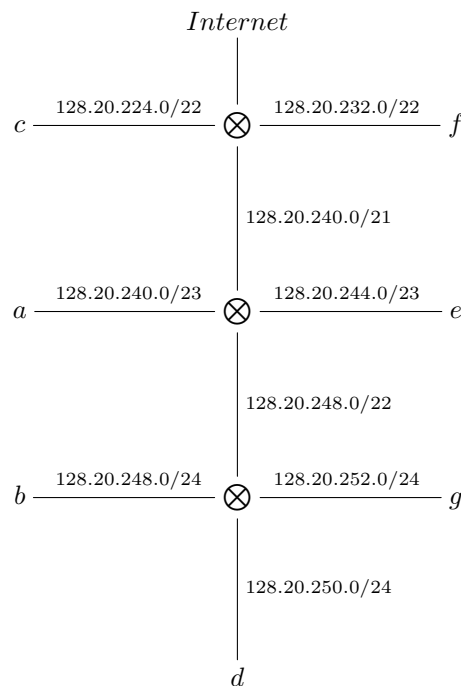


תרגיל

לספק ניתנו כתובות IP 128.20.224.0/20. יש להקצות ל7 לקוחות:

<i>a</i>		500
<i>b</i>		250
<i>c</i>		1000
<i>d</i>		250
<i>e</i>		500
<i>f</i>		1000
<i>g</i>		250

עם מספק מינימלי של נתבים, לכל נתב 4 ממשקים.



Wireshark

Wireshark היא תוכנה שמאפשרת להאזין לחבילות. היא מאפשרת להציג רשימה של כל חבילה שנשלחת מכרטיס הרשת או מתקבלת דרכו. דרך התוכנה הזו ניתן לראות שרשת Wireless מתפקדת כHub - כולם משדרים לכולם, וכל אחד יכול לקלוט לכל מה שהאחרים משדרים. זה אומר גם שאפשר לראות סיסמאות שאחרים שולחים כדי להתחבר לאתרי אינטרנט - אלא אם כן הם שולחים אותם בצורה מוצפנת(למשל https).

DHCP

אפשר לראות שם גם את החבילות שנשלחות לשרת ה-DHCP - כלומר בקשות לקבלת כתובת IP. החבילות האלו נשלחות לכתובת IP 255.255.255.255 - כלומר Broadcast - שזה אומר לשלוח לכל הרשת. אמנם כל המחשבים רואים את כל החבילות, אבל מחשבים בד"כ מתעלמים מחבילות שלא מיועדות אליהם.

חבילת DHCP היא תמיד באותו מבנה. ההודעה הראשונה היא Discover - מחשב הלקוח מחפש את שרת ה-DHCP. מחשב ששולח Discover שולח IP 0.0.0.0 - כי עדיין אין לו כתובת IP. לכן הוא גם שולח את כתובת ה-MAC שלו, כדי שיהיה אפשר להבחין בין מחשבים חדשים שונים הרוצים להתחבר לרשת. השרת שולח בחזרה Offer, ואז המחשב שולח לו Request כדי לבקש כתובת IP. השרת שולח Ack וכו'.

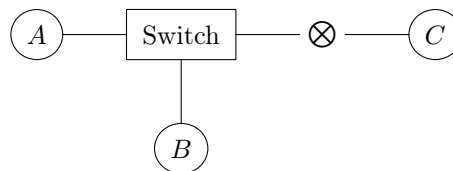
Address Resolution Protocol(ARP)

מטרה: תרגום בין כתובות פיזיות לכתובות IP.

בשביל לשלוח באותה רשת, מחשבים צריכים לדעת מה הכתובת הפיסית של מחשב היעד. לכן נרצה לתרגם בין כתובות MAC לכתובת IP. ב-ARP שולחים את כתובת ה-MAC ואת כתובת ה-IP שלי, ואת כתובת ה-MAC של המחשב המבוקש. אם לא יודעים את כתובת ה-MAC של המחשב המבוקש - אז שולחים MAC 00 : 00 : 00 : 00 : 00 : 00, ואם לא יודעים את כתובת ה-IP שולחים IP 0.0.0.0. המחשב שמתאים לכתובת שנשלחה שולח בחזרה את התשובה.

דוגמה

יש לנו רשת:



הנתונים של מחשב A הם

Device	MAC Address	IP	Network Address
A	AA:AA:AA:AA:AA:AA	1.2.3.4	1.2.3.16/28

$\text{AND} \begin{cases} 00010000 \\ 11111100 \end{cases} = 00010000 = 16$ היא כתובת הרשת! כי כתובת הרשת היא 16

ואילו כתובת הרשת של A היא 4 $\text{AND} \begin{cases} 00000100 \\ 11111100 \end{cases} = 00000100 = 4$. כדי שהמחשב יהיה ברשת, צריך או לשנות את כתובת המחשב או להקטין את ה-Subnet Mask - למשל

ל24, ואז $\text{AND} \left\{ \begin{array}{l} 00010000 \\ 11000000 \end{array} \right\} = 0 = \text{AND} \left\{ \begin{array}{l} 00000100 \\ 11000000 \end{array} \right\}$. נבחר את האופציה השנייה, וניתן כתובות גם לשאר המכשירים:

Device	MAC Address	IP	Network Address
A	AA:AA:AA:AA:AA:AA	1.2.3.4	1.2.3.0/24
B	BB:BB:BB:BB:BB:BB	1.2.3.16	1.2.3.0/24
⊗(With A and B)	DD:DD:DD:DD:DD:DD	1.2.3.1	
⊗(With C)	DD:DD:DD:DD:DD:DD	7.6.128.33	
C	CC:CC:CC:CC:CC:CC	7.6.128.35	7.6.128.32/30

מה קורה כאשר מחשב A רוצה לשלוח חבילה לC? בעזרת בדיקת Subnet Mask מגלים שכתובת הIP של C לא ברשת של A. לכן A מחפש את Gateway - כלומר את הנתב. הוא יודע את כתובת הIP של הנתב, אבל הוא צריך לדעת מה הכתובות הפיסיות שלו, ולכן הוא שולח חבילת ARP Broadcast כדי למצוא את הנתב הפיסית של 1.2.3.1 - זה בכלל לא קשור לC! אבל צריך לעבור דרך Gateway בשביל להגיע לC. הבקשה מגיעה לכל המכשירים ברשת(כלומר A, B, הSwitch והנתב) אבל רק הנתב מחזיר לו תשובה: DD : DD : DD : DD : DD : DD. לכן A שולח ל⊗ חבילה שמיועדת לC. ⊕ בודק אם החבילה איתו ברשת - את הבדיקה הוא מבצע לפי כרטיס הרשת שקיבל את החבילה, כלומר זה שמחובר לרשת 1.2.3.0/24. הוא רואה שהיא לא שם, ולכן הוא בודק בכרטיסי הרשת האחרים שלו לאן לשלוח.

מה קורה אם יש הבדלים בSubnet Mask?

אם מחשב ונתב משתמשים בSubnet Mask אחר, אז יכולות להיות בעיות. אם A חושב שC איתו ברשת ו⊗ חושב שלא, יכולות להיזרק חבילות - כי A ינסה למצוא את כתובת הMAC של C באמצעות ARP ולא יצליח. אם A חושב שC לא איתו ברשת, ו⊗ חושב שכן, אז ⊗ ישלח את החבילה למקום הנכון - אבל זה בזבוז של זמן, כי A היה יכול לשלוח ישירות לC.