סיכום קורס בתקשורת :

תהליך אליס ובוב :

המקרה: ישנו את אליס ויש את בוב שהוא web server המכיל דף אינטרנט.

אליס נמצאת בבית שלה ויש לה את הראוטר המכיל איזו ספק שירות שמחבר בין כל שני ראוטרים בפרוטוקול **BGP** (הדבק של האינטרנט – דואג לכך שניתן להגיע לפרפיקסים מסויימים).

לנתב (לראוטר) יש טבלת ניתוב המחולקת ל internal ול Intelout .

לנתב יש עוד תפקידים (לאו דווקא בתור נתב): הוא מנהל את הרשת המקומית (PHCP) ,NAT וגם הlocal DNS .

לפני שאליס תוכל לשולח הודעה היא צריכה להתחבר לרשת.

מה הדברים שאליס צריכה כדי להתחבר לרשת ?

כרטיס רשת, כתובת ip ,get way, צריך לדעת מי הוא הDNS שלי ,זמן (t), mask - באיזו רשת אני נמצא (כדי שאני אדע אם ה ip שאני שולח נמצא אצלי ברשת או לא).

כלומר **DHCP** יכיל בתוכו – time , mask , ip DNS, ip gw (get way), ip alice .

כדי שאליס תוכל לקבל את הפרטמים הנ"ל מהפרוטוקול DHCP אני צריך שרת DHCP ואז קודם נשאל האם ברשת קיים שרת DHCP ולאחר מכן נבקש ממנו שירות (סה"כ ארבע הודעות – כלומר ה DHCP עטוף בUDP שעטוף בIP שעטוף ב LINK (ethernet או wifi).

כעת אליס פותחת דפדפן וכותבת את כתובת האתר.

(בהנחה שאנחנו צריכים את כל התהליך והIp לא נמצא בטבלת לוק אפ של אליס).

בעיקרון מה שהיא רצתה לעשות זה לשלוח **http request** שיביא לה את ה html,ואנו יודעים ש http עובד מעל **TCP** שמשתמש ב 3 way handshake.

כלומר בצורה עקרונית אליס יכלה לעשות את זה – יש לה את כל הנתונים היא הייתה יכולה לבנות heater של TCP ואז לבנות heater של Ip.

אך חסר לה את הדבר העיקרי – לאן אני פונה – ip destination ולכן מגיע לעזרת חבר בקשת **הDNS** שבונה לעצמו את ההודעה וכדי לקבל את ה ip dest הוא פונה לlocal DNS וכך הוא מקבל את הip dest (כלומר תהליך הDNS מביא את זה).

כעת נכנס לפעולה **הNAT** שנותן לנו Ip חדש, ip חיצוני ולכן בהודעת הDNS הip src ישתנה ל ip החיצוני.

ש. מדוע יש בווירשאק 2 הודעות DNS ואילו בתהליך עצמו יוכל להיות 8 ?

ת. מה שאני רואה בווירשארק זה מה שנכנס ויוצא מכרטיס הרשת שלי והתקשורת בין הנתבים עצמם לא מופיעים.

נשוב לתהליך – לאחר פתיחת **TCP** (שליחת בקשת syn , קבלת synACK והחזרת ACK (3 way handshake)) , נפתח סוקט ונשלח בקשת http request ושאותו נעטוף ב TCP וב IP.

יש לציין שבקרה שלנו ה mac distention שנמצא בשכבת הלינק שונה מip distention , נקבל את הmac dis ע"י בקשת **ARP** (עושה resolving מip לmac).

כעת ההודעה שמורכבת מכל הנ"ל (בקשת HTTP, עוטפים בTCP, עוטפים בIP ובETH) תשלח ותעבור בכל הנתבים וכל נתב יסתכל על ip dis ואז נלך לטבלת הניתוב שלו, בטבלת הניתוב נחפש האם

התחילית (הprefix) מתאימה ל Ip שלי ואם כן נמשיך לחפש תחילית יותר ארוכה כלומר ננסה למצוא כמה שיותר מדויק (יש טבלאות שכבר ממוינות וכך הולכים ישר לארוך ביותר ואם יש תיאום אנו יוצאים החוצה).

הראוטר של אליס יודע לאן לשלוח הלאה את הבקשות שלה כיוון ש הראוטר הוא חלק מאיזור אוטונומי.

לדוגמא בבזק בינלאומי שמחזיק מלא נתבים יש מישהו שמנהל את האזור האוטונומי, הוא מפעיל פרוטוקול ניתוב intra routing, או את RIP או OSPF. כלומר כל הראוטר יודע להגיע לכל אחת מהרשתות בתוך האזור האוטונומי.

האזור האוטונומי הזה מחובר לוגית בgateway גם לאזורים אוטונומיים אחרים, והוא יודע לאיזה prefix הוא יכול להגיע לוגית. הוא מפרסם לכל הרשת בiBGP לאן אפשר להגיע ממנו, ובeBGP לאן אפשר להגיע ממנו (ע"פ מדיניות – למשל ישראל לא תעביר תקשורת דרך אירן).

נעבור לצד של בוב, לשרת.

אליס שלחה HTTP REQUEST וקיבלה HTTP RESPONSE תהליך הקבלה התבצע כך :

השרת רואה את הבקשה, ומבין שהיא רוצה נניח html, הוא מסדר את הheader, ומעביר את הכל לשכבת התעבורה, אבל שכבת התעבורה לא בטוח שתצליח להעביר את הכל במכה, אז היא תסדר ותחלק לסגמנטים שישלחו במקצב מסוים שעולה בקצב אקספוננציאלי עד בעיה מסוימת למשל trash hold ולינארי החל ממנו או בעיה של 3 duplicate ack או timeout תוריד את הקצב של השליחה.

תזכורת: **TCP** כפרוטוקול אמין נפתח ב3 הודעות, ונסגר ב4 הודעות.

מי שאחראי על סגמנטציה ושליחה של סגמנטים היא שכבת הטרנספורט ולא האפליקציה, קצת כמו חברת שליחויות שמקבלת משימה ומנהלת את שליחת המשאיות (מעמיס את המשאית וסע או שהמשאית חיכתה יותר מדי זמן וסעי מה שיש לך).

כעת נבין באיזו גרסת **HTTP** אנחנו.

אם אנחנו ב1.0 אנחנו פותחים וסוגרים קשר על כל בקשה וקבלה.

ב1.1 אנחנו לא סוגרים אלא ממשיכים לבקש ולקבל,

ב1.1.p אנחנו נבקש כמה וכמה אובייקטים ביחד ונקבל אותם אחד אחרי השני.

אם אנחנו ב**http 2** יכול להיות שהסרבר יעשה לנו push וידחוף לנו אובייקטים אחד אחרי השני.

אם אנחנו ב**http3** אין לנו בכלל TCP אלא הכל מתנהל אצל QUIC .

כעת במקרה שאנחנו נמצאים **ב web proxy** אזי אליס מדבר איתו ואם האובייקט אצלו הוא יביא לו ואם לו הוא יתנהל מול הweb server (web proxy נמצא בצד של הלקוח מחזיק אובייקטים שהלקוחות רוצים ונועד לקצר את הזמן).

לסיכום, התהליך במודל חמשת השכבות :

לפני הכל כדי שבכלל יהיה תקשורת אנחנו צריכים להשתמש בפרוטוקול DHCP כדי שנוכל להתחבר לרשת לכן קודם נשאל האם קיים ברשת שרת DHCP ונבקש ממנו שירות.

בשכבה החמישית אנו בבקשת HTTP REQUEST ונשתמש בנוסף בבקשת DNS בכדי שנקבל את ה Ip destination .

כעת נעבור לשכבה הרביעית ונשתמש בפרוטוקול TCP ,הפרוטוקול הזה יפתח לנו ערוץ תקשורת עם ה web server ויתחיל את התקשורת עם מגנון 3 way hand shake ולאחר מכן יתחיל לקבל אובייקטים וייסגר עם אותו המנגנון ב4 פעולות.

כעת אנו בשכבה השלישית שכבת הרשת , פרוטוקול הNAT ימיר לנו מ Ip פנימי ל Ip חיצוני ולכן בהודעת הDNS הIp src ישתנה ל Ip החיצוני.

כעת כל נתב בדרך ישתמש בטבלת הניתוב שלו בכדי להעביר לנתב הבא הנמצא ברשת עד שנגיע לweb server (הזיהוי בטבלת הניתוב יהיה ע"פ מזהה הרשת ונשאף להיות כמה שיותר מדויקים).

כל הנ"ל תלוי בשכבה השנייה שבכלל אומרת לך באיזה פרוטוקול אנו משתמשים בכדי להעביר את הנתונים אם בקשר ישיר, קווי – Ethernet או לחילופין ב Wi-Fi .

גם רוחב הפס נגרר משכבה זו, כרטיס הרשת שלך הוא זה שקובע את מהירות קבלת הנתונים.

לכל כרטיס רשת צריך שיהיה מזהה MAC ואת המזהה הזה נשיג באמצעות פרוטוקול ARP שממפה בין כתובות לוגיות של שכבת הרשת לכתובות פיזיות של שכבת הקו.

כעת כל הנ"ל עובר בשכבה הפיזית באמצעות כבלי רשת, סיבים אופטיים, לוויין וכו'.

כאשר השכבה עצמה מעבירה כל פעם ביט אחד – 0 או 1.

מושגים :

CDN – נועד לבעלי התוכן (ל web server לדוגמא) והוא נותן לבעלי התוכן לשמור את התוכן בשרתים שקרובים ללקוחות שלהם ואז שהלקוח רוצה משהו הCDN אומר לו בוא קח את זה ממקום קרוב.

BGP - הוא פרוטוקול שרץ על TCP. מקשר בין שני gateways אם אין בעיות מדיניות הם מדווחים אחד לשני ואומרים "בוא אלי אם אתה רוצה להגיע אל הprefix הזה והזה". כל gateways יעביר לכל הרשת אוטונומית את כל הprefix שאפשר להגיע ממנו והלאה (הם כבר יודעים את הדרך אליו)

CC -congestion control - אלגוריתמים שיודעים להתמודד עם גודש, כלומר אתה עולה ועולה שולח ושולח כמה שיותר פאקטות ומנסה להגיע כמה שיותר גבוהה בלי לאבד פאקטות אם איבדת פאקטות הבנת שלא עמדת בעומס, אלגוריתמים כגון reno ו cubic שמטרתם למצוא את הנקודה הזו.

ישנם כמה מנגנונים לבקרה :

Slow start – נתחיל מחלון בגודל 1 ונגדיל את החלון בצורה אקספונניציאלית.

Congestion avoidance - גודל החלון גדל בקצב ליניארי בעת הגעה למצב sstresh.

3 ACK Duplicate – אם קיבלנו 3 פעמים ACK אזי נקטין את גודל החלון ונחלק אותו ב2.

Timeout – אם קיבלנו timeout , נתחיל מ slow start וה sstresh מתחלק ב2.

ICMP - פרוטוקול שבא לעזור לנו בניהול הרשת. לדוגמא, הודעות פינג, מדידה של TTL. גודל של פרגמנטציה, בדיקה של האם צד שני חי. זה פרוטוקול ברמת הnetwork.

ICMP-header - מורכב מהסוג (type – 0 or 8),הקוד (ECHO),checksum,data .

Ping – תוכנה כמו הטרמינל לדוגמא שכאשר היא שולחת ICMP .

TTL – זהו מספר ה hop שפאקטה יכולה לעבור עד שהיא תשמיד את עצמה כלומר זהו תנאי עצירה שאם הפאקטה הגיעה אליו אזי כנראה שהיא לא הגיע ליעד ולכן תשמיד את עצמה.

NIC – זה מה שמחבר את המחשב שלך לרשת ברמה הפיזיקלית ניתן לראות את זה אם נעשה igconfig.

NI -network interface – בעל ממשקים לוגים או פיזים – הכרטיס רשת שלך מחולק לפונקציות שונות ממש כדי שיוכלו להאזין במקביל.

Ethernet – השכבה הפיזית, למחשב ולנתב המחוברים בינהם אין Ip והם מדברים בינהם דרך כבל אך מחשבים שהם תחת אותה רשת מדברים דרך כתובת MAC שהיא כתובת יותר נמוכה וכך המחשבים מתקשרים.

Promiscuous mode – הרשאות לכרטיס הרשת, כלומר כל מה שעובר על הכרטיס רשת נגיש.

Monitor mode – הרשאות יותר עדינות השייכות לwi-fi.

Raw socket – סוקט מסוג זה מאפשר לך לעקוף את השכבה של התעבורה ובעצם מקבל גישה ישירה לחומרה, כלומר הוא עוקף את TCP/ip שזה בניגוד לסוקט רגיל שמשתמש בTCP/ip והשליטה בו מוגבלת כי הוא מכוון מטרה.

BSD packet filter (BPD) – פילטר הבנוי מstruct וכל מה שלא נמצא בפילטר הוא זורק אותו וקולט רק את הפאקטות הנכונות לבאפר.

תהליך ההסנפה – במידה ואנו מדברים על wi-fi אזי יש באוויר פאקטות המחכות להיקלט ובכל פאקטה יש קוד MAC וע"י הקוד הזה מתבצע הסינון כלומר בעצם ההסנפה מסננת את הקוד MAC המתאים בין הפאקטה למחשב עצמו וכך הוא מכניס רק את הפאקטות המתאימות.
בפילטר הזה אנו יכולים לסנן עוד קטגוריות ובכל מקום שיש כרטיס רשת יש כזה פילטר.

Pcap – ספריה שמשמת במערכת ההפעלה את כל מה שצריך כדי להסניף, כיוון שיש גם בעיה שהפילטרים לא ניידים לכן לPcap יש שפוי Api יחיד.

Spooging – התחזות, כאשר יש משהו מזוייף למשל שהיעד שלו הוא אחר לגמרי זה נקרא spoofing ,ההתחזות יכולה להיות גם בפאקטות מסוג ICMP וגם מUDP.

Endianness- תהליך העברת הביטים – מאיזה צד אני מתחיל להעביר את הביטים.

TCP לעומק –

תכונות :
קשר נקודה לנקודה – רק מחשבי הקצה משתתפים ללא הנתבים בדרך.
Full duplex – גם מאזין וגם משדר.
בקרת זרימה – השולח לא ישלח יותר ממה שהמקבל יכול לקבל (הבפאפר שלו).
חיסכון בזמן - TCP שולח ACK ויכול לאסוף אותם ולשלוח ביחד.
3way-handshak – מבצע חיבור לפני תחילת התקשורת.
תחילת ההתקשרות מבוצעת ע"י ACK וseq, כאשר המשתמש שולח seq and ACK, data והשרת מחזיר את אותה הדאטה וגם ACK ו seq אזי מתחילה ההתקשרות,גם בסגירת ההתקשרות מתבצע תהליך דומה (בעל 4 שלבים).

ש. מה ההבדל בין **NAT לDHCP**?

ת. DHCP נותן לנו את הקונפיגורציה (הC מתוך הDHCP) ל host , הNAT מבצע את ההמרה בין ip חיצוני לip פנימי.

שאלות ותשובות :

ש.מה ההבדל בין DNS ל DOH ?

ת. DOH- מורכב מהודעת DNS שעטופה בhttp שעטופה בפרוטוקול TLS ואת החבילה הזו אני שולח כבקשה.

לעומת DNS שאינה מאובטחת ונשלחת כבקשת DNS לבד.

- DNS- עובד בפורט 53 ובצורה לא מאובטחת (משתמש בUDP) ולכן לא מוצפן.
- DOH- משתמש בTCP ולכן מוצפן. מעביר את בקשת הDNS בHTTPS בניגוד לבקשת DNS רגיל ולכן גורם שלישי לא יכול לצפות בתעבורה.
- **הבדלים בין DNS לDOH -** ההבדל העיקרי הוא השימוש ב TCP לעומת UDP השימוש בTCP מקנה מספר **יתרונות** – איתור מהיר יותר באיבוד פאקטות (3way-hanshke),אמין יותר.

חסרונות – עומס – יש מעט שרתים לעומת DNS.

ש. מה ההבדל בין NAT לDHCP?

ת. DHCP נותן לנו את הקונפיגורציה(תצורה) (הC מתוך הDHCP) ל host , הNAT מבצע את ההמרה בין Ip חיצוני לIp פנימי.

ש. מדוע יש בווירשאק 2 הודעות DNS ואילו בתהליך עצמו יוכל להיות 8 ?

ת. מה שאני רואה בווירשארק זה מה שנכנס ויוצא מכרטיס הרשת שלי והתקשורת בין הנתבים עצמם לא מופיעים.

ש. מה התפקיד של הNAT ברשת, האם הNAT יכול להיות גם בצד של הserver ?

ת. להמיר מ Ip פנימי ל ip חיצוני (משתמשים בזה בטלפונים, ובראוטרים, כי זה חוסך המון כסף, על כל מחשב שלא מקבל כתובת ציבורית משלו).

וכן יכול להיות NAT בצד של הסרבר.

ש. מה אליס צריכה בשביל להתחבר לרשת ? לפני בקשת DHCP

ת. כרטיס רשת, כתובת ip, get way, צריך לדעת מי הוא הDNS שלי, זמן (t), mask - באיזו רשת אני נמצא (כדי שאני אדע אם ה ip שאני שולח נמצא אצלי ברשת או לא).

ש. באיזה פרוטוקול נשתמש בצפייה בסרטון שנמצא אצל בוב ?

ת.. פרוטוקול UDP כיוון שהוא פחות אמין הוא יותר מהיר והוא נועד להעביר אובייקטים יותר גדולים.

ניתן להשתמש גם בפרוטוקול dash.

ש. אם בן אדם אחד מחובר לרשת ומבקש להתחבר לאתר, ואז בן אדם אחר הולך לאוניברסיטה נגיד, מחבר את המחשב ומבקש להתחבר לאותו אתר, מה ההבדל ?

והאם יכול להיות שניגש לip שונה?

ת. ההבדל בחלק הראשון זה שמי שמחובר ברשת ביתית לא יבקש בקשת DHCP ומי שרק חיבר תמחשב כן.

ויש מצב שילכו ל IP שונה, כי אולי יש העתק של העתק במקום קרוב יותר (chache).

ש. מה ההבדלים בין IPv4 ל IPv6?

ת..

- הגדלת מרחב הכתובות מ32 ביט ל128 ביט בIPv6 .
- IPv6 מהיר יותר בשליחת פאקטות כיוון שהheader שלו קצר יותר.
- בIPv6 אין יותר את השדות fragmentation/reassembly ולכן אם מגיעה חבילה גדולה יותר מהליק היוצא הראוטר פשוט יזרוק את החילה ושולח הודעת שגיאה.
- שדה ה options לא קיים ובמקום אחד מהאפשריות בפוינטרים next header כלומר ש TCP/UDP יכולים להיות הפרוטוקולים הבאים.

ש. אם הוא sniffer שנמצא ב dns איזה פאקטות הוא יסניף?

ת..

ש. מה יש ב header של ה Doh?

ת.. http, tcp, ip, eth ויש גם את ה dns .

ש. אם אליס ובוב מחוברים ברשת האם תשלח הודעת ARP אצל אליס?

ת. לא, כיוון שהודעת ARP זה פרוטוקול שעושה resolving מ IP ל MAC ולכן אם הם באותו רשת אין מה לשלוח הודעה כזו כי זה אותו IP כלומר יש להם את אותו הmac destination .

היא תשלח הודעה כאשר לא ידענו את הmac source ו mac destination.

לסיכום :

אם היא מחוברת לרשת היא יודעת מה הIP של הgateway שלה, אבל בשביל לדעת מה הMAC - היא צריכה ללכת לARP table

ואם זה לא נמצא בטבלה אז צריך להוציא הודעת ARP.

ש. אם יש שרת CDN איך זה משפיע על הבקשה לקבלת האתר ?

ת. CDN – נועד לבעלי התוכן (ל web server לדוגמא) והוא נותן לבעלי התוכן לשמור את התוכן בשרתים שקרובים ללקוחות שלהם ואז שהלקוח רוצה משהו הCDN אומר לו בוא קח את זה ממקום קרוב, אך יכול להיות שרת עם פחות עומס או שרת חדש.

ש. מה קורה כאשר ביצירת קשר יש הרבה איבוד פאקטות ?

ת.. יקח זמן להתחבר וההודעות ישלחו שוב.

ש. איך ניתן לדעת מה הרוחב פס ?

ת.. ע"י כרטיס הרשת שלך שיכול להיות מחובר לאחת מן המהירויות הבאות – 10/100/1000 mps.

הכרטיס צריך להיות מתואם לפרוטוקול ברשת בה הוא פועל – Ethernet, wifi וכו'.

ישנו מושג הנקרא צירוף חיבורים (**Link Aggregation**) ותפקידו הוא לאפשר חיבור של מספר כבלי Ethernet (LAN) במקביל כדי להגדיל את הרוחב פס.