

به نام خدا

## تنظیمات روترهای Cisco



مدرس: مهندس علیزاده

تهیه و تنظیم: اسماعیل وفانور

برای انجام تنظیمات بر روی روتر های سیسکو بایستی دستورات را در محیط متنی تنظیم روتر (که به محیط CLI معروف است) وارد کنیم.

## انواع mode کاری:

در این محیط متنی 3 مد (mode) کاری مختلف وجود دارد. هر مد ویژگی های مخصوص خود را دارد و دستورات خاصی در آن قابل اجراست. این مد ها به شرح زیر هستند:

1 – User mode: این محیط با علامت > (hostname) شناخته می شود و پایین ترین سطح دسترسی را دارد و دستوراتی که در این محیط اجرا می شوند، کاربرد ی تنها در حد مشاهده بعضی گزارشات ساده در مورد دستگاه دارند.

Router>

2 – Privileged Mode: این مد نسبت به مد قبلی سطح دسترسی بالا تری دارد و با علامت hostname# شناخته می شود. بسیاری از گزارشات پیشرفته به کمک دستورات این محیط قابل مشاهده است.

نکته: برای رفتن از مد user به مد privileged از دستور Enable استفاده می شود. مثال:

Router>enable

Router#

نکته: برای رفتن از مد privileged به مد user از دستور exit استفاده می شود. مثال:

Router#exit

Router>

3 – Global mode: این مد نسبت به مد قبلی سطح دسترسی بالا تری دارد و بسیاری از تنظیمات اصلی سیستم در این محیط انجام می شود. این مد با علامت hostname(config)# شناخته می شود.

نکته: برای رفتن از مد privileged به مد Global از دستور configure terminal استفاده می شود.

مثال:

```
Router#configure terminal
Router(config)#
```

نکته: برای رفتن از مد Global به مد privileged از دستور `exit` استفاده می شود. مثال:

```
Router(config)#exit
```

```
Router#
```

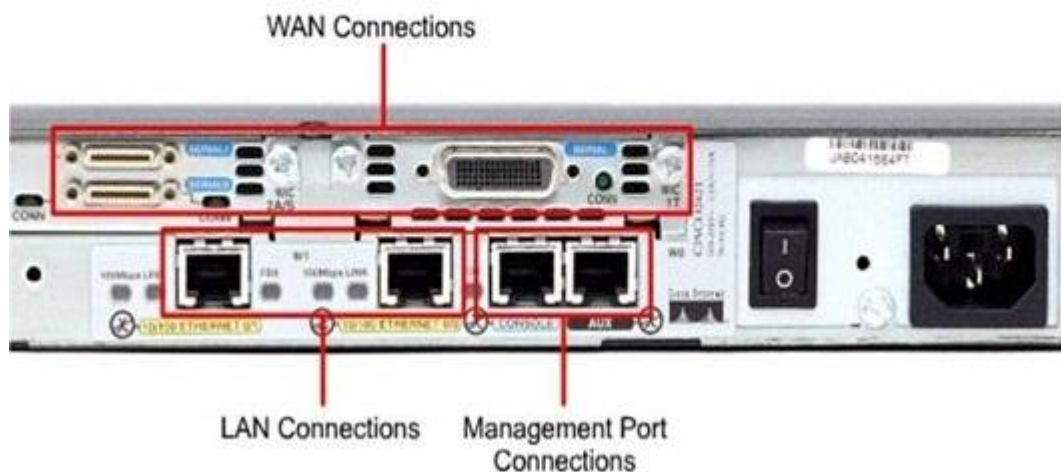
نکته: همیشه برای برگشتن از یک مد با دسترسی بالاتر به مد قبل از آن می توان از دستور `exit` استفاده کرد.

## Interface ها:

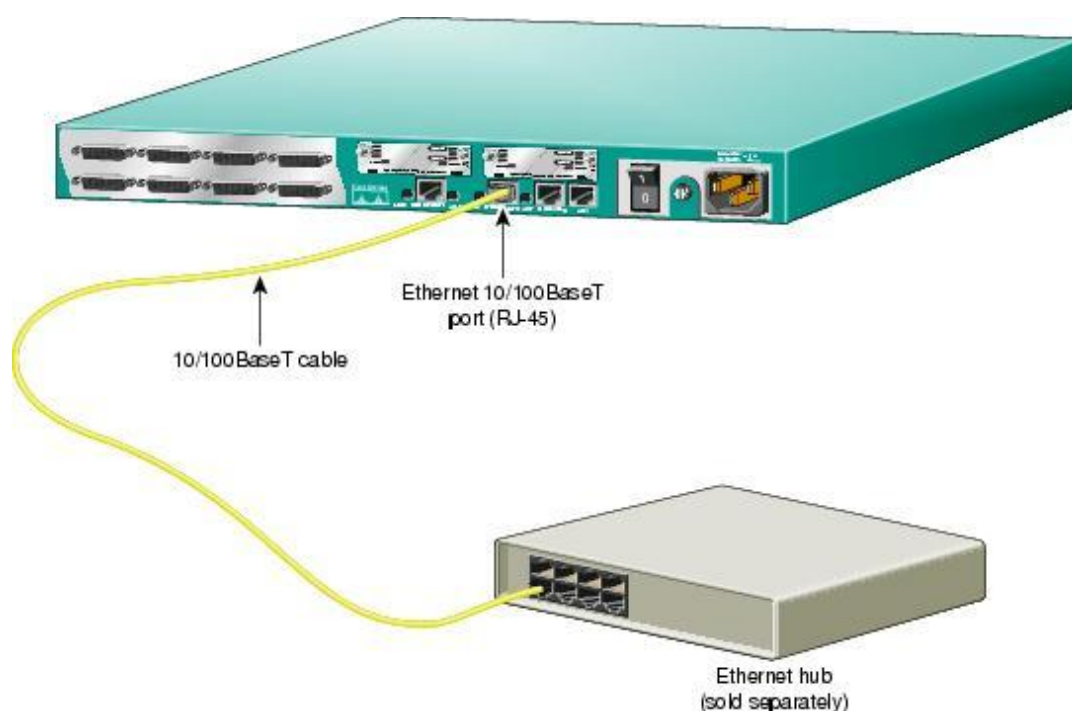
در مد Global همچنین `submode` مهمی به نام محیط `interface` وجود دارد که از آن برای تنظیم کردن هر یک از `interface` های (پورت های) روتر استفاده می شود. این `Submode` با علامت `Router(config-if)#` شناخته می شود.

`Interface` ها در واقع همان پورت هایی هستند که با اتصال کابل های مختلف به آنها می توان آنها را به یک سوئیچ، کامپیوتر و حتی یک روتر دیگر متصل کرد. `Interface` ها انواع مختلفی دارند، که برخی از آنها را در شکل زیر می توانید ملاحظه کنید:

## Router Interfaces



در شکل زیر اتصال یکی از interface های روتر از نوع fast ethernet را به یک هاب مشاهده می کنید.



نکته: برای ورود به محیط یک interface خاص بایستی در محیط Global دستور زیر را وارد کنیم:

شماره اینترفیس نوع اینترفیس Router(config)#interface

مثال:

```
Router(config)#interface fastethernet 0/1
Router(config-if)#
```

در مثال فوق fastethernet نوع اینترفیس و 0/1 شماره آن است. در خط بعدی عبارت Router(config-if)# نشان می دهد که با موفقیت وارد محیط اینترفیس شده ایم.

نکته: برای تنظیم آدرس ip روی یک interface خاص پس از ورود به محیط آن interface از دستور زیر استفاده میکنیم:

Router(config-if)# ip address      آدرس آی پی      Subnet mask

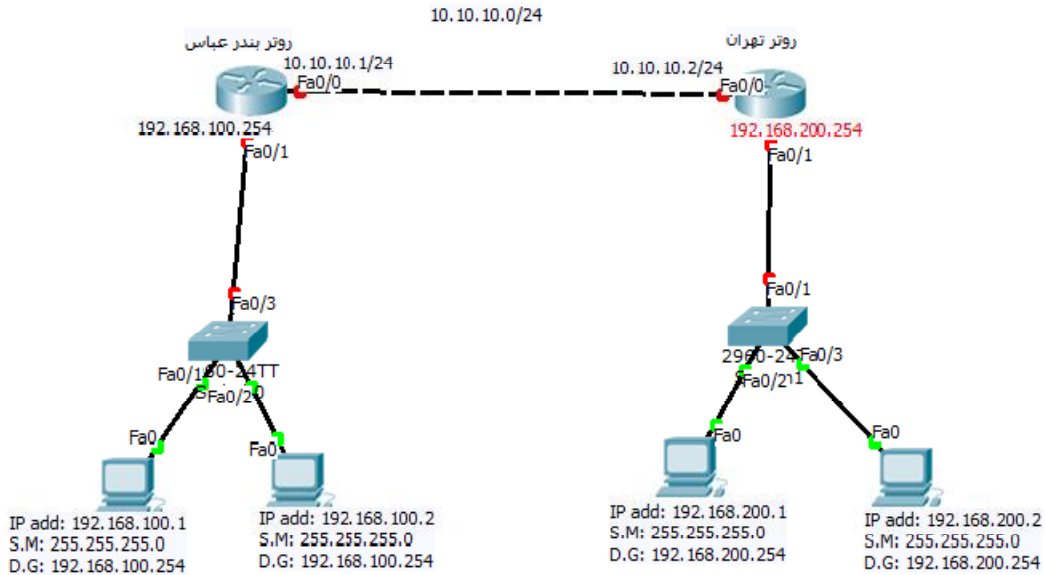
مثال:

```
Router(config-if)#ip address 192.168.200.254 255.255.255.0
```

نکته : **interface** ها در حالت پیش فرض غیر فعال هستند و امکان ارتباط با دیگر دستگاه ها را ندارند برای فعال کردن آنها بایستی از دستور **no shutdown** در محیط همان **interface** استفاده کنیم. مثال:  
**Router(config-if)#no shutdown**

نکته : برای خروج از محیط یک **interface** می توان از دستور **exit** استفاده کرد. مثال:  
**Router(config-if)#exit**  
**Router(config)#**

## تنظیم جدول مسیریابی روتر:



روتر برای شناخت شبکه های مجاور خود نیاز به تنظیم خاصی ندارد و به صورت خودکار قادر است بسته ها را در این مسیرها هدایت کند ولی برای اینکه روتر شبکه های غیر مجاور خود را بشناسد و بسته های مربوط به آنها را به مسیر مربوطه هدایت کند بایستی مسیر بسته مربوط به هر شبکه را در جدول مسیریابی روتر مشخص کنیم.

### الف - مسیریابی ایستا:

یکی از روش های تعیین مسیر بسته استفاده از مسیر یابی static (ایستا یا دستی) است که در آن مدیر شبکه به صورت دستی مسیر تمام شبکه های غیر مجاور را به روتر معرفی میکند، و در جدول مسیریابی روتر ثبت می کند.

برای معرفی مسیر بسته های مربوط به یک شبکه غیر مجاور به صورت دستی از دستور زیر در محیط Global استفاده میکنیم:

Router(config)#ip route {نوع و شماره پورت خروجی بسته} {سابنت شبکه مقصد} {آدرس آی پی شبکه مقصد}

مثال:

```
Router(config)#ip route 192.168.100.0 255.255.255.0 fastethernet 0/0
```

روش دیگر: می توان به جای نوع و شماره پورت خروجی، آدرس آی پی دستگاه بعد از روتر را که می تواند بسته را به مقصد برساند وارد کرد. مثلا در سناریوی ذیل در روتر تهران می توانیم آدرس آی پی روتر بندرعباس (10.10.10.1) را بنویسیم:

```
Router(config)#ip route 192.168.100.0 255.255.255.0 10.10.10.1
```

## ب - مسیر یابی پویا :

در این روش به جای اینکه مدیر شبکه تک تک شبکه ها را به همه روتر ها معرفی کند، روتر ها خودشان شبکه های مجاور خود را به یکدیگر معرفی میکنند و با هم مرتبا در تماسند تا جداول مسیریابی مرتب بروزرسانی شود. پرتکل مسیریابی RIP یکی از روش های مسیریابی پویاست. در این روش ما با دستور router نوع پرتکل مسیریابی را معرفی می کنیم سپس آدرس شبکه های مجاور روتر را که میخواهیم روتر به بقیه معرفی کند با دستور network معرفی می کنیم. مثال:

در روتر تهران:

```
Router(config)#router RIP
Router(config-router)#ver 2
Router(config-router)#network 192.168.200.0
Router(config-router)#network 10.10.10.0
Router(config-router)#exit
```

در روتر بندرعباس:

```
Router(config)#router RIP
Router(config-router)#ver 2
Router(config-router)#network 192.168.100.0
Router(config-router)#network 10.10.10.0
Router(config-router)#exit
```

پس از آن در صورتی که تنظیمات مربوط به آدرس و غعال سازی سایر پورت ها به درستی انجام شده باشد . روتر ها خودشان شبکه های مجاور خود را به هم معرفی می کنند و مسیر بسته ها بین دو شبکه غیر مجاور بر قرار می شود.

### ذخیره تنظیمات روتر:

دستوراتی که برای روتر مینویسیم در حافظه موقت روتر ثبت و اعمال می شوند به همین علت با خاموش شدن روتر همگی پاک میشوند، برای اینکه تنظیمات بر روی روتر ذخیره شود و با خاموش شدن روتر پاک نشود می توان از دستور

copy running-config startup-config و یا دستور Write در محیط Privileged استفاده کرد.

مثال:

```
Router#copy running-config startup-config
```

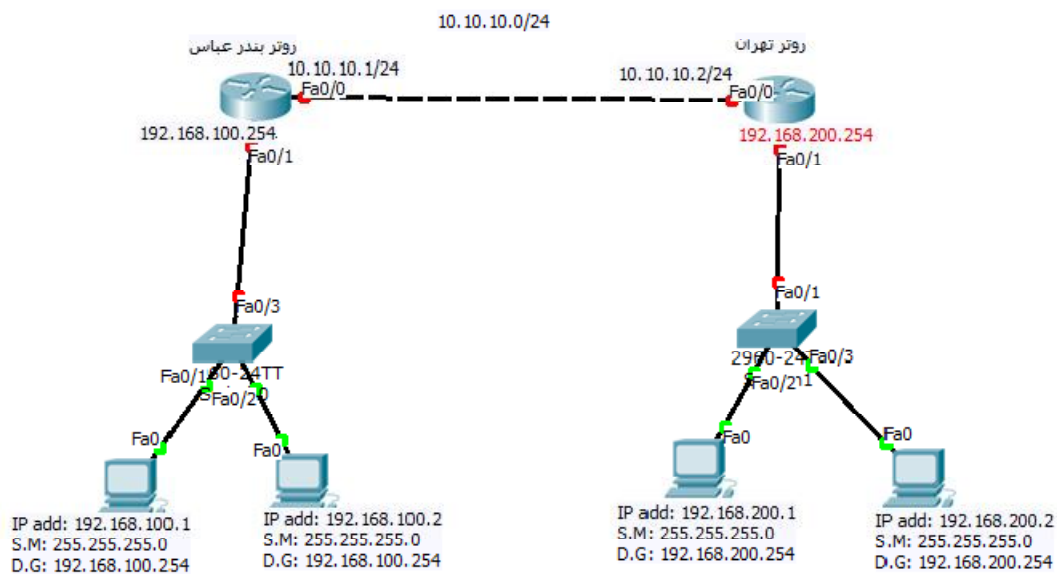
یا

```
Router#write
```



## شرح سناریو تمرین 1:

میخواهیم بین دو شبکه مختلف که در دو منطقه متفاوت قرار گرفته اند و آدرس IP شبکه آنها با هم متفاوت است با استفاده از دو دستگاه روتر سیسکو ارتباط برقرار کنیم. به گونه ای که به عنوان مثال کامپیوتر با آدرس آی پی 192.168.100.1 بتواند با کامپیوتر 192.168.200.1 مطابق شکل زیر ارتباط برقرار کند.



برای این منظور پس از برقراری ارتباط مناسب بین سیستم ها با سوئیچ ها و روتر ها ابتدا آدرس های IP را به همراه subnet mask و Default Gateway مطابق شکل فوق بر روی کامپیوتر ها تنظیم میکنیم. سپس در هر روتر تنظیمات زیر را انجام می دهیم.

در روتر تهران:

در این روتر ابتدا از مد user به مد privileged می رویم ، سپس با دستور `configure terminal` به مد global می رویم، سپس با دستور `interface fastethernet 0/1` وارد محیط fastethernet 0/1 می شویم و آدرس آی پی آن را تنظیم میکنیم. و با دستور `shutdown` این interface را فعال می کنیم. سپس خارج شده و به سراغ fastethernet 0/0 می رویم و آن را نیز فعال و آدرس دهی میکنیم. سپس خارج شده و به مد Global بر میگردیم و با دستور `IP ROUTE` مسیر بسته ها را برای رفتن به شبکه 192.168.100.0 مشخص میکنیم. در پایان نیز دستورات را ذخیره میکنیم. متن کامل دستورات:

```
Enable>enable
Router#configure terminal
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 192.168.200.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 10.10.10.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 192.168.100.0 255.255.255.0 fastethernet 0/0
Router(config)#exit
Router#copy running-config startup-config
```

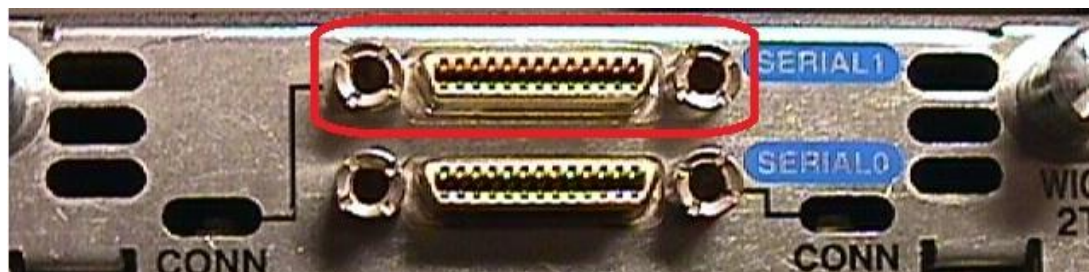
در روتر بندر عباس:

در این روتر نیز همه تنظیمات مانند روتر تهران است فقط آدرس های آی پی متفاوت هستند.

```
Enable>enable
Router#configure terminal
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 192.168.100.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 192.168.200.0 255.255.255.0 fastethernet 0/0
Router(config)#exit
Router#copy running-config startup-config
```

## اتصال دو روتر با استفاده از کابل سریال:

گاهی اوقات برای اتصال دو روتر در فواصل دور از هم در بستر مخابراتی از مودم هایی استفاده می کنیم که با پورت سریال روتر وصل می شوند. برای این منظور باید روتر ما دارای پورت سریال باشد:

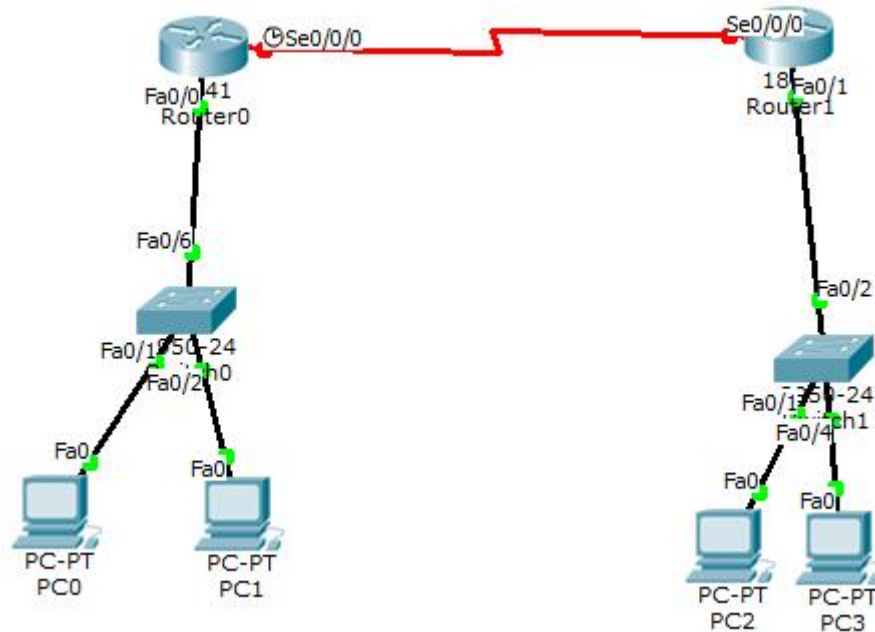


اگر روتر ما فاقد پورت سریال باشد ولی امکان نصب ماژول را داشته باشد می توانیم ماژول پورت سریال را بر روی روتر نصب کنیم:



به عنوان مثال می توان به روتر cisco1841 ماژول WIC-1T را اضافه نمود.

به این ترتیب می توان دو روتر را با استفاده از پورت سریال به هم مرتبط نمود.



تنظیمات این روش نیز مانند حالت قبل است. فقط هنگام تنظیم کردن آدرس آی پی روی **interface**ها و فعال کردن آنها باید توجه کنیم که نوع **interface** از **fastethernet** به **serial** تبدیل شده است:

```
Router(config)#interface serial 0/0/0
```

```
Router(config-if)#ip address 192.168.100.254 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config-if)#exit
```

### دستور Clock rate:

در موارد استفاده از پورت سریال باید در سمتی که با نام **CSU** شناخته می شود ( با علامت ساعت مشخص می شود) از دستور **Clock rate 64000** استفاده کنیم. این دستور در محیط همان **interface** سریال نوشته می شود. مثال: در روتر بندرعباس می نویسیم:

```
Router(config)#interface serial 0/0/0
```

```
Router(config-if)#clock rate 64000
```

```
Router(config-if)#exit
```

## تنظیمات امنیتی روترها:

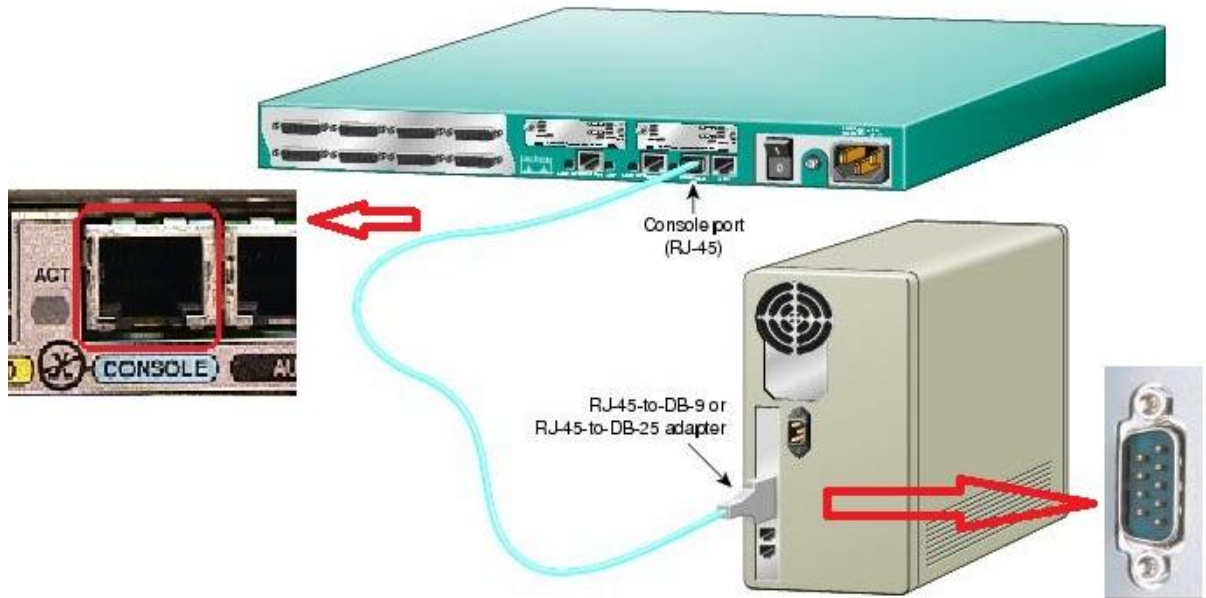
برای اینکه هر شخصی نتواند به تنظیمات روتر ما دسترسی پیدا کند و در آن اختلال یا از آن سوء استفاده کنید بایستی بر روی روتر رمز عبور گذاشته شود. از آنجا که روتر به روش های مختلف و در محیط های مختلف قابل دسترس است برای هر محیط و هر روش می توان رمز جداگانه ای قرار داد.

برخی از روش های دسترسی به روتر عبارتند:

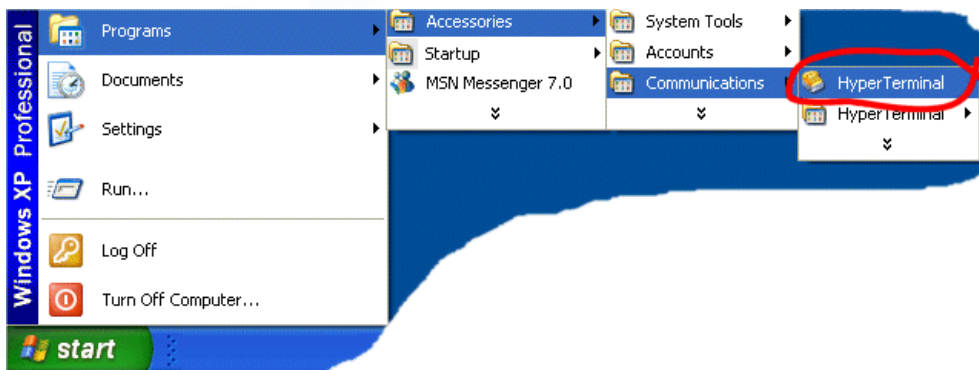
### 1 - دسترسی به روتر با استفاده از کابل کنسول:



این روش در دسترس ترین راه برای کسانی است که به صورت فیزیکی و از نزدیک به روتر دسترسی دارند. همچنین هنگام تنظیم اولیه روتر معمولاً از این روش استفاده می شود. در این روش از کابلی به نام کابل کنسول استفاده می شود، یک سر آن که سوکت RJ45 دارد به پورت Console روتر و سر دیگر آن به پورت سریال کامپیوتر متصل می شود.



پس از این اتصال با کمک نرم افزاری مانند **hyper terminal** و یا **putty** می توان به روتر متصل شد. با خاموش و روشن کردن روتر، دسترسی به محیط **CLI** روتر از طریق نرم افزار ممکن می شود.



در نرم افزار **cisco packet tracer** در هر کامپیوتر در قسمت **Desktop** محیطی به نام **Terminal** وجود دارد که مشابه نرم افزار **hyper terminal** واقعی عمل می کند.

برای قرار دادن یک رمز عبور برای کاربران متصل شده با کابل کنسول دستورات زیر را در محیط **global** می نویسیم:

```
Router-tehran(config)#line consol 0
Router-tehran(config-line)#password cisco
Router-tehran(config-line)#login
Router-tehran(config-line)#exit
```

در مثال فوق پس از اجرای دستورات از این به بعد عبارت **cisco** به عنوان کلمه عبور تعیین شده و از کاربران متصل شده با کابل کنسول پرسیده می شود.

## 2- دسترسی به روتر با استفاده از telnet:

این روش برای کاربرانی که می خواهند از راه دور به روتر متصل شوند و آنرا تنظیم یا بررسی کنند بسیار مناسب است.

در این روش آنها دستور **telnet** را در محیط **Command Prompt** سیستم عامل خود به صورت زیر استفاده میکنند:

آدرس آی پی روتر **telnet**

مثال: دسترسی به روتر تهران با **telnet** در مثال فوق:

```
PC1>telnet 192.168.200.254
```

برای فعال کردن اتصال از طریق **Telnet** و قرار دادن یک رمز عبور برای کاربران متصل شده از طریق **Telnet** دستورات زیر را در محیط **global** می نویسیم:

```
Router-tehran(config)#line vty 0 5  
Router-tehran(config-line)#password ccna  
Router-tehran(config-line)#login  
Router-tehran(config-line)#exit
```

در مثال فوق پس از اجرای دستورات از این به بعد عبارت **ccna** به عنوان کلمه عبور تعیین شده و از کاربران متصل شده از طریق **telnet** پرسیده می شود.

## برخی نکات در مورد امنیت روترها:

### 1 - قرار دادن رمز عبور برای ورود به Privileged Mode :

از آنجا که مد Privileged دارای دسترسی سطح بالا است و پیش زمینه ورود به مد Global نیز هست ، همیشه سعی می شود با قرار دادن رمز عبور برای ورود به این مد امنیت روتر را بالا برد. برای قرار دادن رمز عبور برای ورود به Privileged Mode در مد global دستور enable password را می نویسیم.مثال:

```
Router-tehran(config)#enable password ccnp
```

در مثال فوق پس از اجرای دستورات از این به بعد عبارت **ccnp** به عنوان کلمه عبور تعیین شده و از تمام کاربرانی که بخواهند (با دستور Enable) وارد مد Privileged شوند به صورت زیر پرسیده می شود:

```
Router-tehran>enable  
Password: ?
```

### 2 - رمز گذاری کلمات عبور :

با توجه به وجود برخی دستورات گزارش گیری (مانند Show running-configuration) که تمام دستورات روتر از جمله رمز های عبور را نمایش می دهند این احتمال هست که رمز های عبور روتر توسط افرادی که در نزدیکی ما قرار دارند سرقت شود، برای جلوگیری از چنین مواردی می توان کلمات عبور را به صورت رمز شده نمایش داد تا به راحتی سرقت نشوند. برای رمز گذاری کلمات عبور دستور زیر را در مد global می نویسیم:

```
Router-bandarabbas(config)#service password-encryption
```

مثال:

قبل از اجرای دستور:

```
Router(config)#do show running-config
```

```
Building configuration...
```

```
no service password-encryption
```



```
hostname Router
```

```
enable password ccna
```

کلمه عبور قابل تشخیص است:

اجرای دستور رمزگذاری کلمات عبور:

```
Router (config)#service password-encryption
```

پس از اجرای دستور:

```
Router(config)#do show running-config
```

```
Building configuration...
```

```
service password-encryption
```

```
hostname Router
```

```
enable password 7 0835495D1D
```

کلمه عبور به رمز در آمده است:

**دستور hostname :**

با استفاده از این دستور یک نام برای روتر انتخاب می کنیم. این نام از این به بعد در محیط CLI در ابتدای هر خط دستور نمایش داده می شود. این دستور در مد Global اجرا می شود. مثال:

```
Router(config)#hostname router-tehran
Router-tehran(config)#
```

**دستورات بررسی وضعیت روتر :**

اکثر این دستورات در مد privileged اجرا می شوند. برخی از آنها عبارتند از:

**دستور show running-config :**

با اجرای این دستور در مد privileged می توان بسیاری از تنظیمات سیستم را مشاهده کرد . مثال:

```
Router#show running-config
Building configuration...

no service password-encryption

hostname Router

spanning-tree mode pvst

interface FastEthernet0/0

ip address 192.168.100.254 255.255.255.0

duplex auto

speed auto

--More--
```

**دستور** : show ip route

با اجرای این دستور در مد **privileged** می توان جدول مسیر یابی را مشاهده کرد . مثال:

Router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

- \* candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

24/10.0.0.0 is subnetted, 1 subnets

C 10.10.10.0 is directly connected, FastEthernet0/1

C 192.168.100.0/24 is directly connected, FastEthernet0/0

S 192.168.200.0/24 is directly connected, FastEthernet0/1

## دستور show interfaces :

با اجرای این دستور در مد privileged می توان اطلاعاتی در مورد interface های روتر مشاهده کرد .  
مثال:

```
Router#show interfaces
```

```
FastEthernet0/0 is up, line protocol is up (connected)
```

```
Hardware is Lance, address is 00d0.bc69.1101 (bia 00d0.bc69.1101)
```

```
Internet address is 192.168.100.254/24
```

## دستور ping :

از این دستور برای بررسی برقراری ارتباط با یک دستگاه دیگر استفاده می شود. در این روش یک یا چند بسته اطلاعاتی برای گیرنده فرستاده می شود و گیرنده پس از دریافت به ما پاسخ می دهد. اگر از سمت مقابل پاسخ دریافت شود یعنی ارتباط برقرار است در غیر این صورت احتمالاً مشکلی وجود دارد. شکل کلی دستور ping به صورت زیر است. در مد privileged می نویسیم:

```
Router#ping آدرس آی پی مقصد
```

مثال:

```
Router#ping 10.10.10.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
```

```
!!!
```

```
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms
```

در مثال فوق علامت های «!» نشانه دریافت صحیح پاسخ (reply) هستند. و نقطه ها «.» نشانه دریافت نشدن پاسخ (time out) می باشند.

**نکته:** در صورتی که در مد Global باشیم و بخواهیم دستورات مد privileged را اجرا کنیم می توانیم قبل از دستور کلمه do را اضافه نماییم. مثال:

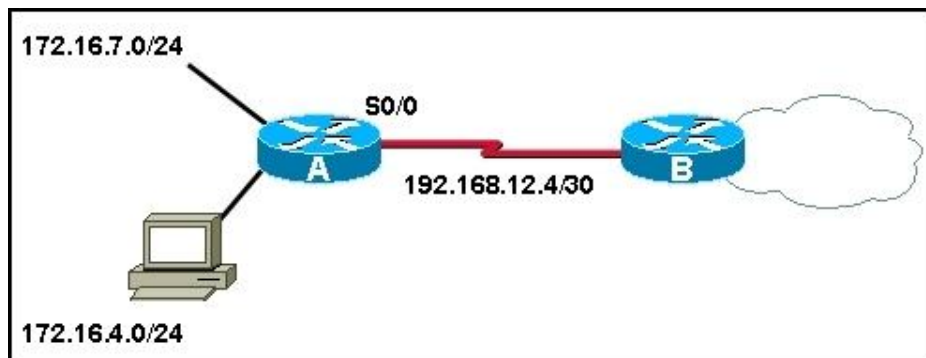
```
Router(config)#do show interfaces
```

```
FastEthernet0/0 is up, line protocol is up (connected)
```

```
Hardware is Lance, address is 00d0.bc69.1101 (bia 00d0.bc69.1101)
```

```
Internet address is 192.168.100.254/24
```

## تنظیم جدول مسیر یابی برای دسترسی به اینترنت:



در این قسمت می خواهیم ارتباط شبکه های مرتبط با روتر را با اینترنت برقرار کنیم. برای این منظور بر روتر در مد global با استفاده از دستور ip route (مسیریابی static) به روتر می گوییم که تمام بسته هایی را که آدرس آنها در زیر شبکه های ما وجود ندارد به سمت آدرس IP که شرکت سرویس دهنده اینترنتی به ما معرفی کرده (به عنوان gateway ما که خودش یک روتر است) هدایت کند. برای مشخص کردن تمام شبکه های ناشناس می توانیم از آدرس شبکه 0.0.0.0 با سابنت 0.0.0.0 استفاده کنیم.

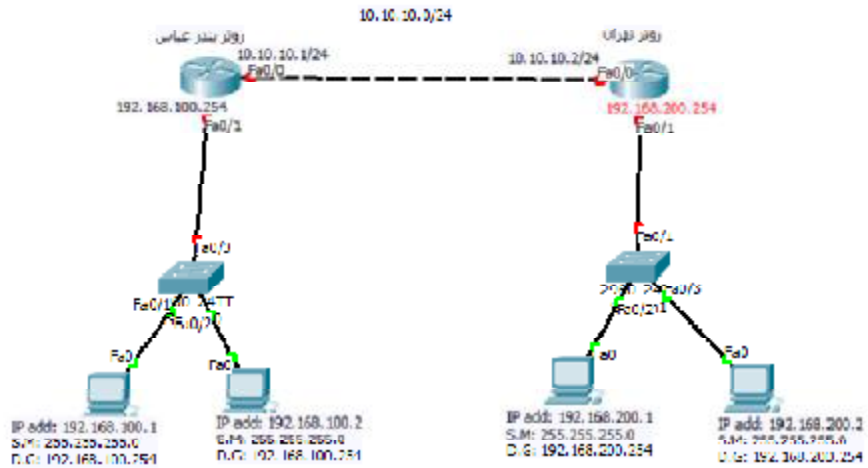
مثلا در شکل فوق فرض کنید روتر A متعلق به ماست و روتر B متعلق به ISP می باشد و آی پی آن (B) 192.168.12.6 می باشد.

ما بایستی در روتر A این دستور را اضافه کنیم:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.12.2
```

البته به جای آدرس آی پی می توان نام پورت خروجی روتر A را نیز نوشت.

**نکته:** اگر می خواهیم این مثال را در packet tracer پیاده سازی کنیم، باید بر روی هر دو روتر قرار داده شده این دستور را بنویسیم تا ارتباط دو طرفه برقرار شود. مثلا فرض کنید روتر تهران را به عنوان Gateway اینترنت در نظر گرفته ایم:



در این صورت:

در روتر بندرعباس:

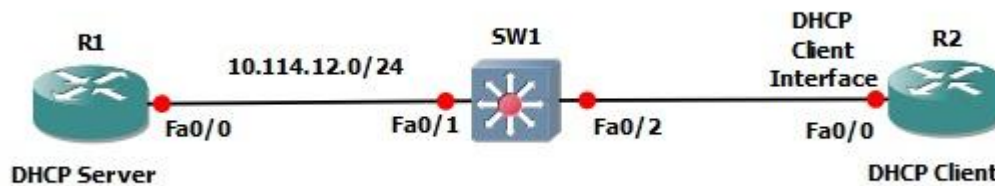
```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

و در روتر تهران:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

## راه اندازی DHCP Server در روتر سیسکو<sup>1</sup>:

در این بخش یاد میگیریم که چطور یک روتر رو به DHCP سرور تبدیل کنیم برای این کار سناریو ساده زیر رو در نظر داریم:



کانفیگ روتر: R1

```
interface FastEthernet0/0
description ### LAN INTERFACE ###
ip address 10.114.12.1 255.255.255.0
no shut
```

در اولین مرحله یک DHCP POOL با نام دلخواه را پیکربندی میکنیم

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool LAB_POOL1
```

اختصاص رنج ip به پول dhcp

```
R1(dhcp-config)#network 10.114.12.0 /24
```



کانفیگ زمان ip Release ها

```
R1(dhcp-config)#lease 7
```

کانفیگ DNS سرور

```
R1(dhcp-config)#dns-server 10.114.18.6 10.114.18.7
```

کانفیگ دیفالت گیت وی:

```
R1(dhcp-config)#default-router 10.114.12.1  
R1(dhcp-config)#end
```

خوب به وقت لازمه که به رنج IP رو از پول بیرون بکشیم که به کلاینت ها اختصاص داده نشه  
برای این کار از کامند زیر در محیط کانفیگ استفاده میکنیم:

```
R1(config)#ip dhcp excluded-address 10.114.18.0 10.114.18.10
```

: کانفیگ سمت کلاینت

```
R2#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#interface FastEthernet0/0  
R2(config-if)#ip address dhcp  
R2(config-if)#end
```

## : NAT

NAT یا همان Network Address Translation مکانیزم ترجمه آدرس می باشد جهت برقراری ارتباط با اینترنت و یا جهت Secure کردن شبکه .  
 NAT با ترجمه کردن آدرسهای Private به آدرسهای رجیستر شده کار ترجمه را انجام می دهد . این ترجمه می تواند یک به یک و یک به چند باشد . بنابراین می توان با توجه به نحوه ترجمه NAT را به سه دسته کلی تقسیم کرد :

- ۱. Static NAT
- ۲. Dynamic NAT
- ۳. Dynamic NAT With Overload

Static NAT ترجمه یک به یک و دوتای آخر ترجمه یک به چند می باشد . روتر اطلاعات لازم برای Translation را در یک Table نگهداری می کند و ترجمه براساس آن صورت می گیرد . در حالتی که Static NAT استفاده کنیم این Table بدون تغییر باقی می ماند در حالی که اگر از Dynamic NAT و یا Dynamic NAT with Overload استفاده شود این Table تغییر می کند .

## راه اندازی NAT استاتیک در روتر سیسکو<sup>2</sup>

در مواقعی که کاربران خارجی به دستگاههای داخلی مثل سرورهای DNS ، WEB و یا کاربران داخلی متصل می شوند، از NAT استاتیک استفاده می کنیم. دستورات بکار رفته به شکل زیرند :

```

1 Router (config)# ip nat inside source static
2 inside_local_source_IP_address
3 inside_global_source_IP_address
4 Router (config)# ip nat outside source static
5 outside_local_destination_IP_address
6 outside_global_destination_IP_address

```

پارامترهای Inside و outside مسیری را که باید عمل ترجمه صورت گیرد را نشان می دهد. برای مثال کلمه inside به این معنی است که یک آدرس inside source local به یک آدرس inside global ترجمه می شود. کلمه outside نیز نشان دهنده این است که یک آدرس outside destination global به یک آدرس outside local ترجمه می گردد. بعد از این مرحله نیز باید interface های داخلی یا inside و خارجی یا outside را تعیین نماییم. به صورت زیر :

```

Router (config)#Interface type [slot_# / ] port_#
2 Router (config-if)#ip nat inside | outside

```

پارامتر inside را در روی interface متصل به LAN و پارامتر outside را در روی interface متصل به اینترنت بکار می‌بریم. برای آشنایی بیشتر با NAT استاتیک به مثالی که در شکل زیر آورده شده توجه کنید. در این مثال یک آدرس global برابر با 200.200.200.1 به سرور WEB داخلی با آدرس 10.1.1.1 تخصیص یافته است. پیکر بندی مربوطه به شکل زیر خواهد بود :

```

1 Router (config)#ip nat inside source static 192.168.1.1 200.200.200.1
2 Router (config)#interface ethernet 0
3 Router (config-if)#ip nat inside
4 Router (config-if)#exit
5 Router (config)#interface serial 0
6 Router (config)#ip nat outside

```

دستور **ip nat inside source static** عمل ترجمه آدرس را فعال می‌کند. عبارات **ip nat** و **ip nat inside** outside نیز مشخص می‌کنند که کدام interface به اینترنت (S0) و کدام interface به LAN داخلی (S1) متصل می‌باشد. به یاد داشته باشید که هر ترافیکی که با قانونهای تعیین شده مطابقت نداشته باشد، بین این دو اینترنتیس منتقل گردند، باید از ACL برای اینکار استفاده نماییم .

## راه اندازی NAT دینامیک در روترهای سیسکو

برای استفاده از NAT دینامیک باید اقدام به مشخص نمودن سه چیز بکنیم :

- لیست آدرسهای داخلی که باید روی آنها عمل ترجمه صورت بگیرد.
- لیست آدرسهای خارجی که آدرسهای داخلی باید به آنها ترجمه شوند.
- اینترنتیس هایی که باید در عمل ترجمه آدرسها دخالت نمایند.

برای رسیدن به هدف اول، یعنی تعیین کردن دستگاههایی که آدرس آنها باید ترجمه شود. دستورات زیر را باید نوشت :

```

Router(config)#ip nat inside source list standard_IP_ACL_# pool
1 NAT_pool_name

```

بعد از دستور **ip nat inside source list** باید شماره ACL حاوی لیست دستگاههای مجاز را بیاوریم. در مورد آدرسهایی که در لیست ACL دارای پارامتر **permit** می‌باشند عمل ترجمه یا **address translation**

صورت گرفته ولی در مورد آدرسهای که با پارامتر deny مشخص شده اند و یا بوسیله implicit deny حذف می شوند، عمل ترجمه صورت نمی گیرد. سپس بعد از پارامتر pool باید اسمی را به این رنج آدرس تخصیص دهیم. هدف دومی که در بالا نیز گفته شد، تعیین کردن رنج آدرسهای عمومی یا public است که آدرسهای داخلی به آنها ترجمه می شوند. دستورات زیر را برای تعیین کردن رنج آدرسهای عمومی بکار می بریم :

```
1Router(config)#ip nat pool NAT_pool_name
2begining_inside_global_IP_address
3ending_inside_global_IP_address
4netmask subnet_mask_of_address
```

بعد از دستور ip nat pool اسمی را که در دستور اول به pool تخصیص داده بودیم نوشته و سپس آدرس شروع و پایانی، به همراه ماسک مربوطه را نیز باید مشخص نمود. آخرین هدف ما تعیین کردن اینترفیس های دخیل در عمل ترجمه می باشد. یعنی باید مشخص کنید که کدام اینترفیس به اینترنت و کدام اینترفیس به LAN متصل است. برای مثال می توان به مورد اشاره شده در مثال قبل اشاره کرد. در این مثال در مورد دو کامپیوتر A و B عمل NAT دینامیک صورت گرفته است. بیکربندی مربوطه چنین خواهد بود :

```
1Router(config)#ip nat inside source list 1 pool ITPro
2Router(config)#access-list 1 permit 192.168.1.10 0.0.0.0
3Router(config)#access list 1 permit 192.168.1.11 0.0.0.0
4Router(config)#ip nat pool ITPro 200.200.200.0 200.200.200.3 netmask
5255.255.255.0
6Router(config)#interface ethernet0
7Router(config-if)#ip nat inside
8Router(config)#interface serial0
9Router(config-if)#ip nat outside
```

دستور اول، آدرس دستگاههایی را که مجاز به ترجمه هستند تعیین می کند. توجه داشته باشید که این دستگاهها، همان دستگاههایی هستند که در ACL 1 مشخص شده اند (192.168.1.11, 192.168.1.10) آدرسهای عمومی یا public را که آدرس های اشاره شده باید به آنها ترجمه شوند را در لیستی به نام ITPro آورده ایم. آدرسهای این لیست توسط دستور ip nat pool مشخص شده اند. سپس ethernet0 به عنوان اینترفیس داخلی و serial0 به عنوان اینترفیس خارجی تعیین شده اند.

## راه اندازی Dynamic NAT with overload (PAT) در روترهای

### سیسکو:

برای پیکربندی NAT به روش dynamic سه مرحله رو انجام میدیم :

- 1- تعریف یک pool با یک نام مشخص و قرار دادن آدرسهای public در داخل آن pool
- 2- تعریف آدرسهای private مجاز به استفاده از NAT با یک Access-list
- 3- فعال کردن NAT به روش dynamic

مراحل پیکربندی PAT شبیه به NAT دینامیک بوده و سه مرحله را برای انجام کار باید طی نمود. اولین مرحله مشخص کردن لیست دستگانهایی است که عمل ترجمه روی آنها انجام خواهد شد. دستوری که برای اینکار استفاده می شود شبیه دستوری است که در NAT دینامیک هم مورد استفاده قرار گرفت. اما در آخر دستور کلمه **overload** را هم باید اضافه نمود که نشان دهنده این است که به جای NAT از PAT استفاده می کنیم :

```
1Router(config)# ip nat source list standard_IP_ACL_#
2pool NAT_pool_name Overload
```

در مرحله دوم لیست آدرسهای global مورد نیاز را باید مشخص نمود. دستور بکار برده شده در اینجا نیز مثل دستوری است که در NAT دینامیک نیز استفاده شد :

```
1Router(config)#ip nat pool NAT_pool_name
2begining_inside_global_IP_address
3ending_inside_global_IP_address
4netmask subnet_mask_of_address
```

مرحله آخر تعیین کردن interface هایی است که در عمل ترجمه شرکت خواهند نمود. دستورات مورد استفاده نیز به صورت ip nat inside و ip nat outside است که به ترتیب نشان دهند interface داخلی و خارجی می باشند. برای درک مسئله (در مثال قبل) فقط یک آدرس در داخل گروه آدرسهای global به صورت 200.200.200.0 قرار دارد :

```
1Router(config)# ip nat inside source list 1 pool ITPro overload
2Router(config)#access-list 1 permit 192.168.1.10 0.0.0.0
3Router(config)#access-list 1 permit 192.168.1.11 0.0.0.0
4Router(config)#ip nat pool ITPro 200.200.200.20 200.200.200.2 net mask
5255.255.255.0
6Router(config)#interface ethernet0
7Router(config)#ip nat inside
8Router(config)#exit
9Router(config)#interface serial 0
9Router(config)#ip nat outside
```

نکته: در دستورات فوق در پیاده سازی PAT بجای دستور خط 1 یعنی:

```
Router(config)# ip nat inside source list 1 pool ITPro overload
```

می توان از دستور زیر نیز استفاده کرد:

```
Router(config)# ip nat inside source list 1 interface ethernet0 overload
```

یعنی می توانیم به جای نام pool نام اینترفیسی را که داخلی ( inside ) است بیاوریم که بسیار کار ما را ساده تر میکند و دیگر نیاز به تعریف pool نداریم.

مراجع:

[1] <http://ciscopersian.blogspot.com/1393/03/03/post-54/#ixzz3Pf0jFYy9>

[2] عاطفه حسین زاده . آموزش راه اندازی NAT و PAT در روترهای سیسکو. انجمن حرفه ای های فناوری اطلاعات ایران.