**סדר פעולות פרויקט**

שימו לב!

בפרויקט יש 3 סניפים. סניפים אלו יהיו בנויים לפי הדרישות הבאות:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| סניף | שכבת ה-Access | שכבת ה-Distribution | שכבת ה-Core | שיטת IP |
| א | מתגים שכבה 2 | מתגים שכבה 2 | נתבים | IPv4 |
| נ | מתגים שכבה 2 | מתגים שכבה 3 | נתבים | IPv4 |
| ג | מתגים שכבה 3 | מתגים שכבה 3 | נתבים | IPv4 |

יש לקפיד לבנות סכמת IP (תוכנית לפריסת כתובות IP ) הלוקחת בחשבון את המבנה הייחודי של כל סניף.

**בכל הסניפים יש לוודא כי הנתבים תומכים ב-VPN !**

**סדר פעולות עבודה (המלצה)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| פעולה | קישור לסרטון או להסבר | ספר פרויקט | PT לוגי | PT  פיזי |
| **תחילת עבודה בספר הפרויקט** |  |  |  |  |
| **מבוא :**   1. הסבר אודות החברה שעבורה אתם בונים את הרשת הארגונית. 2. דרישות החברה מהרשת (איזה שירותים הם דורשים מהרשת, מה נדרש מבחינת יכולות רשת ודרישות אבטחה) את הדרישות הללו אתם מיישמים אחרי זה בפרויקט עצמו |  | \* |  |  |
| בניית תרשים ארגוני | [סרטון](https://www.youtube.com/watch?v=HmL1TSCTofY) 1  [סרטון](https://www.youtube.com/watch?v=B3LHSBxcEY0) 2 | \* |  |  |
| **מחלקות בסניפים:**   1. סיכום קצר על תפקיד כל מחלקה 2. איזה ציוד רשת/מחשבים נדרש על מנת לתת מענה לדרישות מחלקה זו |  | \* |  |  |
| **בנית טבלת סניפים/מחלקות/VLAN-ים/כתובות IP**   1. הסבירו כיצד אתם מתכננים את כתובות ה-IP שתחלקו לכל סניף 2. איזה כתובות IP תחלקו לרשת ה-WAN שמחברת בין הסניפים 3. איזה כתובות IP תחלקו בתוך כל סניף 4. איזה כתובות IP תחלקו לכל מחלקה בסניפים | [דוגמא 1](https://1drv.ms/b/s!ArsUE93dRwWk73WKPUmt8OcTCFFI)  [דוגמא 2](https://1drv.ms/b/s!ArsUE93dRwWk73QJx23f6BfgqCSq) | יש לפתוח פרק חדש ולבנות טבלה המתארת את המחלקות השונות/סניפים שונים בהתאם לדוגמאות |  |  |
| **הגדרת מדיניות שמות של הציוד**   1. על מנת לייעל את העבודה מול הציוד/התקנים הפיזיים (מחשבים/שרתים/מתגים/חומות אש/נתבים/מדפסות/נקודות גישה אלחוטיות, יש לתת לכל התקן שם שממנו ניתן להבין מה תפקידו והיכן הוא נמצא 2. הסבר איך בחרת לתת את השמות האלו, מה ההיגיון שעומד מאחורי בחירה זו. |  | לרשום הסבר קצר וברור בחוברת מה המבנה וכיצד לפרש את השמות של הציוד [דוגמא](https://1drv.ms/w/s!ArsUE93dRwWk723YCdF3RPqqtp9J)  [עוד דוגמא](https://1drv.ms/b/s!ArsUE93dRwWk73BZ3AdW8uSVUEBw)  [עוד דוגמא](https://1drv.ms/b/s!ArsUE93dRwWk72-u-fJmnA6rBh-T) |  |  |
|  |  |  |  |  |
| **עבודה על העולם הפיזי ב-PT**  הוספת תמונה המתארת את ה"עולם" שבו נמצאים הסניפים בתוך ה-Intercity | [פרויקט רשתות תקשורת - יצירת מרחב פיזי - חלק א'](https://www.youtube.com/watch?time_continue=1&v=P0Vq3Z96030)[פרויקט רשתות תקשורת - יצירת מרחב פיזי - חלק ב'](https://www.youtube.com/watch?v=U1ZmfkXiqRY) |  |  | \* |
| פריסת ציוד רשת ומחשבים בסניף הראשון **על פי החלוקה למחלקות להקפיד לשים את המחשבים שמופיעים בעולם הלוגי באותן מחלקות בעולם הפיזי.** |  |  | \* |  |
| שינוי השמות של כל ההתקנים ב-PT בהתאם למדיניות השמות שנקבעה **יש לבצע בעולם הלוגי על פי המחלקות שבניתם** |  | בהמשך למשימה הקודמת יש להראות בצילום מסך את השינוי של שם של מתג או נתב לשם החדש. | \* |  |
| הוספת תמונה המתארת את ה"עולם" שבו נמצאים הסניפים בתוך ה-Intercity |  |  |  | \* |
| **הוספת שתי ערים בתוך ה- Intercity**   1. PT מגיע עם עיר אחת בתוכה ישנו בניין אחד ובתוכו קומה אחת. יש להוסיף בתוך המסך של ה-intercity עיר ובתוכה להוסיף בניין ובתוכו להוסיף קומה. 2. תהליך זה יש לבצע פעמיים כך שבסופו של דבר יהיו 3 ערים שבתוכם 3 סניפים. 3. יש לשנות את התמונה של ה-office לתמונה של תוכנית הבניין שבחרתם. |  |  |  | \* |
| **פריסת המחשבים של הסניף השני והשלישי**  **שימו לב כאשר מפזרים את המחשבים בסניפים יש להקפיד קודם לכן לעבור לסניף המתאים בעולם הלוגי**   1. יש לפזר את הציוד הפיזי בתוך בניין המשרדים הפיזי **על פי החלוקה למחלקות להקפיד לשים את המחשבים שמופיעים בעולם הלוגי באותן מחלקות בעולם הפיזי.** 2. פריסת המחשבים של הסניף השלישי בתוך בניין המשרדים הפיזי |  |  |  | \* |
| **עבודה על VLAN-ים** | [סרטון מסכם על ניהול VLAN-ים על ידי פרוטוקול VTP](https://www.youtube.com/watch?v=FX3J4Rf1NQg) | |  |  |
| 1. הגדרת מתג אחד כ-vtp server והיתר כ-vtp client.   **שימו לב ! בטופולוגיה שכולה מתגים שכבה 3, ה-VLAN-ים מוגדרים מקומית רק על מתגי ה-ACCESS ולא דרך VTP!** | [הסבר ופקודות](https://drive.google.com/open?id=1JAibdBiohYSWh4DJD5gFUhg_1Tn76DjV) | יש לכתוב פרק המתאר את מה זה VTP למה משתמשים ב-VTP איך מגדירים VTP ואיך מראים (SHOW) ש-VTP הוגדר | להגדיר את המתגים |  |
| 1. הגדרת ה-VLAN-ים על מתג ה-SERVER. יש להגדיר ראשית את מספר ה-VLAN ואז את השם של ה-VLAN |  | יש לרשום בחוברת פרק המתאר מהו VLAN, איך מגדירים, למה משתמשים ב-VLAN-ים ואיך מראים שהם הוגדרו כנדרש | להגדיר את ה-vlan-ים על גבי המתג שהוא שרת VTP לאחר מכן לבדוק שה-VLAN-ים שוכפלו למתגים האחרים |  |
| 1. הגדרת החיבורים בין המתגים לבין מתגים אחרים כ-Trunk. בדיקה האם הם הוגדרו על ידי   Show interface trunk | [איך מגדירים Trunk על ממשק Fa0/24](https://www.youtube.com/watch?v=zhkUoiSuh2k)  [הסבר מה זה Trunk](https://tikshuv.site/trunk/) | יש לרשום בחוברת פרק המתאר מהו Trunk , איך מגדירים, למה משתמשים ב-Trunk-ים ואיך מראים שהם הוגדרו כנדרש | \* |  |
| 1. בדיקה האם ה-VLANים הופצו כנדרש לכל המתגים בסניף. **שימו לב ! בטופולוגיה שכולה מתגים שכבה 3, ה-VLAN-ים מוגדרים מקומית רק על מתגי ה-ACCESS ולא דרך VTP!** |  |  | \* |  |
| 1. שיוך ה-PORT-ים ל-VLAN-ים המתאימים |  |  | \* |  |
| **הגדרת EtherChannel**   1. יש לקבוע היכן נדרש ליישם EtherChannel. 2. יש להגדיר לפחות EtherChannel אחד בסניף ולדעת להסביר מדוע בחרתם ליישם אותו במיקום זה. 3. לקבוע ולהגדיר כנדרש את פרוטוקול ה- EtherChannel. |  |  |  |  |
| **הסבר על מתגים שכבה 3 - המשימה הזו נעשית בחוברת!** |  | **יש לחפש באינטרנט הסבר על ההבדל בין מתגים שכבה 2 ושכבה 3 ולרשום את ההבדלים כולל היתרונות והחסרונות של מתגים שכבה 3.** |  |  |
| **הגדרת מתגים שכבה 3**  **סניף אחד יעבוד עם EIGRP, סניף אחד עם OSPF וסניף שלישי עם OSPFv3 ועם IPv6!**   1. יש להגדיר את המתגים כולם שיעשו ניתוב על ידי הפקודה ip routing 2. יש להגדיר כתובות IP **בהתאם לכללים** על גבי הממשקים המחברים את המתגים זה לזה. |  | **יש לצרף הסבר על פרוטוקול הניתוב. כולל הסבר מהו הפרוטוקול איך מגדרים, צילומי מסך של ההגדרה ושל הוכחה שהגדרתם כנדרש.** | \* |  |
| 1. יש להגדיר פרוטוקול ניתוב (לבחירתכם פרט ל-RIP) בין המתגים/נתבים 2. יש לדאוג לאבטח את פרוטוקולי הניתוב ככל האפשר וככל ש-PT מאפשר. |  | \* |  |
| **הגדרות STP**   1. יש להגדיר מי הוא ה-Root Bridge |  |  | \* |  |
| **הגדרת HSRP**   1. יש להגדיר HSRP על הנתבים המתאימים 2. שים לב אין צורך להגדיק HSRP על הסניף בו כל המתגים הם מתגים שכבה 3. |  |  |  |  |
| **הגדרת DHCP**   1. יש להגדיר שרת DHCP על שרת או על נתב לבחירתכם |  |  | \* |  |
| 1. לבדוק האם המחשבים מקבלים IP מה-DHCP |  |  | \* |  |
| **הגדרת שרת דואר**   1. יש להגדיר שרת דואר בכל סניף 2. הגדרת 2 תחנות לפחות כלקוחות דואר. |  |  | \* |  |
| **הגדרת שרת FTP**   1. יש להגדיר שרת FTP בכל סניף 2. הגדרת 2 תחנות לפחות כלקוחות FTP. |  |  | \* |  |
|  |  |  |  |  |
| הגדרה בסניף אחד (לפחות) של ספק אינטרנט אליו הגישה מתאפשרת באמצעות מודם ADSL |  |  | \* |  |
| **תשתית BGP**   1. יש לבנות תשתית BGP המחברת את הסניפים 2. התשתית תהיה בנויה מ-6 נתבים לכל הפחות. 3. בין הנתבים יוגדר פרוטוקול BGP 4. בכל סניף הנתבים המקומיים יחוברו ראשית לנתב או שניים הנמצאים בתוך ספק התשתית 5. ספק התשתית הוא המתווך לרשת ה-BGP והוא מחובר בצידו האחד לסניף המקומי ובצידו האחר לתשתית ה-BGP. 6. יש להגדיר את הניתובים על פי ההגדרות שתקבלו בזמן השיעור. |  |  |  |  |

**חלק זה עוסק בעיקר באבטחת מידע בפרויקט**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| פעולה | קישור לסרטון או להסבר | ספר פרויקט | PT לוגי | PT פיזי |
| **הגדרות אבטחה ראשוניות**   1. הגדרת Banner בכל המתגים והנתבים 2. הגדרת סיסמאות מגובבות בכל הנתבים והמתגים 3. הגדרת סיסמאות גישה ל-Enable 4. הגדרת סיסמאות גישה לניהול **לכל** ההתקנים. |  |  |  |  |
| הגדרת SERVICE PASSWORD ENCRYPTION בכל ההתקנים |  |  |  |  |
| **הגדרות AAA**   1. הגישה להתקנים למטרת ניהול תהיה אך ורק דרך SSH ובאימות על ידי AAA בכל התקן התומך בכך 2. הגדרת שרתי AAA בכל אחד מהסניפים. יש להגדיר שרת מסוג Tacacs+ לפחות בסניף אחד ושרת Radius אחד לפחות בסניף אחר. 3. יש לבנות רשימות אימות בהתאם על ההתקנים השונים. 4. יש להקפיד ולהגדיר משתמש מקומי אחד לפחות על ההתקן. |  |  |  |  |
| **הגדרת PORT SECURITY**   1. יש להגדיר מהי מדיניות האבטחה מבחינת Port Security. 2. לקבוע מה ה-Violation Mode הנדרש מבחינת מדיניות האבטחה שלכם. 3. יש ליישם את המדיניות ולהגדיר PS על גבי כל ההתקנים במיוחד אלו של שכבת ה-Access. |  |  |  |  |
| **הגדרות ACL**   1. יש לבנות מדיניות אבטחה שתגדיר מי מהמחלקות יכולה לקבל גישה להתקנים של מחלקה אחרת ומי לא. 2. יש ליישם ACL-ים בנתבים המממשים מדיניות זו. 3. יש להגדיר לשימוש מאוחר יותר רשימת גישה לטובת סינון מי שיהיה זכאי להשתמש בשירותי NAT ומי שיהיה זכאי להשתמש בשירותי VPN |  |  |  |  |
| **הגדרת NAT**   1. יש להגדיר NAT OVERLOAD בנתבים היוצאים מהסניפים עם רשימת גישה (ACL) מתאים למדיניות האבטחה של הארגון. 2. יש להגדיר NAT סטטי עבור שרתים הנמצאים בתוך הסניף. |  |  |  |  |
| **הגדרת STP**   1. יש לאבטח את המתגים בפני התקפות STP 2. ליישם Portfast ו-BPDU Guard 3. ליישם Root Guard היכן שנדרש |  |  |  |  |
| **הגדרת שרת SYSLOG+NTP**   1. יש להגדיר שרת SYSLOG 2. על מנת ששירות זה יעבוד כראוי יש להגדיר שרת NTP |  |  |  |  |
| **הגדרת ASA**   1. בסניף המחזיק שרת הנותן שירות לגורמים מחוץ לסניף או לארגון יש להקים מבנה של inside outside ו-dmz על ידי התקן ASA |  |  |  |  |
| יש להגדיר על כל הנתבים הנמצאים בכניסה/יציאה מהסניפים רשימות גישה בהתאם למדיניות האבטחה של הארגון |  |  |  |  |
| יש לאבטח באמצעות סיסמה את כל פרוטוקולי הניתוב |  |  |  |  |
| **הגדרת VPN**  הקמת VPN בין נתב הנמצא בסניף עם נתב הנמצא מחוץ לסניף. |  |  |  |  |
| **הגדרות אבטחה בשכבה 2**   1. ביטול IP domain-lookup 2. הגדרת Login Banner 3. אבטחת גישה ברמת ה-Console ו-SSH 4. אבטחת המעבר למצב Privileged EXEC mode 5. סגירת חיבורי TCP שאינם פעילים 6. מניעת חיבור מבוסס HTTP/HTTPS 7. ביטול CDP 8. מניעת שימוש ב-Vlan1 9. ביטול DTP על כל הפורטים שאינם TRUNK 10. סגירת כל הפורטים שאינם בשימוש 11. הגדרת כל הפורטים שאינם בשימוש ל-VLAN שלא מחובר לכלום 12. הגדרת Port Snooping 13. הגדרת IP Source Guard 14. הגדרת ARP Security 15. הגדרת Dynamic ARP Inspection 16. הגדרת BPDU Guard 17. שנוי ה-NATIVE VLAN |  |  |  |  |