שם התלמיד : אלעד דפנה

מבחן סופי:

הכתובת ההתחלתית שהבאת לי כנתון + הכתובת שאני סיפקתי הם מ Class C
כמו כן שתבין מה עשיתי מספרתי את מספרי ה Host משמאל לימין כאשר (1 זה ההכי שמאלי , ו -9 זה הכי ימני)

שאלה 1 א.

מחלקת it - =192.168.1.0/24
Host1- 192.168.1.1/24

Host2-192.168.1.2/24

Host3-192.168.1.3/24

מחלקת R&D – 192.168.2.0/24
Host4 – 192.168.2.1
Host5 - 192.168.2.2
Host 6 - 192.168.2.3

מחלקת Support – 192.168.3.0/24
Host7 – 192.168.3.1
Host8 - 192.168.3.2
Host9 – 192.168.3.3

בעזרת Vlan בעצם נאפשר ייעול אפקטיבי ברשת ע"י הפרדה של הכתובות לכל מחלקה שונה, בעצם כל מחלקה תקבל רצף ייחודי של כתובות ובנוסף זה יכול לסייע בבקרה ואבטחה.

שאלה 1 ב.

בעזרת VLAN – Virtual Local Area Network/Virtual Lan אפשר לחלק בצורה מאובטחת את שלושת המחלקות,
Vlan – טכניקה ברשתות המשתמשת לקבוצות חיבורים להפעלת מכשירים ושירותים בתחומי רשת מופרדים ובלתי תלויים לדוגמא: אני מגדיר שמחלקת it תוכל להיכנס רק לתוכן הספציפי שהיא צריכה ולא לדוגמא למחלקת R&D .

שאלה 2.

UDP	TCP
Best Effort – נסיתי להעביר מידע > לא הצלחתי > לא אכפת לי כמובן **שלא** יוצרים חיבור לפני	חובה לבצע Connection oriented הכוונה שיוצרים חיבור לפני השליחה
במקרה של אובדן חבילה – **לא** שולחים שוב	במקרה של אובדן חבילה, החבילה נשלחת שוב
מתאים ל Voice	מתאים ל דוא"ל, דפדפן
פרוטוקול מהיר (מהיר פי כמה מ TCP)	פרוטוקול איטי
הפקטות יכולות להגיע באותו סדר **אך לא בהכרח** שהם יגיעו לפי הסדר	הפקטות בוודאות יגיעו בדיוק באותו סדר
	פרוטוקול אמין

שאלה 3 א

IPv4 ו-IPv6 הם שני פרוטוקולים לתקשורת ברשתות, והם משתמשים בכתובות IP כדי לזהות מכשירים ברשת

Ipv4 – 32 BIT , קיבולת: 4 מיליארד כתובות, אבטחה בסיסית ללא אימות והצפנה

ipv6 – BIT128 , קיבולת: 340 (הכוונה 340 עם 36 אפסים מספר עצום) כתובות, אבטחה משורפת עם אימות והצפנה

מבחינת יעילות הרשת :ipv4
בשל המגבלות בכמות הכתובות ב-IPv4, יש צורך בפתרונות כמו NAT כדי למקם את המכשירים ברשת. בנוסף NAT יכול ליצור בעיות יעילות ובידוד של רשת.

מבחינת יעילות הרשת :ipv6
מספק כל כך הרבה כתובות שאין צורך ב-NAT לאותו המדרג, בנוסף יעילות הרשת ניתנת לשיפור בזכות כתובות ייחודיות לכל מכשיר.

לסיכום ipv6 מציע יתרונות בגודל הכתובות ויעילות הרשת, והתקן זה נוצר על מנת לפתור בעיה זו, בניגוד לכך לפי שלמדנו ישראל עדיין לא שם (גם אם 5% משתמשים בipv6 ישראל עדיין לא שם)

שאלה 3 ב.

MAC -היא כתובת הצרובה על רכיב החומרה ופועלת בפרוטוקול OSI שממומש ב -Data Link . בנוסף כתובת Mac מורכבת מ BIT48 או byte6 ומטרתה לקשר בין שני מכשירים.
יתרה מכך לכל מכשיר יש כתובת צרובה לדוגמא: רכיב בלוטוס , WIFI וכו'.
חייבת להיות כתובת סטטית ללא יכולת שינוי.
כתובת ה Mac קשורה לשכבת ה DataLink במודל ה OSI

IP Address- כתובת של 32 BIT (או BIT128 אם משתמשים ב IPV6) הפועלת בפרוטוקול OSI שממומשת בשכבת ה Network . בנוסף את אותה כותבת IP מחלקים ל- HOST id ול- Network id .
כתובת IP יכולה להיות קבועה \ דינמית בנוסף ממומשת במודל ה OSI בשכבת ה Network (כאשר כל מספר עד הנקודה הוא 8 BIT וגם נקרא אוקטטה). כמו כן פועל בשכבת ה Network במודל OSI

Network port- פועלות בשכבה התעבורה במודל ה OSI , הן בעצם נקודות וירטואליות לתקשורת ברשת מחשבים. הם משמשות כדי להבחין בין שירותים או יישומים שונים הפועלים במכשיר ובנוסף עוזרות להפנות נתונים לתהליך או לשירות הנכון במכשיר.

לסיכום כתובת Mac משמשת לתקשורת מקומית (בתוך אותו רשת) , כתובות IP זאת בעצם הכתובת הלוגית לתקשורות בין רשתות שונות , Network Port עוזרות לפנות נתונים ליישומים או שירותים הפועלים במכשיר. כמו כן כל אחד מהם פועל במיקום אחר במודל ה OSI כמו שציינתי לעייל.

שאלה 3 ג.

פרוקוטול CSMA/CD (כבר לא משתמשים בו היום בגלל שיש Full duplex וזה פתר את כל הבעיות של ההתנגשות)- פרוטוקול Wireless, פרוטוקול שכל המהות שלו לטפל בשגיאות / אובדנים / למנוע התנגשויות בתקשורת בזמן אמת ברשת ובנוסף לטפל בהם בצורה יעילה.

Half duplex – רק לכיוון אחד (ובזמן הזה החוט תפוס)

Full duplex – לשני הכיוונים (לשלוח ולקבל בו זמנית)

כמו כן בהעברת נתונים ברשת יש את השלבים הבאים:

שלב האזנה - המכשיר בודק האם הקו פנוי לשידור

שלב ההחלטה-אם הקו פנוי מחליט לשדר את הנתונים

שלב ההמתנה - המכשיר ממתין כמה רגעים להתפנותו לפני שהוא מנסה לשדר מחדש

שלב התשדורת - אם אין פעילות ברשת המכשיר ישלח את הנתונים.

אם יהיה התנגשויות ברשת הוא יפסיק ויחזור להאזנה.

שאלה 4:

1. (Network Address Translation) NAT- הוא פרוטוקול ברשתות המאפשר למכשירים ברשת לשתף כתובת IP חיצונית אחת. בעזרת NAT, כתובת ה-IP של מכשיר ברשת הפנימית מתורגמת לכתובת החיצונית כאשר המכשיר יוצא לאינטרנט. זה מפחית את צורך בכתובות IP ייחודיות וחוסך מקורות. NAT מספק גם שכל המכשירים ברשת יכולים להשתמש באותה כתובת חיצונית לגישה לרשת החיצונית. פרטיות ואבטחה נוספת, בנוסף נפוץ ברשתות הבית והעסקית, מסייע בניהול תעבורת רשת ומספק פתרונות למגוון רחב של התקנים.

החיסרון ב NAT – מאט את מהירות משום שאולי צריך לעבור בכמה רואטרים עד שיתבצע שידור החוצה

יתרונות- מאפשר לי להרחיב את מרחב הכתובות

2. ARP היא בעצם פקודה רק בלינוקס אשר מראה בעצם מי מחובר לרשת שלי, יתרה מכך הוא פרוטוקול שמשמש לקשר בין כתובות IP לבין כתובות MAC ברשת מקומית.

בנוסף אם אני יודע את הכתובת IP ולא יודע את הכתובת הפיזית (MAC) אני השתמש בפקודת ARP.

אך אם אני יודע את כתובת ה MAC ולא יודע את כתובת ה IP אני השתמש ב Reverse ARP

3. DNS - בעצם אחראי לתרגם שמות של אתרים (URL) לכתובות IP . פרוטוקול זה עובד אך ורק באמצעות UDP משום שאנחנו לא רוצים לחכות המון זמן עד שנכנס לאתר.

יתרה מכך, פרוקוטול זה חשוב משום שקשה לזכור כתובות IP בעל פה, אפשר להשוות את זה למספרי טלפון אשר קשה לזכור אותם בעל פה, לדוגמא: בפאלפון אנו שומרים פעם 1 בנאדם עם המספר שלו ואחר מכן כדי להתקשר לאותו בנאדם אנו צריכים לזכור רק את שמו ולא את המספר פאלפון שלו.

4. זאת בעצם פקודה שבודקת קישוריות ומודדת זמנים. הפקודה בעצם שולחת פינג, זאת אומרת – המחשב שלי שולח היי מה קורה לשרת ומיד לאחר מכן והשרת עונה לי הכל בסדר אני חי.

הפקודה עצמה שכתבת בעצם שולחת 5 חבילות של סימן חיים

5. מטרתה של הפקודה היא להראות לי את הכתובת IP של המכשירים ברשת, את כתובת ה Mac שלהם ובנוסף את סוג החיבור לדוגמא Eth0

6. כנראה שאתה מתכוון לפקודת Traceroute .. פשוט לא רציתי לשאול אותך כדי לא להגיד את התשובה, לכן אני מתכוון לפקודה זו.
פקודת Traceroute היא פקודה בלינוקס שמראה את כל הניטובים שאני צריך לעבור על מנת להגיע לאתר מסויים לדוגמא Ynet. בעצם מראה מה אני עובר עד שאני מגיע ישירות לאתר YNET

7. פקודת Ipconfig בווינדוס / Ifconfig בלינוקס בעצם מראה:
ipv4 / ipv6 בהתאם לתצורת המחשב, Default Gateway, subnet Mask , DNS ,
, Mac Adress
Mac addres, ipv6, ipv4, dns , ציינתי בשאלות למעלה,
Default Gateway - הכתובת של הרואטר
Subnet Mask - היא הגדרה של מספר הסיביות בכתובת ה־IP המשמשות לקביעת כתובת הרשת. (מכילה 0 HOST או 255 לכל אורכה).

8. פקודת nslookup היא כלי שמשמש לבדיקת ופתרון בעיות קשורות לרשת, בעיקר בהקשר של DNS. הפקודה עובדת גם בווינדוס וגם בלינוקס.
הפקודה מספקת מידע על שרתי DNS שבהם נרשם המחשב.
כלי זה עוזר לפתרון בעיות ברשת משום שאם יש בעיה בקבלת כתובות IP משמות דומיין, הפקודה יכולה לעזור לבדוק את הגדרות ה-DNS במחשב ולוודא שהן תקינות.
לדוגמא: nslookup example.com
וזה בעצם נותן לי את IP של הסרבר שחיפשתי

9. כתובת IP של YNET בעצם השתמשתי בפקודה: ping ynet.co.il - 88.221.169.121
כתובת ip של CNN השתמשתי בפקודה: ping cnn.com - 151.101.131.5

שאלה 5:
DataLink - Mac
Network - IP
Transport – UDP
Transport -TCP
Physical - HUB
DataLink- Switch

Network - Router

Skype – שכבת האפליקציה

<u>שאלה 6</u>

<u>192.168.1.10/24</u>

Class-C

192.168.1.0 – Network Adress

192.168.1.1 – First Adress

192.168.1.254 – Last Adress

192.168.1.255 – Broadcast address

192.168.1.254 -192.168.1.1 – IP Adress range for hosts

255.255.255.0 – Subnet mask

8 - Number Hots

24 – Number Network

<u>שאלה 7:</u>

גודל פקטה – 3980 + Header IP של 20

MTU – 1000 + IP Header 20

Fragment 1: Total Length 1000 byte (ip header + data) , Offset: 0 , MF=1

Fragment 2: Total Length 1000 byte (ip header + data) , Offset: 122.5 , MF=1

Fragment 3: Total Length 1000 byte (ip header + data) , Offset: 245 , MF=1

Fragment 4: Total Length 1000 byte (ip header + data) , Offset: 367.5 , MF=0