MAC Addresses

Ցանցի յուրաքանչյուր հոսթ ունի իր սեփական 48 -բիթանոց (6 octets) Media Access Control (MAC) հասցեն, որը ներկայացված է տասնվեցական ձևաչափով: MAC-ը մեր ցանցային ինտերֆեյսների physical address-ն է: MAC հասցեի համար կան մի քանի տարբեր ստանդարտներ՝

- Ethernet (IEEE 802.3)
- Bluetooth (IEEE 802.15)
- WLAN (IEEE 802.11) կամ Անլար ցանց (IEEE 802.11)

Սա պայմանավորված է նրանով, որ MAC հասցեն վերաբերում է հոսթի ֆիզիկական միացմանը (ցանցային քարտ, Bluetooth կամ WLAN ադապտեր): Յուրաքանչյուր network card ունի իր անհատական MAC հասցեն, որը կարգավորվում է մեկ անգամ արտադրողի սարքային կողմում, բայց միշտ կարող է փոխվել, գոնե ժամանակավորապես:

Եկեք դիտարկենք նման MAC հասցեի օրինակ.MAC address:

- DE:AD:BE:EF:13:37
- DE-AD-BE-EF-13-37
- DEAD.BEEF.1337

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ

Binary Երկուական	1101 1110	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	DE	AD	BE	EF	13	37

Երբ IP փաթեթը առաքվում է, այն պետք է հասցեագրվի layer 2 ՝ նպատակակետի հոսթի ֆիզիկական հասցեին կամ ռաուտերին / NAT-ին, որը պատասխանատու է երթուղավորման համար: Յուրաքանչյուր փաթեթ ունի sender address և destination address :
MAC հասցեն բաղկացած է ընդհանուր առմամբ 6 bytes : Առաջին կեսը (3 bytes / 24 bit) այսպես կոչված Organization Unique Identifier -ն է (OUI), որը սահմանվում է Institute of Electrical and Electronics Engineers -ով (IEEE) համապատասխան արտադրողների համար:

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1101 1110	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	DE	AD	BE	EF	13	37

MAC հասցեի վերջին կեսը կոչվում է Individual Address Part կամ Network Interface Controller (NIC), որը հատկացնում են արտադրողները: Արտադրողը այս բիթային հաջորդականությունը սահմանում է միայն մեկ անգամ և այդպիսով ապահովում է, որ ամբողջական հասցեն եզակի լինի:

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1101 1110	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	DE	AD	BE	EF	13	37

Եթե նույն ենթացանցում գտնվում է նույն IP հասցեն ունեցող հոսթը, ապա առաքումը կատարվում է անմիջապես նպատակային համակարգչի ֆիզիկական հասցեին: Սակայն, եթե այս հոսթը պատկանում է այլ ենթացանցի, Ethernet շրջանակը հասցեագրվում է պատասխանատու ռաութերի MAC address (default gateway): Եթե Ethernet շրջանակի նպատակակետի հասցեն համընկնում է իր layer 2 address , ռաութերը կուղղորդի շրջանակը ավելի բարձր շերտեր: Address Resolution Protocol (ARP) օգտագործվում է IPv4-ում՝ IP հասցեների հետ կապված MAC հասցեները որոշելու համար:
Ինչպես IPv4 հասցեների դեպքում, MAC հասցեի համար նույնպես կան որոշակի պահուստավորված տարածքներ: Դրանք ներառում են, օրինակ, MAC հասցեի տեղական տիրույթը:

Local Range Տեղական տիրույթ
02:00:00:00:00:00 0 2 :00:00:00:00:00
06:00:00:00:00:00 0 6 :00:00:00:00:00
0A:00:00:00:00:00 0 A :00:00:00:00:00
0E:00:00:00:00:00 0 E :00:00:00:00:00

Ավելին, առաջին օկտետի վերջին երկու բիթերը կարող են խաղալ մեկ այլ կարևոր դեր: Վերջին բիթը, ինչպես արդեն գիտենք, կարող է ունենալ երկու վիճակ՝ 0 և 1: Վերջին բիթը MAC հասցեն նույնականացնում է որպես Unicast (0) կամ Multicast (1): unicast դեպքում դա նշանակում է, որ ուղարկված փաթեթը կհասնի միայն մեկ որոշակի հոսթի:

MAC Unicast

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1101 1110 1101 111 0	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	DE	AD	BE	EF	13	37

---

multicast դեպքում փաթեթը միայն մեկ անգամ է ուղարկվում տեղական ցանցի բոլոր հոսթերին, որոնք այնուհետև որոշում են՝ ընդունել փաթեթը, թե ոչ՝ հիմնվելով դրանց կոնֆիգուրացիայի վրա: multicast հասցեն եզակի հասցե է, ինչպես broadcast հասցեն, որն ունի ֆիքսված օկտետային արժեքներ: Ցանցում Broadcast ներկայացնում է հեռարձակված զանգ, որտեղ տվյալների փաթեթները միաժամանակ փոխանցվում են մեկ կետից ցանցի բոլոր անդամներին: Այն հիմնականում օգտագործվում է, եթե փաթեթի ստացողի հասցեն դեռևս հայտնի չէ: Օրինակ են ARP (for MAC addresses) և DHCP (for IPv4 addresses) արձանագրությունները:Յուրաքանչյուր օկտետի սահմանված արժեքները նշված են green :

MAC Multicast MAC բազմահեռարձակում

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	0000 0001	0000 0000	0101 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	01	00	5E	EF	13	37

MAC Broadcast MAC հեռարձակում

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1111 1111	1111 1111	1111 1111	1111 1111	1111 1111	1111 1111
Hex Տասնվեցական	FF	FF	FF	FF	FF	FF

Առաջին օկտետի նախավերջին բիթը որոշում է, թե արդյոք դա IEEE-ի կողմից սահմանված global OUI է, թե locally administrated MAC հասցե:

Global OUI

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1101 1100 1101 11 0 0	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111
Hex Տասնվեցական	DC	AD	BE	EF	13	37

Locally Administrated Տեղականորեն կառավարվող

Representation Ներկայացուցչություն	1st Octet 1-ին օկտետ	2nd Octet 2-րդ օկտետ	3rd Octet 3-րդ օկտետ	4th Octet 4-րդ օկտետ	5th Octet 5-րդ օկտետ	6th Octet 6-րդ օկտետ
Binary Երկուական	1101 1110 1101 11 1 0	1010 1101	1011 1110	1110 1111	0001 0011	0011 0111

Hex Տասնվեցական	DE	AD	BE	EF	13	37

MAC Address Attack Vectors

MAC հասցեները կարող են փոփոխվել/մանիպուլացվել կամ կեղծվել, և, հետևաբար, դրանք չպետք է համարվեն անվտանգության կամ նույնականացման միակ միջոց: Ցանցի ադմինիստրատորները պետք է ներդնեն լրացուցիչ անվտանգության միջոցառումներ, ինչպիսիք են ցանցի սեգմենտացումը և ուժեղ նույնականացման արձանագրությունները՝ հնարավոր հարձակումներից պաշտպանվելու համար:

Կան մի քանի հարձակման վեկտորներ, որոնք կարող են շահագործվել MAC հասցեների օգտագործման միջոցով.

- MAC spoofing . Սա ենթադրում է սարքի MAC հասցեի փոփոխություն՝ այն համապատասխանեցնելով մեկ այլ սարքի MAC հասցեին, սովորաբար ցանցին չարտոնված մուտք ստանալու համար:

- MAC flooding . Սա ենթադրում է տարբեր MAC հասցեներով բազմաթիվ փաթեթների ցանցային կոմուտատորին ուղարկում, ինչի հետևանքով այն հասնում է իր MAC հասցեների աղյուսակի ծավալին և արդյունավետորեն խոչընդոտում է դրա ճիշտ գործունեությանը:

- MAC address filtering . Որոշ ցանցեր կարող են կարգավորված լինել միայն այնպիսին, որ թույլ տան մուտք գործել միայն որոշակի MAC հասցեներ ունեցող սարքեր, որոնք մենք կարող ենք շահագործել՝ փորձելով մուտք գործել ցանց կեղծ MAC հասցեի միջոցով:

Address Resolution Protocol

Հասցեի լուծման արձանագրություն

Address Resolution Protocol (ARP) ցանցային արձանագրություն է: Այն ցանցային հաղորդակցության կարևոր մասն է, որն օգտագործվում է network layer-ի (3-րդ շերտ) IP հասցեն link layer-ի (2-րդ շերտ) MAC հասցեի վերափոխելու համար: Այն կապում է հոսթի IP հասցեն համապատասխան MAC հասցեի հետ՝ տեղական ցանցի (LAN) սարքերի միջև հաղորդակցությունը հեշտացնելու համար: Երբ տեղական ցանցի սարքը ցանկանում է հաղորդակցվել մեկ այլ սարքի հետ, այն ուղարկում է broadcast հաղորդագրություն, որը պարունակում է նպատակակետի IP հասցեն և իր սեփական MAC հասցեն: Համապատասխան IP հասցե ունեցող սարքը պատասխանում է իր սեփական MAC հասցեով, և երկու սարքերը կարող են անմիջապես հաղորդակցվել՝ օգտագործելով իրենց MAC հասցեները: Այս գործընթացը հայտնի է որպես ARP լուծում:
ARP-ը ցանցային հաղորդակցման գործընթացի կարևոր մասն է կազմում, քանի որ այն թույլ է տալիս սարքերին ուղարկել և ստանալ տվյալներ՝ օգտագործելով MAC հասցեներ, այլ ոչ թե IP հասցեներ, ինչը կարող է ավելի արդյունավետ լինել: Կարելի է օգտագործել հարցման երկու տեսակ՝

ARP Request ARP **հարցում**

Երբ սարքը ցանկանում է կապ հաստատել տեղական ցանցի մեկ այլ սարքի հետ, այն ուղարկում է ARP հարցում՝ նպատակակետային սարքի IP հասցեն իր MAC հասցեի հետ կապելու համար: Հարցումը հեռարձակվում է տեղական ցանցի բոլոր սարքերին և պարունակում է նպատակակետային սարքի IP հասցեն: Համապատասխան IP հասցե ունեցող սարքը պատասխանում է իր MAC հասցեով:

ARP Reply ARP **պատասխան**

Երբ սարքը ստանում է ARP հարցում, այն ուղարկում է ARP պատասխան հարցում ուղարկող սարքին՝ նշելով դրա MAC հասցեն: Պատասխան հաղորդագրությունը պարունակում է հարցում ուղարկող և պատասխանող սարքերի IP և MAC հասցեները:

Tshark Capture of ARP Requests

MAC Addresses

1 0.000000 10.129.12.100 -> 10.129.12.255 ARP 60 Who has 10.129.12.101? Tell 10.129.12.100
2 0.000015 10.129.12.101 -> 10.129.12.100 ARP 60 10.129.12.101 is at AA:AA:AA:AA:AA:AA

3 0.000030 10.129.12.102 -> 10.129.12.255 ARP 60 Who has 10.129.12.103? Tell 10.129.12.102
4 0.000045 10.129.12.103 -> 10.129.12.102 ARP 60 10.129.12.103 is at BB:BB:BB:BB:BB:BB

Առաջին և երրորդ տողերում « who has » հաղորդագրությունը ցույց է տալիս, որ սարքը հարցում է կատարում նշված IP հասցեի MAC հասցեի համար, մինչդեռ երկրորդ և չորրորդ տողերը ցույց են տալիս ARP պատասխանը՝ նպատակակետային սարքի MAC հասցեով:
Սակայն այն նաև խոցելի է հարձակումների նկատմամբ, ինչպիսին է ARP Spoofing-ը , որը կարող է օգտագործվել ցանցում երթևեկությունը խափանելու կամ մանիպուլյացիայի ենթարկելու համար: Այնուամենայնիվ, նման հարձակումներից պաշտպանվելու համար կարևոր է ներդնել անվտանգության միջոցառումներ, ինչպիսիք են firewall-ները և ներխուժման հայտնաբերման համակարգերը:
ARP spoofing , որը հայտնի է նաև որպես ARP cache poisoning կամ ARP poison routing , հարձակում է, որը կարող է իրականացվել Ettercap կամ Cain & Abel նման գործիքների միջոցով, որոնց միջոցով մենք LAN-ի միջոցով ուղարկում ենք կեղծ ARP հաղորդագրություններ: Նպատակն է մեր MAC հասցեն կապել ընկերության ցանցում գտնվող օրինական սարքի IP հասցեի հետ, ինչը թույլ է տալիս մեզ արդյունավետորեն խլել օրինական սարքի համար նախատեսված երթևեկությունը: Օրինակ, սա կարող է հետևյալ տեսք ունենալ.

MAC Addresses MAC հասցեներ

1 0.000000 10.129.12.100 -> 10.129.12.101 ARP 60 10.129.12.101 is at AA:AA:AA:AA:AA:AA
2 0.000015 10.129.12.100 -> 10.129.12.255 ARP 60 Who has 10.129.12.101? Tell 10.129.12.100
3 0.000030 10.129.12.101 -> 10.129.12.100 ARP 60 10.129.12.101 is at BB:BB:BB:BB:BB:BB
4 0.000045 10.129.12.100 -> 10.129.12.101 ARP 60 10.129.12.101 is at AA:AA:AA:AA:AA:AA

Առաջին և չորրորդ տողերը ցույց են տալիս, թե ինչպես է թիրախը (10.129.12.100) կեղծ ARP հաղորդագրություններ ուղարկում թիրախին՝ կապելով նրա MAC հասցեն նրա IP հասցեի հետ (10.129.12.101): Երկրորդ և երրորդ տողերը ցույց են տալիս, թե ինչպես է թիրախը ուղարկում ARP հարցում և պատասխանում մեր MAC հասցեին: Սա նշանակում է, որ մենք թունավորել ենք թիրախի ARP քեշը, և որ թիրախի համար նախատեսված ողջ տրաֆիկը այժմ կուղարկվի մեր MAC հասցեին:
Մենք կարող ենք օգտագործել ARP թունավորումը տարբեր գործողություններ կատարելու համար, ինչպիսիք են զգայուն տեղեկատվության գողությունը, երթևեկության վերահասցեավորումը կամ MITM հարձակումներ իրականացնելը: Այնուամենայնիվ, ARP կեղծումից պաշտպանվելու համար կարևոր է օգտագործել անվտանգ ցանցային արձանագրություններ, ինչպիսիք են IPSec-ը կամ SSL-ը, և ներդնել անվտանգության միջոցառումներ, ինչպիսիք են firewall-ները և ներխուժման հայտնաբերման համակարգերը: