

## تمرین: تحلیل و رفع مشکلات شبکه با استفاده از دستورات خط فرمان و مفاهیم شبکه

### شرح تمرین:

در این تمرین، شما با استفاده از دستورات خط فرمان و بررسی مفاهیم کلیدی شبکه، باید مشکلات شبکه را شناسایی و تحلیل کنید. این تمرین به شما کمک می‌کند تا به عنوان یک برنامه‌نویس بک‌اند، با مفاهیم شبکه آشنا شوید و درک بهتری از نحوه کارکرد زیرساخت‌های شبکه داشته باشید.

### مراحل تمرین:

1. تحلیل ارتباط بین دو دستگاه با استفاده از ping:
  - از دستور ping برای بررسی ارتباط بین کامپیوتر خود و یک سرور مشخص مثل google.com استفاده کنید.
  - توضیح دهید که آیا ارتباط برقرار شده یا خیر، و اگر برقرار نشده، چه عواملی ممکن است دخیل باشند (مثل عدم دسترسی به اینترنت، فایروال، یا مشکلات شبکه).
2. بررسی مسیر ارتباطی با استفاده از traceroute/tracert:
  - از دستور traceroute در ویندوز یا tracetop در لینوکس برای بررسی مسیر ارتباطی بین کامپیوتر خود و یک سرور مشخص مثل google.com استفاده کنید.
  - مسیری که بسته‌ها از آن عبور می‌کنند را بررسی کرده و نقش روترها و سوئیچ‌ها در این مسیر را توضیح دهید.
3. نمایش پیکربندی شبکه با استفاده از ipconfig/ifconfig:
  - از دستور ipconfig (در ویندوز) یا ifconfig (در لینوکس) برای نمایش اطلاعات شبکه دستگاه خود استفاده کنید.
  - اطلاعاتی مثل IP آدرس public و private، Subnet Mask، Default Gateway را تحلیل کنید و نقش هر یک را توضیح دهید.
4. بررسی NAT (Network Address Translation):
  - توضیح دهید که NAT چیست و چه نقشی در ترجمه آدرس‌های IP خصوصی به عمومی و بالعکس دارد.
  - مثال‌هایی از شبکه خود یا تنظیمات مودم/روتر خانگی تان ارائه دهید.
5. بررسی اتصالات شبکه با استفاده از netstat:
  - از دستور netstat برای مشاهده اتصالات فعال شبکه بر روی دستگاه خود استفاده کنید.
  - وضعیت اتصالات TCP و UDP را بررسی کنید و تفاوت این دو پروتکل را توضیح دهید.
6. تحلیل DNS با استفاده از nslookup:
  - از دستور nslookup برای تبدیل یک نام دامنه مثلاً google.com به IP آدرس استفاده کنید و نحوه کارکرد DNS را شرح دهید.
7. بررسی Netmask و Subnetting:
  - با استفاده از اطلاعات شبکه خود از ipconfig/ifconfig، Netmask دستگاه خود را شناسایی کنید و توضیح دهید که این Netmask چگونه شبکه شما را به زیرشبکه‌های مختلف تقسیم می‌کند.
8. تحلیل پورت‌ها:

- با استفاده از netstat یا ابزار دیگری، پورت‌های باز در سیستم خود را شناسایی کنید.
- توضیح دهید که پورت‌ها چه نقشی در ارتباطات شبکه دارند و چرا پورت‌های خاص برای سرویس‌های خاص مانند HTTP روی پورت 80 و HTTPS روی پورت 443 (استفاده می‌شوند).

#### 9. درک پروتکل HTTP و RESTful API ها:

- یک درخواست HTTP به یک API عمومی ارسال کنید (مثلاً با استفاده از curl یا Postman) و پاسخ آن را بررسی کنید.
- توضیح دهید که چه نوع درخواستی ارسال شده (GET, POST, ...) و چه کد وضعیتی (Status Code) برگشته است.

#### 10. شبیه‌سازی تنظیمات روتر و سوئیچ (اختیاری):

- اگر دسترسی دارید، وارد تنظیمات روتر یا سوئیچ خانگی خود شوید و برخی از تنظیمات مرتبط با NAT، IP، و پورت‌ها را بررسی کنید. تفاوت‌های اصلی بین روتر و سوئیچ را توضیح دهید.

#### موارد اضافی (اختیاری):

- شبیه‌سازی مشکلات شبکه: با قطع اتصال به اینترنت یا تغییر تنظیمات شبکه، مشکلاتی را ایجاد کرده و با استفاده از دستورات بالا مشکلات را تحلیل و برطرف کنید.
- بررسی Load Balancing: مطالعه‌ای کوتاه انجام دهید و توضیح دهید که Load Balancing چگونه می‌تواند در یک شبکه با ترافیک بالا مفید باشد.

این تمرین به شما کمک می‌کند تا با مفاهیم و ابزارهای مهم شبکه آشنا شوید و توانایی شناسایی و رفع مشکلات شبکه را به عنوان یک برنامه‌نویس بک‌اند تقویت کنید. اگر سؤالی داشتید، حتماً در گروه مطرح کنید.