Digital Whisper Technologic Papers

על VLANs ועל Private VLANs

מאת רון הרניק

הקדמה

המדריך שבי מקשה עלי מאוד להניח הנחות בקשר לאנשים שלהם אני מסביר משהו. כך שיכול להיות שבמהלך המאמר הזה אפרט על נושאים מסויימים היכולים להראות כמובנים מאליו לחלקיכם, אבל אני כן רוצה להשאיר הידע הזה פתוח לאנשים שבאים מתחומים שונים, אז תרגישו חופשי לדלג קדימה אל הדברים הטובים (זה בסדר, אני לא אעלב).

במאמר זה אדבר על נושא הנקרא Private VLANS, ואשתמש בציוד Cisco בכדי להדגים אותו. אני משתמש בציוד Cisco מהסיבה שהוא זמין לי ועליו יש לי יותר ניסיון. אך חשוב להבין שאנחנו מדברים ברעיונות, והיישום של הרעיון, לאחר ההבנה שלו, הוא החלק הקל. אספק קישור למדריך הגדרה גם למכשירי Juniper.

לפני שאנחנו יכולים לצלול אל תוך הנושא המרכזי שלנו, יש לוודא שאנחנו מבינים כמה טכנולוגיות בסיסיות.

VLAN - Virtual Local Area Network

הרעיון של VLAN הוא לא רעיון שונה מכל סוג אחר של וירטואליזציה. אנו מבצעים חלוקה לוגית של תשתית פיזית כלשהי. כמו שאנו מחלקים את הכונן במחשב למחיצות, אך הכונן הוא מקשה פיזית אחת, כך גם אנו יכולים לחלק מתג (Switch) לרשתות שונות.

רוב המתגים בנויים בצורה כזו שמאפשרת לנו להשתמש בהם כמכשירי Plug & Play, אנו יכולים לחבר שתי תחנות קצה למתג, לתת לתחנות כתובות IP וכרגע התחנות הם חלק מאותה הרשת.

כאשר אנו מחלקים מתג ל-VLANS, אנו בעצם גורמים למתג להתנהג כמו מספר מתגים שונים. החלוקה מתבצעת ב-L2, ויידרש מכשיר בעל יכולות L3 בכדי לנתב בין הרשתות הוירטואליות שלנו. השיוך ל-VLANS מתבצע על בסיס פורטים. ברגע ששיכנו פורט מסויים ל-VLAN, כל Frame אשר יכנס לפורט יקבל שדה נוסף הנקרא VLAN Tag, שדה זה, פשוטו כמשמעו, מציין לאיזה VLAN אותה חבילת מידע שייכת. אם אותה חבילת מידע אשר נכנסה לפורט היא למשל הודעת Broadcast, ההודעה תתפשט אך ורק

בפורטים השייכים לאותה VLAN. כאשר אנו עובדים עם VLANS אנו מחלקים את הפורטים שלנו לשני סוגים -

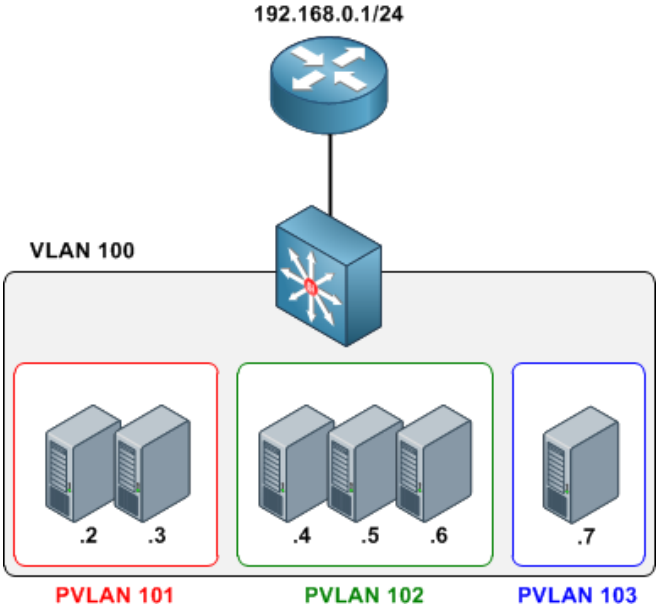
Access Ports - פורטים המשוכיים ל-VLAN ספציפית אחת בלבד, ואינם מעבירים את ה-VLAN Tag. כאשר תחנת הקצה שולחת חבילת מידע אל הפורט, התיוג מתבצע וחבילת המידע ממותגת הלאה לפי טבלת ה-MAC של ה-VLAN, כאשר חבילת המידע יוצאת מפורט ה-Access המתאים המתג "מקלף" את ה- VLAN Tag מחבילת המידע.

Trunk Ports - פורטים המסוגלים להעביר VLAN Tags, נשתמש בפורטים אלו בכדי להעביר VLANS בין מתגים. פורטים אלו אינם משוייכם לVLAN ספציפית אך ניתן להגדיר אילו VLANS יכולות לחצות את ה-Trunk. הפרוטוקול הנפוץ ביותר לתיוג VLANS ובניית Trunks הוא 802.1q.

אז הרעיון של VLAN הוא טוב ויפה, מספק לנו מידור, חוסך תנועה מיותרת, מידה מסויימת של אבטחה וחסכון בציוד. אך מה קורה כאשר אנו רוצים לשלוט בתקשורת בין תחנות הנמצאות באותה ה-VLAN? אנו רוצים מסיבה מסויימת להשאיר את התחנות (או הלקוחות) באותו טווח כתובות IP, ובאותה הרשת, אך אנו רוצים לוודא שחלק מהתחנות אינן מסוגלות לתקשר אחת עם השניה וחלקן כן. במידה ומצאתם את עצמכם במצב המאוד ספציפי הזה, Private VLAN הוא פתרון אפשרי.

PRIVATE VLANS

PVLANS פותחו בכדי לאפשר לנו לבודד תחנות קצה ב-L2. באמצעות פתרון זה ניתן להגדיר מספר תחנות באותה רשת IP ותחת אותה VLAN, אך לשלוט ביכולת של אותן תחנות לתקשר אחת עם השניה.



[התמונות נלקחו ממצגות הלימוד של Cisco]

כפי שניתן לראות בשרטוט, הרעיון ב-PVLANS הוא להגדיר VLAN ראשית אחת, ותחתיה Sub-VLANS המשוייכות אליה. ה-VLAN הראשית היא VLAN רגילה לחלוטין כמו אלו שאנו מכירים ואוהבים. ה-VLANS המשניות (Secondary VLAN) הן VLANS אשר אנו משייכים להם אחד משני התפקידים הספציפיים הבאים:

- **Isolated** - נקודות הקצה המשוייכות ל-VLAN הזו לא מסוגלות לתקשר אחד עם השניה, וכמו כן לא מסוגלות לתקשר עם נקודות קצה המשוייכות ל-Private VLAN אחרת.

- **Community** - נקודות הקצה המשוייכות לאותה Community VLAN מסוגלות לתקשר אחת עם השניה אך לא מסוגלות לתקשר עם Community נוספת או עם ה-Isolated.

Access Port הפועל ב-Private VLAN מתפקד באחד משני המצבים הבאים:

- **Host** - הפורט "יורש" את תפקידו לפי סוג ה-VLAN אליה הוא משוייך, כלומר, פורט המשוייך ל-Isolated-VLAN יבודד לחלוטין את תחנת הקצה. פורט המשוייך ל-Community יאפשר לתקשורת לנקודות קצה באותה ב-Community.

- **Promiscuous** - הפורט ה"מופקר" מסוגל לתקשר עם כל נקודות הקצה המשוייכות לאותה Primary VLAN. פורט זה בדרך כלל יפנה לכיוון ה-Default Gateway או לכיוון משאב משותף מסויים. ה-Promiscuous מסוגל לתקשר עם כל Community ועם כל Isolated.

לפני שנמשיך הלאה להגדרות הבסיסיות ואז לחלקים היותר מתקדמים, בואו נסכם את סוגי ה-VLANS שקיימות תחת רעיון ה-Private VLANS, ואילו נתונים עוברים בכל אחת:

Primary VLAN - ה-VLAN הראשית אשר מאגדת תחתיה את ה-Secondary VLANS, VLAN זאת תעביר נתונים ב-Downstream בין ה-Promiscuous לכל סוגי הפורטים האחרים ב-VLAN, בין אם הם Community או Isolated.

Secondary Isolated VLAN - VLAN זו מבודדת את הנקודות המשוייכות אליה אחת מהשניה, ומאפשרת להן לתקשר רק עם ה-Promiscuous. מאחר וכל פורט המשוייך ל-Isolated מבודד לחלוטין מהפורטים האחרים, ניתן ליצור רק Isolated VLAN אחת תחת כל Primary.

Secondary Community VLAN - VLAN זו מעבירה נתונים בין נקודות קצה המשוייכות לאותה Community, וביניהן אל ה-Promiscuous. ניתן ליצור Communities רבות תחת אותה Primary.

הגדרת PRIVATE VLANS

יש כל כך הרבה דברים שניתן להגדיר במכשירים האלו, שאני תמיד מעדיף לעבוד לפי שלבים מסודרים בנוגע לכל הגדרה. אלו הם השלבים להגדרת ה-Private VLANS, לאחר מכן נראה את הפקודות עצמן:

1. הגדירו את מצב ה-VTP של המתג ל-Transparent.
2. צרו את ה-Secondary VLANS.
3. צרו את ה-Primary VLAN.
4. שייכו את ה-Secondary VLANS ל-Primary (mapping)
5. הגדירו פורטים כ-Isolated או Community.
6. שייכו את הפורטים לצמד Primary-Secondary VLAN.
7. הגדירו פורט כ-Promiscuous.
8. שייכו את ה-Promiscuous לצמד ה-Primary-Secondary VLAN.

VTP על קצה המזלג

VTP הוא פרוטוקול הפועל במכשירי Cisco המאפשר למתגים ללמד אחד את השני באופן דינמי על VLANS. VTP מגדיר שלושה מצבים שבהם המתגים יכולים לפעול:

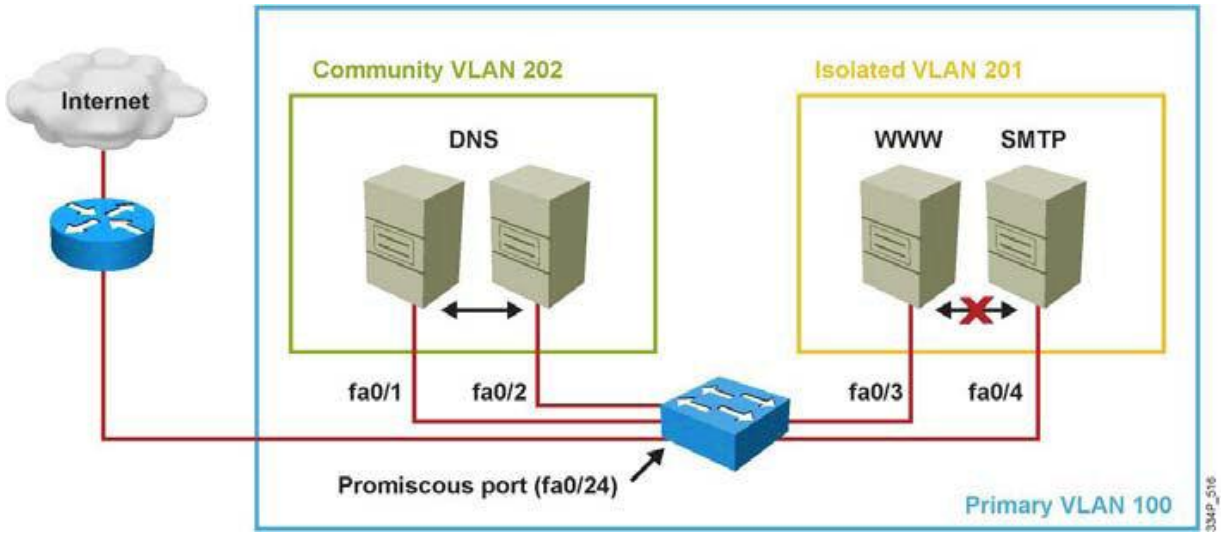
Server - מסוגל ליצור ולגרוע VLANS, ומלמד את המתגים האחרים על כל שינוי שמתבצע.

Client - לא מסוגל ליצור או לגרוע VLANS, ומסוגל אך ורק ללמוד מה-Server ולהעביר את העדכונים הלאה אל מתגים נוספים.

Transparent - מסוגל ליצור ולגרוע VLANS אך באופן מקומי בלבד, ואינו לומד או מלמד ממתגים אחרים במערכת.

כאשר עובדים עם Private VLANS יש להגדיר את המתגים כ-Transparent מכיוון ש-VTP אינו תומך ואינו מכיר ב-Private VLANS, ולא מסוגל להעביר את הנתונים שלהן. הגרסה החדשה של VTP, VTPv3 - צפויה להיות מסוגלת לעבוד עם Private VLANS.

ניקח לדוגמא את המצב הבא:



[התמונות נלקחו ממצגות הלימוד של Cisco]

אנו רוצים לאפשר לשרתי ה-DNS לתקשר אחד השני, אך לבודד לחלוטין את שרתי ה-Web וה-SMTP. שני שרתי ה-DNS יושבים באותה Community, והשרתים הנוספים הוגדרו כ-Isolated. לכן כרגע שרתי ה-DNS מסוגלים לדבר אחד עם השני ועם ה-Promiscuous המחובר לנתב, ושרתי ה-Web וה-SMTP מסוגלים לדבר עם הנתב בלבד.

ההגדרות על המתג, לפי השלבים שצויינו למעלה:

הגדרת VTP כ-Transparent:

```
Switch(config)# vtp transparent
```

יצירת ה-Secondary VLANS וקביעת תפקידן:

```
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan community
```

יצירת ה-Primary ושיוכה ל-Secondary:

```
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 201,202
```

הגדרת ה-Promiscuous:

```
Switch(config-vlan)# interface fastethernet 0/24
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 201,202
```

הגדרת הפורטים ב-Community:

```
Switch(config-if)# interface range fastethernet 0/1 - 2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 202
```

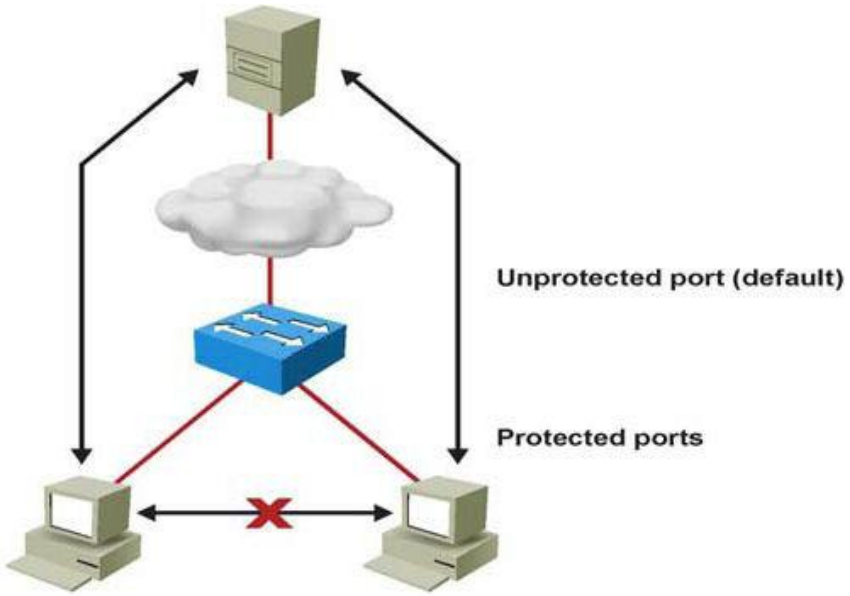
הגדרת הפורטים ב-Isolated:

```
Switch(config-if)# interface range fastethernet 0/3 - 4
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 201
```

שימו לב שאין פקודה ספציפית אשר מגדירה פורט מסויים במצב Isolated או Community, אלא ההגדרה מתבצעת לפי השיוך לצמד ה-Primary-Secondary בלבד.

במידה ואנחנו רוצים להגדיר טופולוגיה בעלת שני מתגים או יותר הפועלים עם Private VLANS ניתן להעביר את כל נתוני ה-VLANS באמצעות Trunks רגילים, כל עוד כל המתגים בנתיב מכירים את כל ה-VLANS המשתתפות, ה-Primary וה-Secondaries. במתגים מסדרת 4500 ו-6000 ישנה אופצית ההגדרה של Private Vlan trunks מיוחדים המספקים שליטה גדולה יותר על מעבר ה-Private VLANS בין המתגים.

במתגים אשר לא תומכים ב-Private VLANS לרוב יש אופציות פשוטות יותר אשר יכולות לספק לנו תוצאה דומה, אך פחות גמישה. לדוגמה, במתגי Cisco פשוטים מסדרת 2960 ניתן להגדיר Protected Ports, עקרון הפעולה שלהם דומה לזה של ה-Isolated. פורטים אשר מוגדרים כ-Protected אינם מסוגלים לדבר זה עם זה אך מסוגלים לדבר עם פורטים רגילים במתג אשר משוייכים לאותה VLAN.



[התמונות נלקחו ממצגות הלימוד של Cisco]

הגדרת Protected Port:

```
Switch(config-if)# switchport protected
```

לסיכום

Private VLANS הוא רעיון אשר מרחיב את יכולות המידור וההפרדה של ה-VLANS הרגילות, ברגע שמבינים רעיון מסויים קל ליישם אותו בסביבות שונות. המאמר הזה יכול לשמש אתכם כמדריך או כ-Reference להגדרות עתידיות.

קישורים לקריאה נוספת

- http://www.juniper.net/techpubs/en_US/junos9.4/topics/example/private-vlans-ex-series.html
- http://www.juniper.net/techpubs/en_US/junos10.4/topics/concept/private-vlans-ex-series.html
- http://blog.internetworkexpert.com/2008/07/14/private-vlans-revisited/
- http://tools.ietf.org/html/rfc5517

על המחבר

רון הרניק (CCNP) הוא מדריך לנושאי תקשורת נתונים במכללת IITC ברמת גן, ומחבר הבלוג The Ping Factory. בנוסף, הוא משתדל לציית לכל הסטראוטיפים המאפיינים את החנון הטיפוסי.

בכל שאלה אתם מוזמנים לפנות אלי במייל, וגם כמובן אם יש לכם הצעות עבור מאמרים נוספים בנושאי תקשורת נתונים. כתובת אימייל ליצירת קשר:

ronh@iitc.co.il