digital whisper
Technologic Papers

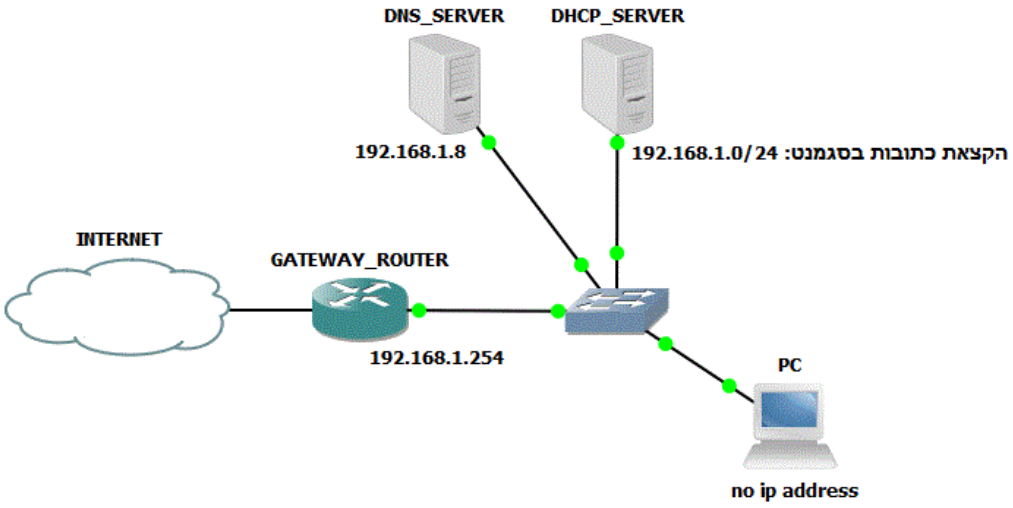
על סוגיות אבטחה ב-DHCP

מאת תומי שלו (פורסם במקור באתר: http://pelegit.co.il, קהילת IT, מחשבים, סיסטם ורשתות)

הקדמה

מנגנון DHCP - Dynamic Host Configuration Protocol הינו מנגנון דינאמי להקצאת פרמטרי רשת שונים בציודי קצה / רשת. פרוטוקול זה מייעל ומפשט תהליכי הקצאת משאבי IP ברשת ונוח מאוד לשימוש והגדרה, יחד עם זאת הוא טומן בחובו פירצות אבטחה ב-L3.

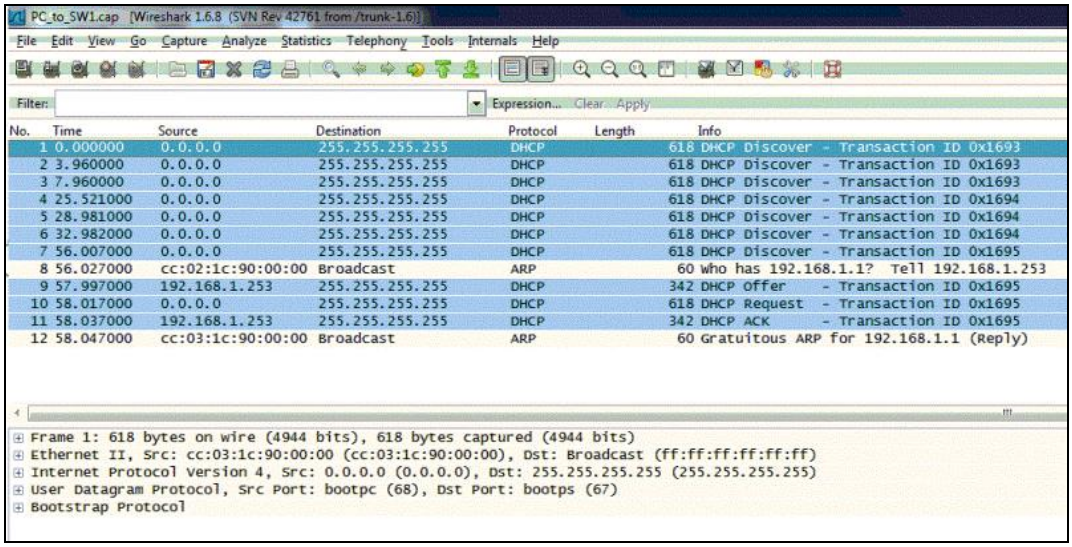
לרוב, שרתים ישמשו כספקי DHCP אך ניתן להגדיר גם ציודי רשת כגון נתבים ומתגים כשרתי DHCP בתהליך הגדרה פשוט. החיסרון העיקרי בהגדרת ציודי רשת כשרתי DHCP הוא חוסר היכולת שלהם להסתנכרן ולעבוד במקביל עם ציוד DHCP נוסף. תצורת רשת פשוטה בה קיימים שרת DHCP, שרת DNS, נתב GW ולקוח DHCP פוטנציאלי תראה כך:



המו"מ שמבצע שרת DHCP אל מול לקוח פוטנציאלי מתרחש ב-4 שלבים עיקריים, כאשר ה"שיחה" בין הלקוח לשרת מתבצעת ב-UDP בפורטים 67 ו-68.

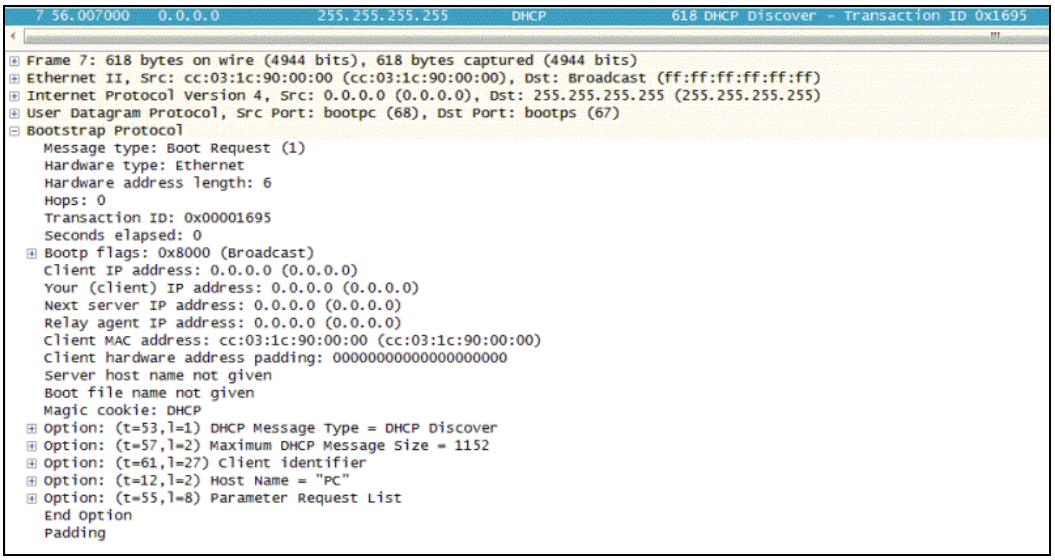
DHCP Handshake

לטובת הבנת תהליך הקצאת הפרמטרים של DHCP נכיר קודם כל את ההודעות הנשלחות במסגרת תהליך ההקצאה, ואלו הן: DHCP DISCOVER, DHCP REQUEST, DHCP OFFER ו-DHCP ACK לדוגמא:



[תהליך המו"מ כפי שנלכד בתוכנת הסניפר WireShark]

שלב 1: לקוח DHCP פוטנציאלי שהוגדר בתצורת DHCP שולח הודעת Discover כהודעת BC(broadcast) בשדות ה-Destination של המסגרת והחבילה (L3+L2). בשדות ה-Source יצויינו כתובת ה-MAC של הלקוח וכתובת IP שהיא 0.0.0.0. כל זאת בתקווה שקיים שרת / ספק DHCP שיאזין להודעתו ויקצה לו את הפרמטרים שביקש.



[בהודעה ניתן לראות את שדה Parameter request list שבו מציין הלקוח את רשימת הפרמטרים שהוא מבקש שהשרת יקצה לו]

שלב 2: שרת DHCP שמקבל את הודעת ה-Discover מלקוח פונטציאלי רוצה כעת "להציע" ללקוח כתובת IP אפשרית, לפני שהוא ישלח לו את ההצעה הוא קודם כל מוודא שב-DB שלו לא קיימת הקצאה של הכתובת, לאחר מכן הוא מבצע בדיקת ARP ע"י שליחה של הודעת ARP request על מנת לוודא כי לא קיים בסגמנט ציוד שהוגדר סטטית עם אותה כתובת ה-IP.

במצב שבו התקבל מענה להודעת ה-request יישלח ICMP echo לווידוא מוחלט - ואם יתקבל מענה גם ל-echo יווצר מצב שנקרא DHCP conflict, כלומר קיימת כתובת מתוך המאגר הפוטנציאלי של השרת שלא הוא הקצה ולא ניתן להקצות אותה זמנית (בתצורות שבהן קיים שרת DHCP מרכזי בליבת הרשת, הוא משתמש ב"סוכנים" שמבצעים עבורו את הבדיקות הללו).

לאחר סט הבדיקות שולח השרת הודעת OFFER כ-BC ב-L2&L3 destination כאשר בשדות ה-SRC הוא מציין את כתובות ה-MAC וה-IP שלו. ההודעה מכילה הצעה עבור כלל הפרמטרים שהלקוח ביקש, בין היתר subnet mask, כתובת IP, כתובת DNS, כתובת GW, זמן השכרה.

```
9 57.997000   192.168.1.253   255.255.255.255   DHCP   342 DHCP Offer   - Transaction ID 0x1695

⊞ Frame 9: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: cc:02:1c:90:00:00 (cc:02:1c:90:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.253 (192.168.1.253), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00001695
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.1 (192.168.1.1)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: cc:03:1c:90:00:00 (cc:03:1c:90:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.253
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  ⊞ Option: (t=58,l=4) Renewal Time Value = 5 minutes
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 8 minutes, 45 seconds
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.8
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
    End Option
    Padding
```

שלב 3: הלקוח שקיבל את הודעת ה-OFFER צריך להגיע כעת להחלטה האם הוא מסכים לקבל את ההצעה מהשרת, אם הוא לא מסכים (למשל מהסיבה שיש לו רשומת ARP שאומרת שכתובת ה-IP שהוצעה לו שייכת בכלל לציוד אחר) הוא ישלח הודעת DECLINE. אם הוא מסכים, הוא ישלח הודעת REQUEST שמהווה בקשה "רשמית" להחיל על עצמו את הפרמטרים שהשרת הציע לו.

הודעה זו מכילה בעצם שדה שמציין מי הוא שרת ה-DHCP, מה הכתובת שהוצעה לו, כתובת ה-MAC של הלקוח (אין קשר ל-MAC במסגרת משום שברשתות גדולות משתמשים בסוכנים המעבירים את ההודעות לשרתי ה-DHCP, לכן מצויין ה-MAC של הלקוח בהודעה עצמה) והזמן לשכירת הפרמטרים (lease time).

```
10 58.017000   0.0.0.0          255.255.255.255      DHCP          618 DHCP Request  - Transaction ID 0x1695

⊞ Frame 10: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits)
⊞ Ethernet II, Src: cc:03:1c:90:00:00 (cc:03:1c:90:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00001695
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: cc:03:1c:90:00:00 (cc:03:1c:90:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ⊞ Option: (t=57,l=2) Maximum DHCP Message Size = 1152
  ⊞ Option: (t=61,l=27) Client identifier
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.253
  ⊞ Option: (t=50,l=4) Requested IP Address = 192.168.1.1
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  ⊞ Option: (t=12,l=2) Host Name = "PC"
  ⊞ Option: (t=55,l=8) Parameter Request List
    End Option
    Padding
```

שלב 4: זהו השלב האחרון בתהליך ההקצאה שבו בעצם שרת ה-DHCP משכיר באופן רשמי את הפרמטרים ללקוח. השרת שולח ב-BC הודעת ACKNOWLEDGE שבה מצויינים כלל הפרמטרים הרלוונטיים שמוקצים ללקוח. שימו לב שהודעה זו זהה לחלוטין להודעת ה-OFFER ואפילו גודל המסגרות הוא זהה (במקרה שלנו bytes324). בסוף תהליך זה ולאחר שהלקוח קיבל את הודעת ה-ACK (בעצם החיל על עצמו את הפרמטרים), הוא שולח הודעת Gratuitous ARP שבה הוא מצהיר על עצמו עם כתובת ה-IP החדשה שהוא קיבל.

הערה: לא כל ציוד שולח הודעת ARP בסוף התהליך.

```
11 58.037000   192.168.1.253   255.255.255.255   DHCP   342 DHCP ACK   - Transaction ID 0x1695

⊞ Frame 11: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: cc:02:1c:90:00:00 (cc:02:1c:90:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.253 (192.168.1.253), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00001695
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.1 (192.168.1.1)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: cc:03:1c:90:00:00 (cc:03:1c:90:00:00)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.253
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
  ⊞ Option: (t=58,l=4) Renewal Time Value = 5 minutes
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 8 minutes, 45 seconds
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.8
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
    End Option
    Padding
```

סוכני DHCP

ברוב הרשתות הגדולות מוצבים מס' שרתי DHCP בליבת הרשת, מצב שבעצם מונע גישה מלקוחות פוטנציאליים אל השרתים משום שהודעות ה-BC שהם שולחים מוגבלות ל-BC DOMAIN של הסמגנט שבו הם יושבים (הלקוחות), ידוע שבאופן רגיל ציוד L3 לא מעביר הודעות BC לרגליים אחרות. הפתרון לכך הוא קיום של "סוכני" DHCP שאחראים להעביר הודעות בין לקוח לשרת, לרוב סוכנים אלו יהיו נתבים, מתגי L3 או Firewalls הנמצאים ברשת.

ניתן להשתמש בסוכנים בכמה אופנים כשהעיקרי שבהם הוא שימוש ב-IP HELPER בסגמנט הרלוונטי. הסוכן בעצם לוקח את הודעת ה-BC שאותה הוא "שמע" מהלקוח ושולח אותה ישירות לכתובת שרת ה-DHCP כשהוא משכתב את ההודעות ומציין בשדה ייעודי שהוא (הסוכן) באותו הסמגנט, ע"פ כתובתו של הסוכן יוכל לדעת שרת ה-DHCP אילו פרמטרים להקצות ובאיזה טווח כתובות להשתמש.

לדוגמא: לפי סוכן שכתובתו היא 10.0.0.1/24 יידע שרת ה-DHCP שכתובתו היא 172.16.1.1 להקצות פרמטרים לפי הסגמנט 10.0.0.0/24.

בואו ונחשוב כעת, מה קורה אם גורם עויין מחבר לרשת ספק כתובות IP משלו ("Rogue DHCP") שמקצה ללקוחות את אותם הפרמטרים בדיוק מלבד כתובת ה-GW שתהיה בעצם הממשק שלו בסגמנט, החבילות מאותם הלקוחות יגיעו אליו, הוא ישמור עותק שלהן ויעביר אותן בשלמותן ל-GW האמיתי בסגמנט מבלי שאף אחד ירגיש.

המקרה שתיארתי הוא סוג של מתקפת MAN-IN-THE-MIDDLE שעשויה להתרחש במרחב ה-LAN של כל סגמנט וניתן לממש אותה לדוגמא גם באמצעות התערבות בתהליכי מנגנון ה-ARP. קיימות מספר דרכים אשר נועדו למנוע סוג כזה של מתקפה, אך אני ארחיב על איך ניתן למנוע מתקפה שכזו כמנהלי רשת, במתגי Cisco שאחראיים על תעבורת ה-L2 בעזרת מנגנון בשם DHCP Snooping.

DHCP Snooping הוא מנגנון פשוט שניתן להפעיל בחלק מהמתגים ועיקרו הוא קביעת "אזורים" בטוחים ו"אזורים" שאינם בטוחים במתג. כשאני מדבר על אזור אני מתכוון לפורט/ממשק L2 שעשויות להתקבל בו הודעות DHCP מספק/ספקים הקיימים ברשת.

מה שעושה מנגנון DHCP Snooping הוא בעצם חלוקה של הפורטים במתג ל-2 סוגים: Trusted ports ו-Untrusted ports, כאשר ספקי ה-DHCP יחוברו לפורטים האמינים ושאר העמדות/שרתים ב-LAN יחוברו לפורטים שאינם אמינים.

רק בפורטים אמינים אפשר שיתקבלו הודעות DHCP Reply מהסוגים השונים שמקורן בשרת/ספק DHCP כלשהו. ומה יקרה אם בפורט לא אמין יתקבלו הודעות שכאלו? פשוט מאוד, הפורט ייכנס אוטומטית למצב Error-disable שלא מאפשר שליחה וקבלת מידע נוספת בפורט לאורך זמן מסויים שהוגדר מראש או עד שיבוצע Shut ומיד לאחר מכן No-shut ע"י מנהל הרשת.

התגובה של המנגנון מונעת מגורם זדוני להתחזות לספק ה-DHCP ברשת ה-LAN ובעצם מדליקה נורה אדומה עבור מנהל הרשת על מנת שיתבצע תחקור לאירוע.

ומה קורה אם השרת נמצא הרחק מהמתג? פשוט וקל! נצטרך להפעיל קצת את הראש ולחזות מהיכן עשויות להגיע הודעות התגובה משרת ה-DHCP שלנו, אם המתג מחובר בתצורה שרידה או מקושר לאזור ה-L3 אז אפשרי שההודעות יגיעו מכל פורט שמקשר אותנו לציוד אחר (נתב, מתג, FW) ולכן את הפורטים הללו נגדיר כ-Trusted ואת השאר כ-Untrusted.

ואם למתג מתחבר מתג נוסף בתצורת זנב (כלומר אנחנו הגישה של המתג הנוסף אל הרשת) אז כמובן שלא נצפה לקבל בממשק שבינינו הודעות שמקורן בספק DHCP ולכן נגדיר את הממשק כ-Untrusted במתג המקומי וכ-Trusted במתג הזנב.

בנוסף לחלוקת המתג לאזורים, מנגון זה משתמש באמצעי אבטחה נוסף שנקרא "DHCP OPTION 82", כדי לוודא שהודעות ה-DHCP שמתקבלות מהשרת אכן עברו לפני כן דרך המתג כבקשות סטנדרטיות.

איך זה פועל? להודעות DHCP שמתקבלות מלקוח (כלומר מפורטים שהוגדרו כ-Untrusted), מוסיף המתג מידע כמו כתובת ה-MAC של הממשק וערך PORT-ID של הממשק וכאשר שרת ישיב להודעות אלו הוא יציין בהן את הערכים המקוריים, כך שהמתג יוכל לדעת שהודעות התשובה שהתקבלו הן עבור בקשות שאכן עברו במתג (לשם כך צריך שהשרת יתמוך ביישום).

לידע כללי, OPTION 82 קיים לשימושים נוספים מלבד זה שציינתי, לדוגמא ניתן להשתמש בשדה זה יחד עם הגדרות נוספות בסוכן ובספק (כאשר עובדים בתצורה כזו) כדי שהסוכן יבקש מהשרת להקצות כתובות בטווח מסויים מה-POOL הכללי. מי שיתעניין בכך יהנה מכמה שזה מגניב למרות שמדובר בחקירה עד רמת הביט ומימוש מעט מסובך, כמו גם שיש שוני במימוש בין חברות התקשורת השונות.

ונעבור לפקודות:

- אפשור כללי של המנגנון במתג:

```
config-if# ip dhcp Snooping
```

- אפשור המנגנון ב-Vlan-ים מסוימים:

```
config-if#ip dhcp Snooping vlan [1,2,3]
```

(הערה: ברגע שמגדירים את אחת מהפקודות הללו, אוטומטית כל הממשקים הרלוונטיים יתפקדו כ"בלתי אמינים".)

- הגדרת ממשק כ"אמין":

```
config-if#ip dhcp Snooping trust
```

לקוח עויין

עד כה דיברנו על סוגיה שבה מתחברת לרשת, "שרת DHCP עויין", כעת נעבור לסוגיה נוספת (ואחרונה) שאדבר עליה, שנקראת "לקוח עויין".

מהו לקוח עויין? לקוח עויין יכול להיות כל ציוד שברגע שמקושר לרשת שלנו יוכל בעצם לגשת למירב המשאבים בדרך כזו או אחרת, או שיכול להפיץ וירוס או תוכנה זדונית אחרת שתטייל לנו ברחבי הרשת ותגיע לכל חלקיה. ל"לקוח" שכזה שמקבל אוטומטית וללא כל מאמץ גישה לרשת בעזרתו של שרת ה-DHCP האדיב יש פוטנציאל נפיץ ביותר, לכן מומלץ לתכנן מראש את הרשת כך שאם כבר נשתמש בשרת / ספק DHCP, נוודא שרק מורשי גישה יוכלו להתחבר לרשת ואם כבר התחברו מן הסתם שיכולותיהם

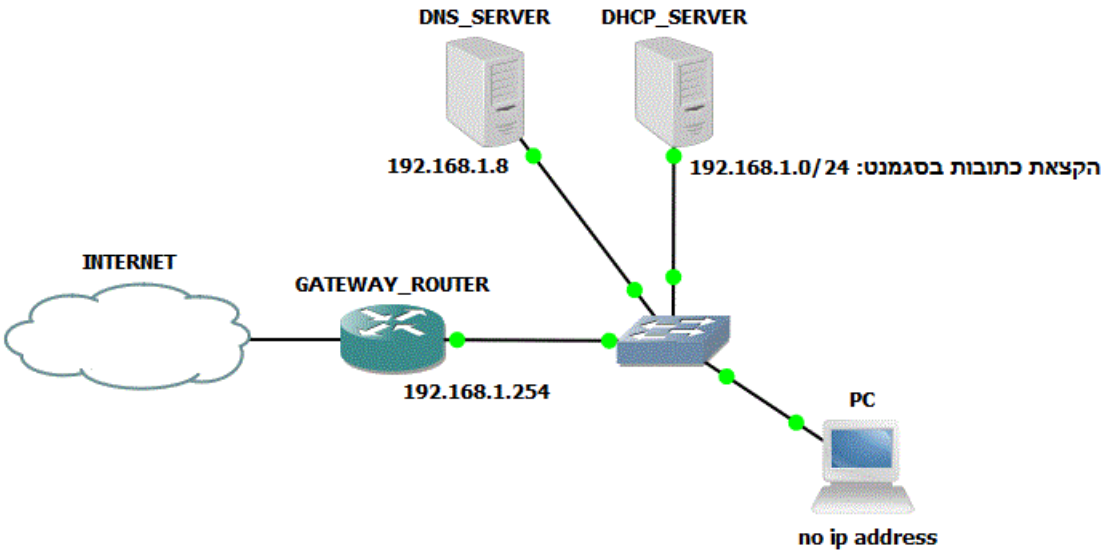
יוגבלו.

איך נממש פתרון הגנה תקשורתי?

- נשתמש בהקצאות סטטיות בספק ה-DHCP.
- לא נאפשר במתגים ממשקים שלא מחובר אליהם כלום, נגדיר ממשקים כאלו על VLAN מדומה כלשהו.
- נשתמש ב-Port-Security.
- נשתמש ב-Dot1X אם יש אפשרות ורצון לנהל את המנגנון הזה.

לכל אלו נוסיף כמובן אפיון חוקה מדוייקת ב-FW לסוגי התעבורה המאופשרים ברשת. בקיצור, לא חסרות לנו אפשרויות מימוש, רק לבחור ולהתחיל לעבוד.

סיימנו לדבר ועכשיו נחזור קצת לתכלס: אחרי שמימשנו והגדרנו את תצורת ה-DHCP שלנו, נתחיל להבין איך בעצם לנתח את הפלטים מפקודות ה-Show של DHCP. בואו ונזכר קודם כל איך נראית הרשת החביבה שלנו:



הפקודה הראשונה שלנו היא:

```
show ip dhcp server statistics
```

```
R1#sh ip dhcp server statistics
Memory usage         24504
Address pools        2
Database agents      0
Automatic bindings   1
Manual bindings      1
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         6
DHCPREQUEST          6
DHCPDECLINE          0
DHCPRELEASE          8
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            6
DHCPACK              6
DHCPNAK              0
R1#
```

פקודה זו תציג לנו נתונים כלליים הקשורים לתפקידו של הציוד כספק DHCP, נוכל לראות מידע לגבי כמות הודעות שנשלחו/התקבלו ע"פ סוגן, כמות הקצאות, זיכרון בשימוש ועוד.

הפקודה השנייה שלנו היא:

```
show ip dhcp binding
```

```
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.5         0063.6973.636f.2d63.    May 06 2014 05:45 PM    Automatic
                    6330.342e.3131.3730.
                    2e30.3030.302d.4661.
                    302f.30
192.168.1.240       0063.6973.636f.2d63.    Infinite                Manual
                    6330.312e.3131.3730.
                    2e30.3030.302d.4661.
                    302f.30
R1#sh clo
R1#sh clock
17:35:17.087 UTC Tue May 6 2014
R1#
```

פקודה זו בעצם מציגה לנו את כל הקצאות ה-DHCP הקיימות שהנתב/מתג L3 מכיר בהן והקצה הוא בעצמו. בפלט שאני מציג לכם ניתן לראות 2 הקצאות לשני לקוחות, הקצאה אחת סטטית כפי שלימדתי במאמר הקודם, והקצאה אחת דינאמית שנבחרה מתוך POOL הכתובות.

העמודה הראשונה כמובן מציינת את כתובת ההקצאה, העמודה השניה מציינת את ערך ה-Client-ID של הלקוח שמצויין בהודעות ה-DHCP שהוא שולח (לפי ערך זה לימדתי שניתן לבצע הקצאה סטטית בציוד מבוסס IOS), העמודה השלישית מציינת את התאריך והשעה המדוייקים שבהם יפוג תוקף ההקצאה - שימו לב שעבור ההקצאה הסטטית מצויין ערך Infinite שמשמעותו היא שאין תוקף להקצאה ושהיא בעצם אינסופית. העמודה הרביעית Type שמה, מציינת את השיטה שבה בוצעה ההקצאה: אוטומטית או ידנית.

אם נרצה מכל סיבה שהיא לנקות את הטבלה הזו ובעצם לגרום לנתב/מתג L3 "לשכוח" את ההקצאות שביצע, נשתמש בפקודת:

```
Clear ip dhcp binding
```

שבהמשכה נציין את ההקצאה שברצוננו למחוק (אם נרצה למחוק את כל הטבלה, נציין כוכבית (*) בסוף הפקודה).

כמובן שלא מומלץ לבצע ניקוי סתם כך, אלא רק להקצאות שאנו יודעים בוודאות שכרגע אינן בשימוש ונשארו בטבלה כשתוקפן עדיין לא פג, משום שהלקוחות לא דיווחו על הויתור עליהן באמצעות הודעת RELEASE. הנתב/מתג L3 מבצע כל כמה זמן בדיקה של הקצאות שתם זמנן ומוחק אוטומטית במקרה הצורך. אציין גם שלא ניתן לנקות הקצאות סטטיות מהטבלה מן הסתם.

הפקודה השלישית שלנו היא:

```
show ip dhcp pool
```

```
R1#sh ip dhcp pool

Pool LAB :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.6          192.168.1.1      - 192.168.1.254     1

Pool client :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 1
 Leased addresses               : 1
 Pending event                  : none
 0 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.240        192.168.1.240    - 192.168.1.240     1
R1#
```

פקודה זו מציגה לנו את כל המידע הרלוונטי על ה-POOL-ים שהגדרנו בנתב/מתג L3.

הפקודה תציג לנו בין היתר: נצילות ה-POOL באחוזים, כמות כוללת של כתובות בטווח המוגדר, כמות הכתובות שכרגע מוקצות, טווח הכתובות ב-POOL, ומבחינתי הפלט הכי חשוב שמוצג כ-Current index ואומר לנו על איזו כתובת IP עומד כרגע האינדקס, כלומר מה כתובת ה-IP הבאה שתוקצה מתוך ה-POOL.

בנתב/מתג L3 אין בחירה אקראית של כתובות מתוך הטווח אלא הקצאה בסדר קבוע שמתחיל בתחילת הטווח, נגמר בסופו ומתקדם בקפיצות של 1. ברגע שהנתב/מתג L3 מגיע לסוף הטווח, האינדקס יקפוץ לכתובת הבאה הפנויה החל מתחילת הטווח.

סיכום

מנגנון DHCP הינו כלי מרכזי במימוש רשת גדולה ויעילה, יחד עם זאת הוא טומן בחובו לא מעט פירצות, שיש לקחת בחשבון ולדעת להתגונן מפניהן. השילוב של DHCP יחד עם רשת מאובטחת יתן לנו יתרונות גדולים מאוד אם נדע לנהל נכון את העניינים.

על המחבר

הנדסאי חשמל ואלקטרוניקה, בן 25 מאשדוד, בעל הסמכת CCNP, עוסק מזה 5 שנים בעיקר בתחום תקשורת הנתונים בשירות המדינה ויכול להגיד מניסיון שהתחום הזה לא מפסיק לגדול ולהתפתח וטוב שכך, זה משאיר אותנו (מי שאוהב את התחום) תמיד צמאים לעוד, ובידיעה שאף פעם לא חסרים דברים חדשים ללמוד עליהם.

לשאלות, טענות, עזרה, ייעוץ, תלונות וכו' - Tomy Shalev בפייסבוק.

Pelegit.co.il הינה קהילת IT שמספקת מידע ועזרה לאנשי המחשוב בתחום, ניתן למצוא באתר מאמרים, משרות הייטק, חדשות בתחום ועוד אינפורמציה לטובת הרחבת הידע.