

In-Band & Out-of-Band

Advanced Configuration

Management Methods

▶ הגדרה וניהול (קינפוג) של כל רכיב רשת ניתן לבצע בשתי צורות, בצורה מקומית ובצורה מרוחקת:

1. **Out-of-band Management**- בצורה זו משיגים גישה לרכיב הרשת בצורה מקומית, זאת אומרת חייבים להיות פיזית קרובים למכשיר. שיטה זו נעשית ע"י כבל ייעודי לניהול (Console), תוכנת טרמינל ומחשב. הגדרה ראשונית תמיד תהיה בשיטה זו.

2. **In-band Management**- בצורה זו משיגים גישה לרכיב דרך הרשת, זאת אומרת בעזרת פרוטוקול או תוכנת שליטה מרחוק. בקצרה ניהול הרכיב מרחוק. כמובן שצורה זו של ניהול חייבת לכלול פרוטוקולי אבטחה במטרה להגביל את הגישה לאנשים מורשים בלבד. *באופן יומי נעדיף להשתמש בשיטה זו, כי היא מאפשרת הגדרה ואיסוף מידע מרכיב הרשת ללא בזבז זמן יקר ולוגיסטיקה מיותרת*.



Remote Access Protocols

- ▶ שליטה מרחוק נעשית בעיקר ע"י שני פרוטוקולים **Telnet** ו-**SSH**. בגלל רמת האבטחה הנמוכה בפרוטוקול **Telnet**, היום הפרוטוקול הנפוץ יותר הוא **SSH** בגלל מנגנון האבטחה המתוחכם שלו.
- ▶ בקצרה על הפרוטוקולים:

- **Telnet**-פרוטוקול זה מאפשר שליטה מרחוק לרכיבי רשת וקצה שונים. פרוטוקול זה בעל מנגנון אבטחה די פשוט ופריץ מאוד כיום. פרוטוקול זה ישן וכלל לא מומלץ להשתמש בו.
- הפורט הלוגי של הפרוטוקול: **23**

- **SSH**-פרוטוקול זה מאפשר שליטה מרחוק לרכיבי רשת וקצה שונים. פרוטוקול זה בעל מנגנון אבטחה מורכב, מתוחכם וקשה לפיצוח. בגלל רמת האבטחה הגבוהה של פרוטוקול זה, השימוש בו רחב מאוד.
- הפורט הלוגי של הפרוטוקול: **22**
- הפרוטוקול עושה שימוש בשיטת ההצפנה **RSA** בעיקר, שיטה זו כוללת שני סוגי מפתחות: פרטי וציבורי.

Remote Access Configuration

▶ הגדרת שליטה מרחוק על נתב ומתג כמעט זהה, פרט לשימוש בממשק וירטואלי במתג.
▶ שלבי הגדרה:

1. יצירת משתמש וסיסמה על גבי הרכיב.
2. הפעלת הערוצים הווירטואליים ברכיב *ערוצי ה-VTY*, פעולה זו מורה לרכיב לקבל חיבורים מרחוק.
3. הגדרת פרוטוקול השליטה המאושר *כברירת מחדל הרכיב מאשר חיבורים משני הפרוטוקולים*.
▶ במתג (Switch) לא אפשרי להגדיר כתובת IP לממשק (פורט) פיזי, לכן קיים SVI סוג נוסף של ממשק במתגים, Switch Virtual Interface הוא פורט וירטואלי (מובנה בתוכנה) שמאפשר הגדרת IP. פורט לוגי זה נקרא VLAN1.
4. הגדרת כתובת IP ו-SM על Interface VLAN 1.
5. הגדרת Default gateway למתג.
 - אופציונלי-הגדרת כתובת IP מסוימת שרק ממנה המתג יאשר התחברות. לדוג' מחשב המנהל (שם הפיצ'ר ACL).



Access The Device

- ▶ גישה לרכיב בעזרת אחד מהפרוטוקולים אפשרית בממשק פקודה וגם בעזרת תוכנת טרמינל:
 - CMD הוא לדוגמה ממשק הפקודה של Windows.
 - Putty היא דוגמה לתוכנת טרמינל.
- ▶ מבנה (Syntax) פקודת ההשתלטות של הפרוטוקולים:
 - דוגמה בחלונית CMD

```
C:\> telnet target-ip
```

```
C:\> ssh -l username target-ip
```



RemoteAccess

Command Page

רשימת הפקודות המלאה והסבר, נמצאת בקובץ Command Page Basic. ►

