICMPv6 ND üzenet egy átirányítási üzenet, melyet a legjobb következő ugrás (next hop) kiválasztásához használnak. Ez viszont meghaladja a tananyag kereteit.

Az IPv6 ND-t az IETF RFC 4861 szabványleírásban definiálták.

Az IPv4 felett működő ARP-hez hasonlóan az IPv6-eszközök az IPv6 feletti ND-t használják címfeloldás céljából, egy ismert IPv6 cím alapján.

Az ICMPv6 Neighbor Solicitation és a Neighbor Advertisement üzeneteket használják a MAC-címek feloldására. Ez hasonló az IPv4 feletti ARP-kérelmekhez és ARP-válaszokhoz. Tegyük fel például, hogy a PC1-ről pingelni szeretnék a PC2-őt a 2001:db8: acad :: 11 IPv6-címen. Az ismert IPv6-cím MAC-címének meghatározásához a PC1 ICMPv6 Neighbor Solicitation üzenetet küld, amint az az alábbi ábrán látható:



Az ICMPv6 Neighbor Solicitation üzeneteket speciális Ethernet és IPv6 multicast címek segítségével küldik el. Ez lehetővé teszi, hogy a fogadó eszköz Ethernet hálózati kártyája meg tudja határozni, hogy a Neighbor Solicitation üzenet neki szól-e, anélkül, hogy feldolgozás céljából el kellene küldenie azt az operációs rendszernek.

A PC2 egy ICMPv6 Neighbor Advertisement üzenettel válaszol a kérésre, amely tartalmazza annak MAC-címét.