

**המכללה האקדמית כנרת
ע"ש אלפרין בעמק הירדן**



סמל מוסד - 270538

פרויקט גמר

הנדסי תקשוב

בהתמחות: מערכות תקשוב

הנושא: הקמה פיתוח ותכנון חברת SoundSync

מנחת הפרויקט : סיון שי

מגיש/ה:

שם : ליאל אשריאן ת.ז. 326442886

תאריך ההגשה : מאי תשפ"ד

תוכן עניינים

1.....	תוכן עניינים
5.....	מבוא
7.....	אודות הפרויקט
8.....	תרשים ארגוני
9.....	מחלקות
11.....	מדייניות הקצאת שמות לרכיבי רשת
14.....	מדייניות חלוקת הכתובות של הסניפים
15.....	טבלת כתובות IP בסניפים
16.....	סניף ראשון ירושלים
18.....	Hostname
18.....	Shutdown
18.....	Banner MOTD (Message Of The Day)
19.....	VTP
23.....	VLANS
28.....	פרישת VLAN על כמה מתגים Trunk –
30.....	Router On A Stick – IEEE 802.1Q
32.....	STP
40.....	HSRP
44.....	DHCP
50.....	Port Security
55.....	EtherChannel
59.....	שרותים בסניף הראשון
62.....	HTTP
66.....	DNS Server
73.....	Mail
79.....	Syslog
83.....	NTP Server
87.....	FTP Server
94.....	TFTP Server
101.....	סניף 2 – תל אביב
103.....	VLAN בסניף השני
107.....	STP סניף 2
109.....	HSRP סניף 2
111.....	פרוטוקול DHCP סניף 2
114.....	Port Security סניף 2

116	שרתים בסניף השני
117	HTTP סניף 2
120	DNS Server
125	Mail
129	Syslog
131	NTP Server
133	FTP Server
137	TFTP Server
142	ניתוב
144	השוואה בין Link state ל Distance Vector
145	EIGRP
156	סניף 3
158	VLAN סניף 3
161	DHCP סניף שלישי
164	הגדרת כתובות IP בין הממשקים
166	Port-Security סניף 3
168	שרתים בסניף השלישי
169	HTTP סניף 3
172	DNS Server
176	Mail
180	Syslog
182	NTP Server
184	FTP Server
188	TFTP Server
193	OSPF
205	רשת רחבה WAN - חיבור בין הסניפים
206	פרוטוקול BGP
214	הגדרת OSPF, ISP , DSR בسانיפים
217	חיבור מטרו
219	NAT
224	GRE Tunnel
228	VPN
237	אייזורי stub
242	פרק 2 - אבטחת מידע
243	מוסגים באבטחת מידע
244	CIA
245	متפקידים איוםים ומנגנוני אבטחה :

245	Password attacks
246	DOS
246	DDOS
247	Spoofing
248	VLAN Hopping
249	MITM Attack
249	STP Attack
250	Sniffer
253	Wireshark
258	הצפנה
259	גיוב (Hash)
260	ACL
267	AAA
271	SSH
273	Firewall ASA
276	Dhcp Snooping
280	איתור תקלות ופתרון
282	צילום של הפרויקט :
286	רפלקציה
287	ביבליוגרפיה :

מבוא

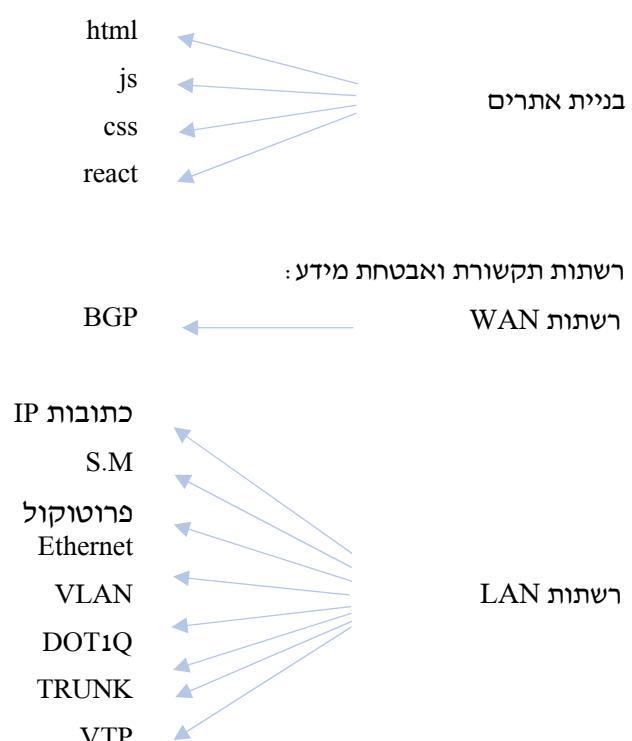
שמי ליאל אשריאן, בת 19 מכפר יונה. למדתי בתיכון איש שלום בכיתת מופת והרחבותי מגמותה תכנו ותוכנות מערכות (הנדסת תכנה סייבר), מדעי המחשב ופיזיקה. במסגרת המגמות והרבה למידה עצמית, התנסיתי במגוון שפות תכנות, מערכות הפעלה ובסיסי נתונים כדוגן

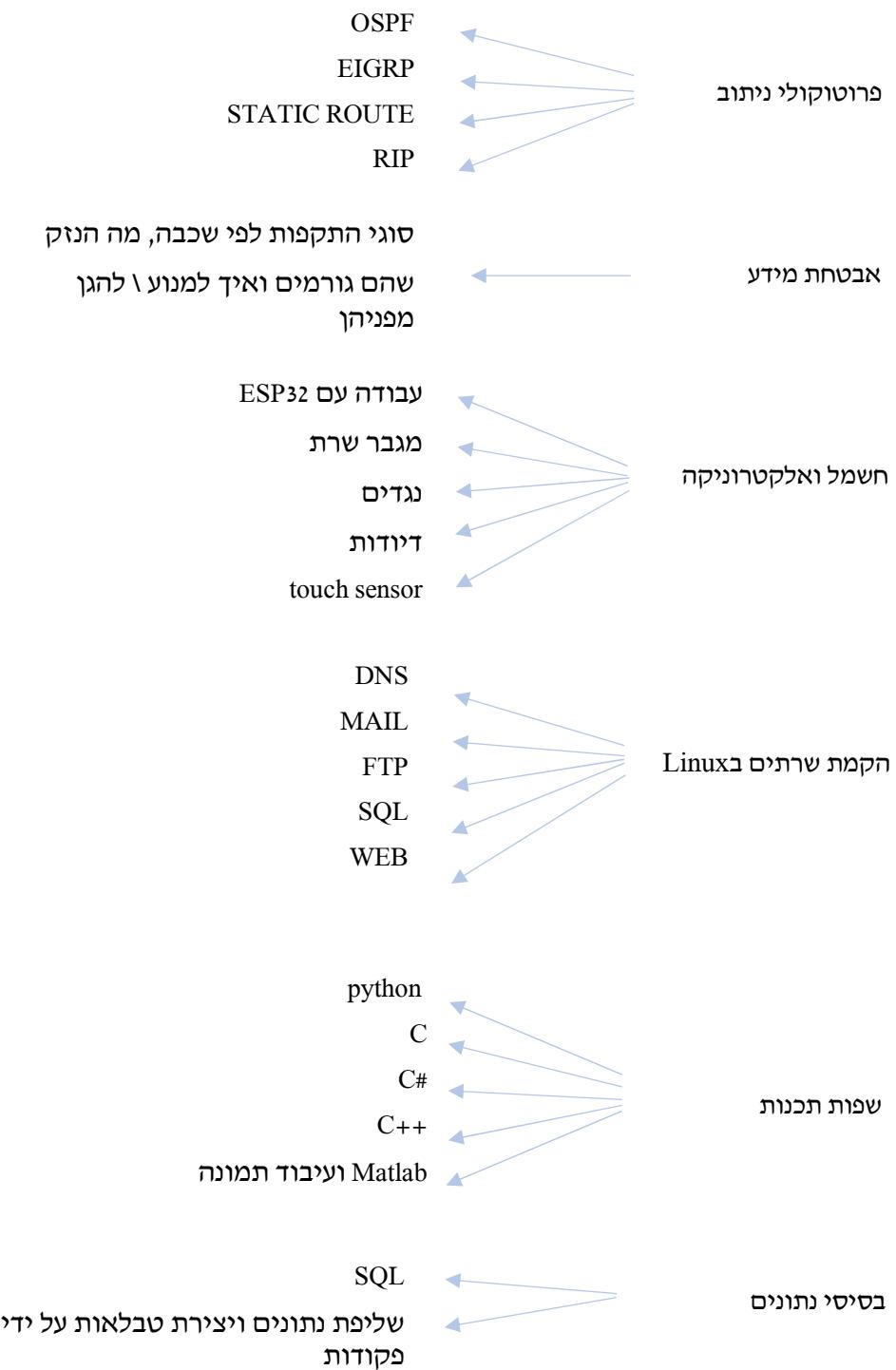
C	-
C#	-
JAVASCRIPT (Angular, react, Node.js, Typescript)	-
Python (cv2, threading, kivy, pygame, socket, learning machine)	-
Assembly	-
Linux (Ubuntu)	-
SQL	-
html	-

כיום אני סטודנטית במכיללת כנרת של לימודי תקשוב במסגרת העתודה הטכנולוגית בחיל האוויר. בזמן הלימודים אני מתוגדרת בקיבוץ אפיקים.

בעקבות המגמות רכשתי תשואה רבה למczęע ולעולם המחשבים והתוכנות. למדנו עבודה עם sockets ושם נחשמתי לראשונה לעולם רשתות התקשרות והבנתי שאני רוצה להרחיב וללמוד על עולם זה במטרה להבין יותר טוב כיצד המידע עובר. לכן המשכתי ללימודים במסגרת העתודה במטרה להעשיר את הידע שלי ולעשות שירות שימושתי בו יכולותיו יוכלו לבוא לידי ביטוי. לאחר הצבא אני מתכונת להשלים את לימודי לתואר הנדסת חשמל מחשבים ולבוד בתפקיד המשלב את עולם הרשותות והתוכנות.

במהלך לימודי במסגרת העתודה הטכנולוגית הרחבענו על עולם רשתות התקשרות ואבטחת המידע בנוסח לשפות תכנות נוספים, CISCOים וידע נוסף באלקטרוניקה בנושאים הבאים :





SoundSync

הינה חברת SoundSync מובילה בתחום טכנולוגיית המוזיקה, המתמחה במכשירים שמחוללים מהפכה בדרך שבה מוזיקאים ואנשי מקצוע באודיו משיגים איזון וסנכרון בקומפוזיציות שלהם. עם התמקדות בלתי פוסקת בשיפור האיכות והדיקוק של הסאונד, SoundSync הפכה לשם מהימן בתעשייה.

באמצעות טכנולוגיה מתקדמת ואומנות קפנית, SoundSync פיתחה מגוון של מכשירים פורציז דרכם המאפשרים למוזיקאים להעריך ולטב את האיזון של המוזיקה שלהם ללא מאץ. בין אם מדובר בעיבוד תזמורתי מורכב, מיקס רוק דינמי או הופעה אקוסטית אינטימית, המכשירים של SoundSync מספקים פתרונות מקיפים להשתתפות הרמונייה וסנכרון מושלמים.

מוצר הדגל של SoundSync, Harmony Analyzer, זכה לשבחים נרחבים בזכות יכולתו לנתח ולהמחיש את האיזון של רכיבי אודיו בזמן אמת. עם המשך האינטואיטיבי והאלגוריתמים העוצמתיים שלו, מוזיקאים יכוליםים כעת לקבל תובנות עמוקות לגבי התפלגות התדרים, הדינמיקה והמיקום המרחבית בתוך הקומפוזיציות שלהם, מה שמאפשר להם לכוון כל פרט ולהציג את האיזון הקולי הרצוי.

SoundSync זכתה לשבחים רבים, כולל פרס Innovation in Music Technology, הכרה בחתירה הבלטי פוסקת של החברה למציאות ומחייבות לדחינת הגבולות של מה שאפשר בתחום הערכת איזון השמע. מסירوتה של החברה למחקר ופיתוח הובילו למספר פטנטים ולהתקדמות פורצת דרך בתחום.

בנוסף להישגים הטכנולוגיים, SoundSync תרם תרומה משמעותית להקללת המוזיקה. החברה משתפת פעולה באופן פעיל עם מוזיקאים בולטים ואנשי מקצוע בתחום האודיו כדי לפזר את הגבולות של הפקה מוזיקלית והנדסת סאונד. ממצאי המחקר והפיתוח שלהם הביאו למספר פטנטים וחידושים פורציז דרכם שקידמו את התחום עוד יותר.

החברה הקומתית ירושלים ובעקבות ההצלחה הרבה וההתפתחותה בתעשייה, החברה התפתחה והוקמו סניפים נוספים של החברה בתל אביב וביון.

מנוע על ידי תשואה לשמלות אודיו, SoundSync נשאר בחזיות החדשנות, ומכשיריהם הפכו לבחירה הנכונה עבור אנשי מקצוע ברחבי העולם. מוזיקאים ידועים, מהנדסי אודיו ואולפני הקלטות אימצו את הטכנולוגיה המתקדמת של SoundSync כדי לנstor נופי סאונד שובי לב וסוחפים. מheyibudim התזמורתיים הגדולים ביותר ועד למיקסים אלקטרוניים מורכבים, SoundSync מעמידה אמנים להציג איזון וסנכרון יוצאי דופן, תוך פיתוח מחוות חדשנות של אפשרויות קוליות.

תרשים ארגוני :



מחלקות

פירוט התפקיד	KİÇOR	שם המחלקה
ניהול כלל המחלקות בחברה, לדאוג שהצווותים מסונכרים אחד עם השני, שהתפקידים נעשים כראוי, שיש מושל וモטיבציה לכל העובדים בחברה ופתרון אנשים במידה ולא מבצעים את תפקידם	MNG	Management
אחריות על פתרת תקלות ותחזוקת המחשבים בחברה. אחריות על תחזוקת הצוד בארגון ועל הרשותות הפנימיות בחברה	IT	IT Department
אחריות על סיפוק רשות אלחותית מאובטחת ומוגנת לחברת	WIFI	WIFI Department
אחריות על הבנת הצרכים של לקוחות ב מוצר ואילו התאמות יש לעשות על מנת שיעלה הצורך שלו בשוק. שיווק ויצירת קמפיין פרסום ועזרה בניתו מכירות החברה	MRKT	Marketing
מבררת את תהליכי החברה ואת העובדים בה ומסיקה מסקנות בנוגע למה ניתן לשפר בחברה ובאנשים על מנת לקדם ולסייע את החברה	CTRL	Control Department
אחריות על פיתוח התוכנות לארגון והפיכתם ליותר נגישים למשתמש, מאובטחים ויעילים. מכילה אנשי פיתוח (מתכנתים) וראשי צוותים האחראים על אנשי הפיתוח.	SFTW	Software Development
תכנן ועיצב מוצר בחברה, שייהו נגישים, נוחים לשימוש	DSGN	Design Department

ויפים לעין ואחראים גם על עיצוב האריזות		
אחראית לנושאים המשפטיים. כגון: רישום פטנטים, זכויות יוצרים תביעות והגנה על החברה.	LGL	Legal Department
אחראית על ניהול המערך הכספי, חלוקת התקציב הקיים בין משכורות העובדים, חומרם לעבודה ופיתוח שאר המחלקות בארגון	FNC	Finance Department
ספק עזרה וסיווע ללקוחות בכלל הקשרו לתמיכה טכנית באתר, בעיות עם המוצרים וחוכר ידע בנוגע למוצרים שאנו מספקים	CSTM	Customer Department
ביצוע הדרכה לעובדים החדשניים בחברה, עדכון העובדים הקיימים במורים, נתונים חדשים עליהם לדעת ואחראים על כך שלכל עובד יש את הידע הנדרש על מנת למלא את תפקידו בחברה	TRN	Training Department
תפקידה לחקור מה ניתן לעשות על מנת לשפר את המוצרים בחברה, איך ליישם את צרכי השוק ולהביא אותם לידי ביטוי במורים ובשירותים שאנו מספקים. לבדוק האם המוצרים שלנו בניוים ומוצגים בצורה האידיאלית ומה ניתן לשפר ולחשיך ממנה מסקנות לעתיד.	RSRC	Research Department

מדיניות הקצאת שמות לרכיבי רשת

סניף ראשון – ירושלים (JRS)

שם הרכיב	מיקום בטופולוגיה	קייזור	הסביר קיזור
PC		PC1-IT-JRS	<n> - number of pc in the department <VLAN> - Departments name
Switch 2960	Access	SW1-A-JRS SW2-A-JRS SW3-A-JRS	SW - Switch A - Access
Switch-PT-Empty	Distribution	SW1-D-JRS SW2-D-JRS	SW – Switch D - Distribution
Router 1941	Core	R1-C-JRS R2-C-JRS	R – Route C – Core
Server	DMZ	SRV<X>-<T>-GRC	SRV- Server

סניף שני - תל אביב (TLV)

שם הרכיב	מיקום בטופולוגיה	קייזור	הסבר קיזור
PC		PC1-IT-T; V	<n> - number of pc in the department <VLAN> - Departments name
Switch 2960	Access	SW1-A-TLV SW2-A-TLV SW3-A-TLV	SW - Switch A - Access
MultiLayer Switch 3650	Distribution	MLS1-D-TLV MLS2-D-TLV	MLS – MultiLayer Switch D - Distribution
Router 1941	Core	R1-C-TLV R2-C-TLV	R – Route C – Core
Server	DMZ	SRV<X>-<T>-TLV SRV1-DHCP-TLV SRV2-DHCP-TLV	SRV- Server <n> - Number <T> - Type

סניף 3 – יונן (GRC)

שם הרכיב	מיקום בטופולוגיה	קייזור	הסביר קייזור
PC		PC< n >-< VLAN >-GRC PC1-IT-GRC	< n > - number of pc in the department < VLAN > - Departments name
Switch 2960	Access	SW1-A-GRC SW2-A-GRC SW3-A-GRC	SW - Switch A - Access
MultiLayer Switch 3650	Distribution	MLS1-D-GRC MLS2-D-GRC	MLS – MultiLayer Switch D - Distribution
Router 1941	Core	R1-C-GRC R2-C-GRC	R – Route C – Core
Server	DMZ	SRV< X >-< T >-GRC	SRV- Server

מדיניות חלוקת כתובות של הסניפים

כתובות IPv4 מורכבות מ4 אוקטוטות. כל אוקטטה בגודל בית אחד כולל 8 ביט. (סה"כ 4 בית – 32 בית).
את כתובות ה-IP של שני הסניפים הראשונים חילקתי בהתאם לתבנית הנ"ל:

אוקטטה מס' 1

זהה בכל הסניפים : X.X.X.10

אוקטטה מס' 2

מייצגת את מספר הסניף :

10.1.X.X	Jerusalem	סניף 1
10.2.X.X	Tel Aviv	סניף 2

אוקטטה מס' 3

מייצגת את מספר ה-VLAN של המחלקה. לדוגמה : X.81.2.10

אוקטטה מס' 4

מייצגת את מספר המחשב באותה VLAN. לדוגמה : 5.92.3.10

בסניף מס' 3 חלוקת כתובות IP מותבוצעות באופן שונה:

אוקטטה מס' 1 +2

X.X.168.192

אוקטטה מס' 3

מייצגת את מספר ה-VLAN של המחלקה. לדוגמה : X.81.168.219

אוקטטה מס' 4

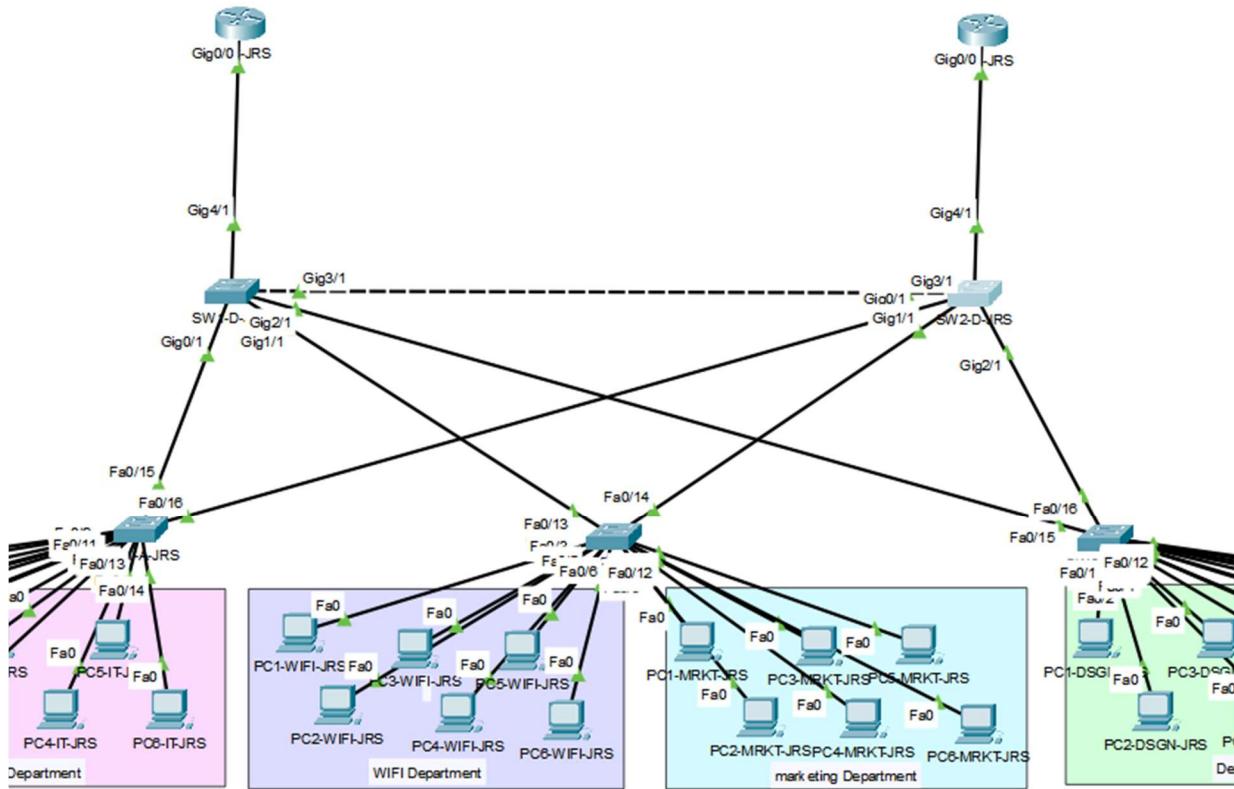
מייצגת את מספר המחשב באותה VLAN. לדוגמה : 5.92.168.192

192.168.X.X	Greece	סניף 3
-------------	--------	---------------

טבלת כתובות IP בסניפים

D.G	S.M	כתובות	כמויות מחשבים VLAN	VLAN Id	סניף
10.1.26.254	255.255.255.0	10.1.26.X	8	26	Jerusalem
10.1.36.254	255.255.255.0	10.1.37.X	6	37	
10.1.48.254	255.255.255.0	10.1.48.X	6	48	
10.1.59.254	255.255.255.0	10.1.59.X	6	59	
10.1.70.254	255.255.255.0	10.1.70.X	8	70	
10.1.81.254	255.255.255.0	10.1.81.X	6	81	
10.2.11.254	255.255.255.0	10.2.8.X	6	8	Tel Aviv
10.2.32.254	255.255.255.0	10.2.19.X	6	19	
10.2.53.254	255.255.255.0	10.2.30.X	6	30	
10.2.64.254	255.255.255.0	10.2.41.X	6	41	
10.2.85.254	255.255.255.0	10.2.52.X	6	52	
10.2.78.254	255.255.255.0	10.2.63.X	6	63	
192.168.10.254	255.255.255.0	192.168.10.X	6	39	Greece
192.168.20.254	255.255.255.0	192.168.20.X	6	50	
192.168.30.254	255.255.255.0	192.168.30.X	6	61	
192.168.40.254	255.255.255.0	1192.168.40.X	6	72	
192.168.50.254	255.255.255.0	192.168.50.X	6	83	
192.168.60.254	255.255.255.0	192.168.60.X	6	94	

סניף ראשון ירושלים



תחת הסניף הראשון אסבירות על רוב הпрוטוקולים אשר יוגדרו בפרויקט ביחד עם פקודות show והגדנות שבאו לידי ביתוי בסניף. בסניף השני והשלישי ארכיב על פרוטוקולים אשר נמצאים בסניפים אלו בלבד ויחודיים להם.

המחלקות בסניף:

WIFI VLAN 48	IT – Vlan 37	Management – Vlan 26
<p>WIFI VLAN 48</p> <p>WIFI Department</p> <ul style="list-style-type: none"> PC1-WIFI-JRS PC2-WIFI-JRS PC3-WIFI-JRS PC4-WIFI-JRS PC5-WIFI-JRS PC6-WIFI-JRS 	<p>IT – Vlan 37</p> <p>IT Department</p> <ul style="list-style-type: none"> PC1-IT-JRS PC2-IT-JRS PC3-IT-JRS PC4-IT-JRS PC5-IT-JRS PC6-IT-JRS 	<p>Management – Vlan 26</p> <p>Management</p> <ul style="list-style-type: none"> PC1-MNG-JRS PC2-MNG-JRS PC3-MNG-JRS PC4-MNG-JRS PC5-MNG-JRS PC6-MNG-JRS PC7-MNG-JRS PC8-MNG-JRS
Customer Service – VLAN 81	Marketing – VLAN 70	Design – VLAN 59
<p>Customer Service – VLAN 81</p> <p>Customer Service</p> <ul style="list-style-type: none"> PC1-CSTM-JRS PC2-CSTM-JRS PC3-CSTM-JRS PC4-CSTM-JRS PC5-CSTM-JRS PC6-CSTM-JRS 	<p>Marketing – VLAN 70</p> <p>Marketing</p> <ul style="list-style-type: none"> PC1-MRKT-JRS PC2-MRKT-JRS PC3-MRKT-JRS PC4-MRKT-JRS PC5-MRKT-JRS PC6-MRKT-JRS 	<p>Design – VLAN 59</p> <p>Design Department</p> <ul style="list-style-type: none"> C1-DSGN-JRS PC2-DSGN-JRS PC3-DSGN-JRS PC4-DSGN-JRS PC5-DSGN-JRS PC6-DSGN-JRS PC7-DSGN-JRS PC8-DSGN-JRS

Hostname

פקודה המאפשרת שינוי / הגדרה של שם ייחודי לרכיבי הרשת. מיושמת על מתגים ונתבים במטרה לזיהות את המכשיר ברשת וליצור הבדלה בין רכיבי רשת שונים בסניף, זאת על מנת לאתר תקלות, ולהחיל הגדרות חדשות ועדכוניות נוספים.

מבנה הפקודה :

hostname [name]
השם אליו נרצה לשנות

הגדרת שם למtag בשכבה Access בסניף הראשון :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1-A-JRS
SW1-A-JRS(config)#
שינוי השם לשונו
```

Shutdown

פקודה המאפשרת לכבות ולהפעיל ממשייקים (interfaces). כבירתת מחדל, כל הממשאים במtag דלוקים כל עוד לא הוגדר עליהם אחרת ובנinet כל הממשאים כבויים כל עוד לא הוגדר עליהם אחרת.

על מנת להגדיר פקודה זו, יש להיכנס לממשק הרצוי :

interface [interface's type] [interface's number]
 סוג הממשק
 shutdown / no shutdown
הדלקת הממשק כיבוי ממشك

הדלקת פורט בנinet בסניף הראשון :

```
R2-C-JRS(config)#int gigabitEthernet 0/0
R2-C-JRS(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
כנית לממשק הדלקת הממשק
```

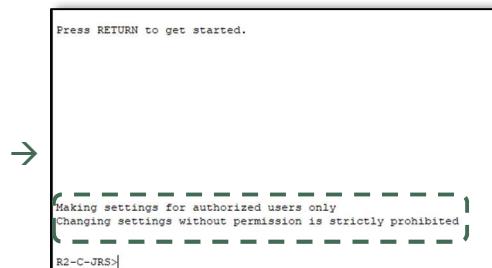
Banner MOTD (Message Of The Day)

הודעה המוצגת בעת כניסה לנinet או מtag דרך חיבור מרוחק (SSH / Telnet) או דרך חיבור בכבלי console. לרוב משתמשים במטרה לידע את המשתמש כי הכניסה למכשיר זה אינה למורים בלבד והשימוש במכשיר ללא אישור הינה השגת גבול.

הודעה שתופיע בעת העלאת המtag/ninet. ההודעה חייבת להתחיל ב-טו מסויים.

לדוגמה @ (ולהסתומים באותו טו)

```
R2-C-JRS(config)#banner motd $
Enter TEXT message. End with the character '$'.
Making settings for authorized users only
Changing settings without permission is strictly prohibited.
$
```



Vlan Trunking Protocol

פרוטוקול קנייני של חברת Cisco הפועל בשכבה 2 במטרה לנוהל תצורות VLAN (Virtual Local Area) על פניו מטגים. הוא מפשט את ניהול ה-VLAN על ידי מתן אפשרות למטרים לשתף מידע באופן אוטומטי. השימוש בו עוזר לשמר על עקביות ומצמצם מאמצי תצורה ידניים ברחבי הרשת. ב프וטוקול VTP נגידר על מטג אחד את כל הגדרותיהם והם יסונכרנו עם שאר המטגים.

מצבי המטג ב-VTP:

- **שרת Server:** מצב בריית המחדר של המטג, מאפשר ליצור, לשנות ולמחוק רשתות VLAN על המטג. מטגים במצב server מפרסמים את מסד הנתונים של ה-VLAN שלהם למטרים אחרים בתחום ה-VTP. הגדרות יסונכרנו עם שאר המטגים באותו אזור.
- **לקוח Client:** מטgi מקבלים הגדרות ועדכוני VTP משרותם ומישימים אותם עליהם. אינם יכולים לבצע שינויים במסד הנתונים של VLAN כמו ליצור לשנות ולמחוק, ככלומר הם לוקחים את הגדרות השרת ומישימים זאת על עצמם.
- **שקוף Transparent:** מטגים שקופים אינם משתמשים בעדכוני VTP אך יכולים להעביר עדכנים למטרים אחרים. הם יכולים ליצור ולשנות רשתות VLAN באופן מקומי. ככלומר, הגדרות server אינם חלים עליהם והם יכולים ליצור לשנות ולמחוק לעצם, אך הם מעבירים את הגדרות server הלאה.

פרמטרים החיביים להיות זהים בכלל המטגים:

- Vtp domain – השינויים שנעים בserver vtp רק על המטגים הנמצאים באותו הדומיין.
- Vtp password – עדכנים נשלחים רק למטרים בעלי אותה מערכת סיסמה כמו של ה-server vtp.

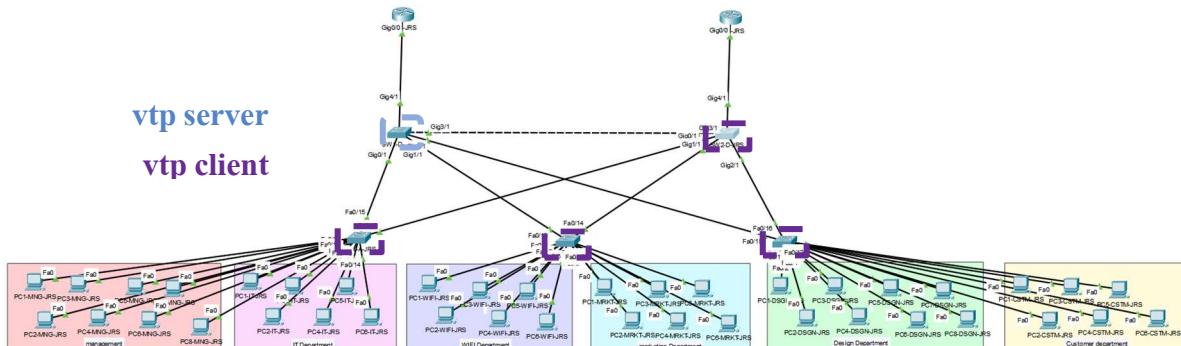
***הערה** – על המטגים להיות מחוברים ב-Trunk כדי לאפשר שיתוף מידע (הרחבה על פקודה זו בהמשך)

על מנת להשתמש ב프וטוקול, נגידר מטג אחד כ-server ואת האחרים כ-client/transparent. נגידר על כולם vtp password וזיהים. כל מטג מעדכן את מספר השינויים שנעשו עליו ובנוסף הפרוטוקול מעדכן את שאר המטגים על כמות השינויים שנעשו ב-VTP Server (נשמר בפרמטר CR)

סוגי הודעות בפרוטוקול VTP:

- **שרתti VTP מפרסמים כל 300 שניות \ בכל פעם שמתՐחש שינוי** . סיכום על ההגדאות שהתרחשו ב-VTP Server. ההודעה מכילה את שם התחום ומספר revision . כאשר מטג מקבל הודעה מסוג זה, הוא משווה את שם התחום והמספר. אם שיק לאותו תחום, יבדוק האם קיימות הגדרות עדכניות יותר מאשר שנמצאים אצלו, אם כן יבקש עדכון מפורט על ידי הודעה Advertisement Request .
- **שלוחת כאשר מטג במצב Client אופס \ איבד מידע לגבי ה-VLAN \ Advertisement Request** . קיבל Summary Advertisement עם מספר גובה יותר מאשר , ולכן נדרש עדכון בנוגע להגדרות, שינויים ולמידע שחרר לו.
- **שלוח על ידי שרת VTP לאחד שמתՐחש שינוי בהגדרות ה-VLAN . Subset Advertisement** . מכיל את השינויים הספציפיים שבוצעו בגוון הוספה שינוי שם \ מחיקה של VLAN .

הגדרת VTP בסטטוס הראשוני :JRS



גדרה בין כל המתגים (הרחבה על פקודה זו בהמשך)

```

SW1-D-JRS(config)#int gigabitEthernet 0/1           ← הגדרת המתג כ trunk
SW1-D-JRS(config-if)#switchport mode trunk          ← הגדרת המתג כ trunk

SW1-D-JRS(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
  
```

הגדרת VTP Server

```

SW1-D-JRS(config)#vtp mode server           ← vtp server
Device mode already VTP SERVER.
SW1-D-JRS(config)#vtp domain JRS           ← הגדרת שם דומיין
Changing VTP domain name from NULL to JRS
SW1-D-JRS(config)#vtp password proj        ← הגדרת סיסמא
Setting device VLAN database password to proj
  
```

הגדרת VTP Client

```

SW2-D-JRS(config)#vtp mode client           ← vtp client
Setting device to VTP CLIENT mode.
SW2-D-JRS(config)#vtp domain JRS           ← הגדרת שם דומיין
Changing VTP domain name from NULL to JRS
SW2-D-JRS(config)#vtp password proj        ← הגדרת סיסמא
Setting device VLAN database password to proj
  
```

show commands

מציג ספירה של הודעות : [show vtp counters](#)

הציג הסיסמה של הודאות : [show vtp password](#)

מציג את מצב הVTP לפני ולאחר יציאת VLAN בمبرכים של שרת ולקוח. : [show vtp status](#)

show vtp counter

```
SW1-D-JRS#show vtp counters
VTP statistics:
Summary advertisements received : 46 ← הודיעות שהתקבלו
Subset advertisements received : 34 ← הודיעות שהועברו
Request advertisements received : 19 ← שגיאות
Summary advertisements transmitted : 25 ←
Subset advertisements transmitted : 25 ←
Request advertisements transmitted : 0 ←
Number of config revision errors : 7 ←
Number of config digest errors : 0 ←
Number of Vl summary errors : 0 ←

VTP pruning statistics:
Trunk          Join Transmitted Join Received      Summary advts received
from           non-pruning-capable device
```

show vtp password

```
SW1-D-JRS#show vtp password
VTP Password: proj
```

vlans לפני הוספת server **show vtp status**

```
SW1-D-JRS#show vtp status
VTP Version : 1 ← VTP גרסה
Configuration Revision : 0 ← CR
Maximum VLANs supported locally : 255 ← מקסימום vlans הנOMICIM
Number of existing VLANs : 5 ← כמות vlans קיימים
VTP Operating Mode : Server ← מצב המתג
VTP Domain Name : JRS ← הדומין בו נמצא המתג
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xC3 0x7F 0xE3 0xB8 0xB1 0x96 0x49 0x7D
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

vlans לפני הוספת client **show vtp status**

```
SW2-D-JRS#show vtp status
VTP Version : 1
Configuration Revision : 0 ← לא נוצרו עדין שינויים
Maximum VLANs supported locally : 255
Number of existing VLANs : 5 ←
VTP Operating Mode : Client ← client במצב
VTP Domain Name : JRS
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xC3 0x7F 0xE3 0xB8 0xB1 0x96 0x49 0x7D
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

vlans אחרי הוספת server show vtp status

```
SW1-D-JRS#show vtp status
VTP Version : 1
Configuration Revision : 12 ← כמות השינויים
Maximum VLANs supported locally : 255 ← שונצרו הוספה
Number of existing VLANs : 11 ← יילאים + נתינת שם
VTP Operating Mode : Server
VTP Domain Name : JRS
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xFA 0xCA 0x2D 0x85 0xA5 0x83 0xA4 0x21
Configuration last modified by 0.0.0.0 at 3-1-93 00:44:15
Local updater ID is 0.0.0.0 (no valid interface found)
SW1-D-JRS#
```

vlans אחרי הוספת client show vtp status

```
SW2-D-JRS#show vtp status
VTP Version : 1
Configuration Revision : 12 ← ← השינויים התעדכנו
Maximum VLANs supported locally : 255 ← ← clients
Number of existing VLANs : 11
VTP Operating Mode : Client
VTP Domain Name : JRS
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xFA 0xCA 0x2D 0x85 0xA5 0x83 0xA4 0x21
Configuration last modified by 0.0.0.0 at 3-1-93 00:44:15
```

Virtual Local Area Network

רשתות VLAN (Virtual Local Area Network), הן רשתות וירטואליות שנוצרות מרשת מקומית אחת או יותר. מאפשרות לקבוצת רכיבי קצה הקיימים במספר רשות להשתלב כרשת לוגית אחת אשר מנוהלת כמו רשת פיזית מקומית. מטרת ה Vlan הינה לחסוך שימוש של רשתות פיזיות רבות. כך, יוכל להגדיר לכל מחלקה רשת וירטואלית משל עצמה במקום להגדיר להן רשתות בקרה פיזית.

יתרונות של שימוש בVLAN :

- **אבטחת רשת משופרת :** רשתות VLAN מספקות אבטחת רשת משופרת על ידי בידוד ומידור של נתונים רגילים והגבלה גישה בין רשתות VLAN, מה שמחזיא את הסיכון לגישה לא מורשית.
- **ניהול תנוצה יעיל :** על ידי חלוקת הרשות לרשתות VLAN, חל צמצום בעומס ברשות ולSHIPOR ביצועי הרשות הכלולים.
- **ניהול רשת בקרה פשוטה :** רשתות VLAN מאפשרות ניהול רשת פשוט יותר על ידי מתן אפשרות ניהול קבוצות של מכשירים בנפרד ושיפור ניהול הרשות הכלול.
- **גמישות ומדריגות :** רשתות VLAN מציעות גמישות ומדריגות, המאפשרות לרשתות להסתגל לצרכים המשתנים על ידי הוספה או הסרה בקלות של התקנים מרשתות VLAN ללא צורך בשינויים פיזיים ברשות.
- **יעילות עלות :** רשתות VLAN יכולות ליעל את משאבי הרשות ולהפחית את הצורך בתשתיות פיזית נוספת (חומרה), וכתוכאה מכך לחסכו בעלות על ידי ניצול יעיל יותר של תשתיות הרשות הקיימת.
- **פתרון בעיות רשת פשוטות :** השימוש ב - VLAN מפשט את פתרון בעיות הרשות על ידי לוקלייזציה של בעיות רשת לרשתות VLAN ספציפיות, מה שמאפשר זיהוי מהיר יותר ופתרון בעיות.

סוגי VLAN :

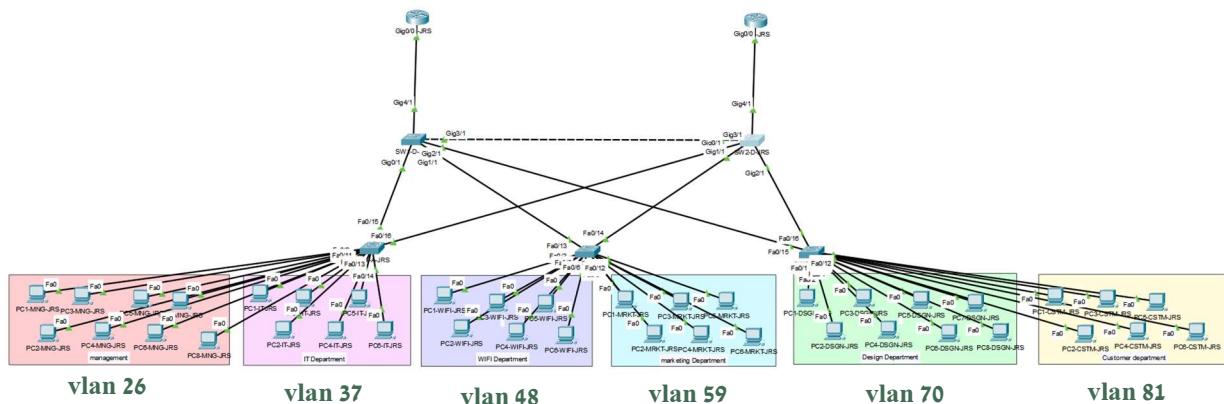
- **Native VLAN – VLAN Default :** ברירת מחדל (Native VLAN) הוא מוגדר על כל ה포רטים אוטומטית. מה שמייחד אותו משאר ה- VLANS זה שלא ניתן לשנות את שמו או למחוק אותו.
- **VLAN - VLAN Data :** המשמש לחלוקת הרשות לשתי קבוצות, קבוצת מכשירים וקבוצת משתמשים. התת רשת הזו (User VLAN) משמשת למעבר מידע שנוצר רק על ידי משתמשים.
- **VLAN – VLAN Management :** המשמש לגישה ליכולות ניהול של המתג כמו לוגים של המערכת. כברירת מחדל 1 VLAN מוגדר כ- VLAN Management אך ניתן להגדיר כל VLAN אחר.
- **הפס מלא .** מומלץ להגדיר את VLAN זה להיות מבטיח שניitan יהיה לתקשר עם המתג גם כאשר רוחב הפס מלא.

- **Vlan - VLAN Voice**
 והוא מאפשר להעביר תובורת קול. הוא מאפשר תובורת שידור גבוהה
 והוא בעל עדיפות לעומת תובורת רשת רגילה. יש צורך להפריד את התובורת ל- VLAN נפרד
 שכן כך ישמר רוחב פס גם לתובורת נוספת.

- **VLAN Native**
 זהו VLAN המשויך רק ל-Trunk פורט והוא משמש לזיהוי תובורת מידע
 המגיע מהפורט ולאינו משוייך לשום VLAN. מומלץ להגדיר את ה-VLAN הזה על VLAN
 שאינו בשימוש כי המידע עלול להיות סכנת אבטחה.

- **VLAN Hole Black**
 זהו VLAN שלא מאפשר תובורת ממנו. מגדירים את כל הפורטים שלא
 בשימוש עליו, כך אם יש פורט שמתחבר אליו מכשיר לмерות שאינו היה אמור להת לחבר, לא תהיה
 אפשרות למכשור החדש לתקשר עם הרשות הקיימת והוא מחובר ל- VLAN אחרת.

הגדרת VLAN בסניף הראשוני: JRS



הגדרת כל VLAN במתג VLAN Server

```
SW1-D-JRS (config) #vlan 26
SW1-D-JRS (config-vlan) #name MNG
```

יצירת VLAN
 נתינת שם

show Commands

: מציג מידע על VLAN באופן מצומצם show vlan brief

: מציג מידע על VLAN באופן מורחב show vlan

: מציג מידע על VLAN ספציפי על פי מספרו show vlan id <VLAN-ID>

: מציג מידע על VLAN ספציפי לפי שמו show vlan name <VLAN-Name>

show vlan brief

SW1-A-JRS#show vlan brief			
VLAN Name	Status	Ports	
1 default	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2	
26 MNG	active		
37 IT	active		
48 WIFI	active		
59 DGN	active		
70 MRKT	active		
81 CSTM	active		
100 dmz	active		
101 DMZ-B	active		
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddinet-default	active		
1005 trnet-default	active		

vlans נוצרו

SW1-D-JRS#show vlan brief			
VLAN Name	Status	Ports	
1 default	active		
26 MNG	active		
37 IT	active		
48 WIFI	active		
59 DGN	active		
70 MRKT	active		
81 CSTM	active		
100 dmz	active		
101 DMZ-B	active		
1002 fddi-default	active		
1003 token-ring-default	active		
1004 fddinet-default	active		
1005 trnet-default	active		

show vlan id <VLAN-ID>

SW1-A-JRS#show vlan id 26							
מספר VLAN		שם VLAN					
VLAN Name		Status	Ports				
26 MNG		active					
VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode Transl Trans2
26 enet	100026	1500	-	-	-	-	0 0

show vlan name <VLAN-Name>

SW1-A-JRS#show vlan name IT							
VLAN Name		Status	Ports				
37 IT		active					
VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode Transl Trans2
37 enet	100037	1500	-	-	-	-	0 0

show vlan

SW1-A-JRS#show vlan										
VLAN	Name	Status	Ports							
1	default	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2							
26	MNG	active								
37	IT	active								
48	WIFI	active								
59	DGN	active								
70	MRKT	active								
81	CSTM	active								
100	dmz	active								
101	DMZ-B	active								
1002	fddi-default	active								
1003	token-ring-default	active								
1004	fddinet-default	active								
1005	trnet-default	active								
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
26	enet	100026	1500	-	-	-	-	-	0	0
37	enet	100037	1500	-	-	-	-	-	0	0
48	enet	100048	1500	-	-	-	-	-	0	0
59	enet	100059	1500	-	-	-	-	-	0	0
70	enet	100070	1500	-	-	-	-	-	0	0
81	enet	100081	1500	-	-	-	-	-	0	0

שיוך פורטים ל-VLANs

```

SW1-A-JRS(config)#interface range fastEthernet 0/1-8 | ← כנישה לממשק
SW1-A-JRS(config-if-range)#switchport mode access | ← מעבר למצב access
SW1-A-JRS(config-if-range)#switchport access vlan 26 | ← שיוך החנות לממשקים
SW1-A-JRS(config-if-range)#interface range fastEthernet 0/9-14
SW1-A-JRS(config-if-range)#switchport mode access
SW1-A-JRS(config-if-range)#switchport access vlan 37

```

בדיקה שהפורטים שייכו:

VLAN Name	Status	Ports
1 default	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
26 MNG	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8
37 IT	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14
48 WIFI	active	
59 DGN	active	
70 MRKT	active	
81 CSTM	active	
100 dmz	active	
101 DMZ-B	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

ניתן לראות שהמשקדים שייכו

פרישת VLAN על כמה מותגים – Trunk

על מנת שהמותג ידע לאן ה-frame אמור לחדוד ובו לאיזה VLAN הוא שייך. Trunk protocol מוסיף tag , header frame המכיל בתוכו את מספר VLAN id . כאשר מותג אחר מקבל את ה-frame, הוא קורא את ה-id VLAN שנמצא בתוך header ובעורתו, יודע לאיזה VLAN שוייך ולאן להעביר אותו. הגדרת Trunk יכולה להיעשות בモתג בלבד.

פרוטוקולים המאפשרים Trunk :

- Inter- switch Link (ISL) נוצר על ידי סיסקו, ביום איינו נתמך בחלוקת מהמותגים החדש של

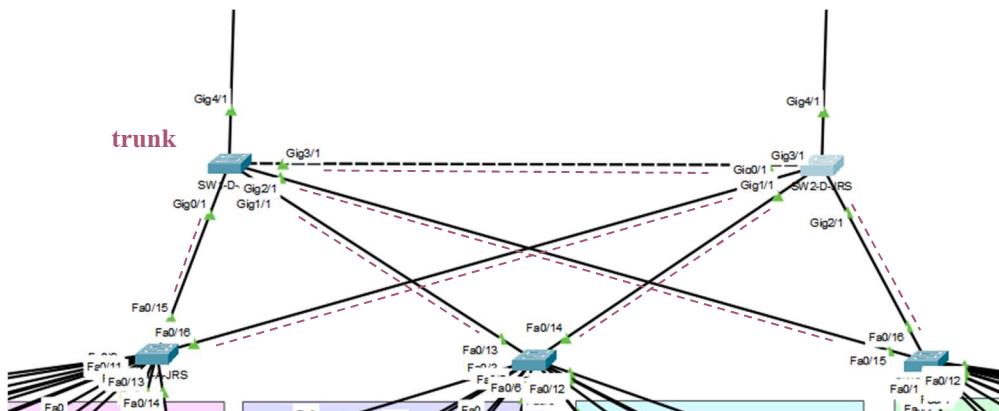
סיסקו והפרוטוקול כמעט ואינו בשימוש.

- IEEE 802.1Q הfrtocol המשמש כברירת מחדל אצל רוב המותגים.

לפננו של מותג שייצרת Trunk בצורה אוטומטית בין שני מותגים. **DTP (Dynamic Trunk Protocol)**

כלומר על מנת שייווצר חיבור מסווג trunk בין שני מותגים, ניתן להגדיר את מצב זה על ממושך של מותג אחד והגדרת סוג החיבור תISONCARO עם המושך של המותג השני.

הגדרת Trunk במתג בסנייף הראשון : JRS



```
SW1-D-JRS(config) #int gigabitEthernet 0/1
SW1-D-JRS(config-if) #switchport mode trunk
```

כניסה למושך

מעבר למצב trunk

Show command

- בדיקת הגדירות Trunk במתג show interfaces trunk

show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Gig0/1	auto	n-802.1q	trunking	1 הוגדר על הממשק
Gig1/1	auto	n-802.1q	trunking	1 במתג השני
Gig2/1	on	802.1q	trunking	1 וווגדרתו Trunk
Gig3/1	on	802.1q	trunking	1 סונכרנה
Gig4/1	on	802.1q	trunking	
Gig5/1	on	802.1q	trunking	

n = negotiated

Port	Vlans allowed on trunk	מצב הממשק trunk	הוגדר על trunk ממשק זה trunk
Gig0/1	1-1005		
Gig1/1	1-1005		
Gig2/1	1-1005		
Gig3/1	1-1005		
Gig4/1	1-1005		
Gig5/1	1-1005		

Port	Vlans allowed and active in management domain
Gig0/1	1,26,37,48,59,70,81,100,101
Gig1/1	1,26,37,48,59,70,81,100,101
Gig2/1	1,26,37,48,59,70,81,100,101
Gig3/1	1,26,37,48,59,70,81,100,101
Gig4/1	1,26,37,48,59,70,81,100,101
Gig5/1	1,26,37,48,59,70,81,100,101

Port	Vlans in spanning tree forwarding state and not pruned
Gig0/1	1
Gig1/1	1,26,37,48,59,70,81,100,101
Gig2/1	1,26,37,48,59,70,81,100,101
Gig3/1	1,26,37,48,59,70,81,100,101
Gig4/1	1,26,37,48,59,70,81,100,101
Gig5/1	1,26,37,48,59,70,81,100,101

Router On A Stick – IEEE 802.1Q

פרוטוקול המאפשר תקשורת בין VLANים אחד מהשני. מטרת ה VLAN היא לחלק את הרשות לרשותות וירטואליות שונות ולכון ללא פרוטוקול זה, מחשבים אשר אינם מצויים באותו רשות וירטואלית, לא יוכל לתקשר אחד עם השני. ב프וטוקול זה, נחלק את המשק הפיזי לתתי משקדים וירטואליים, בעלי כתובות IP (Default Gateway) ייחודיות לכל VLAN ובכך יוכל שני מכשירים אשר אינם מצויים בשרות וירטואליות שונות לתקשר דרך משק בודד ולהשוך בחיבור נפרד על גבי משקדים פיזיים בראטור.

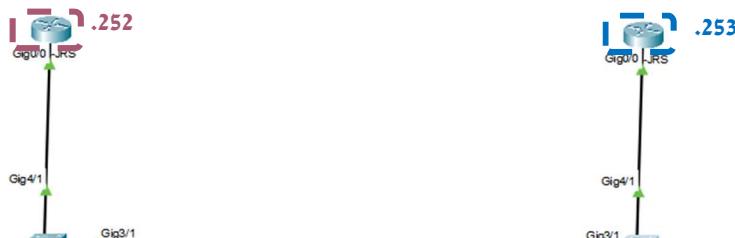
תקשרות בין VLANים – פרוטוקול 802.1Q

על מנת לאפשר תקשורת בין מכשירים הנמצאים ב VLAN שונה, יש צורך בהתקן שעובד בשכבה שלוש – נתב או switch 3 layer

הערות להגדירת dot1q :

- אין להגדיר כתובות IP על המשק הראשי, אלה רק על תת-המשקדים
- יש להדילק את המשק הראשי (no shutdown)

הגדרת dot1q בסינייף הראשוני JRS:



- הערכה* - במצב בו מחובר נתב אחד לרשות, נשים במקום של הכתובת default gateway של הרשות. במצב בו מחוברים שני נתבים או יותר, נשים בכל אחד מהנתבים בפקודת ה- address IP כתובות שונות מה - d.g. ולבסוף נאחד אותם לכתובת וירטואלית אחת באמצעות פרוטוקול HSRP עליו ארchip במכשיר. זאת מכיוון שלא ניתן להגדיר אותה כתובות ל-2 נתבים באותה הרשות על מנת להימנע ממצב בו המותג לא ידע לאיזה נתב להעביר את הפריים.

במוגן:

מעבר את המשק המחבר בין נתב לנתב למצב Trunk :

```
SW1-D-JRS (config)#int gigabitEthernet 4/1           ← כניסה לממשק
SW1-D-JRS (config-if)#switchport mode trunk          ← מעבר למצב Trunk
```

בנתב:

נכנס לתת המשק

נשייך אותו ל VLAN וניתן לו כתובות IP ו.m.s. מתאימים

```
R1-C-JRS (config)#int gigabitEthernet 0/0.26           ← vlan
R1-C-JRS (config-subif)#encapsulation dot1Q 26          ← dot1q
R1-C-JRS (config-subif)#ip address 10.1.26.252 255.255.255.0 ← נתינת כתובות IP
```

show Commands

vlans – פקודה המראה את כל הגדירות שבוצעו על הנטב \ המtag (במtag לא כולל הגדירות (vtp)

מציגה סיכום של כל הממשקים (interfaces) שבנתב ומציגה מידע על כל אחד מהם.

show run

```
interface GigabitEthernet0/0.26
encapsulation dot1Q 26
ip address 10.1.26.252 255.255.255.0
!
interface GigabitEthernet0/0.37
encapsulation dot1Q 37
ip address 10.1.37.252 255.255.255.0
!
interface GigabitEthernet0/0.48
encapsulation dot1Q 48
ip address 10.1.48.252 255.255.255.0
!
interface GigabitEthernet0/0.59
encapsulation dot1Q 59
ip address 10.1.59.252 255.255.255.0
!
interface GigabitEthernet0/0.70
encapsulation dot1Q 70
ip address 10.1.70.252 255.255.255.0
!
interface GigabitEthernet0/0.81
encapsulation dot1Q 81
ip address 10.1.81.252 255.255.255.0
```

הגדירות
שהוגדרו

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	NVRAM	up	up
GigabitEthernet0/0.26	10.1.26.252	YES	manual	up	up
GigabitEthernet0/0.37	10.1.37.252	YES	manual	up	up
GigabitEthernet0/0.48	10.1.48.252	YES	manual	up	up
GigabitEthernet0/0.59	10.1.59.252	YES	manual	up	up
GigabitEthernet0/0.70	10.1.70.252	YES	manual	up	up
GigabitEthernet0/0.81	10.1.81.252	YES	manual	up	up

ניתן לראות
ששתאי
המשקדים
קיבלו את IP

כתובת IP

Spanning Tree Protocol

פרוטוקול לניטור ומוניטור לולאות בשכבה 2

כאשר מtag מקבל מסוג Frame Broadcast, הוא ישדר אותו דרך כל הממשקים המחברים אליו חוץ מההארט interfaceno נכנס ה-frame. אין מגנו TTL (time to live) כמו בframe, ולכן ה-frame ישדר בין המתגים ללא סוף, וכך את כל רוחב הפס ועלול לגרום להשבחת הרשת.

stp הינו פרוטוקול שמטרתו לאתר את לולאות אלו ולמנוע אותם.

על מנת לגלוות לולאות מיתוג ברשת, המtag שולח כל 2 שניות BPDU Packet. אם הפקטה חוזרת למtag דרך ממשך אחר זה אומר שיש לולאה וצריך לסגור אותה.

גרסאות:

- stp – הסטנדרט הראשון, יצא בשנת 1993. הפרוטוקול עובד בשכבה השנייה במודול OSI לפוי תקן 802.1D. הבעה המרכזית הנה שלוקח בין 50-30 שניות עד שהמשק נכנס למצב פעיל.
- Per-VLAN Spanning Tree (PVST+) – זהו פרוטוקול שפיתחה CISCO ובו לכל VLAN יש Root Bridge נפרד ובמקרה של Loop אין צורך חיבור לגמרי אלה ניתן להשאירו פעיל בhanlv מסוים בלבד וכן ניתן לנצל את רוחב הפס בצורה טובה יותר. במתגיisco פרוטוקול זה הינו ברירת מחדל.
- Rapid STP (RSTP) – עובד בשכבה השנייה של מודול OSI לפוי תקן 802.1W. הוא מעביר משק ממצב blocking forwarding לבן (לעומת STP אשר מבצע זאת ב50%). ההבדל בין לבין STP פסיבי (כיון שמחכה בכל פעם לבדוק את מצב המשק) לעומת RSTP שהוא אקטיבי (מהיר יותר מאשר STP).
- Per-VLAN Rapid STP (PVRST) – פרוטוקול שפותח על ידי Cisco והוא שילוב של PVST+ ו-RSTP (עובד עם VLANS ומהיר יותר).

.PVRST משתמש בפרויקט

Root Bridge – המtag שיימש כנקודת ייחוס למתגים אחרים ברשת. יש לדאוג שהוא יהיה במרכז הרשת. כאשר מtag מאתר לולאה עלייה להחלטת איזה משק הוא סגור על מנת לבטל את הלולאה. זאת נעשית על ידי מציאת הנתיב הטוב ביותר Root Bridge ל-Root Bridge וחסימת כל נתיב אחר.

הчисוב שנעשה על המתגים על מנת להחליט את הדרך הטוב ביותר ביוטר ל-Root Bridge נקרא Cost. והושה על כל משק. cost נמוך יותר מציביע על דרך מהירה יותר root bridge rootbridge ולפניהם המשק עם הנמוך ביותר ישאר דולק וכל השאר ייחסמו.

: Root Bridges

המtag שיבחר לביוטר הוא המtag עם ה-ID Bridge (או בקיצור BID) הנמוך ביותר.

BID הוא מספר ייחודי שיש לכל מtag ומורכב משני חלקים :

מספר בין 0-65535 – Bridge Priority -
כתובת MAC -

* כבירות מחדר ערך הינו 32768 ולן כבירות מחדר המtag עם כתובת MAC
הנמוכה ביותר יתפקד כRoot Bridge

בחירה הנטיב הטוב ביותר:

Root - מספר שמקבל כל ממשק בתב, משקף את מהירות החיבור מהמשק שבמtag ועד לRoot Bridge

Cost Root bridge יותר --> דרכ מהירה יותר לRoot bridge

המשק עם Cost הנמוך ביותר ישאר דлок ושאר המשקים יחסמו

• אם Cost בשני המשקים שווה, נבדוק את ה-Bridge ID (BID).

○ המtag עם BridgeID הנמוך ביותר יבחר וכל שאר המשקים יחסמו

Bandwidth	Cost
10Mbps	100
100Mbps	19
1Gbps	4
10Gbps	2

תפקידים המשקים:

Root Port – מסמן את הנטיב המהיר ביותר Root Bridge. קיימ אחד לכל מtag

Designated Port – הפורט שמעביר את המידע. כאשר מחברים שני מטגים בהכרח צד אחד יהיה

Root Port/ Non-Designated Designated

Non-designated port – הפורט שנחסם כיון שהcost שלו בloopaggi גובה (עדין מעביר

(BPDUs

Disabled Port – פорт לא פעיל (administratively shut down) -

Alternate Port – מחליף מידע כדי למנוע לולאות (Root Port RSTP יש)

מצבי ממשקים:

כאשר מחברים התקן למtag, לוקח 30-50 שניות עד שהוא מעביר מידע לרשותascoftp הוא עבר מסטר שלבים :

הקשבה לתעבורה BPDU Packets ולמידת מצב הרשות (20 שניות) – Blocking

שליחת/קבלת של הודעות BPDU (15 שניות) – Listening

למידת Mac Address של התקנים המוחברים לממשק (15 שניות) – Learning

המשק במצב פעיל המעביר מידע – Forwarding

(בRSTP יש learning, forwarding, discarding (חסימה) ולוקח 2 שניות לעבר learning (forwarding)

:portfast

כום עקב הפיתוח הטכנולוגי, קיימים מצב בו מערכות ההפעלה עלות בזמן קצר לפני שימוש המtag הספיק לעבור למצב forwarding מה שuvwll גורם למצב של חוסר תקשורת בין התקני הקצה עד שהמשק יעלה. לכן יש צורך בזמינות משק בפחות מ30 שניות. **Portfast** מנטראל את stp ועובד מידית ממצב blocking למצב forwarding תוך כדי הקיפת מצבים Listening ו-Forwarding ובכך יגבר על הקושי שנוצר עקב מהירות עליית מערכות ההפעלה. נגיד פקודה זו על הממשקים לכיוון התקני הקצה משומש שכיוונים לא יתכו לולאות מיתוג.

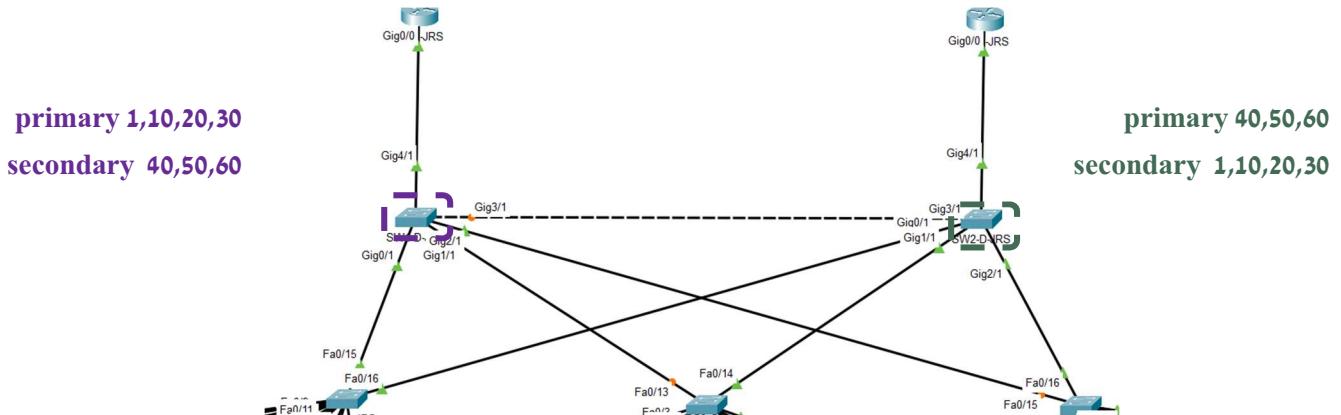
BPDU Guard

נשתמש בה לאחר שהגדכנו PortFast. גורמת לכך שאם הגיע BPDU Packet המשק לא עבר יוטר מידע ויכנס למצב ErrDisable. במצב זה רק מנהל הרשות יכול לפתח חזרה את המשק. מוגדר על כלל הפורטים ב망גים בשכבות Hd ונוועד כל מנת למנוע חיבור של מtag חדש (מתוחזה) עם BID נמוך יותר שהתחבר במטרה להפוך לRoot Bridge.

מבנה הודעת BPDU

Protocol Identifier	Protocol Version Identifier	BPDU Type	Flags	Root Identifier	Root Path Cost	Bridge Identifier	Port Identifier	Message Age	Max Age	Hello Time	Forward Delay
---------------------	-----------------------------	-----------	-------	-----------------	----------------	-------------------	-----------------	-------------	---------	------------	---------------

הגדרת stp בסניף הראשוני: JRS



הגדרת RPVST בכל המתגים

```
SW1-D-JRS (config)#spanning-tree mode rapid-pvst
```

הגדרת RPVST

הגדרת vlans שמגיעים לROOT בכל מתג בשכבה A

```
SW3-A-JRS (config)#spanning-tree vlan 26
SW3-A-JRS (config)#spanning-tree vlan 37
SW3-A-JRS (config)#spanning-tree vlan 48
SW3-A-JRS (config)#spanning-tree vlan 59
SW3-A-JRS (config)#spanning-tree vlan 70
SW3-A-JRS (config)#spanning-tree vlan 81
```

הגדרה לכל vlan

נחלק את VLANS שלנו בין 2 המתגים, כך שלכל מתג יש 3 VLANS שעבורם הוא PRIMARY וPRIMARY הוא secondary והפוך במתג השני. כך חלוקת העומסים מתחולק בין שני המתגים

```
SW1-D-JRS (config)#spanning-tree vlan 1,26,37,48 root primary
```

הגדרת המתג root לוילאים מסויימים לאחרים backup

```
SW1-D-JRS (config)#spanning-tree vlan 59,70,81 root secondary
```

```
SW2-D-JRS (config)#spanning-tree vlan 1,26,37,48 root secondary
```

```
SW2-D-JRS (config)#spanning-tree vlan 59,70,81 root primary
```

הגדרת PortFast בכל המתגים בשכבה Access

```
SW2-A-JRS (config) int range fastEthernet 0/1-12
SW2-A-JRS (config-if-range)#spanning-tree portfast
```

כניסה לממשק
הגדרת Portfast

הגדרת BPDU Guard בכל המתגים בשכבה Access

```
SW2-A-JRS (config-if-range)#spanning-tree bpduguard enable
```

הגדרת ROOT Bridge על ממשקים מתג ה ROOT Guard

```
SW1-D-JRS (config)#int range gig0/1, gig1/1, gig2/1, gig3/1, gig4/1, gig5/1  
SW1-D-JRS (config-if-range)#spanning-tree guard root
```

הגדרת ROOT Backup על ממשקים מתג ה ROOT Guard

```
Switch(config)#int range gig0/1, gig1/1, gig2/1, gig3/1, gig4/1, gig5/1  
Switch(config-if-range)#spanning-tree guard root
```

show commands

מציג את סוג הstp ו את מצב הוילאנים שהוגדרו .
מראה את מצב הstp על פורט ספציפי – show spanning-tree interface [interface]
פקודה המראה בפיירוט מידע על ההגדרות של הпрוטוקול על כל פורט – show spanning-tree details
בנפרד במתג. מציגה את הזמנים של mac address ,priority number ,hello massages והMbps של הפורטים
הפורטים מראה את כל הפורטים שעלייהם הוגדר ה- vlan, מצב הפורט cost ו show spanning-tree vlan [number]

show spanning-tree summary

מצב stp						
Name	Blocking	Listening	Learning	Forwarding	STP	Active
VLAN0001	0	0	0	5	5	
VLAN0026	0	0	0	6	6	
VLAN0037	0	0	0	6	6	
VLAN0048	0	0	0	6	6	
VLAN0059	0	0	0	6	6	
VLAN0070	0	0	0	6	6	
VLAN0081	0	0	0	6	6	
VLAN0100	0	0	0	5	5	
VLAN0101	0	0	0	5	5	
9 vlans	0	0	0	51	51	

show spanning-tree interface [interface]

Vlan	Role	Port	Cost	Prio.	Nbr	Type
VLAN0001	Desg	FWD	19	128.15		P2p
VLAN0026	Root	FWD	19	128.15		P2p
VLAN0037	Root	FWD	19	128.15		P2p
VLAN0048	Root	FWD	19	128.15		P2p
VLAN0059	Altn	BLK	19	128.15		P2p
VLAN0070	Altn	BLK	19	128.15		P2p
VLAN0081	Altn	BLK	19	128.15		P2p
VLAN0100	Desg	FWD	19	128.15		P2p
VLAN0101	Desg	FWD	19	128.15		P2p

עלוות מס' vlan מצב תפקיך תיעודן

– show spanning-tree details

```
SW2-A-JRS#show spanning-tree detail
```

VLAN0001 is executing the **rstp** compatible Spanning Tree Protocol
 Bridge Identifier has priority of **32768**, sysid 1, 0010.115B.E678
 Configured **hello_time 2**, **max_age 20**, **forward_delay 15**
 Current root has priority **32769**
 Root port is 14 (FastEthernet0/14), cost of root path is **19**
 Topology change flag not set, detected flag not set
 Number of topology changes 0 last change occurred 00:00:00 ago
 from FastEthernet0/1
 Times: hold 1, topology change 35, notification 2
 hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 300

Port 13 (FastEthernet0/13) of VLAN0001 is alternate blocking
 Port path cost 19, Port priority 128, Port Identifier 128.13
 Designated root has priority 32769, address 000A.F384.3A10
 Designated bridge has priority 32769, address 00D0.5882.6E67
 Timers: message age 16, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 Link type is point-to-point by default

Port 14 (FastEthernet0/14) of VLAN0001 is root forwarding
 Port path cost 19, Port priority 128, Port Identifier 128.14
 Designated root has priority 32769, address 000A.F384.3A10
 Designated bridge has priority 32769, address 000A.F384.3A10
 Timers: message age 16, forward delay 0, hold 0
 Number of transitions to forwarding state: 1
 Link type is point-to-point by default

VLAN0026 is executing the **rstp** compatible Spanning Tree Protocol
 Bridge Identifier has priority of **32768**, sysid 26, 0010.115B.E678
 Configured **hello_time 2**, **max_age 20**, **forward_delay 15**
 Current root has priority **24602**
 Root port is 13 (FastEthernet0/13), cost of root path is 19
 Topology change flag not set, detected flag not set
 Number of topology changes 0 last change occurred 00:00:00 ago
 from FastEthernet0/1
 Times: hold 1, topology change 35, notification 2
 hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 300

סוג פרוטוקול של המתג Priority

ערכי הטימרים root bridge של Priority

עלוות (cost)

show spanning-tree vlan [number]

Spanning tree enabled protocol rstp					
Root ID	Priority	Address	תיעודן	טימרים	
	24602	00D0.5882.6E67			
	19				
	13 (FastEthernet0/13)				
	Hello Time 2 sec	Max Age 20 sec	Forward Delay 15 sec		
Bridge ID	Priority	Address	תיעודן	MRI ציון המותג ממנה	
	32794 (priority 32768 sys-id-ext 26)	0010.115B.E678			
	2 sec	Max Age 20 sec	Forward Delay 15 sec		
	Aging Time 20			MRI ציון את הפקודה	
Interface	Role	sts	Cost	Prio.Nbr	Type
Fa0/13	Root	FWD	19	128.13	P2p
Fa0/14	Altn	BLK	19	128.14	P2p

עלוות

תפקיד ומצב

ממשק

מידע על root bridge

מידע על המותג ממנה

MRI ציון את הפקודה

Hot Standby Router Protocol

פרוטוקול קנייני של חברת Cisco וחלק משפחת ה프וטוקולים: HSRP, VRRP, GDBP. מטרת ה프וטוקול הינה לאפשר יתירות ברשת, כלומר אפשר של שני נתבים או יותר לשמש כשער ברירת המחדל (Default Gateway) ברשת.

הוא עובד ב- UDP וקיימות לו 2 גרסאות

Version 2	Version 1	
224.0.0.102	224.0.0.2	כטובה multicast
עד 400 קבוצות	עד 225 קבוצות	מספר קבוצות

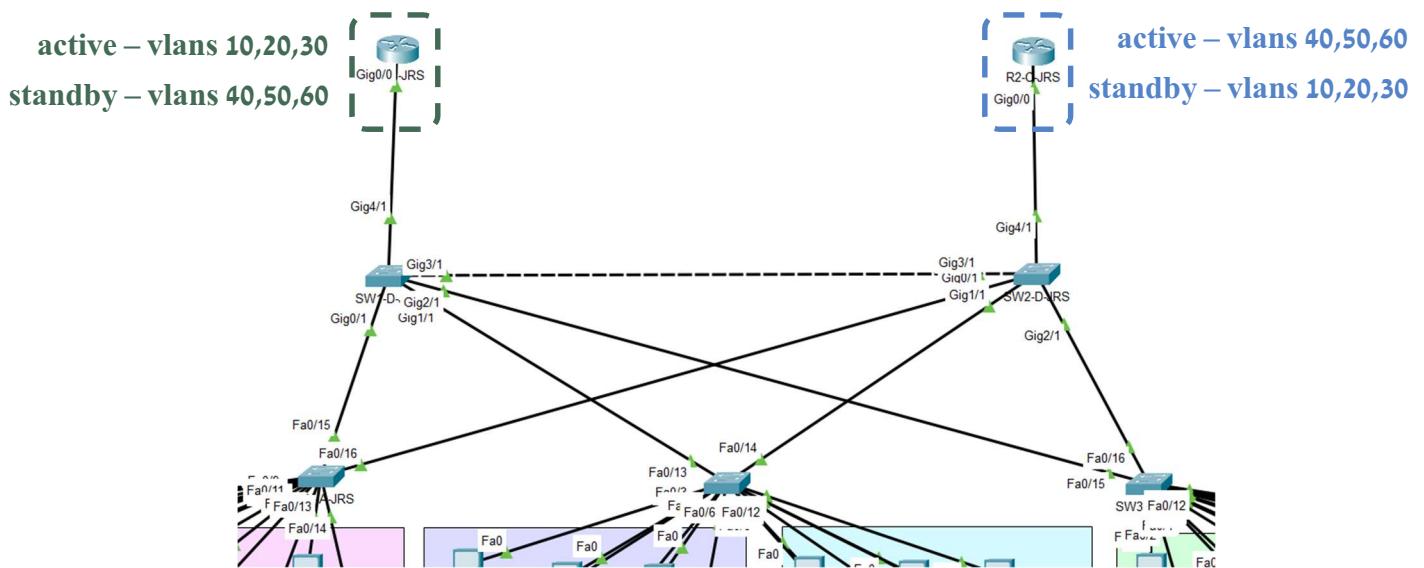
הנתבים ב프וטוקול חולקים כתובת MAC ו- IP ווירטואליים ומהווים ביחד את שער ברירת המחדל ברשת. בפרוטוקול זה, מספר נתבים נמצאים במצב standby בעוד אחד במצב active. הנתב אשר נמצא במצב active יהיה אחראי על העברת התעבורה ברשת, במקרה בו יש תקלה, אחד הנתבים אשר נמצא במצב standby יחליפו אותו והנתב החדש יהיה אחראי על התעבורה.

את כתובת MAC הוירטואלית יוצר ה프וטוקול בצורה אוטומטית וכתובת IP הוירטואלית ניתנת בצורה ידנית על ידי מנהל הרשת. הנתב אשר יתפקד כactive יבחר על ידי ערך priority הגבוה ביותר. במידה וערך priority שוויים, יבחר הנתב בעל כתובת הקן הגבוהה ביותר. שאר הנתבים יתפקדו standby.

הנתבים מעבירים הודעות Hello עם שכיניהם כל שלוש שניות על מנת לוודא קשר. במידה בה נתבים אינם מקבלים הודעה Hello ב-3 שניות מתבב כלשהו, הסיבה לכך עלולה להיות או שהנתב נפל או שיש עומס ברשת, לכן יჩכו את Hold down timer שערכו הדיפולטיבי הינו 10 שניות (ניתן לשינוי). כאשר ערך ה- hold down timer נגמר, אותו הנתב אינו יתפקד כשכנו ויפסיקו להישלח אליו הודעה Hello. במצב בו הנתב במצב active נפל ונגמר זמן hold down timer, הנתב בעל priority השני הגבוהה ביותר, יתפקד active. במידה והם שוויים יבחר הנתב בעל כתובת הקן הגבוהה ביותר.

כאשר קיים כשל בנתב במצב active נתב אחר יקח את מקומו. במידה בו הנתב חוזר, הוא יתפקד standby ואינו יחזור להיות active. על מנת שיכל לחזור להיות active באופן אוטומטי, יש להגדיר על הנתבים את הפקודת preempt אשר תאפשר לנtab active שנפל לחזור לתפקידו ולהיות אחראי על התעבורה.

הגדרת HSRP בסניף הראשוני: JRS



הגדרת HSRP על הנטבטים בסניף הראשוני: JRS

```
R1-C-JRS (config) #int gigabitEthernet 0/0.26
R1-C-JRS (config-subif) #standby 1 ip 10.1.26.254
R1-C-JRS (config-subif) #standby 1 priority 110
R1-C-JRS (config-subif) #standby 1 preempt
```

הגדרת כתובות הIp הוירטואלית

הגדרת priority

```
R1-C-JRS (config-subif) #int gigabitEthernet 0/0.81
R1-C-JRS (config-subif) #standby 1 ip 10.1.81.254
R1-C-JRS (config-subif) #standby 1 priority 90
R1-C-JRS (config-subif) #standby 1 preempt
```

נוכל לראות כי מצב הממשקים הוירטואליים משתנה לפי priority שניינו להם

```
*Dec 23, 16:51:46.5151: %HSRP-6-STATECHANGE: GigabitEthernet0/0.70 Grp 1 state Standby -> Active
*Dec 23, 16:51:46.5151: %HSRP-6-STATECHANGE: GigabitEthernet0/0.59 Grp 1 state Standby -> Active
*Dec 23, 16:51:47.5151: %HSRP-6-STATECHANGE: GigabitEthernet0/0.81 Grp 1 state Standby -> Active
*Dec 23, 16:52:03.5252: %HSRP-6-STATECHANGE: GigabitEthernet0/0.37 Grp 1 state Speak -> Standby
*Dec 23, 16:52:04.5252: %HSRP-6-STATECHANGE: GigabitEthernet0/0.48 Grp 1 state Speak -> Standby
*Dec 23, 16:52:04.5252: %HSRP-6-STATECHANGE: GigabitEthernet0/0.26 Grp 1 state Speak -> Standby
```

Show commands

HSRP – מראה נתונים על show standby

– מראה נתונים על HSRP בצורה מצומצמת טבלאית ומסודרת

:R1

: Show standby

```
R2-C-JRS(config)#do show standby
GigabitEthernet0/0.26 - Group 1
  State is Standby
    3 state changes, last state change 00:00:05 ← מס' קבוצה
    Virtual IP address is 10.1.26.254 ← מצב הממשק הווירטואלי
    Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (vl default) ← כתובות ה-IP הווירטואלית
    Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.029 secs ← כתובת active לוקלית
    Preemption enabled ← אם הוגדר preempt
    Active router is 10.1.26.252 ← כתובת IP של הממשק הווירטואלי של הנטב השני
    Standby router is local ← priority שלו
    Priority 90 (configured 90)
    Group name is hsrp-Gig-1 (default)
GigabitEthernet0/0.37 - Group 1
  State is Standby
    3 state changes, last state change 00:00:04
    Virtual IP address is 10.1.37.254
```

show standby brief

Interface	Grp	Pri	State	Active	Standby	Virtual IP
Gig	1	90	P Standby	10.1.26.252	local	10.1.26.254
Gig	1	90	P Standby	10.1.37.252	local	10.1.37.254
Gig	1	90	P Standby	10.1.48.252	local	10.1.48.254
Gig	1	110	P Active	local	10.1.59.252	10.1.59.254
Gig	1	110	P Active	local	10.1.70.252	10.1.70.254
Gig	1	110	P Active	local	10.1.81.252	10.1.81.254
Gig	1	90	P Standby	10.1.100.252	local	10.1.100.254
Gig	1	110	P Active	local	10.1.101.252	10.1.101.254

כתובת IP וירטואלית כתובת IP של standby כתובת IP של active מס' פרט מושך

– כתובת המוגדרת local
על הנטב ממנו מתבצעת הפקודה

:R2

show standby

```
GigabitEthernet0/0.10 - Group 1                         מספר קבוצה
State is Standby                                         מצב הממשק הווירטואלי
    7 state changes, last state change 00:00:31          כמות ה שינויים האחרונים
Virtual IP address is 192.168.10.254                      כתובת IP הווירטואלית
Active virtual MAC address is 0000.0C07.AC01            כתובת MAC הווירטואלית
    Local virtual MAC address is 0000.0C07.AC01 (vl default)
Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.963 secs
Preemption enabled                                         האם הוגדר preempt
Active router is 192.168.10.252 priority 110 (expires in 9 sec)   כתובת IP של הממשק
    MAC address is 0000.0C07.AC01
Standby router is local                                     כתובת העדיף לוקלית standby
Priority 90 (configured 90)                               priority שלו
Group name is hsrp-Gig-1 (default)
```

כתובת IP של הממשק
הווירטואלי של הראوتر השני

Show standby brief

```
R2-C-JRS#show standby brief
      P indicates configured to preempt.

Interface Grp Pri P State Active Standby Virtual IP
Gig     1   90  P Standby 192.168.10.252 local
192.168.10.254
Gig     1   90  P Standby 192.168.20.252 local
192.168.20.254
Gig     1   90  P Standby 192.168.30.252 local
192.168.30.254
Gig     1   110 P Active local           192.168.40.252
192.168.40.254
Gig     1   110 P Active local           192.168.50.252
192.168.50.254
Gig     1   110 P Active local           192.168.60.252
192.168.60.254
```

כתובת IP וירטואלית כתובת IP של active מצב standby priority קבוצה מס' ממשק

Dynamic Host Configuration Protocol

על מנת שנוכל לתקשר ברשת WAN ו LAN, יש צורך בהגדרת נתונים אשר יאפשרו לנו את תקשורת זו. נתונים אלו הינם כתובות IP - כתובות לוגית, S.M מסכת רשות שגדירה את טווח הכתובות הקיימים ברשת זו, כתובת D.G שנחוצה על מנת לצאת לרשת אחרת, ושרת DNS שנחוץ על מנת לחבר בין כתובות דומיין לכתובות IP. את נתונים אלו ניתן להגדיר בצורה סטטית על המחשב אך כאשר ישנו מחשבים רבים הגדירה הידנית עלולה להיות לא יעילה. לכן DHCP הינו פרוטוקול להגדרת כתובות בצורה דינמית. פרוטוקול זה הינו פרוטוקול מסווג client server המספק את הנתונים באופן דינامي על ידי שרת, זאת על מנת שחלוקת כתובות IP למכשורי הקצה תיעשה בצורה נוחה ומהירה. חוסך ממנהל הרשות הגדרת כתובות נתונים נוספים באופן ידני על כל רכיב ברשת.

פרוטוקול זה פועל בUDP, הודעות מצד השרת נשלחות בפורט 67 והודעות מצב הלוקה נשלחות בפורט 68.

יתרונות :

- מונע כפיליות של כתובות IP ברשת
- חלוקה מהירה ויעילה יותר של הכתובות
- קל להגדירה

ניתן להגדיר את פרוטוקול DHCP בשני אופנים : באמצעות שרת DHCP ובאמצעות נתב שישמש כשרת DHCP. לשתי השיטות קיימות יתרונות וחסרונות :

ההדרת DHCP על נתב :

- חיסרונו – הנתב משמש אותו לניתוב בין רשתות שונות ולכן ההדרת שרת DHCP עליו יוסיף עומס על הנתב. **איטיות**
- יתרונו – אין צורך לקנות שרת המועד לפרוטוקול DHCP **חסכו בכספי ומשאבים**

שרת DHCP

- יתרונו - שרת שתפקידו היחיד הינו חלוקת כתובות למיכשיים. מכיוון שאין לו תפקידים נוספים, **מחלוקת הכתובות תיעשה בצורה מהירה יותר. מהירות**
- חיסרונו - יש צורך בקניית שרת ייחודי שישמש כDHCP ויחלק כתובות. **כספי ומשאבים**

תהליך חלוקת הכתובות ב프וטוקול DHCP

Discover

הודעת broadcast אשר נשלחת מהמחשב החוצה במטרה לחפש שירות DHCP ברשות שיחلك למחשב כתובת IP .D.G – S.M

Offer

כאשר שירות DHCP זמין בעל כתובות ברשות אשר פנוiot לחלוקת מקובל את הودעת DISCOVER שלחה המחשב, הוא שולח הצעת כתובת IP למחשב אשר שלח את ההודעה.

Request

לאחר קבלת הודעת offer מהשרת המכילה כתובת IP, המחשב שולח הודעת request המביאה על כך שהמחשב רוצה את הכתובת שהציע השירות. הודעה זו נשלחת במטרה לעדכן את שרתי DHCP שכתובת זו תפופה ברשות על מנת שלא יקצו אותה כתובות זו למחשב אחר להיות ואסור שייהיו שתי כתובות זהות למכשורי קצה שונים באותו הרשת.

Acknowledge

השרת שולח הודעה כי אישר את בקשת המחשב. הוא מנסה למכשור קצה זה את כתובת ה- IP שהועצמה בהודעת offer ואת שרתי נתוני הרשות כגון M.S., G.D – . לאחר הודעה זו, יוכל המחשב להשתמש בתנאים אלו לזמן קצר (lease) אשר רשום בהודעה, על מנת לתקשר עם מכשורים נוספים.

זמן הקצאה Lease

כתובות ה- IP אשר ניתנות באופן דינامي על ידי שירות DHCP מוקצות ללקוח (מכשור הקצאה) לזמן מוגבל. זמן זה ניתן בשלב ה- acknowledge ואומר כי בתום זמן הקצאה, כתובת ה- IP תחזור לשרת, אלה אם ביקש הלקוח להאריך את זמן הקצאה. לאחר 50% מזמן הקצאה הלקוח ישלח לשרת הודעה מסוג Request על מנת לחדש את lease. אם השירות לא עונה לו (לדוגמא אם הוא נפל), יჩכה המחשב ל- 87.5% מזמן הקצאה וינסה לפנות שוב לשרת בבקשת Request. אם השירות אינו עונה בשלב זה וудין אינו מצליח לתקשר, ישלח הלקוח הודעה מסוג Discover במטרה לחפש שירות DHCP אחר שיוכל לתת לו כתובת IP. אם לאחר 100% מזמן הקצאה לא ענה לו השירות הקודם ולא מצא שירות DHCP אחר, הלקוח יתנו לעצמו כתובת מסוג APIPA.

- הערכה* כאשר מגדרים DHCP על נטב, כלל ההודעות בתהליך DORA אשר מגיעות מהמחשב אל המTARGET במצב BROADCAST משנתנות להודעות מסוג UNICAST בדרך אל הנטב מכיוון שהנטב חוסם הודעות מסוג BROADCAST.

כתובת APIPA :

כתובת APIPA (Automatic Private IP Address) הינה כתובת אשר הלוקוח נותן לעצמו במצב בו הוא אינו מוצא שרת DHCP זמין או כאשר קיים שירות אך נגמרו לו כתובות החלוקה, כלומר לאחר שלוחת ארבע הודעות מסווג **Discover** ולא קיבל חוזה הودעת **Offer** משרת DHCP. הכתובת הינה כתובת IP מהרשף $169.254.0.0/16$ כלומר תיראה כ - $X.X.169.254$ ובעזרת כתובת זו יוכל המחשב לדבר בתחום הרשת שלו אך אינו יוכל לצאת החוצה אל הרשת החיצונית. גם לאחר שקיבל כתובת זו, הלוקוח ימשיך לשולח פעם בשלוש הודעות **Discover** במטרה לחפש שירות DHCP אשר יתן לו כתובת דינמית.

מה נעשה במצב בו קיים יותר משרת DHCP אחד זמין

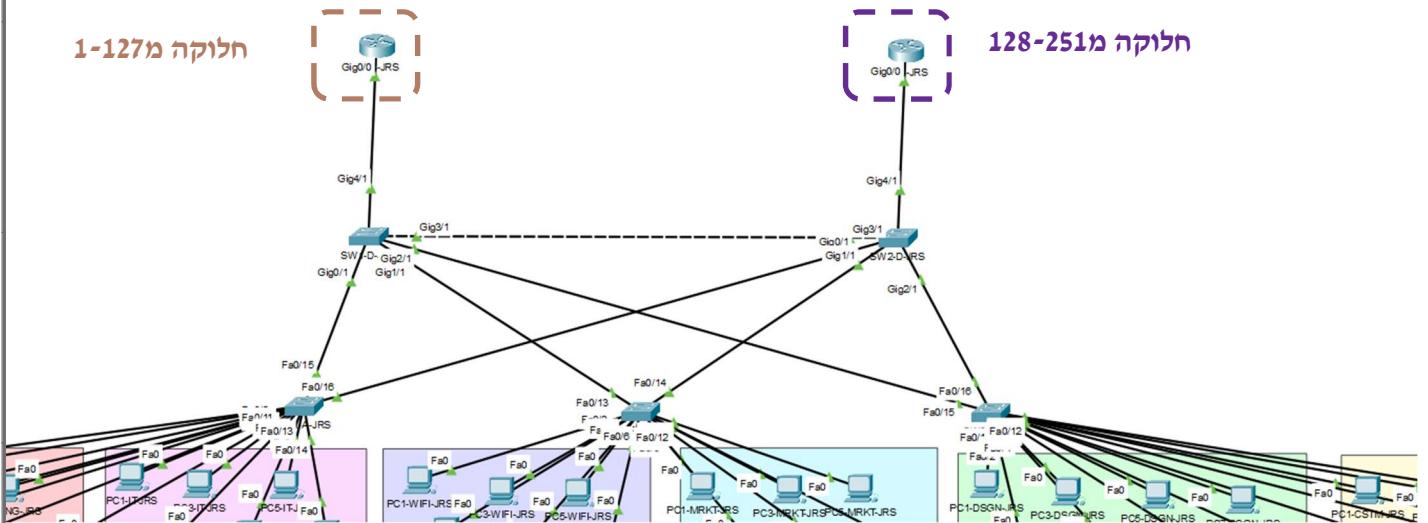
הלוקוח שולח הודעת Broadcast וلن נשלחת בכל הרשות. במצב בו קיים יותר משרת DHCP אחד, הלוקוח יקבל ברשות כמה הודעות מסווג **Offer** אשר מוכנות להצעה לו כתובת IP. במצב זה, הלוקוח יקח את הכתובת מהשרת ששלח את הודעת **Offer** הראשונה.

מצבים שלDHCP

- **הקצאה ידנית** – (manual allocation) מצב בו ניהולו של הפרוטוקול נעשה על ידי טבלת כתובות **interfaces** של MAC של מכשירים ברשות וכותבת ה - IP שהוקצתה לכל אחד מה - **.interfaces**.
- **הקצאה אוטומטית** – (automatic allocation) הגדרת תחום כתובות על שירות DHCP על ידי מנהל הרשות. מאפשר לכל מכשיר ברשות לפנות אל השירות ולבקש ממנו כתובת IP מתוך התוחום המוגדר.
- **הקצאה דינמית** – (dynamic allocation) – הגדרת תחום כתובות על שירות DHCP בדומה להקצאה אוטומטית, אך הכתובות יוקצו למכשיר ברשות לתקופת זמן מוגבלת מרוגע קבלת הודעת **(Lease)** acknowledgement. במצב בו המחשב לא מבקש מחדש את הכתובת שניתנה לו (על ידי השלבים שמוגדרים תחת הכוורת: זמן הקצאה), הכתובת תחזור למאגר כתובות IP של השירות ותוכל להינתן למכשיר רשות אחר שירצה לקבל כתובת.

הגדרת שרת DHCP בسنיף הראשון JRS:

על מנת לחלק עומסים בין שני הנטבים בסניף, אגדיר את אחד הנתבים לחלוקת כתובות vlans בטוווח 1-127 ובסניף השני אגדיר חלוקת כתובות בטוווח 128 – 251 (לא ניתן לחלק את 252 – 254 מכיוון שתפוזות על ידי כתובות ה - D.G ופרוטוקול ה - HSRP)



הגדרת הכתובות בכל נתב שאינו ניתן לחלוקת

הגדרה בנתב 1:

```
R1-C-JRS(config)#ip dhcp excluded-address 10.1.26.128 10.1.26.254
R1-C-JRS(config)#ip dhcp excluded-address 10.1.37.128 10.1.37.254
R1-C-JRS(config)#ip dhcp excluded-address 10.1.48.128 10.1.48.254
R1-C-JRS(config)#ip dhcp excluded-address 10.1.59.128 10.1.59.254
R1-C-JRS(config)#ip dhcp excluded-address 10.1.70.128 10.1.70.254
R1-C-JRS(config)#ip dhcp excluded-address 10.1.81.128 10.1.81.254
```

הגדרת תחומי הכתובות שלא יחולקו
תחום הכתובות שהרואטר השני מחלק, כולל
הכתובות של DOT1Q ו-HSRP

הגדרה בנתב 2:

```
R2-C-JRS(config)#ip dhcp excluded-address 192.168.26.1 192.168.26.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.37.1 192.168.37.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.48.1 192.168.48.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.59.1 192.168.59.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.70.1 192.168.70.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.81.1 192.168.81.127
R2-C-JRS(config)#ip dhcp excluded-address 192.168.26.252 192.168.26.254
R2-C-JRS(config)#ip dhcp excluded-address 192.168.37.252 192.168.37.254
R2-C-JRS(config)#ip dhcp excluded-address 192.168.48.252 192.168.48.254
R2-C-JRS(config)#ip dhcp excluded-address 192.168.59.252 192.168.59.254
R2-C-JRS(config)#ip dhcp excluded-address 192.168.70.252 192.168.70.254
R2-C-JRS(config)#ip dhcp excluded-address 192.168.81.252 192.168.81.254
```

הגדרת תחומי הכתובות שלא יחולקו
תחום הכתובות שהרואטר השני מחלק, כולל
הכתובות של DOT1Q ו-HSRP

הגדרת רשות חלוקה

בנתב 1:

```
R1-C-JRS (config)#ip dhcp pool lan26 | → pool ← שם הpool
R1-C-JRS (dhcp-config)#network 10.1.26.0 255.255.255.0 → ip network
R1-C-JRS (dhcp-config)#default-router 10.1.26.254 → Default Gateway
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3 → חלוקת כתובות שרת DNS שנגזר בפרק הבא
R1-C-JRS (dhcp-config)#ip dhcp pool lan37
R1-C-JRS (dhcp-config)#network 10.1.37.0 255.255.255.0
R1-C-JRS (dhcp-config)#default-router 10.1.37.254
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3
R1-C-JRS (dhcp-config)#ip dhcp pool lan48
R1-C-JRS (dhcp-config)#network 10.1.48.0 255.255.255.0
R1-C-JRS (dhcp-config)#default-router 10.1.48.254
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3
R1-C-JRS (dhcp-config)#ip dhcp pool lan59
R1-C-JRS (dhcp-config)#network 10.1.59.0 255.255.255.0
R1-C-JRS (dhcp-config)#default-router 10.1.59.254
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3
R1-C-JRS (dhcp-config)#ip dhcp pool lan70
R1-C-JRS (dhcp-config)#network 10.1.70.0 255.255.255.0
R1-C-JRS (dhcp-config)#default-router 10.1.70.254
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3
R1-C-JRS (dhcp-config)#ip dhcp pool lan81
R1-C-JRS (dhcp-config)#network 10.1.81.0 255.255.255.0
R1-C-JRS (dhcp-config)#default-router 10.1.81.254
R1-C-JRS (dhcp-config)#dns-server 10.1.100.3
```

הראתה זאת גם בפרק
(הראתה זאת גם בפרק)

בנתב 2:

```
R2-C-JRS (config)#ip dhcp pool lan26
R2-C-JRS (dhcp-config)#network 10.1.26.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.26.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
R2-C-JRS (dhcp-config)#ip dhcp pool lan37
R2-C-JRS (dhcp-config)#network 10.1.37.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.37.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
R2-C-JRS (dhcp-config)#ip dhcp pool lan48
R2-C-JRS (dhcp-config)#network 10.1.48.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.48.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
R2-C-JRS (dhcp-config)#ip dhcp pool lan59
R2-C-JRS (dhcp-config)#network 10.1.59.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.59.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
R2-C-JRS (dhcp-config)#ip dhcp pool lan70
R2-C-JRS (dhcp-config)#network 10.1.70.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.70.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
R2-C-JRS (dhcp-config)#ip dhcp pool lan81
R2-C-JRS (dhcp-config)#network 10.1.81.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.81.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3
```

show commands

— מראה מידע על כל pools שיצרנו. show ip dhcp pool

— מראה את אותם הנתונים על ה VLAN - show ip dhcp pool <pool_name>

show ip dhcp pool <pool_name>

R1-C-JRS#show ip dhcp pool lan10		
Pool lan10 :		
Utilization mark (high/low)	:	100 / 0
Subnet size (first/next)	:	0 / 0
Total addresses	:	254
Leased addresses	:	1
Excluded addresses	:	6
Pending event	:	none
1 subnet is currently in the pool		
Current index	IP address range	Leased/Excluded/
Total	192.168.10.1 - 192.168.10.254	1 / 6 / 254

כתובת IP הבאה שתחולק ב pool

טוחה הכתובות ברשת זו

על מנת לראות את הכתובות IP שחולקו:

how ip dhcp binding

IP address	Client-ID Hardware address	Lease expiration	Type
10.1.26.2	00E0.F91C.6D50	--	Automatic
10.1.26.3	0006.2A52.B482	--	Automatic
10.1.37.1	00E0.F9A8.DE1C	--	Automatic
10.1.37.2	0001.975B.C83B	--	Automatic
10.1.48.1	0002.1641.1E69	--	Automatic
10.1.48.2	0001.C9AD.6333	--	Automatic
10.1.70.1	000C.85DA.7201	--	Automatic

סוג החלוקה lease כתובות IP שחולקו כתובות MAC של מכשיר הקצה

כפי שניתנו לראות, למחשבים ניתנו הנתונים הדורשים להם לתקורת מחוץ לרשת המקומית

Interface	FastEthernet0
IP Configuration	DHCP
IPv4 Address	192.168.20.128
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.254

Interface	FastEthernet0
IP Configuration	DHCP
IPv4 Address	192.168.10.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254

Port Security

Port security הינה טכנולוגיה המאפשרת לבדוק את ההתקנים המתמחברים למstag בשכבות 1 ו-2. במציאותו, מtag לא אפשר להתקן שאינו מורשה להתחבר למסך. הטכנולוגיה מבוססת על סינון גישה בהתבסס על כתובות פיזיות. הוא מאפשר להגדיר שתי מגבלות לכל מסך :

- הגבלת מספר ההתקנים שיוכלו להתחבר למסך המtag.
- קביעת הכתובת הפיזית שהמסך ילמד.

Violation

במצב בווא התקן לא מורשה מתמחבר למtag, מתרחש violation – הפרה של המדיניות שהוגדרה על הממשק שנים שני מצבים בהם יכולה להתראות הפרעה :

- מצב בו כתובות שנלמדה במשק אחד מנסה להתחבר דרך משק אחר
- מצב בו כתובת אשר לא מורשת להתחבר מנסה להתחבר למשק

קיימים שלושה סוגי הגדרות שניתנו להגדיר כתגובה למצב של violation :

סוגי תגודות:

Shutdown – מצב זה מוגדר כמצב בריית מחדר ב-port security. במצב זה, המשק נכבה ועובד

למצב shutdown, נשלחת הודעת SNMP וווצר קובץ Log שנועד לתעד את ה violation. כאשר ה-port נופל במצב זה בעקבות הפרעה, המשק יכנס במצב Err Disable. על מנת להחזיר את המשק לפעילות יהיה צורך בביצוע שתי פקודות :

- פקודה shutdown – פקודה שבעקבותיה המשק יכoba על ידי מנהל הרשות
- פקודה no shutdown – החזרת המשק לפעולה

הסיבה שבמנגנון זה יש צורך בפקודה shutdown כחלק מתהליך החזרת הפורט הוא על מנת לידע

את מנהל הרשות שנפילת הפורט קרתה עקב הפרעה ולא בעקבות סיבת אחרת. רק מנהל הרשות יכול להציג את הפורט ולהחזיר אותו לפעולה.

Restrict – במצב זה המשק אינו נכבה, ההתקן הזר שניסה להתחבר אינו קיבל גישה להתחבר

ולכן ההודעות אותן ינסה לשדר לא יגיעו ליעדם. תישלח הודעת SNMP וווצר קובץ Log שנועד לתעד את ה violation.

Protect – במצב זה המשק אינו נכבה, ההתקן הזר שניסה להתחבר אינו מקבל גישה להתחבר

ולכן ההודעות אותן ינסה לשדר לא יגיעו ליעדם. לא תישלח הודעת SNMP ולא יווצר קובץ Log

שלבי הפעלת Port Security

- כניסה לממשק המבוקש
- הגדרת הממשק הרצוי במצב Access (היוות ומצב ברירת המחדל מוגדר כdynamic Auto)
- מאפשר הגדרה של port security (port security על מנת לשנות את מצבו מ-Disable ל-Enable ונתינת ההגדרות)
- הפעלת Port Security מקסימלית וכתובות סטטיות \ דיביקות.
- המבוקשות מבחינת כתובות MAC מקסימלית וכתובות סטטיות \ דיביקות.

Maximum Mac Addresses

הגדרה המאפשרת להגדיל את כתובות MAC מקסימלית למינן (כברירת מחדל כתובות מקסימלית הינה אחת)

Mac Address Learning

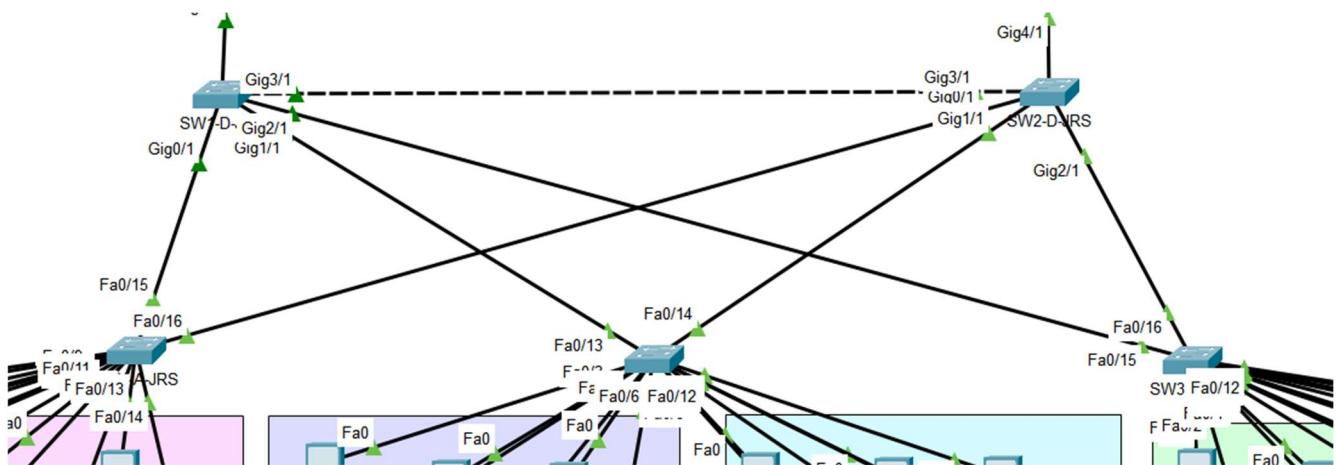
ניתן ללמוד את המתג על כתובות MAC בשתי דרכים :

- הגדרת כתובות MAC שיורשו באופן ידני – Static Port Security
- הגדרת המתג שילמד את הכתובות באופן דינאמי כאשר המחשב שולח הודעה או פינג.

MAC Address Aging

במתג לאחר כמה זמן הממשקים ישכח את הכתובות שנלמדו. קיימים שני מצבים –
Absolute – מצב בו לאחר כמה דקות המשק ישכח את הכתובות שלם. בברירת מחדל הזמן המוגדר הוא 0, כלומר הכתובות שהוא רשם אינם ימחקו.
Inactivity – מצב בו לאחר כמה דקות של חוסר פעילות ממוקור הכתובת, המשק ישכח את הכתובת.

הגדרת Port Security JRS



מצבי הממשקים במתגים במצב Violation

מחלקה	מצב
מחלקות אלו חשובות ומקבלות ומכילות מידע רגיש על עובדי חברה, משתמשים והנהלה. לכן נרצה שהמשק ידליך ויכבה עם התערבות מנהל הרשות בלבד	Shutdown
נרצה שתעבורה לא תעבור + קובץ לוג והודעת IT - SNMP אין צורך בכינוי משק. לא נרצה שייהיו לנו בעיות בהעברת ציוד ומודיע או בעיות תקשורת בסניף.	Restrict
אין צורך בכינוי משק, מספיק שהתעבורה תחסם.	Protect

- הגדרתי את שלושת המצביעים בפרויקט על מנת להבין את דרך פעולהיהם. 3 מחלקות בעלות מידע רגיש ב shutdown, שתי מחלקות חשובות בעלות מידע רגיש פחות restrict ושתי מחלקות נוספות protect.

הגדרת shutdown על שלושת המחלקות עם כתובות mac address ידני

```
SW1-A-JRS(config)#int range fastEthernet 0/1-14 ← כנישה למשק
SW1-A-JRS(config-if-range)#switchport port-security ← הדרת port security
SW1-A-JRS(config-if-range)#switchport port-security violation shutdown ← הגדרת סוג כותבות shutdown
SW1-A-JRS(config-if-range)#switchport port-security maximum 1 ← הגדרת כמות כותבות MAC
                                         ← המוגבלים למיזה
```

```
SW1-A-JRS(config)#int fa 0/1
SW1-A-JRS(config-if)#switchport port-security mac-address 000C.850A.46CE
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/2
SW1-A-JRS(config-if)#switchport port-security mac-address 00D0.D3B9.2226 ← כנisha למשק
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/3
SW1-A-JRS(config-if)#switchport port-security mac-address 0003.E463.2030
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/4
SW1-A-JRS(config-if)#switchport port-security mac-address 00E0.B049.81B1
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/5
SW1-A-JRS(config-if)#switchport port-security mac-address 00E0.F91C.6D50
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/6
SW1-A-JRS(config-if)#switchport port-security mac-address 00D0.FF1A.9697
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/7
SW1-A-JRS(config-if)#switchport port-security mac-address 00D0.D3D6.1021
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/8
SW1-A-JRS(config-if)#switchport port-security mac-address 0006.2A52.B482
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/9
SW1-A-JRS(config-if)#switchport port-security mac-address 00E0.F9A8.DE1C
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/10
SW1-A-JRS(config-if)#switchport port-security mac-address 0006.2AD2.346E
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/11
SW1-A-JRS(config-if)#switchport port-security mac-address 0002.4A75.5505
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/12
SW1-A-JRS(config-if)#switchport port-security mac-address 00E0.F7BA.A437
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/13
SW1-A-JRS(config-if)#switchport port-security mac-address 0001.975B.C83B
SW1-A-JRS(config-if)#exit
SW1-A-JRS(config)#int fa 0/14
SW1-A-JRS(config-if)#switchport port-security mac-address 0060.70D0.2214
SW1-A-JRS(config-if)#exit
```

הגדרת כותבת MAC המאפשרת על המשק

כנisha למשק

הגדרת כותבת mac-address על המשק

המוגבלים למיזה

הגדרת restrict עם כותבות במצב sticky

```
SW2-A-JRS(config)#int range fa0/1-6 ← כנisha למשק
SW2-A-JRS(config-if-range)#switchport port-security ← הדרת port security
SW2-A-JRS(config-if-range)#switchport port-security violation restrict ← הגדרת סוג restrict
SW2-A-JRS(config-if-range)#switchport port-security maximum 1 ← כמות כותבות MAC המוגבלים למיזה
SW2-A-JRS(config-if-range)#switchport port-security mac-address sticky ← כותבות sticky (נשמרות)
```

הגדרת protect

```
SW3-A-JRS(config)#int range fa0/1-6 ← כנisha למשק
SW3-A-JRS(config-if-range)#switchport port-security ← הדרת port security
SW3-A-JRS(config-if-range)#switchport port-security violation protect ← הגדרת סוג protect
SW3-A-JRS(config-if-range)#switchport port-security maximum 1 ← כמות כותבות MAC המוגבלים למיזה
SW3-A-JRS(config-if-range)#switchport port-security mac-address sticky ← כותבות sticky (נשמרות)
```

Show commands

מציגה מידע על מצב ה-port security על הממשקים

מראה את מצב ה-port security על ממשק

show port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	1	0	Restrict
Fa0/2	1	1	0	Restrict
Fa0/3	1	1	0	Restrict
Fa0/4	1	1	0	Restrict
Fa0/5	1	1	0	Restrict
Fa0/6	1	1	0	Restrict
Fa0/7	1	1	0	Protect
Fa0/8	1	1	0	Protect
Fa0/9	1	1	0	Protect
Fa0/10	1	1	0	Protect
Fa0/11	1	1	0	Protect
Fa0/12	1	1	0	Protect

כמויות הפרעות שהיו כמה MAC למד מספר ממשק כמות MAC מקסימלית מהו mode

show port-security interface

Port Security	: Enabled	אפשרות port security
Port Status	: Secure-up	
Violation Mode	: Protect	סוג ה-mode שהגדנו
Aging Time	: 0 mins	
Aging Type	: Absolute	
SecureStatic Address Aging	: Disabled	
Maximum MAC Addresses	: 1	מקסימום כתובות MAC שהגדנו
Total MAC Addresses	: 0	
Configured MAC Addresses	: 0	כמויות הכתובות שלמד
Sticky MAC Addresses	: 0	
Last Source Address:Vlan	: 0000.0000.0000:0	
Security Violation Count	: 0	

הינה טכנולוגיה המאפשרת חיבור של ממשקים פיזיים רבים לכדי ממשק לוגי אחד. החיבור של הממשקים לממשק לוגי יחיד מאפשר ליצור ממשק בעל מהירות של כל הממשקים הפיזיים המחברים.

EtherChannel

- Duplex זהה בכל הממשקים
- מהירות חיבור זהה בכל הממשקים
- הגדרות VLAN זהות
- מצבים ממשקים זהים (לדוגמא Trunk או Access)

Etherchannel

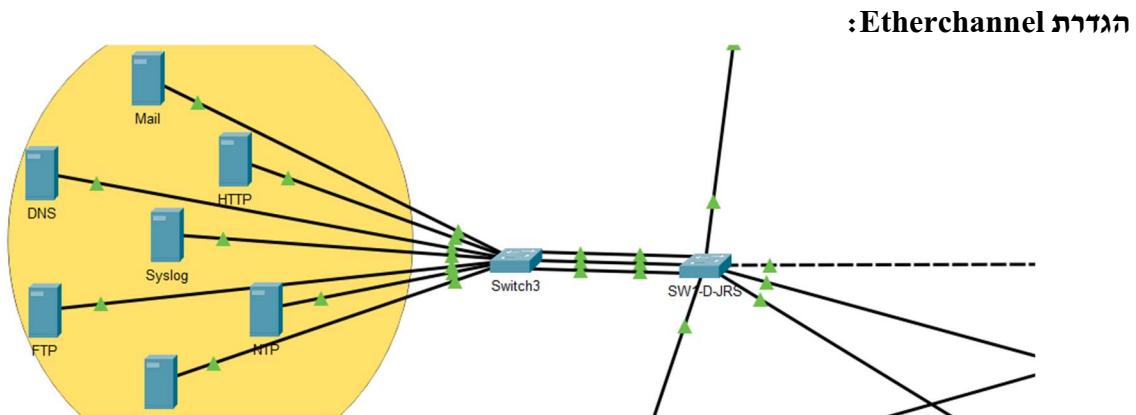
- קיימים שני פרוטוקולים המאפשרים יצרה אוטומטית של Etherchannel.
- (Port Aggregation Protocol) PAgP - פרוטוקול קנייני של חברת Cisco הנitin להפעלה על מתגי Cisco או מתגים המורשים על ידי ספקיהם לתמוך בפרוטוקול זה. הפרוטוקול מאפשר יצרה אוטומטית של Etherchannel על ידי החלפה של הודעות בין שני המתגים. גם לאחר שנוצר הממשק הלוגי בין שני המתגים, ימשיכו להישלח הודעות כל 30 שניות כדי לתחזק ולפעול את הפרוטוקול בצורה שוטפת.
- מאפשר חיבור של עד 8 ממשקים פיזיים לממשק וירטואלי אחד.
- לפרוטוקול זה קיימים 3 מצבים :
- – מצב בו הממשק מנסה ליצור משא ומתן עם הצד השני Desirable
 - – מצב בו הממשק אינו יתחל משא ומתן, הוא יচכה להודעה מהצד השני על מנת להתחילה את המשא ומתן Auto
 - – במצב זה לא נעשה שימוש בשום פרוטוקול. הוא מוגדר ידנית על מנת לחבר בין הממשקים בלי ניהול משא ומתן בין המתגים. הוא חייב להיות מוגדר בשני הצדדים על מנת ליצור EtherChannel
- LACP (Link Aggregation Control Protocol) – פרוטוקול פתוח אשר נוצר על ידי ארגון IEEE, זהה ברובו ל PAGP. נבדל בכך שפרוטוקול זה יכול לעבוד על כלל המתגים ולא רק על מתגי Cisco. מצב העבודה זהים לפוטוקול השני אך שמות שונים.
- – מצב בו הממשק מנסה ליצור משא ומתן עם הצד השני Active
 - – מצב בו הממשק אינו יתחל משא ומתן, הוא יחכה להודעה מהצד השני על מנת להתחילה את המשא ומתן Passive
 - – במצב זה לא נעשה שימוש בשום פרוטוקול. הוא מוגדר ידנית על מנת לחבר בין הממשקים בלי ניהול משא ומתן בין המתגים. הוא חייב להיות מוגדר בשני הצדדים על מנת ליצור EtherChannel

יתרונות:

- שיפור ביצועים ורוחב פס : EtherChannel מאפשר איחוד של מספר פורטים פיזיים ל קישור לוגי אחד, מה שմgiaר את רוחב הפס הזמין ומשפר את ביצוע התקורת ברשת.
- גמישות וסקלibility: היא מאפשרת למנהל רשות להתקאים את הקישוריות לדרישות הרשת המשתנות, תוך כדי שמירה על יכולת להרחיב את הרשות בקלות יותר ללא צורך בשדרוג התשתיה הפיזית.
- אמינות: על ידי איחוד של פורטים, EtherChannel מפחית את הסיכון לנזקודות כשל יחידה ומספק הגנה מפני נזקודות כשל פוטנציאליות, מכיוון שההתקורה יכולה להימשך גם אם אחד מהקישורים נכשל.
- תמיכה ב מדיניות נתוניות ואבטחה : EtherChannel מאפשר יישום של מדיניות אבטחה ונתוניות על פני מספר פורטים כאילו היו פорт אחד, מה שמקל על הגדרת מדיניות אחידה.

מניעת לולאות מיתוג

EtherChannel מסייעת במניעת לולאות מיתוג ברשתות מחשבים על ידי איחוד של מספר פורטים פיזיים ל קישור לוגי אחד. במצב בו מספר פורטים פועלים כיחידה אחת, מנגנוןים שנועדו לולאות, כמו Spanning Tree Protocol (STP), מתייחסים לכל האיחוד כאל נתיב אחד בלבד. זה מונע את הצורך בחישובים מרובים של STP על כל פорт בנפרד, מה שמחית את הסיכוי להיווצרות של לולאות מיתוג. בנוסף, על ידי הקטנת המרכיבות והפשטה התקשורת של הרשת, EtherChannel מסייעת בהקלת ניהול הרשת ומצעריה את הסיכויים לטעויות תצורה שעולות להוביל להיווצרות לולאות. באופן זה, EtherChannel תורמת לשיפור האמינות והיציבות של רשתות מחשבים על ידי מתן פתרון יעיל ו邏יקי לאחת הביעות הנפוצות ביותר בניהול רשתות.



:Etherchannel הגדרת Trunk והגדרת

:switch1

```
SW1-D-JRS(config)#interface range GigabitEthernet5/1, GigabitEthernet6/1, GigabitEthernet7/1
SW1-D-JRS(config-if-range)#switchport mode trunk
SW1-D-JRS(config-if-range)#channel-group 1 mode desirable
```

הגדרת Trunk
הגדרת הממשק במצב desirable

switch2

```
Switch(config)#interface range GigabitEthernet0/1, GigabitEthernet8/1, GigabitEthernet9/1
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#channel-group 1 mode auto
```

הגדרת Trunk
הגדרת הממשק במצב desirable

Show Commands

מציג את הקבוצות שנוצרו, ה프וטוקול והממשקים המשויכים – show etherchannel summary

מציג מידע על הממשקים של קבוצה מסוימת – show interfaces port-channel [num]

מציג מידע על כל קבוצה – show etherchannel port-channel

show etherchannel summary

```
SW1-D-JRS# show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       L - Layer2
      U - in use        f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

דגלים שעוזרים להבין את הפלט

מספר ערוצים בשימוש
Number of channel-groups in use: 1
מספר ערוצים שנוצרו ופועלים במתוג
Number of aggregators: 1

Group	Port-channel	Protocol	Ports
1	Pol(SU)	PAgP	Gig5/1(P) Gig6/1(P) Gig7/1(P)

ממשקים שאוחדו (בסוגרים הדגל)
הדגלים מספר קבוצה
פרוטוקול מספר קבוצה

show interfaces port-channel 1

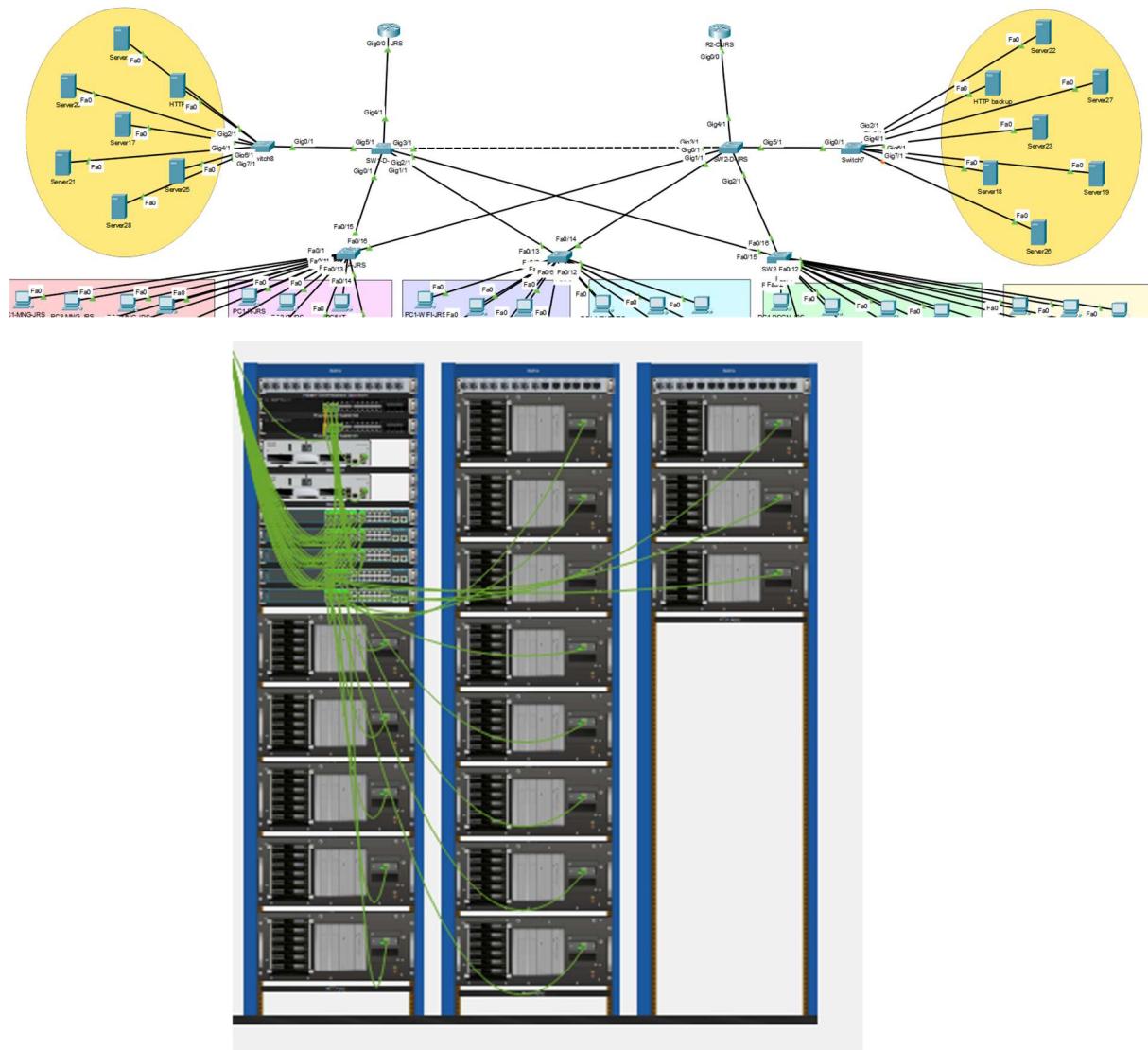
```
SW1-D-JRS#show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
Hardware is [EtherChannel], address is 0000.0c41.6126 (bia 0000.0c41.6126)
MTU 1500 bytes, BW 3000000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
[Half-duplex, 3000Mb/s]           רוחב הפס עלה בעקבות איחוד הממשקים
input flow-control is off, output flow-control is off
Members in this channel: [Gig5/1 ,Gig6/1 ,Gig7/1], הממשקים שאוחדו
```

show etherchannel port-channel

```
SW1-D-JRS#show etherchannel port-channel
    Channel-group listing:
    -----
    Group: 1      מספר קבוצה
    -----
        Port-channels in the group:
    -----
Port-channel: Po1
    -----
Age of the Port-channel = 00d:00h:40m:33s
Logical slot/port = 2/1      Number of ports = 3
GC                = 0x00000000      HotStandBy port = null
Port state        = Port-channel
Protocol          = [PAGP]          סוג פרוטוקול
Port Security     = Disabled

Ports in the Port-channel:
Index  Load  Port      EC state      No of bits
-----+-----+-----+
  0    00   Gig5/1   Desirable-S1    0
  0    00   Gig6/1   Desirable-S1    0
  0    00   Gig7/1   Desirable-S1    0
Time since last port bundled: 00d:00h:07m:46s [Gig7/1]
```

שרטים בסניף הראשון



על מנת לחבר את השירותים, נחבר למתגים בשכבה החומרית שני מתגים מסווג EMPTY
ולמתגים אלו נחבר את השירותים בטופולוגיה.

נדיר את המתגים החדשניים clients vtp על מנת שיוכלו לקבל את הווילאנים הנוכחיים. נוסיף להם את השם והסיסמה של שאר המתגים על מנת שיוכלו לתקשר איתם.

```

Switch(config)#vtp mode client          ← vtp clients
Setting device to VTP CLIENT mode.
Switch(config)#vtp domain JRS           ← Domain
Changing VTP domain name from NULL to JRS
Switch(config)#vtp password proj       ← נתגט סיסמא
Setting device VLAN database password to proj

```

עביר את החיבור בין המתגים החדשניים למתגים בשכבה ה-2 למצב Trunk Distribution

```

SW1-D-JRS(config-if)#switchport mode trunk ← trunk
SW1-D-JRS(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet5/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet5/1, changed
state to up

```

נדיר vlans חדשניים על מתג ה - vtp server יהיה שייך לוילאן 100 ושרותי הגיבוי (DMZ BACKUP) יהיו שייכים ל-VLAN 101.

```

SW1-D-JRS(config)#vlan 100             ← הגדרת הוילאנים החדשניים
SW1-D-JRS(config-vlan)#name DMZ        ← נתינת שם לוילאנים
SW1-D-JRS(config-vlan)#exit
SW1-D-JRS(config)#vlan 101
SW1-D-JRS(config-vlan)#name DMZ-B

```

נשייך את השירותים אל ה - VLAN אליו הם שייכים

```

Switch(config)#int gigabitEthernet 2/1   ← כניסה לממשק
Switch(config-if)#switchport mode access  ← העברת הממשק ל-access
Switch(config-if)#switchport access vlan 100 ← שייך הוילאן לממשק

```

נוסיף את vlan ב프וטוקול dot1q

```

R1-C-JRS(config)#int gi0/0.100           ← כניסה לממשק הוילאן
R1-C-JRS(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.100, changed state

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to up

R1-C-JRS(config-subif)#encapsulation do
R1-C-JRS(config-subif)#encapsulation dot1Q 100 ← הגדרת qtag על הממשק
R1-C-JRS(config-subif)#ip add
R1-C-JRS(config-subif)#ip address 10.1.100.252 255.255.255.0 ← נתינת כתובת IP לממשק
R1-C-JRS(config-subif)#exit

```

נוסיף אותו בפרוטוקול הsrp –

```
R1-C-JRS(config)#int gigabitEthernet 0/0.101
R1-C-JRS(config-subif)#standby 1 ip 10.1.101.254
R1-C-JRS(config-subif)#standby 1 priority 90
R1-C-JRS(config-subif)#standby 1 preempt
```

כניתה למשק הוילאן
הגדרת הכתובת הווירטואלית
הגדרת priority
הגדרת preempt למקרה בו המשק נופל וחוזר

נדיר spanning tree על המתגים החדשניים וbpdu gurard & portfast על המשקים לכיוון השירותים

```
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#int gi2/1
Switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on GigabitEthernet2/1 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if)#spanning-tree bpduGuard enable
```

נדיר root guard על המתגים בשכבות היס לכיוון המתגים החדשניים

```
SW2-D-JRS(config)#int gigabitEthernet 5/1
SW2-D-JRS(config-if)#spanning-tree guard root
```

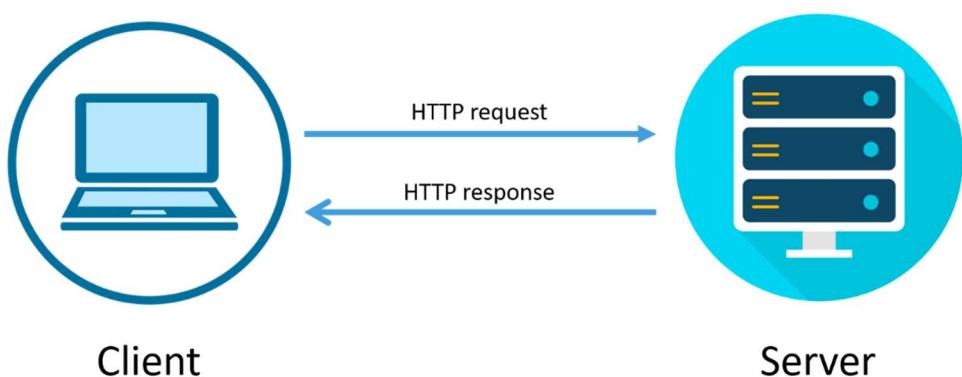
Hypertext Transfer Protocol

פרוטוקול (Protocol) HTTP (Hypertext Transfer Protocol) מהווה את אבן יסוד לתקשורת ברשת האינטרנט. הוא משמש להעברת מידע בין תקני הלקוח (דףנים ותוכנות דומות) והשתטים באמצעות פרוטוקול תקשורת מסוג TCP. ה-HTTP הוא פרוטוקול העובד בשכבה השביעית של מודל-ה-OSI ופועל בפורט 80. מטרתו הינה להבטיח אמינות ושלמות בהעברת המידע ברשת.

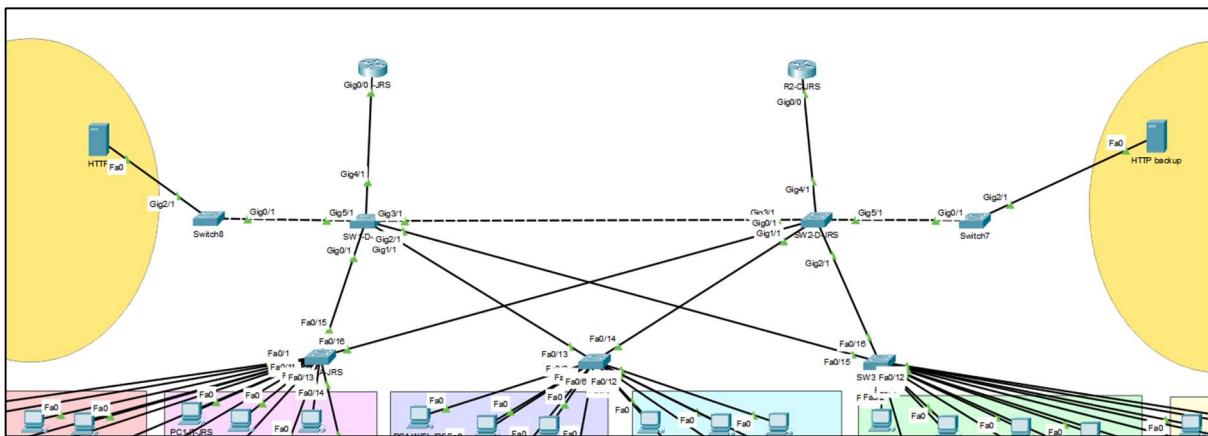
תהליך התקשורת באמצעות HTTP מתבצע כך: הלקוח (דףן) שולח בקשות לשרתים, והשתטים יחזירו בתגובה על מנת למלא את הבקשות. שירות האינטרנט מכיל תוכנה שמחכה לבקשת HTTP ומטפלת בהן באופן מתמיד כאשר הן מתקבלות. כל בקשה מעוברת מהלקוח לשרת דרך פועל GET, שמניעה לכתובת ה-IP של ה-URL המבוקש. תהליך זה משתמש בשירות DNS לתרגום של הכתובת.

בתגובה, התוכנה בשרת היעד שולחת לדף המבוקש, אשר נכתב בשפת HTML (Hypertext Markup Language). HTML היא שפת תגיוט המשמשת לכתיבה, עיצוב, ויצוף של דפי האינטרנט. בנוסף ל-HTML, ישנן שפות נוספות כמו XML ו-XHTML המשמשות למטרות דומות.

בנוסף לאבטחה, ניתן לזהות את האתרים המאבטחים באמצעות פרוטוקול HTTPS, הפעול בפורט 443. אתרים מאבטחים משתמשים בכתובת URL המתחילה ב-`https://`, לעומת זאת HTTPS משתמש ב-`http://`. ניתן גם לזהות את האבטחה דרך סימן המופיע בחלון הדפדפן.

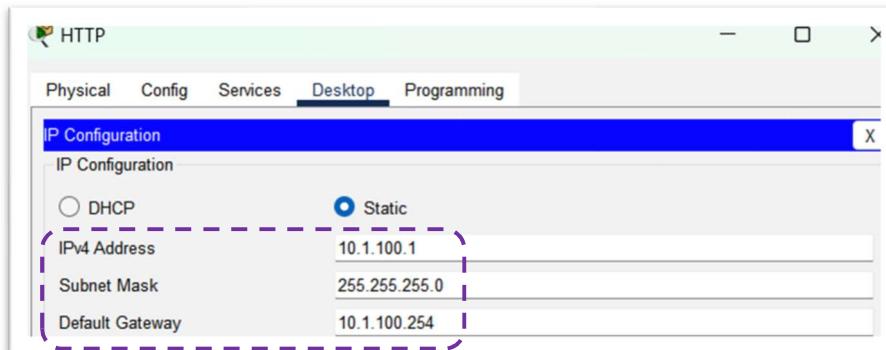


הגדרת שרת HTTP בסניף הראשון



הגדרה בשרת הראשי

הגדרת כתובות IP לשרתים

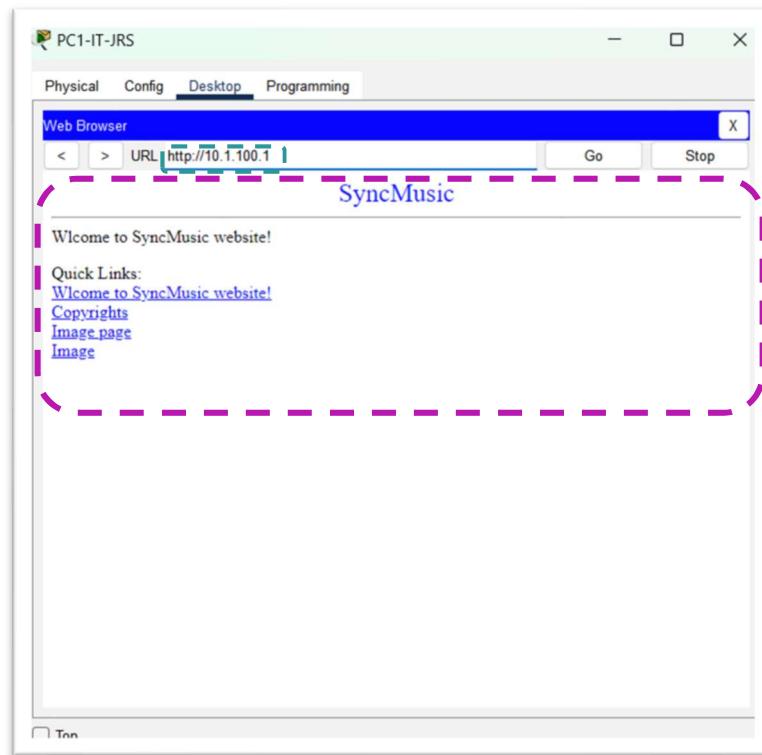


הגדרת שירות HTTP:

HTTP		HTTPS הפעלה																			
HTTP	<input checked="" type="radio"/> On	Off	<input checked="" type="radio"/> On																		
File Manager	<table border="1"> <thead> <tr> <th>File Name</th> <th>Edit</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>1 copyrights.html</td> <td>(edit)</td> <td>(delete)</td> </tr> <tr> <td>2 cscoptlogo177x111.jpg</td> <td></td> <td>(delete)</td> </tr> <tr> <td>3 helloworld.html</td> <td>(edit)</td> <td>(delete)</td> </tr> <tr> <td>4 image.html</td> <td>(edit)</td> <td>(delete)</td> </tr> <tr> <td>5 index.html</td> <td>(edit)</td> <td>(delete)</td> </tr> </tbody> </table>			File Name	Edit	Delete	1 copyrights.html	(edit)	(delete)	2 cscoptlogo177x111.jpg		(delete)	3 helloworld.html	(edit)	(delete)	4 image.html	(edit)	(delete)	5 index.html	(edit)	(delete)
File Name	Edit	Delete																			
1 copyrights.html	(edit)	(delete)																			
2 cscoptlogo177x111.jpg		(delete)																			
3 helloworld.html	(edit)	(delete)																			
4 image.html	(edit)	(delete)																			
5 index.html	(edit)	(delete)																			

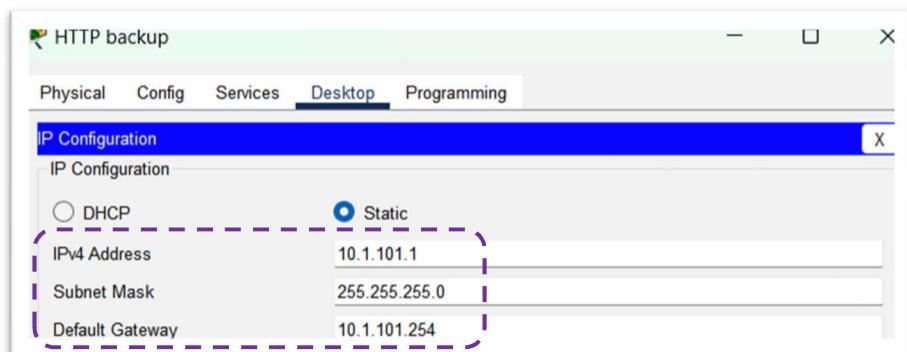
הקובץ של האתר

בדיקה שנייתן לגלווש אל האתר ממחשב



הגדרת Backup בשרת ה-HTTP

הגדרת כתובות IP לשרתים



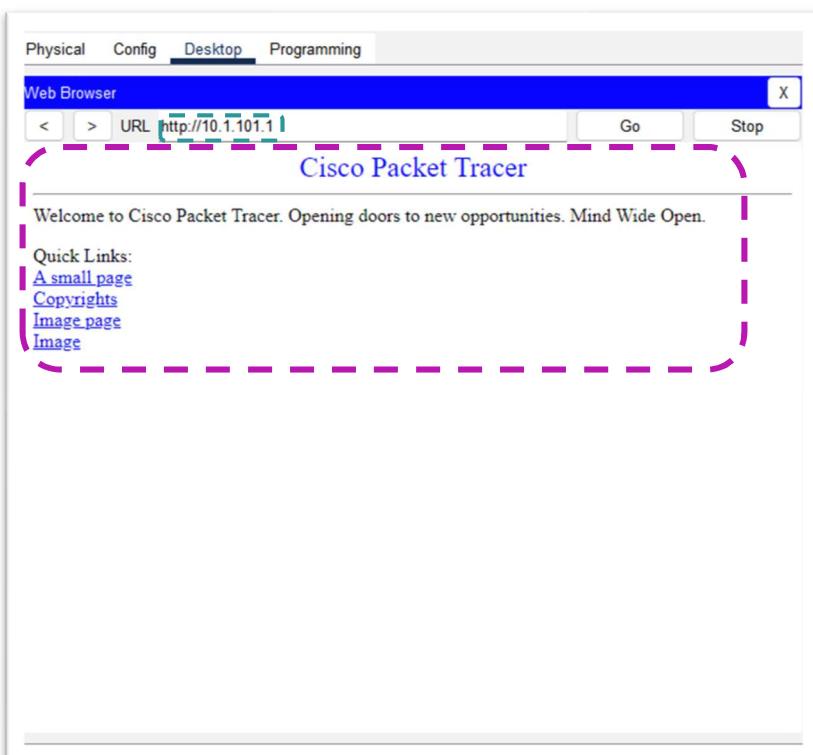
הגדרת שירות HTTP

The screenshot shows a configuration interface with two service status buttons at the top: 'HTTP הפעיל' (HTTP active) and 'HTTPS הפעיל' (HTTPS active), both set to 'On'. Below these are two radio buttons labeled 'Off'. Underneath is a 'File Manager' section with a table:

File Name	Edit	Delete
1 copyrights.html	(edit)	(delete)
2 cscoptlogo177x111.jpg		(delete)
3 helloworld.html	(edit)	(delete)
4 image.html	(edit)	(delete)
5 index.html	(edit)	(delete)

הקובץ של האתר

בדיקות שניות לגלווש מהאתר אל המחשב



Domain Name Server

פרוטוקול DNS הינו פרוטוקול שמטרתו להמיר כתובות URL לכתובת IP. פרוטוקול זה עובד בשכבה 7 במודול ה- OSI. הוא משתמש בפורט 53 בתקשורת UDP כברירת מחדל. כל התקן מאופיין בכתבota IP הייחודית לו, בה התקנים אחרים משתמשים על מנת לזהות את התקן ולתקשר אליו. ניתן לתקשר על ידי כתובות IP אך תקשור זה מצרייך לזכור כתובות ומספרים רבים אשר עלולים לבבל את המשתמשים. יותר קל לזכורשמות ואתרים מאשר כתובות ומספרים ולכן DNS נועד על מנת לפחות ולמairy את הכתובות של האתרים אל כתובות IP שלהם על מנת שנוכל לגשת אליהם.

DNS מושגים

Nslookup – שאלילת DNS המבצעת במטרה לקבל את כתובות IP שם הדומיין שהוכנס. אם נזין בשאלילת את שם הדומיין נקבל את כתובות IP ואם נזין את כתובות IP נקבל את שם הדומיין (נקרא .arpa dns).

Cache – הזיכרון של שרת DNS. נמצא בתחום השאלות הקודמות שנעשה. אם ממבצע שאלילה שבוצעה בעבר ושמורה בזיכרון cache ולא נגמר TTL (הסבר בהמשך), השרת יחזיר את הכתובת הנמצאת לו בזיכרון. אם היא אינה שמורה, השרת יעשה חיפוש רקורסיבי עליו ארחיב בהמשך על מנת להשיג את כתובות IP של הדומיין המבוקש. על מנת לרוקן את זיכרון Cache נריץ את הפקודה ipconfig /flushdns

Registrar – שרת המוכיר דומיינים חדשים. השרת יודא שהדומיין שנרכש יהיה שייך רק למי שקנה אותו (מוודא עם אחרים) ומלמד את אחד משורייניו Root dns על כל דומיין חדש שנוסף.

סוגי שירות DNS

Root DNS Servers – זהו שרת המאחסן רשימה של שרתי TLD. נכון לשנת 2019 קיימים 13 קיימים בעולם

TLD – שרת המנהל סיומות של URL. כגון .com, .net, .il ועוד

Domain DNS – שרת המנהל דומיינים.

מבנה כתובות URL

com, org, il (Top Level Domain) TLD -
Second-Level Domain -
Sub Domain -

Sub domain	Second-Level domain	TLD
www	google	com

תפקידו של שירות DNS

.1 - Recursive - כאשר משתמש פונה לשרת עם שאלתה לדוגמא www.abc.com על השרת יהיה לספק את כתובת IP : הפעולה של המורה משם דומין לכתובת זו נקראת Recursive DNS

Recursive DNS

אם הקן המבוקש לשאלתה שנשאר נמצא בcache הוא יחזיר אותו ישירות

אם לא יעשה את הפעולות הבאות :

- יפנה לשרת root - לשרת dns root שלנו יש רשימה של 13 שרת root בעולם, הוא פונה

לאחד מהם וسؤال אותו האם הוא יודע מי השירות TLD בעולם שמנהל את הסיומת .com. הוא עונה נכון (ה乞ן של השירות TLD בעולם שמנהל את הסיומת .com.).

- לאחר מכן יפנה לשרת TLD שמתפל בסיוומת .com. (דרך הכתובת 4.4.4.4) - שואל אותו

אם הוא יודע מי מנהל את השירות abc.com (השירות מתפל בכלכל הכתובת - מי שיש לו

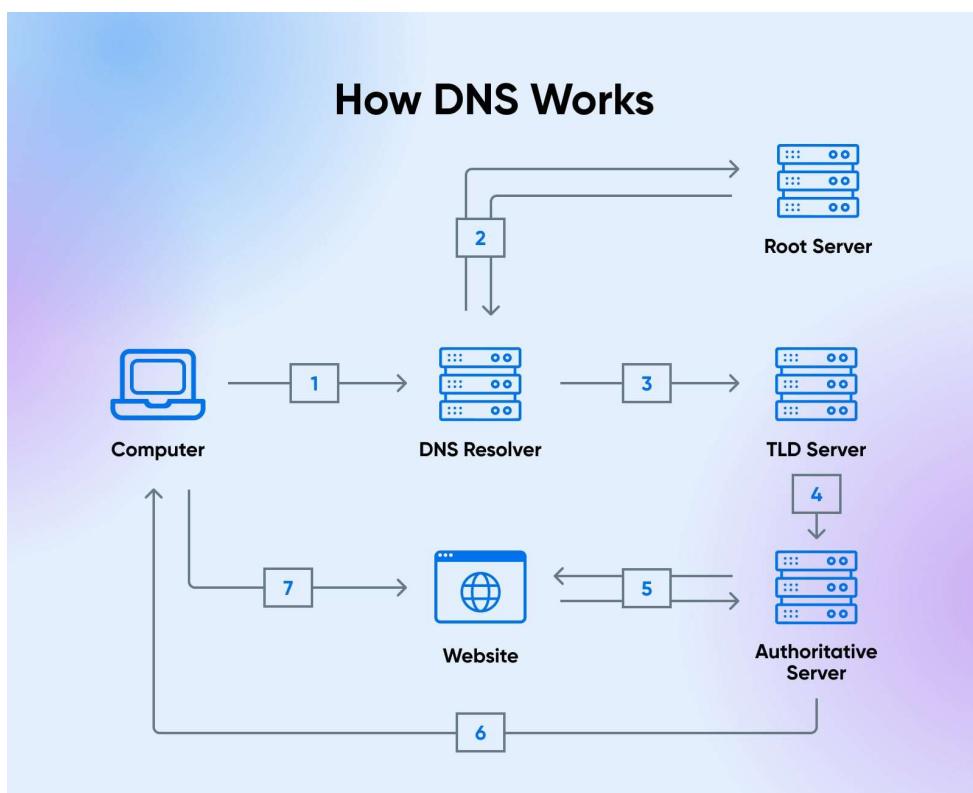
- סמכות לענות על הדומיין הסופי) (דרך הכתובת 5.5.5.5) - והוא מוחזיר לו לדוגמא

1.2.4.15 וזאת הכתובת שהשרות DNS שלו יחזיר לשימוש וישמור בזיכרון אצלך

בפעם הבאה שמייחחו ישאל עליו הוא יחזיר תשובה מהר כי יזכיר לפי כמות הזמן
שההערכיס לו בשניות (ברירת מחדל 3600 שניות) כלומר אחראי שעה יפנה
לaspers הシリיאלי השתנה. אם כן, הוא יקח את הדטה הבסיס ויבדוק אם הIP השתנה, אם כן
יעדכן את כתובת הIP.

* אם השירות DNS מקבל IP ושותה הIP המקורי אך לא נגמר TTL הוא יוכל לקבל את
השינוי רק בסוף TTL כלומר הוא יושלח לשרת הישן

.2 - authoritative DNS - מי שנותן תשבות לדומיינים מסוימים (מאחסן אצליו דומיינים).



רשומות DNS

- [time, default 3600] - מנגנון ויסות, אומר לשרת DNS בעולם כל כמה זמן מותר להם לבוא ולעשות שאילתת על שרת DNS של יישוב (Time To Live). למה שעיה ולא נגיד שבוע? אם תעשה עדכון בשרת ייקח לך שבוע לקבל את העדכון זהה הרבה זמן וכך מקובל בין שעיה לשעותיים
- SOA Record - מכילה מידע על הדומיין : אימייל של בעל השירות, כתובת שירות DNS, תאריך שינוי אחרון ומספר סיריאלי. בניו כך ; serial ; YYYYMMDD . מצינו متى היה העדכון האחרון בשרת.
- עוזר להוריד את העומס על השירות. פוטנציאלית יש מיליארד שרתים באינטרנט שיכולים לפנות אליו. המספר הסיריאלי משמש כdgeל : בפעם הראשונה שימושו פונה אליו והוא קיבל את המידע ויקח את המספר הסיריאלי. בפעם השנייה קיבל את המידע מחדש רק אם ורק אם TTL תקף ורף אם המספר הסיריאלי השתנה אז קיבל מספר סיריאלי חדש. אם לא השתנה אין צורך לחתול ולקראת את כל המידע (db) שוב.
- NS Record (Name Server) – כתובת שירות DNS שמנהל את החומרה DomainName
- MX Record (Mail eXchange) – מצין מי שירות Mail של דומיין זה, לאיזה שרת לשולח את הדואר. ניתן להכניס כמה כתובות והן יהיו שונות בתיעודו של דומיין. ככל שהמספר יותר קטן התיעודו יותר גבוה.
- TXT Record – לאפשר לבאים של הדומיין לשים במרקאות אייזה טקסט שבאו. כל מי שעשה שאילתת nslookup יכול לשאול גם על txtrecord. TXTRECORDS הוא גם מנגנון אונטיקציה (אמינות) כי רף הבאים יכול להוסיף טקסט
- A Record – הרשומה המכילה את כתובת IP של הדומיין
- AAAA Record – אותו דבר כמו A Recordbut(IPV6)
- CNAME Record – מעתק את כתובת ה IP לשם דומיין אחר. זה לא כתובת IP אלא את שם הדומיין שמננו אנחנו רוצים להעביר את כתובת ה IP.
- PTR Record – משמש לכתובת IP לכתובת URL. להמרה מכתובת IP לכתובת Reverse DNS. הפוך A Records

```
named.atuda.local.          IN      SOA     student274.atuda.local. adi.kinneret.co.il. (2022121301; serial; 28800; refresh: every 8 hours; 7200; retry: 2h; 604800; expire 1 week; 14400; minimum 4h)

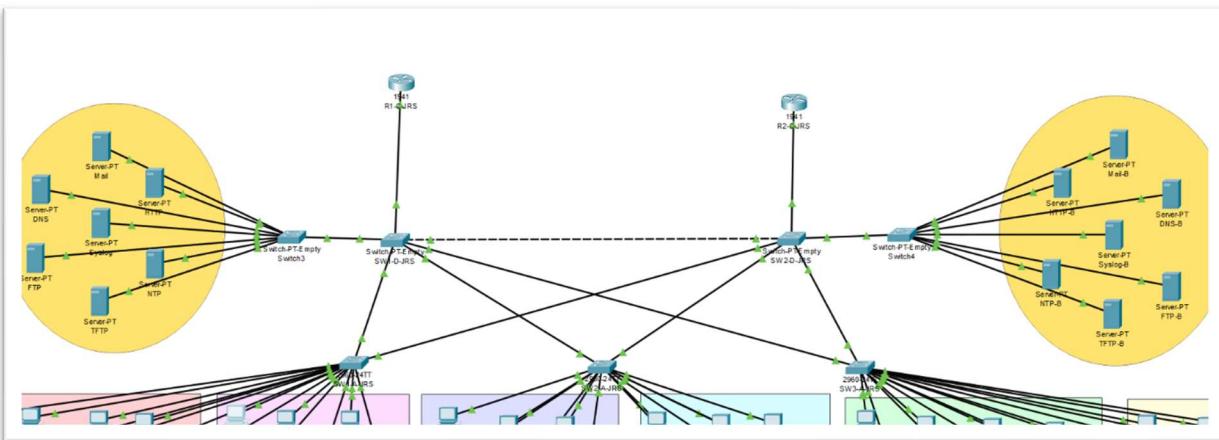
name servers
    IN      NS      student274.atuda.local.

MX Records
    IN      MX      10      student274.atuda.local.

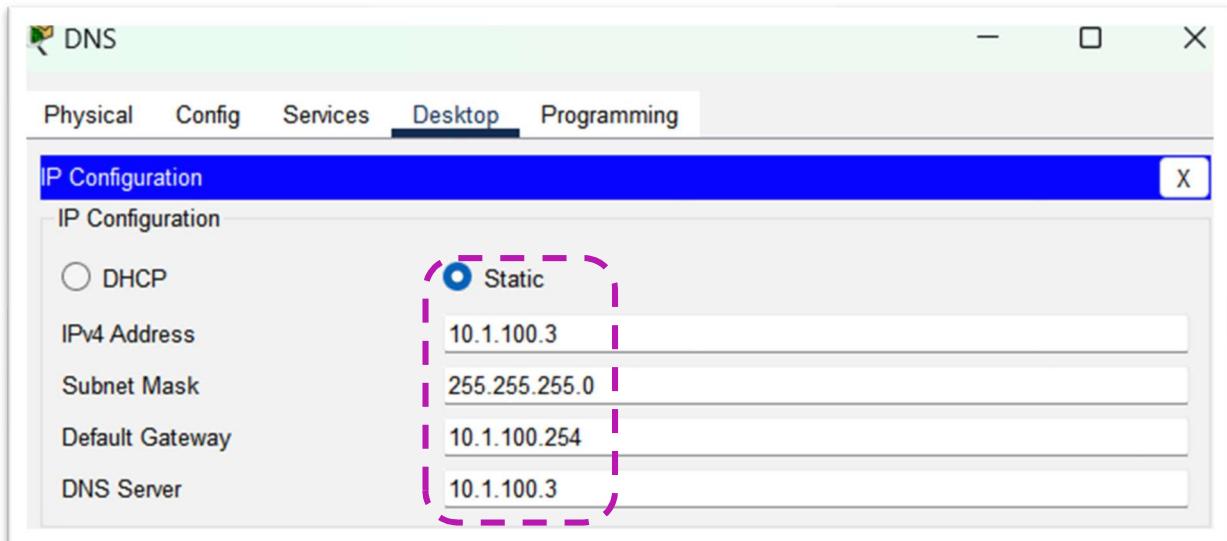
set the domain to answer calls
    IN      A       192.168.11.174
    IN      TXT     "v=spf1 ip4:192.168.10.0/23 ~all"

loopback address
localhost           IN      A       127.0.0.1
vm1<----><-----><----->IN<---->A<---->192.168.10.1
firewall           IN      A       192.168.10.254
student274         IN      A       192.168.11.174
server<----><----->IN<---->CNAME<->student274
```

הגדרת שרת DNS ראשי



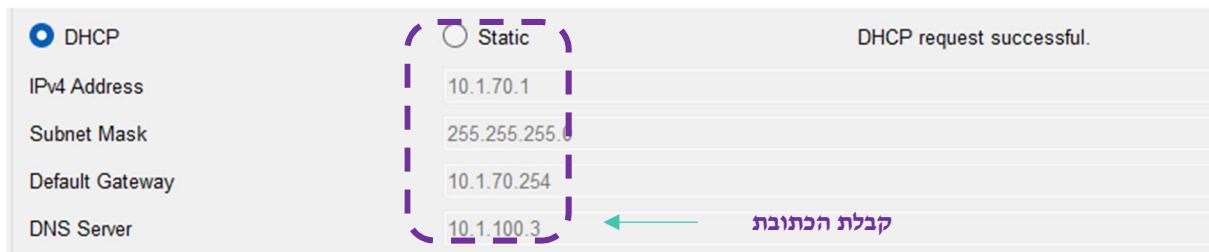
ネットית כתובת לשורת הראשי



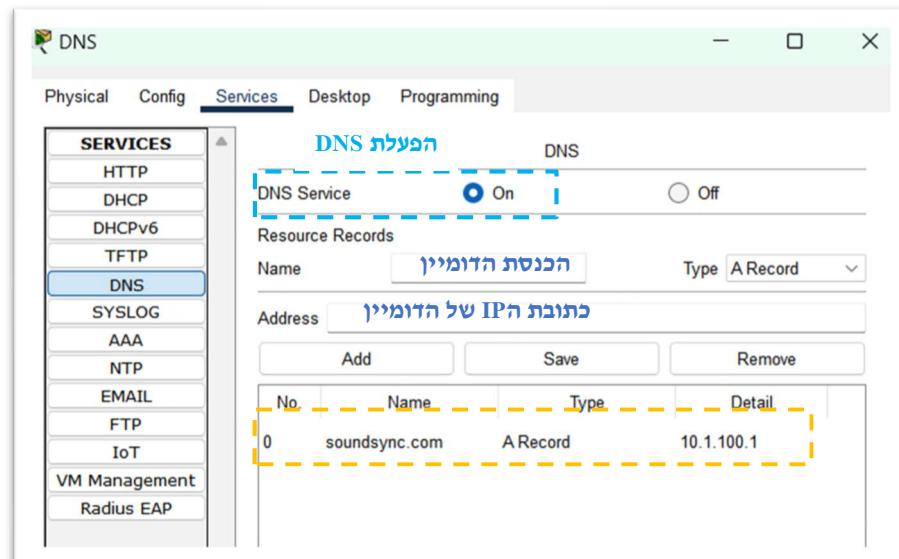
הוספה כתובות dns server בחלוקת כתובות על ידי dhcp

```
R2-C-JRS (config)#ip dhcp pool lan26 ← כנישת לpool
R2-C-JRS (dhcp-config)#network 10.1.26.0 255.255.255.0
R2-C-JRS (dhcp-config)#default-router 10.1.26.254
R2-C-JRS (dhcp-config)#dns-server 10.1.100.3 ← שיזן כתובות
server dns
```

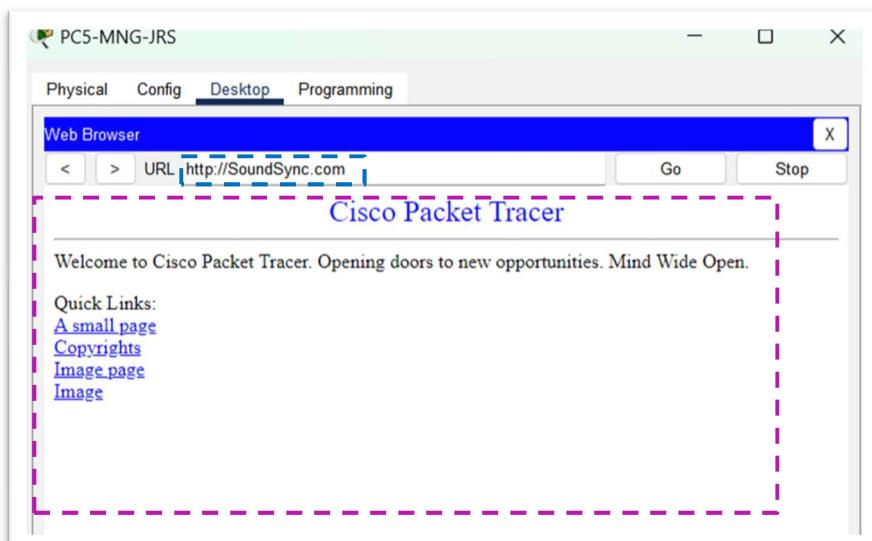
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנתב קיבלו את כתובת DNS של השירות הראשי



הגדרת שירות DNS

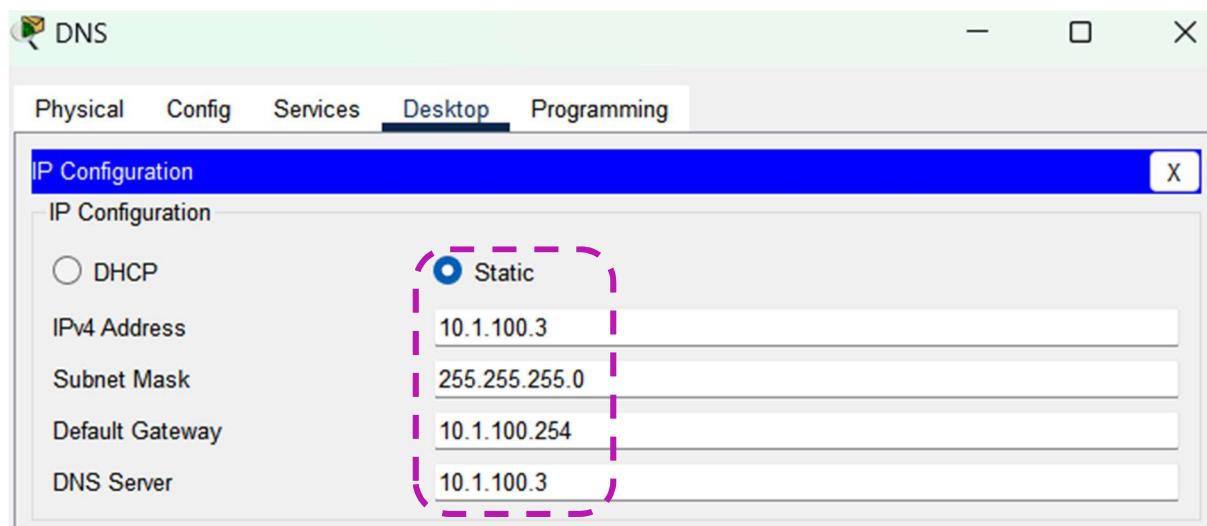


בדיקה על ידי גלישה לאתר לפי כתובת הדומיין



הגדרת שירות DNS גיבוי

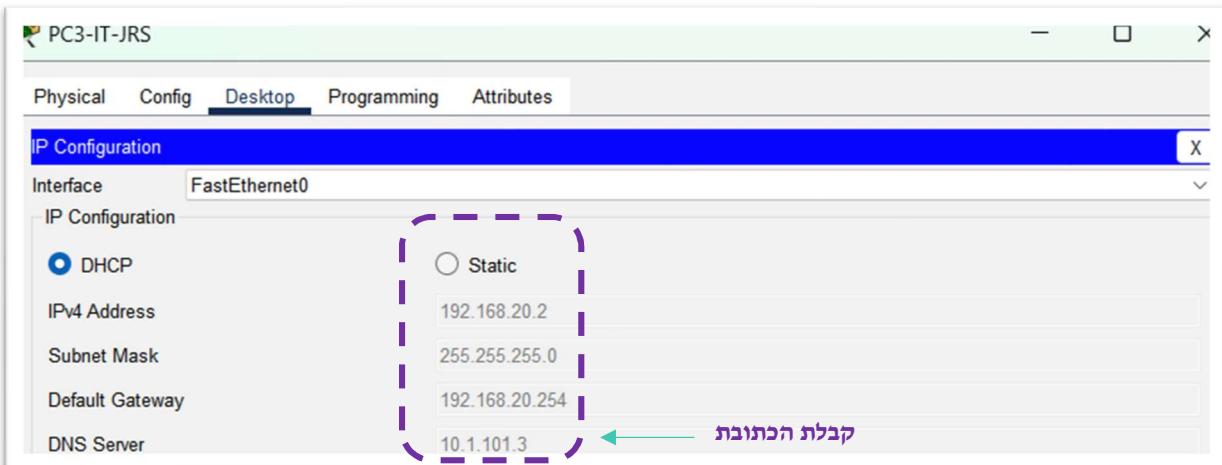
נתינת כתובות לשרת גיבוי



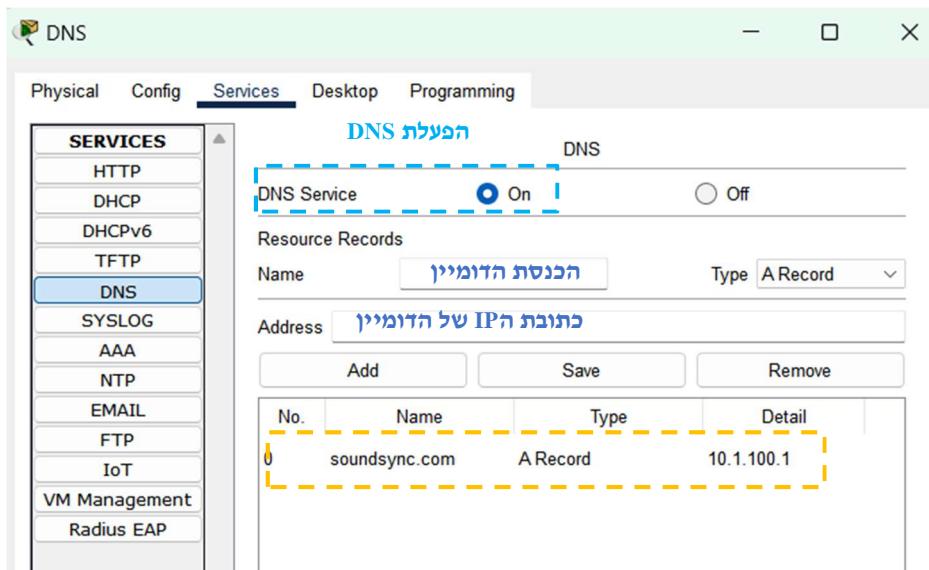
הוספה כתובות dns server בחלוקת כתובות על ידי dhcp

```
R1-C-JRS (config)#ip dhcp pool lan40 ← כניסה לpool
R1-C-JRS (dhcp-config)#dns-server 10.1.101.3 ← שיווק כתובות
R1-C-JRS (dhcp-config)#exit
R1-C-JRS (config)#ip dhcp pool lan50
R1-C-JRS (dhcp-config)#dns-server 10.1.101.3
R1-C-JRS (dhcp-config)#exit
R1-C-JRS (config)#ip dhcp pool lan60
R1-C-JRS (dhcp-config)#dns-server 10.1.101.3
R1-C-JRS (dhcp-config)#exit.
```

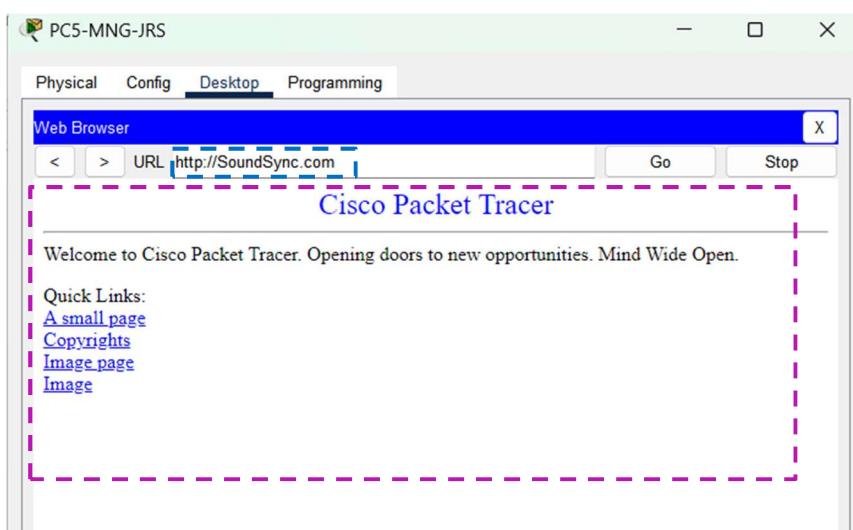
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנתב קיבלו את כתובת DNS של השירות גיבוי במקורה והשירות DNS הראשי נפל



הגדרת שירות DNS



בדיקה על ידי גלישה לאתר לפי כתובת הדומיין



שרת דואר (Mail Transfer Agent) MTA הינו שירות שמטרתו קיבלת דואר אלקטרוני נכנסת עבור משתמשים מקומיים בעלי תיבת מייל משולחים מרוחקים ובנוסף העברת דואר אלקטרוני מהמשתמשים כלפי חוץ. לשרת המייל קיימות תוכנות מסוימות המאפשרות לו ליצור מערכת הודעות המכילה את כל היישומים הנדרשים על מנת לשמור על תעבורת חלקה של הדואר. על מנת להשתמש במודול המכילה את כל ולקראם ממנה את ההודעות, עליו להשתמש במכשיר אינטרנט או תכנה, לדוגמה : outlook .outlook

פרוטוקולים המשמשים לשילוח וקבלת דואר אלקטרוני:

שליחת דואר :

SMTP (Simple Mail Transfer Protocol)

SMTP הוא פרוטוקול הפועל בשכבה 7 במודל OSI והוא הפרוטוקול הסטנדרטי המשמש לשילוח דואר אלקטרוני. פרוטוקול זה עובד בפורט 25 ובתקורת מסог TCP .

כאשר משתמש רוצה לשלוח דואר, הוא פותח אל השירות SMTP חיבור מסוג TCP . שירות SMTPamazon באופן תמידי ולכוamazon כאשר המשתמש פותח חיבור. لأن שנוצר החיבור, ישלח דואר המשתמש.

קבלת דואר :

POP3 (Post Office Protocol)

POP3 הוא פרוטוקול בשכבה 7 במודל OSI והוא פרוטוקול המשמש למשיכת מיילים משרת הדואר. הפרוטוקול עובד בפורט 110 ובתקורת מסוג TCP .

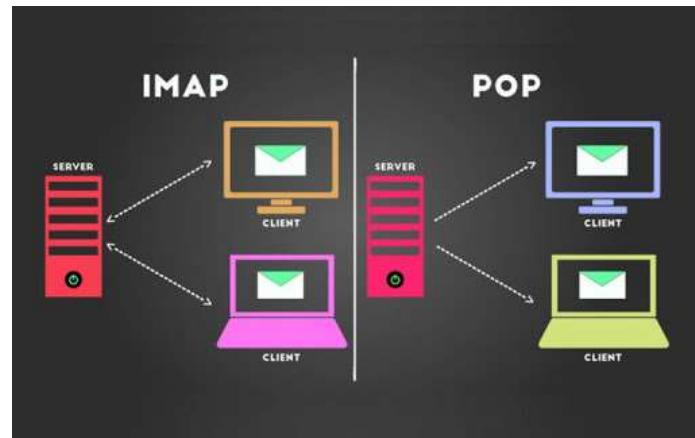
בפרוטוקול זה, המשתמש צריך להיכנס לתוכנת הדואר ומשם למשוך את הדואר מהשרת אל המחשב הפרטיא שלו. לאחר המשיכה והקריה של הדואר, ההודעה תימחק מהשרת.

IMAP (Internet Message Access Protocol)

IMAP הוא פרוטוקול בשכבה 7 במודל OSI והוא פרוטוקול המשמש למשיכת מיילים משרת הדואר. הפרוטוקול עובד בפורט 143 ובתקורת מסוג TCP . פורט 143 משמש כברירת מחדל במצב ובו אין הצפנה. על מנת להשתמש בהצפנה נעשה שימוש בפורט 993 .

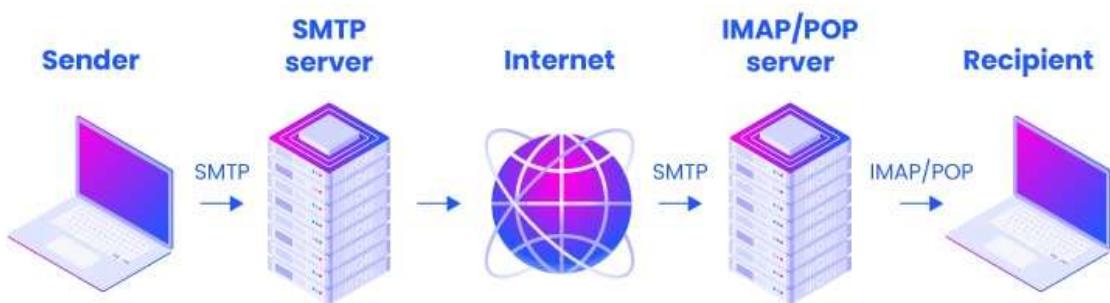
בIMAP בנויגוד לPOP3, המשתמש אינו צריך למשוך את הדואר אליו למחשב על מנת לקבל את המידע. הלקוח מתחבר לשרת מרוחק ויכול לקרוא את ההודעות בכל זמו שירצה (לדוגמה gmail@gmail.com משתמש בPOP3)

לשימוש בIMAP קיימים יתרונות כגון אבטחה, סyncron, וגישה מרוחק, וחסרונות כגון מרכיבות תחזקה, תמיכה בכל סוג הודעה, זמינות הדואר תלויה בחיבור לאינטרנט ועוד .

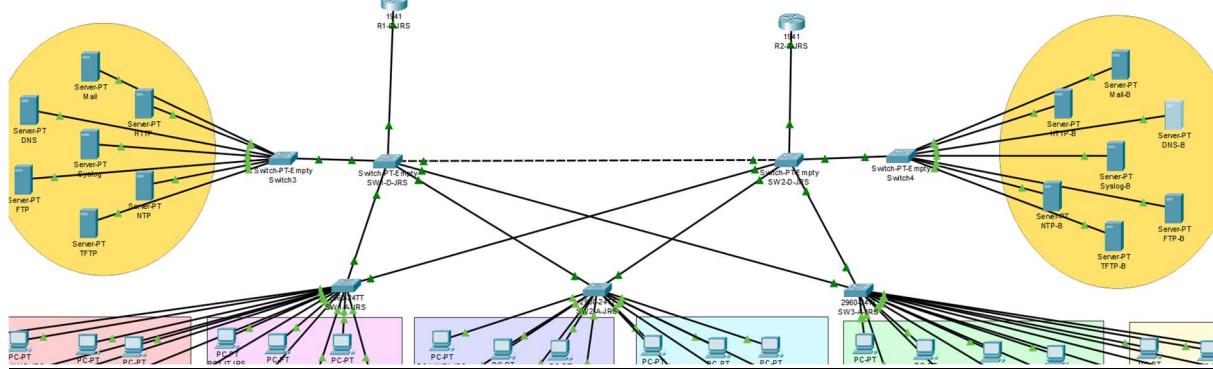


תהליך עבודה שרת המail

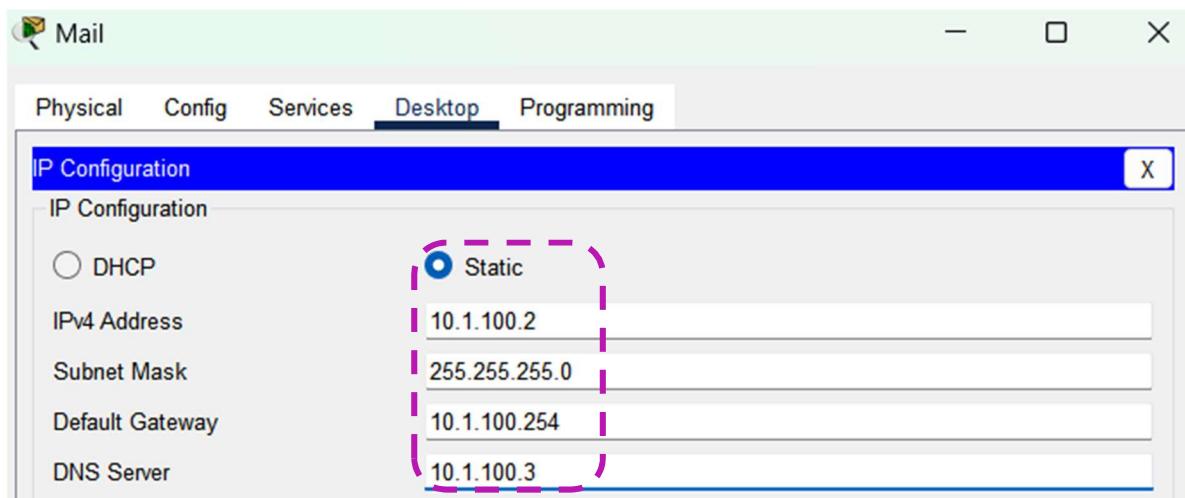
- כתיבת המail על ידי המשתמש תוך שימוש בתוכנה שאליה הוא מחובר ולחיצה על כפתור שלח
- התחברות המשתמש לשרת SMTP
- זיהוי ועיבוד כתובת הדואר האלקטרוני של הנמען, תוכן ההודעה וקבצים נוספים שצורפו, על ידי שרת SMTP
 - אם שם הדומיין שווה לשם השולח, ההודעה תישלח אל דומיין זה ישירות
 - אם שם הדומיין אינו שווה לשם השולח, יפנה שרת המail אל שרת DNS במטרה להציג את כתובת שרת המail המקורי של הנמען היota ושרת המail לא מכיר את שם דומיין זה
 - שרת DNS יוכל חיפוש וקורסיבי במטרה למצוא את הכתובת של שרת המail המקומי של הנמען ויעביר את הכתובת אל שרת המail
 - שרת המail שלנו ישלח את המail לכתובת שרת המail של הנמען, אותו קיבל משרת DNS



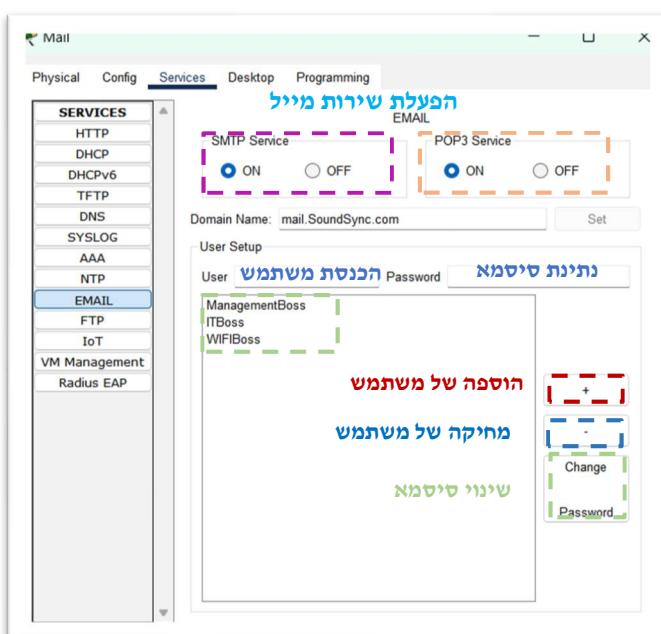
הגדרת שירות מייל ראשי



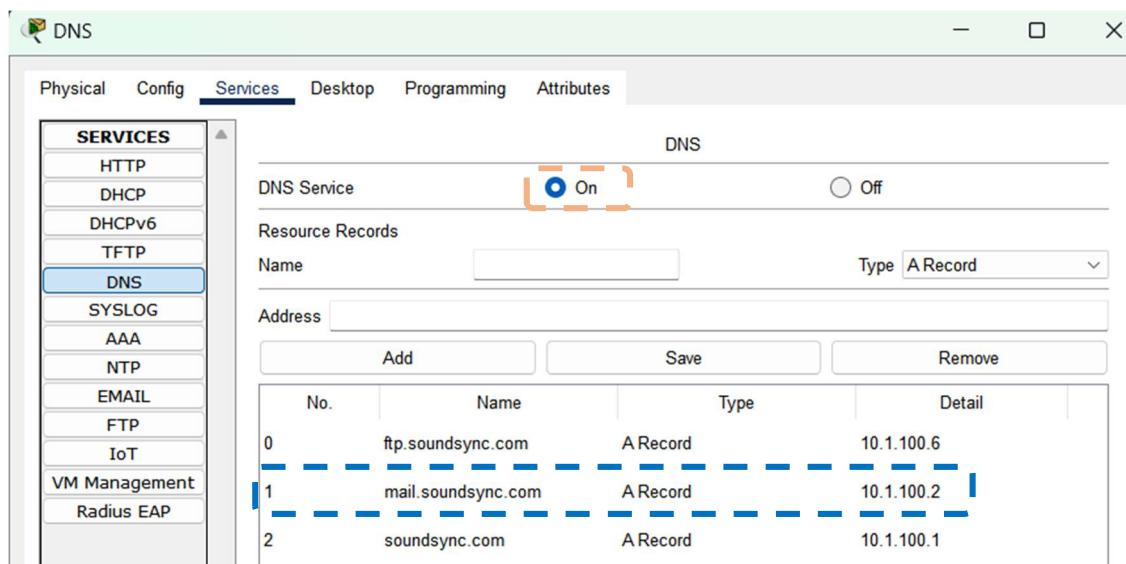
נתינת כתובות לשרת



הגדרת שירות mail

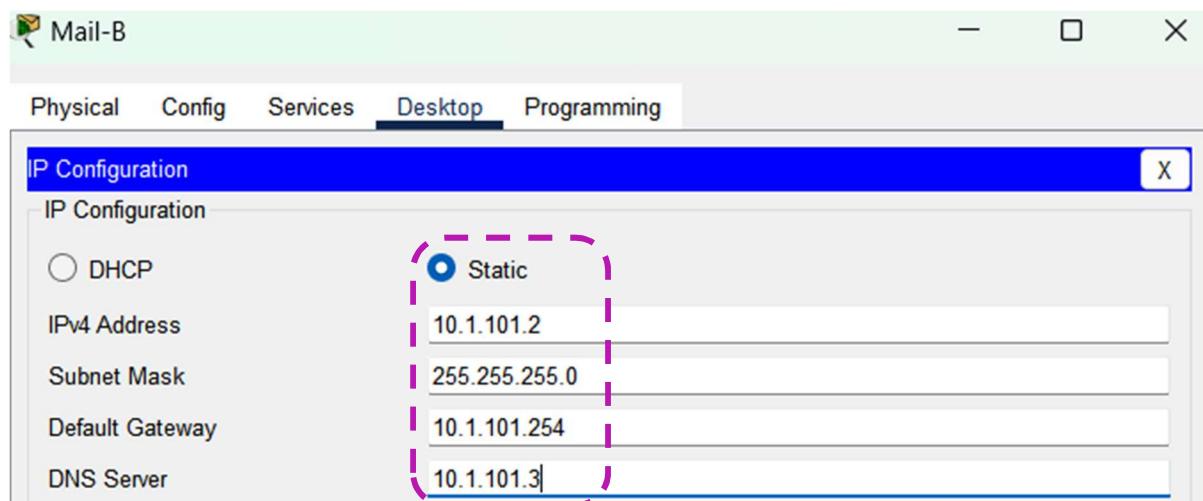


הוספת הילן לשרת mail

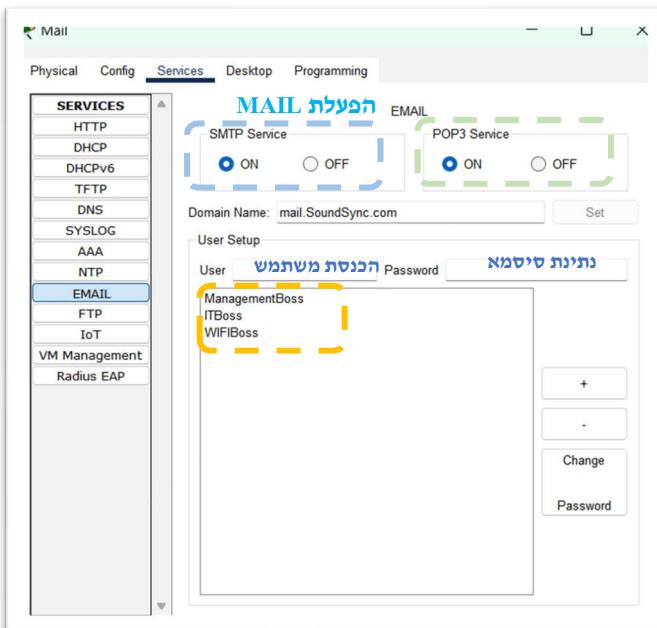


הגדלת שרת מייל Backup

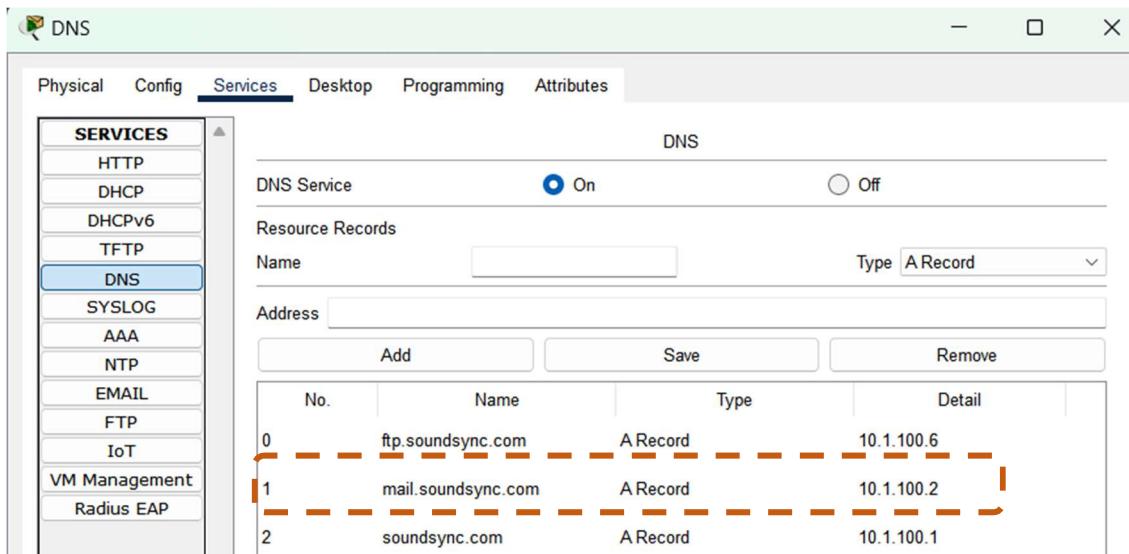
נתינת כתובות לשרת



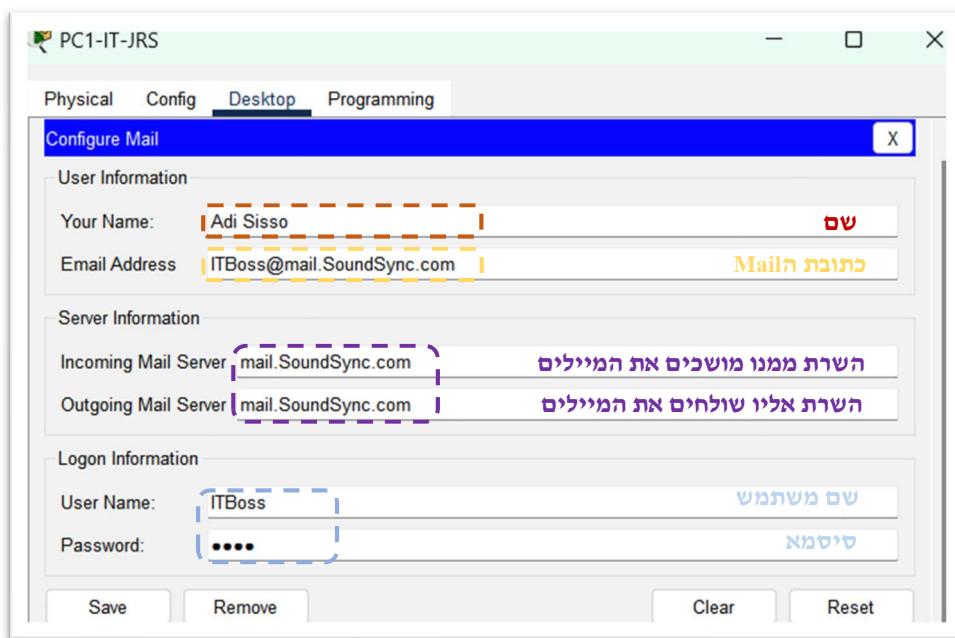
הגדרת שירות Mail



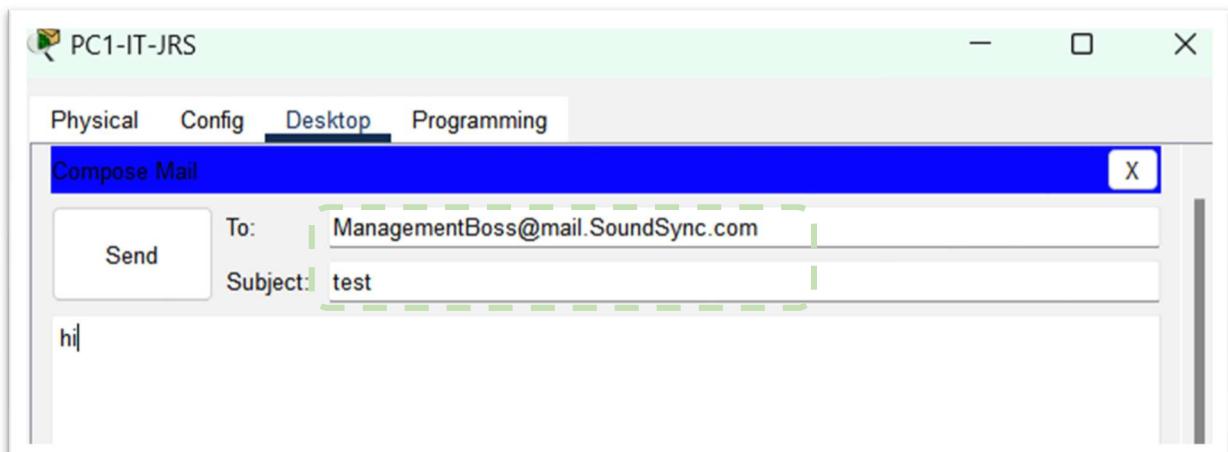
הוספה ה-SNMP לשירות mail



בדיקה – התחברות משתמש דרך מחשב



בדיקה – שליחת מייל



בדיקה – קבלת מייל

	From	Subject	Received
1	ITBoss@mail.Sound...	test	Sun Dec 3 2023 00:35:58

שרת Syslog

logs – רשומותיו יומן. ההתקנים בשרת יוצרים Logs המתעדים אירועים ומצבים המתרחשים בשרת, לדוגמא בport security כאשר מתרחש violation נוצרת הודעה log המתעדת את ההפרעה. כאשר המערכת קטנה, המעקב אחר הלוגים אפשרי, אך כאשר הרשות גדולה וכמות הרשומות הוא גדול, החיפוש אחר log ספציפי קשה מאוד. לכן משתמשים בשרת syslog

syslog

syslog הינו פרוטוקול סטנדרטי השולח הודעות logs שונים מהתקני הרשות, ועוזר לנו לאת הרשומות השונות בצורה נוחה. ה프וטוקול יכול לשמש על מנת לטעוד אירועים שונים כמו שינוי במצב של מסך, בדיקה במצב בו קرتה פועלה לא שגרתית או חסודה בשרת, פריצה או עומס חריג בשרת, הפעלה מחדש של מערכת ועוד. כל הפעולות הללו יתועדו באמצעות קבצי log אותם ניתן לראות על מנת לאתר את הבעיה, להבין ממה היא נובעת ולהציג מידע על מנת לתקן אותה.

פרוטוקול זה עובד בפורט 514 ובתקשורת מסוג UDP. אם נרצה שהשרת יעבד בצורה מאובטחת יותר, נגיד רישיון בתקשורת מסוג TCP ובפורט 6514.

על מנת שרשומות המידע יהיו אמינים מבחינת זמן, שרת זה יעבד בשיתוף עם שרת NTP בשביל חותמות זמן (Timestamp). על שרת NTP נרჩיב בהמשך.

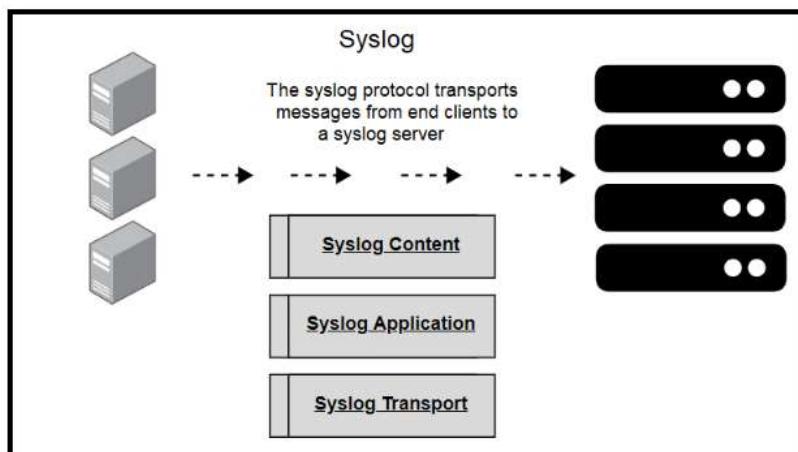
הפעולות שנעשות/syslog

פרוטוקול syslog עובד בשלושה שכבות : שכבת התוכן, שכבת התעבורת ושכבת היישום

שכבת התוכן – שכבה זו נמצאים הנתונים הנמצאים בהודעה המתארת את האירוע

שכבת התעborת – שכבה זו אחראית על העברת ההודעה בשרת

שכבת היישום – שכבה זו אחראית על ייצור ההודעה ואחסוננה, פירוש ההודעה וניטובה בשרת.



רמת חומרה של הודעות syslog

רמת החומרה של הודעה מגדירה אילו הודעות ישלחו אל השרת. ללא רמת חומרה, כל הודעות syslog ישלחו אל השרת, כמוות רבה של הודעות משמעו עומס רב על השרת ועלול להביא למצב שהשרת יסתם. לכן על השרת שלנו נגדיר מאייזה רמה נרצה שהרשות ישמרו

תיאור	שם	רמה
המערכת אינה שמיישת	Emergency	0
יש לפעול באופן מיידי	Alert	1
תנאים קריטיים	Critical	2
תנאי שגיאה	Error	3
תנאי אזהרה	Warning	4
מצב תקין אך משמעוני	Notice	5
מידע	Informational	6
איתור באגים	Debugging	7

רמה 7 – ההתראות הכיו פחות חשובות, רמה נמוכה, תיעודף נמוך.

רמה 0 – ההתראות הכי חשובות, רמה קריטית, תיעודף גבוהה

כאשר נבחר את רמת ההתראות שנרצה שהשרת יתייחס אליהן, השרת יתייחס לכל ההתראות מהרימה שבחרכנו ולהתראות ברמות שמתחרתיה ככלומר אם נבחר שהשרת יראה הודעות מרמה 5, השרת יתייחס לרמות 5 4 3 2 1 0 .

מבנה הודעות Syslog

seq – מספר סידורי המציין את סדר ההודעה

– חותמת המציין את הזמן המדויק בו קרה האירוע Timestamp

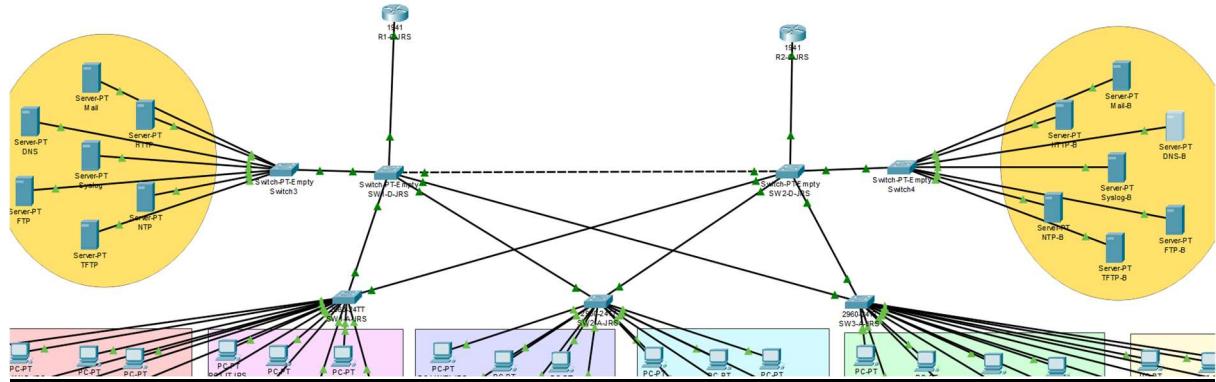
– ערך המציין את התהליך אשר יצר את ההודעה במכשיר Facility

– מאפיין את חומרת האירוע , 0 – 7 לפי הטבלה לעילו. Severity

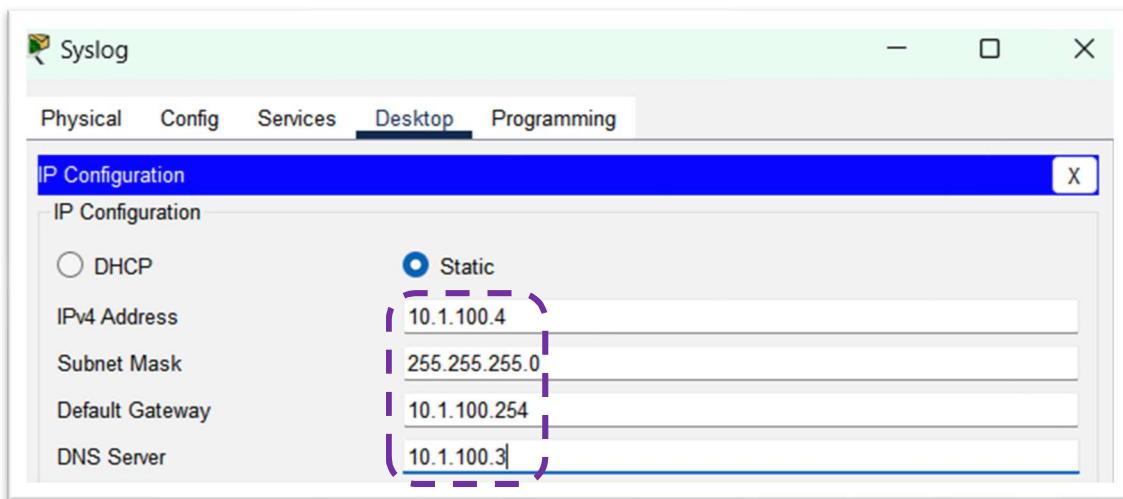
– קוד המאפיין את האירוע שקרה בקיצור MNEMONIC

– מידע המפרט את האירוע שקרה Description

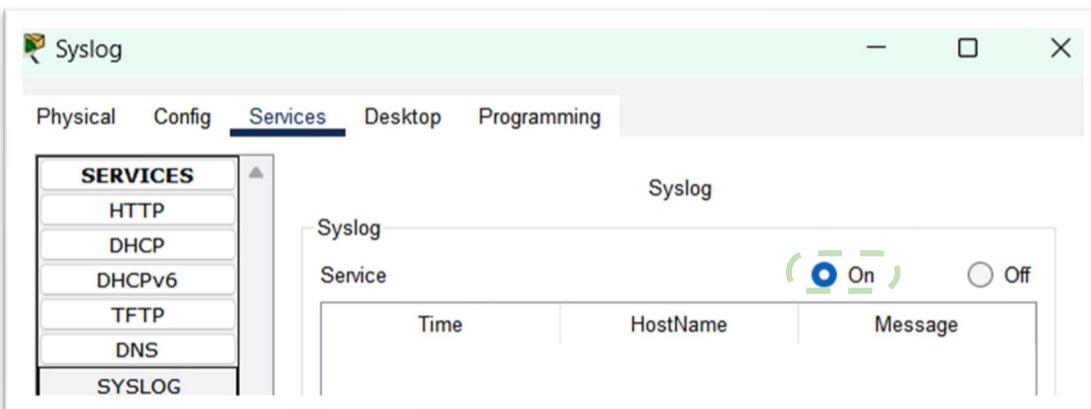
הגדרת שרת Syslog הראשי



הגדרת כתובות IP לשרת



הפעלת syslog

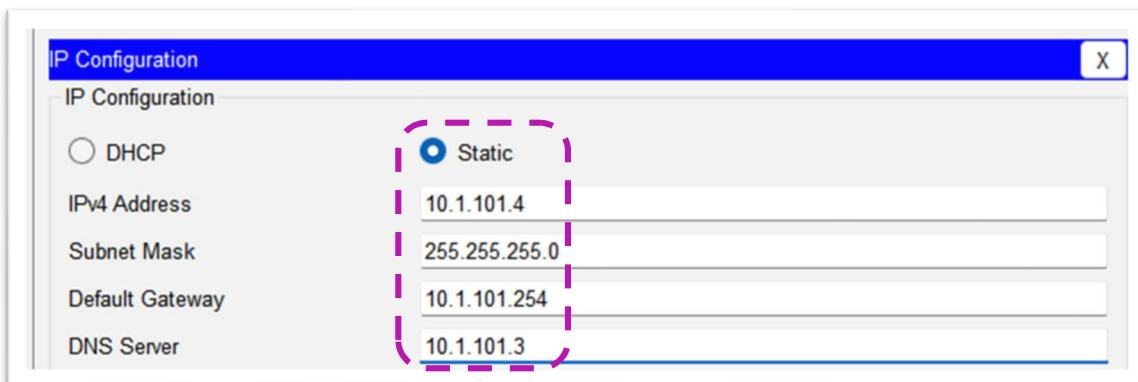


הפעלת שירות Syslog על המתגים והנתבים ברשת

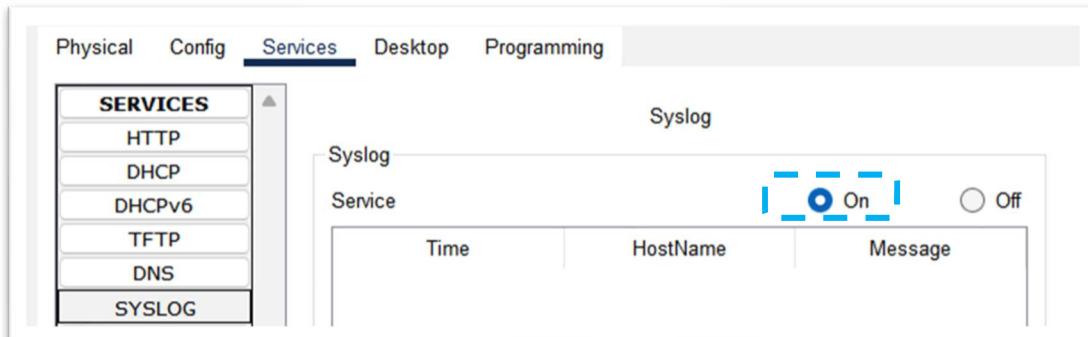
```
R1-C-JRS (config) #logging host 10.1.100.4 |  
R1-C-JRS (config) #logging host 10.1.101.4 |  
                                     גדרה מי שרת syslog
```

הגדרת שרת Backup Syslog

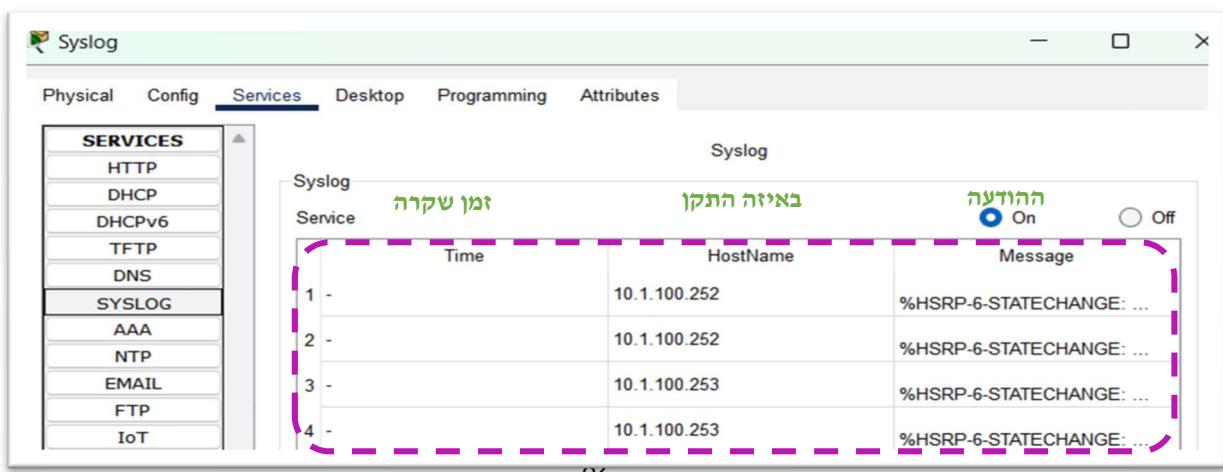
הגדרת כתובת IP לשרת



הפעלת שירות Syslog על המתגים והנתבים ברשת



בדיקה שליחת רשומות Logs



Network Time Protocol

על השעונים של כל ההתקנים ברשת להיות מסונכרים ביניהם על מנת שתיהה האפשרות לעקוב בצורה אמינה ולתעד את logs הנשלחים על ידי Syslog. קיימים שתי דרכי לסקורן את השעונים של ההתקנים ברשת:

- הגדרת השעה והתאריך באופן ידני
- הגדרה באופן אוטומטי על ידי פרוטוקול NTP

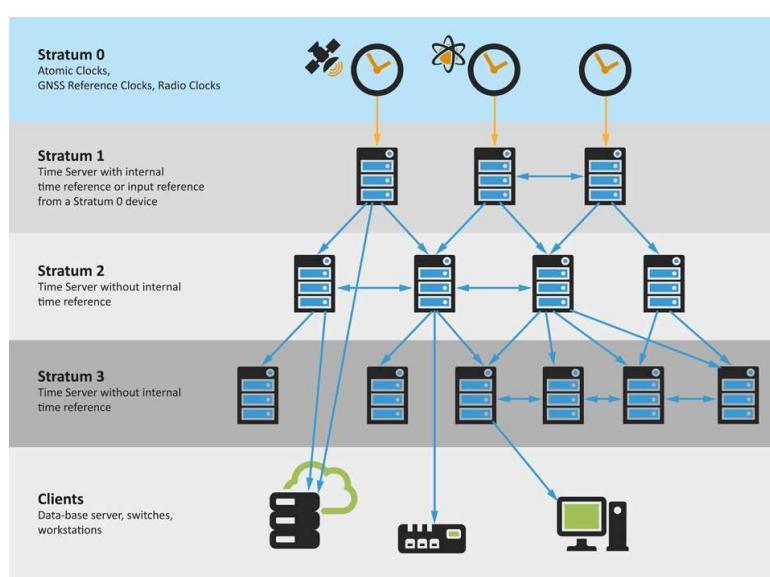
NTP הוא פרוטוקול אינטראקטיבי שמטרתו לסקורן את השעונים בהתקנים ברשת. פרוטוקול זה פועל בשכבה 7 במודל ה-OSI.

לפי NTP קיימים מספר תכונות

- לשרתים - NTP קיים גישה לשעונים אוטומטים וشعוני GPU מדויקים על מנת להבטיח סync'ון מירבי
- NTP משתמש בזמן אוניברסלי על מנת לסקורן את השעון של המעבד
- NTP מספר שבירת זמן באופן עקבי בשלבי הקבצים

תהליכי עבודה NTP:

פרוטוקול זה עובד במבנה היררכית. בשכבה 0 קיימים שעוני GPU או שעוני אוטומטים. שעונים אלו מחושרים אל שרת NTP הנמצא בשכבה 1, לשרת זה יחויבו שרתים נוספים הנמצאים בשכבה 2, אליו יחויבו שרתים הנמצאים בשכבה 3 וכך אלה. ככל שמספר השכבות גבוה יותר כך רמת האמינות נמוכה יותר. ערך האמינות שווה למספר השכבה בה נמצא השרת אשר ממנו הרשות לocket את המידע. ערך נמוך יותר משמע אמינות המידע גבוהה יותר. המידע נחשב כאמין עד שכבה מס' 9.

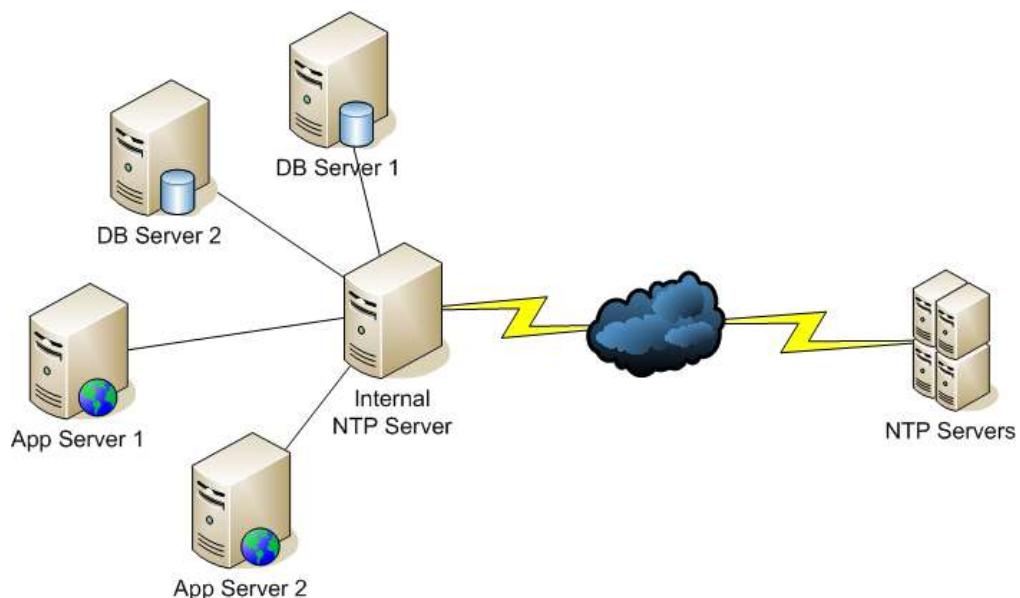


יתרונות לשנכרון על ידי NTP:

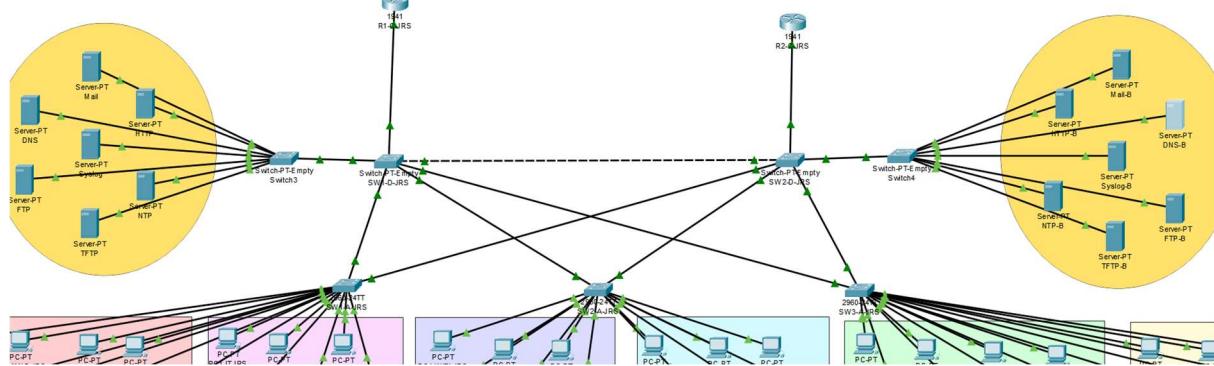
- סנכרון אינטראני בין המכשירים בראשת
- אבטחה משופרת
- שימוש במערכות Authentication
- האצה של הרשת על מנת לפחות בעיות

חסרונות לשנכרון על ידי NTP:

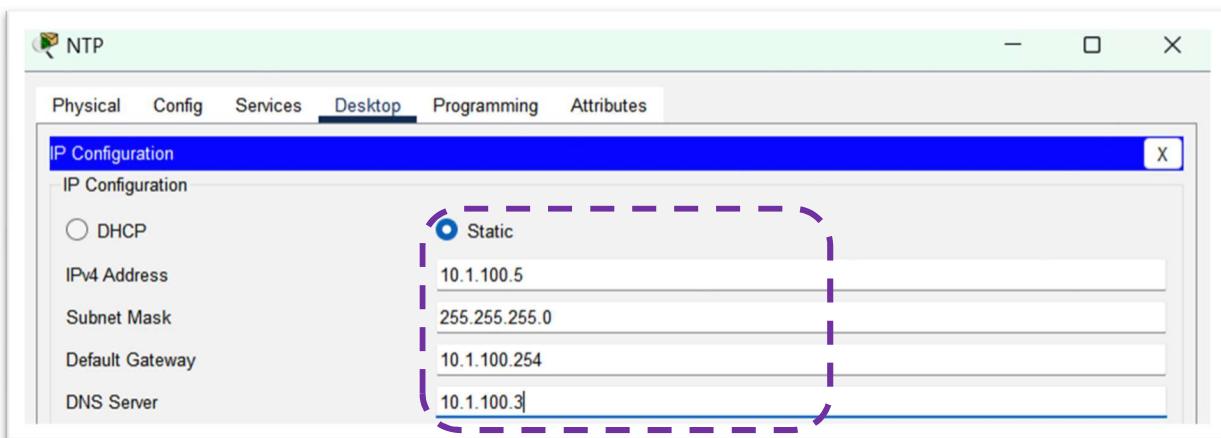
- עקב איזורי הזמן השונים, שירותי אלו עלולים למועד לשגיאות רבות מה שיכול להוביל להתקשרות.
- כבilities NTP גדולות עלולות לגרום להתקשרות בסנכרון.
- ניתן לעשות מניפולציה בסנכרון
- זמן הסנכרון מושפע כאשר השירותים מושבתים



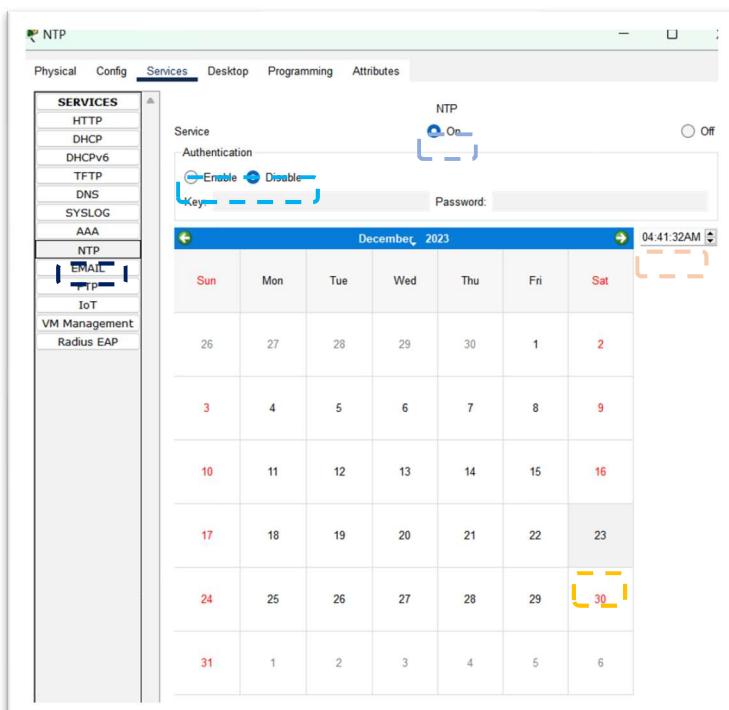
הגדרת שירות NTP ראשי



הגדרת הכתובות בשרת הראשי



הפעלת שירות NTP



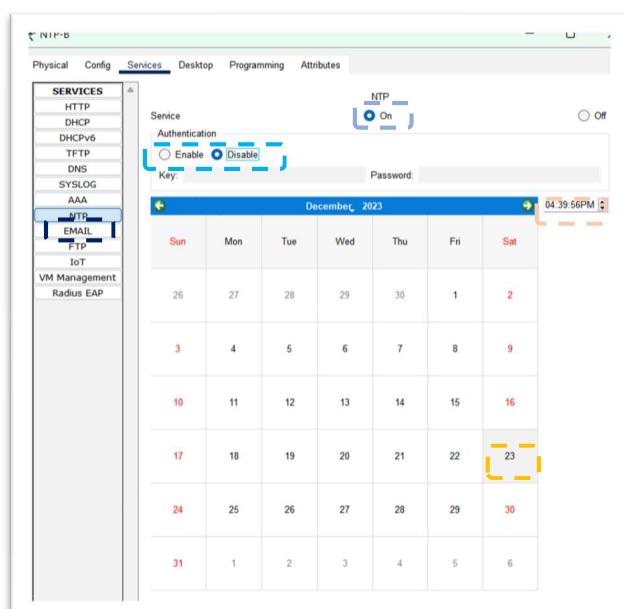
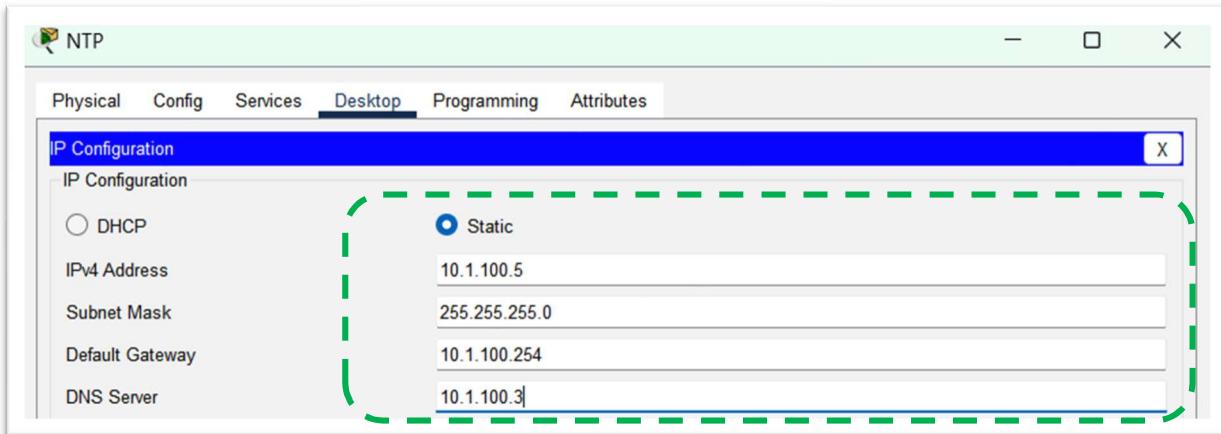
הפעלת השירות על כל הנטבים והמתגים ברשת

```
R1-C-JRS (config)#ntp server 10.1.100.5  
R1-C-JRS (config)#ntp server 10.1.101.5  
R1-C-JRS (config)#service timestamps log datetime msec
```

הגדרה מי שרת ה NTP
הוספה זמן ללוגים

הפעלת שירות NTP בשרת ה Backup

הגדרת הכתובות בשרת הראשי ובשרת ה Backup



הפעלת שירות NTP

בדיקות שהשירות עובד

DHCP	DHCPv6	TFTP	DNS	SYSLOG	AAA	Service	On	Off
						Time	12.23.2023 04:41:59.588 PM	10.1.100.253
						HostName		%SYS-5-CONFIG_I: Configured from console by console

Message: %SYS-5-CONFIG_I: Configured from console by console

Message: %SYS-5-CONFIG_I: Configured from console by console

File Transfer Protocol

FTP הינו פרוטוקול המשמש להעברת קבצים בין התקנים שונים ברשת. הוא פועל בשכבה 7 במודל ה – OSI והוא הפרוטוקול הסטנדרטי המשמש לשילוח דואר אלקטרוני. פרוטוקול זה עובד בפורט 20 ו – 21 ובתקורת מסוג TCP, כאשר פорт 20 משמש על מנת לשלוח את המידע ופורט 21 משמש על מנת לקבל את בקשת הלכה אשר מעוניין במידע. העברת המידע אינה מוצפנת, על מנת לספק הצפנה לתעבורה ניתן להשתמש בפרוטוקול SFTP.

שימוש בFTP

פרוטוקול FTP הוא פרוטוקול תקשורת כמו HTTP לדוגמא. פרוטוקולי התקשורת האחרים משמשים גם הם להעברת קבצים בין התקנים שונים, אך אינם ממוקדים בהשוואה לFTP. יתר על כן, המרכיבות המשותפות בFTP יכולות להיות שונות בפורמטרים מסוימים ופרוטוקול זה יודע להגן על המשתמש מהבדלים אלה ולהעביר את הנתונים באמינות על אף ההבדלים.

תהליכי העבודה של FTP

החיבור בFTP נוצר בין שתי מערכות המתחשרות זו עם זו בעזרת הרשות. כאשר ייוצר החיבור, ייווצרו שני ערוצי תקשורת :

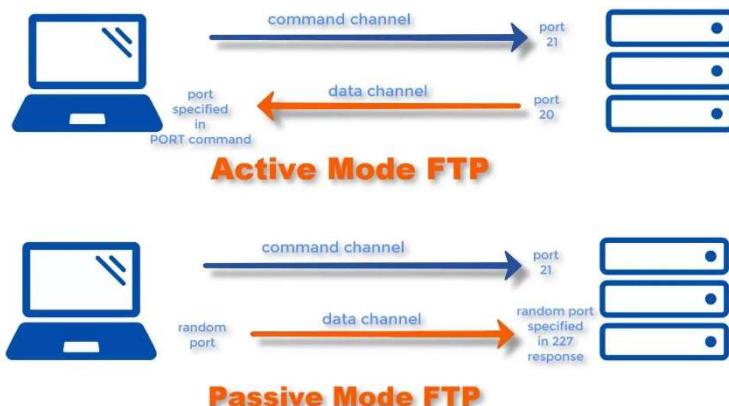
- **ערוץ הנתונים** – ערוץ המשמש להעברת המידע (הקבצים) בין הלכה לשרת. ערוץ זה משתמש בפורט 20 בFTP Active ובפורט אקראי בטוח של 65000 – 48000 .Passive FTP
- **ערוץ הפקודה** – ערוץ המשמש להעברת הפקודות מהלקוח לשרת ואת התשובות מהשרת ללכה. ערוץ זה משתמש בפורט 21

סוגי התחברות בFTP

Active FTP – בחיבור מסוג Active , הלכה מתחבר בפורט מקור אקראי בטוח 48000-64000 הנבחר על ידי ההתקן ופורט היעד יהיה 21 של שרת ה – FTP, בכך נוצר ערוץ. נשלחת על ידי הלכה פקודת PORT שמטרתה לציין לאיזה פорт השרת צריך להתחבר מצד הלכה על מנת ליצור את הערוץ. שרת FTP מתחבר מפורט 20 אל הפורט מצד הלכה המיועד לערוץ הנתונים. ערוץ הפקודה (פורט 21) קיים על מנת להעביר את הפקודות ולקלב את הביקשות מן השרת וערוץ הנתונים (פורט 20) קיים על מנת להוריד קבצים אל מחשב הלכה.

Passive FTP – בחיבור מסוג Passive , הלכה מתחבר בפורט מקור אקראי בטוח 48000-64000 הנבחר על ידי ההתקן ופורט היעד יהיה 21 של שרת ה – FTP. נשלחת על ידי הלכה פקודת PASV שמטרתה להתחבר לפורט מצד השרת על מנת להעביר נתונים. ההבדל בין Active Passive הוא שכון הלכה הוא זה שיצור את ערוץ הנתונים ואת ערוץ הפקודה. כשרת FTP יגיב, הוא יציין ללהקה את מהספר הפורט

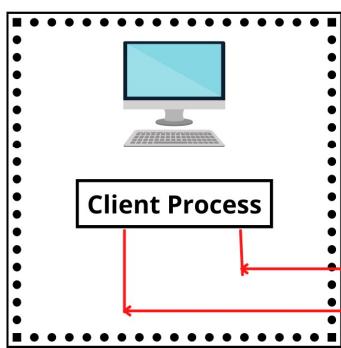
שהוא פותח לעורץ הנטונים (המספר לא יהיה 20 אלה מספר רנדומלי בין 48000 – 64000). הלוקוח יתחבר לפורט זה בעזרת פורט אקראי באותו טווח וייצרך עורץ הנטונים.



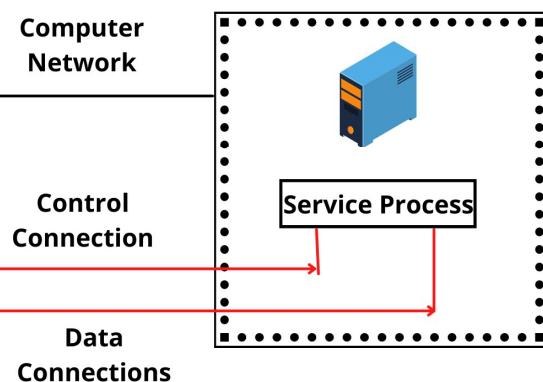
Anonymous FTP

Anonymous FTP מאפשר גישה ציבורית אל הקבצים ללא חיוב בהזדהות על ידי שם משתמש וסיסמה. הלוקוח משתמש בכתובת URL בה ניתנת פקודה FTP וכותבת שרת FTP. כאשר השרת והлокוח יוצרים חיבור ברשות, הлокוח יתחבר על ידי הזדהות עם שם משתמש וסיסמה או על ידי כניסה אונונימית (אם השרת מאפשר סוג כניסה זו). לאחר שהשרת מאמת את זהות המשתמש, הוא יכול ללקוח לגשת אל הקבצים שבשרת ולהעביר אותם. לאחר סיום הלקוח להעברת הקבצים נדרש, הוא יצא מההמשה והחיבור יסתירם.

FTP Client



FTP Server



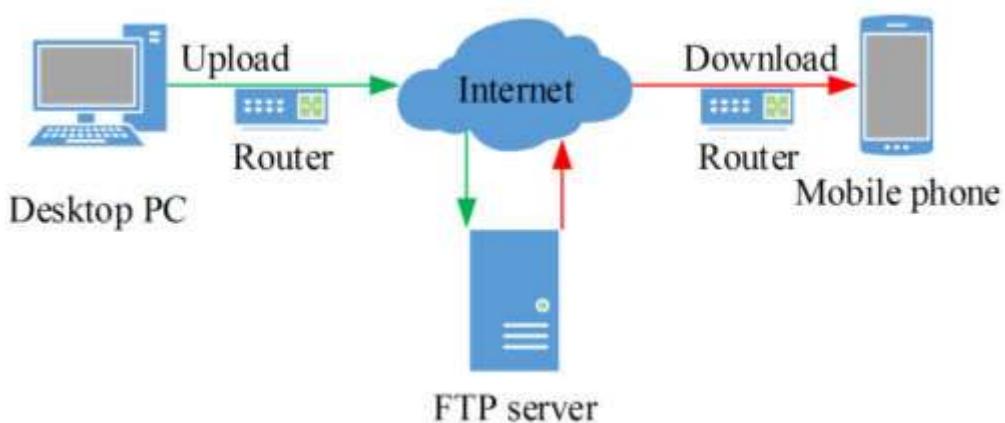
הרשאות FTP

בשירותי FTP קיימות מספר הרשאות אשר יכולות להינתן ללקוח:

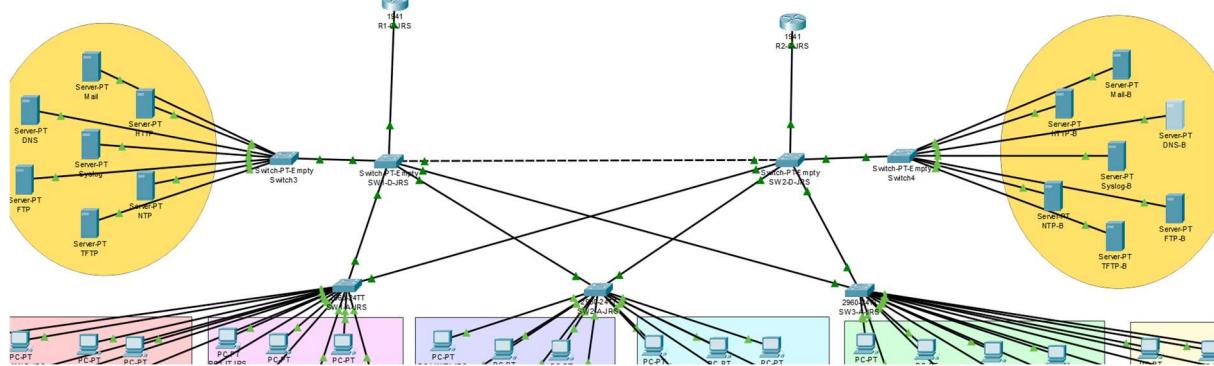
- קריאה – Read
- כתיבה – Write
- מחיקה – Delete
- שינוי שם – Rename
- הוספה לרשימה – List

יתרונות FTP

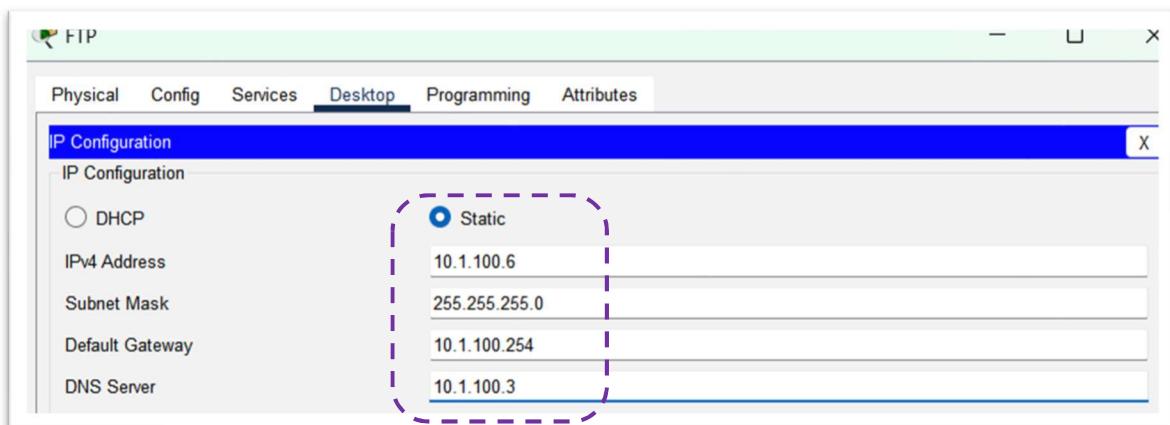
- אבטחה – FTP מאפשר כניסה והעברה של קבצים רק אחרי Authentication . יתר על כן, ניתן ליצור רמות גישה וחוקים על מנת לקבוע מי יכול לגשת לשרת ואיזה הרשות לתת מהירות – FTP הינה הדרך המהירה ביותר על מנת להעביר קבצים דרך האינטרנט ממחשב אחד לאחר יעילות – FTP עוזר לארגן את הקבצים ולהעביר אותם ביעילות העברת גדולה של קבצים – FTP מאפשר להעביר מספר קבצים גדולים בין מערכות שונות העברת רציפה – במקרה בו הורדת הקובץ הופסקה, המשמש יכול לחזור את ההורדה של הקובץ בכל פעם session נוצר פשוט ליישום ולשימוש



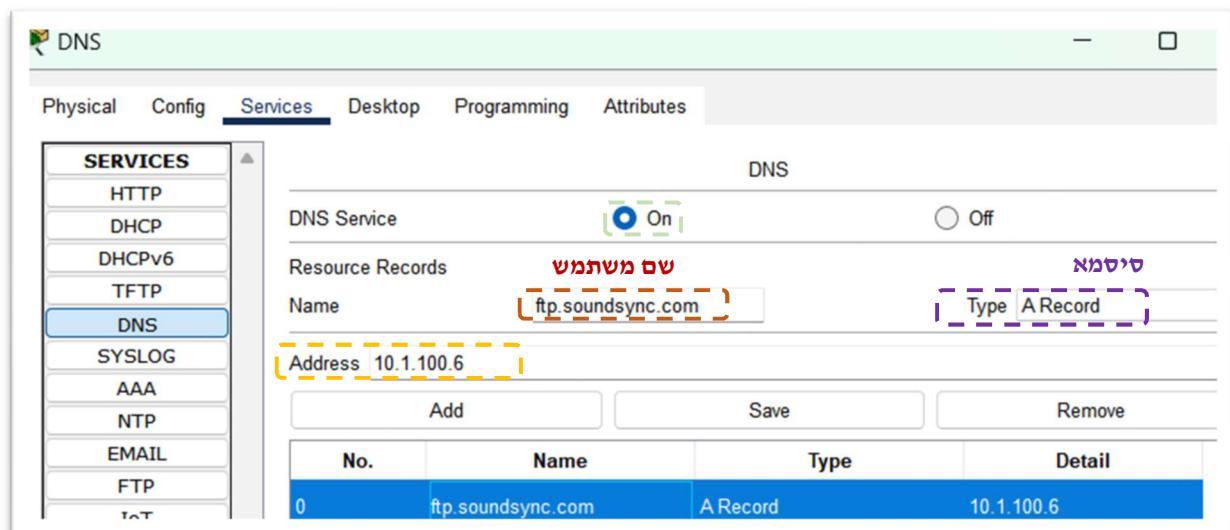
הגדרת שירות FTP ראשי



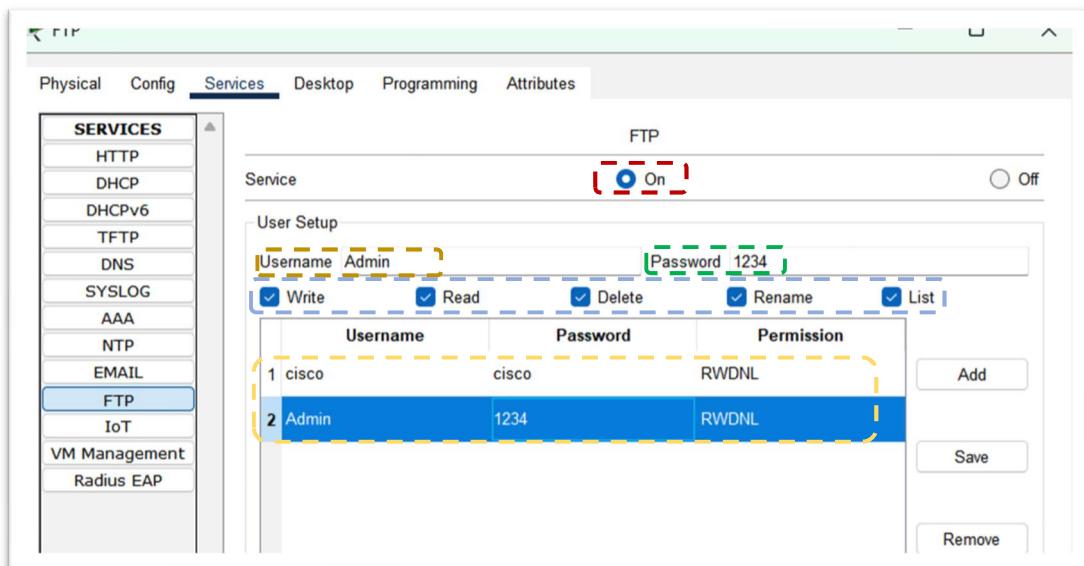
הגדרת כתובות לשירות



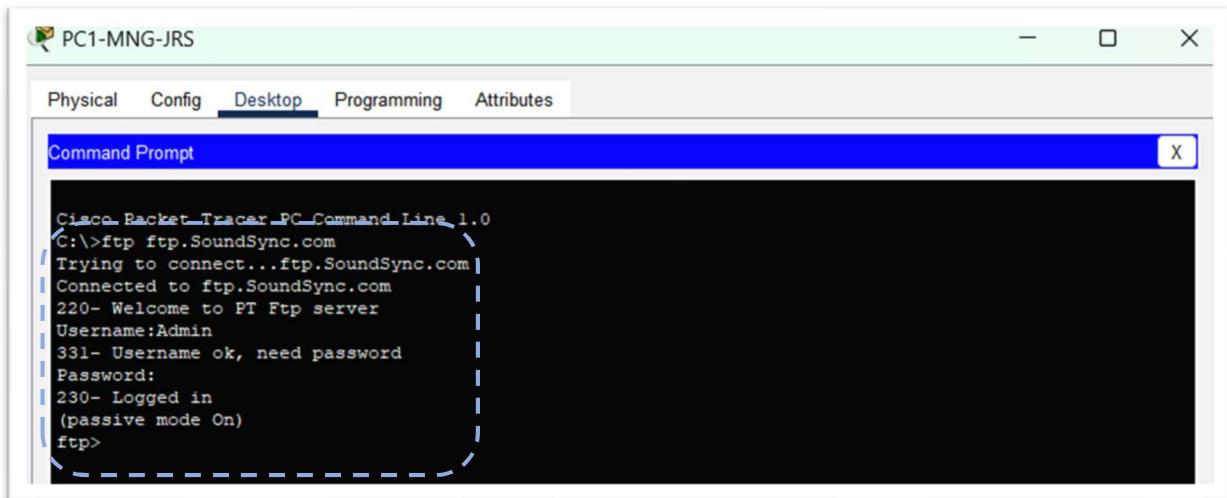
הוספה הdns לשירות ftp



הוספה של שירות FTP

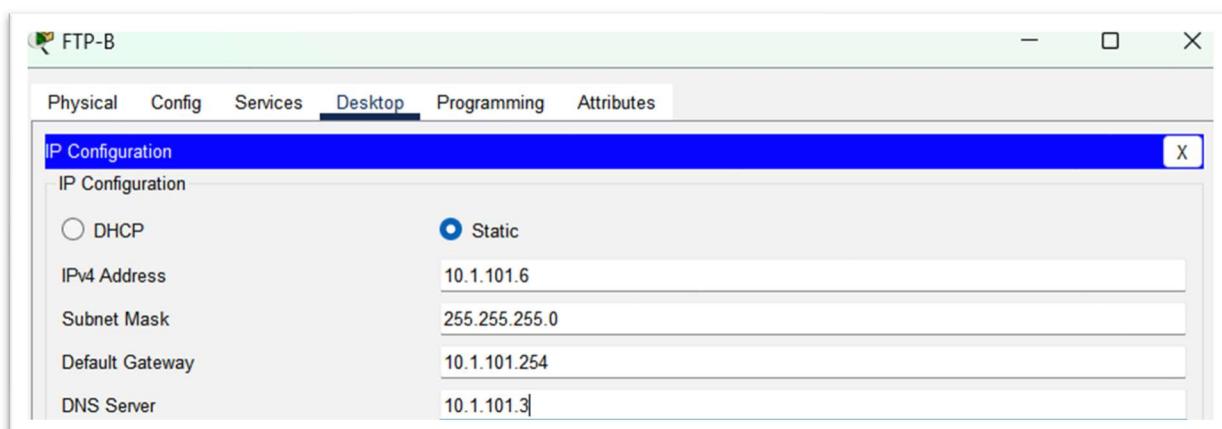


בדיקה – התחברות FTP על ידי כתובת IP ו URL

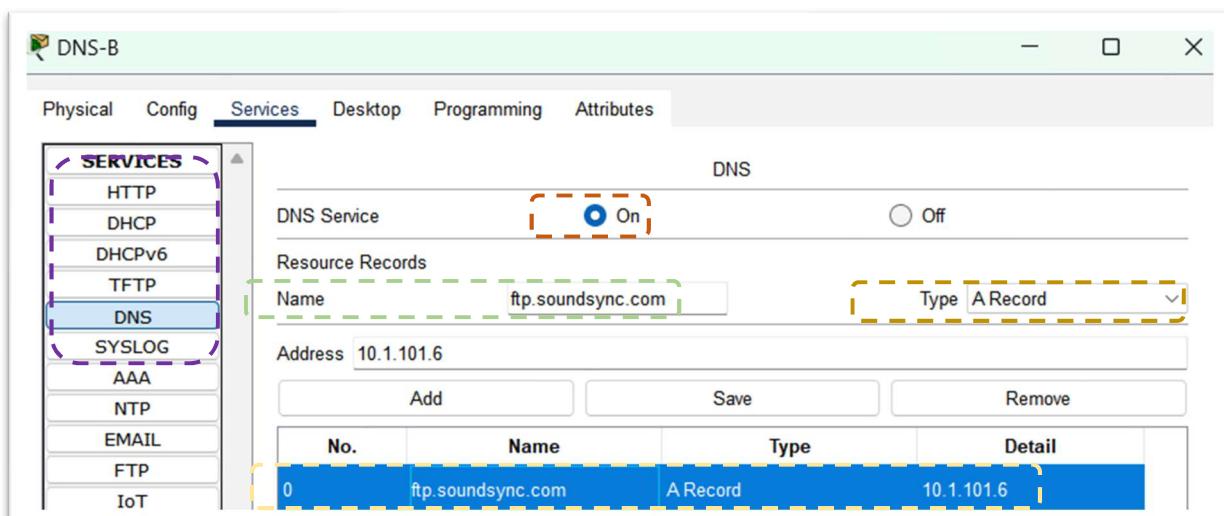


```
C:\>ftp 10.1.100.6
Trying to connect...10.1.100.6
Connected to 10.1.100.6
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

הגדרת שרת FTP גיבוי



הגדרת כתובות לשרת



הוספת שירות FTP

The screenshot shows the 'FTP-B' configuration interface. The 'Services' tab is selected. On the left, a sidebar lists various services: Physical, Config, Services, Desktop, Programming, Attributes, SERVICES (HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, **FTP**, IoT, VM Management, Radius EAP). The 'FTP' service is highlighted. The main panel shows the 'FTP' service is turned 'On'. Under 'User Setup', there is a table with two rows:

Username	Password	Permission
1 cisco	cisco	RWDNL
2 Admin	1234	RWDNL

Buttons for Add, Save, and Remove are visible on the right.

בדיקה – התחברות FTP על ידי כתובת IP וURL

The screenshot shows the 'PC1-MNG-JRS' desktop interface. The 'Desktop' tab is selected. A 'Command Prompt' window is open, displaying the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp ftp.SoundSync.com
Trying to connect...ftp.SoundSync.com
Connected to ftp.SoundSync.com
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Trivial File Transfer Protocol

TFTP הינו פרוטוקול המשמש להעברה של קבצים. הוא פועל בשכבה 7 במודל OSI ועובד בפורט 69 בתקשורת מסוג UDP. הוא משמש בעיקר לקריאה של קבצים או כתיבה של קבצים משרת מרוחק. לעומת FTP, TFTP אינו מספק אבטחה וAuthentication בזמן ההעברה של הקבצים, אך השימוש בו נעשה בעיקר על מנת להעביר קבצים של מערכות הפעלה או קבצי הגדרות של רכיבי רשת.

לרוב לא נעשה שימוש ב프וטוקול TFTP על ידי משתמשים ברשתות מחשבים, זאת מכיוון שהוא אבטחה שלו והשימוש בUDP הופך אותו למסוכן לשימוש דרך האינטרנט ולסיכון של איבוד פאקטו ומידע חיוני. אך משתמשים בTFTP בעיקר ברשתות מקומיות ופרטיות.

סוגי הודעות TFTP

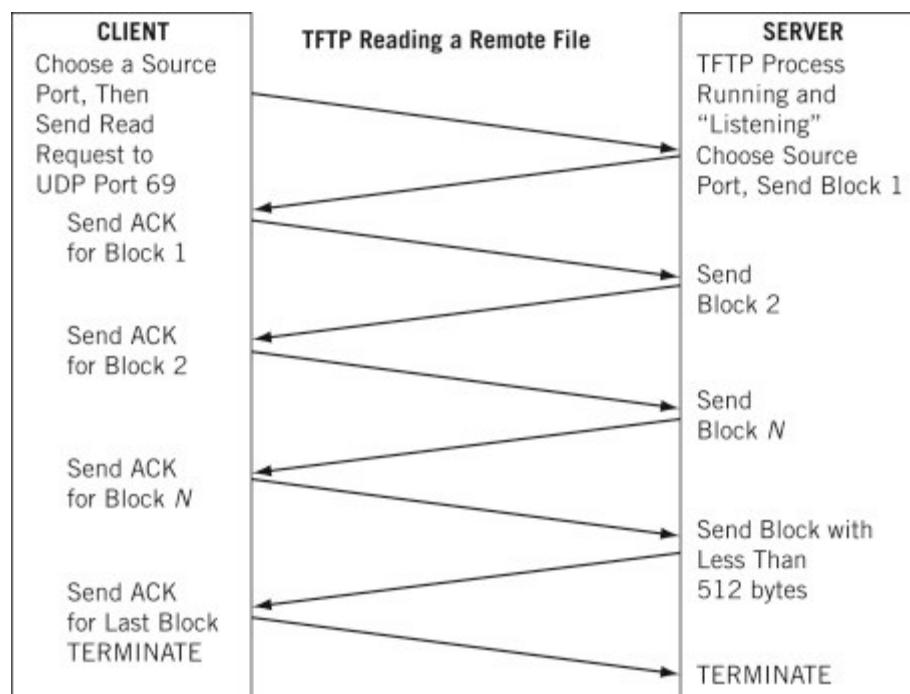
- **RRQ** – בקשה לקריאה של קובץ
- **WRQ** – בקשה לכתיבה בקובץ
- **DATA** – שילית בלוקים של נתונים הקשורים לקובץ. גודל הקובץ נע בין 0 – 512 bytes, הבלוק האחרון יהיה קטן מ-512
- **ACK** – אישור שהקבצים התקבלו
- **ERROR** – במקרה, במצב זה השרת מודיע למכשיר השולח שלא ניתן לבצע את הפעולה שניתנה בפעם השנייה

דרך העבודה של שרת TFTP:

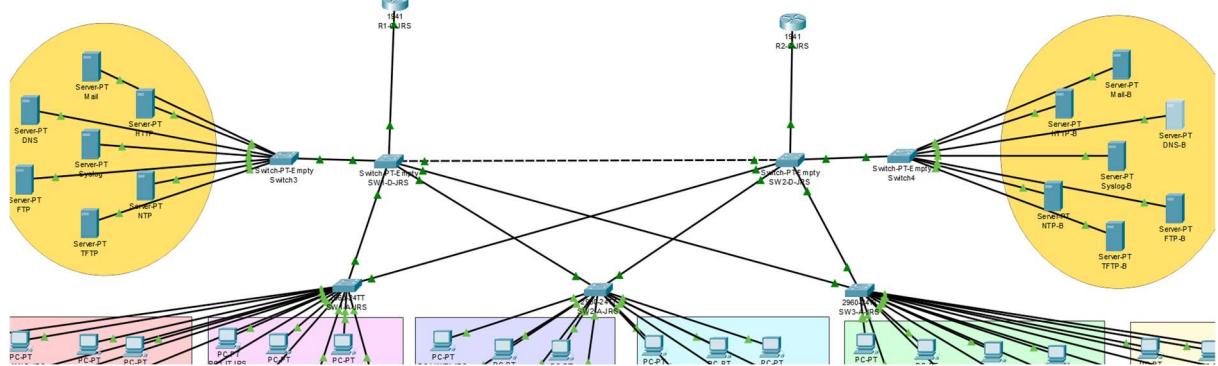
1. הלקוח שולח הודעה RRQ (הודעת קריאה) מפורט אקראי גדול מ-1024, לפורט 69 UDP עליו מזמן השרת
2. לאחר שתתקבל הודעה מהלוח, השרת ישיב תגובה עם הבלוק הראשון של הנתונים או במידה והייתה בעיה עם הודעה ERROR. במצב בו הקובץ המבוקש והחיבור תקין, ישלח השרת את הבלוק הראשון של הבלוק הראשון. התקשרות נוספת על ידי שרת ה-TFTP ללקוח אינה מפורט, 69 השרת בוחר גם ה-PORT אקראי שמספרו מעל 1024.
3. הבלוקים ממוספרים ונשלחים על פי הסדר. לאחר קבלת הבלוק הראשון, תשלח הודעה ACK לשרת שהבלוק קיבל וכך אלה עד שישלחו כל הבלוקים.

השוואה בין TFTP לFTP

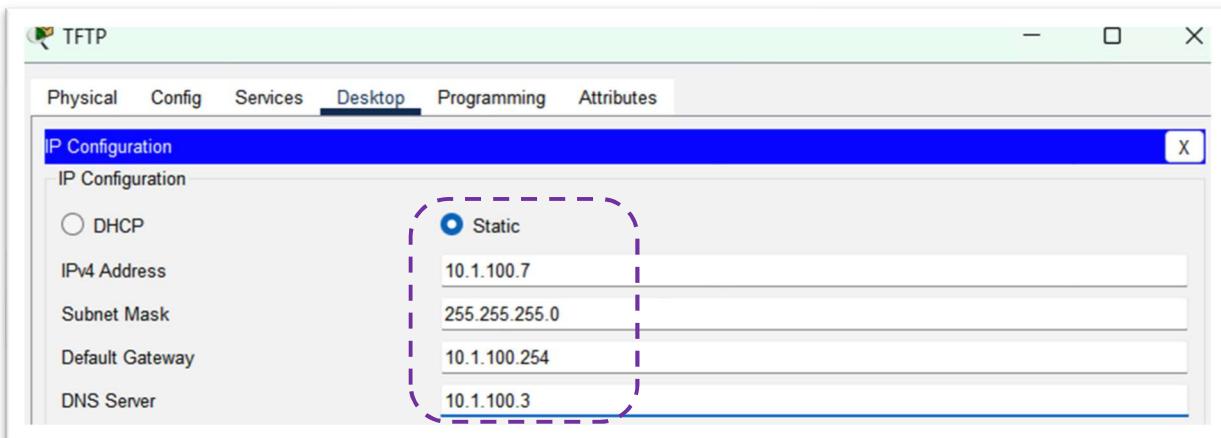
TFTP	FTP
עובד עם פורט 69	עובד בפורטים 20 – 21
עובד ב프וטוקול UDP	עובד בפרוטוקול תקשורת TCP
5 הודעות	קיימים הרבה פקודות וההודעות
איינו מצרייך Authentication	מצרייך Authentication
פרוטוקול מהיר	פרוטוקול איטי יחסית לFTP
תכנה קטנה	תכנה גדולה
פרוטוקול לא אמין	פרוטוקול אמין



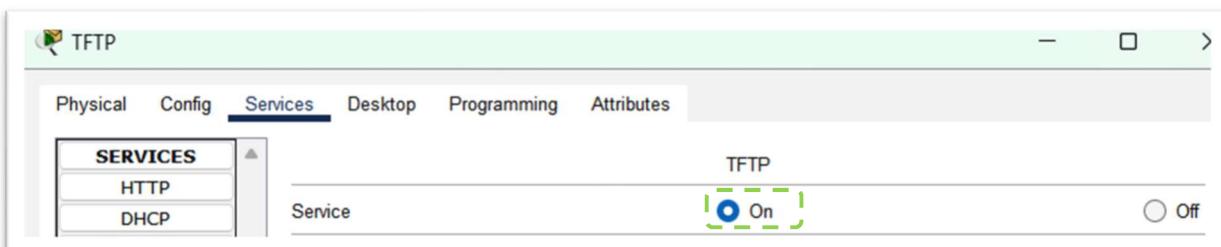
הגדרת TFTP על השרת הראשי



הגדרת כתובות על השרת



הפעלת שירות TFTP



העתקת זיכרון NVRAM של המtab לשרת TFTP הראשי

```
R1-C-JRS#copy startup-config tftp  
Address or name of remote host []? 10.1.100.7  
Destination filename [R1-C-JRS-config]? R1-C-JRS.config  
  
Writing startup-config....!!  
[OK - 3001 bytes]  
  
3001 bytes copied in 3.008 secs (997 bytes/sec)
```

نمחק את config מהמtab

```
R1-C-JRS#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

חיבור הרשת של חוות השירותים אל הרouter (מכיוון שנמכוו ההגדרות)

```
Router(config)#int gigabitEthernet 0/0  
Router(config-if)#ip add  
Router(config-if)#ip address 10.1.100.254 255.255.255.0  
Router(config-if)#no shutdown
```

קבלת קובץ config מהשרת

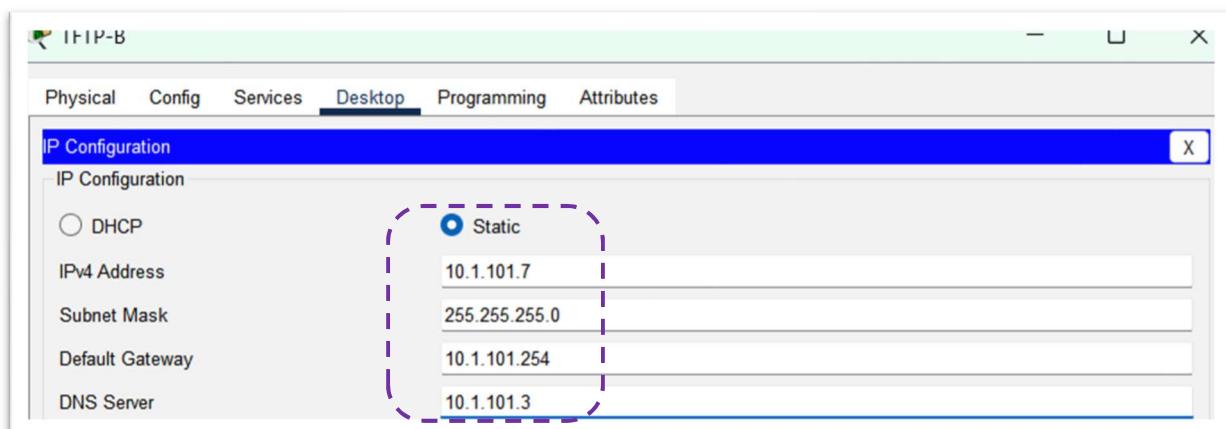
```
Router#copy tftp: running-config  
Address or name of remote host []? 10.1.100.7  
Source filename []? R1-C-JRS.config  
Destination filename [running-config]?  
  
Accessing tftp://10.1.100.7/R1-C-JRS.config....  
Loading R1-C-JRS.config from 10.1.100.7: !  
[OK - 3001 bytes]
```

בדיקות שכל ההגדרות התקבלו

```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 10.1.100.3
ip dhcp pool lan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 10.1.100.3
```

הגדרת TFTP על השרת הראשי

הגדרת כתובות על השרת



הפעלת שירות TFTP



העתקת ה startup-config לשרת TFTP

```
R1-C-JRS#copy startup-config tftp
Address or name of remote host []? 10.1.101.7
Destination filename [R1-C-JRS-config]? C1-D-JRS.conf

Writing startup-config....!!
[OK - 3001 bytes]

3001 bytes copied in 1.84467e+16 secs (0 bytes/sec)
```

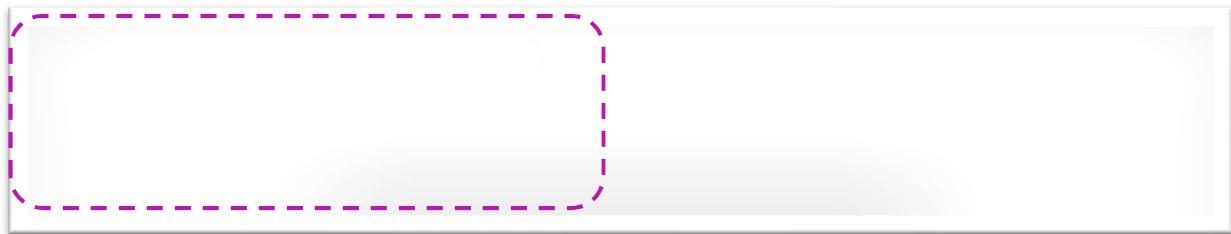
نمחק את startup-config מהנתב

```
R1-C-JRS#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
>1>_TDS#vratn
```

חיבור הרשות של חוות השירותים אל הרואוטר (מכיוון שנמחקו ההגדרות)

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip add
Router(config-if)#ip address 10.1.100.254 255.255.255.0
Router(config-if)#no shutdown
```

קיבלה קבועה startup-config מהשרת



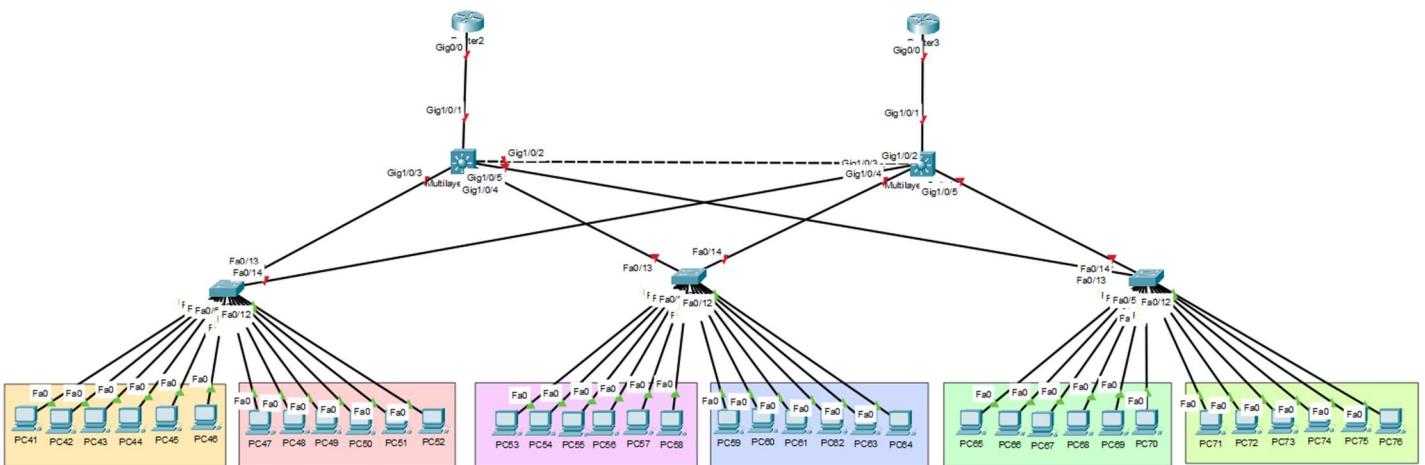
בדיקה שכל ההגדרות התקבלו

```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.254
  dns-server 10.1.100.3
ip dhcp pool lan20
  network 192.168.20.0 255.255.255.0
  default-router 192.168.20.254
  dns-server 10.1.100.3
```

סניף 2 – תל אביב

היות וחלק מן הגדירות בסניף זה זהות להגדירות בסניף הראשון, אצין ואסביר על הגדירות אשר ייחודיות לסניף זה בעקבות הטופולוגיה השונה ואציג את פקודות show של הגדירות אשר הוסברו. במצב בו יוגדר פרוטוקול בסניף זה אשר לא הוסבר עליו בסניף הראשון, ארכיב עליו בסניף זה.

טופולוגיה הסניף

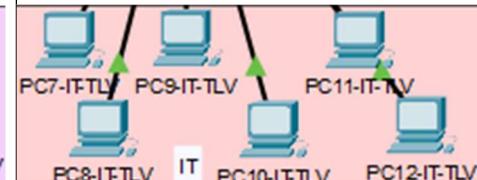
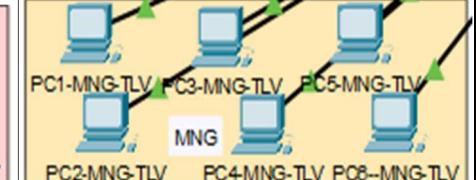


בטופולוגיה זו יש שימוש במתגים מסווג MultiLayer אשר יכולים לעבוד גם עם כתובות MAC (שכבה 2) וגם עם כתובות IP (שכבה 3). כמובן, מתגי MultiLayer יכולים לתקן גם כתובים ברשותות מקומיות וגם לבצע את התפקיד של הראوتر ולנתב בין רשותות.

הבדלים בין מתג שכבה 2 למתג שכבה 3:

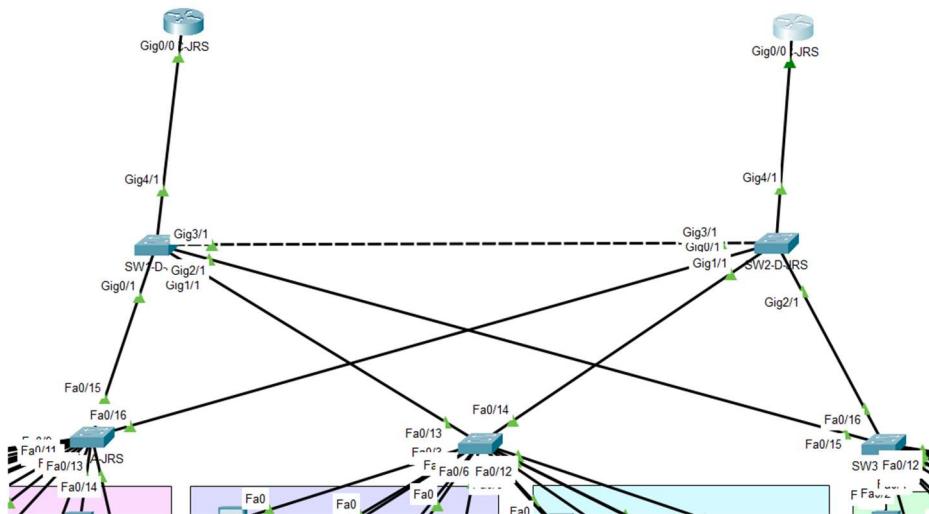
Switch layer 2	Multilayer Switch (layer 3 switch)
אינו יכול לבצע ניתוב	ניתן לבצע באמצעות ניתוב דינמי וסטטי
מכשיiri הקצה יכולים לתקשר הן באותה רשת פנימית והן ברשותות אחרות	מכשיiri הקצה יכולים לתקשר רק אם נמצא באותו רשת פנימית
המשകים יודעים לעבוד גם בשכבה 2 באמצעות כתובות MAC וגם בשכבה 3 עם כתובות IP. זאת בהתאם לדרכם ניהול הרשת הגדרת המשק	המשקדים יודעים לעבוד עם שכבה 2 בלבד באמצעות כתובות MAC
המיתוג איטי יותר מכיוון שעל המתג לבחון גם את שכבה 2 וגם את 3 לפני שליחת החבילות אל המיקום המבויש	המיתוג מהיר יותר מכיוון שהוא בשכבה 2 בלבד

המחלקות בסניף :

WIFI VLAN 30	IT – Vlan 19	Management – Vlan 8
		
Training – VLAN 63	Legal – VLAN 52	Control – VLAN 41
		

בسانיף VLAN השני

בין הגדרות הוילאן בטופולוגיה זו לטופולוגיה בסניף הראשון קיימים מספר הבדלים.
מכיוון שלמתק ה-MLR אשר נמצא בשכבה ה-0 Distribution קיימת גם האפשרות לנtab בין רשתות
שונות, אנחנו נגידיר עליו גם את ההגדרות שהגדרכנו למתקים בשכבה ה-D וגם נגידיר עליו ממשקים
וירטואליים עם כתובות IP שיחליפו את פרוטוקול ה-[.dot1q](#).



הגדרת VLAN'S בسانיף השני

תחילה נגידיר על המתקים בשכבה ה-Access ושבכנת המיזיגר Distribution כפי שעשינו בסניף
הקודם. על היזיגר רק את הוילאנים המחבררים לשירות ועל היזיגר את כל הוילאנים

```
SW3-D-TLV(config)#vlan 52
SW3-D-TLV(config-vlan)#name LGL
SW3-D-TLV(config-vlan)#vlan 63
SW3-D-TLV(config-vlan)#name TRN
```

```
MLS1-D-TLV(config-vlan)#name MNG
MLS1-D-TLV(config-vlan)#vlan 19
MLS1-D-TLV(config-vlan)#name IT
MLS1-D-TLV(config-vlan)#vlan 30
MLS1-D-TLV(config-vlan)#name WIFI
MLS1-D-TLV(config-vlan)#vlan 41
MLS1-D-TLV(config-vlan)#name CTRL
MLS1-D-TLV(config-vlan)#vlan 52
MLS1-D-TLV(config-vlan)#name LGL
MLS1-D-TLV(config-vlan)#vlan 63
MLS1-D-TLV(config-vlan)#name TRN
```

ובמתקנים בשכבה 2 נשייך את ה-`vlan`s למשקימים

```
SW1-A-TLV(config)#int range fastEthernet 0/1-6
SW1-A-TLV(config-if-range)#switchport mode access
SW1-A-TLV(config-if-range)#switchport access vlan 8
SW1-A-TLV(config-if-range)#exit
SW1-A-TLV(config)#int range fastEthernet 0/7-12
SW1-A-TLV(config-if-range)#switchport mode access
SW1-A-TLV(config-if-range)#switchport access vlan 19
SW1-A-TLV(config-if-range)#exit
```

נעביר את הממשקים המחברים בין המתקנים במצב Trunk

```
int range gigabitEthernet 1/0/2-5
switchport mode trunk
```

מכיוון שהמתקנים מסוג MLS בשכבה ה-D צריכים לנtab בין הרשותות, נדרש להגדיר להם את הרשותות הווירטואליות אותן יצרכו לנtab. נעשה זאת באמצעות **שימוש בז'אנס** (משק וירטואלי) עליו ארחיב בהמשך.

```
 MLS1-D-TLV(config)#interface vlan 8 → כניסה לממשק SVI של הולאן
MLS1-D-TLV(config-if)#ip address 10.2.8.252 255.255.255.0 → נתינת כתובת IP
MLS1-D-TLV(config-if)#no shutdown → הידקמת הממשק (לא חובה)
MLS1-D-TLV(config-if)#interface vlan 19
MLS1-D-TLV(config-if)#ip address 10.2.19.252 255.255.255.0
MLS1-D-TLV(config-if)#no shutdown
MLS1-D-TLV(config-if)#interface vlan 30
MLS1-D-TLV(config-if)#ip address 10.2.30.252 255.255.255.0
MLS1-D-TLV(config-if)#no shutdown
MLS1-D-TLV(config-if)#interface vlan 41
MLS1-D-TLV(config-if)#ip address 10.2.41.252 255.255.255.0
MLS1-D-TLV(config-if)#no shutdown
MLS1-D-TLV(config-if)#interface vlan 52
MLS1-D-TLV(config-if)#ip address 10.2.52.252 255.255.255.0
MLS1-D-TLV(config-if)#no shutdown
MLS1-D-TLV(config-if)#interface vlan 63
MLS1-D-TLV(config-if)#ip address 10.2.63.252 255.255.255.0
MLS1-D-TLV(config-if)#no shutdown
MLS1-D-TLV(config-if)#exit
```

show commands

show vlan

```
MLS1-D-TLV#show vlan

VLAN Name          Status    Ports
---- --
1   default        active    Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                                Gig1/0/11, Gig1/0/12, Gig1/0/13, Gig1/0/14
                                Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18
                                Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22
                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                Gig1/1/3, Gig1/1/4
8   MNG           active
19  IT            active
30  WIFI          active
41  CTRL          active
52  LGL           active
63  TRN           active
1002 fddi-default active
1003 token-ring-default active
1004 fdnet-default active
1005 trnet-default active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- --
1   enet   100001    1500   -     -     -     -     0     0
8   enet   100008    1500   -     -     -     -     0     0
19  enet   100019    1500   -     -     -     -     0     0
30  enet   100030    1500   -     -     -     -     0     0
41  enet   100041    1500   -     -     -     -     0     0
52  enet   100052    1500   -     -     -     -     0     0
63  enet   100063    1500   -     -     -     -     0     0
1002 fddi  101002    1500   -     -     -     -     0     0
1003 tr    101003    1500   -     -     -     -     0     0
1004 fdnet 101004    1500   -     -     -     ieee  0     0
1005 trnet 101005    1500   -     -     -     ibm   0     0

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- --
```

show interface trunk

```
MLS2-D-TLV#show interfaces trunk

Port      Mode      Encapsulation | Status       Native vlan
Gig1/0/2  on       802.1q        | trunking    1
Gig1/0/3  on       802.1q        | trunking    1
Gig1/0/4  on       802.1q        | trunking    1
Gig1/0/5  on       802.1q        | trunking    1

Port      Vlans allowed on trunk
Gig1/0/2  1-1005
Gig1/0/3  1-1005
Gig1/0/4  1-1005
Gig1/0/5  1-1005

Port      Vlans allowed and active in management domain
Gig1/0/2  1,8,19,30,41,52,63
Gig1/0/3  1,8,19,30,41,52,63
Gig1/0/4  1,8,19,30,41,52,63
Gig1/0/5  1,8,19,30,41,52,63

Port      Vlans in spanning tree forwarding state and not pruned
Gig1/0/2  1,8,19,30,41,52,63
Gig1/0/3  1,30,41,52,63
Gig1/0/4  1,8,19,30,41,52,63
```

show run

```
interface FastEthernet0/1
switchport access vlan 8
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/2
switchport access vlan 8
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/3
switchport access vlan 8
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
```

```
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/4
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/5
switchport mode trunk
spanning-tree guard root
```

סנייף 2 STP

היות והסברתי על פרוטוקול זה והגדירות STP בסנייף
זה זהות להגדירות STP בסנייף הקודם, הראה את פקודות show בלבד.

show spanning-tree summary

```
MLS1-D-TLV#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: default MNG IT WIFI
Extended system ID      is enabled
Portfast Default         is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtherChannel misconfig guard is disabled
UplinkFast               is disabled
BackboneFast              is disabled
Configured Pathcost method used is short

Name          Blocking Listening Learning Forwarding STP Active
-----+-----+-----+-----+-----+-----+
VLAN0001       2      0      0      4      6
VLAN0008       2      0      0      4      6
VLAN0019       2      0      0      4      6
VLAN0030       2      0      0      4      6
VLAN0041       2      0      1      3      6
VLAN0052       2      0      0      4      6
VLAN0063       2      0      0      4      6
-----+-----+-----+-----+-----+
7 vlans        14     0      1      27     42
```

show spanning-tree vlan [vlan_num]

```
MLS1-D-TLV#show spanning-tree vlan 8
[VLAN0008]
  Spanning tree enabled protocol rstp
  Root ID    Priority 24584
              Address 00D0.5895.179A
              This bridge is the root !
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority 24584 (priority 24576 sys-id-ext 8)
              Address 00D0.5895.179A
              Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 20

  Interface   Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+
  Gil/0/5    Desg FWD 19      128.5    P2p
  Gil/0/4    Desg FWD 19      128.4    P2p
  Gil/0/3    Desg FWD 19      128.3    P2p
  Gil/0/2    Desg FWD 4       128.2    P2p
```

על מותג בשכבה ה access על how run

```
interface FastEthernet0/5
switchport access vlan 8
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/6
switchport access vlan 8
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 19
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/8
switchport access vlan 19
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
```

Distribution על מותג בשכבה ה show run

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1,8,19,30 priority 24576
spanning-tree vlan 41,52,63 priority 28672
```

```
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/4
switchport mode trunk
spanning-tree guard root
!
interface GigabitEthernet1/0/5
switchport mode trunk
spanning-tree guard root
!
```

הגדרת HSRP בסניף השני : TLV

בניגוד להגדרת ה `hsrp` בסניף הקודם שהוגדרו על הממשקים הפיזיים לפי מס' VLAN, נגידר את פרוטוקול HSRP על ממשקיו וילאן וירטואליים כפי שהגדכנו את VLANs בסניף זה.

הגדרות שהוגדרו על שני המתגים בשכבה ה-2 : Distribution

```
MLS2-D-TLV(config)#interface Vlan 8
MLS2-D-TLV(config-if)#standby 1 ip 10.2.8.254
MLS2-D-TLV(config-if)#standby 1 priority 110
MLS2-D-TLV(config-if)#standby 1 preempt
MLS2-D-TLV(config-if)#interface Vlan 19
MLS2-D-TLV(config-if)#standby 1 ip 10.2.19.254
MLS2-D-TLV(config-if)#standby 1 priority 110
MLS2-D-TLV(config-if)#standby 1 preempt
MLS2-D-TLV(config-if)#interface Vlan 30
MLS2-D-TLV(config-if)#standby 1 ip 10.2.30.254
% Warning: address is not within a subnet on this interface
MLS2-D-TLV(config-if)#standby 1 priority 110
MLS2-D-TLV(config-if)#standby 1 preempt
MLS2-D-TLV(config-if)#interface Vlan 41
MLS2-D-TLV(config-if)#standby 1 ip 10.2.41.254
MLS2-D-TLV(config-if)#standby 1 priority 90
MLS2-D-TLV(config-if)#standby 1 preempt
MLS2-D-TLV(config-if)#interface Vlan 52
MLS2-D-TLV(config-if)#standby 1 ip 10.2.52.254
MLS2-D-TLV(config-if)#standby 1 priority 90
MLS2-D-TLV(config-if)#standby 1 preempt
MLS2-D-TLV(config-if)#interface Vlan 63
MLS2-D-TLV(config-if)#standby 1 ip 10.2.63.254
MLS2-D-TLV(config-if)#standby 1 priority 90
MLS2-D-TLV(config-if)#standby 1 preempt
```

הערות:
הגדרת כ吞吐 וירטואלית priority נזינית

פקודות show ל프וטוקול זה:

:show run

```

interface Vlan8
mac-address 0060.5ccc.0707
ip address 10.2.8.253 255.255.255.0
standby 1 ip 10.2.8.254
standby 1 priority 110
standby 1 preempt

interface Vlan19
mac-address 0060.5ccc.0708
ip address 10.2.19.253 255.255.255.0
standby 1 ip 10.2.19.254
standby 1 priority 110
standby 1 preempt

interface Vlan30
mac-address 0060.5ccc.0701
ip address 10.2.30.253 255.255.255.0
standby 1 ip 10.2.30.254
standby 1 priority 110
standby 1 preempt

```

show standby brief

```

MLS2-D-TLV#show standby brief
          P indicates configured to preempt.

Interface Grp Pri P State Active Standby Virtual IP
V18       1   110 P Active local   10.2.8.252 10.2.8.254
V119      1   110 P Active local   10.2.19.252 10.2.19.254
V141      1   90  P Standby 10.2.41.252 local   10.2.41.254
V152      1   90  P Standby 10.2.52.252 local   10.2.52.254
V163      1   90  P Standby 10.2.63.252 local   10.2.63.254
V130      1   110 P Active local   10.2.30.252 10.2.30.254

```

show standby

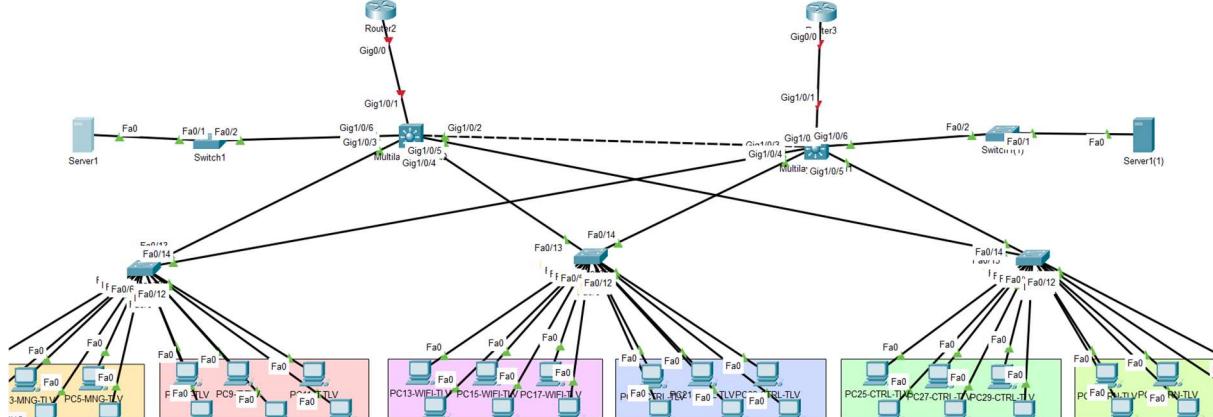
```

MLS1-D-TLV#show standby
Vlan8 - Group 1
  State is Standby
    6 state changes, last state change 00:00:15
    Virtual IP address is 10.2.8.254
    Active virtual MAC address is 0000.0C07.AC01
      Local virtual MAC address is 0000.0C07.AC01 (vl default)
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 0.322 secs
    Preemption enabled
  Active router is 10.2.8.253
  Standby router is local
  Priority 90 (configured 90)
  Group name is hsrp-V18-1 (default)

```

פרוטוקול DHCP סניף 2

בסניף הבודם הגדרנו את פרוטוקול DHCP על שני נתבים. בסניף זה, נגדיר את פרוטוקול DHCP על שני שרתים פיזיים. כל אחד מהם יהיה מחובר למוגש שכבה 2 ואותו נחבר לMLS בשכבה ה-LS.



מכיוון שתהליכי DHCP עובד בראוטר והMLS broadcast מותפק באנטיפיזיסים המוחברים less broadcast, נשתמש בפקודת IP HELPER על ה-MLS להעביר את הودעות של ה-MLS לתהליכי DHCP.

בסניף זה הקמנו 2 שרתים של DHCP ולכн' נגדיר על כל אחד מהם את כל ה-*vlangs* אך כל אחד מהם ייחל טווח כתובות שונה ובצורה זו, יהיו שני שרתים אשר יוכלו לתת שירות DHCP והעומס על השירותים יתחלק בין שניהם.

הגדרת DHCP על שרת:

ניתור pool חדש

נתן לו את הכתובת ההתחלהית אותו ירצה לחלק

נגדיר לו כמה כתובות יחלק הנטב

ונגדיר את Default Gateway של הרשת

הגדרת POOL בשרת והדלקתו :

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
LAN63	10.2.63.254	10.2.100.3	10.2.63.1	255.255.255.0	127	0.0.0.0	0.0.0.0
LAN52	10.2.52.254	10.2.100.3	10.2.52.1	255.255.255.0	127	0.0.0.0	0.0.0.0
LAN41	10.2.41.254	10.2.100.3	10.2.41.1	255.255.255.0	127	0.0.0.0	0.0.0.0
LAN30	10.2.30.254	10.2.100.3	10.2.30.1	255.255.255.0	127	0.0.0.0	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
LAN63	10.2.63.254	10.2.101.3	10.2.63.128	255.255.255.0	125	0.0.0.0	0.0.0.0
LAN52	10.2.52.254	10.2.101.3	10.2.52.128	255.255.255.0	125	0.0.0.0	0.0.0.0
LAN41	10.2.41.254	10.2.101.3	10.2.41.128	255.255.255.0	125	0.0.0.0	0.0.0.0
LAN30	10.2.30.254	10.2.101.3	10.2.30.128	255.255.255.0	125	0.0.0.0	0.0.0.0

הגדרת כתובות לשרתים

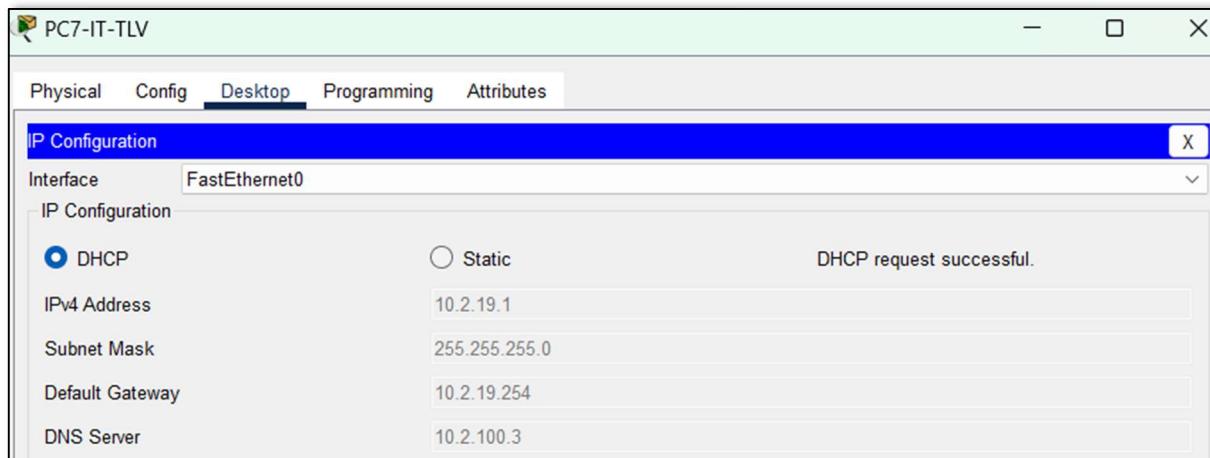
IPv4 Address	10.2.100.1
Subnet Mask	255.255.255.0
Default Gateway	10.2.100.254
DNS Server	0.0.0.0

IPv4 Address	10.2.101.1
Subnet Mask	255.255.255.0
Default Gateway	10.2.101.254
DNS Server	0.0.0.0

הוספת IP על הממשקים הווירטואליים במתגי MLS בשכבה ה-MLS Helper

```
MLS1-D-TLV(config)#interface Vlan81
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
MLS1-D-TLV(config-if)#interface Vlan19
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
MLS1-D-TLV(config-if)#interface Vlan30
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
MLS1-D-TLV(config-if)#interface Vlan41
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
MLS1-D-TLV(config-if)#interface Vlan52
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
MLS1-D-TLV(config-if)#interface Vlan63
MLS1-D-TLV(config-if)#ip helper-address 10.2.100.1
MLS1-D-TLV(config-if)#ip helper-address 10.2.101.1
```

נבדוק שהמחשבים מצליחים לקבל כתובת IP



סניף 2 Port Security

ההגדרות בסניף זה זהות להגדרות בסניף הראשון עליהם פירטתי לעיל. אצרף בסניף זה את טבלת ההגדרות ואת פקודות show

	מחלקה	מצב
מחלקות אלו חשובות ומקבלות ומכילות מידע רגיש על עובדי חברה, משתמשים והנהלה. לכן נרצה שהממשק יידלק וכיכבה עם התערבות מנהל הרשות בלבד	Management	Shutdown
	IT	
נרצה שתעבורה לא תעבור + קובץ לוג והודעת 33 IT - SNMP אין צורך בכיבוי משתק. לא נרצה שייהו לנו בעיות בהעברת ציוד ומידיע או בעיות תקשורת בסניף.	WIFI	Restrict
	Control	
אין צורך בכיבוי משתק, מספיק שהתעבורה תחסם.	Legal	Protect
	Training	

show port-security

Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Action
(Count)	(Count)	(Count)	(Count)	
Fa0/1	1	0	0	Shutdown
Fa0/2	1	0	0	Shutdown
Fa0/3	1	0	0	Shutdown
Fa0/4	1	0	0	Shutdown
Fa0/5	1	0	0	Shutdown
Fa0/6	1	0	0	Shutdown
Fa0/7	1	0	0	Shutdown
Fa0/8	1	0	0	Shutdown
Fa0/9	1	0	0	Shutdown
Fa0/10	1	0	0	Shutdown
Fa0/11	1	0	0	Shutdown
Fa0/12	1	0	0	Shutdown

מספר משתק

כמה MAC למד

כמה MAC מקסימלית

כמות הפרעות שהיו

שהוגדר mode

show port-security

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	0	0	Restrict
Fa0/2	1	0	0	Restrict
Fa0/3	1	0	0	Restrict
Fa0/4	1	0	0	Restrict
Fa0/5	1	0	0	Restrict
Fa0/6	1	0	0	Restrict
Fa0/7	1	0	0	Restrict
Fa0/8	1	0	0	Restrict
Fa0/9	1	0	0	Restrict
Fa0/10	1	0	0	Restrict
Fa0/11	1	0	0	Restrict
Fa0/12	1	0	0	Restrict

מספר מושך כמה MAC למד כמה MAC מקסימלית כמות הפרעות שהיו mode שהוגדר

show port-security

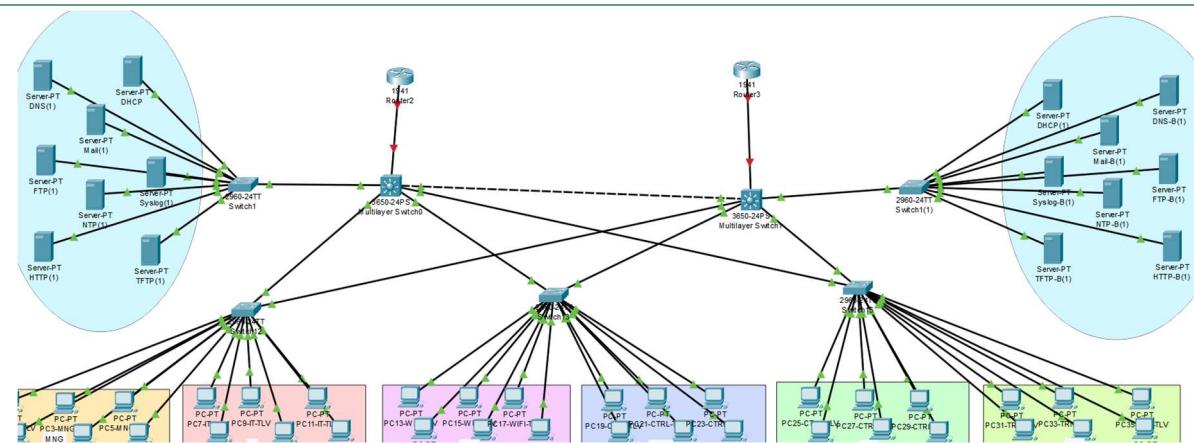
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	0	0	Protect
Fa0/2	1	0	0	Protect
Fa0/3	1	0	0	Protect
Fa0/4	1	0	0	Protect
Fa0/5	1	0	0	Protect
Fa0/6	1	0	0	Protect
Fa0/7	1	0	0	Protect
Fa0/8	1	0	0	Protect
Fa0/9	1	0	0	Protect
Fa0/10	1	0	0	Protect
Fa0/11	1	0	0	Protect
Fa0/12	1	0	0	Protect

מספר מושך כמה MAC למד כמה MAC מקסימלית כמות הפרעות שהיו mode שהוגדר

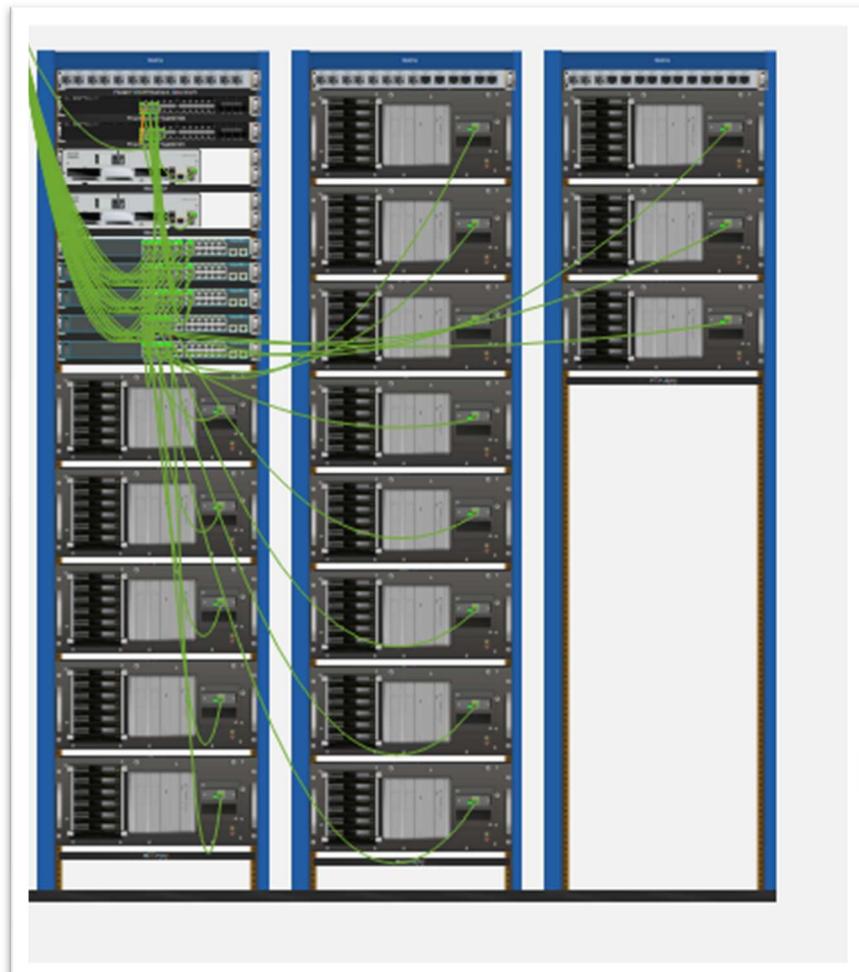
show port-security interface

Port Security	: Enabled	אפשרות port security
Port Status	: Secure-up	
Violation Mode	: Shutdown	סוג mode שהוגדרנו
Aging Time	: 0 mins	
Aging Type	: Absolute	
SecureStatic Address Aging	: Disabled	
Maximum MAC Addresses	: 11	מקסימום כתובות MAC שהוגדרנו
Total MAC Addresses	: 0	כמות הכתובות שלמדו
Configured MAC Addresses	: 0	
Sticky MAC Addresses	: 0	
Last Source Address:Vlan	: 0000.0000.0000:0	
Security Violation Count	: 0	

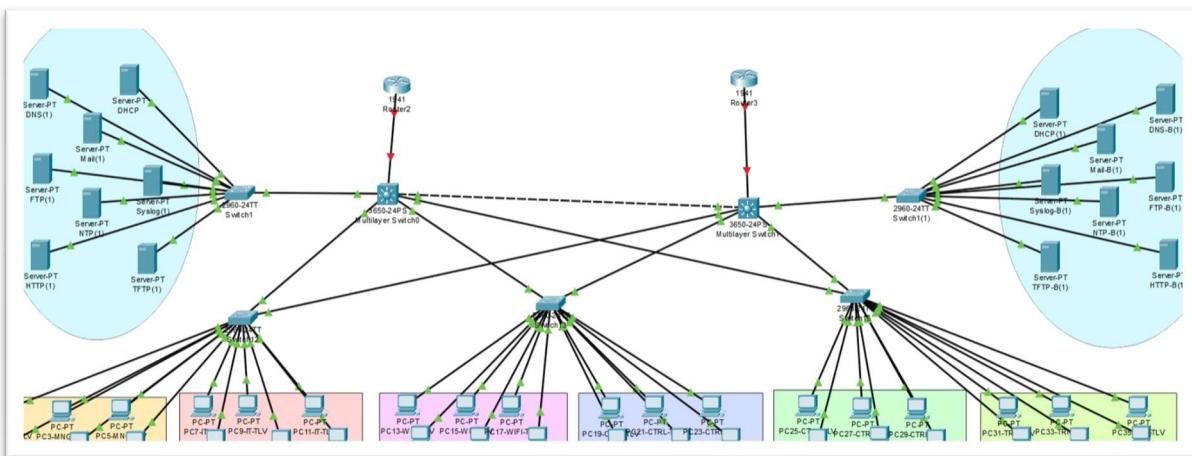
שרטים בסניף השני



על מנת לחבר את השרטים, נחבר למוגדים בשכבה החומרה שני מוגדים מסוג PT – EMPTY Distributionani, ולמוגדים אלו נחבר את השרטים בטופולוגיה.

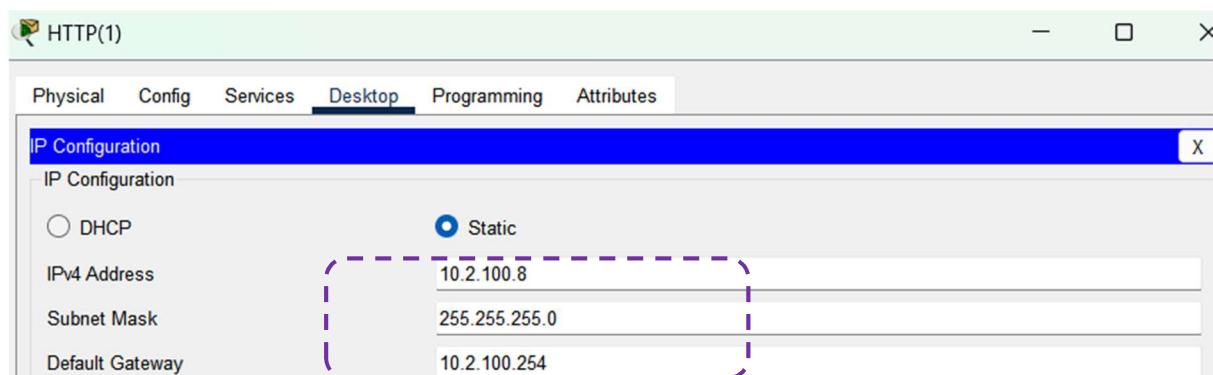


2 סני 2 HTTP



הגדירה בשרת הראשי

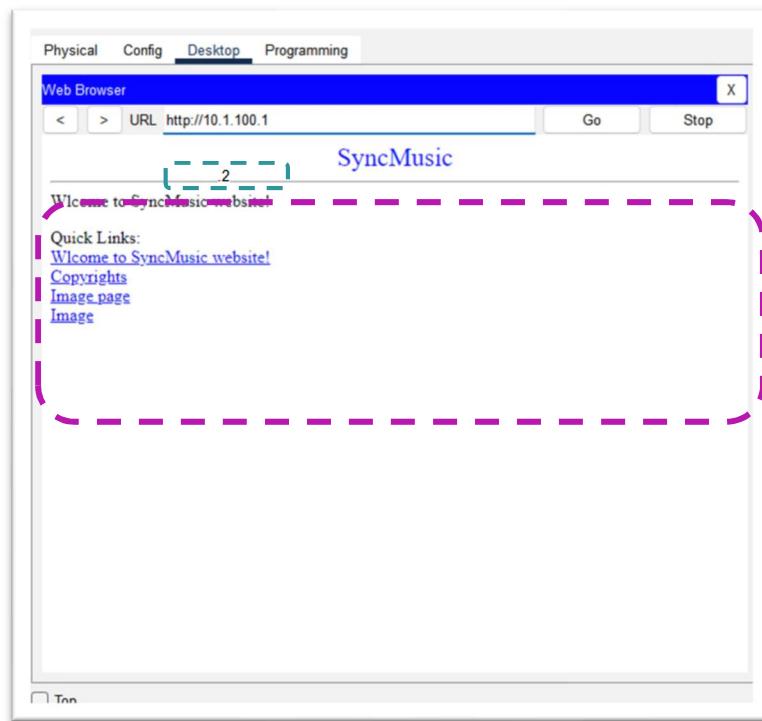
הגדירה כתובות IP לשירותים



הגדירת שירותים HTTP:

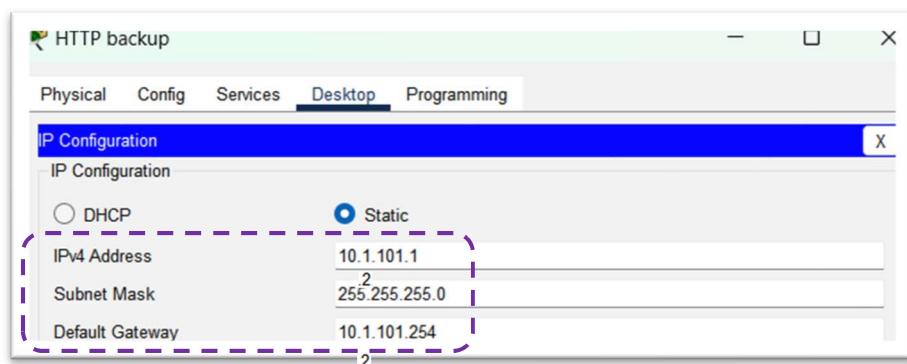
File Name	Edit	Delete
1 copyrights.html	(edit)	(delete)
2 cscoptlogo177x111.jpg		(delete)
3 helloworld.html	(edit)	(delete)
4 image.html	(edit)	(delete)
5 index.html	(edit)	(delete)

בדיקה שניית לגלוש אל האתר ממחשב



הגדרת HTTP בשרת ה-IP

הגדרת כתובת IP לשרתים

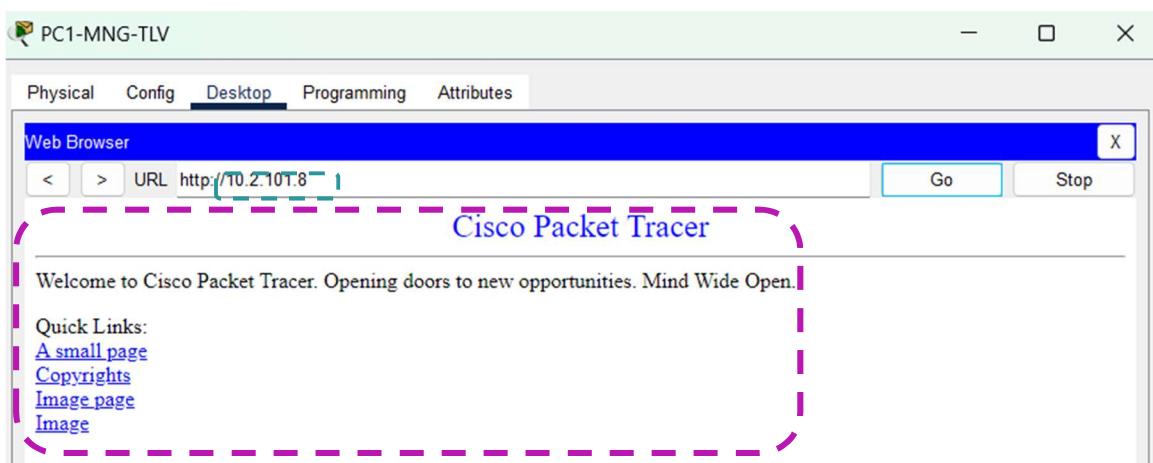


הגדרת שירות HTTP

The screenshot shows a configuration interface for a service. At the top, there are two sections: 'HTTP' and 'HTTPS'. Each section has a radio button labeled 'On' (selected) and 'Off'. Below these sections is a 'File Manager' table:

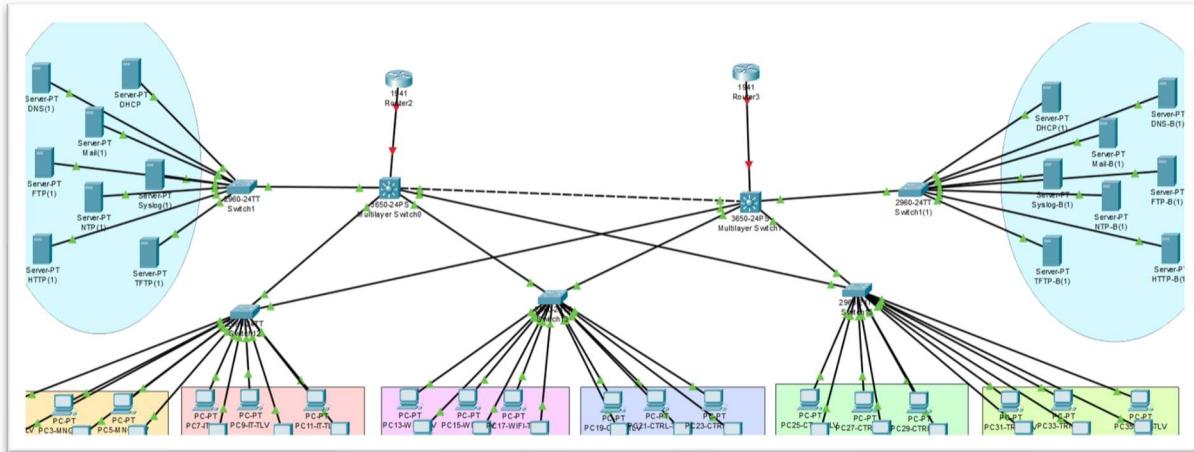
File Name	Edit	Delete
1 copyrights.html	(edit)	(delete)
2 cscoptlogo177x111.jpg		(delete)
3 helloworld.html	(edit)	(delete)
4 image.html הקובץ של האתר	(edit)	(delete)
5 index.html	(edit)	(delete)

בדיקה שנייתן לגלוש מהאתר אל המחשב

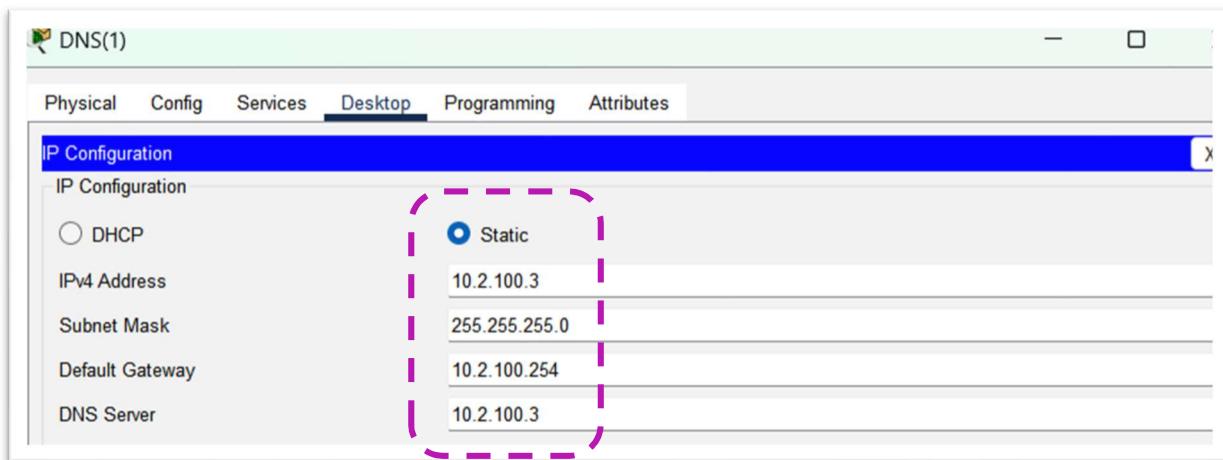


DNS Server

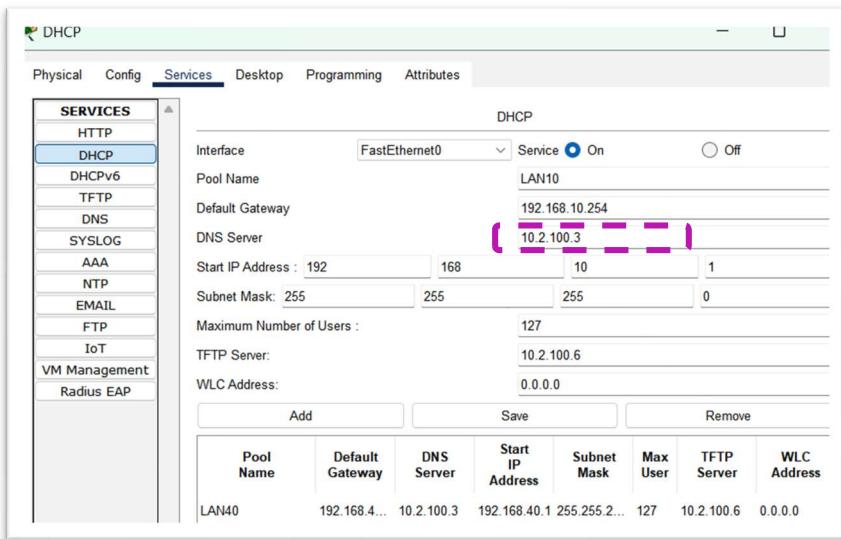
הגדרת שרת DNS ראשי



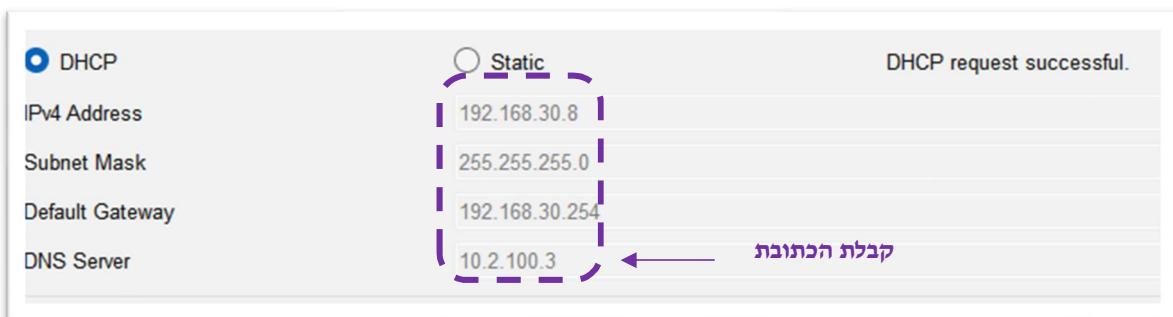
נתינת כתובות לשרת הראשי



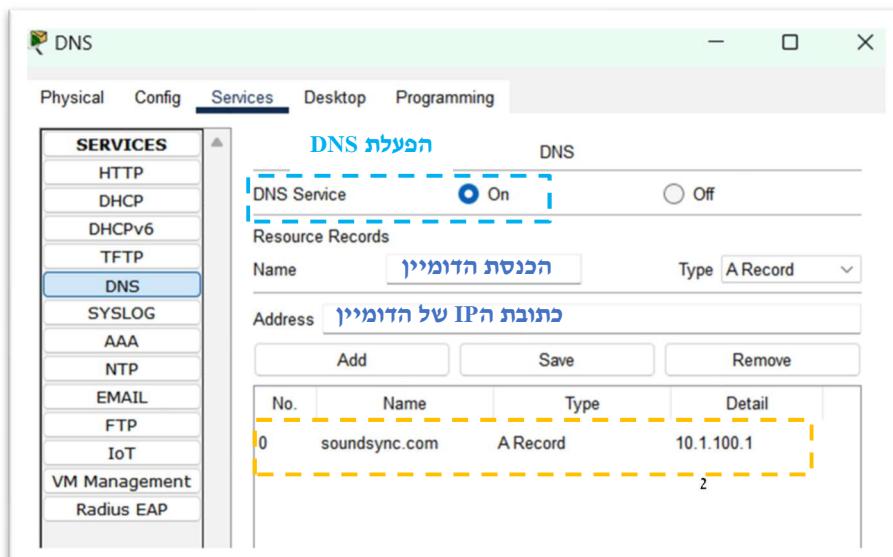
הוספת כתובות dns server בחלוקת כתובות על ידי ה-dhcp



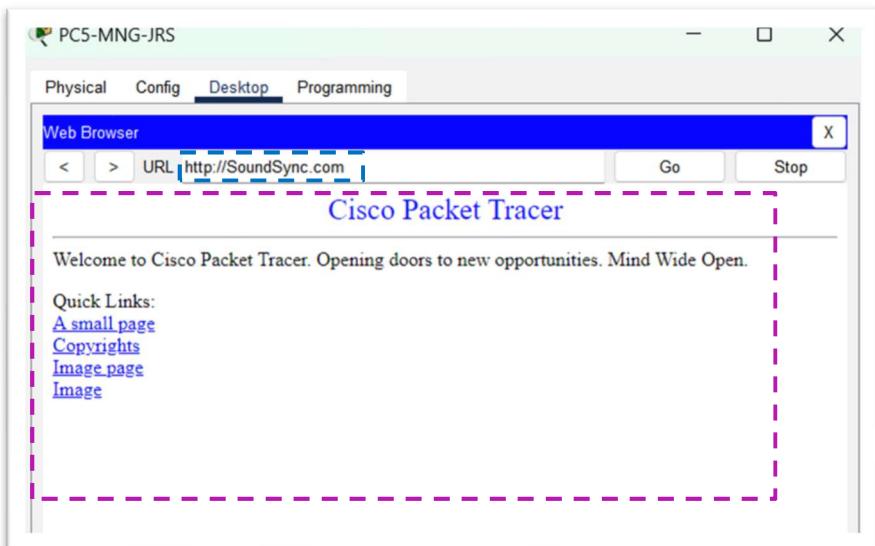
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנתב קיבלו את כתובת dns של השרת הראשי



הגדרת שרת dns

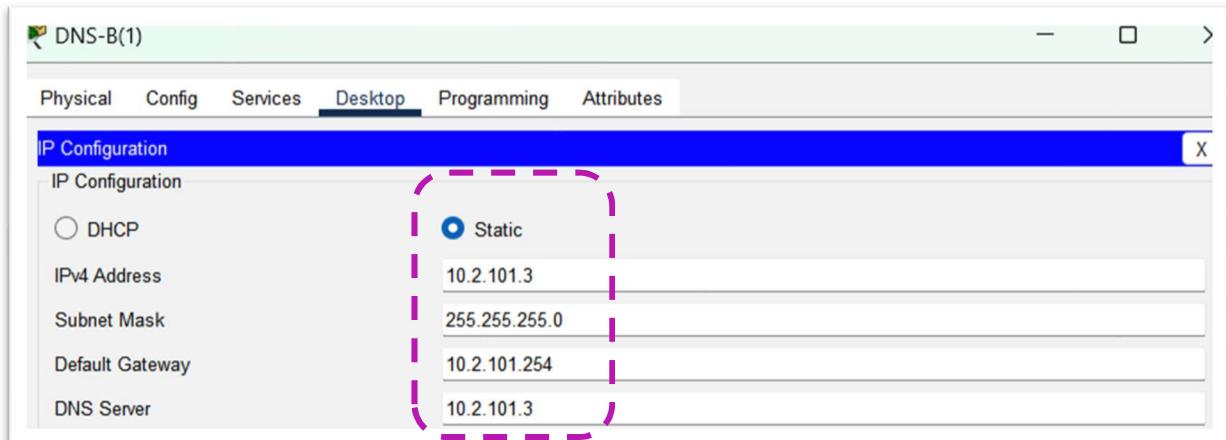


בדיקה על ידי גלישה לאתר לפי כתובת הדומיין



הגדרת שרת DNS גיבוי

נתינת כתובת לשרת גיבוי



הוספת כתובות dns server בחלוקת כתובות על ידי ה-dhcp

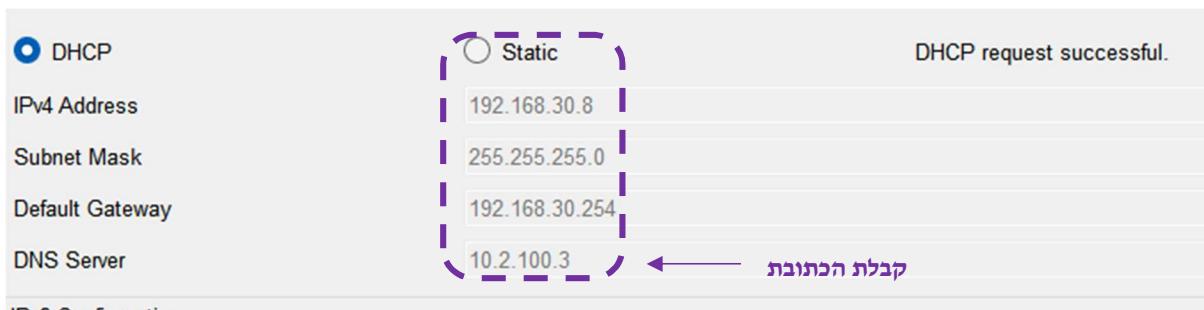
The screenshot shows the DHCP configuration page in Winbox. The left sidebar under 'SERVICES' has 'DHCP' selected. The main area is titled 'DHCP' and contains the following fields:

- Interface:** FastEthernet0
- Service:** On (radio button selected)
- Pool Name:** LAN10
- Default Gateway:** 192.168.10.254
- DNS Server:** 10.2.100.3 (highlighted with a red box)
- Start IP Address:** 192.168.10.1
- Subnet Mask:** 255.255.255.0
- Maximum Number of Users:** 127
- TFTP Server:** 10.2.100.6
- WLC Address:** 0.0.0.0

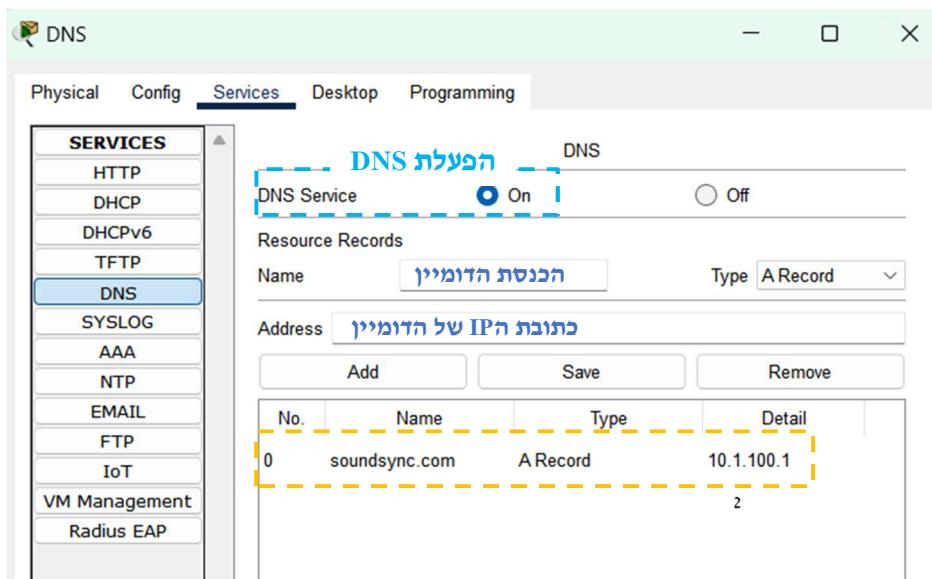
Below these fields are three buttons: 'Add', 'Save', and 'Remove'. A table at the bottom lists the pool configuration:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
LAN40	192.168.40.1	10.2.100.3	192.168.40.1	255.255.255.0	127	10.2.100.6	0.0.0.0

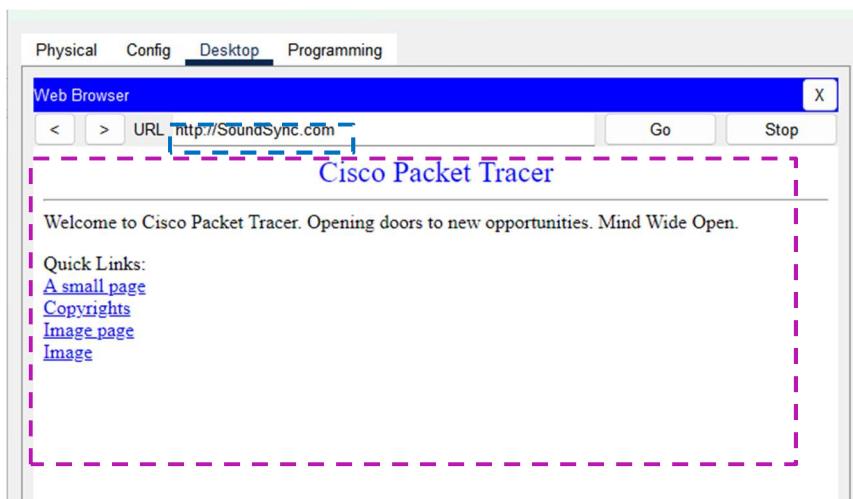
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנטב קיבלו את כתובות dns של השרת גיבוי
במקרה והשרת dns הראשי נפל



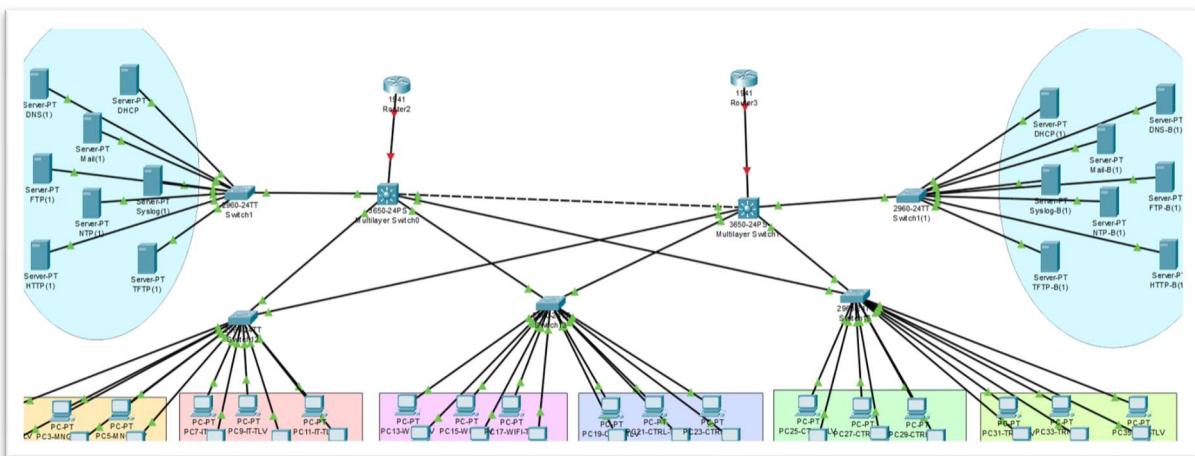
הגדרת שירות DNS



בדיקה על ידי גישה לאתר לפי כתובות הדומיין

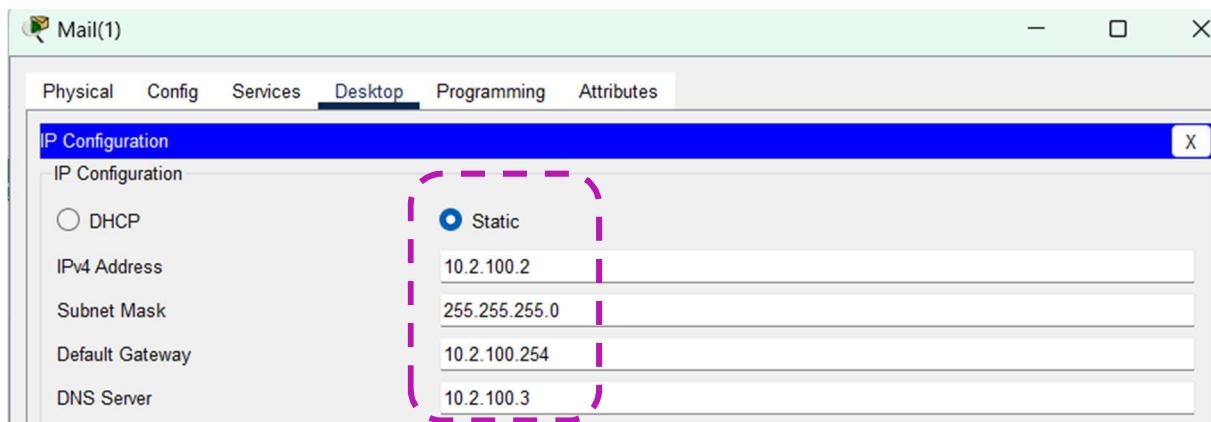


Mail

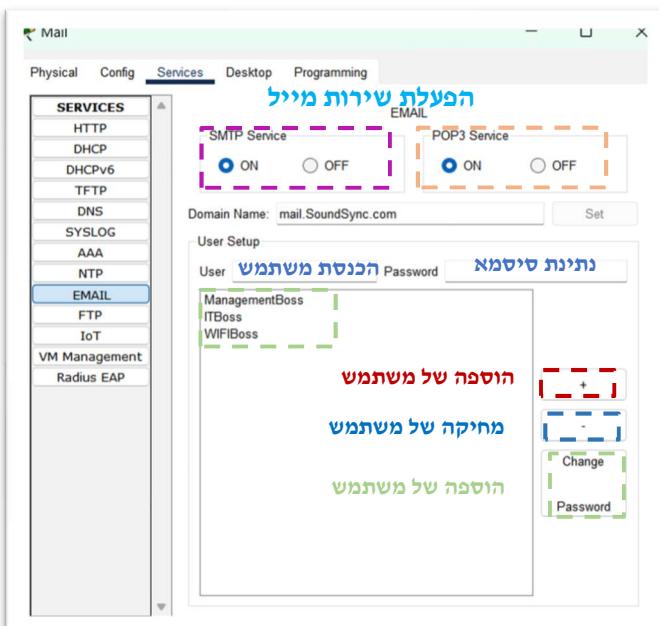


הגדרת שרת מייל ראשי

נתינת כתובות לשרת



הגדרת שרת-mail



הוספה mail לשרת DNS

The screenshot shows the 'DNS(1)' configuration window. The 'Services' tab is selected. On the left, a sidebar lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS (which is selected and highlighted in blue), SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main pane is titled 'DNS' and contains sections for 'DNS Service' (with an 'On' button) and 'Resource Records'. Under 'Resource Records', there is a table:

No.	Name	Type	Detail
0	ftp.soundsync.com	A Record	10.2.100.6
1	mail.soundsync.com	A Record	10.2.100.2
2	soundsync.com	A Record	10.2.100.1

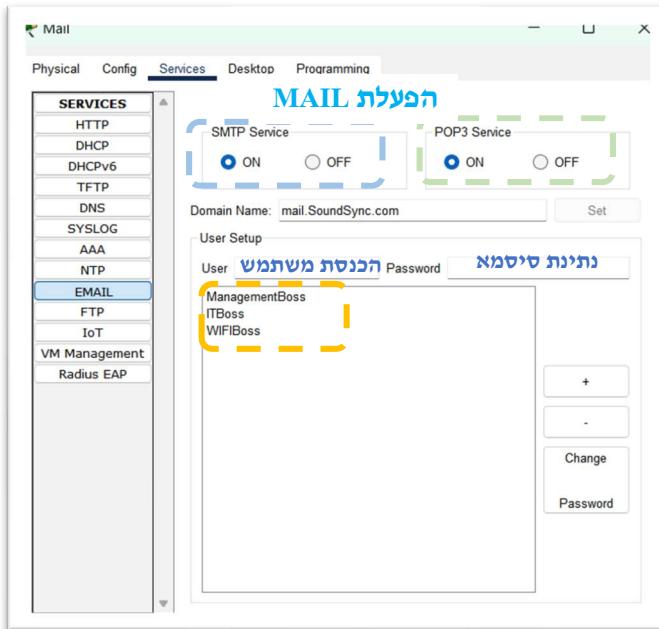
הגדלת שרת מייל Backup

נתינת כתובות לשרת

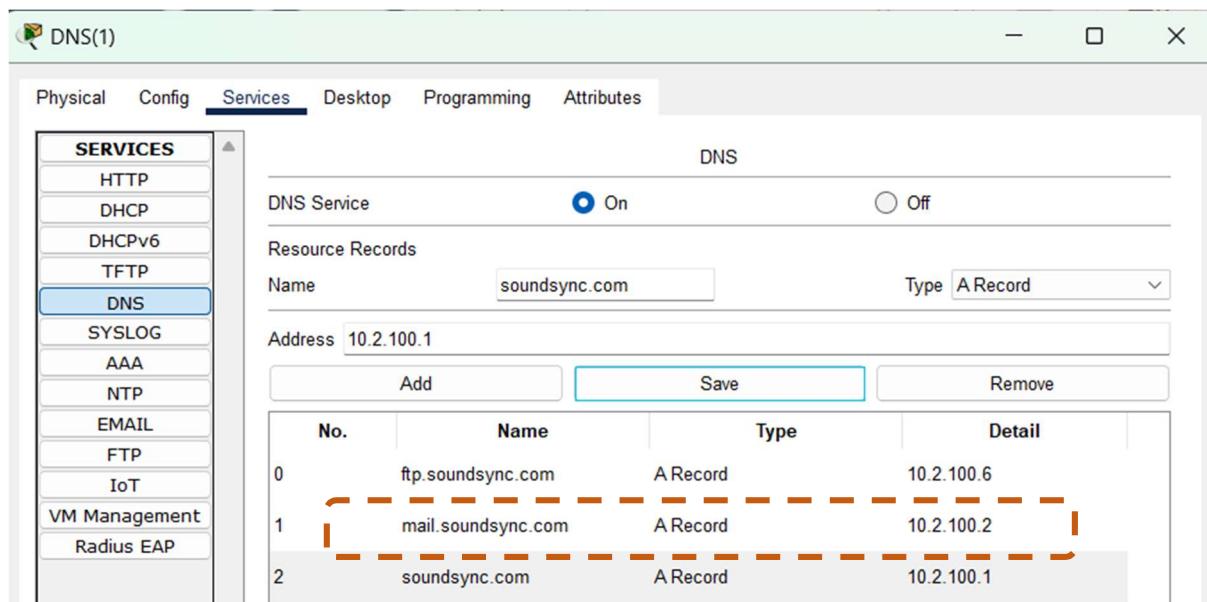
The screenshot shows the 'Mail-B(1)' configuration window. The 'Desktop' tab is selected. In the left sidebar, under 'IP Configuration', the 'Static' option is selected. The configuration fields are:

IPv4 Address	10.2.101.2
Subnet Mask	255.255.255.0
Default Gateway	10.2.101.254
DNS Server	10.2.101.3

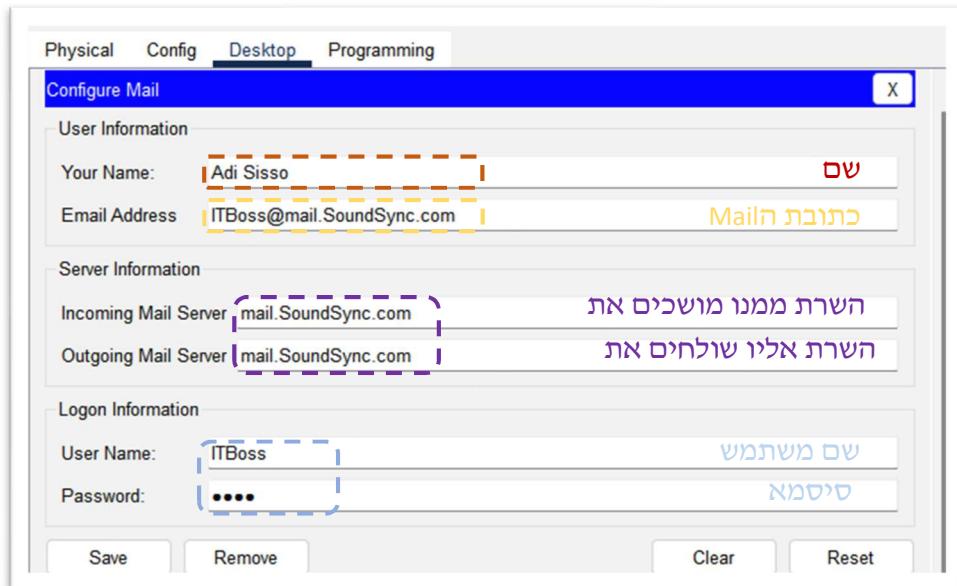
הגדרת שירות mail



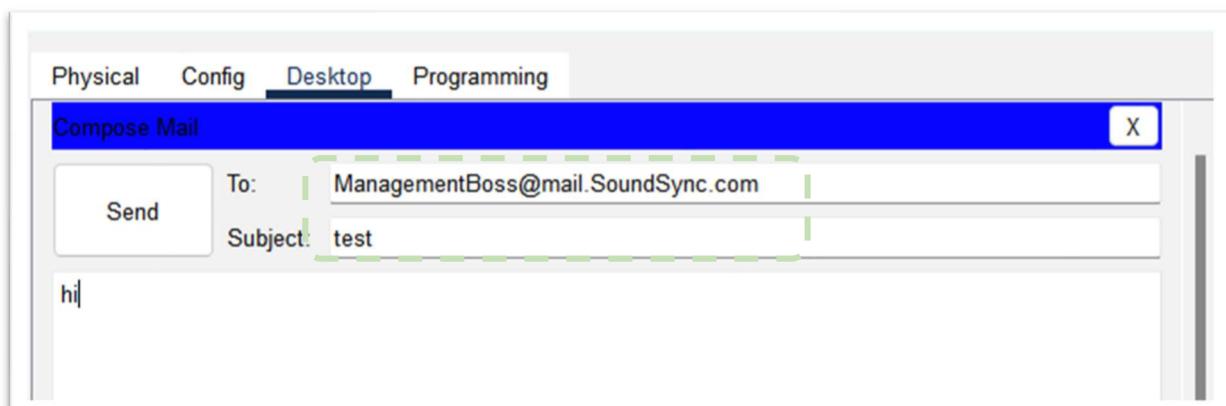
הוספה ה-DNS לשירות mail



בדיקה – התחברות משתמש דרך מחשב



בדיקה – שליחת מייל

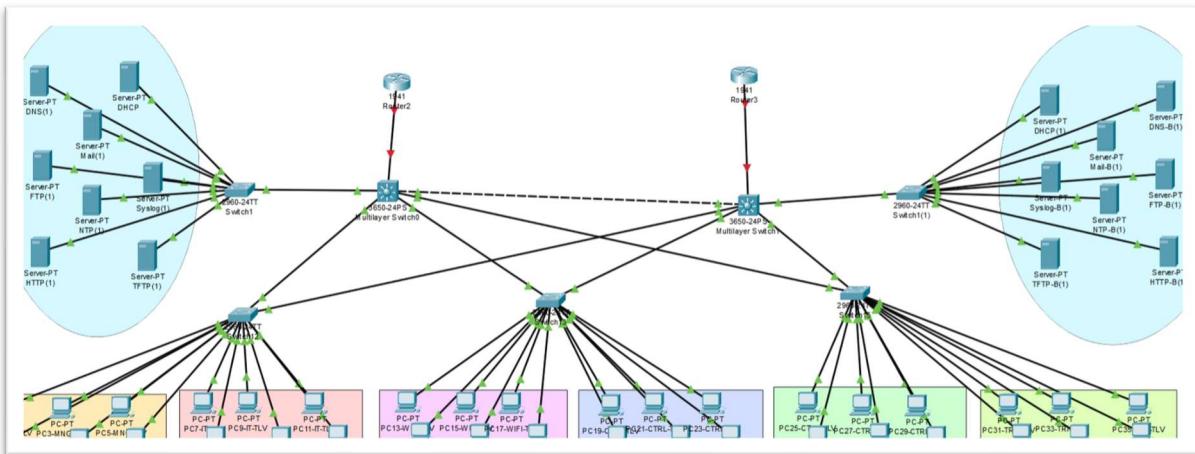


בדיקה – קבלת מייל

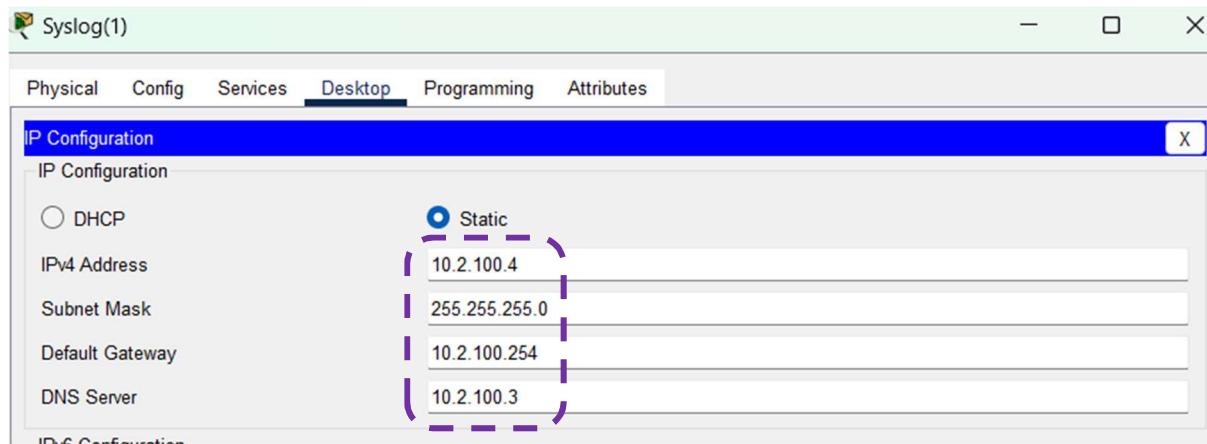
	From	Subject	Received
1	ITBoss@mail.Sound... (highlighted with a purple dashed box)	test	Sun Dec 3 2023 00:35:58 (highlighted with a purple dashed box)

שרת Syslog

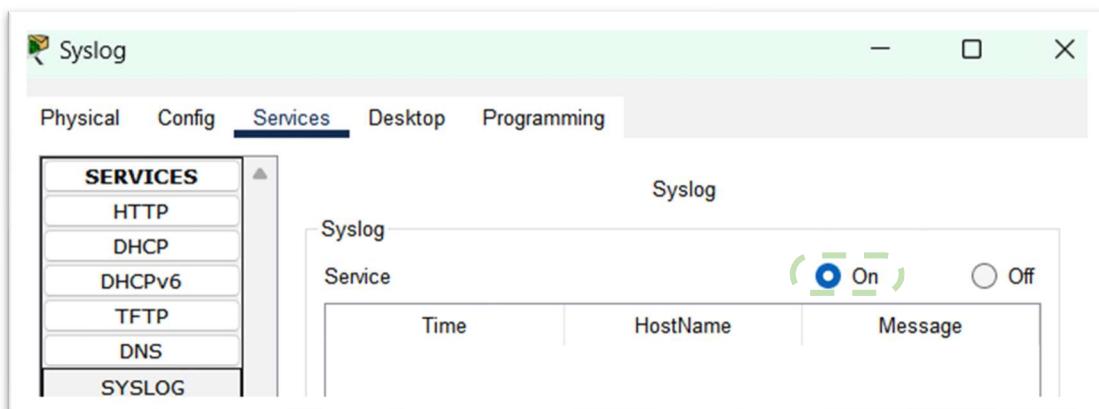
הגדרת שרת Syslog ראשי



הגדרת כתובת IP לשרת



הפעלת syslog



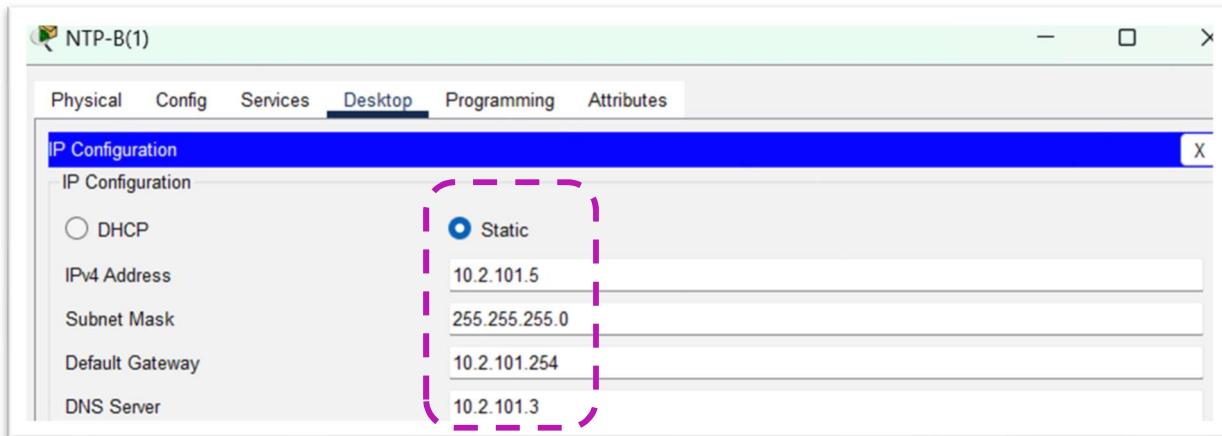
הפעלת שירות Syslog על המתגים והנתבים ברשת

```
MLS1-D-TLV(config)#logging host 10.2.100.4
MLS1-D-TLV(config)#logging host 10.2.101.4
```

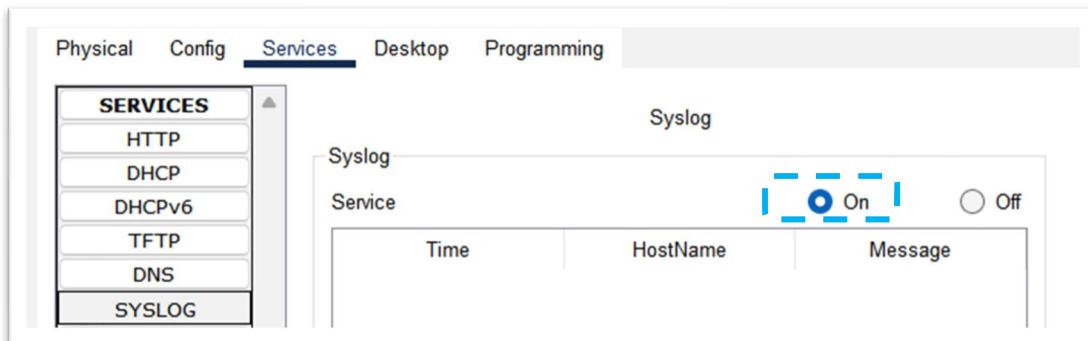
הגדרה מי שרתית syslog

הגדרת שרת Backup Syslog

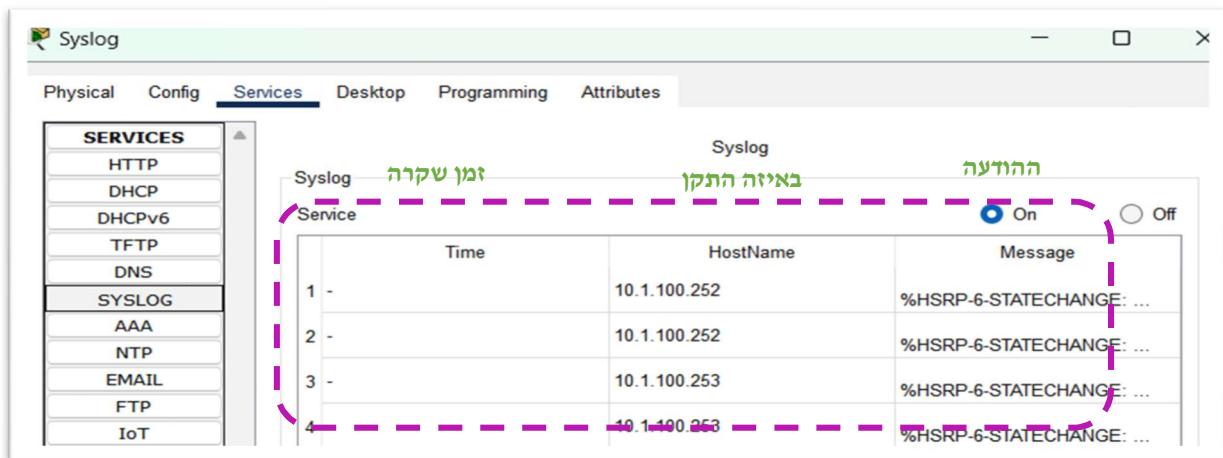
הגדרת כתובת IP לשרת



הפעלת שירות Syslog על המתגים והנתבים ברשת

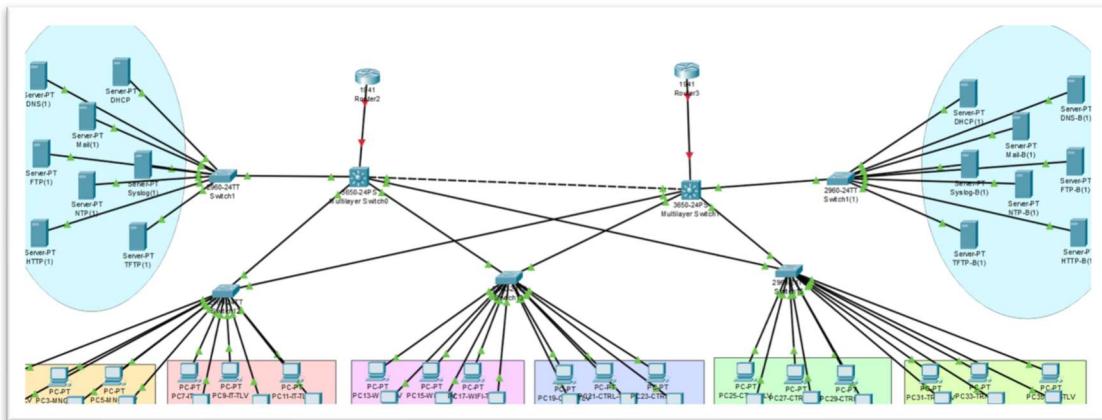


בדיקות שליחת רשומות Logs

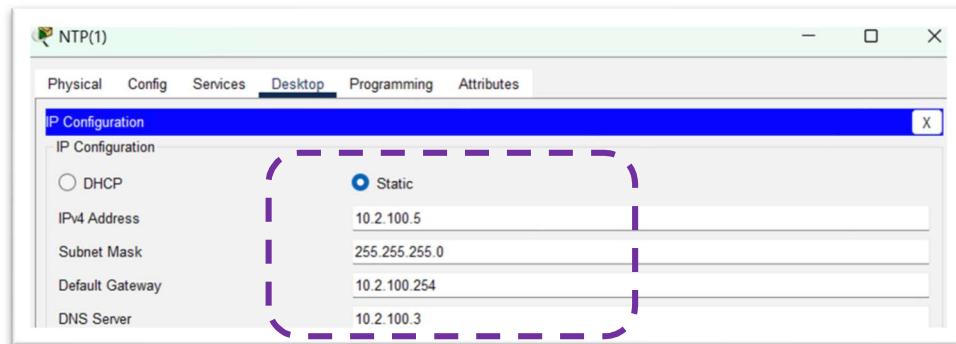


NTP Server

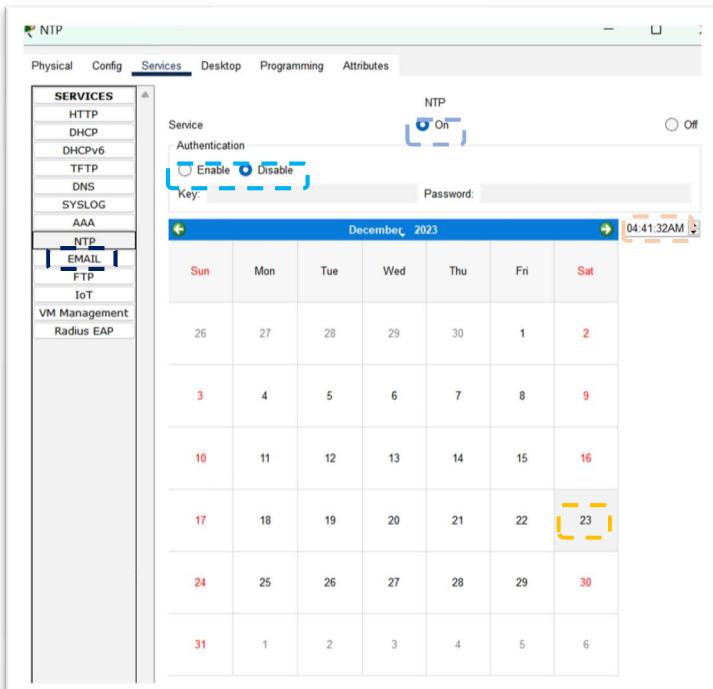
הגדרת שירות NTP ראשי



הגדרת הכתובות בשרת הראשי



הפעלת שירות NTP

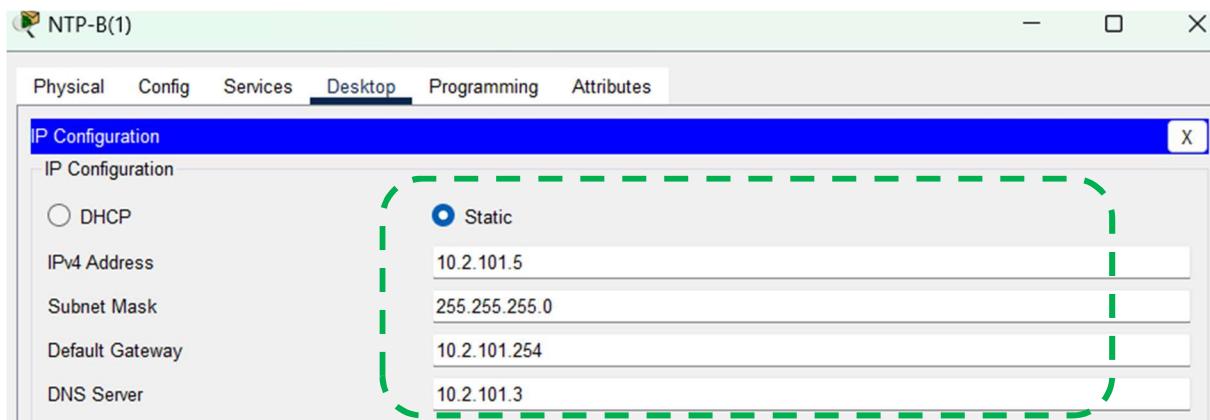


הפעלת השירות על כל הנטבים והמתגים ברשת

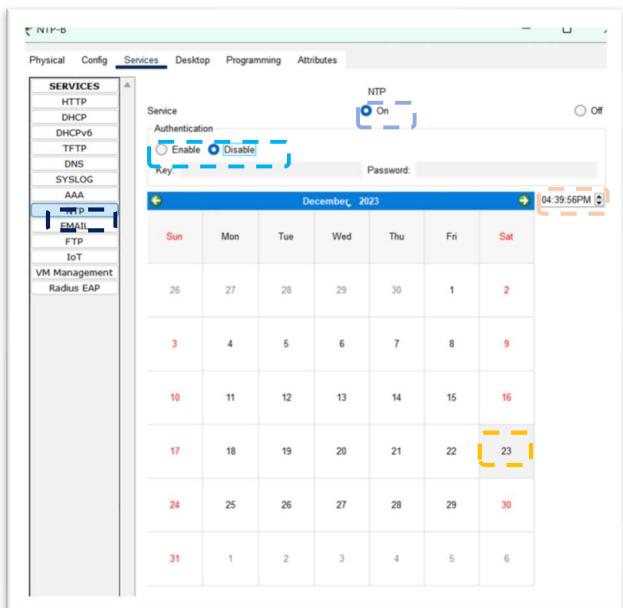
```
MLS1-D-TLV(config)#ntp server 10.2.100.5 | הגדרה מי שרת הNTP  
MLS1-D-TLV(config)#ntp server 10.2.101.5 | הוספה זמן ללוגים
```

הפעלת שירות NTP בשרת Backup

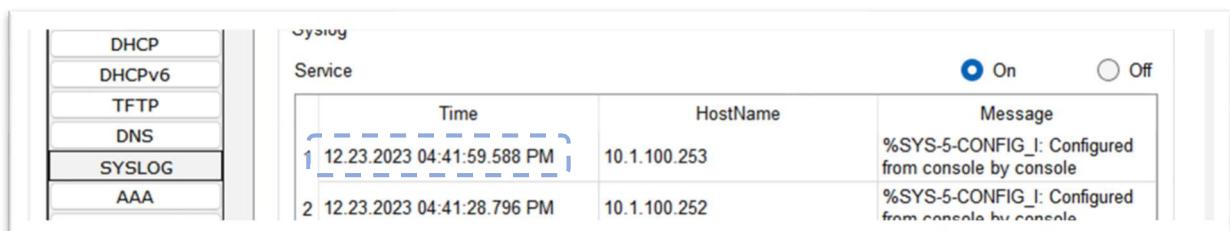
הגדרת הכתובות בשרת הראשי ובשרת Backup



הפעלת שירות NTP

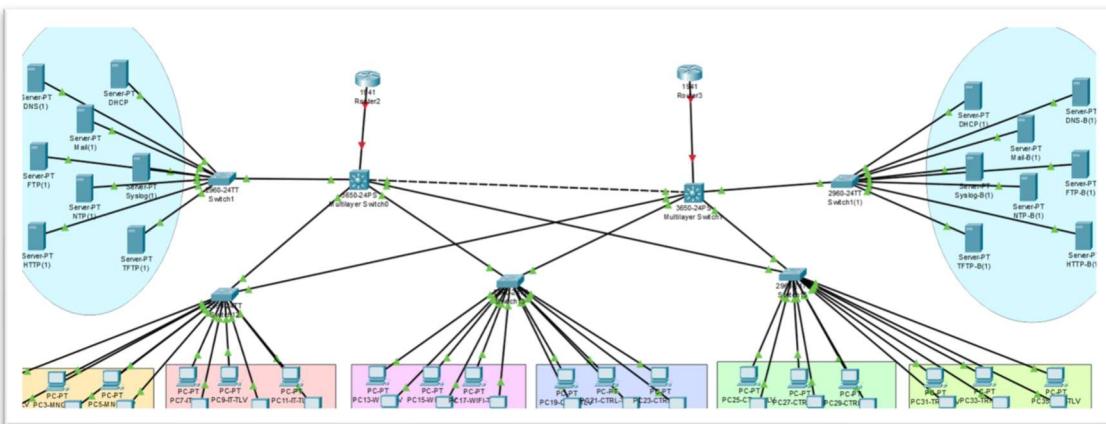


בדיקות שהשירות עובד



FTP Server

הגדרת שירות FTP ראשי



הגדרת כתובות לשרת

FTP(1)

- Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

- DHCP
- Static

IPv4 Address	10.2.100.6
Subnet Mask	255.255.255.0
Default Gateway	10.2.100.254
DNS Server	10.2.100.3

הוספה הקט בשרת DNS

DNS

DNS Service On Off

Resource Records

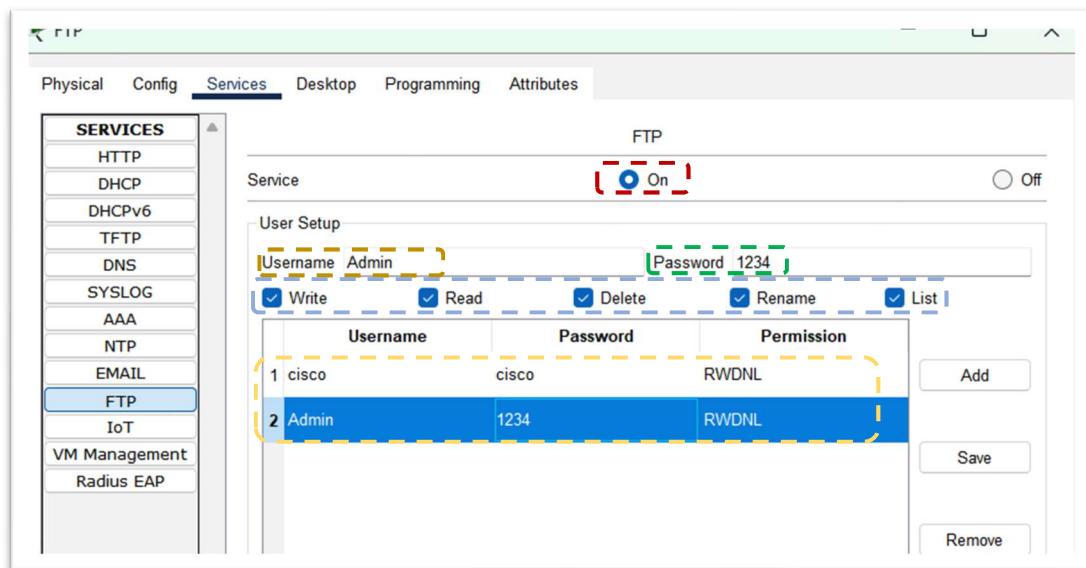
Name	Type
ftp.soundsync.com	A Record

Address 10.2.100.6

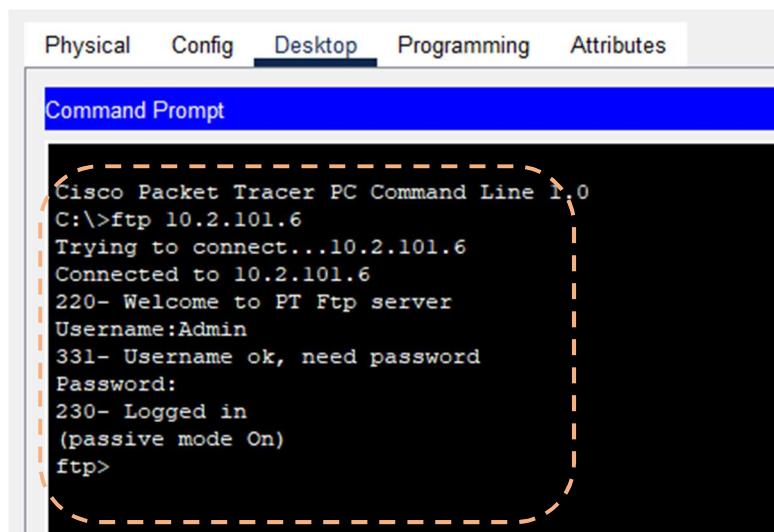
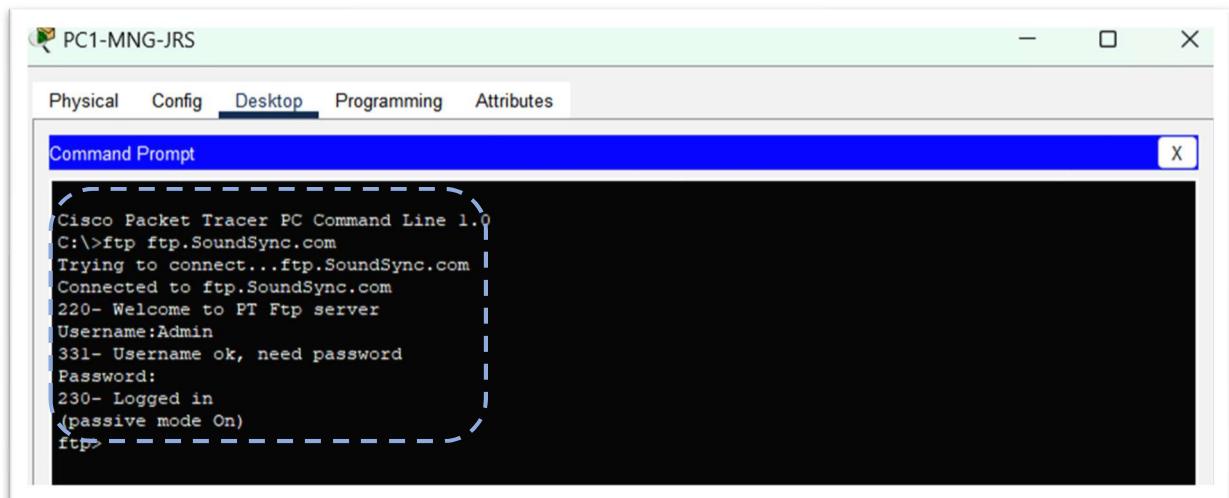
Add Save Remove

No.	Name	Type	Detail
0	ftp.soundsync.com	A Record	10.2.100.6

הוספה של שירות FTP

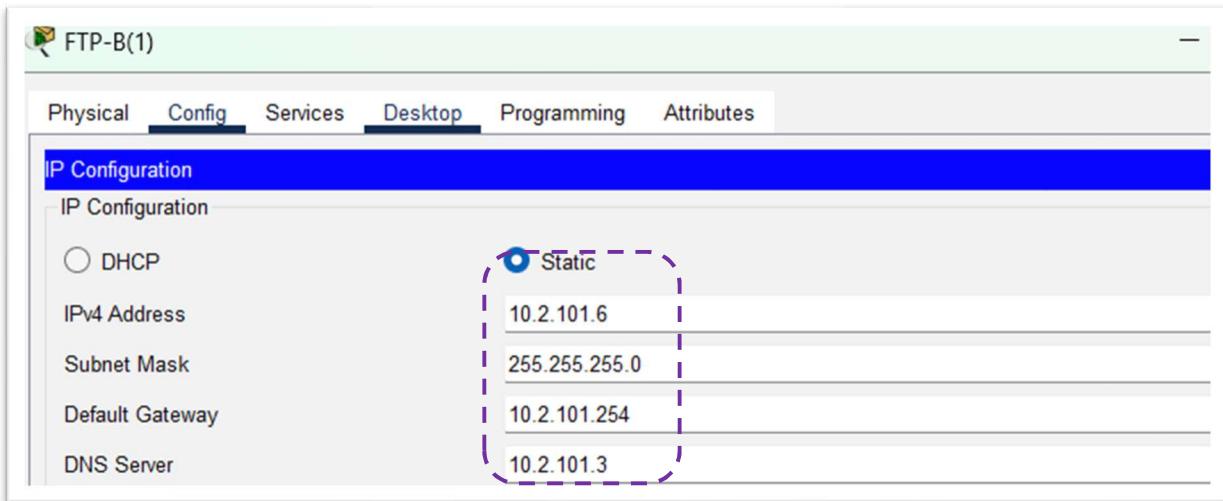


בדיקה – התחרויות FTP על ידי כתובות IP ו URL

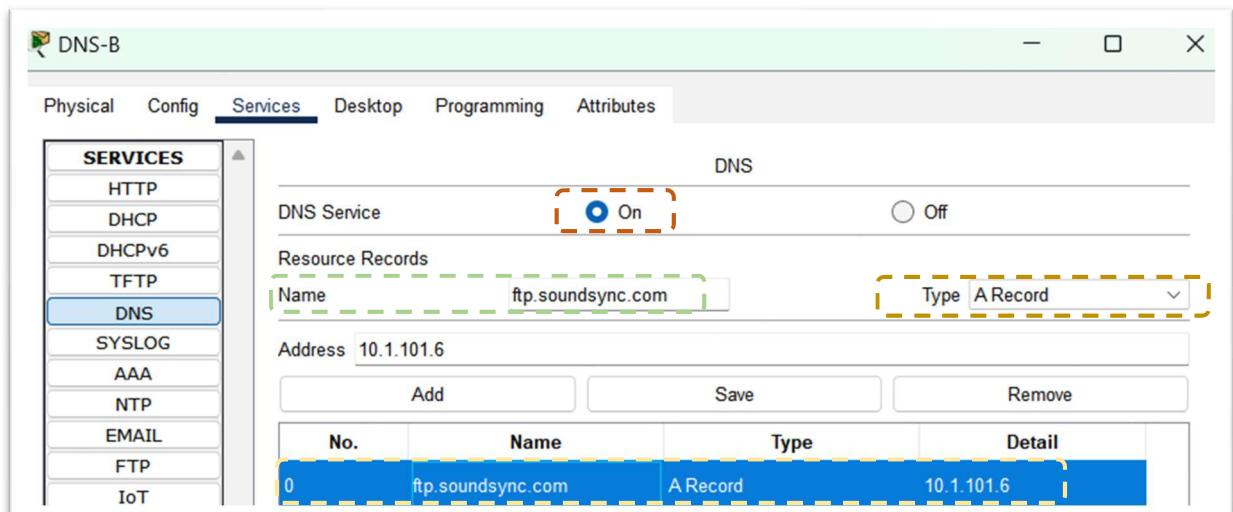


הגדרת שירות FTP גיבוי

הגדרת כתובות לשרת



הוספה הftp בשרת DNS



הוספה שירות FTP

The screenshot shows the 'Services' tab selected in the Cisco Packet Tracer interface. On the left, a sidebar lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, **FTP**, IoT, VM Management, and Radius EAP. The 'FTP' option is highlighted. The main panel displays the 'FTP' configuration screen. It includes fields for 'Service' (set to 'On'), 'Username' (Admin), 'Password' (1234), and checkboxes for 'Write', 'Read', 'Delete', 'Rename', and 'List'. A table lists two users: 'cisco' with password 'cisco' and permission 'RWDNL', and 'Admin' with password '1234' and permission 'RWDNL'. Buttons for 'Add', 'Save', and 'Remove' are visible on the right.

בדיקה – התחברות FTP על ידי כתובת IP וURL

The screenshot shows a 'Command Prompt' window from Cisco Packet Tracer. The user has typed 'C:\>ftp ftp.SoundSync.com' and is prompted for a password. The response shows the connection to the SoundSync.com FTP server, version 1.0, and the user is logged in with the username 'Admin'.

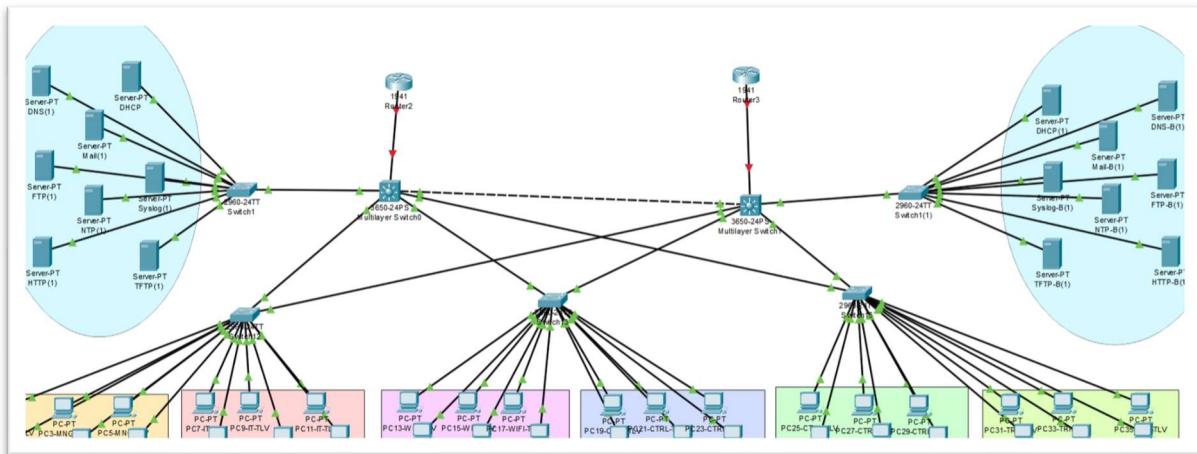
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp ftp.SoundSync.com
Trying to connect...ftp.SoundSync.com
Connected to ftp.SoundSync.com
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

The screenshot shows a second 'Command Prompt' window from Cisco Packet Tracer. The user has typed 'C:\>ftp 10.2.101.6' and is prompted for a password. The response shows the connection to the local host at IP 10.2.101.6, version 1.0, and the user is logged in with the username 'Admin'.

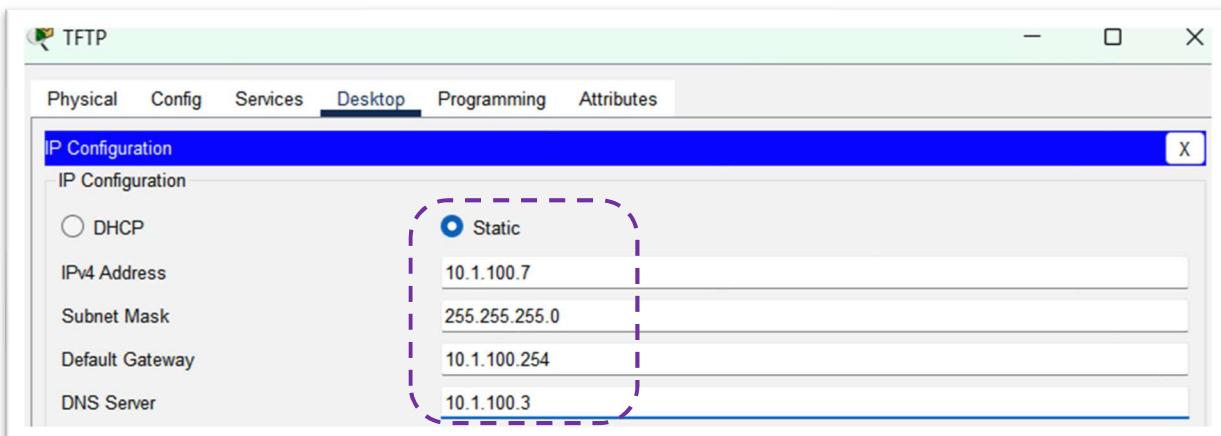
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.2.101.6
Trying to connect...10.2.101.6
Connected to 10.2.101.6
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

TFTP Server

הגדרת TFTP על השרת הראשי



הגדרת כתובות על השרת



הפעלת שירות TFTP



העתקת זיכרון NVRAM של המtab לשרת TFTP הראשי

```
R1-C-JRS#copy startup-config tftp  
Address or name of remote host []? 10.1.100.7  
Destination filename [R1-C-JRS-config]? R1-C-JRS.config  
  
Writing startup-config....!!  
[OK - 3001 bytes]  
  
3001 bytes copied in 3.008 secs (997 bytes/sec)
```

نمחק את config המtab

```
R1-C-JRS#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

חיבור הרשת של חוות השירותים אל הרouter (מכיוון שנמכוו ההגדרות)

```
Router(config)#int gigabitEthernet 0/0  
Router(config-if)#ip add  
Router(config-if)#ip address 10.1.100.254 255.255.255.0  
Router(config-if)#no shutdown
```

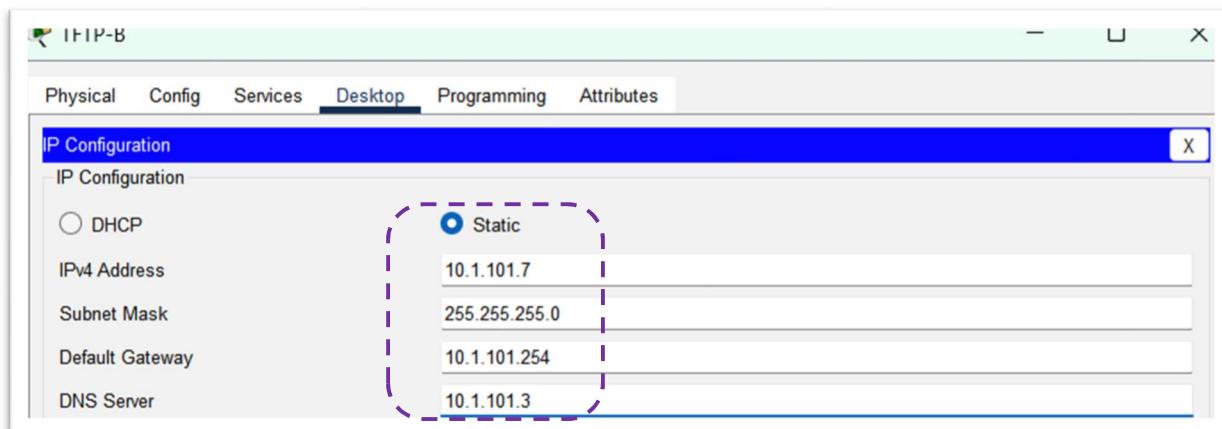
קיבלה קובץ config מהשרת

בדיקה שכל ההגדרות התקבלו

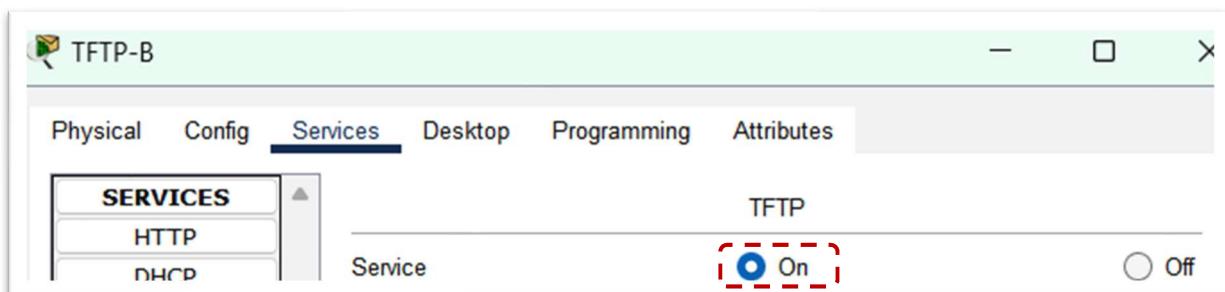
```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
dns-server 10.1.100.3
ip dhcp pool lan20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
dns-server 10.1.100.3
```

הגדרת TFTP על השרת הראשי

הגדרת כתובות על השרת



הפעלת שירות TFTP



העתקת ה-TFTP לשרת startup-config

```
R1-C-JRS#copy startup-config tftp
Address or name of remote host []? 10.1.101.7
Destination filename [R1-C-JRS-config]? C1-D-JRS.conf

Writing startup-config....!!
[OK - 3001 bytes]

3001 bytes copied in 1.84467e+16 secs (0 bytes/sec)
```

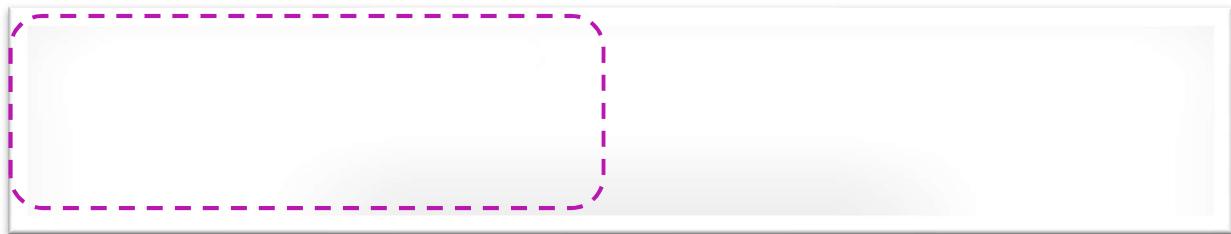
نمחק את config startup מהנתב

```
R1-C-JRS#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
>1_>_>_>_>_>_>_>_>
```

חיבור הרשות של חוות השירותים אל הרואוטר (מכיוון שנמכוו ההגדרות)

```
router(config)#int gigabitEthernet 0/0
router(config-if)#ip add
router(config-if)#ip address 10.1.100.254 255.255.255.0
router(config-if)#no shutdown
```

קיבלה קבועה startup-config מהשרת



בדיקה שכל ההגדרות התקבלו

```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.254
  dns-server 10.1.100.3
ip dhcp pool lan20
  network 192.168.20.0 255.255.255.0
  default-router 192.168.20.254
  dns-server 10.1.100.3
```

ניתוב הוא התהליך שבו מכשירים ברשות או מנהל הרשות מחליט להפנות מידע ונתונים מהמקור אל היעד. כאשר פאקטה נשלחת ברשות, היא עשויה לעבור דרך מסוימת מכשירים ונتابים עד שהיא מגיעה אל היעד, שכן יש צורך בקביעה של מסלולים אשר ישמשו להעברה של המידע.

פרוטוקול ניתוב – מסיע לנתב להעביר מידע אל רשותות אשר אין מחוברות אליו באופן ישיר.

קיימים שני סוגי של ניתוב:

- **ניתוב סטטי** - מסלולים קבועים המוגדרים ידנית על ידי מנהל הרשות, ללא התערבותה דינמית של הנتابים והתחשבות בתנאי הרשות. בתהליך זה, מנהל הרשות מגדיר באופן ידני את המסלולים המועדפים לשילוח חבילות הנתונים בין המקורות והיעדים ברשות.

יתרונות:

- פשוטות ויציבות: ניתוב סטטי הוא פשוט להגדירה ולהפעלה. מנהלי הרשות יכולים להגדיר מסלולים קבועים פעם אחת ולשכוח עליהם, מה שמקל על ניהול הרשות.
- פרודוקטיביות גבוהה: כיוון שהמסלולים קבועים ולא משתנים בהתאם לתנאי הרשות, ניתן לצפות בביצועים יציבים ובטוחים.
- מתאים לרוב לרשותות קטנות: ברשותות קטנות עם מבנה פשוט ומספר נמוך של נתבים, ניתוב סטטי יכול להיות פתרון מספק ופרקטי.

חסרונות:

- חוסר גמישות: ניתוב סטטי אינו גמיש ואינו יכול להתמודד באופן אוטומטי עם שינויים ברשות, כגון תקלות או עומס תעבורה.
- תגובה לאירועים: במקרה של שינויים ברשות, כגון פיצול דרך או נפילת קישור ניתוב סטטי לא יכול להתאים את המסלולים באופן אוטומטי, ולכן ניתן כי תגובה איטית או לא מתאימה

- **ניתוב דינامي** - תהליך בו הנתבים ברשות משתמשים באלגוריתמים ובפרוטוקולים כדי לקבוע את המסלולים המיטביים להעברת הנתונים ברשות בהתאם למצב הרשות בכל רגע נתון. בניתוב דינמי, הנתבים מקבלים מידע מתעדכן על תנאי הרשות ועל התעבורה על מנת לקבוע את המסלולים האופטימליים לשילוח הנתונים. הניתוב דינמי מאפשר לרשות להתאים ולהציג בזמן אמיתי לשינויים ברשות, כולל תקלות, שינויים בעומס, ושינויים במבנה הרשות. הנתבים מתעדכנים באופן רציף על ידי חישובים אוטומטיים ותהליכי עדכון כדי להבטיח שהמסלולים יהיו המתאימים ביותר לתנאי הרשות בזמן אמיתי.

יתרונות:

- גמישות ואופטימיזציה : היכולת להתאים את המסלולים לתנאי הרשות עשויה לשפר את ביצועי הרשות ואת זמינותה.
- התאמה אוטומטית : הנטים מקבלים החלטות בזמן אמת על מסלולי הנתונים, מה שcosaץ זמן ומשאבים למנהל הרשות.
- עמידות בפני תקלות : כיוון שהנתוב מתבצע בזמן אמת, הרשות מסוגלת להתמודד ביעילות עם תקלות כגון נפילות קישור או שינויים בתנאי הרשות.

חסרונות:

- משאבים נוספים : נתוב דינמי דורש יותר משאבי מערכת מניטוב סטטי, ועשוי להוביל להורדת ביצועי הרשות במקרים של עומס גבוה.

נתוב דינامي גם הוא מחלק לשני סוגי משפחות : Distance vector ו Link state :

השוואה בין Link state ל Distance Vector

Link State	Distance Vector	
OSPF	BGP, EIGRP, RIP	פרוטוקולים שעובדים בשיטה זו
מכיר את כל הטופולוגיה	מכיר רק את הנטים השכנים	הכרת הטופולוגיה
התכנסות מהירה במקורה של שינוי טופולוגיה (1 - 5 שניות)	התכנסות איטית (30 - 90 שניות), הנטים מכירים רק את הנטים השכנים שלהם ולן לוקח יותר זמן למצאו נתיב חלופי	התכנסות - הזמן שלוקח לחישוב מיציאת נתיב חלופי במקורה והנתיב הראשי נפל
OSPF - Dijkstra/spf	EIGRP - Dual RIP - Bellman-Ford	אלגוריתם חישוב נתיב
רוחב פס גבוה: • דרש הכרות עם כל הטופולוגיה • מצריך חישובים מורכבים יותר • יכול לעבד עם מספר Process ID	רוחב פס נמוך • לוקח פחות משאבי עיבוד וזיכרון	שימוש ברוחב פס
הראוטר מחליט איזה נתיב לבחור בהתאם על המידע שיש לו על השכנים שלו	בחירה נתיב	

Enhanced Interior Gateway Routing Protocol

פרוטוקול EIGRP הינו פרוטוקול ניתוב דינامي אשר פותח על ידי חברת Cisco אך נתמך גם בנתבים אחרים. פרוטוקול זה שיך למשפחת Distance Vector אך מקיים מאפיינים גס של משפחת Link state协议. לכן נחassoc כפרוטוקול היברידי (IGP) ככלומר, כמוות המידע שלו על טופולוגיה הרשות מצומצם אך הוא שומר גם נתיבי גיבוי. הוא משתמש באלגוריתם הנקרא Dual על מנת לחשב מהו הנתיב הטוב ביותר ולמנוע לולאות ניתוב ברשת. תוצאת החישוב של האלגוריתם נקראת metric.

הפרוטוקול עובד עם פורט 88, וערך AD (Administrative Distance) שלו הוא 90 כאשר מוגדר באופן מקומי ו-170 כאשר מוגדר חיצונית (External).

గורסאות ה프וטוקול:

- EIGRP העובד עם כתובות IPv4
- EIGRP העובד עם כתובות IPv6

מאפייני Diatance Vector

Link State	Distance Vector
מסנכרן טבלאות ניתוב בעת הקמת שכנות	שולח את העלות של הנתיבים לכל רשות
משתמש ב프וטוקול אמינות (RTP) על מנת להעביר עדכוני ניתוב	סופר קפיצות (ברירת מחדל 100, מקסימום 255)
בודק לולאות ניתוב	שולח עדכוני Distance Vector המכילים מידע על הרשותות
שולח עדכונים רק במצב של שינוי בטופולוגיה	משתמש בפרמטרים המשויכים למשפחה זו על מנת לחשב את הנתיב לעוד: Bandwidth, Load, Reliability, Delay

בחירה הנתיבים בטוביים ביותר: metric וערך k

קיים חמשה ערכי k המשמשים לחישוב metric של כל נתיב על מנת לבחור את הנתיבים הטוביים ביותר

- **K1 רוחב פס (Bandwidth)** – מהירות השידור דרך ממושך, קבוע על פי רוחב הפס הנМОך ביותר בנתיב. ניתן לשנות את ערך זה באופן ידני לכל ממושך
- **K2 אמינות (Reliability)** – אמינות המושך. איזה נתיב הכי יציב עם הכי פחות נפילות. קבוע על פי ערך האמינות הנMOך ביותר בממושך. הערך נע בין 0 – 255 כאשר הערך 255 מעיד על 100% אמינות במושך. ככלומר המושך תקין ב100%
- **K3 עיקוב (Delay)** – מעיד כמה עיקוב יש על אותו ממושך. קבוע על פי סוג המושך וסכום העיקובים בכל נתיב. ניתן לשנות את ערך זה בצורה ידנית על המושכים
- **K4 עומס (Load)** – העומס על המושך. קבוע על פי ערך האמינות (K2) הנMOך ביותר, כאשר ערך של 255 אומר כי המושך 100% עמוס.
- **K5 גודל מקסימלי של הפאקטה (Maximum Transmission Unit) MTU** – 5K

בברירת המחדל הערכים של K1 ו-K3 הם 1 ושל שאר ה-K הוא 0. EIGRP משתמש רק בערכי K1 ו-K3 על מנת לחשב את ה-Metric של הנתיב, זאת מכיוון שהעומס על המושך והאמינות שלו מרבבים להשתנות מה שעלול לגרום לשינויים רבים בטבלת הניתוב בזמן קצר. ניתן לשנות את ערכיים אלו בצורה ידנית.

הנוסחה לחישובי metric:

$$\text{Metric} = \left[\left(K1 * \text{BW}_{\min} + \frac{K2 * \text{BW}_{\min}}{256 - \text{load}} + K3 * \text{delay} \right) * \frac{K5}{K4 + \text{reliability}} \right] * 256$$

$$\text{where } \text{BW}_{\min} = \frac{10^7}{\text{least-bandwidth}}$$

ערכים ה-K חייבים להיות זהים בכל הראותרים על מנת ליצור יחסי שכנות. כאשר הערכים שונים, אין תקשורת.

בחירהו הנכון בטוב ביותר

עריך metric₁ / RD (Reported Distance / Advertised Distance) נתיב. עלות המרחק מהנתיב השכן אל רשות היעד. כאשר נתיב מפרסם לשכניו נתיב, הוא מפרסם בנוסף גם את RD של הנתיב.

עריך Matrix₂ FD (Feasible Distance) הכלול של כל נתיב, מהנתיב אל רשות היעד. עלות המרחק המלאה מנtab אל היעד כולל עלות המרחק מהשכן אל היעד.

הנתיבים הנבחרים:

S – הנתיב הטוב ביותר, יבחר לפי הנתיב בעל ערך FD הנמוך ביותר. והוא יבחר לנתייב הראשי. כבירות מחדל יכול להיות 4 successors לכל רשות.

FS (Feasible Successor) – נתיב גיבוי, יבחרו אלו שיש להם ערך FD יותר גבוה מהנתיב הנבחר, משמשים כנתיב גיבוי ומואחסנים בטבלת הטופולוגיה במקרה שהנתיב הראשי יפול רק נתיבים אחדים נמוך מערכם – FS של הנתיב הנבחר ייחשבו כנתיבי גיבוי. ככלומר :

FS = FD(Successor) > AD

Router ID

לעומת OSPF, בו קיימת חשיבות לכך שערך Router ID יהיה שונה בכל אחד מהנתבים על מנת לקיים תקשורת, ביג'פ EIGRP הינו מקומי בלבד (локלי) ואינו מופץ החוצה לשאר הנתבים. אין חשיבות למספר בעט ביצוע הניתוב ולכן ניתן לתת לכמה רוטרים Router ID זהה, למروת שלא נהוג.

דרך הבחירה של id router זהה לזה של ה-ospf:

- .1 הגדרה ידנית
- .2 כתובות הloopback הגבוהה ביותר
- .3 כתובות הקן הגבוהה ביותר

סוגי הודעות ב-EIGRP

- הودעה הנשלחת כל כמה שניות על מנת לתחזק קשר עם שכנים קיימים ולגלות שכנים חדשים.
- הודעת עדכון, במידה וمتבצע שינוי כלשהו בטופולוגיה, תשלח הודעה זו. במידה ומוגלה שכן חדש, ישלחו אליו הודעות עדכון שמעבירים לו את כל טבלת הטופולוגיה.
- במקורה שתיב הופך ללא זמין, הנטב שולח הודעה זו במטרה לחפש נתיב חלופי.
- נשלחת בתגובה להודעת Query.
- נשלחת כאישור על קבלת ההודעות האחרות.
- ACK



טבלאות ב-EIGRP

- פרוטוקול זה מתחזק 3 טבלאות:
- **טבלה שכנים** – טבלה המכילה רשימה של כתובות IP של השכנים והמשקים דרכם אפשר להגיע אל שכנים אלו. ב프וטוקול זה השכנים הינם הנתבים המוחברים לנטב באותו Broadcast Domain ושיכים אותה מערכת אוטונומית (AS).
 - **טבלה ניתוב** – טבלה המכילה מידע על הנתבים הטובים ביותר לכל רשות מוכרת. בפרוטוקול זה יכולים להיות עד 4 נתבים בעלי אותה עלות. היתרונו הינו איזון עומסים
 - **טבלה טופולוגיה** – טבלה המכילה רשימה של הנתבים אשר נלמדו מן הנתבים השכנים

טבלת טופולוגיה

כאשר הנטבים יצרו ביניהם יחסים שכנות, הם יתחלו לשתף מידע של ניתוב אחד עם השני. עדכון של כל נתב מכיל רשימה של הנטבים אותו הוא מכיר ואת Metric של כל אחד מהם. נתבים אלו יכנסו לטבלה הטופולוגיה של EIGRP אותה ניתן לראות עם הפקודה **show ip eigrp topology**. האלגוריתם Dual משמש בטבלה זו על מנת לזרות עד ארבעה נתבים ראשיים שונים ולהעביר אותם לטבלת הניתוב. בטבלה זו נראה את הFD ואת AD של כל אחד מהשכנים.

טבלת ניתוב

בטבלת הניתוב יופיעו הנתבים הטובים ביותר אל היעד (עד 4 נתבים). טבלה זו מ מלאת על ידי תוצאות החישוב של האלגוריתם Dual המבוצע על טבלת הטופולוגיה.

EIGRP Neighbors

פרוטוקול EIGRP יוצר יחסי שכנות הנקראים **Adjacencies** עם הנטבים האחרים הנמצאים אליו באותו **domain Broadcast** ובאותה מערכת אוטונומית. גילוי של שכנים אלו והתחזוקה של הקשר איתם, נעשית על ידי שליחת הודעות **Hello**.

הודעות אלו נשלחות כל 5 שניות כברירת מחדל בהודעת broadcast לכתובת 224.0.0.10 (במשקים איטיים נשלחות כל 60 שניות). לכל הודעה **Hello** קיימת חותמת זמן המגדירה כמה זמן ההודעה בתוקף. חותמת זאת נקראת **hold time**. אם עבר הזמן המוקצב ב-**hold time** והנתב השכן לא החזיר הודעה hello, השכן יחשב כאזמין והנתב ימחק אותו מטבלת השכנים. ערך ברירת המחדל של **Hold time** הוא פי 3 מהזמן המוקצב של שליחת הודעה **Hello** (15 במשקים רגילים, 180 במשקים איטיים יותר).

על מנת להראות את טבלת השכנים נשימוש בפקודה **show ip eigrp neighbors** זו יוכל לראותו כמה פרמטרים:

- Hold time – ספירה לאחר מכן מהיקת הנתב מטבלת השכנים במצב בו הנתב אינו מקבל הודעה hello מהשכן
- Uptime – כמה זמן אתה שכן עם הנתב, כמה זמן הוא נמצא בטבלה. ככל שהזמן גבוה יותר כך הוא נחשב יותר אמין
- Q count – כמה הודעות ממתיינות לשילוח, אם המספר גבוה מ 0 זה אומר שהנתיב איטי
- Num seq – המספר של ההודעה الأخيرة שהתקבלה מסוג **Query** ו-**Reply** ו-**Update**. מספר זה צריך להיות תואם לזה של השכן
- SRIT – הזמן שלקחת לחבילת EIGRP להגיע אל השכן ולהזור חזרה לנtab
- RTO – הזמן שהחכה הנתב לפני ששלח הודעה **Unicast** במקרה בו לא התקבלה הודעה מהשכן

על מנת ליצור יחס שכך ישנים כמה פרמטרים אשר חייבים להיות זהים בכל הנתבים

ערכיהם זהים

מסכת רשת M.S	-
מספר AS	-
ערכי K	-
אותה סיסמת אימות – Authentication	-

מצבי נתבים

האלגוריתם Dual מבצע חישובים על נתבים על מנת למצוא את הנתבים הטובים ביותר אל היעד

הנתיב זמין, לא מבוצעים על נתיב זה חישובי .EIGRP – <u>Passive (P)</u>	-
הנתיב אינו זמין, מבוצעים על נתיב זה חישובי .EIGRP – <u>Active (A)</u>	-
נשלחה הודעה עדכון לרשת זו. – <u>Update (U)</u>	-
נשלחה הודעה Reply לרשת זו. – <u>Reply (R)</u>	-

Auto Summarization

במצב בו קיימות רשתות גדולות עם M.S שונה, נרצה להפחית את כמות הנתבים שהנתב צריך לזכור ולתזק ולהפחית מכמות העדכנים. לכן, משתמש בסכימה רשתות שהיא שיטה לייצוג רשתות רבות תחת כתובות אחת המסכםת את רשתות אלו. ניתן לעשות סכימה של רשתות באופן ידני ואוטומטי. לעומת פרוטוקולי ניתוב אחרים, EIGRP תומך בסכימה אוטומטית של רשתות.

על מנת לסכם את הרשתות נרשם את הפקודה auto-summary

אייזון עומסים

במקרה בו קיימים כמה נתבים עם עלות זהה, יתקיים אייזון עומסים וכל הנתבים בעלי אותה עלות יכנסו לטבלת הניתוב והתעבורה בראש תעבור דרכן 2 הנתבים הללו בצורה שווה.

לעתם פרוטוקולים אחרים, EIGRP תומך באיזון עומסים גם אם $cost$ של הנתבים אינו זהה.

הפקודה לכך נקראת Variance והוא ערך מספרי בין 1 – 128. מטרתה להגיד לנtab בין אילו נתבים לבני אייזון עומסים ולהכניס אותם לטבלת הניתוב כל הנתבים אשר $cost$ שלהם קטן יותר מהמספר שהגדנו בפקודת variance כפול העלות הנמוכה ביותר אל היעד.

כמויות הנתבים המקסימלית אשר ניתן לאיזן את העומסים ביניהם הינה 32.

EIGRP Passive Interface

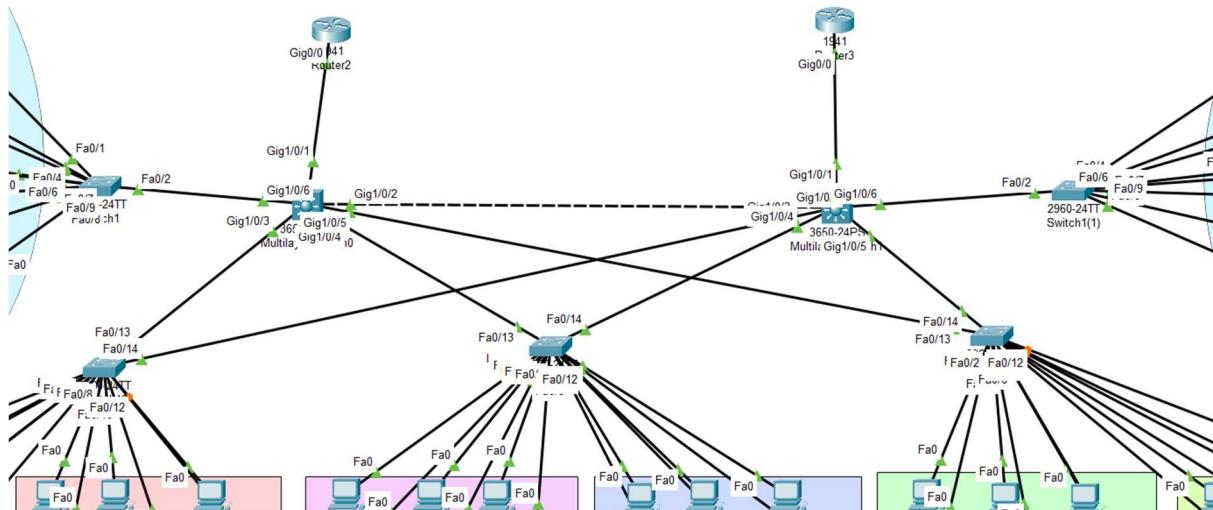
ב-EIGRP ניתן להגדיר מושקים כפאסיביים. מושק פאסיבי הינו מושק אשר לא נשלחות אליו ודרכו הודעות Hello. נגדיר את פקודה זו לכיוון רשתות LAN, זאת מכיוון שכיוון רשותת אלו לא קיימים ראותרים אשר יכולים לקיים יחס שכננות או לתחזק אותם. לכן אין צורך בשילוח הודעות HELLO לכיוון מושק זה היות והודעות אלו אשר נשלחות פעם ב-5 שניות עלולות להכחיד על הרשת.

הפקודה להגדרת מושק כפאסיבי:

Authentication

בפרוטוקול זה קיימת האפשרות להגדיר אימות על הנטב במטרה לאמת את המקור של חבילות המידע המתקבלות. זאת במטרה למנוע סייטואציה בה נתב אחר מתחזה לשכן של הנתב על מנת להוציא מידע מהרשות או להעביר דרכו מידע. על מנת למנוע מצב זה משתמשים בauthentication כדי למנוע מצב זה לקרות. האימות תומך בהצפנה מסוג MD5.

הגדרת EIGRP בסניף 2



רשתות

כתובת IP	marshak	מכשור
10.210.2.1	G1/0/1	MLS1
10.2.100.254	G1/0/5	
10.210.2.2	G0/0	R1
10.210.2.1	G1/0/1	MLS2
10.2.101.254	G1/0/5	
10.210.1.2	G0/0	R2

נדיר כתובות IP בין המתגים שכבה שלוש לנטים

```
interface GigabitEthernet1/0/1
no switchport
ip address 10.210.2.1 255.255.255.0
```

```
interface GigabitEthernet0/0
ip address 10.210.2.2 255.255.255.0
```

```
interface GigabitEthernet0/0
ip address 10.210.1.2 255.255.255.0
```

```
interface GigabitEthernet1/0/1
no switchport
ip address 10.210.1.1 255.255.255.0
```

גדר את הפרווטוקול וນפרסם את הרשותות השכנות

```
MLS1-D-TLV(config)#router eigrp 100
MLS1-D-TLV(config-router)#network 10.210.2.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.8.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.19.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.30.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.41.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.52.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.63.0 0.0.0.255
MLS1-D-TLV(config-router)#network 10.2.100.0 0.0.0.255
```

Show Commands

מראה את הרשותות שהנתב מכיר \ למד , דרך איזה ממשק עליו לצאת ואיזה כתובת IP עליו לעבור (next hop) על מנת להגיע אל רשות זאת.

EIGRP - [show ip eigrp interfaces](#) - מציגת מידע על הממשקים שבhos מופעל הפרווטוקול

[show ip eigrp neighbors](#) - מציגת רשימה של השכנים ומציג עליהם

[show ip eigrp topology](#) - מציגת מידע על הטופולוגיה, ועל הרשותות השונות

מציגת את הסוגים ובמאות ההודעות והתקבלו – [show ip eigrp traffic](#)

(R1-C-TLV) על show ip route

```
R1-C-TLV#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 21.2.22.1 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
D  10.2.8.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.19.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.30.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.41.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.52.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.63.0/24 [90/25625856] via 10.210.2.1, 00:02:42, GigabitEthernet0/0
D  10.2.100.0/24 [90/5376] via 10.210.2.1, 01:18:11, GigabitEthernet0/0
D  10.2.101.0/24 [90/25628416] via 10.210.2.1, 00:00:41, GigabitEthernet0/0
D  10.210.1.0/24 [90/25626112] via 10.210.2.1, 00:00:41, GigabitEthernet0/0
C  10.210.2.0/24 is directly connected, GigabitEthernet0/0
L  10.210.2.2/32 is directly connected, GigabitEthernet0/0
```

טיפוס פרוטוקול	טיפוס היעד	רשות	כתובת IP	המשק דרכו
AD / METRIC	אליה יש לעבור			תצא הפקטה

show ip eigrp interfaces

```
MLS1-D-TLV#show ip eigrp interfaces
IP-EIGRP interfaces for process 100
```

Interface	Peers	Xmit Queue	Mean RTT	Pacing Time	Multicast Flow Timer	Pending Routes
		Un/Reliable	SRTT	Un/Reliable		
Gig1/0/1	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Vlan	1	0/0	1236	0/10	0	0
Gig1/0/6	0	0/0	1236	0/10	0	0

ממשק

switch - 0

ממוצע הזמן

מספר הנטיבים

router - 1

שלקח לפאקטה

הממתיינים

להגעה ולהזoor

לשילחה

מחשכן

show ip eigrp neighbors

```
MLS1-D-TLV#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
```

H	Address	Interface	Hold Uptime	RTT	Q	Seq
			(sec)	(ms)	Cnt	Num
0	10.210.2.2	Gig1/0/1	13	353141:09:1240	1000	0 130
1	10.2.8.253	Vlan	11	353141:45:0940	1000	0 87
2	10.2.19.253	Vlan	14	353141:45:0940	1000	0 88
3	10.2.30.253	Vlan	11	353141:45:0940	1000	0 89
4	10.2.41.253	Vlan	14	353141:45:0940	1000	0 90
5	10.2.52.253	Vlan	11	353141:45:0940	1000	0 91
6	10.2.63.253	Vlan	13	353141:45:0940	1000	0 92

מספר host

כתובת אל השכן

הממשק של הרouter היוצא לשכן

Holdup time

זמן שילוח

חבילות

מספר חיבור

לפני שילוח

לחבילה EIGRP

המקנות

אחרון שהתקבל

ספרה לאחר

של איקבלת

שליחת

לשליחה

הודעת unicat

להגעה לשכן

מהשכן

Hello

ולחזר

מהשכן

כasher לא

התגובה

מהשכן

התגובה Hello

מהשכן

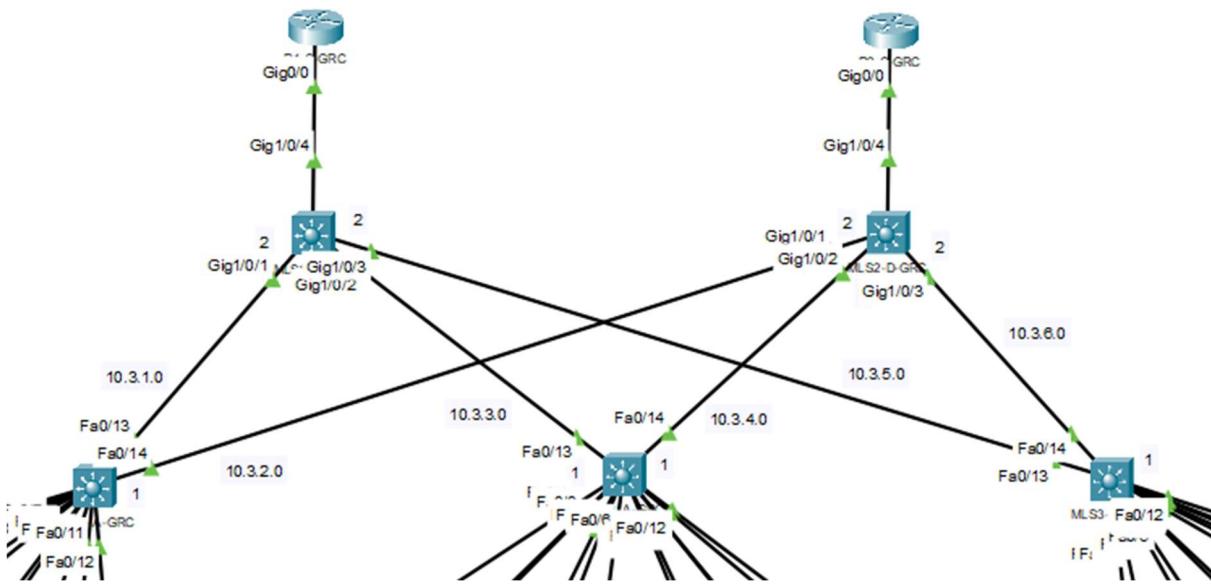
התקבלה תשובה

show ip eigrp topology

ממשק פאטיובי	כמה successors	של AD / FD	כל אחד	מהagtivities
MLS1-D-TLV#show ip eigrp topology				
IP-EIGRP Topology Table for AS 100/ID(192.168.60.252)				
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - Reply status				
P 10.2.8.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan8				
P 10.2.19.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan19				
P 10.2.30.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan30				
P 10.2.41.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan41				
P 10.2.52.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan52				
P 10.2.63.0/24,	1 successors,	FD is 25625600		
via Connected, Vlan63				
P 10.2.100.0/24,	1 successors,	FD is 5120		
via Connected, GigabitEthernet1/0/6				
P 10.2.101.0/24,	6 successors,	FD is 25628160		
via 10.2.19.253 (25628160/5120), Vlan19				
via 10.2.30.253 (25628160/5120), Vlan30				
via 10.2.52.253 (25628160/5120), Vlan52				
via 10.2.8.253 (25628160/5120), Vlan8				
via 10.2.63.253 (25628160/5120), Vlan63				
via 10.2.41.253 (25628160/5120), Vlan41				
P 10.210.1.0/24,	6 successors,	FD is 25625856		
via 10.2.19.253 (25625856/2816), Vlan19				
via 10.2.30.253 (25625856/2816), Vlan30				
via 10.2.52.253 (25625856/2816), Vlan52				
via 10.2.8.253 (25625856/2816), Vlan8				
via 10.2.63.253 (25625856/2816), Vlan63				
via 10.2.41.253 (25625856/2816), Vlan41				
P 10.210.2.0/24,	1 successors,	FD is 2816		
via Connected, GigabitEthernet1/0/1				

show ip eigrp traffic

MLS1-D-TLV#show ip eigrp traffic				
IP-EIGRP Traffic Statistics for process 100				
Hellos sent/received: 728/635				
Updates sent/received: 112/104				
Queries sent/received: 64/47				
Replies sent/received: 47/56				
Acks sent/received: 188/154				
Input queue high water mark 1, 0 drops				
SIA-Queries sent/received: 0/0				
SIA-Replies sent/received: 0/0				



היות וחלק מן ההגדירות בסניף זה זהות להגדירות בסניף הראשון, אצין ואסביר על ההגדירות אשר ייחודיות לסניף זה בעקבות הטופולוגיה השונה ואציג את פקודות ה `show` של ההגדירות אשר הוסברו. במצב בו יוגדר פרוטוקול בסניף זה אשר לא הוסבר עליו בסניף הראשון, ארכחיב עליו בסניף זה.

בסניף מס' 1 בו יהיו מתגים שכבה 2 בשתי השכבות.

בסניף מס' 2 בו יהיו מתגים שכבה 2 ב `access` ומתגים שכבה 3 בשכבה המIDDLE. ה `MLS` (Multilayer Switch) משלו נמצאים בסניף השלישי הינה שגם בשכבה `access` וגם בשכבה `middle` נמצאים סוויצרים שכבה 3.

מכיוון שנמצאים בשתי השכבות `MLS`, אנו נבצע את התקשרות בסניף זה באמצעות ניתוב, לעומת הסניפים האחרים שעבדו עם מיתוג.

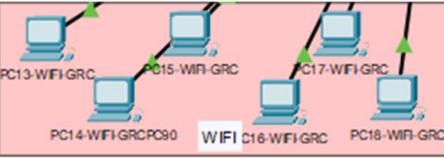
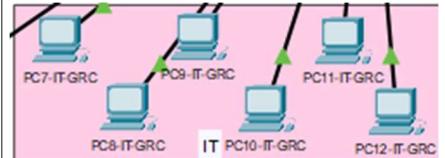
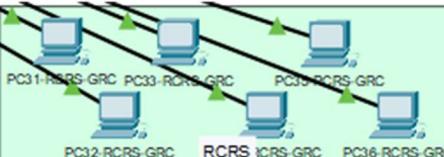
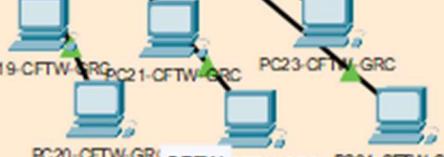
הרכיב השלישי:

שכבה `Access` : שלושה מתגים שכבה 3 – `3560-24PS Multilayer Switches` מסוג `3560-24PS`.

שכבה `Distribution` : שני מתגים שכבה 3 – `3650-24PS Multilayer Switches` מסוג `3650-24PS`.

שכבה `Core` : רואוטרים מסוג `1941`.

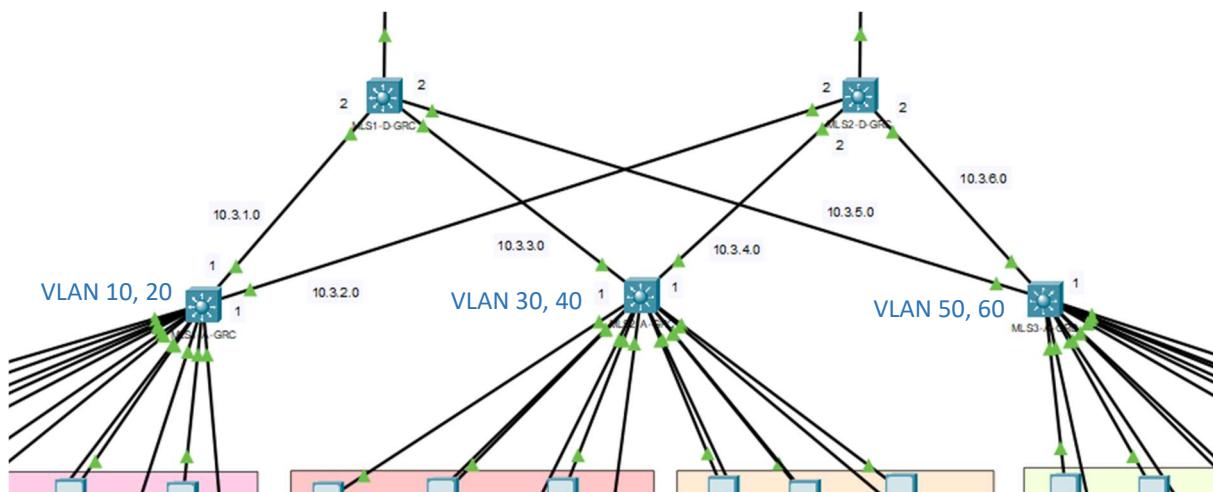
המחלקות בסניף:

WIFI VLAN 30	IT – VLAN 20	Management – VLAN 10
		
Research – VLAN 60	Finance – VLAN 50	Software Development – VLAN 40
		

סניף 3 VLAN

בסניף זה נגידר על כל מtag בשכבה ה-Access של שתי המחלקות אליו אותו המtag מחובר בלבד בהתאם לסדרתו. VLAN אלו נקראים וילאים מקומיים. בנוסף, נוצרת תשתית משק לכל VLAN כלומר נגידר לכל אחד SVI לפי אותן הגדרות שבייצעו בסניף הקודם.

הגדרת VLAN בסניף 3



נגידר על כל מtag בשכבה ה-Access את הוילאים המתואימים לו לפי המחלקות המוחברות אליו

```
MLS1-A-JRC(config)#vlan 10
MLS1-A-JRC(config-vlan)#name MNG
MLS1-A-JRC(config-vlan)#vlan 20
MLS1-A-JRC(config-vlan)#name IT
```

```
MLS3-A-JRC(config)#vlan 50
MLS3-A-JRC(config-vlan)#name FNC
MLS3-A-JRC(config-vlan)#vlan 60
MLS3-A-JRC(config-vlan)#name RCRS
```

```
MLS2-A-JRC(config)#vlan 30
MLS2-A-JRC(config-vlan)#name WIFI
MLS2-A-JRC(config-vlan)#vlan 40
MLS2-A-JRC(config-vlan)#name CFTW
```

נגידר על המטגים בשכבה ה-D את כלל ה-VLANS

```
MLS2-D-GRC(config)#vlan 10
MLS2-D-GRC(config-vlan)#name MNG
MLS2-D-GRC(config-vlan)#vlan 20
MLS2-D-GRC(config-vlan)#name IT
MLS2-D-GRC(config-vlan)#vlan 30
MLS2-D-GRC(config-vlan)#name WIFI
MLS2-D-GRC(config-vlan)#vlan 40
MLS2-D-GRC(config-vlan)#name CFTW
MLS2-D-GRC(config-vlan)#vlan 50
MLS2-D-GRC(config-vlan)#name FNC
MLS2-D-GRC(config-vlan)#vlan 60
MLS2-D-GRC(config-vlan)#name RCRS
```

```
MLS2-D-GRC(config)#vlan 10
MLS2-D-GRC(config-vlan)#name MNG
MLS2-D-GRC(config-vlan)#vlan 20
MLS2-D-GRC(config-vlan)#name IT
MLS2-D-GRC(config-vlan)#vlan 30
MLS2-D-GRC(config-vlan)#name WIFI
MLS2-D-GRC(config-vlan)#vlan 40
MLS2-D-GRC(config-vlan)#name CFTW
MLS2-D-GRC(config-vlan)#vlan 50
MLS2-D-GRC(config-vlan)#name FNC
MLS2-D-GRC(config-vlan)#vlan 60
MLS2-D-GRC(config-vlan)#name RCRS
```

נשייך את ה-svans למחשבים בהתאם לסרטוט שמצורף למעלה

```
MLS1-A-JRC(config)#int range fastEthernet 0/1-6
MLS1-A-JRC(config-if-range)#switchport mode access
MLS1-A-JRC(config-if-range)#switchport access vlan 10
MLS1-A-JRC(config-if-range)#exit
MLS1-A-JRC(config)#int range fastEthernet 0/7-12
MLS1-A-JRC(config-if-range)#switchport mode access
MLS1-A-JRC(config-if-range)#switchport access vlan 20
```

Distribution SVI גם על המתגים בשכבה ה-Access וגם על המתגים בשכבה ה-*Distribution*

```
MLS2-D-GRC(config)#interface vlan 10
MLS2-D-GRC(config-if)#ip address 192.168.10.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
MLS2-D-GRC(config)#interface vlan 20
MLS2-D-GRC(config-if)#ip address 192.168.20.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
MLS2-D-GRC(config)#interface vlan 30
MLS2-D-GRC(config-if)#ip address 192.168.30.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
MLS2-D-GRC(config)#interface vlan 40
MLS2-D-GRC(config-if)#ip address 192.168.40.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
MLS2-D-GRC(config)#interface vlan 50
MLS2-D-GRC(config-if)#ip address 192.168.50.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
MLS2-D-GRC(config)#interface vlan 60
MLS2-D-GRC(config-if)#ip address 192.168.60.254 255.255.255.0
MLS2-D-GRC(config-if)#no shutdown
MLS2-D-GRC(config-if)#exit
```

Show Commands

Show vlan							
VLAN Name		Status	Ports				
1 default		active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2				
10 MNG		active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6				
20 IT		active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12				
1002 fddi-default		active					
1003 token-ring-default		active					
1004 fddinet-default		active					
1005 trnet-default		active					
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	
1	enet	100001	1500	-	-	-	
10	enet	100010	1500	-	-	-	
20	enet	100020	1500	-	-	-	
1002	fddi	101002	1500	-	-	-	
1003	tr	101003	1500	-	-	-	
1004	fdnet	101004	1500	-	-	ieee	
1005	trnet	101005	1500	-	-	ibm	
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	
1	enet	100001	1500	-	-	-	
10	enet	100010	1500	-	-	-	
20	enet	100020	1500	-	-	-	
1002	fddi	101002	1500	-	-	-	
1003	tr	101003	1500	-	-	-	
1004	fdnet	101004	1500	-	-	ieee	
1005	trnet	101005	1500	-	-	ibm	
Remote SPAN VLANs	Primary	Secondary	Type	Ports			

show vlan brief

```
MLS2-A-JRC#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
30 WIFI	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6
40 CFTW	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

show vlan id [num_id]

```
MLS3-A-JRC#show vlan id 50
```

VLAN Name	Status	Ports
50 FNC	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6
<hr/>		
<hr/>		
VLAN Type	SAID	MTU Parent RingNo BridgeNo Stp BrdgMode Transl
Trans2		
50 enet	100050	1500 - - - - 0 0 1

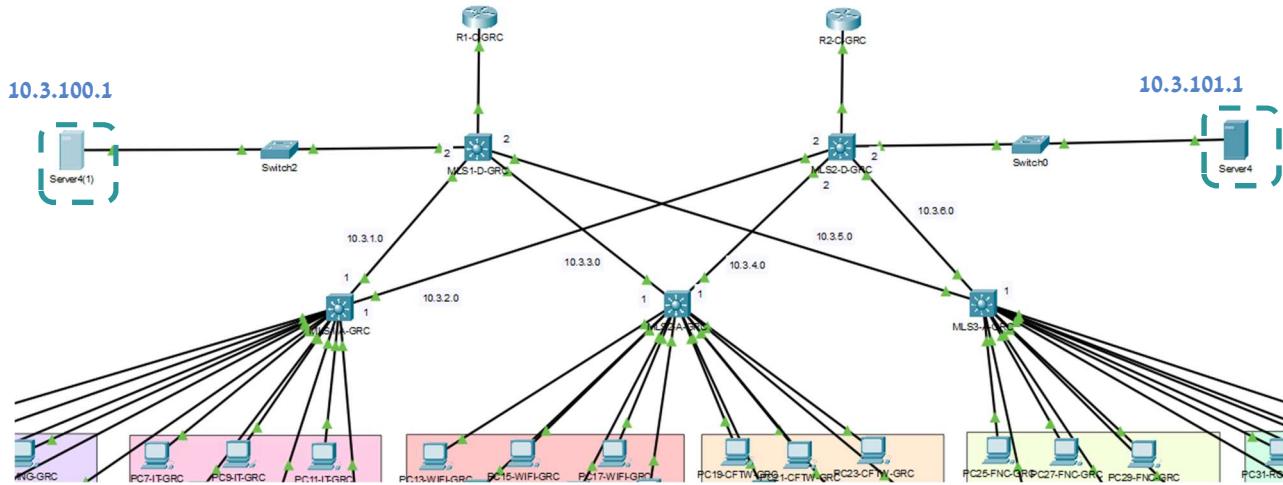
show vlan name [vlan_name]

```
MLS2-D-GRC#show vlan name FNC
```

VLAN Name	Status	Ports
50 FNC	active	
<hr/>		
<hr/>		
VLAN Type	SAID	MTU Parent RingNo BridgeNo Stp BrdgMode Transl
Trans2		
50 enet	100050	1500 - - - - 0 0 1

סניף שלישי DHCP

ההגדרות על השירותים בסניף השלישי זהות לאלו שבסניף השני תחת הכותרת "סניף שני". גם בסניף זה, נגידר את פרוטוקול DHCP על שרת lone, אצראן תמונות המראות את הגדרת השירותים



תזכורות: הגדרת DHCP על שרת:

- ניצור pool חדש
- ניתן לו את הכתובת ההתחלתית אותו ירצה לחלק
- נגידר לו כמה כתובות יחלק הנטב
- ונדיר את Default Gateway של הרשת

הגדרת POOL בשרת והדלקתו:

The screenshot shows two server configuration windows side-by-side, illustrating the setup of DHCP pools.

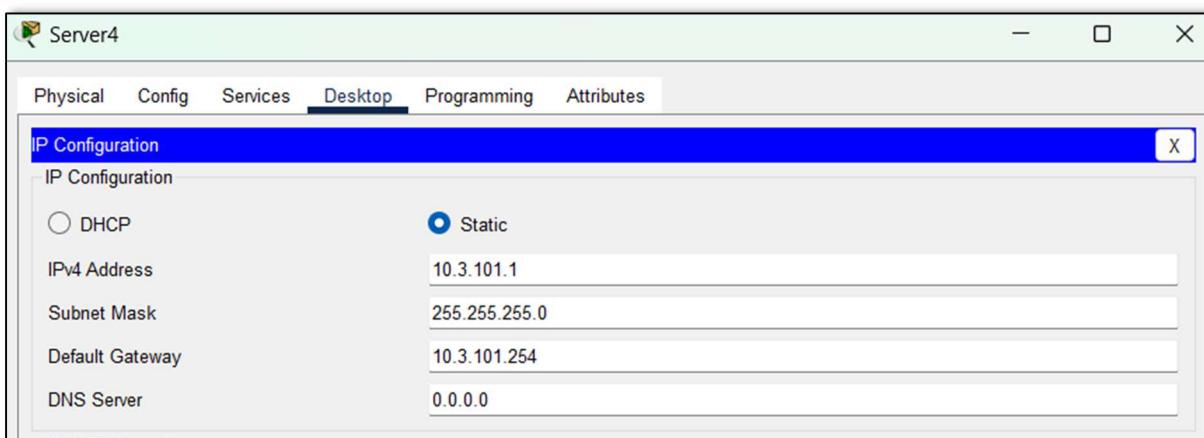
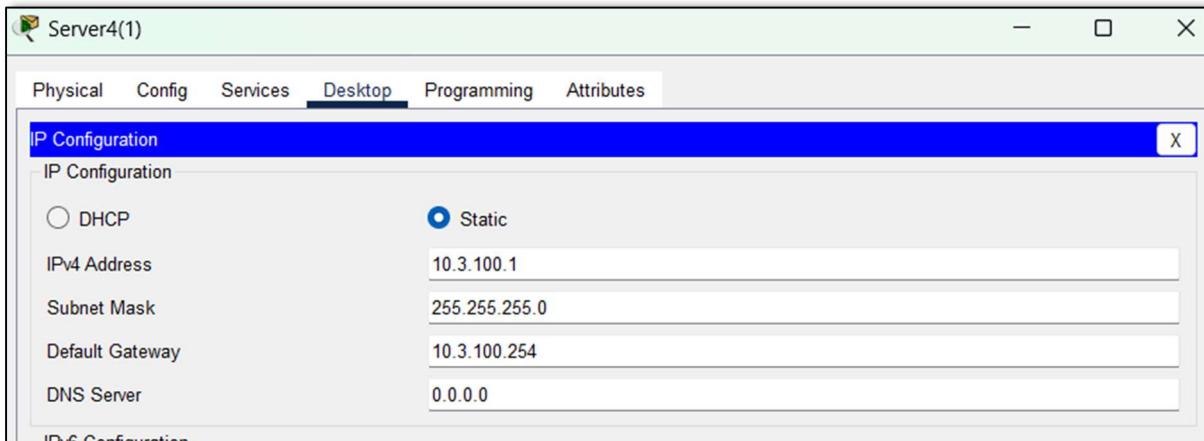
Left Window (Server4(1)):

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WL Addr
In30	192.168....	0.0.0.0	192.168....	255.255....	127	0.0.0.0	0.0.0.0
In20	192.168....	0.0.0.0	192.168....	255.255....	127	0.0.0.0	0.0.0.0
In10	192.168....	0.0.0.0	192.168....	255.255....	127	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

Right Window (Server4):

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WL Addr
In60	192.168....	0.0.0.0	192.168....	255.255....	126	0.0.0.0	0.0.0.0
In50	192.168....	0.0.0.0	192.168....	255.255....	126	0.0.0.0	0.0.0.0
In40	192.168....	0.0.0.0	192.168....	255.255....	126	0.0.0.0	0.0.0.0
In30	192.168....	0.0.0.0	192.168....	255.255....	126	0.0.0.0	0.0.0.0

הגדרת כתובות לשרתים



כעת נגידר על MLS בשכבה ה **o**nion Distribution כתובת IP לכיוון השירותים על מנת שהשרות והמתג יהיו באותו הרשת ויכולו לתקשר ביניהם. נגידר כתובת את ה g.d.
שהגדירו בשרתים

```
MLS2-D-GRC(config)#int gigl/0/5
MLS2-D-GRC(config-if)#no switchport
MLS2-D-GRC(config-if)#ip address 10.3.100.254 255.255.255.0
```

```
MLS2-D-GRC(config)#int gigabitEthernet 1/0/5
MLS2-D-GRC(config-if)#no switchport
MLS2-D-GRC(config-if)#ip address 10.3.101.254 255.255.255.0
```

- בסנייף השני הגדרנו את פקודת `ip helper` על שני המתגים שכבה 3 (MLS) בשכבה Broadcast Distribution. מכיוון שהם לאו שקיבלו את הودעת זה העברת המידע מתבצעת באמצעות ניתוב, המתגים שכבה 3 **בשכבה Access** הם אלו שיקבלו את הודעת `.ip helper`Broadcast ולכן הם אלו שנוצרך להגדיר עליהם את פקודת Broadcast

```

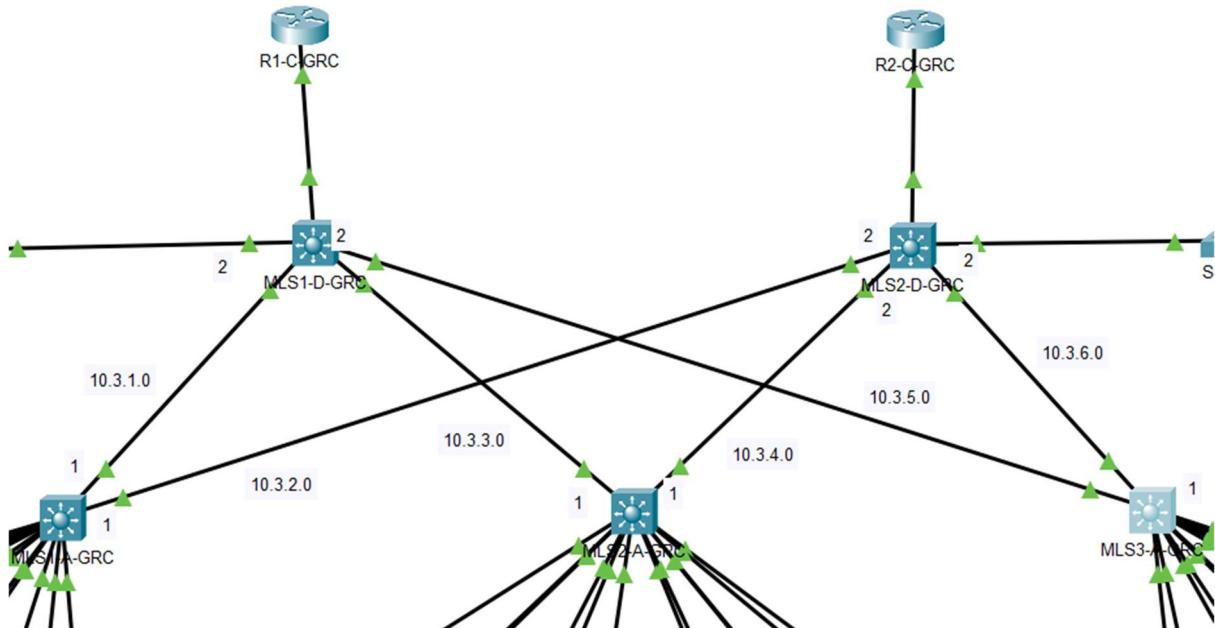
MLS1-A-JRC(config)#int vlan 10
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1
MLS1-A-JRC(config-if)#int vlan 20
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1
MLS1-A-JRC(config-if)#int vlan 30
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1
MLS1-A-JRC(config-if)#int vlan 40
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1
MLS1-A-JRC(config-if)#int vlan 50
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1
MLS1-A-JRC(config-if)#int vlan 60
MLS1-A-JRC(config-if)#ip helper-address 10.3.100.1
MLS1-A-JRC(config-if)#ip helper-address 10.3.101.1

```

הגדרת כתובות IP בין הממשקים

העברת המידע בסנייף זה הולכת להתבצע על ידי ניתוב. על מנת שנוכל לבצע ניתוב בין המכשירים השונים ברשות עליינו להגדיר בין כל חיבור של שני ממשקים של מתגים MLS כתובות IP ו-S.M.

הרשאות בסנייף השלישי:



- כל הרשאות עם פרפיקס 24 (255.255.255.0)

הגדרת הרשאות בסנייף:

נכנס לממשקים ונגידר כתובות IP לפי הסרטוט המוצג להלן.

דוגמא להגדרה בין MLS1-A-GRC ל-MLS1-D-GRC

```
MLS1-A-JRC(config)#int fastEthernet 0/13
MLS1-A-JRC(config-if)#ip address 10.3.1.1 255.255.255.0
```

```
MLS2-D-GRC(config)#int gigabitEthernet 1/0/1
MLS2-D-GRC(config-if)#ip address 10.3.1.2 255.255.255.0
```

show commands

show run

```
interface GigabitEthernet1/0/1
no switchport
ip address 10.3.2.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/2
no switchport
ip address 10.3.4.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet1/0/3
no switchport
ip address 10.3.6.2 255.255.255.0
duplex auto
speed auto
```

show ip interfaces

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1/0/1	10.3.1.2	YES	manual	up	up
GigabitEthernet1/0/2	10.3.3.2	YES	manual	up	up
GigabitEthernet1/0/3	10.3.5.2	YES	manual	up	up
GigabitEthernet1/0/4	unassigned	YES	unset	up	up
GigabitEthernet1/0/5	10.2.201.254	YES	manual	up	up
GigabitEthernet1/0/6	unassigned	YES	unset	down	down

3 סניף Port-Security

ההגדרות בסניף זה זהות להגדרות בסניף הראשון עליהם פירטתי לעיל. אציג בסניף זה את טבלת ההגדרות ואת פקודות show

	מחלקה	מצב
מחלקות אלו חשובות ומקבלות ומכילות מידע רגיש על עובדי חברה, משתמשים והנהלה. לכן נרצה שהmask ידליך וככבה עם התערבות מנהל הרשות בלבד	Management	Shutdown
	IT	
נרצה שתעבורת לא תעבור + קובץ לוג והודעת 33 IT - SNMP אין צורך בכינוי משך. לא נרצה שייהו לנו בעיות בהעברת ציוד ומידע או בעיות תקשורת בסניף.	WIFI	Restrict
	Finance	
אין צורך בכינוי משך, מספיק שהתעבורת תחסן.	Software Development	Protect
	Research	

show port-security

Secure Port	MaxSecureAddr	CurrentAddr	Security Violation	Security Action
	(Count)	(Count)	(Count)	
Fa0/1	1	0	0	Shutdown
Fa0/2	1	0	0	Shutdown
Fa0/3	1	0	0	Shutdown
Fa0/4	1	0	0	Shutdown
Fa0/5	1	0	0	Shutdown
Fa0/6	1	0	0	Shutdown
Fa0/7	1	0	0	Shutdown
Fa0/8	1	0	0	Shutdown
Fa0/9	1	0	0	Shutdown
Fa0/10	1	0	0	Shutdown
Fa0/11	1	0	0	Shutdown
Fa0/12	1	0	0	Shutdown

מספר ממישק כמות MAC מקסימלית כמה MAC למד כמה הפרעות שהיו מהו מצב mode

show port-security					
Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security	Action
	(Count)	(Count)	(Count)		
Fa0/1	1	0	0	Restrict	
Fa0/2	1	0	0	Restrict	
Fa0/3	1	0	0	Restrict	
Fa0/4	1	0	0	Restrict	
Fa0/5	1	0	0	Restrict	
Fa0/6	1	0	0	Restrict	
Fa0/7	1	0	0	Restrict	
Fa0/8	1	0	0	Restrict	
Fa0/9	1	0	0	Restrict	
Fa0/10	1	0	0	Restrict	
Fa0/11	1	0	0	Restrict	
Fa0/12	1	0	0	Restrict	

מספר משקל כמות MAC מקסימלית כמה MAC למד כמה הפרעות היו מהו mode שהוגדר

show port-security

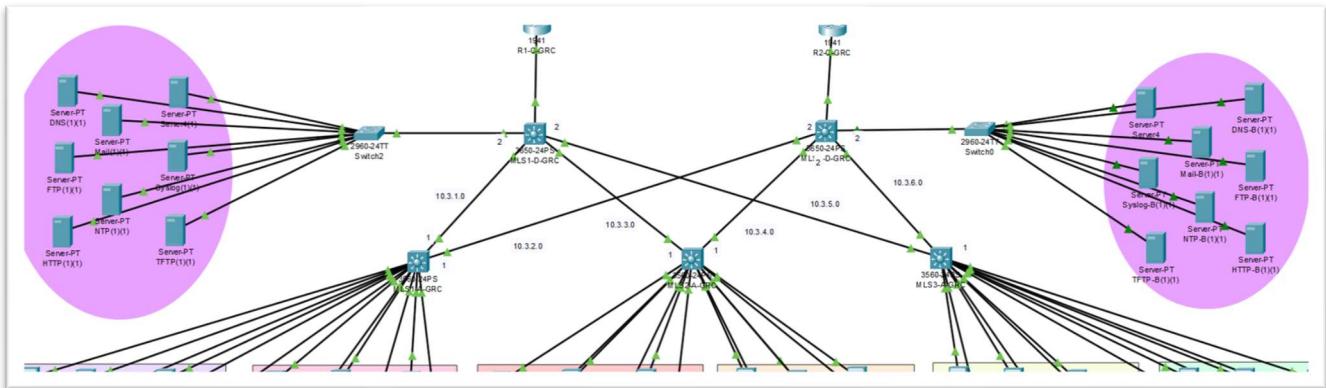
Switch(config)#do show port-secu					
Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security	Action
	(Count)	(Count)	(Count)		
Fa0/1	1	0	0	Protect	
Fa0/2	1	0	0	Protect	
Fa0/3	1	0	0	Protect	
Fa0/4	1	0	0	Protect	
Fa0/5	1	0	0	Protect	
Fa0/6	1	0	0	Protect	
Fa0/7	1	0	0	Protect	
Fa0/8	1	0	0	Protect	
Fa0/9	1	0	0	Protect	
Fa0/10	1	0	0	Protect	
Fa0/11	1	0	0	Protect	
Fa0/12	1	0	0	Protect	

מספר משקל כמות MAC מקסימלית כמה MAC למד כמה הפרעות היו מהו mode שהוגדר

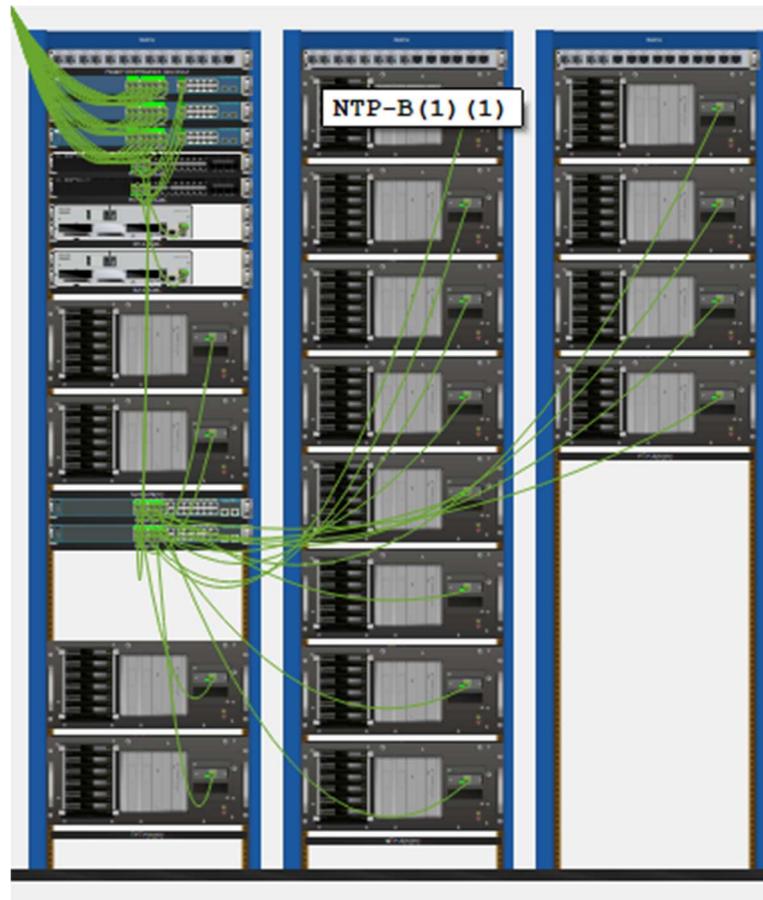
show port-security interface

Switch#show port-security interface fastEthernet 0/5	
Port Security	: Enabled ← אפשרות
Port Status	: Secure-up
Violation Mode	: Shutdown ← סוג mode שהגדנו
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1 ← מקסימום בתוכנות MAC שהגדנו
Total MAC Addresses	: 0 ← כמה הכתובות שלמדו
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0000.0000.0000:0
Security Violation Count	: 0

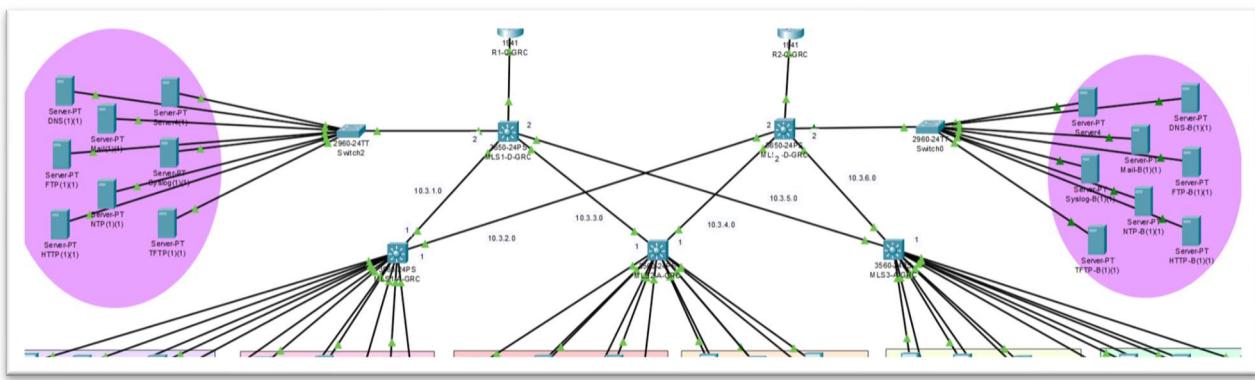
שרטים בסניף השלישי



על מנת לחבר את השירותים, נחבר למשתגים בשכבה החומרה שני מותגים מסווג EMPTY.
ולמשתגים אלו נחבר את השירותים בטופולוגיה.

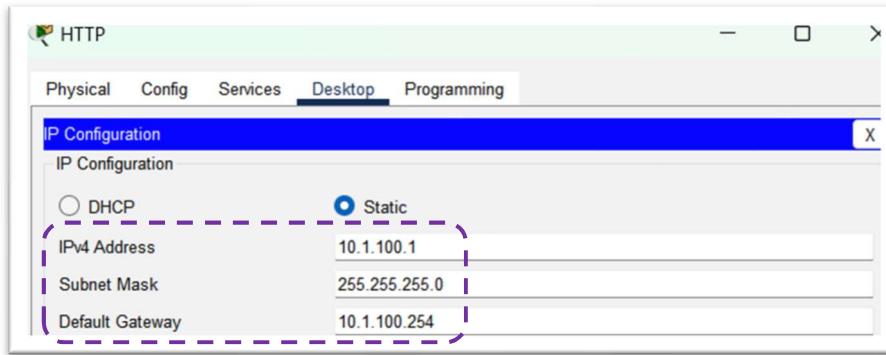


3 סניף HTTP

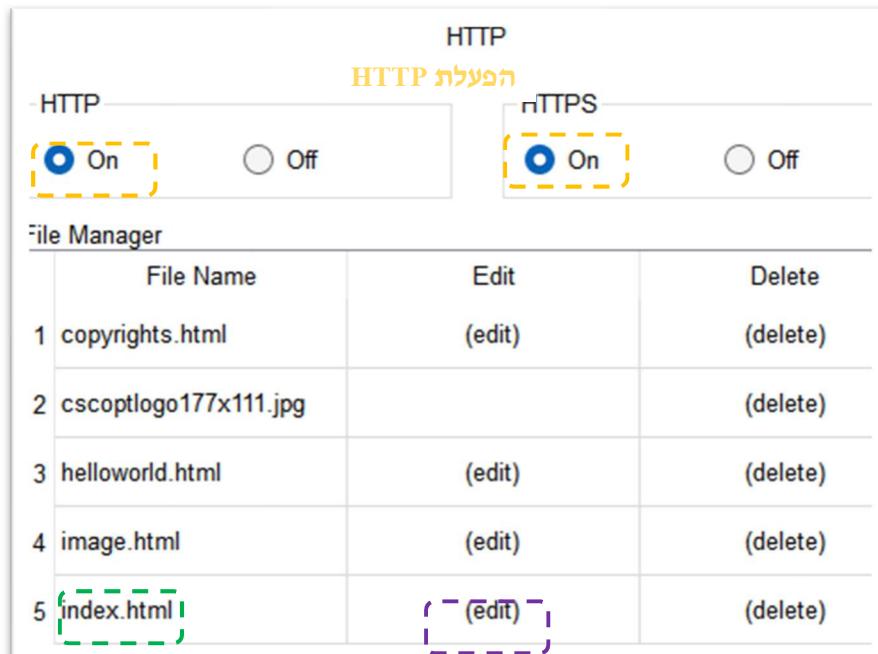


הגדרה בשרת הראשי

הגדרת כתובות IP לשירותים

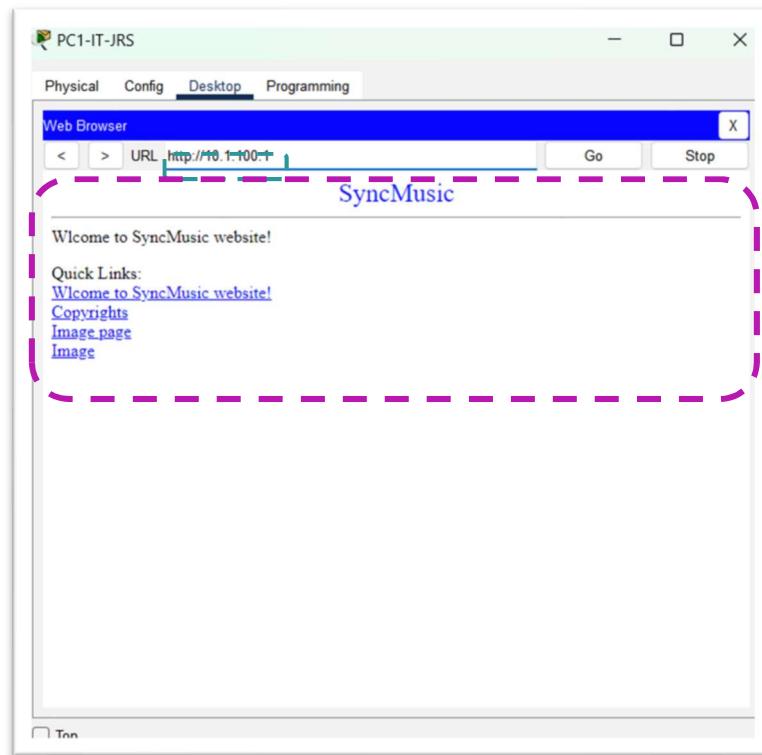


הגדרת שירותים HTTP:



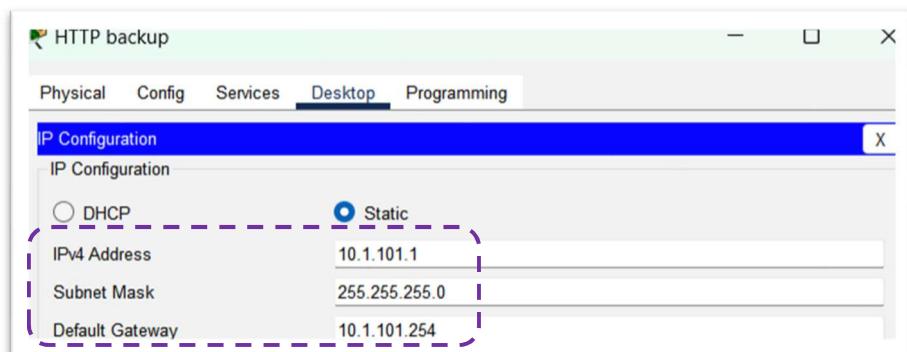
הקובץ של האתר

בדיקה שנייתן לגלווש אל האתר ממחשב



הגדרת Backup בשרת ה-HTTP

הגדרת כתובות IP לשרתים



הגדרת שירות HTTP

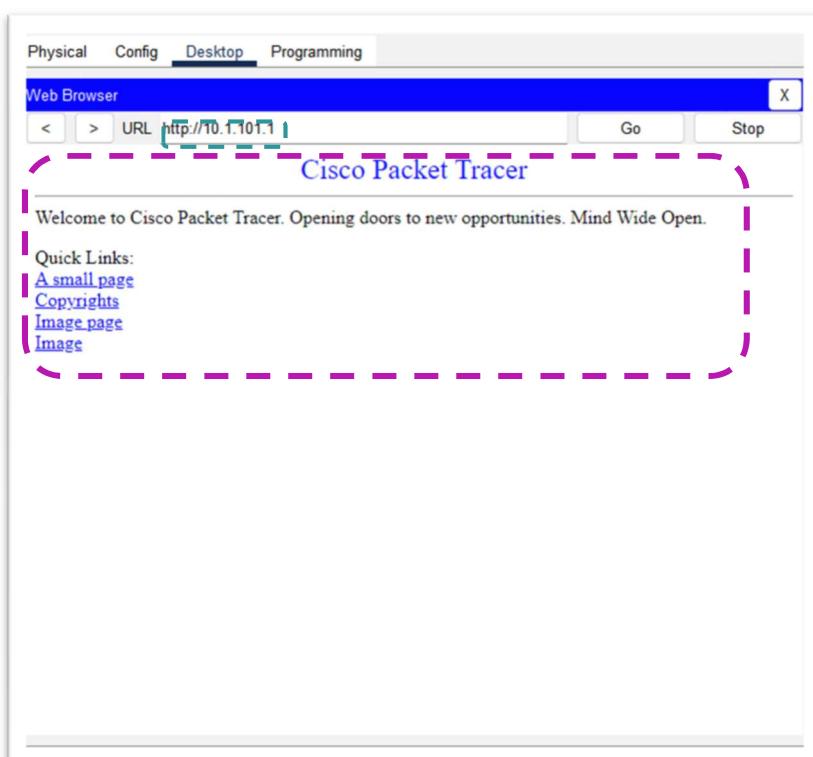
The screenshot shows a configuration interface with the following sections:

- HTTP**: A section with two radio buttons: "On" (selected) and "Off".
- HTTPS**: A section with two radio buttons: "On" (selected) and "Off".
- File Manager**: A table listing files:

File Name	Edit	Delete
1 copyrights.html	(edit)	(delete)
2 cscoptlogo177x111.jpg		(delete)
3 helloworld.html	(edit)	(delete)
4 image.html	(edit)	(delete)
5 index.html	(edit)	(delete)

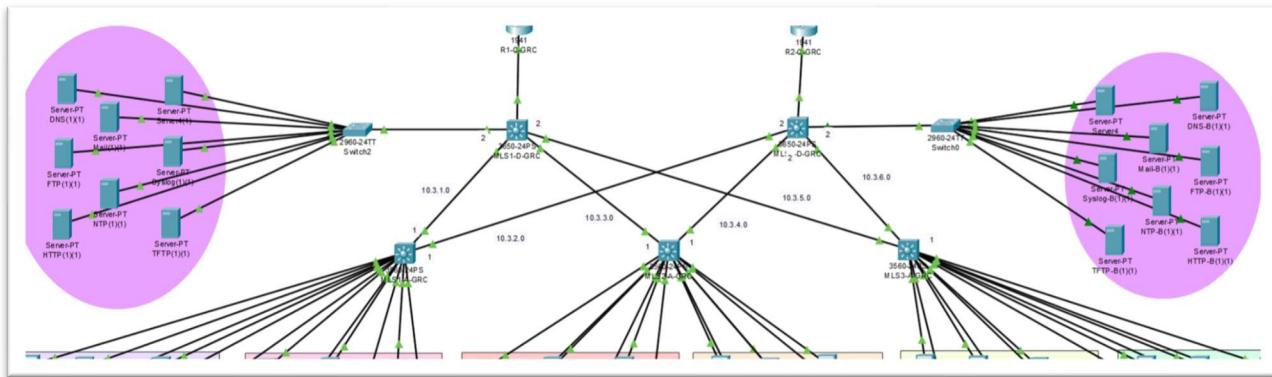
הקובץ של האתר

בדיקות שנייתן לגלוש מהאתר אל המחשב

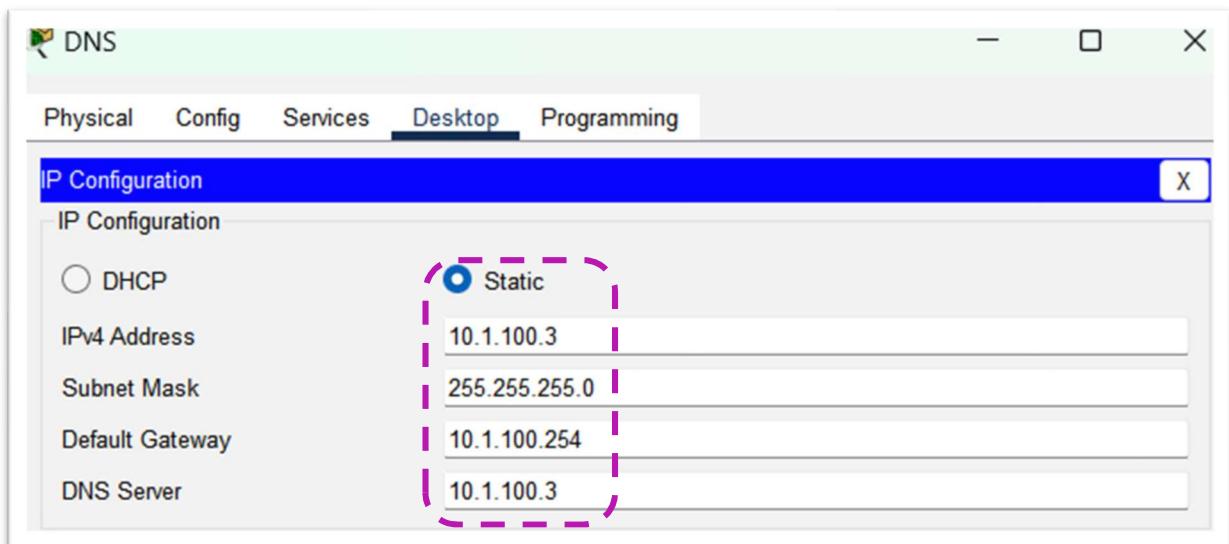


DNS Server

הגדרת שרת DNS ראשי



נתינה כתובות לשרת הראשי

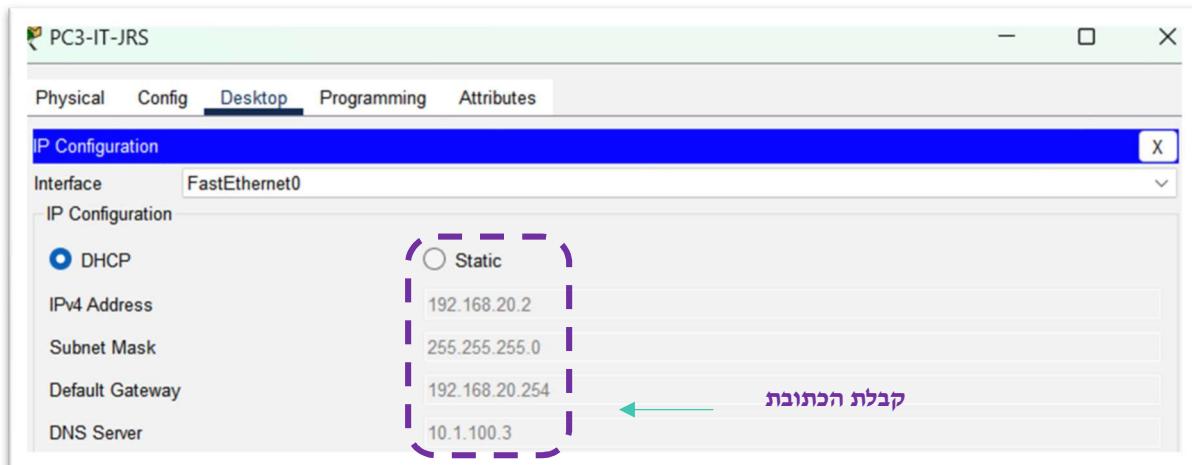


הוספה כתובות dns server בחלוקת כתובות על ידי dhcp

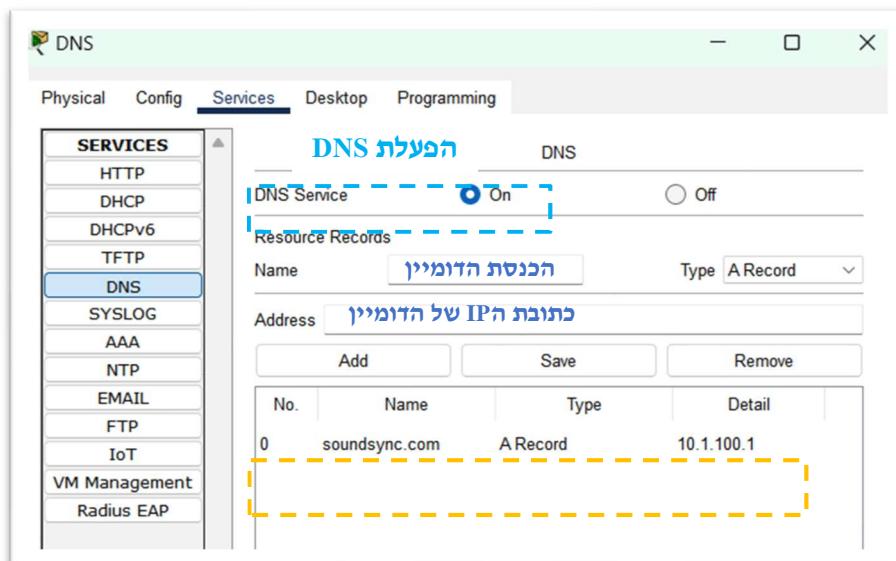
```
R1-C-JRS (config) #ip dhcp pool lan10 ← כניסה לpool
R1-C-JRS (dhcp-config) #dns-server 10.1.100.3 ← שיוך כתובות
R1-C-JRS (dhcp-config) #exit
R1-C-JRS (config) #ip dhcp pool lan20
R1-C-JRS (dhcp-config) #dns-server 10.1.100.3
R1-C-JRS (dhcp-config) #exit
R1-C-JRS (config) #ip dhcp pool lan30
R1-C-JRS (dhcp-config) #dns-server 10.1.100.3
R1-C-JRS (dhcp-config) #exit
```

שייך כתובות
server dns

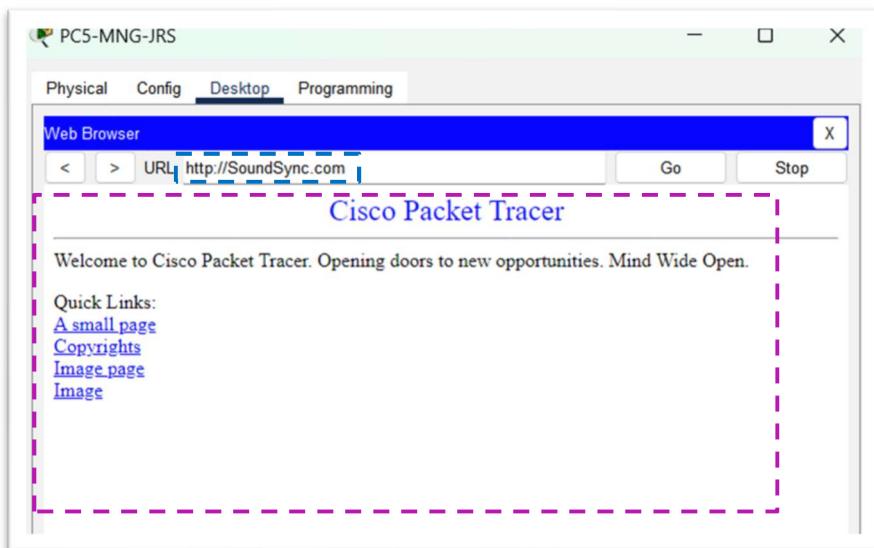
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנתב קיבלו את כתובת DNS של השרת הראשי



הגדרת שרת DNS

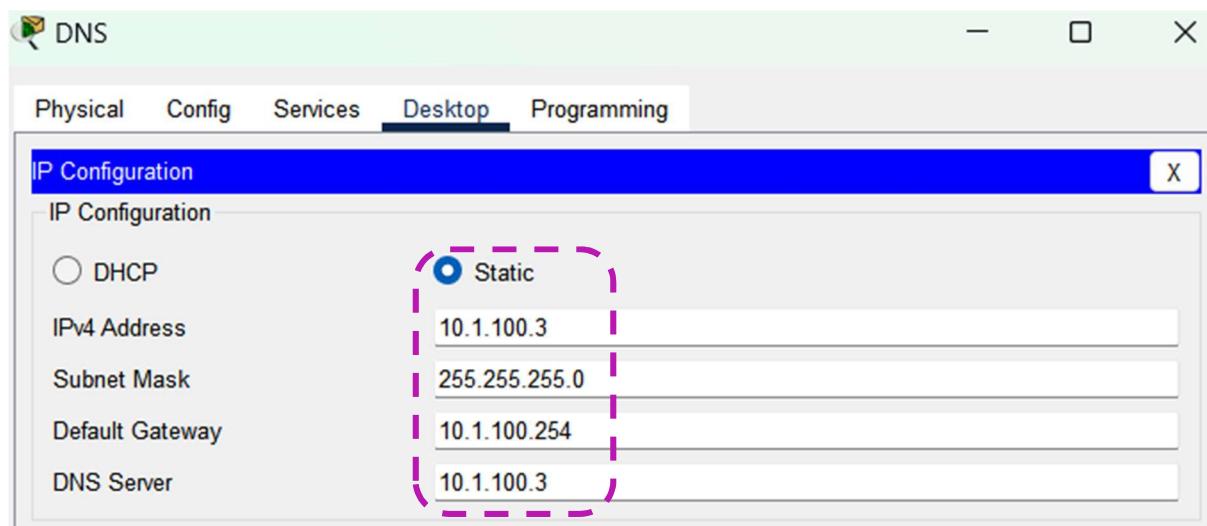


בדיקה על ידי גלישה לאתר לפי כתובת הדומיין



הגדרת שרת DNS גיבוי

נתינה כתובת לשרת גיבוי



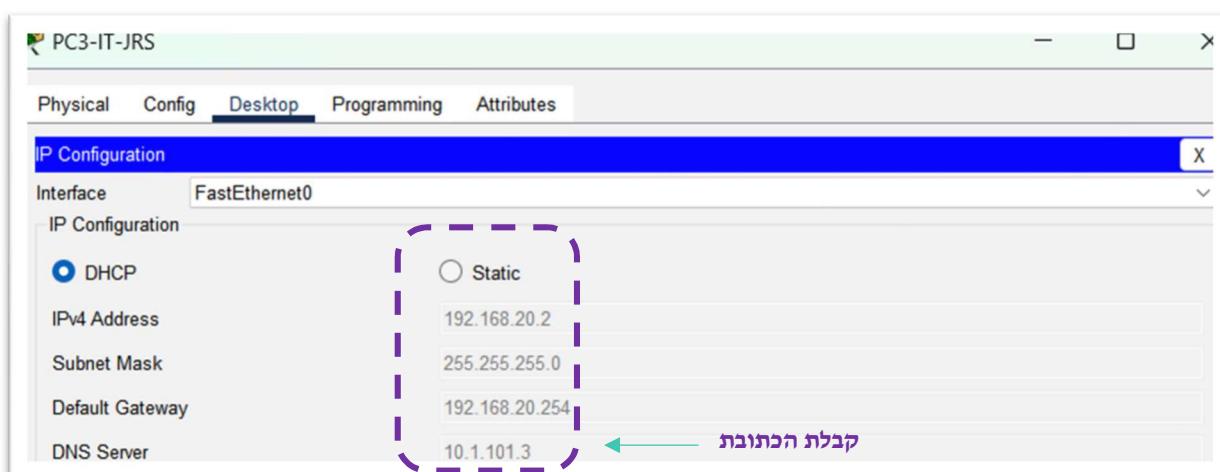
הוספה כתובת dns server בחלוקת כתובות על ידי dhcp

```

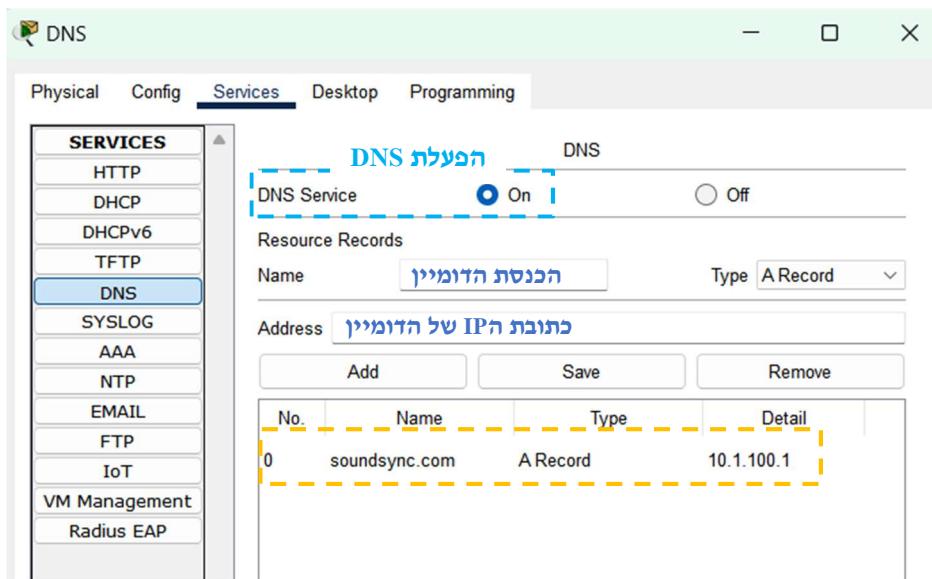
R1-C-JRS (config) #ip dhcp pool lan40
R1-C-JRS (dhcp-config) #dns-server 10.1.101.3 ← כנישת dns
R1-C-JRS (dhcp-config) #exit
R1-C-JRS (config) #ip dhcp pool lan50
R1-C-JRS (dhcp-config) #dns-server 10.1.101.3 ← שיקן כתובת
R1-C-JRS (dhcp-config) #exit
R1-C-JRS (config) #ip dhcp pool lan60
R1-C-JRS (dhcp-config) #dns-server 10.1.101.3 ← dns server
R1-C-JRS (dhcp-config) #exit

```

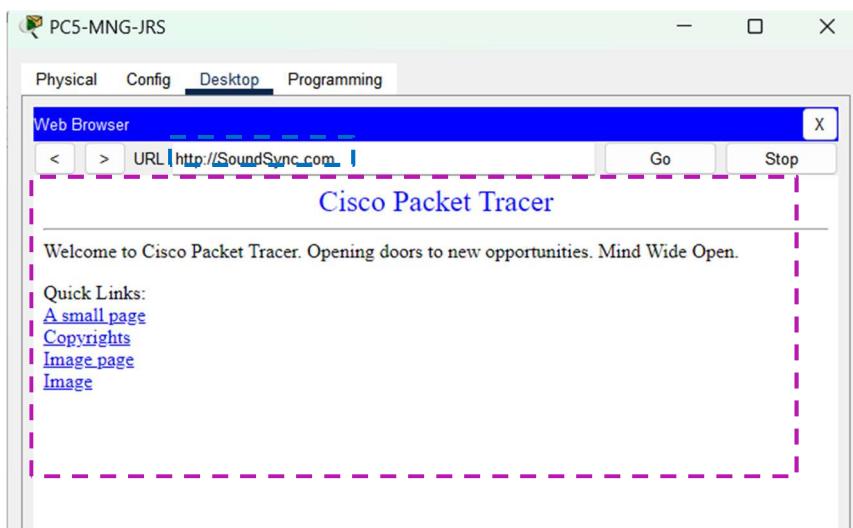
בדיקה שהמחשבים שקיבלו את הכתובות שליהם מהנתב קיבלו את כתובת dns של השירות גיבוי
במקרה והשרת dns הראשי נפל



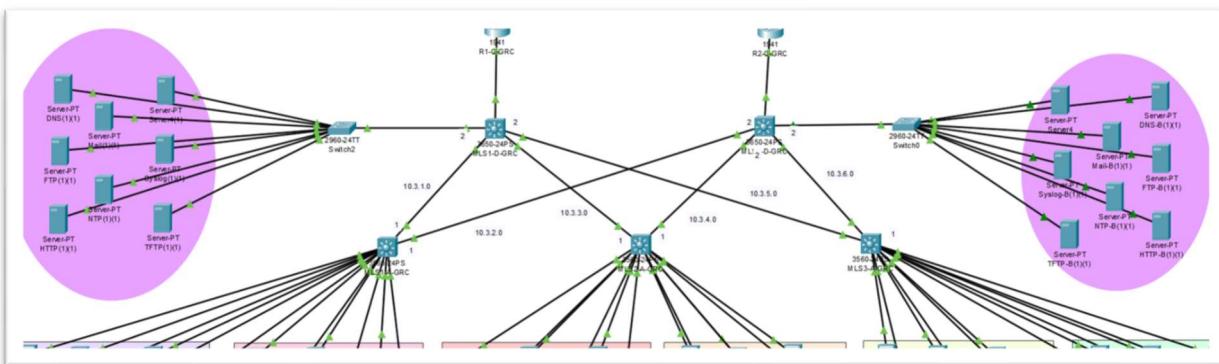
הגדרת שירות DNS



בדיקה על ידי גישה לאתר לפי כתובות הדומיין

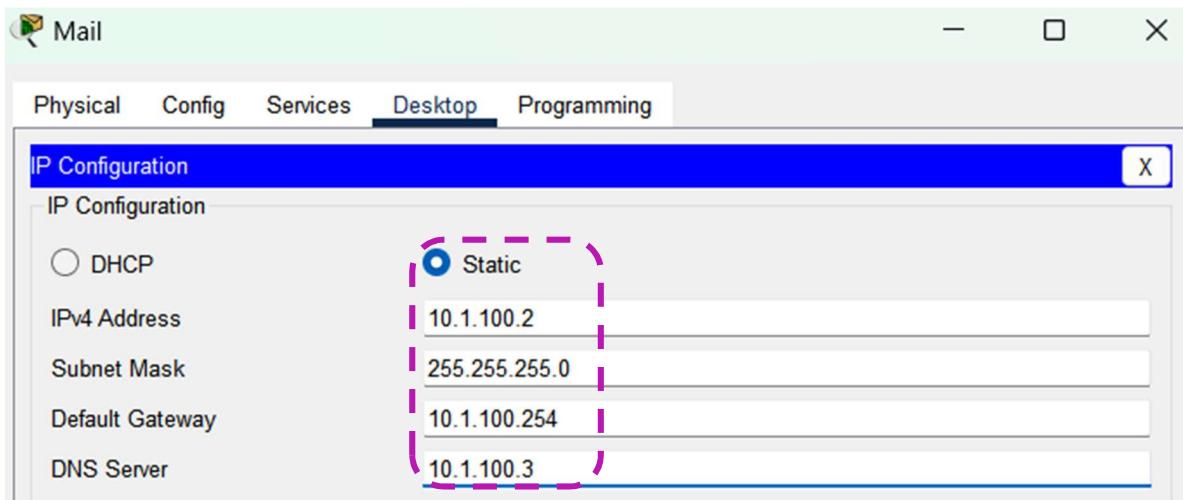


Mail

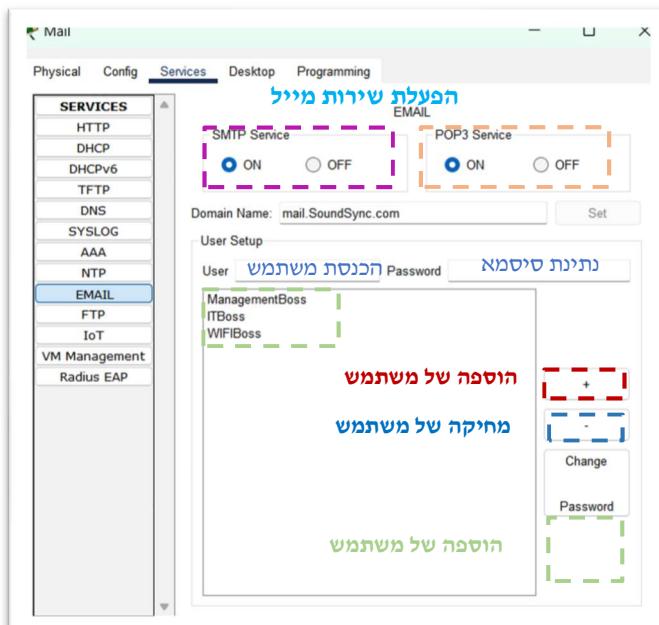


הגדרת שירות מייל ראשי

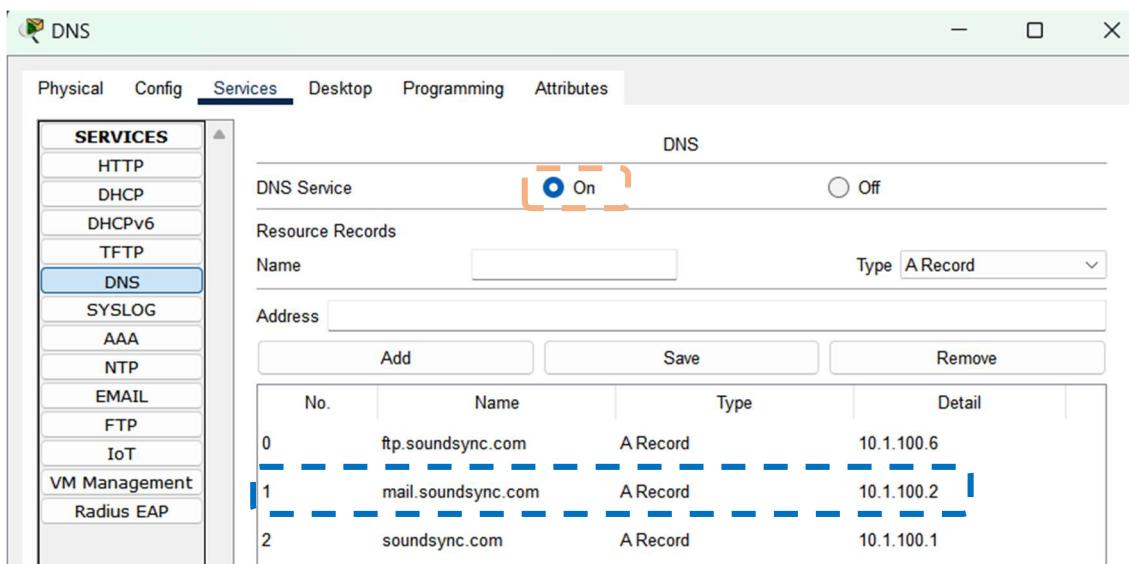
נתינה כתובות לשרת



הגדרת שירות-mail

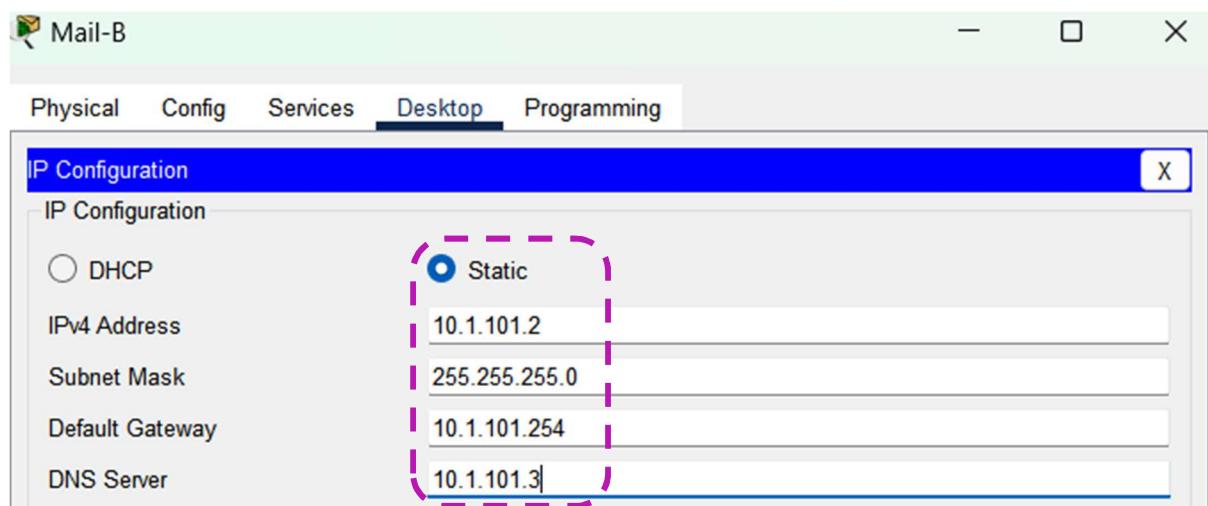


הוספת mail לשרת DNS

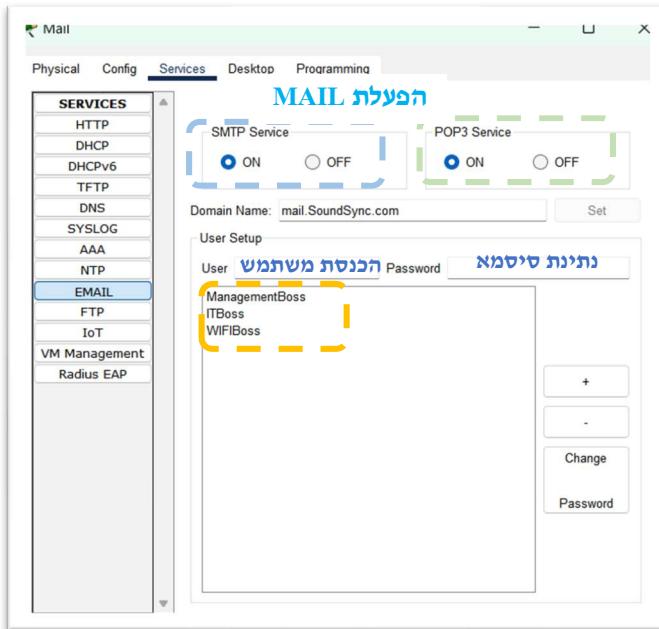


הגדלת שרת מייל Backup

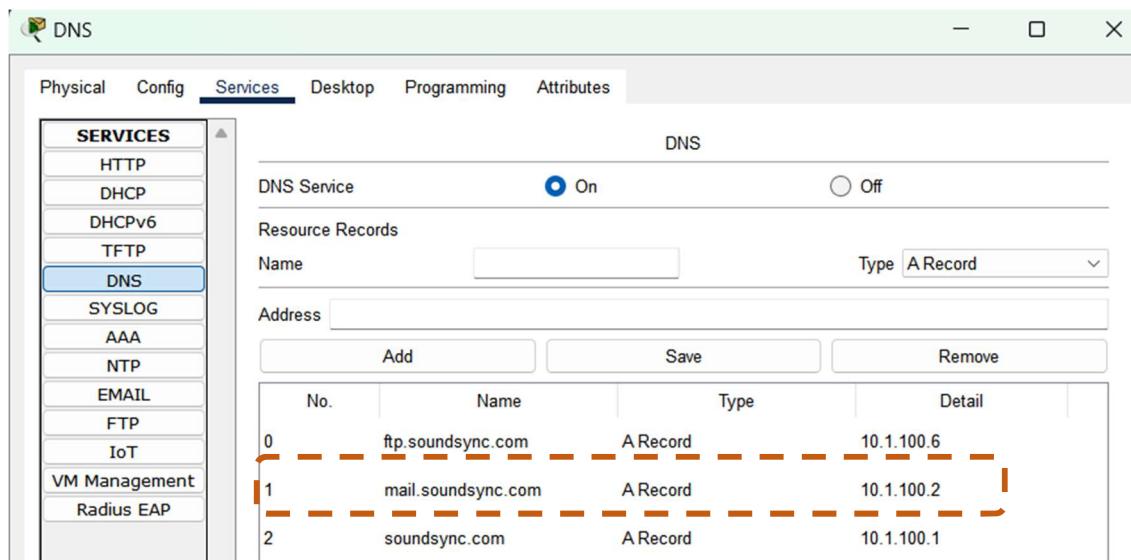
נתינת כתובות לשרת



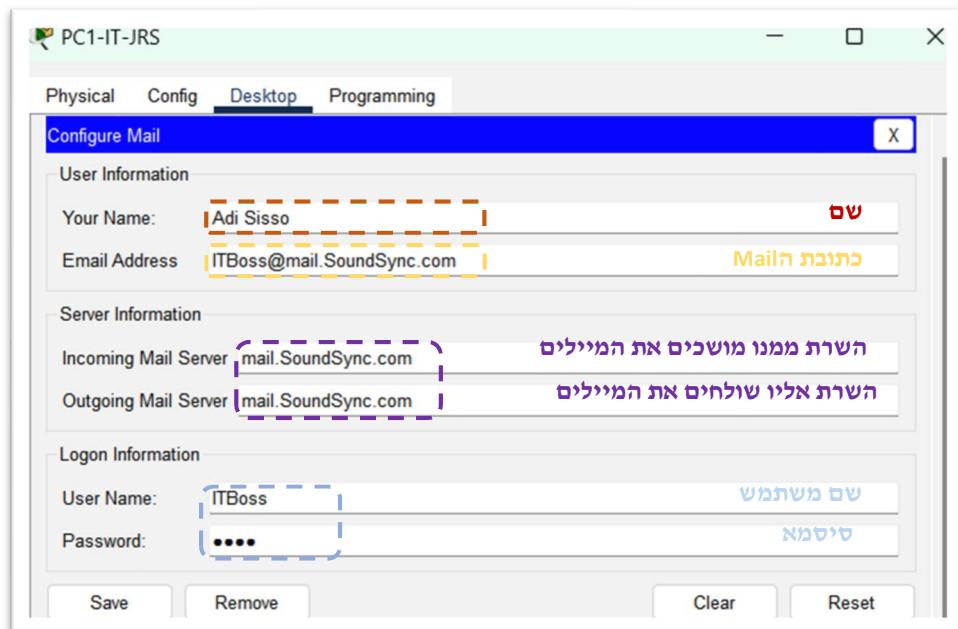
הגדרת שירות mail



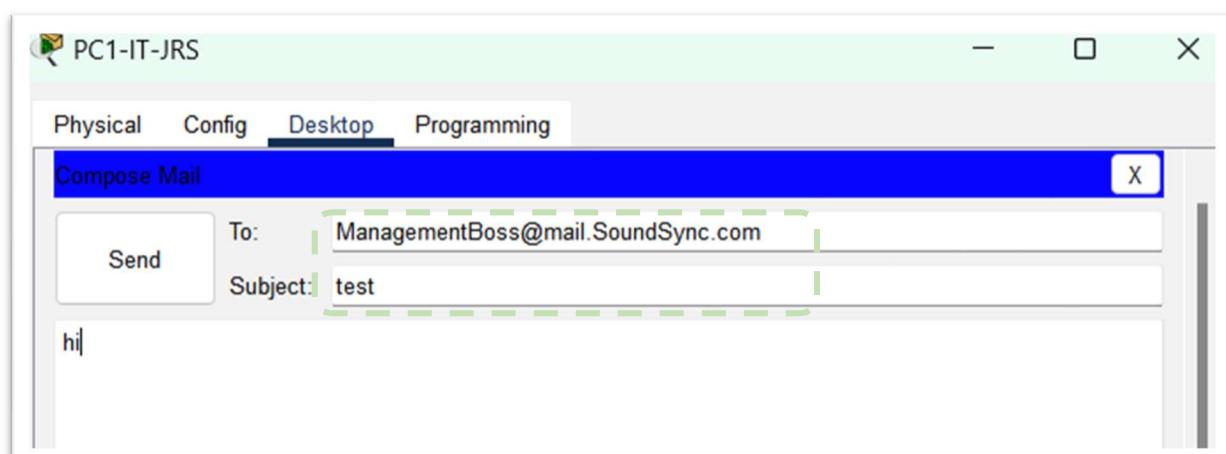
הוספה של DNS לשירות mail



בדיקה – התחברות משתמש דרך מחשב



בדיקה – שליחת מייל

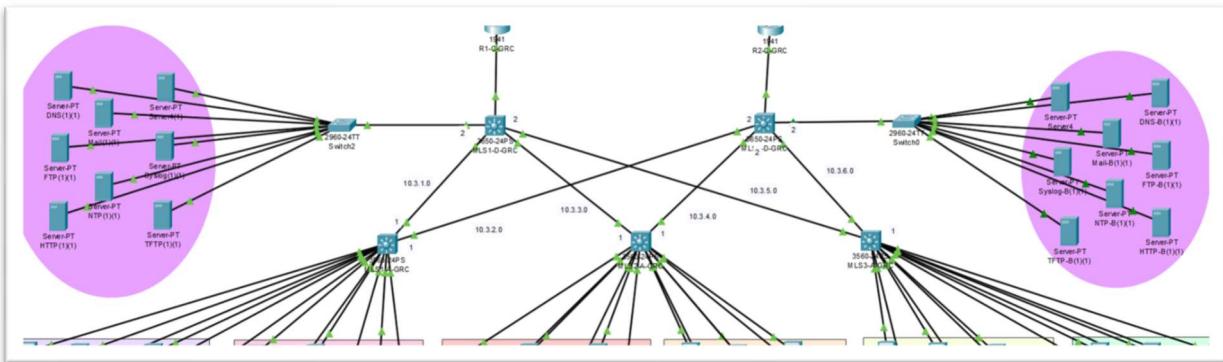


בדיקה – קבלת מייל

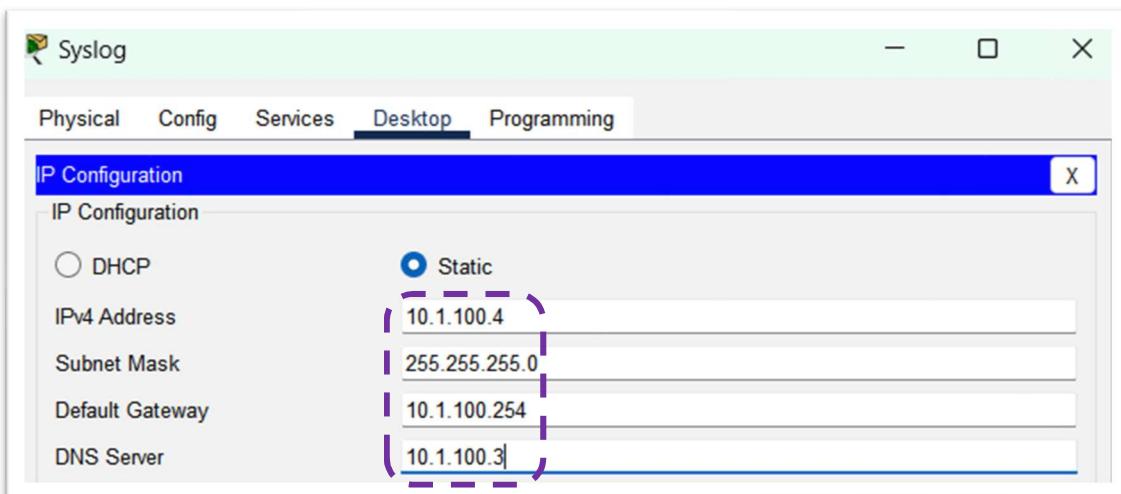
	From	Subject	Received
1	ITBoss@mail.Sound...	test	Sun Dec 3 2023 00:35:58

שרת Syslog

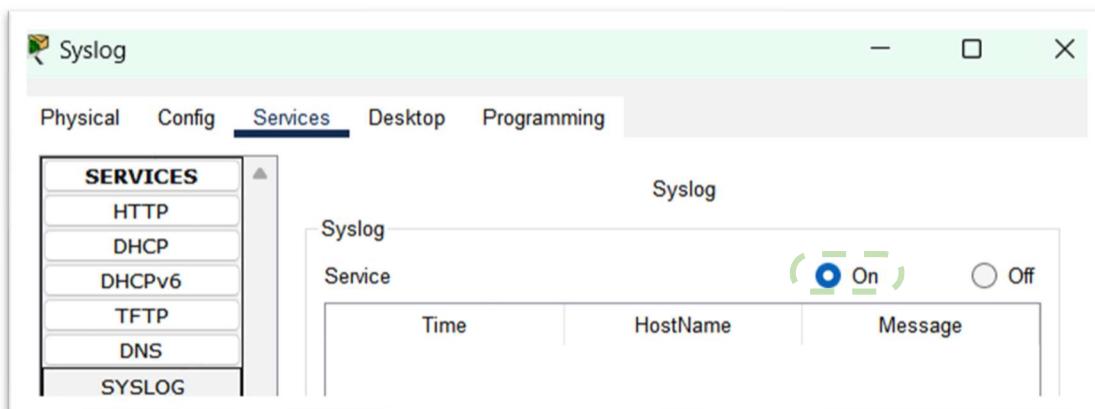
הגדרת שרת Syslog ראשי



הגדרת כתובת IP לשרת



הפעלת syslog



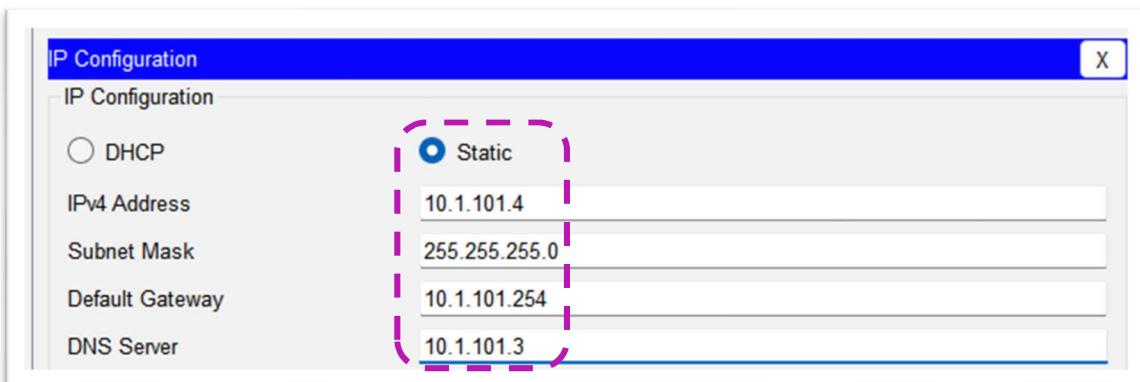
הפעלת שירות Syslog על המתגים והנתבים בראשת

```
R1-C-JRS (config) #logging host 10.1.100.4
R1-C-JRS (config) #logging host 10.1.101.4
```

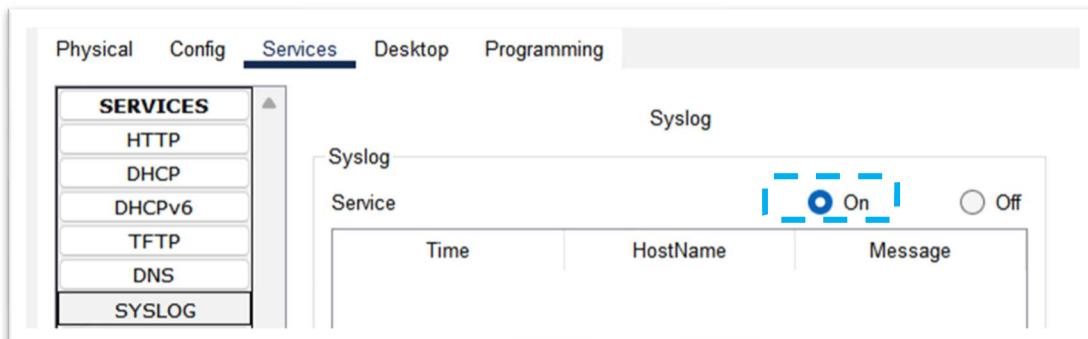
הגדרה מי שרת syslog

הגדרת שרת Syslog

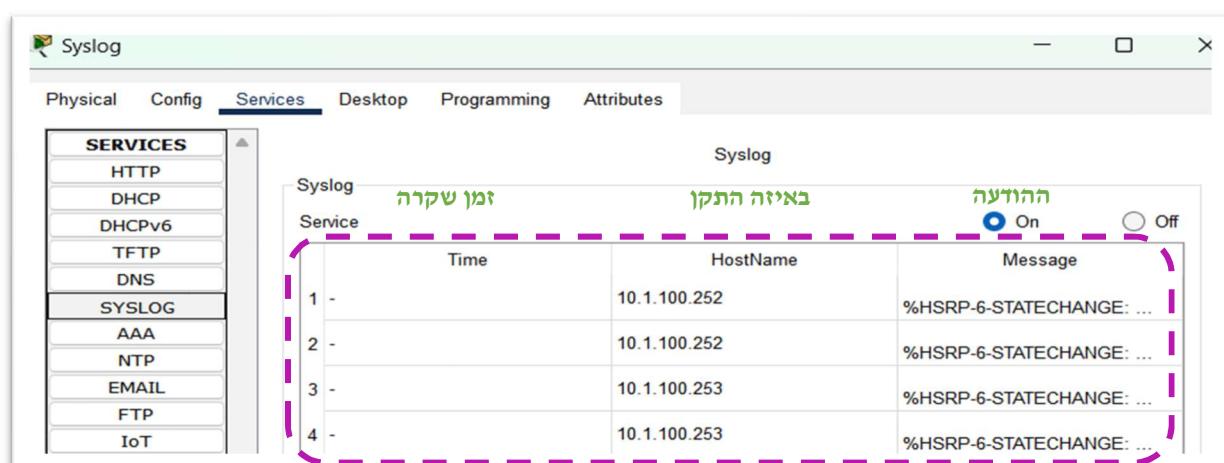
הגדרת כתובת IP לשרת



הפעלת שירות Syslog על המתגים והנתבים בראשת

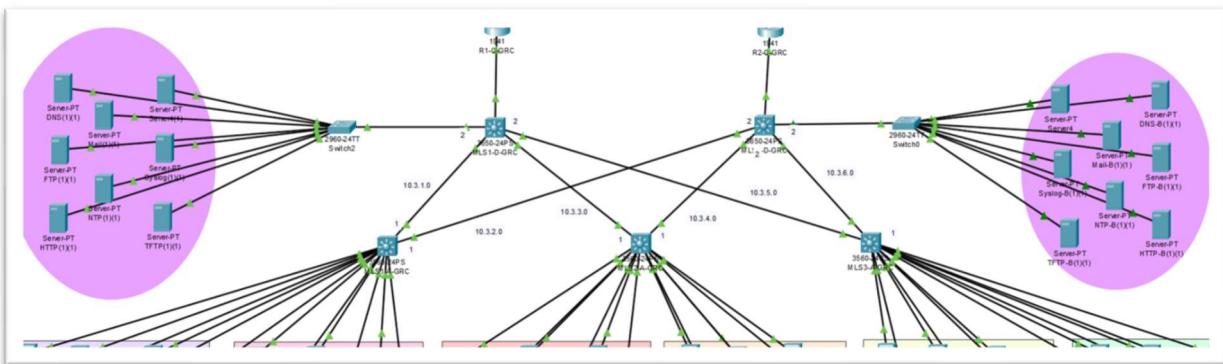


בדיקות שליחת רשומות Logs

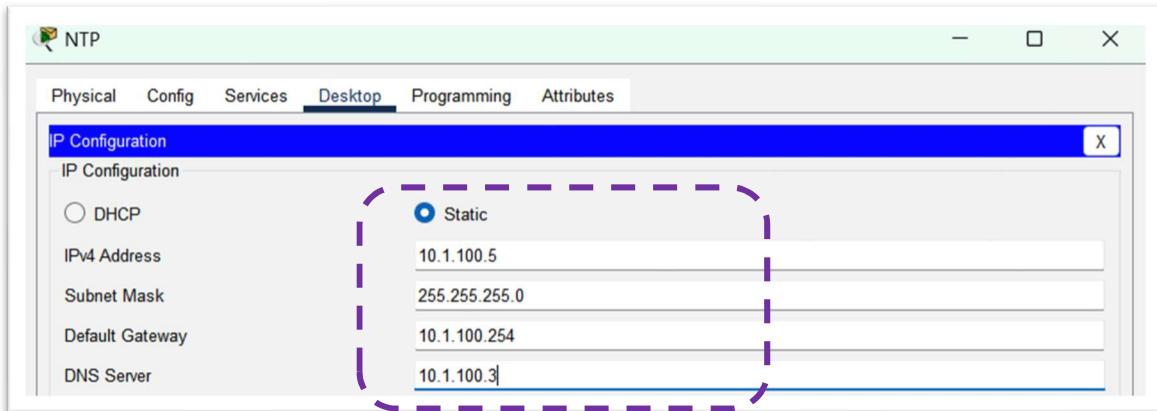


NTP Server

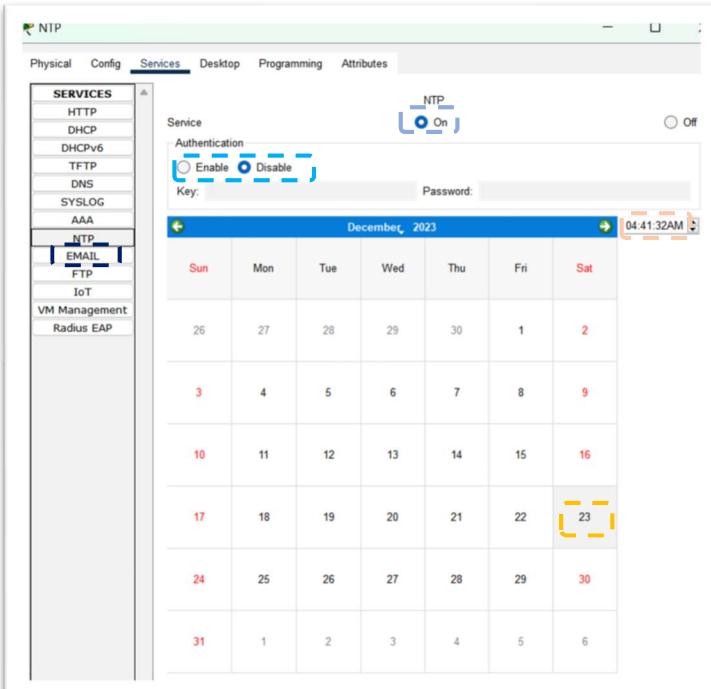
הגדרת שירות NTP ראשי



הגדרת הכתובות בשרת הראשי



הפעלת שירות NTP



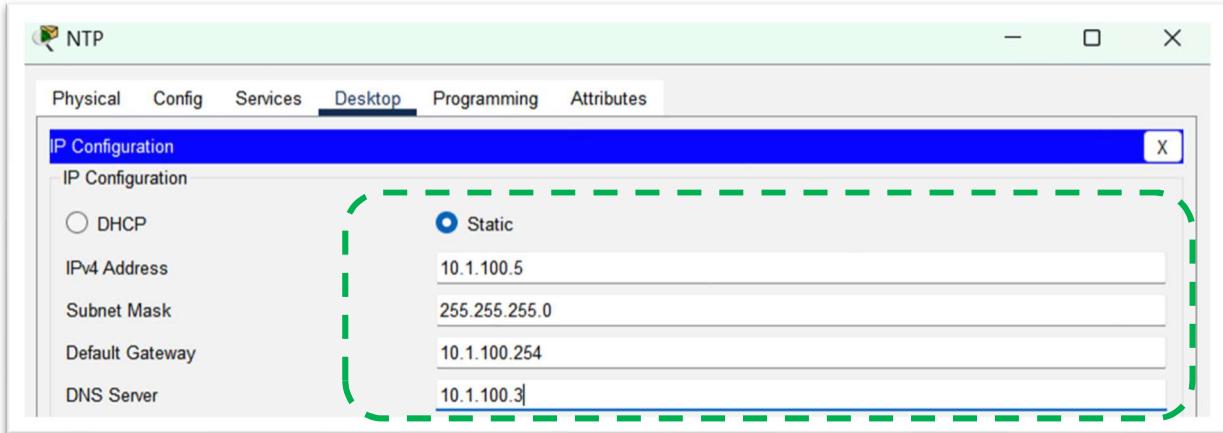
הפעלת השירות על כל הנטבים והמתגים ברשת

```
#ntp server 10.1.100.5  
#ntp server 10.1.101.5  
#service timestamps log datetime msec
```

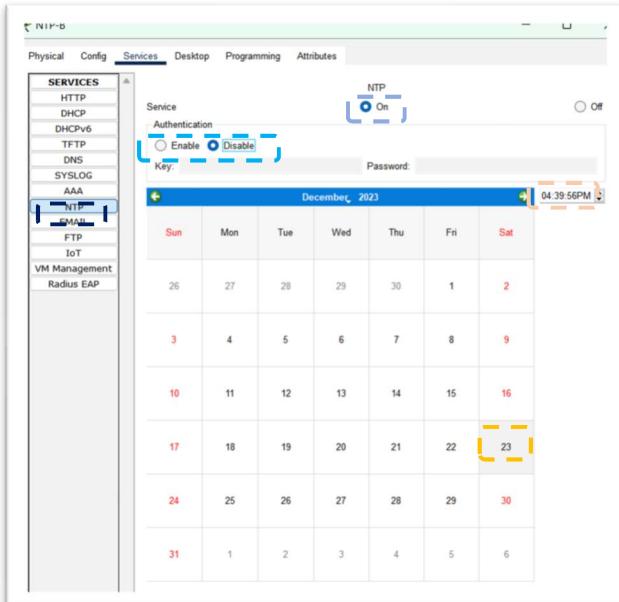
הגדירה מי שרת הNTP
הוספה זמן ללוגים

הפעלת שירות NTP בשרת הker

הגדרת הכתובות בשרת הראשי ובשרת הker



הפעלת שירות NTP

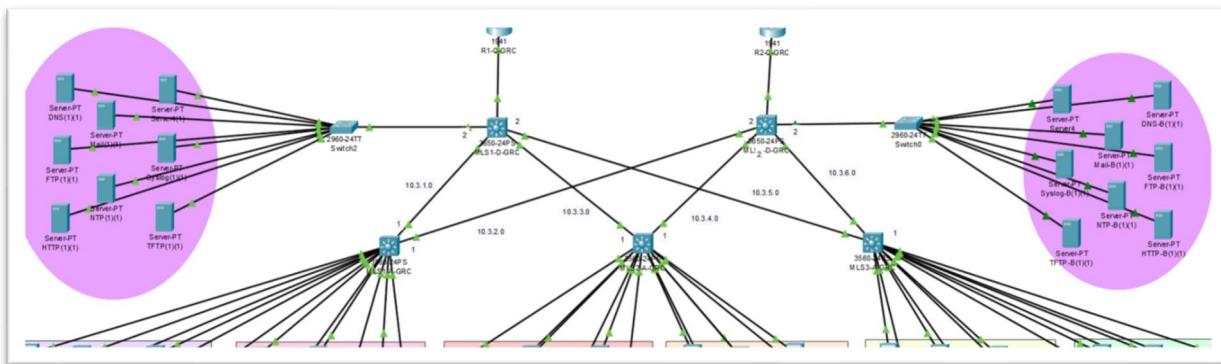


בדיקות שהשירות עובד

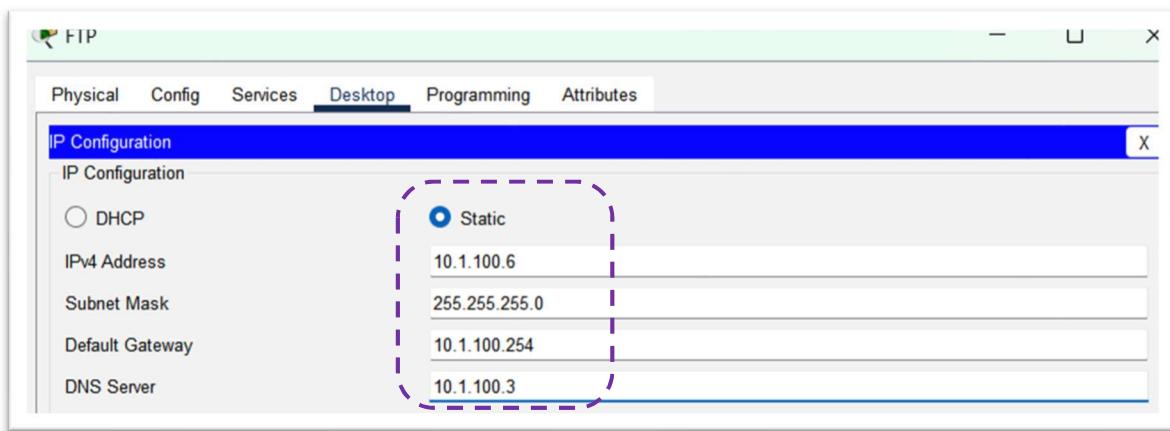
Service	Time	HostName	Message
1	12.23.2023 04:41:59.588 PM	10.1.100.253	%SYS-5-CONFIG_I: Configured from console by console
2	12.23.2023 04:41:28.796 PM	10.1.100.252	%SYS-5-CONFIG_I: Configured from console by console

FTP Server

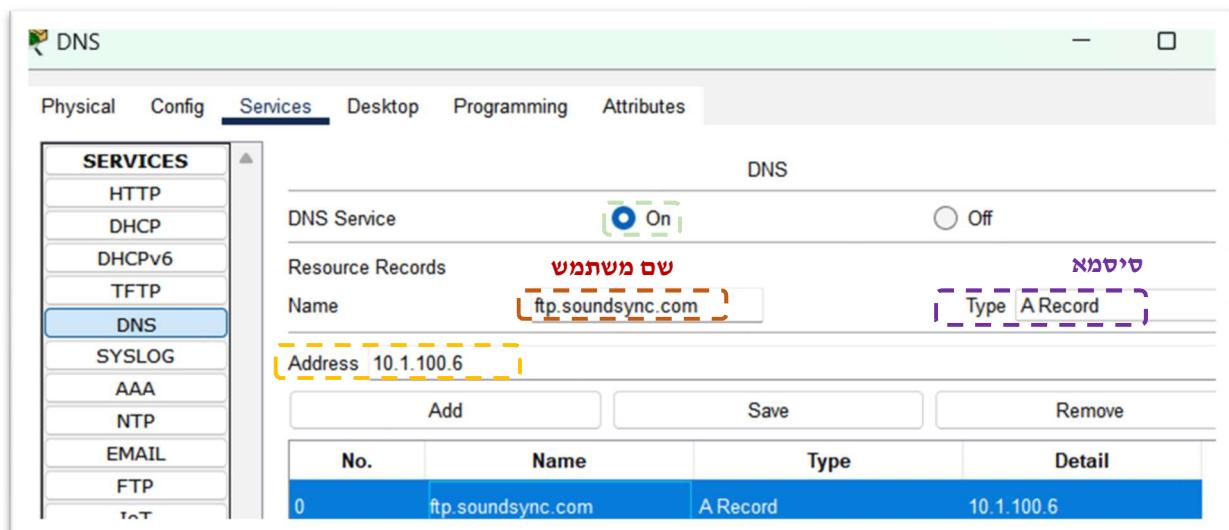
הגדרת שירות FTP ראשי



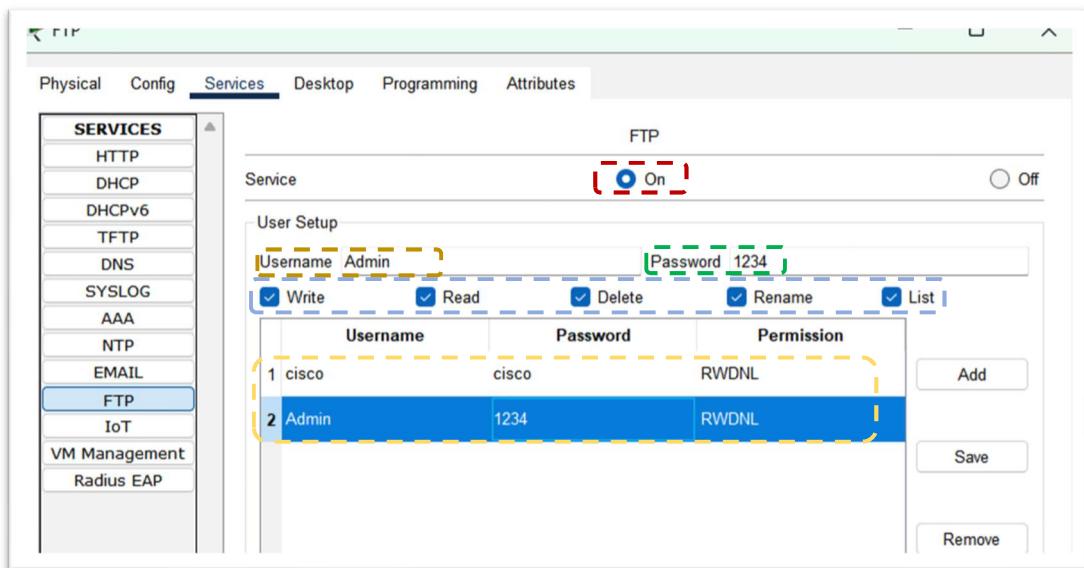
הגדרת כתובות לשירות



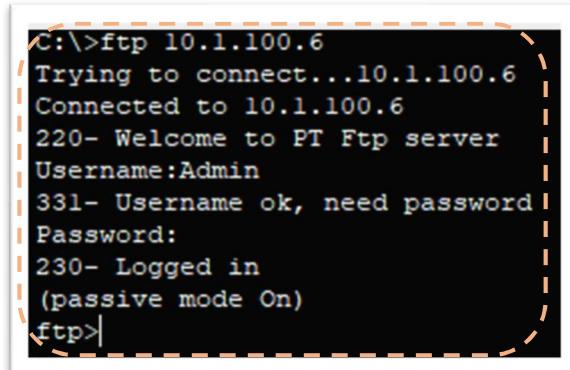
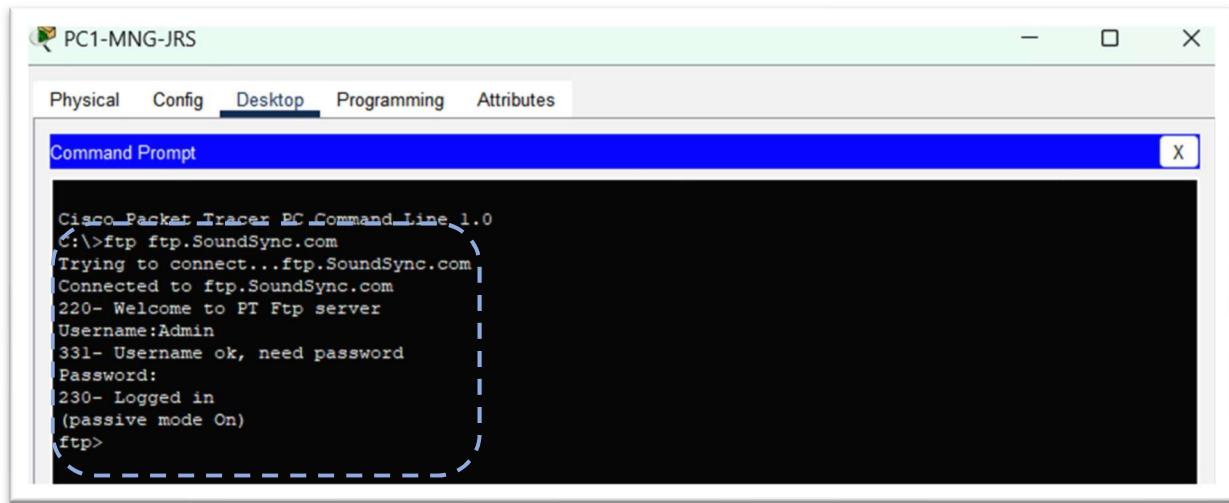
הוספה הקפota בשרות DNS



הוספה של שירות FTP

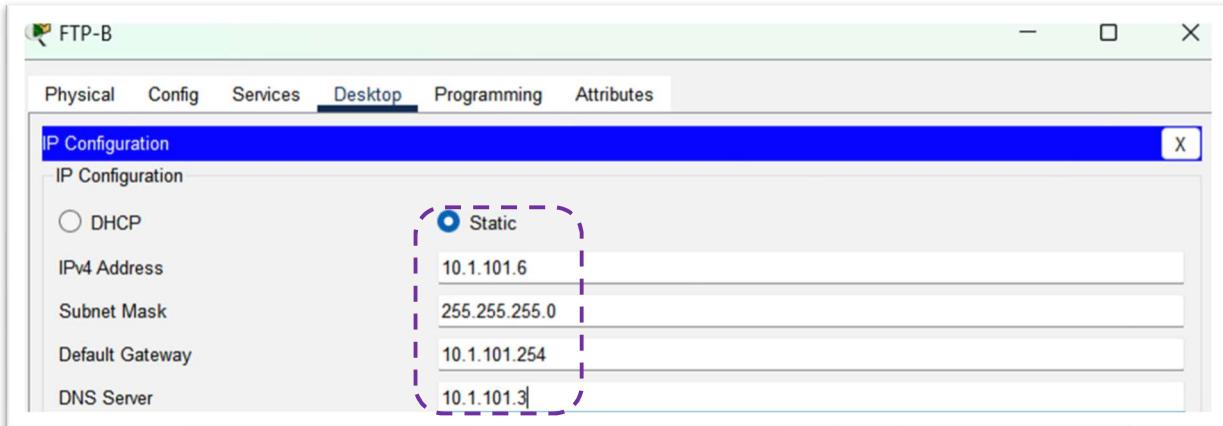


בדיקות – התחברויות FTP על ידי כתובות IP ו URLs

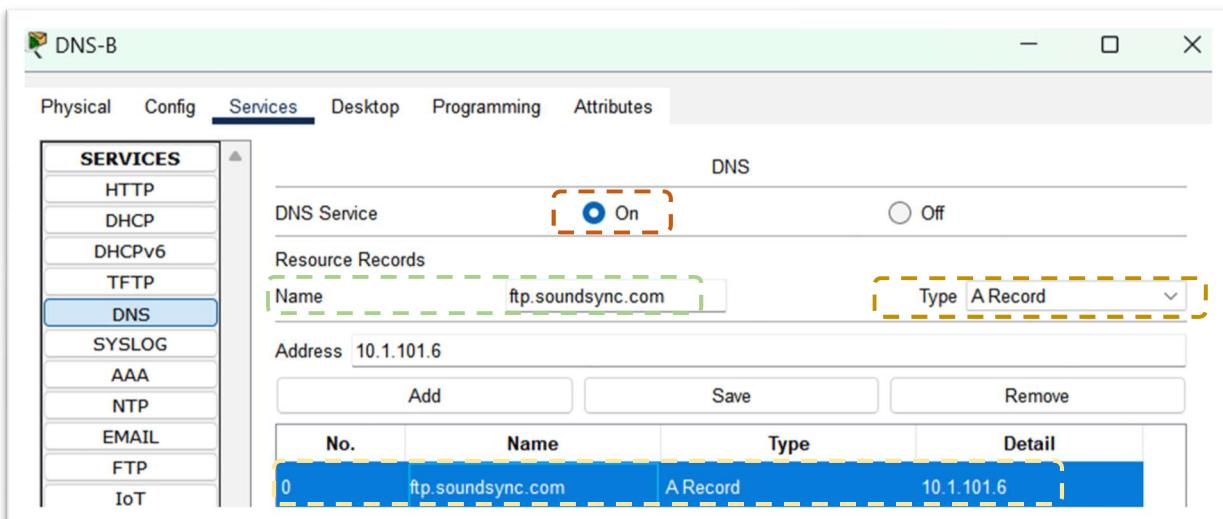


הגדרת שירות FTP גיבוי

הגדרת כתובות לשירות



הוספה הftp בשרות DNS



הוספת שירות FTP

The screenshot shows the 'FTP-B' configuration interface. The 'Services' tab is selected. On the left, a sidebar lists various services: Physical, Config, Services, Desktop, Programming, Attributes, SERVICES (HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, **FTP**, IoT, VM Management, Radius EAP). The 'FTP' service is highlighted. The main panel shows the 'FTP' service is turned 'On'. Under 'User Setup', there is a table with two rows:

Username	Password	Permission
1 cisco	cisco	RWDNL
2 Admin	1234	RWDNL

Buttons for Add, Save, and Remove are visible on the right.

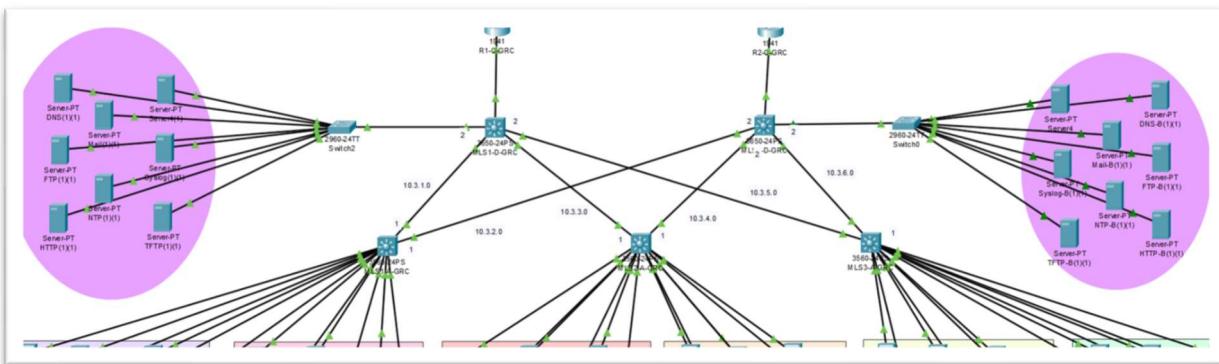
בדיקה – התחברות FTP על ידי כתובת IP וURL

The screenshot shows the 'PC1-MNG-JRS' desktop interface. The 'Desktop' tab is selected. A 'Command Prompt' window is open, displaying the following output:

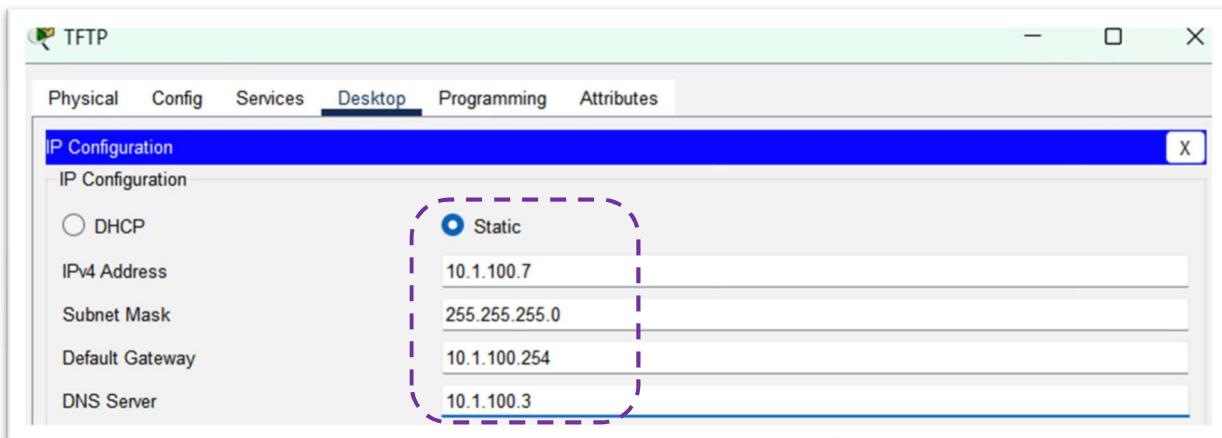
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp ftp.SoundSync.com
Trying to connect...ftp.SoundSync.com
Connected to ftp.SoundSync.com
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

TFTP Server

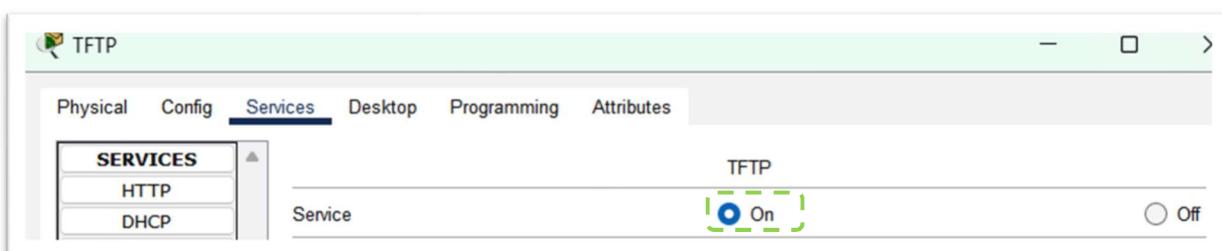
הגדרת TFTP על השירות הראשי



הגדרת כתובות על השירות



הפעלת שירות TFTP



העתקת זיכרון NVRAM של המtab לשרת TFTP הראשי

```
R1-C-JRS#copy startup-config tftp  
Address or name of remote host []? 10.1.100.7  
Destination filename [R1-C-JRS-config]? R1-C-JRS.config  
  
Writing startup-config....!!  
[OK - 3001 bytes]  
  
3001 bytes copied in 3.008 secs (997 bytes/sec)
```

نمחק את config startup מהtab

```
R1-C-JRS#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

חיבור הרשת של חוות השירותים אל הרouter (מכיוון שנמכוו ההגדירות)

```
Router(config)#int gigabitEthernet 0/0  
Router(config-if)#ip add  
Router(config-if)#ip address 10.1.100.254 255.255.255.0  
Router(config-if)#no shutdown
```

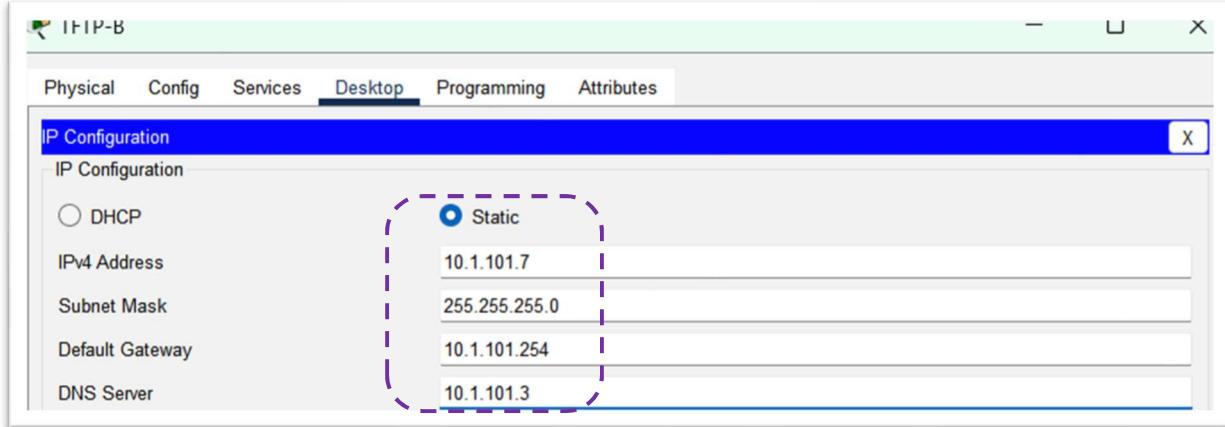
קבלת קובץ config startup מהשרת

בדיקות שכל ההגדרות התקבלו

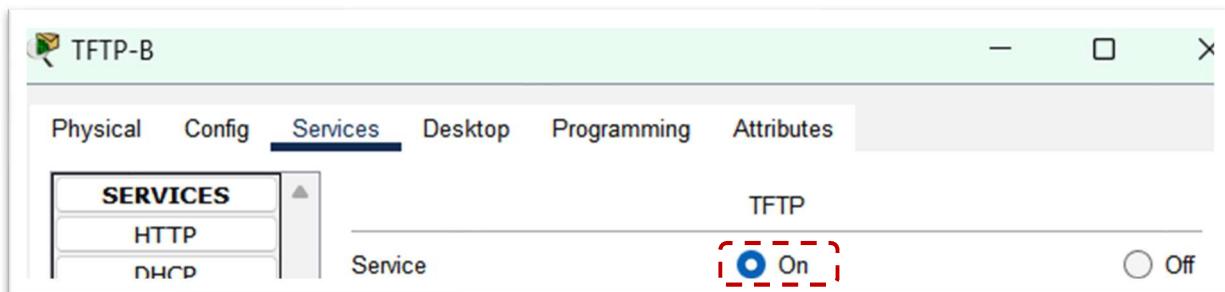
```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 10.1.100.3
ip dhcp pool lan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 10.1.100.3
```

הגדרת TFTP על השרת המשני

הגדרת כתובות על השרת



הפעלת שירות TFTP



העתקת config לשרת startup-config

```
R1-C-JRS#copy startup-config tftp
Address or name of remote host []? 10.1.101.7
Destination filename [R1-C-JRS-config]? C1-D-JRS.conf

Writing startup-config....!!
[OK - 3001 bytes]

3001 bytes copied in 1.84467e+16 secs (0 bytes/sec)
```

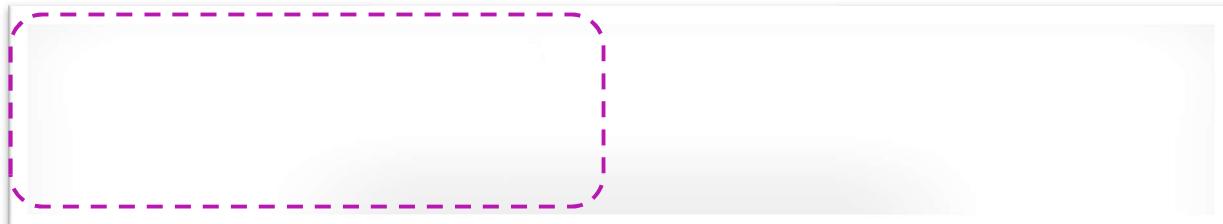
نمחק את `startup-config` מהנתב

```
R1-C-JRS#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
>1_>_>_>_>_>_>
```

חיבור הרשות של חוות השירותים אל הרואוטר (מכיוון שנמחקו ההגדרות)

```
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip add
Router(config-if)#ip address 10.1.100.254 255.255.255.0
Router(config-if)#no shutdown
```

קבלת קובץ `startup-config` מהשרת



בדיקות שכל ההגדרות התקבלו

```
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1-C-JRS
!
!
!
!
ip dhcp excluded-address 192.168.10.128 192.168.10.254
ip dhcp excluded-address 192.168.20.128 192.168.20.254
ip dhcp excluded-address 192.168.30.128 192.168.30.254
ip dhcp excluded-address 192.168.40.128 192.168.40.254
ip dhcp excluded-address 192.168.50.128 192.168.50.254
ip dhcp excluded-address 192.168.60.128 192.168.60.254
!
ip dhcp pool lan10
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.254
  dns-server 10.1.100.3
ip dhcp pool lan20
  network 192.168.20.0 255.255.255.0
  default-router 192.168.20.254
  dns-server 10.1.100.3
```

Open Shortest Path First

פרוטוקול OSPF הוא פרוטוקול המשמש לניתוב אקטואות **Autonomous system זהה**. חישוב המסלול נעשה באמצעות אלגוריתם הנקרא SPF (Shortest Path First) או בשמו השני Dijkstra. הערך行政 Distance 89. כאשר הניתוב באותו AS הינו 110 ומחוץ ל-AS המקומי הינו 150, והוא משמש בעיקר לרשות גודלות. משפחת Link state ב프וטوكול זה נשלחים עדכוניים כאשר יש שינוי כלשהו ברשות ושולח את הטבלאות המעודכנות כל חצי שעה. הנתבים מתחזקים את קשרי השכנות ביניהם ומזהים שכנים חדשים על ידי שליחת הודעות Hello. אם נתב שכן נפל, ישלח עדכון לשאר הנתבים באזור שחל שינוי ברשות.

עלות ממושך Cost

עלות המושך קבועה ביחס לרוחב הפס (bandwidth). ככל רוחב הפס של המושך גבוה יותר כך העלות של אותו מושך יהיה כל מושך יש עלות, הנתיב בעל העלות הנמוכה ביותר מקבל עדיפות על פני נתבים אחרים. הנוסחה לחישוב עלות :

- חילוק של ייחוס רוחב הפס ברוחב הפס של הפורט.
- ערך ייחוס רוחב הפס (default reference bandwidth) של הפורט שנבחר בברירת מחדל הוא 100Mbps

רוחב פס גבוה --> עלות נמוכה --> תיעודו גבוה

cost		interface
1	10 Gbps	10 Giga Ethernet
1	1 Gbps	Giga Ethererner
1	100 Mbps	Fast Ethernet
10	10 Mbps	Ethernet
64	1.544 Mbps	Serial
781	128 Kbps	Serial
1562	64 Kbps	Serial

RID (Router ID)

בכל נתב מוגדר RID שמצויה אותו

תחלק בבחירה הRouter ID

- הגדרה ידנית { router-id }

- אם לא מוגדר ידני, הממשק loopback עם הכתובת IP הגדולה ביותר ישמש כRID

- אם לא הוגדר ידנית ואין ממשק loopback או הממשק הפעיל עם הכתובת הגדולה ביותר יבחר Router ID

כדי לראות את ה- RouterID על נתב, השתמש בפקודה show ip ospf

DR (Designated Router)

ברשתות Multi-access קיימת אפשרות ליצור יחס ייחודי בין שכנים, מה שבוביל להודעות עדכון רבות העוברות בין השכנים, במצב של נתיב חדש, בשל בניתו וגודלה. אם הודעות העדכון היו מתפרסמות על ידי רואוטר לכל השכנים שלו, שהיו מעבירים את זה לשכנים שלהם וכך אלה, היה מתרחש בזבוז רחב של רוחב הפס ולעומס ברשת.

לכן, בפרוטוקול זה נבחר נתב אשר נקרא Designated Router אשר מטרתו לקבל את כל הודעות העדכון הנשלחות ולהעביר אותן אל שאר השכנים.

בכל מתחם Broadcast Domain יבחר נתב אחד שיישמש כDR

BDR (Backup Designated Router)

מקבל את כל העדכנים כמו DR. כאשר DR נופל, BDR מחליף אותו

כאשר הנתבים שולחים אותה לכתובתicast 224.0.0.6 (multicast) עליה מאזינים רק DR והוא - BDR. DR משדר את העדכנים לשאר הנתבים לכתובת 224.0.0.5 עליה מאזינים כל הנתבים.

הDR נבחר על ידי הרואוטר עם priority הכי גבוהה, השני הכי גבוהה יבחר כBDR. ערך priority יכול להיות בין 0 - 255 וכברירת מחדל הערך הוא 1. כאשר הpriority מוגדר כ0 זה קבוע שהנתב לא יוכל להיות DR או BDR. אם DR priority שווה, DR יבחר לפי Router ID (הRouter ID הגדולה ביותר יבחר DR והבא אחריו יבחר BDR). אם צור, נתב חדש בעל עדיפות גבוהה מזו של הנתב שנבחר להיות DR, הוא לא יתפוס את מקומו.

ABR (Area Border Router)

ישנם נתבים שכולים להיות שייכים למספר אזוריים, הם משמשים לחבר בין אזוריים שונים.
בכך נתבים אלו יכולים מגרי מידע לכל אזור בנפרד.

ASBR (Autonomous System Border Router)

נתב יכול להפוך ל – ASBR באחת משתי דרכים :

- על ידי חיבור למערכת אוטונומית נפרדת אחרת.
- כאשר קיימים ברשת שלי גם פרוטוקולי ניתוב אחרים, אז תפקידו הוא לחבר בין פרוטוקולי הניתוב והתעבורה תעבור כרגע.

SPF(Shortest Path First)

SPF או בשם השני Dijkstra, הינו אלגוריתם אשר מטרתו ליצור מעין מפה של הרשות שעל פיה יבחרו הנתיבים הטוביים ביותר וטבלת הניתוב תיבנה בהתאם. האלגוריתם מtabסס על המידע הנמצא בסיס הנתונים (Link state Database) והנתיבים שיבחרו יהיו אלו בעלי העלות (cost) הנמוכים ביותר. בכל פעם שיהיה שינוי בטופולוגיה הרשת, כל מפת הרשות תוחשב מחדש ולפיה טבלת הניתוב עשויה לשינוי.

טבלאות ב-OSPF

הפרוטוקול שיך למשפחת Link state כלומר כל נתב מאחסן מידע על כלל הטופולוגיה ולא רק על השכנים שלו. כל נתב המשמש בפרוטוקול זה על מנת לנ.tab, בונה מתחזק 3 טבלאות נפרדות

טבלת ניתוב – טבלה המכילה את המסלול הטוב ביותר עבור כל רשות מוכרת. בברירת מחדל נכני עד 4 נתיבים בעלי עלות זהה לטבלה. זאת על מנתקיימים איזון עומסים (Load Balancing)

טבלת הטופולוגיה – מכילה רשימה של כל הנתיבים האפשריים לכל הרשות המוכרת באזור מסוים. טבלה שכנים – טבלה המכילה רשימה של כל הנתיבים השכנים.

טבלת השכנים נבנית בעזרת הודעות ה – Hello ומכילה:

- ID Router של כל נתב שכן.
- המצב הנוכחי של כל נתב שכן.
- מהו הממשק שמתחבר לכל שכן.
- כתובת ה – IP של הממשק המרוחק לכל שכן.

OSPF Neighbors

יחסים שכנות OSPF נקראים Adjacencies הנטב יוצר יחסי שכנות עם הנטבים האחרים באותו area על ידי שליחת הודעות Hello. לאחר שהוקמו יחסי השכנות, יוכל הנטבים לשותם ביניהם מידע בנוגע לניטוב ברשת.

תהליך ייצור יחסי שכנות:

- הנטב R1 שולח הודעה מסוג Hello לכתובת Multicast 224.0.0.5
- אם עוד נתב R2 נמצא ב-OSPF ומקבל את ההודעת Hello הוא ירשום אותו כשכן זמני (init)
- R2 שולח הודעה Hello בה מצין את RID של R1
- כאשר הוא מקבל את הפאקטה, הוא מכניס את R2 לטבלת השכנים (way)
- R1 ישלח Hello packet ל-R2 וIOSIF אותו לטבלת השכנים (way2)

לאחר שנוסף הנטב לטבלת השכנים ישלחו הודעות Hello בין השכנים כל 10 שניות. מטרת ההודעות הינה לתזקק את הקשר בין השכנים הקיימים.

– אכמת זמן שבה ימתין הנטב בלי לשם שום הודעה מהשכן. בברירת המחדל הזמן הוא 40 שניות. כאשר עבר הזמן המוגדר, הנטב יכריז על אותו נתב כלא פעיל. במשך סריאלי הודעה Hello נשלחת כל 30 שניות ו-Interval Dead – כל 120 שניות.

על מנת שנתבי OSPF יהפכו להיות שכנים, ישנס כמה פרמטרים שחיברים להיות זהים בכל הودעת Hello וכמה שרכייכים להיות שונים

פרמטרים שחיברים להיות זהים בהקמת יחסי שכנות:

- ID Area – על הנטבים להיות באותו אזור.
- אזור סוג (stub, NSSA).
- Prefix.
- מסכת רשת (S.M).
- Hello Interval
- Dead Interval
- (Broadcast, Point-to-Point) שידור סוג
- אימות – מהו סוג האימות המשומש.

פרמטרים שחיברים להיות שונים בעת הקמת יחסי שכנות:

- Router ID
- כתובת IP –

סוגי רשותות ב-OSPF

- access-Multiaccess – טופולוגיה בה העברת המידע נעשיתBroadcast. בסוג זה, כלל הראותרים מחוברים למתקן ולכל חולקים את אותה הרשות. ברשות זו יבחרו DR ו-BDR אשר יהיו אחראים על פרסום העדכנים לשאר הנתבים בחיבור
- P2P (Point to Point) – טופולוגיה בה 2 נתבים מתחברים ישירות. בחיבור מסוג זה אין בחירה של DR ו-BDR כיון שאינם מחוברים אחד לשני. עדכוני LSA נשלחים לכתובת 224.0.0.5 ..Multicast

הודעות ב-OSPF

מתקשר OSPF בין הנתבים. משדר לכתובת 224.0.0.5 בתקורת רגילה בין הנתבים ובכתובת 224.0.0.6 לעדכון נתבי DR ו-BDR

סוגי הודעות ותהליכי סנכרון הטעלאות:

- DBD (DataBase Description packet) : סיכום טבלה שנשלח לשאר הנתבים כדי לדעת אם בסיס הנתונים שלהם מסונכרן או שחרר להם מידע
- LSR (Link-State Request) - אם הנתב לא מסונכרן (לפי הودעת DBD שנשלחה), הוא שולח בקשה מבסיס הנתונים של נתב מסונכרן
- LSU (Link-State Update) - שליחת מידע כתגובה לLSR
- LSAck (Link-State Acknowledgement) - שליחת אישור על קבלת HSU.

הודעת LSA (Link-State Advertisements) – הודעות המכילות מידע על הקישור והרשות כגון סוג ממושך, עלות (cost), ומאפיינים נוספים. הודעות אלו עוברות על מנת לתזוק את בסיס הנתונים של הטופולוגיה ולעוזר לנtab להחליט את הנתיב הקצר והטוב ביותר אל רשות היעד. הודעות אלו עוברות בכתבota Multicast מה שמאפשר תזוק של המסדר נתונים ועדכונו ובכך להבטיח כי לנתבים יש את המידע המעודכן על מצב הרשות בהתאם לשינויים שקרו.

סוגי הודעות LSA:

Router LSA (Type 1) – נשלחת על ידי כל הנטבים ומודפסת לנטבים באותו איזור. מכילה קישורים ישירים לנטב, מצב ועלות של הממשקים. יופיע בטבלת הניתוב כ-O.

Network LSA (Type 2) – נשלחת על ידי נתבי DR בחיבור מסווג Multi Access. מכילה רשימה של כל הנטבים המוחברים לאותה רשת.

Network Summary LSA (Type 3) – נשלחת על ידי ה-ABR. מכילה רשימה של האיזורים המוחברים אליו ונשלחת בין איזורים שונים על מנת לאפשר תקשורת של ניתוב מסווג Inter Area.

ASBR Summary LSA (Type 4) - נשלחת על ידי ה-ASBR. מכילה מידע על מיקום נתבי ה-ASBR במערכת.

External LSA (Type 5) – נשלחת על ידי ה-ASBR. מכילה נתיבים לרשותה אשר נמצאות מחוץ למערכת האוטונומית המקומית. ככלומר רשותן שנלמדו דרך פרוטוקול ניתוב שונה או ניתוב דיפולטיבי (ברירת מחדל). הודעות אלו מוצפנות לכל האיזורים במערכת.

לא בשימוש כיום – **Multicast OSPF (Type 6)**

NSSA LSA (Type 7) – אזור ב-OSPF שאינו מאפשר הודעות Type 5. הودעה זו משמשת כהסואה להודעות מסווג חמוץ על מנת לאפשר מיידת ניתובים לרשותה יעד מחוץ למערכת המקומית בסוגי איזורים מסוימים אשר אינם מאפשרים מעבר של הודעות מסווג 5.

מצבי הנטב:

המצבים בהם נמצא נתב בתהליך לייצירת יחס שכנות עם נתב אחר :

Down – המצב ההתחלתי, הנתב מפיץ הודעות Hello במטרה לגלוות שכנים חדשים אך עדין לא קיבל הודעות Hello אל הנתב.

Init – קבלת הודעת Hello על ידי שכן, אך מכיוון שהשכן לא יודע עדין על קיומו של הנתב הנל, לא בכללה בהודעה המזזה של הנתב. לכן, ישלח הנתב הודעת Hello לאותו שכן על מנת לאשר כי קיבל את הודעת Hello שלו.

2-way – שני הנטבים קיבלו את הודעות Hello אחד של השני ולכון נוצרה תקשורת דו כיוונית

Exstart – לאחר בחרת DR והוא - BDR מתבצע תהליך החלפת המידע אחד עם השני (Link State)

Exchange – הנטבים מחליפים ביניהם הודעות DBD אשר מכילים רק את ה-LSA headers על מנת לבדוק איזה מידע חסר להם

Loading – הנטבים שולחים Link State Request על המידע שחשר להם לפי ה-LSA headers שנשלחו בשלב הקודם. השכנים מספקים את המידע על ידי שליחת Link State Update.

Full – קיים סyncron מלא בין הנטבים

Areas

כasher הרשות גדולה, אנחנו מחלקים אותה לרשותות יותר קטנות, כל רשות מחולקת היא אזור (Area). כל הנטבים הנמצאים באותו אזור מכילים טבלת טופולוגיה זהה. נתב מודע רק לאזור שבו הוא נמצא ולא יודע שום מידע על אזוריים אחרים ברשות. חברת Cisco מציעה שלא יהיה יותר מ – 50 נתבים באזור אחד. על האזוריים חייבים להתחבר לאזור הנקרא Backbone והוא 0.Area

יתרונות העבודה ברשות היררכית :

- טבלאות ניתוב קטנות יותר.
- תחליק התקנסות מהיר יותר.
- תקלת באזור אחד לא תשפיע על שאר האזוריים ברשות.
- פחות חישובים שמתבצעים בנתב.
- פחות עדכנים עוביים ברשות

סוגי אזוריים

- Intra Area – נתבים הנמצאים בתוך האזור של הנתב נקראים Intra Area. בטבלת הניתוב נראה את ניתובים אלו מסומנים באות O.

- Inter Area – נתבים העוברים דרך נתב ABR. ככלומר, נתבים הנמצאים באזור שונה משם הנתב נקראים Inter Area – ניתוב בין אזוריים. בטבלת הניתוב נראה את ניתובים אלו מסומנים ב – IA O.

- External – קיימים שני סוגי של Type 1 ו Type 2 :
1. Type 1 – חישוב העלות (cost) של הנתיב. סוג 2 מכיל רק את הערות החיצונית בעוד סוג 1 מכיל גם את הערות החיצונית וגם את הערות הפנימית. נתיב סוג 1 קיבל עדיפות על נתיבים מסוג 2. אלו נתבים הנלמדים דרך ניתוב סטטי או דרך פרוטוקול ניתוב שונה. ניתוב 2 Type נמצא כברירת מחדל. בטבלת הניתוב נראהו את ניתובים אלו מסומנים ב – O E1 ו – O E2 .

איזורים ב OSPF :

Backbone – האיזור המרכזי ברשות מסווג OSPF. כל האיזורים יהיו מחוברים אליו. אזור זה תמיד יהיה 0 (area 0) והוא תומך בהודעות LSA מסווג 1 בלבד.

הגדרה של איזור Backbone :

Network {NetID} area 0

- Standard Area
הנתבים באיזור זה ישלו הודעות LSA 1 ונתבי DR (אם קיימים כלומר אם החיבור מסווג Multi Access), ישלו הודעות LSA 2. כאשר כל הנתבים יסוכרכנו ויקבלו את כל העדכונים, טבלאות הטופולוגיה של הנתבים יהיו זהות.

הנתבים יקבלו בנוסף הודעות LSA 3 של סיכום הרשת, המכילים מידע על מסלולים על מנת להגיע לאזוריים אחרים ברשת, והודעות מסווג LSA 4 – 5 המכילים את הנתיב ל-ASBR ונתיבים נוספים אל רשתות חיצונית.

- Stub Area – מונע הצפה של נתיבים חיצוניים אל האיזור.

כמו אזוריים רגילים, ישלו הודעות LSA מסווג 1 ו-2 כלומר הנתבים יקבלו מידע על הנתבים הנמצאים אותם באותו איזור ויתקבלו גם הודעות מסווג 3. לעומת זאת איזור רגיל, לא יתקבלו הודעות LSA 4 ו-5 כלומר הנתיב לא יוכל מידע על רשתות מחוץiae לאיזור, אלה יוצר ניתוב בברירת מחדל המתקבל מ-ABR על מנת להגיע אל רשתות אלו : stub הגדרה של איזור

area [area num] stub

- Totally Stubby Area – מונע הצפה של נתיבים חיצוניים ובין אזוריים

כמו אזוריים רגילים, ישלו הודעות LSA מסווג 1 ו-2 כלומר הנתבים יקבלו מידע על הנתבים הנמצאים אותם באותו איזור. לעומת זאתStub Area, לא יתקבלו הודעות מסווג 3. זאת במטרה לצמצם את כמות הודעות LSA ובכך לחסור ברוחב הפס של הנתיב. יוצר ניתוב בברירת מחדל על מנת להעביר את המידע לאזוריים שונים וחיצוניים

: Totally Stub הגדרה של איזור

area [area num] stub no-summary

- NSSA (Not So Stuby Area) – מונע הצפה של נתיבים חיצוניים לאיזור בדומה לStubbut

הגעה מ-ASBR שבתוך איזור NSSA. הוא תומך בהודעות מסווג 3-1. אם קיים באיזור זה, ASBR, תישלח הودעה מסווג 7. איזור זה לא מקבל מידע של ניתוב בברירת מחדל מה-ABR בغالל שמקבל מה-SBR שמחובר באותו איזור מידע על רשתות ש망יעות מפרוטוקול ניתוב שונה ואחת מהודעות אלו הינה ניתוב מסווג ברירת מחדל.

: NSSA הגדרה של איזור

Area [area num] NSSA

Totally Stubby (Totally Not So Stubby Area) – דומה ל-Stubbut

תומך בהודעות מסווג 1 ו-2 ואם קיים באיזור ASBR יתמוך גם בהודעות LSA 7. דומה ל-NSA פרט לכך שאינו מקבל LSA 3 כלומר לא מכיל מידע על אזוריים שונים.

Virtual Link

כמו שהסבירנו, יש חוק מרכזי ב – OSPF שכל אזור חייב להיות מחובר לאזור 0, ה – Backbone. דבר זה דורש המון משבבים והמון כסף כי צריך לחבר את האזוריים בניהם ומדובר פה על מרחקים מאד גדולים, או שלאזורים מסוימים אין קשר ישיר לאזור 0 ולכן נדרש לעבור דרך אזוריים אחרים. link virtual היא שיטה לחבר בין אזוריים מרוחקים לאזור 0 על ידי לחבר ווירטואלי דרך נתבים הממחברים לאזור 0.

מגדירים link Virtual המחברים בין אזוריים. על נתב ה – ABR שמחובר לאזור 0 נגידר שרשת היעד היא של הנתב המרוחק ועל נתב ה – ABR שלו ימחובר האזור המרוחק נגדיר שרשת היעד היא הרשת של הנתב שמחובר לאזור 0. ובכך באיזור שבין האזור המרוחק לאזור 0 יהיה לחבר וירטואלי, מעין "מנטור" בצד אחד בין האזוריים.

הגדרת

צריך להגדיר בנתב ה – ABR שמחובר לאזור 0 שרשת היעד היא הרשת של הנתב הנמצא באיזור מרוחק. הפקודה :

R1(config-router)# area <area-id> virtual link <not directly connected router_id>

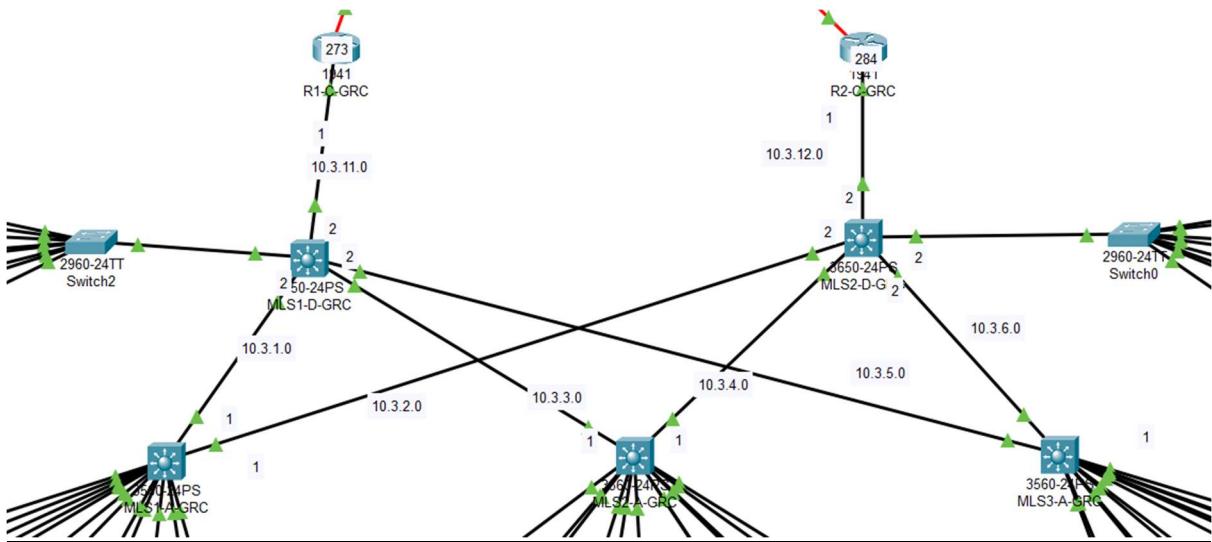
צריך להגדיר בנתב ה – ABR שמחובר לאיזור המרוחק שרשת היעד היא הרשת של הנתב הנמצא באיזור 0. הפקודה :

R2(config-router)# area <area-id> virtual link <area 0 router router_id>

<id-area> שבפקודה מדברת על האיזור שנמצא בין איזור 0 לאיזור המרוחק.
*הערה - במידה ויש Router ID נשתמש בו ולא בהגדה של רשות היעד.

משק פאסייבי - משק שהוגדר כמשק פאסייבי אינו שולח או מקבל הודעות Hello ואינו מבצע יחס
שכנות

הגדרת OSPF בסניף השלישי



כרגע לא עוברת תעבורת בין מחשבים ב – VLANs שונים. על מנת שתקשרו תעבור ביןיהם יש לאפשר ניוטוב במתג שכבה 3 על ידי הפקודה `z0 no cll legrouting ip`. על ידי פקודה זו יוכל להגדיר גם פרוטוקול ניוטוב. בשבייל שהמחשבים יכולים לתקשר עם השירותים אלו נגדיר במתגים

הגדרת כתובות IP לממשקים

```

interface GigabitEthernet1/0/1
no switchport
ip address 10.3.1.2 255.255.255.0
duplex auto
speed auto

!
interface GigabitEthernet1/0/2
no switchport
ip address 10.3.3.2 255.255.255.0
duplex auto
speed auto

!
interface GigabitEthernet1/0/3
no switchport
ip address 10.3.5.2 255.255.255.0
duplex auto
speed auto

!
interface GigabitEthernet1/0/4
no switchport
ip address 10.3.11.2 255.255.255.0
duplex auto
speed auto

!
interface GigabitEthernet1/0/5
no switchport
ip address 10.2.201.254 255.255.255.0
duplex auto
speed auto

```

הגדרת OSPF בשכבהisis

```
router ospf 1
  router-id 4.4.4.4
  log adjacency-changes
  network 10.3.1.0 0.0.0.255 area 0
  network 10.3.3.0 0.0.0.255 area 0
  network 10.3.5.0 0.0.0.255 area 0
  network 10.3.11.0 0.0.0.255 area 0
```

הגדרת OSPF בשכבהAccess

```
router ospf 1
  router-id 1.1.1.1
  log adjacency-changes
  network 10.3.1.0 0.0.0.255 area 0
  network 10.3.2.0 0.0.0.255 area 0
  network 192.168.10.0 0.0.0.255 area 0
  network 192.168.20.0 0.0.0.255 area 0
```

Show Commands

show ip ospf database

Router Link States (Area 0)					
Link ID	ADV Router	Age	Seq#	Checksum	Link count
4.4.4.4	4.4.4.4	1276	0x8000000d	0x004316	4
10.3.12.1	10.3.12.1	1281	0x80000006	0x00f1f5	1
2.2.2.2	2.2.2.2	1278	0x8000000b	0x00d2d4	4
1.1.1.1	1.1.1.1	1277	0x8000000b	0x007b64	4
5.5.5.5	5.5.5.5	1276	0x8000000e	0xbba4	5
10.3.11.1	10.3.11.1	1275	0x80000006	0x00edfd	1
3.3.3.3	3.3.3.3	1272	0x8000000b	0x002a45	4
Net Link States (Area 0)					
Link ID	ADV Router	Age	Seq#	Checksum	
10.3.1.2	4.4.4.4	1281	0x8000000d	0x009clb	
10.3.3.2	4.4.4.4	1281	0x8000000e	0x001f70	
10.3.5.2	4.4.4.4	1276	0x8000000f	0x00d0d2	
10.3.6.2	5.5.5.5	1281	0x8000000d	0x00e0ba	
10.3.4.2	5.5.5.5	1281	0x8000000e	0x00dcc3	
10.3.12.1	10.3.12.1	1281	0x80000005	0x00641b	
10.3.2.2	5.5.5.5	1276	0x8000000f	0x008429	
10.3.11.1	10.3.11.1	1275	0x80000005	0xa3ef	

מזהה הממשק – מזהה הנטב.

זמן בשניות של חבילת LSA

הנטב ששלח את הודעה

מספר חבילה

האחרונה שהתקבלה

show Ip ospf interfaces

```
MLS2-D-GRC#show ip ospf interface

GigabitEthernet1/0/1 is up, line protocol is up
  Internet address is 10.3.1.2/24 Area 0
    מזזה עלות כתובת ואיזור
    Process ID 1, Router ID 4.4.4.4, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR Priority 1 מי ה-DR
    Designated Router (ID) 4.4.4.4, Interface address 10.3.1.2 סוג נטב ועיפוי
    Backup Designated Router (ID) 1.1.1.1, Interface address 10.3.1.1
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     >Hello due in 00:00:08 מתי תשלח חבילת hello הבאה בשניות
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 1, maximum is 1
    Last flood scan time is 0 msec, maximum is 0 msec כמה שכנים יש
    Neighbor Count is 1, Adjacent neighbor count is 1
     Adjacent with neighbor 1.1.1.1 (Backup Designated Router)
    Suppress hello for 0 neighbor(s)
  GigabitEthernet1/0/2 is up, line protocol is up מי השכנים ומה תפקידם
```

show ip ospf neighbors

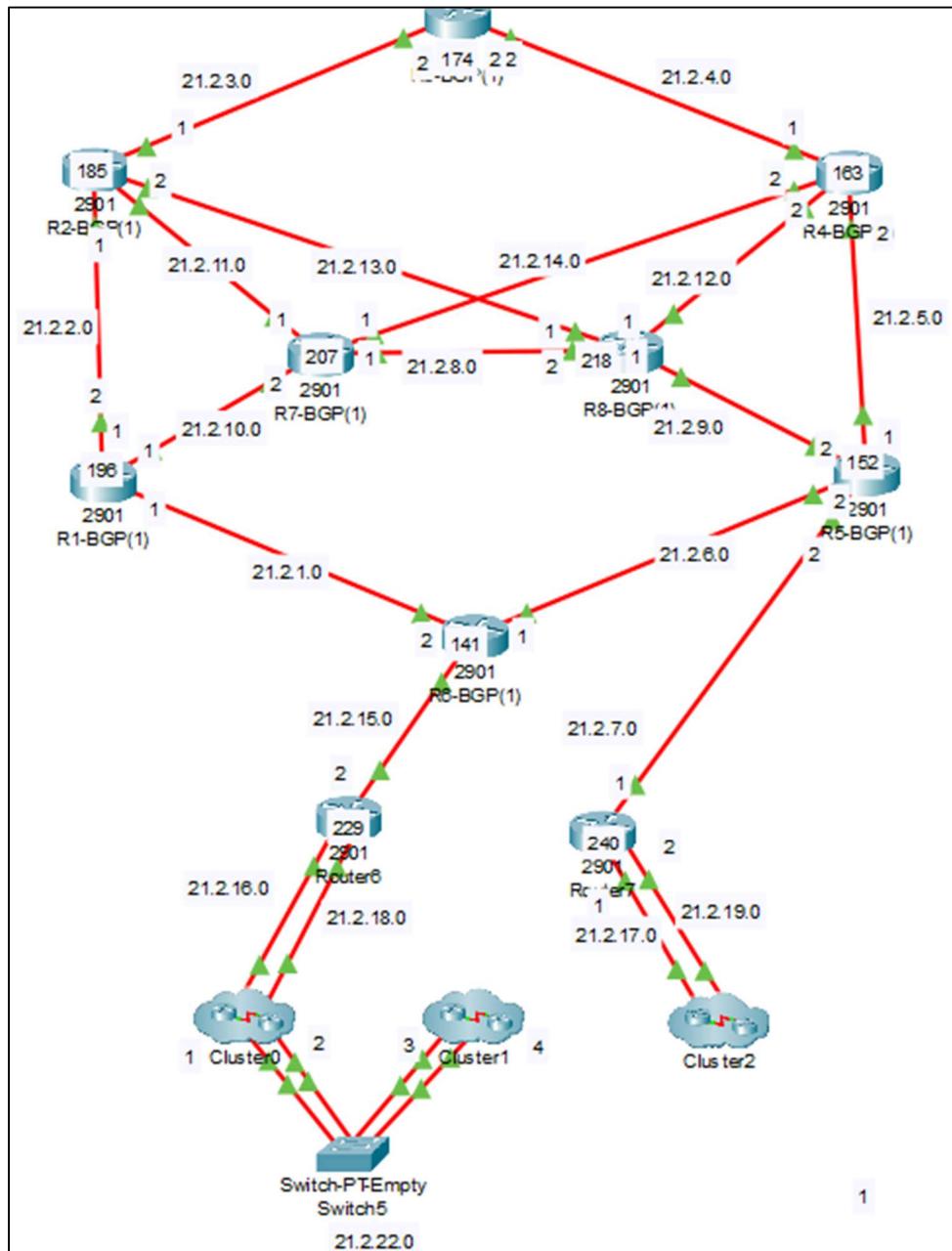
מזהה שכן	עדיפות	טפקי השכן الآخر	מספר לאחור	כתובת הממשק	הממשק של ראייר זה שדרכו נמצא השכן
Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	00:00:39	10.3.3.1	GigabitEthernet1/0/2
10.3.11.1	1	FULL/DR	00:00:38	10.3.11.1	GigabitEthernet1/0/4
1.1.1.1	1	FULL/BDR	00:00:39	10.3.1.1	GigabitEthernet1/0/1
3.3.3.3	1	FULL/BDR	00:00:38	10.3.5.1	GigabitEthernet1/0/3

MLS2-D-GRC#show ip protocols

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4 מספר אזורים וסוגים
  Routing for Networks: רשתות המחברות ישרות
    10.3.1.0 0.0.0.255 area 0
    10.3.3.0 0.0.0.255 area 0
    10.3.5.0 0.0.0.255 area 0
    10.3.11.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway           Distance   Last Update
    1.1.1.1            110       00:23:48
    2.2.2.2            110       00:23:49
    3.3.3.3            110       00:23:43
    4.4.4.4            110       00:23:47
    5.5.5.5            110       00:23:47
    10.3.11.1          110       00:23:46
    10.3.12.1          110       00:23:52
  Distance: (default is 110) ערך AD
```

רשת רחבה WAN - חיבור בין הסניפים

עד כה יצרנו 3 סניפים נפרדים : סניף בירושלים, בתל אביב וביוזן.
 כלומר 2 סניפים אשר מצויים בעיר שוניות באותה מדינה, וסניף אחד הנמצא במדינה אחרת.
 על מנת לחבר את הערים הנמצאים באותה מדינה השתמשתי בחיבור מסוג מטרו.
 את החיבור של הסניף השלישי לסניפים האחרים עשית על ידי חיבור הסניף הראשון והשלישי ל 2 ISP
 שונים אשר יתקשרו זה עם זה דרך טבעת BGP . על חיבורים אלו ארכחיב בהמשך.



פרוטוקול BGP הינו פרוטוקול ניתוב מסוג Path vector המשמש בעיקר על מנת לספק חיבור והחלפת מידע בין מערכות אוטונומיות. התקשרות של הנטבים אחת עם השנייה מושג על ידי peer to peer ומאפשר לרשותה לשЛОוח ולקבל מידע אחד מהשני. משתמשים ב프וטוקול זה במערכות אוטונומיות היוות ומסוגל לשמר טבלאות ניתוב גדולות ולהכיל מידע רב. הוא משתמש בתכונות רבות על מנת לבחור את הנטיב האידייאלי

דרך העבודה של פרוטוקול BGP

כאשר נתב צריך להתחבר לרשתות אחרות, הוא אינו יודע לבדו לאיזה רgel לשЛОוח את המידע על מנת הגיעו לעד ובדרך הטובה ביותר. BGP בוחר את הנטיב אשר עבר הכיכת מעתות אוטונומיות שונות. כל שכן משותף עם שאר השכנים את המידע אשר יש לו על הנטובים ברשות. הפרוטוקול הוא זה שבוחר את הנטיב הטוב ביותר.

סוגי BGP

- IBGP (Internal BGP) – סוג זה משמש על מנת לנtab בין נטבים אשר נמצאים באותו מערכת אוטונומית. משמש לניתוב פנימי. ערך AD שלו הוא 2 – וערך ה TTL מוגדר כ255.
- EBGP (External BGP) – סוג זה משמש על מנת לנtab בין נטבים אשר נמצאים במערכות אוטונומיות שונות. חיבור זה מוקם בדרך כלל על ידי נטבים המוחברים בצורה ישירה זה עם זה ולכן ערך ה TTL יוגדר לרוב כ1. ערך AD שלו הוא 20.

תכונות לבחירת נתיב:

קיימים שני סוגי של תכונות :

- Known-Well – תכונות אשר מופצות בהכרח לכל השכנים. מחולק לשני סוגים :
- Mandatory – תכונות המופיעות בכל בכל הודעה UPDATE.
- Discretionary – תכונות שלא בהכרח מופיעות בכל הודעה UPDATE.
- Optional – אין חיבת בהכרח להיות מופצת לשכנים. מחולק לשני סוגים :
- Transitive - מועברות לכל השכנים גם אם אינם מכירים את ה Attribute .
- Transitive-Non – לא נדרש להעביר לשכנים אם לא מכירים

Attribute Name	Attribute Code	Attribute Type
Origin	1	Well-known mandatory
AS Path	2	Well-known mandatory
Next Hop	3	Well-known mandatory
Multiple Exit Discriminator	4	Optional nontransitive
Local Preference	5	Well-known discretionary
Atomic Aggregate	6	Well-known discretionary
Aggregator	7	Optional transitive
Community	8	Optional transitive
Originator ID	9	Optional nontransitive
Cluster List	10	Optional nontransitive
Multiprotocol Reachable NLRI	14	Optional nontransitive
Multiprotocol Unreachable NLRI	15	Optional nontransitive
Extended Community	16	Optional transitive

- מקור הניתוב : Origin
- IGP – המסלול נמצא ב-AS הנוכחי, מצוין באות "i" בטבלת BGP. לדוגמה, אם בטבלה מצוין : i , 9, 20, זאת אומרת שבכדי להגיע לעיד צרייך לעבור 20 AS ואז ל – 9 AS והיעד נמצא כבר בתוך 9 AS. ומשם יונטב בפרוטוקול מסווג IGP.
- EGP – כבר איןנו נתמך, מצוין באות "e" בטבלת BGP.
- Incomplete – מסלול שאינו ידוע או שנלמד באמצעות אמצעים אחרים. לרוב קורה כאשר המסלול נלמד מפרוטוקול ניתוב שונה (Redistribute). מצוין ב – "?" בטבלת BGP.

- – רשימה של מספרי AS על מנת להגיע ליעד.
- – כתובות ה – IP של הקפיצה הבאה על מנת להגיע אל היעד.
- – מידע לשכנים חיצוניים על הנתיב המועדף לתוך AS בעל מספר כניסה. ה – MED מופץ לשכני EBGP והם מפיצים את ה – MED בתוך ה – AS שלהם.
- – מידע לנטים המקומיים ב – AS על מנת קבע את המסלול המועדף בצד יצאת מה – AS. ערך ברירת המחדל הוא 100. מוחלף אך ורק בין שכני IBGP.
- – ציון המסלולים שסוכמו. Atomic aggregate
- – על מנת לסנן מסלולים נכנים או יוצאים, נתבי BGP יכולים לティיג נתבים עם אינדיקטור ולאפשר לנטים אחרים לקבל החלטות על סמך-tag זה. MED – נתינת מידע לשכנים חיצוניים על הנתיב המועדף לתוך AS בעל מספר כניסה. ה – MED מופץ לשכני EBGP והם מפיצים את ה – MED בתוך ה – AS שלהם.

Cisco Weight Attribute

תכונה קניינית של חברת Cisco. אלה כאשר לנtab יש מספר יציאות. אך בשונה מ – Preference Local. תכונת Weight מוגדרת באופן מקומי על נתב ולא מופצת אל שום נתב אחר.

תהליך בחירת הנתיב הטוב ביותר

- .1. ערך Weight גבוה.
- .2. ערך Local Preference גבוה.
- .3. נתוב שמקורו הנתוב שלו מקומי.
- .4. ערך נמוך יותר של AS-PATH - מספר קפיצות נמוך יותר.
- .5. Origin נמוך יותר (INC>EGP>IGP)
- .6. ערך MED נמוך יותר.
- .7. עדיפות של EBGP על IBGP.
- .8. אם כל התרחישים עד כה זהים, ההעדפה תהיה למסלול אליו ניתן להגיע דרך שכן ה – IGP הקרוב ביותר.
- .9. במידה והנתיב הפנימי זהה, כתובות ה – ID Router – ID יהיה השובר שווין:

במידה ומוגדרת כתובות ID Router או הכתובת הנמוכה ביותר.

במידה ולא מוגדרת כתובות ID Router – Loopback, כתובות ה – ID Router הגבוהה ביותר תשמש כ – ID Router. במידה וגמ כתובות Loopback לא מוגדרת, כתובות ה – IP הגבוהה ביותר של הנתב תשמש כ – ID Router.

סוגי הודעות ב프וטוקול BGP

הוועת	תוכן	הודעה
גרסה וזמן Hold חייבים להיות זמינים במערכות.	גרסה, מספר מערכות אוטונומית, זמן Hold (בברירת מחדל 180 שניות), optional ,BGP ID.	OPEN
ש ני הראשונים מתייחסים לניטובים אשר יש להסיר מטבלת הניתוב ושני האחראונים מתייחסים אל הניטובים שיש להוסיף אל טבלת הניתוב.	Unfeasible Route Length, Withdrawn Routes, Path Attributes, NLRI.	UPDATE
הודעת שגיאה, הودעה זו גורמת לסגירת TCP session בין שני נתבים.	Error Code, Error Subcode, Data	NOTIFICATION
נשלחות כל 60 שניות בכדי לשמור על קשרי השכנות.		KEEPALIVE
לאחר שינוי קונפיגורציה מבוצע reset תוכנות לתהליך ה – BGP מול השכן הרלוונטי, מטרת ההודעה היא ליזום תהליך זהה בנתב השכן.		ROUTE REFRESH

תהליך הקמת יחס שכנות

BGP FSM (Finite State Machine)

במהלך עבודה מול שכן, ישנו שיישם מצבים בהם ייצא ה קישור.

Idle – לא קיים קשר עם אף שכן, תישלח הודעה SYN וכמו כן תעשה האזנה לבקשת SYN משבכים פוטנציאליים בפורט 179 עם מנת ליצור תקשורת TCP.

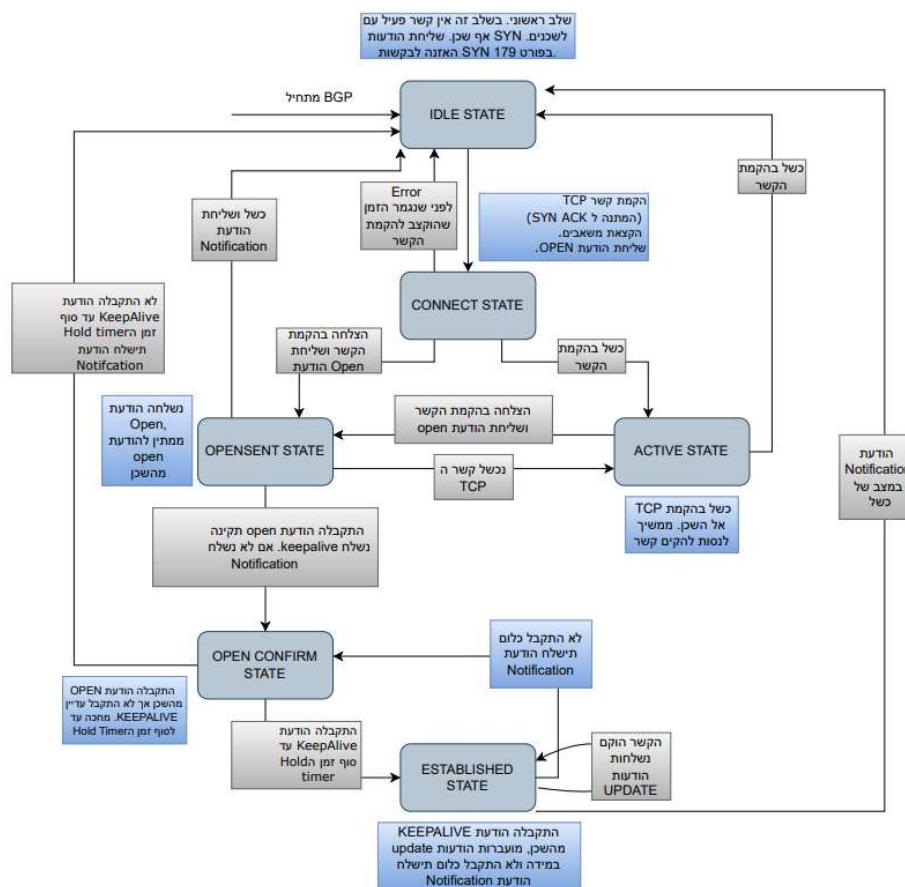
– בשלב זה מוקדם קשר TCP נשלחת הודעה OPEN – Connect

Active – שלב זה מתאר מצב בו כשל תהליכי הקמת קשר TCP עם השכן, הנטב ינסה להקים את הקשר מחדש. אם הקשר הוקם, הנטב ישלח הודעה OPEN. אם הקמת הקשר כשל, נחזור לשלבIdle.

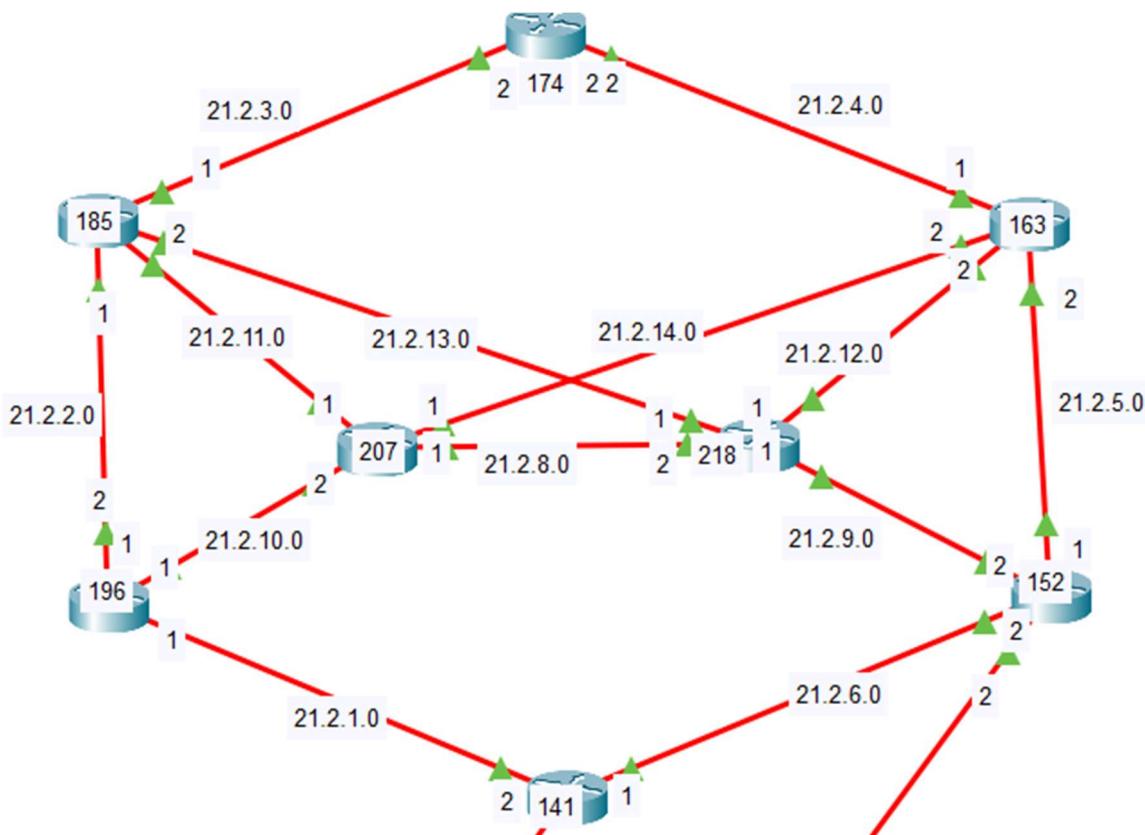
– Open sent – בשלב זה נשלחה הודעה OPEN אך עדין לא התקבלה הודעה OPEN מהשכן. כאשר הודעה מתתקבלת, תיבדק תקינותה. אם היא תקינה תישלח הודעה Keep Alive, במידה ולא תקינה תישלח הודעה Notification.

– Open Confirm – בשלב זה התקבלה הודעה OPEN מהשכן אך לא התקבלה הודעה KEEP ALIVE. אם לא התקבלה הודעה זו בזמן המוקצב בHold, חוזרים לשלב ההתחלה,Idle.

– Established – בשלב זה התקבלה הודעה KEEPALIVE מהשכן וMOVEBRWOT הודעות UPDATE. במצב של כשל נשלחת הודעה Notification.



הגדרת טבעת BGP



הגדרת כתובות לממשקים

```
Router(config)#int gigabitEthernet 0/1/0 ← כנישה לממשק
Router(config-if)#ip address 21.2.6.1 255.255.255.0 ← נתינת כתובות IP
```

הגדרת יחס שכנות עם הנתבים המוחברים לשירות

```
Router(config)#router bgp 163 ← 163 AS עם BGP
Router(config-router)#nei
Router(config-router)#neighbor 21.2.4.2 remote-as 174 ← יצרית שכנות עם ראיון
Router(config-router)#neighbor 21.2.5.1 remote-as 152
Router(config-router)#BGP-5-ADJCHANGE: neighbor 21.2.5.1 Up

Router(config-router)#neighbor 21.2.12.1 remote-as 218
Router(config-router)#neighbor 21.2.14.1 remote-as 207
```

פריטום הרשותות המחויבורות לשירות לנット

```
Router(config-router)#network 21.2.4.0 mask 255.255.255.0
Router(config-router)#network 21.2.5.0 mask 255.255.255.0
Router(config-router)#network 21.2.12.0 mask 255.255.255.0
Router(config-router)#network 21.2.14.0 mask 255.255.255.0
```

: show commands

show ip route

```
Router#show ip route
Codes: L - local, C - connected, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      21.0.0.0/8 is variably subnetted, 24 subnets, 2 masks
B   21.2.1.0/24 [20/0] via 21.2.2.2, 00:00:00
C   21.2.2.0/24 is directly connected, GigabitEthernet0/1/0
L   21.2.2.1/32 is directly connected, GigabitEthernet0/1/0
C   21.2.3.0/24 is directly connected, GigabitEthernet0/0/0
L   21.2.3.1/32 is directly connected, GigabitEthernet0/0/0
B   21.2.4.0/24 [20/0] via 21.2.3.2, 00:00:00
B   21.2.5.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.6.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.7.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.8.0/24 [20/0] via 21.2.11.1, 00:00:00
B   21.2.9.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.10.0/24 [20/0] via 21.2.11.1, 00:00:00
C   21.2.11.0/24 is directly connected, GigabitEthernet0/3/0
L   21.2.11.2/32 is directly connected, GigabitEthernet0/3/0
B   21.2.12.0/24 [20/0] via 21.2.13.1, 00:00:00
C   21.2.13.0/24 is directly connected, GigabitEthernet0/2/0
L   21.2.13.2/32 is directly connected, GigabitEthernet0/2/0
B   21.2.14.0/24 [20/0] via 21.2.11.1, 00:00:00
B   21.2.15.0/24 [20/0] via 21.2.2.2, 00:00:00
B   21.2.16.0/24 [20/0] via 21.2.2.2, 00:00:00
B   21.2.17.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.18.0/24 [20/0] via 21.2.2.2, 00:00:00
B   21.2.19.0/24 [20/0] via 21.2.13.1, 00:00:00
B   21.2.22.0/24 [20/0] via 21.2.2.2, 00:00:00
```

show ip bgp neighbors

```

Router#show_ip_bgp_neighbors
BGP neighbor is 21.2.3.2, remote AS 174, external link
  BGP Version 4, remote router ID 21.2.4.2
  BGP state = Established, up for 00:37:04
  Last read 00:37:04, last write 00:37:04, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

      Sent          Rcvd
  Opens:           8          8
  Notifications:  7          0
  Updates:        767        417
  Keepalives:     259        252
  Route Refresh:  0          109
  Total:          1041       786

Default minimum time between advertisements runs is 30 seconds
  
```

מי השכן ובאייזה AS נמצא

הגרסת ה BGP id של השכן

שנשלחו והתקבלו

סוגי הודעות

show ip bgp summary

```

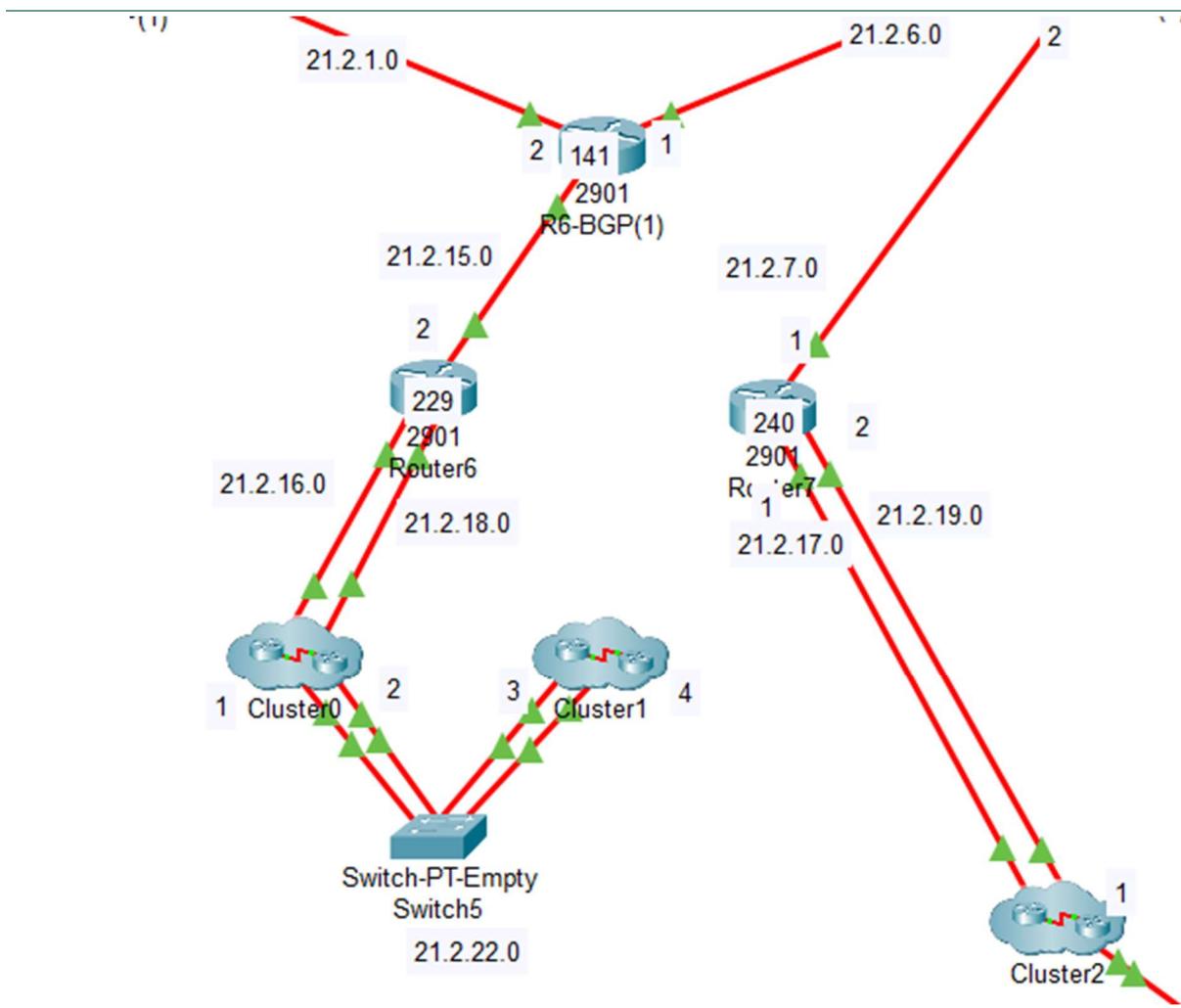
Router#show ip bgp summary
BGP router identifier 21.2.13.2, local AS number 185
BGP table version is 725, main routing table version 6
77 network entries using 10164 bytes of memory
77 path entries using 4004 bytes of memory
73/64 BGP path/bestpath attribute entries using 12604 bytes of memory
8 BGP AS-PATH entries using 192 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 26996 total bytes of memory
BGP activity 20/0 prefixes, 77/0 paths, scan interval 60 secs

  
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
21.2.3.2	4	174	678	275	725	0	0	00:38:01	4
21.2.11.1	4	207	1374	277	725	0	0	00:38:01	4
21.2.13.1	4	218	1867	278	725	0	0	00:38:01	4
21.2.2.2	4	196	1063	277	725	0	0	00:38:01	4

שכנים	גרסת	AS	הודעות	הודעות	זמן שכנות
BGP	BGP	שנתkov	שנתkov	שלחת	
שלחת					

הגדלת Static Route , DSR ,ISP בסניפים

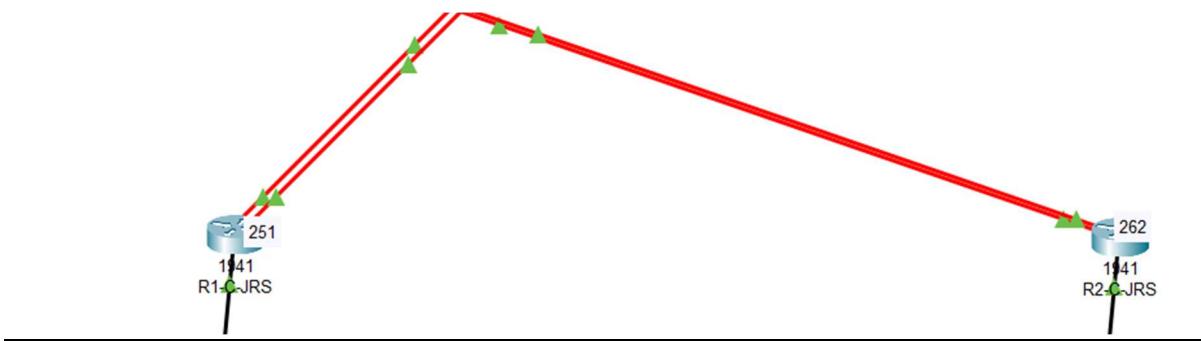


הסניף הראשון והשלישי מחוברים ישירות ל-ISP שונים המוחברים לטבעת BGP. חיבור נפוץ בין מדינות שונות ולפעמים ערים שונות. בפרויקט זה השתמש בסוג חיבור זה על מנת לחבר את הסניף הראשון (ירושלים) ואת הסניף השלישי (יונן) הנמצאים ב-2 מדינות שונות. את חיבור הסניף השני (תל אביב) אראה בהמשך.

מהסניפים לכיוון ISP נגדיר Default Static Route

מחסניפים לכיוון ISP נגדיר static route

ב森יף הראשון:



: הגדרת default route לכיון ISP

```
R1-C-JRS(config)#ip route 0.0.0.0 0.0.0.0 21.2.16.1
```

```
R2-C-JRS(config)#ip route 0.0.0.0 0.0.0.0 21.2.18.1
```

מכיוון שמוגדר על ראותרים אלו גם OSPF וגם ניתוב סטטטי נבצע redistribute

: הגדרת ISP Default route מההטבעת BGP

```
ISP1(config)#ip route 0.0.0.0 0.0.0.0 21.2.15.1
```

הגדרת ניתוב סטטי מהרואוטר המחבר בטעעת BGP אל הסניף הראשון :

```
BGP-141(config)#ip route 21.2.16.0 255.255.255.0 21.2.15.2  
BGP-141(config)#ip route 21.2.18.0 255.255.255.0 21.2.15.2
```

redistribute

פקודה המאפשרת שילוב של כמה פרוטוקולי ניתוב.

כאשר יש שילוב של פרוטוקול ניתוב דינامي וסטטי, ניכנס לניתוב הדינامي ונגידיר בו redistribute לסטטי.

כאשר יש שילוב בין שני פרוטוקולי ניתוב דינאמיים. נגידיר redistribute בשני פרוטוקולי הניתוב.

מכיוון שהרואוטר המחבר בטעעת BGP פועל גם BGP וגם הגדרכנו ניתוב סטטי, נגדיר redistribute, על מנת שיוכלו לנtab בין הרשותות של הסניפים אל טופולוגיה הkgbg.

```
BGP-141(config)#router bgp 141  
BGP-141(config-router)#redistribute static
```

בסניף השלישי



הגדרת default route מהרoutersים בסניף לכיוון ISP :

```
R1-GRC(config)#ip route 0.0.0.0 0.0.0.0 21.2.17.1
```

```
R2-GRC(config)#ip route 0.0.0.0 0.0.0.0 21.2.19.1
```

מכיוון שהוגדרו על הרouterים גם OSPF על מנת לנtab בתוכה הסניף וגם ניתוב סטטטי לכיוון ISP , נבצע redistribute

פקודת redistribute static שnantב את הניתובים הסטטטיים שהוגדרו עליו, אך אינה משתפת כברירת מחדל ניתובים דיפולטיבים. (0.0.0.0). על מנת שהnantb יוכל לשtab ניתוב דיפולטיבי נגדיר default-information originate

```
R1-GRC(config)#router ospf 1
R1-GRC(config-router)#redistribute static subnets
R1-GRC(config-router)#default-information originate
```

```
R2-GRC(config)#router ospf 1
R2-GRC(config-router)#redistribute static subnets
R2-GRC(config-router)#default-information originate
```

הגדרת ISP אל הטבעת BGP Default route

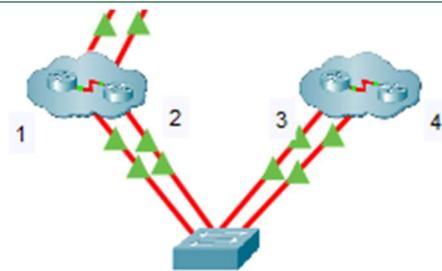
```
ISP2(config)#ip route 0.0.0.0 0.0.0.0 21.2.7.2
```

הגדרת ניתוב סטטי מהrouter המחבר בטבעת BGP אל הסניף השלישי :

```
BGP-152(config)#ip route 21.2.17.0 255.255.255.0 21.2.7.1
BGP-152(config)#ip route 21.2.19.0 255.255.255.0 21.2.7.1
```

היות ועל ראותך זה מוגדרים גם BGP ונתוב סטטטי, נעשה redistribute

```
BGP-152(config)#router bgp 152
BGP-152(config-router)#redistribute static
```



21.2.22.0

חיבור זה נפוץ לרוב בחיבור בין ערים שונות הנמצאות באותו מדינה.

בחיבור זה הראוטרים מחוברים לסוויץ כלומר הראוטרים ב-2 הסניפים מחוברים וחולקים רשת אחת משותפת. בנוסף גדר OSPF ונשף את הרשות הפנימיות ואת הרשות המשותפת, מה שיגרום לכך שכל הנטבים וMLS בשני הסניפים מכירים את הרשות הפנימית אחת של השניה ויכולים לתקשר ביניהם ללא צורך בנתם עליו ארכיב בהמשך.

21.2.22.1	R1-JRS
21.2.22.1	R2-JRS
21.2.22.1	R1-GRC
21.2.22.1	R2-GRC

גדר את הכתובות על הראוטרים

```
R1-C-TLV(config)#interface GigabitEthernet0/0/0
R1-C-TLV(config-if)#ip address 10.5.22.3 255.255.255.0
```

גדר OSPF על הראוטרים ונפרנס את הרשות המשותפת

```
R1-C-JRS(config)#router ospf 110
R1-C-JRS(config-router)#router-id 17.11.11.11
R1-C-JRS(config-router)#network 21.2.16.0 0.0.0.255 area 0
R1-C-JRS(config-router)#network 10.5.22.0 0.0.0.255 area 0
```

על מנת שהניתוב הדיפולטיבי לכיוון ISP יעבור גם לטניף השני, נוסיף הראוטרים בסניף הראשון שישתפו את ה- DSR ב프וטוקול זה, נוסף ינשיף

```
R1-C-JRS(config)#router ospf 110
R1-C-JRS(config-route)#redistribute static subnets
R1-C-JRS(config-router)#default-information originate
```

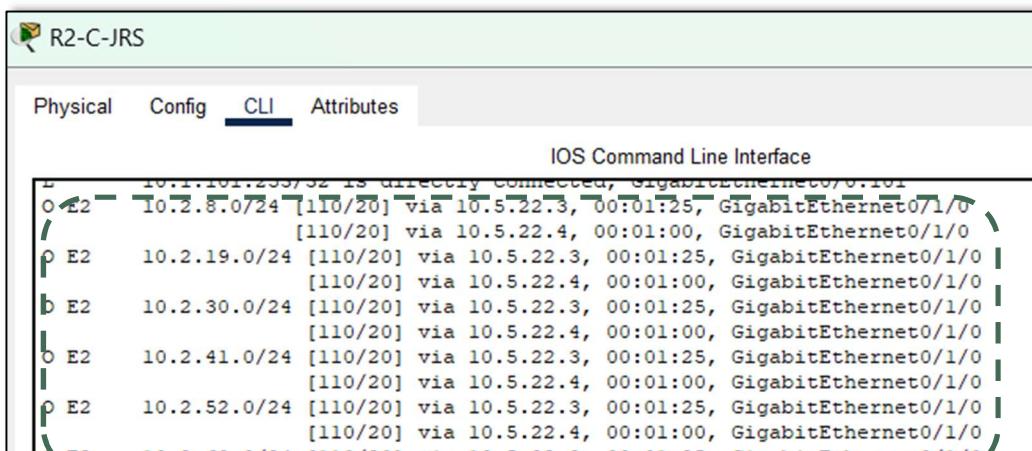
```
R2-C-JRS(config)#router ospf 110
R2-C-JRS(config-router)#redistribute static subnets
R2-C-JRS(config-router)#default-information originate
```

יתר על כן נרצה שהראוטרים בסניף הראשון יכירו את הרשותות הפנימיות של הסניף השני על מנת שיידעו להעביר אליהם פאקטות. בסניף השני מידע זה מיותר להיות ומוגדר DSR שהועבר מהסניף הראשון ולכון לכל כתובת שאינה בסניף, הפקטה תעבור דרך המטרו. נוסף redistribute בין פרוטוקול OSPF של המטרו לבין פרוטוקול EIGRP המוגדר בסניף השני

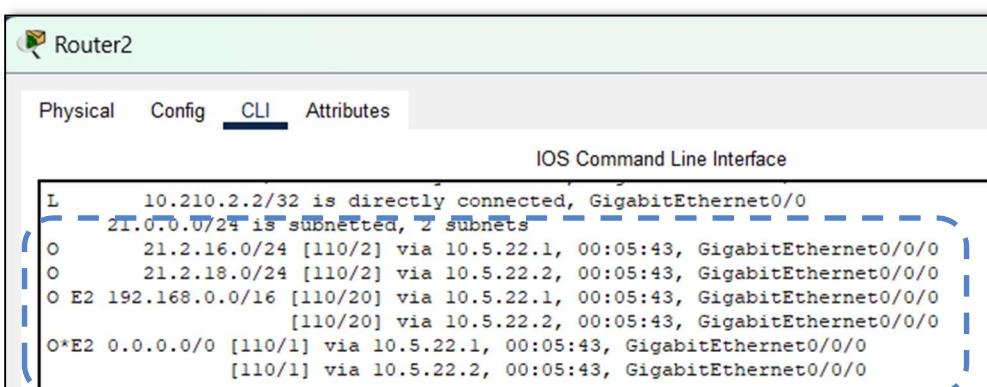
```
R1-C-TLV(config)#router ospf 110
R1-C-TLV(config-router)#redistribute eigrp 100 subnets
R1-C-TLV(config-router)#exit
R1-C-TLV(config)#router eigrp 100
R1-C-TLV(config-router)#redistribute ospf 110 metric 1 1 1 1 1
```

נבדוק ב show ip route

סניף ראשון : נראה את הרשותות הפנימיות של הסניף השני



סניף שני : נראה ניתוב סטטי



ברשותה המקומית אנו משתמשים בכתובות פרטיות על מנת לתקשר בין רכיבים ומשתמשים ברשות. כמוות הכתובות הקיימות הינה מוגבלת ולכן היתרון בכתובות פרטיות הינה שהן לא ייחודיות לכל רכיב בעולם. ככלומר יכול להיות כפליות בכתובות אלו, כל עוד אין נמצאות באותה רשות מקומית. אך לא ניתן לצאת עם כתובות אלו החוצה, מכיוון שעקב הcpfilioות בכתובות אלו בעולם הרכיבים ברשות החיצונית אין ידוע לאן לנtab את המידע. לכן ברשות החיצונית נשתמש בכתובות חיצונית, שלאו כתובות ייחודיות ברשות שאין ניתנות לשימוש כפול והן נועדו על מנת לנtab ברשות החיצונית.

פרוטוקול NAT נועד על מנת להמיר בין הכתובות הפנימיות אל הכתובות החיצונית על מנת שהרכיבים ברשות המקומית יוכל לנtab החוצה אל הרשות החיצונית.

פרוטוקול NAT:

פרוטוקול המשמש להמרה בין כתובות IP פנימיות לחיצונית וההפק. הסיבה העיקרית לשימוש הינה על מנת לאפשר לרכיבים ברשות הפנימית לתקשר עם רכיבים אשר אינם נמצאים איתם באותו רשות, ככלומר ברשות הרחבה.

מגדירים את פרוטוקול NAT על הראوتر המחבר גם לרשות הפנימית וגם לכיוון ISP. כאשר פקטה מגיעה מהרשות הפנימית והיעד שלה נמצא ברשות החיצונית, פרוטוקול NAT יdag להמיר את כתובות IP הפנימית שלו רכיב פנימי אל כתובות IP חיצונית, וכך אשר פקטה מגיעה מהרשות החיצונית אל הפנימית, יdag להמיר את הכתובות החיצונית לפנימית.

יתרונות:

- חיסכון בכתובות ציבוריות
- פרטיות – כתובות IP הפנימית של אותו רכיב תהיה מוסתרת ואינה תצא אל האינטרנט
- יישום כתובות IP לפי פרוטוקול גלובלי

כתובות NAT:

כתובת IP הפנימית שהוגדרה על הרכיב הפנימי. הכתובת שתומר על ידי הפטוקול.
כתובת IP הציבורית אליה הכתובת הפרטיה תומר, כאשר הפקטה תצא אל הרשת הרחבה.

כתובת IP הציבורית של היעד

כתובת IP הפרטיה של היעד

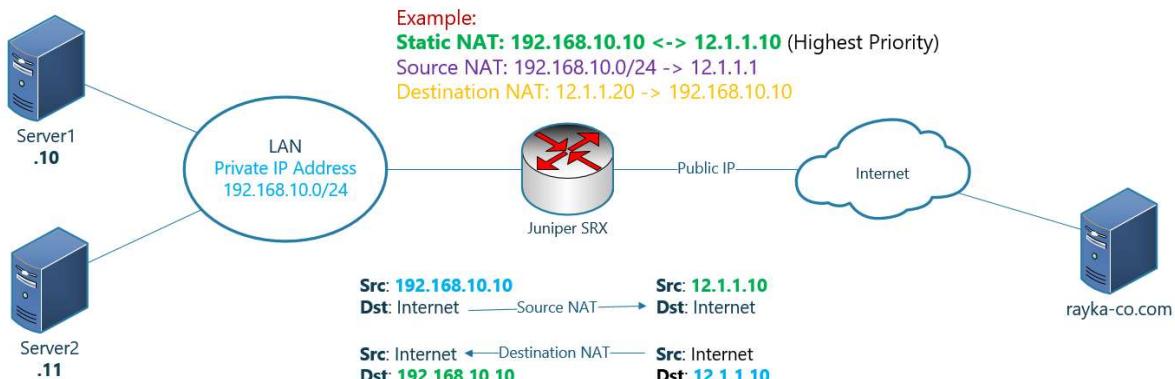
סוגי NAT:

קיים שלושה סוגים של NAT:

Static Nat

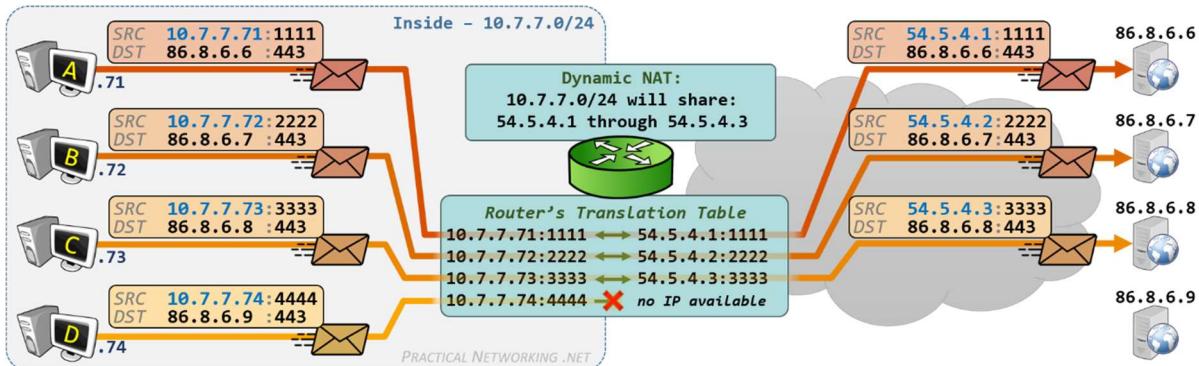
לכל כתובת פנימית יש כתובת חיצונית משלה שמייצגת אותה (One-to-One)
לא משומש בארגונים מכיוון שהכל ארגון קיימים מכשירים רבים, בשיטה זו חייב לכל כתובת פנימית
תהיה כתובת חיצונית מיוצגת, אך אם יש 50 מחשבים צריך לפחות 50 כתובות IP, כתובות חיצונית
מאוד יקרות וכן שיטה זו לא יעילה.

Static NAT



Dynamic NAT

בשיטת זו יש מאגר של ציבוריות. הרכיבים מקבלים כתובת חיצונית מתחום המאגר, כל כתובת IP עדין
משתמשת רקבי אחד בכל פעם. כלומר, אם קיימים 3 כתובות IP 3 רקבים בכל פעם יוכל לצאת החוצה
אל הרשת המקומית ושאר הרכיבים יאלצו להcorractsות מהרכיבים המשמשים בכתובת החיצונית יסימנו את
הession שלהם. כלומר הם לוקחים לפי זמינות של הכתובת הציבורית. אם יש מחשב שצריך כתובת
אבל אין כתובת פנوية הוא ייכה עד שמחשב יסימן עם הכתובת שלו ואז יקח אותה. החבילה תישמט
והרכיב לא יוכל לצאת אל האינטרנט עד שתכתובת מהמאגר תתפנה. משתמשים בשיטה זו כאשר מספר
המשתמשים קבוע אך שיטה זו עדין יקרה בעקבות כך שהארגון עדין יצרך לפחות כמה כתובות IP
חיצונית שכן יקרות מאוד.

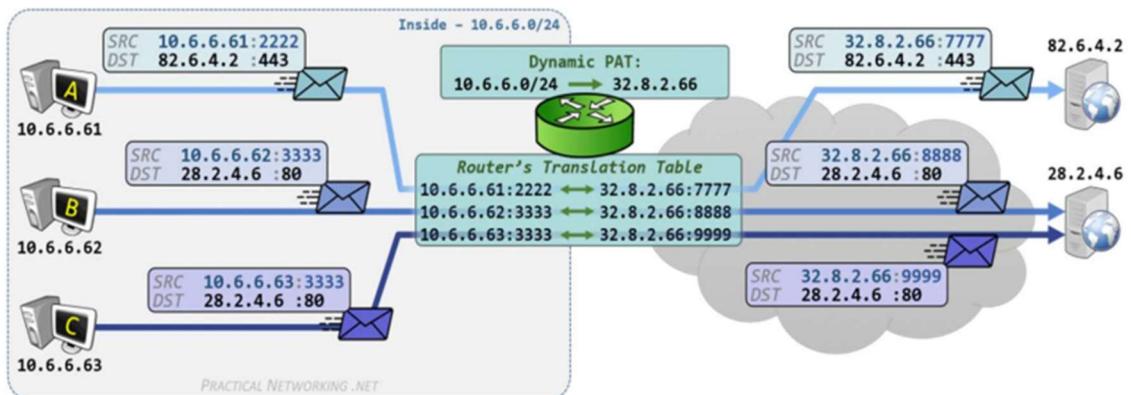


PAT (Port Address Translation) / NAT Overload

בשיטת זו כל הרכיבים ברשת הפנימית יוצאים עם כתובת חיצונית אחת. הרכיבים הפנימיים נבדלים זה מזה על ידי מספר פורט ייחודי עבור כל זרימה של תקשורת, כאשר ניתו להשתמש ב-65535 פורטים בו זמנית. ככלומר יש צורך רק בכתובת אחת עבור מספר גדול של רכיבים. שיטה יעילה ופחות יקרה.

המחשבים נבדלים לפי ה-`port` שלהם `src` שנitinן רנדומלית על ידי המחשב והוא בין 0-48000-64000. כאשר מגיעה פקודה לראוטר `laddr`, הראוטר ישמר את הפורט הפנימי בטבלה.

מה אם 2 המכשירים בחרו את אותו `sport`? מנגנון `laddr` לטפל בכך, הוא משנה את הפורט של השני ויעדכו אצלו לאחד ה포רטים הפנויים כדי שיוכלו לצאת לאינטרנט.



על מנת לאפשר תקשורת בין הסביבים נשתמש ב-NAT Overload (השיטה השלישית), על מנת להמיר את הכתובות הפנימיות לחיצניות והחפק.

נדיר מהם הממשקים הפנימיים והמשקיקים החיצוניים. יתר על כן נגדיר רשיימת גישה התאפשר לרשותו לצאת עם NAT.

הגדרת NAT

גדר בסניף הראשון והשלישי

נגיד את הממשקים של ה-`vlans` ה-`inside` (בשיניפ' הראשון נגידר גם על הממשק לכיוון המטרו לשיניפ' השני) :

```
R1-C-JRS(config)#int gigabitEthernet 0/0.26
R1-C-JRS(config-subif)#ip nat inside
R1-C-JRS(config-subif)#exit
R1-C-JRS(config)#int gigabitEthernet 0/0.37
R1-C-JRS(config-subif)#ip nat inside
R1-C-JRS(config-subif)#exit
```

כניסה למשק nat inside

נגידר את הממשקים היוצאים לכיוון ISP כ NAT Outside :

```
R1-C-JRS(config)# int gigabitEthernet 0/0/0
R1-C-JRS(config-if)# ip nat outside
R1-C-JRS(config-if)# int gigabitEthernet 0/1/0
R1-C-JRS(config-if)# ip nat outside
```

כניתה לממשק הגדרת nat outside

יצור ACL מורחב שיאפשר מעבר של כתובות:

```
R1-C-JRS(config)#ip access-list extended ACL-NAT  
R1-C-JRS(config-ext-nacl)#permit ip any any
```

יצירת ACL

אפשרות לכלל הכתובות

נחיל את ה NAT Overload על המושקים החיצוניים :

```
R2-C-JRS(config)# ip nat inside source list ACL-NAT interface gigabitEthernet0/0/0 overload  
R2-C-JRS(config)# ip nat inside source list ACL-NAT interface gigabitEthernet0/1/0 overload
```

Show commands:

:show ip nat translation

R1-C-JRS#show ip nat translations				
Protocol	Inside global	Inside local	Outside local	Outside global
icmp	21.2.22.1:1	10.1.26.1:1	21.2.1.2:1	21.2.1.2:1
icmp	21.2.22.1:2	10.1.26.1:2	21.2.1.2:2	21.2.1.2:2
icmp	21.2.22.1:3	10.1.26.1:3	21.2.1.2:3	21.2.1.2:3
icmp	21.2.22.1:4	10.1.26.1:4	21.2.1.2:4	21.2.1.2:4
icmp	21.2.22.1:5	10.1.26.1:5	21.2.1.2:5	21.2.1.2:5

הכתובת החיצונית אליה נתרגם	הכתובת הפנימית של המארח	הכתובת של היעד	הכתובת החיצונית של היעד
----------------------------	-------------------------	----------------	-------------------------

Show ip nat statistics

```
R1-C-JRS#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0/0 ממשק outside
Inside Interfaces: GigabitEthernet0/1/0 , GigabitEthernet0/0.26 , GigabitEthernet0/0.37 ,
                  GigabitEthernet0/0.48 , GigabitEthernet0/0.59 , GigabitEthernet0/0.70 , GigabitEthernet0/0.81 ממשקים inside
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
```

הגדרת חיבור מנקודה לנקודה על פני הרשת. הוא משתמש ב프וטוקול Tunnel על מנת לכלול סוגים שונים. הוא מאפשר שימוש בפרוטוקולים שלרבות אינם נתמכים ברשת על ידי כך שוטף את פרוטוקולים אלו בפרוטוקולים שנתמכים. משתמשים בGRE על מנת לאפשר להוסטים ברשנות הפנימיות שונות באיזורים גיאוגרפיים שונים לתקשר זה עם באמצעות הכתובות הפנימיות שלהם.

כasher המנהרה מוגדרת, המעבר בין הנטים מופיע כקפיצה אחת מרשת אחת לרשת שנייה, זאת למרות שנמצאים באיזורים שונים והחיבור עברת כמות גדולה יותר של נטים על מנת להגיע אל היעד.

דרך פעולה : GRE

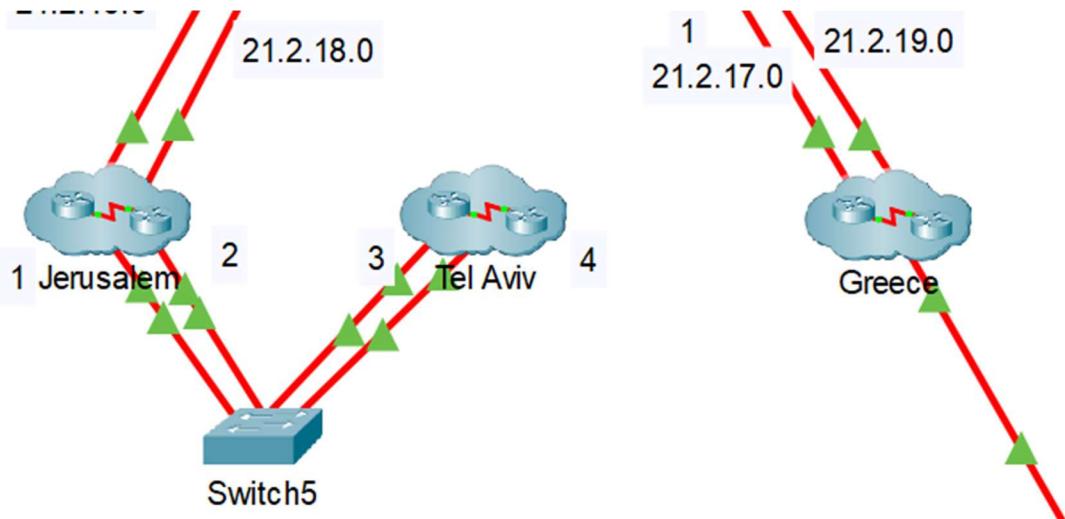
התעלה עשויה פעולה encapsulation, בכך שעוטפת את הפקטה המקורית בתוך IP Header חדש אשר ישמש בהמשך לניטוב של הפקטה ברשת החיצונית. Payload

המנירה עשויה לטעורה מסוג Broadcast ו Multicast שאינם יכולים לעבור בראשת החיצונית, וממיר אותם ל Unicast. כאשר הטעורה מגיעה לידע, נעשו פעולה decapsulation אשר מורידה את Tunnel Header, ומחזירה את הטעורה לטעורה מסוג multicast ו Broadcast.

לשימוש ב gre tunnel קיים חסרון : הטעורה אשר עברת בתוך התעלת אינה מוצפנת, היא עברת טקסט נקי ולא מוצפן. לכן נעשה בפרויקט זה שימוש ב gre ולביש אותו על תעלת VPN עליו אסביר בהמשך.

הVPN אינו שולח הודעות מסוג Broadcast ו Multicast, אלא שולח הודעות Unicast, מוצפנות, לעומת זאת GRE אשר שולח הודעות Multicast ו Broadcast לא מוצפנות.

הגדרת GRE Tunnel



:GRE מנהרות 2

- בין R1-GRC ל R1-JRS
- בין R2-GRC ל R2-JRS

ניצור משקדים למנחרות, ניתן כתובות IP פנימיות לכל קצה שכשהמקור והיעד יהיה הכתובות החיצונית של הנטבים (במקור נבחר במשק שפונה לפני חוץ וביעד ניתן את הכתובת החיצונית של הנטב שבסניף האחר). לבסוף נגידר את המנהרה כ – GRE .

כתובת	S.M	רשת	רכיב	
172.16.1.2	255.255.255.0	172.16.1.0	R1-C-JRS	Tunnel ראשוני
172.16.1.1			R1-C-GRC	
172.16.2.2	255.255.255.0	172.16.2.0	R2-C-JRS	Tunnel שני
172.16.2.1			R2-C-GRC	

הגדרת Tunnel 1

ב : R1-C-JRS

יצירת ממשק למנהרה

```
R1-C-JRS(config)# interface Tunnel0
```

שיוך כתובת IP לממשק

```
R1-C-JRS(config-if)# ip address 172.16.1.2 255.255.255.0
```

שיוך המנהרה – הממשק היוצא עם הכתובת החיצונית

```
R1-C-JRS(config-if)# tunnel source GigabitEthernet0/0/0
```

יעד – הכתובת החיצונית של הצד השני

```
R1-C-JRS(config-if)# tunnel destination 21.2.17.2
```

R1-C-GRC ב

יצירת ממשק למנהרה

```
R1-GRC(config)# interface Tunnel0
```

שיוך כתובת IP לממשק

```
R1-GRC(config-if)# ip address 172.16.1.1 255.255.255.0
```

שיוך המנהרה – הממשק היוצא עם הכתובת החיצונית

```
R1-GRC(config-if)# tunnel source GigabitEthernet0/0/0
```

יעד – הכתובת החיצונית של הצד השני

```
R1-GRC(config-if)# tunnel destination 21.2.16.2
```

הגדרת המנהרה GRE (בשני הצדדים את הפקודה)

```
R1-GRC(config-if)# tunnel mode gre ip
```

show commands

Show interfaces tunnel 0 -

show ip interface brief -

נעsha בדיקת ping ו traceroute – לבודיקת קישוריות במנהרה.

show int tunnel 0

```
R1-GRC#show interfaces tunnel 0
Tunnel0 is up, line protocol is up (connected) | המנהרה פועלה
Hardware is Tunnel,
Internet address is 172.16.1.1/24
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255 כימוס אקטואות במנהרה
[Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source [21.2.17.2 (GigabitEthernet0/0/0)], destination [21.2.16.2] מוקור המנהרה ממושך ויעד
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
```

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.3.11.1	YES	NVRAM	up	up
GigabitEthernet0/1	unassigned	YES	NVRAM	administratively down	down
GigabitEthernet0/0/0	21.2.17.2	YES	NVRAM	up	up
Tunnel0	172.16.1.1	YES	manual	up	up

מצב הפתוטזוקול | , האם יכולה
לשלוח ולקבל אקטואות
פינג בין 2 צדי המנהרה

```
R1-C-JRS#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Traceroute

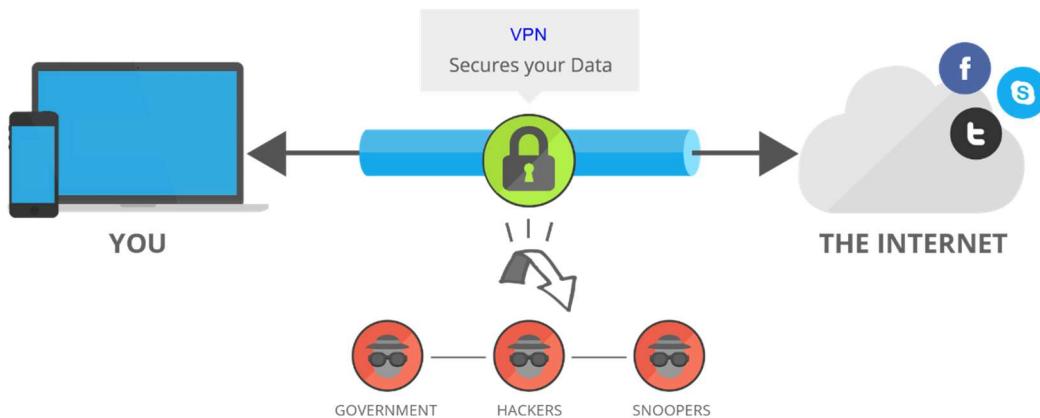
```
R1-C-JRS#traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
1 172.16.1.1 0 msec 0 msec 0 msec | עבר דרך המנהרה – קפיצה אחת
R1-C-JRS#
```

Virtual Private Network

VPN היא טכנולוגיה אשר יוצרת חיבור מוצפן ומאובטח בין איזורים שונים על גבי רשת שפתוחה מאובטחת כגון רשת האינטרנט. השימוש בVPN נעשה על מנת לקשר רשתות פנימיות שונות מרוחקות, ככלומר מחוברות דרך איזוריים חיצוניים, זאת על ידי רשת "פרטית וירטואלית". משתמשים בVPN על גבי פרוטוקולי מנהור כגון GRE על מנת ליצור חיבור מאובטח.

תעבורה VPN

VPN מרחיב את הרשת הפנימית על ידי חיבור על גבי תעלת דרך האינטרנט. בעקבות כך שהתקשורת מוצפנת בין המכשיר לבין הרשת, היא תישאר מוצפנת גם בזמן העברה.



יתרונות VPN:

- אין גבלה מבחינה גיאוגרפית
- אונונימיות מסופקת
- אבטחה והגנה מפני מתקפות סייבר
- מניעה של חסימות רוחב פס
- יכולת לעקוף Firewall

חסרונות:

- מהירות העברה נמוכה יותר
- לעיתים נ필ת חיבור בעת החיבור לVPN
- מורכב להגדרה

סוגי VPN:

Site-to-Site VPN

חיבור מסווג Site to site מאפשר לרשותות פנימיות במקומות מרוחקים לשתף ביניהם משאבים וلاتקשר כרשת אחת. משמש לדוגמה לחבר סניפים מרוחקים בארגון אשר צריכים לגשת לרשות הארגון ולהשתמש בה ולקחת ממנה מידע.

בשיטת זו מגדירים Tunnel VPN בין שתי נקודות קצה

מצבי מנוט ה IP ,Tunnel : Transport

- תעבורת (Transport) – המידע בתוך החבילה מוצפן אך ניתן לראות את כתובות ה IP המקורית לא מוצפנת
- מנהרה (Tunnel) – המידע בתוך כל חבילה מוצפן ובנוסף, ה IP Header מוצפן גם הוא

קיימים מספר דרכים להגדרת Site to Site VPN. בפרויקט שלנו נגידר את ה GRE על גבי תעלת

IKE (Internet Key Exchange)

IKE הינו פרוטוקול משא ומתן אשר מאפשר לשני מארכחים שונים לבצע אימוט. הוא מופרד לשני שלבים
שוניים : Phase1 ,Phase2 .
ביצוע אימוט אוטומטי לשני הצדדים . SA (Security Association)

IKE Phase1/ ISKAMP

מטרתו העיקרית של שלב זה היא לאמת את המארחים ולהקם עורך מוצפן ומאובטח אשר ישמש את המארחים בניהול המשא ומתן בשלב 2 אשר עליו יורח במשך. לאחר שלב 1 מסתיים, עברו המארחים אל שלב 2. לא ניתן להתחיל את שלב 2 במידה ושלב 1 כושל.

שלב 1 מבצע את הפונקציות הבאות :

ביצוע משא ומתן על מדיניות IKE זהה בין המארחים

	Parameter	Value
IKE	HASH	SHA2-256 (default), SHA1, MD5, SHA2-384 and SHA2-512.
	Authentication	PSK / RSA.
	Encryption	AES-128 , AES-192, AES-256 and 3DES.
	Diffie-Hellman Group	14, 1, 2, 5, 19, 20 באזורי מסויימים רק 2 – 15 ,14 Group
	Lifetime (s)	86400 (default) Unit: second Value range: 60 - 604800

- ניהול מפתחות (Key Management)

פרוטוקול Diffie-Hellman הינו פרוטוקול שיתוף המפתח הראשון. אלגוריתם זה מאפשר לשני מארחים שלא נפגשו מעולם ליצור מפתחות סימטריים בצורה מאובטחת על מנת לאבטח את התקשרות בין שני הצדדים. הוא יוצר מפתחות סימטריים בצורה דינמית אשר ישמשו להצפנה המידע. יתר על כן, הוא משמש להחלפה מאובטחת של מפתחות.

הגדרת מנהרה על מנת לבצע משא ומתן בשלב 2

ביצוע Authentication בין הצדדים. כל אחד מהמחשרים מספק מזהה שלב 1 אשר יכול להיות שם התחום, כתובת IP וכדומה. ההגדרה של VPN בכל מכשיר מצינית את המזהה שלב 1 של כל מכשיר מקומי מרוחק. ההגדרות בשני הצדדים חייבות להיות תואמות.

IKE Phase 2 / IPsec SA Tunnel

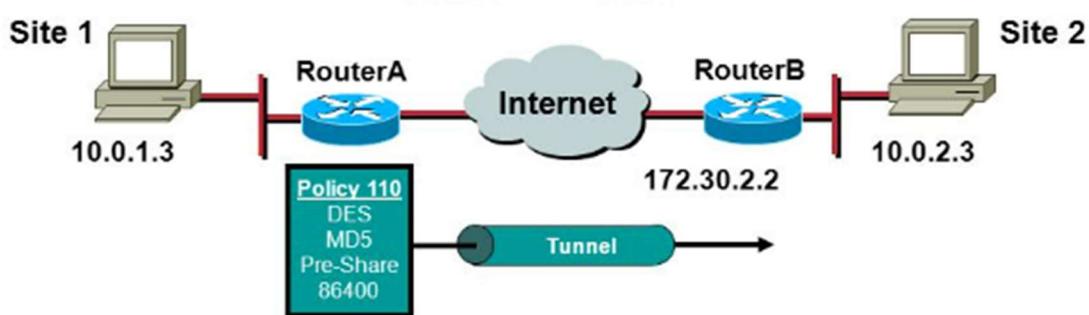
מטרת שלב זה הינה לנהל משר ומתן על הקמת מנהרה. למעשה, קבוצה של פרטי תעבורת שאומרים לממשר Aiזו תעבורת לשולח דרך VPN – וכי怎ה להצפין ולאמתת תעבורת זו. ביצוע משא ומתן על פרמטרים אלו

IPsec SA	Parameter	Value
	HASH	SHA2-256 , SHA1, MD5, SHA2-384 and SHA2-512.
	Encryption	AES-128 , AES-192, AES-256 and 3DES.
	PFS / D-H Group	14 , 1, 2, 5, 19, 20 באזורי מסויימים רק ב- 15 ,14 Group – 2 זמינים.
	Lifetime (s)	3600 (default) Unit: second Value range: 480 - 604800

הפרמטרים בשני הצדדים חייבים להיות זהים פרט לערך **Lifetime**.

Crypto ACL

על מנת להגדיר איזה תובורה נרצה שיüber בVPN, אילו רשות ופרוטוקולים יעברו ואיזה לא, נוצר רשימת גישה. כל מידע שיüber תחת הכללים המאפשרים העברת של מידע יוצפן ויועבר דרך VPN.



Remote Access VPN

SSL (Secure Sockets Layer) VPN

מאפשר למשתמשים לגשת מרוחק אל הרשות של הארגון. מספק תקשורת בטוחה באמצעות חיבור מוצפן לכל סוג המכשירים, ללא קשר אם הגישה היא דרך הרשות הציבורית או רשות מאובטחת אחרת. כל התעבורה באינטרנט אל המכשיר נעשו בצורה מוצפנת על ידי פרוטוקול SSL או TLS. המשתמשים אינם צריכים לבחור באיזה פרוטוקול להשתמש, ה – VPN SSL משתמש בפרוטוקול ההצפנה החדש והמעודכן ביותר שהותקן על הדפדפן של המשתמש.

קיימות 2 סוגי של VPN :

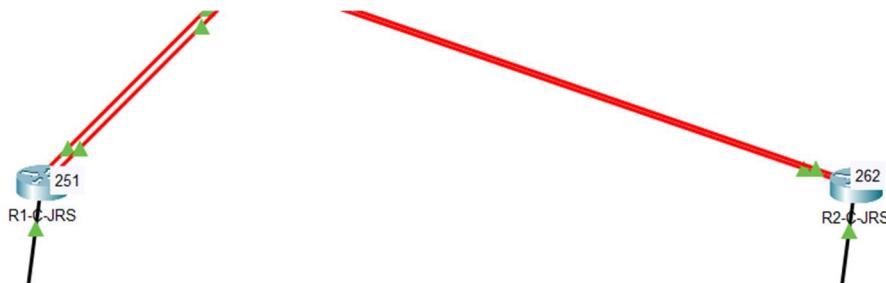
SSL Portal VPN -

מאפשר חיבור אחד אל אתר אינטרנט, אשר יאפשר גישה למגוון של שירותים רשות פרטית. החיבור נקרא פורטל מכיוון שהוא עומד באינטרנט אשר מוביל למשאיים אחרים רבים. המשתמשים יכולים לגשת לדף זה באמצעות כל דפדפן באינטרנט, הם יזינו שם משתמש וסיסמה הנิตנים על ידי נתן השימוש וייהיו רשאים להתחבר ולגשת למשאיים אלו.

SSL Tunnel VPN -

הגדרה של חיבור מרוחק אל רשות מקומית בארגון. ברגע שהמשתמש יתחבר עם שם משתמש וסיסמה, יהיה כאילו המחשב מחשב בראשת הפרטית של הארגון ויכול לגשת למשאיים בו. התעבורה של המחשב תעבור דרך FIREWALL של הארגון כל עוד מחובר.

הגדרת VPN סניף 1



הגדרת השלב הראשון קביעת Isakmp Policy

```
R1-C-JRS(config)#crypto isakmp policy 1
R1-C-JRS(config-isakmp)#[encryption 3des] שיטת הצפנה
R1-C-JRS(config-isakmp)#[hash md5] אלגוריתם גיבוב
R1-C-JRS(config-isakmp)#[authentication pre-share] מפתח משותף
R1-C-JRS(config-isakmp)#[group 5] קבוצה 5 דיפי - הלמן
```

הגדרת מפתח משותף עם הנטב מהסניף השלישי

```
R1-C-JRS(config)#crypto isakmp key [vpn] address 21.2.19.2
```

השם של המפתח המשותף

IKE Phase 2 יצירת סט המירה להגנת נתוניים

```
R1-C-JRS(config)#crypto ipsec transform-set VPN-TS [sp-3des esp-md5-hmac]
```

אלגוריתם גיבוב שיטת הצפנה שם סט

יצירת ACL מורחב

```
R1 R1-C-JRS(config)#ip access-list extended VPN-TRAFFIC
R1 R1-C-JRS(config-ext-nacl)#permit gre host 21.2.18.2 host 21.2.19.2
```

אפשר מעבר בuttle לאחת הכתובות היוצאות מהרשות החיצונית של הצד השני אליו

Crypto

```
R1-C-JRS(config)#crypto map JRS-CMAP 10 ipsec-isakmp שם מפה ומספר
% NOTE: This new crypto map will remain disabled until a peer שוכן
      and a valid access list have been configured.
R1-C-JRS(config-crypto-map)#set peer 21.2.19.2 סט חוקים
R1-C-JRS(config-crypto-map)#set transform-set VPN-TS רשיימת גישה
R1-C-JRS(config-crypto-map)#match address VPN-TRAFFIC
```

החלת המפה על הממשק של הנטב לכיוון החיצוני

```
R1-C-JRS (config)#int gig0/0/0  
R1-C-JRS (config-if)#crypto map JRS-CMAP
```

הגדרת VPN סנייפ 3

**הגדרת השלב הראשון ISKAMP / IKE Phase 1
קביעת Isakmp Policy**

```
R1-C-GRC (config)#crypto isakmp policy 1  
R1-C-GRC (config-isakmp)#encryption 3des  
R1-C-GRC (config-isakmp)#hash md5  
R1-C-GRC (config-isakmp)#authentication pre-share  
R1-C-GRC (config-isakmp)#group 5
```

הגדרת מפתח משותף עם הנטב מהסניף השלישי

```
R1-C-GRC (config)#crypto isakmp key vpn address 21.2.18.2
```

IKE Phase 2

יצירת סט מרמה להגנת נתונים

```
R1-C-GRC (config)#crypto ipsec transform-set VPN-TS esp-3des esp-md5-hmac
```

יצירת ACL מורחב

```
R1-C-GRC (config)#ip access-list extended VPN-TRAFFIC  
R1-C-GRC (config-ext-nacl)#permit gre host 21.2.19.2 host 21.2.18.2
```

יצירת מפה Crypto

```
R1-C-GRC (config)#crypto map GRC-CMAP 10 ipsec-isakmp  
% NOTE: This new crypto map will remain disabled until a peer  
and a valid access list have been configured.  
R1-C-GRC (config-crypto-map)#set peer 21.2.18.2  
R1-C-GRC (config-crypto-map)#set transform-set VPN-TS  
R1-C-GRC (config-crypto-map)#match address VPN-TRAFFIC
```

החלת המפה על הממשק של הנטב לכיוון החיצוני

```
R1-GRC (config)#int gig0/0/0  
R1-GRC (config-if)#crypto map GRC-CMAP
```

show commands:

- מציגה את התעללה הראשונה של ה – VPN, את מצבה ואת כתובות היעד והמקור.

- מציגה מידע על התעללה השנייה, מיהו השכן, כמו חבילות עברו כימוס והוצפנו, כמה חבילות פוענחו.

- מציגה מידע על מפות שהוגדרו.

show crypto isakmp sa

מצב התקשורת	כתובת יעד הנ才干 השכן	כתובת המissor	מצב התעללה	ID חיבור	מצב התעללה
נתב זה	21.2.16.2	21.2.17.2	QM_IDLE	1082	0 ACTIVE

show crypto ipsec sa

```
R1-GRC#show crypto ipsec sa
הממשק עלייו חלה המפה
interface: GigabitEthernet0/0/0
Crypto map tag: GRC-CMAP, local addr 21.2.17.2
כתובת משקל ושם המפה

protected vrf: (none)
local ident (addr/mask/prot/port): (21.2.17.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (21.2.16.2/255.255.255.255/47/0)
current_peer 21.2.16.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts[encaps: 10, #pkts encrypt: 10, #pkts digest: 0  פאקטות שעברו כימוס ונפתחו
#pkts[decaps: 10, #pkts decrypt: 10, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 | מספר שגיאות שנשלחו והתקבלו

local crypto endpt.: 21.2.17.2, remote crypto endpt.:21.2.16.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: 0xFD1BB4B9(4246451385)

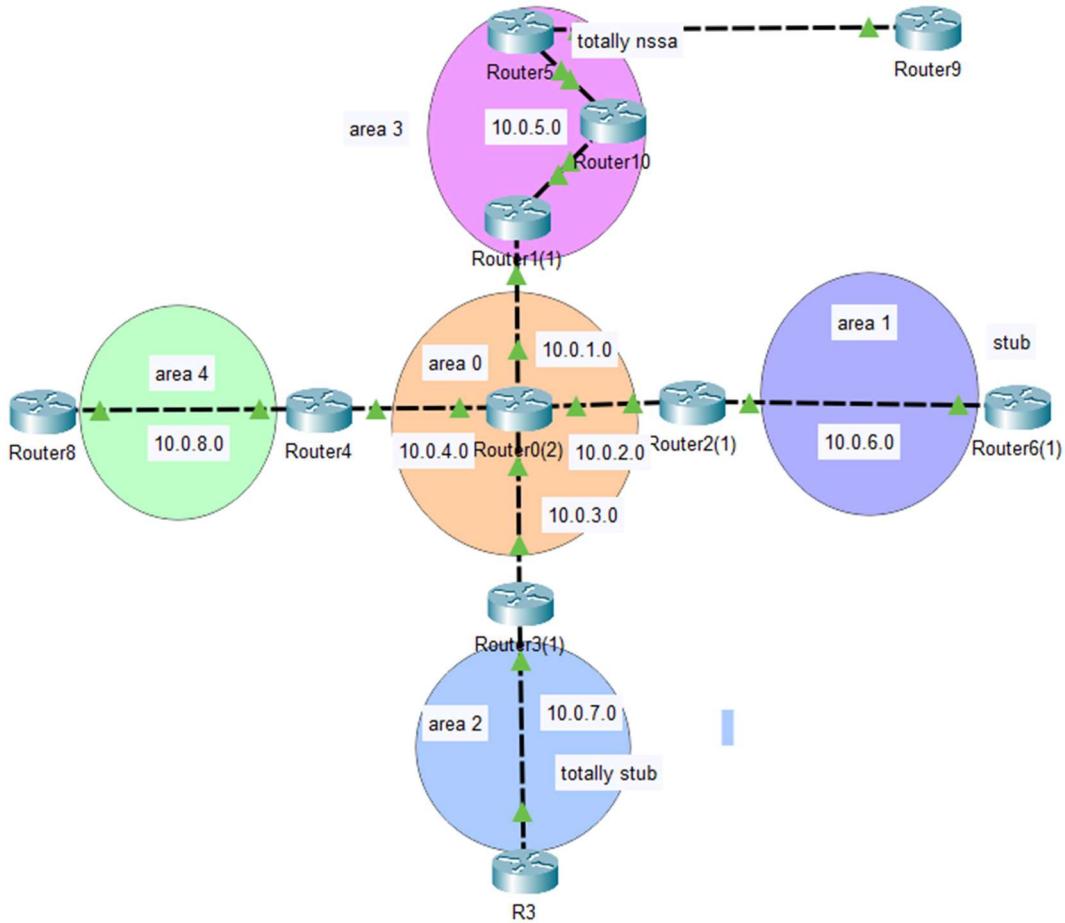
inbound esp sas:
  spi: 0x0A639F81(174301057)
```

show crypto map

```
R1-GRC#show crypto map
Crypto Map GRC-CMAP-10 ipsec-isakmp שם המפה ומספרה
  Peer = 21.2.16.2
  Extended IP access list VPN-TRAFFIC רשיימת הגישה שהושמה במפה
    access-list VPN-TRAFFIC permit gre host 21.2.17.2 host 21.2.16.2
  Current peer: 21.2.16.2 שcn נוכחי
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    VPN-TS סט המורה
  }
  Interfaces using crypto map GRC-CMAP: הממשק עליו חלה המפה
    GigabitEthernet0/0/0
```

אייזורי stub

באייזור זה נגידר רשותות שונות הנמצאות באיזוריים שונים. כל אחד מהאייזוריים נגידר בסוג שונה ובודוק



כיצד כל סוג אייזור משפייע על טבלת הניתוב של הנתבים הנמצאים בו.

סוג אייזור	
stub	Area 1
totally stub	Area 2
totally nssa	Area 3
nssa	Area 4

הגדרות:

נדיר כתובות IP לראוטרים :

לנתבים מסוג זה קיימים 2 ממשקים מסוג GigabitEthernet HWIC (4ESW). אגדיר SVI (Switch Virtual Interface) את כתובות IP למשקיי שכבה 2 שהוספה. היות ונתב R30 צריך 4 ממשקים על מנת שטופולוגיה זאת תתקיים, הוסףו לנתב ממשק סוויץ' HWIC.

כלומר לממשקים אלו תהיה כתובה IP באמצעותם יוכל הנתב לתקשר עם שכנו.

ניצור את הוילאים בנתב

```
Router#vlan database vlan 10
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

Router(vlan)#vlan 10   הגדרת VLAN 10
VLAN 10 added:
  Name: VLAN0010
Router(vlan)#vlan 20
VLAN 20 added:
  Name: VLAN0020
Router(vlan)#vlan 30
VLAN 30 added:
  Name: VLAN0030
Router(vlan)#vlan 40
VLAN 40 added:
  Name: VLAN0040
```

ניצור את הממשקים הווירטואליים ונוסיף להם כתובות IP

```
interface Vlan10  ייצרת SVI
R30(config-if)#ip address 10.0.1.1 255.255.255.0
R30(config-if)#exit
R30(config)#interface Vlan20
R30(config-if)#ip address 10.0.2.1 255.255.255.0
R30(config-if)#exit
R30(config)#interface Vlan30
R30(config-if)#ip address 10.0.3.1 255.255.255.0
R30(config-if)#exit
R30(config)#interface Vlan40
R30(config-if)#ip address 10.0.4.1 255.255.255.0
R30(config-if)#exit
```

נותינת כתובות IP

נשייך את הממשקים הווירטואליים

```
interface FastEthernet0/0/0
R30(config-if)#switchport mode access
R30(config-if)#switchport access vlan 10
```

שיוך ממשק

הגדרת כתובת IP בשאר הנתבים :

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)# ip address 10.0.8.2 255.255.255.0
Router(config-if)#no shutdown
```

הגדרת OSPF - פרסום רשותות המחברות לנתב בהתאם לאזור בו הם נמצאים :

```
R32(config)#router ospf 1
R32(config-router)#router-id 3.3.3.3
R32(config-router)#network 10.0.6.0 0.0.0.255 area 1
R32(config-router)#network 10.0.2.0 0.0.0.255 area 0
```

פרסום רשותות

נדיר redistribute על שני הנתבים ועשה על

```
Router(config)#router eigrp 30
Router(config-router)#net
Router(config-router)#network 10.0.9.0 0.0.0.255
Router(config-router)#redistribute ospf 1 metric 1 1 1 1
Router(config)#router ospf 1
Router(config-router)#redistribute eigrp 30 subnets
```

כעת אם נעשה show ip route נראה כי כל הנתבים הטופולוגיה זו מכירים את כלל הרשותות.

הרשאות שפורסמו דרך הנתבים האחרים מוכרים כIA (OSPF Inter Area) O כלומר רשותות הנמצאות באזוריים שונים. בנוסף נראה את הרשות שלigrp E2.

```
R32#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGE
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O       10.0.1.0/24 [110/2] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
C       10.0.2.0/24 is directly connected, GigabitEthernet0/0
L       10.0.2.2/32 is directly connected, GigabitEthernet0/0
O       10.0.3.0/24 [110/2] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
O       10.0.4.0/24 [110/2] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
O  IA    10.0.5.0/24 [110/3] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
C       10.0.6.0/24 is directly connected, GigabitEthernet0/1
L       10.0.6.1/32 is directly connected, GigabitEthernet0/1
O  IA    10.0.7.0/24 [110/3] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
O  IA    10.0.8.0/24 [110/3] via 10.0.2.1, 00:08:59, GigabitEthernet0/0
O  E2    10.0.9.0/24 [110/20] via 10.0.2.1, 00:01:56, GigabitEthernet0/0
```

כל הרשותות בטופולוגיה

הגדרת Stub

בהגדרת Area [num Area] Stub וגם על הנטים האחרים באזור זה, stub

```
R36(config)#router ospf 1
R36(config-router)#area 1 stub
```

```
R36#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 10.0.6.1 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA    10.0.1.0/24 [110/3] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O IA    10.0.2.0/24 [110/2] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O IA    10.0.3.0/24 [110/3] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O IA    10.0.4.0/24 [110/3] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O IA    10.0.5.0/24 [110/4] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
C     10.0.6.0/24 is directly connected, GigabitEthernet0/0
L     10.0.6.2/32 is directly connected, GigabitEthernet0/0
O IA    10.0.7.0/24 [110/4] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O IA    10.0.8.0/24 [110/4] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
O*IA  0.0.0.0/0 [110/2] via 10.0.6.1, 00:00:16, GigabitEthernet0/0
```

Totally Stub

בהגדרת Area [num area] stub no-summary ABRn Totally stub ועל שאר הנטים נגידר stub

```
R33(config)#router ospf 1
R33(config-router)#area 2 stub no-summary
```

על ה-ABR

```
R37(config)#router ospf 1
R37(config-router)#area 2 stub
```

על הנטים הרגילים

ניתן לראות שנוצר ניתוב סטטי לרשותות חיצונית (לדוגמא eigrpma)

```
R37#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 10.0.7.1 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.0.7.0/24 is directly connected, GigabitEthernet0/0
L        10.0.7.32 is directly connected, GigabitEthernet0/0
O_E2_  10.0.9.0/24 [110/20] via 10.0.7.1, 00:05:59, GigabitEthernet0/0
O_IA 0.0.0.0/0 [110/2] via 10.0.7.1, 00:00:22, GigabitEthernet0/0
```

ניתן לראות שנוצר ניתוב סטטי לכל הרשותות באזוריים השונים

הגדרת nssa

נדיר על גם על הנתבים area [area num] nssa

```
Router(config)#router ospf 1
Router(config-router)#area 4 nssa
```

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O IA  10.0.1.0/24 [110/3] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.2.0/24 [110/3] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.3.0/24 [110/3] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.4.0/24 [110/2] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.5.0/24 [110/4] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.6.0/24 [110/4] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
O IA  10.0.7.0/24 [110/4] via 10.0.8.1, 00:06:47, GigabitEthernet0/0
C    10.0.8.0/24 is directly connected, GigabitEthernet0/0
L    10.0.8.2/32 is directly connected, GigabitEthernet0/0
```

ניתן לראות כי לא נוצר ניתוב לרשותות מפrotוקול ניתוב שונה (eigrp)

הגדרת totally nssa

נדיר על הנתבים area [num area] nssa no-summary ASBR

נדיר על שאר הנתבים area [num area] nssa

```
Router(config)#router ospf 1
Router(config-router)#area 3 nssa no-summary
```

```
Router(config)#router ospf 1
Router(config-router)#area 3 nssa
```

```
Router#show ip route
Codes: L - local, C - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 10.0.5.1 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.5.0/24 is directly connected, GigabitEthernet0/0
L       10.0.5.2/32 is directly connected, GigabitEthernet0/0
D N2    10.0.9.0/24 [110/20] via 10.0.11.2, 00:00:14, GigabitEthernet0/1
E       10.0.11.0/24 is directly connected, GigabitEthernet0/1
L       10.0.11.1/32 is directly connected, GigabitEthernet0/1
D*IA 0.0.0.0/0 [110/2]
```

רשות של פרוטוקול ניתוב שונה, מומרת מהודעות סוג 5 להודעות סוג 7 . לכן O N2

פרק 2 - אבטחת מידע

פרק זה מכיל רקע תיאורטי בתחום אבטחת המידע ומתמקד בדרישות האבטחה של הארגון, פירוט על מתקפות וחולשות אבטחה וכייצד ההתגוננות מפניהם באה לידי ביטוי בפרויקט.

מושגים באבטחת מידע

Asset (נכס)

כל ארגון מכיל נכסים. נכס הוא משאב או פריט בעל ערך לארגון שיש להגן עליו מפני גישה בלתי חוקית, חשיפה ושינוי. נכס יכול להיות מוחשי, כמו שרטטים ומכשירים טכנולוגיים, או לא מוחשי, כמו נתונים עסקיים ומגרי מידע. כמות הזמן והמשאים שיוקצו על מנת להגן על נכסים אלו תלויות בסוג הנכס, ערכו, מיקומו ורמת החשיפה אליו.

Vulnerability (חולשה)

פיגועות במערכות או בתשתיות המידע הניתנת לניצול במטרה לגרום לפגיעה בסודיות שלמות או זמיינות הנכסים של הארגון. ככל שניצול החולשה עלול לגרום לנזק גדול יותר לנכסים הארגון כגון מידע רגיש, תשתיות מרכזיות, או מערכות מידע מרכזיות, כך הוא נחשב לפוטנציאלי יותר, ונשקייע יותר ממשאים בטיפול בחולשה זו.

Threat (איום)

כל הסיכוןים או האירועים הפוטנציאליים שעשוים לגרום לפגעה באבטחת המידע או הנכסים של הארגון. כולל בתוכו איומים, כגון התקפות סייבר, פרצחות באבטחת המידע, תקיפות פיזיות ועוד. על מנת להגן על הארגון, חשוב לזהות, ולהעריך את גודל ההשפעה של האיום על הנכסים ארגון.

Risk (סיכון)

איום מהויה סיכון רק כאשר יש חולשה אשר אותו איום יכול לנצל. הסיכון מושפע מהאיום והחולשה. ככל שהאיום גדול יותר כך הסיכון גבוה יותר. ככל שהחולשה קלה יותר לניצול כך הסיכון גבוה יותר.

Exploit (ニיצול החולשה)

כלי או תוכנה בו התוקף משתמש על מנת לנצל חולשה קיימת במערכת או בתוכנה.

Payload

החלק בקוד שמבצע פעולות זדוניות או לא מורשות על מערכת היעד לאחר שניצל את החולשה ותקף את הנכס. לדוגמה: חסיפת מידע רגיש, שינוי הרשאות מחיקה ו שינוי של המידע ועוד.

CIA

Confidentiality, Integrity, Availability

מודל המשמש ככלי להערכת ותכנון בטחוני של האבטחה בארגון. כל העקרונות במודל צריכים לבוא לידי ביטוי בעת התייחסות לאבטחה של חומרה תוכנה ותקשורת נתונים. כל אמצעי אבטחתני שימושם בארגון צריך לתרום להשגת או לחיזוק של לפחות אחד משלוש העקרונות.

סודיות המידע (Confidentiality) -

מידור של המידע ומונעה ממנו הגיע אל גורמים לא מורשים. סודיות המידע עשויה להיפגע עקב גורמים זדוניים המשמשים בהתקפות שונות על מנת להשיג מידע, כגון (Man In The Middle) MITM, dns spoofing, Password attacks, ועוד. כמוות המשאבים שיושקעו על מנת להגן על סודיות המידע תלויות ברגישותו. ככל שהמידע רגיש כך נעשה יותר מאץ ונרצה להדקיע יותר משאבים על מנת להגן על המידע. השמירה על עיקרונו זה יכולה להתבצע במגוון דרכים כגון: הצפנה של המידע, רישומות גישה, חלוקה של VLAN ושמירה על העקרונות במודול AAA, שהרחבה עלייה בהמשך בפרק AAA.

שלמות המידע (Integrity) -

להבטיח כי המידע אמין שלם ואינו שונה על ידי גורמים שאינם מורשים לכך. שלמות המידע עשויה להיפגע עקב גורמים זדוניים שמטרתם להטעק ולפגוע בשלמות הנתונים. הם עושים זאת במגוון דרכים לדוגמא החדרה של וירוסים, כניסה וחיבור פיזי לרשות הארגון וביצוע פעולות בהרשאות שונות ועוד.

הشمירה על עיקרונו זה מתבצעת באמצעות גיבוב (Hashing), גיבוי של המידע, שימוש ברישומות גישה ושימוש בערכי checksum.

זמינות המידע (Availability) -

לודא זמינות מתמחכת של המערכת והמידע שבה. העיקרונו כולל הגנה על המערכת מפני תקלות טכניות או תקיפות שיכולות להשפיע על היכולת של המערכת לפעול בצורה תקינה. זמינות המידע עשויה להיפגע עקב עומס ברשות, מתקפות למניעת שירות (DDOS / DOS), תקלות פיזיות לדוגמא בעיה בכבל המשמש להעברה של מידע, נפילת מכשירים ועוד. השמירה על עיקרונו זה מתבצעת במגוון דרכים לדוגמא: גיבוי של המידע, יתרונות במקרה של נפילת חיבורים או מכשירים, חלוקת עומסים (Load Balancing), אמצעים להגבלת כמות בקשות שירותי ועוד.



מתകפות איוםים ומנגנוני אבטחה:

Password attacks

כיום, חשבונות ומערכות רבות דורשות אימות באמצעות סיסמה לצורך הזרחות, כגון מערכות מחשב, שירותי, חשבונות משתמשים ושרותים. מטרת המתקפה הינה להשיג את סיסמאות אלו ולהיכנס לحسابות אלו על מנת לקבל הרשאות ולהציג מידע ונתונים.

דרכים נפוצות לגניבת סיסמאות:

Brute Force Attack - שיטה בה התוקף מנסה לפרוץ למערכת או לחשבו על ידי הכנסת מספר

רב של סיסמאות אפשריות עד שהוא מצליח ליזוח את הסיסמה הנכונה. לרוב ישמש התוקף בתוכנה אוטומטית או בקוד שיכניס את הסיסמאות מה שמאפשר לו לנחש מספר רב של סיסמאות במהירות גבוהה. המהירות שבה יצליח התוקף לפרוץ את הסיסמה תלויות באורך ובמורכבות הסיסמה של המערכת או של החשבון. ככל שהסיסמה קצרה יותר, כך כמות הסיסמאות שיידרשו להיבדק עד שתימצא הסיסמה הנכונה קטנה יותר.

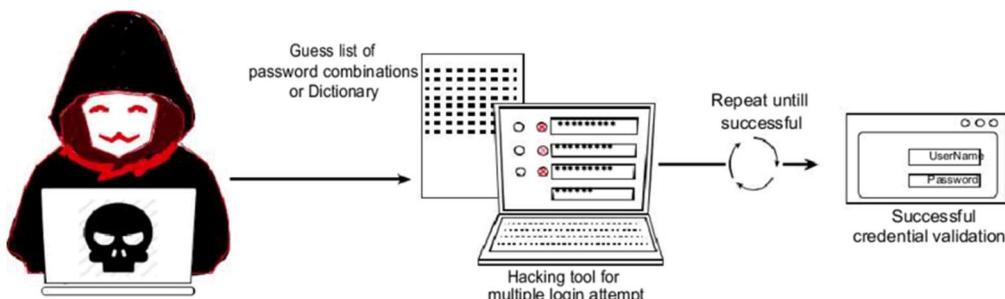
Dictionary Attack - שיטה בה התוקף משתמש במילון המכיל צירופי סיסמאות נפוצים. הוא משתמש בתוכנה או בקוד שעוברים על המילון ומכוונים בכל פעם ערך אחר כסיסמה. דרך זו לא תמיד עובדת מכיוון שהמילון אינו מכיל את כל הצירופים האפשריים, לכן נהוג לבצע את מתקפה זו לפני השימוש ב-Brute Force Attack. ככל שהסיסמה של החשבון או המערכת נפוצה יותר כך הסיכוי שהסיסמה הנכונה תגעה לידי התוקף גדול יותר.

Hybrid - שילוב של Brute Force Attack ושל Dictionary Attack. שימוש במילונים וניסיונות brute force על מנת להגדיל את סיכון ההצלחה למציאת הסיסמה.

Rainbow table - טבלה המתרגם ערבי hash לסיסמאות לפני הגיבוב. אם לתוקף קיימת הסיסמה באופן מגובב, יוכל לפענה אותה על ידי השוואה של הערך המגובב שברשותו לערך מגובב זהה הנמצא בטבלה ומשם להשיג את הסיסמה המתאימה לערך hash. התקפה מסוג זה אינה תמיד עובדת מושם שטבלאות אלה אין מכילות את כל הערכות והסיסמאות האפשריות. לכן ככל שהסיסמה ארוכה וחזקה יותר, כך הסיכויים שערבה יהיה בטבלה נמוכים יותר והסיכוי שתיפרץ באמצעות מתקפה זו נמוך יותר.

על מנת להתגונן מפני התקפות מסוג password attack רצוי להגדיר סיסמאות ארוכות ולהשתמש בתווים נוספים לצורך אימות (MFA). יתר על כן, נהוג להגביל את מספר הניסיונות להכנסת סיסמא ביחס לפרק זמן מסוים.

הרחבת והגדלה של הגבלת מספר הניסיונות להתחברות למתקנים והנתבים בארגון הנו בחיבור קונסול והן מרוחק, נמצאים בפרק SSH



DOS

Denial Of Service

מתתקפה שמטרתה להשכית שירות מסוים ולהפוך אותו לבליתי זמין. נעשה על ידי הצפת נתונים השירות בבקשתות מיותרות בניסיון להעמיס על המערכת, למנוע מבקשות לגיטימיות של משתמשים מלהתמכנס וכתוצאה מכך למניע את מתן השירות למשתמשים אחרים.

דוגמאות למתתקפות DOS :

Syn Flooding - שליחת כמות מאסיבית של בקשות לפתח חיבור מסווג TCP עם השרת אך ללא

יצירת החיבור. ככלומר, התוקף ישלח הודעות רבות מסווג SYN. כל הודעת SYN גורמת לשרת לפתוח חיבור פורט חדש באופן זמני. השרת יענה לכל אחת מההודעות אלו עם הודעת SYN/ACK, אך מכיוון שההתוקף לא ישלים את יצירת החיבור (לא ישלח בחזרה ההודעות ACK), תהליך ה- 3 way handshake לא יסתתיים מה שיגרום זמני לכך שכל הפורטים ליצירת חיבור מצד השרת תפוסים ולכך לא יוכל לפתוח חיבור עם משתמשים לגיטימיים הדריכים שירות.

Buffer overflow attack - הzcורה הנפוצה ביותר של מתתקפת DOS. משתמשת לרעה בתקלה

הנקראת "buffer overflow". כאשר תוכנית מנסה לכתוב מידע לתוך buffer שאינו מסוגל לאחסן את כמות הנתונים המועברת אליו, המידע המיוצר מופזר לתיבת זיכרון סמוכה או לאזוריים אחרים בזיכרון, מה שעולל לגרום לדרישת של נתונים אחרים שבו בזיכרון. בתתקפה זו התוקף משדר יותר תעבורה לרשת משהמערכת יכולה להתמודד, מה שגורם לצריכה של המאגרים הזמינים ושל אזורי האחסון בזיכרון המחזיקים נתונים באופן זמני מה שוביל לביצועים איטיים וקריסות מערכות.

ICMP Floods - ניצול של התקני רשת שלא הוגדרו כראוי. בהתקפות מסווג זה, התוקף ישלח

חבילות מזויפות שלוחות הודעת echo request לכל מכשיר ברשת ללא חוכות לתשובה, מה שמעmis על הרשות במנות מסווג echo replay כשתשובה להודעת ששלח התוקף, ועלול לפגוע בזמיןויות התעborה והשירותים האחרים ברשת.

DDOS

Distributed Deny Of Service

בשונה ממתתקפות DOS, בהן יש שימוש במחשב אחד וכנתובת IP אחת על מנת לבצע את המתתקפה, במתתקפות מסווג DDOS, מקור ההתקפה מגע מספר מקומות ומספר מכשירים. התוקף משתמש ברשת של מחשבים נזועים בנגיף (botnet) כדי לשולח כמות גדולה של בקשות לשירות מסוים. השימוש במחשבים מרוחקים מפוזרים על הרשות מבקשת על הגנה ועל זיהוי המתתקפה. כאשר השירות או האתר מתמוטטים מכמות הביקורת, הם מפסיקים להיות זמינים למשתמשים רגילים.

על מנת להציגן מפני התקפות DOS וDDOS נהוג להגביל גישה לשירותים ולמשתמשים שאינם מוכרים על ידי רשימות גישה (ACL) ולהשתמש בכלים לאייתור ומניעת פעולות חשודות ברשות כגון IDS, IPS.

הרחבת והגדלה של רשימות גישה לשירותים ומשתמשים נמצא בפרק ACL

Spoofing

זיהוי זהות, במתקפה מסווג זה, התוקף מתחזה למשהו אחר (לדוגמא שרת, רכיב בראשת) במטרה לקבל גישה למשאבים שירותי ותקורת בין רכיבים שונים בראשת, להשיג מידע רגיש, למנוע זיהוי ומעקב אחר פעולתו, לשבש את התקורת ולפגוע בזמןיות ושלמות המידע.

קיימים מספר דרכים לביצוע מתקפה מסווג Spoofing

- **Mac Address Spoofing** – שינוי כתובות MAC, שימוש כזיהה ייחודי של מכשירים בראשת, על מנת להתחזות למכשיר אחר. משומש לניצול חולשות בשכבה 2

- **IP Address Spoofing** – שינוי כתובות ה-IP, כתובות ה-IP משמשת כזיהה עבור מכשירים בראשת כך שתתאים לכנתובת של מכשיר אחר בראשת או לכנתובת שאינה משוויכת לו.

- **Application / Service Spoofing** – תוקף משנה את זהותו על מנת להתחזות לשירות או אפליקציה.

- **ARP Spoofing** – התוקף שולח הודעות ARP replay מזויפות בראשת המקומיית. ההודעות ישלחו בתגובה להודעות מסווג Arp request שנשלחו על ידי רכיב בראשת במטרה לגלוות מהי כתובות ה- MAC של, מחשב, נתב או שרת בארגון שמחזיק בכנתובת לוגית (IP) ספציפית. התוקף יענה להודעה וישיך לה את כתובת MAC שלו. באמצעות זיהוי הודעת ARP, מכשיר התוקף יקבל את המידע והנתונים שהיו מיועדים למכשיר המקורי המחזיק בכנתובת IP. משמש לביצוע התקפות מסווג MITM .

התוגנות מפני מתקפה מסווג זה בפרויקט port security – הגבלת כמות כתובות MAC היכולות להילמד על ידי ממשק מסויים. הרחבת על נושא זה והגדתו בפרויקט נמצא בפרק port security .

- **DNS Spoofing** – התוקף מתחזה לשרת DNS לגיטימי בארגון. כאשר מכשיר בראשת ישלח בקשה DNS במטרה לתרגם דומיין לכנתובת IP, שרת DNS של התוקף יפנה אותו לכנתובת IP שוגיה, לרוב אתר המדמה את האתר המקורי, במטרה לאפשר לתוקף גישה למידע רגיש או להשתיל במכשיר הקצה וירוס או תולעת המאפשרים לתוקף להשיג להצפן או להר奥斯 מידע ונתונים.

ניתן לבצע את המתקפה זו בראשת המקומיית

○ על ידי שימוש ב - **Man In The Middle Attack** -

○ התחזה לשרת DHCP שישיק למכשירי הקצה את כתובות שרת DNS של התוקף

התוגנות מפני מתקפה מסווג זה בפרויקט DHCP snooping ,port security – DHCP snooping – הגדרה מאילו משקים יוכל המתג לקבל הודעות Offer ו Acknowledge . הרחבת על נושא זה והגדתו בפרויקט DHCP snooping ,port security נמצא בפרקים .

- **DHCP Spoofing** – התוקף מתחזה לשרת DHCP לגיטימי בארגון. כאשר מכשיר בראשת ישלח בקשה Discover במטרה לקבל כתובת IP, שרת DHCP יענה לו ויכול לספק לו כתובות IP, S.M Default Gateway לבחירתו שיוכל לשמש למתקפות מסווג MITM וכנתובת DNS שיוכל לשמש למתקפות מסווג DNS Spoofing .

התוגנות מפני מתקפה מסווג זה בפרויקט DHCP Snooping ,port Security . הרחבת על המתקפה DHCP snooping ,port security ו הגדרת התוגנות אלו בפרויקט נמצא בפרקם .

VLAN Hopping

. – משמש לייצירת Trunk בצורה אוטומטית בין שני מותגים. Dynamic Trunk Protocol – DTP התקפה זו תצליך רק במקרה שבו התוקף מחובר למסך שייך ל-Native VLAN. במקרה זה, התוקף ינסה את ה-Frame המקורי על מנת להוסיף שתי תגים. תג החיצוני המציין את ה-VLAN של התוקף, ותג המוסתר המציין את ה-VLAN של הקורבן. כאשר ה-Frame יגיע למstag, הוא יוכל לראות את התג החיצוני בלבד של ה-VLAN של המחבר אליו. הוא יסיר את התג VLAN החיצוני וכאשר הוא מסגרת תתקבל על ידי המtag הבא, הוא יפתח את ההמסגרת ויראה את התג הפנימי ויעביר את המידע של VLAN המתאים.

על מנת להציגו ממתකפות מסווג זה נהוג לשנות את native vlan על המותגים

שינויי VLAN

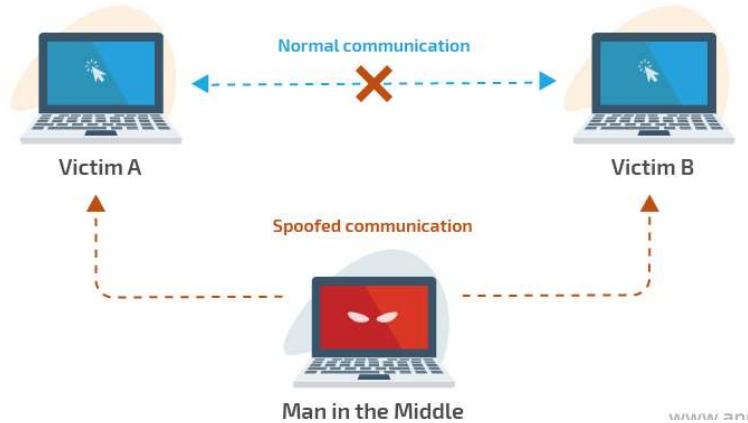
```
SW1-A-JRS(config)#int range fastEthernet 0/15-16  
SW1-A-JRS(config-if-range)#switchport trunk native vlan 240
```

vlan שלא בשימוש בסנייפ

MITM Attack

Man In The Middle

במתקפה זו, התוקף נמצא בין התעבורה של התקנים המעבירים ביניהם מידע, ובכך יכול להאזין למידע העובר ביניהם ואף לשנותו. המטרה היא לגרום לשני הצדדים להאמינו שהם מדברים ישירות אחד עם השני בחיבור פרטי כשלמעשה כל השיחה בשליטתו של התוקף. מאפשר לתוקף להזין ולשנות תעבורת במטרה להשיג מידע רגיש כגון סיסמאות ופרטיים אישיים אותם יוכל לנצל על מנת להשיג גישה לא מורשת, פגוע באבטחת הרשות ולפרוץ למערכות.



על מנת להגן מפני התקפות מסוג זה ולמנוע מחשבים לא מורשים להתחבר לרשת הארגון שלנו, ניתן להגדיר port security שלא יאפשר חיבור למוחשי התוקף. יתר על כן ניתן להשתמש בהצפנה בתקשורת בתקשורת בין רכיבים שונים. הרחבה על הצפנות בהמשך הפרק בנושא – הצפנות.

STP Attack

Spanning Tree Protocol

STP הינו פרוטוקול לניטור ומונעת לולאות בשכבה 2. המתנים משתפים ביניהם BPDUs Packets המכילים פרטיים על המtag ומשתמשים בהם כדי לוודא לולאות. המtag בעל ה-ID הכי נמוך יקרא Root Bridge וככל ההודעות יעברו דרכו. בסוף בחירתו הנטיב שיחסם בלולאה יבחר לפי העלות שלו Root Bridge. בתקופה זו, התוקף מתחבר מtag לרשת ומוריד לו את ערך priority כך שהיא תהיה כRoot Bridge. חיבור המtag יכול לשמש לכמה מטרות:

- ביצוע התקפה מסוג MITM, משום שהוגדר Root Bridge כל הודעה עוברות דרכו, ככלומר התוקף יכול להאזין למידע העובר ברשת ולשנותו.
- ביצוע התקפה מסוג DOS. שליחה של הודעות BPDU רבות ולגרום לחסימה של ממשקים רבים בטופולוגיה.

על מנת להגן מפני התקפה זו יש להגדיר Root Guard ו- BPDU Guard שפירוט והרחבה עליהם ניתן למצוא בפרק Spanning Tree Protocol.

Sniffer

sniffers הינו חומרה או תוכנה המאפשר להאזין לחבילות מידע העוברות בנקודת כלשהי ברשת, לטעוד ולנתח אותם. משתמשים בסניפר על מנת לזהות בעיות ברשת ואת סיבותיהן, לאתר תעבורה זדונית ולקראן ולנתח את המידע שעובר ברשת.

תוכפים עולמים להשתמש בסניפר לביצוע מתקפת MITM על מנת להאזין ולקבל מידע מן התעבורה שעוברת ברשת.

קיימים שני סוגי של הסניפות:

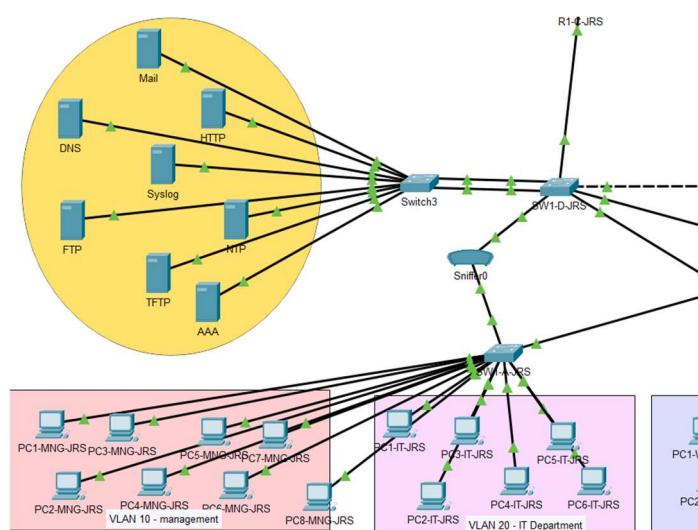
Passive Sniffing – בהסיפה פאסיבית, נעשית האזנה לתעבורה הרשות ותיעוד של כל החבילות העוברות מבלי להשפיע על התעבורה. יתרון מרכזי בסוג זה הוא שהוא ניתן לביצוע באופן דיסקרטי ואין מעורר חשד ברשת.

Active Sniffing – גם בהסיפה אקטיבית, נעשית האזנה לתעבורה הרשות ותיעוד של החבילות העוברות בה, אומנם התוקף מתערב בתעבורה הרשות ושולח אקטואות מזויפות (spoofing) במטרה להשפיע על התעבורה ולקבל מידע נוסף שלא היה נגיש ללא החתערות בתעבורה.

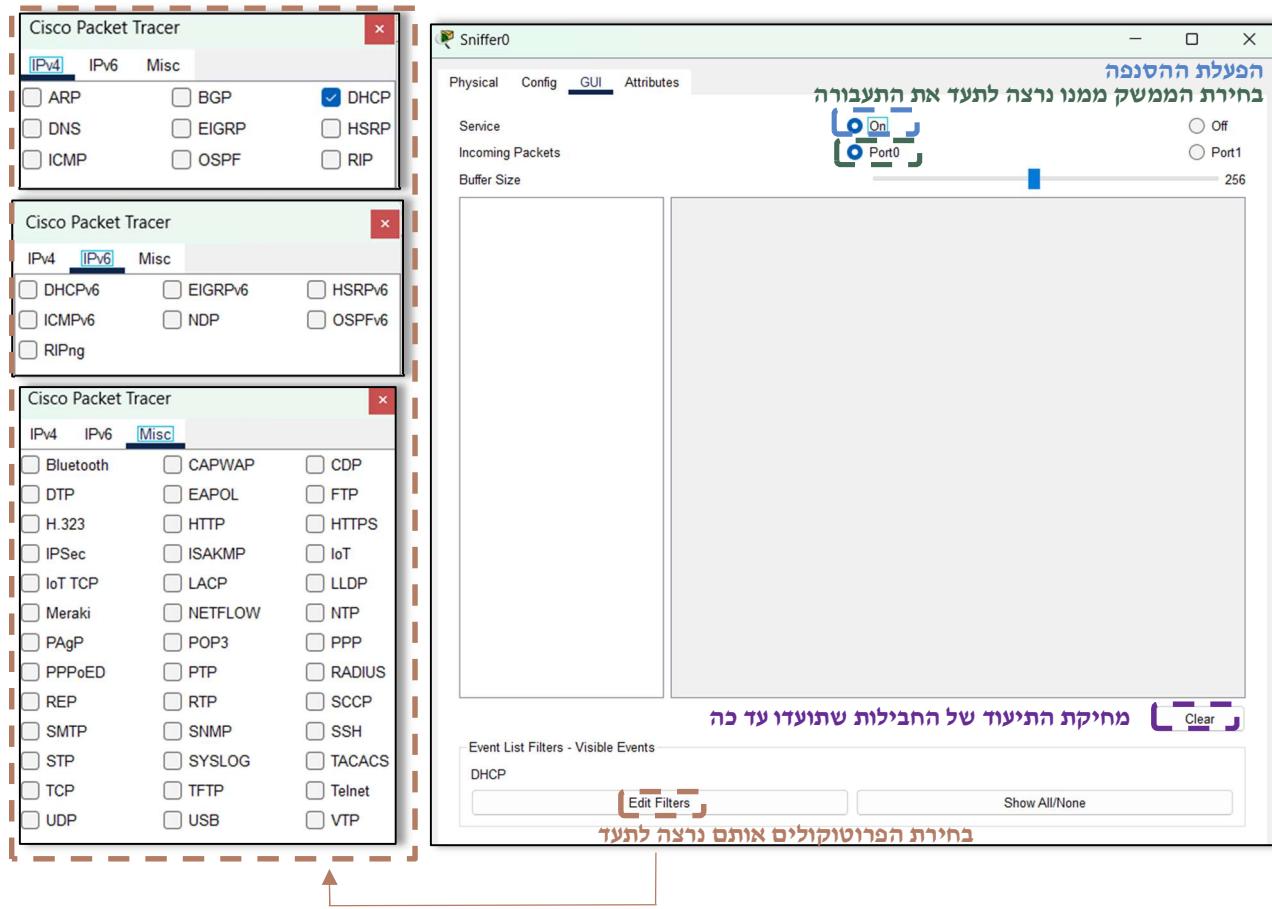
ברשת, מידע יכול לעבור בשני צורות עיקריות: גלויה ומוצפנת. בצורה גלויה (clear / plain text), המידע נשלח כפי שהוא בנסיבות הרגילה, ללא הצפנה. זה אומר שתוקף בעל גישה לתעבורה הרשות, יוכל לקרוא ולהבין את המידע.

לעומת זאת, בצורה מוצפנת (cipher text), המידע מוצפן בשליחתו (cipher) כך שרק הנמען המקורי או מי שמחזיק ב מפתח המתאים יוכל לפענה אותו ולהבין את התוכן. לעומת זאת, התוקף לא יוכל לקרוא את המידע או להבין את התוכן שלו.

שימוש בpacket tracer sniffers

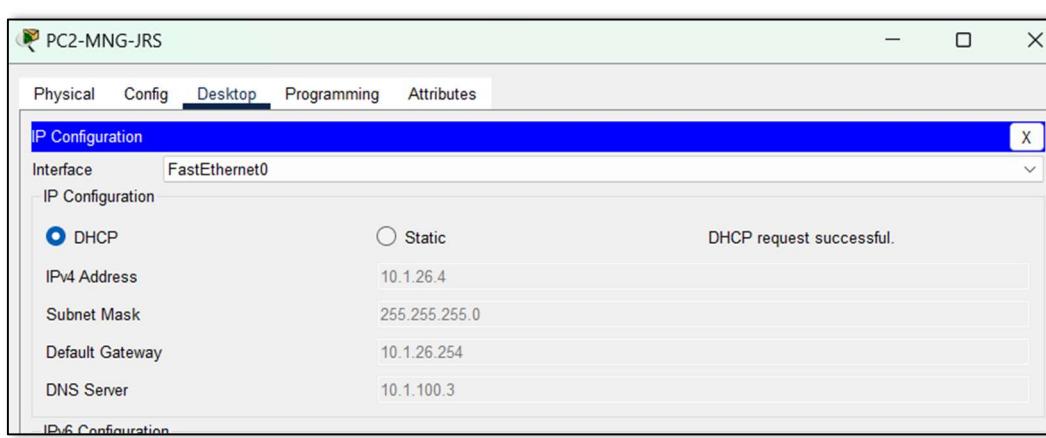


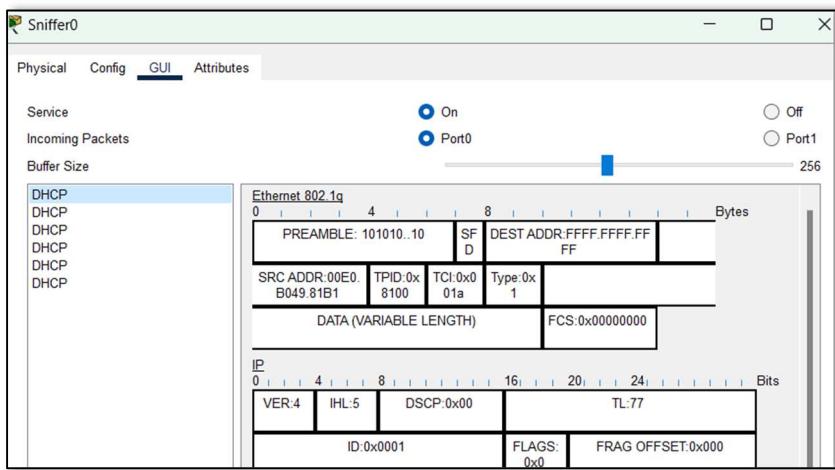
לצורך ההדגמה, חיבורתי רכיב מסוג sniffer בין המתגים בשכבה access distribution במטרה להאזין לתעבורה העוברת ביניהם.



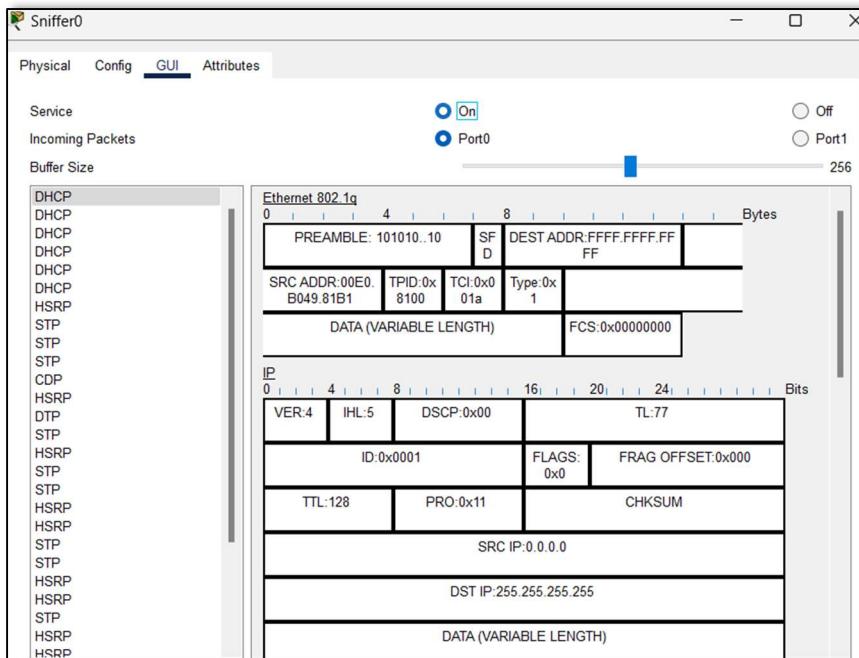
לצורך ההדגמה, בחרתי לטעוד תעבורת מסוג DHCP בלבד.

הסניפר מחובר בport0 מכיוון המותג בשכבה ההוּאַדְרָיָה distribution כלומר המידע שיתיעוד יבוא מכיוון זה
כעת אשלח בקשה לכתובת IP בצורה דינמית מאחד המחשבים ונראה את החבילות שנתפסו בעת
ההאזנה לטעבורה





כפי שניתן לראות התעבורה שעוברת ברשות במהלך תהליך קבלת הכתובת משרת DHCP תועדה בסיניפר. כמו כן ניתן לראות תיעוד של פרוטוקולים נוספים, כולל לראות גם תעבורה מסוג arp, stp, hsrp ועוד.



Wireshark

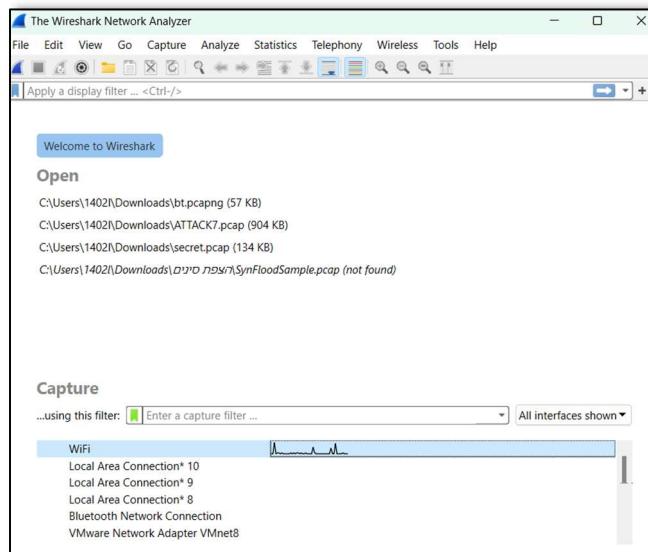
sniffer פופולרי שעומד בסביבת windows וlinux. משמש לניתוח תעבורת רשת, במטרה להאזין לתקשורת המתקבלת והנשלחת ברשת, ולנתח אותה על מנת לזהות בעיות, לאתר תקלות, ולהבין את פעולה הרשת. wireshark תומך במנועו רחב של פרוטוקולים ויכול להציג את הנתונים בצורה ברורה ונוחה לקריאה מאפשר לראות את מקור החבילה והיעד שלו, את סוג הפרוטוקולים המשמשים בתוך החבילות, את המידע המתקבל והנשלח בכל חבילה ומידע נוסף.



sniffing – PCAP/CAP FILES (Packet Capture File) – קובץ הנוצר על ידי חומרה או תוכנת המשמש לтиיעוד ואחסון של התעבורה, חברות נתוניים שנקלטו או שנשלחו ברשת, כולל כל המידע הקשור לחבילה כגון כתובות מקור ויעד, פרוטוקולים, ומידע נוסף.

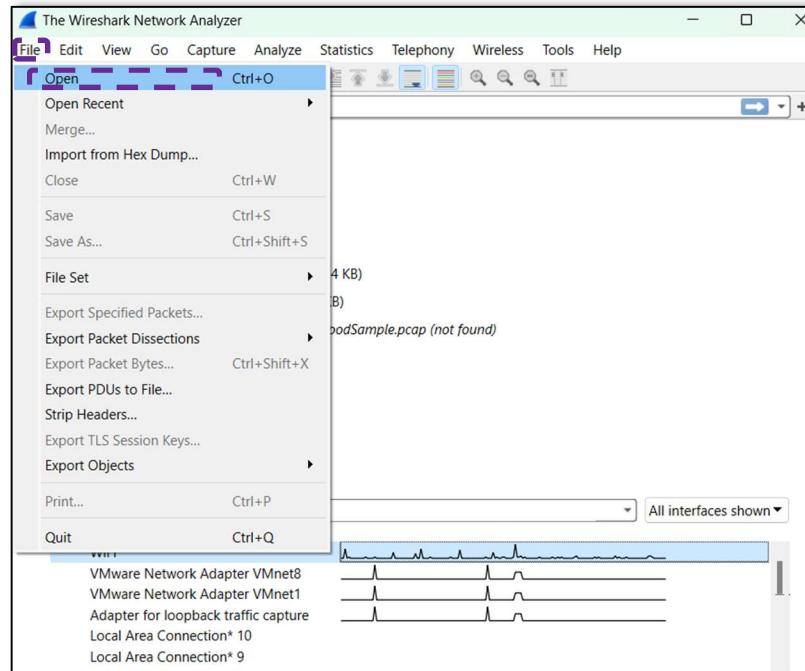
הנתוניים בקובץ pcap מסודרים לפי הזמן בו הם נקלטים או נשלחים ברשת. כל חבילה בתעבורה הרשות מתווספת לקובץ ה- pcap כחלק מהתהליך הניטור והניתוח של פעילות הרשת.

שימוש Wireshark



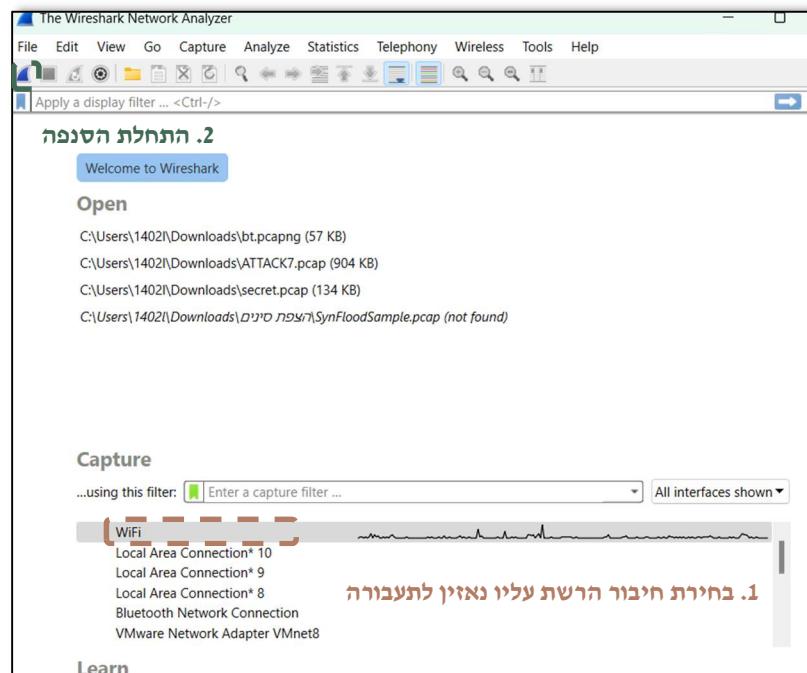
פתיחה קובץ pcap קיים

נבחר את קובץ pcap-> open <- file



הסנה חדש של תעבורה

נבחר את חיבור הרשות עליו נרצה להזין -> נלחץ על הסימן של הסנפיר על מנת להתחיל את ההסנה capture



לאחר מכון מתחwil הסניף להאזין ולתעד את התעבורה. נוכל לראות את המידע שנקלט. על מנת לסייע את ההסנה נלחץ על המרובה האדום.

No.	Time	Source	Destination	Protocol	Length	Info
250	19.518719	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	ICMPv6	86	Neighbor Advertisement 2a00:a041:375c:c00:9cee:a87d:7897
251	19.538258	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	ICMPv6	118	Echo (ping) request id=0x5b21, seq=0, hop limit=64 (request)
252	19.538364	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	2a00:a041:375c:c00:... fe80::46d4:54ff:fe9:...	ICMPv6	118	Echo (ping) reply id=0x5b21, seq=0, hop limit=64 (request)
253	19.784245	fe80::9f45:fa26:6a2... ff02::16		ICMPv6	90	Multicast Listener Report Message v2
254	19.799931	192.168.1.36	192.168.36.4	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (request)
255	20.667398	2a00:a041:375c:c00:... 2a01:111:f100:a004:...	2a01:111:f100:a004:...	TLSv1.2	133	Application Data
256	20.690345	9:a:ba:a7:86:72:21	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.35
257	20.761963	2a01:111:f100:a004:...	2a00:a041:375c:c00:...	TLSv1.2	122	Application Data
258	20.805366	2a00:a041:375c:c00:...	2a01:111:f100:a004:...	TCP	74	64478 + 443 [ACK] Seq=60 Ack=49 Win=513 Len=0
259	21.378717	192.168.1.36	192.168.1.26	TCP	164	64785 + 8009 [PSH, ACK] Seq=441 Ack=441 Win=511 Len=116
260	21.382315	192.168.1.26	192.168.1.36	TCP	164	8009 + 64785 [PSH, ACK] Seq=441 Ack=551 Win=548 Len=116
261	21.424870	192.168.1.36	192.168.1.26	TCP	54	64785 + 8009 [ACK] Seq=551 Ack=551 Win=511 Len=0
262	21.934218	192.168.1.36	5.188.95.9	TCP	55	[TCP Keep-Alive] 64824 + 443 [ACK] Seq=1 Ack=1 Win=510
263	21.958281	5.188.95.9	192.168.1.36	TCP	54	[TCP Keep-Alive] 443 + 64824 [ACK] Seq=0 Ack=2 Win=501
264	21.958341	192.168.1.36	5.188.95.9	TCP	54	[TCP Keep-Alive ACK] 64824 + 443 [ACK] Seq=2 Ack=1 Win=501
265	22.002667	5.188.95.9	192.168.1.36	TCP	66	[TCP Dup ACK 18#1] 443 + 64824 [ACK] Seq=1 Ack=2 Win=501
266	22.388626	192.168.1.38	224.0.0.251	MDNS	124	Standard query 0x0000 PTR _companion-link._tcp.local, "
267	22.388626	fe80::4da:dc56:53c...	ff02::fb	MDNS	144	Standard query 0x0000 PTR _companion-link._tcp.local, "
268	23.445590	192.168.1.36	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

לפנינו כמה זמו
מתחwil ה激发
נשלחה הפאקטה

כתובת מקור
כתובת יעד
פרוטוקול
מודיע נוסף גודל הפאקטה
כלול header, data ו trailer

אם נלחץ 2 לחיצות על אחת מהחbillות שנטפסו, נוכל לראות בפיירוט את השדות של החבילה שנטרפה לפי השכבה ואת ערכיה.

דוגמא לשאלתת DNS שנטפסה בהסנה

Wireshark - Packet 564 - WiFi	
> Frame 564: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface \Device\NPF_{403CCD2E-6EF9-455A-9AC6-5D670C8F2C69}, id=0	
> Ethernet II, Src: Intel_28:b9:fa (2c:6d:c1:28:b9:fa), Dst: SagemcomBroa_9f:10:1c (44:d4:54:9f:10:1c)	
Internet Protocol Version 6, Src: 2a00:a041:375c:c00:9cee:a87d:7897:cd77, Dst: 2001:4860:4860::8888	
0110 = Version: 6	
.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)	
.... 1010 0100 1000 1100 1001 = Flow Label: 0xa48c9	
Payload Length: 49	
Next Header: UDP (17)	
Hop Limit: 64	
Source Address: 2a00:a041:375c:c00:9cee:a87d:7897:cd77	
Destination Address: 2001:4860:4860::8888	
> User Datagram Protocol, Src Port: 65211, Dst Port: 53	
User Datagram Protocol (query)	
Transaction ID: 0xeb30	
Flags: 0x0100 Standard query	
Questions: 1	
Answer RRs: 0	
Authority RRs: 0	
Additional RRs: 0	
Queries	
[Response In: 566]	
0020 a8 7d 78 97 cd 77 20 01 48 60 48 60 00 00 00 ..}x-w . H' H ..	
0030 00 00 00 00 88 88 fe bb 00 35 00 31 d2 a5 eb 30 - 5 1 .. 0	

במהלך הסנה, נתפסות כמותות גדולות של מידע. לרוב נרצה להתמקד ולהפיץ סוגים תעבורה ספציפית. לכן
נשתמש בפילטרים שנועד לעוזר לנו למצוא את התעבורה אותה הספציפית אותה אנו מחפשים.

פילטרים נפוצים:

- סינון לפי פרוטוקול מסוים

מבנה פקודה: נכתוב את שם הפרוטוקול

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
85	9.947062	192.168.1.36	192.168.36.4	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128
193	14.808070	192.168.1.36	192.168.36.4	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128

- סינון לפי כתובת IP (גט source וgmt ip.addr == [ip]

מבנה פקודה: [ip.addr == [ip]]

ip.addr == 192.168.1.36						
No.	Time	Source	Destination	Protocol	Length	Info
83	9.571304	192.168.1.36	20.250.77.142	TCP	55	65384 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP]
84	9.636485	20.250.77.142	192.168.1.36	TCP	66	443 → 65384 [ACK] Seq=2 Ack=2 Win=251 Len=0 [TCP]

- סינון לפי כתובת IP מקור ip.src == [source ip]

מבנה פקודה: [source ip == [ip.src]]

ip.src == 192.168.1.36						
No.	Time	Source	Destination	Protocol	Length	Info
72	8.988658	192.168.1.36	13.107.42.12	TCP	54	65346 → 443 [ACK] Seq=2862 Ack=3454 Win=132352 Len=0
73	9.057387	192.168.1.36	13.107.42.12	TCP	1494	65346 → 443 [ACK] Seq=2862 Ack=3454 Win=132352 Len=1440 [TCP]

- סינון לפי כתובת IP יעד ip.dst == [destination ip]

מבנה הפקודה: [destination ip == [ip.dst]]

ip.dst == 192.168.1.36						
No.	Time	Source	Destination	Protocol	Length	Info
56	8.665140	13.107.42.12	192.168.1.36	TCP	66	443 → 65346 [SYN, ACK] Seq=0 Ack=1 Win=65535
59	8.742204	13.107.42.12	192.168.1.36	TCP	54	443 → 65346 [ACK] Seq=1 Ack=502 Win=4194048 [TCP]

- סינון לפי פורט

מבנה הפקודה: [port == [port] \ tcp.port == [port] \ udp.port == [port]]

tcp.port == 443						
No.	Time	Source	Destination	Protocol	Length	Info
69	8.988399	13.107.42.12	192.168.1.36	TCP	1514	[TCP Out-Of-Order] 443 → 65346 [ACK] Seq=14:1514
70	8.988514	192.168.1.36	13.107.42.12	TCP	66	[TCP Dup ACK 62#1] 65346 → 443 [ACK] Seq=2862

udp.port == 53						
No.	Time	Source	Destination	Protocol	Length	Info
105	14.502912	2a00:a041:375c:c00:... 2001:4860:4860::8888	DNS	90	Standard query 0x11d0 AAAA dns.google	
106	14.503220	2a00:a041:375c:c00:... 2001:4860:4860::8888	DNS	90	Standard query 0xb339 A dns.google	

ניתן לשנן בנוסף לפי כמה חוקים על ידי שימוש ב

אופרטורים

&&	and
	or
!	not

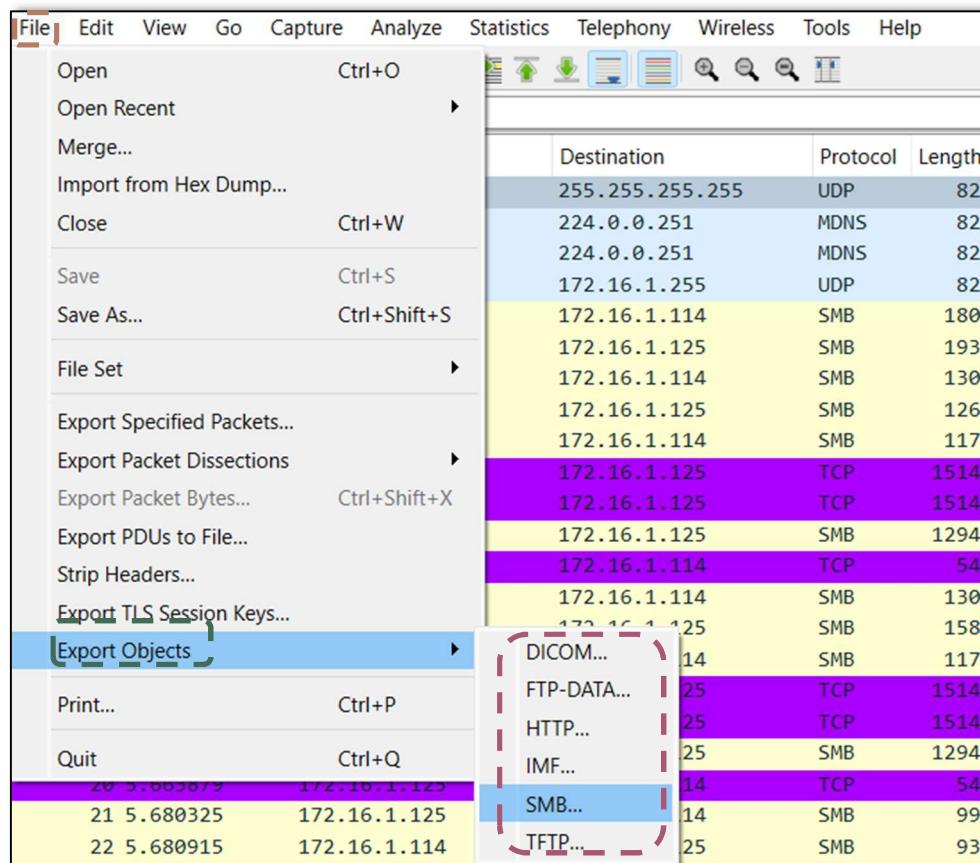
==	equal
!=	not equal
<	smaller than
>	bigger than

<=	small or equal
>=	big or equal

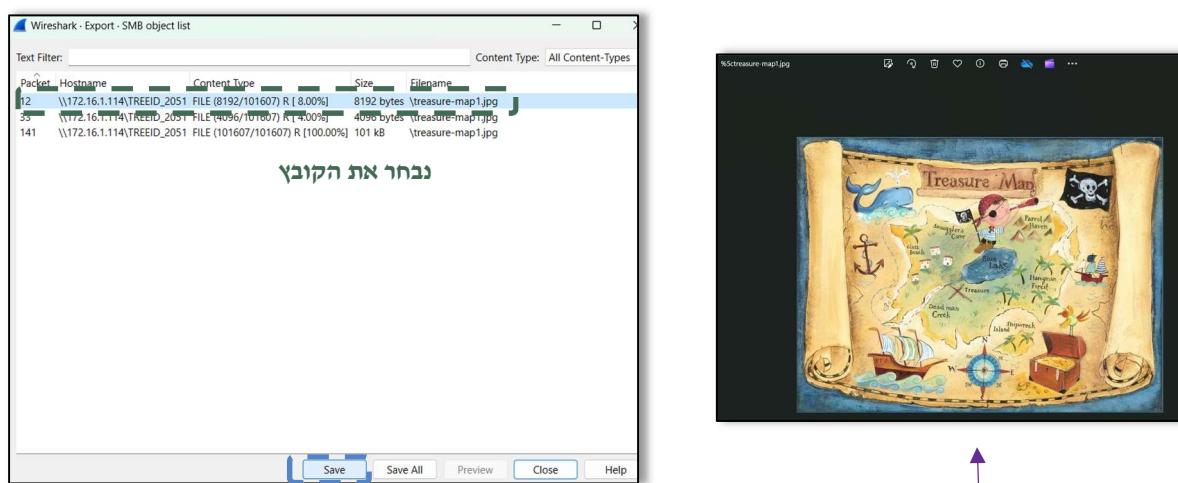
udp.port <= 443 && ip.src == 192.168.1.36						
No.	Time	Source	Destination	Protocol	Length	Info
167	14.746431	192.168.1.36	142.251.37.67	QUIC	79	Handshake, DCID=e8d03238768
173	14.748886	192.168.1.36	142.251.37.67	QUIC	81	Handshake, DCID=e8d03238768

תפיסה של קבצים

-> export objects <- file בחרת ה프וטוקול בו השתמשו על מנת להעביר את הקובץ



כפי שניתן לראות קיבלו גישה לקבצים שהועברו בראשת זה יכול להיות קבצי תמונה, text, excel ועוד. ניתן להוריד אותם למחשב על מנת לפתוח אותם



נבחר את הקובץ

ניתן לראות את הקובץ מההספנה

כאשר נפתח מהמחשב

הצפנה

הצפנה היא תהליך קריפטוגרפי, שמשתמש לרוב באלגוריתמים מתמטיים כדי להמיר את המידע המקורי למוצפן. הצפנה נועדה להסתיר את המידע מעיני האנשים או המערכות שאינם מורשים לצפות בו, לשמר על הפרטיות ולהגן על המידע מפני גישה לא מורשית.

תהליך ההצפנה והפיענוח של המידע נעשה על ידי שימוש במפתחות הצפנה. חזק ההצפנה תלוי בין היתר באורך המפתח. מכיוון שכמויות המפתחות השונות האפשריים הינו 2 בחזקת אורך המפתח (2^{length} אפשרים 2 ערכאים אפשריים בבינארי - 0 ו-1), ככל שכמויות הצירופים האפשריים גדולה יותר, כך הסיכויים למצוא את המפתח הנכון קטנים יותר, וכך ככל שאורך המפתח גדול יותר כך ההצפנה חזקה יותר.

קיימות שתי שיטות הצפנה

- **הצפנה סימטרית** – בשיטה זו קיים מפתח אחד המשותף לכל הצדדים. המפתח משמש גם להצפנה וגם לפיענוח.

קיימים שני סוגים של צפנים :

- **Block Cipher** – המידע מוחלק לבLOCKים בגודל קבוע, כל BLOCK יוצפן בנפרד ויוצג על ידי מספר קבוע של BITSים.
- **Stream Cipher** – כל Byte מוצפן בנפרד אחד אחורי השני. נהוג להשתמש כאשר אורך המידע המיועד להצפנה אינו ידוע מראש. מהיר יותר מבLOCKים אך חלש יותר ונותרים להישבר בתדריות גבוהה יותר

דוגמאות לאלגוריתמים :

○ **(Data Encryption Service) DES** – השפעה באופן משמעותי על תחום הקריפטוגרפיה ותרם להתקדמותו. עובד בשיטת cipher block כאשר כל BLOCK באורך bit 64. המפתח שלו מורכב מbits 56 ונחשב ללא מאובטח עקב אורך המפתח.

○ **(Triple Data Encryption Standard) 3DES** – גרסה משופרת של DES, בה המידע מוצפן שלוש פעמים בשימוש בשלושה מפתחות שונים, כל אחד באורך של 56 BITSים. בכך, אורך המפתח כולל הוא 168 BITS (3⁵⁶), מה שהופך אותו לעמידה גבוהה. גם הוא נחשב כיום ליחסית חלש.

○ **(Advanced Encryption Standard) AES** – אלגוריתם המשתמש במפתח באורך 128/192/256 BITS. עובד בשיטת Block Chiper כאשר כל BLOCK באורך bit 128. מהיר וצריך מעט משאבים. נחשב כיום לאלגוריתם הסימטרי החזק ביותר.

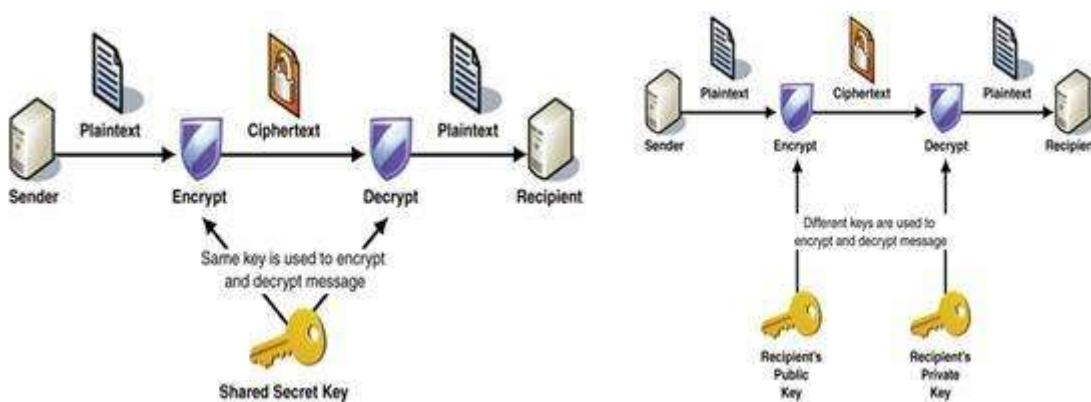
○ **(Ron's Cipher) RC** – אלגוריתם המשתמש במפתח באורך 128 bits.

○ **RC4** – עובד בשיטת Streaming Chiper ומשמש בהצפנה אלחוטית WPA/WEP, SSL, SSH ועוד. RC5 ו-RC6 עובדים בשיטת Cipher Block Chiper ומשתמשים למערכות יציבות וחזקות להצפנה.

הצפנה אסימטרית – בשיטה זו קיימים שתי מפתחות, פרטי וציבורי, כאשר מפתח אחד משמש להצפנה והשני משמש לפיענוח. לכל מפתח ציבורי קיים אץ וرك מפתח פרטי ייחיד המתאים לו, ולהפוך (חח"ע ועל). לרוב המפתח הציבורי משמש להצפנה ונפוץ אותו לאנשים מהם נרצה לקבל את הקוד המוצפן והמפתח הפרטי ישמש לפיענוח.

דוגמאות לאלגוריתמים:

- **(Rivest Shamir Adleman) RSA** – אלגוריתם המשמש להצפנה ולייצירת חתימות דיגיטליות. ניתן ליצור מפתחות באורך 512 או 1024 או יותר ביטים. הוא משמש SSH, TLS, SSL ויכול לשמש להחלפה של מפתחות. כיום משמש כסטנדרט בתחום אבטחת המידע.
- **(Diffie Hellman) DH** – אלגוריתם המשמש להחלפת מפתחות סימטריים על ידי שימוש במפתח אסימטרי. לאלגוריתם יש קבוצות המגדירות את אורך וסוג המפתח.



גיבוב (Hash)

אלגוריתם שממיר קלט באורך משתנה לפלט באורך קבוע, לרוב קצר בהרבה. האלגוריתם הוא חד-כיווני כלומר לא ניתן לתרגם את הערך המגוובב חוזרת ל-data. משתמשים בhash על מנת לוודא שלומות של המידע וכי לאחסן סיסמאות. קיימת אפשרות כי שני ערכי קלט שונים ייווצר פלט hash זהה, מה שעלול לגרום להתקשרות. ככל שאורך hash גבוה יותר ההסתברות פחת נפוצה.

דוגמאות לאלגוריתמים:

- **(Message Digest Algorithm) MD5** – יוצר במפתח באורך 128 bits. אלגוריתם פופולרי אך נחשב כפגיע עקב בעיות התנגשות.
- **(Secure Hash Algorithm) SHA-1** – יוצר מפתח באורך 160 bits. כיום נחשב לא בטוח עקב בעיות התנגשות.
- **(Secure Hash Algorithm) SHA-2** – יוצר מפתח באורך 256/384/512 bits.

רשימות גישה (ACL) הינה רשימה אותה מגדירים על מנת לסנן תובורת רשות לפי חוקים ו מדיניות המוגדרים מראש. רשימות גישה אלו מיושמות לרוב על נתבים חוממות אש ומתקנים, זאת על מנת להגן על הרשת מפני לא מורשת, למדר את המידע, למניע איוומי אבטחה וסיכון נוספים.

הרשת מוגישה לא מורשת, למדר את המידע, למניע איוומי אבטחה וסיכון נוספים.

התובורה נקבעת על פי פרמטרים כגון סוג פרוטוקול, סוגי הודעות בפרוטוקול, כתובות IP של המקור, כתובות IP של היעד ויציאות. לאחר יצירת ACL יהיה ניתן להכיל אותו על המשק, ניתן להחיל אותו על תובורה כניסה ותובורה יוצאת.

קיימים שני סוגי ACL – סטנדרטי ומורחב. ACL הסטנדרטי מגביל ומאפשר תובורה על פי כתובות IP של היעד בלבד. ACL המורחב מגביל ומאפשר תובורה על פי פרמטרים נוספים כгון כתובות IP של היעד פרוטוקולים וסוגי הודעות.

כללי ACL נבדקים אחד אחרי השני, ככלומר הכלל שהגדנו ראשון יבדק ראשון וכך אלה, וכך כאשר נגידר את ACL נגידר קודם את החוקים הספציפיים יותר ולאחר מכן את החוקים הכלליים. חשוב לוודא שהסדר נכון, על מנת להבטיח כי התובורה תסונן כראוי ובהתחם לצרכי הטופולוגיה.

כאשר מגדירים ACL ורוצים להגדיר כתובת רשות של מקור או יעד נרשם את שם הרשות ואת הWildcard. זאת על מנת לציין טווח של כתובות IP. מסכת wildcard דומה ל subnet mask אך משמשות בהיפוך על מנת להגדיר את הטווח, ככלומר כל אוקטטה wildcard תהיה שווה ל 255 פחות האוקטטה ב subnet mask

בסוף ACL קיים כלל דיפולטיבי של Deny שאומר כי אם לא היה כלל ברשימה גישה שאפשר להזעדה זאת לעבור, כבירות מחדר ההזעדה אינה רשאית לעבור והຕובורה תזיהה. ניתן לעקוב וэт על ידי הגדרת permit בסוף הרשימה

המיקום בו נגידר את ACL משפיע על האבטחה והביצועים של הרשות, אנו נמוקם את ACL קרוב ביותר למקור וליעד בהתאם לסוג הרשימה גישה ובהתחם לחוקים על מנת להקטין ככל האפשר את התובורה המיותרת שתעבור עיבוד.

Standard ACL

Standard ACL הינה סוג של ACL אשר מסנן את התעבורה על פי כתובת IP של המקור בלבד. רישומות אלה משמשים לרוב כדי לשנות לגישה למשאים בראשת כגון רשותות משנה ושרותים. רישומות גישה סטנדרטיות מוגדרות על ידי מספר בטוחה 99-1 או 1300-1999.

כנתית ACL סטנדרטי:

Access-list [num] [permit / deny] [source_ip] [log]

num – מצין את מספר ACL אשר ישמש לזיהוי.

permit / deny – מצין אם הכלל מאפשר תעבורת המקור שצוין או חוסם את התעבורה מהכתובות.

אפשר : **permit**

איסור : **deny**

source – נרשם את כתובת IP של המקור או את הרשות עלייה תחול הכלל. ניתן להשתמש בwildcard על מנת להחיל על כמה כתובות. אם נרצה להגיד את הכלל רק על פי כתובת ספציפית, נהוג לשים לפני כתובת המקור את המילה **host**.

log: (אופציונלי) – מאפשר רישום עבור תעבורת התואמת לכל ACL זה.

דוגמא ACL סטנדרטי

access-list 3 permit 10.1.11.0 0.0.0.255

. 10.1.11.0/24 ומאפשרת תעבורת מרשת המקור .

- רישומות גישה סטנדרטיות נהוג להגיד כמה שיותר קרוב אל היעד. זאת מכיוון ACL מסווג זה מסננים על פי כתובת IP של המקור, וכן מניעת תעבורת מקור ספציפי עלול לחסום תעבורת לgitימית מכותבות זאת אל מקורות אחרים

Extended ACL

Extended ACL הינה סוג ACL המסנן את התעבורה על פי כתובת IP מקור ויעד, מספרי פורטים, סוגי הודעות ועוד. הם משמשים על מנת לישם חוקים המאפשרים וחושמים תעבורת ספציפית יותר כגון הגבלת גישה למשאים או חסימה ספציפית של תעבורת.

רישומות אלו מוגדרות על ידי מספרים בטוחה 199-100 או 2699-2000.

כנתית ACL מורחב:

access-list [num] [permit/deny] [protocol] [source] [destination] eq [port] [log]

num – מצין את מספר ACL אשר ישמש לזיהוי.

permit / deny – מצין אם הכלל מאפשר תעבורה מכתובת המקור שצוייניב או חוסם את התעבורה מהכתובות.

אפשר : **permit**

איסור : **deny**

protocol – סוג הпрוטוקול אליו נרצה לעשות פילטור (ip / tcp / udp ועדי)

source – רשום את כתובת IP של המקור או את הרשות עלייה תחול הכלל. ניתן להשתמש בwildcard על מנת להחיל על כמה כתובות. אם נרצה להגדיר את הכלל רק על פי כתובת ספציפית, נהוג לשים לפני כתובת המקור את המילה **host**

destination – רשום את כתובת IP של המקור או את הרשות עלייה תחול הכלל. ניתן להשתמש בwildcard על מנת להחיל על כמה כתובות. אם נרצה להגדיר את הכלל רק על פי כתובת ספציפית, נהוג לשים לפני כתובת המקור את המילה **host**

port – במידה ולא רשנו בפראוטוקול ip אלה נרצה להתייחס לפראוטוקול ופורט ספציפי, רשום את המספר \ השם של הפראוטוקול.

log: (אופציונלי) – מאפשר רישום עבור תעבורה התואמת לכל ACL זה.

דוגמא ACL מורחב:

access-list 107 permit tcp 10.2.11.0 0.0.0.255 host 10.0.0.1 eq 143

כל זה יוצר ACL מורחב מספרו 107 ומאפשר תעבורת TCP מרשת המקור 10.2.11.0.0/24
למארח היעד 10.0.0.1 בפורט 143

סניף ירושלים

מחלקה שירותים גיבוי	מחלקה שירותים ראשית	Costumer Service	Marketing	Design	WIFI	IT	Management	IP	Vlan	מקור/יעד
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	81	70	59	48	37	26			
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	-	+	+	-	-	-	10.1.5 9.0	59	Design
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	+	+	+	-	-	-	10.1.7 0.0	70	Marketing
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	+	+	-	-	-	-	10.1.8 1.0	81	Customer Service

סניף תל אביב

מחלקה שירותים גיבוי	מחלקה שירותים ראשית	Training	Legal	Control	WIFI	IT	Management	IP	Vlan	מקור/יעד
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	63	52	41	30	19	8			
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	-	-	+	-	+	+	10.2.41.0	41	Control
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	-	+	+	-	+	-	10.2.59.0	52	Legal
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	+	-	-	-	+	-	10.2.63.0	63	Training

סניף 3 יונן

מחלקה שרותי גיבוי	מחלקה שרותי ראשית	Research	Finance	Software Development	WIFI	IT	Management	IP	Vlan	מקור/יעד
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	60	50	40	30	20	10			
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	-	+	+	+	+	-	192.168.40.0	40	Software Development
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	+	+	-	-	+	-	192.168.40.0	50	Finance
All – Syslog, NTP, TFTP	All – Syslog, NTP, TFTP	+	+	-	-	-	-	192.168.40.0	60	Research

- נאפשר למחלקות אלו לשלווח הודעות dhcp על מנת שהמחשבים יכולים לקבל כתובות
- נחסום מן מחלקות אלו גישה להתחבר לרכבי הרשת ב ssh ו-telnet.

יצירת ACL

```

יצירת ACL מורחב | R1-C-JRS (config)#
R1-C-JRS (config-ext-nacl)#remark deny access to Management, IT, WIFI, Costumer Service, Syslog
server, NTP server and TFTP server
R1-C-JRS (config-ext-nacl)#permit icmp any any echo-reply
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 10.1.26.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 10.1.37.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 10.1.48.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 10.1.81.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.100.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.100.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.100.7
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.7
R1-C-JRS (config-ext-nacl)#deny tcp any any eq telnet
R1-C-JRS (config-ext-nacl)#deny tcp any any eq 22
R1-C-JRS (config-ext-nacl)#permit ip 10.1.59.0 0.0.0.255 any
R1-C-JRS (config-ext-nacl)#permit udp any any eq 67
R1-C-JRS (config-ext-nacl)#permit udp any any eq 68
R1-C-JRS (config-ext-nacl)#exit
R1-C-JRS (config)#
R1-C-JRS (config)#
יצירת חוקים | R1-C-JRS (config)#
R1-C-JRS (config)#
יצירת ACL מוגן | R1-C-JRS (config)#
R1-C-JRS (config-ext-nacl)#remark deny access to Management, IT, WIFI, Syslog server, NTP server and
TFTP server
R1-C-JRS (config-ext-nacl)#permit icmp any any echo-reply
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 10.1.26.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 10.1.37.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 10.1.48.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 host 10.1.100.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 host 10.1.100.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.70.0 0.0.0.255 host 10.1.100.7
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.7
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.8
R1-C-JRS (config-ext-nacl)#deny tcp any any eq telnet
R1-C-JRS (config-ext-nacl)#deny tcp any any eq 22
R1-C-JRS (config-ext-nacl)#permit ip 10.1.70.0 0.0.0.255 any
R1-C-JRS (config-ext-nacl)#permit udp any any eq 67
R1-C-JRS (config-ext-nacl)#permit udp any any eq 68
R1-C-JRS (config-ext-nacl)#exit
R1-C-JRS (config)#
יצירת ACL מוגן | R1-C-JRS (config)#
R1-C-JRS (config-ext-nacl)#remark deny access to Management, IT, WIFI, Design, Syslog server, NTP
server and TFTP server
R1-C-JRS (config-ext-nacl)#permit icmp any any echo-reply
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 10.1.26.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 10.1.37.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 10.1.48.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 10.1.59.0 0.0.0.255
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 host 10.1.100.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 host 10.1.100.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.81.0 0.0.0.255 host 10.1.100.7
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.4
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.5
R1-C-JRS (config-ext-nacl)#deny ip 10.1.59.0 0.0.0.255 host 10.1.101.7
R1-C-JRS (config-ext-nacl)#deny tcp any any eq telnet
R1-C-JRS (config-ext-nacl)#deny tcp any any eq 22
R1-C-JRS (config-ext-nacl)#permit ip 10.1.81.0 0.0.0.255 any
R1-C-JRS (config-ext-nacl)#permit udp any any eq 67
R1-C-JRS (config-ext-nacl)#permit udp any any eq 68
R1-C-JRS (config-ext-nacl)#exit

```

שיוך לממשקים:

```
כניתה לממשק / תת ממשק |  
R2-C-JRS(config)#int gig0/0.59 |  
R2-C-JRS(config-subif)#ip access-group MRKT-ACL in  
R2-C-JRS(config-subif)#exit  
R2-C-JRS(config)#int gig0/0.70  
R2-C-JRS(config-subif)#ip access-group DSGN-ACL in  
R2-C-JRS(config-subif)#exit  
R2-C-JRS(config)#int gig0/0.81  
R2-C-JRS(config-subif)#ip access-group CSTM-ACL in  
R2-C-JRS(config-subif)#exit
```

AAA הינו פרוטוקול המימוש על מערכות רשות על מנת להבטיח מעקב אחר פעולות המשתמשים וגישה בטוחה למשתמשים ולרשת. AAA המתייחס לשולשה עקרונות בסיסיים בתחום אבטחת המידע

Authentication – אימות, התהליך בו המשתמש מזוהה על ידי המערכת ומאמת לפניה גישה לרשות ולמשתמש. האימות יכול להשתנות במגוון דרכי, המוכרת כוונת הינה שם משתמש וסיסמה. האימות נועדת על מנת לספק ביטחון ולאפשר רק למשתמשים מורשים בלבד לגשת אל המשתמשים.

Authorization – הרשאה, לאחר שהמשתמש אומת יש לאפשר למשתמש רק את המשאבים אותם הוא צריך. כלומר authorization הינו שלב בו ניתנת או נדחת גישה למשתמשים, על פי הרשאות והתפקיד של המשתמש שאומת בשלב הראשון. קיימים על מנת להבטיח כי משתמשים יכולים לגשת אך ורק למשתמש שהורשו להם ולמנוע גישה למשתמשים ומערכות שאינם מורשים.

Accounting – השלב בו נעשה מעקב אחר פעולות המשתמש ושימושיו במשתמשים לשם בדיקה וביקורת. שלב זה כולל ניטור של נסיעות גישה מורשים ובלתי מורשים, שימוש במשתמשים ומידע נוסף ופעולות נוספות אותן יכול לבצע המשתמש

את פרוטוקול AAA ניתן ליישם על ידי שרתים שונים כגון TACACS+ ו-Radius.

TACACS+

TACACS הינו פרוטוקול רשות אשר נוצר על מנת לספק שירות מסווג AAA. הוא משמש על מנת לאבטחו גישה מרוחק לרכיבים ברשת כגון חוממות אשר נתבים ומוגדים. נקרא **TACACS+** היות והוא הגרסתה המעודכנת לפרוטוקול TACACS המקורי אשר פותח על ידי חברת Cisco.

הפרוטוקול משתמש בשיטת client-server. לkus ה-TACACS מותקן על רכיב הרשות והשרות על שרת פיזי מהרכיב.

Authentication

- משתמש מנסה לגשת למפעיל רשות על ידי שימוש בשם משתמש וסיסמה.
- לkus ה- TACACS+ שולח בקשה אימות לשרת TACACS+, יחד עם הפרטיהם של המשתמש.
- השירות מאמת את זהות המשתמש על ידי בדיקת הפרטיהם של המשתמש מול מסד הנתונים המקיים.
- אם הפרטיהם של המשתמש נכונים, השירות ה- TACACS+ שולח תגובה אימות לkus, המציג נתן שהמשתמש מורשה לגשת להתקן הרשות.

Authorization

1. לאחר אימות המשתמש, לkus ה- TACACS+ שולח בקשה הרשות לשרת TACACS+, המציג

- את רמת הגישה וההרשאות של המשתמש.
2. השרת בודק את ההרשאות של המשתמש מול מסד הנתונים המקומי שלו.
 3. אם המשתמש מורה לגשת למשאים המבוקשים, שרת TACACS+ שולח תגבורת הרשאה ללקוח + המציג את רמת הגישה שהוענקה למשתמש.

90

Accounting

1. פרוטוקול TACACS+ תומך גם במקב, הכול מעקב אחר פעילות המשתמש ושימוש במשאים למטרת ביקורת.
2. כאשר משתמש ניגש להתקן רשות, לקוח TACACS+ שולח בקשה למקב לשרת TACACS+. המציג את פעילות המשתמש ושימוש | במשאים.
3. לאחר מכן, שרת TACACS+ רושם את פעילות המשתמש והשימוש במשאים מסד הנתונים שלו.

Radius

כל פרוטוקול ה- RADIUS-TACACS+ משמשים לאבטחת גישה להתקני רשות וספקים אימונות והרשאה למשתמשים. אך ישנו הבדלים משמעותיים ביניהם:

סוג פרוטוקול:

RADIUS הוא פרוטוקול פתוח ווטנדי, בעודו TACACS+ הוא פרוטוקול קנייני שפותח על ידי סיסקו.

אימונות והרשאה:

ב-RADIUS, אישורי המשתמש מאומתים תחיליה, ולאחר מכן נקבעת רמת הגישה. ב-TACACS+, האישורים מאומתים בשלב נפרד לפני קביעת רמת הגישה.

הצפנה:

TACACS+ מספק הצפנה מקצועית האימונות, הרשאה והמקב, בעודו RADIUS מספק רק את האישורים של המשתמש.

מעקב:

TACACS+ מספק מידע מעקב מפורט יותר, בעודו RADIUS פחות מפורט.

תקשורת והתפתחות:

RADIUS משתמש בפרוטוקול UDP לתקשורת, ואף על פי שהוא פחות אמין מ-TCP המשמש את TACACS+, RADIUS יכול להתמודד ביעילות עם מספר גדול יותר של בקשות במקביל.

תכונה	TACACS+	RADIUS
סוג ה프וטוקול	קנייני ליסיקו	תקן פתוח
 הפרצת תהליכיים	הפרדה בין פונקציות AAA אפשר של שימוש בפונקציה אחת בלבד או שילוב עם שיטה אחרת	שילוב פונקציית אימוץ והרשאה ביחד ומקשא על הפעלת פונקציה בודדת
הצפנה	מצפין את כל התקשרות	מצפין רק את הסיסמה בזמן הקמת קשר עם הרשת
תאיימות	יכול לעבוד עם מכשירים של יצרנים שונים יכול לעבוד בצויר לא שונם יכול לעבוד בכל תקינה או לא לעבוד כלל	שימוש במכשירים של יצרנים שונים יכול לעבוד ברמת הרשות Cisco או לא לעבוד כלל
הרשאה	יכול לשולוט ברמת הרשות Cisco באמצעות מקובל בצד Cisco	אינו יכול לשולוט ברמת הרשות Cisco
פרוטוקול תקשורת	TCP נורט 49	1813 / 1812 UDP

הגדרה :

```

כינסה לממשק וירטואלי                                     הגדרת AAA
R2-C-JRS(config)#int loopback 0                                     נתינת כתובת
R2-C-JRS(config-if) #ip address 10.1.150.2 255.255.255.0
R2-C-JRS(config-if) #no shutdown
R2-C-JRS(config-if)#exit
R2-C-JRS(config)#username admin privilege 15 password Admin
R2-C-JRS(config)#aaa new-model                                     הגדרת סוג כניסה
R2-C-JRS(config)#aaa authentication login default group tacacs+ local
R2-C-JRS(config)#tacacs-server host 10.1.100.9 key proj            קישור הרשות
R2-C-JRS(config)#ip domain-name proj
R2-C-JRS(config)#crypto key generate rsa
*Dec 23, 16:45:22.4545: %LINK-5-CHANGED: Interface Loopback0, changed state to up
*Dec 23, 16:45:22.4545: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
The name for the keys will be: R2-C-JRS.proj
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R2-C-JRS(config)#line vty 0 4
*Dec 23 16:45:25.459: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2-C-JRS(config-line)#transport input ssh
R2-C-JRS(config-line)#login authentication default
R2-C-JRS(config-line)#exit
R2-C-JRS(config)#
R2-C-JRS(config)#enable secret admin

```

AAA

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

AAA

Service On Off Radius Port 1645

Network Configuration

Client Name SW2-D-JRS Client IP 10.3.150.4
Secret proj ServerType Tacacs

	Client Name	Client IP	Server Type	Key
2	R2-C-JRS	10.3.150.2	Tacacs	proj
3	SW1-D-JRS	10.3.150.3	Tacacs	proj
4	SW2-D-JRS	10.3.150.4	Tacacs	proj
5	SW1-A-JRS	10.3.150.5	Tacacs	proj
6	SW2-A-JRS	10.3.150.6	Tacacs	proj

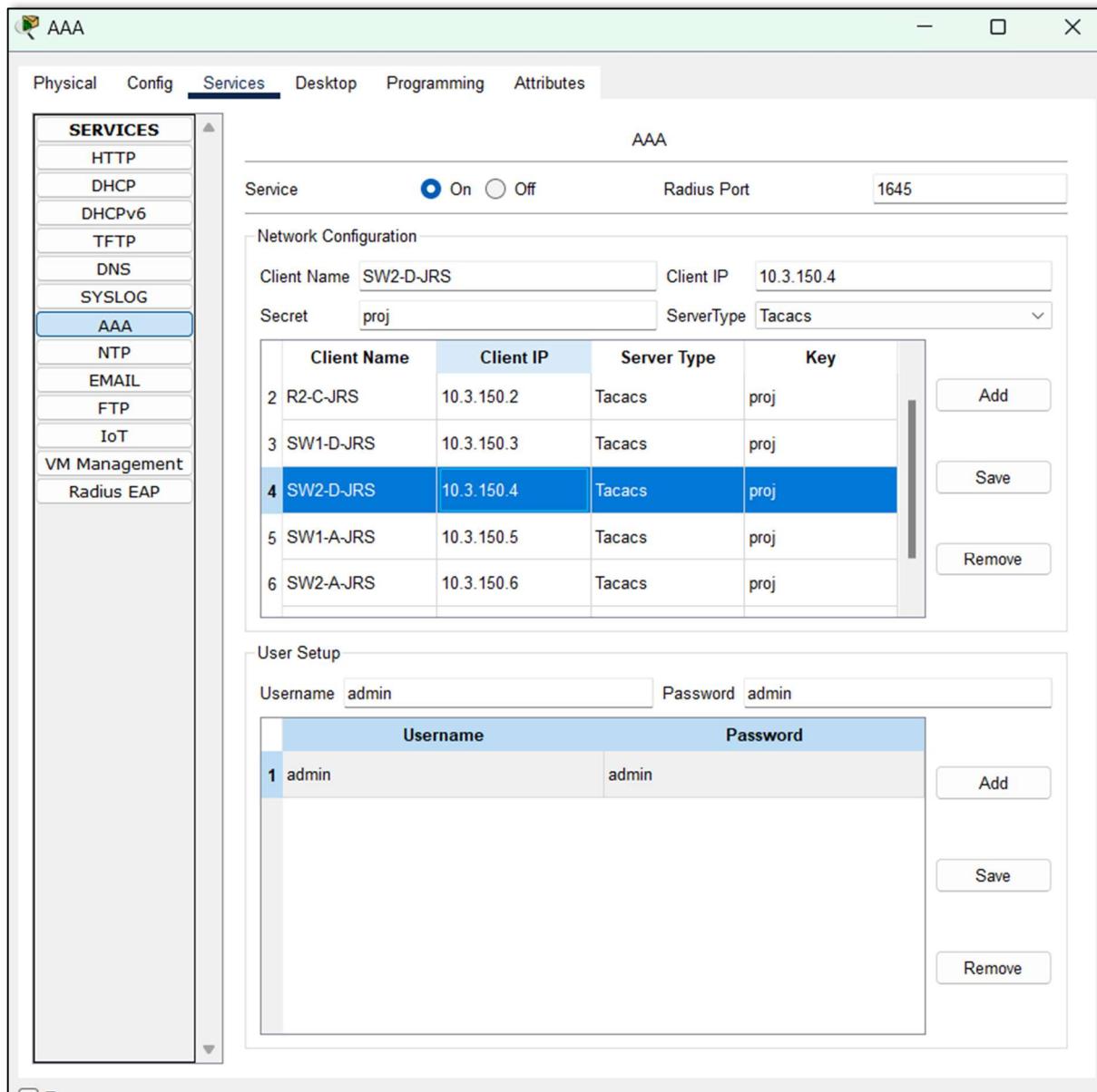
Add Save Remove

User Setup

Username admin Password admin

	Username	Password
1	admin	admin

Add Save Remove



פרוטוקול SSH הינו פרוטוקול רשת מאובטח המספק תקשורת מוצפנת בין שני התקנים ברשת. השימוש בSSH נעשה על מנת לאפשר כניסה מרוחק להתקן רשת, כגון שרת או נתב, ולביצוע פקודות מרוחק.

בקשת חיבור מהלקוות לשרת:

הלקוות שולח בקשה לשרת כדי להתחבר. בבקשת זו, הלקוות מצין את גרסת הפרוטוקול שלו ורשימת אלגוריתמי הצפנה והאימות הנומכמים.

תגובהו של השרת:

השרת משביב בבקשת עם גרסת הפרוטוקול שלו ורשימת אלגוריתמי הצפנה והאימות שהוא תומך בהם. השירות עשו גם לשלוח את המפתח הציבורי שלו לאימות המכונה ללקוות, אם הלקוות לא קיבל את המפתח בעבר.

בקשת אימות מהלקוות:

לאחר אימות המפתח הציבורי של השירות, הלקוות שולח בבקשת אימות לשרת. בבקשת זו, הלקוות מצין את פרטי המשתמש שלו: שם משתמש וסיסמה.

אימות הלקוות על ידי השירות:

השרת מאמת את פרטי המשתמש שסופקו בבקשת האימות. אם האימות הצלחה, השירות שולח הודעה הצלחה בחזרה ללקוות.

יצירת חיבור מאובטח:

לאחר האימות ההצלחה, נוצר חיבור מאובטח בין הלקוות לשרת. כל התקשורת הבאה בין המכונות מוצפנת באמצעות אלגוריתם ההצפנה המוסכם.

גישה מרוחק:

כעת, עם החיבור המאובטח הנוצר, הלקוות יכול לגשת מרוחק לשרת ולבצע פעולות כגון פקודות או משימות אחרות לפי הצורך.

הגדרות:

```

SW1-A-JRS(config)#int vlan 37
SW1-A-JRS(config-if)#no shutdown
SW1-A-JRS(config-if)#ip address 10.1.37.153 255.255.255.0
SW1-A-JRS(config-if) enable secret 123
SW1-A-JRS(config) ip domain-name proj
SW1-A-JRS(config) #username admin privilege 0 password Admin
SW1-A-JRS(config) #line vty 0 4
SW1-A-JRS(config-line) transport input ssh
SW1-A-JRS(config-line) #login local
SW1-A-JRS(config-line) #exit
SW1-A-JRS(config) crypto key generate rsa
*Mar 01, 00:48:31.4848: %LINK-5-CHANGED: Interface Vlan37, changed state to up
*Mar 01, 00:48:31.4848: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan37, changed state to up
The name for the keys will be: SW1-A-JRS.proj
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

```

צירמת סיסמא ל
privilege
נתיתן domain name
צירמת user

בדיקה : פקודות show

```

C:\>ssh -l admin 10.1.150.1

Password:
R1-C-JRS>en
Password: |

```

```

MLS1-A-JRC#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3

```

ה- ASA Cisco הוא פתרון אבטחה מתקדם שמציע חומת אש, VPN ושירותים נוספים. חומת האש משמשת להגנה על הרשת מפני איומים חיצוניים כגון התקפות וירוסים. התהילה בסיסי שבו פועלת חומת האש על ידי בדיקת התעבורה הנכנסת וקבלת החלטות בהתאם למידיניות האבטחה המוגדרת מראש.

ה-ASA משתמש בשילוב של טכניקות בדיקה מתקדמות על מנת לוודא כי כל התעבורה נבדקת במספר שכבות של מודול OSO. למשל, הוא בודק את התעבורה בשכבות של הטרנספורט והישום כדי לזהות ולחשוף פעולות חשודות ואיומים.

יתרונות בשימוש בחומת האש של ASA Cisco

- **בדיקות מתקדמות:** Cisco ASA מציע ערכים גבוהים של בטיחות ואבטחה על ידי פתרונות מתקדמים כמו חומת אש, סקירה חכמה של תעבורה, ניהול תעבורה, אימות מתקדם, ניטור וזיהוי איומים.
- **VPN:** ה-ASA מספק תמיכה מלאה בפתרונות VPN, כולל VPN רשמי (Site-to-Site VPN) ו- VPN רשמי (Remote Access VPN) המאפשרים חיבור מרוחק מאובטח לרשות הארגונית.
- **תקשורת עם קיבולת גבוהה:** ASA מציעה תמיכה בקיבולות גבוהה ויכולת לתקשורת מהירה ואמינה בשרותות גולשות בעומס גבוה.
- **ניהול ונטור:** ה-ASA מציעה פלטפורמה מרכזית לניהול ונטור של כל הפעולות הקשורות לאבטחה, כולל ניהול מרוחק, ניהול תעבורה, ניהול אירועים והתראות.
- **אימות והפנית תעבורה:** ה-ASA מסוגלת לבצע אימות מתקדם ולנהל את תנועת התעבורה על פי מדיניות אבטחה מותאמת אישית.
- **הגנה מתקפות:** עם סולמות טכנולוגיות אבטחה כמו IPS/IDS (מערכת זיהוי ומונעת התקפות) ו- Content Security, ה- ASA מספקת הגנה מתקפות שונות ועדכניות לאיומים החדשניים ביותר.
- **רמת התאמה:** Cisco ASA מציעה גמישות רבה ויכולת להתאים את הפתרון לצרכי העסק ולסביבת הרשת באופן יעיל ואמין.
- **פעול וניהול קלים:** ה- ASA מציעה פעולה ניהול פשוטים על ידי ממשך משתמש ידידותי וכליים נוחים לניהול, ניטור וACHINE נתונים.

ה-ASA עובדת بصورة היררכית, ברמה הגבוהה יותר האזור המאובטח ביותר, ברמה הנמוכה יותר האזור הכי פחות מאובטח. הרמה המקסימלית שנייה לתת לאזור היא 100 והרמה המינימלית 0.

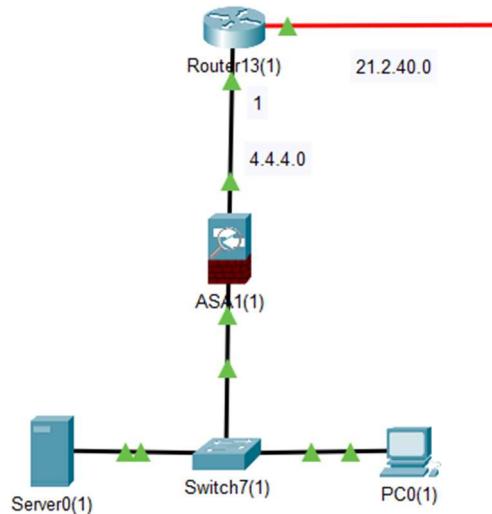
חומר האש פועלת על פי מבנה של שלוש רמות אבטחה: Inside, DMZ ו-Outside. כל אחת מהרמות מייצגת את אזור מסוים ברשות ומקבעת את רמת האבטחה שלו.

רמת האבטחה Inside מייצגת את הרשת הפנימית, כלומר רשת ה-LAN. ברמה זו, האבטחה היא הגבוהה ביותר, והיא מיועדת להגן על המשאים החשובים והרגשיים ביותר ברשות. רמת האבטחה כאן היא 100.

רמת האבטחה DMZ מייצגת את אזור ה-DMZ בראשת, שם מאוחסנים משאבים שצרכים להיות זמינים מהרשות החיצונית וגם מהרשות הפנימית, אך עדין דורשים רמה מסוימת של הגנה. רמת האבטחה ב-DMZ היא 50.

רמת האבטחה Outside מייצגת את הרשות החיצונית, כוללת את רשת ה-WAN. ברמה זו, האבטחה היא הנמוכה ביותר, מאחר ומדובר ברשות החיצונית של הארגון. היא מכילה סיכונים פוטנציאליים רבים ולכן רמת האבטחה שלה היא 0.

הגדרת ASA



```
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#ip address 4.4.4.1 255.255.255.0
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
```

הגדרת כתובת IP לכיוון חוץ
נתינת שם
הגדרת security level

```
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet1/3, changed state to down
ciscoasa(config-if)#ip address 172.16.159.254 255.255.255.0
ciscoasa(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)#security-level 50
```

הגדרת אובייקט מסוג DMZ
הגדרת רשות האיזור dmz
נתינת שם
הגדרת security level

```
ciscoasa(config)#access-list outsideinside extended permit icmp any any echo-reply
ciscoasa(config)#access-list outsideinside extended permit tcp any host 4.4.4.1 eq www
ciscoasa(config)#access-list outsideinside extended permit tcp any host 4.4.4.1 eq 443
ciscoasa(config)#access-list outsideinside extended permit udp any host 4.4.4.1 eq domain
```

יצירת access list
ושיווך

```
ciscoasa(config)#access-list nat-acl extended permit ip any any
ciscoasa(config)#access-group nat-acl out interface inside
```

יצירת access list
ושיווך

```
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 4.4.4.2
```

הגדרת IP Route

Dhcp Snooping

– במתקפה זו, האקר בעל שירות DHCP מתחזק לשרת DHCP של הארגון ומחלק את כתובות IP לרכיבי הקצה. היא מספקת להאקר את כתובות הIP של הרכיבים, וממשירי העובדים והמנהלים, ומאפשרת להאקר להשיג מידע נוסף ולבצע מתקפות נוספות :

- MTM (Man In The Middle) – האקר יגדר את השולק לשרתים Default Gateway.
- לכנתובות של האקר, מה שמאפשר לכך שכל התעבורה שתגיע מהארגון, תעבור דרך האקר.
- DNS Spoofing – לשרתים DHCP קיימת אפשרות לספק את כתובות השירות DNS של הרכיבים. במתקפה זו, האקר יגדר את כתובות השירות DNS שתחולק לרכיבים בארגון כתובות שבעלות האקר. אפשרות להאקר להפנות את המשתמש שביקש אתר מסוים לכתובת IP אחרת שמובילה לאתר מזוייף, ממנו יוכל האקר לקלוט פרטיים אישיים ולגנוב מידע.

על מנת להתגונן מפני DHCP Spoofing נמצא מגנון dhcp snooping

כאשר מפעילים את מגנון dhcp snooping, כל הממשקים של המtag הופכים למצב untrusted ואינם יכולים לקבל הודעות מסווג DHCP OFFER (כלומר אינם יכולים לבקש כתובות IP), מה שמנע קבלה של הודעות משרת DHCP לא נכון. (המגנון חוסם גם הודעות ACK)

את הפורטים אשר מחוברים לכיוון שירות DHCP נגידר כTrust וallow יהיו הפורטים מהם יוכל לקבל הודעות OFFER ובכך כתובות IP למכשירים בארגון. לעומת זאת, שירותי אחרים עדין יכולים לשלוות הצעות (OFFER) לכתובות IP אך ההודעה תיחסם כאשר תגיאו למstag ואינה תישלח לרכיבים בארגון. DHCP Starvation – במתקפה זו, האקר שולח בקשות DHCP מרובות כתובות פיזיות שונות, במטרה לסיים את pool הכתובות ממנו השירות יכול לחלק, על מנת שלא יסופקו כתובות למכשירים אחרים.

הדריכים להתגונן ממתקפה זו :

- שימוש ב-Port Security : הגבלה כמות הכתובות אשר יכולות להילמד על ידי משק מסויים
- שימוש ב-rate limit אשר מגביל את כמות הבקשות לכתובות IP שניתן לבקש DHCP Snooping בפרק זמן מסוים. בכך מונע ניסיון לבקש מרבבות לצורך מתקפה.

הגדרת DHCP Snooping בכלל הנטויפים

את הגדרות אלו נגידיר על המתגים בשכבות ה-

```
SW1-A-JRS (config)#ip dhcp snooping
SW1-A-JRS (config)#ip dhcp snooping vlan 26,37
SW1-A-JRS (config)#no ip dhcp snooping information option
SW1-A-JRS (config)#int range f0/15-16
SW1-A-JRS (config-if-range)#ip dhcp snooping trust
SW1-A-JRS (config-if-range)#ip dhcp snooping limit rate 1
```

הגדרת DHCP Snooping
אפשרות vlans ספציפית

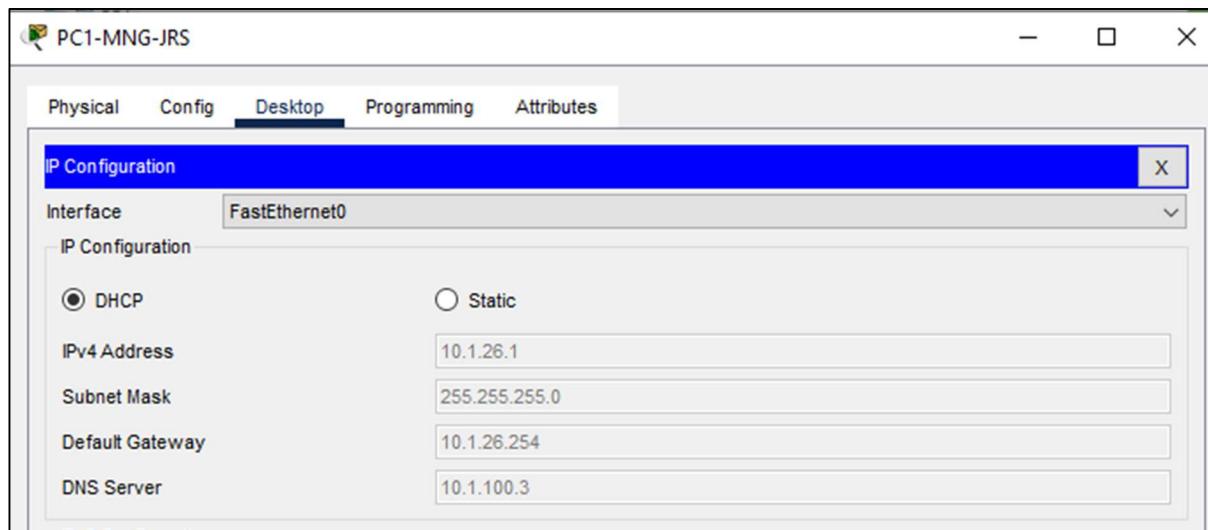
אפשרות לקבל הוזעות offer ו ack ממשקדים אלו

הגבלת כמות ההודעות בפרק זמן מסוים

```
SW2-A-JRS (config)#ip dhcp snooping
SW2-A-JRS (config)#ip dhcp snooping vlan 48,59
SW2-A-JRS (config)#no ip dhcp snooping information option
SW2-A-JRS (config)#int range f0/13-14
SW2-A-JRS (config-if-range)#ip dhcp snooping trust
SW2-A-JRS (config-if-range)#ip dhcp snooping limit rate 1
```

```
SW3-A-JRS (config)#ip dhcp snooping
SW3-A-JRS (config)#ip dhcp snooping vlan 70,81
SW3-A-JRS (config)#no ip dhcp snooping information option
SW3-A-JRS (config)#int range f0/15-16
SW3-A-JRS (config-if-range)#ip dhcp snooping trust
SW3-A-JRS (config-if-range)#ip dhcp snooping limit rate 1
```

נודא שהמחשבים עדיין מצליחים לקבל כתובות IP משרת DHCP



Show commands

show ip dhcp snooping binding

MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface
00:0C:85:0A:46:CE	10.1.26.1	0	dhcp-snooping	26	FastEthernet0/1
00:E0:F9:A8:DE:1C	10.1.37.1	0	dhcp-snooping	37	FastEthernet0/9
Total number of bindings: 2					
כתובת mac	כתובת IP משוייך	סואג	vlan	ממשק אליו מחובר	

show ip dhcp snooping

Interface	Trusted	Rate limit (pps)
FastEthernet0/15	yes	1
FastEthernet0/16	yes	1
FastEthernet0/9	no	unlimited
FastEthernet0/1	no	unlimited

ממשק

האם ניתן לקבל

כמהות בבקשת הכתובות

כתובות משרת dhcp

היכולות להישלח בפרק

דרך משק זה

זמן מסויים

Show ip dhcp database

Agent URL :	
Write delay Timer :	300 seconds
Abort Timer :	
Agent Running :	No
Delay Timer Expiry :	Not Running
Abort Timer Expiry :	Not Running
Last Succeeded Time :	None
Last Failed Time :	None
Last Failed Reason :	No failure recorded.
Total Attempts :	3
Successful Transfers :	0
Successful Reads :	0
Successful Writes :	3
Media Failures :	0
Startup Failures :	0
Failed Transfers :	0
Failed Reads :	0
Failed Writes :	0

הגנות נוספות לידי ביטוי בסניפים:

- שימוש ב-VTP Password בסניף הראשון על מנת לאשר אימומת לפני העברת הגדרות VLANs בין המתגים השונים. הרחבה על הנושא בפרק VTP.
- שימוש בACPV על מנת להעביר תעבורת בין סניפים מרוחקים בצורה מוצפנת. הרחבה על הנושא בפרק VPN.

איתור תקלות ופתרונות

תקלה:

סניף ראשון- `vlangs` : חסר יכולת לתקשר בין וילאים שונים

פתרון:

להעביר את החיבור בין המתג לנtab במצב `trunk`

תקלה:

סניף ראשון- שרתים : אי קבלת מיילים משרת MAIL

פתרון:

לשיק את המשק של המתג שמחובר לשרת `lanv` של השירותים

תקלה:

NAT : הכתובת לא מומר לכטובת חיצונית כאשר מגיעה מהסניף השני

פתרון:

היות ומחובר במטרו, להציג על משק שמחבר בין הסניף הראשון לשני `ip nat inside`

תקלה:

סניף שלישי – OSPF : בעיה בעדכון בטבלת הניתוב בעובודה עם פרוטוקול `ospf`

פתרון:

`clear ip ospf process` הפקודה

תקלה:

ASA : כאשר שולחים `nslookup` לשרת `dns` שנמצא באיזור `asa` אין תגובה

פתרון:

מכיוון שהפאקט טרייסר אינו בניו להגדרות הרבות שישמו בפרויקט, יש להעביר במצב סימולציה ולהעביר במצב זה את התעבורה.

תקלה:

AAA : שרת AAA אינו מוכר על ידי הנtab

פתרון:

הכנסת כתובת IP הנקונה של השרת כאשר מדיררים את AAA

תקלה:

התעבורה באיזור virtual link אינה מצליחה להגיע לטבעתbgp : Virtual Link

פתרונות:

הגדרה על ממשק זה מהסניף השלישי ip nat inside

תקלה:

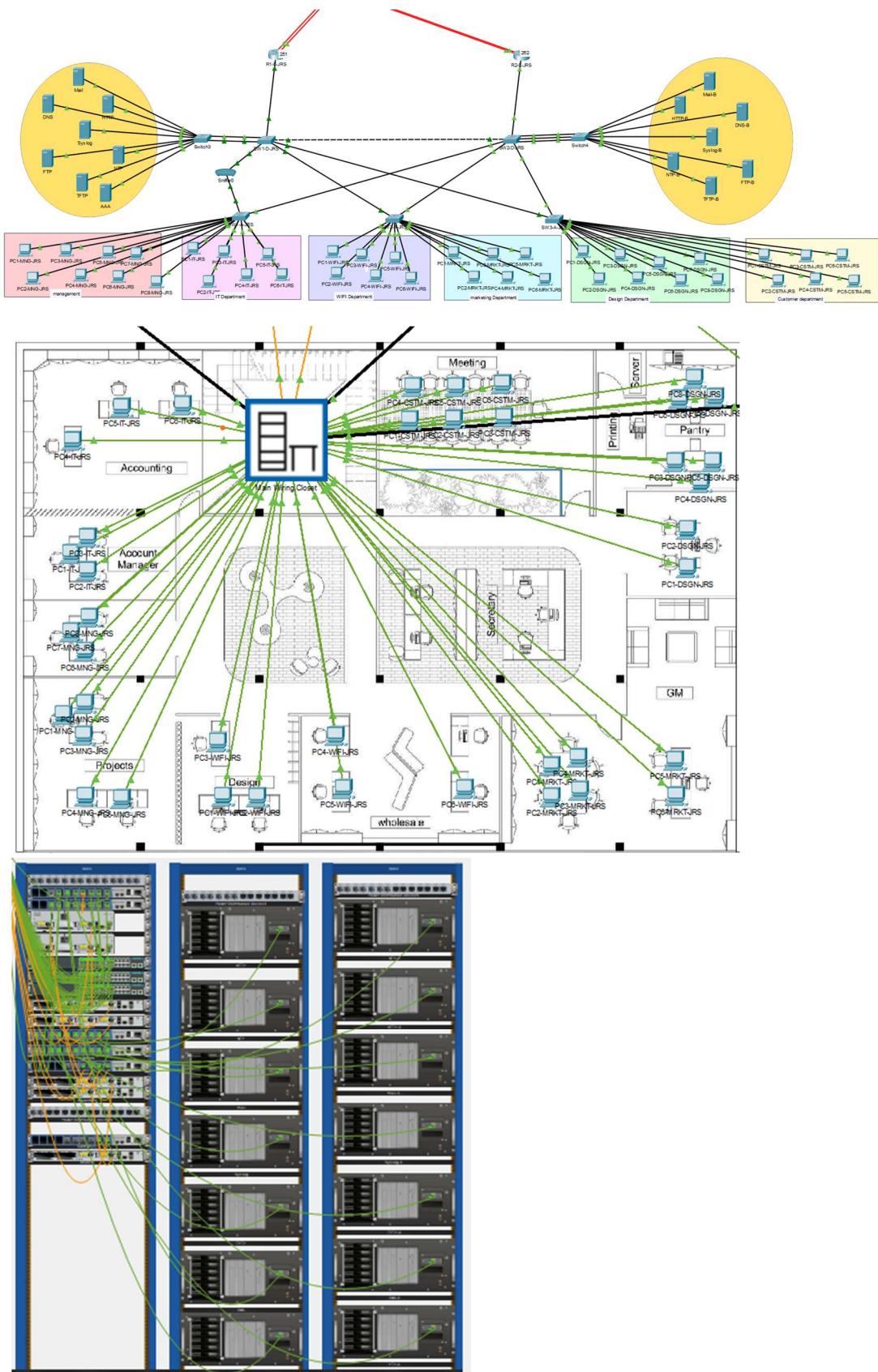
הרשת באיזור stub אינה יכולה לצאת אל טבעתbgp : stub areas

פתרונות:

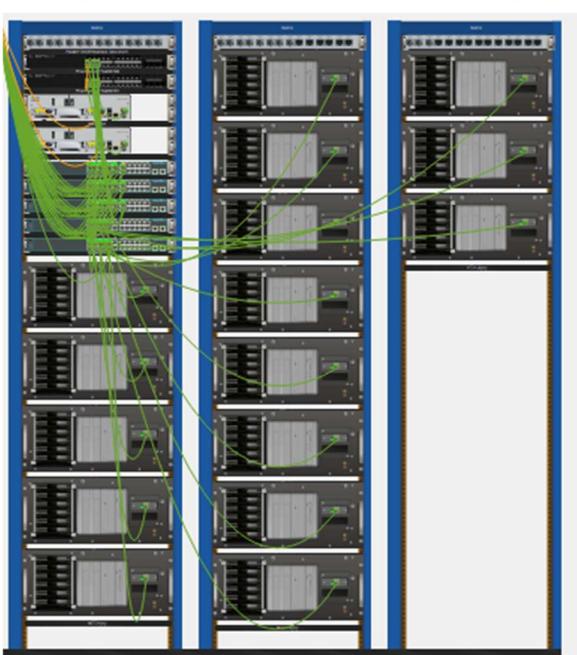
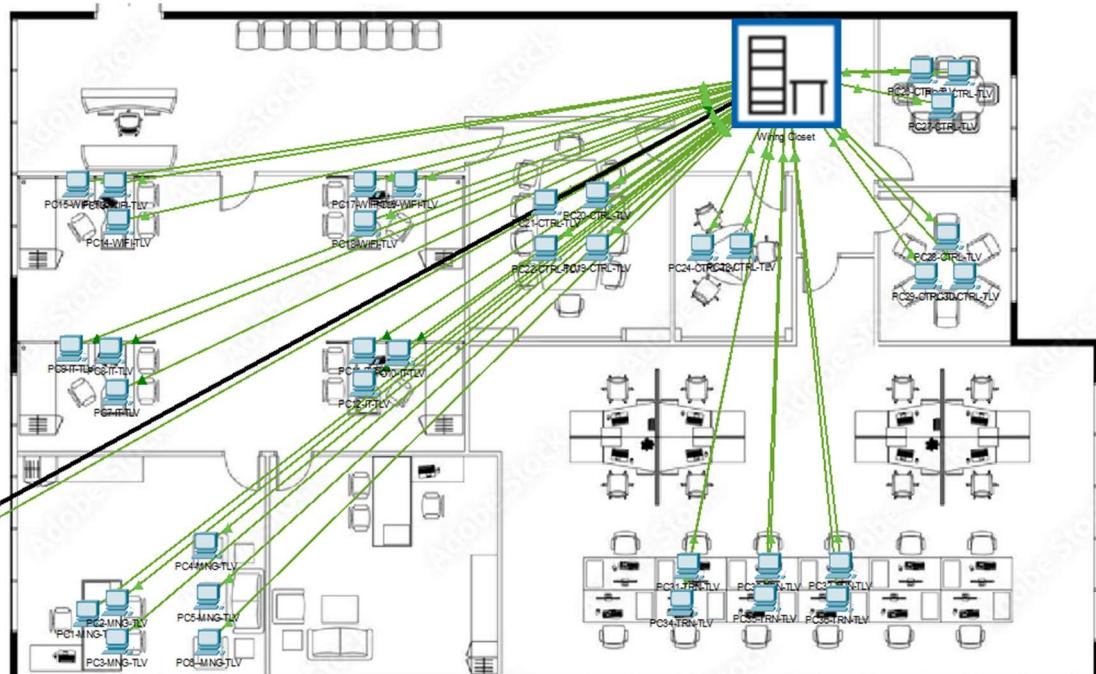
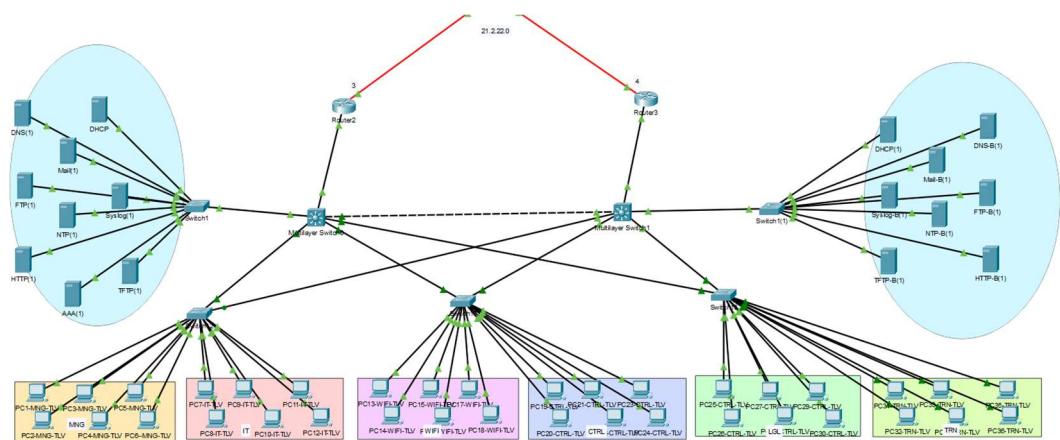
יצירת ניתוב סטטי בראوتر בטבעתbgp אל הרשת החיצונית שמחברת בין ISP לנtb המחבר לstub על מנת שנטים נוספים בטבעת ידעו על רשת חיצונית זו ומיומה.

צילום של הפרויקט:

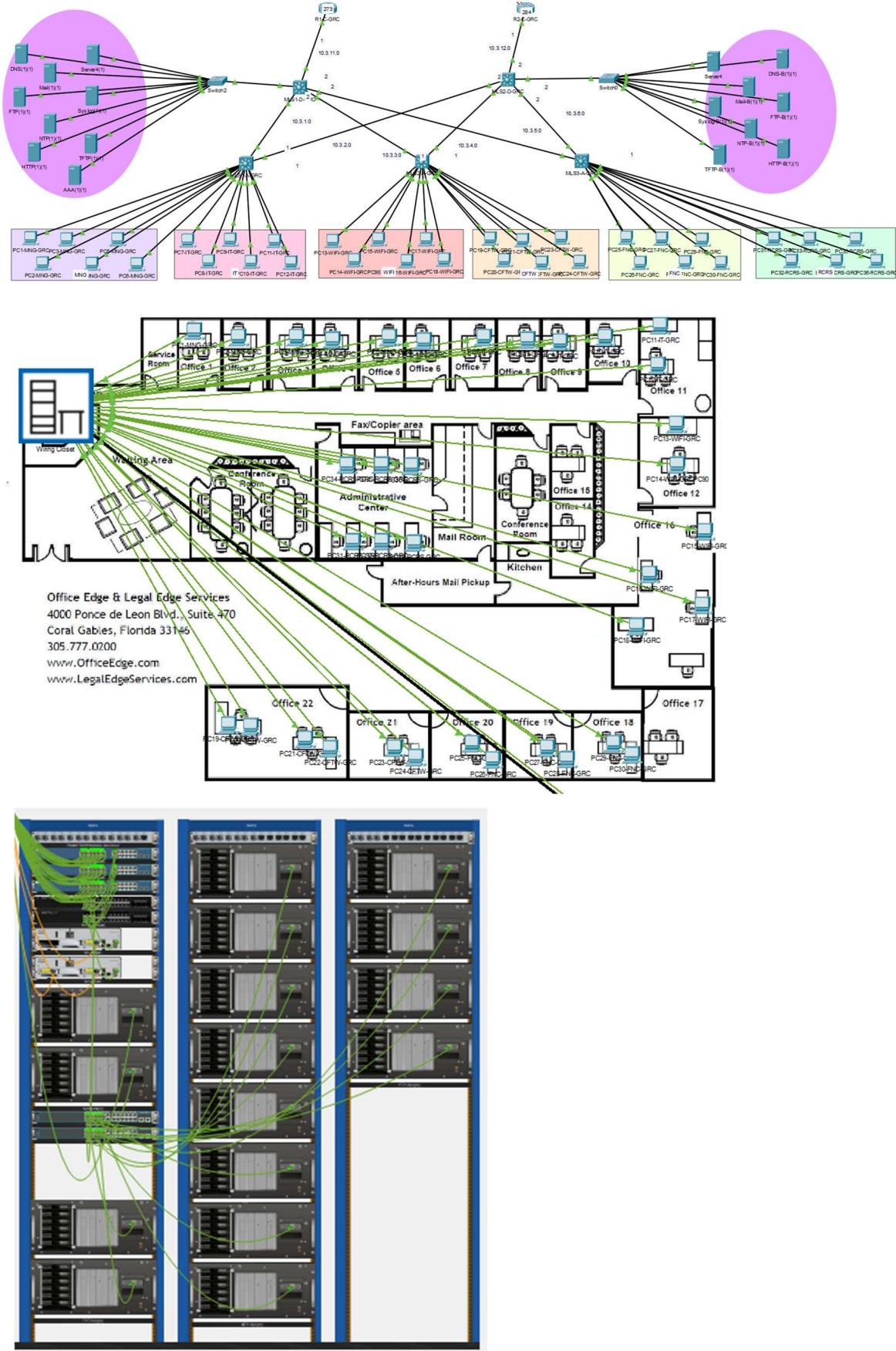
סניף ראשון JRS



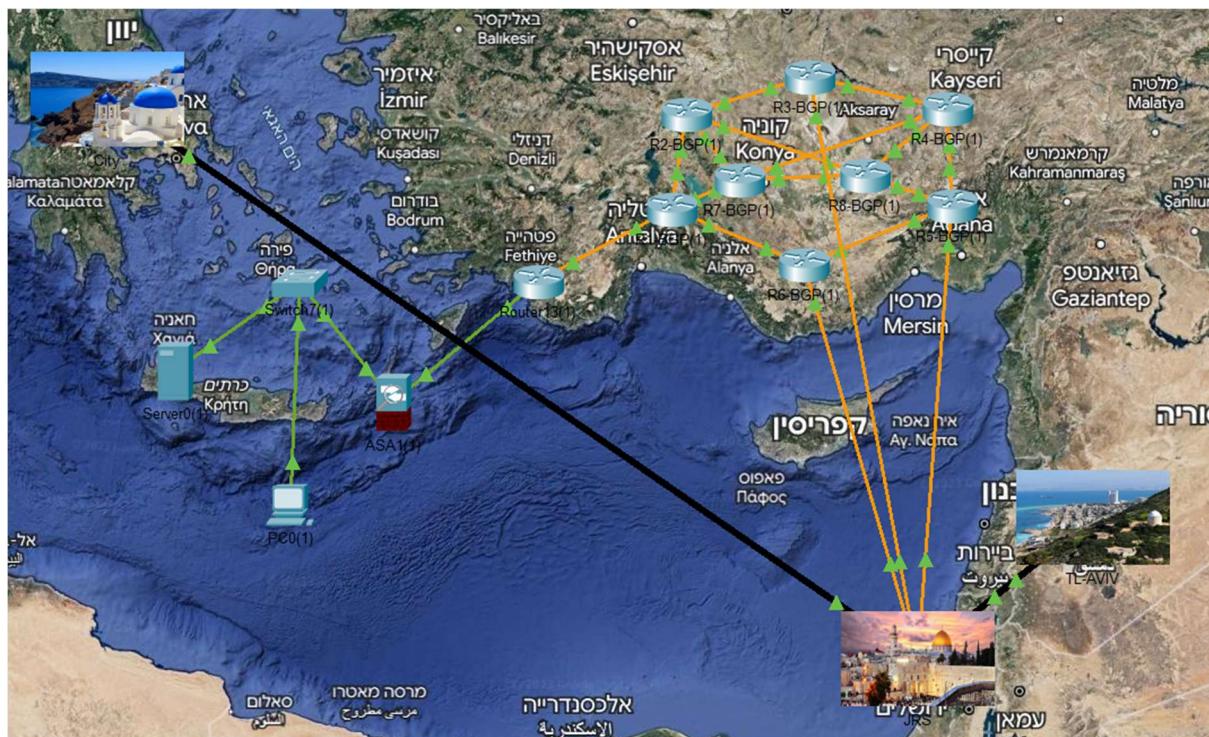
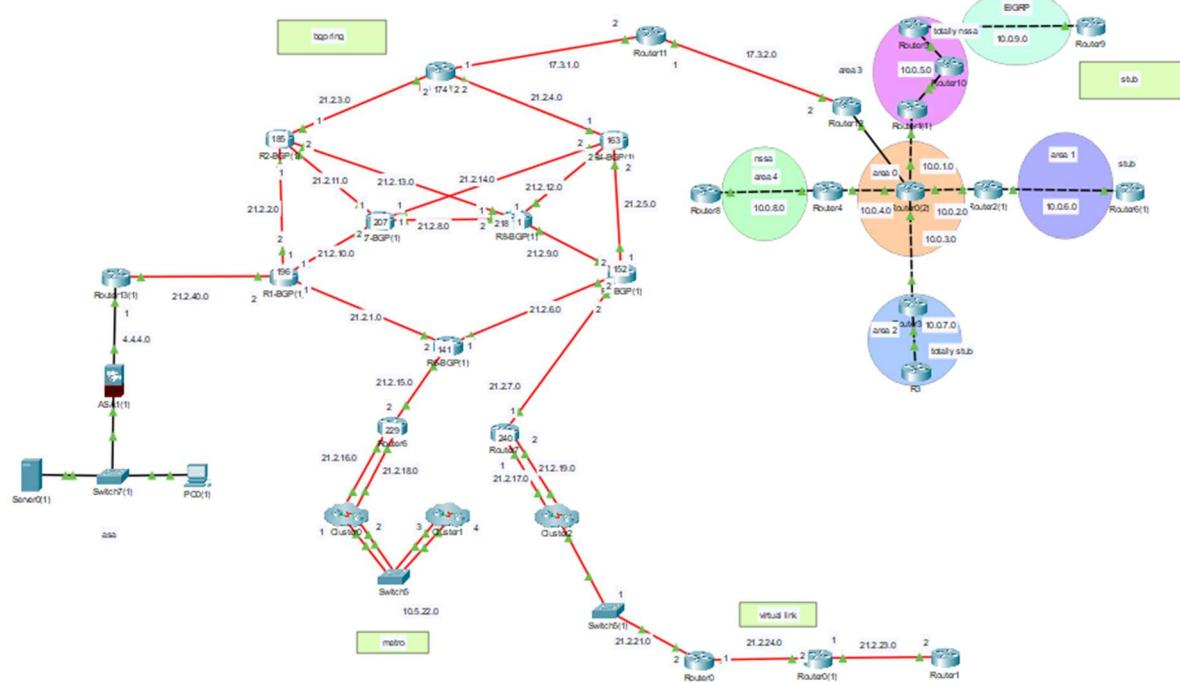
סניף שני TLV



סניף שלישי GRC



wan



רפלקציה

את פרויקט הסיום התחילנו בקייז כיתה יג לאחר שלמדנו חלק גדול מן הידע התיאורטי שנדרש על מנת לבצע את הפרויקט. רכזת המסלול שלחה הוראות מפורטות על כל שלב ושלב והעלה אותנו לתוכנית Monday. ראייתי את כמות ההשגות והידע אותו נדרשו לישים בפרויקט והבנתי שעל מנת להגיש את הפרויקט בצורה הטובה ביותר עלי לחשיך זמן ומחשבה, ללמוד ולישם את הרקע התיאורטי שלמדנו. הפרויקט תרם רבות לידי בתחום רשתות התקשרות ואבטחת המידע. היסכום על הנושאים שנלמדו בכוונות עצמנו, ויצירת פרויקט המכיל את כל הנושאים שנלמדו בתחום זה, נתן לי כלים רבים, ידע וניסיון שעזרו לי להבין את החומר בצורה טובה יותר.

בנוסף במהלך שנת יד למדנו נושאים חדשים והרחבנו נושאים ישנים. החידוד והלימוד לעומק של הנושאים אותם למדנו בשנת יג ביחד עם הניסיון שצברנו עקב העבודה על הפרויקט לימדה אותה רבת ואני מרגישה שהידע שלי בתחום זה רחב בזכות העבודה על הפרויקט והתמייה של המרצים במכיליה. דבר נוסף שעזר לי לצבור ניסיון היה לעזור לחברים מהמסלול בפתרון בעיות ותקלות בפרויקטים שלהם. הייתה לי שבחת עם סטודנטים על מנת למצוא את התקლות בפרויקט שלהם ולהבין למה ההגדרות שהגדירו אין פועלות כראוי. אני מרגישה שפתרונות התקנות לסטודנטים אחרים גרים לי לרצות להבין את החומר יותר לעומק במטרה לפתרו את הבעיה.

יתר על כן, במהלך שנת יד התנסנו במערכות פיזיות בכיתה. היינו מרכיבים טופולוגיות על מוגדים ונתבים אמייניטיים, מגדרים אוטם ומסיקים מהם מסקנות. בנוסף לכך הייתה מעבדות נוספות על הציוויף הפיזי לאחר שעות הלימודים על מנת לבדוק פקודות שאינן נתמכות בpacket tracer, להתנסות במערכות מורכבות ולשפר את יכולותיי בנושא.

בנוסף לכך הייתה מתרגלת במהלך שנת יג את כוונות יג בתחום התוכנה (python, js) ובתחום רשתות התקשרות. התרגולים שיפורו לי יכולות כגון עמידה ודיבור מול קהל, עזרו לי להשתפר בלימוד ובהසברה וגרמו לי לדעת את החומר בצורה הרבה יותר טובה.

אני רוצה להודות לסיוון רכזת המסלול וכל המרצים במכיליה על החוויה, והידע שצברתי במהלך השנתים האלה במכיליה. למדתי המון על עצמי ועל תחום רשתות התקשרות, אבטחת מידע ותחום התכנות.

ביבליוגרפיה :

כללי:

<https://tikshuv-ccna.com>

<https://app.diagrams.net>

<https://shushan.co.il>

:vtp

<https://www.pearsonitcertification.com/articles/article.aspx?p=1868081>

https://en.wikipedia.org/wiki/VLAN_Trunking_Protocol

:vlan

<https://www.techtarget.com/searchnetworking/definition/virtual-LAN>

:Trunk + dot1q

<https://shushan.co.il/%D7%94%D7%A1%D7%91%D7%A8-%D7%A2%D7%9C-trunk-%D7%A2%D7%9C-802-1q>

https://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_iee_e_802.1q.html

:hsrp

<https://networklessons.com/cisco/ccie-routing-switching/hsrp-hot-standby-routing-protocol>

:dhcp

<https://avocado89.medium.com/dhcp-packet-analysis-c84827e162f0>

<https://www.spiceworks.com/tech/networking/articles/what-is-dhcp>

<https://www.webinside.co.il/%D7%9B%D7%9C-%D7%9E%D7%94-%D7%A9%D7%97%D7%A9%D7%95%D7%91-%D7%9C%D7%93%D7%A2%D7%AA-%D7%A2%D7%9C-dns>

:ftp

<https://halemo.net/info/internet/ftp.html>

https://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

:EIGRP

https://en.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol

<https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

:OSPF

<https://www.ibm.com/docs/en/i/7.4?topic=routing-open-shortest-path-first>

<https://shushan.co.il/%D7%94%D7%A1%D7%91%D7%A8-%D7%95%D7%94%D7%92%D7%93%D7%A8%D7%AA-ospf>

:NAT

<https://www.fortinet.com/lat/resources/cyberglossary/network-address-translation>

:GRE

<https://www.juniper.net/documentation/us/en/software/junos/interfaces-ethernet-switches/topics/topic-map/switches-interface-gre.html>

:VPN

https://en.wikipedia.org/wiki/Virtual_private_network

<https://www.cisco.com/web/EA/solutions/en vpn>

:ASA

<https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html>