پیش گزارش آزمایش ۳

آزمایشگاه شبکه‌های کامپیوتری

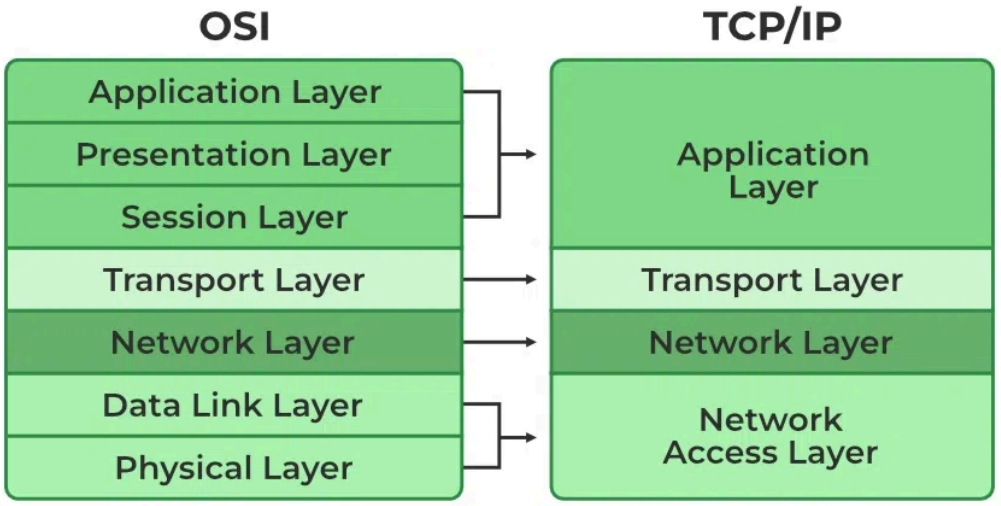
امیرمحمد کلاکی 40131038

فهرست

سوال ۱)

الف)

هر زمان که بخواهیم چیزی را از طریق اینترنت با استفاده از مدل TCP/IP ارسال کنیم، مدل TCP/IP داده‌ها را به بسته‌هایی (packets) در نقطه‌ی انتهایی (end point) فرستنده تقسیم می‌کند و همان بسته‌ها باید در نقطه‌ی انتهایی گیرنده دوباره ترکیب شوند تا همان داده‌ها را تشکیل دهند و این اتفاق برای حفظ دقت داده‌ها رخ می‌دهد. مدل TCP/IP داده‌ها را به 4 لایه تقسیم می‌کند و این داده‌ها به ترتیب وارد این لایه‌ها می‌شوند و دوباره در گیرنده به ترتیب معکوس، لایه‌ها را پیمایش می‌کنند تا به همان شکل در نقطه‌ی انتهایی گیرنده سازماندهی شوند.
اما در مدل OSI هر لایه از مدل OSI به طور مستقیم با لایه‌ی بالایی و زیرین آن تعامل دارد و داده‌ها را در ساختارهای (structure) از پیش تعیین شده کپسول و بسته‌بندی می‌کند تا انتقال دهد. این روش به متخصصان شبکه کمک می‌کند تا راحت‌تر مشکلات درون شبکه را عیب‌یابی کنند، زیرا مشکلات را می‌توان در یک لایه خاص از ۷ لایه‌ی آن جدا کرد.



شکل (۱)

ب)

در مدل OSI لایه‌ی شبکه برای انتقال داده‌ها از یک host به host دیگر واقع در شبکه های مختلف کار می کند. همچنین مسئول مسیریابی بسته (packet) و مراقبت از آن نیز می‌باشد. یعنی باید کوتاه‌ترین مسیر را برای انتقال بسته از تعداد مسیرهای موجود تشخیص دهد. آدرس IP فرستنده و گیرنده نیز توسط لایه‌ی

شبکه در header قرار می گیرد. لایه‌ی شبکه توسط دستگاه‌های شبکه مانند روترها و سوئیچ‌ها پیاده سازی می‌شود.
طبق شکل (۱) و دانسته‌های قبلی که در کلاس کسب شده، این لایه در مدل TCP/IP متناظر با لایه‌ی شبکه در مدل OSI است. هر دو پروتکل‌هایی را تعریف می‌کند که مسئول انتقال منطقی داده‌ها هستند.
پروتکل‌های اصلی موجود در این لایه به شرح زیر است:

1. IP:

IP مخفف Internet Protocol است و وظیفه‌ی تحویل بسته‌ها از میزبان در مبدا به میزبان در مقصد را با نگاه کردن به آدرس‌های IP در header بسته‌ها بر عهده دارد.

2. ICMP:

ICMP مخفف عبارت Internet Control Message Protocol است. این در داخل دیتاگرام‌های IP محصور شده است و وظیفه‌ی ارائه‌ی اطلاعات مربوط به مشکلات شبکه را بر عهده دارد. به طور ساده‌تر مسئول برقراری ارتباط مطمئن و صحیح در شبکه است به طوری که هیچ بسته‌ای (packet) در انتقال lost نشود.

3. ARP:

ARP مخفف Address Resolution Protocol است. وظیفه آن یافتن آدرس سخت‌افزاری host از یک IP شناخته شده است.

سوال ۲)

الف)

sniffer که به آن تحلیلگر بسته (packet analyzer) یا تحلیلگر شبکه (network analyzer) نیز گفته می شود، ابزاری است که برای ضبط و تجزیه و تحلیل ترافیک شبکه‌ها استفاده می‌شود. این نرم‌افزار یا ابزار سخت‌افزاری است که بسته‌های (packet) ارسال شده بین کامپیوترها یا دیگر دستگاه‌های موجود در شبکه را رهگیری و ثبت می‌کند.

ب)

این بسته ها را در لایه‌ی data link می‌گیرد و می‌تواند headerهای پروتکل‌های مختلف را برای استخراج اطلاعاتی مانند آدرس‌های IP مبدا و مقصد، پورت‌ها و محتویات درون بسته‌ها (packet) را تجزیه و تحلیل کند. اسنیفرها معمولا برای کارهایی مانند عیب‌یابی شبکه، نظارت بر عملکرد و تجزیه و تحلیل امنیتی استفاده می‌شود.

سوال ۳)

Wireshark یک تحلیلگر بسته‌ی (packet analyzer) رایگان و منبع باز (open-source) است و برای عیب‌یابی شبکه، تجزیه و تحلیل شبکه و جنبه‌های امنیتی آن، توسعه‌ی نرم‌افزار و پروتکل‌های ارتباطاتی و ... استفاده می‌شود.

Wireshark به کاربران این امکان را می‌دهد که کنترل‌کننده‌های رابط شبکه (network interface controllers) را در حالت بی‌وقفه قرار دهند، تا بتوانند تمام ترافیک قابل مشاهده در آن interface را ببینند. از جمله ترافیک unicast که به آدرس MAC کنترل‌کننده‌ی رابط شبکه (network interface controller) ارسال نشده است. با این حال، هنگام ضبط با یک packet analyzer در حالت بی‌وقفه روی پورت سوئیچ شبکه، همه ترافیک سوئیچ لزوما به پورتی که در آن capturing انجام می‌شود ارسال نمی‌شود، بنابراین ضبط در حالت بی‌وقفه الزاما برای مشاهده کل ترافیک شبکه کافی نیست.