**קורס רשתות – מבחן מסכם**

**חלק א': יצירת רשת ב-Packet Tracer**

הנחיות:

1. למד על הכלי Packet Tracer
2. פתח את Packet Tracer ויצר רשת בסיסית הכוללת:
   * 2 ראוטרים
   * 4 מחשבים
   * קבע כתובות IP לכל מכשיר (IPv4) כך שכל מחשב יוכל לתקשר עם המחשב השני.
3. ודא שכל המחשבים יכולים לבצע פינג אחד לשני (ping)
4. לאחר יצירת הרשת, שמור את הקובץ והגש אותו לבחינה

**חלק ב': הבנה של מושגים ברשתות**

1. מהו IP (Internet Protocol)?
   * הסבר מהו IP ולמה הוא משמש ברשתות מחשבים.
2. מה ההבדל בין כתובת IP פרטית לכתובת IP ציבורית?
   * הגדר מהי כתובת IP פרטית ומהי כתובת IP ציבורית. פרט דוגמה לכל אחד מהסוגים והסבר מתי נשתמש בכל אחד מהם.
3. מהו פרוטוקול DNS ולמה הוא משמש?
4. מהו פרוטוקול NAT (Network Address Translation)
   * הסבר את עקרון הפעולה שלNAT , כיצד הוא פועל ברשתות תקשורת, ואיך הוא מסייע בשימוש בכתובות IP פרטיות בתוך רשת ארגונית.
5. אילו פרוטוקולים מרכזיים קיימים ברשתות תקשורת?
   * פרט לפחות שלושה פרוטוקולים מרכזיים לדוגמה: (TCP, UDP,ICMP) והסבר על תפקידם וחשיבותם ברשתות תקשורת.
6. פרט בהרחבה את כל התהליך אשר מתבצע מאחורי הקלעים, מא' ועד ת', כאשר אתה ניגש מהמחשב הביתי שלך לFacebook.com ומקבל ממנו מענה. הסבר את ההבדלים בין התהליך שמתבצע בעת פנייה לFacebook, לעומת בעת ביצוע שיחת וידאו.

**תשובות חלק ב':**

1. לכל מחשב יש כתובת ייחודית כך שיוכלו המכשירים לתקשר זה עם זה את הכתובת מקבלים מספק האנטרנט או מהראוטר ,ודרכו המחשב יודע לאן לשלוח את המידע באנטרנט שעובר דרך הראוטרים. כתובת ip בעצם משמשת ככתובות לוגית שמאפשר למחשבים וראוטרים להבין איך לנתב מידע בין רשתות שונות. הכתובת מורכבת מ32 ביטים.
2. כתובת IP פרטית משמשת לרשת מכשירים מקומית כמו משרד או בית ,שיתקשרו אחד עם השני ואין גישה לתקשור עם אינטרנט מבחוץ. לדוגמא 192.168.1.2. לכל מכשיר עם כרטיס רשת נקבע כתובת MAC על ידי היצרן , כתובת זו משמשת ברשת מקומית. כל מכשיר ברשת המקומית שומר את כתובת הMAC עבור כל כתובת IP שהוא מכיר על ידי הarp , ככה כאשר נשלחת בקשה למחשב באותה רשת נשלח בקשה לכל המכשירים שבאותה רשת ושואלים את כולם למי יש את האייפיי שנשלח כאשר מכשיר עונה אז באמצעות הarp יודעים איזה כתובת MAC שייכת למכשיר הזה ושולחים את הקשה אליו.

ואילו כתובת IP ציבורית היא כתובת ייחודית לרשת שמאפשרת גישה ישירה לאינטרנט ומסופקת מספק האינטרנט ה- NAT דואג לשבור את הכתובת ip הפנימית לכתובת ip ציבורית ,יש לו טבלה בה שומר פורט פרטי כתובת פרטית וכן ציבורי וכך כשהשרת מחזיר תשובה הראוטר יודע לאיזה מחשב פנימי לשלוח את התשובה דרך הפורט. הצורך ברשת פרטית וציבורית נובע בין היתר כי כתובות ציבוריות הן מוגבלות וגם כתובת פרטית מאובטחת יותר.

1. DNS זה מערכת שמתרגמת כתובת אינטרנט, שמובנת לאדם ושיותר קל לזכור , לכתובת IP שהמחשב מבין.
2. בגלל שכתובות ציבוריות הן מוגבלות לכל מכשיר יש כתובת פרטית ופרוטקול NAT דואג להמיר את הכתובת לכתובת ציבורית. מה שעוזר לחסוך בכתובות ציבוריות ואבטחה. כמו כן הnat , מנהל כתובות IP ואת הפורט ברשת החיצונית. יש לו טבלה בה שומר פורט פרטי כתובת פרטית וכן ציבורי וכך כשהשרת מחזיר תשובה הראוטר יודע לאיזה מחשב פנימי לשלוח את התשובה דרך הפורט. ברשת המקומית הnat לא יכול לעזור כי שם יש צורך בזיהוי של המכשירים ברמת החומרה.
3. TCP- **א. אמינות** שולחים פקטה ומחכים לאישור שהתקבל ככה מוודאים שאף פקטה לא נאבדה בדרך. טוב למייל והעברת קבצים. **ב. קשר בין הלקוח לשרת** לפני שהנתונים נשלחים על ידי הנדשייק שבו הלקוח והשרת מסכמים את אופן העברת הנתונים. **ג. שומר על סדר הנתונים** ואם חבילה נאבדה בדרך או לא נשלחה ידאג לשלוח מחדש ולסדר את העברה. **ד. זרימה של הנתונים** בקצב שלא יעמיס על הצד המקבל.
4. UDP- **א. אי אמינות** שולחים פקטה אחת אחרי השנייה במהירות בלי אישור שהתקבל ולכן יכול לצאת מצב שנאבדה בדרך פקטה או שלא הגיעה בסדר הנכון. טוב לשיחות ווצאפ. **ב. אין קשר בין הלקוח לשרת** ואין בדיקה עם הצד השני מוכן לקבל או לא לכן מהיר יותר אך פחות אמין. **ג. לא שומר על סדר הנתונים** ואם חבילה נאבדה בדרך או לא נשלחה **לא** ידאג לשלוח מחדש ולסדר את העברה. **ד. ללא בקרת זרימה של הנתונים** ולכן יכול לצאת מצב שהצד המקבל מוצף.

ICMP - אינו מיועד להעברת נתונים אלא לבקרה ומציאת תקלות ולניהול רשתות.

1. כאשר המשתמש מקליד facebook.com דבר ראשון נשלח לשרת ה dns בקשה לקבל את כתובת ה- ip- הציבורית של פייסבוק. אם לא נמצא במטמון א, המחשב מעביר את הבקשה לשרת ה-DNS של ספק האינטרנט .המחשב שולח את הבקשה לכתובת של הראוטר , הראוטר צריך לתרגם אותן לכתובת IP **ציבורית** אחת ,ואז הוא רושם בטבלת NAT פורט X שייך למחשב Y. לפי הפרוטוקול אם משתמשים ב-tcp מבצעים חיבור לשרת על ידי בקשת SYN והשרת מחזיר ACK SYN והמחשב עונה בחזרה ACK , ואז השרת שולח תגובת HTTP עם תוכן האתר. בעת חיבור לשליחת הודעות משתמשים בפרוטוקול ה TCP , כדי לשמור על רצף ושאף נתון לא יאבד בדרך. ובשיחות וידאו משתמשים בUDP כי אין צורך לשמור על כל הנתונים הנשלחים.

|  |
| --- |
|  |