دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دستور کار آزمایشگاه شبکه‌های کامپیوتری

مسئول آزمایشگاه:

دکتر مسعود صبایی

بهار ۱۴۰۴

قوانین آزمایشگاه شبکه های کامپیوتری

برای افزایش کارآیی درس آزمایشگاه شبکه‌های کامپیوتری، رعایت عدالت بین تمامی گروه‌های آزمایشگاهی و آموزش حداکثری مطالب درس به صورت عملی، مدرسین و دانشجویان ملزم به رعایت نکات و قوانین ذیل هستند:

۱. تعداد جلسات در طول نیم‌سال ۱۰ تا ۱۲ جلسه خواهد بود.
۲. مدرسین و دانشجویان موظفند رأس ساعت مقرر در کلاس حضور یابند.
۳. قبل از انجام هر آزمایش، مبحث تئوری مربوط به آن آزمایش باید به طور کامل مطالعه شود، زیرا در حین جلسه وقت کافی برای توضیح و یادگیری مطالب تئوری وجود ندارد.
۴. پس از گذشت پنج دقیقه از شروع کلاس، به ازای هر پنج دقیقه تأخیر ۱۰ درصد نمره آن جلسه کسر میشود.
۵. حداکثر میزان تاخیر ۳۰ دقیقه است.
۶. هر آزمایش شامل یک پیش گزارش است که باید پیش از شروع آزمایش‌ها به مدرس تحویل داده شود. پیش گزارش مطلوب هر آزمایش در دستور کار آمده است.
۷. به ازای هر آزمایش، یک گزارش کار تهیه می‌شود که شامل تمامی مواردی است که در حین آزمایش با آن‌ها برخورد شده است. در این گزارش باید تمامی مشکلات پیش آمده و نحوه برطرف کردن آن‌ها ذکر گردد. همچنین، چگونگی انجام آزمایش مشتمل بر تحلیل آزمایش، به همراه اسکرین شات از مراحل انجام آزمایش ها تهیه شود.
۸. جهت کسب نمره قبولی در آزمایشگاه، کسب حداقل نمره قبولی در درس الزامی است.
۹. به منظور حفظ حرمت کلاس و نظافت آزمایشگاه، از خوردن و آشامیدن در طول کلاس خودداری نمایید.
۱۰. وارد آوردن هرگونه خسارت به تجهیزات آزمایشگاه مستلزم جبران خسارت است.

فهرست آزمایش ها

۱۰- آشنایی با مکانیسم NAT و پروتکل DHCP

۱-۱۰- هدف آزمایش

هدف از انجام این آزمایش آشنایی با آدرس‌دهی شبکه برای استفاده از سرویس‌های اینترنت است. بدین منظور عملکرد و پیکربندی مکانیسم NAT، PAT و پروتکل DHCP بررسی می‌شود.

۲-۱۰- مطالب مقدماتی

مکانیسم NAT برای تبدیل یک فضای آدرس IP به یک فضای آدرس دیگر انجام می‌شود. یکی از کاربردهای مهم این مکانیسم در تبدیل آدرس خصوصی و عمومی به یکدیگر است که برای دسترسی سیستم‌های با آدرس IP خصوصی به شبکه اینترنت ضروری است.

در NAT آشنایی با مفاهیم آدرس خصوصی[۱] یا غیر معتبر و آدرس IP عمومی یا معتبر از اهمیت ویژه‌ای برخوردار است. طبق RFC 1918، آدرس‌های IP خصوصی، آدرس‌هایی هستند که به‌وسیله شبکه‌هایی که مستقیما به اینترنت متصل نیستند، استفاده می‌شوند. در RFC 6890 لیستی از آدرس IP خصوصی و نحوه برخورد با آن ها ارائه شده است. به منظور اینکه سیستم‌ها با آدرس شبکه‌های خصوصی به اینترنت متصل شوند می‌بایست از NAT استفاده شود. آدرس‌های IPخصوصی در اینترنت قابل مسیریابی نیستند و معمولا توسط ISP[2]ها فیلتر می‌شوند. یک آدرس عمومی در اینترنت قابل مسیریابی است. سازمان IANA[3] مسئول اختصاص آدرس IP عمومی در اینترنت است. سازمان IANA نیز این مسئولیت را به سازمان‌های محلی واگذار می‌کند. به عنوان مثال ARIN[4] مسئول تخصیص آدرس‌های IP عمومی در آمریکای شمالی است.

مکانیسم NAT، یک آدرس (معمولا آدرس مبدا) در سرآیند بسته‌ها با یک آدرس دیگر (معمولا آدرس عمومی) جایگزین می‌کند. این مکانیسم معمولا در دیواره آتش شبکه پیاده‌سازی می‌شود. در حالت کلی، سه روش برای پیاده‌سازی NAT وجود دارد.

- Static: در این حالت یک نگاشت یک‌به‌یک و ثابت بین آدرس‌های‌اصلی و مپ شده وجود دارد. در این حالت اگر ۱۰ آدرس خصوصی داشته باشید، نیاز به ۱۰ آدرس عمومی خواهید داشت.
- Dynamic: در این حالت دستگاه‌ها در شبکه داخلی، به‌صورت خودکار از یک pool آدرس عمومی، آدرس دریافت می‌کنند.

---

[۱] private

[۲] Internet Service Provider

[۳] Internet Address Numbers Authority

[۴] American Registry for Internet Numbers

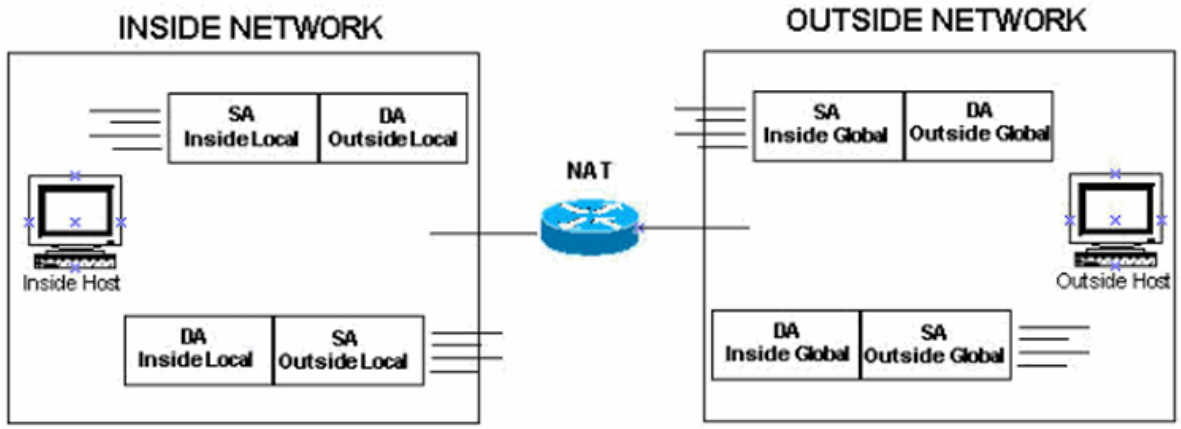
- Overload: در این حالت، یک بازه از آدرس‌های خصوصی، به یک آدرس عمومی مپ می‌شوند. در این حالت برای اینکه مسیریاب قادر به تفکیک درخواست‌ها باشد، شماره پورت موجود در بسته‌ها را نیز با یک شماره پورت دیگر عوض کرده و نگاشتی از این تعویض پورت نگهداری می‌کند.

در کتب درسی، هر ۳ مکانیسم‌ها به صورت یکپارچه با نام NAT شناخته می‌شوند.

در مکانیسم NAT آدرس‌های مختلفی ممکن است به دستگاه‌ها تعلق بگیرد که عبارت‌اند از:

- Inside Local: آدرس IP خصوصی یک دستگاه در شبکه داخلی.
- Inside Global: آدرس IP عمومی یک دستگاه در شبکه داخلی. این آدرس، می‌تواند آدرسی باشد که آدرس خصوصی به آن مپ شده است.
- Outside Local: آدرس IP یک دستگاه در شبکه خارجی که برای شبکه داخلی قابل رویت است. این آدرس الزاما یک آدرس عمومی نیست ولی لزوما باید قابل مسیریابی در شبکه داخلی باشد. در حالتی که از NAT برای آدرس‌های مقصد استفاده شود این آدرس می‌تواند با آدرس Outside Global متفاوت باشد. در غیر این صورت مقدار آن برابر Outside Global است.
- Outside Global: آدرس IP عمومی یک دستگاه در شبکه خارجی.

روند کلی تغییر آدرس‌ها را در شکل ۱ مشاهده می‌کنید.



شکل ۱: روند کلی تغییر آدرس‌ها

در این حالت مسیریاب هم‌زمان آدرس مبدا و آدرس مقصد بسته را ترجمه می‌کند. در این آزمایش صرفا به تغییر آدرس مبدا بسته خواهیم پرداخت.

مراحل تنظیم NAT به صورت پویا عبارت است از:

۱. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
۲. ایجاد یک pool آدرس عمومی که می‌تواند به صورت پویا به آدرس‌های شبکه خصوصی اختصاص یابد.
۳. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۴. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۵. تنظیم دسترسی ACL برای استفاده از NAT و pool ایجاد شده.

در این حالت به راحتی می‌توان مشاهده کرد که آدرس‌های Inside local به چه آدرس Inside global مپ شده و به چه آدرس Outside global متصل شده است.

برای تنظیم مپ کردن به صورت ایستا نیازی به تعریف ACL ندارید. مراحل تنظیم NAT ایستا عبارت است از:

۱. به صورت ایستا، برای هر آدرس داخلی یک آدرس خارجی تعریف کنید.
۲. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۳. مشخص کردن اینترفیس شبکه خارجی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.

در این حالت از آن‌جایی که نشست ها به صورت پویا برقرار نمی‌شوند، اطلاعات نشست شامل اینکه آدرس داخلی به چه آدرس outside global متصل شده است وجود نخواهد داشت.

همان‌گونه که توضیح داده شد، مکانیسم‌های NAT توضیح داده شده نیاز به تعداد زیادی آدرس عمومی دارند تا بتوانند تبدیل آدرس را انجام دهد. با توجه به محدودیت آدرس‌های IPv4، نیاز به مکانیسم دیگری احتیاج می‌شود که آدرس‌های خصوصی را به تعداد محدودی آدرس عمومی نگاشت کند. این مکانیسم که بخش دیگری از مکانیسم NAT است از تبدیل پورت مبدا در سرآیند بسته استفاده می‌کند و با نام PAT نیز شناخته می‌شود. همان‌طور که میدانید، در سرآیند TCP و UDP آدرس پورت مبدا و مقصد نیز وجود دارد. در این مکانیسم علاوه بر تبدیل آدرس در سرآیند IP، آدرس پورت مبدا نیز در سرآیند TCP و UDP نیز با یک مقدار یکتای دیگر جایگزین می‌شود. این مقدار، به یک پورت بر روی دستگاهی که مکانیسم PAT را پیاده‌سازی کرده اشاره می‌کند و بنابراین همه دستگاه‌های شبکه داخلی می‌توانند صرفا یک آدرس global local داشته باشند و با استفاده از پورت از یکدیگر تشخیص داده شوند.

مراحل تنظیم PAT عبارت است از:

۱. ایجاد یک لیست ACL که بیانگر این است چه آدرس‌هایی می‌توانند از این مکانیسم استفاده کنند.
۲. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل به آدرس را انجام دهد.
۳. مشخص کردن اینترفیس شبکه داخلی بر روی دستگاهی که قرار است تبدیل آدرس را انجام دهد.
۴. تنظیم دسترسی ACL برای استفاده از PAT: به اسن صورت که یک اینترفیس باید به صورت overload مشخص شود.

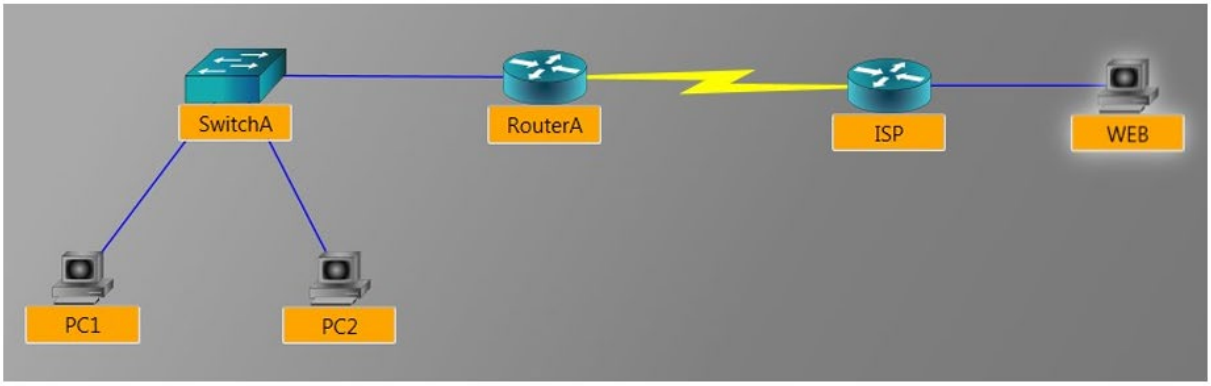
به عنوان مثال کلی، هنگامی که بسته SYN به سمت دروازه شبکه فرستاده می‌شود، دستگاه NAT آدرس IP و شماره پورت در سرآیند TCP را با آدرس IP عمومی و یک شماره پورت یکتا عوض می‌کند و بسته را به سمت شبکه عمومی ارسال می‌کند. در جواب اگر آدرس پورت مقصد بسته در جدول دستگاه NAT وجود داشته باشد، تبدیل آدرس دوباره انجام می‌شود و بسته به شبکه داخلی ارسال می‌شود.

۳-۱۰- شرح آزمایش

در ابتدا به بررسی مکانیسم NAT می‌پردازیم و با تنظیمات NAT پویا، NAT ایستا و PAT آشنا خواهیم شد. سپس پروتکل DHCP را مورد بررسی قرار خواهیم داد.

۱-۳-۱۰- مکانیسم NAT

توپولوژی که در این آزمایش بررسی می‌شود در شکل ۲ نشان داده شده است. آدرس‌های IP واسط‌ها در این آزمایش در جدول ۱ آمده است.



شکل ۲: توپولوژی آزمایش NAT ایستا

جدول ۱: آدرس‌های مورد نیاز آزمایشNAT ایستا

Subnet Mask	IP Address	Interface	Device
255.255.255.0 255.255.255.252	192.168.100.1 200.152.200.2	FastEthernet 0/0 Serial 0/0	RouterA
255.255.255.252 255.255.255.252	25.16.59.1 200.152.200.1	FastEthernet 0/0 Serial 0/0	ISP
Default Gateway	Subnet Mask	IP Address	Device
192.168.100.1	255.255.255.0	192.168.100.2	PC1
192.168.100.1	255.255.255.0	192.168.100.129	PC2
25.16.59.1	255.255.255.252	25.16.59.2	Web

۲-۳-۱۰- مکانیسم NAT ایستا

- واسط‌های دستگاه‌ها مطابق آدرس‌های داده شده در جدول ۱ تنظیم شده است. آیا PC1 و PC2 قادر به Ping کردن یکدیگر هستند؟ چرا؟ آیا از PC1 می‌توانید ISP را Ping کنید؟چرا؟
- بر روی مسیریاب RouterA باید مکانیسم NAT تنظیم شود. برای این کار، ابتدا از محیط تنظیم عمومی وارد تنظیمات اینترفیس fastethernet 0/0 شده سپس با استفاده از دستور

ip nat inside

آن را به عنوان اینترفیس داخلی انتخاب کنید. سپس وارد تنظیم اینترفیس serial 0/0 شوید و با دستور

ip nat outside

آن را به عنوان اینترفیس خارجی انتخاب کنید.

- در محیط تنظیم عمومی مسیریاب RouterA دستور زیر را وارد کنید. با استفاده از این دستور صرفا آدرس IP مبدا در بسته خروجی از شبکه تغییر می‌کند.

ip nat inside source static 192.168.100.2 200.152.200.1

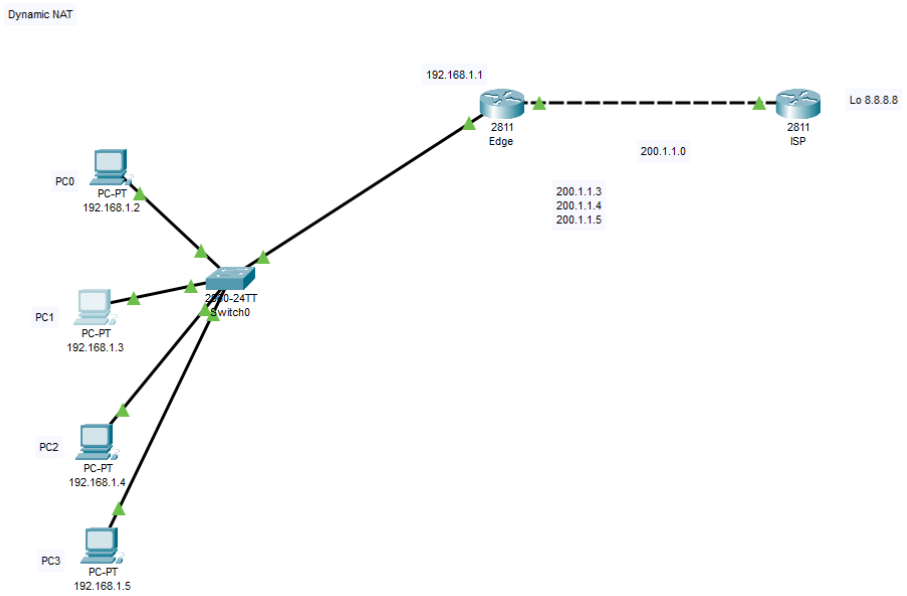
- از PC1 و PC2 مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟
- با استفاده از دستور

Show ip nat translations

جدول NAT در RouterA را مشاهده کنید و آن را شرح دهید.

۳-۳-۱۰- مکانیسم NAT پویا

ابتدا توپولوژی موجود در شکل ۳ را ایجاد کرده و بر اساس اطلاعات داده شده، تنظیمات لازم را انجام دهید.



شکل ۳: توپولوژی آزمایش NAT پویا

تنظیمات مورد نیاز:

PC0: 192.168.1.2
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

PC1: 192.168.1.3
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

PC2: 192.168.1.4
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

PC3: 192.168.1.5
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

کد های موردنیاز برای تنظیم Router:

- !ISP Configuration:

```
en
config t
hostname ISP

int f0/0
ip add 200.1.1.2 255.255.255.0
no sh

int lo 0
ip add 8.8.8.8 255.0.0.0
```

- !Edge Router configuration:

```
en
config t
hostname EDGE

int f0/0
ip add 200.1.1.1 255.255.255.0
no sh

int f0/1
ip add 192.168.1.1 255.255.255.0
no sh


ip route 0.0.0.0 0.0.0.0 200.1.1.2
```

- ! Dynamic NAT Configuration:

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool abc 200.1.1.3 200.1.1.5 netmask 255.255.255.0
ip nat inside source list 1 pool abc

int f0/0
ip nat outside
int f0/1
ip nat inside
```

- لیستی را که توسط کد زیر ایجاد کرده‌ایم چه نقشی دارد، توضیح دهید.

access-list 1 permit 192.168.1.0 0.0.0.255

- کد استفاده شده برای ایجاد pool را که در زیر آورده شده است را توضیح دهید.

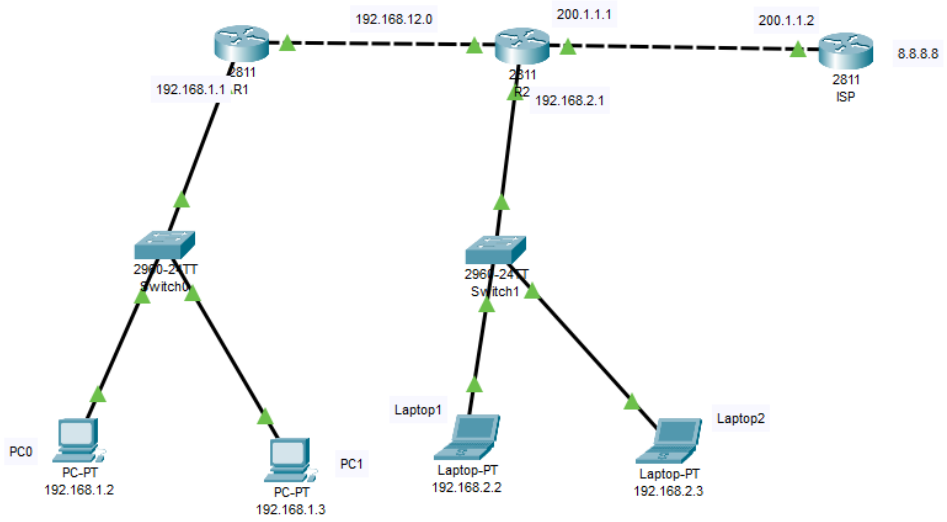
ip nat pool abc 200.1.1.3 200.1.1.5 netmask 255.255.255.0

- در ترمینال تمامی PC ها کد زیر را اجرا کنید، چرا یکی از این PCها قابلیت Ping کردن ندارد؟

ping -t 8.8.8.8

۴-۳-۱۰- مکانیسم PAT

سناریو شکل ۴ را در نظر بگیرید و تنظیمات لازم را بر اساس کدهای زیر انجام دهید.



شکل ۴: توپولوژی آزمایش PAT

تنظیمات مورد نیاز:

برای این سناریو خاص نیاز هست که برای R2 یک پورت اضافه شود (NM-2FE2W).

PC0: 192.168.1.2
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

PC1: 192.168.1.3
subnet mask: 255.255.255.0
default gateway: 192.168.1.1

Laptop 0: 192.168.2.2
subnet mask: 255.255.255.0
default gateway: 192.168.2.1

Laptop 1: 192.168.2.3
subnet mask: 255.255.255.0
default gateway: 192.168.2.1

کد های موردنیاز برای تنظیم Router:

- !ISP Configuration:

```
en
config t
hostname ISP

int f0/0
ip add 200.1.1.2 255.255.255.0
no sh

int lo 0
ip add 8.8.8.8 255.0.0.0
```

- !R1 Configuration:

```
en
config t
hostname R1

int f0/0
ip add 192.168.12.1 255.255.255.0
no sh

int f0/1
ip add 192.168.1.1 255.255.255.0
no sh

router ospf 1
int f0/0
ip ospf 1 area 0
int f0/1
ip ospf 1 area 0
```

- !R2 Configuration:

```
en
config t
hostname R2

int f0/0
ip add 192.168.12.2 255.255.255.0
no sh

int f0/1
ip add 200.1.1.1 255.255.255.0
no sh

int f1/0
ip add 192.168.2.1 255.255.255.0
no sh

router ospf 1
int f0/0
ip ospf 1 area 0
int f1/0
ip ospf 1 area 0
```

- PAT(R2) in global configuration

```
config t
ip route 0.0.0.0 0.0.0.0 200.1.1.2

access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

ip nat inside source list 1 int f0/1 overload

int f0/0
ip nat inside

int f0/1
ip nat outside

int f1/0
ip nat inside

#router ospf 1
#default-information originate
```

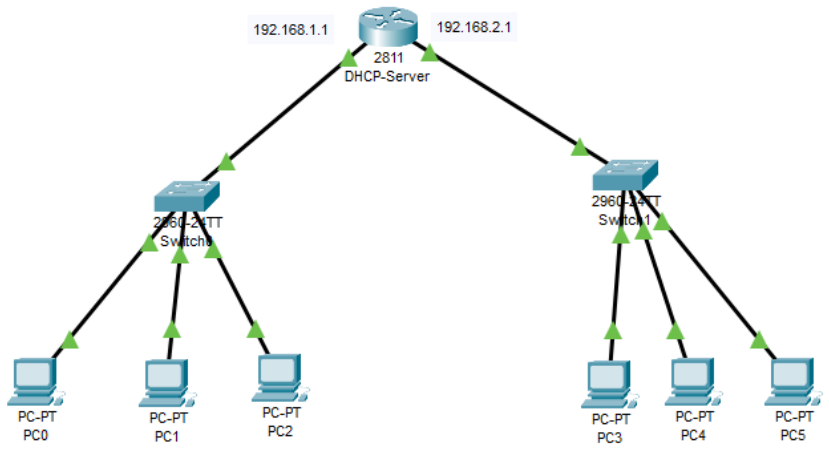
- بین لپ تاپ ها و کامپیوتر ها مسیریاب ISP را Ping کنید. چه اتفاقی می‌افتد؟
- با استفاده از دستور

show ip nat translations

جدول NAT را مشاهده کنید و با آزمایش قبلی مقایسه کنید.

۵-۳-۱۰- پروتکل DHCP

توپولوژی شکل ۵ را ایجاد کرده و تنظیمات لازم را بر اساس کدهای زیر انجام دهید.



شکل ۵: توپولوژی آزمایش DHCP

کد های موردنیاز برای تنظیم DHCP-Server:

- DHCP-Server Step 1

```
en
config t
hostname dhcp-server

int f0/0
ip add 192.168.1.1 255.255.255.0
no sh

int f0/1
ip add 192.168.2.1 255.255.255.0
no sh
```

- Step 2: in config

  ip dhcp excluded-address 192.168.1.1
  ip dhcp excluded-address 192.168.2.1

- Step 3: dhcp pool in config

  ip dhcp pool 192.168.1.1(NAME)

  in dhcp-config: network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8

- Step 4: dhcp pool in config

  ip dhcp pool 192.168.2.1

  in dhcp-config: network 192.168.2.0 255.255.255.0
  default-router 192.168.2.1
  dns-server 8.8.8.8

- For checking dhcp:
  sh run | sec dhcp

- دلیل استفاده از ۲ دستور زیر را توضیح دهید.

ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1

- وارد قسمت تنظیمات IP هر کدام از PC ها بشوید، آیا dhcp به درستی IPهای مورد نیاز را اختصاص می‌دهد؟ گزارش دهید.
- آیا ارتباط بین کامپیوترها موجود است؟ برای این کار در PC3 کد زیر را وارد کنید.

ping 192.168.1.2