21 ARP: פרוטוקול פתרון כתובת

כמחשב ברשת, יש לנו בעיה.

אנו רוצים לשלוח נתונים ברשת המקומית (LAN) למחשב אחר על אותו תת-רשת.

הנה מה שעלינו לדעת כדי לבנות מסגרת Ethernet:

- הנתונים שאנו רוצים לשלוח ואורכם
- כתובת ה-MAC שלנו
- כתובת ה-MAC של היעד שלהם

הנה מה שאנו יודעים:

- הנתונים שאנו רוצים לשלוח ואורכם
- כתובת ה-MAC שלנו
- כתובת ה-IP שלנו
- כתובת ה-IP של היעד שלהם

מה חסר? למרות שאנו יודעים את כתובת ה-IP של המחשב השני, איננו יודעים את כתובת ה-MAC שלו. איך נוכל לבנות מסגרת Ethernet בלי כתובת ה-MAC שלו? לא נוכל. עלינו להשיג אותה איכשהו.

שוב, לחלק זה אנו מדברים על שליחה ברשת המקומית, ה-Ethernet המקומית. לא דרך האינטרנט עם IP. זה בין שני מחשבים על אותו רשת פיזית.

חלק זה עוסק ב-ARP, פרוטוקול פתרון כתובת. זהו הדרך בה מחשב אחד יכול למפות את כתובת ה-IP של מחשב אחר לכתובת ה-MAC של אותו מחשב.

21.1 מסגרות שידור Ethernet

אך תחילה, אנו צריכים קצת רקע.

זכרו שהחומרה של הרשת מקשיבה למסגרות Ethernet שמופנות אליה באופן ספציפי. מסגרות Ethernet שמיועדות לכתובת MAC אחרת נזנחות.

הערה צדדית: הן נזנחות אלא אם כרטיס הרשת נמצא במצב פרומיסקי, במצב כזה הוא מקבל את כל התעבורה ברשת המקומית ומעביר אותה למערכת ההפעלה.

אבל יש דרך לעקוף את זה: מסגרת השידור. זוהי מסגרת שמיועדת לכתובת MAC ff:ff:ff:ff:ff:ff. כל המכשירים ברשת המקומית יקבלו את המסגרת הזו.

אנו הולכים לנצל את זה עם ARP.

21.2 ARP–פרוטוקול פתרון כתובת

אז יש לנו את כתובת ה-IP של היעד, אבל לא את כתובת ה-MAC שלו. אנו רוצים את כתובת ה-MAC שלו.

הנה מה שיקרה:

המחשב השולח ישדר מסגרת Ethernet מיוחדת שמכילה את כתובת ה-IP של היעד. זוהי בקשת ARP.

(זכרו את שדה EtherType מפרק קודם? חבילות ARP יש להן EtherType 0x0806 כדי להבחין בינן לבין חבילות Ethernet רגילות.)

כל המחשבים ברשת המקומית יקבלו את בקשת ה-ARP ויבדקו אותה. אבל רק המחשב עם כתובת ה-IP שצוינה בבקשת ה-ARP ימשיך. המחשבים האחרים ייפסלו את החבילה.

המחשב היעד עם כתובת ה-IP שצוינה יבנה תגובת ARP. מסגרת Ethernet זו מכילה את כתובת ה-MAC של המחשב היעד.

המחשב היעד שולח את תגובת ARP חזרה למחשב השולח.

המחשב השולח מקבל את תגובת ARP, ועכשיו הוא יודע את כתובת ה-MAC של המחשב היעד.

ועכשיו, המשחק מתחיל! עכשיו כשאנחנו יודעים את כתובת ה-MAC, אנו יכולים לשלוח בלי חשש.

21.3 Cache של ARP

מכיוון שזה מציק לבקש ממחשב את כתובת ה-MAC שלו כל פעם שאנו רוצים לשלוח לו משהו, נשמור את התוצאה במטמון לכמה זמן.

לאחר מכן, כשנרצה לשלוח ל-IP מסוים ברשת המקומית, נוכל להסתכל במטמון ARP ולראות אם הזוג IP/ Ethernet כבר שם. אם כן, אין צורך לשלוח בקשת ARP–פשוט נוכל לשלוח את הנתונים מייד.

הער entries במטמון יתפוגגו ויימחקו אחרי פרק זמן מסוים. אין זמן תקן לפג תוקף, אבל ראיתי ערכים שנעים בין 60 שניות ל-4 שעות.

הער entries עשויות להתיישן אם כתובת ה-MAC משתנה לכתובת IP נתונה. אז הער entry במטמון יהיה לא עדכני. הדרך הקלה ביותר לזה לקרות היא אם מישהו סוגר את המחשב הנייד שלו ועוזב את הרשת (ולוקח את כתובת ה-MAC שלו איתו), ואז מישהו אחר עם מחשב נייד שונה (כתובת MAC שונה) מגיע ומקבל את אותה כתובת IP. אם זה יקרה, מחשבים עם הער entry הישנה ישלחו את המסגרות לאותו IP לכתובת ה-MAC הלא נכונה (הישנה).

21.4 מבנה ARP

נתוני ARP נמצאים בחלק ה-Payload של מסגרת Ethernet. מדובר באורך קבוע. כמו שנאמר קודם, הוא מזוהה על ידי קביעת שדה EtherType/אורך חבילה ל-0x0806.

במבנה ה-Payload למטה, כאשר כתוב "Hardware" זה מתייחס לשכבת הקישור (למשל, Ethernet בדוגמה הזו) וכשכתוב "Protocol" זה מתייחס לשכבת הרשת (למשל, IP בדוגמה הזו). הם משתמשים בשמות הכלליים הללו לשדות מכיוון שאין דרישה ש-ARP ישתמש ב-Ethernet או ב-IP–הוא יכול לעבוד עם פרוטוקולים אחרים גם.

המשמעות של ה-Payload, עם אורך קבוע של 28 אוקטטים:

- 2 אוקטטים: סוג חומרה (Ethernet הוא 0x0001)
- 2 אוקטטים: סוג פרוטוקול (IPv4 הוא 0x8000)
- 1 אוקטט: אורך כתובת החומרה באוקטטים (Ethernet הוא 0x06)
- 1 אוקטט: אורך כתובת הפרוטוקול באוקטטים (IPv4 הוא 0x04)
- 2 אוקטטים: פעולה (0x01 לבקשה, 0x02 לתגובה)
- 6 אוקטטים: כתובת החומרה של השולח (כתובת MAC של השולח)
- 4 אוקטטים: כתובת הפרוטוקול של השולח (כתובת IP של השולח)
- 6 אוקטטים: כתובת החומרה של היעד (כתובת MAC של היעד)

- 4 אוקטטים: כתובת הפרוטוקול של היעד (כתובת IP של היעד)

21.5 בקשה/תגובה של ARP
זה נעשה קצת מבלבל, כי שדות "השולח" תמיד מוגדרים מנקודת המבט של המחשב ששולח, ולא מנקודת המבט של מי שמבצע את הבקשה.

אז נכריז שמחשב 1 שולח את בקשת ה-ARP, ומחשב 2 יגיב לה.

בבקשת ARP ממחשב 1 ("אם יש לך כתובת IP זו, מהי כתובת ה-MAC שלך?"), השדות הבאים מוגדרים (בנוסף לשאר השדות הסטנדרטיים של בקשת ARP שצוינו למעלה):

- כתובת החומרה של השולח: כתובת MAC של מחשב 1
- כתובת הפרוטוקול של השולח: כתובת IP של מחשב 1
- כתובת החומרה של היעד: לא בשימוש
- כתובת הפרוטוקול של היעד: כתובת ה-IP שמחשב 1 מתעניין בה

בתגובה של ARP ממחשב 2 ("יש לי את כתובת ה-IP הזו, וזו כתובת ה-MAC שלי"), השדות הבאים מוגדרים:

- כתובת החומרה של השולח: כתובת MAC של מחשב 2
- כתובת הפרוטוקול של השולח: כתובת IP של מחשב 2
- כתובת החומרה של היעד: כתובת MAC של מחשב 1
- כתובת הפרוטוקול של היעד: כתובת IP של מחשב 1

כאשר מחשב 1 מקבל את תגובת ה-ARP שמציינת אותו כיעד, הוא יכול להסתכל בשדות "השולח" ולקבל את כתובת ה-MAC ואת כתובת ה-IP המתאימה לה.

לאחר מכן, מחשב 1 יכול לשלוח תעבורת Ethernet לכתובת ה-MAC הידועה כעת של מחשב 2.

וזה איך שמגלים את כתובת ה-MAC עבור כתובת IP מסוימת!

21.6 תכונות נוספות של ARP
21.6.1 הכרזות ARP
לא נדיר שמחשבים שעולים לרשת מייד יכריזו על המידע שלהם ב-ARP ללא בקשה. זה נותן לכל השאר הזדמנות להוסיף את הנתונים למטמוניהם, ולשדרג נתונים ישנים במטמון.

21.6.2 חיפוש ARP
מחשב יכול לשלוח בקשת ARP מיוחדת שמבוססת על "האם מישהו אחר משתמש בכתובת IP זו?"

לרוב הוא שואל באמצעות כתובת ה-IP שלו; אם הוא מקבל תגובה, הוא יודע שיש לו קונפליקט IP.

21.7 IPv6 ו-ARP
ל-IPv6 יש גרסה משלו של ARP שנקראת NDP (פרוטוקול גילוי שכנים).

העין החדה מביניכם אולי שמעה ש-ARP תומך רק בכתובות פרוטוקול (למשל, כתובת IP) של עד 4 בתים, וכתובות IPv6 הן 16 בתים.

NDP פותר את הבעיה הזו ועוד, ומגדיר מספר ICMPv6 (פרוטוקול הודעות אינטרנט עבור IPv6) שניתן להשתמש בהם במקום ARP, בין השאר.

21.8 השתקפות

תארו את הבעיה ש-ARP פותרת.

למה הער entries במטמון ARP חייבות לפוג תוקף?

למה IPv6 לא יכול להשתמש ב-ARP?