

# گزارش هشتم آزمایشگاه شبکه های کامپیوتری

اعضای گروه:

پارسا عصمت‌لو

سهیل شهرابی

# فهرست مطالب

2..... فهرست مطالب

3..... سوالات تحلیلی آزمایش هشتم

3..... سوال ۱

4..... سوال ۲

6..... سوال ۳

8..... گزارش آزمایش هفتم

8..... مرحله اول

8..... گام اول

9..... گام دوم

9..... آی پی دهی هاست ها-توضیحات تشریحی

9..... آی پی دهی هاست و نتورک-جدول

9..... گام پایانی

9..... بینگ گرفتن

11..... مرحله دوم

11..... گام اول

13..... گام پایانی

13..... بینگ گرفتن

14..... مرحله سوم

14..... گام اول

14..... گام دوم

14..... آی پی دهی هاست ها-توضیحات تشریحی

15..... گام پایانی

15..... بینگ گرفتن

16..... مرحله چهارم

16..... گام اول

16..... گام دوم

17..... گام پایانی

17..... بینگ گرفتن

# سوالات تحلیلی آزمایش هشتم

## سوال ۱

حمله میانی (Man-in-the-Middle یا MITM) یک نوع حمله است که در آن مهاجم به طور مخفیانه در ارتباطات بین دو طرف (مثلاً یک کاربر و یک سرور) وارد می‌شود و می‌تواند داده‌های مبادله‌شده را استراق سمع کرده، تغییر دهد یا تزریق کند. روند اجرای این حمله به طور کلی به شرح زیر است:

1. شنود (Eavesdropping): مهاجم ابتدا تلاش می‌کند به جریان داده‌های در حال انتقال بین دو طرف دسترسی پیدا کند. این کار می‌تواند با استفاده از ابزارهای شنود شبکه مانند Wireshark انجام شود. روش‌های مختلفی برای این کار وجود دارد:
  - a. شنود بی‌سیم: مهاجم در یک شبکه بی‌سیم قرار می‌گیرد و به ترافیک شبکه گوش می‌دهد.
  - b. شنود سیمی: مهاجم در مسیر ارتباطی مانند روترها یا سوئیچ‌های شبکه نفوذ کرده و به ترافیک دسترسی پیدا می‌کند.
2. جعل هویت (Impersonation): مهاجم خودش را به عنوان یکی از طرفین (کاربر یا سرور) جا می‌زند. این کار معمولاً با جعل آدرس IP یا آدرس MAC صورت می‌گیرد. در این مرحله، مهاجم می‌تواند:
  - a. جعل DNS: مهاجم ترافیک DNS را دستکاری کرده و کاربر را به یک وب‌سایت تقلبی هدایت می‌کند.
  - b. جعل ARP: مهاجم جدول ARP شبکه محلی را دستکاری کرده و آدرس MAC خود را به عنوان آدرس دستگاه دیگر معرفی می‌کند.

3. اعمال تغییرات (Modification): پس از ورود موفق به ارتباط، مهاجم می‌تواند داده‌های مبادله‌شده را تغییر دهد. به عنوان مثال:
- a. تغییر محتوای پیام‌ها: مهاجم می‌تواند محتوای پیام‌های ارسالی بین طرفین را تغییر دهد.
  - b. تزریق کد مخرب: مهاجم می‌تواند کدهای مخرب را به داده‌ها تزریق کند، مثلاً اسکریپت‌های جاوا اسکریپت در صفحات وب.
4. استراق سمع (Interception) مهاجم تمامی داده‌های مبادله‌شده بین طرفین را می‌تواند ذخیره کرده و برای اهداف خود استفاده کند، مثلاً:
- a. دسترسی به اطلاعات حساس: مهاجم می‌تواند به رمزهای عبور، اطلاعات بانکی، و سایر اطلاعات حساس دسترسی پیدا کند.
  - b. کپی‌برداری از ارتباطات: مهاجم می‌تواند تمامی مکالمات و پیام‌ها را ضبط کرده و برای تحلیل‌های بعدی استفاده کند.

روش‌های پیشگیری از حملات MITM

برای مقابله با حملات MITM می‌توان اقدامات زیر را انجام داد:

- استفاده از ارتباطات امن (SSL/TLS): اطمینان از اینکه تمامی ارتباطات با استفاده از پروتکل‌های امن مانند HTTPS انجام می‌شوند.
- احراز هویت قوی: استفاده از روش‌های احراز هویت دو مرحله‌ای (2FA) و گواهی‌نامه‌های دیجیتال.
- مانیتورینگ شبکه: نظارت دقیق بر شبکه برای شناسایی فعالیت‌های مشکوک.
- استفاده از VPN: ایجاد تونل‌های امن برای انتقال داده‌ها.
- به‌روزرسانی منظم نرم‌افزارها و سخت‌افزارها: اطمینان از به‌روز بودن تمامی نرم‌افزارها و تجهیزات شبکه.

## سوال ۲

معماری Split-MAC در Cisco Unified Wireless Solution یک روش ابتکاری برای بهینه‌سازی عملکرد شبکه‌های بی‌سیم و مدیریت آن‌ها است. در این معماری، وظایف

مربوط به کنترل و انتقال داده‌ها بین دو نوع دستگاه مختلف تقسیم می‌شوند: Access Points (APs) و Wireless LAN Controllers (WLCs). هدف اصلی این تقسیم کار، بهبود مقیاس‌پذیری، امنیت و کارایی شبکه‌های بی‌سیم است. در ادامه، به شرح جزئیات این معماری می‌پردازیم:

## 1. Access Points یا AP

Access Points دستگاه‌هایی هستند که به عنوان نقطه اتصال بی‌سیم برای دستگاه‌های کاربر عمل می‌کنند. در معماری AP، Split-MAC وظایف زیر را بر عهده دارند:

- Beacons و Probing: ارسال سیگنال‌های بی‌سیم برای شناسایی دستگاه‌های کاربر و پاسخ به درخواست‌های آن‌ها.
- Association و Reassociation: مدیریت فرآیندهای اتصال اولیه و مجدد دستگاه‌های کاربر به شبکه بی‌سیم.
- Hand-off و Roaming: مدیریت جابه‌جایی دستگاه‌های کاربر بین APها بدون قطع ارتباط.

## 2. Wireless LAN Controllers یا WLC

Wireless LAN Controllers وظایف کنترلی و مدیریتی شبکه‌های بی‌سیم را بر عهده دارند. این وظایف شامل موارد زیر است:

- Authentication و Authorization: مدیریت فرآیندهای احراز هویت و مجوز دسترسی دستگاه‌های کاربر.
- Security Management: اعمال سیاست‌های امنیتی و رمزنگاری داده‌های شبکه.
- RF Management: مدیریت خودکار فرکانس‌های رادیویی برای بهینه‌سازی پوشش شبکه و کاهش تداخل.
- Policy Enforcement: اعمال قوانین و سیاست‌های شبکه بر اساس کاربران و دستگاه‌ها.

## نحوه عملکرد معماری Split-MAC

در معماری Split-MAC، وظایف MAC (Media Access Control) به دو بخش تقسیم می‌شوند:

1. Local MAC (AP-based): برخی وظایف MAC به صورت محلی توسط APها انجام می‌شوند. این وظایف شامل مدیریت ارتباطات اولیه، beaconing، probing، و سایر عملیات‌های محلی است.
2. Centralized MAC (WLC-based): وظایف MAC پیشرفته‌تر و مدیریتی به WLCها منتقل می‌شوند. این وظایف شامل احراز هویت، مدیریت امنیت و اعمال سیاست‌های شبکه است.

### مزایای معماری Split-MAC

- بهینه‌سازی عملکرد: تقسیم وظایف بین APها و WLCها باعث افزایش کارایی و کاهش بار کاری هر یک از دستگاه‌ها می‌شود.
- مقیاس‌پذیری بهتر: امکان مدیریت تعداد بیشتری از APها و کاربران با استفاده از یک WLC.
- امنیت بالاتر: متمرکز شدن وظایف امنیتی در WLCها باعث بهبود کنترل و مدیریت امنیت شبکه می‌شود.
- مدیریت ساده‌تر: متمرکز کردن وظایف مدیریتی و کنترلی در WLCها باعث ساده‌تر شدن مدیریت شبکه‌های بزرگ می‌شود.

### نتیجه‌گیری

معماری Split-MAC در Cisco Unified Wireless Solution یک روش کارآمد برای بهبود عملکرد، امنیت و مقیاس‌پذیری شبکه‌های بی‌سیم است. با تقسیم وظایف بین APها و WLCها، این معماری امکان مدیریت ساده‌تر و کارآمدتر شبکه‌های بزرگ را فراهم می‌کند و به کاربران امکان می‌دهد تا از یک شبکه بی‌سیم با کیفیت و پایدار بهره‌مند شوند.

### سوال ۳

در استاندارد پایه IEEE 802.11a، که برای شبکه‌های بی‌سیم در باند فرکانسی 5 گیگاهرتز طراحی شده است، تعداد کانال‌های بدون همپوشانی بستگی به پهنای باند استفاده شده دارد. استاندارد 802.11a از کانال‌هایی با پهنای باند 20 مگاهرتز استفاده می‌کند.

## تعداد کانال‌های بدون همپوشانی در 802.11a

باند 5 گیگاهرتز به چند زیر باند تقسیم می‌شود و هر زیر باند دارای کانال‌هایی با فرکانس مرکزی خاصی است. در این باند، کانال‌های 20 مگاهرتزی با فاصله 20 مگاهرتزی از یکدیگر قرار می‌گیرند و به دلیل فرکانس‌های بالاتر و فضای فرکانسی وسیع‌تر، همپوشانی کمتری نسبت به باند 2.4 گیگاهرتز دارند.

برای مثال، در ایالات متحده، باند 5 گیگاهرتز به زیر باندهای زیر تقسیم می‌شود:

- U-NII-1: کانال‌های 36، 40، 44 و 48
- U-NII-2A: کانال‌های 52، 56، 60 و 64
- U-NII-2C (یا U-NII-2E): کانال‌های 100، 104، 108، 112، 116، 120، 124، 128، 132، 136 و 140
- U-NII-3: کانال‌های 149، 153، 157، 161 و 165

## کانال‌های بدون همپوشانی

با در نظر گرفتن زیر باندهای مختلف و فاصله 20 مگاهرتزی بین کانال‌ها، تعداد کانال‌های بدون همپوشانی می‌تواند متفاوت باشد. اما به طور کلی، هر کانال 20 مگاهرتزی در باند 5 گیگاهرتز به اندازه کافی از کانال‌های مجاور فاصله دارد که همپوشانی زیادی نداشته باشد. بنابراین، در استاندارد 802.11a، تمامی کانال‌های ذکر شده در زیر باندهای مختلف می‌توانند بدون همپوشانی مورد استفاده قرار گیرند، هرچند که باید توجه داشت که قوانین و مقررات منطقه‌ای ممکن است تعداد و محدوده کانال‌های قابل استفاده را محدود کنند.

## جمع‌بندی

در نتیجه، در استاندارد IEEE 802.11a در باند 5 گیگاهرتز، تعداد کانال‌های بدون همپوشانی به تعداد کانال‌های موجود در هر زیر باند بستگی دارد و می‌تواند تا 24 کانال بدون همپوشانی باشد، با توجه به زیر باندهای مختلف و قوانین منطقه‌ای.

## مثال کانال‌های بدون همپوشانی

برای مثال، در ایالات متحده، تعداد کانال‌های بدون همپوشانی به شرح زیر است:

- 4: U-NII-1 کانال (36، 40، 44، 48)
- 4: U-NII-2A کانال (52، 56، 60، 64)
- 11: U-NII-2C کانال (100، 104، 108، 112، 116، 120، 124، 128، 132، 136، 140)
- 5: U-NII-3 کانال (149، 153، 157، 161، 165)

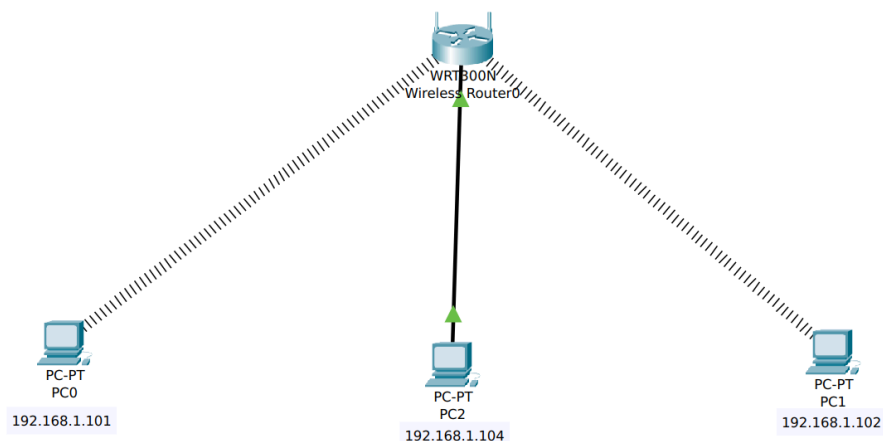
جمعاً 24 کانال بدون همپوشانی در باند 5 گیگاهرتز برای استاندارد IEEE 802.11a وجود دارد.

## گزارش آزمایش هفتم

### مرحله اول

#### گام اول

در گام اول تمامی ذکر شده در صورت سوال به همراه End device ها را گذاشته و اتصالات را میان آنها وصل کردیم. شکل ذیل حالت نهایی است.





## گام دوم

آی پی دهی هاست ها-توضیحات تشریحی

در مرحله دوم شروع به اطلاق IP به تک تک دیوایس ها و interface روتر ها به صورت Classfull کردیم. از آنجایی که در این توپولوژی تنها ۱ شبکه داریم، به اینترفیس LAN روتر آی پی 192.168.1.1 دادیم و از بخش GUI روتر، ابتدا DHCP Server را روشن کردیم و سپس رنج آدرس هایی که DHCP Server به دیوایس ها می‌دهد را از ۱۰۰ تا ۱۴۹ ست کردیم. سپس اینترفیس اترنت PC ها را حذف کرده و با اینترفیس WMP300N که ماژول وایرلس است جایگزین کردیم. پس از آن، از سمت روتر به سمت PC هایی که قرار بود از طریق WIFI متصل شوند، یک خط هاشوری به معنای برقراری ارتباط شکل گرفت.

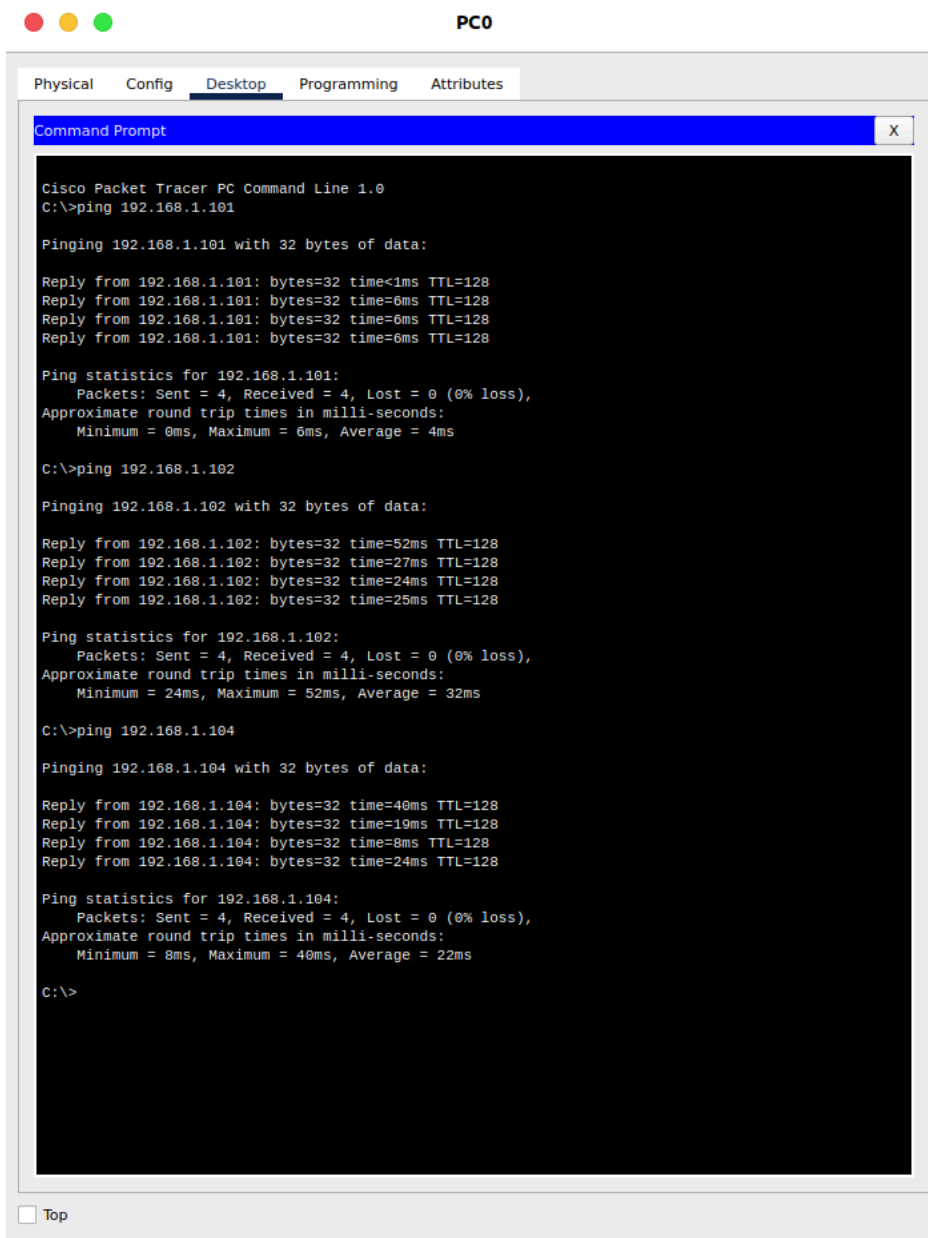
آی پی دهی هاست و نتورک-جدول

Device name	Ip	Mask	Network	Port
PC0	192.168.1.101	255.255.255.0	192.168.1.0	Wireless0
PC1	192.168.1.104	255.255.255.0	192.168.1.0	Wireless0
PC2	192.168.1.102	255.255.255.0	192.168.1.0	FastEthernet0

## گام پایانی

پینگ گرفتن

در پایان برای اطمینان از اتصالات و کانفیگ ها هاست های مختلف را پینگ گرفتیم و موفقیت آمیز بود.

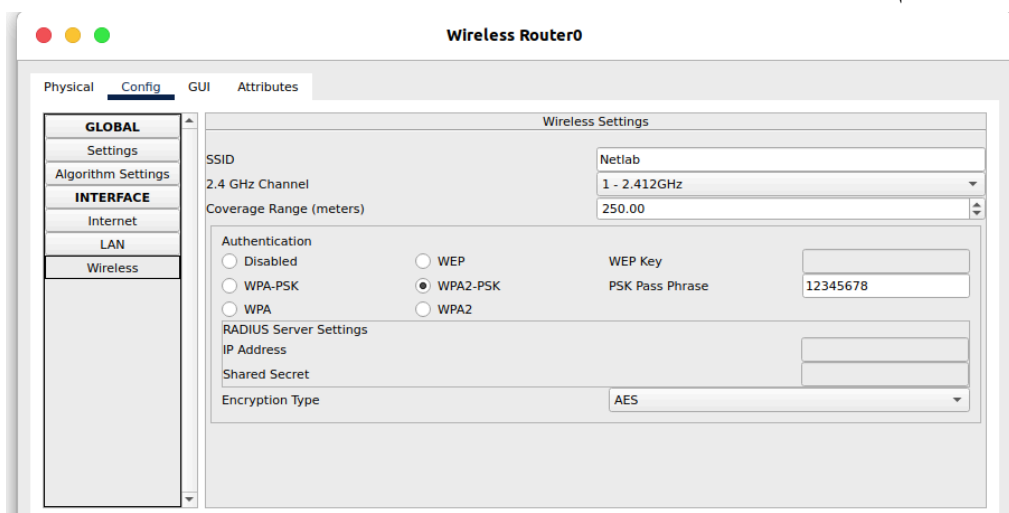


همانطور که در تصویر بالا مشخص است، با هاستی از آی پی 192.168.1.101 باقی هاست ها را با آی پی 192.168.1.102 و 192.168.1.104 را پینگ گرفتیم و موفقیت آمیز بود.

## مرحله دوم

گام اول

در این گام ما ابتدا از قسمت Config -> Wireless -> Authentication یک رمز برابر 12345678 را بر روی شبکه Wireless اعمال کردیم و سپس در PC ها از بخش Connect -> PC Wireless -> Desktop پس از اعمال رمز، به شبکه متصل شدیم.



PC0

PhysicalConfigDesktopProgrammingAttributes

Link InformationConnectProfiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Netlab	1	100%

Site Information

Wireless ModeInfrastructure

Network TypeMixed B/G/N

Radio BandAuto

SecurityWPA2-PSK

MAC Address0006.2A95.8B06

Refresh

Connect

2.4GHz



Adapter is Active

Wireless-N Notebook Adapter

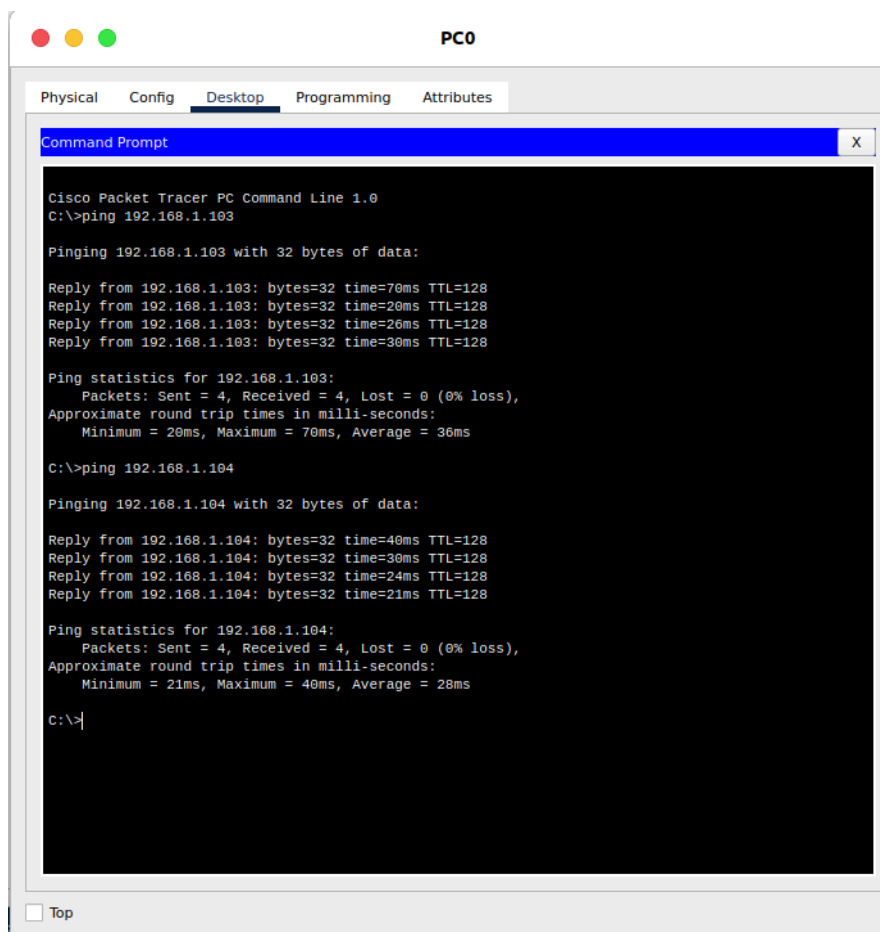
Wireless Network Monitor v1.0

Model No. WPC300N

☐ Top

گام پایانی

پینگ گرفتن



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC0. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the output of two ping commands: 'ping 192.168.1.103' and 'ping 192.168.1.104'. Both commands show successful results with 4 packets sent and received, 0% loss, and approximate round trip times in milliseconds.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.103

Pinging 192.168.1.103 with 32 bytes of data:

Reply from 192.168.1.103: bytes=32 time=70ms TTL=128
Reply from 192.168.1.103: bytes=32 time=20ms TTL=128
Reply from 192.168.1.103: bytes=32 time=26ms TTL=128
Reply from 192.168.1.103: bytes=32 time=30ms TTL=128

Ping statistics for 192.168.1.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 70ms, Average = 36ms

C:\>ping 192.168.1.104

Pinging 192.168.1.104 with 32 bytes of data:

Reply from 192.168.1.104: bytes=32 time=40ms TTL=128
Reply from 192.168.1.104: bytes=32 time=30ms TTL=128
Reply from 192.168.1.104: bytes=32 time=24ms TTL=128
Reply from 192.168.1.104: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.1.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 40ms, Average = 28ms

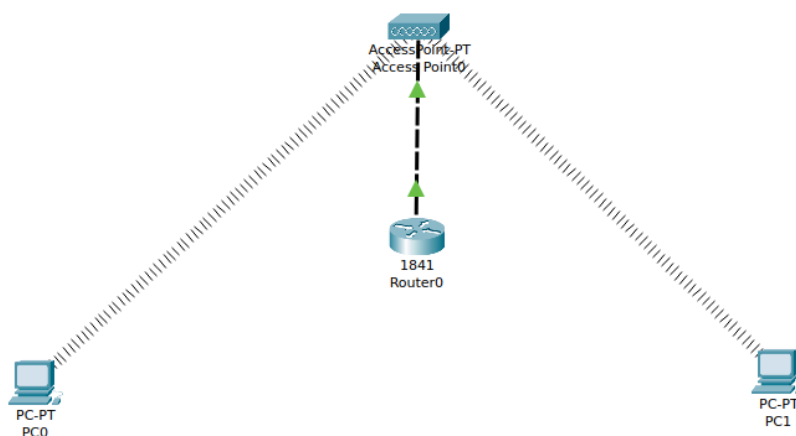
C:\>
```

همانطور که در تصویر بالا مشخص است، با هاستی از آی پی 192.168.1.101 باقی هاست ها را با آی پی 192.168.1.104 و 192.168.1.103 را پینگ گرفتیم و موفقیت آمیز بود.

## مرحله سوم

### گام اول

در گام اول در کنار فایل توپولوژی مرحله اول، یک روتر جدید اضافه کردیم و PC قبلی که به Ethernet به روتر متصل بود را برداشتیم و نحوه گرفتن آی پی هر PC را از DHCP برداشتیم و به صورت استاتیک آی پی دادیم.



### گام دوم

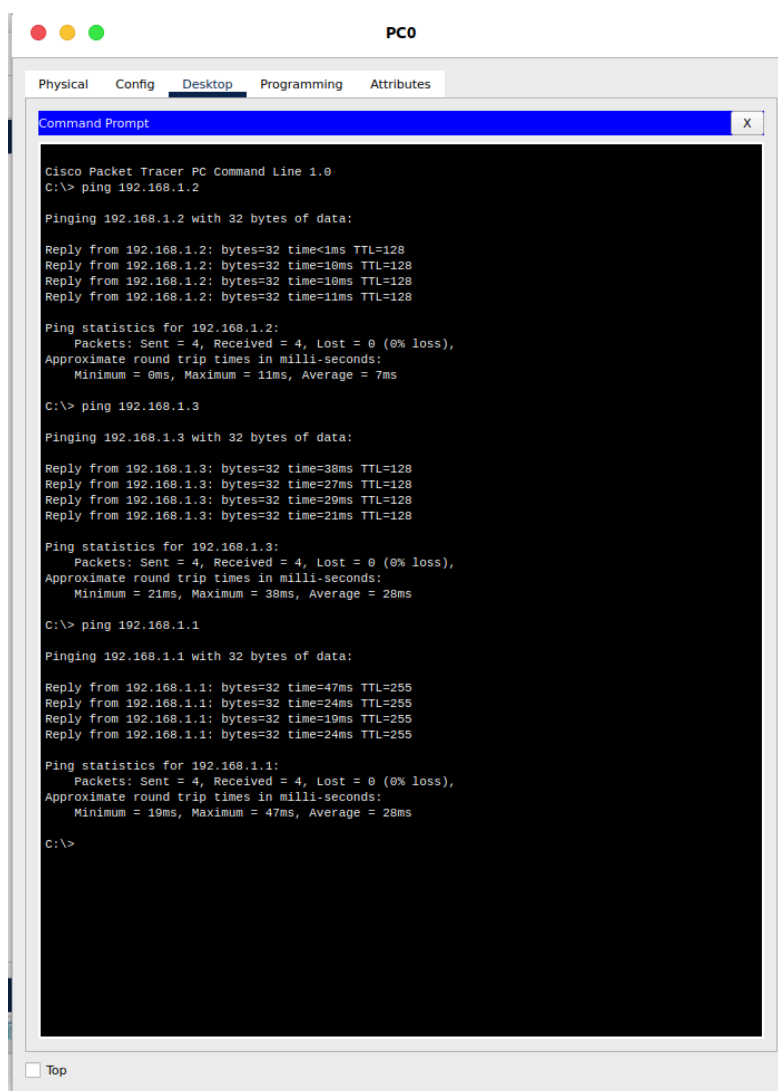
آی پی دهی هاست ها-توضیحات تشریحی

در مرحله دوم آی پی اینترفیس روتر را برابر 192.168.1.1 گذاشتیم و Default Gateway های PC ها را برابر همین آی پی قرار دادیم. پس از آن در Access Point، از قسمت Config آن، Port 0 که روتر به آن متصل بود را روشن کردیم و Port 1 را برای برقراری ارتباط Wireless روشن و رمز وای فای آن را برابر 12345678 گذاشتیم.

گام پایانی

پینگ گرفتن

در پایان برای اطمینان از اتصالات و کانفیگ ها هاست های مختلف را پینگ گرفتیم و موفقیت آمیز بود.



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time=10ms TTL=128
Reply from 192.168.1.2: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 7ms

C:\> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=38ms TTL=128
Reply from 192.168.1.3: bytes=32 time=27ms TTL=128
Reply from 192.168.1.3: bytes=32 time=29ms TTL=128
Reply from 192.168.1.3: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 38ms, Average = 28ms

C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=47ms TTL=255
Reply from 192.168.1.1: bytes=32 time=24ms TTL=255
Reply from 192.168.1.1: bytes=32 time=19ms TTL=255
Reply from 192.168.1.1: bytes=32 time=24ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 47ms, Average = 28ms

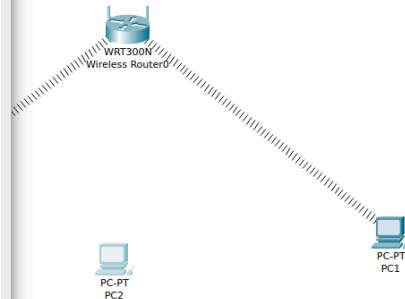
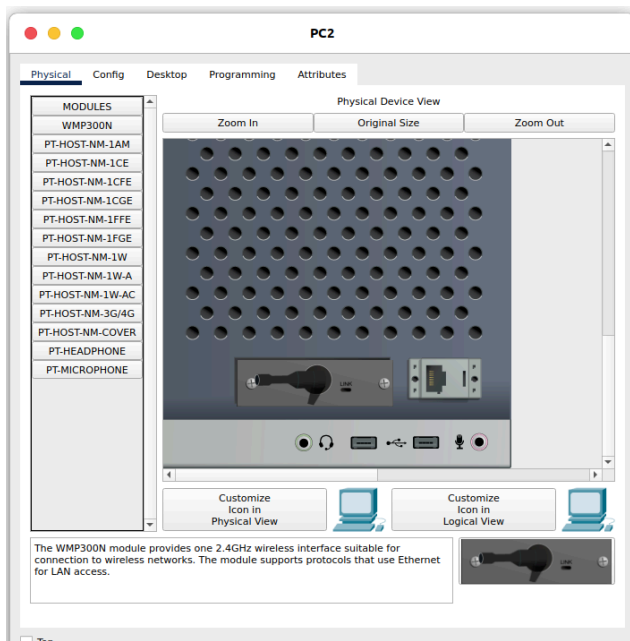
C:\>
```

همانطور که در تصویر بالا مشخص است، با هاستی از آی پی 192.168.1.2 باقی هاست ها را با آی پی 192.168.1.1 و 192.168.1.3 را پینگ گرفتیم و موفقیت آمیز بود.

## مرحله چهارم

### گام اول

در گام اول ابتدا فایل توپولوژی مرحله اول را برداشته و ابتدا ارتباط آن را به صورت Wireless می‌گذاریم.



### گام دوم

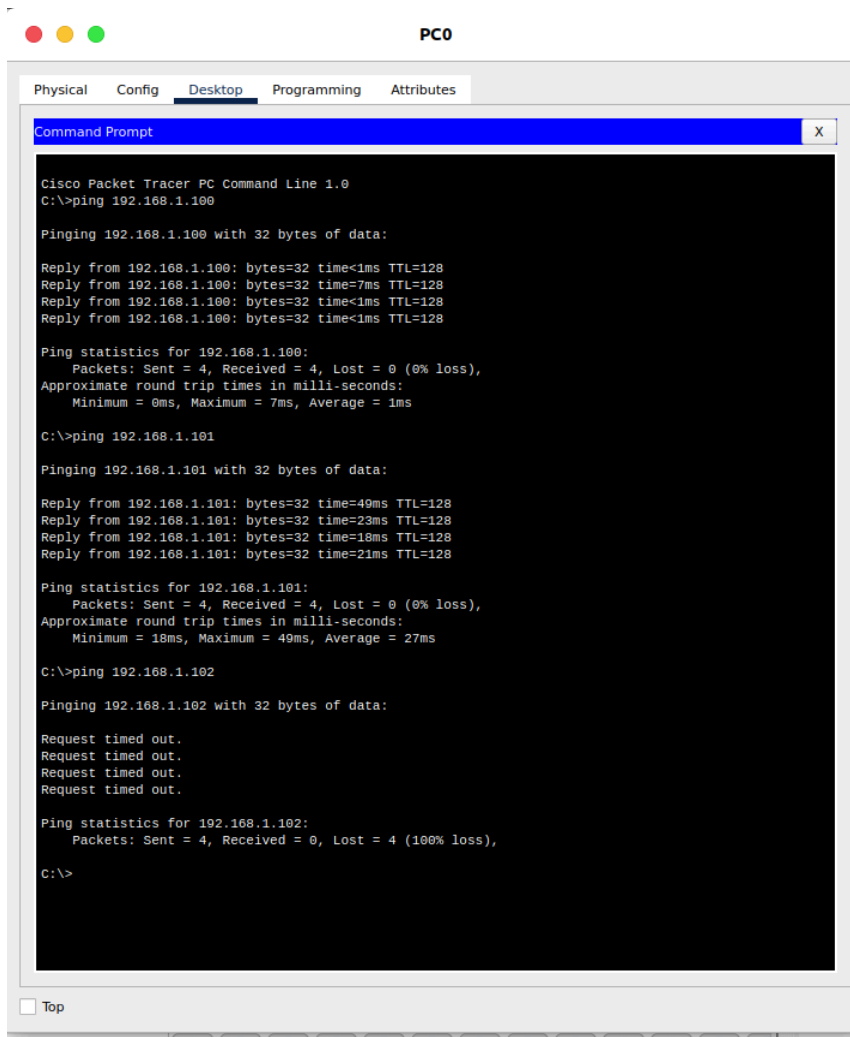
سپس مک آدرس PC2 را از قسمت Wireless0 -> Config کپی کردیم. بعد از آن با یکی دیگر از PC ها از قسمت Web Browser -> Desktop یک مرورگر بالا آوردیم و به آدرس 192.168.1.1 رفتیم، در این مرحله پس از ورود رمز و پسورد ادمین که حالت دیفالت آن برای تمامی روتر ها همان admin است رفتیم و از قسمت Access -> Wireless Mac Filter -> Wireless Resolution آدرس مک PC2 را در بخش Prevent PCs listed below



PC2 با دیگر PC ها به طور کامل قطع شد. پس از آن ارتباط from accessing the wireless network وارد کردیم.

گام پایانی

پینگ گرفتن



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 1ms

C:\>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Reply from 192.168.1.101: bytes=32 time=49ms TTL=128
Reply from 192.168.1.101: bytes=32 time=23ms TTL=128
Reply from 192.168.1.101: bytes=32 time=18ms TTL=128
Reply from 192.168.1.101: bytes=32 time=21ms TTL=128

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 49ms, Average = 27ms

C:\>ping 192.168.1.102

Pinging 192.168.1.102 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

همانطور که در تصویر بالا مشخص است، با هاستی از آی پی 192.168.1.100 باقی هاست ها را با آی پی 192.168.1.101 و 192.168.1.102 پینگ گرفتیم، پینگ ۱۰۱ موفقیت آمیز بود، اما پینگ ۱۰۲ که برای دیوایس PC2 بود موفقیت آمیز نبود که نشان می‌دهد این دیوایس دیگر دسترسی به network ندارد.