Text

Description automatically generated

**סמל מוסד - 270538**

**פרויקט גמר**

**הנדסאי מערכות תקשוב**

**התמחות: מערכות תקשוב**

**הנושא: הקמה, תכנון ופיתוח לחברת BlueSpace**

**מנחת הפרויקט : סיון שי**

**המגיש:**

שם: סוקולוב אדוארד ת.ז. 213761711

תאריך ההגשה: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[מבוא 5](#_Toc132914161)

[אודות החברה 6](#_Toc132914162)

[תרשים ארגוני 7](#_Toc132914163)

[מבנה החברה 8](#_Toc132914164)

[מדיניות הקצאת שמות לרכיבי הרשת 10](#_Toc132914165)

[טבלת כתובות של סניפים 13](#_Toc132914166)

[הגדרת שמות וMTOD לרכיבים 14](#_Toc132914167)

[הגדרת שמות לרכיבים בסניף הראשון: 14](#_Toc132914168)

[הגדרת שמות לרכיבים בסניף השני: 15](#_Toc132914169)

[הגדרת שמות לרכיבים בסניף השלישי: 16](#_Toc132914170)

[VTP 18](#_Toc132914171)

[VTP Domain 18](#_Toc132914172)

[VTP Modes 18](#_Toc132914173)

[VLAN’s 21](#_Toc132914174)

[כיצד פועלים רשתות VLAN 21](#_Toc132914175)

[הגדרת vlan’s 21](#_Toc132914176)

[Trunk 28](#_Toc132914177)

[HSRP 30](#_Toc132914178)

[מהו HSRP 30](#_Toc132914179)

[כיצד מורכבת פקטת HSRP 30](#_Toc132914180)

[הגדרת HSRP 32](#_Toc132914181)

[STP 34](#_Toc132914182)

[בעיות שהSTP פותר 34](#_Toc132914183)

[Broadcast storm 34](#_Toc132914184)

[STP port states 35](#_Toc132914185)

[Root Bridge 35](#_Toc132914186)

[Root Port 36](#_Toc132914187)

[Designated Port 36](#_Toc132914188)

[Alternative Port 36](#_Toc132914189)

[Path Cost 36](#_Toc132914190)

[Bridge Protocol Data Units (BPDU) 37](#_Toc132914191)

[סוגים נוספים של STP 37](#_Toc132914192)

[RSTP 37](#_Toc132914193)

[PVST 37](#_Toc132914194)

[Rapid-PVST 37](#_Toc132914195)

[הגדרות בסיסיות ואבטחתיות של STP 37](#_Toc132914196)

[Portfast 37](#_Toc132914197)

[BPDU Guard 37](#_Toc132914198)

[Root Guard 37](#_Toc132914199)

[Router On a Stick (Dot1Q) 43](#_Toc132914200)

[Sub-interfaces 43](#_Toc132914201)

[**DHCP** 45](#_Toc132914202)

[יתרונות הDHCP 45](#_Toc132914203)

[תצורת כתובת IP אמינה 45](#_Toc132914204)

[ניידות 45](#_Toc132914205)

[שרת DHCP 45](#_Toc132914206)

[לקוח DHCP 45](#_Toc132914207)

[מאגר כתובות IP 45](#_Toc132914208)

[Subnet 45](#_Toc132914209)

[תהליך הקצאת כתובות IP 46](#_Toc132914210)

[**DHCP Snooping** 46](#_Toc132914211)

[הגדרת DHCP 47](#_Toc132914212)

[Port-Security 52](#_Toc132914213)

[איך זה עובד? 52](#_Toc132914214)

[הגדרת port security 53](#_Toc132914215)

[IP Routing 55](#_Toc132914216)

[EIGRP 55](#_Toc132914217)

[Distance vector vs Link State 55](#_Toc132914218)

[יחסי שכנות 56](#_Toc132914219)

[Feasible Distance vs Advertised Distance 57](#_Toc132914220)

[Variance command 57](#_Toc132914221)

[ערכי K 57](#_Toc132914222)

[OSPF 62](#_Toc132914223)

[סיכום של תהליך OSPF 62](#_Toc132914224)

[יחסי שכנות 63](#_Toc132914225)

[טבעת BGP 74](#_Toc132914226)

[הגדרת ISP 78](#_Toc132914227)

[יישום OSPF על גבי הMetro Ethernet 79](#_Toc132914228)

[VPN 81](#_Toc132914229)

[הגדרת VPN 82](#_Toc132914230)

[פקודות SHOW 82](#_Toc132914231)

[ACL 86](#_Toc132914232)

[SSH+AAA 90](#_Toc132914233)

[ASA 95](#_Toc132914234)

[ביבליוגרפיה 98](#_Toc132914235)

[איתור תקלות ופתרונן 99](#_Toc132914236)

# מבוא

קוראים לי אדוארד סוקולוב, אני בן 19 וגר בחיפה.

למדתי המדעי המחשב 10 יחל בתיכון חוגים,חיפה במשך 3 שנים וכרגע אני לומד להנדסאי תקשוב במרום תקשוב במכללת כנרת.

הגעתי ללימודים האלה על מנת לצבור כלים חדשים בתחום המחשוב לקריירה העתידית שלי ובעיקר לפרויקטים האישיים שלי שיעזרו לי לממש את הרעיונות שלי בין אם זה בתוכנה או בחומרה.

השאיפה שלי היא לצאת לאזרחות עם כלים שיעזרו לי לנווט את הסביבה שלי לניצול מקסימאלי של הטכנולוגיה למען איכות חיים טובה יותר, בין אם זה משהו קטן שיעשה את חיים נוחים יותר או משהו הרבה יותר מזה.

נושאים שלמדתי בשנת יג + יד:

א. בסיסי נתונים: שליפת נתונים ויצירת טבלאות על ידי פקודות.

ב. רשתות תקשורת: רשתות LAN - כתובות IP וsubnet, פרוטוקול Ethernet, ,VLAN

TRUNK, VTP ,DOT1Q

.OSPF, EIGRP,RIP,STATIC ROUTE :ניתוב פרוטוקולי – WAN רשתות

.ועודDNS, DHCP,STP,NAT :ושרתים פרוטוקולים

ג.JS, CSS, HTML - בניית אתרים, ותכנות שלהם.

ד. שפת תכנות כמו: c,c# וpython

Linux: DNS, MAIL,FTP,SQL,WEB ב שרתים הקמת. ה

ו. חשמל ואלקטרוניקה. הכרה של רכיבים חשמליים ואת פעולותיהם.

ז.מערכות ספרתיות. הכרות עם שערים לוגים,אוגרים, מקודדים ועוד.

ח.HACKERU : למידה על מתקפות שונות ואיך למנוע.

ט. אבטחת מידע: למידה על כל מיני סוגי התקפות, דרכים להגן מפניהם, סוגי נוזקות ועוד.

# אודות החברה

BlueSpace היא חברה המתעסקת בפיתוח, תחזוקה, ותמיכה טכנית למוצרים שלה אשר מתרכזות בכל הקשור למערכות ניהול עסק מתקדם מרחוק.

לחברה יש שלושה סניפים ברחבי הארץ כאשר כל אחד מהם מתמקד בחלק שבו הוא הכי מתמחה. הסניף העיקרי של החברה נמצא בתל אביב, ושם נמצא הדירקטוריון של החברה.

המוצרים שהחברה מציאה ללקוחות שלה הן פתרונות אוטומציה ובקרה לבתי עסק גדולים וקטנים המאפשרים לבעלי העסק יותר שליטה על העסק, ובעלויות קטנות יותר ממה שיציע מנהל אנושי.

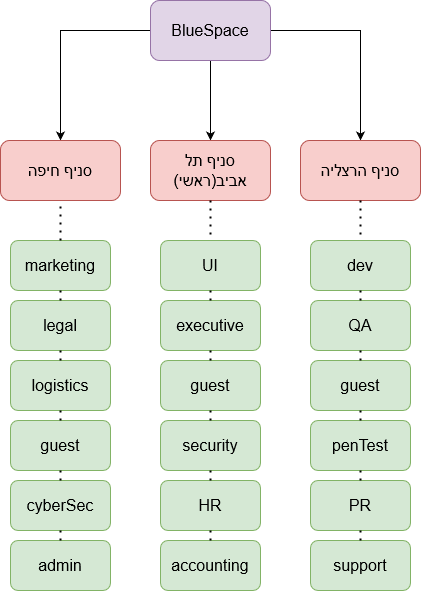
בסופו של היום כל עלות נוספת למעסיק עובר ללקוחות, וכאשר למדינה יש בעיה של יוקר מחייה, לא יזיק לקצץ בעלויות בכל מקום שאפשר, ובמיוחד במשרה שגם ככה מקבלת שכר גבוה בהרבה מהממוצע.

כרגע החברה נמצאת בשלב של סטארט-אפ בה היא מנסה לגייס הון דרך השקעות וחובות. על מנת למתן סיכונים, דירקטוריון החברה הוציא הנחייה לא להוציא כספים על מוצרים מיותרים שאינם תורמים לתפעול החברה, וכתוצאה מכך נדרש מהמנהלי רשת לתכנן רשת אופטימלית ככל הניתן מבלי לשבש את פעילותה ואבטחתה התקינה (יש לקחת בחשבון שיתירות מינימלית נדרשת על מנת להבטיח את פעילותה התקינה של הרשת).

כאשר החברה תהיה רווחית היא תדרוש יותר משאבים מהרשת. על מנת לצמצם עלויות נוספות חשוב למנהלי רשת לקחת בחשבון גדילה עתידית של הרשת ולתכנן אותה בהתאם.

ניתן גם להוסיף שככל שהחברה תגדל בשווי והרווחיות שלה היא תידרש להתמודד עם איומים חדשים ומתוחכמים יותר, לכן חשוב לתת לה בסיס אבטחתי טוב כך שלפחות איומים בסיסים יותר יחסמו ישר. המטרה של מנהלי הרשת בחברה היא לתקן את כל פרצות האבטחה הידועות בפרוטוקולי ורכיבי התקשורת הקיימים ברשת הארגונית.

# תרשים ארגוני



# מבנה החברה

חברת Bluespace מתפרסת לשלושה סניפים ברחבי הארץ: סניף ראשי בתל אביב , ושני סניפי משנה

בחיפה והרצליה. המחלקות השונות ותפקידן :

|  |  |  |
| --- | --- | --- |
| שם המחלקה | קיצור | תפקיד |
| Admin | Adm | תחזוק מערכות מחשוב ותקשורת אשר מתעסקת בתחזוק כל הרשת הארגונית. זקוקה לגישה מלאה לרשת הארגונית |
| Executive | Exc | מחלקה למנהלי החברה מתעסקת בניהול כל החברה והיא כוללת מסמכים רגישים מאוד, כך שנדרשת אבטחה גבוהה מן הרגיל |
| Guest | Gst | מחלקה לאורחים ופנאי אשר ממוקמת בכל סניף. מחלקה זו פתוחה באופן מוחלט וחייבת בידוד מלא מהרשת הארגונית |
| Security | Sec | מחלקה למאבטחי הבניין. מחלקה זו מתעסקת בקישור מצלמות האבטחה למסכים של המאבטחים |
| HR | Hr | מחלקת משאבי אנוש. מחלקה המתעסקת במשאבי אנוש ומחייבת קישור למסד נתונים בו יש מידע על כל העובדים. מחלקה זו זקוקה לאבטחת מידע מוגברת |
| Accounting | Act | מחלקת חשבונאות לניהול תקציבי החברה. מחלקה זו זקוקה לקישור למסד נתונים בו נשמר המידע הפיננסי, והיא זקוקה לאבטחה מוגברת |
| dev | Dev | מחלקת פיתוח מוצרים. מחלקה זו מצריכה גישה לאינטרנט על מנת שהעובדים יוכלו להיעזר בו, אך היא גם זקוקה לאבטחה מוגברת כיוון שהsource code נשמר בו |
| QA | Qa | מחלקת בדיקת איכות. מחלקה זו אחראית לבדיקת איכות המוצר |
| penTest | Pnt | רשת נפרדת לבדיקת חדירויות. רשת זו מחייבת בידוד מוחלט מהרשת האירגונית כיוון שנעשים בו בדיקות חדירויות אשר עשויות לפגוע במכשירים. |
| PR | Pr | מחלקת יחסי ציבור. מחלקה זו מתעסקת ביחסי ציבור והיא זקוקה לחיבור לאינטרנט |
| support | Sup | מחלקת שירות לקוחות ותמיכה טכנית. מחלקה זו אחראית על מתן עזרה ללקוחות שלה והיא מצריכה חיבור לאינטרנט, קישור למסד נתונים השומר נתוני לקוחות, והבטחה מוגברת על מנת שהמידע לא יזלוג החוצה |
| Marketing | Mkt | מחלקת שיווק. במחלקה זו נדרש חיבור לאינטרנט |
| Legal | Lgl | מחלקת משפטים. זקוקה לחיבור לאינטרנט |
| Logistics | Lgs | מחלקת לוגיסטיקה. מחייבת קישור למסד נתונים המתעסק בלוגיסטיקה |
| cyberSec | Cys | מחלקת אבטחת מידע. מחלקה שמחפשת ניסיונות פריצה בזמן אמת.זקוקה לגישה מלאה לרשת הארגונית. |
|  |  |  |

# מדיניות הקצאת שמות לרכיבי הרשת

**סניף ראשון – הרצליה (HZL)**

|  |  |  |  |
| --- | --- | --- | --- |
| **הסבר קיצור** | **קיצור** | **מיקום**  **בטופולוגיה** | **שם הרכיב** |
| RT = Router  C = Core | RT01-C-HZL RT02-C- HZL | Core | Router 1941 |
| SE = Switch Empty  D = Distribution | SE1-D- HZL  SE2-D- HZL | Distribution | Switch-PT-Empty |
| SW = Switch A = Access | SW01-A- HZL  SW02-A- HZL | Access | Switch 2960 |
| <n> = Number in the  department  <d> = Department name | <d>-HZL-<n> | - | PC |
| <s> = server type  <n> = number | HZL-<s>-<n> | - | server |

**דוגמאות לשמות התקני הקצה בסניף הרצליה (HZL)**

|  |  |  |
| --- | --- | --- |
| **שם ההתקן** | **קיצור מחלקה** | **מחלקה** |
| dev-HZL-01  dev-HZL-02 | dev | Development |
| PR-HZL-05 | PR | PR |
| QA-HZL-05 | QA | QA |

**סניף שני – תל אביב (TLV)**

|  |  |  |  |
| --- | --- | --- | --- |
| **הסבר קיצור** | **קיצור** | **מיקום**  **בטופולוגיה** | **שם הרכיב** |
| RT = Router  C = Core | RT01-C- TLV RT02-C- TLV | Core | Router 1941 |
| SE = Switch Empty  D = Distribution | SE1-D- TLV  SE2-D- TLV | Distribution | Switch-PT-Empty |
| SW = Switch A = Access | SW01-A- TLV  SW02-A- TLV | Access | Switch 2960 |
| <n> = Number in the  department  <d> = Department name | <d>- TLV -<n> | - | PC |
| <s> = server type  <n> = number | TLV-<s>-<n> | - | server |

**דוגמאות לשמות התקני הקצה בסניף תל אביב (TLV)**

|  |  |  |
| --- | --- | --- |
| **שם ההתקן** | **קיצור מחלקה** | **מחלקה** |
| UI-TLV-02  UI-TLV-03 | UI | UI |
| exec-TLV-02 | exec | Executive |

**סניף שלישי – חיפה (HFA)**

|  |  |  |  |
| --- | --- | --- | --- |
| **הסבר קיצור** | **קיצור** | **מיקום**  **בטופולוגיה** | **שם הרכיב** |
| RT = Router  C = Core | RT01-C-HZL RT02-C- HFA | Core | Router 1941 |
| SE = Switch Empty  D = Distribution | SE1-D- HFA  SE2-D- HFA | Distribution | Switch-PT-Empty |
| SW = Switch A = Access | SW01-A- HFA  SW02-A- HFA | Access | Switch 2960 |
| <n> = Number in the  department  <d> = Department name | <d>- HFA -<n> | - | PC |
| <s> = server type  <n> = number | HFA-<s>-<n> | - | server |

**דוגמאות לשמות התקני הקצה בסניף חיפה (HFA)**

|  |  |  |
| --- | --- | --- |
| **שם ההתקן** | **קיצור מחלקה** | **מחלקה** |
| admin-HFA-02  admin -HFA-03 | Adm | admin |
| legal -HFA-03 | lgl | legal |

# טבלת כתובות של סניפים

הקצאת כתובות הip נעשת כך שהאוקטטה הראשונה היא 10 מכיוון שמדובר בכתובת רשת פנימית ממחלקה A, האוקטטה השניה מציינת את מספר הסניף:1 – הרצליה, 2 – תל אביב, 3 – חיפה, האוקטטה השלישית מציינת את הvlan Id של המחלקה, והאוקטטה הרביעית שייכת לhosts.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| סניף | מחלקה | כמות שרתים | כמות מחשבים | VLAN ID | NETID | Subnet Mask | Default Gateway |
| הרצליה | Dev |  | 8 | 10 | 10.1.10.0 | 255.255.255.0 | 10.1.10.254 |
| QA |  | 6 | 20 | 10.1.20.0 | 255.255.255.0 | 10.1.20.254 |
| Guest |  | 8 | 30 | 10.1.30.0 | 255.255.255.0 | 10.1.30.254 |
| penTest |  | 6 | 40 | 10.1.40.0 | 255.255.255.0 | 10.1.40.254 |
| PR |  | 6 | 50 | 10.1.50.0 | 255.255.255.0 | 10.1.50.254 |
| Support |  | 6 | 60 | 10.1.60.0 | 255.255.255.0 | 10.1.60.254 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| סניף | מחלקה | כמות שרתים | כמות מחשבים | VLAN ID | NETID | Subnet Mask | Default Gateway |
| תל אביב | UI |  | 8 | 10 | 10.2.10.0 | 255.255.255.0 | 10.2.10.254 |
| Executive |  | 6 | 20 | 10.2.20.0 | 255.255.255.0 | 10.2.20.254 |
| Guest |  | 8 | 30 | 10.2.30.0 | 255.255.255.0 | 10.2.30.254 |
| Security |  | 8 | 40 | 10.2.40.0 | 255.255.255.0 | 10.2.40.254 |
| HR |  | 8 | 50 | 10.2.50.0 | 255.255.255.0 | 10.2.50.254 |
| accounting |  | 8 | 60 | 10.2.60.0 | 255.255.255.0 | 10.2.60.254 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| סניף | מחלקה | כמות שרתים | כמות מחשבים | VLAN ID | NETID | Subnet Mask | Default Gateway |
| חיפה | marketing |  | 6 | 10 | 10.3.10.0 | 255.255.255.0 | 10.3.10.254 |
| legal |  | 8 | 20 | 10.3.20.0 | 255.255.255.0 | 10.3.20.254 |
| Guest |  | 6 | 30 | 10.3.30.0 | 255.255.255.0 | 10.3.30.254 |
| logistics |  | 9 | 40 | 10.3.40.0 | 255.255.255.0 | 10.3.40.254 |
| cyberSec |  | 6 | 50 | 10.3.50.0 | 255.255.255.0 | 10.3.50.254 |
| admin |  | 6 | 60 | 10.3.60.0 | 255.255.255.0 | 10.3.60.254 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# הגדרת שמות וMTOD לרכיבים

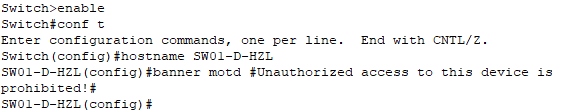
על מנת ליצור סדר ברשת ניתן לתת שם רכיב לכל רכיב רשת בעזרת הפקודה hostname. לאחר הגדרת הפקודה ניתן יהיה לראות את שם הרכיב המעודכן בפתיחה של כל שורת פקודה.

לפני כניסה למשתמש חשוב להראות למשתמש הצהרה שכניסה לא מורשת לרכיבים אסורה.

על מנת להגדיר שם לרכיב יש להכנס תחילה למצב קונפיגורציה ואז לרשום את הפקודה hostname ומיד לאחריו לרשום את השם

## הגדרת שמות לרכיבים בסניף הראשון:

הגדרת שם לSW01-D-HZL :



הגדרת שם לSW02-D-HZL :

Text

Description automatically generated

הגדרת שם לSW01-A-HZL :

Text

Description automatically generated

הגדרת שם לSW02-A-HZL :

Text

Description automatically generated

הגדרת שם לSW03-A-HZL :

Text, letter

Description automatically generated

הגדרת שם לRT01-C-HZL :

Text

Description automatically generated

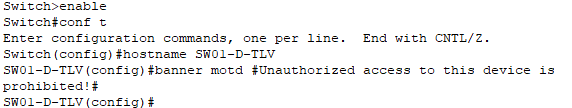
הגדרת שם לRT02-C-HZL :

Text

Description automatically generated

## הגדרת שמות לרכיבים בסניף השני:

הגדרת שם לSW01-D-TLV :

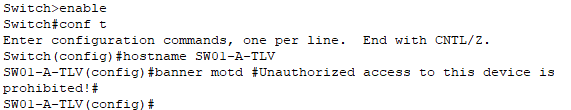


הגדרת שם ל SW02-D- TLV:

Text

Description automatically generated

הגדרת שם ל SW01-A- TLV:



הגדרת שם ל SW02-A- TLV:

Text

Description automatically generated

הגדרת שם ל SW03-A- TLV:

Text

Description automatically generated

הגדרת שם ל RT01-C- TLV:

Text

Description automatically generated

הגדרת שם ל RT02-C- TLV:

Text, letter

Description automatically generated

## הגדרת שמות לרכיבים בסניף השלישי:

הגדרת שם לSW01-D-HFA :

Text

Description automatically generated

הגדרת שם ל SW02-D- HFA:

Text

Description automatically generated

הגדרת שם ל SW01-A- HFA:

Text, letter

Description automatically generated

הגדרת שם ל SW02-A- HFA:

Text, letter

Description automatically generated

הגדרת שם ל SW03-A- HFA:

Text

Description automatically generated

# VTP

VTP הוא פרוטוקול רשתות בשכבה 2 שנועד לנהל את היצירה והמחיקה של רשתות VLAN ולשמור על סנכרון מסדי נתונים של VLAN ברחבי הרשת. באמצעות פרוטוקול זה, מנהל רשת יכול להוסיף או למחוק רשתות VLAN ולהעביר את השינויים הללו באופן אוטומטי לכל שאר המתגים ברשת. ללא VTP, מתגים אינם מחליפים מידע על רשתות VLAN ומנהל הרשת היה צריך להגדיר VLAN ידנית על כל אחד מהמתגים.

הפרוטוקול עוצב סביב רעיון הניהול הריכוזי. למתג אחד או יותר מוקצה התפקיד של שרת VTP. כל עדכונים שנעשו על מתגים אלה נשלחים דרך VTP למתגים האחרים, שהם לקוחות VTP.

## VTP Domain

VTP Domain מוגדר על ידי כל המתגים שחולקים את אותו שם תחום VTP. מתג יכול להיות בדומיין אחד בלבד.

כברירת מחדל, למתגים אין שם תחום VTP שהוקצה. כאשר הם מקבלים VTP advertisement דרך חיבור Trunk, הם יורשים את שם הדומיין ומספר גרסת ה-VTP שנמצא בהודעה. ניתן להגדיר את השם באופן ידני באמצעות הפקודה vtp name.

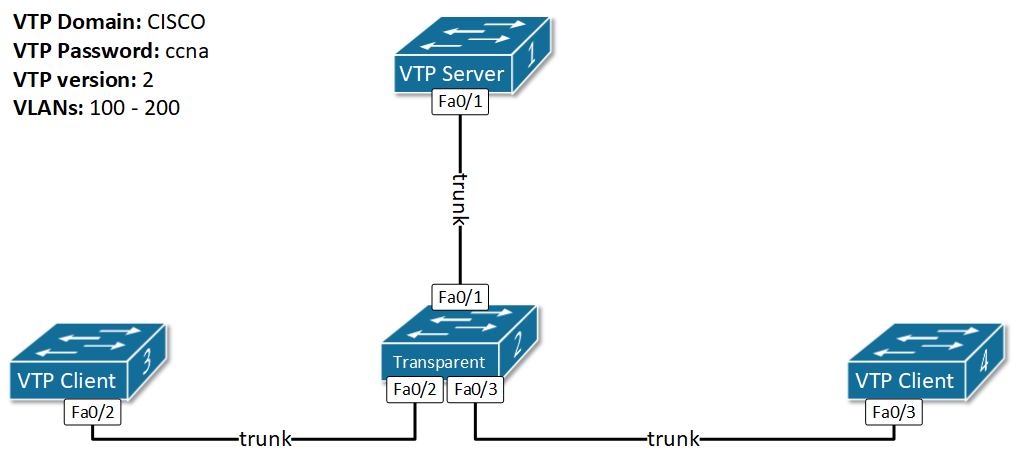
כל השינויים שנעשו בשרת ה-VTP מופצים רק למתגים בתחום ה-VTP. אם יש מתג שמוגדר עם שם תחום VTP אחר, הוא לא יקבל את הפרסומות ולא יעדכן את מסד הנתונים של ה-VLAN שלו.

## VTP Modes

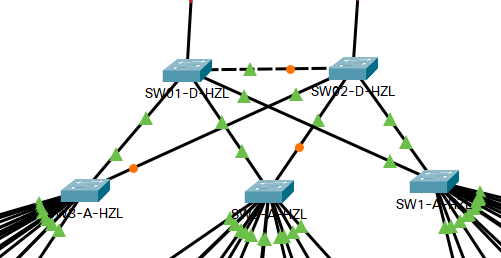
**VTP Server -** שרת VTP הוא מצב ברירת המחדל במתגי סיסקו. במצב Server, המתג מפרסם את כל השינויים במסד הנתונים של VLAN לכל שאר המתגים באותו VTP Domain. הודעות broadcast אלו נשלחות דרך קישורי trunk

**VTP Client -** לקוחות VTP משדרים ומקבלים עדכוני VTP אך אינם יכולים ליצור או למחוק רשתות VLAN. כל השינויים ב-VLAN נעשים על המתג במצב שרת.

**VTP Transparent -** מתגים במצב VTP Transparent משדרים ומקבלים עדכוני VTP אך אינם מעדכנים את מסד הנתונים של ה-VLAN שלהם. הם אינם משתתפים כלל ב-VTP ורק מעבירים הודעות VTP.



יש להגדיר חיבורי TRUNK בין כל המתגים שמשתמשים בVTP לפני הגדרת הVTP.



הגדרת VTP במתג SW01-D-HZL בתור השרת:

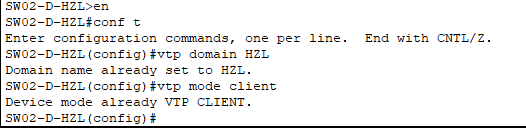
תחילה ניכנס למצב הקונפיגורציה. נגדיר למתג שיעבוד במצב שרת, ולאחר מכן נגדיר לו שם דומיין.

Text

Description automatically generated

הגדרת VTP במתג SW02-D-HZL בתור לקוח:

תחילה ניכנס למצב הקונפיגורציה. נגדיר למתג שיעבוד במצב לקוח, ולאחר מכן נגדיר לו שם דומיין.



פקודת show vtp status בתור שרת:

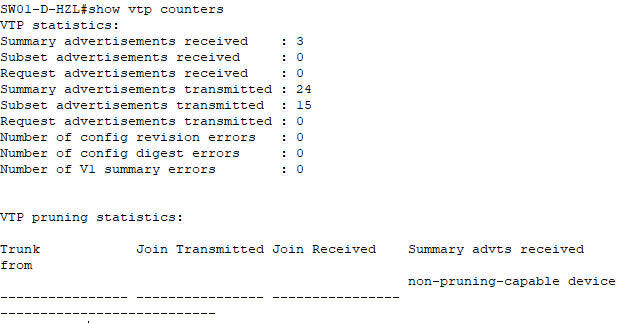
בפקודה זו ניתן למצוא פרטים כללים על הVTP כמו הגרסה שלו, הConfiguration Revision, באיזה מצב המתג עובד, באיזה דומיין הוא נמצא

Text

Description automatically generated

פקודת show counters:

בפקודה זו אנו מקבלים נתונים סטטיסטים על המידע שעובר בפרוטוקול VTP.



# VLAN’s

רשת LAN וירטואלית (VLAN) היא רשת לוגית שמקבצת יחד תת-קבוצה של התקנים החולקים רשת LAN פיזית, ומבודדת את התעבורה עבור כל קבוצה.

LAN היא קבוצה של מחשבים או התקנים אחרים באותו מקום - למשל, באותו בניין או קמפוס - שחולקים את אותה רשת פיזית. LAN משויך בדרך כלל לתחום שידור בשכבה 2, שהוא קבוצת התקני הרשת שחבילת שידור Ethernet יכולה להגיע אליה.

מחשבים ברשת ה-LAN מתחברים לאותו מתג רשת, ישירות או דרך נקודות גישה אלחוטיות (APs) המחוברות לאותו מתג. מחשבים יכולים גם להתחבר לאחד מתוך קבוצה של מתגים המחוברים זה לזה דרך חיבור trunk.

VLAN, כמו ה-LAN שהוא יושב עליו, פועל בשכבה 2 של הרשת, ברמת ה-Ethernet. רשתות VLAN מחלקות רשת מיתוג יחידה לקבוצה של רשתות וירטואליות מכוסות על גבי, שיכולות לעמוד בדרישות תפקודיות ואבטחה שונות. חלוקה זו מונעת את הצורך להחזיק במספר רשתות פיזיות שונות עבור מקרי שימוש שונים ובכך מאפשרת לחברה לחסוך לא מעט כסף על ציוד רשת.

מהנדסי רשת משתמשים ב-VLAN מסיבות מרובות, כולל הבאות:

לשיפור הביצועים

להדק את האבטחה

כדי להקל על הניהול

## כיצד פועלים רשתות VLAN

VLAN מזוהה במתגי רשת על ידי ID VLAN. לכל יציאה במתג ניתן להקצות מזהה VLAN אחד או יותר והוא יעבור ל-VLAN ברירת מחדל אם לא יוקצה עוד אחד. כל VLAN מספק גישה לקישור נתונים לכל hosts המחוברים ליציאות מתג המוגדרות עם מזהה ה-VLAN שלו.

מזהה VLAN מתורגם לתג VLAN, שדה של 12 סיביות בנתוני הכותרת של כל מסגרת Ethernet שנשלחת לאותו VLAN. מכיוון שתג הוא באורך 12 סיביות, ניתן להגדיר עד 4,096 רשתות VLAN לכל תחום מיתוג.

כאשר מתקבלת frame Ethernet מhost ​​מחובר, אין לה תג VLAN. המתג מוסיף את תג VLAN.

הוא מעביר קדימה frames מתויגות לעבר כתובת mac של היעד, ומעביר רק ליציאות שאיתן משויך ה-VLAN. תעבורת broadcast, unicast ו-multicast לא ידועה מועברת לכל היציאות ב-VLAN. קישורי trunk בין מתגים יודעים אילו רשתות VLAN נמצאות על המתגים, מקבלים ומעבירים לאורך כל התעבורה עבור כל VLAN שנמצא בשימוש משני צידי הtrunk.

# הגדרת vlan’s

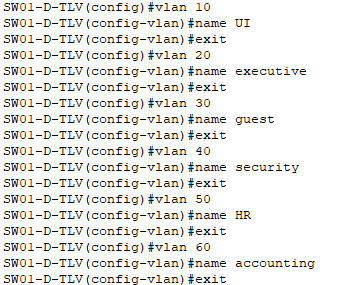
על מנת להגדיר vlan נכתוב תחילה vlan ואז המספר שלו. לאחר הפקודה הזו אנו נכנסים למצב קונפיגורציה של הVLAN ובו נגדיר תשם שלו על ידי הפקודה name.

הגדרת VLAN במתג SW01-D-HZL:

Text, table

Description automatically generated

הגדרת VLAN במתג SW01-D-TLV (תקף לכל המתגים ברשת TLV):



הגדרת VLAN במתג SW01-D-HFA (תקף לכל המתגים ברשת HFA):

Text

Description automatically generated

פקודת show vlan brief בסניף הראשון:

הפלט של הפקודה show vlan brief מציג מידע על רשתות ה-VLAN המוגדרות במתג של Cisco. הפלט כולל את מזהה ה-VLAN, השם, הסטטוס והיציאות שהוקצו לכל VLAN. הפלט יכול לעזור בפתרון בעיות VLAN או לאמת תצורות VLAN.

Table

Description automatically generated

פקודת show vlan בסניף הראשון:

הפלט של הפקודה show vlan מורכב ממספר שדות, כגון:

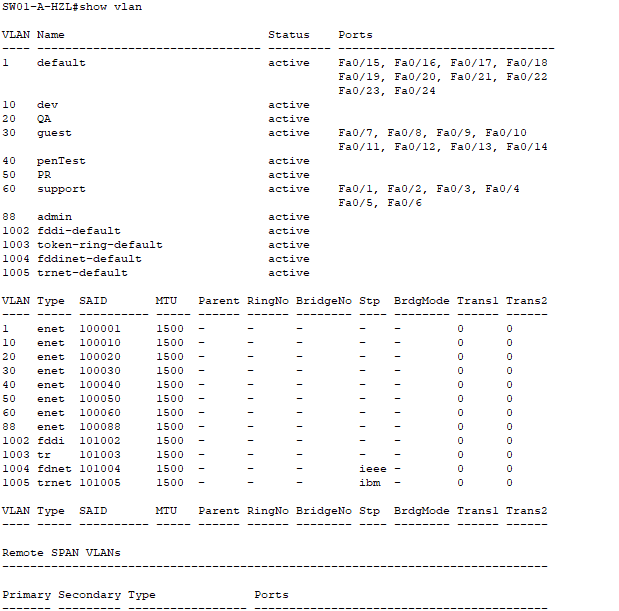
- מזהה VLAN: זהו מזהה מספרי עבור ה-VLAN, הנע בין 1 ל-4094. מזהי VLAN מסוימים שמורים למטרות מיוחדות, כגון VLAN 1 (ברירת המחדל של VLAN), VLAN 1002-1005 (ברירת המחדל של FDDI ו-Token Ring VLANs ) ו-VLAN 4095 (החור השחור VLAN).

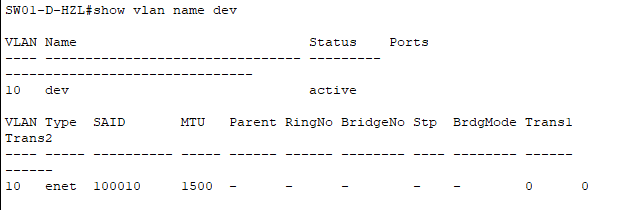
- שם: זהו שם תיאורי ל-VLAN, שאורכו יכול להיות עד 32 תווים. ניתן לשנות את השם עם הפקודה vlan name במצב תצורה גלובלית.

- סטטוס: זה מציין אם ה-VLAN פעיל או מושעה. VLAN פעיל יכול להעביר תעבורה, בעוד VLAN מושעה לא יכול. ניתן לשנות את המצב עם הפקודה state במצב תצורת vlan.

- יציאות: זה מפרט את יציאות המתג המוקצות ל-VLAN. ניתן להקצות יציאה ל-VLAN עם הפקודה switchport access vlan במצב תצורת ממשק. ניתן להגדיר יציאה גם כיציאת טראנק, שיכולה לשאת תעבורה ממספר VLANs עם פקודת trunk mode switchport.

- סוג: זה מציין את סוג ה-VLAN, שיכול להיות Ethernet, FDDI או Token Ring. הסוג קובע את האנקפסולציה ופורמט המסגרת בשימוש ה-VLAN. ניתן לשנות את הסוג עם פקודת המדיה במצב תצורת vlan.



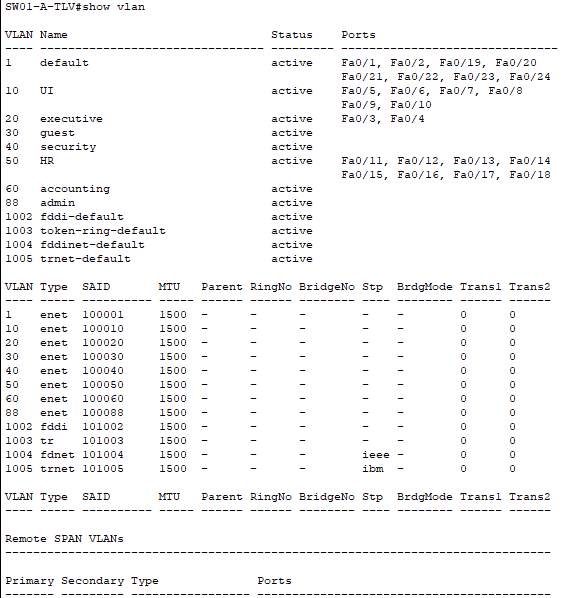


פקודת show vlan brief בסניף השני:

Table

Description automatically generated with low confidence

פקודת show vlan בסניף השני:

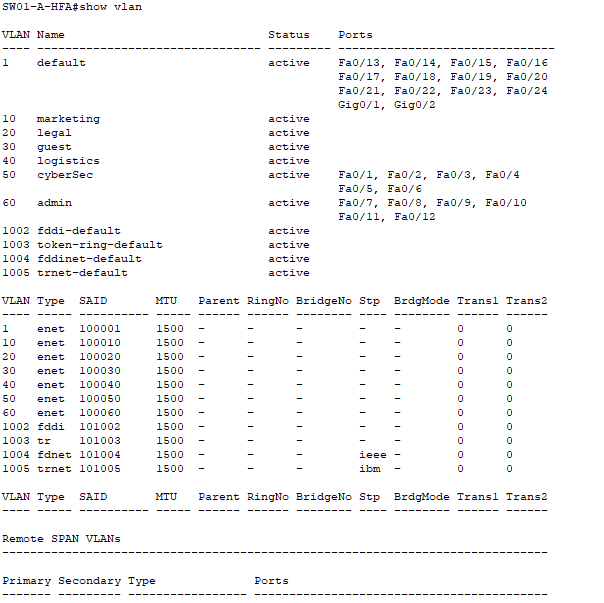


פקודת show vlan brief בסניף השלישי:

Table

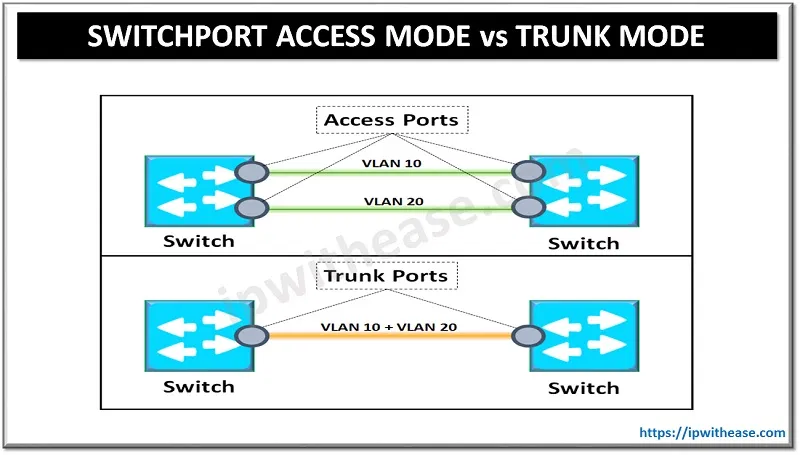
Description automatically generated with medium confidence

פקודת show vlan בסניף השלישי:



# Trunk

Trunk הוא הגדרה של ממשק שדרכו ניתן להעביר יותר מvlan אחד. בחיבור הזה משתמשים כמעט בכל רשת מקומית בין מתגים או מתג לנתב. על מנת להגדיר ממשק כtrunk יש להיכנס תחילה להגדרות הממשק דרך הפקודה interface ואז לכתוב switchport mode trunk.



הגדרת ממשק כ trunk במתג שכבה 2 בסניף הראשון:

נכנסים למצב הגדרת ממשק

מגדירים את הswitchport לעבוד כtrunk

Text, letter

Description automatically generated

הגדרת ממשק כ trunk במתג שכבה 3 בסניף השני:

במתגי שכבה 3 יש להוסיף את הפקודהswitchport trunk encapsulation dot1q על מנת שהנתב יוכל לעבוד בtrunk.



כדי לבדוק האם הגדרנו את הממשק כtrunk, נשתמש בפקודה show interfaces trunk:

הפלט של פקודת trunk show interfaces מורכבת ממספר חלקים. החלק הראשון מציג את היציאה, סוג האנקפסולציה, הסטטוס וה-VLAN המקורי של כל יציאת trunk. היציאה היא שם הממשק, כגון FastEthernet0/1 או GigabitEthernet1/0/1. סוג האנקפסולציה הוא פרוטוקול התיוג המשמש את יציאת הtrunk, 802.1Q או ISL. המצב מציין אם יציאת הtrunk פעילה או לא. ה-VLAN המקורי הוא ה-VLAN שאינו מתויג ביציאת הtrunk, כלומר שלמסגרות השייכות ל-VLAN זה אין מידע VLAN נוסף.

הסעיף השני מציג את רשתות ה-VLAN המותרות בכל יציאת טראנק. זוהי רשימה של מספרי VLAN המורשים להעביר תעבורה דרך יציאת הtrunk. כברירת מחדל, כל רשתות ה-VLAN מותרות ביציאת trunk, אלא אם כן הם נדחים במפורש באמצעות פקודת switchport trunk allowed vlan. הרשימה יכולה להיות טווח של מספרי VLAN, כגון 1-4094, או רשימה מופרדת בפסיקים של מספרי VLAN בודדים, כגון 10,20,30.

הסעיף השלישי מציג את ה-VLAN הפעילים בכל יציאת טראנק. זוהי תת-קבוצה של רשתות ה-VLAN המותרות ביציאת הטראנק שנמצאות בפועל בשימוש על ידי מכשירים משני קצות הקישור. VLAN נחשב פעיל אם יש לו לפחות ממשק אחד במצב למעלה משני צדי קישור הטראנק.

Table

Description automatically generated

# HSRP

רשת מודרנית דורשת זמינות תמידית בכל רגע נתון גם אם ישנה תקלה באחד ממכשירי הרשת עם הבנה זו, פרוטוקולי יתירות First Hop פותחו והופעלו ברוב הרשתות כדי לספק גמישות, זמינות ויתירות. מנקודת המבט של הלקוח אם השער בריירת מחדל יירד, הגישה לרשת שלמה תרד. פרוטוקולי First Hop Redundancy protocol )FHRP) יאפשרו יתירות שער ברירת מחדל, דרך יותר מנתב אחד.

במקרה של תקלה בנתב, יש מכשיר גיבוי שיכנס וימשיך להעביר תעבורה לרשתות מרוחקות ובכך ימנע מצב של ניתוק מרשתות אחרות. להלן 3 סוגי טכנולוגיית FHRP:

פרוטוקול נתב המתנה חם (HSRP)

פרוטוקול יתירות נתב וירטואלי (VRRP)

פרוטוקול איזון עומסים של שער (GLBP)

## מהו HSRP

Hot Standby Router Protocol (HSRP) הוא פרוטוקול בבעלות של CISCO, המספק מנגנון שנועד לתמוך בכשל של תעבורת רשת בנסיבות מסוימות. במקרה זה, שני נתבים או יותר נותנים אשליה של נתב וירטואלי. HSRP מאפשר לך להגדיר נתבים עם כתובת IP משותפת שמשמשת כ default gateway ורק נתב בודד כפעיל בכל פעם. כל הנתבים בקבוצת HSRP חולקים כתובת MAC וכתובת IP אחת, המשמשת כשער ברירת מחדל לרשת המקומית. הנתב הפעיל מעביר את התנועה. אם הנתב הפעיל נכשל, נתב הגיבוי לוקח על עצמו את כל האחריות של הנתב הפעיל ומעביר את התעבורה.

## כיצד מורכבת פקטת HSRP

Opcode הוא 8 סיביות.

0 Opcode - ה-HSRP פועל ומסוגל להפוך לנתב הפעיל או המתנה.

Opcode 1 - הפיכה. הנתב הופך לנתב הפעיל.

Opcode 2 - התפטר. הנתב אינו עוד הנתב הפעיל.

HSRP States הוא 8 סיביות.

1. פעיל - זהו המצב של המכשיר שמעביר תנועה באופן פעיל.

2. Init או Disabled - זהו המצב של מכשיר שעדיין לא מוכן או מסוגל להשתתף ב-HSRP.

3. למד - זהו המצב של מכשיר שעדיין לא קבע את כתובת ה-IP הוירטואלית ועדיין לא ראה הודעת hello ממכשיר פעיל.

4. הקשב - זהו המצב של מכשיר שמקבל הודעות hello.

5. דיבור - זהו המצב של מכשיר ששולח ומקבל הודעות hello.

6. המתנה – זהו מצבו של מכשיר שמוכן לקחת על עצמו את חובות העברת התנועה מהמכשיר הפעיל.

hello time הוא 8 ביטים. המרווח בין הודעות HSRP helloעוקבות מנתב נתון הוא 3 שניות.

החזק זמן את המרווח בין קבלת הודעת hello לבין ההנחה שהנתב השולח כשל לאחר 10 שניות.

העדיפות היא 8 ביטים.

עדיפות ברירת המחדל היא 100. נתב עם עדיפות גבוהה יותר זוכה. שדה עדיפות משמש בתהליך הבחירות הנתבים הפעילים וההמתנה. במצב של שבירת שוויון, כתובת ה-IP הגבוהה ביותר מנצחת.

הקבוצה היא 8 ביט.

שדה זה מזהה את קבוצת ההמתנה בין 0 ל-255.

השמור הוא 8 ביט.

נתוני אימות הם 64 סיביות.

שדה זה מכיל טקסט ברור של 8 תווים בסיסמה בשימוש חוזר. אם לא מוגדרים נתוני אימות, ערך ברירת המחדל המומלץ הוא 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.

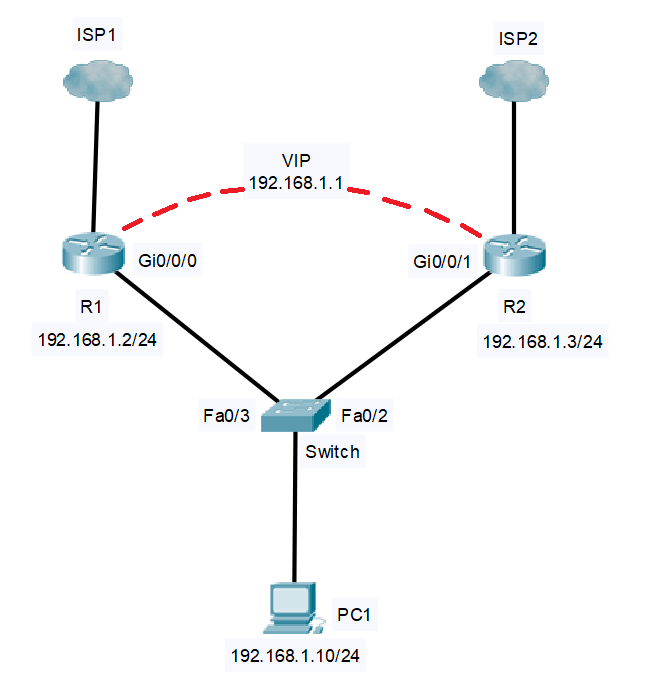
כתובת IP וירטואלית היא 32 סיביות.

כתובת ה-IP הוירטואלית שבה משתמשת קבוצה זו. אם כתובת ה-IP הוירטואלית אינה מוגדרת בנתב, ייתכן שהיא נלמדת מהודעת hello מהנתב הפעיל. יש ללמוד כתובת רק אם לא הוגדרה כתובת והודעת Hello מאומתת.

הראוטר שהוא Active עונה לבקשות ARP של Router על ידי ה Virtual Mac Adress, והוא יודע את כתובת ה IP הוירטואלית שלו.

הראוטר שבמצב Active שולח הודעת Hello לראוטר במצב Passive כל 3 שניות. במידה והראוטר Passive לא קיבל את ההודעה הוא יהפוך את עצמו לActive, וזאת כי הוא הניח שהרשת נפלה.

כאשר הראוטר הקודם שהיה Active חוזר לרשת הוא עובר לעבוד במצב Passive. במידה ואנחנו מעדיפים שהוא יעבוד כActive בכל רגע שהוא פועל, נשתמש בפקודה preempt שתדרוש מראוטרים אחרים לתת לו להיות Active במקומם.



# הגדרת HSRP

הגדרת HSRP בנתב הראשי בסניף הראשון על VLAN 10:

תחילה אנו נכנסים לתת ממשק ומגדירים שיעבוד בvlan 10

לאחר מכן נגדיר כתובת IP לממשק (חשוב שהכתובת תהיה ייחודית לממשק הזה ברשת!).

בפקודה הבאה אנו מגדירים את כתובת הIP הוירטואלית שלו(הכתובת ברירת מחדל).

נגדיר את הפקודה preempt כך שהתעבורה תעבור תמיד דרך הנתב הראשי כל עוד הוא עובד.

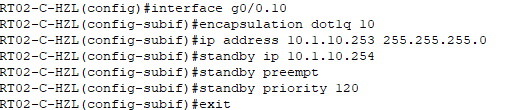
ניתן לנתבpriority הכי גבוה כך שהוא יהיה הנתב הראשי

Text, letter

Description automatically generated

הגדרת HSRP בנתב המשני בסניף הראשון על VLAN 10:

בנתב המשני חוזרים על אותם הפעולות רק מגדירים priority נמוך יותר כך שיחשב למשני.



הגדרת HSRP במתג שכבה 3 בסניף השני:

במתג שכבה 3 חוזרים על אותם פעולות כמו בנתב רק שמגדירים HSRP על ממשק VLAN ולא תת ממשק.

Text

Description automatically generated

הפקודה show standby מציגה את המידע הבא:

- כתובת ה-IP הווירטואלית וכתובת ה-MAC של קבוצת HSRP

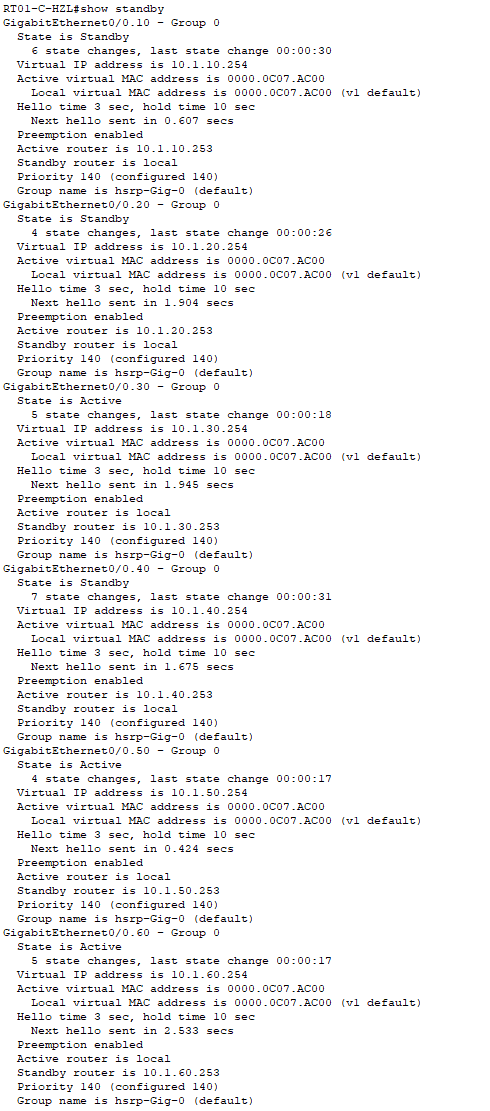
- העדיפות והמצב של הנתב המקומי ונתב העמיתים

- הטיימרים hello ו hold, הקובעים באיזו תדירות נתבי HSRP שולחים הודעות זה לזה וכמה זמן הם מחכים לתשובה לפני שהם מכריזים על כישלון

- שיטת האימות והמחרוזת, אם בכלל, המשמשות לאבטחת הודעות HSRP

- דגל הקדם, המציין אם הנתב המקומי יכול להשתלט על התפקיד הפעיל אם יש לו עדיפות גבוהה יותר מהנתב הפעיל הנוכחי

- ממשק המסלול וערך ההפחתה, אם בכלל, משמשים כדי להתאים את העדיפות של הנתב המקומי בהתבסס על המצב של ממשק אחר



# STP

stp או spanning tree protocol הוא פרוטוקול בשכבה 2 במודל הOSI האחראי על מניעת לולאות בתוך רשת מחשבים.

STP נוצר כדי למנוע את הבעיות המתעוררות כאשר מחשבים מחליפים נתונים ברשת מקומית (LAN) המכילה נתיבי גיבוי. אם זרימת התעבורה אינה מפוקחת ונשלטת בקפידה, הנתונים יכולים להיתפס בלולאה שמסתובבת סביב מקטעי רשת, משפיעה על הביצועים ועלולה אף לגרום לעצירה כמעט מוחלטת של התעבורה.

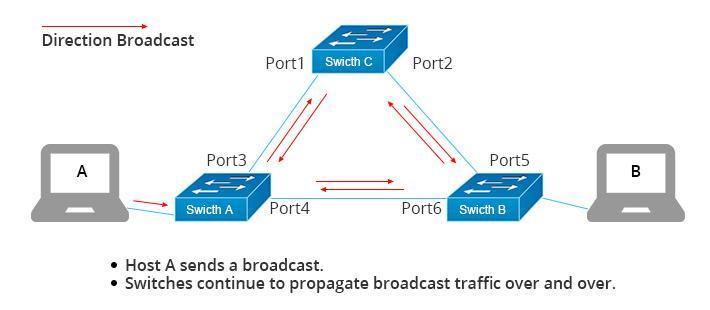
ברשתות תקשורת של ארגונים רבים ניתן למצוא יתירות בכבלים ורכיבי רשת אשר מאפשרים גלישה גם במידה ואחד הרכיבים לא פועל כמו שצריך. יתירות זו יוצרת מספר נתיבים דרכם המידע יכול לעבור מה שעלול ליצור מצב של לולאה.

STP יכול לסייע במניעת לולאת ברשתות LAN הכוללות חיבורים מיותרים. ללא STP, יהיה קשה ליישם את היתירות הזו ועדיין להימנע מלולאת רשת. STP מנטר את כל חיבורי הרשת, מזהה חיבורים מיותרים ומשבית את היציאות שעלולות להוביל ללולאה.

## בעיות שהSTP פותר

### Broadcast storm

הבעיה הראשונה והגדולה מכולם נקראת broadcast storm והיא למעשה נגרמת כאשר יש הודעת broadcast שנשלחת לרשת. מכיוון שמדובר בהודעת broadcast המתגים מעבירים אותה לכל הממשקים שיש לה הנמצאים באותו vlan או במצב trunk , וזה גורם לבעיה מכיוון שכל מתג יעביר את ההודעה למתג הבא ואם הם מחוברים במעגל זה יצור לולאה אינסופית אשר בקלות יכולה לתקוע את הרשת.



**unstable mac table**

הבעיה השניה נקראת unstable mac table והיא נגרמת מזה שהמתג לומד על הmac באמצעות הפריימים שעוברים דרכה, וכאשר נוצרת לולאה הפריימים מבלבלים את המתג.

Diagram

Description automatically generated

**Duplicate Frame**

הבעיה השלישית והאחרונה היא duplicate frame והיא נוצרת כאשר אותו פריים עובר דרך כמה נתיבים בו זמנית מה שהופך את העברת המידע ללא יעילה.

## STP port states

כאשר STP מופעל על מתג ברשת, כל יציאה מוגדרת לאחד מחמישה מצבים כדי לשלוט בהעברת frames:

1. Disabled – הממשק אינו משתתף בהעברת frames.
2. Blocking - הממשק אינו משתתף בהעברת frames ומבטל frames שהתקבלו מקטע הרשת המצורף. עם זאת, הממשק ממשיך להאזין ולעבד BPDUs.
3. Listening - ממצב החסימה, הממשק עובר למצב האזנה. הממשק משליך frames. עם זאת, הוא מקבל BPDUs ומעבד אותם.
4. Learning - הממשק עובר ממצב האזנה למצב הלמידה. הוא מאזין ומעבד BPDUs אך משליך frames. הוא גם מתחיל לעדכן את טבלת הכתובות עם המידע שנלמד. בנוסף, הוא מעבד frames אך אינו מעביר את אותם.
5. Forwarding - הממשק עובר ממצב הלמידה למצב ההעברה ומתחיל להעביר פריימים על פני מקטעי הרשת. זה כולל frames מקטע הרשת המצורפת ואלו שהועברו מיציאה אחרת. היציאה גם ממשיכה לקבל ולעבד BPDUs, וטבלת הכתובות ממשיכה להתעדכן.

### Root Bridge

זה המתג דרכו חייבת לעבור כל התעבורה. לכל הגשרים ברשת LAN יש נתיב לroot bridgh. STP מאפשר לך לבחור את גשר השורש באופן אוטומטי. עם זאת, אם מנהל רשת STP רוצה, הוא או היא יכולים לשנות את ה-RB בהתאם לרשת.

כיצד נבחר הroot bridge ברשת?

כל המתגים ברשת מכריזים על עצמם כroot bridge ומתחילים להחליף BPDUs משלהם. ה-BPDU עם הpriority הנמוך ביותר ייחשב כעליון. כעת המתג המקבל את ה-BPDU העליון מבצע שינויים ב-BPDU שלו ומעביר הלאה למתגים השכנים שלו. הוא משנה את הערך של root Bridge I'd עם הroot ID של ה-BPDU העליון שלו. תהליך זה נמשך עד שכל המתגים יודעים למי יש את הpriority הנמוך ביותר והמתג הזה יוכרז כroot bridge .

### Root Port

ממשק הroot הוא ממשק המוביל לroot bridgh.

## Designated Port

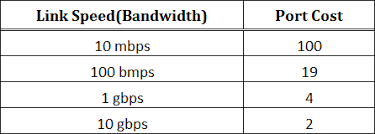
ממשק זה מקבל את המידע ומעביר אותו לroot port

### Alternative Port

ממשק זה משמש כממשק חלופי לממשק root והוא נמצא במצב חסימה.

### Path Cost

עוזר להחליט על הטופולוגיה הטובה ביותר ביחס למהירות ההעברה. ככל שמהירות ההעברה של החיבור גדולה יותר כך הcost שלה נמוך יותר. הרשת תמיד תעדיף את הנתיב שסכום הcosts שלו הוא הנמוך ביותר.



## Bridge Protocol Data Units (BPDU)

פרוטוקול Spanning Tree דורש התקן רשת STP להחליף הודעות כדי לעזור מטופולוגיה לוגית נטולת לולאות. הודעות אלו נקראות BPDUS (Bridge Protocol Data Units). כל התקן רשת שולח BPDUs, שעוזר להחליף מידע טופולוגי.

BPDUS עוזר למתגים לבצע את הפעולות הבאות:

* לבחור מתג בודד שיפעל כroot
* BPDU גם עוזר לחשב את הנתיב הקצר ביותר מעצמו למתג הroot.
* לחסום alternative ports

## סוגים נוספים של STP

### RSTP

Stp אשר עולה מהר יותר אך גם צורך יותר משאבים.

### PVST

Stp אשר פועל על כמה vlans במקביל.

### Rapid-PVST

Rapid-pvst הוא pvst אשר עולה מהר יותר אך גם צורך יותר משאבים.

## הגדרות בסיסיות ואבטחתיות של STP

### Portfast

Switchport המחובר למכשיר קצה מאפשר לאותו מכשיר להתחבר לרשת באופן מידי, במקום לחכות שהממשק יעבור ממצבי האזנה ולמידה למצב העברה. לא רצוי להגדיר portfast לחיבור אשר לא מתחבר למכשיר קצה כיוון שהוא מדלג על שלבים חשובים אשר עוזרים למנוע לולאות.

### BPDU Guard

BPDU Guard היא תכונה המגנה על הטופולוגיה של Layer 2 Spanning Tree Protocol (STP) מפני איומים הקשורים ל-BPDU ונועדה להגן על רשת המיתוג. יש להפעיל את תכונת ה-BPDU guard ביציאות שלא אמורות לקבל BPDUs מהתקנים מחוברים.

### Root Guard

Root guard הוא תכונת STP המופעלת על הroot bridgh אשר מתעלמת מפאקטות BPDU עליונות. זה מונע מממשק מוגדר להפוך לroot port. Root guard מונע ממתג במורד הזרם (לעתים קרובות מוגדר שגוי או זדוני) להפוך לroot bridgh בטופולוגיה

הגדרת STP במתג שכבה 2 בשכבת ה Distribution בסניף הראשון SW01-D-HZL מוגדר כRoot bridgh:

Text, letter

Description automatically generated

הגדרת STP במתג שכבה 2 בשכבת ה Distribution בסניף הראשון SW02-D-HZL מוגדר כBackup:

Text

Description automatically generated

הגדרת STP במתג שכבה 2 בשכבת ה Access בסניף הראשון SW01-A-HZL:

A screenshot of a computer

Description automatically generated with medium confidence



פקודות show:

הפלט של הפקודה show span-tree מורכבת ממספר קטעים. הסעיף הראשון מציג את מזהה ה-Root Bridge, שהוא שילוב של ערך עדיפות וכתובת MAC, ואת ה-Root Port, שהיא היציאה הקרובה ביותר ל Root Bridge מבחינת עלות הנתיב. עלות הנתיב היא מדד המשקף את רוחב הפס של קישור. ככל שעלות המסלול נמוכה יותר, כך הקישור מועדף יותר. מזהה Root Bridge ויציאת השורש מציינים באיזה מתג ויציאה משתמשים כדי להגיע ל Root Bridge מהמתג הנוכחי.

הסעיף השני מציג מידע על כל VLAN (Virtual Local Area Network) המוגדר על המתג. VLAN הוא קיבוץ לוגי של מכשירים החולקים את אותו תחום שידור. עבור כל VLAN, הפלט מציג את מזהה הגשר של המתג הנוכחי, עדיפות הגשר, זמן הזדקנות הכתובות, זמן שלום, הגיל המרבי וההשהיה קדימה. אלו פרמטרים שמשפיעים על אופן פעולת STP ועל התדירות שבה הוא מעדכן את המידע שלו. הפלט מציג גם את מספר השינויים בטופולוגיה שזוהו ב-VLAN ואת הזמן מאז השינוי האחרון.

החלק השלישי מציג מידע על כל יציאה במתג המשתתף ב-STP. עבור כל יציאה, הפלט מציג את מספר היציאה, התפקיד, המצב, העלות, העדיפות, הסוג והגשר והיציאה המיועדים. התפקיד מציין איזו פונקציה הפורט מבצע ב-STP. ישנם חמישה תפקידים אפשריים:

- שורש: היציאה שהכי קרוב לגשר השורש מבחינת עלות השביל.

- ייעודי: היציאה שאחראי על העברת תעבורה לקטע וממנו.

- חלופי: היציאה המספקת נתיב חלופי לגשר השורש במקרה של תקלה.

- גיבוי: היציאה המספקת נתיב גיבוי לקטע במקרה של תקלה.

- מושבת: היציאה שנכבה באופן ידני או אוטומטי.

המצב מציין באיזה מצב תפעולי היציאה נמצאת. ישנם חמישה מצבים אפשריים:

- חסימה: היציאה אינה מעבירה או מקבלת תעבורה כלשהי, אך היא מאזינה להודעות STP.

- האזנה: הפורט אינו מעביר או מקבל תעבורה כלשהי, אך הוא מאזין להודעות STP ומתכונן למעבר למצב אחר.

- למידה: הפורט לא מעביר שום תעבורה, אבל הוא לומד כתובות MAC מפריימים נכנסים ומתכונן למעבר למצב אחר.

- העברה: הפורט מעביר ומקבל תעבורה כרגיל.

- מושבת: הפורט מושבת ואינו משתתף ב-STP.

Table

Description automatically generated

Text, letter

Description automatically generatedA picture containing text

Description automatically generatedTable

Description automatically generated

# Router On a Stick (Dot1Q)

נתב על מקל הוא אחת הדרכים לאפשר ניתוב בין רשתות VLAN. סוג זה של התקנה מורכב מנתב ומתג המחוברים דרך חיבור אחד המוגדר כחיבור trunk 802.1q. תצורה כזו אופיינית ברשתות שבהן לא קיים מתג שכבה-3.

בעת קביעת תצורה של רשתות VLAN חדשות ביציאות מתג, חילקנו את תחום השידור שבו הוא הוצב לחלקים קטנים יותר מוגבלים ל-VLAN. המתג הבסיסי אינו יכול לנתב מידע בין תחומי שידור. ידוע שהנתב הוא מכשיר שמנתב פאקטות ומפריד בין תחומי שידור.

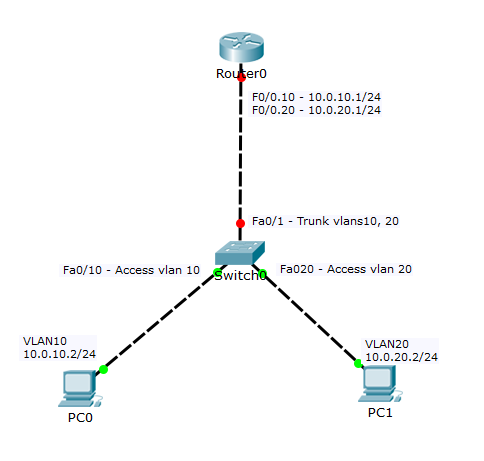
ניתן להשתמש ב שכבה 3 כדי לאפשר תקשורת בין התקנים מ-VLAN שונים. ראוטר על מקל היא דרך אחת בה נוכל ליישם זאת.

## Sub-interfaces

Sub interface הוא תכונה מרכזית של הנתב על מקל. הוא מוגדר עבור כל רשת בנתב.

ממשקי משנה הם המרכיבים הלוגיים של ממשק פיזי. הודות לגישה זו אין צורך להשתמש ב-X ממשקים פיזיים של הנתב ב-Y VLANs. במקום זאת, קיים קישור trunk בין מתג לנתב, כך שמנות מסומנות עוברות לנתב. לאחר מכן, הנתב מסיר את התוויות ומציג תצוגה מקדימה של טבלת הניתוב.

חשוב להגדיר encapsulation 802.1Q על כל תת ממשק ותג VLAN תואם גם כן.



**הגדרת dot1q**

**יש להיכנס לתת ממשק של הממשק המחובר כTRUNK ואז ולהגדיר את פקודת ה encapsulation dot1q ואת מספר מזהה הvlan.**

****

# **DHCP**

DHCP הוא מנגנון הקצאת כתובות IP למארחים קבועים וניידים המחוברים קווית או אלחוטית.

אם פרוטוקול DHCP לא היה קיים, מנהלי רשת יצטרכו לחלק באופן ידני כתובות IP מהמאגר הזמין, דבר שיצרך זמן רב, לא יעיל ונוטה לשגיאות.

כאשר מכשיר רוצה גישה לרשת המשתמשת ב-DHCP, הוא שולח בקשה לכתובת IP שנקלטת על ידי שרת DHCP. השרת מגיב במסירת כתובת IP למכשיר, ואז עוקב אחר השימוש בכתובת ומחזיר אותה לאחר זמן מוגדר או כשהמכשיר נכבה. לאחר מכן, כתובת ה-IP מוחזרת למאגר הכתובות המנוהל על ידי שרת ה-DHCP כדי להיות מוקצה מחדש למכשיר אחר בזמן שהוא מחפש גישה לרשת.

בעוד שהקצבת כתובות IP היא הפונקציה המרכזית של הפרוטוקול, DHCP גם מקצה מגוון פרמטרים קשורים לרשת, כולל כתובת שער ברירת מחדל וכתובת שרת DNS.

## יתרונות הDHCP

DHCP מספק מגוון יתרונות למנהלי רשת:

### תצורת כתובת IP אמינה

לא יכולים להיות שני משתמשים עם אותה כתובת IP מכיוון שזה יוצר התנגשות שבה אחד או שני המכשירים לא יכולים להתחבר לרשת. DHCP מבטל שגיאות אנוש כך שהתנגשות כתובות או שגיאות הקלדה פשוטות ממוזערות.

### ניידות

DHCP מטפל ביעילות בשינויי כתובת IP עבור משתמשים במכשירים ניידים שעוברים למיקומים שונים ברשתות קוויות או אלחוטיות.

### שרת DHCP

זהו מכשיר רשת המריץ את שירות DHCP שמכיל כתובות IP. זה לרוב שרת או נתב אבל יכול להיות כל דבר שמתפקד כhost

### לקוח DHCP

תוכנת נקודת קצה זו מבקשת ומקבלת מידע משרת DHCP. ניתן להתקין זאת על מחשב, מכשיר נייד, IoT או כל דבר אחר שדורש קישוריות לרשת. רובם מוגדרים לקבל מידע DHCP כברירת מחדל.

### מאגר כתובות IP

טווח כתובות ה-IP הזמינות ללקוחות. כתובות בדרך כלל מחולקות ברצף מהנמוך לגבוה ביותר.

### Subnet

ניתן לחלק רשתות IP למקטעים המכונים subnet.

**Lease**

משך הזמן שבו לקוח DHCP מחזיק את פרטי כתובת ה-IP. כאשר חוזה שכירות מסתיים, על הלקוח לחדשו.

בשרתות המאפשרות גישה למכשירים ניידים רצוי לקבוע זמן נמוך על מנת לשחרר את הכתובת ip כמה שיותר מוקדם לאחר שהמכשיר התנתק מהרשת.

**relay DHCP**

נתב או מארח המאזין להודעות לקוח המשודרות ברשת זו ולאחר מכן מעביר אותן לשרת מוגדר המוגדר כ-DHCP. לאחר מכן השרת שולח תגובות בחזרה לrelay שמעביר אותן ללקוח. זה יכול לשמש כדי לרכז שרתי DHCP במקום שיהיה שרת בכל תת רשת.

## תהליך הקצאת כתובות IP

השאלה הקיומית הקשורה ל-DHCP היא כיצד משתמש קצה מתחבר לרשת מלכתחילה מבלי שיש לו כתובת IP?

ראשית, כל מערכות ההפעלה המודרניות של המכשיר כוללות לקוח DHCP, המופעל בדרך כלל כברירת מחדל. על מנת לבקש כתובת IP, מכשיר הלקוח שולח הודעת שידור –DISCOVER. הרשת מפנה את הבקשה לשרת ה-DHCP המתאים.

לאחר מכן השרת קובע את כתובת ה-IP המתאימה ושולח חבילת OFFER ללקוח, אשר מגיב בחבילת REQUEST. בשלב האחרון בתהליך, השרת שולח חבילת ACK המאשרת שהלקוח קיבל כתובת IP.

כל זה נעשה במהירות ובאופן אוטומטי וללא צורך בפעולה כלשהי של משתמש.

**אבטחת DHCP**

עם DHCP, ההקצאה הראשונית של כתובת IP מתוכננת להיות מהירה ויעילה. הפשרה היא שפרוטוקול DHCP אינו דורש אימות.

תוקף עלול להשתלט או לזייף את שרת ה-DHCP ולחלק מידע גרוע למשתמשי קצה לגיטימיים, לשלוח אותם לאתר מזויף. או שהוא יכול לחלק כתובות IP לגיטימיות למשתמשים לא מורשים. זה עלול להוביל להתקפות "man in the middle" ולהתקפות של מניעת שירות.

# **DHCP Snooping**

DHCP Snooping היא טכנולוגיית אבטחה על מתג רשת שכבה 2 שיכולה למנוע משרתי DHCP לא מורשים לגשת לרשת שלך. זוהי הגנה מפני hosts שרוצים להפוך לשרתי DHCP Snooping. DHCP פועל כהגנה מפני התקפות " man in the middle ". DHCP עצמו פועל על שכבה 3 של שכבת OSI בעוד DHCP snooping פועלת על התקני שכבה 2 כדי לסנן את התעבורה שמגיעה מלקוחות DHCP.

במתגים של Cisco, DHCP Snooping מופעלת באופן ידני. יש להגדיר trusted ports באופן ידני ושאר היציאות לא מוגדרות נחשבות ליציאות untrusted. רוב המכשירים המחוברים ל trusted ports הם נתבים, מתגים ושרתים. לקוחות DHCP כמו PC ומחשבים ניידים מחוברים בדרך כלל ליציאה untrusted.

## הגדרת DHCP

הגדרת שרת DHCP בנתב cisco בסניף הראשון RT01-C-HZL:

נכנסים למצב קונפיגורצית הנתב.

משתמשים בפקודת ip dhcp excluded-address לכל הכתובות שאנו לא רוצים שהdhcp יחלק.

נכנסים למצב הגדרת DHCP pool לכל pool בנפרד על ידי הפקודה ip dhcp pool ואז השם שלה.

בתוך למצב הגדרת DHCP pool נגדיר את שם הרשת וה subnet mask שלה.

נגדיר את הdefault gateway של הרשת על מנת לשלוח אותה לרכיבים שידעו אותה.

Text

Description automatically generated

הגדרת שרת DHCP על שרת קצה בPacket tracer בסניף השני:

לאיזה ממשק נגדיר DHCP פועל או כבוי.

כאשר אנו רוצים ליצור pool חדש נמלא את הפרטים הבאים ונלחץ על הכפתור save.

Graphical user interface, application

Description automatically generated

הגדרת מתגי שכבה 3 בשכבת הDistribution כך שיעבירו DHCP לשרת DHCP בשרת אחרת:

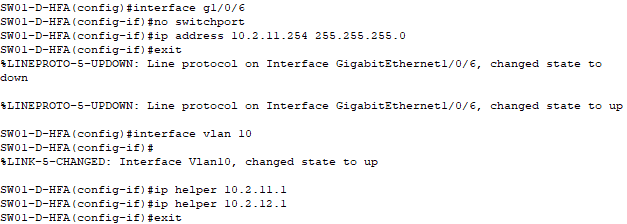
תחילה ניכנס לממשק המחובר לרשת בה נמצא שרת הDHCP.

נגדיר שהממשק יעבוד בשכבה 3 ולא כswitchport.

ניתן לו כתובת IP על מנת שיוכל לתקשר ברשת של הDHCP.

נכנס למצב הגדרת VLAN לכל אחד מהVLANים.

נגדיר את פקודת הip helper אשר יעביר DHCP לכתובת המוגדרת.



פקודות show

פקודת show ip dhcp pool:

מראה פרטים על כל POOL בנפרד.

Diagram

Description automatically generated with medium confidence

פקודת show ip dhcp binding:

פקודה המציגה את כל הקצאות הכתובות IP לכתובות mac, לכמה זמן ,ואיזה סוג.

Table

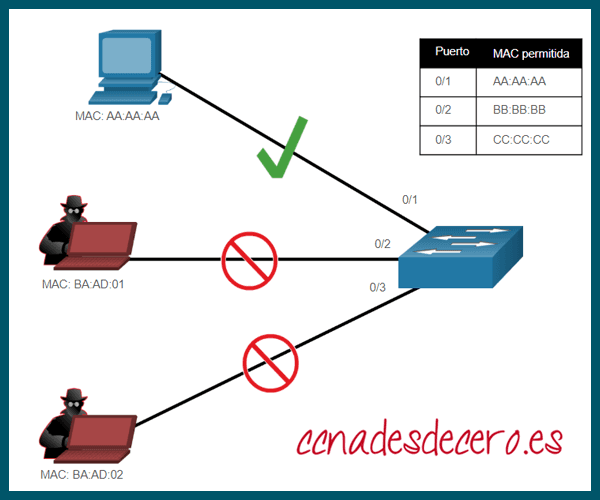
Description automatically generated

# Port-Security

רשתות LAN פגיעות מאוד להתקפה מכיוון שיציאות המתג פתוחות לשימוש כברירת מחדל. התקפות שונות כגון התקפת Dos בשכבה 2, זיוף כתובות יכול להתרחש. על מנת לפתור את הבעיה זו, נוצר מנגנון port security אשר מונע גישה לרשת לרכיבים אשר לא מורשים להיכנס.

## איך זה עובד?

מתגים לומדים כתובות MAC כאשר ה frame מועבר דרך switchport. על ידי שימוש בport security, משתמשים יכולים להגביל את מספר כתובות MAC שניתן ללמוד ליציאה, להגדיר כתובות MAC סטטיות ולהגדיר violation עבור אותה יציאה אם רכיב לא מורשה מנסה להתחבר דרכו . משתמשים יכולים להשתמש בפקודות restrict, shutdown או protect על port security.



* Protect – מצב זה מפיל את החבילות עם כתובות mac מקור לא ידועות עד שתסיר מספיק כתובות mac מאובטחות כדי לרדת מתחת לערך המקסימלי.
* Restrict – מצב זה מבצע את אותה פונקציה כמו הגנה, כלומר מוריד מנות עד שיוסרו מספיק כתובות Mac מאובטחות כדי לרדת מתחת לערך המקסימלי. בנוסף לכך, הוא יפיק log.
* Shutdown – מצב זה מועדף בעיקר בהשוואה למצבים אחרים מכיוון שהוא מכבה את הממשק מיד אם מתבצעת גישה לא מורשית ויפיק log. יציאה זו תישאר במצב כיבוי עד שמנהל המערכת יבצע את הפקודה "ללא כיבוי".
* Sticky – על ידי שימוש בפקודה sticky, המשתמש מספק אבטחת כתובת Mac סטטית מבלי להקליד את כתובת MAC המוחלטת. לדוגמה, אם המשתמש מספק מגבלה מקסימלית של 2 אז 2 כתובות ה-Mac הראשונות שנלמדו ביציאה זו יוצבו בתצורה הפועלת. לאחר כתובת ה-Mac השניה שנלמדה, אם המשתמש השלישי רוצה לגשת, המערכת תיצור violation.

הערה – port security יעבוד על access port בלבד, כלומר כדי לאפשר port security, המשתמש צריך קודם כל להפוך אותה לaccess port.

## הגדרת port security

כאשר אנו רוצים להגדיר port security ניכנס תחילה למצב קונפיגורצית ממשק.

נהפוך את הswitchport לעבוד במצב access.

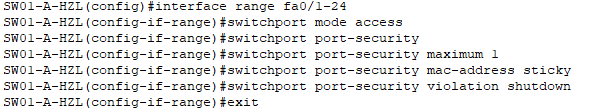
נפעיל את הport security.

נגדיר לו שילמד מקסימום כתובת mac אחת.

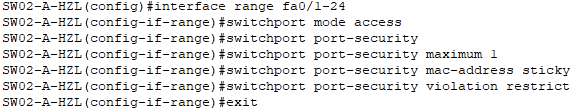
נגדיר שילמד את הכתובת mac בצורה אוטומטית.

נגדיר לו violation mode ל shutdown.

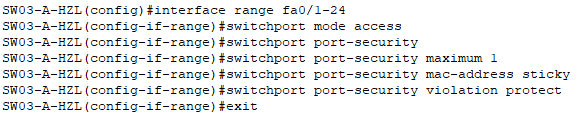
הגדרת port security במתג sw01-A-HZL violation shutdown:



הגדרת port security במתג sw02-A-HZL violation restrict:



הגדרת port security במתג sw03-A-HZL violation protect:



פקודות SHOW

פקודת show port-security:

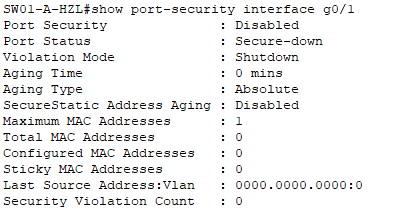
בפקודה זו ניתן לראות טבלה אשר מראה לכל ממשק כמה מקסימום כתובות היא יכולה לשמור, כמה כתובות היא שומרת כרגע, כמה פעמים מכשיר לא מורשה ניסה להתחבר, ובאיזה פעולה יש לנקוט כאשר מכשיר לא מזוהה מתחבר.

Table

Description automatically generated

פקודת show port security interface:

פקודה זו מראה port security על ממשק ספציפי.



# IP Routing

Routing IP הוא תהליך של שליחת packets מhost ברשת אחת לhost ברשת אחרת. תהליך זה נעשה בדרך כלל על ידי נתבים אך גם על ידי מתגים בשכבה 3 במידה ומגדירים את הפקודה ip routing.

# EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) הוא פרוטוקול ניתוב דינמי המשמש למציאת הנתיב הטוב ביותר בין מכשירים העובדים על שכבה 3 במודל הOSI. הפרוטוקול פותח על ידי חברת cisco ובמקור עבד רק על המכשירים שלהם, ובהמשך הוא הפך להיות סטנדרט פתוח . EIGRP עובד על פרוטוקול בשכבת הרשת ומשתמש בפרוטוקול מספר 88. הוא משתמש במדדים כדי לגלות את הנתיב הטוב ביותר בין שני התקני שכבה 3 (נתב או מתגי שכבה 3) הפועלים על EIGRP. EIGRP מגיע ממשפחת פרוטוקולי ניתוב הנקראת Distance vector אך יש המחשיבים אותה כהיברידית מפני שיש לה גם תכונות ממשפחת הLink State.

אלגורידם שהEIGRP משתמש בו נקרא: DUAL

ערך הAD של EIGRP Summarization הוא: 5

ערך הAD של EIGRP Internal הוא: 90

ערך הAD של EIGRP External הוא: 170

היתרונות של EIGRP הם:

* שימוש נמוך מאוד במשאבי רשת במהלך פעולה רגילה; רק הודעות HELLO מועברות ברשת יציבה.
* כאשר מתרחש שינוי בטופולוגיה, רק שינויים בטבלת הניתוב מופצים, לא כל טבלת הניתוב; זה מפחית את העומס שפרוטוקול הניתוב עצמו מטיל על הרשת.
* זמני התכנסות מהירים לשינויים בטופולוגית הרשת (במצבים מסוימים ההתכנסות יכולה להיות כמעט מיידית).

## Distance vector vs Link State

|  | **Distance vector** | **Link state** |
| --- | --- | --- |
| פרוטוקולים | RIP, EIGRP | OSPF |
| אלגורידם | DUAL | Dijsktra |
| Network view | מידע על נתיבים שהשכנים מכירים | מידע מלא על הטופולוגיה |
| בחירת נתיב הכי טוב | Based on the least number of hops | על בסיס cost |
| עדכונים | Full routing table | Link state updates |
| תדירות עדכונים | כל פרק זמן קבוע | כאשר יש שינוי בטופולוגיה |
| משאבים | לוקח מעט משאבים | לוקח הרבה משאבים |
| מורכבות | מורכבות נמוכה | מורכבות גבוהה |
| Convergence time | Moderate | Fast |
| עדכונים באמצעות | broadcast | multicast |
| Hierarchical structure | No | Yes |
| Intermediate Nodes | No | Yes |

## יחסי שכנות

על מנת ליצור יחסי שכנות הנתבים משתמשים בהודעות Hello. הודעות Hello אחראיות על מציאת ווידוי הימצאותם אחרי כל כמה זמן. הנתב שולח כל כמה זמן הודעת Hello לנתבים המחוברים אליו ישירות ובמידה ויש התאמה בכל הקריטריונים הוא אמור לקבל הודעת Hello בחזרה.

* הודעותhello נשלחות בMulticast דרך הכתובת 224.0.0.10

קריטריונים כדי ליצור שכנות EIGRP, יש לדאוג לקריטריונים הבאים:

1. ערכי הK חייבים להיות תואמים.
2. מספר הAS חייב להיות תואם.
3. במידה והגדרנו Authentication, הוא חייב להיות תואם.(ID וpassword זהה)
4. הsubnet mask חייב להיות תואם.

* מספר המזהה של הנתב לא חייב להיות ייחודי ברשת(בניגוד לפרוטוקולים אחרים). אך הוא לא יוכל לקבל עדכונים מרשת חיצונית.

Timers:

Hello timer - המרווח זמן שבו EIGRP שולח הודעת HELLO בממשק. זה 5 שניות כברירת מחדל.

Hold timer - המרווח זמן שבו השכן יוכרז כלא פעיל אם לא יוכל לשלוח את חבילת HELLO. זה 15 שניות כברירת מחדל.

נ.ב: נהוג שזמן ה Dead timerחייב להיות גדול פי 3 מזמן ה Hello timer.

**עדכון טבלאות הניתוב**

* **מתרחש רק כאשר יש שינוי בטופולוגיה.**
* **מחיקת נתיבים אשר עוברים דרך נתב שכן שעבר את זמן ה** Hold timerמבלי לענות.
* כאשר נתיב לרשת מסוימת נקטע ואין נתיב גיבוי, הנתיב יכנס למצב Active. במצב הזה הנתב ישלח חבילת Quary לכל השכנים שלו כדי לשאול האם מישהו מכיר נתיב אחר לרשת שהוא מחפש. השכן יענה באמצעות חבילת Reply ויתן לו מסלול חלופי במידה ויש.
* מידע על ניתוב עובר באמצעות חבילת הUpdate. כאשר הנתב מקבל את חבילת ה הUpdate הוא עונה בחזרה עם חבילת Ack לנתב ממנו קיבל את ה הUpdate.

**כתובות multicast:**

**הכתובת 224.0.0.10 משמשת את EIGRP על מנת לאפשר לנתבי EIGRP לשתף מידע ניתוב עם נתבי EIGRP אחרים בקטע רשת.**

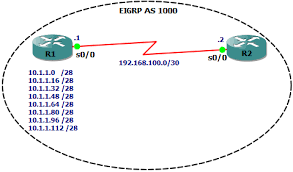
**EIGRP Summarization**

**סכימת רשתות הוא תהליך דרכו ניתן להכליל מספר רשתות תקשורת בטבלת הניתוב לרשת תקשורת אחת גדולה יותר.**

**היתרון של סכימת רשתות הוא צמצום טבלאות ניתוב אשר מקלות על משאבי רשת ותיעדוף מסלול על ידי הAD הנמוך יותר שיש לו.**

**החיסרון בסכימה הוא במידה ויש רשת שלא נמצאת בתוך הסכימה הנתב עלול לפספס אותה.**

**ניתן להגדיר סכימה בצורה ידנית או אוטומתית על נתבי cisco.**

****

## Feasible Distance vs Advertised Distance

Advertised Distance (AD) – הmetric של הנתיב כפי שהנתב השכן פרסם אותו.

Feasible Distance (FD) – הmetric של הנתיב הכולל גם את הmetric של הנתב הנוכחי מהשכן דרכו הנתיב עובר.

**Successor vs Feasible Successor**

* Successor – הנתיב עם הmetric הטוב ביותר ליעד. הנתיב הטוב ביותר הוא הנתיב שהFD שלו הוא הכי קטן.בברירת מחדל יש מקסימום 4 נתיבי successor. ניתן לפתוח עד 32 נתיבי successors.
* Feasible Successor – נתיב גיבוי אם ה Successorנופל. ל Feasible Successor חייב להיות AD קטן יותר מהFD של ה Successor. אין הגבלה לכמות נתיבי הfeasible successor .

במידה ולא נמצא נתיב גיבוי המערכת תיכנס למצב של לולאה.

## Variance command

* פקודה היוצרת load balancing.
* על מנת לאפשר מספר נתיבי successors נכפיל את הFD של הsuccessor בערך הvariance.
* ערך ברירת המחדל של הvariance הוא 1.
* כל הנתיבי feasible successors עם FD שווה או נמוך יותר מתוצאת המכפלה של הsuccessor עם הvariance יהפוך להיות successor בנוסף.

## ערכי K

חישוב הmetric ב EIGRP משתמש בשילוב של 5 משתנים, אך רק 2 משמשים כברירת מחדל (K1 ו-K3). הערכים המשולבים הם:

K1 (bandwidth) **= 1**  
K2 (load)  = 0  
K3 (delay)  = 1  
K4 (reliability)  = 0  
K5 (MTU - maximum transmit unit) = 0

רוחב הפס, העומס, ההשהיה, האמינות, ה-MTU הנמוכים ביותר לאורך הנתיב בין המקור ליעד נלקח בחשבון בmetric על מנת לחשב את העלות.

נוסחה לחישוב הmetric:

metric = ([K1 \* bandwidth + (K2 \* bandwidth) / (256 - load) + K3 \* delay] \* [K5 / (reliability + K4)]) \* 256

passive-interface

הגדרת ממשק פסיבי מונעת מהממשק לשלוח עדכוני ניתוב

**הגדרת EIGRP**

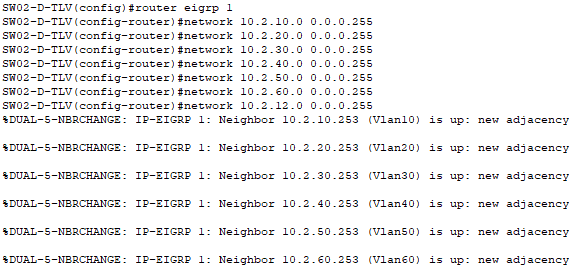
הגדרת פרוטוקול EIGRP במתג שכבה 3 בסניף השני:

תחילה נגדיר את כל הממשקים דרכם אנו רוצים לבצע ניתוב כממשקים בשכבה 3 על ידי הפקודה no switchport.

נגדיר כתובת Ip לכל אחד מהממשקים.

ניכנס למצב קונפיגורצית EIGRP בAS 80.

נגדיר לכל הרשתות המחוברות אלינו פיזית אשר נרצה לעשות ניתוב דרכן את הפקודה network אשר מבצעת יחסי שכנות עם כל הנתבים באותה רשת.



**פקודות SHOW**

show ip eigrp interfaces:

מראה סטטיסטיקה של כל הממשקים העובדים עם EIGRP

Interface – שם הממשק

Peers – כמות השכנים שהנתב מכיר בממשק

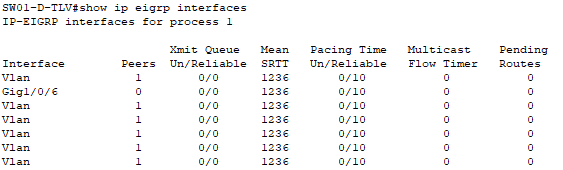
Xmit Queue Un/Reliable -

Mean SRTT-

Pacing Time Un/Reliable -

Multicast Flow Timer -

Pending Routes -



show ip eigrp neighbors:

בפקודה זו ניתן לראות טבלה של כל השכנים אשר הנתב מכיר ומידע נוסף עליהם כמו כתובת הIP שלהם, מאיזה ממשק הם הגיעו, מספר השניות שנותר להם לעדכן את נוכחותם.

Address – כתובת הIP של השכן.

Interface – הממשק המקומי דרכו מחובר השכן.

Hold – ספירה לאחור לפני מחיקת הנתב מהטבלה.

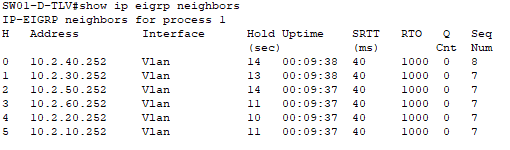
Up time – כמה זמן השכן בטבלה.

SRTT – הזמן שלקח לחבילת EIGRP להגיע לשכן ולחזור בחזרה.

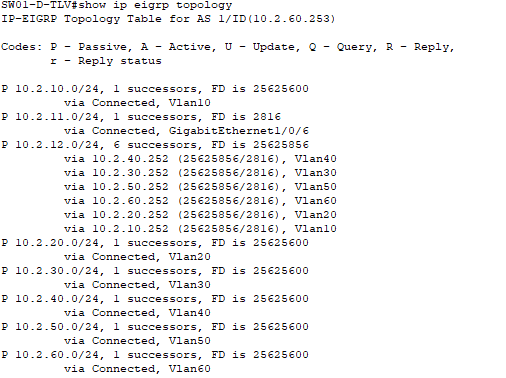
RTO – הזמן שהנתב יחכה לפני שישלח הודעת unicast במקרה ולא התקבלה חבילה מהשכן.

Q count - כמות החבילות שממתינות לשליחה.

Seq num – המספר הסידורי של החבילה האחרונה שהתקבלה.



בפקודה זו אנו רואים את כל הרשתות שהeigrp מכיר בין אם הן מחוברות ישירות או דרך שכן. לכל נתיב יש אות אשר אומרת לנו את המצב בו נמצא הנתיב. כשרואים את האות P הנתיב נמצא במצב Passive מה שאומר שהוא תקין ולא נדרש לחפש דרך להגיע ליעד. כאשר רואים את האות A הנתב מחפש בצורה אקטיבית דרך להגיע ליעד ולכן הנתיב אינו זמין. במידה ויש מספר נתיבים שאפשר לעבור דרכן לרשת מסוימת יהיה אפשר לראות אותם כfeasible successors. המספר הראשון בסוגריים הוא הFD והמספר השני הוא הAD.



באמצעות פקודה זו ניתן לראות מידע סטטיסטי על packets הרלוונטיים לeigrp.

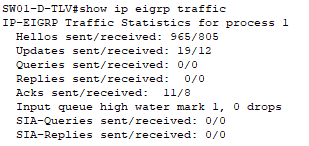
כמות חבילות הHELLO שנשלחו והתקבלו

כמות חבירות הUPDATES שנשלחו והתקבלו

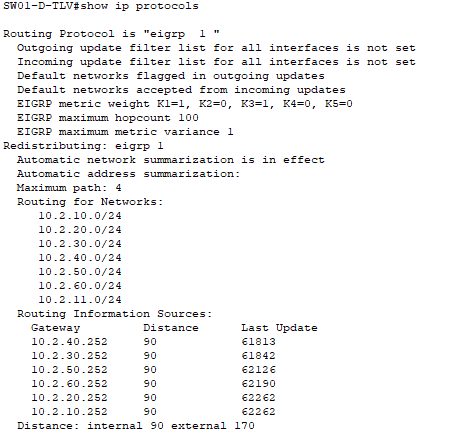
כמות חבירות QUERIES שנשלחו והתקבלו

כמות חבירות REPLIES שנשלחו והתקבלו

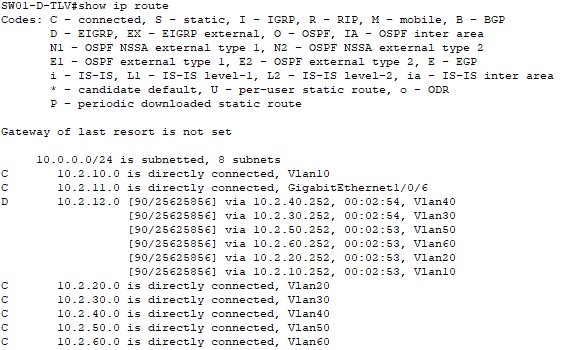
כמות חבירות ACK שנשלחו והתקבלו



Show ip protocols:



Show ip route:



# OSPF

Open Shortest Path First (OSPF) הוא פרוטוקול Link State המשמש למציאת הנתיב הטוב ביותר בין המקור לנתב היעד תוך שימוש ב-Shortest Path First שלו. OSPF פותח על ידי Internet Engineering Task Force (IETF) כאחד מפרוטוקול Interior Gateway (IGP), כלומר, הפרוטוקול שמטרתו להעביר את החבילה בתוך מערכת אוטונומית גדולה או תחום ניתוב. זהו פרוטוקול שכבת רשת שעובד על פרוטוקול מספר 89 ומשתמש בערך AD 110 . OSPF משתמש בכתובת multicast 224.0.0.5 לתקשורת רגילה ו-224.0.0.6 לעדכון לנתב ייעודי (DR)/נתב ייעודי גיבוי (BDR).

ערך הAD שלOSPF הוא: 110

OFPF הוא:

* OSPF הוא פרוטוקול שער פנימי (IGP).
* הוא פועל בתוך תחום ניתוב יחיד, כגון מערכת אוטונומית (AS).
* הוא משתמש במושג שנקרא areas, כדי לייעל את תעבורת הרשת ולפשט את הניהול.
* הוא פועל על פרוטוקול IP אך אינו משתמש בפרוטוקול תחבורה (כגון TCP או UDP) כדי להקיף את הנתונים שלו.

אלגורידם שהOSPF משתמש בו נקרא: Dijsktra

היתרונות של OSPF הם:

* זה מבוסס על תקן פתוח. זה יכול לפעול ברוב הנתבים.
* הוא משתמש באלגוריתם SPF כדי לספק טופולוגיה נטולת לולאות.
* זה תומך בשתי הגרסאות של IP. פרוטוקול OSPFv2 תומך ב-IPv4 ו-OSPFv3 תומך ב-IPv6.
* הוא תומך באיזון עומסים עם מסלולים בעלות שווה לאותו יעד.

החסרונות של OSPF הם:

* הוא זקוק למידע רב כדי לחשב את המסלול הטוב ביותר עבור כל יעד. כדי לאחסן מידע זה, OSPF צורך יותר זיכרון מאשר פרוטוקולי ניתוב אחרים.
* כדי לחשב את המסלול הטוב ביותר, הוא מריץ את אלגוריתם SPF הדורש עיבוד CPU רב.
* זה מורכב להגדרה וקשה לפתרון בעיות. ברשת גדולה, רק מנהלי רשת מנוסים יכולים להגדיר אותה.

## סיכום של תהליך OSPF

* + - 1. כל נתב לומד על הרשתות שמחוברות אליו ישירות
      2. כל נתב אחראי לשלוח חבירות HELLO לשכניו שמחוברים ישירות.
      3. כל נתב בונה חבילת LSP שמכילה את מצב (State) של כל ה Links
      4. כל נתב מציף Floods את חבילות הLSP לכל שכניו, אשר אוגרים את כל החבילות שהתקבלו בתוך הDatabase
      5. כל נתב משתמש בDatabase , בכדי לבנות "מפה כוללת" של טופולוגית הרשת , ומחשב את המסלול הטוב ביותר ליעדים.

שימוש בOSPF:

בדרך כלל, OSPF משמש ברשתות ארגוניות גדולות המשתמשות בציוד ניתוב של ספקים שונים. OSPF משמש גם בחברות שיש להן מדיניות להשתמש בפרוטוקול סטנדרטי פתוח לניתוב המעניק להן גמישות כאשר הן צריכות להחליף נתב קיים או להוסיף נתב חדש.

## יחסי שכנות

הודעות Hello של OSPF משמשות כדי לאפשר לנתב לגלות נתבים סמוכים אחרים בקישורים וברשתות המקומיות שלו. ההודעות מייצרות קשרים בין התקנים שכנים (הנקראים adjacencies) ומעבירות פרמטרים מרכזיים לגבי אופן השימוש ב-OSPF במערכת או בAS. בזמן פעולה רגילה, נתבים שולחים הודעות hello לשכניהם במרווחי זמן קבועים (hello interval); אם נתב יפסיק לקבל הודעות שלום מהשכן, לאחר תקופה מוגדרת (dead interval), הנתב יניח שהשכן ירד.

תנאים ליצירת יחסי שכנות:

Hello ו- Hold זהים

Area זהה

Password

subnet

שלבים עד ליצירת יחסי שכנות:

* Down
* Init
* Two-way
* Extart – מצב בו נבחר הDR והBDR
* Exchange – הנתבים מחליפים ביניהם description packet
* Loading – מעבירים ביניהם request packet וDBD
* Full - יחסי שכנות מלאים

ניתן למצוא את המצב הנוכחי באמצעות פקודת show ip ospf neighbor

דרכים שבהן OSPF יכול לקבוע את מזהה הנתב:

1. מזהה נתב מוגדר ידנית: זוהי השיטה הנפוצה ביותר להגדרת מזהה הנתב. מנהל הרשת מגדיר באופן ידני את מזהה הנתב בכל נתב ברשת. מזהה הנתב יכול להיות כל ערך של 32 סיביות, המתבטא בדרך כלל בסימון מנוקד-עשרוני, כגון 192.168.1.1.

2. כתובת ה-IP הגבוהה ביותר בממשק loopback: OSPF תבחר את כתובת ה-IP הגבוהה ביותר המוגדרת בממשק loopback כמזהה הנתב. אם ישנם ממשקי לולאה מרובים, OSPF יבחר את זה עם כתובת ה-IP הגבוהה ביותר.

3. כתובת ה-IP הגבוהה ביותר בממשק ללא לולאה: אם לא מוגדרים ממשקי לולאה חוזרים, OSPF תבחר את כתובת ה-IP הגבוהה ביותר שהוגדרה בכל ממשק פעיל כמזהה הנתב.

timers:

Hello timer - המרווח זמן שבו EIGRP שולח הודעת HELLO בממשק. זה 10 שניות כברירת מחדל.

dead timer - המרווח זמן שבו השכן יוכרז כלא פעיל אם לא יוכל לשלוח את חבילת HELLO. זה 30 שניות כברירת מחדל.

נ.ב: נהוג שזמן ה Dead timerחייב להיות גדול פי 3 מזמן ה Hello timer.

מושגים בOSPF:

* Router I’d - זוהי כתובת ה-IP הפעילה הגבוהה ביותר הקיימת בנתב. ראשית, הכתובת הloopback ביותר נחשבת. אם לא מוגדרת loopback, כתובת ה-IP הפעילה הגבוהה ביותר בממשק של הנתב נחשבת.
* Router priority - זהו ערך של 8 סיביות המוקצה לנתב המפעיל OSPF, המשמש לבחירת DR ו-BDR ברשת שידור.
* Designated Router (DR) - זה נבחר כדי למזער את מספר הסמיכות שנוצרו. DR מפיץ את ה-LSAs לכל שאר הנתבים. DR נבחר ברשת שידור שאליה כל שאר הנתבים חולקים את ה-DBD שלהם. ברשת שידור, הנתב מבקש עדכון ל-DR, ו-DR יגיב לבקשה זו בעדכון.
* Backup Designated Router (BDR) - BDR הוא גיבוי ל-DR ברשת שידור. כאשר DR יורד, BDR הופך ל-DR ומבצע את תפקידיו.
* DBD –

Link state packets:

* Link state request (LSR) - הודעות LSR משמשות נתב אחד כדי לבקש מידע מעודכן על חלק מה-LSDB מנתב אחר. ההודעה מציינת את הקישור/ים שעבורם המכשיר המבקש רוצה מידע עדכני יותר.
* Link state update (LSU) - הודעות LSU מכילות מידע מעודכן לגבי מצבם של קישורים מסוימים ב-LSDB. הם נשלחים בתגובה להודעת LSR, וגם משודרים או משודרים בmulticast על ידי נתבים על בסיס קבוע. התוכן שלהם משמש לעדכון המידע ב-LSDBs של נתבים שמקבלים אותם.
* Link state acknowledgment (LSAck) - הודעות LSAck מספקות מהימנות לתהליך Link state update, על ידי אישור מפורש על קבלת הודעת LSU.

תהליך בחירת הDR - בחירות DR ו-BDR מתקיימות ברשת broadcast. להלן הקריטריונים לבחירות:

1. נתב בעל Router priority הגבוהה ביותר יוכרז כ-DR.
2. אם יש שוויון בעדיפות הנתב אז הנתב עם ה Router I’d הגבוה יותר יוכרז כ-DR.

סוגי LSA:

n OSPF (Open Shortest Path First), ישנם ארבעה סוגים עיקריים של LSAs (Link State Advertisements) המשמשים להחלפת מידע ניתוב בין נתבים:

1. LSAs מסוג 1: LSAs אלה נוצרים על ידי כל נתב כדי לתאר את הקישורים המחוברים ישירות שלו ומוצפים לכל שאר הנתבים באותו אזור.

2. סוג 3 LSAs: LSAs אלה נוצרים על ידי ABR (נתב אזור גבול) כדי לתאר את המסלולים לרשתות באזורים אחרים. ה-ABR מסכם את המסלולים ומייצר LSA Type 3 עבור כל סיכום שמופץ לכל שאר הנתבים באזור.

3. סוג 5 LSAs: LSAs אלה נוצרים על ידי ASBRs (נתבי מערכת גבולות אוטונומית) כדי לתאר מסלולים חיצוניים המופצים מחדש לתחום OSPF. LSAs מסוג 5 מוצפים לכל הנתבים בתחום OSPF.

4. סוג 7 LSAs: LSAs אלה משמשים ב-NSSA (Not-So-Stubby Area) כדי לתאר מסלולים חיצוניים המופצים מחדש לתחום OSPF. LSAs מסוג 7 מוצפים רק בתוך ה-NSSA ומתורגמים ל-LSAs מסוג 5 על ידי ה-ABR לפני שהם מוצפים לתחום OSPF.

Path Cost

OSPF משתמש Path Cost כמדד הניתוב הבסיסי שלו, שהוגדר על ידי התקן שלא ישווה לשום ערך סטנדרטי כגון מהירות, כך שמעצב הרשת יכול לבחור מדד חשוב לתכנון. בפועל, זה נקבע על ידי השוואת מהירות הממשק לרוחב פס ייחוס עבור תהליך OSPF. העלות נקבעת על ידי חלוקת רוחב הפס הייחוס במהירות הממשק (אם כי ניתן לעקוף את העלות עבור כל ממשק באופן ידני). אם רוחב פס ייחוס מוגדר ל-'10000', קישור של 10 ג'יגה-ביט/שניה יהיה בעל עלות של 1. כל מהירויות הנמוכות מ-1 מעוגלות כלפי מעלה ל-1.

OSPF Summarization

ניתן להגדיר את סיכום הרשת ב-OSPF בנתב OSPF בגבול האזור או בגבול ה-AS.

בגבול האזור, נתב יכול לסכם את המסלולים של כל רשתות המשנה באזור מסוים ולפרסם מסלול מסוכם יחיד לאזור זה לאזורים אחרים. זה מקטין את גודל טבלת הניתוב ואת כמות התעבורה הנדרשת לפרסום רשתות המשנה. הנתב יכול לבצע סיכום על הממשק היוצא של האזור או על ידי יצירת כתובת סיכום באופן ידני.

בגבול AS, סיכום מתבצע על ידי סיכום מסלולים ממספר אזורים למסלול אחד. זה נעשה כדי להקטין את גודל טבלת הניתוב ולשפר את יעילות הניתוב. הנתב יכול לבצע סיכום על הממשק היוצא של ה-ASBR (Autonomous System Boundary Router) או על ידי יצירת כתובת סיכום באופן ידני.

Virtual link

ב-OSPF (Open Shortest Path First), קישור וירטואלי הוא חיבור לוגי בין שני ABRs (Area Border Routers) שאינם מחוברים ישירות אך בעלי אזור משותף. קישור וירטואלי משמש ליצירת קישוריות בין שני חלקים של תחום OSPF שאחרת היו מבודדים עקב היעדר חיבור פיזי.

קישורים וירטואליים משמשים בדרך כלל במצבים שבהם חיבור פיזי בין שני ABRs אינו אפשרי, אך יש אזור משותף בין שני ABRs. לדוגמה, נניח שיש שלושה אזורים בתחום OSPF, A, B ו-C, ו- ABR1 מחבר אזור A לאזור B ו- ABR2 מחבר אזור B לאזור C. אם אין קשר פיזי ישיר בין ABR1 ל- ABR2, אך שניהם מחוברים לאזור B, ניתן ליצור קישור וירטואלי בין ABR1 ל-ABR2 דרך אזור B. זה מאפשר לתנועה לזרום מאזור A לאזור C, למרות שאין קשר ישיר בין ABR1 ל-ABR2.

כדי להגדיר קישור וירטואלי, יש לעמוד בדרישות הבאות:

1. שני ה-ABRs חייבים להיות באותו תחום OSPF וחייבים להיות בעלי אזור משותף.

2. האזור שדרכו נוצר הקישור הוירטואלי חייב להיות לא עמוד שדרה.

3. לשני ה-ABRs חייב להיות רשת מלאה של חיבורים מנקודה לנקודה לאזור המשותף.

4. כתובות ה-IP המשמשות בקישור הווירטואלי חייבות להיות נגישות לשני ה-ABRs.

לאחר עמידה בדרישות אלו, ניתן להגדיר את הקישור הווירטואלי על ידי ציון מזהה הנתב של הקצה השני של הקישור הווירטואלי, יחד עם האזור שדרכו הקישור הוירטואלי יוקם.

לאחר מכן מתייחסים לקישור הוירטואלי כקישור OSPF רגיל, ושני ה-ABRs מחליפים מידע ניתוב כאילו היו מחוברים ישירות. זה מאפשר לתחום OSPF לתפקד כאילו היה קישור פיזי בין שני ה-ABRs, ומאפשר הפצת מידע ניתוב בכל תחום ה-OSPF.

Stub

ב-OSPF (Open Shortest Path First), אזור בדל הוא אזור שבו חלק מהנתיבים החיצוניים אינם מתפשטים. זה מקטין את גודל מסד הנתונים של OSPF והופך את הרשת ליעילה יותר על ידי הפחתת כמות מידע הניתוב שיש לתחזק ולהחליף.

באזור בדל, ה-ABR (נתב הגבול האזורי) מייצר סוג מיוחד של LSA (מודעת קישור מדינתית) הנקראת LSA סיכום 3 שמסכם את המסלולים מאזורים אחרים. לאחר מכן, ה-ABR מזריק את המסלולים המסוכמים לאזור הבדל. מסלולים חיצוניים (LSA סוג 5) אינם מותרים באזורי בדל, וכל מסלול כזה המתקבל על ידי ה-ABR אינו מופץ לאזור הסטב.

ישנם שני סוגים של אזורי בדל ב-OSPF: אזורי בדל רגילים ואזורים גדושים לחלוטין.

אזור בדל רגיל: באזור בדל רגיל, מסלולים חיצוניים אינם מותרים, אך מסלול ברירת מחדל מוזרק על ידי ה-ABR. נתיב ברירת מחדל זה משמש להפניית תעבורה לרשתות מחוץ לתחום OSPF.

אזור קשוח לחלוטין: באזור קשוח לחלוטין, הן מסלולים חיצוניים והן תקצירי LSA מסוג 3 אינם מותרים. ה-ABR מחדיר נתיב ברירת מחדל לאזור הקשוח לחלוטין, וכל התנועה ליעדים מחוץ לתחום OSPF מופנית לנתיב ברירת המחדל הזה.

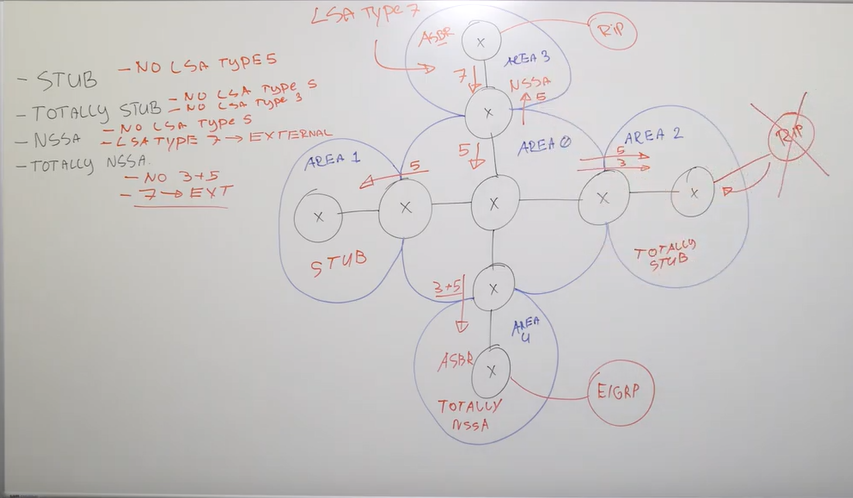
בנוסף לאזורי בדל, OSPF תומך גם ב-Non-So-Stuby Areas (NSSAs). NSSA הוא אזור בו מותרים מסלולים חיצוניים, אך רק באופן מוגבל. NSSAs דומים לאזורי בדל בכך שהם מקטינים את גודל מסד הנתונים של OSPF ומגבילים את כמות מידע הניתוב שיש לתחזק ולהחליף. ב-NSSA, מסלולים חיצוניים מתפרסמים באמצעות סוג מיוחד של LSA הנקרא Type 7 LSA. ה-ABR מתרגם את ה-LSAs הללו ל-LSAs מסוג 5 ומחדיר אותם לתחום OSPF.

ישנם שני סוגים של NSSAs ב-OSPF: NSSAs רגילים ו-NSSAs לחלוטין.

NSSA רגיל: ב-NSSA רגיל, מסלולים חיצוניים מותרים, אך מסלול ברירת מחדל מוזרק על ידי ABR כדי למנוע הפצה של LSAs מסוג 5 מאזורים אחרים.

NSSA לחלוטין: ב-NSSA לחלוטין, הן מסלולים חיצוניים והן תקצירי LSA מסוג 3 אינם מותרים. ה-ABR מזריק מסלול ברירת מחדל ומתרגם LSAs Type 7 ל-LSAs Type 5, אך אינו מפיץ אף LSA מסוג 3.

אזורי Stub, NSSA ו- Totally NSSA נמצאים בשימוש נפוץ ברשתות OSPF גדולות כדי לשפר את ביצועי הרשת ומדרגיות. על ידי הפחתת כמות מידע הניתוב המוחלף בין נתבים, אזורים אלה יכולים לעזור להפחית את כמות תעבורת הרשת ואת העיבוד הנדרש על ידי נתבים. בנוסף, אזורים אלה יכולים לסייע במניעת לולאות ניתוב ובעיות רשת אחרות על ידי הגבלת כמות המידע המשותף בין אזורים שונים ברשת.



**הגדרת OSPF**

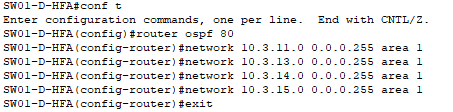
הגדרת פרוטוקול OSPF במתג שכבה 3 בסניף השלישי:

תחילה נגדיר את כל הממשקים דרכם אנו רוצים לבצע ניתוב כממשקים בשכבה 3 על ידי הפקודה no switchport.

נגדיר כתובת Ip לכל אחד מהממשקים.

ניכנס למצב קונפיגורצית EIGRP בprocces ID 80.

נגדיר לכל הרשתות המחוברות אלינו פיזית אשר נרצה לעשות ניתוב דרכן את הפקודה network אשר מבצעת יחסי שכנות עם כל הנתבים באותה רשת.



show ip ospf:

הפקודה show ip ospf משמשת להצגת מידע על פרוטוקול הניתוב Open Shortest Path First (OSPF). הפלט של הפקודה show ip ospf כולל את המידע הבא:

- מזהה התהליך של OSPF, המזהה את מופע OSPF הפועל על הנתב.

- מזהה הנתב, שהוא מזהה ייחודי עבור הנתב בתחום OSPF.

- מזהה האזור, שהוא מספר 32 סיביות המגדיר קיבוץ לוגי של נתבים ורשתות שחולקים את אותו מידע מצב קישור.

- סטטיסטיקת ביצוע אלגוריתם SPF, המראים כמה פעמים הנתב רץ את אלגוריתם הנתיב הקצר ביותר (SPF) כדי לחשב את המסלולים הטובים ביותר, וכמה זמן לקח להשלים כל חישוב.

- מספר האזורים והממשקים המשתתפים ב-OSPF בנתב.

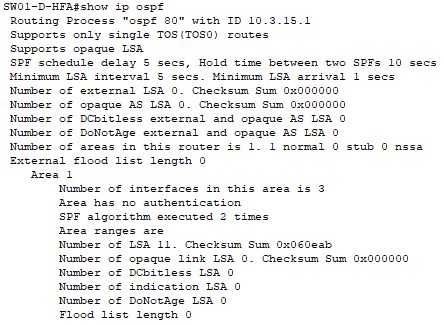
- סוג האימות ושם שרשרת המפתחות המוגדרים עבור OSPF בנתב.

- רוחב הפס הייחוס המשמש לחישוב מדד עלות OSPF עבור כל ממשק.

- מידע ההפצה מחדש שמראה אילו מסלולים מפרוטוקולי ניתוב אחרים או מסלולים סטטיים מופצים מחדש ל-OSPF, ועם אילו ערכי מדד ותג.

- מידע על אזור ה-Stub המציג אילו אזורים מוגדרים כאזורי בדל או לא-כל-כך-אזורים (NSSAs), ואיזה פרמטרים משמשים עבורם.

- מידע סיכום המסלול החיצוני שמראה כמה מסלולים חיצוניים (סוג 1 או סוג 2) נמצאים במסד הנתונים של OSPF, ומהי העלות הכוללת שלהם.



show ip ospf database:

הפלט של הפקודה show ip ospf database מציג את המידע הבא עבור כל LSA:

- סוג LSA: סוג ה-LSA, כגון נתב, רשת, סיכום, AS חיצוני או NSSA חיצוני.

- מזהה מצב קישור: המזהה של ה-LSA, התלוי בסוג ה-LSA. לדוגמה, עבור LSAs של נתב, זהו מזהה הנתב של הנתב המקורי; עבור LSAs ברשת, זוהי כתובת ה-IP של ממשק DR; עבור LSAs סיכום, זוהי כתובת הרשת והמסיכה; עבור AS חיצוניים או NSSA LSAs חיצוניים, זוהי כתובת הרשת החיצונית ומסיכה.

- נתב Adv: מזהה הנתב של הנתב שמקורו או פרסם את ה-LSA.

- גיל: הזמן בשניות מאז נוצר או רענון ה-LSA.

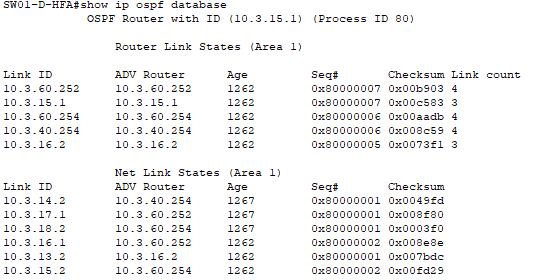
- Seq#: מספר הרצף של ה-LSA, המשמש לזיהוי LSAs ישנים או כפולים.

- Checksum: סכום הבדיקה של ה-LSA, המשמש לאימות תקינות ה-LSA.

- אורך: אורך ה-LSA בבתים.

הפלט של הפקודה show ip ospf database מציג גם פרטים נוספים על כל LSA כאשר אתה מזין סוג LSA ספציפי כארגומנט. לדוגמה, נתב מסד הנתונים של show ip ospf יציג מידע נוסף על כל נתב LSA, כגון מספר הקישורים, סוג הקישור, מזהה קישור, נתוני קישור, עלות קישור ומצב קישור.

הפקודה show ip ospf מסד נתונים שימושית לפתרון בעיות ניתוב OSPF, כגון כשלי סמיכות, לולאות ניתוב או מסלולים שגויים. על ידי בחינת מסד הנתונים של OSPF, אתה יכול לוודא אם לנתבים יש תצוגה עקבית של טופולוגיית הרשת ואם הם קיבלו ועיבדו את כל ה-LSAs בצורה נכונה.

****

show ip ospf interface :

הפקודה cisco cli show ip ospf מציגה מידע על הממשקים התומכים ב-OSPF בנתב. הפלט של פקודה זו כולל פרמטרים שונים המתארים את המצב והתצורה של הממשק, כגון:

- שם הממשק והכתובת

- מזהה תהליך OSPF ומזהה אזור

- סוג רשת OSPF ועלות

- OSPF Hello ו-dead intervals

- סוג ומפתח האימות של OSPF

- ספירת השכנים של OSPF ומצב הסמיכות

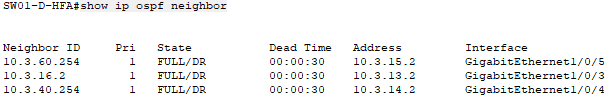
- מזהים וכתובות של נתב ייעודי OSPF (DR) ושל נתב ייעודי לגיבוי (BDR).

- הנתונים הסטטיסטיים של OSPF קישור-מצב פרסומת (LSA).

הפקודה show ip ospf interface יכולה להיות שימושית לפתרון בעיות של OSPF, כגון סמיכות שכנות, סוגי רשת, עלויות ממשק והצפה של LSA. לדוגמה, אם שכן OSPF תקוע במצב INIT, הפקודה show ip ospf interface יכולה לעזור לזהות אם יש חוסר התאמה בסוג הרשת, מרווח שלום, מרווח מת או הגדרות אימות בין שני הנתבים. אם ממשק OSPF אינו מקבל או שולח LSAs, הפקודה show ip ospf interface יכולה לעזור לאמת אם הממשק מופעל עבור OSPF, אם יש לו כתובת IP ומזהה אזור חוקיים, ואם יש לו שכנים או תפקידי DR/BDR .



show ip ospf neighbor:



show ip route:

הפקודה show ip route משמשת להצגת טבלת ניתוב IP של נתב Cisco. טבלת ניתוב ה-IP מכילה מידע על המסלולים ליעדי רשת שונים שהנתב למד ממקורות שונים, כגון מסלולים סטטיים, פרוטוקולי ניתוב דינמיים או ממשקים מחוברים ישירות. ניתן לחלק את הפלט של הפקודה show ip route למספר חלקים:

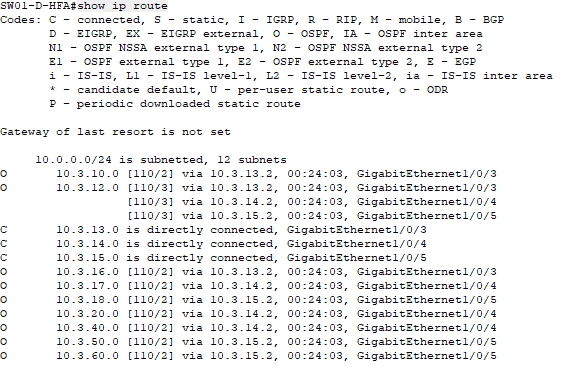
- השורה הראשונה מציגה את שם המארח של הנתב ואת התאריך והשעה שבהם הפקודה בוצעה.

- השורה השנייה מציגה את הקודים המשמשים לזיהוי המקור של כל כניסה למסלול. לדוגמה, C פירושו מחובר, S פירושו סטטי, R פירושו RIP, O פירושו OSPF, וכן הלאה.

- השורות הבאות מציגות את ערכי המסלול בפועל בפורמט של [קוד] [רשת] [מסכה] [הקפיצה הבאה] [מרחק אדמיניסטרטיבי] [מדד]. לדוגמה, C 192.168.1.0/24 מחובר ישירות, FastEthernet0/0 אומר שהרשת 192.168.1.0/24 מחוברת ישירות לממשק FastEthernet0/0 של הנתב.

- השורה האחרונה מציגה את מספר המסלולים בטבלת הניתוב ומספר רשתות המשנה.

הפקודה show ip route יכולה גם לקבל אפשרויות ופרמטרים שונים לסינון או לשנות את הפלט. לדוגמה, show ip route summary מציג תקציר של טבלת הניתוב, show ip route ospf מציג רק את המסלולים שנלמדו מ-OSPF, show ip route 10.0.0.0 מציג רק את המסלולים לרשת 10.0.0.0 וכן הלאה.



show ip protocols:

הפקודה show ip protocols משמשת להצגת מידע על פרוטוקולי הניתוב המוגדרים בנתב של סיסקו. הפלט של פקודה זו כולל:

- השם ומזהה התהליך של כל פרוטוקול ניתוב שפועל על הנתב

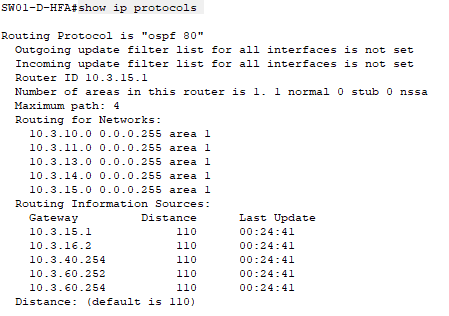
- הרשתות המפורסמות לפי כל פרוטוקול ניתוב והמרחק הניהולי של רשתות אלו

- הטיימרים והמדדים המשמשים כל פרוטוקול ניתוב

- השכנים שנקבעים לפי כל פרוטוקול ניתוב ומעמדם

- המסננים וכללי הפצה מחדש המוחלים על כל פרוטוקול ניתוב

הפקודה show ip protocols יכולה להיות שימושית לפתרון בעיות ניתוב, אימות תצורות ניתוב וניטור ביצועי ניתוב. לדוגמה, באמצעות פקודה זו, ניתן לבדוק אם פרוטוקול ניתוב מופעל על הנתב, אם הוא מפרסם את הרשתות הנכונות, אם הוא מקבל עדכונים מנתבים אחרים, אם הוא מסנן או מפיץ מחדש מסלולים כצפוי, וכן הלאה. עַל.



# טבעת BGP

**BGP**

BGP הוא פרוטוקול path-vector, מה שאומר שהוא משתמש בגישה מבוססת נתיב לניתוב. במילים אחרות, נתבי BGP מחליפים מידע על הנתיבים לרשתות שונות, ולא רק על היעדים עצמם. זה מאפשר ל-BGP לקחת בחשבון גורמים כמו מדיניות רשת, עלויות קישור וגורמים אחרים שעשויים להשפיע על הנתיב הטוב ביותר ליעד מסוים.

BGP הוא גם פרוטוקול classless, מה שאומר שהוא תומך במסכות משנה באורך משתנה (VLSM). זה מאפשר ל-BGP להיות גמיש יותר בניתוב תעבורה לרשתות שונות עם מסכות רשת שונות.

נתבי BGP מחליפים מידע על מסלולים באמצעות סדרה של הודעות הנקראות עדכוני BGP. כאשר נתב BGP מקבל עדכון מנתב שכן, הוא משווה את המידע בעדכון לטבלת הניתוב שלו ומבצע את כל העדכונים הדרושים. נתבי BGP גם מחליפים הודעות Keepalive כדי להבטיח שעדיין ניתן להגיע לשכניהם.

בארכיטקטורת טבעת BGP, נתבים מרובים המריצים BGP מחוברים בטופולוגיה מעגלית. כל נתב בטבעת מחובר לשני נתבים אחרים, ויוצרים לולאה סגורה. כל נתב בטבעת נחשב ל"עמית" לנתבים האחרים, והם מחליפים מידע ניתוב באמצעות פרוטוקול BGP.

אחד היתרונות המרכזיים של טבעת BGP הוא שהיא מספקת יתירות. אם נתב או קישור אחד בטבעת נכשל, BGP יכול לנתב מחדש את התעבורה באופן אוטומטי דרך נתיב אחר, ולמזער את ההפרעה לתקשורת ברשת. זה ידוע בשם "התכנסות מהירה" מכיוון שהוא מאפשר לרשת להסתגל במהירות לשינויים בטופולוגיית הרשת.

יתרון נוסף של טבעת BGP הוא שהיא יכולה לסייע במניעת לולאות ניתוב. לולאות ניתוב מתרחשות כאשר יש תצורה שגויה בטבלת הניתוב, הגורמת להעברת מנות בלולאה. מכיוון שלטבעת BGP יש טופולוגיה של לולאה סגורה, סביר להניח שהיא תחווה לולאות ניתוב.

ניתן להשתמש בטבעת BGP גם לחיבור מספר מערכות אוטונומיות (AS) יחד. AS הוא אוסף של רשתות תחת תחום ניהול משותף, ו-BGP משמש לעתים קרובות להחלפת מידע ניתוב בין ASes שונים. ניתן להשתמש בטבעת BGP כדי לחבר מספר ASes יחד באופן המספק יתירות ועוזר למנוע לולאות ניתוב.

Chart, radar chart

Description automatically generated

A picture containing text

Description automatically generated

ISP

ספק שירותי אינטרנט (ISP) היא חברה המספקת גישה לאינטרנט ללקוחות. ספקיות אינטרנט מחברות לקוחות לאינטרנט באמצעות מגוון טכנולוגיות, כולל קווי טלפון נחושת, כבלים וסיבים אופטיים.

אחת הדרכים הנפוצות ביותר שבהן ספקיות אינטרנט מספקות גישה לאינטרנט היא באמצעות קווי טלפון נחושת, הידועים גם בתור קווי DSL (Digital Subscriber Line). טכנולוגיית DSL מאפשרת העברת נתונים על אותם קווי טלפון נחושת המשמשים לשירות טלפוני. הנתונים מועברים בתדירות גבוהה יותר מאות הטלפון, מה שמאפשר להפריד בין שני האותות בחצר הלקוח באמצעות מסנן DSL.

דרך נוספת שבה ספקיות האינטרנט מספקות גישה לאינטרנט היא באמצעות קווי טלוויזיה בכבלים. אינטרנט בכבלים פועל על ידי שליחת נתונים ללקוחות דרך אותם קווי טלוויזיה בכבלים המשמשים להעברת תכניות טלוויזיה. מודמי כבלים משמשים להמרת הנתונים לאות, שניתן להעבירו על גבי קווי הכבלים ולאחר מכן להמיר אותם בחזרה לאות שמיש עבור הלקוח.

קווי סיבים אופטיים משמשים גם ספקי אינטרנט מסוימים כדי לספק גישה לאינטרנט. קווי סיבים אופטיים עשויים מחוטים דקים של זכוכית או פלסטיק המסוגלים להעביר נתונים במהירויות גבוהות במיוחד. הנתונים מועברים כפולסי אור לאורך קווי הסיבים האופטיים. קווי סיבים אופטיים מהירים ואמינים יותר מקווי נחושת או כבלים, אך הם גם יקרים יותר להתקנה.

ברגע ש-ISP חיבר לקוח לאינטרנט, למחשב או למכשיר של הלקוח מוקצית כתובת IP. כתובת IP זו משמשת לזיהוי מכשיר הלקוח באינטרנט ולניתוב נתונים אל המכשיר וממנו.

רשת של ספק שירותי אינטרנט היא התשתית המאפשרת אספקת שירות אינטרנט ללקוחות. הרשת מורכבת ממספר מרכיבים מרכזיים:

רשת עמוד שדרה: זוהי הרשת המהירה למרחקים ארוכים המחברת את מרכזי הנתונים של ספק שירותי האינטרנט ורכיבי רשת ליבה אחרים זה לזה. רשת עמוד השדרה מורכבת בדרך כלל מקישורי סיבים אופטיים במהירות גבוהה ומיועדת להתמודד עם כמויות גדולות של תעבורת נתונים.

רשת גישה: זוהי הרשת המחברת את רשת השדרה ללקוחות. רשת הגישה יכולה לכלול מגוון טכנולוגיות כגון DSL, כבלים וקווי סיבים אופטיים. רשת הגישה אחראית להפסקת החיבור של הלקוח לאינטרנט ולספק ללקוח כתובת IP.

נתבים: מכשירים אלה אחראים להעברת מנות נתונים ליעדם. ספקיות האינטרנט משתמשות בנתבים כדי להפנות תעבורת נתונים למכשירי הלקוח וממנו ולרשתות אחרות באינטרנט.

שרתי תרגום כתובות רשת (NAT): שרתי NAT משמשים ספקי אינטרנט כדי לאפשר למספר לקוחות לשתף כתובת IP אחת. שרתי NAT מתרגמים את כתובות ה-IP הפרטיות המשמשות ברשת ה-LAN של הלקוח לכתובת IP ציבורית אחת המשמשת באינטרנט.

חומות אש: חומות אש משמשות לאבטחת הרשת של ספק שירותי האינטרנט על ידי שליטה בגישה לרשת וממנה. ניתן להשתמש בהם כדי לחסום תעבורה לא רצויה וכדי להגן על הרשת מפני התקפות זדוניות.

רשתות אספקת תוכן (CDN): ספקי שירותי אינטרנט משתמשים לרוב ב-CDN כדי לשפר את אספקת התוכן ללקוחות. CDNs הם רשתות של שרתים המופצות ברחבי העולם ומשמשות לאחסון ואספקת תוכן קרוב יותר ללקוח, תוך הפחתת זמן ההשהיה ושיפור הביצועים.

לסיכום, ISP היא חברה המספקת גישה לאינטרנט ללקוחות באמצעות טכנולוגיות שונות, כגון DSL, כבלים וסיבים אופטיים. רשת ISP מורכבת ממספר מרכיבים מרכזיים, כולל רשת עמוד השדרה, רשת גישה, נתבים, שרתי NAT, חומות אש ו-CDNs. רכיבים אלו פועלים יחד כדי לספק שירות אינטרנט ללקוחות ולהבטיח את האבטחה והאמינות של הרשת

## הגדרת ISP

A picture containing text

Description automatically generated

Metro Ethernet

Metro Ethernet היא סוג של רשת מהירה המשתמשת בטכנולוגיית Ethernet כדי לחבר מספר מיקומים בתוך אזור מטרופולין. הוא מספק פתרון ניתן להרחבה וחסכוני לעסקים שצריכים לחבר אתרים מרובים, כגון משרדים או מקומות קמעונאיים, על גבי רשת רחבה (WAN).

ניתן לבנות רשתות Metro Ethernet באמצעות מגוון טכנולוגיות שונות, כולל כבלי סיבים אופטיים, כבלי נחושת וקישורים אלחוטיים. הסוג הנפוץ ביותר של רשת Metro Ethernet משתמש בכבלי סיבים אופטיים כדי לספק קישוריות מהירה ואמינה בין אתרים. סוג זה של רשת נקרא לעתים קרובות רשת Fiber Ethernet או Fiber Metro Ethernet.

אחד היתרונות המרכזיים של Metro Ethernet הוא היכולת שלו לגדול. עסקים יכולים בקלות להוסיף רוחב פס נוסף או חיבורים נוספים ככל שהצרכים שלהם משתנים, מה שמאפשר להם להגדיל את הרשת שלהם ככל שהעסק שלהם גדל. בנוסף, Metro Ethernet ניתנת להתאמה אישית רבה, ומאפשרת לעסקים לבחור את רמת השירות ואיכות השירות המתאימה ביותר לצרכיהם.

Metro Ethernet מספקת גם פתרון חסכוני לעסקים שצריכים לחבר מספר מיקומים. על ידי שימוש בתשתית קיימת כגון כבלי סיבים או נחושת קיימים, עסקים יכולים להימנע מהעלויות הגבוהות הכרוכות בבניית רשת חדשה מאפס.

Metro Ethernet מספקת גם סוגים שונים של שירותים (CoS) לסוגי תעבורה שונים, כגון קול, וידאו ונתונים, מה שנותן לעסקים את היכולת לתעדף סוגים שונים של תעבורה ולהבטיח שיישומים קריטיים יקבלו את רוחב הפס הדרושים להם.

בפן הטכני, רשתות Metro Ethernet משתמשות באותה טכנולוגיית Ethernet כמו רשתות מקומיות (LAN), אך הן מיועדות לפעול על פני שטח רחב. ההבדל העיקרי בין רשתות LAN ורשתות Metro Ethernet הוא המרחק שבו הרשת מורחבת. רשתות Metro Ethernet יכולות להשתרע על פני מרחקים של עד כמה מיילים, בעוד שרשתות LAN בדרך כלל מתרחבות על פני מרחקים של פחות ממייל.

בסך הכל, Metro Ethernet הוא פתרון גמיש וחסכוני לעסקים שצריכים לחבר מספר אתרים בתוך אזור מטרופולין. הוא מספק קישוריות מהירה ואמינה וניתן להרחבה בקלות ולהתאמה אישית כדי לענות על הצרכים הייחודיים של כל עסק.

## יישום OSPF על גבי הMetro Ethernet

כדי לגרום לרשת Metro Ethernet לעבוד עם פרוטוקול ניתוב OSPF (Open Shortest Path First), הרשת חייבת להיות מוגדרת עם נתבים התומכים OSPF בכל מיקום. OSPF הוא פרוטוקול ניתוב המשמש לגילוי ועדכון מידע ניתוב באופן דינמי בין מיקומים שונים ברשת. על ידי הגדרת הנתבים עם OSPF, הרשת יכולה לגלות באופן אוטומטי חיבורים חדשים ולעדכן טבלאות ניתוב כדי להבטיח שהנתונים נשלחים בנתיב היעיל ביותר.

ברגע ש-OSPF מוגדר ופועל ברשת Metro Ethernet, הוא יגלה אוטומטית חיבורים חדשים ויעדכן טבלאות ניתוב כדי להבטיח שהנתונים נשלחים בנתיב היעיל ביותר. זה מבטיח ביצועים ואמינות מיטביים של הרשת.

זכור ש-OSPF אינו פרוטוקול הניתוב היחיד שניתן להשתמש בו ברשת Metro Ethernet, אחרים כגון ניתוב סטטי יכולים לשמש גם בהתאם לצרכים הספציפיים של הרשת.

Chart

Description automatically generated

# VPN

רשת פרטית וירטואלית (VPN) היא טכנולוגיה שיוצרת חיבור מאובטח ומוצפן על גבי רשת פחות מאובטחת, כגון האינטרנט. VPNs משמשים לעתים קרובות כדי להגן על נתונים רגישים ולספק גישה מאובטחת לרשתות מרוחקות, כגון רשת פנימית של חברה או רשת ביתית בזמן נסיעה.

VPNs פועלים על ידי יצירת "מנהרה" בין המכשיר של המשתמש לשרת של ספק ה-VPN. המנהרה הזו מצפינה את כל הנתונים שנשלחו והתקבלו, מה שמקשה על כל אחד ליירט את הנתונים. הצפנה זו נעשית בדרך כלל באמצעות פרוטוקולים כגון OpenVPN, IKEv2/IPSec ו-L2TP/IPSec.

ניתן להשתמש ב-VPN במגוון דרכים. כמה שימושים נפוצים כוללים:

גישה מרחוק: עובדים יכולים להשתמש ב-VPN כדי לגשת בצורה מאובטחת לרשת הפנימית של החברה תוך כדי עבודה מרחוק.

גלישה מאובטחת: VPNs יכולים להגן על הפעילות המקוונת של המשתמשים מפני מעקב ותיעוד על ידי ספק שירותי האינטרנט שלהם (ISP) או צדדים שלישיים אחרים.

עקיפת צנזורה: VPNs יכולים לעזור למשתמשים לגשת לאתרים ולתכנים חסומים על ידי ניתוב תנועה דרך שרת שנמצא במדינה אחרת.

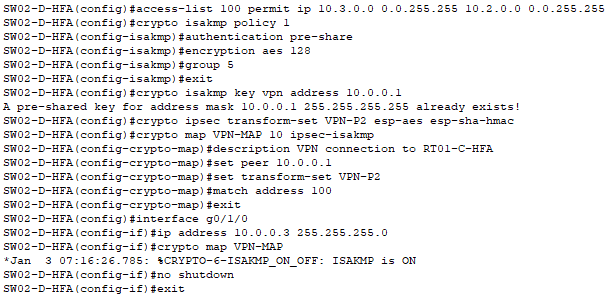
שיפור האבטחה: ניתן להשתמש ב-VPN לאבטחת תקשורת ברשתות Wi-Fi ציבוריות, כמו אלה בשדות תעופה ובתי קפה.

ישנם מספר סוגים של VPNs, כולל:

Remote-access VPNs: מאפשר למשתמשים להתחבר לרשת מרוחקת מכל מקום.

Site-to-site VPNs: מחברים מספר אתרים קבועים יחד, כגון חיבור סניף לרשת מטה.

## הגדרת VPN



## פקודות SHOW

הפקודה show crypto ipsec sa משמשת להצגת המצב והפרמטרים של IPsec (SA). IPsec פלט הפקודה מציג מידע כגון:

- כתובות ה-IP המקומיות והמרוחקות של העמיתים המעורבים ב-IPsec SA

- אלגוריתמי ההצפנה והאימות המשמשים להגנה על הנתונים

- מצב האנקפסולציה (מנהרה או תחבורה) והפרוטוקול (ESP או AH) המשמשים עבור ה-IPsec SA

- משך החיים והזמן הנותר של ה-IPsec SA

- מספר החבילות והבתים המוצפנים ומפוענחים על ידי ה-IPsec SA

- מדיניות האבטחה (מפת קריפטו) התואמת את ה-IPsec SA

ניתן להשתמש בפקודה show crypto ipsec sa עם אפשרויות שונות לסינון או לשנות את הפלט. לדוגמה, אתה יכול לציין כתובת עמית, ממשק, שם מפת קריפטו או כיוון (נכנס או יוצא) כדי להציג רק את ה-IPsec SAs הרלוונטיים. אתה יכול גם להשתמש באפשרות הפירוט כדי להציג מידע מפורט יותר על כל IPsec SA, כגון:

- ערך אינדקס פרמטר האבטחה (SPI) המזהה את ה-IPsec SA

- גודל החלון נגד שידור חוזר ומספר הרצף

- שם סדרת השינוי והעדיפות

- שיטת קבוצת דיפי-הלמן והחלפת מפתחות

- סטטוס וקבוצה של סודיות קדימה (PFS) מושלמת

- מצב הדחיסה והאלגוריתם

אחד השדות בפלט הוא מוני החבילות, שמראים כמה מנות הוצפנו ופועחנו על ידי ה-IPsec SA. מוני החבילות מחולקים לשתי קטגוריות: שליחה וקבלה. מוני השליחה מראים כמה מנות נשלחו מהמכשיר המקומי למכשיר המרוחק באמצעות ה-IPsec SA. מוני הקבלה מראים כמה מנות התקבלו מהמכשיר המרוחק למכשיר המקומי באמצעות ה-IPsec SA.

מוני החבילות יכולים לעזור לזהות אם יש אובדן מנות או אי התאמה בין שני המכשירים. לדוגמה, אם מונה השליחה גבוה בהרבה ממונה הקבלה במכשיר אחד, זה עשוי להצביע על כך שמנות מסוימות נשמטות או נדחות על ידי ההתקן המרוחק. לעומת זאת, אם מונה הקבלה גבוה בהרבה ממונה השליחה במכשיר אחד, זה עשוי להצביע על כך שחלק מהמנות משוכפלות או מושמעות מחדש על ידי המכשיר המרוחק.

מוני החבילות יכולים גם לעזור לאמת אם ה-IPsec SA פועל בצורה נכונה ומאובטחת. לדוגמה, אם המונים המוצפנים והמפוענחים שווים בשני המכשירים, זה אומר שכל החבילות מוצפנות ומפענחות בהצלחה על ידי ה-IPsec SA. עם זאת, אם יש אי התאמה בין המונים המוצפנים והמפוענחים בכל אחד מהמכשירים, זה עשוי להצביע על בעיה בתהליך ההצפנה או הפענוח, כגון מפתח או אלגוריתם שגויים.

ניתן לאפס את מוני החבילות באמצעות פקודת clear crypto ipsec sa. זה יכול להיות שימושי למטרות בדיקה או בעת פתרון בעיות ספציפיות. עם זאת, איפוס מוני החבילות יאפס גם שדות אחרים בפלט, כגון משך החיים ומספר הרצף של ה-IPsec SA.

הפקודה show crypto ipsec sa שימושית לפתרון בעיות ואימות תצורות IPsec VPN. זה יכול לעזור לך לזהות בעיות כמו פרמטרי אבטחה לא תואמים, IPsec SAs שפג תוקפם או לא חוקיים, נפילות או שגיאות של מנות, או אי התאמה של מדיניות.

Text, letter

Description automatically generated

הפקודה show crypto ipsec transform-set מציגה את הפרמטרים המוגדרים עבור כל סט טרנספורמציה. ערכת טרנספורמציה היא שילוב של פרוטוקולי אבטחה ואלגוריתמים המגדירים כיצד לאבטח את זרימת הנתונים במנהרת IPsec. הפלט של פקודה זו כולל את המידע הבא:

- שם ערכת ההמרה

- סוג האנקפסולציה שבה נעשה שימוש (ESP או AH)

- אלגוריתם ההצפנה בשימוש (כגון AES, DES, 3DES וכו')

- אלגוריתם האימות בשימוש (כגון SHA, MD5 וכו')

- אופן הפעולה (מנהרה או תחבורה)

Text, letter

Description automatically generated

# ACL

רשימות גישה (ACL) הן מאפיין אבטחה ברשתות מחשבים המשמשות לשליטה בזרימת תעבורת הרשת על סמך מערכת כללים. ACLs מיושמים בדרך כלל בנתבים, מתגים וחומות אש והם מאפשרים למנהלי רשת לסנן תעבורה נכנסת ויוצאת על סמך קריטריונים שונים, כגון כתובות IP מקור ויעד, סוגי פרוטוקולים, מספרי יציאות ותוכן מנות.

רשימות גישה משמשות לאכיפת מדיניות אבטחת רשת על ידי התרת או מניעת סוגים ספציפיים של תעבורה. לדוגמה, ניתן ליצור רשימת גישה כדי לאפשר תעבורה נכנסת מטווח כתובות IP ספציפי תוך מניעת תעבורה מכל כתובות ה-IP האחרות. באופן דומה, ניתן להשתמש ברשימת גישה כדי לחסום תעבורה ביציאות או פרוטוקולים מסוימים, כגון מניעת גישה לאתרים או שירותים מסוימים.

ניתן להגדיר רשימות גישה במגוון דרכים, בהתאם למכשיר ולדרישות הספציפיות של הרשת. ניתן להחיל אותם על תעבורה נכנסת או יוצאת, וניתן להגדיר אותם על בסיס ממשק או פרוטוקול. ישנם שני סוגים עיקריים של רשימות גישה: סטנדרטית ומורחבת. רשימות גישה סטנדרטיות משמשות לסינון תעבורה על סמך כתובות IP מקור בלבד, בעוד שרשימות גישה מורחבות יכולות לסנן תעבורה על סמך שילוב של כתובות IP מקור ויעד, פרוטוקולים ומספרי יציאה. רשימות גישה מורחבות הן בדרך כלל חזקות וגמישות יותר מרשימות גישה רגילות.

סקירה קצרה של טווחי ה-ACL הסטנדרטיים והמורחבים שמציעה Cisco:

1. ACLs סטנדרטיים - אלה ממוספרים מ-1 עד 99 וניתן להשתמש בהם כדי לסנן תעבורה על סמך כתובת ה-IP המקור בלבד. ניתן להחיל אותם נכנסים או יוצאים והם משמשים בדרך כלל כדי להגביל גישה לכתובות IP או רשתות משנה ספציפיות. לדוגמה, כדי למנוע גישה לכתובת IP ספציפית, תוכל ליצור ACL סטנדרטי עם הפקודה "access-list 1 deny <ip-address>".

2. ACLs מורחבים - אלה ממוספרים מ-100 עד 199 וניתן להשתמש בהם כדי לסנן תעבורה בהתבסס על כתובות ה-IP של המקור והיעד, הפרוטוקולים ומספרי היציאה. ניתן להחיל אותם נכנסים או יוצאים והם משמשים בדרך כלל כדי לשלוט בגישה לשירותים או יישומים ספציפיים. לדוגמה, כדי לאפשר גישה לאתר ספציפי, תוכל ליצור ACL מורחב עם הפקודה "access-list 101 permit tcp any host <website-ip-address> eq 80".

3. ACLs עם שם - בנוסף ל-ACLs הסטנדרטיים והמורחבים, Cisco מציעה גם ACLs עם שם שניתן להשתמש בהם כדי לספק שמות תיאוריים יותר ל-ACLs. ACLs עם שם מזוהים על ידי שם מוגדר על ידי משתמש במקום מספר וניתן להשתמש בהם כדי לסנן תעבורה באותו אופן כמו ACL ממוספרים.

חשוב לציין כי בעת קביעת תצורה של ACL במכשירי Cisco, חיוני לקחת בחשבון את סדר יישום הכללים כאשר הכללים מעובדים מלמעלה למטה. חשוב למקם את הכללים הספציפיים ביותר בחלק העליון של ה-ACL, ולאחר מכן לעבור לכללים הכלליים יותר לכיוון התחתון. גישה זו מבטיחה שה-ACL מעובד בצורה היעילה ביותר האפשרית וממזערת את ההשפעה על ביצועי הרשת.

טבלאות ACL המיושמות בפרויקט:

**סניף ראשון - HZL**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **support** | **PR** | **penTest** | **guest** | **QA** | **dev** | **ip** | **vlan** | **מקור/יעד** |
| 60 | 50 | 40 | 30 | 20 | 10 |  |  |  |
| - | - | + | - | + |  | 10.1.10.1/24 | 10 | dev |
| - | - | + | - |  | + | 10.1.20.1/24 | 20 | QA |
| - | - | - |  | - | - | 10.1.30.1/24 | 30 | guest |
| - | - |  | - | + | + | 10.1.40.1/24 | 40 | penTest |
| - |  | - | - | - | - | 10.1.50.1/24 | 50 | PR |
|  | - | - | - | - | - | 10.1.60.1/24 | 60 | support |

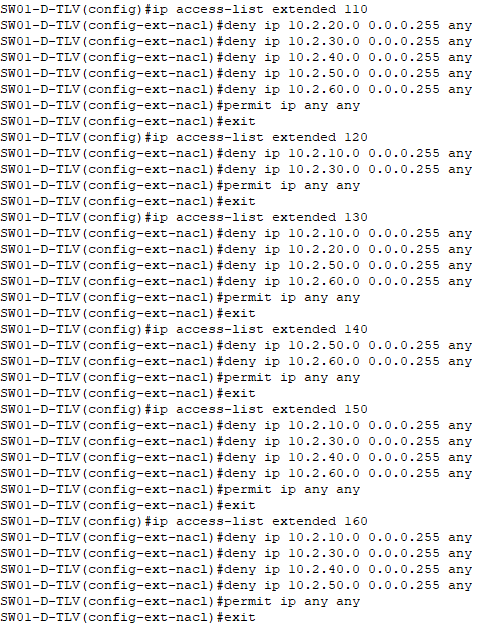
**סניף שני – TLV**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **acounting** | **HR** | **security** | **guest** | **executive** | **UI** | **ip** | **vlan** | **מקור/יעד** |
| 60 | 50 | 40 | 30 | 20 | 10 |  |  |  |
| - | - | - | - | - |  | 10.2.10.1/24 | 10 | UI |
| + | + | + | - |  | - | 10.2.20.1/24 | 20 | executive |
| - | - | + |  | - | - | 10.2.30.1/24 | 30 | guest |
| - | - |  | + | + | - | 10.2.40.1/24 | 40 | security |
| - |  | - | - | + | - | 10.2.50.1/24 | 50 | HR |
|  | - | - | - | + | - | 10.2.60.1/24 | 60 | acounting |

**סניף שלישי – HFA**

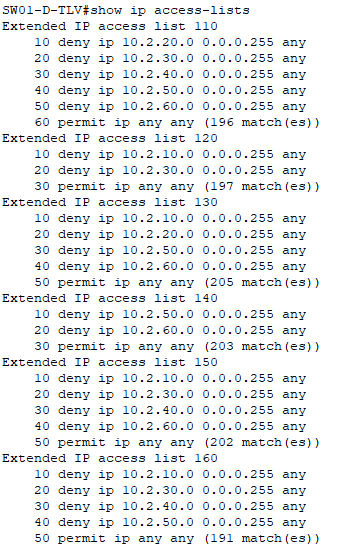
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **admin** | **cyberSec** | **logistics** | **guest** | **legal** | **marketing** | **ip** | **vlan** | **מקור/יעד** |
| 60 | 50 | 40 | 30 | 20 | 10 |  |  |  |
| + | + | - | - | - |  | 10.3.10.1/24 | 10 | marketing |
| + | + | - | - |  | - | 10.3.20.1/24 | 20 | legal |
| - | - | - |  | - | - | 10.3.30.1/24 | 30 | guest |
| + | + |  | - | - | - | 10.3.40.1/24 | 40 | logistics |
| + |  | + | - | + | + | 10.3.50.1/24 | 50 | cyberSec |
|  | + | + | - | + | + | 10.3.60.1/24 | 60 | admin |

**הגדרת ACL**

****

****

**Show ACL**

****

# SSH+AAA

SSH (Secure Shell) הוא פרוטוקול רשת קריפטוגרפי המאפשר כניסה מאובטחת מרחוק ותקשורת בין שני מחשבים ברשת לא מאובטחת. הוא נמצא בשימוש נרחב לגישה מרחוק לשרתים, ניהול תשתית רשת והעברת קבצים בצורה מאובטחת.

SSH נוצר כתחליף לפרוטוקולי Telnet ו-FTP המסורתיים ששידרו נתונים בטקסט רגיל, מה שהופך אותם לפגיעים ליירוט ופריצה. SSH משתמש בהצפנה כדי להגן על הנתונים המועברים, מה שהופך אותם לאבטחים גם ברשת לא מהימנה.

AAA ראשי תיבות של אימות, הרשאה וחשבונאות. זוהי מסגרת אבטחה המשמשת לשליטה בגישה למשאבי רשת, ניהול הרשאות משתמש ומעקב אחר שימוש למטרות חיוב וביקורת.

כך פועל כל רכיב של AAA:

אימות: רכיב זה מאמת את זהותו של משתמש המנסה לגשת למשאבי רשת. ניתן לעשות זאת בשיטות שונות, כגון שם משתמש וסיסמה, תעודות דיגיטליות או נתונים ביומטריים. התקני Cisco תומכים במגוון רחב של פרוטוקולי אימות, כולל TACACS+, RADIUS ו-Kerberos.

הרשאה: ברגע שמשתמש מאומת, רכיב ההרשאה קובע לאילו משאבי רשת המשתמש רשאי לגשת ולאילו פעולות הוא יכול לבצע. זה נעשה על ידי הקצאת תפקידים והרשאות למשתמש על סמך זהותו, חברותו בקבוצה או גורמים אחרים.

הנהלת חשבונות: רכיב זה עוקב אחר השימוש במשאבי הרשת על ידי משתמשים, כולל כמות הנתונים המועברים, משך ההפעלה והמשאבים הספציפיים אליהם ניגש. ניתן להשתמש בנתונים אלה למטרות חיוב וביקורת, כמו גם לאיתור הפרות אבטחה או הפרות מדיניות.

**Tacacs VS RADIUS**

TACACS+ (Terminal Access Controller Access-Control System Plus) ו-RADIUS (שירות חיוג אימות מרחוק) הם שני פרוטוקולים נפוצים של אימות, הרשאה וחשבונאות (AAA). בעוד ששני הפרוטוקולים משרתים מטרות דומות, ישנם כמה הבדלים מרכזיים ביניהם.

להלן כמה מההבדלים העיקריים בין TACACS+ ל-RADIUS:

פונקציונליות: TACACS+ מספק תהליכי אימות, הרשאות וחשבונאות נפרדים, מה שהופך אותו לגמיש יותר מ-RADIUS. עם TACACS+, מנהלי מערכת יכולים להתאים אישית כל תהליך כדי לענות על דרישות ספציפיות. RADIUS, לעומת זאת, משלב אימות והרשאה לתהליך אחד.

הצפנה: TACACS+ משתמש בהצפנה עבור כל החבילה, כולל המטען, בעוד RADIUS מצפין רק את הסיסמה. זה הופך את TACACS+ למאובטח יותר מ-RADIUS.

מדרגיות: RADIUS ניתן להרחבה יותר מ-TACACS+. עם RADIUS, שרת יחיד יכול להתמודד עם אימות, הרשאה וחשבון עבור התקני רשת מרובים. TACACS+, לעומת זאת, דורש שרת נפרד לכל תהליך.

תמיכה בפרוטוקולים שאינם IP: TACACS+ תומך בפרוטוקולים שאינם IP, כגון AppleTalk ו-Novell IPX, בעוד RADIUS תומך רק בפרוטוקולים מבוססי IP.

תמיכת ספקים: TACACS+ נתמך בעיקר על ידי Cisco, בעוד RADIUS נתמך על ידי מגוון רחב של ספקים.

באופן כללי, TACACS+ נחשב לאבטח וגמיש יותר מ-RADIUS, אך הוא גם דורש יותר משאבים ופחות ניתן להרחבה. RADIUS, לעומת זאת, קל יותר ליישום ונתמך באופן נרחב יותר, אך עשוי שלא להציע את אותה רמת התאמה אישית ואבטחה כמו TACACS+. הבחירה בין שני הפרוטוקולים תלויה בסופו של דבר בדרישות הספציפיות של הרשת ושל המכשירים שבהם נעשה שימוש.

**הגדרת AAA וSSH**

הגדרה במתג שכבה 3(תקף גם לנתבים)

Text

Description automatically generated

הגדרה במתג שכבה 2

Text

Description automatically generated

**פקודות SHOW**

****

**הפקודה show aaa sessions מציגה מידע על הפעלות האימות, ההרשאה והחשבון הפעילים (AAA) במכשיר Cisco. פלט הפקודה כולל את המידע הבא:**

**- מזהה ההפעלה, שהוא מזהה ייחודי עבור כל הפעלת AAA.**

**- שם המשתמש, שהוא שם המשתמש שיזם את ההפעלה.**

**- הממשק, שהוא שם הממשק שבו נוצרה הפגישה.**

**- הפרוטוקול, שהוא סוג הפרוטוקול המשמש לסשן, כגון SSH, Telnet, HTTP וכו'.**

**- שיטת האימות, שהיא סוג האימות המשמש להפעלה, כגון מקומי, TACACS+, RADIUS וכו'.**

**- שיטת ההרשאה, שהיא סוג ההרשאה המשמשת להפעלה, כגון מקומית, TACACS+, RADIUS וכו'.**

**- שיטת החשבונאות, שהיא סוג החשבונאות המשמשת להפעלה, כגון מקומית, TACACS+, RADIUS וכו'.**

**- שעת ההתחלה, שהם התאריך והשעה שבהם ההפעלה התחילה.**

**- זמן הסרק, שהוא משך הזמן מאז הפעילות האחרונה במפגש.**

**- משך הזמן, שהוא משך הזמן הכולל שבו הפגישה הייתה פעילה.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

# ASA

Cisco ASA (Adaptive Security Appliance) הוא התקן אבטחת רשת שנועד להגן על רשת מפני גישה לא מורשית ואיומי אבטחה אחרים. זהו פתרון חומת אש חזק וגמיש המספק תכונות אבטחה מתקדמות כגון קישוריות VPN (רשת וירטואלית פרטית), מניעת חדירה, סינון תוכן ובקרת יישומים.

מכשיר Cisco ASA מספק מגוון שירותי אבטחה הניתנים להתאמה אישית לצרכים הספציפיים של עסק או ארגון. שירותים אלו כוללים:

1. הגנת חומת אש - חומת האש של Cisco ASA מספקת קו הגנה ראשון מפני גישה לא מורשית לרשת. הוא מנטר ושולט על התעבורה הנכנסת והיוצאת מהרשת כדי למנוע איומי אבטחה.

2. קישוריות VPN - ה-Cisco ASA מאפשר למשתמשים מרוחקים להתחבר בצורה מאובטחת לרשת פרטית דרך האינטרנט. זה מאפשר לעובדים לגשת למשאבי החברה מכל מקום בעולם תוך שמירה על אבטחת הרשת.

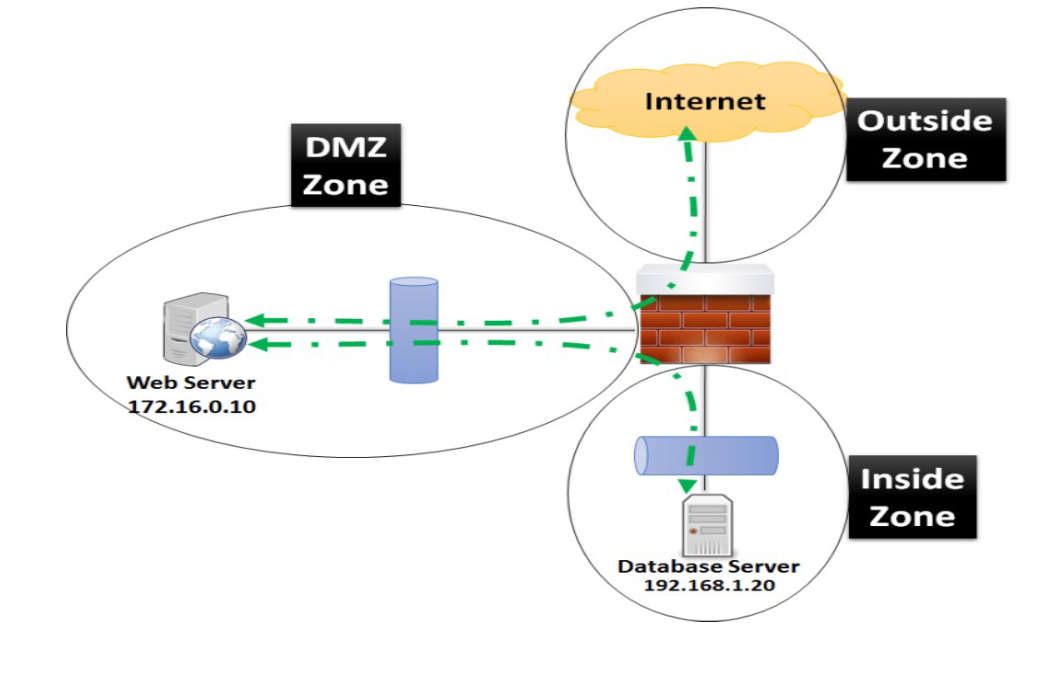
3. מניעת חדירה - ה-Cisco ASA יכול לזהות ולמנוע התקפות נגד הרשת על ידי ניטור דפוסי תעבורה וזיהוי פעילות זדונית.

4. סינון תוכן - ה-Cisco ASA יכולה לחסום גישה לאתרים ספציפיים או לתוכן על סמך מדיניות מוגדרת מראש. זה יכול להיות שימושי במניעת מעובדים גישה לאתרים לא הולמים או שאינם קשורים לעבודה.

5. בקרת יישומים - Cisco ASA יכולה לזהות ולשלוט ביישומים ושירותים ספציפיים המורשים לגשת לרשת. זה יכול לסייע במניעת התפשטות תוכנות זדוניות ואיומי אבטחה אחרים.

Cisco ASA זמין במספר דגמים, כל אחד עם רמות שונות של ביצועים ופונקציונליות. סדרת ASA 5500-X היא הדור האחרון של מכשירי ASA, המציעה תכונות אבטחה מתקדמות ויכולות בעלות ביצועים גבוהים.

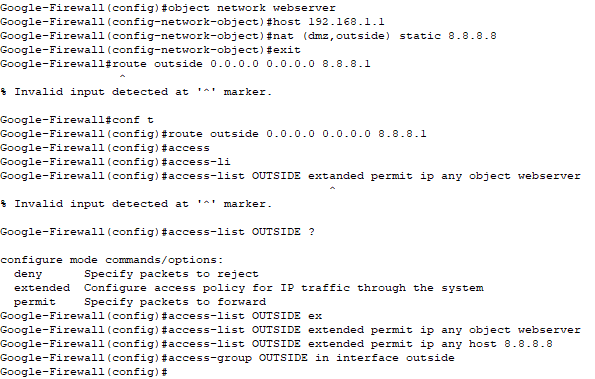
בסך הכל, Cisco ASA הוא פתרון אבטחה חזק ואמין שיכול לעזור לעסקים להגן על הרשתות שלהם מפני איומי אבטחה.



הגדרת ASA

A screenshot of a computer program

Description automatically generated with medium confidence



# ביבליוגרפיה

<https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html>

<https://en.wikipedia.org/wiki/VLAN>

<https://en.wikipedia.org/wiki/Trunking>

<https://networklessons.com/cisco/ccie-routing-switching/hsrp-hot-standby-routing-protocol>

<https://www.guru99.com/stp-spanning-tree-protocol-examples.html>

<https://www.networkacademy.io/ccna/ethernet/router-on-a-stick>

<https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>

<https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html>

# איתור תקלות ופתרונן

במהלך קונפיגורציה פרוטוקול STP בסניף הרצליה נתקלתי בבעיה חיבוריות בכמה vlans ספציפיים, שלא יכלו לתקשר אחד עם השני או עם מכשירים בתוך אותה הרשת. הבעיה נבעה מהגדרה ידנית של priority על המתגים שאמורים להיות מוגדרים כהroot bridgh והגיבוי שלו. כאשר אחד המתגים האחרים נתן לעצמו priority נמוך יותר בצורה אוטומתית זה שיבש למעשה את כל התעבורה. הפתרון לבעיה הזו הוא להגדיר את הroot bridgh והגיבוי שלו באמצעות הפקודות root primary ו root secondary.

בעיה נוספת שהתמודדתי איתי הייתה שטופולוגיית ה-STP לא הייתה יציבה וחלק מהפורטים התנופפו בין מצבי חסימה והעברה. זה גרם ללולאות וסערות שידור ברשת. הבנתי שזה נובע מפרמטרי STP לא עקביים, כמו עדיפות, מזהה גשר ועלות יציאה. כדי לפתור זאת, הייתי צריך להגדיר את אותם פרמטרי STP בכל המתגים באמצעות פקודות ה-spanne-tree.

רפלקציה

פרויקט הגמר שלי ברשתות מחשבים היה לתכנן ולהטמיע טופולוגיית רשת באמצעות packet tracer, כלי סימולציה המאפשר לי ליצור ולבדוק תרחישי רשת שונים. הפרויקט כלל הקמת נתבים, מתגים, חומות אש, שרתים והתקני קצה, והגדרתם עם הפרוטוקולים ואמצעי האבטחה המתאימים. הייתי צריך גם לתעד את עיצוב הרשת ולהסביר את הרציונל מאחורי הבחירות שלי.

הפרויקט היה מאתגר אך מתגמל, שכן הוא עזר לי ליישם את המושגים התיאורטיים שלמדתי בקורס לבעיה מעשית. למדתי כיצד להשתמש ב-Packet Tracer ביעילות, כיצד לפתור בעיות רשת וכיצד לייעל את ביצועי הרשת והאבטחה. השגתי גם הבנה מעמיקה יותר של שכבות הרשת, הפרוטוקולים וההתקנים השונים, וכיצד הם מתקשרים זה עם זה. כמה מהמיומנויות שפיתחתי במהלך הפרויקט הן:

- עיצוב רשת: למדתי כיצד לתכנן ולעצב טופולוגיית רשת העונה על הדרישות והאילוצים של התרחיש. הייתי צריך לשקול גורמים כמו מדרגיות, אמינות, יתירות, עלות ואבטחה. הייתי צריך גם לבחור את ההתקנים המתאימים, הכבלים, הממשקים ותכניות הכתובות עבור כל מקטע רשת.

- תצורת רשת: למדתי כיצד להגדיר התקני רשת שונים באמצעות ממשק שורת הפקודה (CLI). הייתי צריך להגדיר פרוטוקולי ניתוב כגון BGP, OSPF ו-EIGRP, החלפת פרוטוקולים כגון VLAN ו-STP, חוקי חומת אש ורשימות בקרת גישה (ACL), שירותי שרת כגון DHCP ו-DNS, והגדרות קצה של מכשיר כגון כתובות IP ושער ברירת מחדל.

- בדיקת רשת: למדתי כיצד לבדוק ולאמת את הפונקציונליות והקישוריות של הרשת באמצעות מצב סימולציה של מעקב מנות וכלים שונים כגון ping, traceroute, telnet ופקודות show. למדתי גם כיצד להשתמש בתכונות הניתוח של מעקב מנות כמו packet sniffer ורשימת אירועים כדי לבחון את הפרטים של תעבורת הרשת ולזהות שגיאות או חריגות כלשהן.

- תיעוד רשת: למדתי כיצד לתעד את עיצוב ותצורת הרשת באמצעות כלי ההערות ומחולל הדוחות של ה-Packet Tracer. למדתי גם איך לכתוב דוח ברור ותמציתי המסביר את טופולוגיית הרשת, המכשירים, הפרוטוקולים, אמצעי האבטחה, תוצאות הבדיקות והאתגרים שבהם נתקלתי.

הפרויקט היה חווית למידה חשובה עבורי, שכן הוא נתן לי הזדמנות ליישם את הידע והכישורים שלי ברשתות מחשבים לתרחיש מציאותי. זה גם עזר לי לפתח את כישורי החשיבה הביקורתית, פתרון הבעיות והתקשורת שלי. נהניתי לעבוד על הפרויקט ואני גאה בתוצאה.