# תיאור טופולוגיה

הטופולוגיה שלי מציגה הדמיה של רשת ארגונית המדמה את google.com.

**תיאור כללי:** הרשת מחולקת לשלוש רשתות שונות, כאשר כל אחת מהן מחולקת לשלושה VLANs. הרשת הארגונית מחוברת לספק האינטרנט (ISP), מה שמאפשר לה גישה אל האינטרנט.

**קונפיגורציות, פרוטוקולים והגדרות ברשת:**

**VLAN Configurations:**

1. **Subnetting:** הקצתי כתובות IP לכל VLAN בהתאם למספר המחשבים ברשת. שלוש כתובות נשמרו למטרות קבועות: Net ID, Default Gateway ו-Broadcast.
2. לכל Host ברשתות ה-VLAN הוקצתה כתובת IP, Subnet Mask ו-Default Gateway מתאימים.
3. **Access Ports:** כל פורט ששויך ל-VLAN הוגדר במצב Access לצורך יצירת רשת מקומית המחולקת לרשתות קטנות.

**VTP (VLAN Trunking Protocol):** פרוטוקול זה מאפשר ניהול מרכזי של VLANs. מתג אחד מוגדר כ"שרת" והשאר כ"לקוחות". השרת מפרסם את הגדרות ה-VLAN לכל המתגים באותו VTP Domain. שינויים ב-VLAN ניתן לבצע רק בשרת. המתגים המוגדרים כ"לקוחות" מקבלים את ההגדרות מהשרת ואינם יכולים לבצע שינויים בעצמם.

**Trunking:** הגדרתי חיבורי Trunk בין המתגים והנתבים, מה שמאפשר העברת מספר VLANs דרך אותו interface. חיבורי Trunk מאפשרים לתעבורה ממספר VLANs שונים לעבור דרך אותו הקישור (link), תוך שמירה על בידוד התעבורה באמצעות תגיות (Tags).

**STP (Spanning Tree Protocol):** פרוטוקול זה מונע לולאות ברשת (Broadcast Storm) באמצעות ניהול חכם של חיבורים בין המתגים. במקום לחסום פורטים מיותרים לחלוטין, STP מייעל את זרימת התעבורה ברשת על ידי חלוקת עומסים בין הקישורים (links) ומניעת לולאות באמצעות הגדרת פורטים במצב המתנה (Standby). הבחירה איזה פורט יוגדר במצב המתנה מתבצעת לפי שני קריטריונים: עדיפות (Priority) וכתובת MAC. ברירת המחדל לעדיפות היא זהה לכל המתגים, ואם אין שינוי בעדיפות, כתובת ה-MAC הנמוכה ביותר תקבע איזה מתג יהפוך ל-Root Bridge. הפורטים במתג ה-Root Bridge תמיד יהיו פעילים וכל התעבורה תעבור דרכו. הפורטים המוגדרים כ-Standby ייכנסו לפעולה רק בעת הצורך, כאשר יש שינוי בדרישות התעבורה או בעומס ברשת, ובכך נשמרת זמינות גבוהה ויעילות בתעבורה.

**Router On A Stick:** כדי לאפשר תקשורת בין רשתות ה-VLAN, הגדרתי נתב עם תת-ממשקים (Sub-Interfaces). פיצלתי את הממשק הפיזי הראשי של הנתב (Interface) למספר תתי-ממשקים (Sub-Interfaces), כך שכל תת-ממשק מקבל כתובת IP המשמשת כ-Default Gateway ל-VLAN המתאים. תהליך זה מאפשר יצירת Inter-VLAN Routing, שבו הנתב מנתב תעבורה בין VLANs שונים דרך ממשק פיזי אחד המפוצל לתת-ממשקים.

**Routing Configurations:**

**הקמת רשת WAN:** כדי לאפשר תקשורת בין רשתות ה-VLAN השונות, חיברתי את הנתבים והגדרתי קונפיגורציות מתאימות.

1. **כתובות IP:** השתמשתי בסאבנט /30, המספק 4 כתובות IP לכל חיבור בין נתבים: כתובת אחת ל-Net ID, אחת ל-Broadcast, ושתיים לפורטים של הנתבים. פורטים אלו משמשים ליצירת חיבורים בין הנתבים ברשת ה-WAN.
2. OSPF: **OSPF (Open Shortest Path First):** הוא פרוטוקול ניתוב דינמי המתבסס על מדד ה-Cost (עלות), הנגזר מרוחב הפס של הקישורים. OSPF משתמש בשלוש טבלאות עיקריות:

טבלת שכנים (Neighbor Table), טבלת טופולוגיה (Topology Table) וטבלת ניתוב (Routing Table). טבלת השכנים כוללת את הנתבים המחוברים ישירות, טבלת הטופולוגיה מציגה את כל הנתיבים האפשריים, וטבלת הניתוב מציגה את הנתיב היעיל ביותר. כל הנתבים נמצאים ב-Area 0 (Backbone Area), שהיא עמוד השדרה של הרשת.

3. **DR & BDR:**

- **DR (Designated Router):** אחראי להפצת עדכונים לכל שאר הנתבים ברשת, מה שמפחית את העומס על הרשת.
- **BDR (Backup Designated Router):** משמש כגיבוי ל-DR במקרה של כשל. אם ה-DR נופל, ה-BDR תופס את מקומו באופן אוטומטי.
- בחירת DR מתבצעת לפי עדיפות (Priority). אם קיימת זהות בערכים, נעשה שימוש ב-Router ID כקריטריון נוסף. ה-Router ID יכול להיקבע באחת משלוש דרכים:
  1. הגדרה ידנית של ה-Router ID.
  2. שימוש בכתובת ה-Loopback הגבוהה ביותר בנתב.
  3. במידה ואין כתובת Loopback, נעשה שימוש בכתובת ה-IP הגבוהה ביותר של הממשק.

**ABR & ASBR:**

- **ABR (Area Border Router):** אחראי על חיבור בין אזורים (Areas) שונים ברשת. נתב כזה לא מופיע בטופולוגיה מאחר ויש רק Area 0.
- **ASBR (Autonomous System Boundary Router):** אחראי על חיבור הרשת לספק האינטרנט.

**Default Route:** הגדרתי ברירת מחדל ליציאה לאינטרנט דרך הנתב המחובר ל-(ASBR) ISP. הנתב מפנה את כל התעבורה שאינה מיועדת לרשתות פנימיות לספק האינטרנט באמצעות ניתוב סטטי.

**פרוטוקולים נוספים:**

**DHCP:** פרוטוקול זה מאפשר חלוקת כתובות IP דינמית ליחידות הקצה. כל נתב משמש כשרת DHCP ומחלק כתובות לרשתות ה-VLAN המחוברות אליו. יצרתי Pools שמגדירים את טווחי הכתובות, והגדרתי כתובת Default Gateway כך שיחידות הקצה ידעו לאן לפנות לקבלת כתובת IP.

**SSH (Secure Shell):** פרוטוקול זה מאפשר גישה מרחוק לרכיבי הרשת בצורה מאובטחת ומוצפנת. יצרתי שמות משתמשים עם סיסמאות מוצפנות (secret) והגדרתי מפתחות RSA בגודל 1000 ביט להצפנה. פרוטוקול SSH עובד עם רמות הרשאה שונות (0-15), מה שמאפשר מידור גישה בהתאם לצרכים.

**Dynamic NAT:** פרוטוקול זה ממיר כתובות IP פרטיות לכתובות ציבוריות ביציאה לאינטרנט. הוא מסייע בהסוואת כתובות פנימיות לצורך אבטחה וחוסך כתובות IPv4. הראוטר מקצה כתובות ציבוריות מתוך טווח מוגדר, ומאפשר ליחידות קצה רבות להשתמש באותה כתובת ציבורית בעת חיבור לרשת החיצונית.

**סיכום:** הטופולוגיה מדמה רשת ארגונית עם חלוקה ל-VLANs, ניתוב דינמי באמצעות OSPF, ניהול רשתות עם VTP, ומנגנוני אבטחה כמו SSH ו-NAT.