



به نام خدا

گزارش آزمایش شماره ۸
آزمایشگاه شبکه‌های کامپیوتری
گروه ۴

ارشیا یوسف‌نیا ۴۰۱۱۱۰۴۱۵
محمدفرحان بهرامی ۴۰۱۱۰۵۷۲۹
امیرمهدی دارایی ۹۹۱۰۵۴۳۱

استاد درس: دکتر صفایی

فهرست

۱	مقدمه	3
۲	ساختار شبکه	3
۳	ساخت DHCP Server	4
۴	تنظیم PC ها روی DHCP	4
۵	تعیین پورت Trust	6
۶	منابع	12

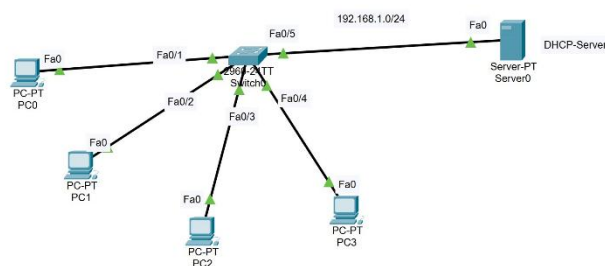
۱ مقدمه

DHCP Snooping یک ویژگی امنیتی مهم در شبکه‌های کامپیوتری است که به طور خاص برای جلوگیری از حملات مختلف در فرآیند تخصیص آدرس‌های IP به دستگاه‌ها طراحی شده است. در شبکه‌های مبتنی بر پروتکل DHCP، سرور DHCP به دستگاه‌های مختلف آدرس‌های IP اختصاص می‌دهد. این فرآیند به طور معمول به صورت خودکار و بدون نیاز به مداخله دستی انجام می‌شود، اما همین ویژگی می‌تواند هدف حملات مختلف قرار گیرد. یکی از رایج‌ترین حملات در این زمینه، حمله DHCP Spoofing است که در آن مهاجم تلاش می‌کند خود را به جای سرور DHCP معرفی کند و آدرس‌های IP جعلی به دستگاه‌ها اختصاص دهد.

DHCP Snooping با نظارت بر پیام‌های DHCP و شناسایی دستگاه‌های مجاز، از این گونه حملات جلوگیری می‌کند. این ویژگی با تعیین پورت‌های Trusted و Untrusted در سوئیچ‌ها، امکان می‌دهد که تنها درخواست‌های معتبر از سوی دستگاه‌های شناخته‌شده پاسخ داده شود و درخواست‌های غیرمجاز از سوی مهاجمان فیلتر شوند.

۲ ساختار شبکه

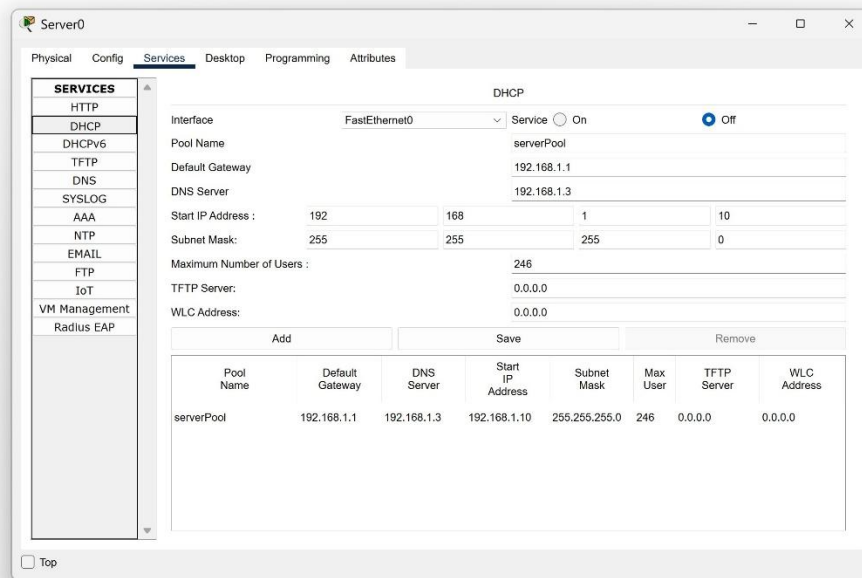
ابتدا نمای کلی شبکه را طبق چیزی که در دستورکار گفته شده است، دستگاه‌ها و سوئیچ را آورده و با اتصالات آن‌ها را می‌بندیم و برای سرور IP آن را برابر با 192.168.1.2 و Subnet Mask را نیز 255.255.255.0 قرار داده و نیز بخش Default Gateway را نیز برابر با 192.168.1.1 قرار می‌دهیم. در نهایت شبکه ساخته شده در تصویر ۱ که مانند شبکه دستورکار است قابل مشاهده است.



تصویر 1) ساختن شبکه مورد نیاز آزمایش.

۳ ساخت DHCP Server

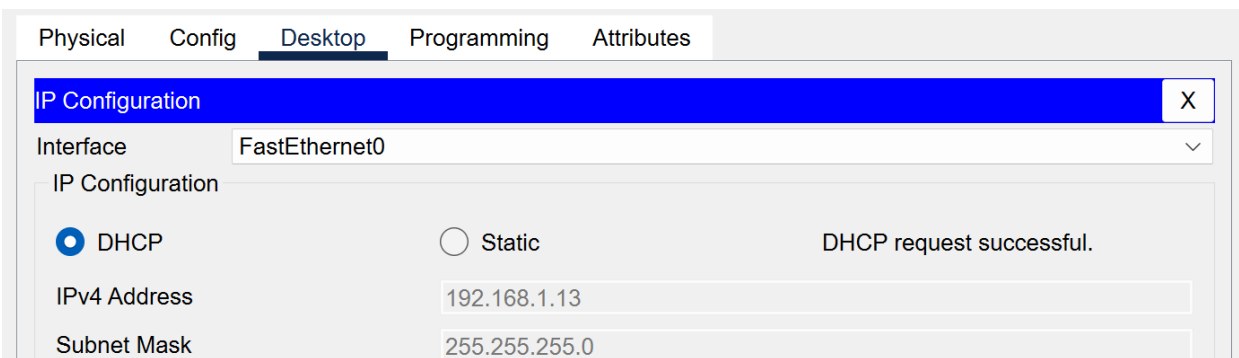
حال باید سرور موجود در شبکه را یک سرور DHCP تعیین کنیم، برای این کار، طبق فیلم راهنما وارد بخش Services در سرور شده و وارد بخش DHCP می‌شویم. تنظیمات مربوطه را طبق راهنما تعیین کرده و گزینه فعال شدن را زده و ذخیره می‌کنیم. در نتیجه ازین به بعد این سرور، یک سرور DHCP است و در تصویر ۲ می‌توان این تنظیمات را مشاهده کرد.



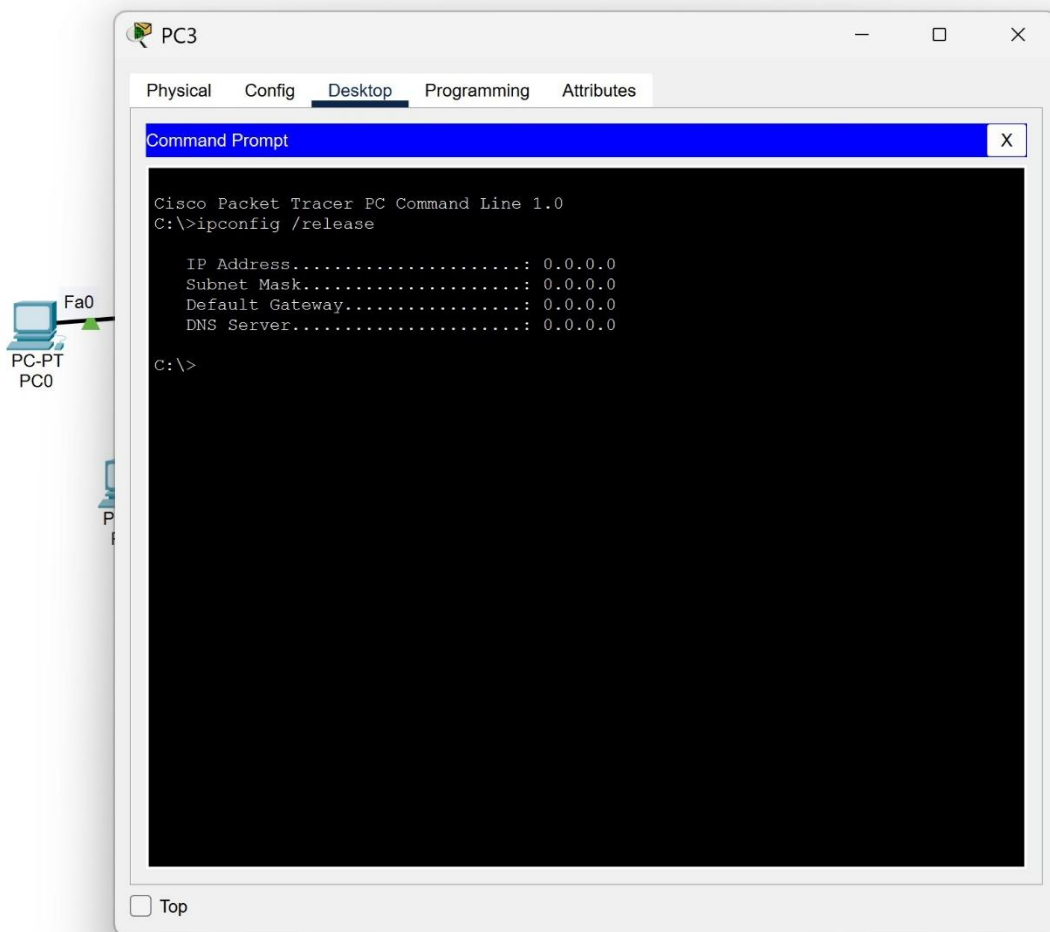
تصویر 2) ساخت سرور DHCP و تنظیم جزئیات.

۴ تنظیم PC ها روی DHCP

حال وارد تک تک PC ها شده و وارد بخش Desktop سپس در بخش IP Configuration شده، حال باید IP Config را روی حالت DHCP گذاشت. مشاهده می‌کنیم که یک درخواست برای سرور فرستاده شده و یک IP به PC اختصاص داده شده است که در تصویر ۳ قابل مشاهده است. درنهایت برای اینکه بتوانیم ادامه آزمایش را به درستی پیش ببریم، باید وارد CLI هر PC شده و دستور /release را وارد کرده تا IP ها پاک شوند که در تصویر ۴ قابل مشاهده است. حال برای ادامه آزمایش آماده هستیم.



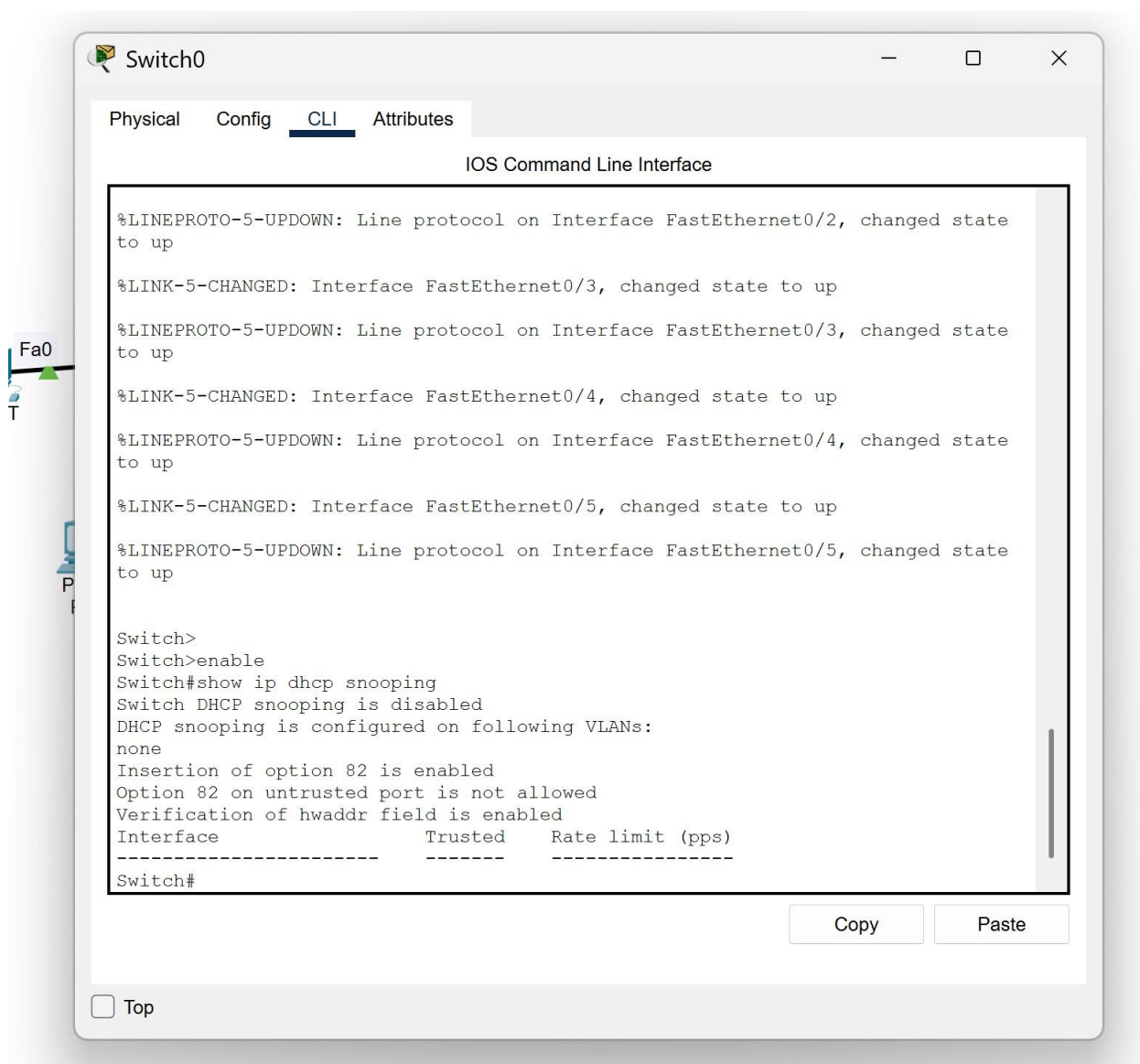
تصویر 3) اختصاص داده شدن IP



تصویر 4) اجرای دستور release در ترمینال.

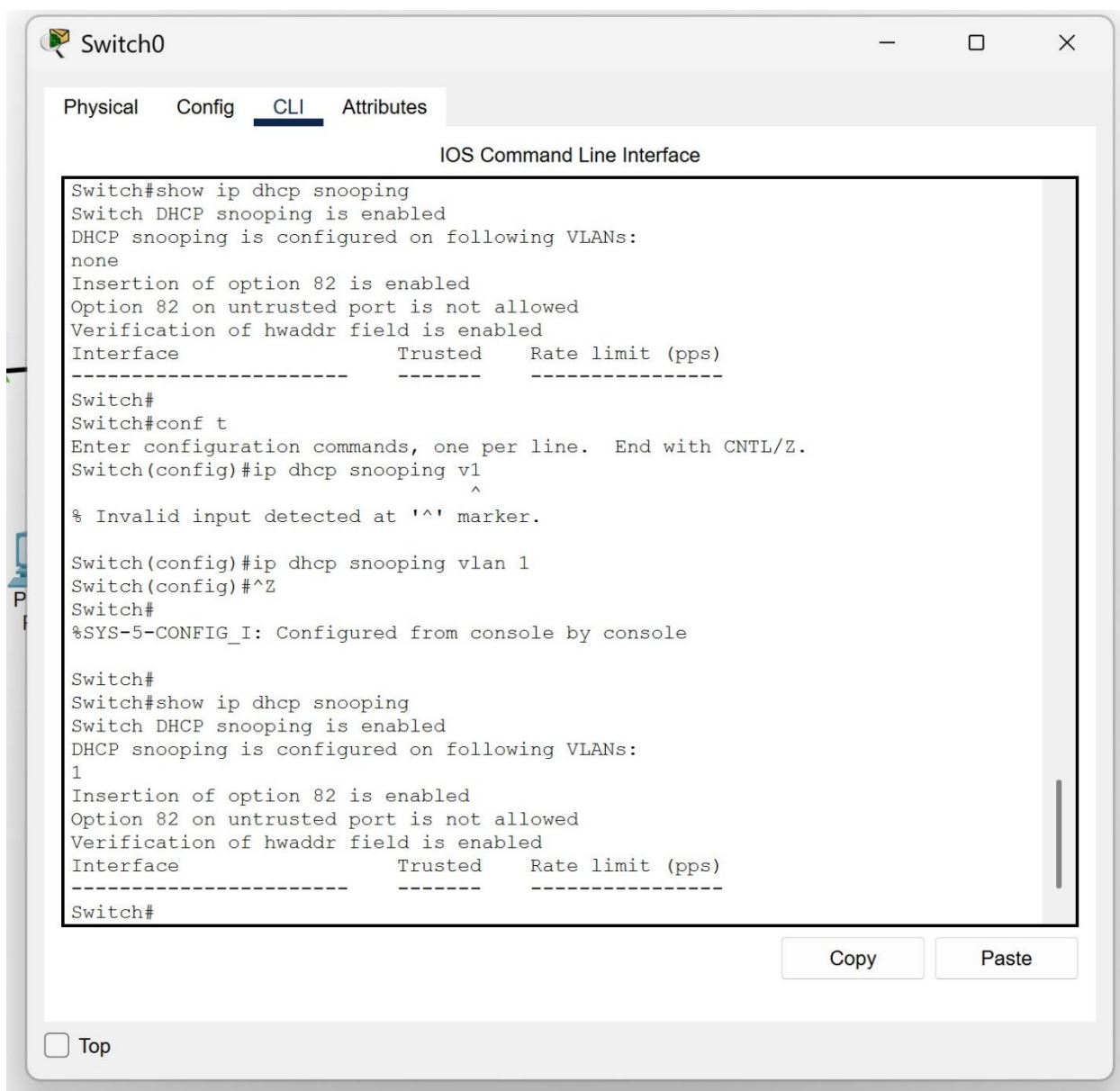
۵ تعیین پورت Trust

وارد ترمینال سوییچ شده و طبق دستور راهنما لیست پورت‌های Trusted را در تصویر ۵ مشاهده می‌کنیم. در این تصویر می‌بینیم که DHCP Snooping فعال نیست.



تصویر 5) مشاهده لیست پورت‌های Trusted.

حال طبق راهنما DHCP Snooping را فعال کرده و روی vlan 1 قرار می‌دهیم که در تصویر ۶ قابل مشاهده است.



The screenshot shows a network switch configuration window titled "Switch0". It has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and displays the following commands and output:

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface          Trusted      Rate limit (pps)
-----
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping vl
^
% Invalid input detected at '^' marker.

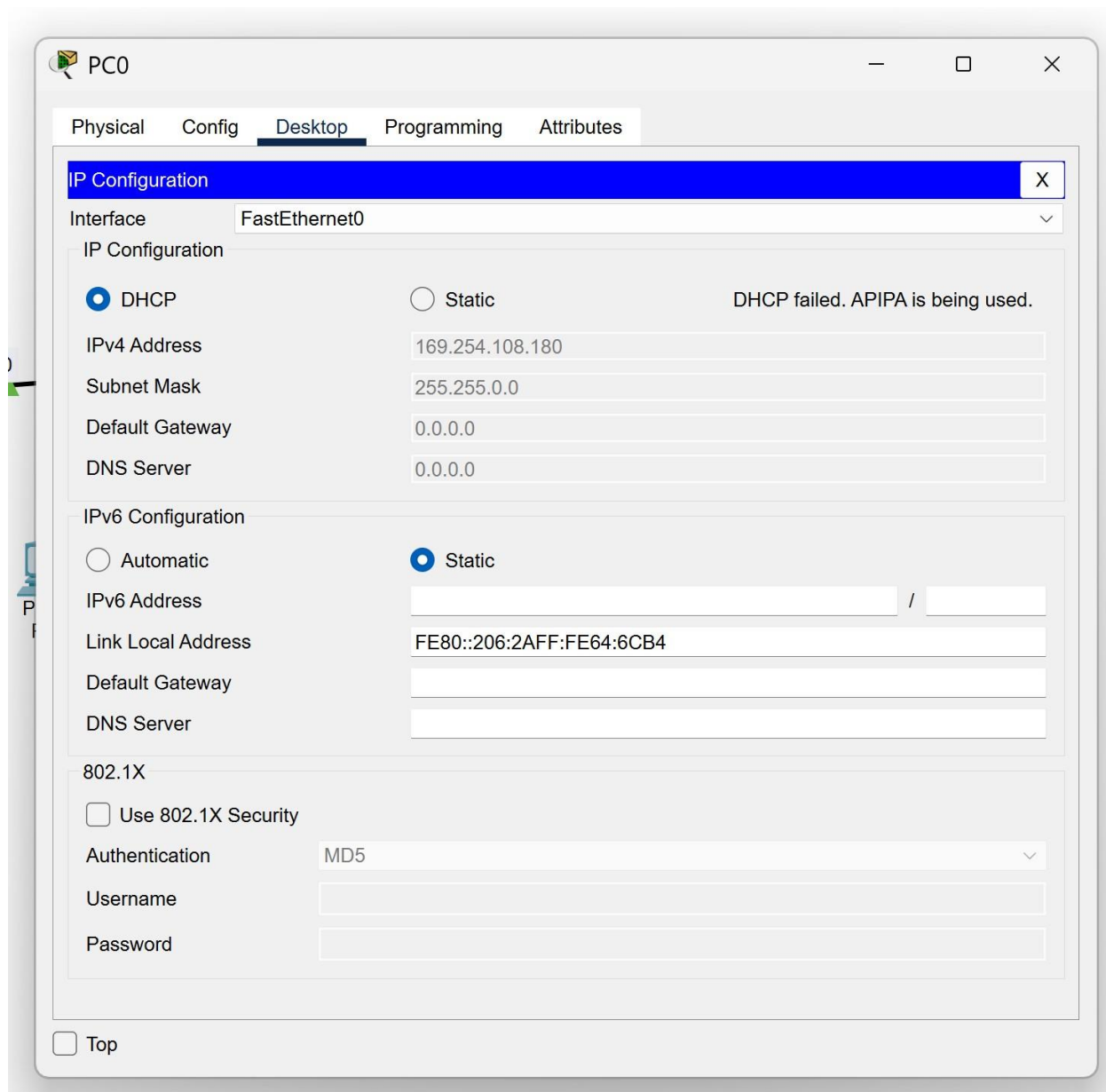
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface          Trusted      Rate limit (pps)
-----
```

At the bottom of the CLI window, there are "Copy" and "Paste" buttons. Below the CLI window, there is a "Top" button with a checkbox.

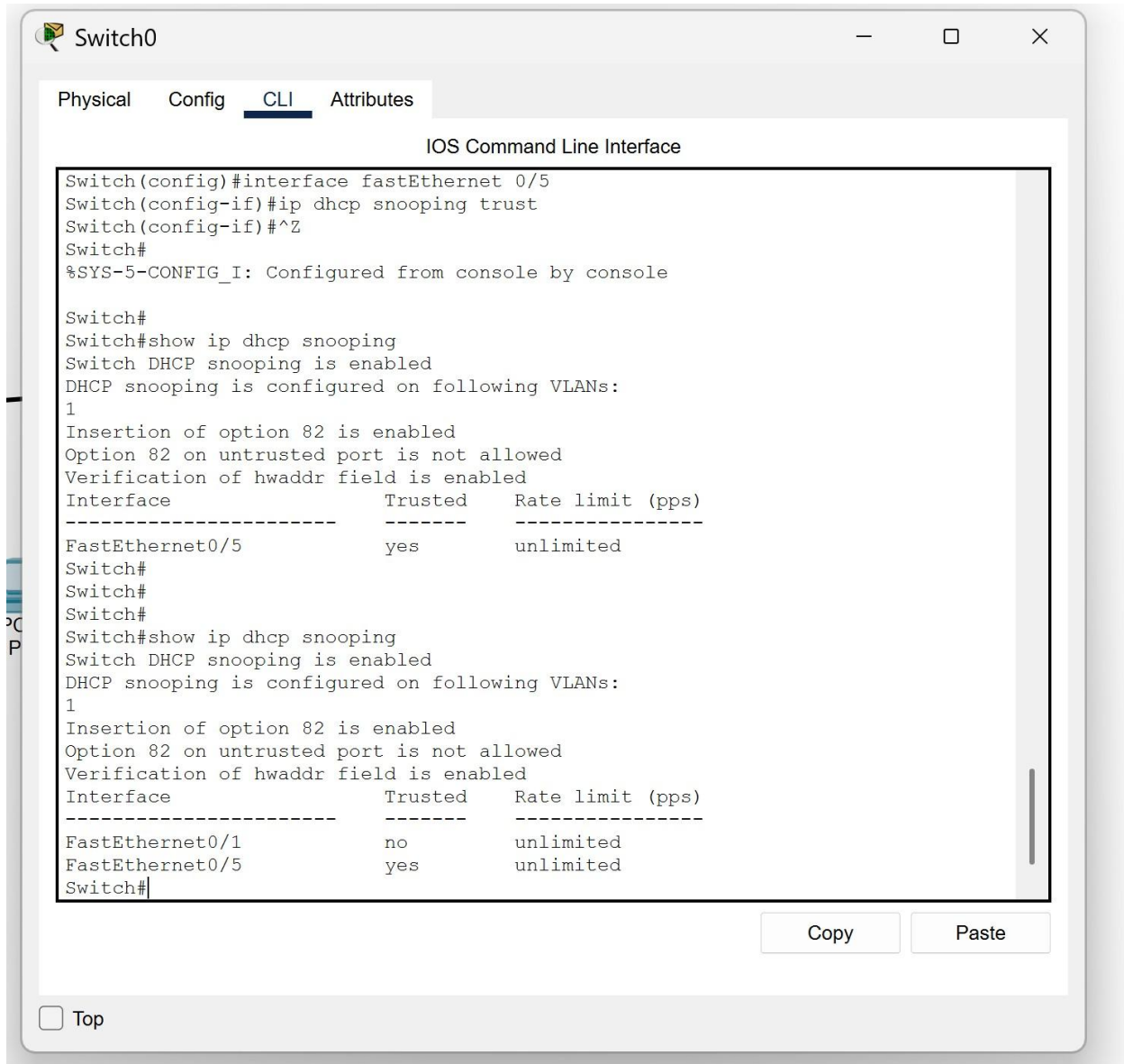
تصویر 6) فعال کردن DHCP Snooping و تعیین حالت vlan1.

حال اگر وارد یکی از PC ها شده و دوباره درخواست DHCP را برای گرفتن IP بزنیم، می بینیم که درخواست خطا می آید که این همان چیزی است که انتظار داریم چون هیچ پورتهی هنوز Trusted نیست. که در تصویر ۷ مشاهده می کنیم.



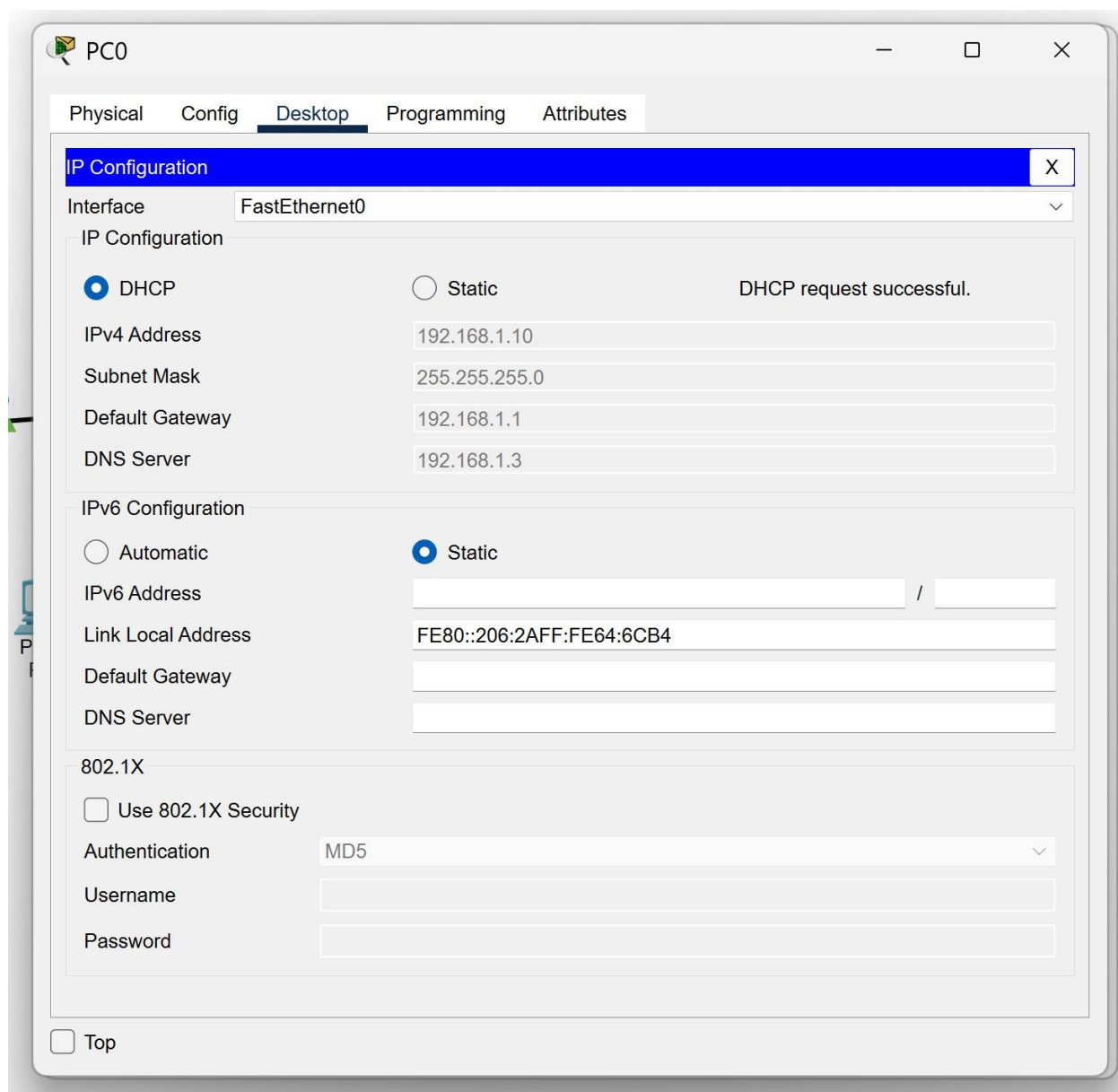
تصویر 7) گرفتن خطا به علت نبود پورت Trusted.

طبق راهنما حال باز وارد ترمینال سوییچ شده و پورت مربوط به سرور را Trusted کرده و با دستور گفته شده دوباره لیست پورت‌های Trusted را مشاهده می‌کنیم که در تصویر ۸ قابل مشاهده است.



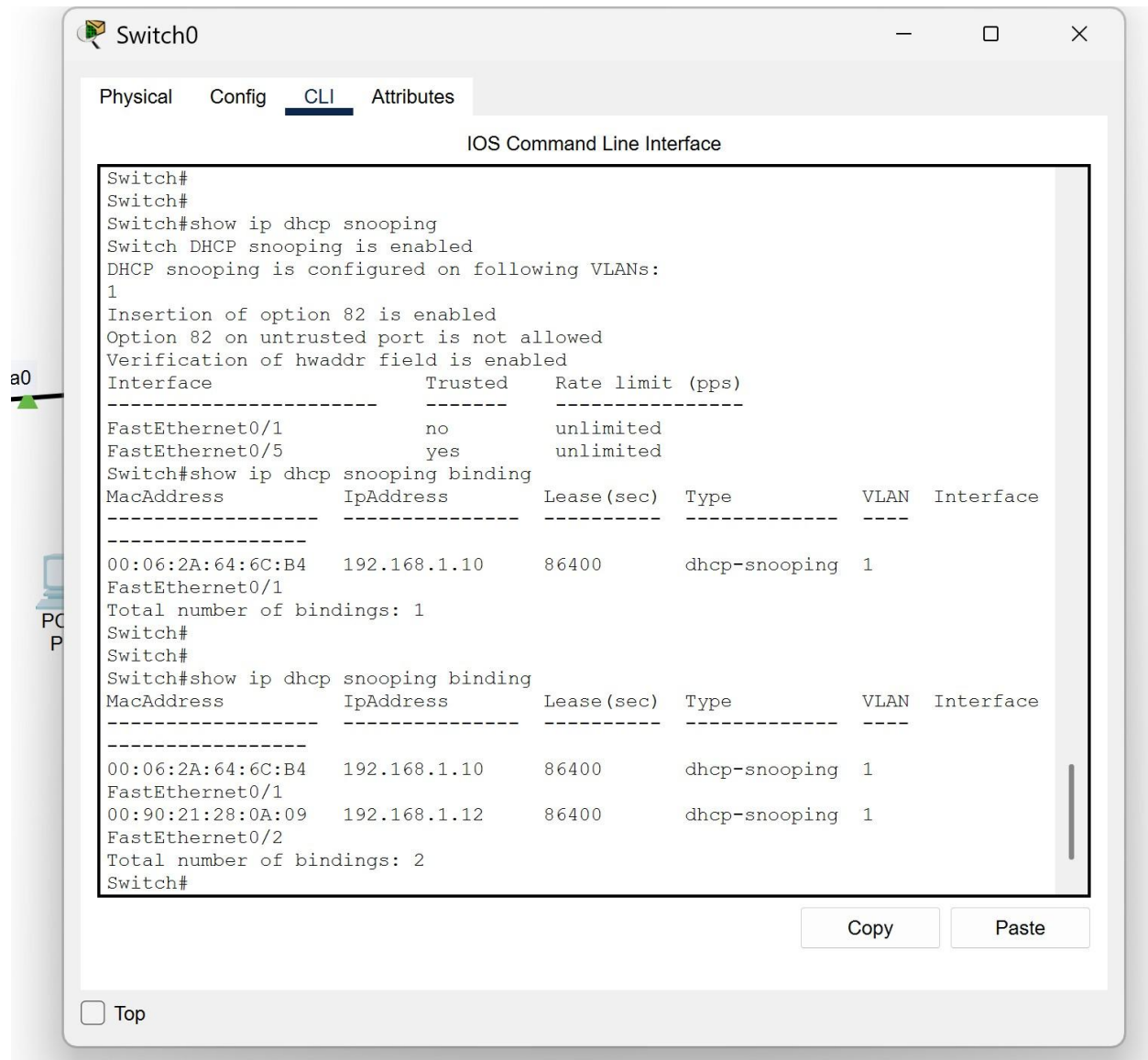
تصویر ۸) فعال کردن حالت Trusted برای پورت سرور.

حال باز وارد یکی از PC ها شده و دوباره درخواست DHCP زده و می بینیم درخواست موفقیت آمیز بوده و یک IP اختصاص داده شده است که در تصویر ۹ قابل مشاهده است.



تصویر 9) گرفتن IP با حالت DHCP Snooping

در نهایت طبق راهنما لیستی را که قبلا مشاهده می کردیم، یک کلمه **binding** را به انتهای دستور اضافه کرده که این دستور اطلاعاتی در مورد دستگاه هایی که آدرس های IP از طریق DHCP دریافت کرده اند، فراهم می کند و این اطلاعات را با توجه به پورت ها، آدرس های MAC، و IP هایی که تخصیص داده شده اند، نمایش می دهد، که در تصویر ۱۰ قابل مشاهده است.



تصویر 10) مشاهده لیست به صورت **binding**

[1] https://en.wikipedia.org/wiki/DHCP_snooping