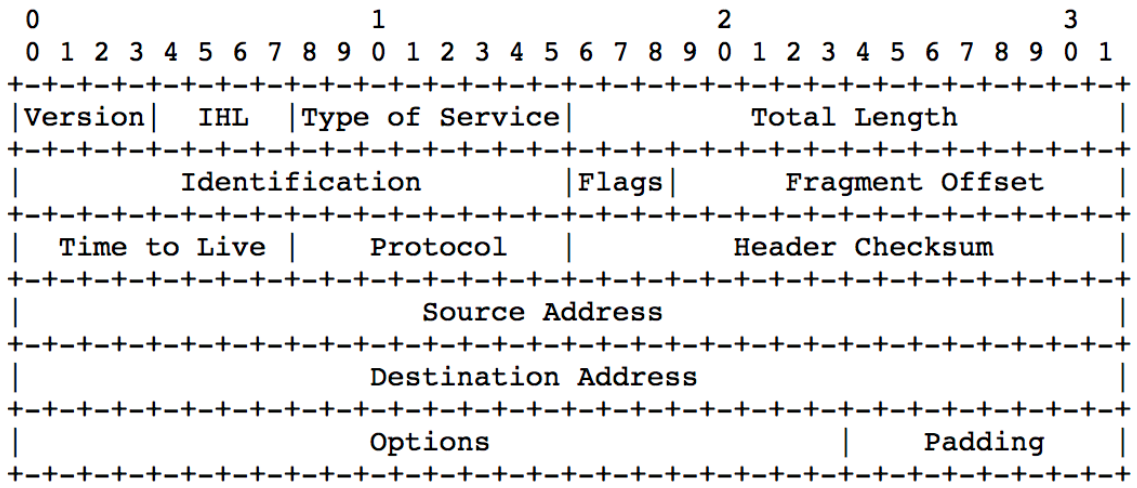
پروژه‌ی دوم درس شبکه‌های کامپیوتری CN

بخش اول: پرسش‌ها

۱. قالب Headerها

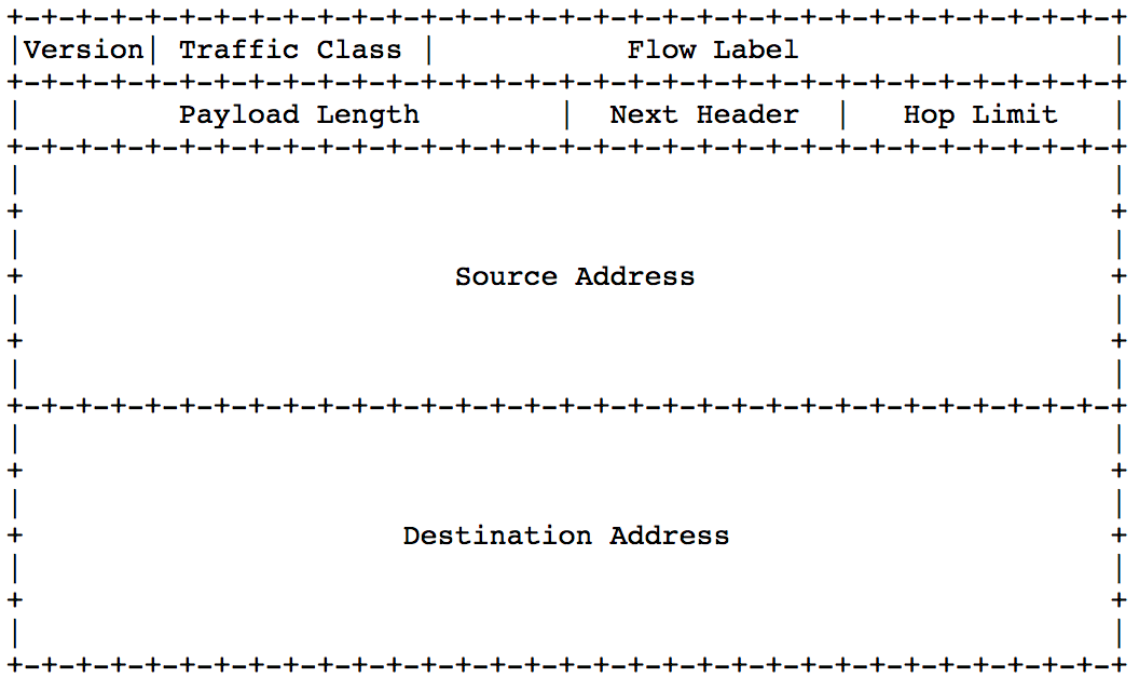
- IPV4:

- **Version**: نسخه‌ی اینترنت بسته (در IPv4: 4)
- **IHL**: طول Header بسته‌ی اینترنت را برحسب تعداد word (4 byte)
- **Type of Service**: 3 بیت اول این بسته، الویتش را مشخص می‌کند. 3 بیت بعدی پارامترهای کیفیت مطلوب (به ترتیب Delay, Throughput, Reliabilty) این بسته را مشخص می‌کند.
- **Total Length**: طول کل بسته‌ی اینترنت.
- **Identification**: یک رشته‌ی ۱۶ بیتی برای شناسایی هر بسته، که در reassemble کردن بسته‌های fragment شده به ما کمک می‌کند.
- **Flags**: بیت دوم این رشته‌ی 3 بیتی مشخص می‌کند که آیا روتر مجاز به fragment کردن بسته هست یا خیر. بیت سوم هم تعیین می‌کند که در صورت fragment شدن، آیا این بسته، بسته‌ی آخر یک سری بسته‌ی fragment شده هست یا خیر.
- **Fragment Offset**: هنگام reassemble کردن بسته‌های fragment شده، برای بازیابی بسته‌ی اصلی، نیاز داریم بدانیم که هر بسته کجای بسته‌ی اصلی را تشکیل داده است. برای این موضوع از Fragment Offset استفاده می‌کنیم.
- **Time to Live**: مدّت زمانی که بسته می‌تواند در شبکه‌ی اینترنت بماند (بر حسب ثانیه). هر روتر حدّاقل یک واحد از این مقدار کم می‌کند. این Field به شبکه کمک می‌کند که بسته‌های غیر قابل ارسال را از خود حذف کند تا ترافیک پایین بیاید.
- **Protocol**: پروتکل سطح بعدی را مشخص می‌کند. این پروتکل می‌تواند مختص لایه‌ی انتقال باشد ((6, TCP) یا (21, UDP)). یا خارج از لایه‌ی انتقال باشد ((1, ICMP).)
- **Header Checksum**: مکانیزم Checksum برای خطایابی روی بیت‌های Header؛ که طریقه‌ی محاسبه‌ی آن به این صورت است که مکمل ۱ تمام Half Wordها را با هم جمع می‌کنیم، سپس از آن مکمل یک می‌گیریم.
- **Source Address**: آدرس ip مبدأ
- **Destination Address**: آدرس ip مقصد
- **Options**:
- **Padding**: یک سری بیت اضافی برای رساندن بخش Header به مضرب 32.

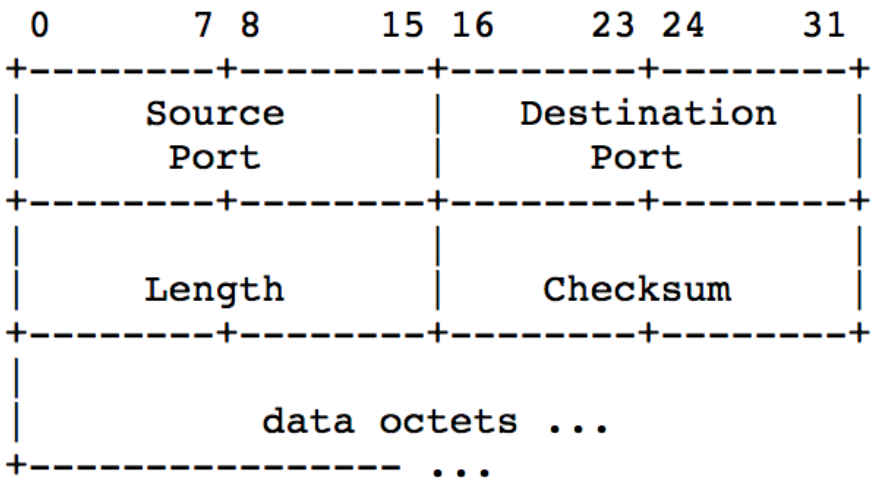


Example Internet Datagram Header

- **IPv6:**
  - **Version**: عدد ۴ بیتی نشان‌دهنده‌ی ورژن بسته (در IPv6: 6)
  - **Traffic Class**: یک عدد ۸ بیتی نشان‌دهنده کلاس ترافیک بسته. این فیلد به نوعی معادل فیلد ToS در IPv4 است، و از آن برای دسته‌بندی بسته‌های ترافیک شبکه، و مدیریت هر یک بنا بر پارامتر کیفیت مطلوبش استفاده می‌شود.
  - **Flow Label**: به گروهی از بسته‌های مرتبط به هم (مثلاً در یک TCP Session) Flow گفته می‌شود. برای شناسایی این Flowها از این فیلد ۲۰ بیتی استفاده می‌شود. در صورتی که یک بسته متعلق به هیچ Flow نباشد، Flow Label آن 0 خواهد بود.
  - **Payload Length**: یک عدد بی‌علامت ۱۶ بیتی، نشان‌دهنده‌ی طول payload این بسته.
  - **Next Header**: نوع Header بعدی را مشخّص می‌کند. برای مثال مشخّص می‌کند Header بعدی مختص پروتکل TCP است.
  - **Hop Limit**: یک عدد بی‌علامت ۸ بیتی، نشان‌دهنده‌ی تعداد گام‌هایی که هر بسته می‌تواند طی کند قبل از drop شدن. (به انتقال از هر روتر به روتر بعدی یک گام گفته می‌شود.) کاربرد این فیلد مانند فیلد TTL در IPv4 است.
  - **Source Address**: آدرس مبدأ به صورت یک رشته‌ی 128 بیتی.
  - **Destination Address**: آدرس مقصد به صورت یک رشته‌ی 128 بیتی.

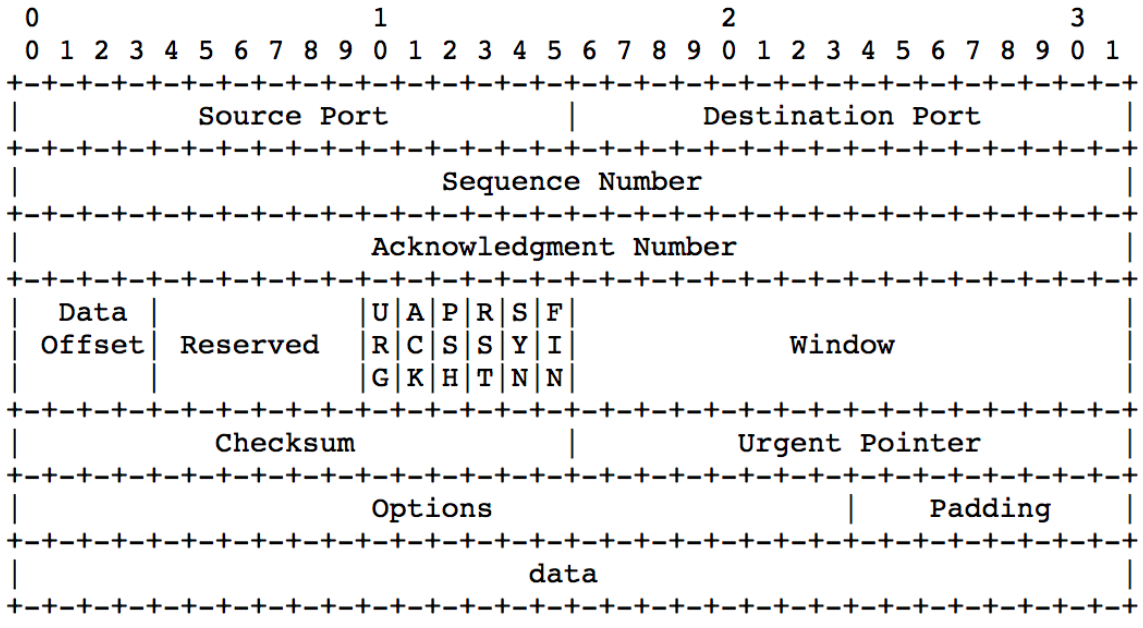


- **UDP**:
  - **Source Port**: یک عدد 16 بیتی، شماره‌ی port مبدأ ارتباط. چون بعضی portها well known هستند، از روی این فیلد و فیلد بعدی می‌توان پروتکل لایه‌ی Application بسته را تشخیص داد.
  - **Destination Port**: یک عدد 16 بیتی، شماره‌ی port مقصد ارتباط.
  - **Length**: طول کل بسته (Header + Payload) بر حسب بایت.
  - **Checksum**: مکانیزم خطایابی روی Header. که به صورت مکمل ۱ گرفتن از مجموع 3 فیلد دیگر Header به دست می‌آید. این مکانیزم در IPv4 اختیاری، و در IPv6 اجباری است.



User Datagram Header Format

- **TCP**:
  - **Source Port**: یک عدد 16 بیتی، شماره‌ی port مبدأ ارتباط. چون بعضی portها well known هستند، از روی این فیلد و فیلد بعدی می‌توان پروتکل لایه‌ی Application بسته را تشخیص داد.
  - **Destination Port**: یک عدد 16 بیتی، شماره‌ی port مقصد ارتباط.
  - **Sequence Number**: این فیلد 32 بیتی Sequence Number اولین بایت دیتای این بسته را مشخص می‌کند، که از آن برای Reliable Data Transfer استفاده می‌شود.
  - **Acknowledgement Number**: در صورت 1 بودن بیت کنترلی Ack، این فیلد 32 بیتی Sequence Number بسته‌ی بعدی مورد انتظار فرستنده را نشان می‌دهد.
  - **Data Offset**: یک عدد 4 بیتی، نشان‌دهنده‌ی اندازه‌ی بخش Header بر حسب Word (4 bytes). از مقدار می‌توان فهمید که قسمت data (payload) از کجا شروع می‌شود.
  - **Reserved**: این 6 بیت فعلاً رزرو هستند و استفاده‌ای ندارند. بنابراین در حال حاضر همواره 0 هستند.
  - **Flags**: 9 بیت کنترلی بسته هستند.
  - **Window**: اندازه‌ی بسته‌هایی که فرستنده‌ی این بسته آمادگی دریافت آن را دارد، بر حسب Window Size Unit.
  - **Checksum**: این Checksum 16 بیتی برای خطایابی در بخش‌های TCP Header & Payload و IP Pseudo Header استفاده می‌شود. منظور از IP Pseudo Header آدرس IP مبدا و مقصد و نوع پروتکل (TCP = 6) می‌باشد.
  - **Urgent Pointer**: در صورتی که بیت کنترلی URG مقدار 1 باشد، از این فیلد برای مشخص کردن آخرین بایت urgent داده، نسبت به sequence number استفاده می‌شود. (در واقع یک offset نسبت به sequence number به ما می‌دهد.
  - **Options**: بیت‌های اختیاری بسته، که طول آن‌ها از روی فیلد Data Offset به دست می‌آیند.
  - **Padding**: یک سری بیت اضافی برای رساندن بخش Header به مضرب 32.



TCP Header Format

۲. TLS: هدف از TLS، فراهم کردن ارتباط امن میان دو برنامه‌ی کاربردی دو دستگاه مختلف است. به عبارت دیگر، با TLS، **لایه‌ی انتقال** یک ارتباط امن و بدون شنود را برای **لایه‌ی بالاترش** (Application) تضمین می‌کند.
در واقع TLS داده‌های لایه‌ی Application را قبل از تحویل به لایه‌ی Transport، رمزنگاری می‌کند.
پس در مدل TCP/ IP، می‌توان آن را بین دو لایه‌ی Application و TCP قرار داد، هر چند که در حقیقت جزو هیچ کدام از این دو نیست.
در مدل OSI، می‌توان TLS را در لایه‌ی Session قرار داد، چرا که پس از ایجاد ارتباط میان پورت‌ها (Transport) و قبل از ایجاد ارتباط میان اپلیکیشن‌ها، یک ارتباط امن میان دو دستگاه تشکیل می‌دهد.
پروتکل‌های لایه‌ی Application زیادی از TLS برای ارتباط امن استفاده می‌کنند که از آن‌ها می‌توان به HTTPS، FTPS، SMTPS و SIPS اشاره کرد که صورت امن شده‌ی پروتکل‌های HTTP، FTP، SMTP و SIP هستند.

۳. IPSec: از IPSec برای امن کردن داده‌ها در لایه‌ی IP استفاده می‌شود؛ به عبارت دیگر هدف از IPSec فراهم کردن یک ارتباط امن و بدون شنود برای لایه‌های بالاتر (Transport, Application) می‌باشد.
دو دستگاه برای ارتباط از طریق IPSec باید دو مورد را مشخّص کنند، روش رمزنگاری داده، و روش Authentication. IPSec طبق روش انتخابی، یک کلید برای ارتباط امن می‌سازد. از این پس، برای فرستادن هر بسته، IPSec در مبدأ با کلید انتخابی، بسته را رمزنگاری کرده و ارسال می‌کند. IPSec در مقصد هم از آن کلید برای رمزگشایی داده استفاده می‌کند.
هر دستگاه هنگام استفاده از IPSec داده‌های ارسالی‌اش را امضاء هم می‌کند (Data Signing) تا طرف مقابل مطمئن باشد که بسته‌ی دریافتی‌اش از یک فرستنده‌ی معتبر است. (Authentication)
IPSec تنظیمات مختلفی دارد. برای مثال می‌توان تنظیم کرد که IPSec روی چه نوع بسته‌هایی اعمال شود، IPSec چگونه بسته‌ها را رمزنگاری کند، و یا فرستنده‌ها را چگونه Authenticate کند.

از مزایای IPSec می‌توان به موارد زیر اشاره کرد.

- در لایه‌ی Network عمل می‌کند و بنابراین می‌تواند بسته‌های لایه‌ی بالاتر را فارغ از هر نوع پروتکلی رمزنگاری کند.

از معایب آن هم می‌توان موارد زیر را نام برد.

- Wide Access Range: یک کامپیوتر خارجی، با دسترسی به تنها یکی از کامپیوترهای شبکه‌ی IPSec Based، می‌تواند تمامی کامپیوترهای آن شبکه را آلوده کند. (مگر این که مکانیزم‌های بیش‌تری لحاظ شوند.)
- CPU Overhead: این پروتکل نیاز به توان پردازشی بالایی دارد.
- Broken Algorithms: بسیاری از الگوریتم‌های رمزنگاری IPSec قابل شکسته شدن هستند.

منبع:
https://bobcares.com/blog/advantages-and-disadvantages-of-ipsec/

۴. فیلد Protocol در IPv4: این فیلد 8 بیتی پروتکل سطح بعدی را مشخص می‌کند. این پروتکل می‌تواند مختص لایه‌ی انتقال باشد ((6, TCP) یا (21, UDP)). یا خارج از لایه‌ی انتقال باشد ((1, ICMP).)
از این فیلد استفاده می‌شود تا بنا به پروتکل، ساختار Header لایه‌ی بعد به درستی تجزیه شده، و اطلاعات درست استخراج شوند.
لیست برخی از شماره‌های این فیلد، و نام پروتکل‌شان را در ادامه مشاهده می‌کنید.

Assigned Internet Protocol Numbers

Decimal	Octal	Protocol Numbers	References
0	0	Reserved	[JBP]
1	1	ICMP	[53,JBP]
2	2	Unassigned	[JBP]
3	3	Gateway-to-Gateway	[48,49,VMS]
4	4	CMCC Gateway Monitoring Message	[18,19,DFP]
5	5	ST	[20,JWF]
6	6	TCP	[34,JBP]
7	7	UCL	[PK]
8	10	Unassigned	[JBP]
9	11	Secure	[VGC]
10	12	BBN RCC Monitoring	[VMS]
11	13	NVP	[12,DC]
12	14	PUP	[4,EAT3]
13	15	Pluribus	[RDB2]
14	16	Telenet	[RDB2]
15	17	XNET	[25,JFH2]
16	20	Chaos	[MOON]
17	21	User Datagram	[42,JBP]
18	22	Multiplexing	[13,JBP]
19	23	DCN	[DLM1]
20	24	TAC Monitoring	[55,RH6]
21-62	25-76	Unassigned	[JBP]
63	77	any local network	[JBP]
64	100	SATNET and Backroom EXPAK	[DM11]
65	101	MIT Subnet Support	[NC3]
66-68	102-104	Unassigned	[JBP]
69	105	SATNET Monitoring	[DM11]
70	106	Unassigned	[JBP]
71	107	Internet Packet Core Utility	[DM11]
72-75	110-113	Unassigned	[JBP]
76	114	Backroom SATNET Monitoring	[DM11]
77	115	Unassigned	[JBP]
78	116	WIDEBAND Monitoring	[DM11]
79	117	WIDEBAND EXPAK	[DM11]
80-254	120-376	Unassigned	[JBP]
255	377	Reserved	[JBP]