بسمه تعالی

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

درس شبکه‌های کامپیوتری، نیم سال دوم سال تحصیلی ۱۴۰۱-۱۴۰۰

پاسخ تمرین سری ششم

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

پاسخ سوال ۱:

الف)

وظایف اصلی لایه شبکه عبارتند از:

- مسیریابی (Routing): پیدا کردن بهترین مسیر بین گره مبدأ و گره مقصد و به‌روزرسانی جدول جلورانی (Forwarding Table)
- جلورانی (Forwarding): هدایت یا جلورانی بسته‌ها به سمت گره مقصد بر اساس مسیرهای تعیین شده (جدول جلورانی)

ب)

همانطور که در بند (الف) بیان شد، لایه شبکه دو وظیفه اصلی (۱) انجام مسیریابی و تولید یا به‌روزرسانی جدول جلورانی و (۲) جلوررانی بسته‌ها را به عهده دارد. وظایف مسیریابی در صفحه کنترل (Control Plane) انجام می‌شود و وظایف جلورانی بسته‌ها در صفحه داده (Data Plane) انجام می‌شود. در شبکه‌های Traditional وظایف صفحه کنترل و صفحه داده توسط یک شرکت تولیدکننده تجهیزات شبکه درون یک مسیریاب پیاده‌سازی می‌شود و برای انجام وظایف صفحه کنترل تجهیزات شبکه (مسیریاب‌ها) به صورت یک سیستم توزیع‌شده عمل می‌کنند. اما در شبکه‌های نرم‌افزار محور (Software Defined Networks - SDN) تجهیزات شبکه فقط وظیفه جلورانی بسته‌ها (صفحه داده) را انجام می‌دهند و صفحه کنترل به صورت متمرکز انجام می‌شود. به عبارت دیگر، در SDN صفحه کنترل و صفحه داده از هم جدا شده و صفحه داده در تجهیزات شبکه و صفحه کنترل به صورت متمرکز و به صورت نرم‌افزاری انجام می‌شود.

ج)

مزایا SDN نسبت به شبکه‌های Traitional عبارتند از:

۱- سهولت نگهداری و پشتیبانی برنامه‌های کنترلی و مدیریت شبکه به صورت متمرکز و نرم‌افزاری

۲- افزایش نوآوری در مدیریت و کنترل شبکه با جداسازی صفحه کنترل و صفحه داده

۳- ایجاد تنوع در تأمین‌کننده تجهیزات، کنترلر و برنامه‌های کنترلی شبکه

۴- امکان یکپارچه‌سازی مدیریت شبکه با مدیریت سیستم و برنامه‌های کاربردی

۵- سهولت بررسی اثرات اعمال تغییرات در مدیریت و کنترل شبکه با ابزارهای نرم‌افزاری Network Emulation

۶- مدل‌سازی تحلیلی عملکرد شبکه و بررسی آن قبل از پیاده‌سازی

۷- کاهش هزینه‌های پیاده‌سازی (سرمایه‌گذاری) با ساده‌تر شدن تجهیزات شبکه

پاسخ سوال ۲:

الف)

سوئیچنگ بسته‌ای اتصال‌گرا یا مدار مجازی، سرویس اتصال‌گرا ارائه شده به لایه بالاتر توسط لایه شبکه است. در شبکه‌های مدار مجازی، لایه بالاتر (از لایه شبکه) باید قبل از ارسال داده‌ها، ابتدا درخواست ایجاد اتصال با لایه بالاتر گره مقصد را بدهد و لایه شبکه با پیدا کردن بهترین مسیر که پاسخگوی نیازمندی‌های لایه بالاتر است، مسیر (مدار مجازی) را ایجاد کند و سپس داده‌های لایه بالاتر را در قالب بسته‌ها از مسیر تعریف شده عبور داده و به مقصد تحویل دهد. در این سرویس پس از آن که لایه بالاتر داده‌ای برای انتقال ندارد، مسیر تعریف شده و منابع رزرو شده برای آن آزاد می‌گردند.

سوئیچینگ بسته‌ای بدون اتصال یا دیتاگرام، سرویس بدون اتصال ارائه شده به لایه بالاتر توسط لایه شبکه است. در شبکه‌های دیتاگرام، لایه بالاتر داده‌های خود را قالب یک سگمنت به لایه شبکه می‌دهد و لایه شبکه با اضافه کردن آدرس مقصد، یک بسته را تولید می‌کند. در شبکه‌های

دیتاگرام، لایه شبکه بر اساس آدرس مقصد و مسیرهای تعیین شده (از قبل)، بسته را به گره بعدی مسیر منتقل می‌کند و بدین ترتیب، هر بسته براساس مقصد گام به گام به جلو رفته تا نهایتاً به گره مقصد رسیده و به لایه بالاتر تحویل داده می‌شود.

ب)

مقایسه شبکه‌های دیتاگرام و مدارمجازی در جدول زیر آمده است:

ردیف	معیار	شبکه دیتاگرام	شبکه مدارمجازی
۱	تضمین کیفیت سرویس	ندارد	دارد
۲	ویژگی مقاوم بودن در برابر خرابی گره‌ها و لینک‌ها	دارد	ندارد
۳	گذردهی بالا سوئیچینگ برای رسیدن به شبکه‌های سرعت بالا	ندارد	دارد
۴	بهره‌وری بالا	دارد	ندارد

ج)

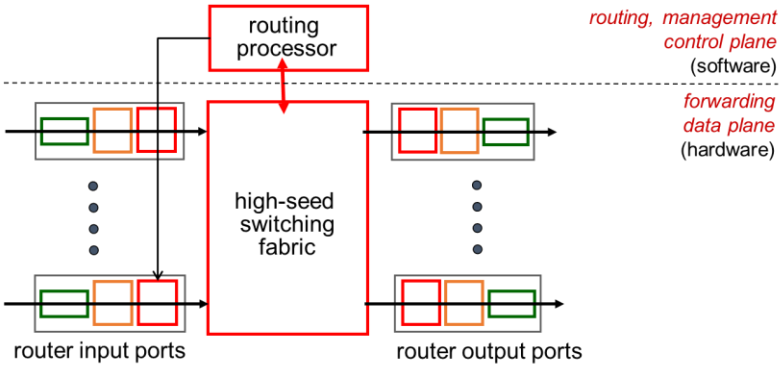
شبکه دیتاگرام ارجح‌تر است. زیرا اگر مسیرهاب‌ها قابل اطمینان نباشند و مرتباً از کار بیفتند، مدارهای مجازی قطع شده و مجدداً باید ایجاد شوند که باعث از دست رفتن تعداد زیادی بسته می‌شود. اما در شبکه‌های دیتاگرام، با تغییر توپولوژی به صورت پویا مسیرها اصلاح شده و جدول‌های جلورانی به‌روز می‌شوند.

د)

شبکه مدارمجازی ارجح‌تر است. زیرا در زمان تعیین مسیر می‌توان منابع لازم (ظرفیت سوئیچنگ و پهنای باند) در مسیر را رزور کرد و کیفیت سرویس را تضمین نمود.

پاسخ سوال ۳:

الف)



ب)

بار اصلی پردازشی در سوئیچ‌های شبکه دیتاگرام (سوئیچینگ بسته‌ای بدون اتصال)، جستجو در جدول جلورانی و پیدا کردن گام بعدی است. اگر این پردازش گلوگاه شود، می‌توان به ازای هر پورت ورودی (یا تعدادی از پورت‌های ورودی)، یک پردازنده (Forwarding engine) در نظر گرفت و با موازی‌سازی بار پردازشی را توزیع نمود.

ج)

بار اصلی پردازشی در سوئیچ‌های شبکه مدار مجازی (سوئیچینگ مدار مجازی)، پردازش ساده بر روی سرآیند بسته‌ها به منظور تغییر شناسه مدارهای مجازی است که می‌بایست به صورت متمرکز انجام شود. برای جلوگیری از overload شدن پردازنده، می‌بایست از پردازنده با قدرت پردازشی بالاتر استفاده نمود.

پاسخ سوال ۴:

الف)

دو مزیت استفاده از روش آدرس‌دهی CIDR عبارتند از:

۱- استفاده بهینه از فضای آدرس IP

۲- کوچک‌تر شدن اندازه جدول مسیریابی با تجمیع آدرس‌ها (اختصاص شناسه شبکه واحد به یک شبکه و یا شبکه‌های با پورت خروجی یکسان)

ب)

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.

ج)

۱- Interface 1
۲- Router 2
۳- Router 2

پاسخ سوال ۵:

الف)

ردیف	عنوان	تعریف
۱	Inside local address	یک آدرس IP خصوصی (Private) است که به یک میزبان در داخل شبکه محلی خودش اختصاص داده شده است.
۲	Inside global address	یک آدرس IP عمومی (Public) است که توسط NAT یک یا چند میزبان داخل شبکه محلی را به شبکه اینترنت معرفی می‌کند.
۳	Outside local address	یک آدرس IP خصوصی است که به میزبان مقصد اختصاص داده شده است. این آدرس بعد از NAT آدرس عمومی (Outside global address) به آدرس خصوصی، آدرس واقعی میزبان مقصد را مشخص می‌کند.
۴	Outside global address	یک آدرس IP عمومی است که معرفی کننده یک یا چند میزبان مقصد از دید بیرون از شبکه محلی است. این آدرس IP در بیرون شبکه محلی مقصد و قبل از ترجمه شدن است.

ب)

شرح این ارتباط به صورت زیر است:

۱- میزبان محلی (PC) با آدرس 172.168.20.10 بسته‌ای با آدرس مقصد 192.100.20.2 و آدرس مبدأ 172.168.20.10 را ارسال می‌کند.

۲- از آنجایی که آدرس مقصد خارج از شبکه محلی است، این بسته توسط مسیریاب دروازه NAT دریافت می‌شود. این مسیریاب یک سطر در جدول NAT خود ایجاد می‌کند و آدرس مبدأ بسته دریافتی و همچنین شماره پورت TCP را مطابق با سطر ایجاد شده در جدول NAT، تغییر داده و این بسته را با همان آدرس مقصد (192.100.20.2) و آدرس مبدأ 192.100.10.25 ارسال می‌کند.

۳- بسته با عبور از مسیریاب ISP توسط سرویس‌دهنده وب دریافت می‌شود. سرویس‌دهنده وب پاسخ را آماده کرده و توسط بسته‌ای با آدرس مقصد 192.100.10.25 و آدرس مبدأ 192.100.20.2 ارسال می‌کند.

۴- بسته با عبور از مسیریاب ISP به آدرس مقصد تعیین شده در بسته یعنی مسیریاب دروازه NAT می‌رسد. این مسیریاب با مراجعه به جدول NAT، آدرس میزبان محلی (172.168.20.10) و شماره پورت TCP را تغییر داده و بسته در داخل ارسال می‌کند.

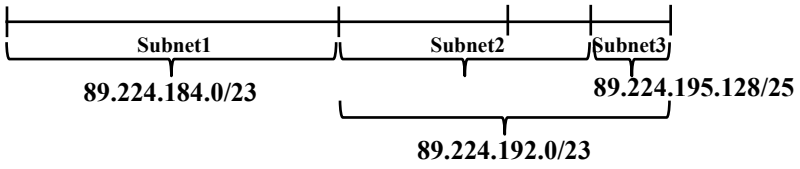
۵- بسته پاسخ توسط گره میزبان محلی (172.168.20.10) دریافت می‌شود.

پاسخ سوال ۶:

محدوده آدرس در اختیار (89.224.184.0/22) برابر است با $2^{10} = 1024$.

آدرس‌های مورد نیاز برای سه زیر شبکه عبارتند از:

SubNet1: $440 \Rightarrow 512$
SubNet2: $300 \Rightarrow 256 + 128 \Rightarrow 512$
SubNet3: $60 \Rightarrow 128$



SubNet1: 89.224.184.0/23
SubNet2: 89.224.192.0/23
SubNet3: 89.224.195.128/25

پاسخ سوال ۷:

الف)

با توجه به اینکه همه بسته‌های تولید شده به بیرون از شبکه ارسال می‌شوند، می‌توان تمام بسته‌های IP تولیدشده توسط میزبان‌های موجود در یک NAT را شنود کرد. از آن جایی که هر میزبان مجموعه‌ای از بسته‌های IP را با شماره‌های متوالی و شماره شناسایی اولیه منحصربه‌فرد (به دلیل انتخاب آن از یک فضای بزرگ) تولید می‌کند، می‌توان بسته‌های IP با شماره‌های شناسایی متوالی را در یک گروه قرار داد. تعداد گروه‌ها، تعداد میزبان‌های موجود در یک NAT را نشان می‌دهد.

ب)

اگر شماره‌های شناسایی مربوط به بسته‌های IP به صورت متوالی اختصاص داده نشود و به صورت تصادفی باشد، تکنیک پیشنهادشده در بخش قبلی، کارساز نخواهد بود. چون در این حالت امکان گروه‌بندی بسته‌های شنودشده وجود ندارد.

پاسخ سوال ۸:

مسیریاب‌های بی‌سیم معمولاً دارای یک سرور DHCP نیز هستند که از آن برای تخصیص آدرس IP به هر کدام از این پنج دستگاه و خود رابط مسیریاب استفاده می‌شود. مسیریاب از NAT استفاده می‌کند، زیرا از ISP فقط یک آدرس IP می‌گیرد و آدرس دستگاه‌های متصل به آن با NAT مدیریت می‌شوند.

پاسخ سوال ۹:

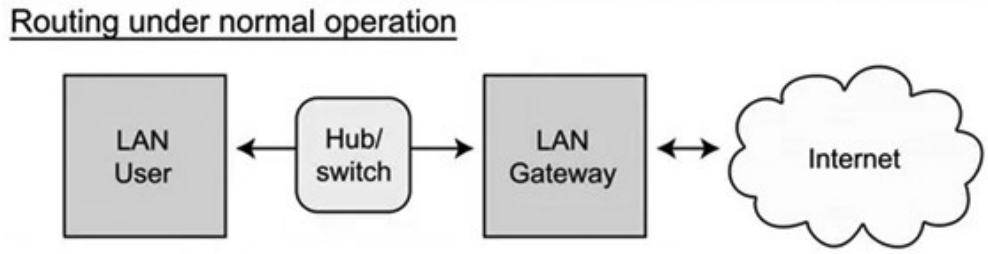
الف)

پروتکل ARP یا Address Resolution Protocol وظیفه‌ی بدست آوردن آدرس فیزیکی یا آدرس MAC گره مقصد با آدرس IP داده شده را دارد. پروتکل ARP برای بدست آوردن آدرس MAC گره مقصد، یک درخواست ARP را داخل شبکه محلی، ارسال فراگیر (Broadcast) می‌کند. محتوای این درخواست آدرس IP گره مقصد است. همه گره‌های شبکه این درخواست را دریافت کرده و طبق پروتکل ARP فقط گره مقصد با آدرس IP مشخص شده در درخواست باید پاسخ دهد. محتوای پاسخ آدرس MAC گره پاسخ‌دهنده است. بدین ترتیب گره درخواست‌کننده با دریافت پاسخ، آدرس MAC گره مقصد را بدست می‌آورد. گره درخواست‌کننده برای استفاده‌های بعدی، آدرس MAC متناظر با آدرس IP را در جدول ARP ذخیره می‌کند. از آنجایی که ممکن است گره‌ها ارتباط‌شان با شبکه قطع شود و آدرس IP آن‌ها به گره‌های دیگری تخصیص یابد، بنابراین آدرس MAC متناظر با آدرس IP نگهداری شده در جدول ARP، طول عمر (بین ۳ تا ۳۰ دقیقه) دارند و پس اتمام طول عمر از جدول ARP حذف می‌شوند.

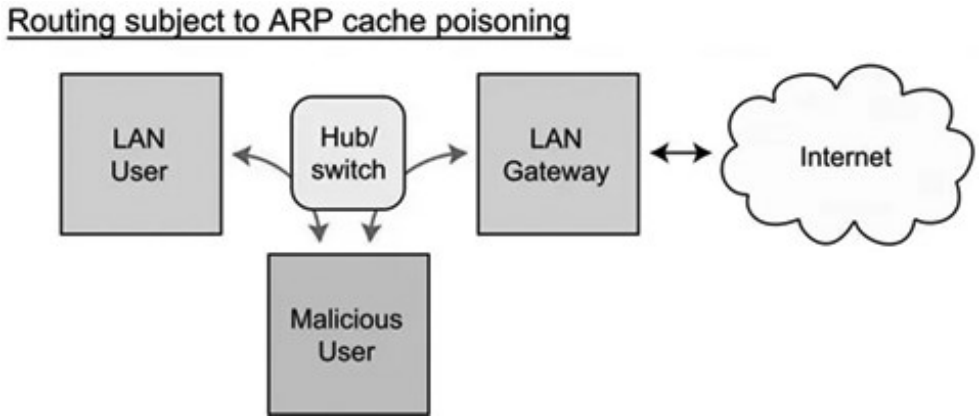
ب)

ARP Spoofing یک تهدید (حمله) امنیتی است. حمله ARP Spoofing از نوع حملات امنیتی Man in the Middle است. در این حمله گره بدخواه (Malicious) آدرس MAC خود را (درپاسخ به درخواست ARP یا حتی بدون وجود درخواست) به عنوان آدرس MAC گره دیگر و معمولاً

به عنوان آدرس MAC گره دروازه (Gateway) ارسال می‌کند و تمام بسته‌ها مربوط به آن گره را دریافت کرده، در صورت امکان شنود کرده و یا حتی تغییر داده و مجدداً برای گره اصلی ارسال می‌کند.



(قبل وقوع حمله)



(بعداز وقوع حمله)

پاسخ سوال ۱۰:

بسته ارسالی توسط گره A:

	Total Length	***Identification***	***MF***	***Fragment Offset***
Original Packet	5000	*K*	0	0

Fragmentهای دریافتی توسط گره B:

	Total Length	***Identification***	***MF***	***Fragment Offset***
Fragment 1	2996	*K*	1	0
Fragment 1	2024	*K*	0	372

Fragmentهای دریافتی توسط گره C:

	Total Length	***Identification***	***MF***	***Fragment Offset***
Fragment 1	1796	*K*	1	0
Fragment 2	1220	*K*	1	222
Fragment 3	1796	*K*	1	372
Fragment 4	248	*K*	0	594

Fragmentهای دریافتی توسط گره D:

	Total Length	***Identification***	***MF***	***Fragment Offset***
Fragment 1	1796	*K*	1	0
Fragment 2	1220	*K*	1	222
Fragment 3	1796	*K*	1	372
Fragment 4	248	*K*	0	594

پاسخ سوال ۱۱:

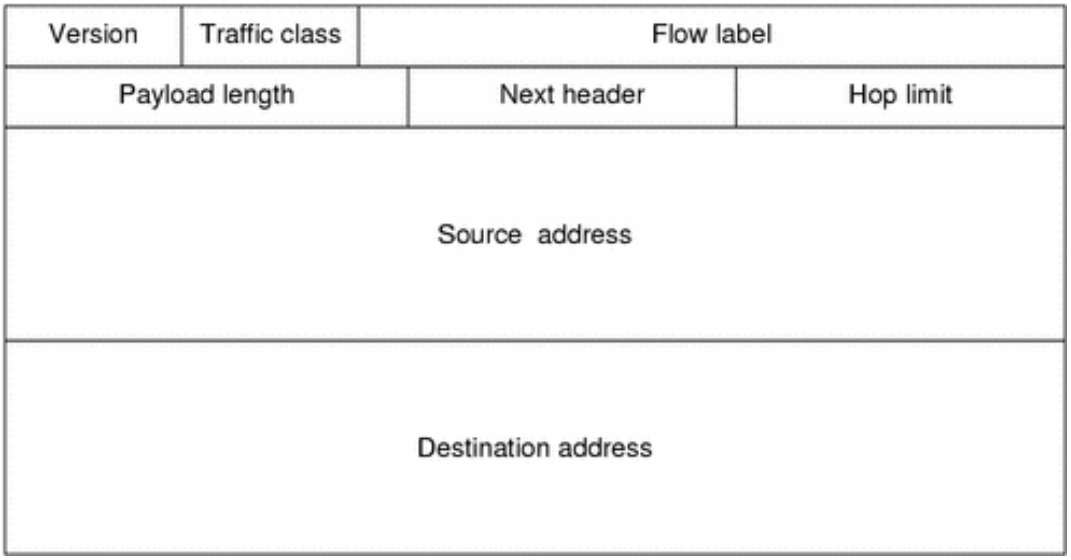
الف)

انگیزه اصلی تعریف پروتکل IPv6 محدودیت فضای آدرس پروتکل IPv4 و افزایش آن در پروتکل IPv6 بود.

ب)

ردیف	مزیت	شرح
۱	فیلد آدرس بزرگتر	در IPv4 فیلد آدرس ۳۲ بیت است، ولی در IPv6 به ۱۲۸ بیت افزایش پیدا کرده است. علاوه بر افزایش اندازه فیلد آدرس که باعث شده از نظر تئوری تا $۲^{۱۲۸}$ ($۳/۴ \times ۱۰^{۳۸}$) آدرس وجود داشته باشد، از نظر سلسله مرتب آدرس‌دهی بسیار مناسب‌ترطراحی شده است.
۲	ساده‌ترشدن سرآیند	سرآیند بسته‌های IPv6 بسیار ساده‌تر شده است و فیلدهایی نظیر IHL و فیلدهای fragmentation حذف گردیده‌اند.
۳	انعطاف‌پذیری بالا در پشتیبانی از optionها	Optionها در extention headerها قرار می‌گیرند که نسبت به IPv4 از انعطاف‌پذیری بالاتری برخوردار هستند.
۴	قابلیت flow label	از این فیلد برای تشخیص جریان بسته‌ها برای ارائه سرویس متمایز به هر جریان استفاده می‌شود.
۵	قابلیت امنیت ذاتی	IPv6 در درون خود از قابلیت تصدیق هویت و رمز نگاری پشتیبانی می‌کند.
۶	پشتیبانی از بسته‌های بزرگتر	IPv6 از بسته‌هایی با اندازه بزرگ‌تر از ۶۴ کیلوبایت (بسته‌های jumbo) پشتیبانی می‌کند.
۷	Fragmentation فقط در مبدأ	امکان Fragmentation فقط در مبدأوجود دارد (سادگی پردازش بسته‌ها در مسیریاب‌های میانی)
۸	عدم وجود فیلد checksum	در IPv6 فیلد checksum برای بالا بردن کارایی مسیریاب‌ها حذف شده است. کنترل خطا در صورت لزوم در لایه‌های بالاتر انجام خواهد شد و تشخیص خطا غالباً در لایه پایین‌تر انجام می‌شود.

ج)



شرح فیلدهای سرآیند بسته‌های IPv6:

ردیف	عنوان فیلد	شرح
۱	Version	این فیلد نسخه IP را نشان می‌دهد. نکته مهم این است جایگاه‌ای این فیلد تغییری نکرده و گره‌های شبکه براحتی می‌توانند آن را تشخیص دهند.
۲	Traffic Class	از این فیلد برای پشتیبانی از سرویس های متمایز (Differentiated) استفاده می‌شود. این فیلد بیان کننده نوع کلاس سرویس از لحاظ کیفیت سرویس مورد نیاز است.
۳	Flow Label	از این فیلد برای مشخص کردن کیفیت سرویس یکسان برای یک دسته از بسته‌ها مربوط به یک جریان داده، استفاده می‌شود که از سوی مبدأ مشخص می‌شود و مسیریاب‌ها با توجه به آن سعی می‌کنند، آن را رعایت کنند. اگر مبدا flow را پشتیبانی نکند باید این فیلد را 0 بگذارد.
۴	Payload length	این فیلد اندازه بسته حمل شده را مشخص می‌کند. با توجه به اینکه این فیلد دارای ۱۶ بیت می‌باشد بنابر این به طور نرمال اندازه بسته حداکثر ۶۴ کیلو بایت است، اما یکی از optionهای IPv6 ارسال بسته‌های بزرگتر از ۶۴ کیلوبایت است که در آن صورت باید از سرآمد اختیاری jumbo packet استفاده کرد.
۵	Next header	این فیلد مشخص می‌کند که آیا optionای وجود دارد یا خیر. این فیلد در صورت وجود option با اشاره به سرآیند بعدی مشخص می‌کند که option استفاده شده چیست. در سرآیند بعدی، نیز فیلد next header، نیز option بعدی را مشخص می‌کند تا نهایتاً فیلد next header به سرآیند پروتکل لایه بالایی (نظیر TCP، UDP، ICMP و ...) اشاره می‌کند.
۶	Hop limit	این فیلد حداکثر تعداد گام‌هایی را که بسته IP می‌تواند در شبکه طی کند تا به مقصد برسد مشخص می‌کند. این فیلد همان فیلد TTL در پروتکل IPv4 است.
۷	Source address and destination address	مشخص کننده آدرس IP مبدأ و مقصد بسته است.

د)

IPv6 از مکانیزم استانداری به نام Path MTU Discovery استفاده می‌کند که از طریق آن گره مبدأ می‌تواند حداقل MTU مسیر را کشف کند. در این مکانیزم اگر گره‌ای بسته بزرگ‌تر از MTU دریافت کند، با حذف بسته و ارسال پیام مدیریتی Packet Too Big، به گره مبدأ برای پیدا کردن حداقل MTU مسیر کمک می‌کند. در پروتکل IPv6، Fragmentation در قالب یک Option استفاده می‌شود و گره مقصد با دریافت بسته‌ای با Option مربوط به Fragmentation تشخیص می‌دهد که بسته Fragment شده و با توجه به اطلاعات موجود در Fragmentation Header و دریافت سایر Fragmentها بازسازی بسته را انجام می‌دهد.

پاسخ سوال ۱۲:

پروتکل DHCP برای پیکربندی پویای گره‌های شبکه اینترنت طراحی شده است. با استفاده از این پروتکل، تنظیمات مورد نیاز هر گره (میزبان) برای دریافت سرویس‌های اینترنت به صورت خودکار از طریق سرویس‌دهنده DHCP انجام می‌شود. این تنظیمات شامل آدرس IP، محدوده آدرس شبکه محلی (Network Mask)، آدرس IP دروازه شبکه (Gateway) و آدرس IP سرویس‌دهنده DNS است.

مزایا و کاربردهای DHCP عبارتنداز:

۱- مدیریت آدرس‌ها به صورت متمرکز
۲- اعمال سیاست‌های مدیریتی در انتساب آدرس‌ها
۳- انتساب آدرس IP به کاربران و سرویس‌گیرندگان موقتی نظیر dialup یا دسترسی WiFi
۴- تنظیمات به صورت خودکار و جلوگیری از خطاهای انسانی

عملیات DHCP به شرح زیر است:

۱- ارسال فراگیر (Broadcast) پیام DCHP Discover برای پیدا کردن سرویس‌دهنده (سرویس‌دهندگان) DHCP توسط گره میزبان

۲- دریافت پیام DCHP Discover و ارسال پیام DHCP Offer به همراه آدرس IP پیشنهادی توسط سرویس‌دهنده DHCP

۳- دریافت پیام DCHP Offer، انتخاب سرویس‌دهنده DHCP در صورت دریافت بیش از یک Offer و ارسال پیام DHCP Request توسط گره میزبان

۴- دریافت پیام DHCP Request و ارسال پیام DHCP Ack به همراه تنظیمات و زمان استفاده (T) از آدرس IP تخصیص داده شده توسط سرویس‌دهنده

۵- دریافت پیام DHCP Ack توسط گره میزبان و استفاده از تنظیمات و آدرس IP تخصیص داده شده و همچنین روشن کردن سه زمانبند (Timer) به نام‌های Renewal Timer ($T1$)، Rebinding Timer ($T2$) و Releasing Timer (T) به ترتیب با مقادیر $T1 = 0.5T$، $T2 = 0.875T$ و T. پس از سپری‌شدن زمان زمانبند Renewal، گره میزبان با ارسال پیام DHCP Request درخواست تمدید زمان دراختیار داشتن آدرس IP از سرویس‌دهنده DHCP می‌کند. درصورت دریافت پیام DHCP Ack، با زمان جدید تعیین شده مجدداً زمانبندها را روشن می‌شوند و اگر تا زمان Timeout زمانبند $T2$ پیام DHCP Ack را دریافت نکرد، با ارسال پیام DHCP Discover سعی می‌کند سرویس‌دهنده DHCPای را پیدا کند که آدرسIP و تنظیمات را از آن دریافت بگیرد، درصورت پیداکردن سرویس‌دهنده DHCP و دریافت آدرس IP، سایر تنظیمات و زمان استفاده از آدرس IP تخصیص داده شده، زمانبندها با زمان جدید مجدداً روشن می‌شوند. اگر تا زمان Timeout زمانبند T گره میزبان نتواند زمان در اختیار داشتن آدرس IP را تمدید کند، حق استفاده از آن نداشته و می‌بایست آدرس IP را رها کند.

پاسخ سوال ۱۳:

الف)

توپولوژی شبکه یک گراف تشکیل شده از مجموعه گره‌ها (میزبان‌ها و مسیریاب‌ها) و مجموعه لینک‌ها است. در این گراف ممکن است، از هر گره به هر گره دیگر، مسیرهای متعددی وجود داشته باشد. اما با توجه به وضعیت لینک‌ها و معیارهای مسیریابی، یکی از آن‌ها بهترین مسیر است. الگوریتم‌های مسیریابی با دریافت اطلاعات مسیریابی، بهترین مسیر را از گره مبدأ به گره مقصد را پیدا می‌کنند. با توجه به معیارهای مسیریابی و براساس وضعیت لینک به هر لینک یک هزینه اختصاص داده می‌شود. بنابراین بهترین مسیر، مسیر با کم‌ترین هزینه است. اگر هزینه را به فاصله تعبیر کنیم، آنگاه بهترین مسیر، کوتاه‌ترین (کم هزینه‌ترین) مسیر است. درنتیجه برای پیداکردن بهترین مسیر می‌توانیم از الگوریتم‌های کوتاه‌ترین استفاده کنیم. خروجی الگوریتم‌های مسیریابی، پس از پیداکردن بهترین مسیر یعنی مسیر (کم‌ترین هزینه یا کوتاه‌ترین مسیر)، تولید جدول جلورانی است تا بسته‌ها از طریق آن بر روی بهترین مسیر هدایت شده و به مقصد خود برسند.

ب)

با توجه به توضیحات بند (الف)، برای پیدا کردن بهترین مسیر از الگوریتم‌های کوتاه‌ترین مسیر استفاده می‌شود. به الگوریتم‌های مسیریابی نظیر الگوریتم Dijkstra که با داشتن توپولوژی شبکه (وضعیت همه لینک‌ها) به صورت متمرکز در هر گره اجرا شده و بهترین مسیرها را، از آن گره به همه گره‌های دیگر شبکه پیدا می‌کند، الگوریتم‌های مسیریابی وضعیت لینک یا Link State گفته می‌شود. در این الگوریتم هر گره یک پایگاه داده وضعیت لینک (Link State Database) دارد که وضعیت همه لینک‌های شبکه در آن به‌روز نگهداری می‌شود.

ج)

با توجه به توضیحات بند (الف)، برای پیدا کردن بهترین مسیر از الگوریتم‌های کوتاه‌ترین مسیر استفاده می‌شود. به الگوریتم‌های مسیریابی نظیر الگوریتم Bellman-Ford که به صورت توزیع شده در هر گره اجرا می‌شود و هر گره براساس هزینه‌های رسیدن گره‌های همسایه به مقصد و هزینه لینک مستقیم، بهترین مسیر را از طریق گره‌های همسایه پیدا می‌کند، الگوریتم‌های بردار فاصله یا Distance Vector گفته می‌شود. با توجه به تعبیر هزینه به فاصله، جدول هزینه‌های گره همسایه به همه گره‌های شبکه، بردار فاصله نامیده می‌شود. بنابراین هر گره برای پیداکردن بهترین

مسیرها به همه گره‌های شبکه نیاز به داشتن و نگهداری بردار فاصله همه گره‌های همسایه و دانستن هزینه‌های لینک‌های مستقیم به آن‌ها را دارد.

د)

مقایسه الگوریتم‌های مسیریابی Distance Vector و Link state در جدول زیر آمده است:

ردیف	معیار مقایسه	الگوریتم Link state	الگوریتم Distance Vector
۱	پیچیدگی پیام	زیاد بدلیل استفاده از الگوریتم flooding در اعلام وضعیت لینک‌ها	کم هر گره فقط تغییرات بردار فاصله خود را به همسایه‌های خود اطلاع می‌دهد
۲	سرعت همگرایی	بالا بدلیل اینکه پس از به‌روزرسانی وضعیت لینک‌ها با یک بار اجرا متمرکز الگوریتم، بهترین مسیرها پیدا شده و جدول‌های جلوررانی به روز می‌شوند	پایین بدلیل تأثیرگذاری تغییر جدول جلوررانی یک گره بر به‌روزرسانی گره‌های همسایه و بالعکس
۳	مقاوم بودن در برابر تغییرات توپولوژی و خطا	زیاد بدلیل اینکه هر گره جدول جلورانی خودش را تولید می‌کند و خطا در پیداکردن بهترین مسیرها و جدول جلورانی در شبکه پخش نمی‌شود	کم بدلیل اینکه هر گره جدول جلورانی خود را بر اساس جدول جلورانی گره‌های همسایه خود تولید می‌کند، بنابراین هر خطا در اجرای الگوریتم .D.V و جدول جلورانی گره همسایه در شبکه پخش می‌شود

پاسخ سوال ۱۴:

الف)

در الگوریتم مسیریابی سیل‌آسا (flooding) هر گره با دریافت یک بسته، یک کپی از آن بسته از طریق تمام پورت‌های خروجی به جز پورتی که از طریق آن بسته را دریافت کرده، ارسال می‌کند. به این کار ارسال فراگیر مجدد (Rebroadcast) گفته می‌شود.

ب)

این الگوریتم در موارد زیر کاربرد دارد:

۱- اطلاع‌رسانی یک اطلاعات به همه گره‌های شبکه، به عنوان مثال، ارسال اطلاعات وضعیت لینک‌ها به همه گره‌های شبکه در پروتکل‌های مسیریابی Link State.

۲- در زمان راه‌اندازی یک گره که اطلاعاتی از توپولوژی شبکه ندارد، نظیر دریافت آدرس یا تنظیمات اولیه.

۳- در کاربردهایی نظیر شبکه‌های بی‌سیم سیار که نرخ تغییرات توپولوژی زیاد است.

ج)

مشکل الگوریتم سیل‌آسا، سربار زیاد ارسال بسته‌ها Rebroadcast شده است که یک گره یک بسته را چندین بار دریافت و Rebroadcast می‌کند. یکی دیگر از مشکلات الگوریتم سیل‌آسا احتمال در Loop افتادن بسته‌ها است.

د)

راه‌حل‌های ارائه شده برای کاهش مشکلات الگوریتم سیل‌آسا عبارتند از:

۱- استفاده از فیلد Hop Limit در سرآیند بسته‌ها برای تعیین طول عمر بسته و حذف آن از شبکه پس از اتمام طول عمر آن

۲- اضافه کردن شناسه (ID) هر گره به سرآیند بسته برای جلوگیری از Loop

۳- نگهداری آدرس مبدأ و شناسه (ID) بسته در هر گره به منظور جلوگیری از ارسال فراگیر مجدد بیهوده و Loop

پاسخ سوال ۱۵:

Step	N'	$D(t),p(t)$	$D(u),p(u)$	$D(v),p(v)$	$D(w),p(w)$	$D(y),p(y)$	$D(z),p(z)$
0	x	$\infty,-$	$\infty,-$	$\underline{3,x}$	$6,x$	$6,x$	$8,x$
1	vx	$7,v$	$\underline{6,v}$		$6,x$	$6,x$	$8,x$
2	uvx	$7,v$			$\underline{6,x}$	$6,x$	$8,x$
3	$uvwx$	$7,v$				$\underline{6,x}$	$8,x$
4	$uvwxy$	$\underline{7,v}$					$8,x$
5	$tuvwxy$						$\underline{8,x}$
6	$tuvwxyz$						

پاسخ سوال ۱۶:

الف)

برای بالابردن سرعت همگرایی الگوریتم D.V. و جلوگیری از مشکل شمارش تا بی‌نهایت (Count to Infinity) از روش Poison Reverse استفاده می‌شود. در این روش، اگر گره همسایه یک گره، گام بعدی برای رسیدن به یک مقصد باشد، آن گره هزینه واقعی خود را به گره همسایه‌ای که گام بعدی برای رسیدن به مقصد است را اعلام نکرده و به جای هزینه بی‌نهایت (∞) را علام می‌کند.

ب)

2 –> time

گره X			
	X	Y	Z
X	0	2	1
Y	5	0	6
Z	6	1	0

گره Y			
	X	Y	Z
X	0	2	1
Y	5	0	6
Z	6	1	0

گره Z			
	X	Y	Z
X	0	∞	1
Y	5	0	6
Z	6	1	0

1

گره X			
	X	Y	Z
X	0	2	1
Y	5	0	6
Z	6	1	0

گره Y			
	X	Y	Z
X	0	3	1
Y	5	0	6
Z	6	1	0

گره Z			
	X	Y	Z
X	0	3	1
Y	5	0	6
Z	6	1	0

مقداردهی اولیه

گره X			
	X	Y	Z
X	0	3	1
Y	∞	∞	∞
Z	∞	∞	∞

گره Y			
	X	Y	Z
X	∞	∞	∞
Y	5	0	6
Z	∞	∞	∞

گره Z			
	X	Y	Z
X	∞	∞	∞
Y	∞	∞	∞
Z	6	1	0

پاسخ سوال ۱۷:

الف)

سیستم مستقل (Autonomous System - AS) یا Domain شبکه‌ای با مجموعه مسیریاب‌ها تحت مدیریت یک سازمان است.

ب)

ردیف	نوع AS	شرح
۱	Stub AS	Stub AS یا Single Homed AS، ASای است که فقط یک اتصال به شبکه اینترنت دارد، بنابراین، برای بسته‌های با آدرس مقصد خارج از شبکه خود نیاز به مسیریابی ندارد. Stub AS بسته‌های با آدرس مقصد خارج از محدوده آدرس‌های خود را از طریق مسیریاب مرزی (Border Gateway) به خارج از شبکه هدایت می‌کند.
۲	Multi-homed AS	Multi-homed AS، ASای است که چند اتصال به اینترنت دارد. این AS گره مبدأ یا گره مقصد بسته‌ها داخل این AS است. بنابراین، از چند طریق می‌تواند بسته‌های با آدرس مقصد خارج از شبکه خود را ارسال کند و همچنین از دید بیرونی نیز از چند طریق قابل دسترس است. Multi-homed AS برای پیدا کردن بهترین مسیر، نیاز به اجرای پروتکل‌های مسیریابی بین ASای دارد. Multi-homed AS برای اجرای پروتکل مسیریابی بین دامنه‌ای (بین ASای)، نیاز به داشتن یک شناسه به نام ASN (Autonomous System Number) دارد. Multi-homed AS ترافیک را از درون خود عبور (Transit) نمی‌کند.
۳	Transit AS	Transit AS، ASای است که با چندین اتصال به ASهای دیگر، ترافیک را از داخل خود عبور (Transi) می‌دهد. این AS برای پیدا کردن بهترین مسیر نیاز به اجرای پروتکل‌های مسیریابی بین دامنه‌ای (بین ASای) دارد. هر Transit AS، یک شناسه AS (ASN) دارد.

ج)

از آنجایی که تعداد گره‌ها در شبکه اینترنت بسیار زیاد است، انجام مسیریابی به صورت متمرکز از نظر پیچیدگی زمانی، حافظه مصرفی و سربار ارتباطی عملاً غیرممکن است. بنابراین باتوجه به اینکه مسیریابی باید دید سراسری داشته باشد، اما به دلیل پیچیدگی بالا اجرای آن به صورت متمرکز امکان‌پذیر نیست. راه‌حل ممکن برای حل این مسئله، اجرای سلسله‌مراتبی مسیریابی است. با اجرای سلسله‌مراتبی مسیریابی، پیچیدگی محاسباتی، حافظه مصرفی و سربار ارتباطی محدود گردیده، انجام مسیریابی مقیاس‌پذیر (Scalable) شده و با افزایش تعداد گره‌های شبکه کارآیی پروتکل‌های مسیریابی تغییرات قابل توجه‌ای ندارند. از طرف دیگر، شبکه اینترنت شبکه‌ای از شبکه‌ها است. شبکه اینترنت از اتصال شبکه‌های مستقل کوچک‌تر تشکیل شده است، بنابراین مدیریت هر شبکه یا سیستم مستقل (Autonomous System - AS) یا دامنه (در اصطلاحات اینترنت دامنه مترداف با AS است)، مستقلاً توسط مدیر آن شبکه انجام می‌شود. در این معماری هر گره انتهایی (میزبان) به عنوان گره مبدأ یا گره مقصد درون یک دامنه قرار دارد و برای پیداکردن یک مسیر بین گره مبدأ و گره مقصد که هر دو داخل یک دامنه هستند باید مسیریابی داخل دامنه‌ای (Intra-Domain) انجام شود. با توجه مدیریت مستقل، هر دامنه می‌تواند پروتکل مسیریابی داخل دامنه‌ای خود را داشته باشد. اما اگر گره مقصد درون دامنه‌ای به غیر از دامنه فرستنده باشد. این بسته باید از چند دامنه عبور کرده تا به دامنه مقصد برسد، بنابراین لازم است، دامنه‌ها با برای پیدا کردن بهترین مسیر بین دامنه‌ای (Inter-Domain) با اجرای یک پروتکل مسیریابی یکسان با هم همکاری کنند. در نتیجه در اینترنت مسیریابی به صورت سلسله‌مراتبی در دو سطح داخل دامنه‌ای و بین دامنه‌ای انجام می‌شود.

د)

در مسیریابی داخل دامنه‌ای، همه گره‌های داخل دامنه با یک خط‌مشی واحد توسط یک مدیریت، اداره می‌شوند. اما در مسیریابی بین دامنه‌ای، مسیریاب‌های مرزی اجراکننده پروتکل مسیریابی بین دامنه‌ای تحت کنترل مدیریت‌های متفاوت با خط‌مشی‌های مدیریتی متفاوت هستند. بنابراین در پروتکل‌های مسیریابی بین دامنه‌ای، مسیریابی با درنظر گرفتن خط‌مشی (ملاحظات) مدیریتی هر دامنه صورت می‌گیرد. درصورتی که در مسیریابی داخل دامنه این‌گونه نیست. به همین دلیل، پروتکل‌های مسیریابی داخل دامنه‌ای با پروتکل‌های مسیریابی بین دامنه‌ای متفاوت هستند.

پاسخ سوال ۱۸:

الف)

پروتکل RIP (Routing Information Protocol) یکی از پروتکل‌های مسیریابی داخل دامنه‌ای است. این پروتکل در لایه شبکه (اینترنت) قرار دارد و برای پیدا کردن بهترین مسیرها و به‌روزرسانی جدول جلوررانی از الگوریتم برار فاصله (Distance Vector) استفاده می‌کند. معیار مسیریابی در پروتکل RIP تعداد گام است. مسیر با کم‌ترین تعداد گام بهنترین مسیر است.

ب)

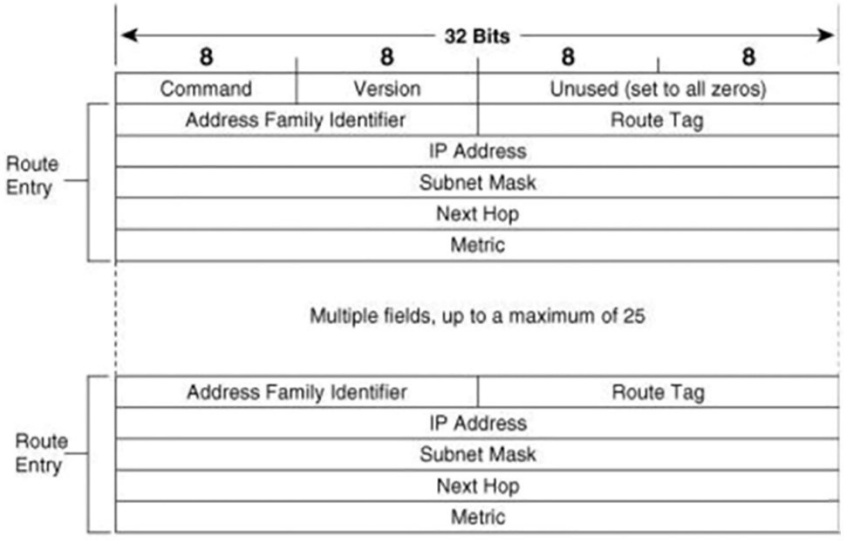
پروتکل RIP برای ارسال اطلاعات مسیریابی (بردار فاصله) از پروتکل UDP با پورت ۵۲۰ استفاده می‌کند. در پروتکل RIP، هر ۳۰ ثانیه یکبار یک بردار فاصله (جدول مسیریابی) از طریق واسطهای ارتباطی به همه مسیریاب‌های همسایه ارسال می‌شود. در صورتی که یک مسیریاب، ۱۸۰ ثانیه هیچ پیامی از مسیریاب همسایه دریافت نکند، اتصال خود با آن همسایه را قطع شده فرض نموده (هزینه لینک مستقیم را بی‌نهایت در نظر می‌گیرد) و جدول مسیریابی را با استفاده از جدول مسیریابی مسیریاب‌های همسایه دیگر و هزینه‌های لینک مستقیم به آن‌ها به‌روز می‌کند.

ج)

در پروتکل مسیریابی RIP معیار مسیریابی تعداد گام است و مسیر با کم‌ترین تعداد گام بهترین مسیر است. حداکثر تعداد گام در پروتکل RIP، ۱۵ است و تعداد گام ۱۶ به معنی بی‌نهایت در نظر گرفته می‌شود. بنابراین پروتکل RIP برای شبکه‌هایی مناسب است که حداکثر تعداد گام آن‌ها کمتر از ۱۵ است.

د)

فرمت پیام‌های RIP در شکل آمده است:



هر مسیر در RIP با فیلدهای اطلاعاتی زیر تعریف می‌شود:

- معرفی‌کننده خانواده آدرس (Address Family Identifier) برای مشخص کردن خانواده آدرس شبکه استفاده می‌شود. این فیلد برای آدرس‌های IP عدد ۲ است.
- برچسب مسیر (Route Tag) برای تمایز بین مسیرهای داخلی (یادگیری‌شده توسط RIP) و مسیرهای خارجی (یادگیری شده از پروتکل‌های دیگر) استفاده می‌شود. معمولاً از این فیلد استفاده نمی‌شود و مقدار آن صفر است.
- آدرس IP (IP address)، آدرس IP شبکه مقصد است.
- ماسک زیرشبکه (Subnet Mask)، تعداد بیت‌های شناسه شبکه () را مشخص می‌کند.
- گام بعدی (Next Hop)، گام بعدی برای رسیدن به مقصد است.

- متریک (Metric)، هزینه رسیدن به گره مقصد است.

در هر پیام RIP حداکثر اطلاعات ۲۵ مسیر قرار دارد.

پاسخ سوال ۱۹:

بله، پروتکل BGP به AS Z این امکان را می‌دهد تا تمام ترافیک AS Y را حمل کند ولی ترافیک AS X را حمل نکند. به دلیل اینکه AS X دارای توافق peering با AS Y و AS Y دارای توافق peering با AS Z است و پروتکل BGP به تمام ASها اجازه می‌دهد که اطلاعات قابلیت دسترسی به زیرشبکه‌ها (SubNetها) را از AS همسایه دریافت کند بنابراین AS Z با تشخیص آدرس زیرشبکه‌ها می‌تواند اینکار را انجام دهد.

پاسخ سوال ۲۰:

از آنجایی که در پروتکل BGP تمام اطلاعات مسیرها از یک AS به مقصدها دردسترس هستند، بنابراین یک BGP Peer مسیری بیاید که دارای شماره همان AS باشد، پس استفاده از آن مسیر موجب ایجاد حلقه می‌شود.

پاسخ سوال ۲۱:

الف)

پروتکل ICMP پروتکل مدیریتی لایه اینترنت (شبکه) است و در لایه اینترنت قرار دارد.

ب)

برنامه Ping از دو پیام Echo Request و Echo Reply پروتکل ICMP به منظور تست برقراری ارتباط و محاسبه زمان رفت و برگشت استفاده می‌کند.

ج)

برنامه Trace Route برای Trace کردن مسیر بین گره مبدأ و گره مقصد استفاده می‌شود. این برنامه با ارسال یک بسته با TTL=1 و دریافت پیام خطا Time Exceeded حذف بسته توسط اولین گره از طریق پروتکل ICMP، اولین گره مسیر را پیدا می‌کند، سپس به همین ترتیب با قرار دادن TTL=2، گره دوم و با ادامه اینکار همه گره‌های روی مسیر تا مقصد را به ترتیب کشف می‌کند.

پاسخ سوال ۲۲:

الف)

مکانیزم‌های MAC به دو دسته کلی مبتنی بر زمانبندی (Schedule-based) و مبتنی بر رقابت (Contention-based) تقسیم می‌شوند، که شرح و کاربرد آن‌ها در جدول زیر آمده است.

ردیف	مکانیزم MAC	شرح	مثال کاربرد
۱	مبتنی بر زمانبندی (Schedule-based)	در روش‌های مبتنی بر رقابت، برای کنترل دسترسی به رسانه مشترک، در هر سیکل ارسال، ایستگاه‌ها با یک مکانیزم هماهنگ‌سازی نظیر سرکشی (Polling) یا رزرواسیون (Reservation) نوبت‌بندی را انجام می‌دهند و هر ایستگاه در نوبت خود ارسال را انجام می‌دهد. در این روش‌ها تصادم وجود ندارد. این روش‌ها برای کاربردهای با بار ترافیکی زیاد مناسب هستند.	• روش Reservation در سرویس داده، شبکه موبایل نسل سوم (GPRS) • شبکه‌های محلی Token Ring، در استاندارد IEEE 802.5
۲	مبتنی بر رقابت (Contention-based)	در روش‌های مبتنی بر رقابت یا دسترسی تصادفی ()، هر ایستگاه بدون هماهنگی با ایستگاه‌های دیگر اقدام به ارسال اطلاعات می‌کند. از آنجایی که احتمال دارد بیش از دو ایستگاه به طور همزمان ارسال داشته باشند. بنابر این احتمال، تصادم وجود دارد. در همه روش‌های دسترسی تصادفی، مکانیزم تشخیص تصادم وجود دارد و همچنین ایستگاهی که تصادم را تشخیص می‌دهد، برای جلوگیری از تصادم	• شبکه اترنت (Ethernet)، استاندارد IEEE 802.3 با استفاده از روش CSMA/CD • شبکه بی‌سیم محلی (WiFi)، استاندارد IEEE 802.11 با

	بعدی باید به اندازه یک زمان تصادفی صبر کرد (Backoff Time) و مجدداً اقدام به ارسال مجدد کند. این روش‌ها برای کاربردهای با بار ترافیکی کم که تأخیر کم نیاز دارند، مناسب هستند. مهم‌ترین روش‌های دسترسی تصادفی عبارتند از: ALOHA، Slotted ALOHA، CSMA/CD، CSMA/CA.	استفاده از روش CSMA/CA

مقایسه مکانیزم‌های MAC مبتنی بر زمانبندی (Schedule-based) و مبتنی بر رقابت (Contention-based) در جدول زیر آمده است:

ردیف	معیار ارزیابی	مبتنی بر زمانبندی (Schedule-based)	مبتنی بر رقابت (Contention-based)
۱	تأخیر	زیاد بدلیل اینکه هر ایستگاه باید صبر کند و در نوبت خود ارسال را انجام دهد.	کم بدلیل اینکه هر ایستگاه هر زمان و بدون هماهنگی با ایستگاه‌های امکان ارسال را دارد.
۲	گذردهی	بالا در بار ترافیکی زیاد، گذردهی بالایی دارد، زیرا سربار روش‌های مبتنی بر زمانبندی تقریباً مستقل از بار ترافیکی است و نسبت سربار به حجم داده‌ها در بار ترافیکی بالا، خیلی کم است.	پایین سربار روش‌های مبتنی بر رقابت، ظرفیت ارسال از دست رفته بدلیل تصادم است. بدلیل اینکه در بار ترافیکی زیاد، احتمال وقوع تصادم افزایش می‌یابد، بنابراین، ظرفیت ارسال از دست رفته افزایش یافته و گذردهی کاهش می‌یابد.
۳	سربار	زیاد بدلیل وجود هماهنگ‌سازی بین گره‌های برای انجام نوبت‌بندی ارسال گره‌ها سربار این روش، خصوصاً در بار ترافیکی کم زیاد است.	کم بدلیل اینکه در این روش گره‌ها مستقل از هم عمل می‌کنند، در نتیجه سربار هماهنگ‌سازی وجود ندارد و سربار روش مبتنی بر رقابت بسیار کم است.
۴	هزینه پیاده‌سازی	زیاد بدلیل پیاده‌سازی پروتکل‌های هماهنگی‌سازی هزینه پیاده‌سازی این روش بالا است.	کم بدلیل اینکه در این روش هر گره به صورت مستقل و بدون هماهنگ‌سازی با دیگران اقدام می‌کند، پیاده‌سازی ساده‌تر و با هزینه کمتری دارد.

ب)

از آنجایی که در شبکه‌های بی‌سیم ناحیه تصادم (Collision Domain) هر ایستگاه با ایستگاه دیگر متفاوت است و تداخل در ایستگاه گیرنده مهم است نه ایستگاه(های) فرستنده، بنابراین دو مسئله در ارسال بی‌سیم به نام‌های ترمینال آشکار (Expose Terminal) و ترمینال مخفی (Hidden Terminal) بوجود می‌آید. در مسئله ترمینال آشکار، ایستگاه در حال ارسال اطلاعات در ناحیه تصادم فرستنده و خارج از ناحیه تصادم گیرنده است و مقصد ایستگاه در حال ارسال خارج از ناحیه تصادم فرستنده است. این مسئله فرستنده را به اشتباه می‌اندازد که اگر فرستنده ارسال کند برای گیرنده خود یا گیرنده ایستگاه در حال ارسال تداخل بوجود می‌آورد و در نتیجه فرستنده ارسال نمی‌کند که باعث کاهش گذردهی می‌شود. در مسئله ترمینال مخفی، ایستگاه درحال ارسال خارج از ناحیه تداخل فرستنده و داخل ناحیه تداخل گیرنده است و یا اینکه فرستنده داخل ناحیه تداخل گیرنده ایستگاه در حال ارسال است. دراین مسئله، چون فرستنده متوجه ارسال ایستگاه دیگر نیست درصورت اقدام به ارسال، در گیرنده یا درمقصد ارسال ایستگاه دیگر تداخل به وجود می‌آورد و اطلاعات ارسال شده از بین رفته و باید مجدداً ارسال شود.

در WiFi از روش کنترل دسترسی به رسانه CSMA/CA استفاده می‌شود. در این روش مسئله ترمینال مخفی تقریباً به طور کامل رفع می‌شود. در روش CSMA/CA، فرستنده زمانی که کانال را خالی تشخیص داد، ابتدا یک پیام بسیار کوتاه به نام درخواست ارسال (RTS) که احتمال تداخل آن کم بسیار پایین است، ارسال می‌کند. گیرنده با دریافت RTS با ارسال پیام پاسخ مبنی بر کانال برای ارسال خالی است (CTS)، اجازه ارسال به فرستنده می‌دهد. از آنجایی که پیام CTS را همه ایستگاه‌های داخل ناحیه تصادم گیرنده می‌گیرند، آن ایستگاه‌ها تا زمان اتمام دریافت

گیرنده مجاز به ارسال نیستند. بدین ترتیب از وقوع تداخل جلوگیری می‌شود. پس از اتمام دریافت اطلاعات، گیرنده با ارسال پیام ACK، آزاد شدن خود را اعلام می‌کند.

پاسخ سوال ۲۳:

جدول سوئیچ براساس Self-learning پر می‌شود. بدین ترتیب که سوئیچ با دریافت اولین فریم ارسالی هر ایستگاه، شماره پورتی که ایستگاه بر روی آن قرار دارد را تشخیص می‌دهد و به جدول MAC خود اضافه می‌کند. اگر سوئیچ فریمی را دریافت کرده که آدرس مقصد آن فریم در جدول MAC وجود نداشته باشد. برای اینکه آن فریم به ایستگاه مقصد برسد، آن فریم را در همه پورت‌های خود به غیر از پورتی که فریم را از آن دریافت کرده است ارسال همگانی (Broadcast) می‌کند.

۱- با دریافت فریم با مبدأ A و مقصد 'A، با توجه به اینکه سوئیچ در جدول MAC خود، مقصد 'A را ندارد. این فریم را در همه پورت‌ها به جز پورت ۱ که فریم از آن دریافت کرده broadcast می‌کند و یک سطر به جدول MAC اضافه می‌کند که ایستگاه A روی پورت ۱ است.

۲- با دریافت فریم با مبدأ 'A و مقصد A، با توجه به اینکه سوئیچ در جدول MAC خود، مقصد A را دارد. این فریم را فقط در پورت ۱ ارسال می‌کند و یک سطر به جدول MAC اضافه می‌کند که ایستگاه 'A روی پورت ۴ است.

۳- با دریافت فریم با مبدأ B و مقصد 'A، با توجه به اینکه سوئیچ در جدول MAC خود، مقصد 'A را دارد. این فریم را فقط در پورت ۴ ارسال می‌کند و یک سطر به جدول MAC اضافه می‌کند که ایستگاه B روی پورت ۲ است.

۴- با دریافت فریم با مبدأ B و مقصد B، با توجه به اینکه سوئیچ در جدول MAC خود، مقصد B را دارد و پورت خروجی در جدول MAC، پورت شماره ۲ است و پورتی که فریم از آن دریافت شده هم پورت شماره ۲ است این فریم حذف می‌شود (از پورتی دریافت شده که مقصد روی همان پورت است)، ولی در جدول MAC، TTL ایستگاه B به‌روز می‌شود.

(Switch MAC Table)

MAC Address	Port	TTL
A	1	57
A'	4	58
B	2	60

پاسخ سوال ۲۴:

(الف) و(ب)