

קורס CCNA

שיעור מס' 7

נושא הלימוד:

ACL (Access Control List)

מרצה: אלי בפלר

Version 2

מבוא

לצורך אבטחת הרשת ברור שיש צורך ב-Firewall (חומת אש) בכל רשת, שהוא כלי יעודי לאבטחת הרשת, תפקידו להגדיר איזה סוג מידע מותר להעביר ברשת וכן למי מותר להעביר את המידע.

בנוסף ל-Firewall ניתן להפעיל בנתב כלי **בסיסי** של Cisco שנקרא ACL = Access Control Lists ותפקידו לסנן (פילטר) את תעבורת הרשת לפי הגדרות מראש, וכך לחסוך תעבורת רשת מיותרת, הפחתת העומס על ה-Firewall והגנה ראשונית בפני פריצה.

ACL יכול לבחון את מקור המידע, יעד המידע, סוג הפרוטוקול הנמצא בשימוש, חסימת מעבר מידע בין מחלקות שונות, וכן פרטים נוספים לפי הגדרה של מנהל הרשת.

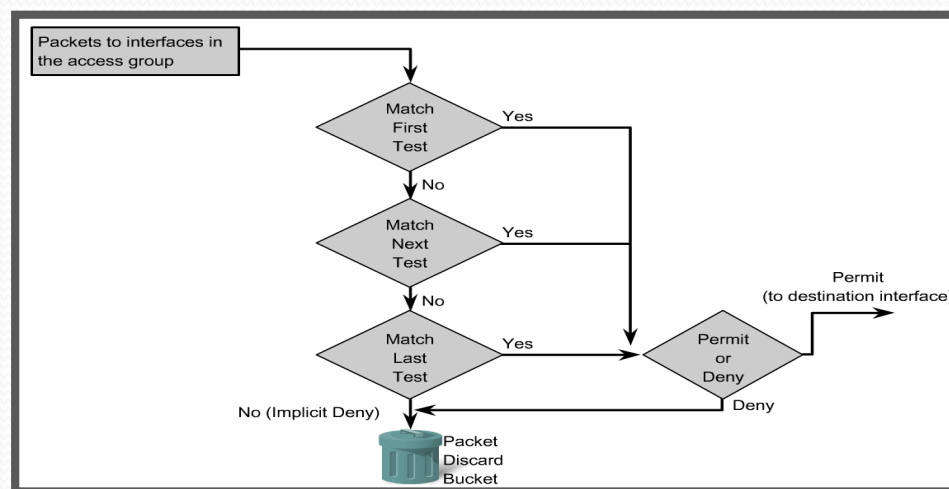
Access Control Lists (ACL)

ACL מתפקד כמו Firewall בסיסי שעובד בשיטת Packet Filtering ומאפשר שליטה בתעבורת רשת נכנסת/יוצאת.

בנוסף ACL משפר את ביצועי הרשת על ידי הפחתת תעבורת רשת מיותרת. כל Packet שנכנס לנתב נבדק אם הוא משתייך לחוק מסויים ואז מופעל עליו החוק (נחסם או עובר בהתאם לחוק)

אם בסופו של דבר לא ימצא אף חוק שחל עליו ה- packet הוא יזרק. החוק האחרון בכל Access-list נוצר אוטומטית וחוסם הכול (Deny Any Any החוק לא נראה).

שימו לב, ההגדרה של in\out (נכנס\יוצא) היא מנקודת מבטו של הנתב המוגדר!



שימוש ב- ACL דורש תכנון מקדים, תכנון לא נכון יכול ליצור עומס על הנתב, והגדרה לא נכונה או מיקום ACL בממשק או נתב לא נכונים יכול לגרום לחסימת מידע חיוני.

שלבי התכנון:

- (1) בדוק מהם דרישות הארגון (דרישות אלו יקבעו איזה סוג תעבורה יעבור/יחסם).
- (2) איזה סוג של ACL יתאים לדרישות (Standard ACL או Extended ACL).
- (3) באיזה נתב, ממשק וכיוון יפעל ACL.

כללים חשובים:

- הצמד ACL לאחד מממשקי הנתב ובדוק תעבורה נכנסת (Inbound) או יוצאת מהנתב (Outbound). **ניתן להצמיד רק ACL אחד לכל כיוון, אחד ליציאה ואחד לכניסה!**
- תעבורה שנוצרת על-ידי הנתב לא נחסמת על ידי ACL של אותו נתב.
- כדי ליעל את הבדיקה, להפחית עומסים ולשחרר את המידע בהקדם, קבע את החוקים שמתייחסים **למרבית** התעבורה ראשונים.
- לא ניתן לבצע שינויים ב- ACL אלא למחוק וליצור מחדש את הרשימה. כדי להקל על העריכה, כתוב את חוקי ACL בכתבן ולאחר מכן, העתק אותם לנתב.

Standard ACL

מאפשר או חוסם Packet רק תוך התאמה לכתובת IP/רשת של המקור.
לא ניתן לציין Port.

Standard ACL מתייחס רק לכתובת המקור ול-wildcard שלו, הוא לא מתייחס ליעד ולכן בדרך כלל ממוקם בנתב הקרוב ליעד.
לכל ACL יש מספר, מספר הרשימה של Standard ACL יכול להיות בטווחים 1-99 או 1300-1999.

הגדרת Standard ACL (שימו לב לשימוש ב-Wildcard)

```
Router(config)# access-list {access-list-number} {deny|permit}  
{source address} {source-wildcard}
```

לאחר חסימה חשוב להוסיף בסוף רשימת הגישה את האפשרות למעבר לכל שאר המקרים!

```
Router(config)# access-list {Number} permit any
```


Wildcard masks

משמש כתחליף ל-subnet mask.

0 מייצג bit שאסור לשנות (כתובת רשת) ו 1 מייצג bit שניתן לשנות (כתובת המחשב).

Wildcard mask that permits a range of hosts for a /24 network:

172.16.22.0 0.0.0.255

Wildcard mask that permits an entire /16 network:

172.16.0.0 0.0.255.255

Wildcard mask that permits an entire /8 network:

10.0.0.0 0.255.255.255

Host parameter

R1(config)#access-list 9 deny 192.168.15.99 0.0.0.0 במקום

R1(config)#access-list 9 deny host 192.168.15.99 נרשום

Any parameter

R1(config)#access-list 9 permit 0.0.0.0 255.255.255.255 במקום

R1(config)#access-list 9 permit any נרשום

Remark – מוסיף הערה ל-Access-List לדוגמה:

Router(config)# access-list Eli remark - this is the inside admin address

שיוך ACL לממשק

```
R1(config-if)#ip access-group {access-list-number | access-list-name} {in | out}
```

```
R1(config)# interface FastEthernet 0/0  
R1(config-if)# ip access-group 1 out
```

לראות פרוט של ACLs

```
Router#show access-list  
Router#show access-lists  
Standard IP access list 10  
deny host 172.17.0.1 (1 match(es))  
permit any (1 match(es))
```

הסרת ACL מממשק

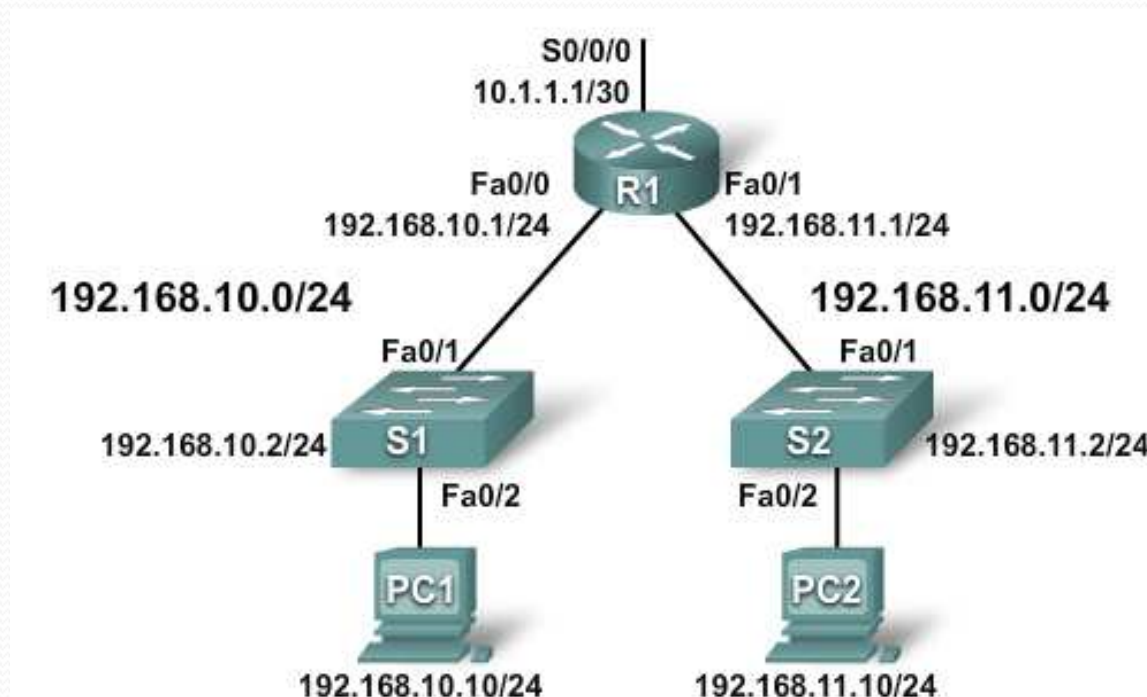
```
R1(config-if)#no ip access-group {access-list-number | access-list-name} {in | out}
```

מחיקת ACL

```
R1(config)#no access-list [access list number]
```

הצגת ה- Access-List הפעילים כרגע

```
R1#show running-config access-list
```



```
R1(config)#access-list 1 deny 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#interface S0/0/0
R1(config-if)#ip access-group 1 out
```


Named ACL

ACL מסוג Standard או Extended שמזוהה על-ידי שם ולא על-ידי מספר.

השלבים בשימוש ב-Named ACL:

1. יצירת Named ACL

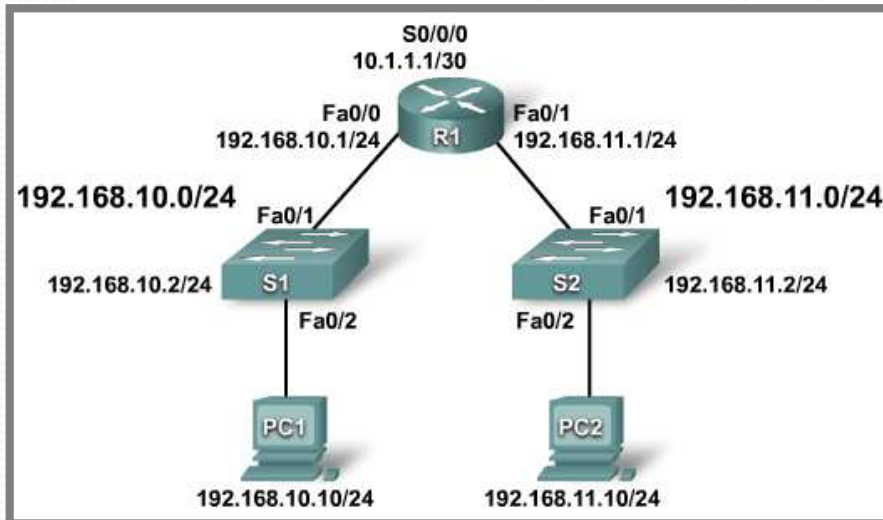
```
Router(config)# ip access-list [standard | extended] name
```

2. יצירת חוקים

```
Router(config-std-nacl)# [permit | deny | remark] {source [source-wildcard]} [log]
```

3. שיוך ACL לממשק

```
Router(config-if)#ip access-group name [in | out]
```



```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
```

עריכת Named ACL

היתרון הגדול ביותר בשימוש ב- Named ACL, זה היכולת לבצע שינויים ב- ACL.

בדיקה:

```
R1# show access-lists
```

```
Standard IP access list WEBSERVER
```

```
10 permit 192.168.10.10
```

```
20 deny 192.168.10.0, wildcard bits 0.0.0.255
```

```
30 deny 192.168.11.0, wildcard bits 0.0.0.255
```

עריכה:

```
R1(config)# ip access-list standard WEBSERVER
```

```
R1(config-std-nacl)# 15 permit host 192.168.11.10
```

בדיקה:

```
R1# sho access-lists
```

```
Standard IP access list WEBSERVER
```

```
10 permit 192.168.10.10
```

```
15 permit 192.168.11.10
```

```
20 deny 192.168.10.0, wildcard bits 0.0.0.255
```

```
30 deny 192.168.11.0, wildcard bits 0.0.0.255
```

פתח את הקובץ Configuring Standard ACLs.pka ועקוב אחרי ההוראות.

Task 1: Investigate the Current Network Configuration

Step 1. View the running configuration on the routers.

Step 2. Confirm that all devices can access all other locations.

Task 2: Evaluate a Network Policy and Plan an ACL Implementation

Step 1. Evaluate the policy for the R1 LANs.

Step 2. Plan the ACL implementation for the R1 LANs.

Step 3. Evaluate the policy for the R3 LAN.

Step 4. Plan the ACL implementation for the R3 LAN.

Task 3: Configure Numbered Standard ACLs

Step 1. Determine the wildcard mask.

Step 2. Determine the statements.



Step 3. Apply the statements to the interfaces.

Step 4. Verify and test ACLs.

Step 5. Check results.

Task 4: Configure a Named Standard ACL

Step 1. Determine the wildcard mask.

Step 2. Determine the statements.

Step 3. Apply the statements to the correct interface.

Step 4. Verify and test ACLs.

Step 5. Check results.

Extended ACL

מאפשר או חוסם Packet לפי כתובת המקור או היעד (בניגוד למקור בלבד ב-Standard), וכן לפי פרוטוקול ומספר Port. (אין ב-Standard) מספרי הרשימה של Extended ACL יכולים להיות בטווחים 100-199 ו-2000-2699.

בדרך כלל נמקם את ה-Extended ACL קרוב למקור וכך נמנע ממידע מיותר לעבור ברשת.

גם כאן חשוב להוסיף בסוף רשימת הגישה את האפשרות למעבר לכל שאר המקרים!

```
Router(config)# access-list {Number\Name} permit any any
```

הגדרת Extended ACL

```
Router (config)#access-list {access-list-number} {permit | deny} protocol  
source source-wildcard [operator port] destination destination-wildcard  
[operator port] [established] [log]
```

Command Parameters	Descriptions
access-list	Main command
access-list-number	Identifies the list using a number in the ranges of 100–199 or 2000– 2699.
permit deny	Indicates whether this entry allows or blocks the specified address.
protocol	IP, TCP, UDP, ICMP, GRE, or IGRP.
source and destination	Identifies source and destination IP addresses.
source-wildcard and destination-wildcard	The operator can be lt (less than), gt (greater than), eq (equal to), or neq (not equal to). The port number referenced can be either the source port or the destination port, depending on where in the ACL the port number is configured. As an alternative to the port number, well-known application names can be used, such as Telnet, FTP, and SMTP.
established	For inbound TCP only. Allows TCP traffic to pass if the packet is a response to an outbound-initiated session. This type of traffic has the acknowledgement (ACK) bits set. (See the Extended ACL with the Established Parameter example.)
log	Sends a logging message to the console.

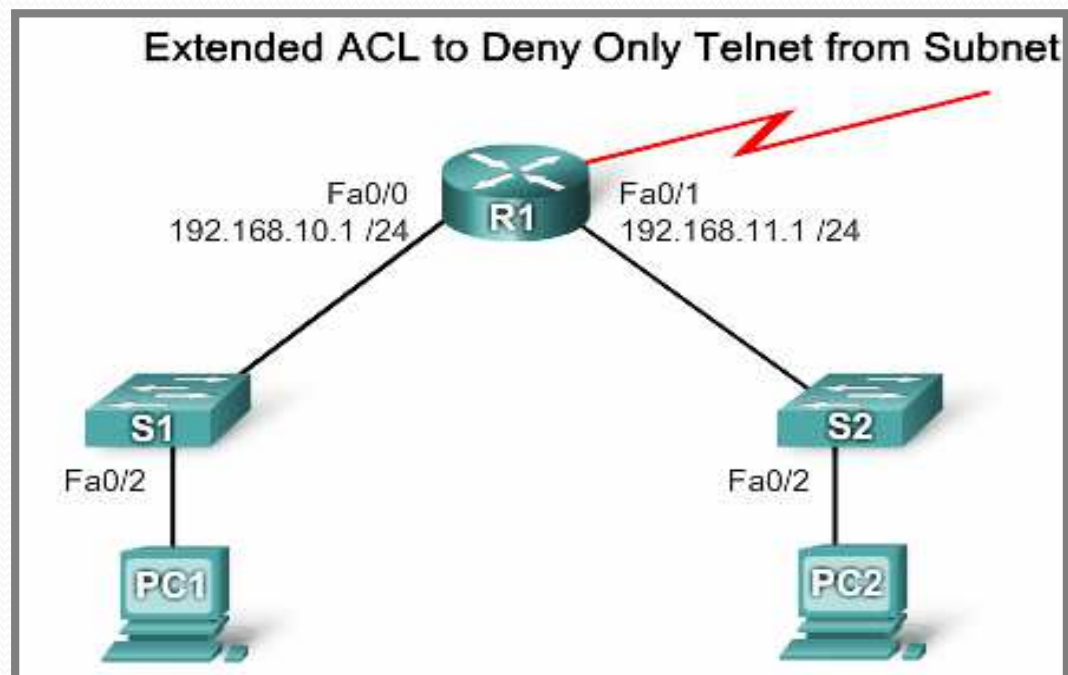
- **EQ** (equal to) = שווה ל...מציינים פורט בודד
- **GT** (greater than) = גדול מ..לדוגמה כל מה שמעל לפורט מס' 1300
- **LT** (less than) = קטן מ.. לדוגמה כל מה שמתחת לפורט 150
- **NEQ** (not equal to) = חוסמים\מאפשרים הכל חוץ מהפורט שצויין
- **Range** = טווח של פורטים

חשוב לדעת שלכל פרוטוקול יש מספר Port Number, לרשימה המלאה בוויקיפדיה:
https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
להלן רשימה של הפרוטוקולים המוכרים ביותר:

Well-Known Port Numbers and IP Protocols

Port Number	IP Protocol
20 (TCP)	FTP data
21 (TCP)	FTP control
23 (TCP)	Telnet
25 (TCP)	Simple Mail Transfer Protocol (SMTP)
53 (TCP/UDP)	Domain Name System (DNS)
69 (UDP)	TFTP
80 (TCP)	HTTP

דוגמה:



```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 any eq 23
R1(config)#access-list 101 permit ip any any

R1(config)#interface Fa0/1
R1(config-if)#ip access-group 101 in
```


פתח את הקובץ Configuring Extended ACLs.pka ועקוב אחר ההוראות.

Task 1: Investigate the Current Network Configuration

Step 1. View the running configuration on the routers.

Step 2. Confirm that all devices can access all other locations.

Task 2: Evaluate a Network Policy and Plan an ACL Implementation

Step 1. Evaluate the policy for the R1 LANs.

Step 2. Plan the ACL implementation for the R1 LANs.

Step 3. Evaluate the policy for the R3 LAN.

Step 4. Plan the ACL implementation for the R3 LAN.

Step 5. Evaluate the policy for traffic coming from the Internet via the ISP.

Step 6. Plan the ACL implementations for traffic coming from the Internet via the ISP.

Task 3: Configure Numbered Extended ACLs

- Step 1. Determine the wildcard masks.
- Step 2. Configure the first extended ACL for R1.
- Step 3. Configure the second extended ACL for R1.
- Step 4. Verify the ACL configurations.
- Step 5. Apply the statements to the interfaces.
- Step 6. Test the ACLs configured on R1.
- Step 7. Check results.

Task 4: Configure a Numbered Extended ACL for R3

- Step 1. Determine the wildcard mask.
- Step 2. Configure the extended ACL on R3.
- Step 3. Apply the statement to the interface.
- Step 4. Verify and test ACLs.
- Step 5. Check results.

Task 5: Configure a Named Extended ACL

Step 1. Configure a named extended ACL on R2.

Step 2. Apply the statement to the interface.

Step 3. Verify and test ACLs.

Step 4. Check results.

לצורך תרגול נוסף בבית, העליתי לכם קובץ בשם `Extended_ACL.pkt`
אתם מוזמנים לחפש פרוטוקולים נוספים ולחסום אותם.

חובה לעשות סימולציות באתר gtut או בכוון!

<http://www.gtut.com/70-ccna-access-list-sim>

וגם

<http://www.gtut.com/78-ccna-access-list-sim-2>

סימולציה 2 CCNA Access List Sim 2

A network associate is adding security to the configuration of the Corp1 router.

The user on host C should be able to use a web browser to access financial information from the Finance Web Server.

No other hosts from the LAN nor the Core should be able to use a web browser to access this server.

Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server.

No other hosts will have web access to the Finance Web Server.

All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to “cisco”.

The Core connection uses an IP address of 198.18.196.65



The computers in the Hosts LAN have been assigned addresses of

192.168.33.1 – 192.168.33.254

Host A 192.168.33.1

Host B 192.168.33.2

Host C 192.168.33.3

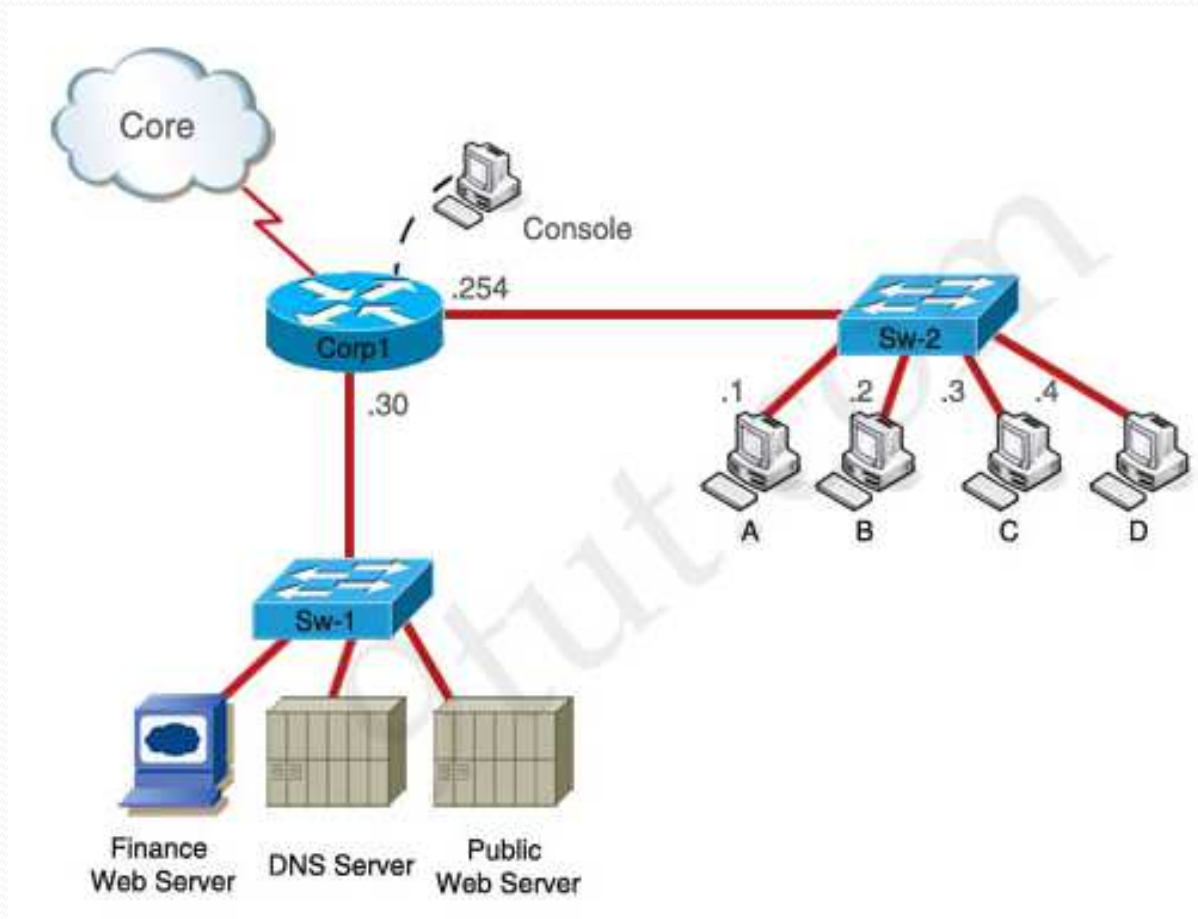
Host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of

172.22.242.17 – 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23.

The Public Web Server is assigned an IP address of 172.22.242.17



הורד את הקובץ Access-list_sim2.pkt מהכונן ופתור לפי הדרישות שנתבקשת בשאלה.

שים לב בסימולציה במבחן תקבל רק 5 שורות לכתובת הפקודות

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 –

192.168.33.254

Host A 192.168.33.1

Host B 192.168.33.2

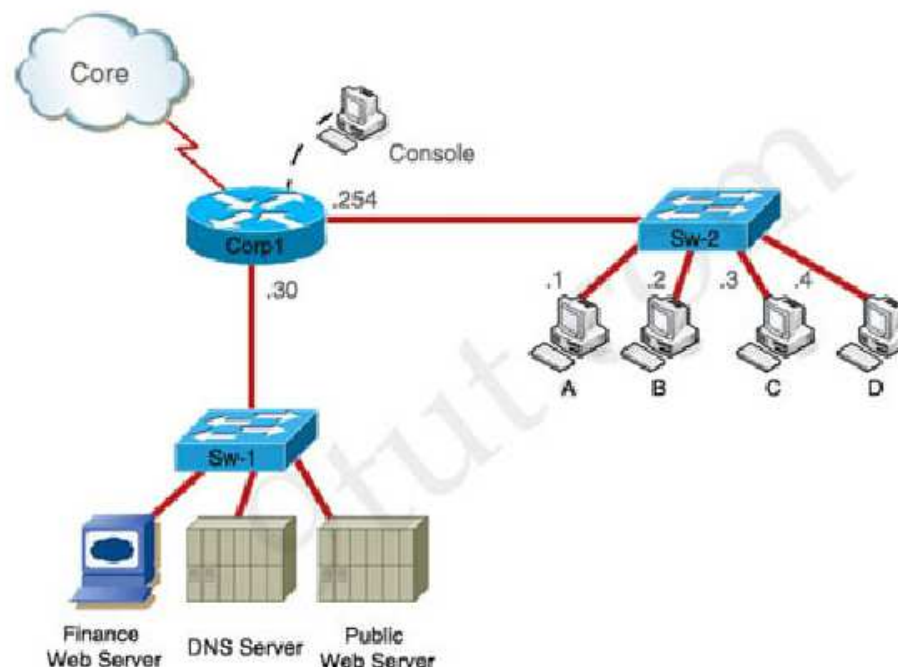
Host C 192.168.33.3

Host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 – 172.22.242.30

The Finance Web Server: 172.22.242.23.

The Public Web Server: 172.22.242.17



Corp1#show running-config

Three statements of access list:

Corp1(config)# (1)

Corp1(config)# (2)

Corp1(config)# (3)

Apply to interface:

Corp1(config)# (4)

Corp1(config-if)# (5)

Question 1

Which item represents the standard IP ACL?

- A. access-list 50 deny 192.168.1.1 0.0.0.255
- B. access-list 110 permit ip any any
- C. access-list 2500 deny tcp any host 192.168.1.1 eq 22
- D. access-list 101 deny tcp any host 192.168.1.1

תשובה A, הטווח שלה- Standard access lists הוא 1-99 וגם 1300-1999 ולכן רק תשובה A נמצאת בטווח.

Question 2

A network administrator is configuring ACLs on a Cisco router, to allow traffic from hosts on networks 192.168.146.0, 192.168.147.0, 192.168.148.0, and 192.168.149.0 only. Which two ACL statements, when combined, would you use to accomplish this task? (Choose two)

- A. access-list 10 permit ip 192.168.146.0 0.0.1.255
- B. access-list 10 permit ip 192.168.147.0 0.0.255.255
- C. access-list 10 permit ip 192.168.148.0 0.0.1.255
- D. access-list 10 permit ip 192.168.149.0 0.0.255.255
- E. access-list 10 permit ip 192.168.146.0 0.0.0.255
- F. access-list 10 permit ip 192.168.146.0 255.255.255.0

Question 4

On which options are standard access lists based?

- A. destination address and wildcard mask
- B. destination address and subnet mask
- C. source address and subnet mask
- D. source address and wildcard mask

Question 5

תשובה D

Refer to the exhibit.

ACL 10

Statements are written in this order:

- A. permit any
- B. deny 172.21.1.128 0.0.0.15
- C. permit 172.21.1.129 0.0.0.0
- D. permit 172.21.1.142 0.0.0.0

Statements A, B, C, and D of ACL 10 have been entered in the shown order and applied to interface E0 inbound, to prevent all hosts (except those whose addresses are the first and last IP of subnet 172.21.1.128/28) from accessing the network. But as is, the ACL does not restrict anyone from the network. How can the ACL statements be re-arranged so that the system works as intended?

- A. ACDB
- B. BADC
- C. DBAC
- D. CDBA

Question 6

Which statement about access lists that are applied to an interface is true?

- A. you can apply only one access list on any interface
- B. you can configure one access list, per direction, per layer 3 protocol
- C. you can place as many access lists as you want on any interface
- D. you can configure one access list, per direction, per layer 2 protocol

תשובה B