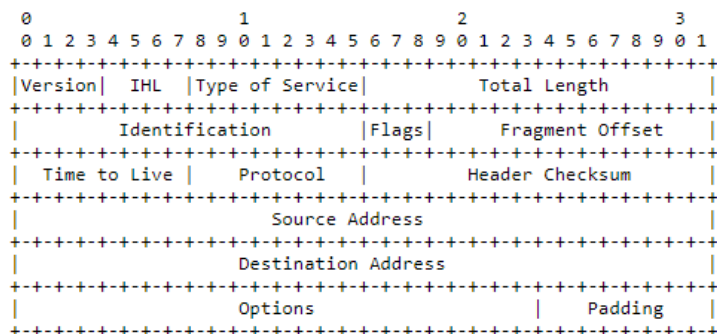


- قالب **HEADER** بسته‌های پروتکل‌های زیر را با رسم شکل بیان کنید و بگویید وظیفه هر **FIELD** چیست. (برای پاسخ به این پرسش می‌توانید از **RFC** های 768، 791، 793، 2473 کمک بگیرید.)

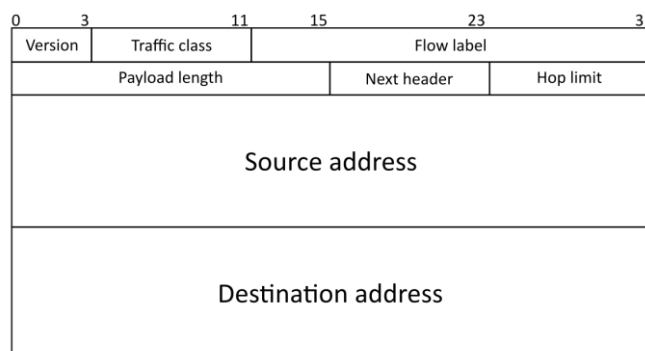
#### IPv4 ■



Example Internet Datagram Header

- Version:** نسخه پروتکل، برای IPv4 این مقدار ۴ است.
- IHL:** اندازه header (حداقل ۵)
- Type of Service:** میزان اهمیت بسته، تأخیر، throughput و reliability را نشان می‌دهد
- Total Length:** تعداد اکتت (۸بیتی)های بسته (header + داده)
- Identification:** مقداری که فرستنده تعیین می‌کند برای کمک در assemble کردن fragmentها
- Flags:** flagهای کنترل، نشان‌دهنده fragment شدن یا نشدن و یا آخرین یا غیر آخرین بودن fragment
- Fragment Offset:** بسته در کجای fragment قرار دارد
- Time to Live:** حداکثر زمانی (ثانیه) که بسته می‌تواند در شبکه بماند
- Protocol:** نشان دهنده پروتکل استفاده‌شده برای داده
- Header Checksum:** checksum (مکمل ۱) header، برای بررسی این که آیا داده تغییر کرده‌است یا خیر
- Source Address:** آدرس مبدأ
- Destination Address:** آدرس مقصد
- Options:** اطلاعات بیشتر در مورد بسته
- Padding:** مقداری که تضمین کند بسته از تعدادی word ۳۲ بیتی تشکیل شده‌است

## IPv6



**Version:** نسخه پروتکل، برای IPv6 این مقدار ۶ است

**Traffic class:** نشان‌دهنده field Differentiated Service (دسته‌بندی بسته‌ها) و Explicit

Congestion Notification (قابلیت کنترل ازدحام) (congestion))

**Flow Label:** بسته متعلق به کدام flow (گروهی از بسته‌ها) است (صفر یعنی به هیچ‌کدام تعلق

ندارد)

**Payload Length:** تعداد اکتت (۸بیتی)های بسته (header + داده)

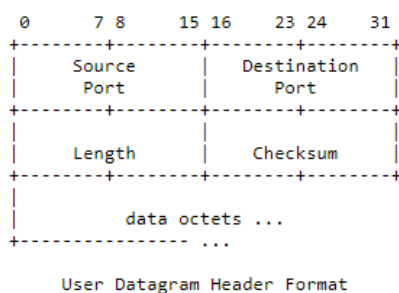
**Next header:** نشان‌دهنده header بعدی (معمولاً پروتکل لایه انتقال)

**Hop Limit:** حداکثر دفعاتی که بسته می‌تواند بین node ها منتقل شود

**Source Address:** آدرس مبدأ

**Destination Address:** آدرس مقصد

## UDP



**Source Port:** پورت مبدأ (فرستنده)

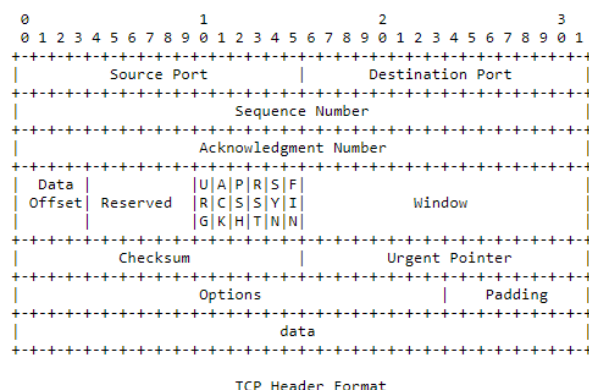
**Destination Port:** پورت مقصد (گیرنده)

**Length:** تعداد اکتت (۸بیتی)های بسته (header + داده)

**Checksum:** برای بررسی این که آیا داده تغییر کرده است یا خیر (تماماً صفر در صورت عدم استفاده)

**Data Octets:** داده‌ای که قرار است منتقل شود

## TCP ■



Note that one tick mark represents one bit position.

**Source Port:** پورت فرستنده

**Destination Port:** پورت مقصد

**Sequence Number:** اگر SYN flag یک باشد، نشان‌دهنده اولین sequence number است؛

در غیر این صورت، نشان‌دهنده sequence number اولین بایت داده این سگمنت است.

**Acknowledgement Number:** اگر بیت کنترلی ACK در flagها یک باشد، نشان‌دهنده

sequence number بعدی است که فرستنده ACK انتظار دارد دریافت کند

**Data Offset:** اندازه header، نشان‌دهنده این که داده از کجا شروع می‌شود

**Reserved:** برای استفاده در آینده؛ باید صفر باشد

**Flags:** نشان‌دهنده ویژگی‌های بسته

**Window:** سایز window دریافت (حجم داده دریافتی بدون گرفتن ACK از فرستنده) را نشان

می‌دهد

**Checksum:** برای بررسی این که آیا داده تغییر کرده‌است یا خیر

**Urgent Pointer:** نشان‌دهنده مکان بسته در داده ضروری (urgent) در صورت یک بودن flag

URG

**Options:** مشخصات بیشتر در مورد بسته

**Padding:** مقداری که تضمین کند بسته از تعدادی word ۳۲ بیتی تشکیل شده‌است

**Data:** داده‌ای که باید منتقل شود

• با جست‌وجو در اینترنت درباره **Transport Layer Security** تحقیق کنید،

کاربردهای آن را بنویسید و جایگاه آن در مدل لایه‌ای را تشریح کنید.

TLS یک پروتکل رمزنگاری که برای ارتباط امن در شبکه‌های کامپیوتری طراحی شده‌است.

کاربردهای TLS:

✓ در web browser ها

✓ برنامه‌های پیام‌رسانی

✓ ایمیل

✓ VoIP

جایگاه TLS در مدل لایه‌ای به صورت کاملاً واضح مشخص نیست؛ TLS بر روی یک پروتکل قابل اطمینان لایه انتقال اجرا می‌شود که نشان‌دهنده این است که بالاتر از لایه انتقال قرار می‌گیرد؛ اما، برنامه‌ها با TLS مانند یک پروتکل لایه انتقال برخورد می‌کنند.

## • در مورد IPSec تحقیق کنید.

### (1) IPSec چیست؟

مجموعه از پروتکل‌های امن است که بسته‌ها را رمزنگاری می‌کند تا ارتباطی امن برقرار شود.

### (2) کاربردهای آن را بنویسید؟

IPSec در VPN‌ها استفاده می‌شود و می‌تواند از جریان اطلاعات بین دو host و یا بین یک gateway و یک شبکه محافظت کند؛ همچنین، از data-origin authentication، data integrity، data confidentiality (encryption) و replay protection پشتیبانی می‌کند.

### (3) مزایا و معایب استفاده از آن را مورد بررسی قرار دهید.

مزایا:

- بر لایه transport اعمال می‌شود و تاثیری بر protocol‌های لایه application ندارد.
- تکنولوژی‌های استفاده شده در client-to-site، site-to-site و client-to-client تفاوتی با یکدیگر ندارند.
- از امنیت بالایی برخوردار است.

معایب:

- سرعت پایینی دارد.
- باید نرم‌افزارهای مخصوصی روی سیستم‌ها نصب شود.

## • در بسته‌های IPv4 مقدار فیلد Protocol چیست؟ و چه مقادیری می‌تواند

داشته‌باشد؟

در بسته‌های IPv4 مقدار فیلد Protocol، مقداری ۸ بیتی بین صفر تا ۲۵۵ (0x00 – 0xFF) است که نوع پروتکل استفاده‌شده را تعیین می‌کند.