

פרויקט מסכם CCNA

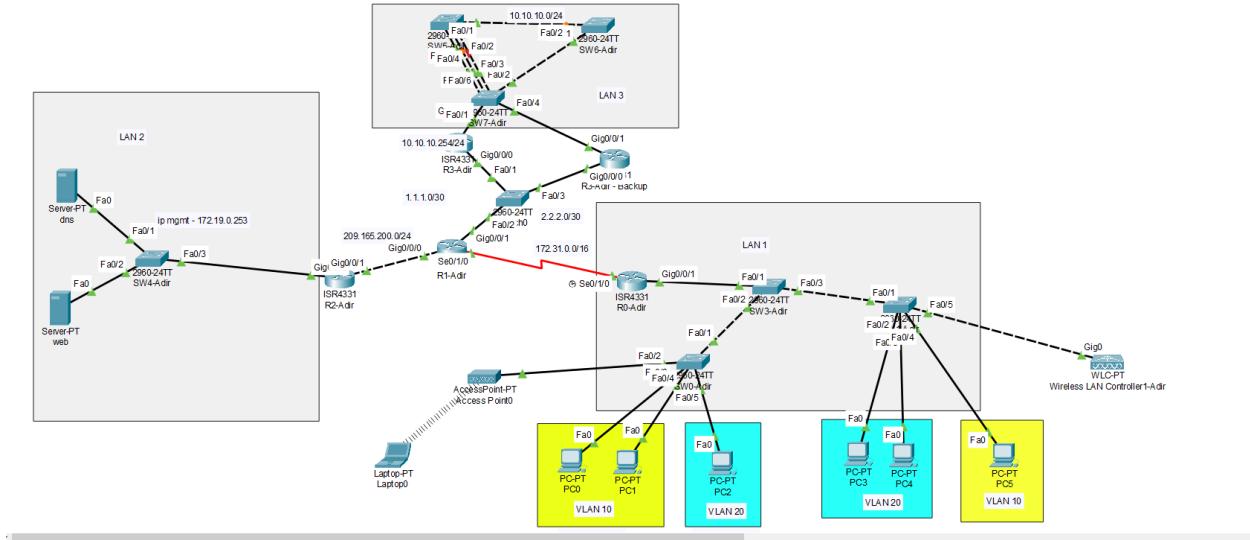
תוכן עניינים

3.....	טופולוגיה
4.....	הגדרת בסיסיות
4.....	הגדרת שם למתג/נתב
4.....	הגדרת סיסמת גישה ל-Console ו-Telnet
5.....	הגדרות סיסמאות גישה מוצפנות ל-Privileged Mode
6.....	czpnnt cll ssimato shocnso o ycnso bwtid
6.....	הגדרת Login Banner
7.....	snccrn houdut lmsn
7.....	mnut tk'uh bwt hklldh sl fk'hdh sgvih
8.....	הגדרת VLAN
8.....	ycrtt VLANS bmtg 0,1,3
8.....	shirr mmshkim l-VLANS
9.....	hadrat DHCP Server brsh LAN1
10.....	hadrat LAN2
13.....	hadrat rsht alhotit Wireless
15.....	hadrat Port Security
15.....	hadrat OSPF
17.....	hadrat nhol zyd htksrot mrchok
17.....	hadrat ACL
18.....	hadrat NAT
19.....	gilshh lsrtt WEB
20.....	HSRP
21.....	EtherChannel+STP
23.....	Syslog

פרויקט סוף – אDIR פרץ – מהנדס רשותות

25.....**מטלת בונוס**

טופולוגיה



הגדרות בסיסיות

הגדרת שם למstag/נתב

1. הגדרת שם לכל מtag/נתב – שם ההתקן צריך לכלול את השם הפרטני שלו.

הגדרות לנתב:

```
enable
```

```
configure terminal
```

```
hostname Adir-R1
```

הגדרות למstag:

```
enable
```

```
configure terminal
```

```
hostname Adir-SW1
```

הגדרת סיסמת גישה ל-Console ול-Telnet

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

הגדרת לנתב:

```
enable
```

```
configure terminal
```

```
line console 0
```

```
password adirabcd
```

```
line vty 0 4
```

```
password adirabcd
```

כאשר ב Line Vty אנו לא מכירים את ההתחברות לעבוד ב SSH אז Telnet מאפשר. יש לציין שモולץ להתחבר ב SSH לרכיב התקשרות(חיבור מאובטח ואמין יותר מ Telnet).

פרויקט סוף – אDIR פץ – מהנדס רשותות

הגדירות 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 סיסמה הטעני + 1234

הגדירות במתג:

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

הגדירות בנתב:

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

הצפנה כל 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 וזהיר 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!#
```

[סמכון הודעות למסך](#)

סמכון הודעות שהנתב/מתג שולח למסך, כך שלא יפריעו לכתיבה 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 VLANים במתג 0,1,3

יש ליצור VLANים 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 לשיר את הממשקים שבמתגים ל-VLANs המתאים

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 LAN1 ברשת DHCP Server

ברשת LAN1, הגדר את Router0 כ-DHCP Server .

- צור Pool DHCP שישמש את VLAN10 (השתמש בכתובת רשת 192.168.10.0/24).
- צור Pool DHCP שישמש את VLAN20 (השתמש בכתובת רשת 192.168.20.0/24).
- הגדר לכל Pool DHCP שמלבד לחلك כתובות IP , הוא ילמד את ה-Gateway Default Clientsgם מיהו ה- .
- הגדר DNS Server (כתובת DNS לאחר NAT).
- 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

הגדירות 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 דינמית ע"י ה pools שהוגדרו בנתב0 .Router0

הגדרת LAN2

הגדר לשירותים ולנתב ב-LAN2, כתובת IP בצורה ידנית לפי כתובת רשת 172.19.0.0/16 .172.19.0.100

- 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 תציג את השרת WEB .

: R2-Adir#ןגדירות בנתב-

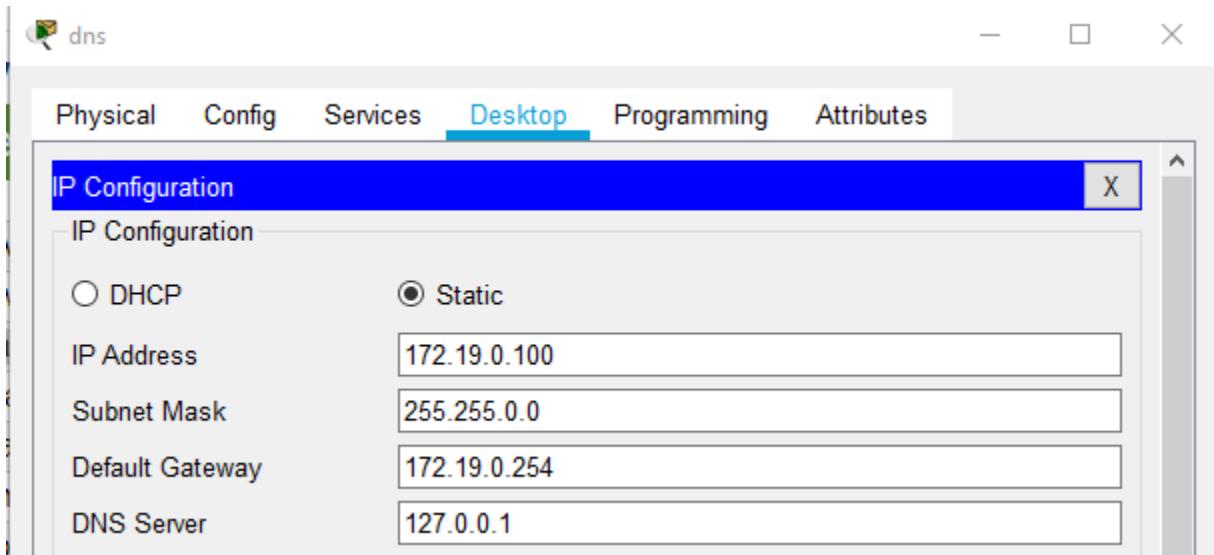
enable

configure terminal

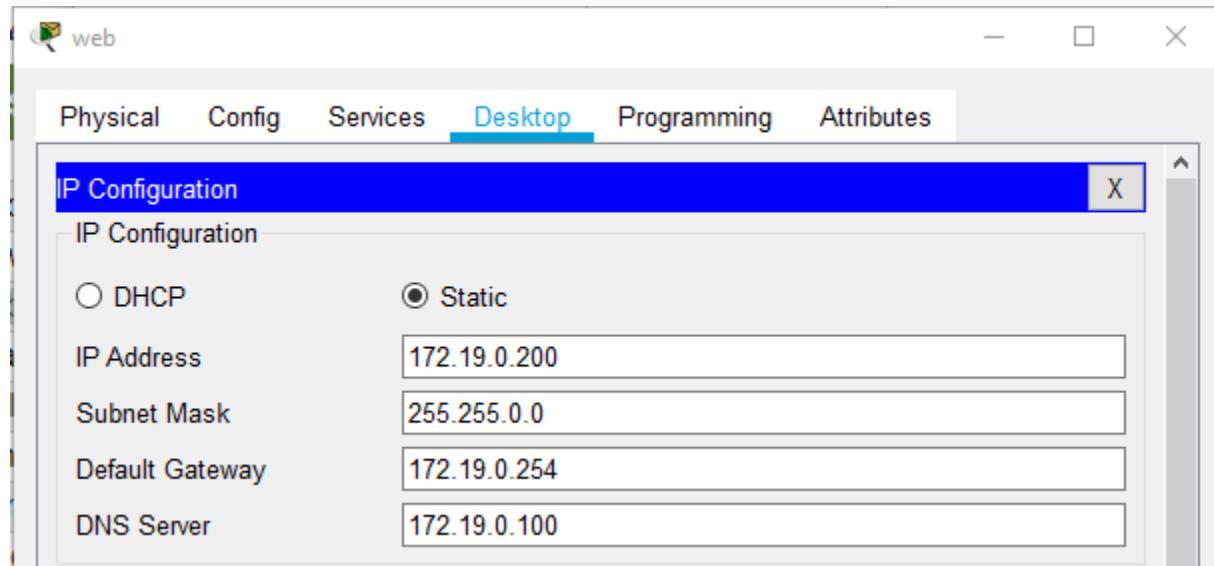
!

```
interface GigabitEthernet0/0/0
ip address 172.19.0.254 255.255.255.0
duplex auto
speed auto
!
```

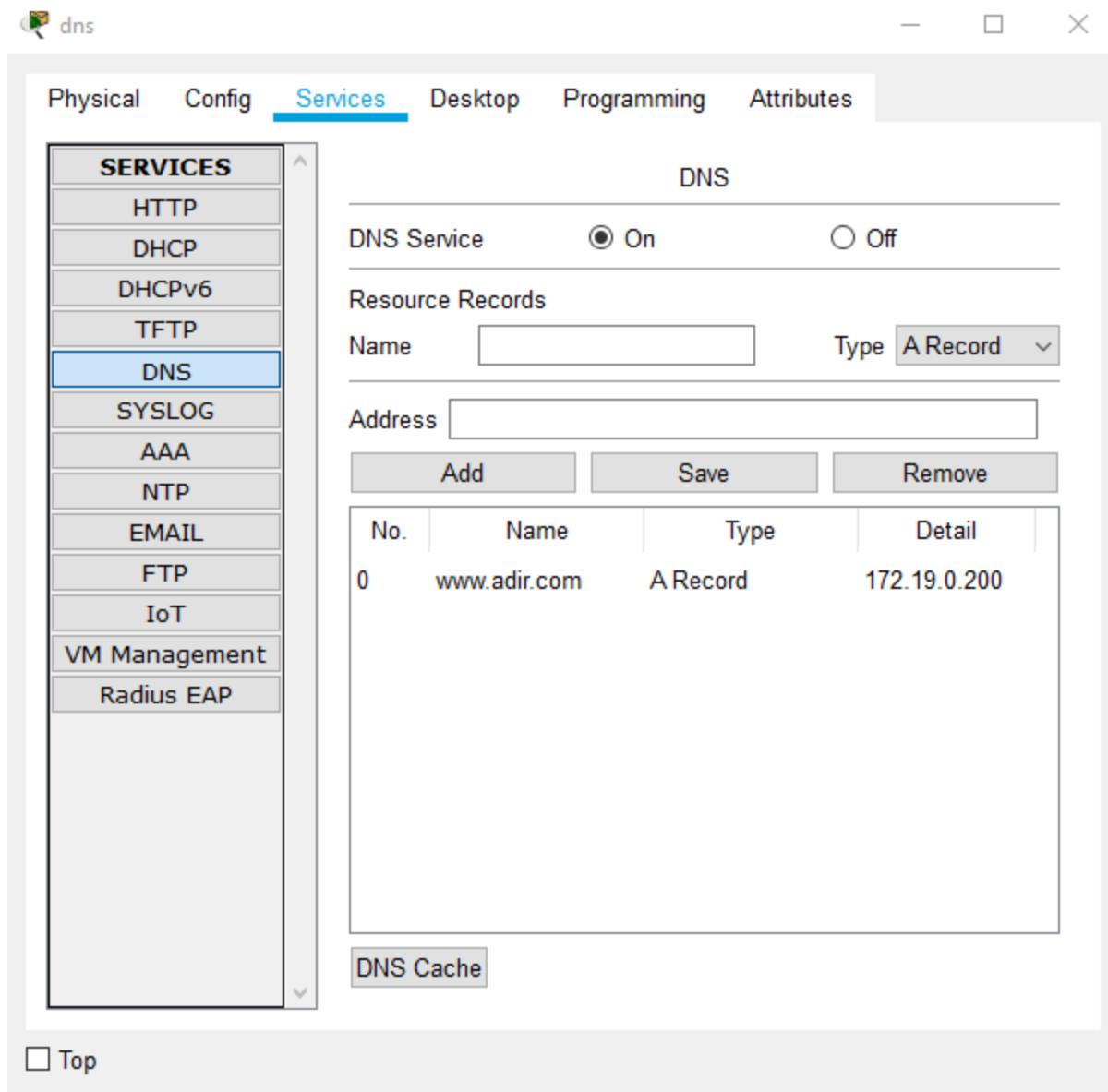
הגדרות רשת ידניות בשרת ה-DNS:



הגדרות רשת ידניות בשרת ה-WEB:



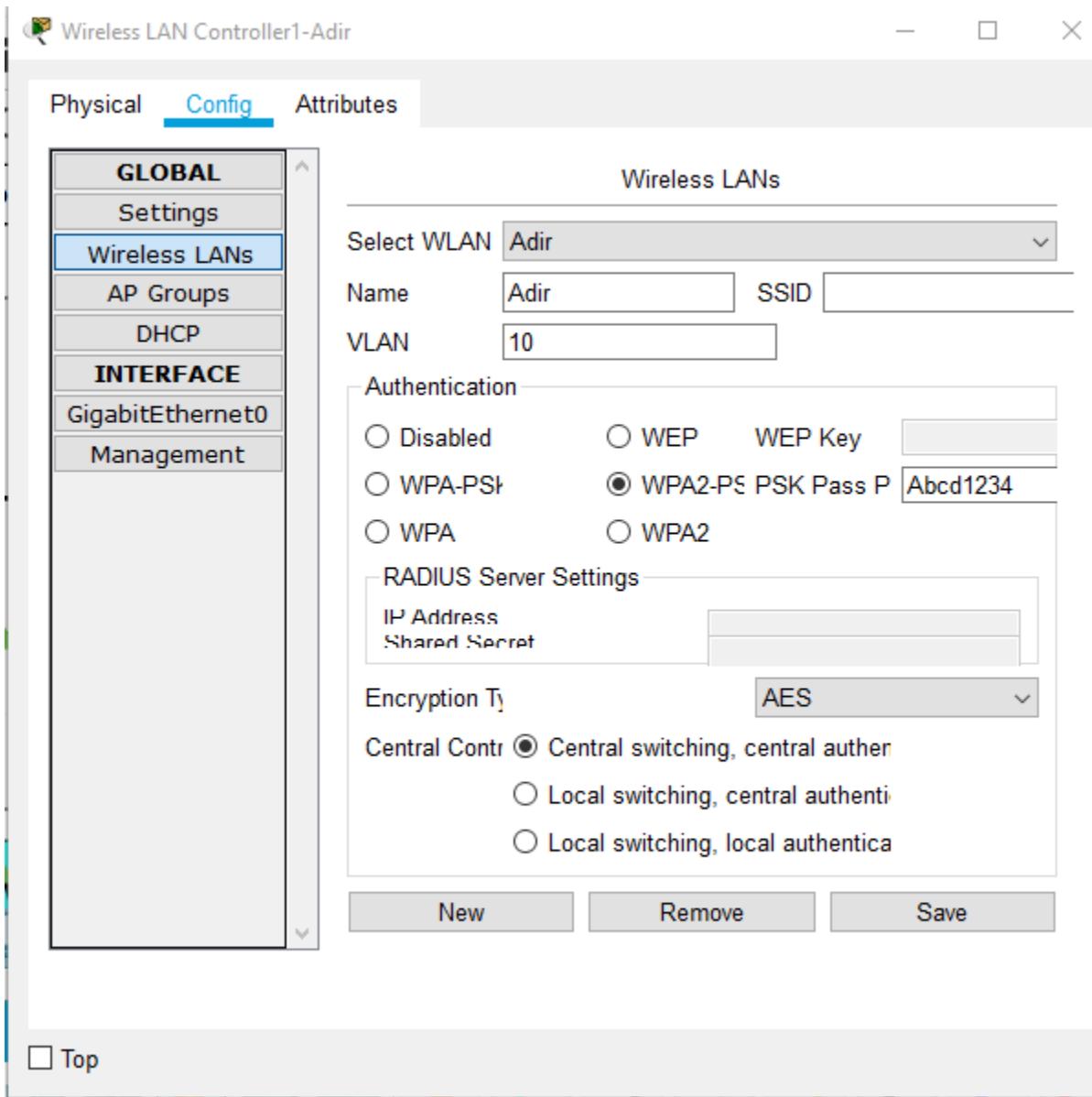
הפעלת שירות DNS והגדרת רשומה עבור www.adir.com



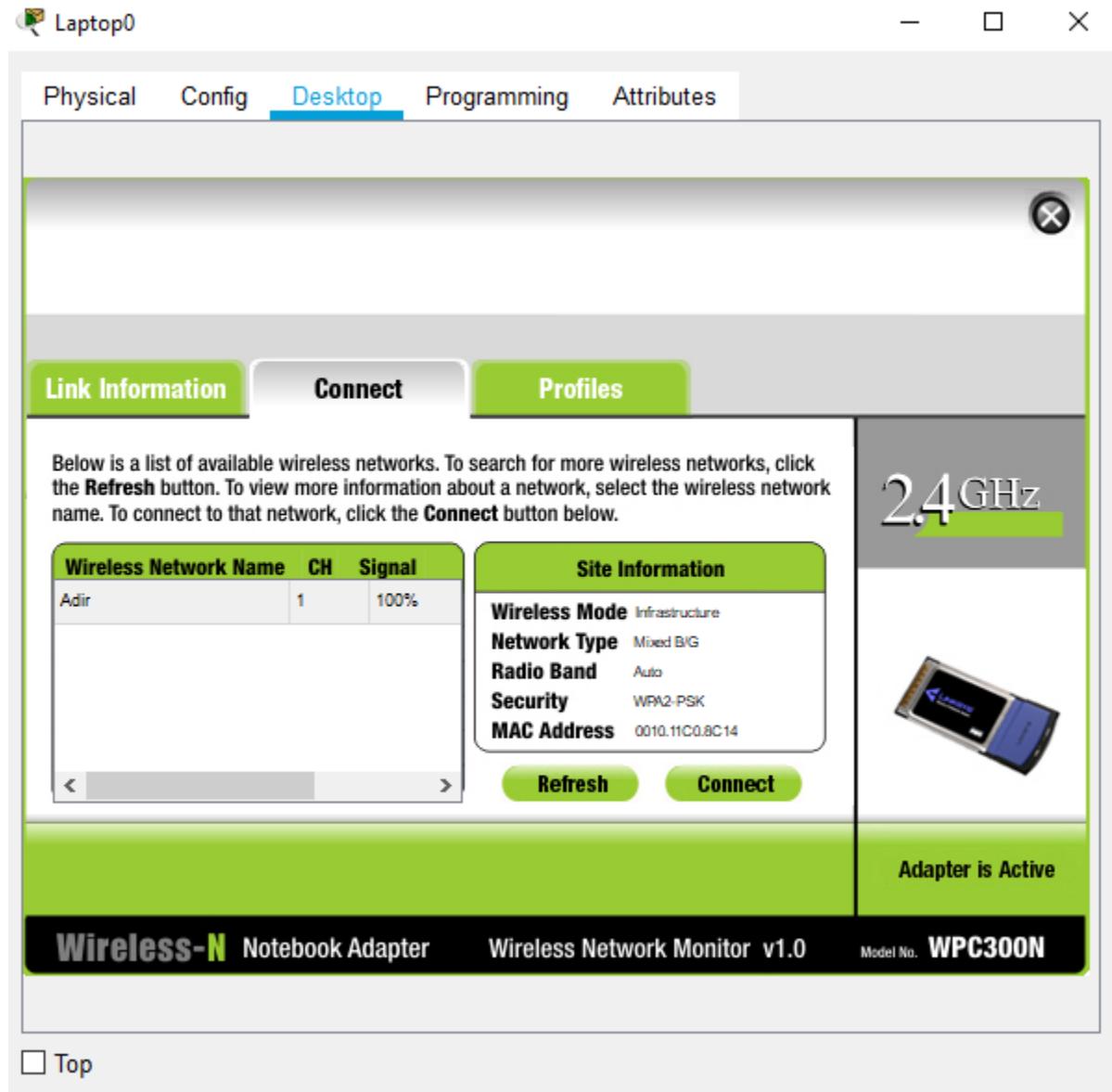
הגדרת רשת אלחוטית Wireless

הגדר את 1 Wireless LAN Controller כבקיר רשת אלחוטית:

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



התחברות בהצלחה של הלפטופ ל AP:



הגדרת Port Security

יש להגדיר port security במתג4 Switch4 שנמצא בחדר שרתים.

- חסום את הממשקים שלא בשימוש בכך שלא ניתן יהיה לחבר מחשב לא מורשה.
- דאג לכך שלא ניתן יהיה לחבר מחשב חליפי בחווות שרתים.
- מצב הפלה 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 1 ID Process ופרסום כל הרשותות המוחברות בConnected.

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 השירותים 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 התקשרות מרוחק

אפשרור SSH בכל ציוד התקשרות.

- ניתן לנוהל את הציוד רק דרך המחשבים שמחוברים לרשת דרכ VLAN10.
- ווגדר 10 interface vlan עם כתובות ניהול באותו סגמנט. רק VLAN 10 יכול 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 עם הסגמנט של VLAN 10 בשיווק על ממשי ה VTY Line.

הגדרת ACL

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

את ההגדרות ה ACL נכיל על הנטב #zir0-Adir Default Gateway של יחידות קצה מ VLAN 10 ו VLAN 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 בPAT).

הגדרת NAT בנתב 2 כדי לאפשר גישה לשרתים בחוות השירותים.

הגדרות בנתב # R2-Adir#

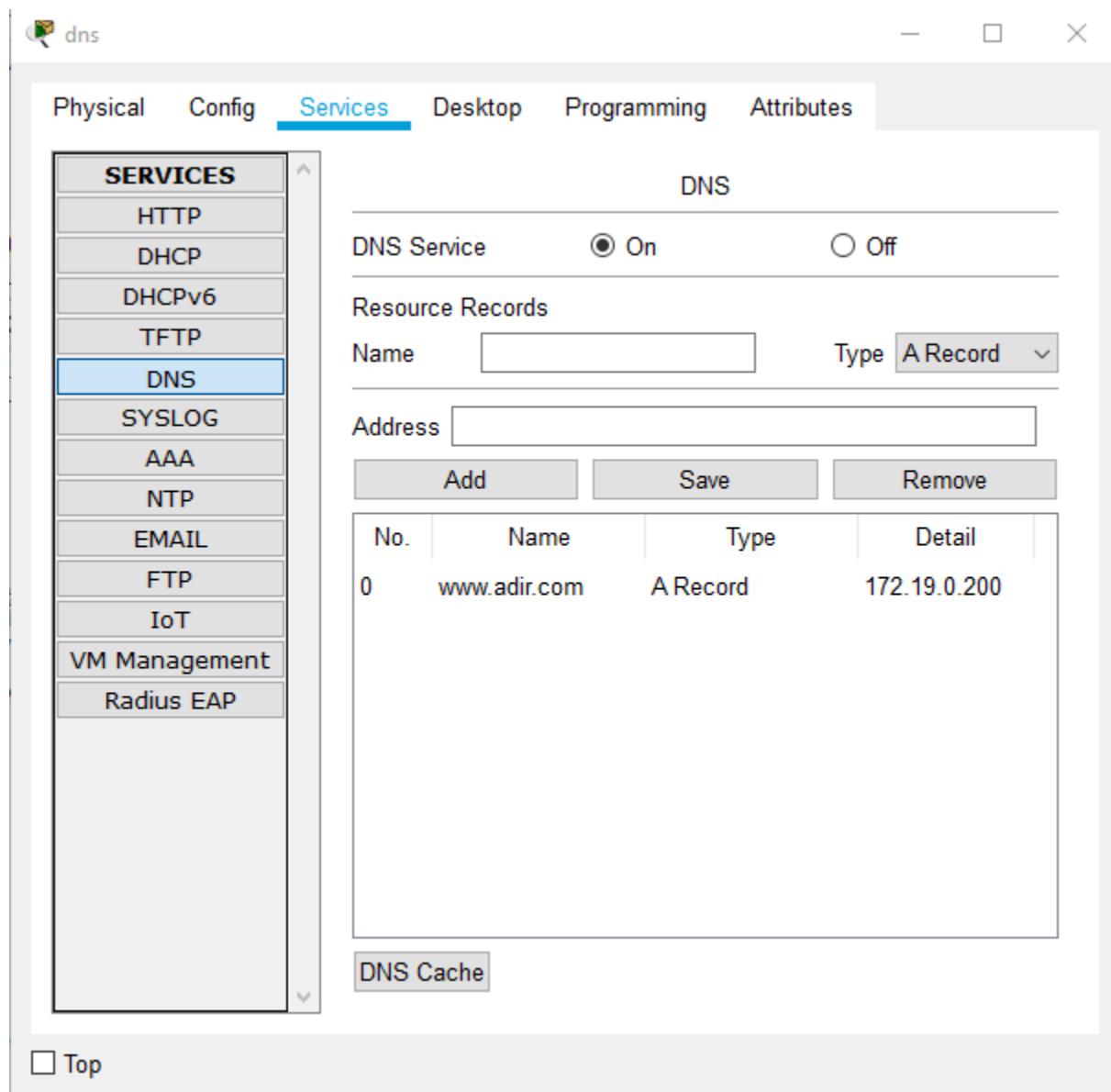
!

```
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
```

גלאייה לשרת WEB

בדוק שכל המחשבים יכולים לפנות לשרת WEB מהדף שלהם.



HSRP

הגדירות 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
```

הגדירות על נתב 3 הגיבו:

```
!
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 הינו נמוך ולכן הוא נבחר.

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

פרויקט סוף – אDIR פרץ – מהנדס רשותות

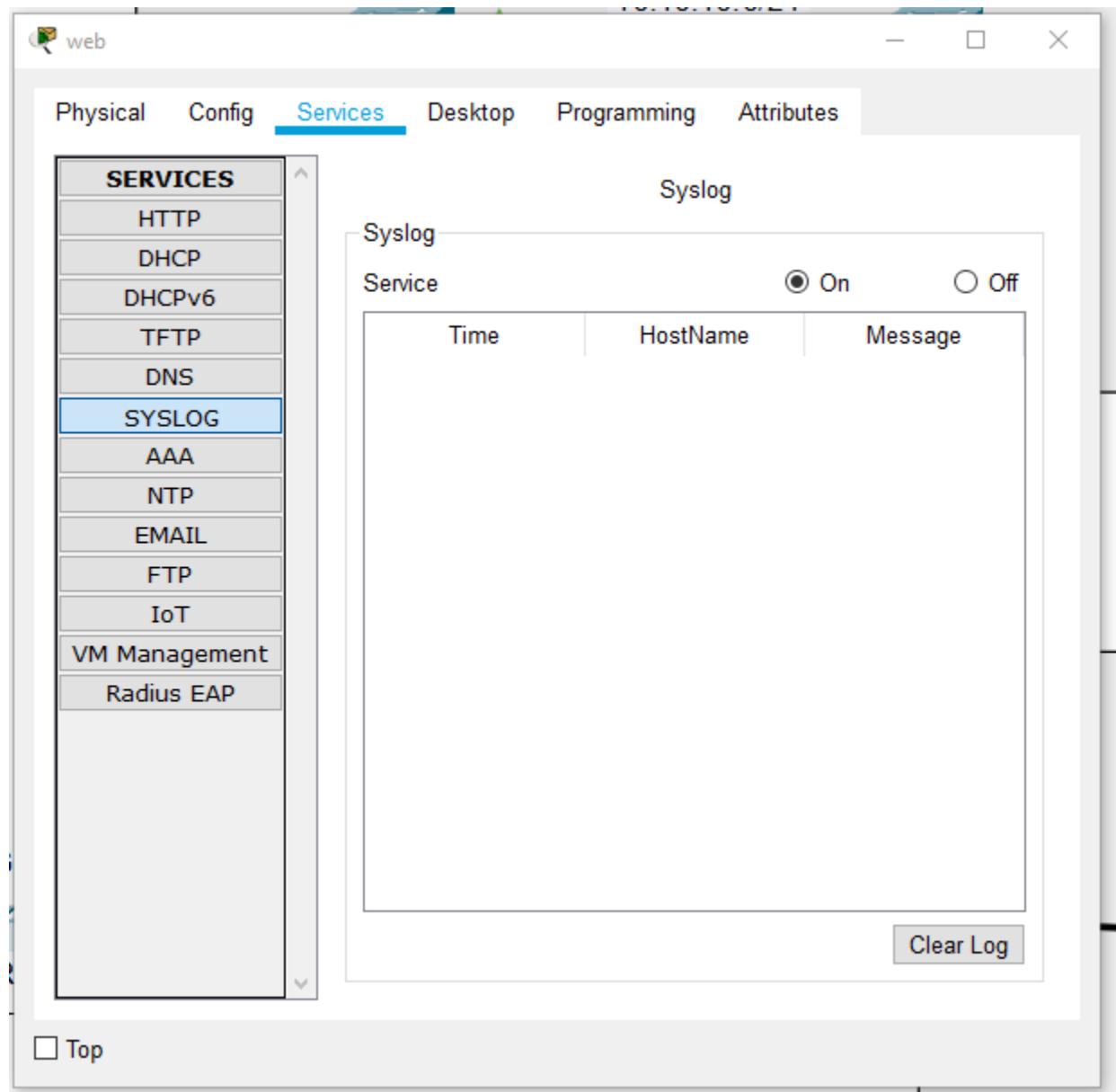
```
SW7-Adir#show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated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

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

Group  Port-channel  Protocol     Ports
-----+-----+-----+
1      Po1(SU)        -          Fa0/3(P)  Fa0/5(P)  Fa0/6(P)
SW7-Adir#
SW7-Adir#
SW7-Adir#
```

Syslog

הגדרת שרת ה-WEB כשרת Syslog



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

פרויקט סוף – אDIR פרץ – מהנדס רשותות

```
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 בرمמה של Debug

R2-Adir(config)#logging trap debugging

דוגמא לאירועים שמגיעים:

The screenshot shows a web-based management interface with a sidebar on the left containing various service icons. The main area is titled 'Syslog' and displays a table of log entries. The table has columns for 'Time', 'HostName', and 'Message'. There are two radio buttons at the top right of the table: 'On' (selected) and 'Off'. The log entries show multiple entries with the same timestamp (172.19.0.254) and host name (172.19.0.254), each followed by three dots in the message column.

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	...

מטלה בונוס

לודא שיש חיבור למתג 4 מ VLAN 10

לצורך כך, הוגדר הוגדר LINE VTY בرمאה של ACL על משקע ה Interface vlan 4. בנוסף, הוגדר ACL בرمאה של LINE VTY על משקע ה Interface vlan 4.

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

```
Password:
```

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

```
SW4-Adir>enable
```

```
Password:
```

```
SW4-Adir#
```

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