پیام: " با سلام. این یک پیام تستی برای پروژه حل تمرین شبکه های کامپیوتری است."

سوال 1:

با فرض اینکه فضای شبکه در این مثال 192.168.184.0 باشد پس mask ان 255.255.255.0 میشود ولی چون نمیدانیم دقیقا این چه محدوده ای است میتوان حداقل فضایی که این شبکه میتواند داشته باشد را هم تعیین کرد. دراین صورت یه subclass از کلاس C داریم که ادرس شبکه ان 192.168.184.0 و mask ان 255.255.255.252 است و فقط دارای 4 ایپی از 184.0.* تا 184.3.* است. ولی همان طور که گفته شد چون در این مورد اطلاعی نداریم فرض میکنیم شبکه مورد نظر کلاس C است و subnetting رخ نداده.

	مبدا	مقصد
Ip address	192.168.184.1	192.168.184.3
MAC address	00:50:56:c0:00:01	00:0c:29:bb:b6:83
Class	C	C
mask	255.255.255.0	
Network address	192.168.184.0	
Broadcast Address	192.168.184.255	

سوال 2:

SIP (Session Initiation Protocol)

SIPپروتکلی است که برای ایجاد، مدیریت و خاتمه تماس‌های صوتی و تصویری در شبکه‌های IP استفاده می‌شود. این پروتکل در لایه کاربرد مدل OSI قرار دارد و به‌طور گسترده‌ای در VoIP (Voice over IP) و ارتباطات چندرسانه‌ای مورد استفاده قرار می‌گیرد .SIP مستقل از پروتکل‌های انتقال داده عمل می‌کند و با استفاده از روش‌های درخواست–پاسخ، تماس‌ها را برقرار، تغییر و خاتمه می‌دهد.

ARP (Address Resolution Protocol)

ARPپروتکلی است که برای تطبیق آدرس‌های IP به آدرس‌های MAC در شبکه‌های محلی (LAN) استفاده می‌شود.

هنگامی که یک دستگاه شبکه نیاز دارد تا آدرس MAC دستگاه دیگری را که آدرس IP آن را دارد، پیدا کند، یک بسته ARP Request به شبکه ارسال می‌کند.

دستگاهی که آدرس IP آن با درخواست ARP Request مطابقت دارد، یک بسته ARP Reply ارسال می‌کند که شامل آدرس MAC آن دستگاه است.

هر دستگاه شبکه یک جدول ARP نگه می‌دارد که شامل نگاشت‌های IP به MAC است تا در ارتباطات بعدی نیازی به ارسال درخواست‌های مکرر نباشد.

ICMP (Internet Control Message Protocol)

ICMPپروتکلی است که برای ارسال پیام‌های خطا و اطلاعات کنترلی در شبکه‌های IP استفاده می‌شود. این پروتکل توسط روترها و دستگاه‌های شبکه برای ارسال پیام‌هایی مانند "Destination Unreachable" یا "Time Exceeded"استفاده می‌شود. یکی از کاربردهای معروف ICMP ابزار پینگ (ping) است که برای تشخیص دسترسی‌پذیری دستگاه‌های شبکه و اندازه‌گیری زمان رفت و برگشت بسته‌ها استفاده می‌شود.

UDP (User Datagram Protocol)

UDPیک پروتکل لایه انتقال است که به ارسال سریع داده‌ها بین دستگاه‌ها کمک می‌کند. برخلافTCP ، UDPارتباط بدون اتصال است و از مکانیزم‌های تضمین تحویل، ترتیب بسته‌ها یا تصحیح خطا استفاده نمی‌کند. این باعث می‌شود که UDPبرای برنامه‌هایی که نیاز به سرعت بالایی دارند و تحویل همه بسته‌ها ضروری نیست، مانند پخش زنده و بازی‌های آنلاین، مناسب باشد.

SSDP (Simple Service Discovery Protocol)

SSDPبخشی از پروتکل‌های UPnP (Universal Plug and Play) است که برای کشف و معرفی دستگاه‌های شبکه و خدمات آن‌ها در شبکه‌های IP استفاده می‌شود .SSDP از پروتکل HTTP بر روی UDP استفاده می‌کند و به دستگاه‌ها امکان می‌دهد تا بدون نیاز به تنظیمات دستی، به‌طور خودکار به یکدیگر متصل شوند و سرویس‌های خود را اعلان کنند.

RTCP (Real-Time Control Protocol)

RTCPهمراه با پروتکل RTP (Real-Time Protocol) برای مدیریت و کنترل جریان‌های داده‌های چندرسانه‌ای در زمان واقعی استفاده می‌شود. RTCP اطلاعات کنترلی مانند آمار ارسال و دریافت بسته‌ها، تأخیر و از دست دادن بسته‌ها را ارسال می‌کند تا به تنظیم کیفیت و کارایی جریان‌های RTP کمک کند. این پروتکل به بهبود تجربه کاربری در برنامه‌های ویدئویی و صوتی زنده کمک می‌کند.

SDP (Session Description Protocol)

SDPپروتکلی است که برای توصیف پارامترهای جلسات چندرسانه‌ای به کار می‌رود. این پروتکل اطلاعاتی مانند فرمت‌های رسانه‌ای، آدرس‌های شبکه و پورت‌ها را که برای ایجاد، تنظیم و مدیریت جلسات چندرسانه‌ای لازم است، ارائه می‌دهد. SDP اغلب در پروتکل‌های SIP و RTSP استفاده می‌شود.

TCP (Transmission Control Protocol)

TCPیکی از پروتکل‌های اصلی لایه انتقال است که برای ارتباطات قابل اعتماد در شبکه‌های IP استفاده می‌شود . TCP ارتباطات بر پایه اتصال را فراهم می‌کند و از مکانیزم‌هایی مانند تصدیق دریافت، کنترل جریان و تصحیح خطا برای تضمین تحویل درست داده‌ها استفاده می‌کند. این پروتکل برای برنامه‌هایی که نیاز به انتقال داده‌های قابل اعتماد دارند، مانند وب، ایمیل و انتقال فایل، مناسب است.

SSHv2 (Secure Shell version 2)

SSHv2پروتکلی است که برای ایجاد ارتباطات امن در شبکه‌های نامطمئن استفاده می‌شود. این پروتکل به کاربران امکان می‌دهد تا به‌طور ایمن به سرورها و دستگاه‌های شبکه متصل شوند و دستورات را اجرا کنند. SSHv2 از رمزنگاری قوی برای حفاظت از حریم خصوصی و یکپارچگی داده‌ها بهره می‌برد و ویژگی‌هایی مانند تصدیق هویت، انتقال داده‌های رمزگذاری‌شده و تونل‌زنی امن را فراهم می‌کند.

سوال 3:

جدول فیلدهای(RTP (Real-Time Protocol

فیلد	توضیحات
Version	نسخه پروتکلRTP ، معمولاً مقدار 2 دارد.
Padding	نشان می‌دهد که آیا در پایان بسته داده‌های پدینگ وجود دارد یا خیر.

Extension	نشان می‌دهد که آیا هدر دارای بخش افزایشی است یا خیر.
CSRC Count	تعداد شناسه‌های منبع همزمان (CSRC) که در هدر آمده‌اند.
Marker	این بیت برای علامت‌گذاری بسته‌های خاص استفاده می‌شود، مثلاً برای نشان دادن آغاز یک فریم ویدیویی جدید.
Payload Type	نوع بار مفید (Payload) که نشان دهنده فرمت داده‌های صوتی یا تصویری در بسته است.
Sequence Number	شماره دنباله که برای تشخیص ترتیب بسته‌ها و از دست رفتن بسته‌ها استفاده می‌شود.
Timestamp	زمان ارسال بسته که برای همگام‌سازی جریان‌های صوتی و تصویری استفاده می‌شود.
SSRC	شناسه منبع همگام‌سازی که یک شناسه منحصر به فرد برای جریان RTP است.
CSRC List	لیستی از شناسه‌های منبع همزمان که در جریان ترکیبی استفاده می‌شود.

جدول فیلدهای(SIP (Session Initiation Protocol

فیلد	توضیحات
Request Line / Status Line	خط اول پیام SIP شامل نوع درخواست) مثل (INVITE, ACK, BYE یا کد وضعیت برای پاسخ‌ها است.
Via	نشان‌دهنده مسیری که پیام SIP طی کرده است.
From	اطلاعات فرستنده پیام، شامل URI و برچسب‌های مرتبط.
To	اطلاعات گیرنده پیام، شامل URI و برچسب‌های مرتبط.
Call-ID	شناسه منحصر به فردی که برای شناسایی یک تماس یا جلسه استفاده می‌شود.
CSeq	شماره دنباله و نوع روش درخواست، برای همگام‌سازی و ترتیب درخواست‌ها در یک جلسه خاص.
Contact	URIتماس که نشان‌دهنده جایی است که پاسخ‌ها باید ارسال شوند.
Max-Forwards	تعداد دفعاتی که یک پیام SIP می‌تواند از یک نود به نود دیگر ارسال شود قبل از آن که حذف شود.
Content-Type	نوع محتوا که نوع داده‌های پیوست شده به پیام) مثل (SDP را مشخص می‌کند.
Content-Length	طول محتوای پیوست شده به پیام.
Expires	زمان انقضای یک پیام SIP یا دعوت‌نامه.
User-Agent	نرم‌افزار کلاینتی که پیام SIP را ارسال کرده است.
Allow	لیستی از روش‌های SIP که توسط سرور یا کلاینت پشتیبانی می‌شود.
Supported	قابلیت‌های افزوده شده که توسط کلاینت یا سرور پشتیبانی می‌شوند.

Require	مشخص می‌کند که کدام ویژگی‌ها باید توسط طرف مقابل پشتیبانی شوند تا درخواست مورد نظر موفق باشد.
Proxy-Authorization	اطلاعات تصدیق هویت که برای عبور از پراکسی‌ها استفاده می‌شود.
Proxy-Require	ویژگی‌هایی که باید توسط پراکسی پشتیبانی شوند تا درخواست موفق باشد.

سوال 4:

تحلیل مشکلات:

1. **تکرار اطلاعات:**

اطلاعات بسته به صورت تکراری آمده است. این تکرار ممکن است ناشی از خطا در جمع‌آوری داده‌ها یا نمایش اطلاعات باشد. از انجایی که این مشکل در بقیه بسته های SIP هم دیده میشود پس مشکل عمومی میباشد.

2. **نبودن فیلدهای ضروری در هدر:SIP**

اطلاعات هدر بسته SIP ناقص است. فیلدهایی مثل `From, To, Call-ID, CSeq, Contact` در جزئیات بسته موجود نیستند. این فیلدها برای عملکرد صحیح پروتکل SIP ضروری هستند و نبودن آنها می‌تواند نشان‌دهنده خطا در تشکیل بسته SIP باشد.

3. **بررسی وضعیت چکسام:**

چکسام‌های بسته‌های IP و UDP به صورت unverified (تأیید نشده) نمایش داده شده‌اند. بررسی چکسام‌ها می‌تواند نشان‌دهنده وجود خطا در انتقال داده‌ها باشد. اگر چکسام‌ها نادرست باشند، ممکن است داده‌ها در طول مسیر خراب شده باشند.

4. **اطلاعات ناقص در بخش:SIP**

جزئیات هدر بسته SIP تنها به Request-Line محدود شده است و سایر فیلدهای هدر موجود نیستند. این می‌تواند نشان‌دهنده مشکل در جمع‌آوری داده‌ها یا تجزیه بسته‌ها باشد.