Technologic Papers

IP כביש 6

מאת: רועי חורב (AGNil)

הקדמה

הפעם הראשונה שיצא לי להתעסק עם IPv6 היתה כשלמדתי להסמכה של סיסקו. אומנם סיסקו דרשו באותו זמן רק ידע בסיסי לגבי הפרטוקול, והתעסקו יותר בהגדרות הספציפיות של הציודים שלהם - אבל הם בהחלט סיפקו בסיס מספק לנושא. לאחר שחזרתי וביקרתי שוב את הנושא - גיליתי שהרבה מהדברים שלמדתי שונו, ו/או לא היו רלוונטיים יותר. אני מאמין שבגלל שהפרוטוקול חדש (יחסית), ובגלל שהוא אינו בשימוש נרחב עדיין מתבצעים בו שינויים. במאמר הבא ניסיתי לדייק בעובדות, אך תקחו לתשומת ליבכם שיכול להיות שישנם דברים שעלולים להשתנות לפי מצב רוחם של הנוגעים בדבר.

האם אנחנו באמת צריכים את IPv6?

כיום התקשורת באינטרנט ובין רשתות בכלל מושתת על פרוטוקול שנקרא IP (Internet Protocol). רוב התקשורת רצה על גירסא 4 של הפרוטוקול, שקיימת כבר זמן ומגיעה כבר למיצוי היכולת שלה (ותכף נרחיב על כך). בכתבה זו נסקור את גירסתו החדשה יותר של הפרוטוקול - IPv6.

פעמים רבות כאשר מדברים על IPv6, נשאלת השאלה מה קרה בדיוק ל-IPv5 ולמה דילגו עליו? הסיפור על גירסא 5 מחזיר אותנו לשנת 79, בה קבוצה של מהנדסים יצרה את הפרוטוקול Internet Stream Protocol. הפרוטוקול נוצר על מנת להעביר וידיאו, קול ומידע בצורה שוטפת על גבי תשתית האינטרנט. כמה חברות גדולות דוגמת: Sun, IBM ו-Apple נתנו יד למען הפרוטוקול, אך הוא לא באמת נכנס לשימוש. למרות ה"פופולוריות" שלו, הוא קיבל את השם IPv5 - וגרם לכך שהשם יהיה תפוס לדור הבא של הפרוטוקול, ולכן נקרא שמו בישראל (ובשאר העולם) IPv6.

הבעיתיות הגדולה ביותר עם גירסא 4 - היתה בעצם הזרז המרכזי ליצירת גירסא 6: מספר כתובות ה-IP אותם ניתן להקצות לאט לאט נגמרו. כתובת ה-IP כמו שאנו מכירים אותה כיום, מורכבת מארבעה חלקים, כל אחד מהם מורכב מ-8 ביט, מה שנותן לנו בסופו של דבר ארבעה מיליארד, 294 מיליון, 967 אלף ו-296 כתובות. אומנם מדובר במספר גדול ומכובד, אך כמעט כולם בשימוש. בעולם קיימים חמישה ארגונים

שאחראים על חלוקת כתובות ה-IP שנקראים רא"א (רשמי אינטרנט איזורי), או בשמם הלועזי "RIR" - Regional Internet Registry.

ואלו הם:

- AfriNIC - אחראית על יבשת אפריקה.
- ARIN- אחראית על ארה"ב, קנדה, חלק מהאיזור הקריבי ואנטרטיקה.
- APNIC - אחראית על אסיה, אוסטרליה, ניו-זילנד ומדינות שכנות.
- LACNIC - אחראית על אמריקה הלטינית, וחלקים נוספים מהאיזור הקאריבי.
- RIPE - אחראית על אירופה, המזרח התיכון, ומרכז אסיה.

כבר מספר רב של שנים ישנם השערות שכתובות ה-IP הולכות להיגמר, והן אינן נגמרות תודות ל-NAT, ושימוש חסכני יותר של כתובות ה-IP על ידי ספקיות האינטנט

ב-3 בפברואר 2011, בטקס במיאמי, ארגון ה-IANA שאחראי על חלוקת הכתובות לחמשת הארגונים האזוריים, חילק את חמשת הסגמנטים האחרונים (/8) לרא"אים, ובכך סיים את חלוקת כל כתובות ה-IP החדשות שהיו לו במלאי. בכל בלוק כזה יש כ-16.7 מיליון כתובות - אז אין מה לדאוג אם מחר בבוקר אתם עדיין צריכים לקנות כתובת, אך לפי קצב השימוש בכתובות - הכמות הזו אמורה אף היא להיגמר בטווח זמן של שישה חודשים.

הבשורה ש-IPv6 מביא עלינו מבחינת מספר כתובות הוא המספר הבא:

340,282,366,920,938,463,463,374,607,431,768,211,456

אם ניקח את המספר הזה, ונחלק אותו לכל האנשים בעולם, כל איש יקבל בערך 5, ואחריו 28 אפסים, כתובות IP. אנחנו מדברים פה על מספר כתובות גדול מאוד.

ישנם חברות גדולות כמו Microsoft לדוגמא, שבמוצרים החדשים שלה כבר מכריחה להשתמש ב-IPv6, ובעצם נותנת לתעשייה את הבעיטה שהיא צריכה על מנת להתחיל להשתמש בגירסא החדשה. Microsoft ד"א, עשתה את אותו הטריק עם שרתי 64 ביט, כשהוציאה את גירסת server 2008 R2 בגירסת 64 ביט בלבד.

אוקיי השתכנעתי, איך זה עובד?

אז מלבד העובדה שהכתובות החדשות מורכבות מ-128 ביט, לעומת 32 ביט בגירסא הקודמת, ישנם כמה שינויים מהותיים נוספים.

שינוי בשיטות ה"דיבור" - בגירסא 4, היה לנו כמה שיטות דיבור:

- Unicast - מחשב מדבר מול מחשב אחר, פונה ישירות לכתובת שלו (נשאר אותו דבר)
- Broadcast - מחשב מדבר אל כל המחשבים שבסגמנט שלו, בגירסא החדשה, המחשב לא "צועק" אל כל הרשת, אלא שולח את הנתונים לכתובת ספיציפית שנקראת broadcast address, ובכך בעצם מונע הרבה "רעש" על קווי הרשת.
- Multicast - מחשב מדבר אל מספר מחשבים שונים, בגירסא 6 האימפלמנטציה של המנגנון הרבה יותר יעילה ואלגנטית.
  בנוסף, IPv6 מציג לנו שיטה חדש שנקראת
- Anycast - מחשב שולח את הנתונים למחשב אחד מתוך קבוצת מחשבים - מה שיכול לספק יתירות, או ניהול עומסים מובנה.

לעומת זאת, ב-IPv6 שיטות הדיבור הן:

Address Type	IPv6 prefix
Unspecified	::/128
Loopback	::1/128
Multicast	FF00::/8
Link-local unicast	FE80::/10
Unique Local Unicast	FC00::/7
Global Unicast	(everything else)

- Global Unicast - הכתובות הרגילות שאמורות להיות מנוטבות על גבי האינטרנט.
- Link Local Unicast - כתובות שאמורות להיות מנוטבות רק בתוך סגמנט מסוים.
- Unique Local Unicast - כתובות ייחודיות, אך שאינן מנוטבות על גבי האינטרנט.

חלוקת כתובות:

- למרות שב IPv6, ניתן להשתמש בשירות dhcp לחלוקת כתובות בתוך רשתות ביתיות וארגוניות, אין ממש צורך. לכל מחשב שתומך ב-IPv6 ישנו מנגנון שנקרא: Stateless Auto configuration (בעברית - אין מצב הגדרה אוטומטית). המנגנון אומר שהנתב ברשת שולח לתחנה את 64 הביט הראשונים של הכתובת, והתחנה בעצמה מייצרת את ה-64 הביטים הבאים (בדר"ך ע"י שימוש בכתובת ה-mac).

הדבר מתבצע פחות או יותר בצורה הבאה:

- המחשב ממציא לעצמו את הכתובת.
- המחשב מבצע בדיקת duplicate address detection - DAD על מנת לוודא שהכתובת שהמציא היא אכן ייחודית ברשת. הפעולה מתבצעת ע"י שליחת NS והמתנה לתוצאות.
- לאחר מכן המחשב שולח בקשת router solicitation לקבלת כתובת מהנתב.
- ברגע שמגיעה הכתובת מהנתב, המחשב מגדיר לעצמו את הכתובת בצורה טנטטיבית (כנראה שהכתובת תהיה שלי).
- מבצע שוב בדיקות אבהות DAD - על מנת לוודא שהכתובת ייחודית ברשת.
- במידה והכתובת פנויה - המחשב הופך אותה לכתובת המועדפת עליו.

1. Security:

אמנם גם בגירסא 4 היה ניתן לעשות שימוש ב-IPSEC, על מנת לאבטח את התעבורה, אך בגירסא 6 השימוש הוא מנדטורי - מה שאמור לספק נדבח הגנה נוסף לגבי המידע שעובר. סביר מאוד להניח ש"המנדטורי" הזה יעלם מהר מאוד - מכיוון שכבר היום באימפלמנטציות, אנחנו רואים שלא תמיד ישים להתשמש ב-IPSEC. כנראה שלבסוף, זה יהיה בדיוק כמו בגירסא הקודמת, והגירסא החדשה לא תהיה קטליזטור לתעבורה מאובטחת יותר.

2. המבנה של ה-Packets בגירסא 6 בנויים בצורה פשוטה יותר. למרות שהם כמעט כפולים בגודל מגירסא 4, ובעלי גודל קבוע, ה-Header עצמו קטן יותר ופשוט יותר. הרבה שדות שלא נמצאים בשימוש נפוץ הועברו לאיזור נידח יותר ברחבי הפקטה. נתבים של IPv6 לא מבצעים פרגמנטציה של הפקטות (חלוקה לחתיכות קטנות יותר), ואין יותר מנגנון checksum - (שאמור לבדוק את תכולת הפקטה), שהועבר לאחריות שכבה ארבע בלבד (TCP, UDP וכו'). השינויים האלה אמורים להקל על הנתבים להעביר את המידע ולחסוך ב-CPU.

הכתובות עצמן בנויות מ-8 חלקים, שכל אחד מהם בנוי מארבע תווי Hex, שמופרדים בינהם ע"י ":", לדוגמא:

```
2001:db8:31:1:20a:95ff:fef5:246e
```

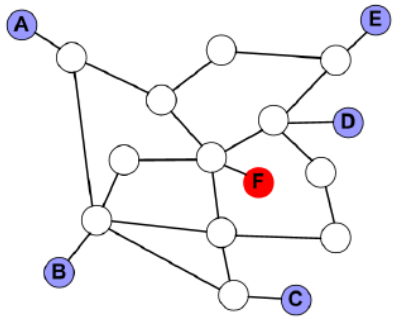
אם יש בתחילת החלק אפסים, ניתן להעלים אותם. אם ישנו חלק גדול המורכב מכמה חלקים של אפסים, ניתן לצמצם גם אותם בצורה הבאה:

```
2001:0db8:0000:0000:020a:95ff:fef5:246e -> 2001:db8::20a:95ff:fef5:246e
```

3. IPv6 מחליף את מנגנון ה-TTL שהיה נהוג בגירסא 4 במנגנון שנקרא Hop Limit, ובעצם סופר את מספר קישורי הרשת שלפקטה מותר לעבור דרך. (מספר הנתבים שהיא עוברת בדרך). המנגנון פותח דלת למספר בעיות, לדוגמא:

   - ניתן לזהות את מערכת ההפעלה על פי ה-Hop Count, לכל מערכת הפעלה יש מספר ברירת מחדל משלו.

   - ניתן לזהות ע"י ה-Hop Count מיקום יחסי של מחשב ברשת - אם אנחנו יודעים מיקום את ה-Hop Count הדיפולטיבי, אנחנו יכולים להסיק באיזה מרחק המחשב המדובר.



Source	Hop Limit
A	61
B	61
C	61
D	62

F is the only node that is:
- 4 "routers" from A
- 4 "routers" from B
- 4 "routers" from C
- 3 "routers" from D

- בנוסף, ניתן לעקוף מערכות IDS\IPS ע"י משלוח פקטות עם Hop Count נמוך מאוד שיגיע רק ל-IPS עצמו, ולא אל התחנה.

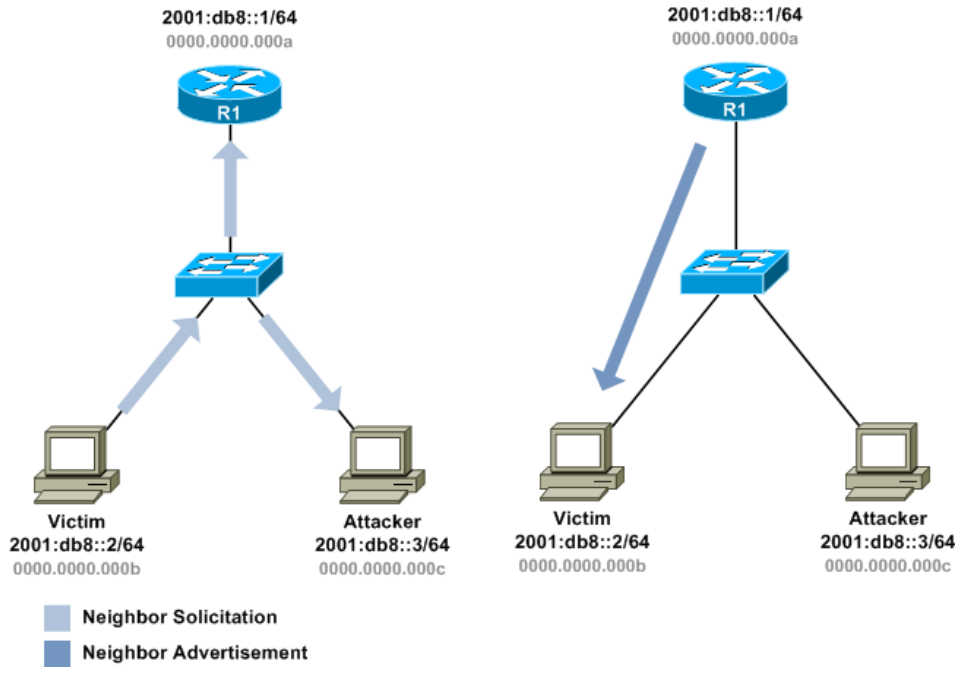
ARP Poisoning Without ARP

בעולם ה-IPv4 ניתן היה לבצע ARP Poisoning על ידי ניצול חוסר מנגנון ההזדהות הקיים בפרוטוקול ה-ARP (קיצור של Address Resolution Protocol), פרוטוקול המשמש לתרגום כתובות IP לכתובות MAC.

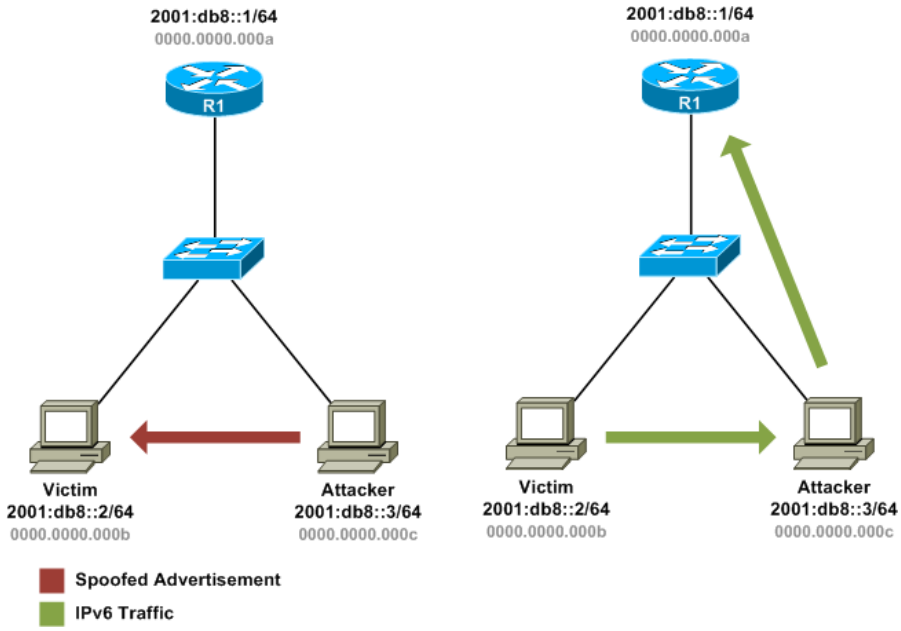
הפרוטוקל הינו פרוטוקול בלתי מאובטח בעליל. ההתקפה הכי נפוצה ופשוטה שהשתמשה בפרוטוקול זה גרמה לתוקף להזדהות בתור ה-Default Gateway של הקורבן, ובכך בעצם כל תעבורת הקורבן עברה דרך התוקף - התקפה הידועה בכינויה Man in the Middle (MitM או בעברית - האיש שבאמצע).

הפרוטוקול ARP כבר אינו בשימוש בגירסא השישית, אך התחליף שלו לא משפר את המצב. הפרוטוקל החדש שנקרא ND - Neighbor Discovery (בעברית - "נוהל שכן"), והוא בונה על פעולות שרצות על ICMPv6 להחלפת פעולות ה-ARP.

החלק שמעניין אותנו מתוך הפרוטוקול הינו החלק בו מחשב אחד צריך לתקשר עם מחשב אחר, ואינו יודע מה הכתובת הפיזית שלו. המחשב המתעניין שולח בקשת Neighbor Solicitation ("פרסום שכן") ב-Multicast, ומחשב היעד שולח Neighbor Advertisement המכיל את הכתובת הפיזית שלו.



בדיוק כמו ב-ARP, אין שום דבר שמונע ממחשבים לבצע "פרסום שכן" שכזה, שמציג את כתובת התוקף כבתור כתובת של מחשבים אחרים בארגון.



בנוסף, אותה בעיה יכולה לעזור להתקפה מסוג אחר, בה התוקף עונה לכל בקשות ה- neighbor solicitation ובכך גורם ל-DOS ברשת.

זו רק דוגמא אחת קטנה, ישנם סכנות הרבה יותר בסיסיות שנובעות מקיומו של IPv6 בשטח.

למשל, הרבה יצרני חומות אש, פשוט מעבירים תעבורת IPv6 עד שהוגדר אחרת. ארגון שעובד IPv4 לחלוטין, יכול להיות לא מודע להגדרה שכזו. והארגון כאשר הוא מתקין שרתים חדשים, לא טורח לבטל את ה-IPv6 על השרת, מכיוון שהוא מופעל כברירת מחדל, ולא מפריע לאף אחד. נובע מכך שבגלל חוסר תשומת לב לקיומו של הפרוטוקול ניתן להגיע לשרת מכל מקום בעולם. מכאן אנחנו מגיעים לבעייה אחרת לגמרי שגוררת אחריה ויכוח ארוך שנים - בין חסידי ה-NAT למתנגדי ה-NAT.

אחד מה"חידושים" שמביא איתו IPv6 הוא כמות ענקית של כתובות שאמורה להעלים את ה-NAT. ארגון ה-IETF (Internet Engineering Task Force) - תמיד טען שה-NAT מונע מהאינטרנט להתפתח וצריך להימנע ממנו. כרגע עם IPv6 זה אפילו אפשרי - אך חשוב לזכור את חומת המגן שה-NAT מספק לארגונים בכך שאי אפשר לגשת מבחוץ לכתובות הפנימיות - אלה אם מוגדר כך מראש. נשמע הזוי שמישהו יוותר על חומת הגנה שכזו - אבל הכל עניין של תפיסה והרגל. בסופו של יום לחומות האש שלנו יש יכולת לחסום תעבורה שכזו.

סיכון נוסף שקיים הוא בפרוטוקלי Tunneling בין IPv6 ל-IPv4 (ISATAP, 6to4, Teredo). אם חומת האש, או ה-IPS, לא יודעים להסתכל על התעבורה שעוברת בתוך ה-Tunnel (כביש המנהרות), אפשר לנצל את הפירצה.

תקופת המעבר עצמה ל-IPv6 תהיה מסוכנת מסיבה נוספת, חברות התקשורת ויצרני אבטחת המידע לא יהיו בשלים מספיק להתמודד עם הפרוטוקול, ויקח זמן מה עד שהם יהיו נקיים יחסית מפגיעויות. פרוטוקולי ה-tunnel רק יסבכו את הסיפור וסיבוכויות תמיד מוסיפה איתה בעיות אבטחה.

סיכום

אני מאמין ש-IPv6 יתחיל לצבור תאוצה משמעותית בשנים הקרובות. שווה להיכנס ולהכיר אותו לפני שצריך ל"תפעל" אותו. כמו שכבר ציינתי - מייקרוסופט, ולהערכתי גם יצרנים נוספים בעתיד, יתנו לתעשייה את הבעיטה בעכוז שהיא צריכה על מנת לדחוף את הפוטוקול קדימה לשימוש המונים.

מקורות

http://www.files.dc9723.org/mh-Recent%20advances%20in%20IPv6%20insecurities-TelAviv.pdf

http://www.internetblog.org.uk/post/1168/the-forgotten-tale-of-ipv5/

http://en.wikipedia.org/wiki/Regional_Internet_Registry

http://en.wikipedia.org/wiki/IPv4

http://en.wikipedia.org/wiki/IPv6

http://en.wikipedia.org/wiki/Anycast

http://arstechnica.com/hardware/news/2007/03/IPv6.ars/2

http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/

http://www.networkworld.com/news/2009/071309-ipv6-network-threat.html?page=2

http://ipv6.com/articles/nat/NAT-In-Depth.htm

http://www.betanews.com/article/Shields-down-IPv6-is-not-ready-for-attack/1307461641

http://www.gont.com.ar/talks/hip2011/fgont-hip2011-hacking-ipv6-networks.pdf