

פרויקט מסכם CCNA

תוכן עניינים

3	טופולוגיה
4	הגדרות בסיסיות
4	הגדרת שם למתג/נתב
4	הגדרת סיסמת גישה ל-Console ול-Telnet
5	הגדרות סיסמאות גישה מוצפנות ל-Privileged Mode
6	הצפנת כלל הסיסמאות שהוכנסו או יוכנסו בעתיד
6	הגדרת Login Banner
7	סנכרון הודעות למסך
7	מניעת תקיעה בעת הקלדה של פקודה שגויה
8	הגדרת VLAN
8	יצירת VLANs במתג 0,1,3
8	שיוך ממשקים ל-VLANs
9	הגדרת DHCP Server ברשת LAN1
10	הגדרת LAN2
13	הגדרת רשת אלחוטית Wireless
15	הגדרת Port Security
15	הגדרת OSPF
17	הגדרת ניהול ציוד התקשורת מרחוק
17	הגדרת ACL
18	הגדרת NAT
19	גלישה לשרת WEB
20	HSRP
21	EtherChannel+STP
23	Syslog

מטלת בונוס.....25

הגדרות בסיסיות

הגדרת שם למתג/נתב

1. הגדרת שם לכל מתג/נתב – שם ההתקן צריך לכלול את השם הפרטי שלי

הגדרות לנתב:

```
enable
configure terminal
hostname Adir-R1
```

הגדרות למתג:

```
enable
configure terminal
hostname Adir-SW1
```

הגדרת סיסמת גישה ל-Console ול-Telnet

2. הגדרת סיסמת גישה ל-Console ול-Telnet. (יש להשתמש בפורמט סיסמא השם שלי + abcd).

הגדרות לנתב:

```
enable
configure terminal
line console 0
password adirabcd
line vty 0 4
password adirabcd
```

כאשר ב Line Vty או לא מכריחים את ההתחברות לעבוד ב SSH או Telnet מאפשר. יש לציין שמומלץ להתחבר ב SSH לרכיב התקשורת(חיבור מאובטח ואמין יותר מ Telnet).

הגדרות למתג:

```
enable
configure terminal
line console 0
password adirabcd
line vty 0 4
password adirabcd
```

הגדרות סיסמאות גישה מוצפנות ל-Privileged Mode

יש להשתמש בפורמט סיסמא השם הפרטי + 1234

הגדרות במתג:

```
enable
configure terminal
enable password adir1234
```

הגדרות בנתב:

```
enable
configure terminal
enable password adir1234
```

הצפנת כלל הסיסמאות שהוכנסו או יוכנסו בעתיד

הגדרות במתג:

```
enable
configure terminal
service password-encryption
```

הגדרות בנתב:

```
enable
configure terminal
service password-encryption
```

הגדרת Login Banner

ההגדרה תכיל את השם שלי ומזהיר משתמשים לא מורשים שלא להתחבר להתקן.

הגדרות במתג:

```
enable
configure terminal
banner motd #Adir-Unauthorized access to this device is prohibited!#
```

הגדרות בנתב:

```
enable
configure terminal
banner motd #Adir-Unauthorized access to this device is prohibited!#
```

סנכרון הודעות למסך

סנכרון הודעות שהנתב/מתג שולח למסך, כך שלא יפריעו לכתיבת פקודות.

הגדרות במתג:

```
enable
configure terminal
line con 0
logging synchronous
```

הגדרות הנתב:

```
enable
configure terminal
line con 0
logging synchronous
```

מניעת תקיעה בעת הקלדה של פקודה שגויה

הגדרות במתג:

```
enable
configure terminal
no ip domain-lookup
```

הגדרות בנתב:

```
enable
configure terminal
no ip domain-lookup
```

הגדרת VLAN

יצירת VLANs במתג 0,1,3

יש ליצור VLANs במתג 0,1,3 – שם+ID לכל VLAN

הגדרות במתג:

```
Enable
Configure terminal
Vlan 10
name VLAN10
Vlan 20
name VLAN20
```

שיוך ממשקים ל-VLANs

יש לשייך את הממשקים שבמתגים ל-VLANs המתאימים

הגדרות במתג- SW0-Adir# :

```
enable
configure terminal
interface range fastEthernet 0/3-4
switchport mode access
switchport access vlan 10
interface fastEthernet 0/5
switchport mode access
switchport access vlan 20
```


הגדרות במתג-SW1-Adir# :

```
enable
configure terminal
!
interface range fastEthernet 0/2-3
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
!
```

הגדרת DHCP Server ברשת LAN1

ברשת LAN1, הגדר את Router0 כ-DHCP Server.

- צור DHCP Pool שישמש את VLAN10 (השתמש בכתובת רשת 192.168.10.0/24)
- צור DHCP Pool שימש את VLAN20 (השתמש בכתובת רשת 192.168.20.0/24).
- הגדר לכל DHCP Pool שמלבד לחלק כתובות IP, הוא ילמד את ה-Clients גם מיהו ה-Default Gateway.
- הגדר בנתב שני תתי ממשקים לשימוש VLAN10 ו-VLAN20.

הגדרת בנתב Router0 עבור שירות ה-DHCP:

```
Enable
configure terminal
ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.0
default-router 192.168.10.254
dns-server 172.19.0.100
ip dhcp pool VLAN20
network 192.168.20.0 255.255.255.0
default-router 192.168.20.254
```

dns-server 172.19.0.100

הגדרות עבור תתי הממשקים של VLAN 10 ו VLAN 20:

Enable

configure terminal

!

interface GigabitEthernet0/0/1.10

encapsulation dot1Q 10

ip address 192.168.10.254 255.255.255.0

!

interface GigabitEthernet0/0/1.20

encapsulation dot1Q 20

ip address 192.168.20.254 255.255.255.0

!

כלל המחשבים ברשת LAN1 מקבלים כתובת IP בצורה דינאמית ע"י ה Pools שהוגדרו בנתב Router0.

הגדרת LAN2

הגדר לשרתים ולנתב ב-LAN2, כתובת IP בצורה ידנית לפי כתובת רשת 172.19.0.0/16.

- הכתובת של השרת DNS תהיה 172.19.0.100/16
- הכתובת של השרת WEB תהיה 172.19.0.200/16
- צור בשרת DNS רשומה בשם www.adir.com הרשומה תייצג את השרת WEB.

הגדרות בנתב-R2-Adir# :

enable

configure terminal

!

interface GigabitEthernet0/0/0

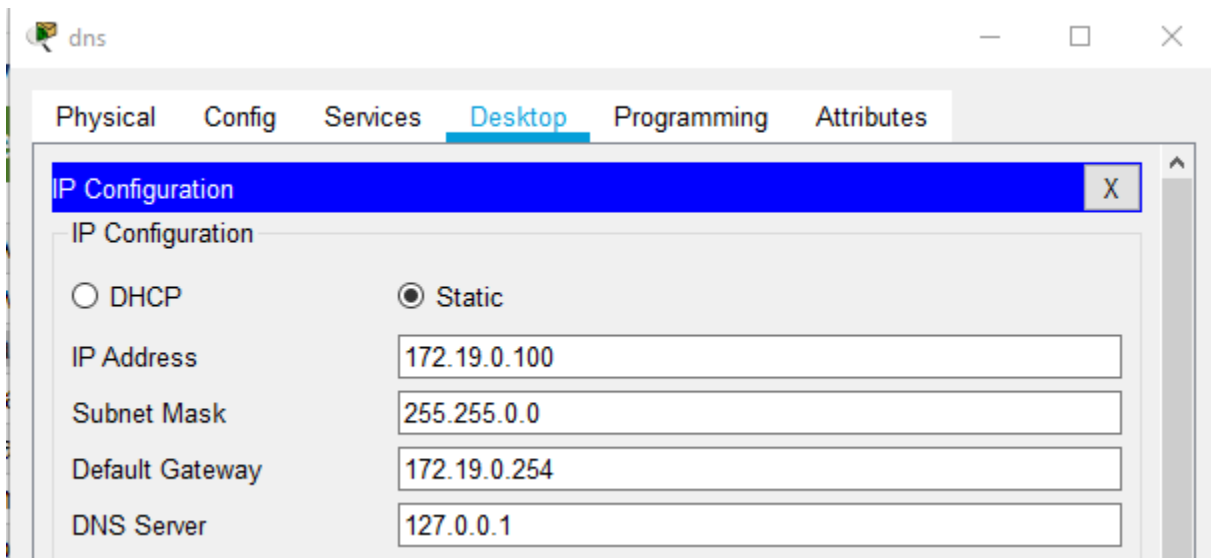
ip address 172.19.0.254 255.255.255.0

duplex auto

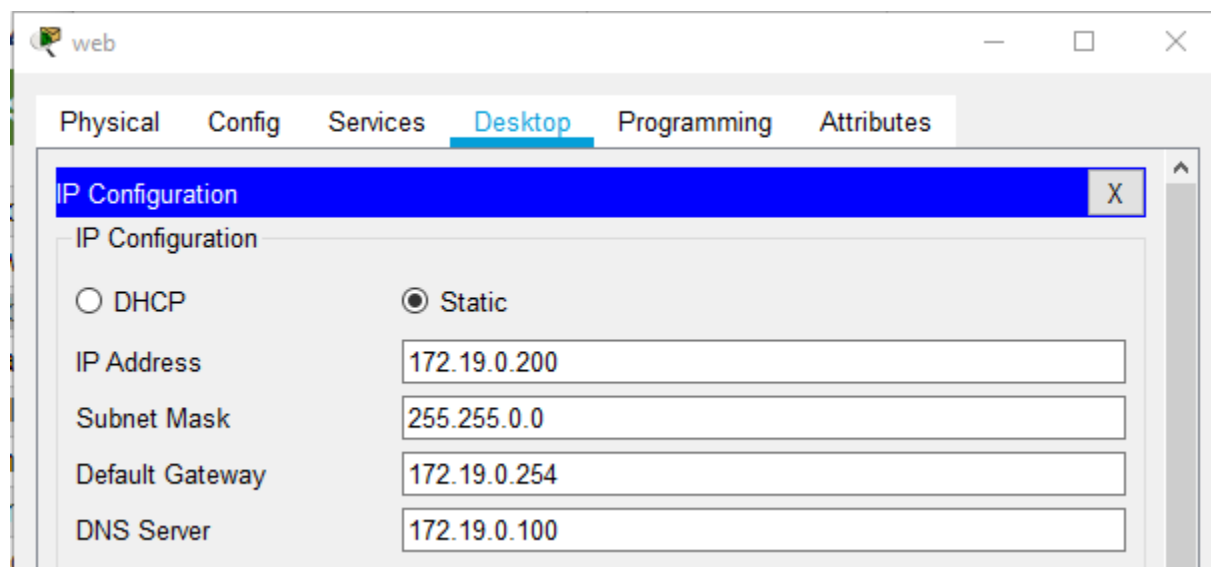
speed auto

!

הגדרות רשת ידניות בשרת ה-DNS:



הגדרות רשת ידניות בשרת ה-WEB:



הפעלת שירות DNS והגדרת רשומה עבור www.adir.com

dns

Physical

Config

Services

Desktop

Programming

Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DNS

DNS Service

☒ On
☐ Off

Resource Records

Name

Type

A Record

Address

Add

Save

Remove

No.	Name	Type	Detail
0	www.adir.com	A Record	172.19.0.200

DNS Cache

☐ Top

הגדרת רשת אלחוטית Wireless

הגדר את Wireless LAN Controller 1 כבקר רשת אלחוטית:

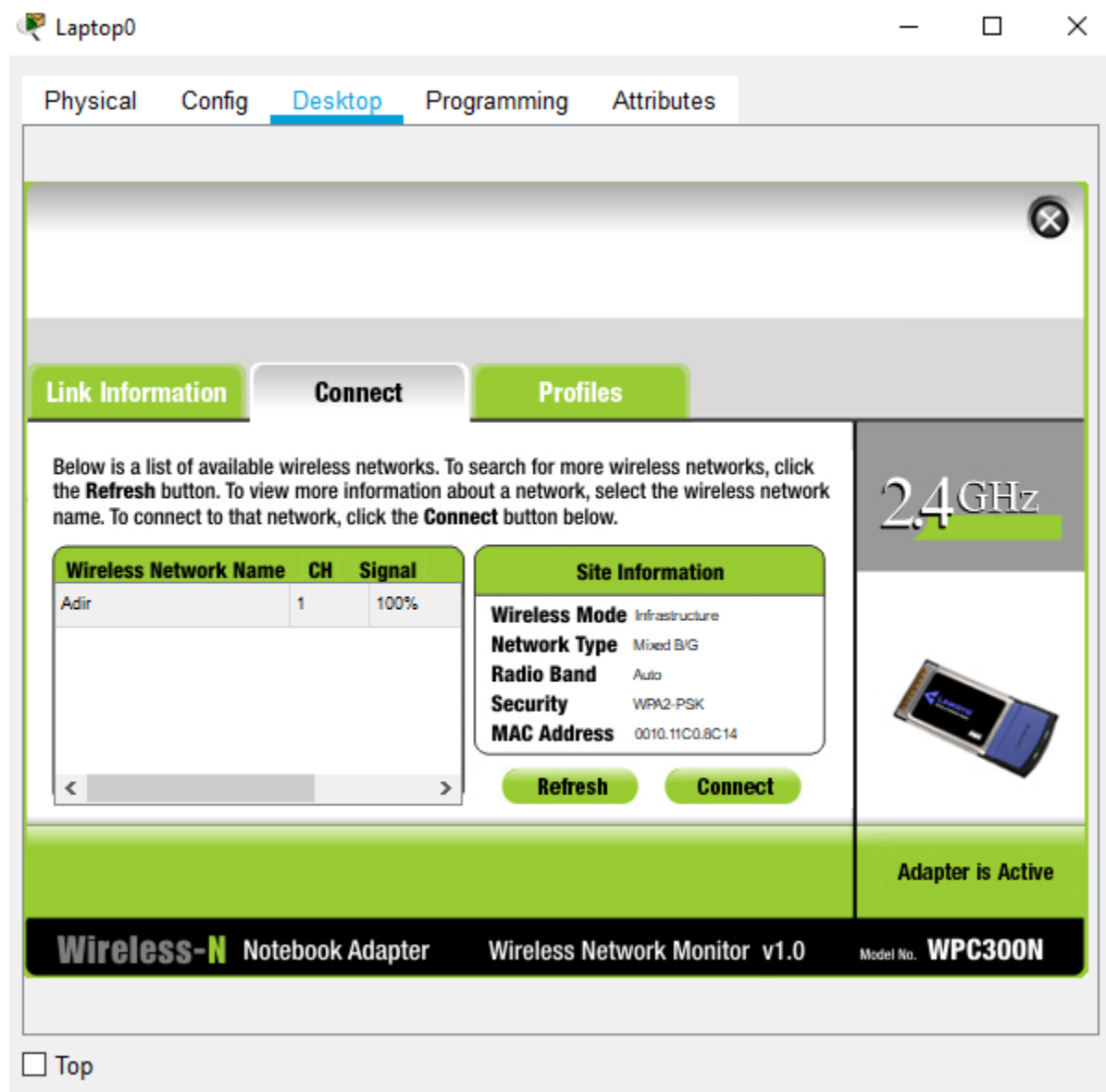
- Adir עם השם SSID
- הצפן סיסמא Abcd1234
- הגדר את Access Point0 כחלק מהרשת האלחוטית
- חבר את המחשב הנייד לרשת האלחוטית דרך Access Point0
- הרשת האלחוטית תהיה מחוברת ל VLAN10

The screenshot shows the configuration window for Wireless LAN Controller1-Adir. The 'Config' tab is selected, and the 'Wireless LANs' section is highlighted in the left sidebar. The main configuration area shows the following settings:

- Select WLAN:** Adir
- Name:** Adir
- SSID:** (empty field)
- VLAN:** 10
- Authentication:**
 - ☐ Disabled
 - ☐ WEP
 - ☒ WPA2-PSK PSK Pass P Abcd1234
 - ☐ WPA
 - ☐ WPA2
- RADIUS Server Settings:**
 - IP Address: (empty field)
 - Shared Secret: (empty field)
- Encryption Type:** AES
- Central Contr:**
 - ☒ Central switching, central auther
 - ☐ Local switching, central authenti
 - ☐ Local switching, local authentica

At the bottom of the configuration area are buttons for 'New', 'Remove', and 'Save'. A 'Top' button is located at the bottom left of the window.

התחברות בהצלחה של הלפטופ ל AP:



הגדרת Port Security

יש להגדיר port security במתג Switch4 שנמצא בחדר שרתים.

- חסום את הממשקים שלא בשימוש בכדי שלא ניתן יהיה לחבר מחשב לא מורשה.
- דאג לכך שלא ניתן יהיה לחבר מחשב חליפי בחוות שרתים.
- מצב הפרה יהיה Restrict.

הגדרות במתג:

```
!  
interface FastEthernet0/1  
switchport port-security mac-address sticky  
switchport port-security violation restrict  
!  
interface FastEthernet0/2  
switchport port-security mac-address sticky  
switchport port-security violation restrict  
!
```

הגדרת OSPF

הוגדר Process ID 1 ופרסום כלל הרשתות המחוברות ב Connected.

לדוגמא:

```
router ospf 1  
log-adjacency-changes  
network 172.19.0.0 0.0.255.255 area 0  
network 209.165.200.0 0.0.0.255 area 0  
!
```

```
R2-Adir#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
209.165.200.2	1	FULL/BDR	00:00:30	209.165.200.2	GigabitEthernet0/0/1

```
R2-Adir#
```

יש פינג מהמחשבים ב LAN1 אל מול השרתים ב LAN2

```
C:\>ping 172.19.0.200
```

```
Pinging 172.19.0.200 with 32 bytes of data:
```

```
Reply from 172.19.0.200: bytes=32 time=8ms TTL=125
```

```
Reply from 172.19.0.200: bytes=32 time=1ms TTL=125
```

```
Reply from 172.19.0.200: bytes=32 time=1ms TTL=125
```

```
Reply from 172.19.0.200: bytes=32 time=1ms TTL=125
```

```
Ping statistics for 172.19.0.200:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 8ms, Average = 2ms
```

```
C:\>ping 172.19.0.100
```

```
Pinging 172.19.0.100 with 32 bytes of data:
```

```
Reply from 172.19.0.100: bytes=32 time=1ms TTL=125
```

```
Reply from 172.19.0.100: bytes=32 time=2ms TTL=125
```

```
Reply from 172.19.0.100: bytes=32 time=1ms TTL=125
```

```
Reply from 172.19.0.100: bytes=32 time=1ms TTL=125
```

```
Ping statistics for 172.19.0.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\>
```


הגדרת ניהול ציוד התקשורת מרחוק

איפשור SSH בכלל ציוד התקשורת.

- ניתן לנהל את הציוד רק דרך המחשבים שמחוברים לרשת דרך VLAN10.

יוגדר interface vlan 10 עם כתובת ניהולית באותו סגמנט. רק VLAN 10 יוכלו לגשת לכתובת זו ולנהל את המתג.

```
!  
ip ssh version 2  
no ip domain-lookup  
ip domain-name adir.com  
!  
Crypto key generate rsa  
#1024#  
username adir secret 5 $1$mERr$a2JiYkp15DZLPxxk0.JXG/  
!  
!  
interface Vlan10  
mac-address 00e0.b066.ed01  
ip address 192.168.10.240 255.255.255.0  
!  
!  
line vty 0 4  
password 7 082048471B18071416  
login local  
transport input ssh  
transport output ssh
```

בנוסף, יוגדר ACL כ Access-Class עם הסגמנט של VLAN 10 בשיוך על ממשקי ה Line VTY.

הגדרת ACL

יש להשתמש ב ACL בכדי לא לאפשר תקשורת בין מחשבים ב VLAN 10 ל VLAN 20.

את ההגדרות ה ACL נכיל על הנתב R0-Adir# אשר משמש כ Default Gateway של יחידות קצה מ VLAN 10 ו 20.

```
!  
interface GigabitEthernet0/0/1.10  
encapsulation dot1Q 10  
ip address 192.168.10.254 255.255.255.0  
ip access-group 100 out  
!
```

```
access-list 100 deny ip 192.168.20.0 0.0.0.255 any  
access-list 100 permit ip any any
```

הגדרת NAT

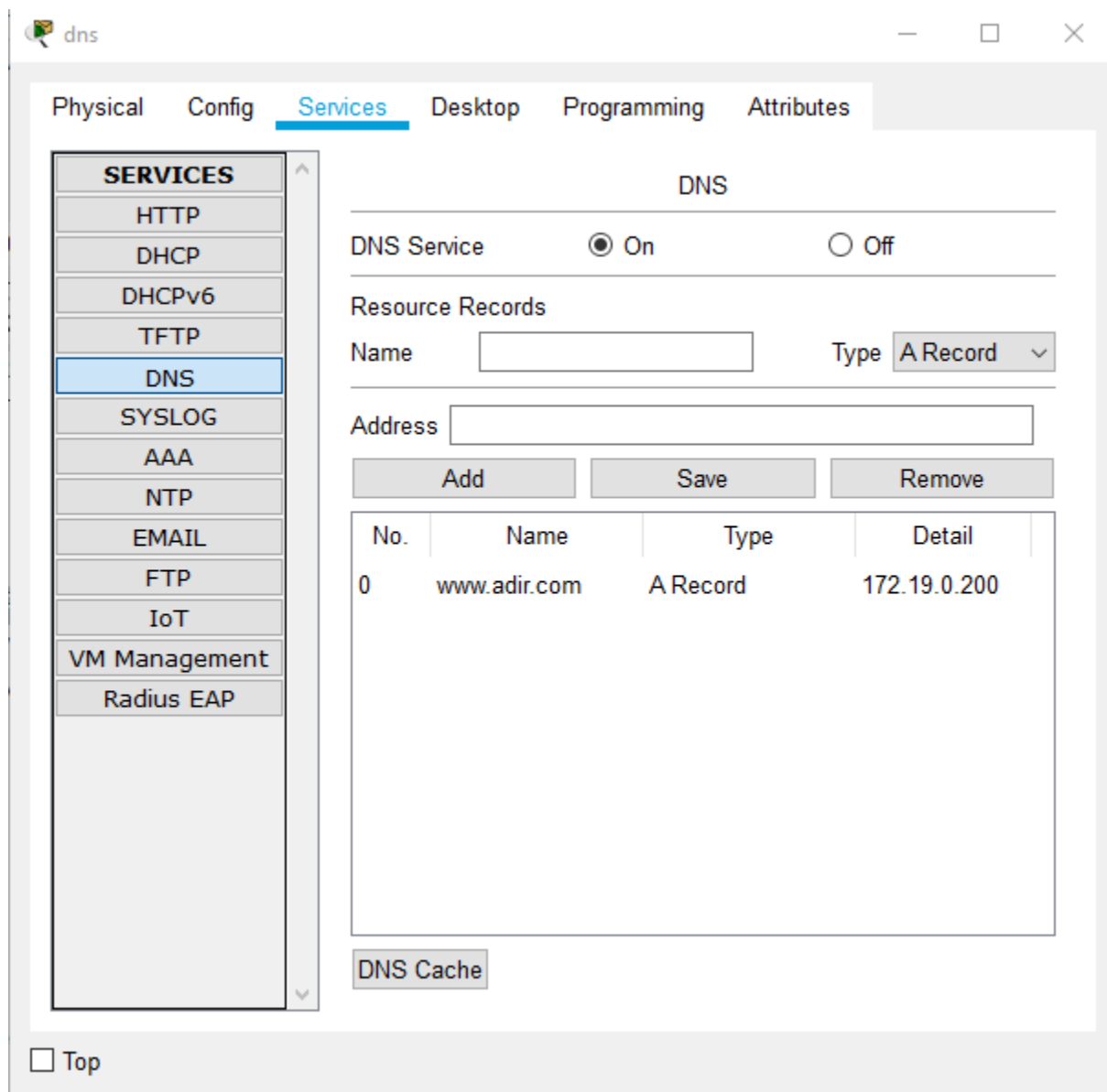
יש להגדיר תקשורת בין רשת 172.31.0.0/16 לבין LAN2 ע"י NAT. (יש להשתמש ב PAT).
הגדרת NAT בנתב 2 כדי לאפשר גישה לשרתים בחוות השרתים.

הגדרות בנתב R2-Adir#

```
!  
interface GigabitEthernet0/0/0  
ip address 172.19.0.254 255.255.255.0  
ip nat inside  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/0/1  
ip address 209.165.200.1 255.255.255.0  
ip nat outside  
duplex auto  
speed auto  
!  
  
access-list 10 permit 172.19.0.0 0.0.0.255
```

גלישה לשרת WEB

בדוק שכל המחשבים יכולים לפנות לשרת WEB מהדפדפן שלהם.



HSRP

הגדרות בנתב R3-Adir#

```
interface GigabitEthernet0/0/0
ip address 1.1.1.253 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
standby 2 ip 1.1.1.254
standby 2 priority 150
standby 2 preempt
!
interface GigabitEthernet0/0/1
ip address 10.10.10.252 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
standby 1 ip 10.10.10.254
standby 1 priority 150
standby 1 preempt
```

הגדרות על נתב 3 הגיבוי:

```
!
interface GigabitEthernet0/0/0
ip address 1.1.1.252 255.255.255.0
ip ospf 1 area 0
duplex auto
speed auto
standby 2 ip 1.1.1.254
!
interface GigabitEthernet0/0/1
ip address 10.10.10.253 255.255.255.0
ip ospf 1 area 0
```

```
duplex auto
speed auto
standby 1 ip 10.10.10.254
!
```

EtherChannel+STP

ברשת LAN3 מתג ה Root הוא מתג 7 :

```
SW7-Adir#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0060.3EAA.2D4C
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0060.3EAA.2D4C
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost          Prio.Nbr Type
-----
Fa0/1            Desg FWD 19           128.1    P2p
Fa0/2            Desg FWD 19           128.2    P2p
Fa0/3            Desg FWD 19           128.3    P2p
Fa0/4            Desg FWD 19           128.4    P2p

SW7-Adir#
```

הסיבה לכך היא שה MAC שלו הכי נמוך ולכן הוא נבחר.

הוספת הכבילה בוצעה בהצלחה ע"י הגדרה של 1 Port-Channel (איגוד מספר ממשקים פיזית לממשק לוגי אחד).

```
SW7-Adir#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
```

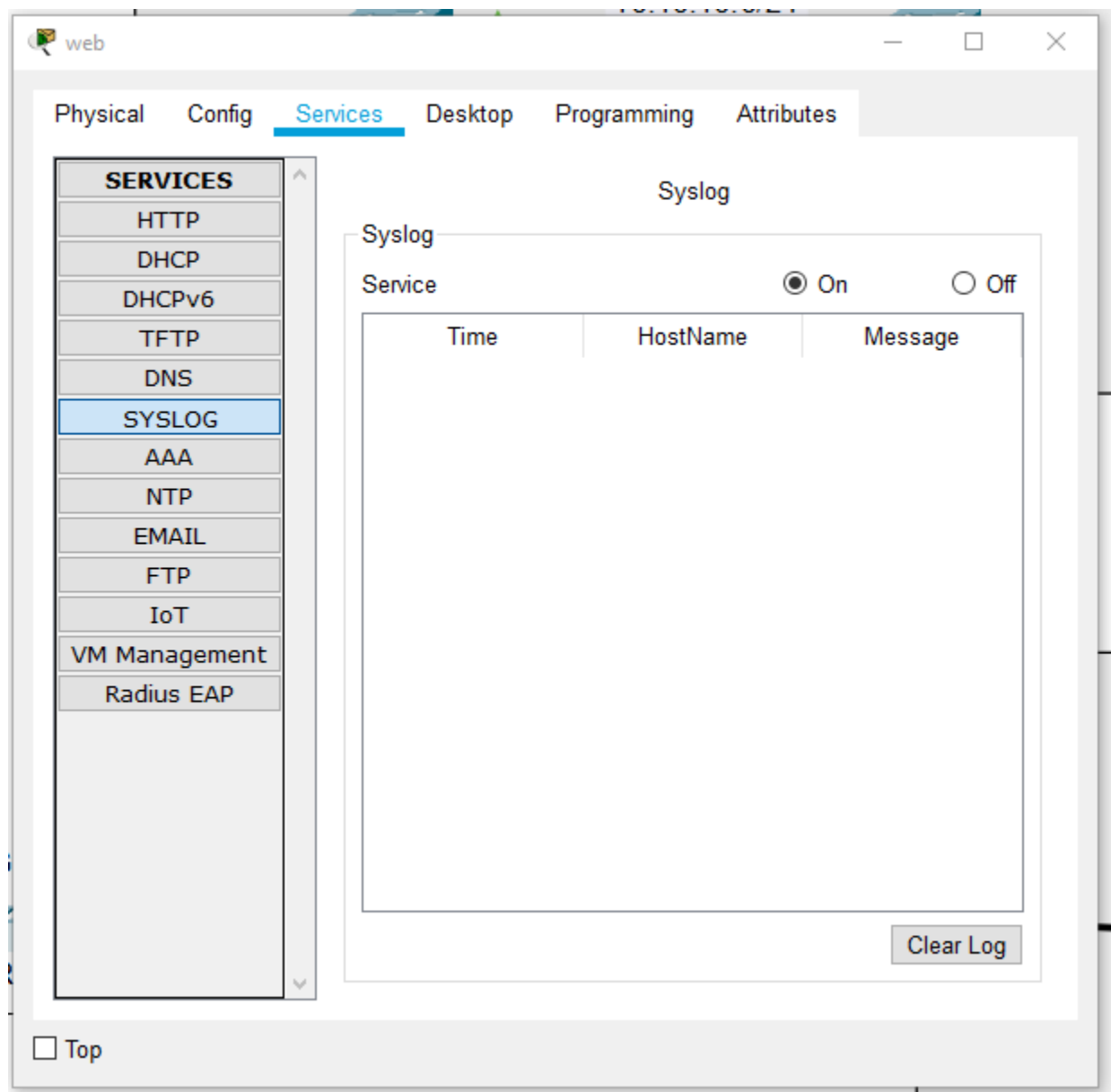
```
Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Pol(SU)	-	Fa0/3(P) Fa0/5(P) Fa0/6(P)

SW7-Adir#
SW7-Adir#
SW7-Adir#

Syslog

הגדרת שרת ה-WEB כשרת Syslog



הגדרה לנתב R2 שישלח Syslog לשרת ה-WEB שהוגדר כ Syslog

```
R2-Adir(config)#logging host 172.19.0.200
R2-Adir(config)#
R2-Adir(config)#
R2-Adir(config)#end
R2-Adir#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.19.0.200 port 514 started - CLI initiated
```

הוגדר לשלוח כל אירוע גם ברמה של Debug:

R2-Adir(config)#logging trap debugging

דוגמא לאירועים שמגיעים:

Service	Time	HostName	Message
1 -		172.19.0.254	...
2 -		172.19.0.254	...
3 -		172.19.0.254	...
4 -		172.19.0.254	...
5 -		172.19.0.254	...
6 -		172.19.0.254	...
7 -		172.19.0.254	...
8 -		172.19.0.254	...
9 -		172.19.0.254	...

מטלת בונוס

ל עודא שיש חיבור למתג 4 מ VLAN 10

לצורך כך, הוגדר Interface vlan במתג 4. בנוסף, הוגדר ACL ברמה של Access-Class על ממשקי ה LINE VTY

```
C:\>ssh -l adir 172.19.0.253
```

```
Password:
```

```
Adir-Unauthorized access to this device is prohibited!
```

```
SW4-Adir>enable
```

```
Password:
```

```
SW4-Adir#
```

```
SW4-Adir#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	unassigned	YES	manual	up	up
FastEthernet0/2	unassigned	YES	manual	up	up
FastEthernet0/3	unassigned	YES	manual	up	up
FastEthernet0/4	unassigned	YES	manual	down	down
FastEthernet0/5	unassigned	YES	manual	down	down
FastEthernet0/6	unassigned	YES	manual	down	down
FastEthernet0/7	unassigned	YES	manual	down	down
FastEthernet0/8	unassigned	YES	manual	down	down
FastEthernet0/9	unassigned	YES	manual	down	down
FastEthernet0/10	unassigned	YES	manual	down	down
FastEthernet0/11	unassigned	YES	manual	down	down
FastEthernet0/12	unassigned	YES	manual	down	down
FastEthernet0/13	unassigned	YES	manual	down	down
FastEthernet0/14	unassigned	YES	manual	down	down
FastEthernet0/15	unassigned	YES	manual	down	down
FastEthernet0/16	unassigned	YES	manual	down	down
FastEthernet0/17	unassigned	YES	manual	down	down
FastEthernet0/18	unassigned	YES	manual	down	down
FastEthernet0/19	unassigned	YES	manual	down	down
FastEthernet0/20	unassigned	YES	manual	down	down
FastEthernet0/21	unassigned	YES	manual	down	down
FastEthernet0/22	unassigned	YES	manual	down	down
FastEthernet0/23	unassigned	YES	manual	down	down
FastEthernet0/24	unassigned	YES	manual	down	down
GigabitEthernet0/1	unassigned	YES	manual	down	down
GigabitEthernet0/2	unassigned	YES	manual	down	down
Vlan1	172.19.0.253	YES	manual	up	up

```
SW4-Adir#
```