بسمه تعالی

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

درس شبکه‌های کامپیوتری، نیمسال دوم سال تحصیلی ۱۴۰۴-۱۴۰۳

پاسخ تمرین سری ششم

سوال ۱:

شبکه دیتاگرام (datagram) و شبکه مدارمجازی (virtual circuit) را شرح داده و با هم مقایسه کنید.

پاسخ:

شبکه دیتاگرام (Datagram Network): در این نوع شبکه، هر بسته داده به صورت مستقل و جداگانه ارسال می‌شود و ممکن است مسیرهای مختلفی را طی کند تا به مقصد برسد. هر بسته شامل آدرس مقصد است و هیچ ارتباطی بین بسته‌ها در شبکه وجود ندارد (شبکه بدون اتصال). این روش مشابه ارسال نامه است.

شبکه مدارمجازی (Virtual Circuit Network): قبل از ارسال داده، یک مسیر مشخص (مدار مجازی) بین فرستنده و گیرنده برقرار می‌شود و تمام بسته‌ها از همین مسیر عبور می‌کنند. این روش شبیه برقراری یک تماس تلفنی است که مسیر از ابتدا تا انتها مشخص و ثابت است.

مقایسه:

شبکه دیتاگرام	شبکه مدارمجازی
مسیر هر بسته مستقل است	مسیر از قبل مشخص شده است
قابل اطمینان کم: گم شدن یا بهم خوردن ترتیب بسته ها	قابلیت اطمینان بالا: تضمین ترتیب و تحویل بهتر بسته ها
سریع: نبود مرحله راه اندازی مسیر	زمان بر: نیازمند مرحله راه اندازی مسیر

سوال ۲:

الف) نقش مسیریاب‌ها و میزبان‌ها در فرایند جلورانی بسته‌ها را مقایسه کنید.

ب) تفاوت بین شناسه شبکه و شناسه میزبان در آدرس IP را تعریف و توضیح دهید.

ج) با توجه به آدرس‌های IP زیر و ماسک زیرشبکه 255.255.255.0 ، چگونگی تقسیم‌بندی آن‌ها به زیرشبکه‌ها را نشان دهید:

- 223.1.1.1
- 223.1.1.2

د) روش CIDR (آدرس‌دهی بدون طبقه) نسبت به روش (قدیمی) آدرس‌دهی با طبقه‌بندی چه بهبود(هایی) را ایجاد کرده است؟

پاسخ:

الف) میزبان‌ها (Hosts) مبدأ و مقصد اصلی بسته‌ها هستند که داده‌ها را تولید و مصرف می‌کنند.

مسیریاب‌ها (Routers) بسته‌ها را از یک شبکه به شبکه دیگر هدایت می‌کنند. وظیفه آنها پیدا کردن بهترین مسیر برای ارسال بسته‌ها به مقصد است و خود داده‌ها را تولید یا مصرف نمی‌کنند.

ب) شناسه شبکه (Network ID) بخشی از آدرس IP است که شبکه‌ای که میزبان در آن قرار دارد را مشخص می‌کند.

شناسه میزبان (Host ID) بخشی از آدرس IP که به یک دستگاه (میزبان) در داخل شبکه اختصاص داده می‌شود.

ج) با ماسک ۲۵۵.۲۵۵.۲۵۵.۰، ۲۴ بیت اول آدرس مربوط به شناسه شبکه است (۲۲۳.۱.۱) و ۸ بیت آخر برای شناسه میزبان. چون هر دو آدرس در شبکه ۲۲۳.۱.۱ قرار دارند، آنها در یک زیرشبکه هستند.

د) CIDR باعث انعطاف بیشتر در تخصیص آدرس‌ها شده است، به طوری که می‌توان اندازه شبکه‌ها را دقیق‌تر تعیین کرد و از هدررفت آدرس‌های IP جلوگیری کرد.

روش قدیمی طبقه‌بندی IP به صورت کلاس A، B، C بود که محدودیت‌های زیادی داشت و باعث هدررفت آدرس می‌شد. CIDR امکان ایجاد شبکه‌های با اندازه‌های مختلف را فراهم می‌کند و باعث بهبود بهره‌وری در استفاده از آدرس‌های IP میشود.

سوال ۳:

محدوده آدرس شبکه 189.222.184.0/22 به یک دانشگاه اختصاص داده شده است. این دانشگاه قصد دارد این محدوده IP را بین ۴ دانشکده اصلی خود با شرح نیازمندی زیر تقسیم کند:

- دانشکده A: ۳۰۰ میزبان
- دانشکده B: ۱۵۰ میزبان
- دانشکده‌های C و D هر کدام ۵۰ میزبان

پس از تخصیص آدرس‌ها به دانشکده‌ها، دانشکده A قصد دارد بخش خود را به سه زیربخش مجزا تقسیم کند، که هر زیربخش به ۶۰ میزبان دارد.

با توجه به اطلاعات داده شده:

الف) یک طرح زیرشبکه‌بندی مناسب برای دانشگاه، شامل ماسک زیرشبکه و محدوده آدرس IP برای هر دانشکده را ارائه دهید.

ب) جزئیات زیرشبکه‌بندی داخلی دانشکده A را برای سه زیربخش آن، شامل محدوده آدرس IP قابل استفاده و ماسک زیرشبکه را مشخص کنید.

ج) جدول مسیریابی (جلورانی) دانشگاه را طراحی کنید تا مشخص شود بسته‌های داده با توجه به مقصد IP، باید به کدام دانشکده یا زیربخش ارسال شوند.

پاسخ:

الف)

$\lceil \log 300 \rceil = 9 \Rightarrow 9\ bit\ is\ needed\ for\ network\ A$
$\lceil \log 150 \rceil = 8 \Rightarrow 8\ bit\ is\ needed\ for\ network\ B$
$\lceil \log 50 \rceil = 6 \Rightarrow 6\ bit\ is\ needed\ for\ network\ C\ and\ D$

Network IP: 10111101.11011110.10111000.00000000
Network Mask: 11111111.11111111.11111100.00000000
A Ip: 10111101.11011110.10111000.00000000
A Mask: 11111111.11111111.11111110.00000000
Network A: 189.222.184.0/23 (from 189.222.184.0 till 189.222.185.255 is available)

B Ip: 10111101.11011110.10111010.00000000
B Mask: 11111111.11111111.11111111.00000000
Network B: 189.222.186.0/24 (from 189.222.186.0 till 189.222.186.255 is available)

C Ip: 10111101.11011110.10111011.00000000
C Mask: 11111111.11111111.11111111.11000000
Network C: 189.222.187.0/26 (from 189.222.187.0 till 189.222.187.63 is available)

D Ip: 10111101.11011110.10111011.01000000
D Mask: 11111111.11111111.11111111.11000000
Network D: 189.222.187.64/26 (from 189.222.187.64 till 189.222.187.127 is available)

ب)

$\lceil \log 60 \rceil = 6 \Rightarrow 6\ bit\ is\ needed\ for\ each\ network\ A\ subnets$

A1 Ip: 10111101.11011110.10111000.00000000
A1 Mask: 11111111.11111111.11111111.11000000
Network A1: 189.222.184.0/26 (from 189.222.184.0 till 189.222.184.63 is available)

A2 Ip: 10111101.11011110.10111000.01000000
A2 Mask: 11111111.11111111.11111111.11000000
Network A2: 189.222.184.64/26 (from 189.222.184.0 till 189.222.184.63 is available)

A3 Ip: 10111101.11011110.10111000.10000000
A3 Mask: 11111111.11111111.11111111.11000000
Network A3: 189.222.184.128/26 (from 189.222.184.128 till 189.222.184.191 is available)

ج)

Destination	Mask	Next Hop
189.222.184.0	255.255.252.0	**A**
189.222.186.0	255.255.255.0	**B**
189.222.187.0	255.255.255.192	**C**
189.222.187.64	255.255.255.192	**D**
189.222.184.0	255.255.255.192	**A1**
189.222.184.64	255.255.255.192	**A2**
189.222.184.128	255.255.255.192	**A3**

سوال ۴:

بر اساس جدول جلورانی زیر گام بعدی برای بسته‌هایی با آدرس‌های مقصد زیر را بدست آورید:

الف) 10.10.20.30

ب) 192.168.0.50

ج) 203.0.113.10

Destination	Mask	Next Hop
10.0.0.0	255.0.0.0	A (172.16.1.1)
10.10.0.0	255.255.0.0	B (172.16.2.1)
192.168.0.0	255.255.255.0	C (172.16.3.1)
172.16.0.0	255.240.0.0	D (172.16.4.1)
100.64.0.0	255.192.0.0	E (172.16.5.1)
0.0.0.0	0.0.0.0	F (172.16.6.1)

پاسخ:

باید بررسی کنیم که آدرس مقصد با کدام ردیف در جدول مسیریابی تطابق بیشتری دارد (یعنی بیشترین تطابق بیت‌های شبکه با استفاده از mask) این تطابق به صورت AND بیت به بیت بین آدرس مقصد و mask هر ردیف انجام می‌شود و سپس با آدرس شبکه (Destination) مقایسه می‌شود.

آدرس اول : بررسی با مسیرهای ممکن

10.10.20.30 = 00001010. 00001010. 00010100. 00011110
Route: 10.0.0.0/8 → Mask: 255.0.0.0
Mask: 11111111.00000000.00000000.00000000
AND: 00001010.00000000.00000000.00000000 = 10.0.0.0 (true)

Route: 10.10.0.0/16 → Mask: 255.255.0.0
Mask: 11111111.11111111.00000000.00000000

AND: 00001010.00001010.00000000.00000000 = 10.10.0.0 (true)

هر دو تطابق دارند، ولی۱۶/ دقیق‌تر از ۸/ است : انتخاب B

آدرس دوم :

192.168.0.50 = 11000000.10101000.00000000.00110010
Route: 192.168.0.0/24 → Mask: 255.255.255.0
Mask: 11111111.11111111.11111111.00000000
AND: 11000000.10101000.00000000.00000000 = 192.168.0.0 (true)

تطابق دارد : انتخاب C

آدرس سوم :

203.0.113.10 = 11001011.00000000.01110001.00001010

هیچ‌کدام از مسیرها با این آدرس تطابق ندارند فقط مسیر پیش‌فرض باقی می‌ماند:

Route: 0.0.0.0/0 → Mask: 00000000.00000000.00000000.00000000
AND: 00000000.00000000.00000000.00000000 = 0.0.0.0

انتخاب F

سوال ۵:

یک سرویس‌گیرنده با آدرس فیزیکی (MAC) 00:1A:2B:3C:4D:5E به شبکه‌ای متصل می‌شود که دارای دو سرویس‌دهنده DHCP است:

- سرویس‌دهنده DHCP شماره ۱ با آدرس 223.1.2.1 و
- سرویس‌دهنده DHCP شماره ۲ با آدرس 223.1.1.1

الف) توالی پیام‌های تبادل‌شده بین سرویس‌گیرنده و سرویس‌دهنده‌های DHCP شامل آدرس‌های IP مبدا و مقصد و هدف هر پیام را در دیاگرامی زمانی رسم کرده و شرح دهید.

ب) اگر هر دو سرویس‌دهنده DHCP پیام DHCP OFFER را ارسال کنند، آنگاه چه اتفاقی می‌افتد و سرویس‌گیرنده چگونه انتخاب می‌کند؟

پاسخ:

الف)

۱. **DHCP Discover**

مبدأ :کلاینت (IP: 0.0.0.0) (MAC: 00:1A:2B:3C:4D:5E)

آدرس IP مبدأ ۰.۰.۰.۰ است، زیرا کلاینت هنوز آدرسی ندارد.

مقصد: به ip ۲۵۵.۲۵۵.۲۵۵.۲۵۵ که مربوط به broadcast هست.

کلاینت که هنوز آدرس IP ندارد، یک پیام Discover را به صورت پخش (Broadcast) در شبکه ارسال می‌کند تا سرورهای DHCP موجود را پیدا کند. این پیام شامل آدرس MAC کلاینت و درخواست تخصیص آدرس IP است.

۲. **DHCP Offer**

مبدأ :سرور ۱(IP: 223.1.2.1)

مقصد :آدرس پخش (۲۵۵.۲۵۵.۲۵۵.۲۵۵)

سرور DHCP در پاسخ بهDiscover ، یک پیام Offer ارسال می‌کند که شامل یک آدرس IP پیشنهادی (مثلاً ۲۲۳.۱.۲.۱۰۰)، ماسک زیرشبکه، دروازه پیش‌فرض، آدرس DNS و سایر اطلاعات پیکربندی است. از آنجا که هنوز کلاینت مقصد آدرس ندارد باز هم از broadcast استفاده می کنیم. این پیام شامل آدرس MAC کلاینت (00:1A:2B:3C:4D:5E) است تا کلاینت بتواند آن را شناسایی کند.

۳. **DHCP Request**

مبدأ :کلاینت(IP: 0.0.0.0)

مقصد :آدرس پخش(255.255.255.255)

کلاینت یکی از پیشنهادهای دریافت‌شده (اگر بیشتر از یک پیشنهاد (از سرور های مختلف) دریافت کرده بود) را انتخاب می‌کند و یک پیام Request ارسال می‌کند تا اعلام کند که کدام آدرس IP را می‌خواهد (مثلاً ۲۲۳.۱.۲.۱۰۰ از سرور 223.1.2.1). این پیام به صورت پخش ارسال می‌شود تا همه سرورهای DHCP در شبکه مطلع شوند و سرورهای دیگر پیشنهادهای خود را آزاد کنند. پیام شامل آدرس MACکلاینت و شناسه سرور DHCP انتخاب‌شده است مثلا در این مثال (۲۲۳.۱.۲.۱)

۴. **DHCP Ack**

مبدا: 223.1.2.1

مقصد :آدرس پخش (۲۵۵.۲۵۵.۲۵۵.۲۵۵) یا آدرس IP تخصیص‌یافته به کلاینت (مثلاً ۲۲۳.۱.۲.۱۰۰)

سرور DHCP تأیید می‌کند که آدرس IP پیشنهادی (۲۲۳.۱.۲.۱۰۰) به کلاینت اختصاص داده شده است و اطلاعات نهایی پیکربندی مانند مدت اجاره، ماسک زیرشبکه، دروازه پیش‌فرض و DNS را ارسال می‌کند. پس از دریافت این پیام، کلاینت می‌تواند آدرس IP را به‌طور رسمی استفاده کند. میزبان نیز زمانبند های T1, T2, T3 را نیز روشن می کند.

ب) همانطور که در قسمت الف نیز ذکر شد زمانی که چند DHCP offer از چند سرور پیشنهاد می شود، کلاینت این امکان را دارد که در مرحله DHCP Request بین آنها انتخاب کند (معمولا پیشنهاد اول انتخاب می شود مگر اینکه تنضیمات خاصی وجود داشته باشد)
بعد از فرستادن DHCP request (برای آنکه مشخص شود که پیشنهاد کدام سرور انتخاب شده است هم پیشنهاد و هم آدرس مربوط به سرور پیشنهاد دهنده در درخواست ارسال می شود) رفتار دو سرور به صورت زیر هست:
سرور انتخاب‌شده (مثلاً سرور ۱) :پیام Ack را ارسال می‌کند و آدرس IP را به کلاینت اختصاص می‌دهد.
سرور دیگر (مثلاً سرور ۲) :پس از دریافت پیام Request و مشاهده اینکه پیشنهادش انتخاب نشده، آدرس پیشنهادی خود (مثلاً ۲۲۳.۱.۱.۱۰۰) را آزاد می‌کند تا برای کلاینت‌های دیگر در دسترس باشد.

سوال ۶:

الف) supernetting چیست؟ فرق آن را با subnetting توضیح دهید.

ب) چرا استفاده از NAT باعث نقض مدل لایه‌ای می‌شود؟

ج) هنگام ارسال درخواست از یک دستگاه خانگی به یک سرویس‌دهنده وب در اینترنت، چه تغییراتی روی بسته‌ها صورت می‌گیرد؟

پاسخ:

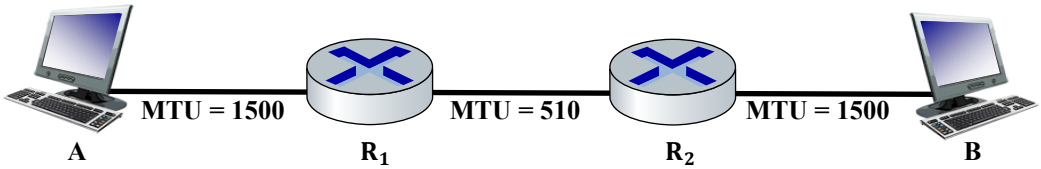
الف) به تجمیع آدرسها در قالب یک آدرس با محدوده بزرگتر Supernetting میگویند. برعکس Subnetting که یک محدوده آدرس IP بزرگ به تعدادی محدوده کوچکتر (Subnet) تقسیم می‌شود.

ب) در مدل مرجع OSI ، هر لایه تنها باید با اطلاعات لایه خودش سروکار داشته باشد. اما NAT برای انجام ترجمه آدرس‌ها، به شماره پورت‌ها (که متعلق به لایه ۴ است) نیاز دارد. در حالی که NAT در لایه ۳ (شبکه) قرار دارد، اما برای عملکرد صحیح باید اطلاعات لایه ۴ را بررسی کند، که این باعث نقض استقلال لایه‌ها در مدل مرجع می‌شود.

ج) آدرس IP مبدأ و شماره پورت مبدأ تغییر می‌کنند: آدرس IP به آدرس خارجی روتر NAT و پورت به یک عدد جدیدی که در جدول NAT ثبت شده، تبدیل می‌شود.

سوال ۷:

با در نظر گرفتن شکل زیر که مسیر بین میزبان A و میزبان B را نشان می‌دهد، میزبان A می‌خواهد بسته‌ای به طول ۲۰۰۰ بایت را به میزبان B ارسال کند. اگر اندازه سرآیند هر بسته IP را برابر با ۲۰ بایت در نظر بگیریم، مشخصات بسته‌های خُرد شده (fragmentation) از قبیل Total length، Packet ID، More Flag و Fragmentation offset را در هر مرحله نشان دهید.



پاسخ:

Original Packet:

	Total length	Packet ID	More Flag	Fragmentation offset
Original packet	2000	X	0	0

From A to R_1:

Header size is 20 → 1500 – 20 = 1480 → 1480 / 8 = 185 (fragment offset)

Number of fragments = $\lceil 2000 / 1480 \rceil = 2$

	Total length	Packet ID	More Flag	Fragmentation offset
Fragment 1	1500	X	1	0
Fragment 2	540	X	0	185

From R_1 to R_2:

Header size is 20 → 510 – 20 = 490 → $\lfloor 490/8 \rfloor = 61$ → total length = $61 * 8 + 20 = 508$

Number of fragments for fragment 1 = $\lceil 1480 / 488 \rceil = 4$

Number of fragments for fragment 2 = $\lceil 520 / 488 \rceil = 2$

	Total length	Packet ID	More Flag	Fragmentation offset
Fragment 1	508	X	1	0
Fragment 2	508	X	1	61
Fragment 3	508	X	1	122
Fragment 4	36	X	1	183
Fragment 5	508	X	1	185
Fragment 6	52	X	0	246

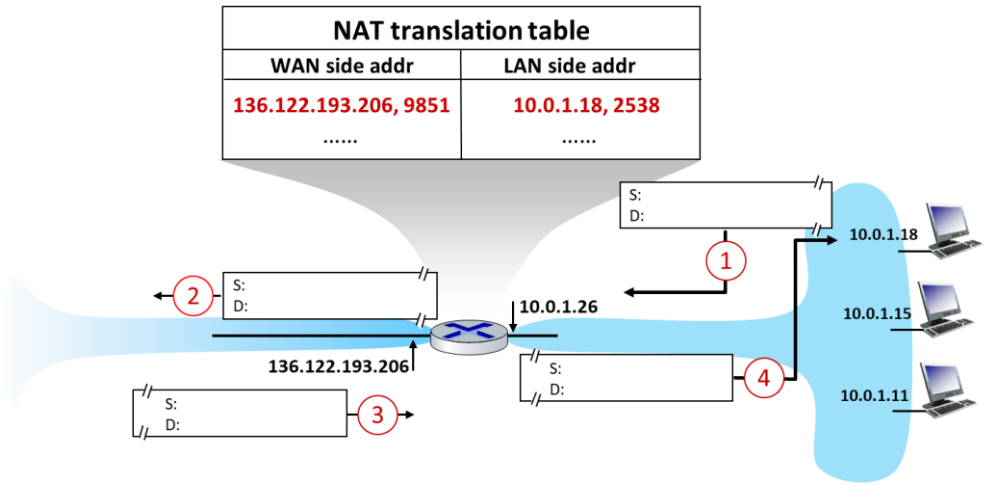
From R_1 to R_2:

No change

	Total length	Packet ID	More Flag	Fragmentation offset
Fragment 1	508	X	1	0
Fragment 2	508	X	1	61
Fragment 3	508	X	1	122
Fragment 4	36	X	1	183
Fragment 5	508	X	1	185
Fragment 6	52	X	0	246

سوال ۸:

سه میزبان با آدرس‌های IPهای خصوصی 10.0.1.11، 10.0.1.15 و 10.0.1.18 در یک شبکه محلی پشت یک مسیریاب قرار دارند. بسته‌های IP که از/به این دستگاه‌ها ارسال می‌شوند باید از مسیریاب عبور کنند. آدرس IP مسیریاب در سمت شبکه LAN برابر با 10.0.1.26 و در سمت شبکه اینترنت برابر با 135.122.193.206 است. میزبان 10.0.1.18 می‌خواهد یک بسته از پورت 3412 به آدرس مقصد 128.119.166.185 و پورت 80 ارسال کند. آدرس IP و شماره پورت مبدأ و مقصد را در هر چهار مرحله نشان داده شده در شکل زیر را بنویسید.



پاسخ:

Step 1:
Source: 10.0.1.18:3412
Destination: 128.119.166.185:80

Step 2:
Source: 136.122.193.206:X (some port that the NAT assigns to port 3412 of 10.0.1.18)
Destination: 128.119.166.185:80

Step 3:
Source: 128.119.166.185:80
Destination: 136.122.193.206:X

Step 4:
Source: 128.119.166.185:80
Destination: 10.0.1.18:3412 (the NAT looks up in its translation table and translates the destination)

سوال ۹:

الف) انگیزه اصلی برای طراحی پروتکل IPv6 چه بوده است؟

ب) IPv6 چه قابلیت‌ها یا بهبودهایی نسبت به پروتکل IPv4 داد.

ج) چه تفاوت‌هایی بین ساختار سرآیند بسته‌های IPv4 و IPv6 وجود دارد؟

د) چرا IPv6 اجازه خُردسازی بسته (fragmentation) را فقط در گره مبدأ می‌دهد؟

ه) ویژگی فیلد "Flow Label" در IPv6 چیست و چرا به عنوان یک ویژگی جدید در پروتکل گنجانده شده است؟

پاسخ:

الف) انگیزه اصلی، محدودیت فضای آدرس‌دهی در IPv4 بود. IPv4 از آدرس‌های ۳۲ بیتی استفاده می‌کند که فقط حدود ۴ میلیارد آدرس منحصربه‌فرد را فراهم می‌کند. این مقدار با رشد اینترنت و دستگاه‌های متصل کافی نبود. به همین دلیل در IPv6، آدرس‌دهی به ۱۲۸ بیت افزایش یافت تا پاسخگوی نیازهای آینده باشد.

ب) IPv6 دارای قابلیت‌ها و بهبودهای متعددی نسبت به IPv4 است، از جمله:

۱. افزایش فضای آدرس‌دهی از ۳۲ بیت به ۱۲۸ بیت

۲. ساده‌سازی سرآیند و ثابت بودن اندازه آن با حذف فیلدهای غیرضروری مانند checksum، fragmentation offset، flags، identification

۳. بهبود عملکرد و کیفیت خدمات با استفاده از Flow Label برای تفکیک جریان‌ها و حذف محدودیت استفاده از گزینه‌ها (Options) و همچنین افزودن مکانیزم‌های امنیتی

۴. جایگزینی فیلدهای قدیمی IPv4 با فیلدهای دقیق‌تر مانند TTL → hop limit، Protocol → Next Header

ج) سرآیند IPv6 یک سرآیند با طول ثابت است که بیشتر گزینه‌های موجود در سرآیند IPv4 را شامل نمی‌شود. با وجود اینکه سرآیند IPv6 شامل دو آدرس ۱۲۸ بیتی (آدرس IP مبدأ و مقصد) است، کل سرآیند تنها طول ثابتی معادل ۴۰ بایت دارد. چندین فیلد از نظر مفهومی مشابه هستند. فیلدهای کلاس ترافیک، طولpayload ، هدر سرآیند و محدودیت پرش (hop limit) در IPv6 به ترتیب جایگزین فیلدهای نوع سرویس، طول datagram، پروتکل لایه بالاتر و time to live در IPv4 هستند. همچنین همانطور که گفته شد فیلدهایی مانند checksum، flags، fragmentation offset در IPv4 برای IPv6 حذف شده‌اند.

د) فرآیند تکه‌تکه‌سازی بسته‌ها (fragmentation) از منابع پردازشی روتر استفاده می‌کند. با الزام به انجام تمام تکه‌تکه‌سازی‌ها در مبدأ، روترها از بار پردازشی اینکار آزاد می‌شوند و در نتیجه می‌توانند سریع‌تر بر روی وظیفه اصلی یعنی مسیریابی عمل کنند. پس این تصمیم با هدف ساده‌سازی پردازش در مسیریاب‌ها و بهبود عملکرد شبکه گرفته شده است.

ه) فیلد Flow Label در IPv6 برای شناسایی بسته‌هایی است که به یک جریان (Flow) خاص تعلق دارند و این امکان را می‌دهد که بسته‌های یک جریان مشخص، با کیفیت خدمات (QoS) مشابه و با گذردهی بالا پردازش شوند. دلیل اضافه شدن این ویژگی، بهبود عملکرد شبکه و کیفیت خدمات‌دهی (QoS) است، مخصوصاً برای بسته‌های مربوط به یک جریان خاص (مثلاً تماس تصویری یا بازی آنلاین) که نیاز به جریان پایدار و با تأخیر کم دارند و باید به‌صورت مشابه پردازش شوند.

سوال ۱۰:

الف) با توجه به حذف بررسی خطا (checksum) در سرآیند IPv6، انتقال داده از طریق کانال‌های بی‌سیم پرنویز با چه چالش‌هایی مواجه است؟ چه راهکارهایی در سایر لایه‌های شبکه برای تضمین صحت انتقال داده‌ها در لایه‌های پایین‌تر وجود دارد؟

ب) فرض کنید یک سازمان دارای مسیریاب‌های قدیمی است که فقط از IPv4 پشتیبانی می‌کنند. چگونه می‌توان بدون ارتقاء تمام تجهیزات، ارتباط بین میزبان‌های IPv6 را در این شبکه برقرار کرد؟

پاسخ:

الف) انتقال روی لینک بی‌سیم پرنویز چالش‌هایی از جمله افزایش احتمال انتقال داده‌های خراب یا دارای خطا در فریم‌های ارسالی را به همراه دارد، زیرا اگر فریم‌ها شامل بررسی خطا نباشند و فیلد checksum حذف شده باشد، بسته‌های دارای خطا ممکن است به روتر تحویل داده شوند و رفتار غیرقابل پیش‌بینی رخ دهد.
برای مقابله با این چالش، تضمین صحت داده‌ها به لایه‌های دیگر مانند لایه پیوند داده (Data Link Layer) یا لایه انتقال (Transport Layer) سپرده شده است. بنابراین اثر خطاهای انتقال، باعث ارسال مجدد فریم‌ها در لایه پیوند داده می‌شود. تنها بسته‌هایی که در فریم‌های بدون خطا دریافت شوند به لایه IP منتقل می‌شوند. به این صورت، حتی بدون وجود checksum در IPv6، همچنان امکان تشخیص و اصلاح خطا در سطوح پایین‌تر یا بالاتر وجود دارد.

ب) برای برقراری ارتباط بین میزبان‌های IPv6 بدون نیاز به ارتقاء همه مسیریاب‌ها، از روش تونل‌سازی (Tunneling) استفاده می‌شود. در این روش بسته‌های IPv6 به شکل کپسوله شده داخل بسته‌های IPv4 قرار می‌گیرند و از طریق زیرساخت IPv4 منتقل می‌شوند. به‌عبارت دیگر، بسته‌ی IPv6 به عنوان بار داده (Payload) در بسته‌ی IPv4 قرار می‌گیرد. به این ترتیب، بسته‌های IPv6 از طریق مسیریاب‌هایی که فقط از IPv4 پشتیبانی می‌کنند عبور می‌کنند. پس با اینکار این امکان فراهم می‌شود که دو نقطه IPv6 از طریق مسیریاب‌های فقط IPv4 با هم ارتباط برقرار کنند بدون آنکه تغییری در زیرساخت قدیمی نیاز باشد.