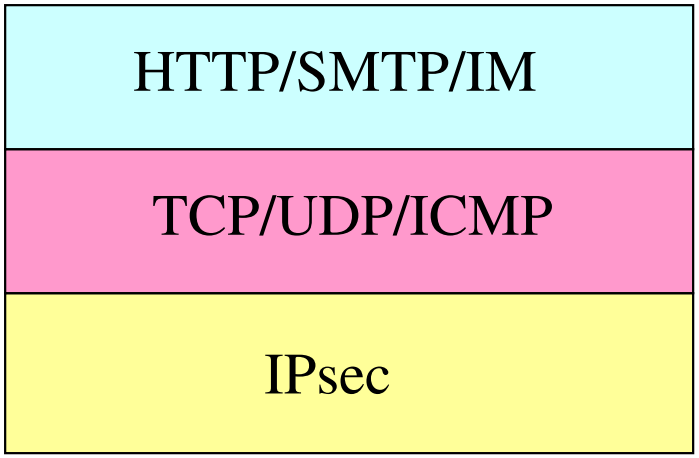
امنیت IP (IPsec)

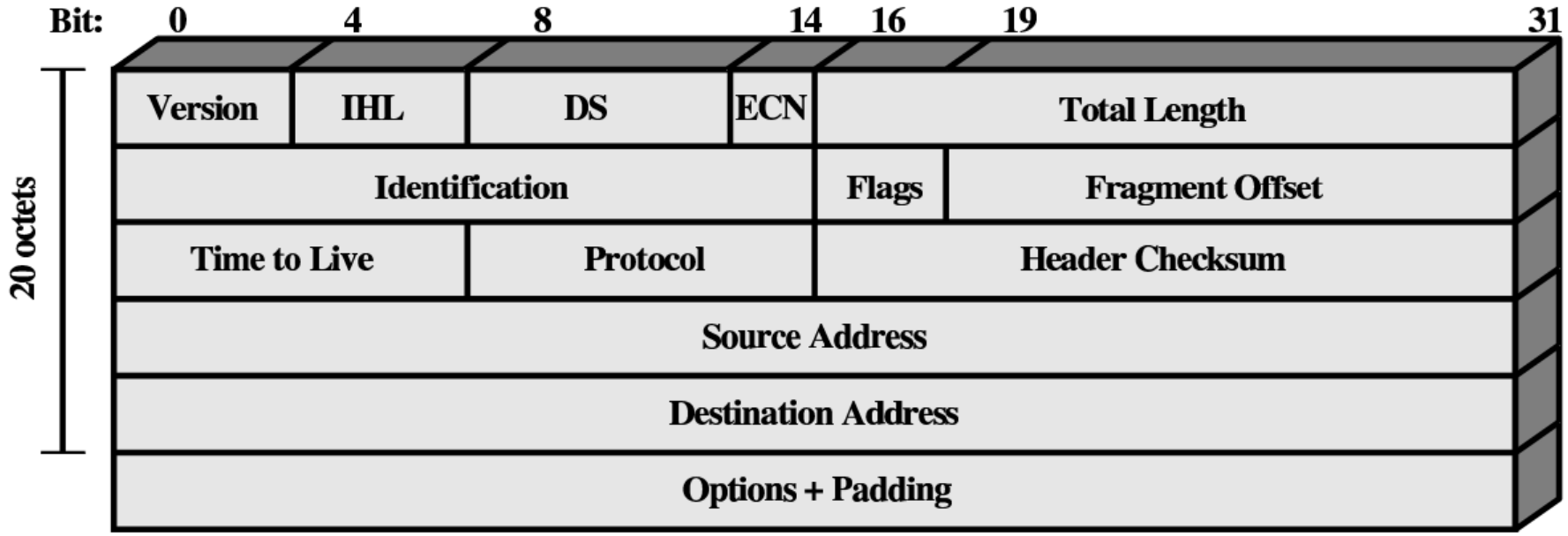
امنیت در لایه های مختلف

- لایه کاربرد: PGP
- لایه انتقال: SSL
- لایه شبکه: IPsec
- لایه لینک: WEP و 802.11i

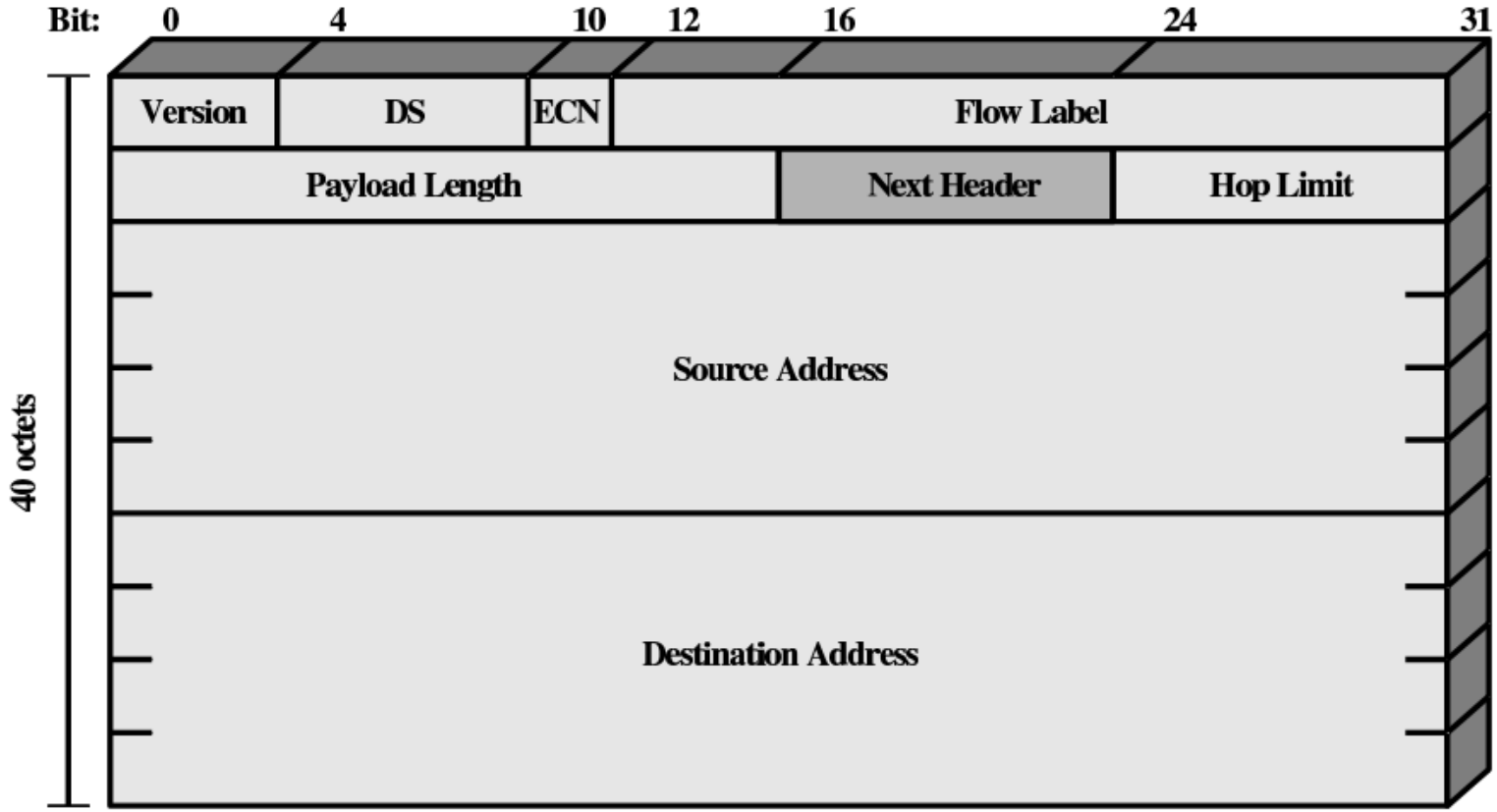


- پروتکل IPsec می تواند امنیت را بین دو موجودیت در شبکه برقرار کند. (دو هاست، دو روتر، هاست و روتر)

IPv4 Header


Bit:
0
4
8
14
16
19
31
20 octets
Version
IHL
DS
ECN
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + Padding

IPv6 Header



DS = Differentiated services field
ECN = Explicit congestion notification field

Note: The 8-bit DS/ECN fields were formerly known as the Type of Service field in the IPv4 header and the Traffic Class field in the IPv6 header.

امنیت IP

- بسته های IP اساساً مکانیزم امنیتی ندارند.
  - IP مبدأ قابل جعل کردن است.
  - محتویات بسته های IP قابل استراق سمع هستند.
  - محتویات بسته های IP قابل تغییر هستند.
  - بسته های IP قابل باز ارسال (Replay) هستند.
- IPsec روشی برای محافظت از بسته های IP است.
  - توسط IETF استاندارد شده است.
  - فقط فرستنده و گیرنده باید از IPsec پشتیبانی کنند.
    - همه روترهای میانی نیازی به پشتیبانی از IPsec ندارند.

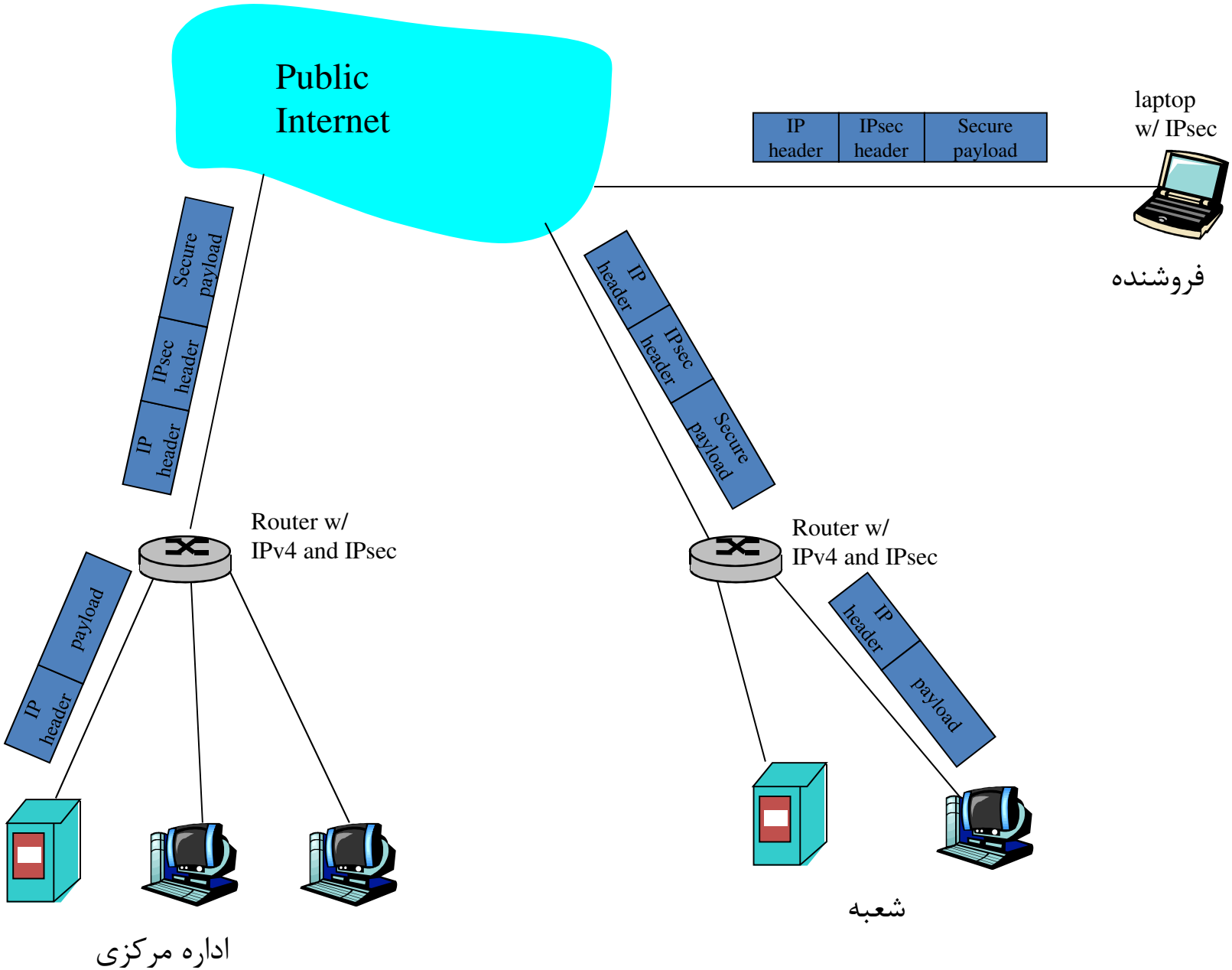
مفهوم محرمانگی در لایه شبکه

بین دو موجودیت شبکه

- فرستنده محتویات تمام بسته های ارسالی را رمز می کند.
  محتویات بسته شامل:
  - سگمنت TCP، سگمنت UDP، پیام ICMP، پیام OSPF
- تمام اطلاعات رد و بدل شده بین دو موجودیت مخفی است:
  - صفحات وب، ایمیل، انتقال فایل از طریق P2P پروتکل، بسته های TCP SYN و غیره

شبکه های خصوصی مجازی
Virtual Private Networks (VPN)

- سازمان ها برای ایجاد امنیت از VPN استفاده می کنند.
  - پر هزینه است. به روتر، لینک و زیر ساخت DNS مجزایی نیاز است.
- ترافیک بین دفاتر سازمان از طریق اینترنت فرستاده می شود.
  - اما این ترافیک قبل از ارسال رمز می شود.


Public
Internet
IP header
IPsec header
Secure payload
laptop
w/ IPsec
فروشنده
Secure payload
IPsec header
IP header
IP header
IPsec header
Secure payload
Router w/
IPv4 and IPsec
Router w/
IPv4 and IPsec
payload
IP header
IP header
payload
اداره مرکزی
شعبه

سرویس های IPsec

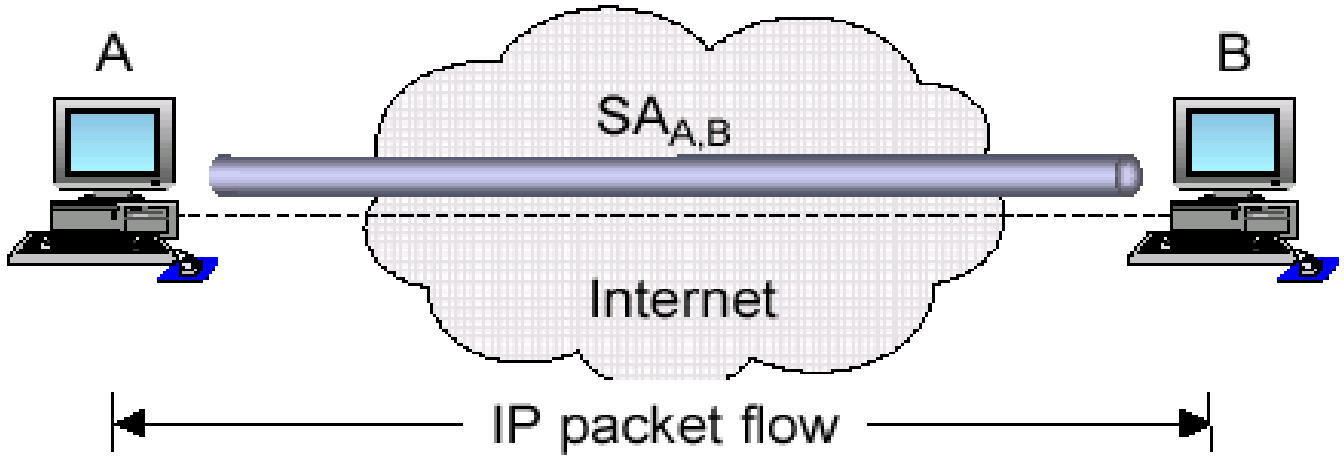
- جامعیت داده
- تأیید هویت مبدأ
- جلوگیری از حمله باز ارسال
- محرمانگی

معماری IPSec

- IPSec از اجزا زیر تشکیل شده است:
  - مد های مختلف استفاده از IPSec
    - مد تونل و مد انتقال
  - دو پروتکل اصلی استفاده شده در IPSec
    - Authentication header protocol (AH)
    - Encapsulated security protocol (ESP)
  - Security Associations (SA)
  - روش تبادل کلید (Internet Key Exchange)
  - الگوریتم های رمزنگاری

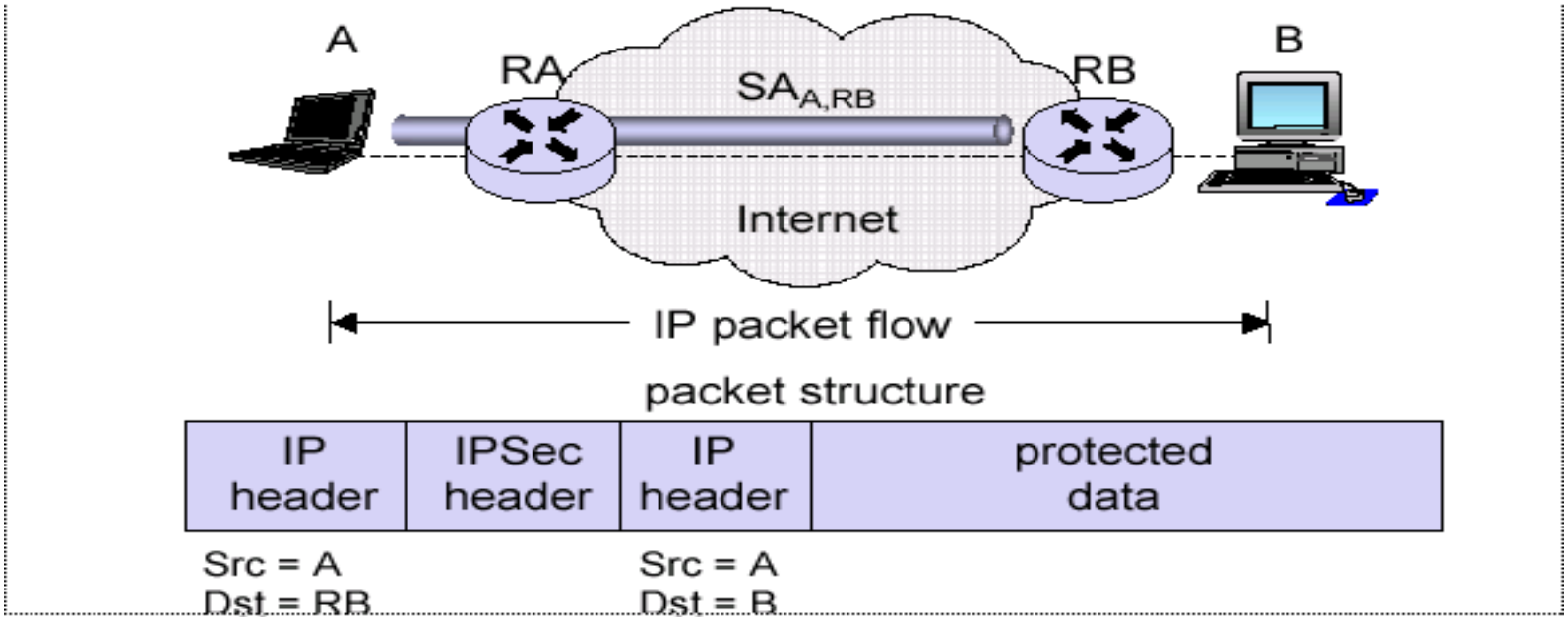
مد انتقال (Transport)

- بسته های IPsec توسط peer اصلی مستقیما ارسال و دریافت می شوند.



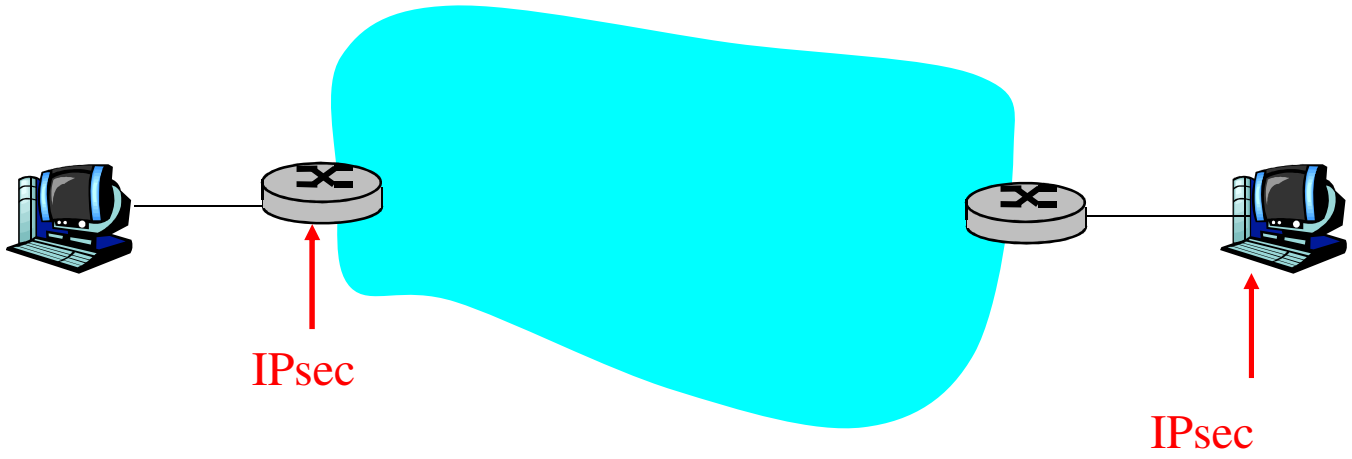
مدل تونل ۱ (Tunneling)

- بسته های IPsec توسط روترهای دو شبکه مورد نظر ارسال و دریافت می شوند و هاست های شبکه نیازی به پشتیبانی از IPsec ندارند.



مدل تونل ۲ (Tunneling)

- یک طرف یک کامپیوتر اصلی و دیگری یک مسیر یاب است

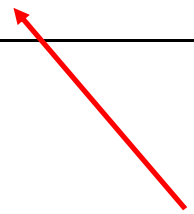


پروتکل های IPsec

- Authentication Header (AH)
  - تأیید هویت مبدأ و جامعیت داده را فراهم می کند.
  - محرمانگی را فراهم نمی کند.
- Encapsulation Security Protocol (ESP)
  - تأیید هویت مبدأ، جامعیت و محرمانگی را فراهم می کند.
  - بیشتر از AH استفاده می شود.

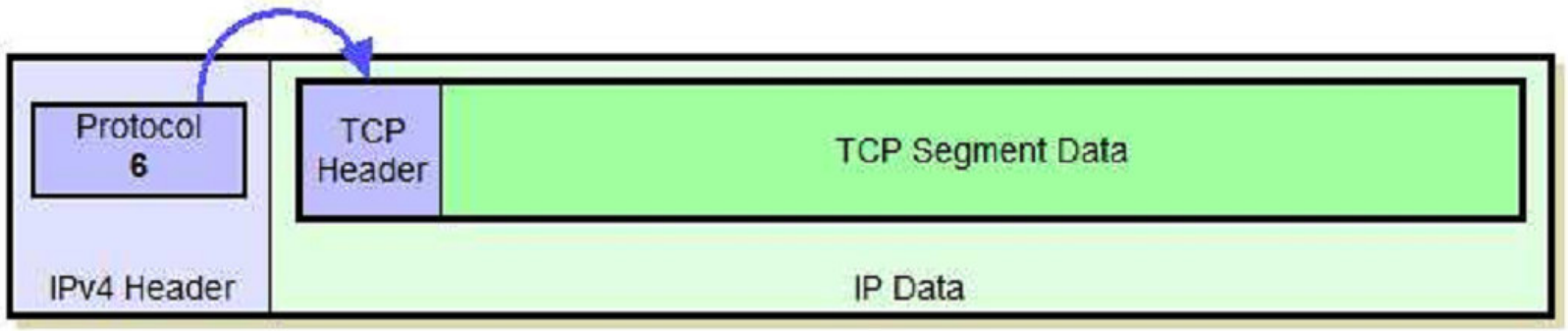
ترکیب مد و پروتکل IPsec

مد انتقال با پروتکل AH	مد انتقال با پروتکل ESP
مد تونل با پروتکل AH	مد تونل با پروتکل ESP

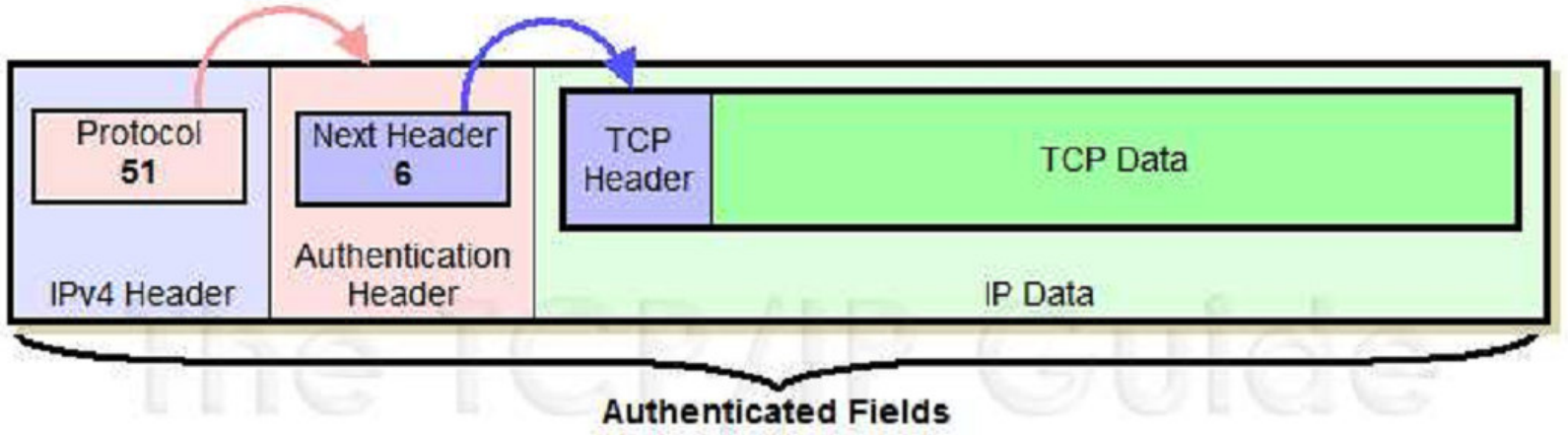


مهمترین و معمول ترین حالت

مد انتقال با پروتکل AH (IPv4)

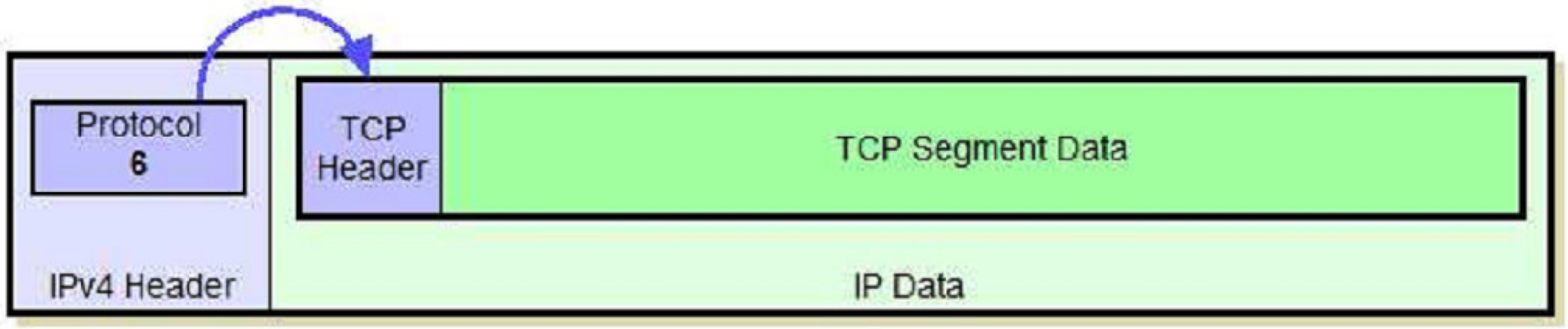


Original IPv4 Datagram Format

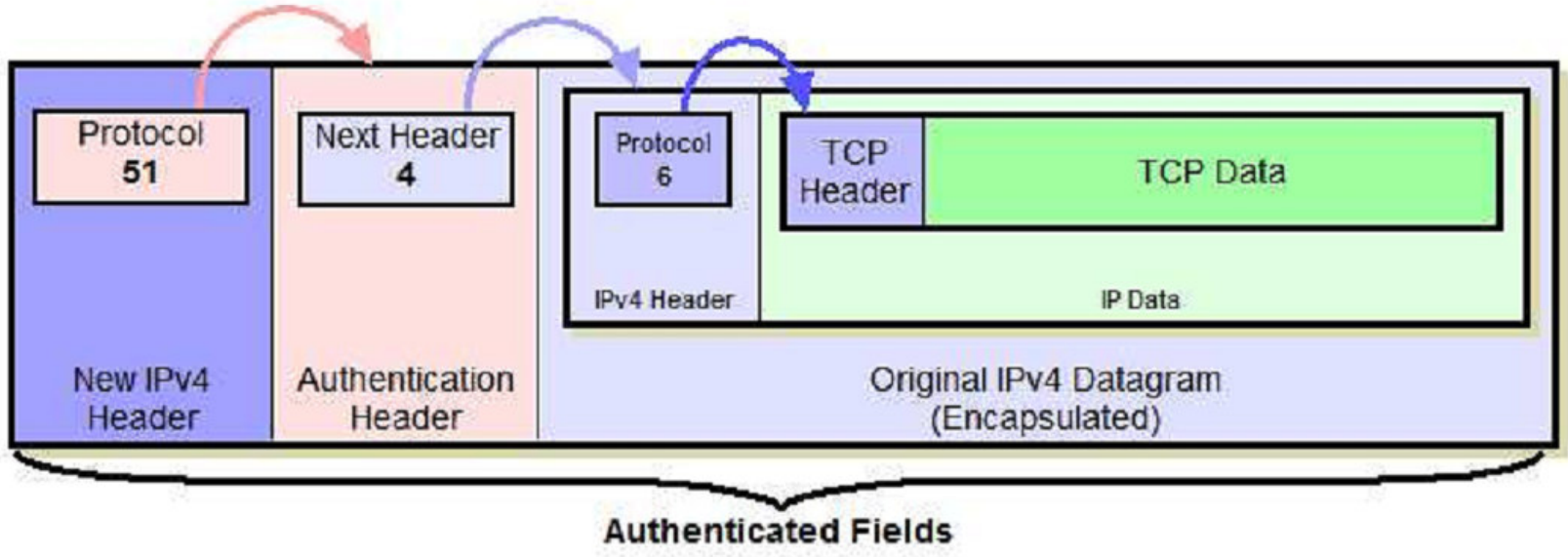


IPv4 AH Datagram Format - IPSec Transport Mode

مد تونل با پروتکل AH (IPv4)

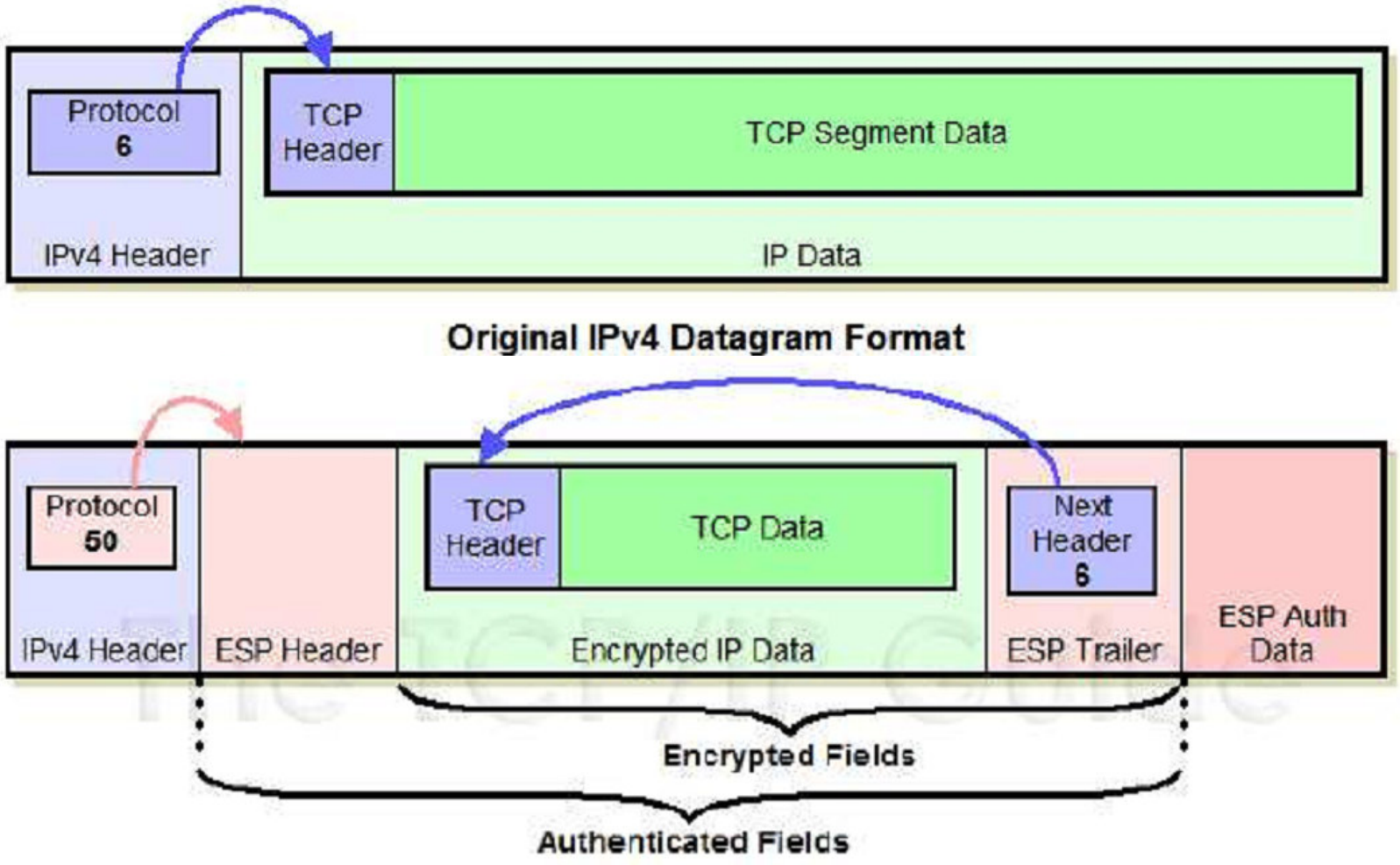


Original IPv4 Datagram Format

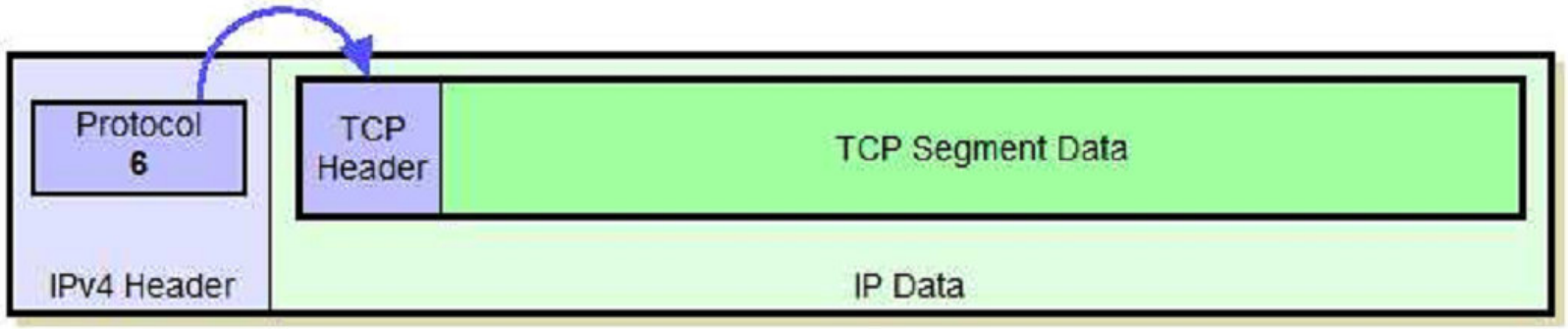


IPv4 AH Datagram Format - IPSec Tunnel Mode

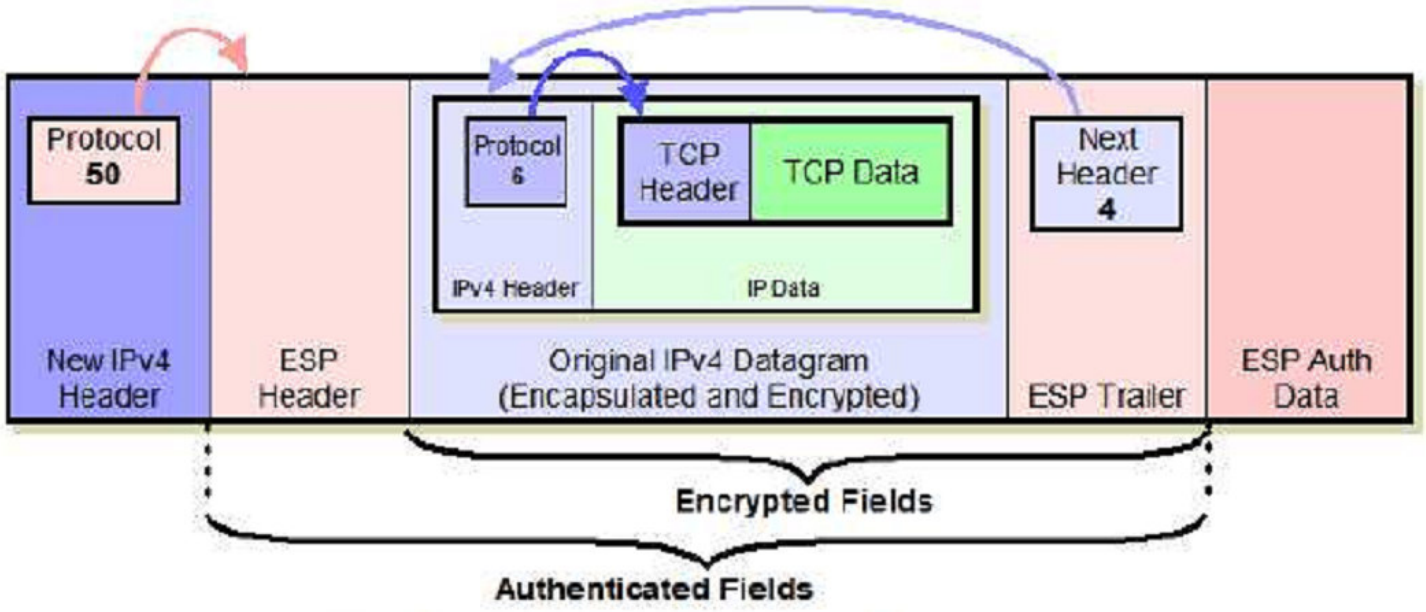
مد انتقال با پروتکل ESP (IPv4)



مد تونل با پروتکل ESP (IPv4)

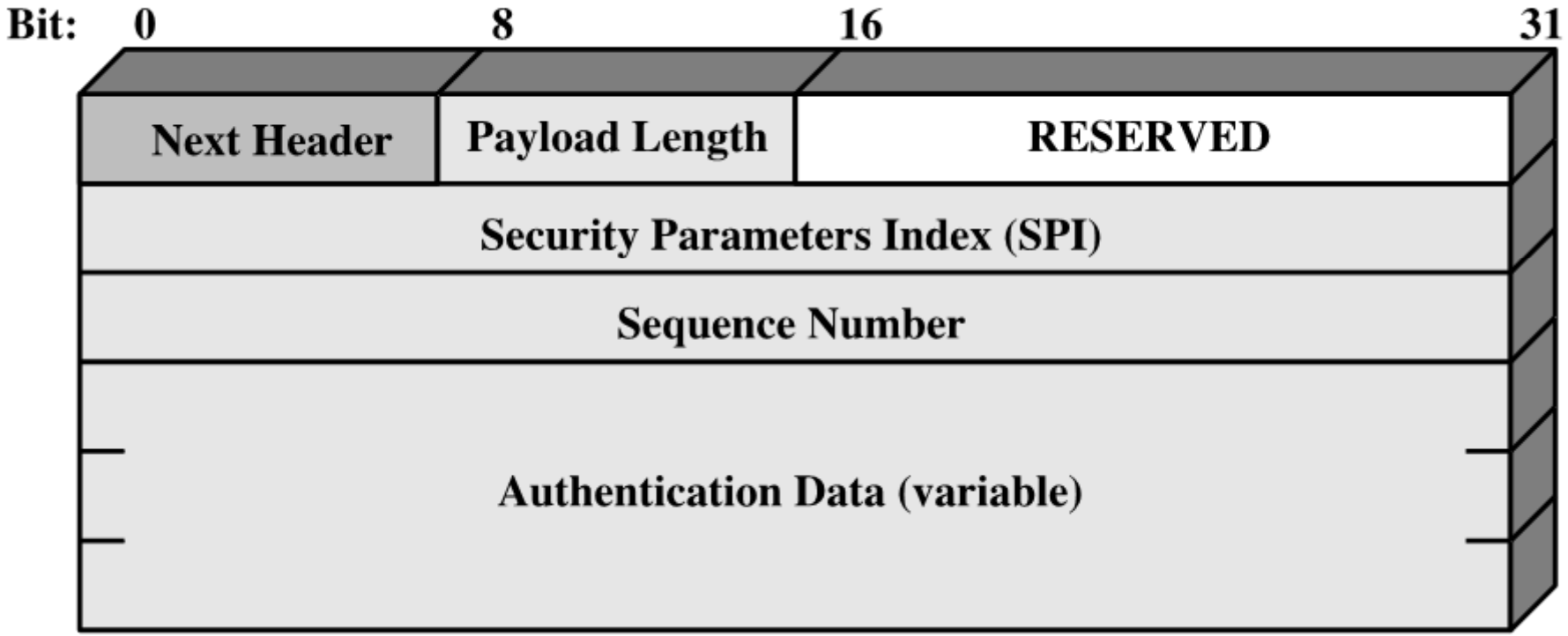


Original IPv4 Datagram Format

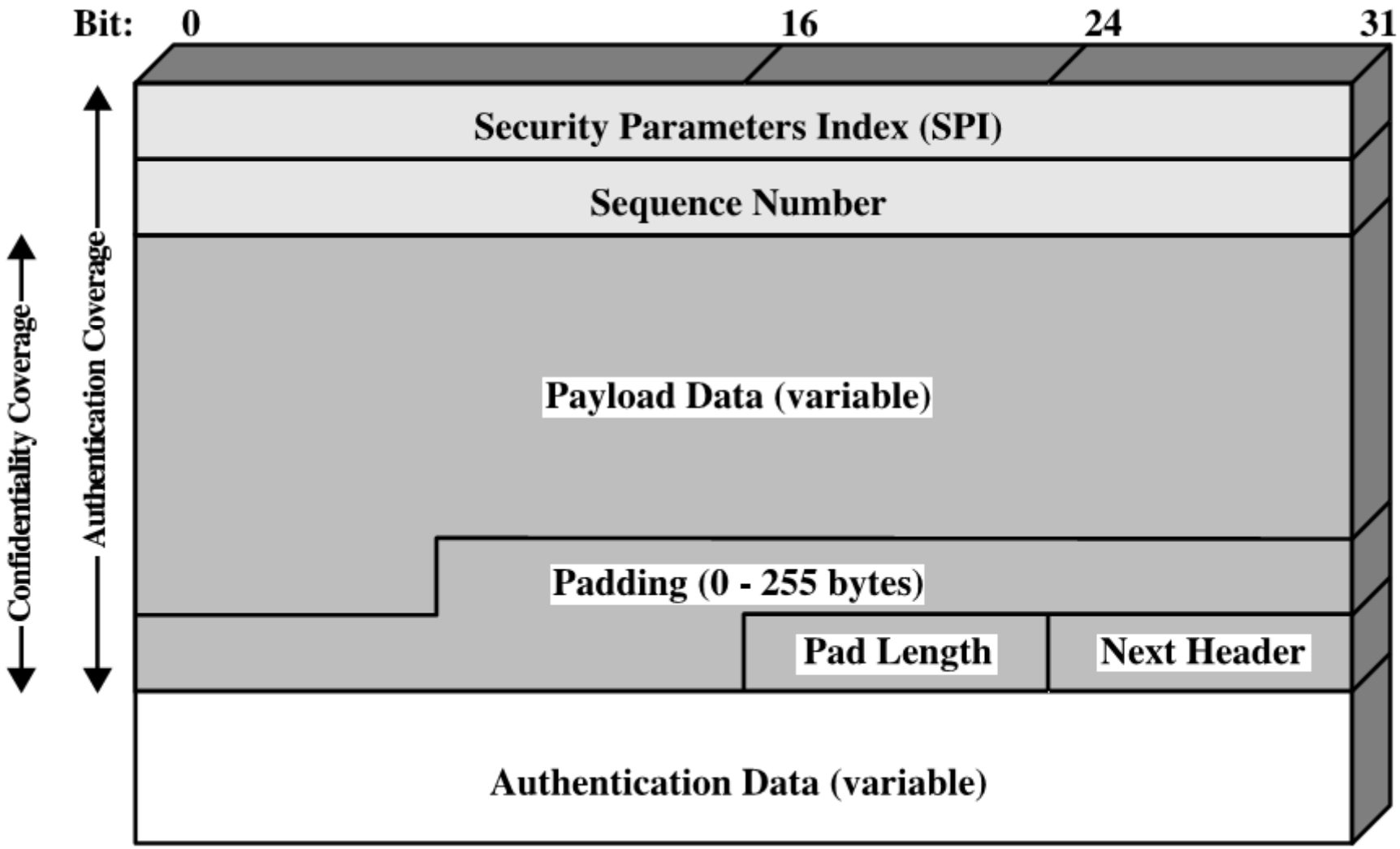


IPv4 ESP Datagram Format - IPSec Tunnel Mode

پروتکل AH


Bit:
0
8
16
31
Next Header
Payload Length
RESERVED
Security Parameters Index (SPI)
Sequence Number
Authentication Data (variable)

پروتکل ESP


Bit:
0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Authentication Coverage
Confidentiality Coverage

Security Association (SA)

- SA: Security Association
  یک چند تائی منشکل از اطلاعات:

  - پروتکل IPSec
  - سیاست امنیتی(Security policy)
  - الگوریتم رمز نگاری

- پایگاه داده سیاست امنیتی(SPD) : نوع امنیت اعمال شده به بسته را معلوم می کند
- پایگاه داده Security Association (SAD) : انـواع SA فعـال بـرای پـردازش خروجـی و ورودی را در خود ذخیره می کند.
- اندیس پارامتر امنیت(SPI: Security Parameter Index.)
  یک عدد ۳۲ بیتی که نوع SA را در طرف گیرنده مشخص می کند و در داخل بسته ارسالی ذخیره می شود.

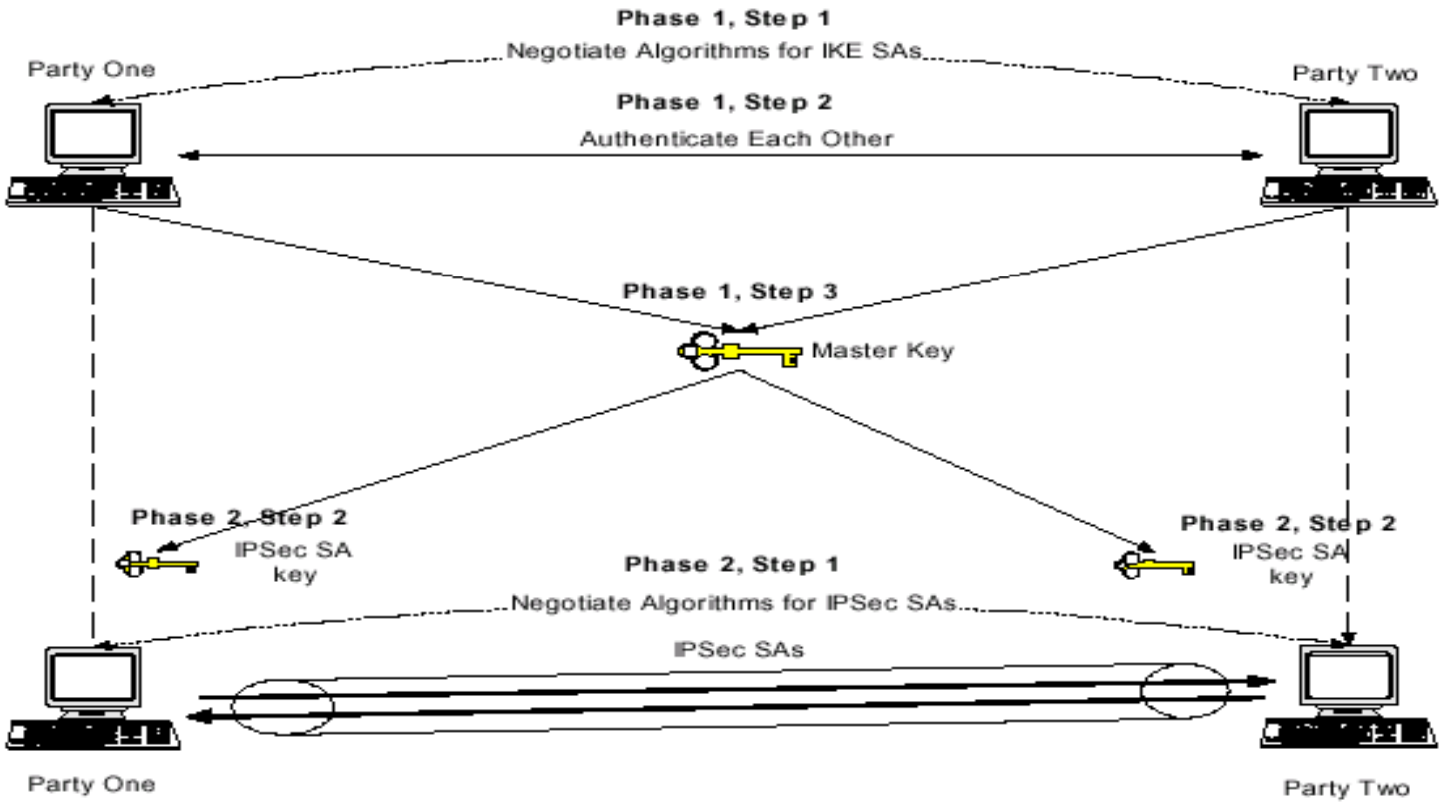
- IKE: Internet Key Exchange
  روش ردبدل کردن کلید. به هنگام برقراری ارتباط امن و قبل از بر قراری SA فعال می شود.

برقراری SA

- قبل از ارسال بسته ها با استفاده از IPSec لازم است بین دو نقطه ارتباط امن یک SA برقرار شود
- IPSec یک روش استاندارد برای برقراری SA تعریف می کند:
  - پروتکل مدیریت SA و کلید(*ISAKMP*)
    - فرمت و پروتکل مذاکره برای برقرای SA را مشخص می کند
  - ردبدل کردن کلید در اینترنت(IKE)
    - روش استاندارد هویت سنجی و انتقال کلید بین دو طرف را معلوم می کند

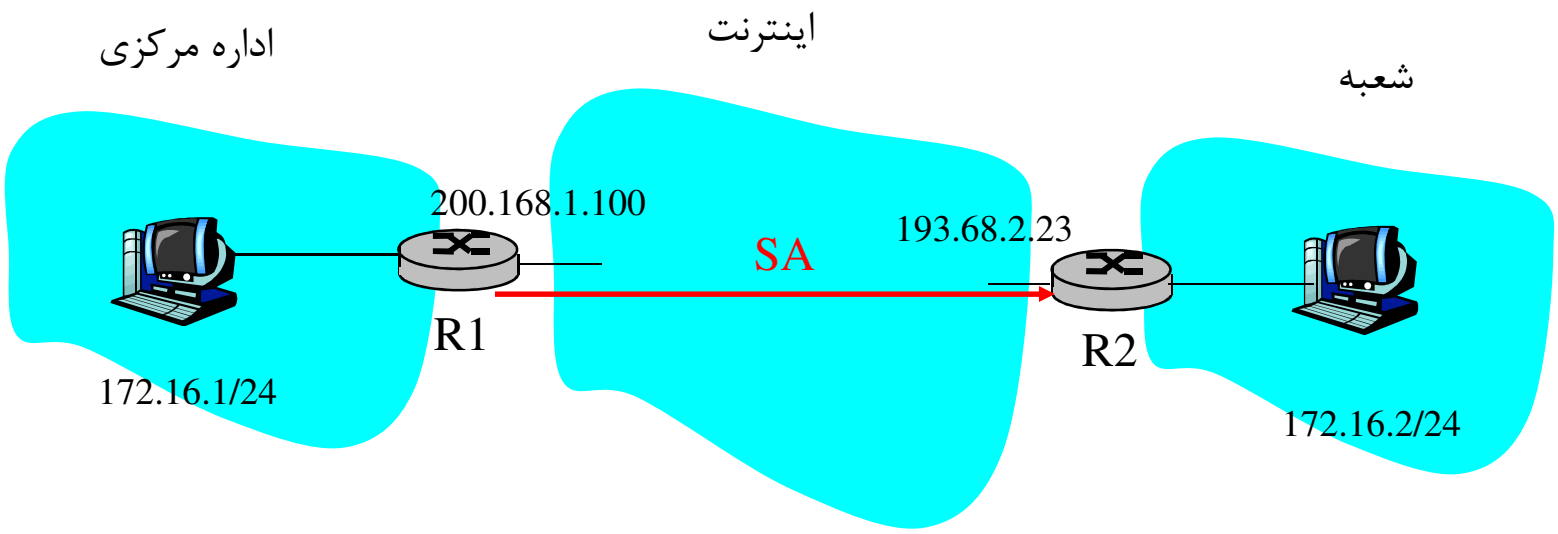
- SA ها بر اساس نوع پروتکل های بین دو طرف مشخص می شود
- SA یک طرفه است.

مدیریت کلید


Phase 1, Step 1
Negotiate Algorithms for IKE SAs
Party One
Party Two
Phase 1, Step 2
Authenticate Each Other
Phase 1, Step 3
Master Key
Phase 2, Step 2
IPSec SA key
Phase 2, Step 2
IPSec SA key
Phase 2, Step 1
Negotiate Algorithms for IPSec SAs
IPSec SAs
Party One
Party Two

مثال: SA از روتر R1 به روتر R2

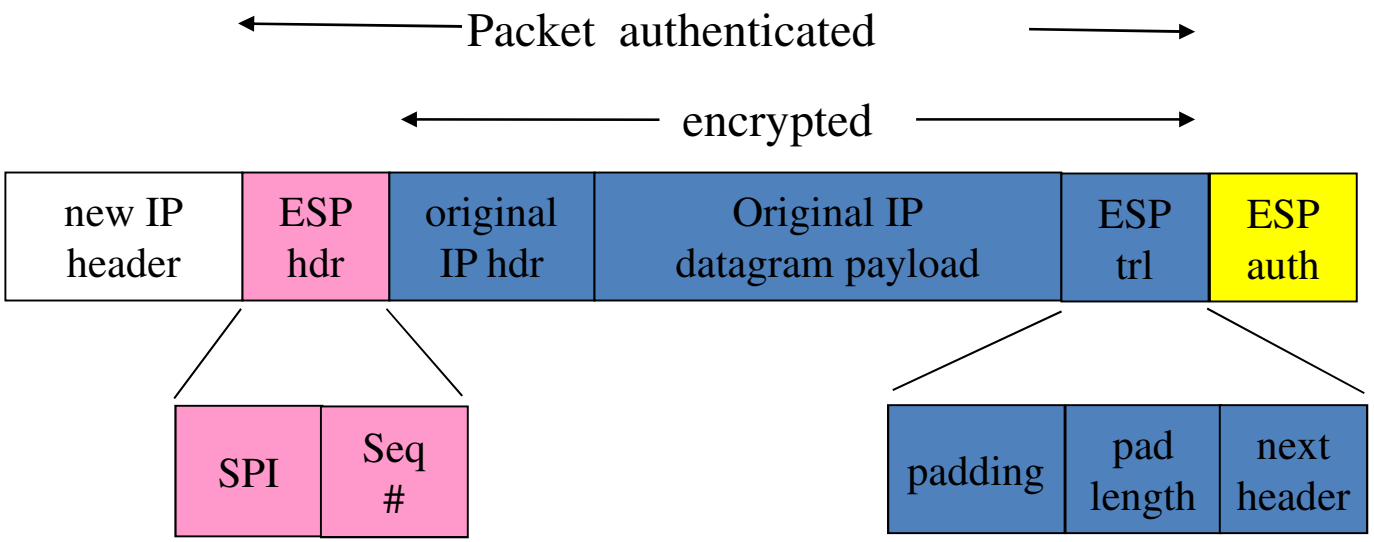
- شناسه ۳۲ بیتی برای SA
  Security Parameter Index (SPI) –
- مبدأ = 200.168.1.100، مقصد = 193.68.2.33
- الگوریتم های رمزنگاری (3DES با CBC) و کلید رمزنگاری
- الگوریتم تأیید هویت (HMAC) و کلید تأیید هویت



Security Association Database (SAD)

- هـر نقطـه انتهـای ارتبـاط، اطلاعـات SAهـایش را در SAD نگهداری می کند.
- با n ارتباط دو طرفه، 2nتا SA در SAD روتر R1 قرار دارد.
- موقـع ارسـال بسـته IPsec، روتـر R1 از SAD بـرای نحـوه پردازش بسته استفاده می کند.
- هنگامی که بسته IPsec به روتـر R2 رسـید، R2 فیلـد SPI بسته IPsec را استخراج می کند و با استفاده از SAD، بسته را پردازش می کند.

مد تونل با ESP



نحوه ساخت بسته IPsec

- روتر R1 به انتهای بسته اولیه، ESP trailer اضافه می کند.
- سپس داده بدست آمده را با الگوریتم و کلید SA رمز می کند.
- سپس به ابتدای داده رمز شده ESP header را اضافه می کند
- روی بسته بدست آمده با استفاده از الگوریتم و کلید SA، MAC را محاسبه کرده و به انتهای بسته اضافه می شود.
- برای محتوای بدست آمده، IP Header ساخته می شود و به ابتدای محتوا می چسباند.

محتوی بسته

- ESP trailer
  - Padding برای رمزنگاری مبتنی بر بلاک
  - طول padding
- ESP header
  - SPI
  - شمارنده توالی: برای جلوگیری از حمله باز ارسال
- ESP auth با استفاده از کلید مشترک ساخته می شود.

شمارنده توالی

- برای SA جدید، فرستنده شمارنده توالی را صفر می گذارد.
- به ازای هر بسته جدید، شمارنده یک واحد افزایش می یابد.
- هدف
  - جلوگیری از حملات باز ارسال
- تکنیک
  - گیرنده با استفاده از پنجره، بسته های تکراری و نیامـده را تشـخیص می دهد.

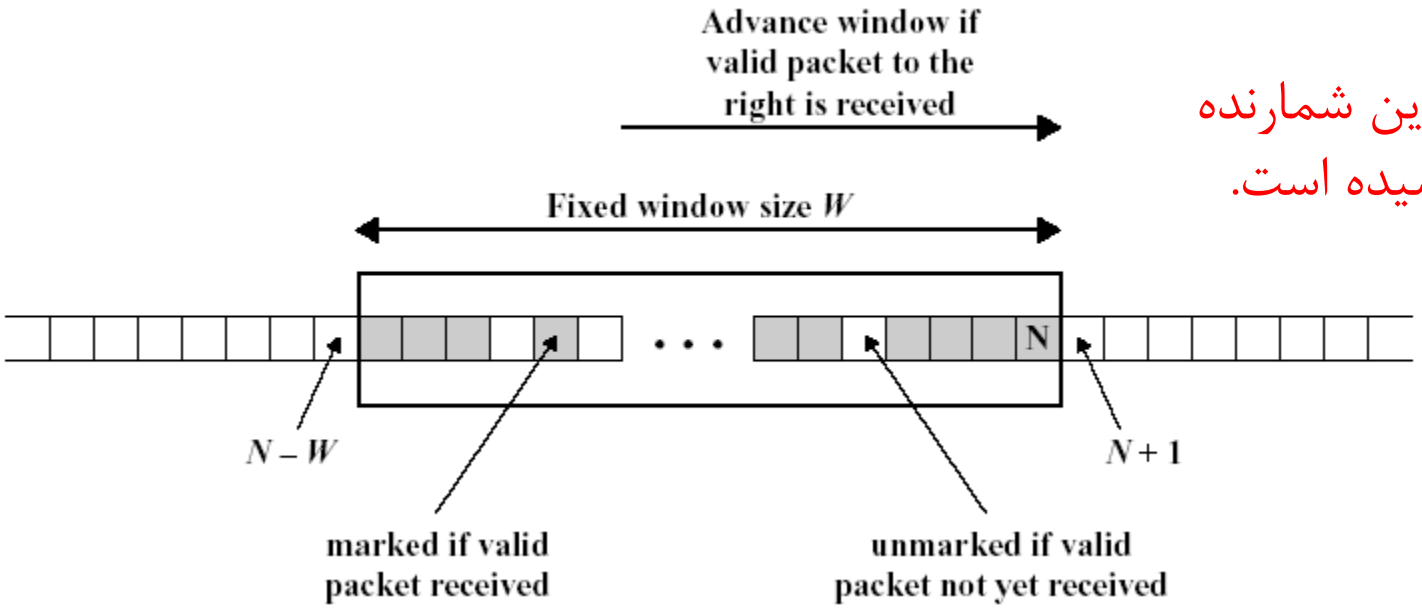
پردازش بسته ها در گیرنده

۱. اگر بسته رسیده در پنجره قرار گیرد و بسته جدید بوده و MAC درست باشد: خانه مورد نظر علامت می خورد.

۲. اگر بسته رسیده در سمت راست پنجره قرار گیرد و MAC درست باشد: پنجره جلو می رود و خانه علامت می خورد.

۳. اگر بسته رسیده در سمت چپ پنجره قرار گیرد یا قبلاً خانه آن علامت خورده باشد یا MAC درست نباشد: بسته دور انداخته می شود.

N بزرگترین شمارنده متوالی رسیده است.

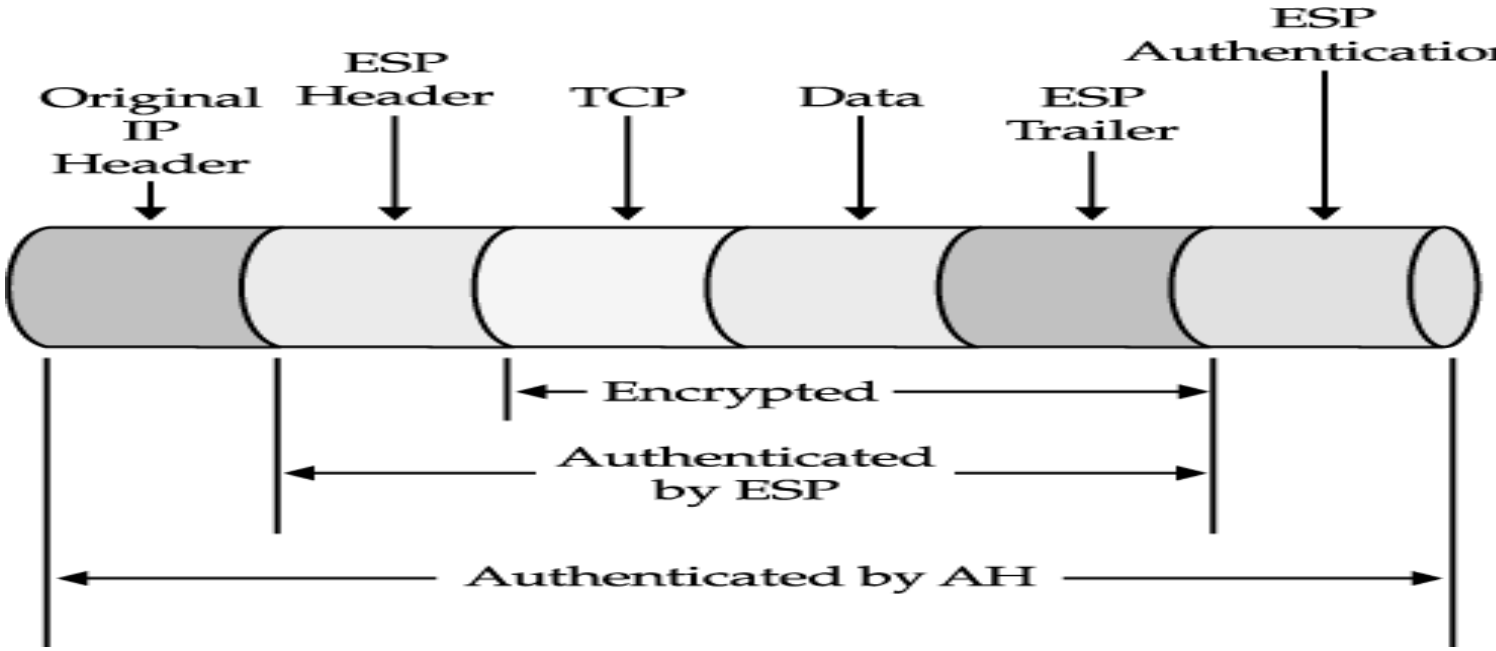


Security Policy Database (SPD)

- خط مشی (Policy)
  - فرستنده برای ارسال یک بسته، باید بداند که آیا باید از IPsec استفاده کند یا خیر؟
  - فرستنده باید بداند از کدام SA استفاده کند؟
    - ممکن است از IP مبدأ و مقصد یا شماره پروتکل استفاده کند.
- SPD تعیین می کند با بسته ها **چه** کاری باید کرد.
- SAD تعیین می کند **چگونه** باید آن کار را انجام داد.

AH and ESP

- پروتکل ESP اول اعمال می شود
- بعد از اعمال ESP کل header با پروتکل AH هویت سنجی می شود.



- Advantage: the ESP header can also be protected by AH

الگوریتم های رمزنگاری مورد استفاده

- DES
- 3DES
- AES
- RC5
- IDEA
- 3-IDEA
- CAST
- BlowFish

مقایسه SSL و IPsec

- SSL در لایه کاربرد است ولی IPsec در لایه شبکه
  - IPsec تمام کاربردها را امن می کند.
- SSL در مقابل حمله DoS آسیب پذیر است.
  - مهاجم یک بسته جعلی TCP با checksum و شمارنده توالی درست به سرور یا کلاینت ارسال می کند.
  - TCP بسته را تصدیق کرده و به SSL می فرستد.
  - SSL بسته را دور می اندازد. (MAC درست نیست)
  - بسته واقعی می رسد و TCP آن را دور می اندازد (شمارنده توالی آن قدیمی است).
  - SSL هیچوقت بسته واقعی را دریافت نمی کند.
- چه اتفاقی می افتد اگر مهاجم بسته جعلی IPsec بفرستد؟
  - گیرنده بسته جعلی را دور می اندازد (MAC درست نیست) و خانه را علامت نمی زند.
  - بسته واقعی به گیرنده می رسد و MAC آن تصدیق شده و به لایه بالاتر فرستاده می شود.

تعیین کلیدهای IPsec

- تعیین کلیدهای IPsec به صورت دستی امکان پذیر نیست.
- Internet Key Exchange (IKE)
  - Pre-shared Secret Key (PSK)
    - طرفین ارتباط یک کلید مشترک محرمانه دارند.
  - Public Key Infra-structure (PKI)
    - طرفین ارتباط، دارای کلیدهای خصوصی/ عمومی و گواهی هستند.
    - شبیه SSL Handshake

جمع بندی

- طرفین IPsec می توانند دو هاست، دو روتر یا یک هاست و یک روتر باشند.
- IPsec دارای دو پروتکل AH و ESP است.
- پروتکل AH جامعیت و تأیید هویت مبدأ را فراهم می کند.
- پروتکل ESP جامعیت، تأیید هویت مبدأ و محرمانگی را فراهم می کند.
- IKE برای مبادله الگوریتم ها، کلیدها و هماهنگی SA استفاده می شود.