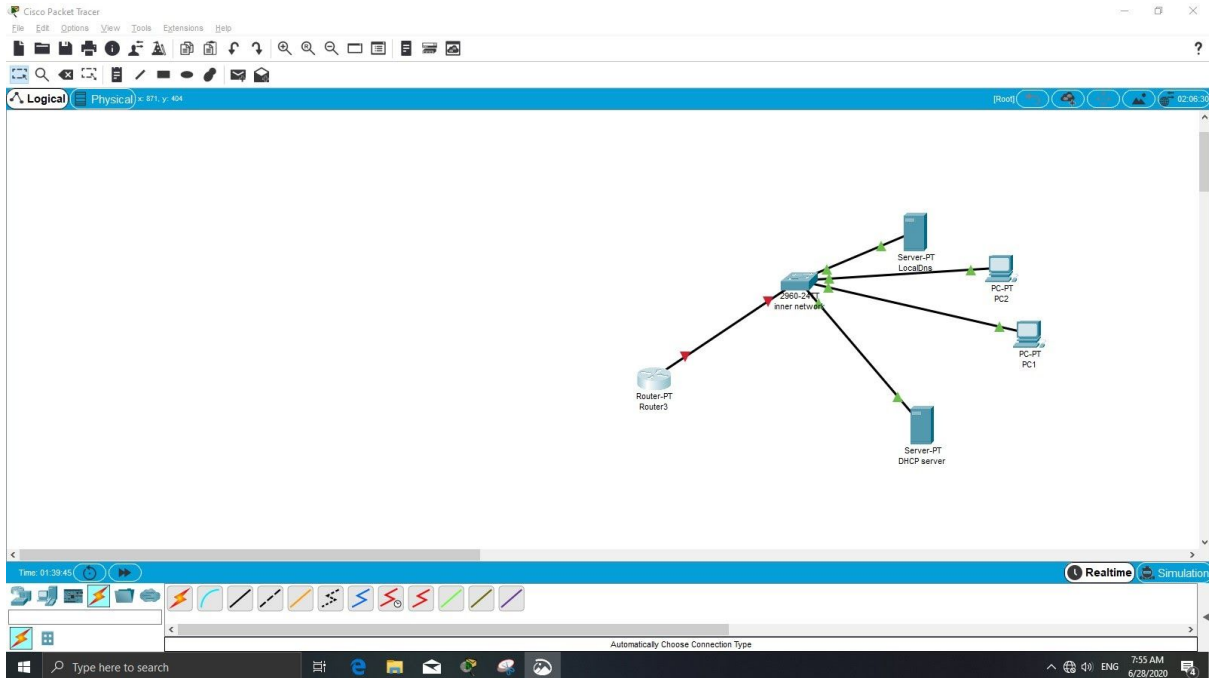
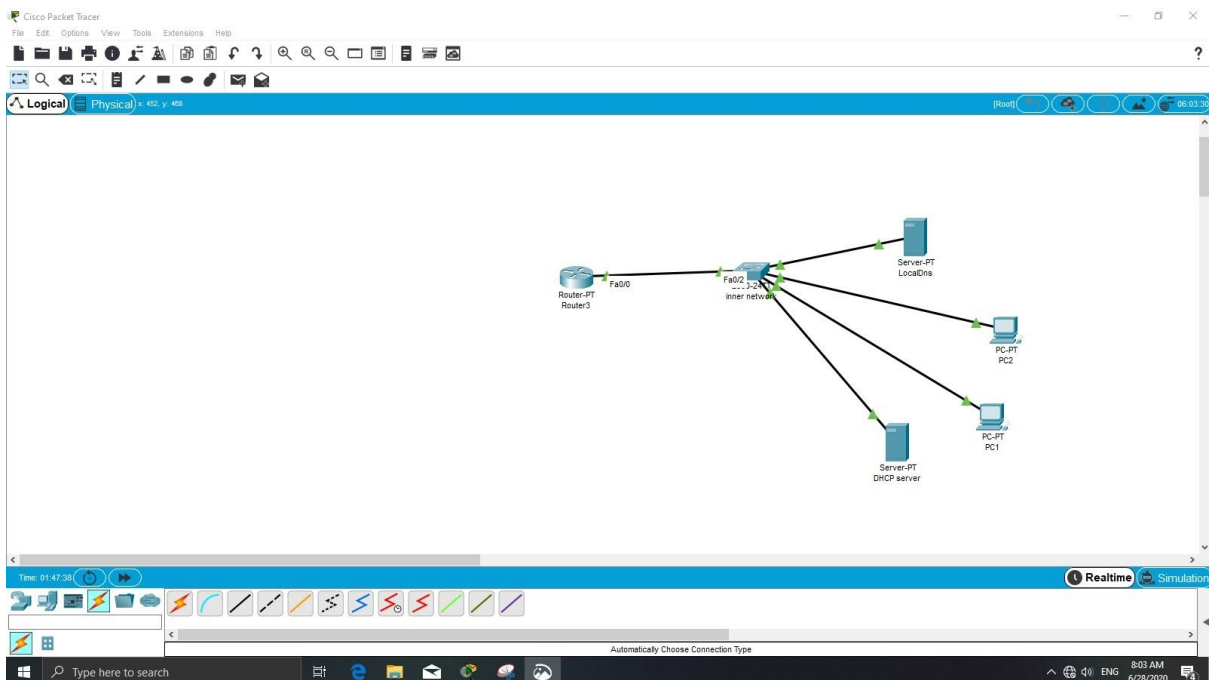



محمد عبدالهی 9530153

من برای پیاده سازی این تمرین از packet tracer که در آزمایشگاه شبکه داشتیم استفاده کردم. در مرحله اول کار ساختار کلی شبکه داخلی را طراحی کردم که با توجه به مطالبی بود که در آزمایشگاه شبکه داشتیم در این ساختار یک dns سرور و یک dhcp سرور و دو کامپیوتر قرار دارد که ip خود را از dhcp سرور میگیرند و همه به یک سویچ مرکزی متصلند.



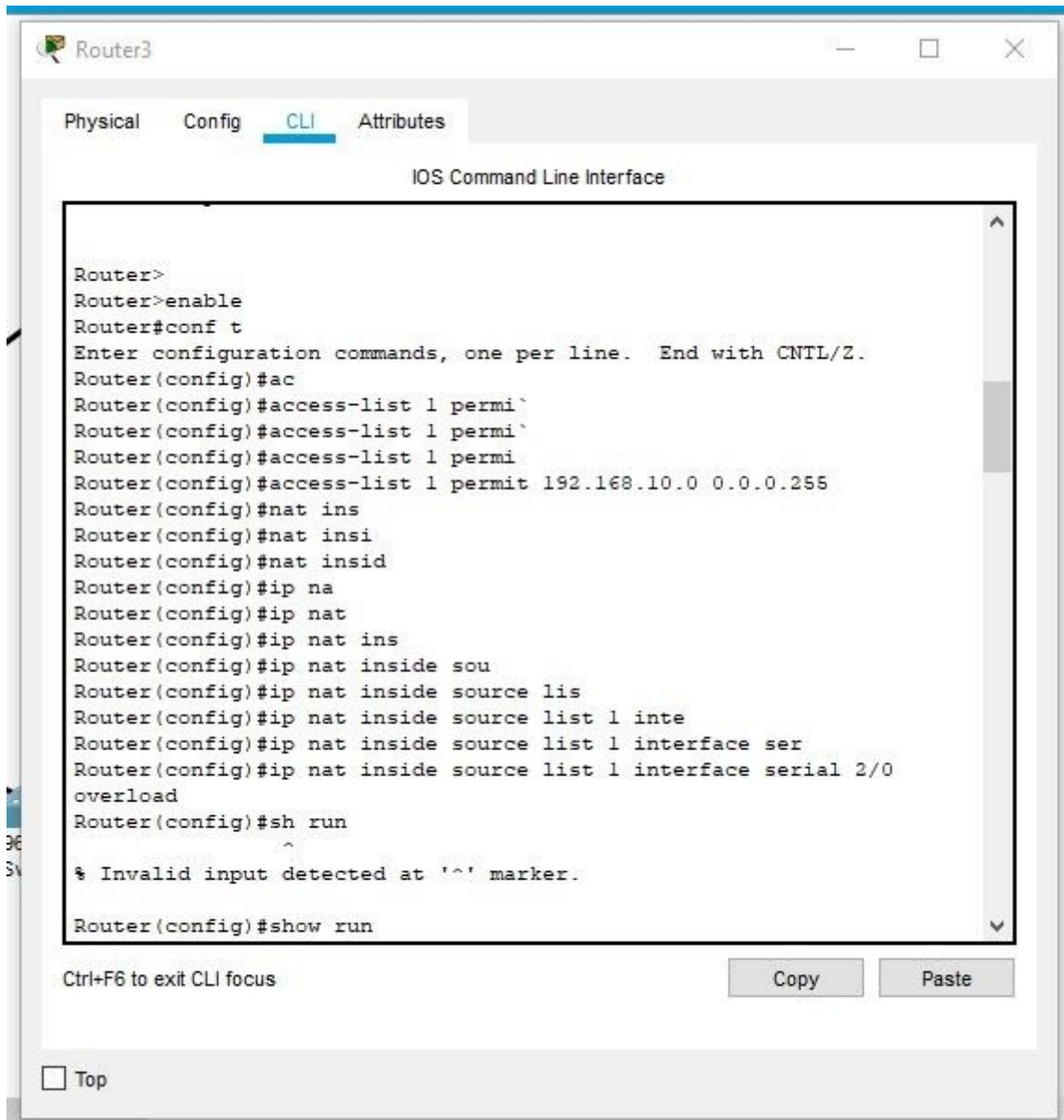
در مرحله بعد لازم بود تا روتر مرکزی شبکه داخلی را کانفیگ کنم. که این امر را هم با توجه به مطالب آزمایشگاه شبکه انجام دادم و ساختار به صورت زیر شد.





The screenshot shows a PC2 window with a web browser open. The browser's address bar displays "http://test.com". The page content includes the title "Cisco Packet Tracer" and a welcome message: "Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open." Below this, there is a section for "Quick Links" with four underlined links: "A small page", "Copyrights", "Image page", and "Image". A green arrow points to the "Image page" link. The browser window has a "Go" button and a "Stop" button. The PC2 window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" being the active tab. A "Top" button is located at the bottom left of the PC2 window.

همانطور که در تصویر هم می بینید یک access-list برای شبکه داخلی معرفی کردم و به این صورت nat کردم که ترافیک این لیست از از مسیر سریال دو روتر مرکزی عبور کند.

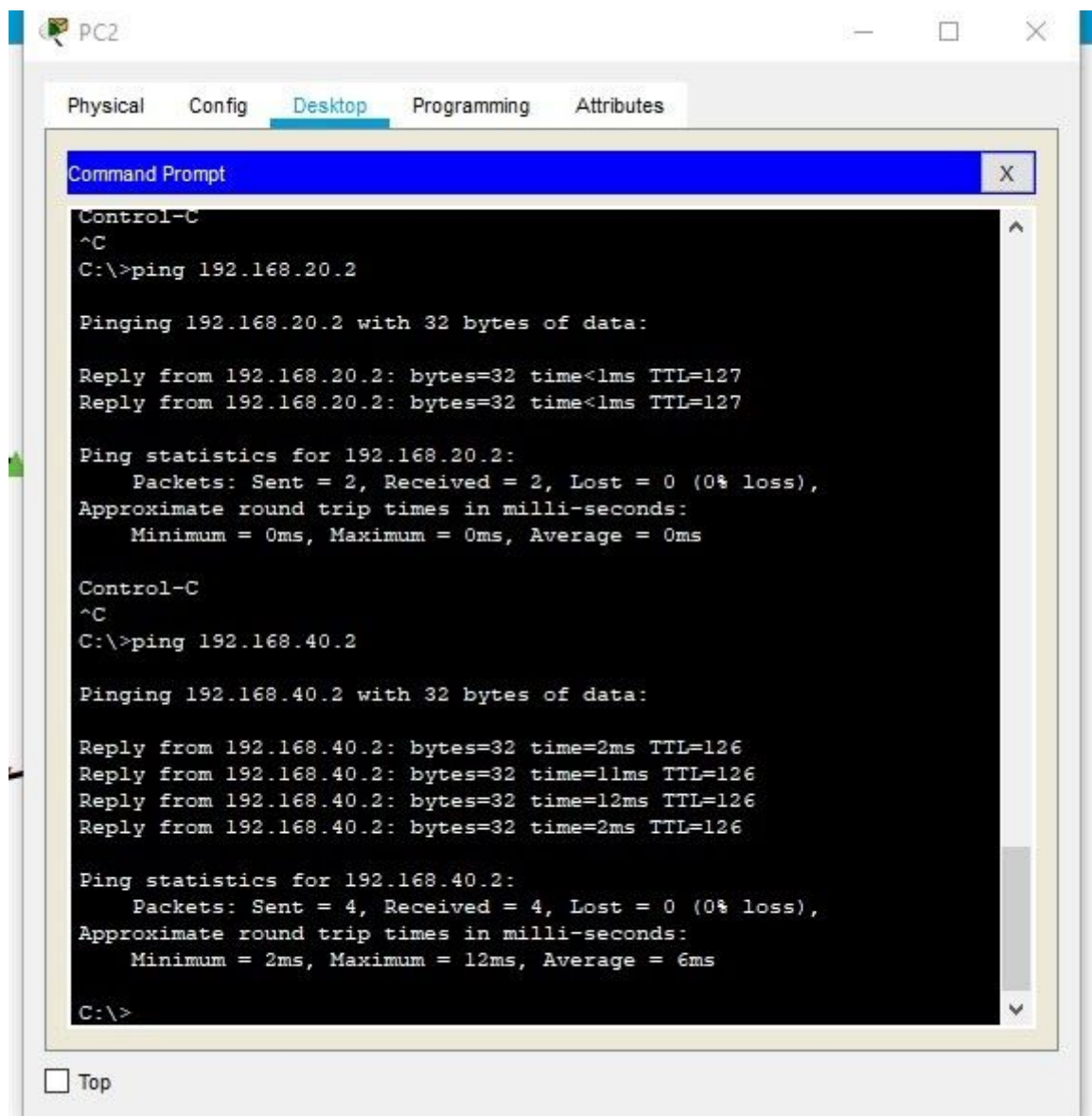


The screenshot shows a Cisco Router CLI window titled "Router3". The "CLI" tab is selected. The command history shows the following sequence of commands:

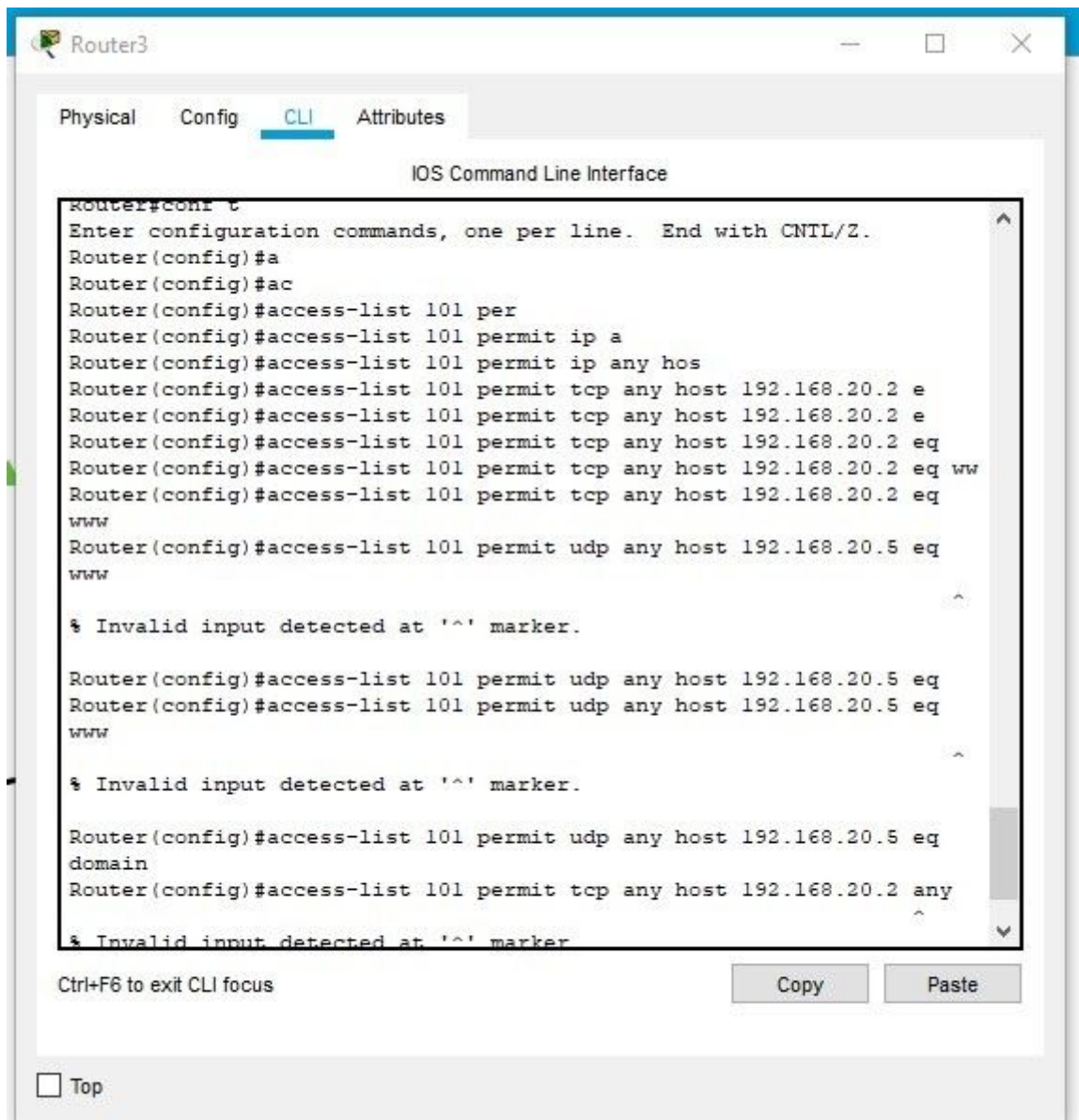
```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ac
Router(config)#access-list 1 permi`
Router(config)#access-list 1 permi`
Router(config)#access-list 1 permi
Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255
Router(config)#nat ins
Router(config)#nat insi
Router(config)#ip na
Router(config)#ip nat
Router(config)#ip nat ins
Router(config)#ip nat inside sou
Router(config)#ip nat inside source lis
Router(config)#ip nat inside source list 1 inte
Router(config)#ip nat inside source list 1 interface ser
Router(config)#ip nat inside source list 1 interface serial 2/0
overload
Router(config)#sh run
^
% Invalid input detected at '^' marker.
Router(config)#show run
```

Below the CLI window, there are buttons for "Copy" and "Paste", and a "Top" button.

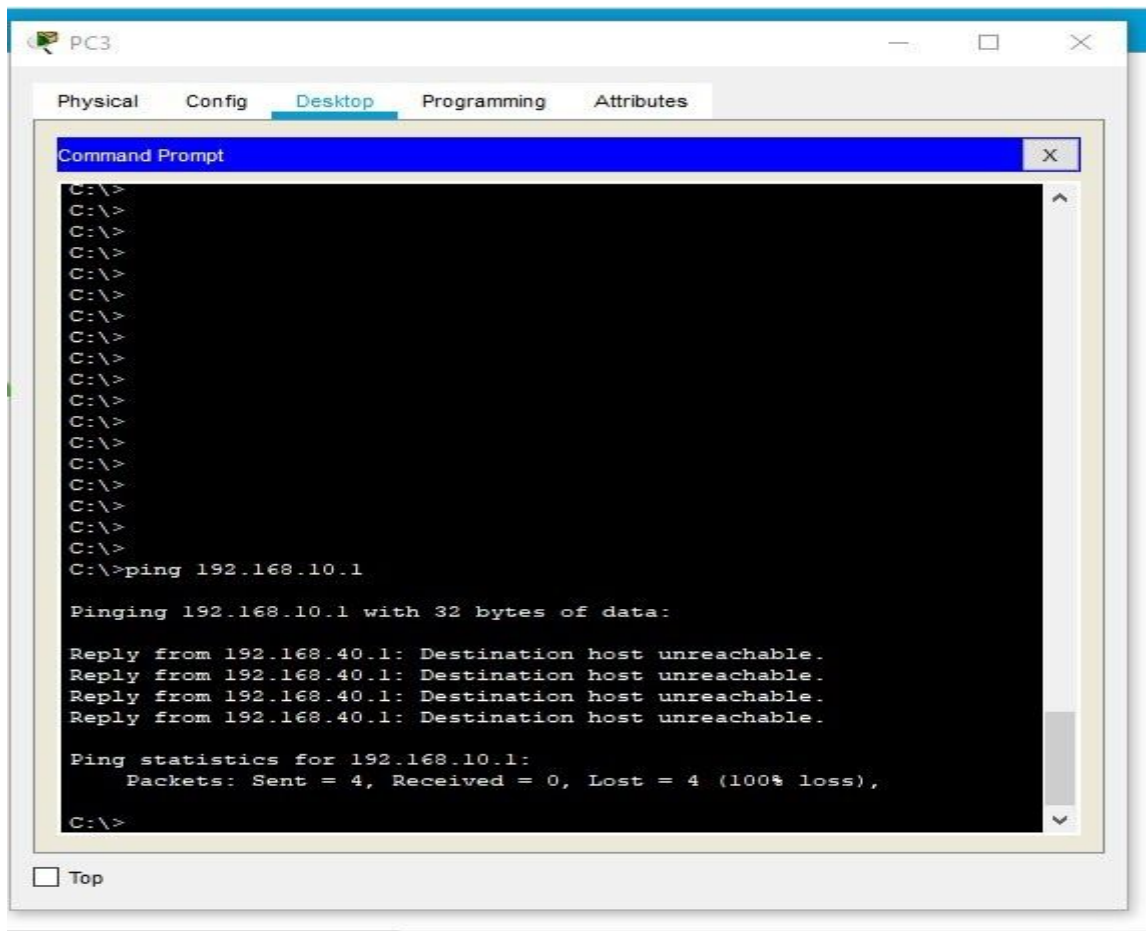
در مرحله بعد برای روتر مرزی شبکه یک روتر default تعریف کردیم که ترافیک هایی که مقصد نامشخص داشتند را به سمت روتر isp ارسال کند. در نتیجه دو عمل بالا ما از شبکه داخلی به بیرون دسترسی خواهیم داشت اما عکس آن برقرار نیست. که با توجه به عکس زیر از شبکه داخلی یکی از هاستهای بیرون شبکه را پینگ کردم و به درستی عمل کرده.



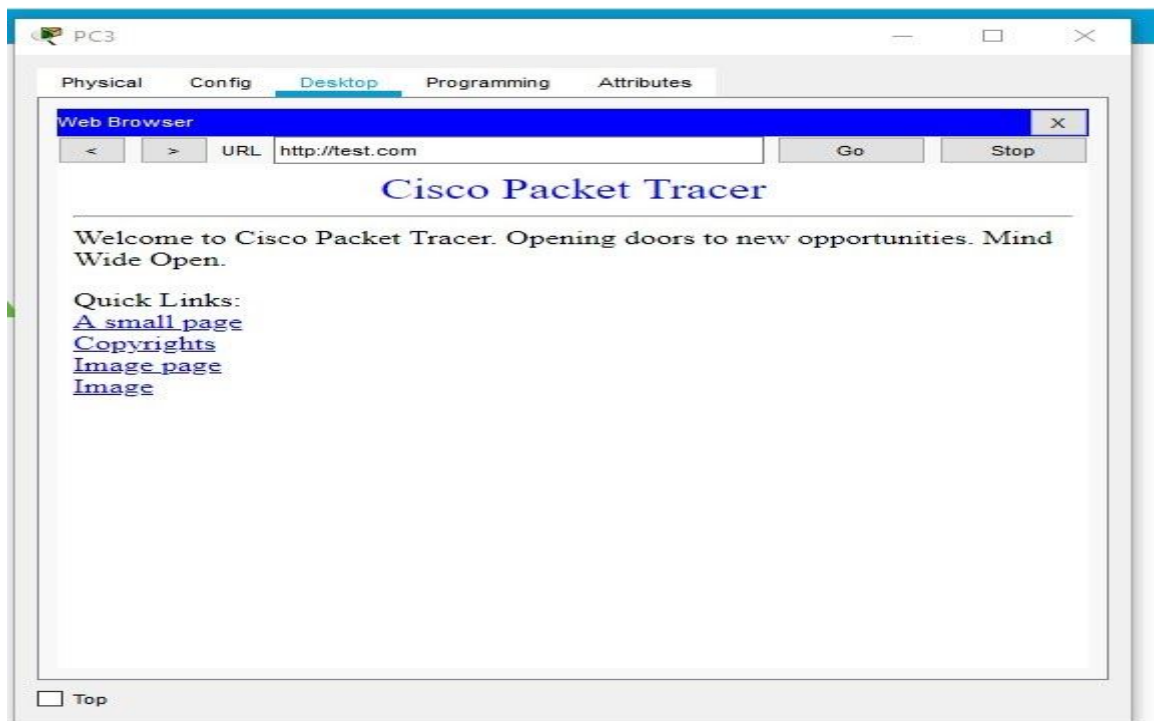
در مرحله بعد رول های مربوط به فایروال را در روتر مرزی قرار دادیم که به واسطه آن ترافیک خارجی فقط میتواند به dns سرور و سرور مربوط به dmz دسترسی پیدا کند.



همانطور که در تصویر هم پیداست هر ترافیکی از بیرون فقط اجازه دسترسی به 192.168.20.2 که سرور dmz و اجازه دسترسی به 192.168.20.5 که dns سرور مربوط به dmz است را دارد. پس شبکه داخلی ما به طور کامل امن بوده و هیچ ترافیکی از بیرون اجازه دسترسی ندارد. از هاست مربوط به شبکه بیرون یکی از کامپیوترهای درون شبکه داخلی را پینگ کردیم که اجازه دسترسی ندارد.



ولی از بیرون اگر test.com را پینگ کند به سرور ناحیه dmz وصل میشود.



در بحث ids هم از طریق کامند های مربوط به روتر میتوان این امر را محقق کرد.

از طریق دو کامند زیر

```
Router(config)# ip audit notify log
```

```
Router(config)# logging console info
```

میتوان log های سیستم را فعال کرد و این لاگ ها بر روی یک سیستم ریموت یا ویرچوال ماشین که در سطح شبکه قرار دادیم ارسال میشوند.

```
Router(config)# ip audit info {action [alarm] [drop] [reset]}
```

```
Router(config)# ip audit attack {action [alarm] [drop] [reset]}
```

از طریق دو کامند بالا میتوان کلیه اقدامات یوزرها را تحت نظر داشت و به عنوان info یا attack ثبت کرد و اقدامات لازم را در برابر آنها انجام داد که لازم است policy های مد نظر را ثبت کرد.