

18.1 מבוא לניתוב

המידע שנע ב-IP צריך להגיע אל היעד שלה (מחשב אחר, שרת, נתב, או כל התקן אחר). כל חבילה שברצוננו לשלוח לא עוצרת במחשב היעד ברגע שהיא יוצאת ממחשב השולח. בדרך ישנם נתבים שונים שמקבלים את החבילה ומעבירים אותה על פי הדרך הטובה ביותר.

הנתב הראשון בשרשרת בדרך כלל יקרא "הנתב ברירת המחדל". הוא זה שיקבע את הדרך אל היעד אם אין לו נתיב ישיר לכתובת ה-IP של היעד.

הדברים שקובעים איך להעביר את החבילה בדרך נלמדים באמצעות אלגוריתמים שמחשבים את הנתיב שהחבילה צריכה לנוע בו. הראוטר מקבל את החבילה ומעביר אותה הלאה בהתאם לשיקוליו.

18.2 טבלאות ניתוב

טבלת ניתוב היא הגדרה של היכן להעביר חבילות על מנת לדחוף אותן לעבר היעד שלהן. או, אם הראוטר נמצא ב-LAN של היעד, טבלת הניתוב מכוונת את הראוטר לשלוח את התעבורה המקומית בשכבת הפיזי (למשל, Ethernet).

מטרת הפרוטוקולים של ניתוב שדיברנו עליהם קודם היא לעזור לראוטרים ברחבי האינטרנט לבנות את טבלאות הניתוב שלהם.

כל מחשב שמחובר לאינטרנט - ראוטרים ושאר מחשבים - יש לו טבלת ניתוב. אפילו על המחשב הנייד שלך, מערכת ההפעלה צריכה לדעת מה לעשות עם כתובות יעד שונות. מה אם היעד הוא localhost? מה אם זה מחשב אחר באותה תת-רשת? מה אם זה משהו אחר?

אם נסתכל על מחשב נייד טיפוסי כדוגמה, מערכת ההפעלה שומרת את התעבורה של localhost בממשק ה-loopback והיא לא יוצאת בכלל לרשת. מבחינתנו כמתכנתי תוכנה, זה נראה כמו פעילות ברשת, אך מערכת ההפעלה יודעת לנתב את התעבורה לכתובת 127.0.0.1 בתוך המערכת.

אבל מה קורה אם אתה שולח פינג למחשב אחר באותה LAN כמוך? במקרה כזה, מערכת ההפעלה בודקת את טבלת הניתוב, מזהה שזה נמצא באותה LAN, ושולחת את החבילה ב-Ethernet ליעד.

אבל מה קורה אם אתה שולח פינג למחשב אחר שנמצא ב-LAN שונה לחלוטין? במקרה כזה, מערכת ההפעלה לא יכולה פשוט לשלוח את החבילה כ-Ethernet frame ולצפות שהיא תגיע ליעד. היעד לא נמצא באותה רשת Ethernet! אז המחשב שלך מעביר את החבילה לנתב ברירת המחדל, הראוטר של "ההזדמנות האחרונה". אם למחשב שלך אין ערך בטבלת הניתוב ליעד הסאב-רשת הזה, הוא שולח את החבילה לנתב ברירת המחדל, שימשיך לשלוח אותה לאינטרנט הרחב.

להלן דוגמת טבלת ניתוב ממחשב הלינוקס שלי, שבמקרה זה הוקצתה לו כתובת 192.168.1.230:

Device	Gateway	Destination	Source
lo	127.0.0.1	127.0.0.1	1

lo	127.0.0.0/8	127.0.0.1	2
lo	127.255.255.255 5	127.0.0.1	3
wlan0	192.168.1.230	192.168.1.230 0	4
wlan0	192.168.1.0/24	192.168.1.230 0	5
wlan0	192.168.1.255	192.168.1.230 0	6
192.168.1. 1	default	192.168.1.230 0	7

בואו נסתכל על החיבור מ-localhost ל-localhost (127.0.0.1). במקרה זה, מערכת ההפעלה בודקת איזה נתיב מתאים ושולחת את המידע על הממשק המתאים. במקרה זה, מדובר בממשק ה-lo (loopback), ממשק "פיקטיבי" שמערכת ההפעלה מציינת כ"ממשק רשת" (לצרכי ביצועים).

אך מה קורה אם אנחנו שולחים נתונים מ-127.0.0.1 לכל כתובת בתוך תת-הרשת 127.0.0.0/8? היא משתמשת גם בממשק lo. אותו הדבר קורה אם אנו שולחים נתונים לכתובת השידור 127.255.255.255 (בתוך תת-הרשת 127.0.0.0/8).

הערכים האחרים מעניינים יותר. זכור שכאשר אנחנו בודקים את המחשב שלי, הוא הוקצה כתובת 192.168.1.230.

אם נסתכל על שורה 4, אנו רואים את המקרה שבו אני שולח מהמחשב שלי אל עצמו. זה כמו localhost, אך אני משתמש בכוונה בכתובת ה-IP שנמצאת במכשיר ה-WLAN שלי, wlan0. מערכת ההפעלה תשתמש בממשק הזה, אך תדע לא לשלוח את המידע דרך החוטים - אחרי הכל, זה היעד.

לאחר מכן, אנחנו רואים את המקרה שבו אנחנו שולחים לכל מחשב אחר בתת-הרשת 192.168.1.0/24. כלומר, כמו אם הייתי שולח מהמחשב שלי בכתובת 192.168.1.230 למחשב אחר, לדוגמה 192.168.1.22.

18.3 אלגוריתם ניתוב

נניח שהפרוטוקולים של הניתוב עשו את העבודה שלהם וכולל את כל המידע שדרוש לראוטרם כדי לדעת לאן לשלוח את החבילות בדרך.

כאשר החבילה מגיעה, הראוטר עוקב אחר סדרת שלבים כדי להחליט מה לעשות בה לאחר מכן. (בדיון הזה נניח שלא מתייחסים לממשק ה-loopback ומניחים שכל התעבורה היא על רשת אמיתית).

אלגוריתם ניתוב IP אם כתובת ה-IP של היעד נמצאת ברשת המקומית המחוברת לראוטר: שלח את החבילה דרך הקישור (שכבת פיזית, לדוג' Ethernet) אם יש רשומה בטבלת הניתוב עבור רשת כתובת ה-IP של היעד: שלח לראוטר הבא לעבר היעד אם קיימת ברירת מחדל: שלח לראוטר ברירת המחדל אחרת: השלך את החבילה שלח הודעת שגיאה "ICMP Destination Unreachable" חזרה לשולח אם יש מספר נתיבים תואמים, בחר את הנתיב עם מסיכת תת-הרשת הארוכה ביותר.

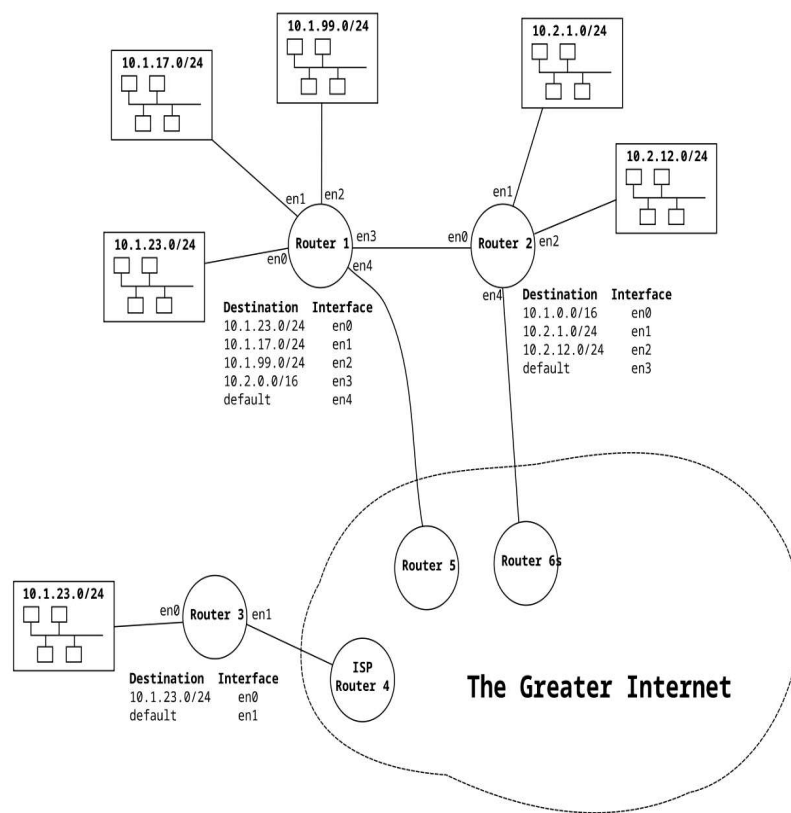
אם יש עוד קשרים, השתמש באלגוריתם ECMP (Equal Cost Multi-Path) - שלח את החבילה דרך שני הנתיבים.

18.4 דוגמת ניתוב

בואו נריץ כמה דוגמאות. אפשר להוריד PDF של הדיאגרמה הזו כדי לראות את זה בצורה ברורה יותר.

בדיאגרמה הזאת יש הרבה דברים חסרים. במיוחד שכל ממשק ראוטר מחובר ל-IP.

כמו כן, ראו שראוטר 1 מחובר ישירות ל-3 תתי-רשתות ויש לו כתובת IP על כל אחד מהם.



18.5 לולאות ניתוב ו-Time-To-Live

זה אמור להיות ברור שזה אפשרי להקים לולאה שבה חבילה נוסעת במעגל לנצח.

כדי לפתור את הבעיה הזאת, ל-IP יש שדה בכותרת שלה שנקרא TTL (time to live). זהו סופר בייט אחד שמתחיל מ-255 ומפחית כל פעם שראוטר מעביר חבילה.

כאשר הסופר מגיע לאפס, החבילה נמחקת והודעת שגיאה "ICMP Time Exceeded" נשלחת חזרה לשולח.

אז החבילה יכולה להסתובב עד 255 "קפיצות", אפילו בלולאה.

הפונקציה traceroute פועלת על ידי שליחת חבילה ליעד עם TTL של 1 וראיית מי מחזיר את הודעת ה-ICMP. לאחר מכן, היא שולחת חבילה נוספת עם TTL של 2 ורואה מי מגיב. היא ממשיכה להגדיל את ה-TTL בכל חבילה חדשה עד שהיעד הסופי מגיב.

18.6 כתובת השידור

יש כתובת מיוחדת ב-IPv4 שנקראת כתובת שידור. זו כתובת ששולחת חבילה לכל מחשב ב-LAN.

זוהי כתובת בתת-רשת עם כל ביטי המחשב מוגדרים ל-1.

לדוגמה:

Broadcast Address	Subnet Mask	Subnet
10.20.30.255	255.255.255.0	10.20.30.0/24
10.20.255.255	255.255.0.0	10.20.0.0/16
10.255.255.255	255.0.0.0	10.0.0.0/8

יש גם את כתובת השידור 255.255.255.255. זו הולכת לכולם...

...ואני מתכוון לכולם ב-LAN. אף חבילות שידור אלה לא עוברות מעבר לנתב, אפילו לא 255.255.255.255. הנתבים לא מעבירים אותן לשום מקום.

העולם היה מקום רועש מאוד אם הם היו מעבירים אותן.

אחת מהשימושים העיקריים לזה היא כשאתה פותח את המחשב הנייד שלך ב-WiFi. המחשב לא יודע את ה-IP שלו, את מסכת תת-הרשת, את נתב ברירת המחדל או אפילו את מי לשאול. אז הוא שולח חבילת שידור ל-255.255.255.255 עם בקשת DHCP שיבקש את המידע הזה. שרת DHCP מאזין ויכול לשלוח חזרה את המידע.

18.7 חשיבה מחדש

מה ההבדל בין פרוטוקול שער פנימי (Interior Gateway Protocol) ופרוטוקול שער חיצוני (Exterior Gateway Protocol)?

מה מטרת פרוטוקול ניתוב באופן כללי?

מהו דוגמה למקום שבו ייעשה שימוש בפרוטוקול שער פנימי? וחיצוני?

מה עושה הראוטר עם טבלת הניתוב כדי לקבוע?

מה עושה ניתוב IP לאחר מכן עם חבילה אם כתובת ה-IP של היעד אינה על אחת מתתי-ההרשת המקומיות שלה?

למה תהליך ישלח משהו לכתובת השידור?