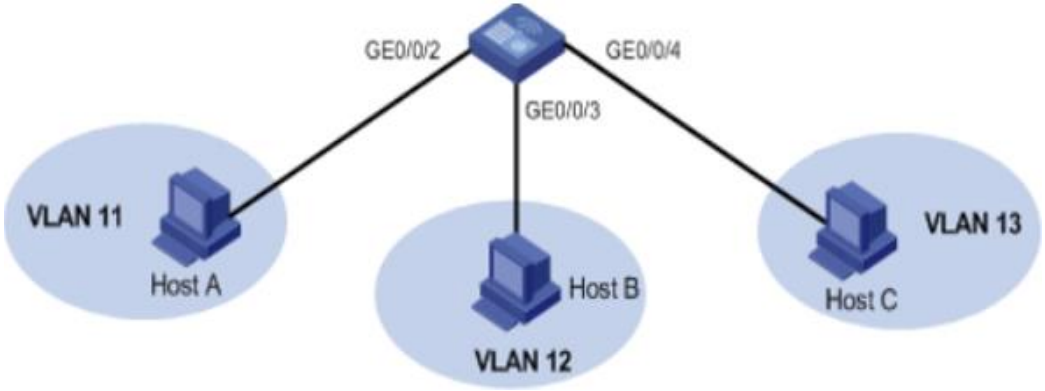
VLAN

Virtual Local Area Network

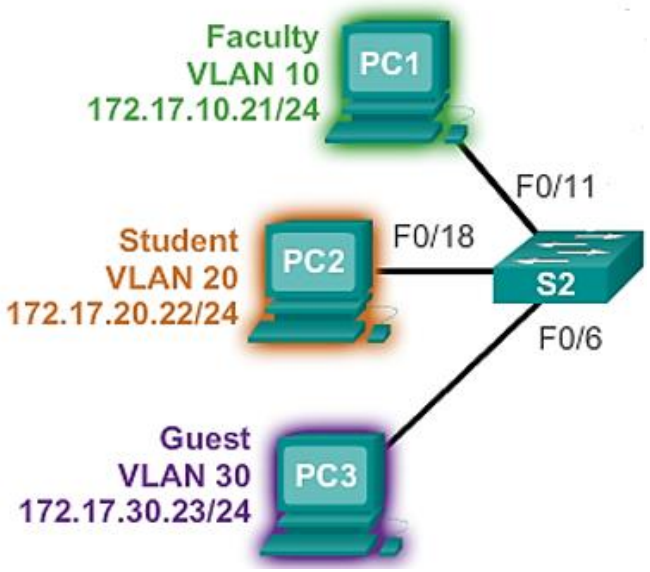
Virtual LAN

- אנו יודעים ומכירים ש-LAN היא רשת שכוללת את כל ההתקנים שמחוברים למתג ובעקבות כך נמצאים באותו Broadcast Domain. לכן החלוקה של הרשת היא בצורה פיזית, כלומר בשביל ליצור LAN אחד עלינו להשתמש במתג אחד, כיום קיימת חלופה.
- ברשתות ארגוניות רבות נעשה כיום השימוש בקונספט ה-VLAN, קונספט זה מאפשר למשתמש ליצור מספר רשתות LAN בצורה וירטואלית על מתג יחיד, כלומר ניתן לאגד מספר פורטים במתג ולשייך אותם לרשת וירטואלית אחת (VLAN) וכך ליצור חציצה לוגית בין מספר רשתות וירטואליות באותו המתג וכל רשת היא Broadcast Domain בפני עצמה. והמידע אינו יכול לעבור בין רשת וירטואלית אחת לרשת וירטואלית אחרת.



Virtual LAN

- מה זה בעצם אומר רשתות וירטואליות ו-Broadcast Domain שונים באותו המתג.
- במידה ורכיב קצה שולח הודעת Broadcast ברשת הווירטואלית בה הוא נמצא, ההודעה תגיע לכל הרכיבים באותה הרשת הווירטואליות, כלומר רק דרך הפורטים שהגדירו ושייכו לאותו ה-VLAN.
- כל רשת וירטואלית VLAN שנגדיר היא רשת נפרדת בפני עצמה בדיוק כמו רשת LAN רגילה רק שהיא קיימת בצורה לוגית, מה שאומר שההפרדה של הרשתות זו מזו היא ברמת המתג.



Virtual LAN

- היתרונות:

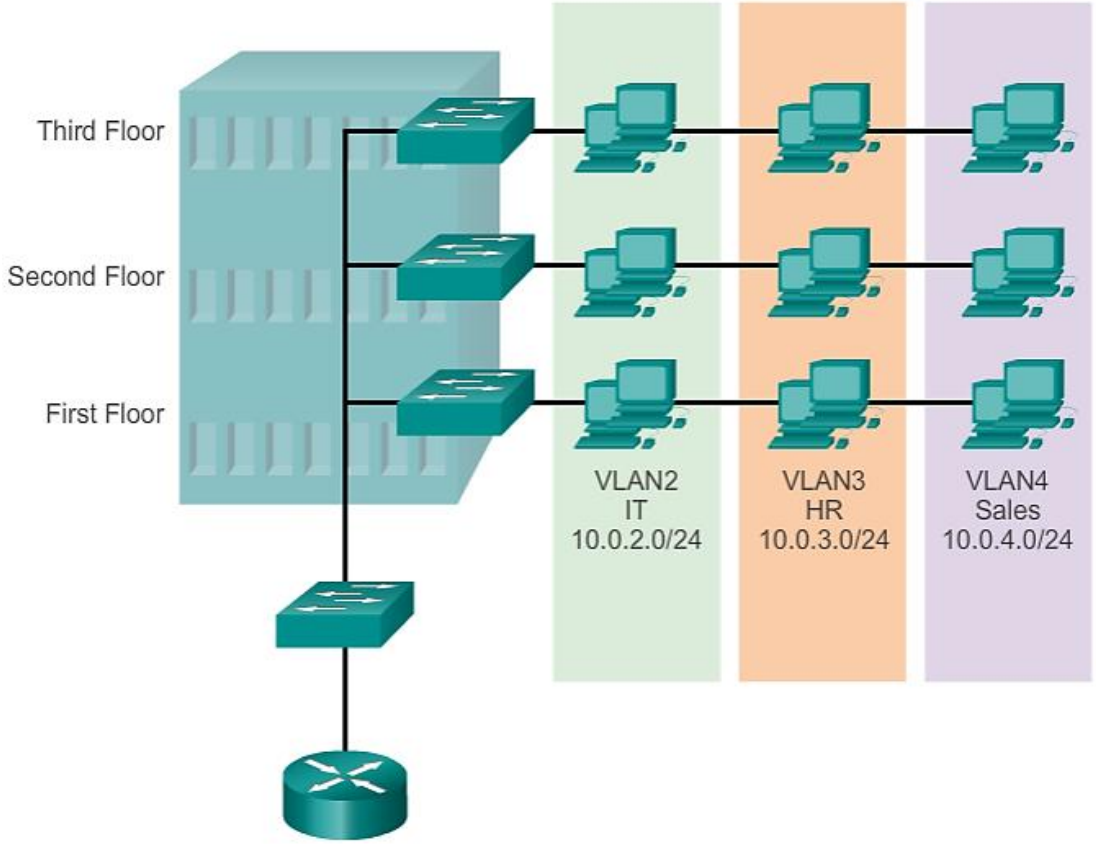
1. אבטחה-יצירת VLAN's מאפשרת לנו להפריד בקלות מחשבים שמחזיקים במידע רגיש לרשת נפרדת.
2. הפחתת עלויות-בעקבות החלוקה הלוגית אין צורך בציוד רשת נוסף, כלומר אין צורך במתגים ונתבים נוספים בכדי ליצור Broadcast Domain.
3. יעילות-קל יותר לאתר תקלות, משום שכשלים ממוקדים בדרך כלל ברשת אחת.
4. גמישות-ניתן להוסיף ולהסיר רכיבי רשת בקלות ללא קשר למיקום הפיזי.

- חסרונות:

1. במידה ונרצה לאפשר תקשורת בין ה-VLAN's השונים עלינו להיעזר בנתב (Router).

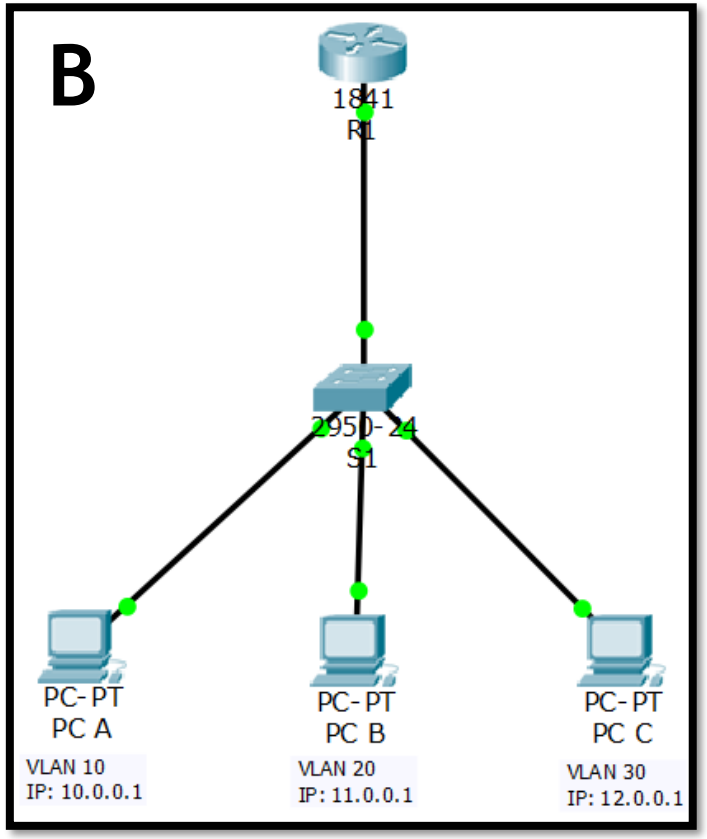
Example

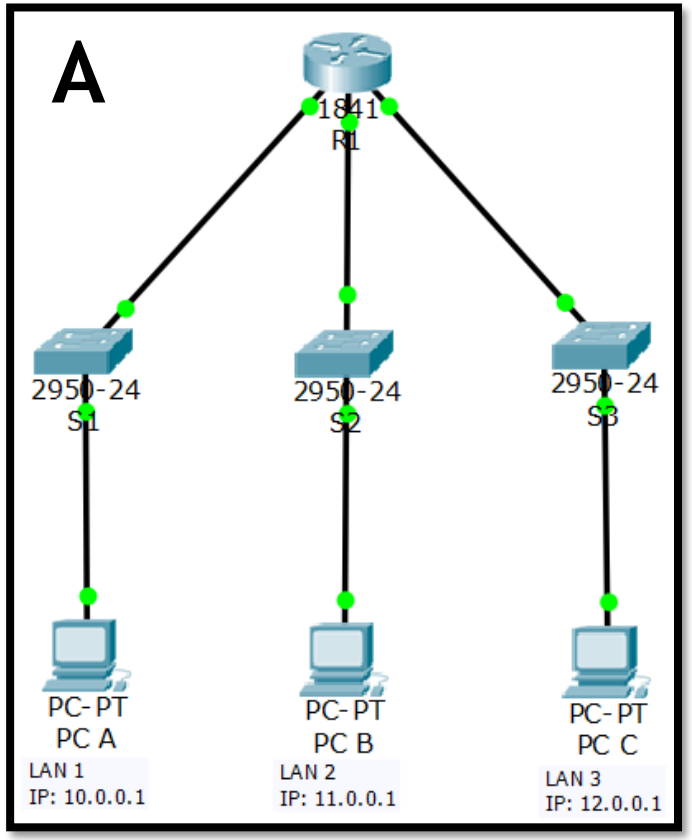
- מאפשר גמישות בתכנון הרשת, מיקומו הפיזי של הרכיב אינו מחייב אותו להיות באותו מרחב פיזי עם שאר הרכיבים. כלומר שאין קשר בין מקומו הפיזי לבין הרשת הלוגית שבה הוא נמצא בה!



Example

- דרישה מצוות IT: תכנון רשת שיספק 3 רשתות נפרדות לסניף חדש בתל אביב.
- באיזו דוגמה אנו חוסכים ציוד רשת יקר? ומקבלים את אותה תוצאה?





VLAN Types

- Default VLAN-סוג זה הוא VLAN המגיע כברירת מחדל עם המתג ולא ניתן להסיר אותו. לדוגמה VLAN 1.

- Data VLAN- סוג זה של VLAN הוא הסטנדרטי ביותר, כלומר VLAN אשר מעביר את המידע של המשתמש אך ורק באותה רשת וירטואלית (VLAN). במתג סטנדרטי ניתן ליצור עד 1005 רשתות וירטואליות.

- Native VLAN-במידה ומגיע למתג מידע, אשר לא שייך לשום רשת וירטואלית (VLAN), לדוגמה שליחת/קבלת עדכונים של פרוטוקול ה-STP, המתג ידאג שהמידע יעבור דרך ה-Native VLAN.

- Management VLAN-סוג זה הוא כל VLAN אשר מיועד להגדרת וניהול המתג. לדוגמה שליטה מרחוק VLAN 1.

Configuring VLAN

- מצב ברירת המחדל של המתג הוא שכל הפורטים שלו משוייכים ל-VLAN1.
  - ניתן לראות אילו פורטים משוייכים ל-VLAN מסוים בעזרת הפקודה Show VLAN Brief.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Configuring VLAN

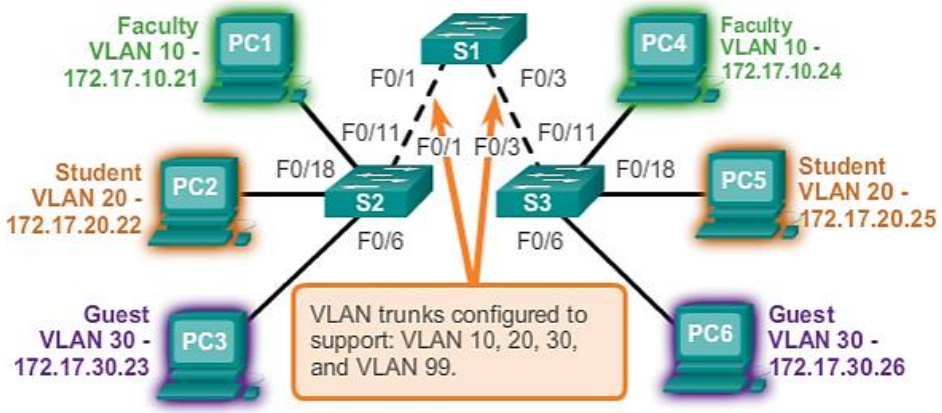
- יצירת VLAN's ושיוך פורטים ל-VLAN כרוך בכמה שלבים:

1. יצירת ה-VLAN מתאפשרת ברגע שאנו מצמידים מספר קטלוגי אליו, לדוגמה VLAN 10. מספרי VLAN 1002-1005 לא ניתנים לשימוש מכיוון שהם שמורים לפעולות המתג.
2. לטובת סדר וארגון ניתן להצמיד ל-VLAN תיאור (שם). לדוגמה VLAN 10 מיועד לרשת המחשבים של הסטודנטים, לכן יקרא גם VLAN Student.
3. שיוך פורט ל-VLAN נעשה ע"י כניסה לפורט/ממשק (Interface) מסויים ראשית, לדוגמה Interface FastEthernet 0/1 ורק שהמשתמש נמצא בתת-מצב (config-if) ניתן לשייך את ה-VLAN לפורט. ניתן להשתמש בפקודת Range (טווח) במטרה לשייך כמה פורטים ל-VLAN מסויים בבת אחת.
4. בחירה באיזה מצב הפורט ימתג (Switchport), כלומר כיצד הפורט יטפל במידע שעובר דרכו. קיימות שני אפשרויות Switchport mode Access ו-Switchport mode Trunk.

Switchport Modes

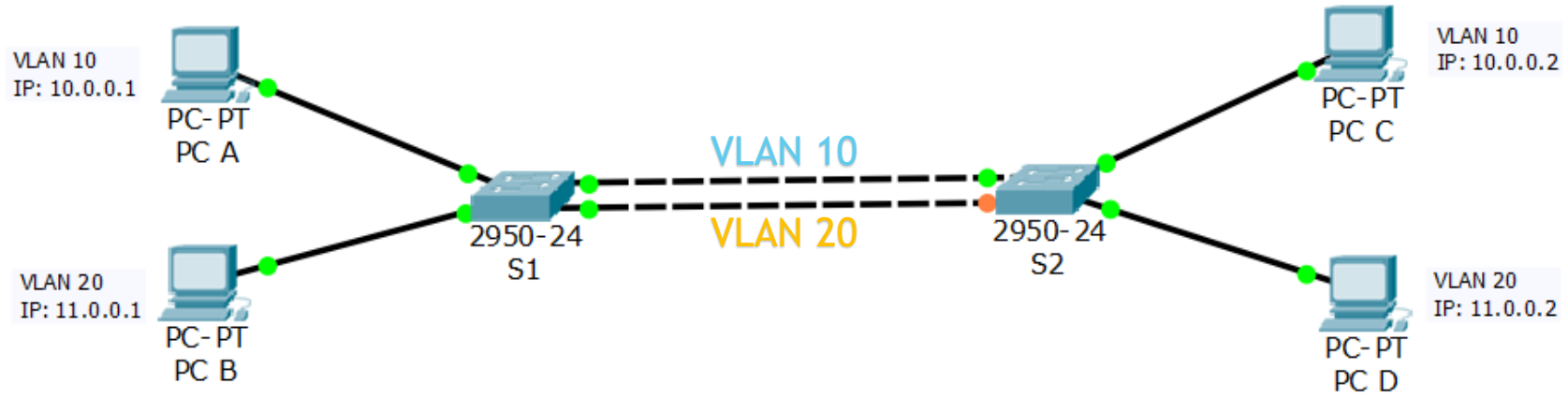
- Switchport mode access-במידה ונגדיר את מצב זה על הפורט, הפורט ידאג להעביר מידע שקשור אך ורק ל-VLAN מסויים, זאת אומרת שמידע של רשת VLAN 10 ו-VLAN 20 לא ישלח/יתקבל יחד באותו הפורט אלא רק מידע מ-VLAN יחיד (ה-Vlan המוגדר על הפורט). נשתמש במצב לדוגמה שהמתג מחובר למחשב או רכיב רשת אחר.

- Switchport mode Trunk-במידה ונגדיר את מצב זה על הפורט, הפורט ידאג להעביר מידע הקשור לכמה VLAN's במקביל, זאת אומרת שמידע לרשתות VLAN 10 ו-VLAN 20 ויותר יתקבל/ישלח יחד דרך אותו הפורט. נשתמש במצב זה לדוגמה שהמתג מחובר למתג אחר או לנתב בעזרת כבל בודד.



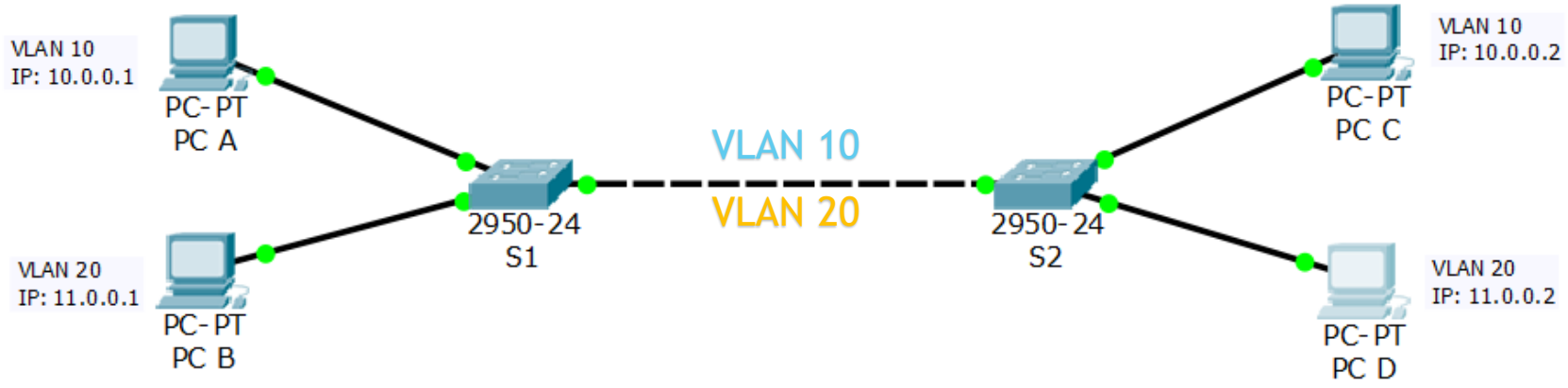
Switchport Modes

- לאור מה שלמדנו, אפשרי לשייך VLAN אחד לממשק אחד, מה שאומר שאם נרצה לחבר בין שני מתגים שמוגדרים עם שני VLAN's זהים, נזדקק לשני כבלים (חיבורים). אחד לטובת VLAN 10 ואחד לטובת VLAN 20. דבר שיוצר לנו בעיה משום שאם נרצה להגדיר יותר VLAN's הדבר יעלה לנו בהרבה ממשקים ובהרבה ציוד כבילה.



Switchport Modes

- בדיוק על בעיה זו מצב Trunk בא לענות, בעזרת מצב Trunk ניתן לשלוח/לקבל מידע של מספר VLAN's באותו הממשק הפיזי ועל אותו הכבל. פתרון שעוזר לנו לחסוך ממשקים וציוד כבילה מיותר.

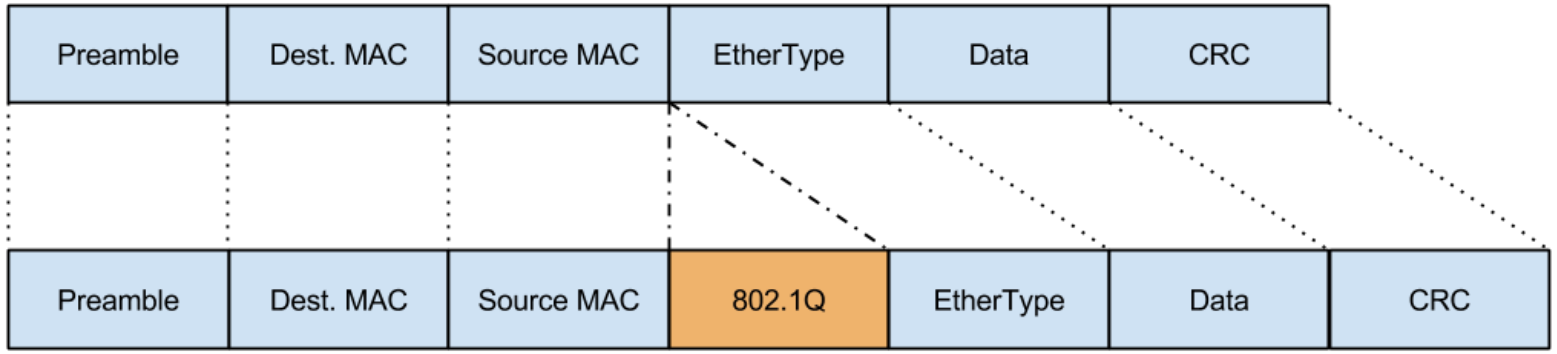


Trunking Protocol

- ממשק במצב Trunk מבצע תהליך על חבילות המידע, כלומר על מנת שהמתג יידע לאיזה VLAN משוייכת חבילת המידע (Frame), הפרוטוקול מבצע תהליך אינקפסולציה (כמו שהכרנו במפגש 3), בתהליך זה הפרוטוקול מכניס/אורז לתוך ה-Frame, TAG ID מספר ה-TAG מציין לאיזה VLAN משוייך ה-Frame . כשהמתג מקבל את חבילות המידע הוא בודק את ה-TAG ID, מזהה אותו ומעביר את ה-Frame ל-VLAN הנכון או ליתר דיוק לממשקים שמשוייכים ל-VLAN הנכון.
- ישנן 2 פרוטוקולים לביצוע האינקפסולציה אשר מוסיפה TAG ID:

1. ISL-Inter-Switch Link-פרוטוקול שפותח ע"י Cisco ונתמך ע"י חלק מרכיבי Cisco.
2. 802.1q-פרוטוקול שפותח ע"י ארגון IEEE ונתמך ע"י רוב סוגי המתגים.

- 802.1q הוא פרוטוקול ברירת המחדל ברוב המתגים כיום.

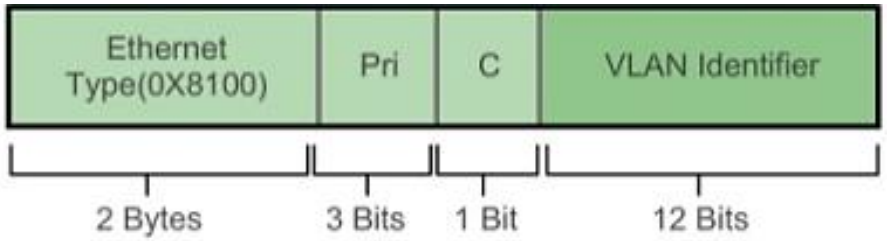


TAG ID

802.1q Header

- ה-Header (TAG ID) שמחדיר פרוטוקול ה-802.1q ל-Frame מכיל כמה נתונים:

1. Type-סוג הפרוטוקול.
2. Priority-עדיפות החבילה (QoS).
3. Canonical Format Identifier-נתון המאפשר לרשתות Tokin Ring לשלוח מידע ברשת Ethernet.
4. VLAN ID-מזהה את הרשת הווירטואלית, תומך ב-ID 1-4096.



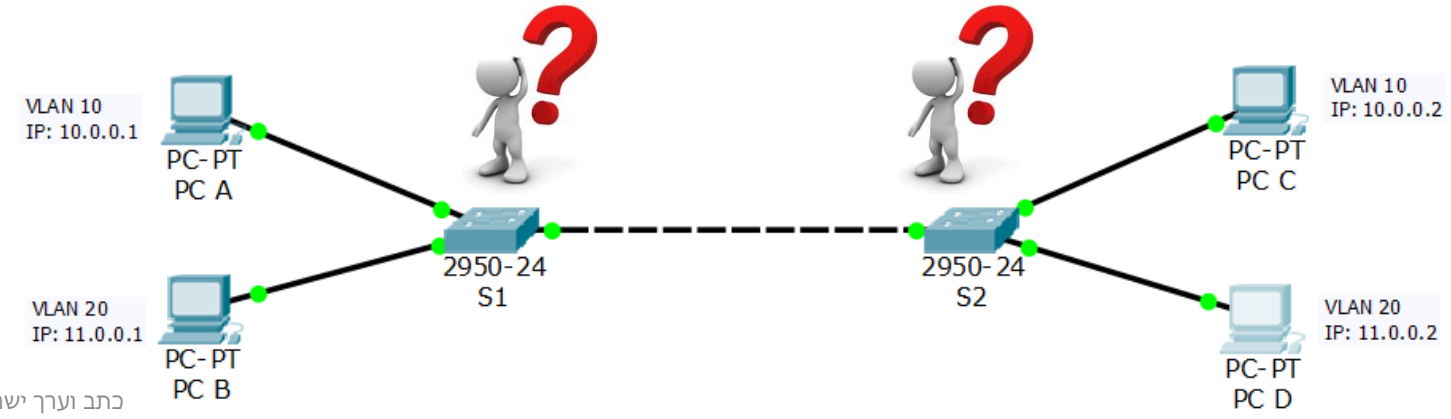
Trunking configuration

- כששני מתגים מחוברים יחדיו, עליהם להשתמש באותו הפרוטוקול לביצוע Trunking (לדבר באותה השפה). קיימות 3 אפשרויות:

1. להגדיר את שני המתגים שישתמשו בפרוטוקול 802.1q.
2. להגדיר את שני המתגים שישתמשו בפרוטוקול ISL.

- שני המתגים ינהלו משא ומתן אחד עם השני על מנת לקבוע את פרוטוקול ה-Trunk בו השתמשו, האחראי על המשא ומתן הוא פרוטוקול בשם Dynamic Trunking Protocol (DTP). בסוף תהליך המשא ומתן שני המתגים יבחרו ב-ISL או 802.1q (לרוב יבחר 802.1q).

- כדי לקבוע את סוג הפרוטוקול נשתמש בפקודה Switchport trunk encapsulation.



Trunking configuration

- ניתן להגדיר עוד שני מצבים על ממשק חוץ מ-Access ו-Trunk:

1. Dynamic Desirable-הגדרה זו קובעת שהממשק יכול להימצא במצב Access או Trunk. על מנת לקבוע את המצב שלו, הממשק ינהל משא ומתן מול הממשק במתג השני אליו הוא מחובר. ממשק שמוגדר על מצב זה **יוזם** יצירת Trunk עם הממשק במתג השני ע"י כך שהוא שולח לו עדכונים/הודעות.
2. Dynamic Auto-הגדרה זו קובעת שהממשק יכול להימצא במצב Access או Trunk. על מנת לקבוע את המצב שלו, הממשק ינהל משא ומתן מול הממשק במתג השני אליו הוא מחובר. הבדל בין מצב זה למצב הקודם הוא שבמצב זה הממשק הוא **פסיבי**, אם הוא יקבל עדכונים/הודעות מהמתג השני לצורך יצירת Trunk, הוא יענה אליהן ויעבור למצב Trunk, אבל הוא לא ייזום בעצמו של יצירת Trunk. זהו מצב ברירת המחדל של כל הממשקים במתג.

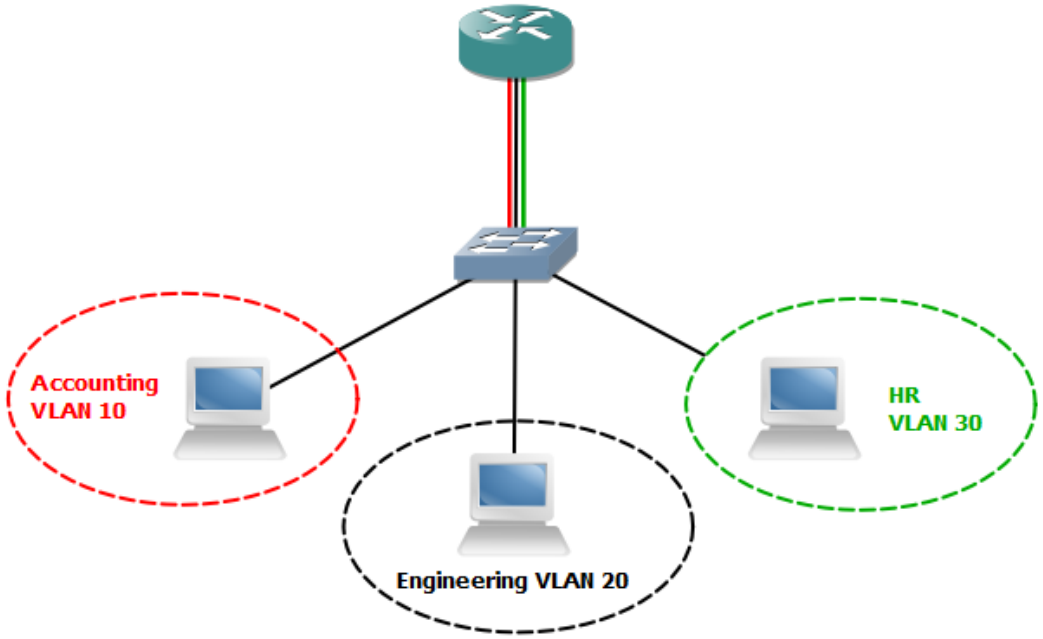
Trunking configuration

- חשוב להבין את ההשלכות של ה-Administrative Mode שאנחנו מגדירים לממשקים אשר מחברים בין מתגים ולדעת באיזה מצב ייווצר Trunk בין המתגים. בטבלה הבאה תוכלו למצוא אתה כל הקומבינציות האפשריות של הגדרת Administrative Mode ומה תהיה התוצאה.
- * כאשר מתג אחד מוגדר על Access והמתג השני על Trunk, נוצרת בעיה. יש להימנע ממצב זה.

Dynamic Desirable	Trunk	Dynamic Auto	Access	Administrative Mode
Access	*	Access	Access	Access
Trunk	Trunk	Access	Access	Dynamic Auto
Trunk	Trunk	Trunk	*	Trunk
Trunk	Trunk	Trunk	Access	Dynamic Desirable

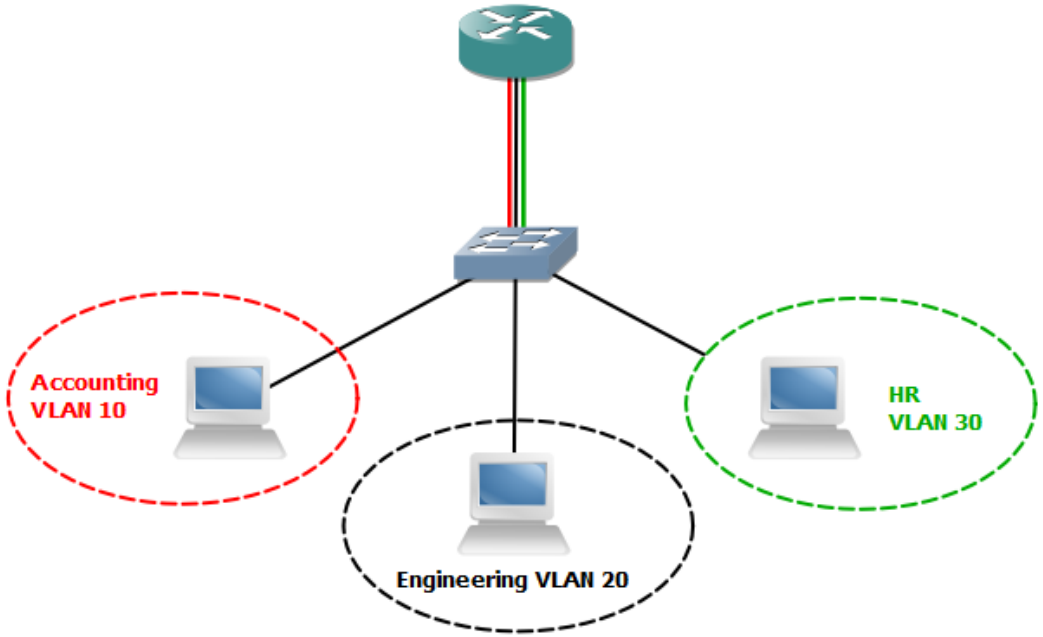
Router-on-a-Stick

- Router-on-a-stick היא שיטה שבאה לתת לנו מענה על חוסר היכולת לקישור בין רשתות וירטואליות שונות (VLAN's) מכיוון שכל VLAN רואה את עצמה כרשת LAN נפרדת עלינו להיעזר בנתב (Router) בכדי לנתב מידע בין הרשתות השונות (VLAN's).



Router-on-a-Stick

- איך בדיוק שיטה זו פועלת...
- הממשק בצד המתג מוגדר על מצב Trunk מה שמאפשר לו, לשלוח/לקבל מידע שקשור לכל ה-VLAN's.
- הממשק בצד הנתב מוגדר בצורה מיוחדת בעזרת תתי-ממשקים, כלומר מספר ממשקים וירטואליים כמספר ה-VLAN's מוגדרים על ממשק פיזי אחד. בנוסף הנתב משתמש בפרוטוקול 802.1q על מנת לתקשר עם המתג באותה צורת אינקפסולציה (שפה) וכיצד להבדיל בין חבילות המידע השונות (מ-VLAN's שונים) המגיעות מהמתג.



VLAN Trunking Protocol (VTP)

- VTP הוא פרוטוקול שפותח ע"י חברת Cisco ואשר התפקיד שלו הוא לגרום למתג לפרסם את ה-VLAN's שהוא מכיר למתגים אחרים ברשת, כאשר המטרה היא שכל המתגים ברשת יכירו את ה-VLAN's שקיימות ברשת. במרבית הארגונים לא נעשה שימוש ב-VTP לכן אין צורך להרחיב עליו, עם זאת יש לפרוטוקול זה השפעה על האופן שבו המתג פועל, גם אם לא נשתמש בו. לכן חשוב להכיר מספר דברים אודותיו.
- כל מתג יכול להימצא באחד משלושה מצבים:

1. Server-אם המתג במצב זה הוא מפרסם את ה-VLAN's לכל הרשת.
2. Client-אם המתג במצב זה הוא מתעדכן מהמתג ה-Server אילו VLAN's יש ברשת.
3. Transparent-המתג לא מפרסם את ה-VLAN's לכל הרשת, נשתמש במצב זה גם אם ברצוננו לבטל את השימוש בפרוטוקול, משום שלא ניתן לבטל את השימוש ב-VTP לחלוטין על מתגים של Cisco.

VLAN Trunking Protocol (VTP)

- נרצה להשתמש במצב Transparent או לבטל לגמרי את השימוש ב-VTP, משום שהוא מגביל אותנו בכמה מאפיינים, כשאנו במצב Transparent אנו יכולים ליצור VLAN's גם מהטווח הרגיל (1-1002) וגם מהטווח המורחב (1005-4096). אם המתג מוגדר על מצב Client או Server, נגלה את הדברים הבאים:

1. נוכל ליצור VLAN's רק מהטווח הרגיל ולא מהמורחב.
2. מתגים שמוגדרים במצב Client לא ניתן ליצור VLAN's כלל.
3. מידע על VLAN's לא יופיע בקובץ ההגדרות Running-config.

- הפקודה Show VTP Status תציג לנו באיזה מצב המתג ואם עלינו לעבור מצב, בכדי להמשיך להגדיר את המתג ללא הפרעות.

VLAN Trunking Protocol (VTP)

- אם ברצוננו להגדיר את הפרוטוקול על המתגים (Switch's) ברשת, ניתן לעשות זאת על ידי כמה שלבים פשוטים:

1. נגדיר את הממשקים שמחברים בין המתגים שיהיו במצב Trunk.
2. נגדיר לפרוטוקול באיזה מצב המתג ימצא (Server, Client, Transparent).
3. נגדיר לפרוטוקול דומיין (Domain) משתוף.
4. נגדיר לפרוטוקול סיסמה.
5. נשתמש בפקודות Show לוודא את ההגדרות.

- דרישה-כל המתגים חייבים להריץ את אותה גרסה של הפרוטוקול.

Command Page

- רשימת הפקודות המלאה והסבר, נמצאת בקובץ Command Page VLAN.