



آزمایش شماره ۶

آز شبکه - دکتر بردیا صفایی

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

نیم سال اول ۰۱-۰۲

گروه ۸:

مهرشاد میرمحمدی - ۹۸۱۰۹۶۳۴

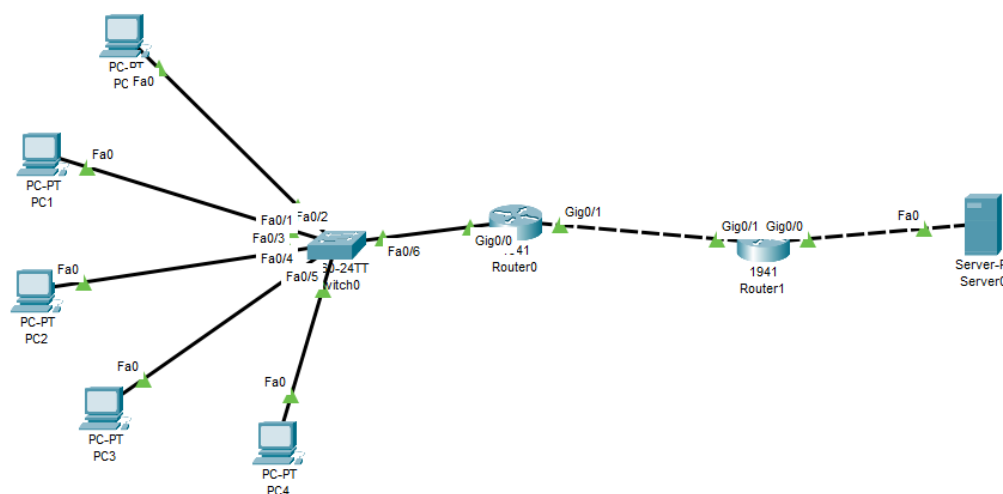
پرهام صارمی - ۹۷۱۰۱۹۵۹

محمد رضا مفیضی - ۹۸۱۰۶۰۵۹



۱ Static Nat

ابتدا در محیط packet tracer سناریو گفته شده در کلاس را طراحی می‌کنیم. نتیجه‌ی طراحی را می‌توانید در شکل ۱ مشاهده کنید. به تمام interface ها هم ای‌پی‌ای همانند سناریوی مشخص شده می‌دهیم. سپس جداول مسیریابی مسیریاب‌ها را همان‌گونه که در آزمایش‌های قبلی یادگرفتیم، تنظیم می‌کنیم.



شکل ۱: تصویر پیاده‌سازی سناریو در محیط packet tracer

سپس دستورات مشخص شده در دستور آزمایش را مطابق تصویر ۲ در مسیریاب ۱ وارد می‌کنیم. در نهایت دستورهای ping 100.0.0.1 و 50.0.0.2 را اجرا می‌کنیم. همان‌طور که از تصویر ۳ مشخص است، نتایج مورد انتظار را بدست می‌آوریم.

۲ Dynamic Nat

ابتدا جداول مسیریابی را به روز می‌کنیم تا از ای‌پی‌های جدید هم پشتیبانی کنند. سپس دستورات مشخص شده را در مسیریاب ۲ وارد می‌کنیم و وارد حالت debug ip nat می‌شویم. بعد از آن هم از سمت کاربران، سرور را ping می‌کنیم تا نتایج شکل ۴ حاصل شود. همان چیزی که انتظار داریم را مشاهده می‌کنیم. در نهایت هم از حالت debug ip nat خارج می‌شویم.

۳ PAT

تغییرات خواسته شده را در مسیریاب ۳ وارد می‌کنیم و سپس از کاربران، سرور را ping می‌کنیم. همان‌طور که انتظار داریم، به درستی ترجمه اتفاق می‌افتد (تصویر ۵). توجه شود در این حالت ممکن است به یک ای‌پی چندین اتصال ترجمه شوند، برای مثال در تصویر ۵ به هر دو کاربر یک ای‌پی نسبت داده شده است. ولی در حالت قبلی به هر ای‌پی فقط یک ای‌پی دیگر می‌توانست ترجمه شود و بنابراین حداکثر به تعداد ای‌پی‌هایی که برای ترجمه داریم، می‌توانستیم اتصال هم‌زمان داشته باشیم.



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#ip nat ins
Router(config)#ip nat inside s
Router(config)#ip nat inside source sta
Router(config)#ip nat inside source static 50.0.0.2 100.0.0.1
Router(config)#interfa
Router(config)#interface Gi
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat in
Router(config-if)#ip nat inside
Router(config-if)#exi
Router(config-if)#exit
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip nat o
Router(config-if)#ip nat outside
Router(config-if)#ex
Router(config-if)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

شکل ۲: اجرای دستورات آزمایش داخل مسیریاب اول

۴ سوالات

۱.۴

سه نوع دستور قابل تولید هستند: inside، outside، pool دستور نوع inside برای ترجمه‌های مربوط به سمت inside مورد استفاده قرار می‌گیرم. دستور مشابه دیگر، نوع outside است که مشابه به دستور بالاست ولی برای ترجمه‌های سمت outside استفاده می‌شود. این دو نوع دستور رو به دو صورت می‌توان اجرا کرد.

- حالت اول: ترجمه‌ی یک به یک است که به صورت زیر استفاده می‌شود.



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 50.0.0.2

Pinging 50.0.0.2 with 32 bytes of data:

Reply from 30.0.0.6: Destination host unreachable.
Reply from 30.0.0.6: Destination host unreachable.
Reply from 30.0.0.6: Destination host unreachable.
Reply from 30.0.0.6: Destination host unreachable.

Ping statistics for 50.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 100.0.0.1

Pinging 100.0.0.1 with 32 bytes of data:

Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126
Reply from 100.0.0.1: bytes=32 time<1ms TTL=126

Ping statistics for 100.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

شکل ۳: حاصل اجرای دستورهای ping در حالت Static Nat

`ip nat inside/outside source static <real ip address> <nat ip address>`
همچنین در این حالت می‌توان پروتکل و پورت‌ها را هم مشخص کرد که دستور به صورت زیر می‌شود.
`ip nat inside/outside source static <protocol>? <outside global ip> <global port>? <outside local ip>
<local port>?`

- حالت دوم: ترجمه با استفاده از `access list` ها و `pool` و `interface` است. `access list` برای مشخص کردن ارتباطی است که قرار است ترجمه شوند و همچنین `pool` هم لیست آدرس‌های قابل استفاده به عنوان ترجمه را می‌دهد. استفاده آن به صورت زیر است.

`ip nat inside/outside source list <access list number or name> pool <pool name>`



The screenshot shows a Cisco Router CLI window titled "Router0". The "CLI" tab is selected. The command history shows the following commands: Router#, Router#, Router#, Router#de, Router#debu, Router#debug ip, Router#debug ip na, Router#debug ip nat, and IP NAT debugging is on. The output shows several NAT translations and ICMP expiring messages. The translations are: NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [122], NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [69], NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [123], NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [70], NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [124], NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [71], NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [125], NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [72], NAT: expiring 40.0.0.3 (30.0.0.1) icmp 119 (119), NAT: expiring 40.0.0.3 (30.0.0.1) icmp 120 (120), NAT: expiring 40.0.0.3 (30.0.0.1) icmp 121 (121), NAT: expiring 40.0.0.3 (30.0.0.1) icmp 122 (122). The window also has a "Copy" button and a "Paste" button. A "Top" button is at the bottom left.

شکل ۴: حاصل گزارش‌گیری از ترجمه در حالت Dynamic Nat

ip nat inside/outside source list <access list name> interface <interface>
در این حالت هم می‌توان با اضافه کردن کلمه‌ی overload به انتهای دستور، از حالت PAT استفاده کرد.
دستور نوع آخر هم برای تعریف کردن pool استفاده می‌شود. این دستور به صورت زیر می‌تواند استفاده شود.
ip nat pool <pool name> [<ip address>] netmask <ip netmask>



The screenshot shows a Cisco Router CLI window titled "Router0". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area displays the "IOS Command Line Interface" with the following commands and outputs:

```
Router#
NAT: expiring 40.0.0.3 (30.0.0.1) icmp 130 (130)
NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [134]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [85]
NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [135]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [86]
NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [136]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [87]
NAT: s=30.0.0.1->40.0.0.3, d=100.0.0.1 [137]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.1 [88]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [16]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [89]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [17]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [90]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [18]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [91]
NAT: s=30.0.0.2->40.0.0.3, d=100.0.0.1 [19]
NAT*: s=100.0.0.1, d=40.0.0.3->30.0.0.2 [92]
```

At the bottom of the window, there is a status bar with "Ctrl+F6 to exit CLI focus", "Copy", and "Paste" buttons. A "Top" button is also visible in the bottom left corner.

شکل ۵: حاصل گزارش‌گیری از ترجمه در حالت Pat

۲.۴

دو نوع Standard و Extended دارند. در حالت استاندارد فقط می‌توان بر حسب آی‌پی مبدا فیلتر کرد. این لیست‌ها از نظر پردازشی کم‌هزینه‌تر هستند. اگر از عددی در بازه ۱-۹۹ یا ۱۳۰۰-۱۹۹۹ استفاده کنیم، به معنای استفاده کردن از حالت استاندارد است. اما حالت دیگر، حالت گسترش‌یافته است که امکان فیلتر کردن بر حسب آی‌پی و پروت مبداء و مقصد و همچنین پروتکل را می‌دهد. اگر از عددی در بازه ۱۰۰-۱۹۹ یا ۲۰۰۰-۲۶۹۹ استفاده کنیم، به معنی استفاده از حالت گسترش یافته است. البته این امکانات بیشتر باعث شده تا از نظر محاسباتی، هزینه‌برتر هم باشند. کاربرد حالت اول زمانی است که بر اساس آی‌پی بخواهیم فیلتر کنیم، برای مثال فقط به اتصالاتی که از ماشین خاصی برقرار شده



باشند، پاسخ دهیم. حالت دوم ولی زمانی مورد استفاده قرار می‌گیرد که به امکانات بیشتری نیاز باشد. برای مثال زمانی که اجازه ندهیم تا به پورت خاصی، دسترسی پیدا شود. چون بر روی آن پورت ممکن است سرور حساسی که نیاز امنیتی دارد، وجود داشته باشد.

دستور 80 eq 100.0.0.1 0.0.0.0 deny tcp any access-list 42 بسته‌هایی که از پروتکل tcp استفاده می‌کنند، از هر مبدای باشند، و مقصدشان 100.0.0.1 باشد با wildcard 0.0.0.0 و پورت 80 داشته باشند را نمی‌گذارد رد بشوند. اگر می‌خواستیم می‌توانستیم آدرس مقصدی هم مشخص نکنیم و آن را هم any بگذاریم.

۳.۴

همان‌طور که قبل‌تر هم گفته شد، در این حالت ممکن است اتصالات مختلف به یک آی‌پی ترجمه شوند اما پورت‌های مختلفی داشته باشند. این خیلی خوب است چون مشکل IPv4 را تا حد زیادی برطرف می‌کند. همان‌طور که در تصویر ۵ هم می‌بینیم، به هر دو کاربر یک و دو، یک آی‌پی داده شده است بنابراین شماره پورت متفاوتی داشته‌اند. اگر بخواهیم می‌توانیم با استفاده از دستور show ip nat translations به صورت دقیق‌تر ببینیم که هر آی‌پی و پورت‌ای به چه آی‌پی و پورت‌ای ترجمه شده‌است.

۴.۴

پورت‌هایی از NAT که از شبکه‌ی خارجی در دسترس است، اهمیت زیادی دارند. چرا که پورت‌های مختلف می‌توانند سرورهای گوش به فرمان مختلفی را داشته باشند که نباید بتوان از دنیای بیرون به آنها متصل شد. همچنین پورت‌های داخلی فقط در داخل NAT معنی دارند و پورت‌های خارجی هم در دنیای بیرون معنی دارند.

برای تعویض پورت خروجی و ورودی هم کافیست پورت‌های مورد انتظار را در زمان ساخت access list همان‌گونه که در حالت گسترش‌یافته در سوال دو دیدیم، اضافه کنیم.