Command Page – ACL

דגשים/כללים בהגדרת ACL:

1. הגדרת ACL מורכבת משני שלבים: 1.יצירת ה-ACL 2.הצבת ה-ACL על ממשק עם כיוון (IN\OUT).
2. ניתן להגדיר ACL אחד לכל פרוטוקול (IPv4 or IPv6), ממשק (Interface) וכיוון (IN or OUT).
3. יש לתכנן באיזה סדר נגדיר את ה-ACL, משום שאכיפה של ACL מתבצעת בסדר כרונולוגי.
4. Implicit Deny-ברגע שהגדרנו ACL, הממשק חוסם את כל מידע שלא תואם ל-ACL. זאת אומרת הכל! לכן חייב להוסיף לסופו של כל ACL שורה שמתירה (Permit Any) לכל שאר חבילות המידע לעבור בחופשיות.
5. יש לתכנן על איזה ממשק ובאיזה כיוון להגדיר את ה-ACL למקסימום אפקט ויעילות:
   - Standard ACL מומלץ להציב על הממשק הכי קרוב **ליעד**.
   - Extended ACL מומלץ להציב על הממשק הכי קרוב **למקור**.

מבנה הפקודה (Syntax) ופרמטרים של Standard ACL:

1. Access-list-number – מספר המזהה את ה-ACL וקובע את סוגו (Standard או Extended).
2. Deny – ACL חוסם גישה ע"פ התנאים.
3. Permit – ACL מאפשר גישה ע"פ התנאים.
4. Remark (Optional) – הוספת הערה ל-ACL, כך שמטרת ה-ACL תהיה מובנת לכלום (הערה מוגבלת עד 100 תווים).
5. Source – הגדרת המקור שעליו נאכוף את ה-ACL, ניתן להגדיר מקור בשלוש דרכים: 1.כתובת IP 2.Any (כולם) 3.Host (משתמש יחיד).
6. Source-wildcard – הגדרת WC מתאים לכתובת ה-IP שמוגדרת כמקור.
7. Log (Optional) – הגדרה זו גורמת לדיווח בצורת שורת log ב-Console במידה ו-ACL זיהה חבילת מידע שתואמת לתנאים שלו.

	תיאור	הפקודה
1	הגדרת Standard ACL ע"פ מספר. *Numbered ACL *Standard ACL נוצר בעזרת המספרים: • 1-99 • 1300-1999 *דוגמה Standard ACL	שלב א'-יצירת ה-ACL: Router(config)#access-list ***access-list-number*** **deny \ permit** ***source*** ***source-wildcard*** *חישוב Wild Card. *שלב ב'-הצבת ה-ACL מספרי על הממשק.
2	הגדרת Standard ACL ע"פ שם. *Named ACL *הגדרה וזיהוי ACL ע"פ שם ולא מספר.	שלב א'-יצירת ה-ACL: Router(config)#ip access-list standard ***name*** Router(config-std-nacl)#**permit \ deny \ remark** ***source*** ***source-wildcard*** **log** *במקום *name* נגדיר שם ל-ACL. *חישוב Wild Card. *שלב ב'-הצבת ה-ACL שמי על הממשק.

מבנה הפקודה (Syntax) ופרמטרים של Extended ACL:

*פרמטרים של Extended ACL זהים לפרמטרים של Standard ACL פרט ל:

1. Protocol – פרוטוקול שישמש כתנאי ל-ACL (לדוג' IP, TCP, UDP, ICMP).
2. Destination – הגדרת היעד שעליו נאכוף את ה-ACL, ניתן להגדיר יעד בשלוש דרכים: 1.כתובת IP 2.Any (כולם) 3.Host (משתמש יחיד).
3. Source-wildcard – הגדרת WC מתאים לכתובת ה-IP שמוגדרת במקור.
4. Operator – משווה אילו מספרי פורטים ה-ACL יאכוף.
5. Port – מספר הפורט (שירות/פרוטוקול) שעליו נאכוף את ה-ACL.

3	הגדרת Extended ACL ע"פ מספר. *Numbered ACL *Standard ACL נוצר בעזרת המספרים: • 100-199 • 2000-2699 *דוגמה Extended ACL *מספרי פורטים נפוצים.	Router(config)#access-list ***access-list-number*** **deny \ permit \ remark** ***protocol source source-wildcard destination destination-wildcard operator port-number*** *חישוב Wild Card. *במקום *operator* נגדיר אחת מהאפשרויות הבאות: eq (equal) – בדיוק אותו מספר פורט. ls (less than) – מספרי פורטים ששווים פחות מהפורט. gt (greater than) – מספרי פורטים ששווים יותר מהפורט. neq (not equal) – מספרי פורטים של שווים לפורט (כולם חוץ ממנו). range -טווח של מספרי פורטים. *שלב ב'-הצבת ה-ACL מספרי על הממשק.
4	הגדרת Extended ACL ע"פ שם. *Named ACL *הגדרה וזיהוי ACL ע"פ שם ולא מספר.	Router(config)#ip access-list extended ***name*** Router(config-std-nacl)# **deny \ permit \ remark** ***protocol source source-wildcard destination destination-wildcard operator port-number*** *במקום *name* נגדיר שם ל-ACL. *חישוב Wild Card. *שלב ב'-הצבת ה-ACL שמי על הממשק.

5	הצבת ה-ACL מספרי על ממשק. *נבחר in לאכיפה של ה-ACL לחבילות מידע שנכנסות אל הממשק. *נבחר out לאכיפה של ה-ACL לחבילות מידע שיוצאות מהממשק.	Router(config)#interface ***interface-id*** Router(config-if)#ip access-group ***access-list-number*** **in \ out** *במקום *access-list-number* נגדיר את המספר של ה-ACL שנוצר בשלב א'.
6	הצבת ה-ACL שמי על ממשק. *נבחר in לאכיפה של ה-ACL לחבילות מידע שנכנסות אל הממשק. *נבחר out לאכיפה של ה-ACL לחבילות מידע שיוצאות מהממשק.	Router(config)#interface ***interface-id*** Router(config-if)#ip access-group ***name*** **in\ out** *במקום *name* נגדיר את השם של ה-ACL שנוצר בשלב א'.

פקודות Show

1. Show access-list – מציגה מידע על כל ה-ACL המוגדרים על הרכיב.
2. Show access-list *ACL-type* *ACL-id* – מצגיה ACL מסויים בהתאם לפרמטרים.

דוגמה להגדרת Standard ACL:

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.255.255
```

דוגמה להגדרת Extended ACL:

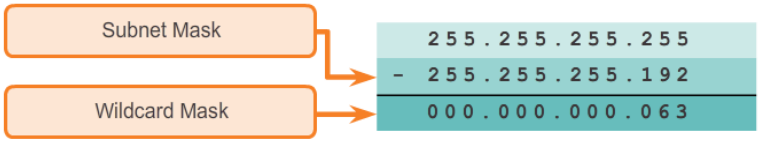
```
Router(config)#access-list 105 permit 172.16.0.0 0.0.255.255 any eq 80
```

חישוב Wild Card:

Wildcard משמש אותנו רבות בכל מיני פיצ'רים של מערכת הפעלה (לדוג' OSPF). Wildcard מתנהג בצורה הפוכה לגמרי מ- Subnet Mask וגם פועל הפוך ממנו (מכן מגיע שמו wild), תפקידו לשמש כמנגנון התאמה. Wildcard פועל בצורה כזו, 0 מייצג אובייקט קבוע בכתובת ה-IP שאליו צריך למצוא התאמה מדוייקת. 1 מייצג אובייקט בכתובת ה-IP שאליו כל אפשרות מתאימה.

לדוגמה:

- 0.0.0.0 הנתב ישווה את כל ארבעת האוקטטות של כתובת ה-IP ויחפש התאמה מדוייקת לאותם מספרים.
- 0.0.0.255 הנתב ישווה רק את שלושת האוקטטות הראשונות.
- 0.0.255.255 הנתב ישווה רק את שתי האוקטטות הראשונות.
- 0.255.255.255 הנתב ישווה רק את האוקטטה הראשונה.
- חישוב WC לתת-רשת (רשת מסובנטת):



פרוטוקולים מספרי פורטים:

זכרו שהפרוטוקולים המשמשים לשליחת מידע הם TCP ו-UDP, פרוטוקולים אלו משתמשים במספרי פורטים שמייצגים שירותים שונים ברשת. מספרי פורטים נפוצים שמומלץ לזכור:

- HTTP -80
- HTTPS-443
- FTP-21
- Telnet-23
- SMTP-25
- POP3-110
- SSH-22
- DNS-53
- RDP-3389

[פקודות באתר Cisco]