یا ذالامن والامان

امنیت IP
(IPSec)

از کتاب

Network Security Essentials

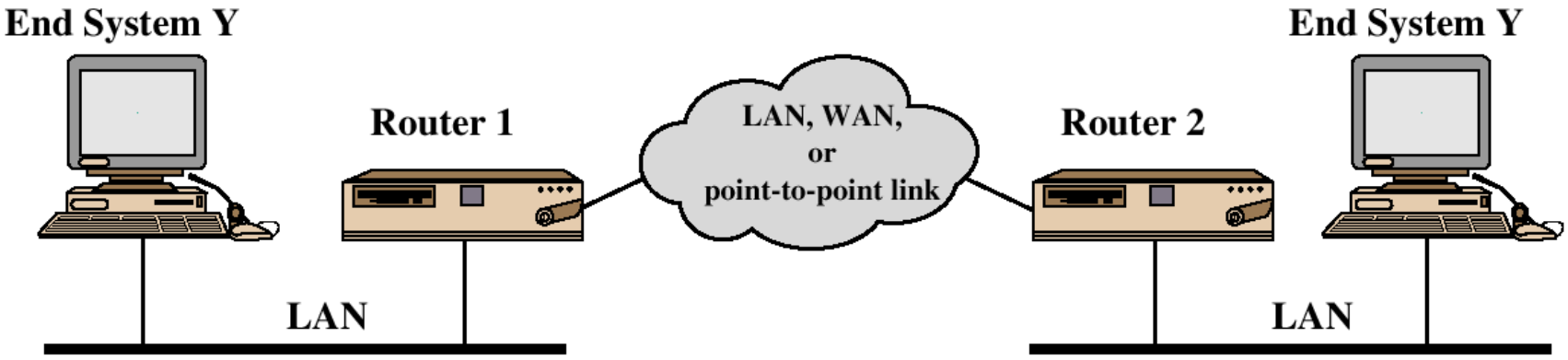
حمید رضا شهریاری

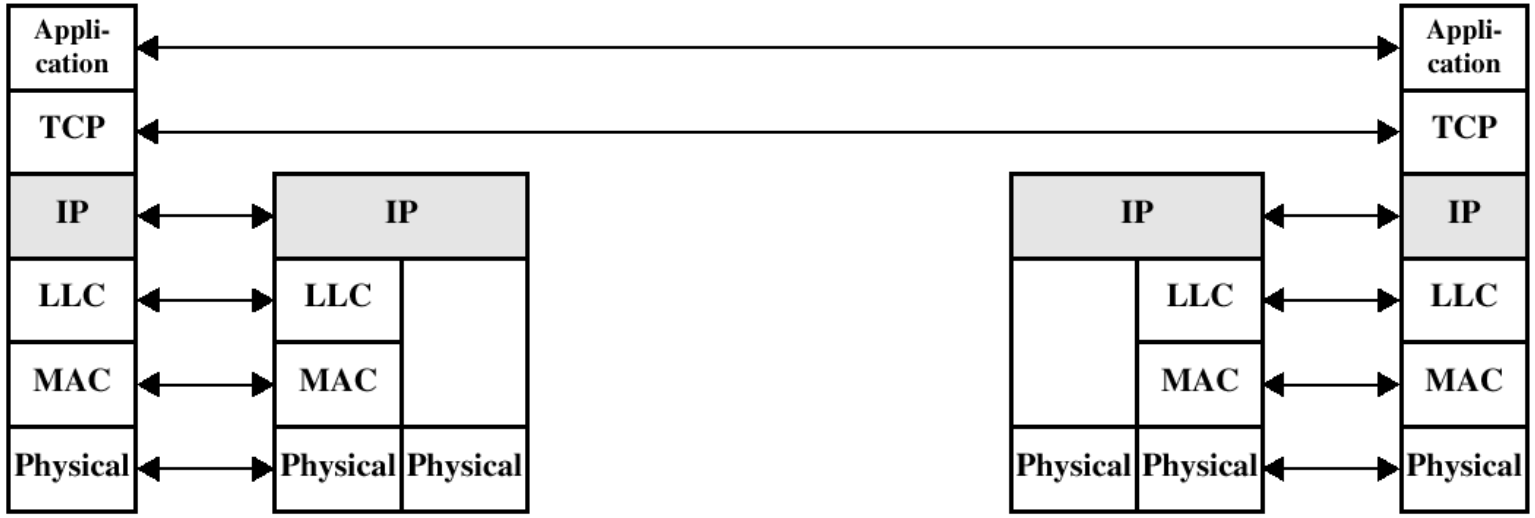
http://atlas.aut.ac.ir

فهرست مطالب

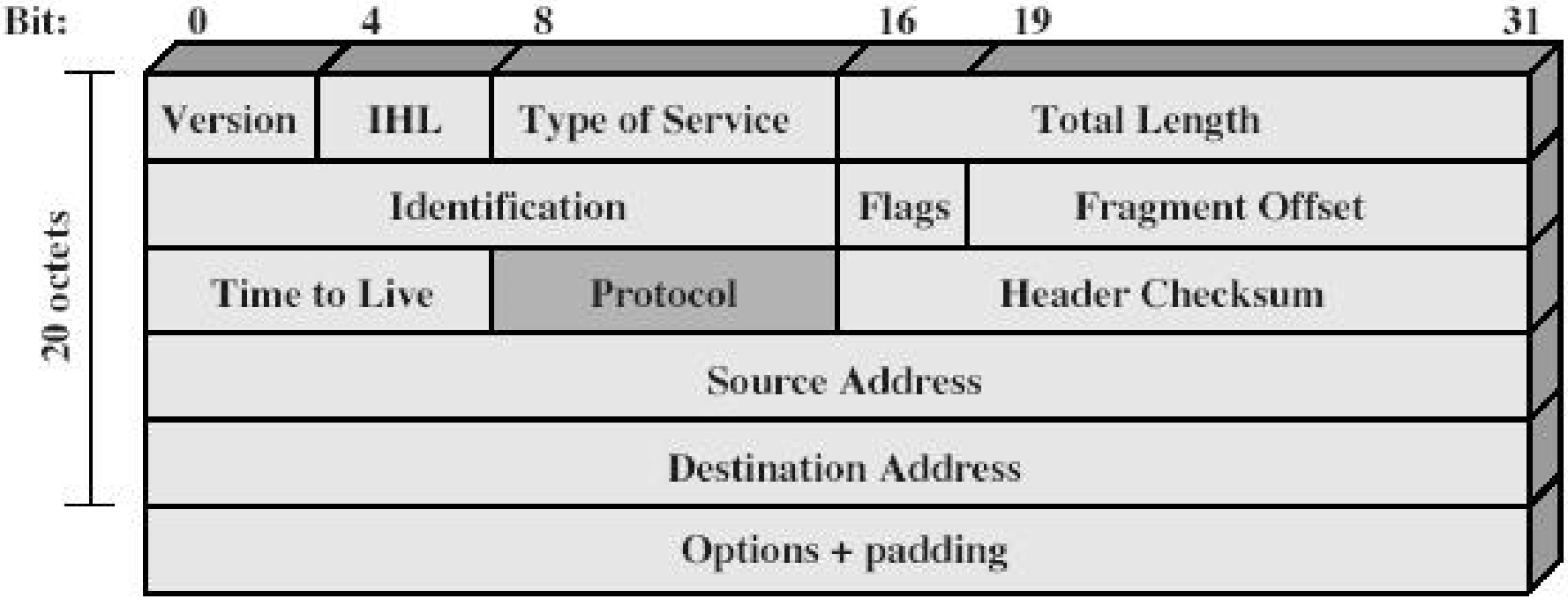
- مقدمه
- معماری IPSec
  - سرویس های IPSec
  - مجمع امنیتی(SA)
  - حالت‌های انتقال بسته‌ها
- AH
- ESP
- ترکیب SAها
- مدیریت کلید

مقدمه – مثالی از TCP/IP





IPV4


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding
20 octets

مقدمه

- راه حل های امنیتی وابسته به کاربرد(تاکنون)
  - S/MIME و PGP : امنیت پست الکترونیکی
  - Kerberos : امنیت بین کاربر-کارگزار(احراز هویت)
  - SSL : ایجاد یک کانال امن در وب
- نیاز به امنیت در سطح IP
  - محرمانگی محتوای بسته های IP
  - احراز هویت فرستنده و گیرنده بسته ها

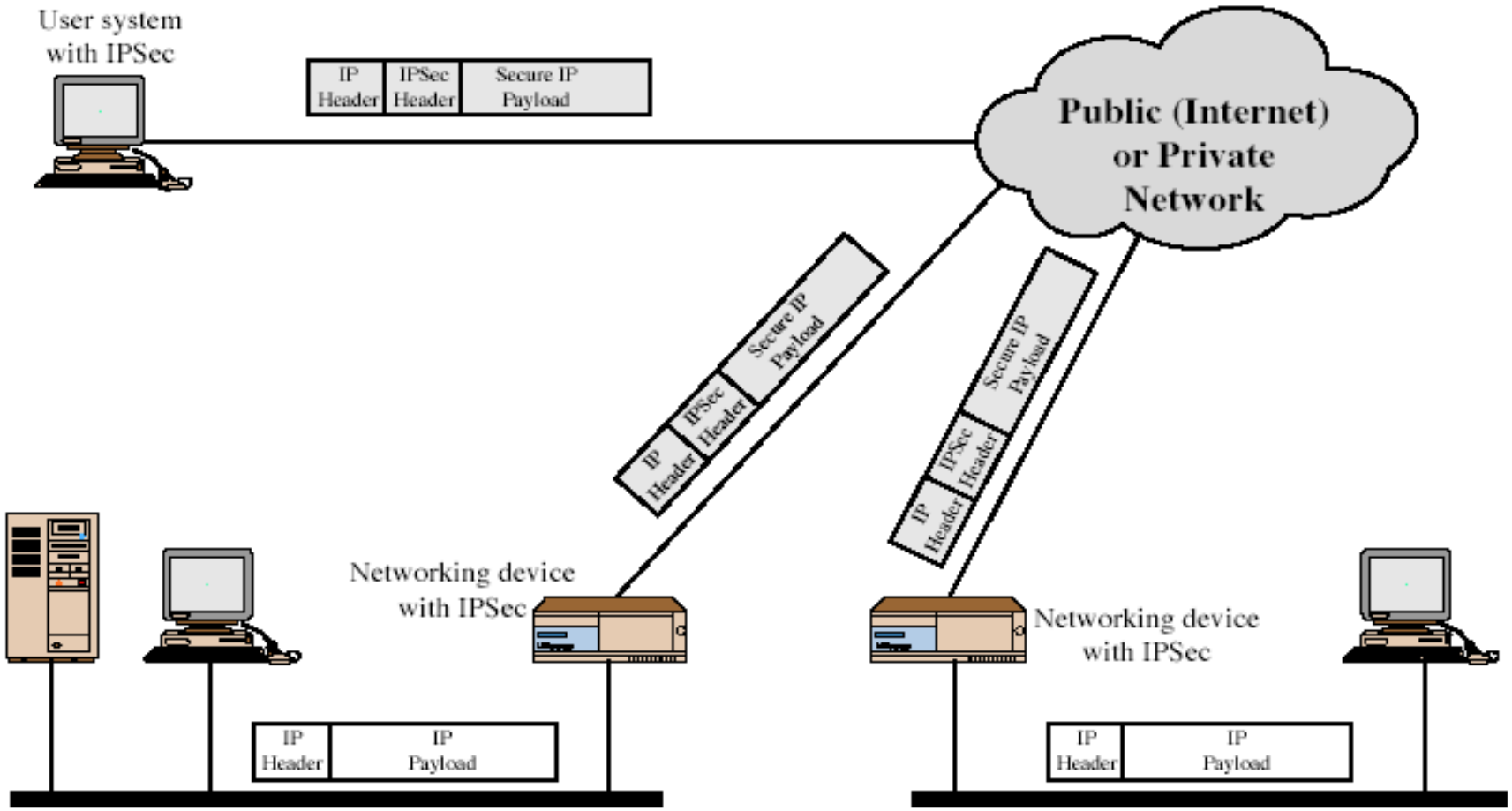
مقدمه

- IPSec یک پروتکل تنها نیست بلکه مجموعه ای از الگوریتمهای امنیتی و چارچوبی کلی فراهم می کند که به کمک آن ارتباط امنی برقرار کرد.
- سرویسهای امنیتی فراهم شده توسط IPSec
  - احراز هویت(به همراه کنترل صحت داده ها)
  - محرمانگی بسته ها
  - مدیریت کلید (تبادل امن کلید)

مقدمه

- نمونه کاربردهای IPSec
  - ایجاد VPN برای شعبه های مختلف یک سازمان از طریق اینترنت
  - دسترسی امن کارمندان شرکت به منابع شبکه از طریق اینترنت
  - امکان ارتباط امن بین چند سازمان
  - به وجود آوردن خدمات امنیتی برای کاربردهای دیگر(مثل تجارت الکترونیک)

IPSec


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload

مقدمه

- مزایای استفاده از IPSec
  - تامین امنیت قوی بین داخل و خارج LAN در صورت بکارگیری در راهیابها و حفاظ ها(Firewallها)
    - عدم سربار رمزنگاری در نقاط انتهایی
  - شفافیت از نظر کاربران
  - شفافیت از دید برنامه های کاربردی لایه های بالاتر
  - ایجاد ارتباط امن بین کارکنان سازمان از خارج به داخل

معماری IPSec: ویژگیها

- ویژگیها
  - دارای توصیف نسبتا مشکل
  - الزامی در IPv6 و اختیاری در IPv4
  - در برگرفتن موارد زیر:
  - پروتکل IPSec در سرآیند (Header)های توسعه یافته و بعد از سرآیند اصلی IP پیاده سازی می شود
  - مستندات IPSec بسیار حجیم بوده و به صورت زیر دسته بندی شده است:
    - Architecture
    - (ESP) Encapsulating Security Payload : رمزنگاری بسته ها (احراز هویت به صورت اختیاری)
    - (AH) Authentication Header : تشخیص هویت بسته ها
    - مدیریت کلید : تبادل امن کلیدها
    - الگوریتم های رمزنگاری و احراز هویت

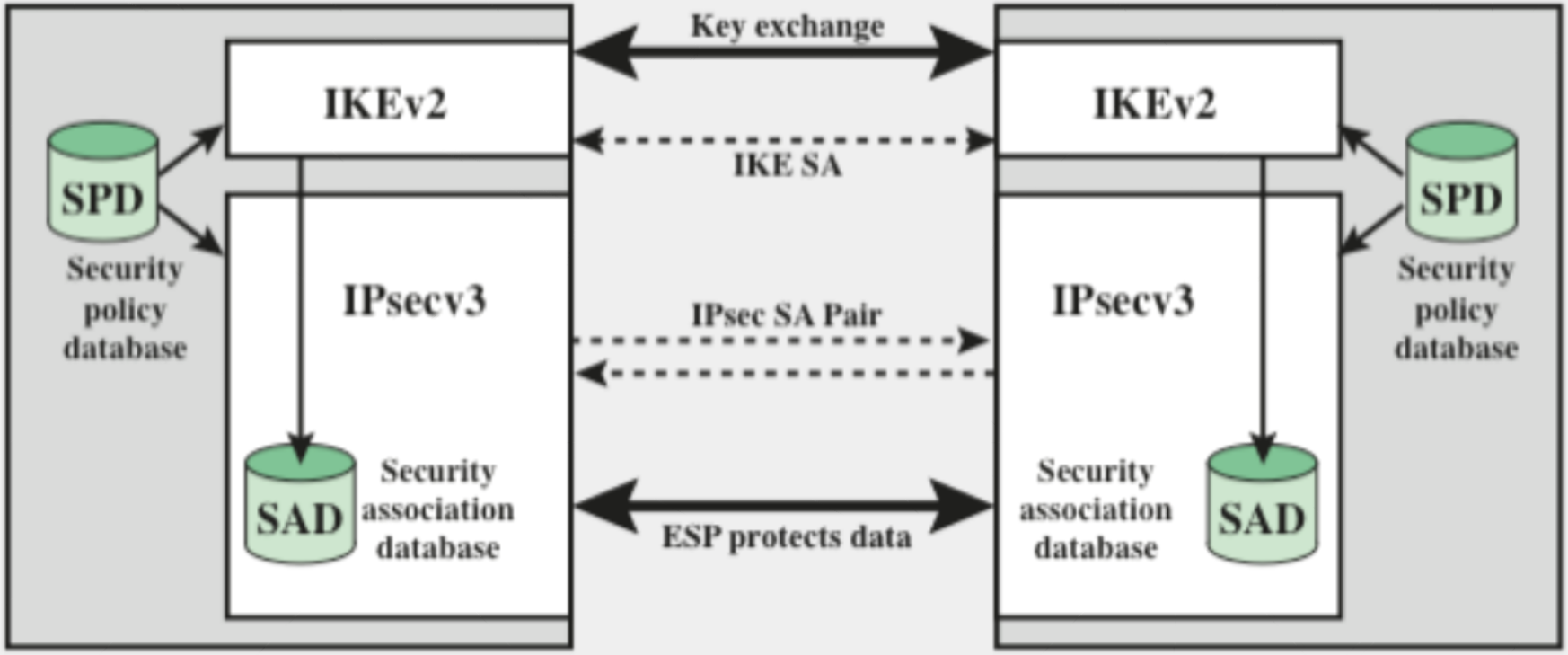


Figure 9.2 IPsec Architecture

معماری IPSec: سرویس ها

- سرویس های ارائه شده : IPSec این امکان را به سیستمها می دهد تا پروتکلها، الگوریتمها و کلیدهای لازم برای ارائه سرویسهای زیر را انتخاب کنند
  - کنترل دسترسی
  - تضمین صحت داده ها در ارتباط Connectionless
  - احراز هویت منبع داده ها (Data Origin)
  - تشخیص بسته های دوباره ارسال شده و رد آنها (Replay Attack)
  - محرمانگی بسته‌ها
  - محرمانگی جریان ترافیک

معماری IPSec: سرویس ها

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

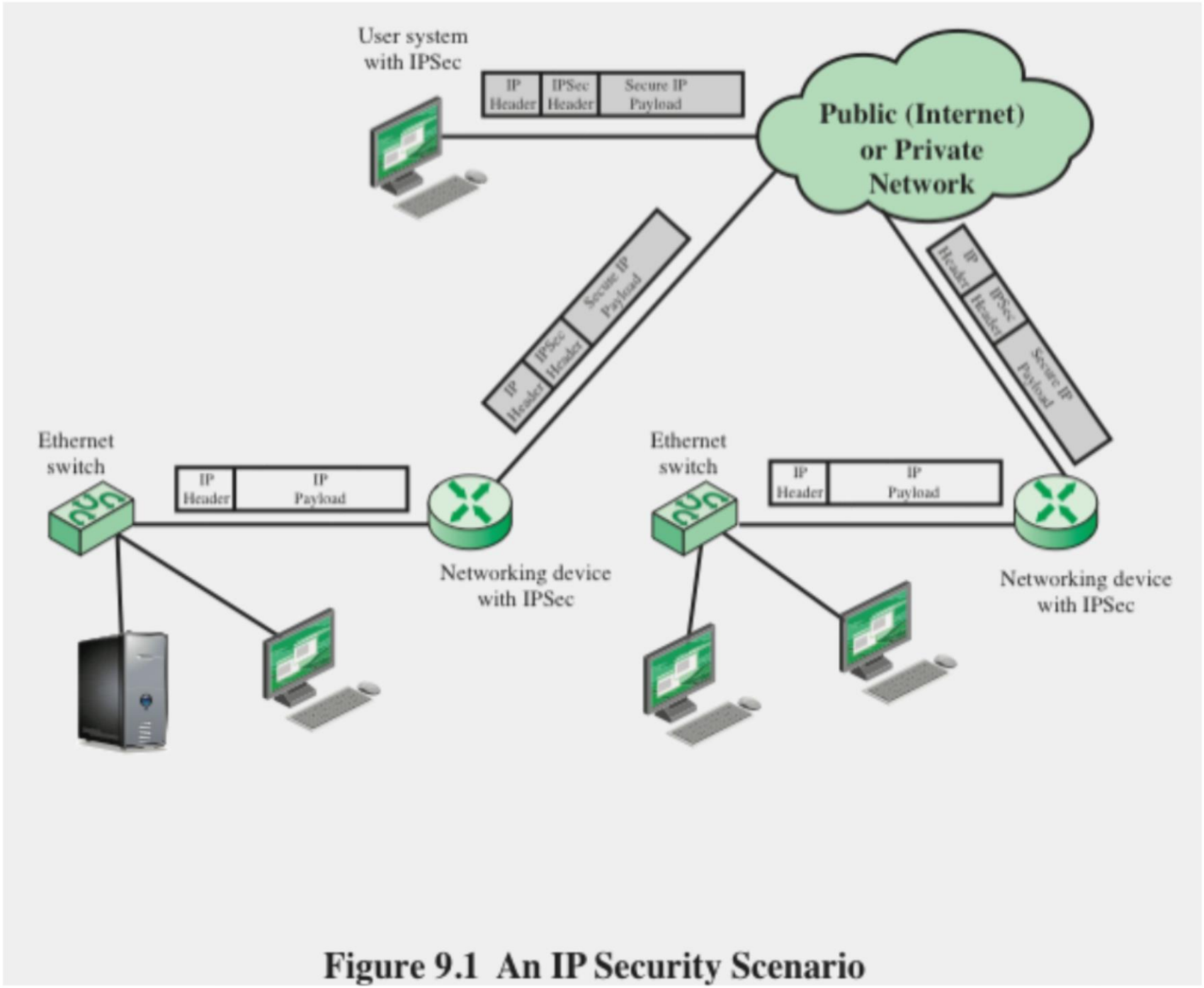


Figure 9.1 An IP Security Scenario

معماری IPSec:
Security Association

- مجمع امنیتی(Security Association) یک مفهوم کلیدی در مکانیزم‌های احراز هویت و محرمانگی برای IP بوده و یک رابطه یک طرفه بین فرستنده و گیرنده بسته ایجاد می کند و سرویس های امنیتی را برای ترافیک خط فراهم می‌کند.

- SA در IP به نوعی معادل Connection در TCP است

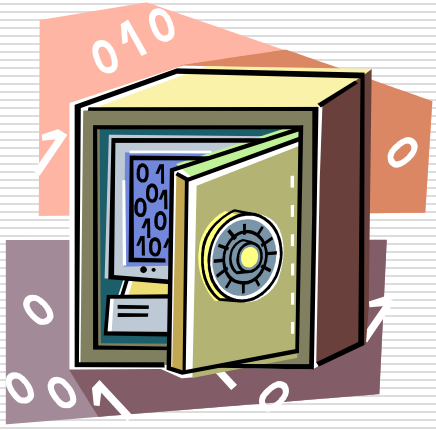
معماری IPSec:
Security Association

ویژگیها :

- **یک SA بصورت یکتا با ۳ پارامتر تعیین می شود:**
  - Security Parameters Index (SPI): یک رشته بیتی نسبت داده شده به SA
  - IP Destination Address : آدرس مقصد نهایی SA
  - Security Protocol Identifier : بیانگر تعلق SA به AH یا ESP

Security Association Database (SAD)

- پارامترهای هر SA را تعیین می‌کند.
- پارامترهای SA:
  - Sequence Number Counter
  - Sequence Counter Overflow
  - Anti Replay Windows
  - AH Information
  - ESP Information
  - SA Lifetime
  - IPSec Protocol Mode
  - Maximum Transmission Unit (MTU)



Security Policy Database (SPD)

- مکانیزمی که مشخص می‌کند هر ترافیک IP مرتبط با کدام SA است.
  - شامل سطرهایی که هر یک زیرمجموعه‌ای از ترافیک IP و SA مربوط است.
- در محیطهای پیچیده‌تر، ممکن است چند سطر مرتبط با یک SA یا چند SA مرتبط با یک SPD باشد.
  - هر مدخل SPD با مجموعه‌ای از مقادیر فیلدهای IP و پروتکل‌های لایه بالاتر تعریف می‌شود که selector نامیده می‌شوند.
  - برای نگاشت ترافیک به یک SA خاص استفاده می‌شوند.

فیلدهای SPD

- selectorها که یک سطر از SPD را مشخص می‌کنند.

Remote IP address	Local IP address	Next layer protocol	Name	Local and remote ports
This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address	This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address	The IP protocol header includes a field that designates the protocol operating over IP	A user identifier from the operating system	These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port
The latter two are required to support more than one destination system sharing the same SA	The latter two are required to support more than one source system sharing the same SA		Not a field in the IP or upper-layer headers but is available if IPsec is running on the same operating system as the user	

مثالی از جدول SPD

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

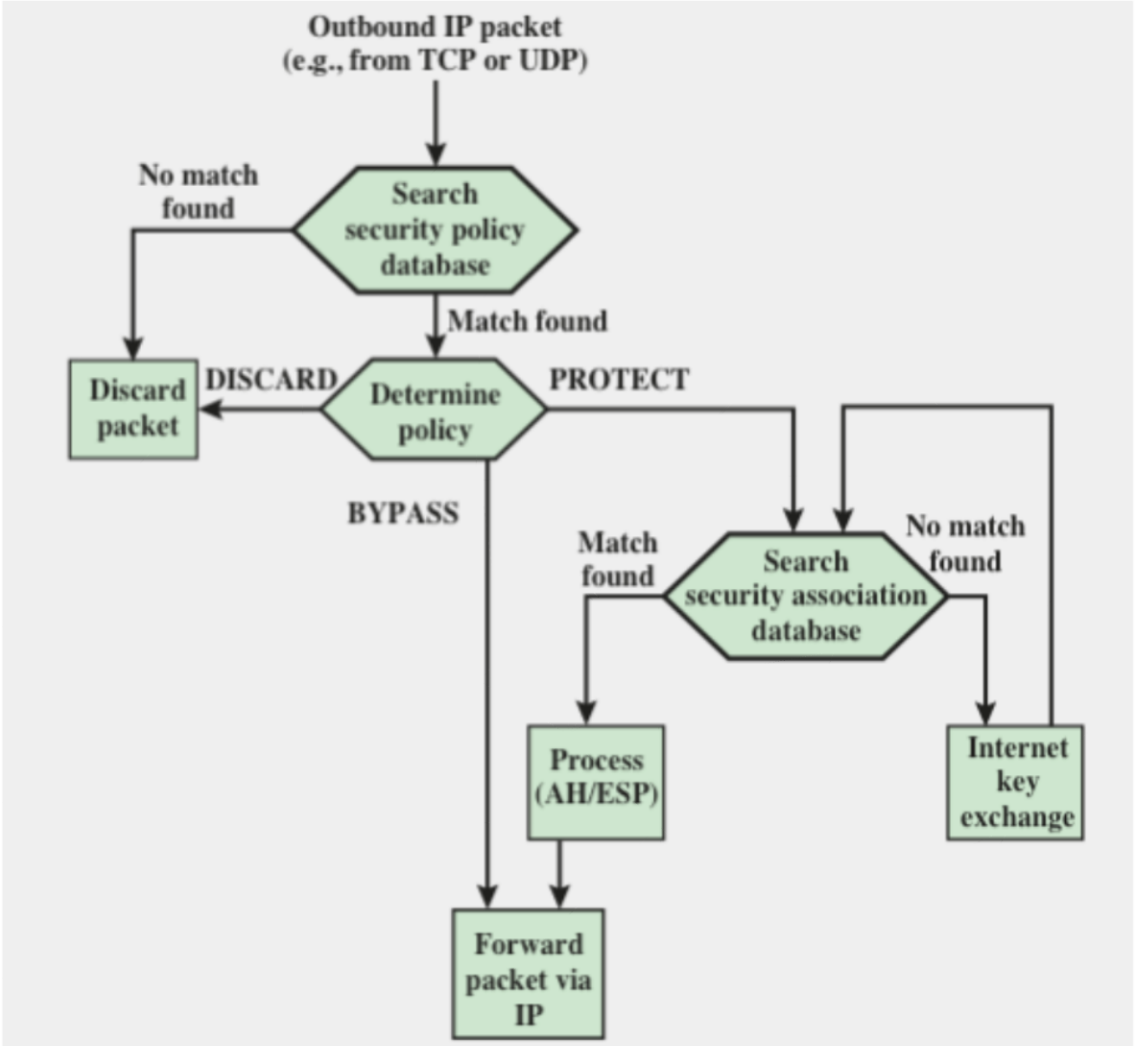


Figure 9.3 Processing Model for Outbound Packets

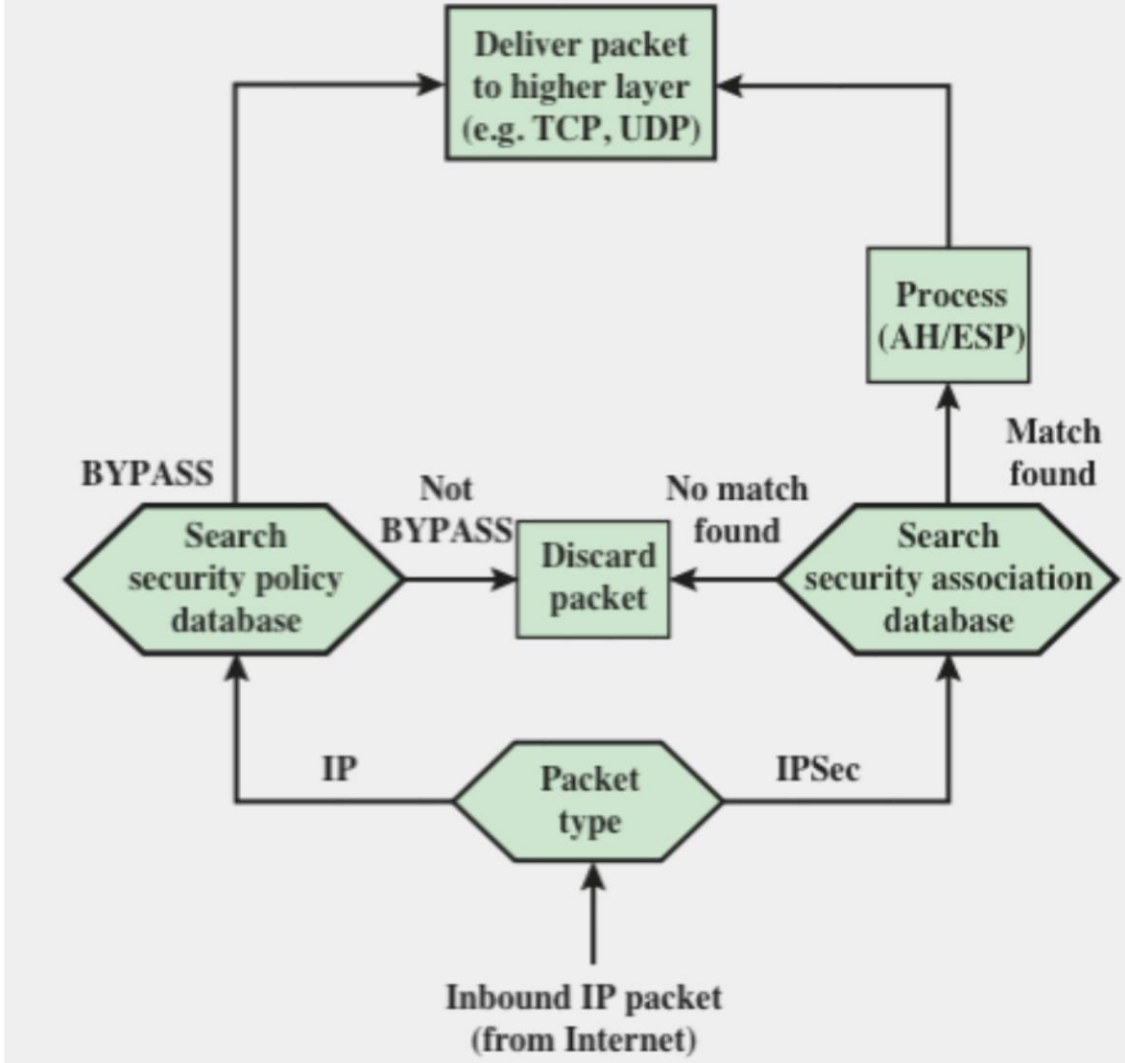
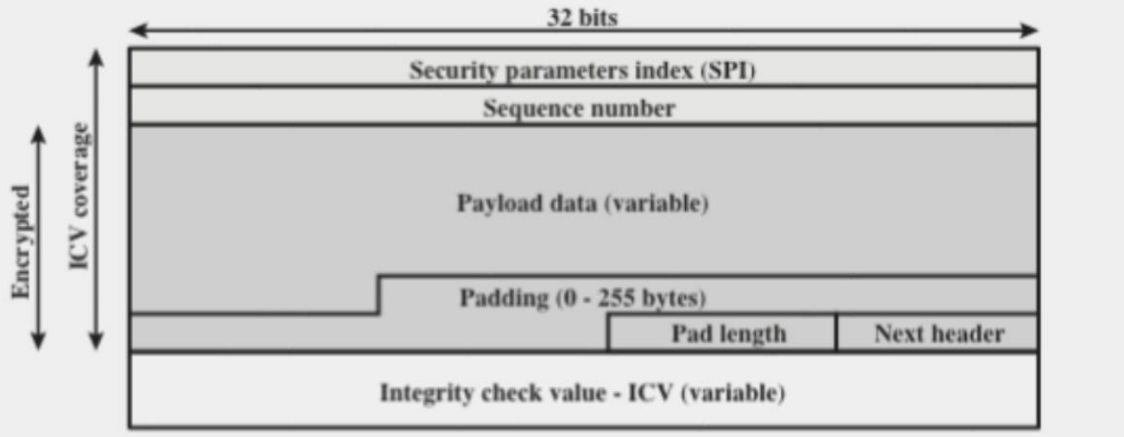
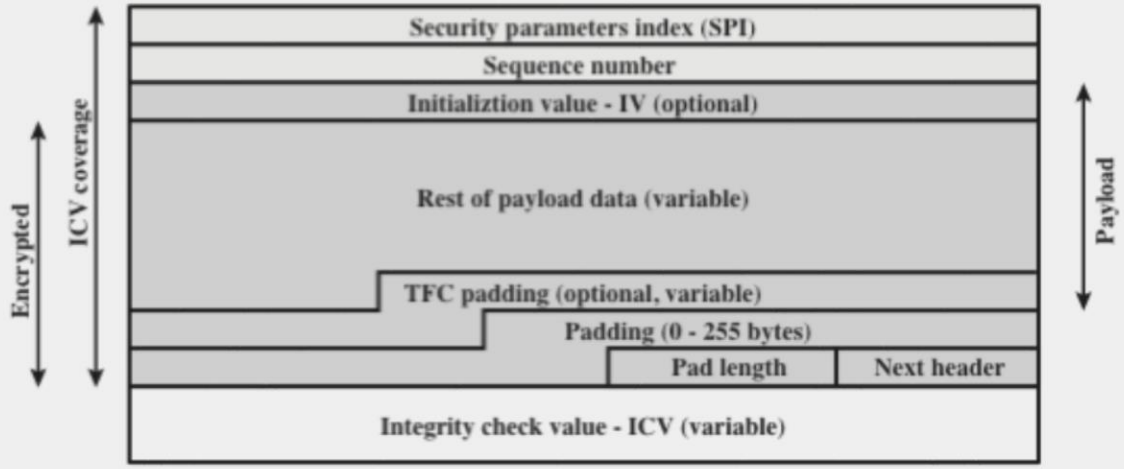


Figure 9.4 Processing Model for Inbound Packets



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

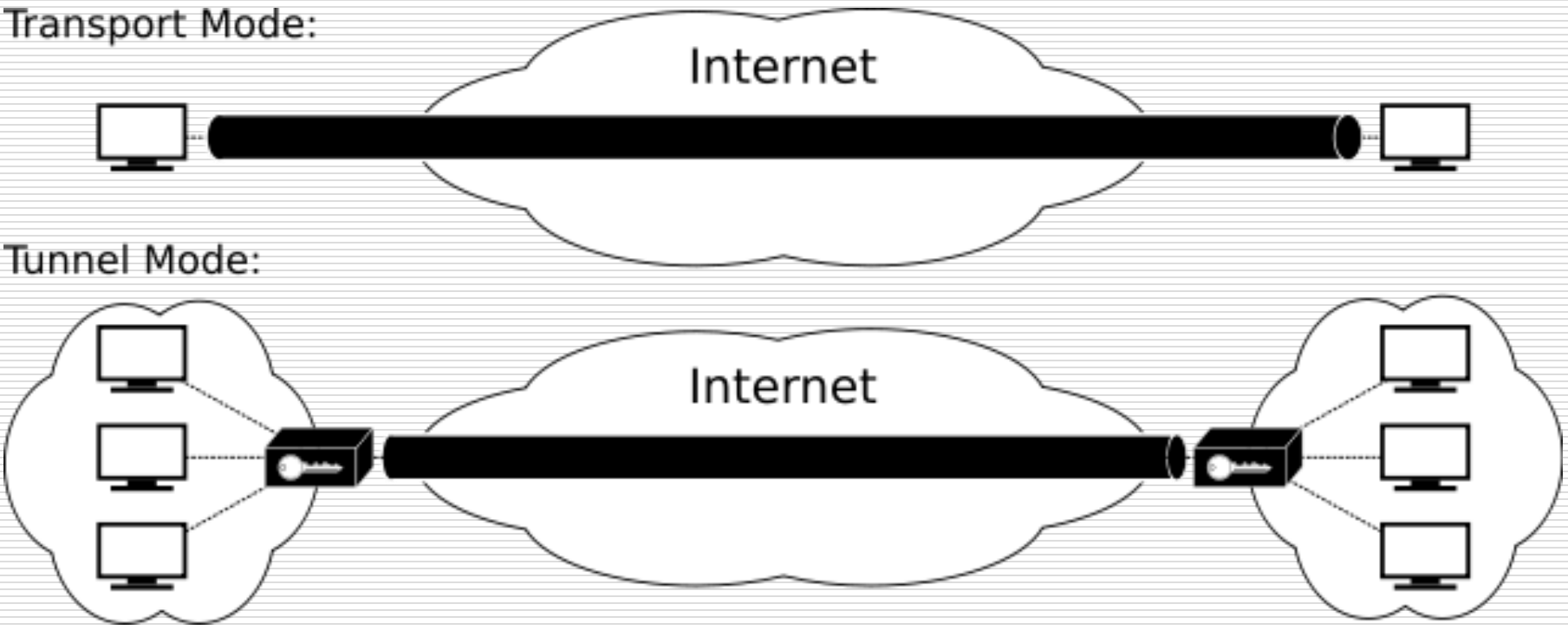
Figure 9.5 ESP Packet Format

معماری IPSec:
حالتهای انتقال بسته‌ها

- در هر دوی AH و ESP دو حالت انتقال وجود دارد:

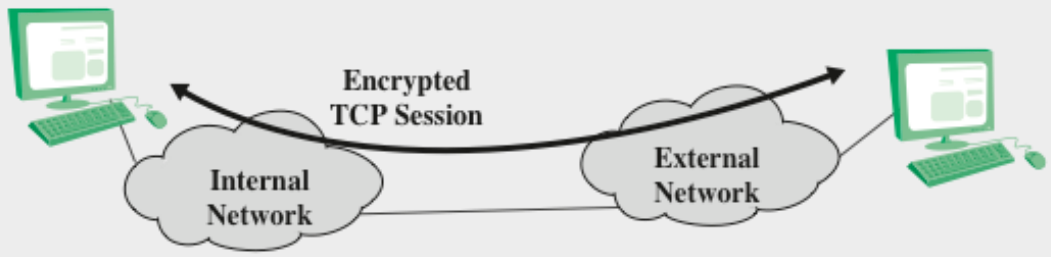
  - حالت انتقال (Transport Mode)
    - تغییرات تنها روی محتوای بسته صورت می گیرد، بدون تغییر سرآیند IP
  - حالت تونل (Tunnel Mode)
    - اعمال تغییرات روی کل بسته IP(سرآیند+Payload) و فرستادن نتیجه به عنوان یک بسته جدید

IPSec Modes

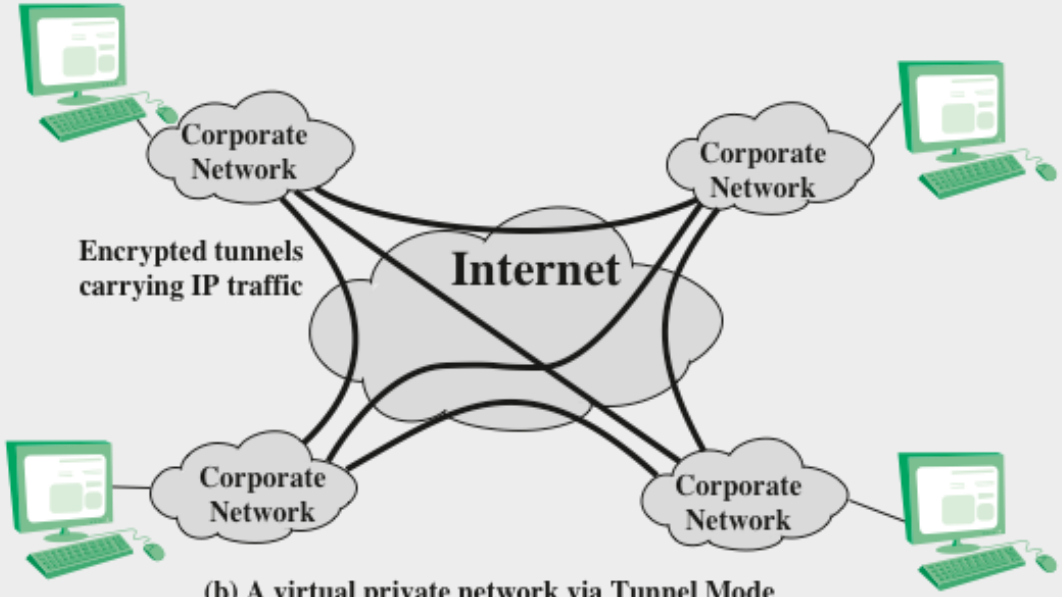


معماری IPSec:
حالتهای انتقال بسته‌ها

- حالت انتقال
  - در کاربردهای انتها به انتها(end-to-end) مثل کارگزار/کارفرما استفاده می‌شود
  - ESP : رمزنگاری (ضروری) و احراز هویت (اختیاری) Payload بسته
  - AH : احراز هویت Payload بسته و قسمتهای انتخاب شده سرآیند بسته



(a) Transport-level security



(b) A virtual private network via Tunnel Mode

Figure 9.7 Transport-Mode vs. Tunnel-Mode Encryption

معماری IPSec:
حالتهای انتقال بسته‌ها

- حالت تونل
  - مورد استفاده در ارتباط Gateway به Gateway
  - هیچ مسیریاب(router) میانی قادر به تشخیص سرآیند داخلی نیست

Functionality of Modes

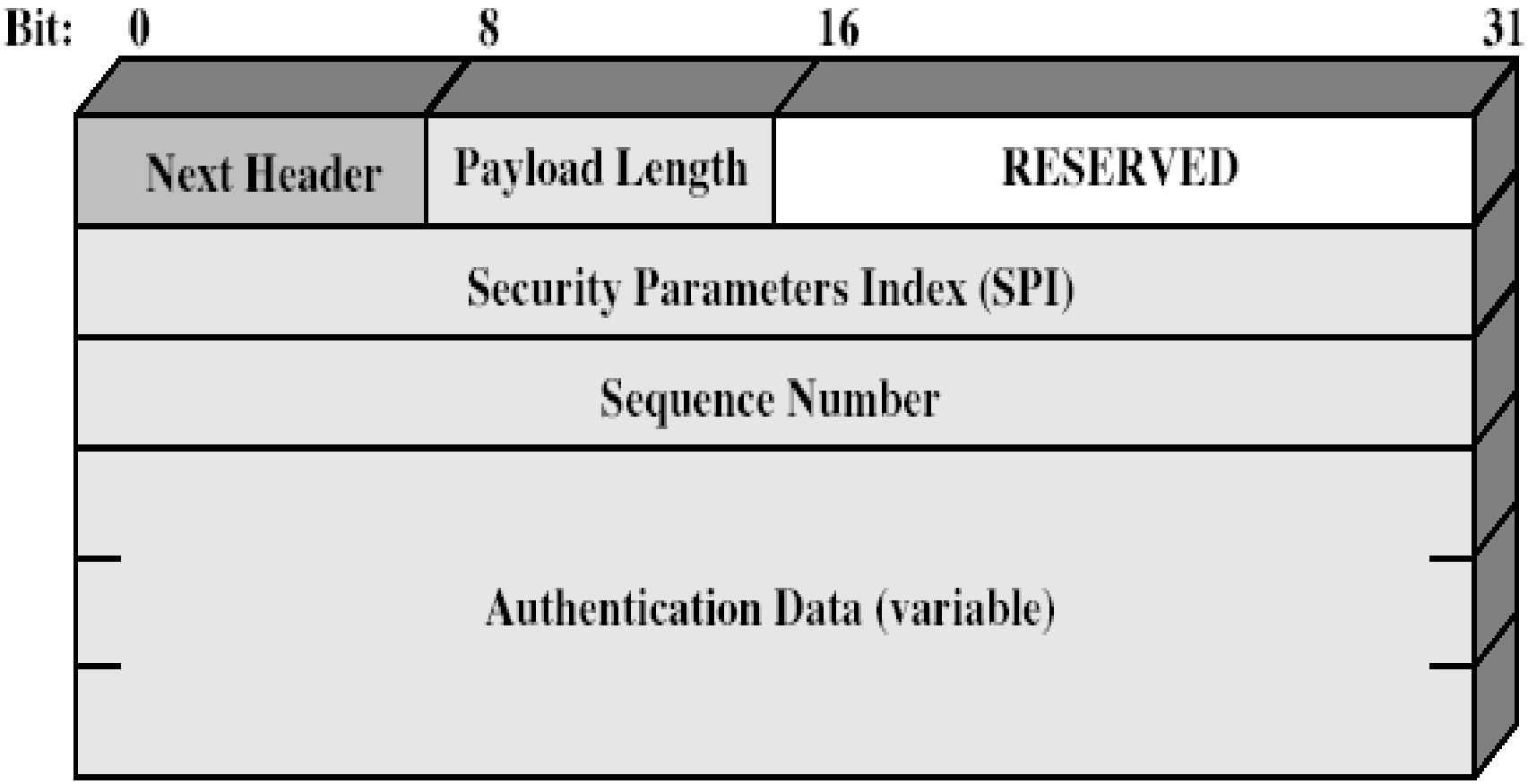
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

Authentication Header (AH)

- Authentication Header
  - تضمین صحت و احراز هویت بسته‌های IP
  - تامین سرویس صحت داده‌ها با استفاده از MAC
    - HMAC-SHA2 یا HMAC-SHA1

- طرفین نیاز به توافق روی یک کلید مشترک متقارن دارند.

Authentication Header



AH

- فیلدهای AH :
  - Next Header(۸ بیت) : نوع سرآیند بعدی موجود در بسته
  - PayLoad Length(۸ بیت) : بیانگر طول AH
  - Reserved(16 بیت) : رزرو شده برای استفاده های آینده
  - Sec. Param. Index(۳۲بیت) : برای تعیین SPI مربوط به SA
  - Sequence Number(۳۲بیت) : شمارنده
  - Authentication Data(متغیر) : دربرگیرنده MAC یا ICV

AH

- محاسبه MAC
  - خروجی الگوریتم HMAC
- محاسبه MAC روی مقادیر زیر انجام می گیرد
  - سرآیند نامتغیر IP، سرآیند نامتغیر AH و محتوای بسته

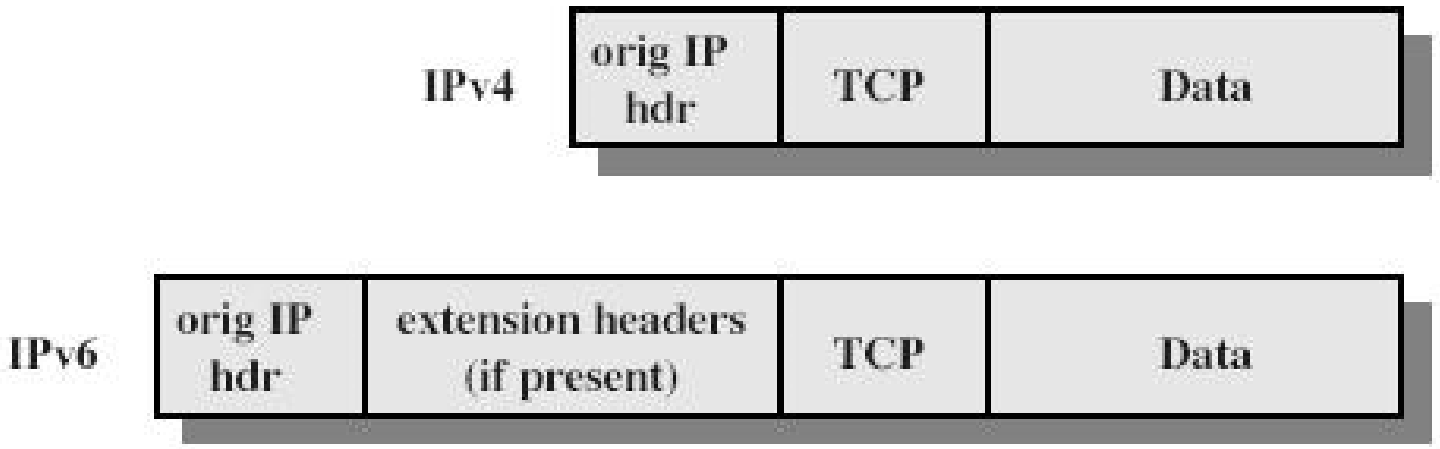
- قسمتهایی از سرآیند که احتمالا در انتقال تغییر می‌کنند(مانند TTL)، در محاسبه MAC صفر منظور می شوند.
- آدرسهای فرستنده و گیرنده نیز در محاسبه MAC دخیل هستند(جهت جلوگیری از حمله جعل IP)

AH

- حالتهای انتقال و تونل در AH :
  - حالت انتقال(Transport) : برای احراز هویت مستقیم بین کامپیوتر کاربر و کارگزار
  - حالت تونل(Tunnel) : برای احراز هویت بین کاربر و حفاظ(firewall)

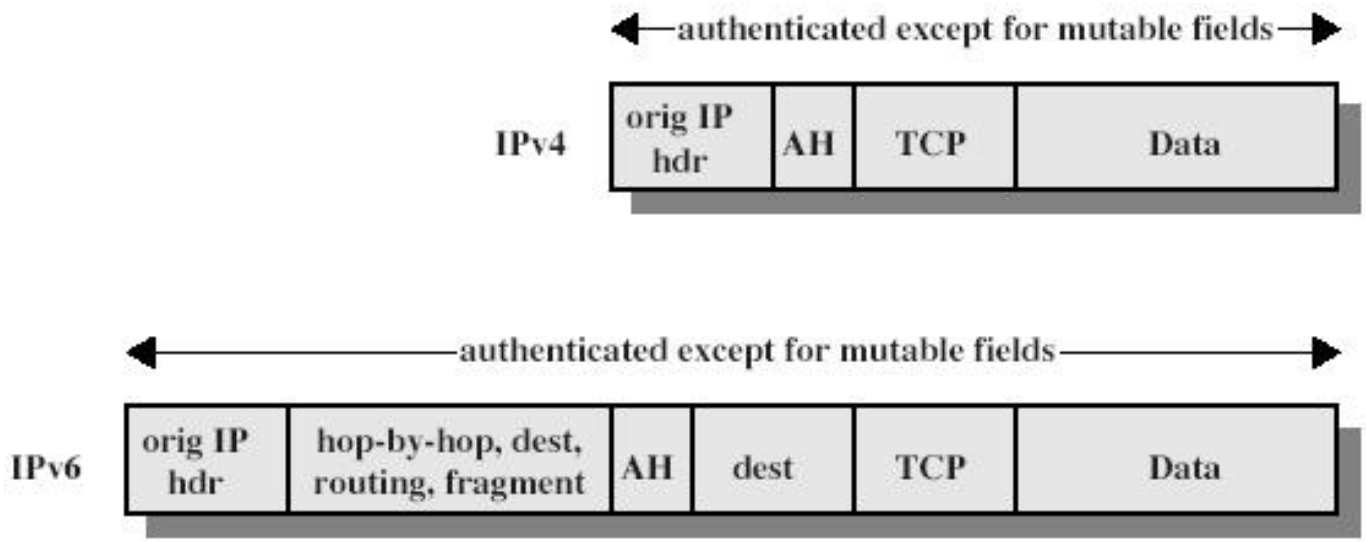
Scope of AH Authentication Before Application

- IP payload is TCP segment (data unit)

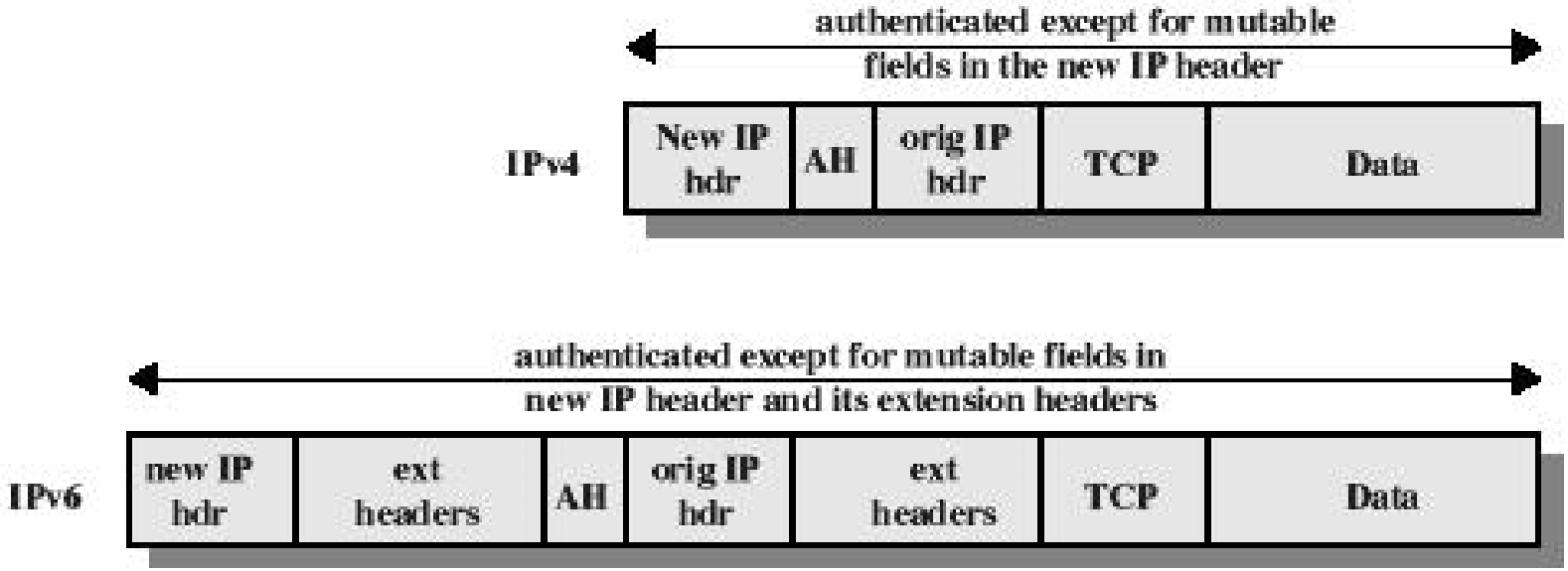


Scope of AH Authentication Transport Mode

- IPv6: AH is end-to-end payload



Scope of AH Authentication Tunnel Mode

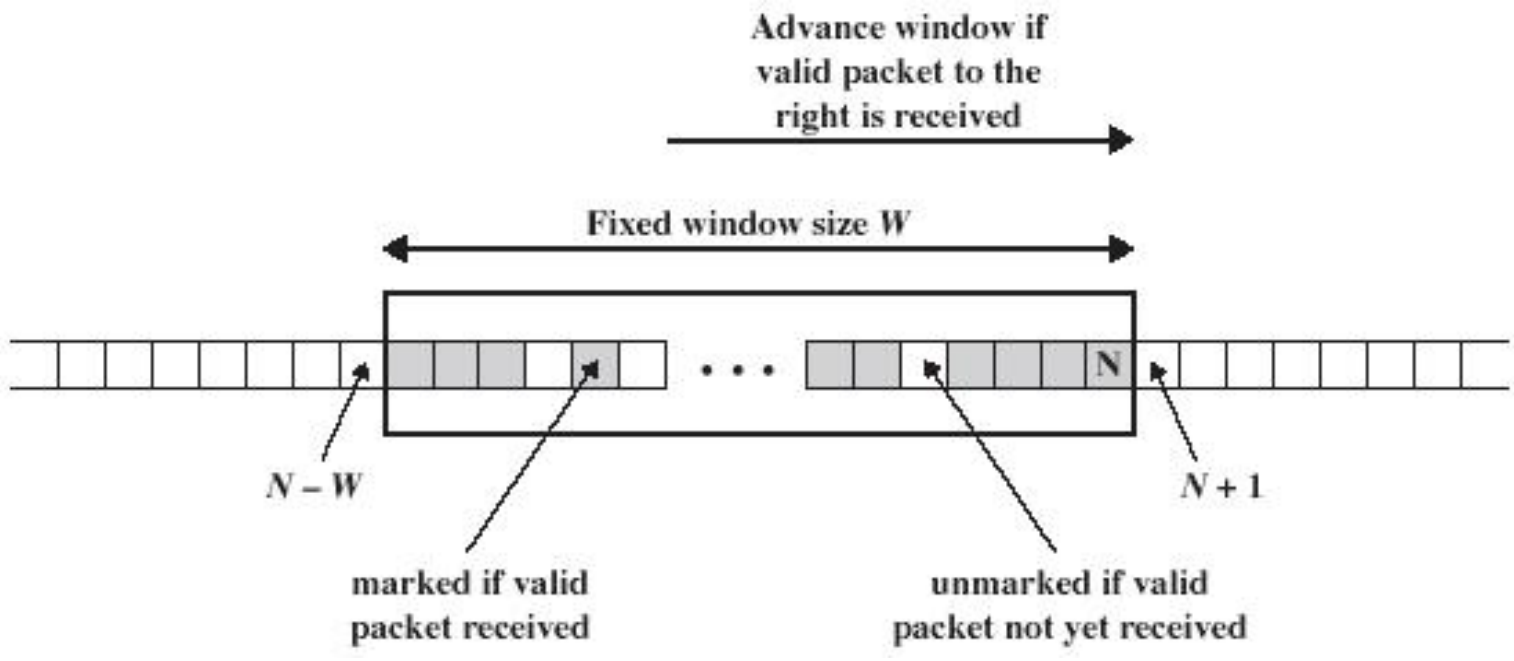


AH

- روش مقابله با حمله تکرار(Replay)
  - اختصاص یک شمارنده با مقدار صفر به هر SA
  - افزایش شمارنده به ازای هر بسته جدید که با این SA فرستاده می شود
  - اگر شمارنده به مقدار $2^{32}-1$ برسد، باید از یک SA جدید با کلید جدید استفاده کرد
  - درنظرگرفتن یک پنجره به سایز (٦٤=) W
  - لبه سمت راست پنجره به بزرگترین شماره بسته رسیده و تاییدشده از نظر صحت می باشد

AH

- مکانیسم برخورد با بسته جدید در پنجره
  - بسته جدید و داخل محدوده پنجره
    - محاسبه MAC و علامت زدن خانه متناظر در پنجره در صورت تایید هویت
  - بسته خارج از محدود پنجره (سمت راست)
    - محاسبه MAC ، تایید هویت و شیفت پنجره به سمت راست، به طوری که خانه متناظر سمت راست لبه پنجره را نشان دهد
  - بسته جدید خارج از محدوده پنجره یا عدم احراز هویت آن
    - دور انداخته می شود!


Advance window if
valid packet to the
right is received
Fixed window size W
N
N – W
N + 1
marked if valid
packet received
unmarked if valid
packet not yet received

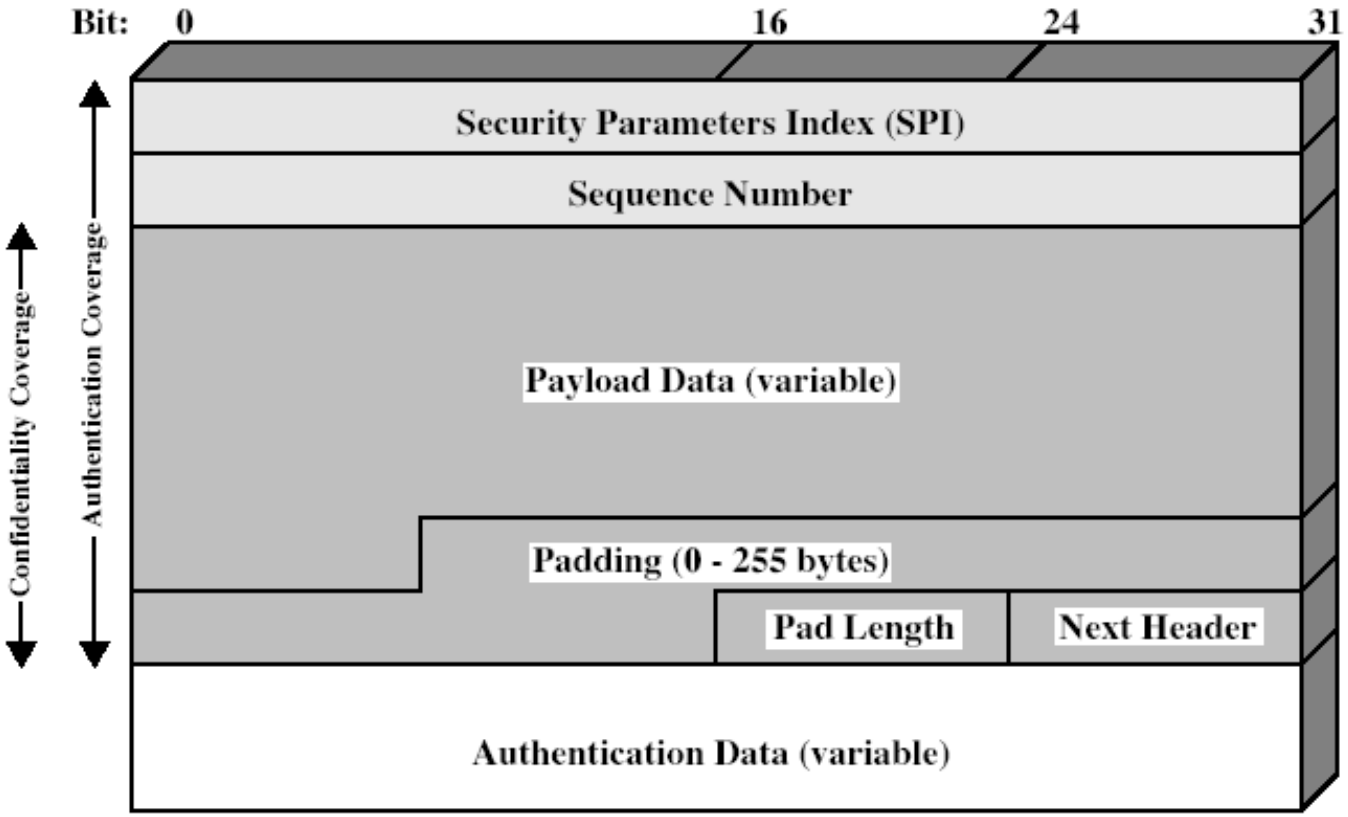
ESP

- ویژگی‌ها
  - پشتیبانی از محرمانگی داده و تا حدی محرمانگی ترافیک
  - امکان استفاده از احراز هویت (مشابه AH)
  - استفاده از الگوریتم‌های متقارن برای رمزنگاری محتوا
    - TripleDES-CBC
    - AES-CBB, AES-CTR, AES-GCM
    - ChaCha2-Poly1305

ESP

- فیلدهای ESP
  - SPI : شناسه SA
  - Sequence Number : شمارنده برای جلوگیری از حمله تکرار مشابه AH
  - Payload : محتوای بسته که رمز می شود
  - Padding : بیتهای اضافی
  - Pad Length : طول فیلد بالا
  - Next Header : نوع داده موجود در Payload Data
  - Authentication Data : مقدار MAC محاسبه شده (بدون در نظر گرفتن خود فیلد)

Encapsulating Security Payload

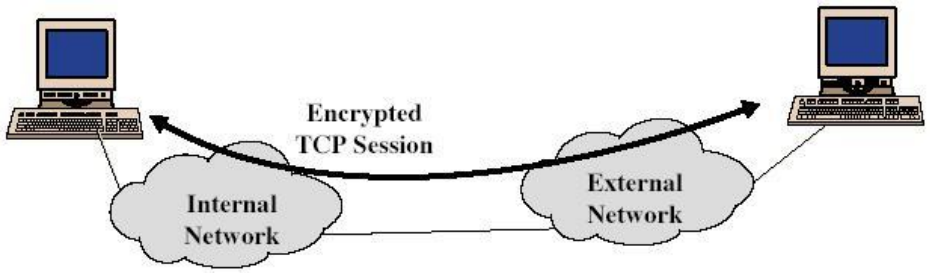


ESP

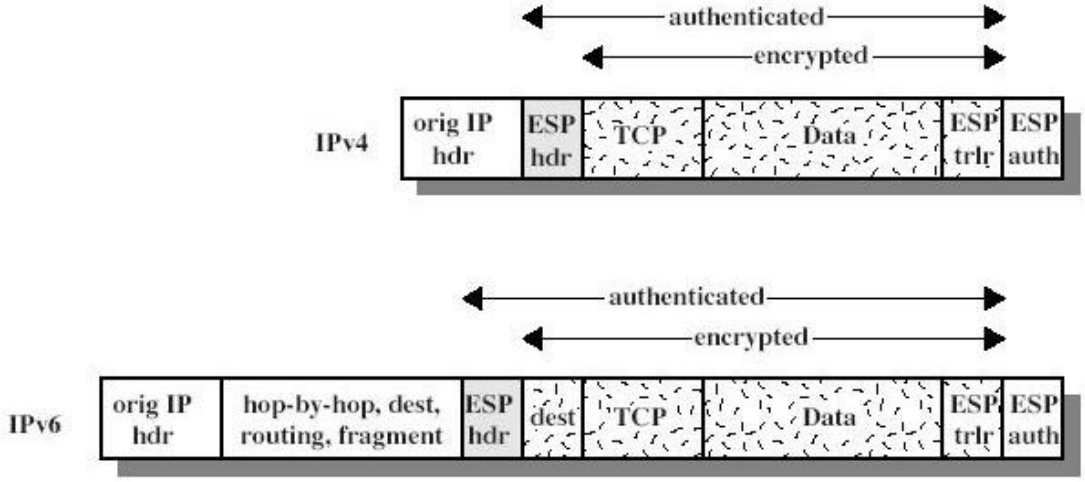
- حالت انتقال
  - تضمین محرمانگی بین host ها
  - رمزنگاری بسته داده، دنباله ESP و اضافه شدن MAC درصورت انتخاب احراز هویت توسط مبداء
  - تعیین مسیر توسط Router های میانی با استفاده از سرآیندهای اصلی(که رمز نشده‌اند)
  - چک کردن سرآیند IP توسط مقصد و واگشایی رمز باقیمانده پیام
  - امکان تحلیل ترافیک

Transport Mode ESP

- used for communication between hosts



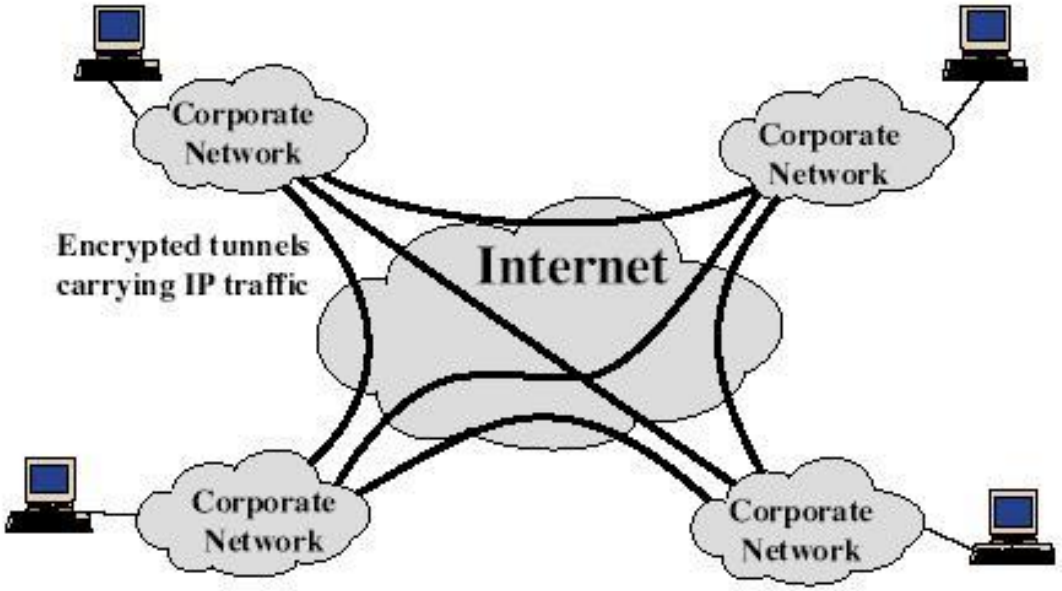
- scope

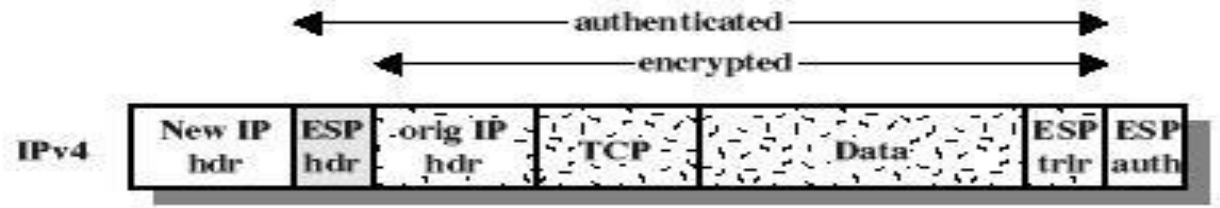


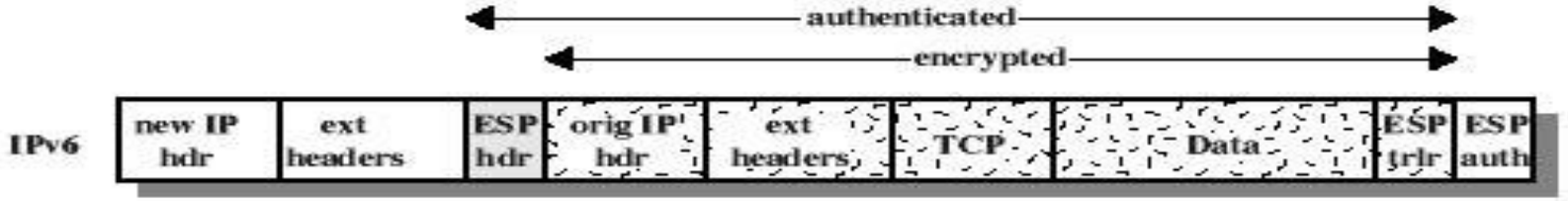
ESP

- حالت تونل
  - اضافه شدن آدرس مبداء و مقصد دروازه های خروجی فرستنده و گیرنده، سرآیند ESP و دنباله ESP و قسمت مربوط به MAC در صورت نیاز(برای هویت‌شناسی)
  - انجام مسیریابی در Routerهای میانی از روی آدرس‌های جدید
  - رسیدن بسته به فایروال شبکه مقصد و مسیریابی از روی آدرس IP قبلی تا گره نهایی
  - حالت تونل IPSec یکی از روشهای ایجاد VPNها است

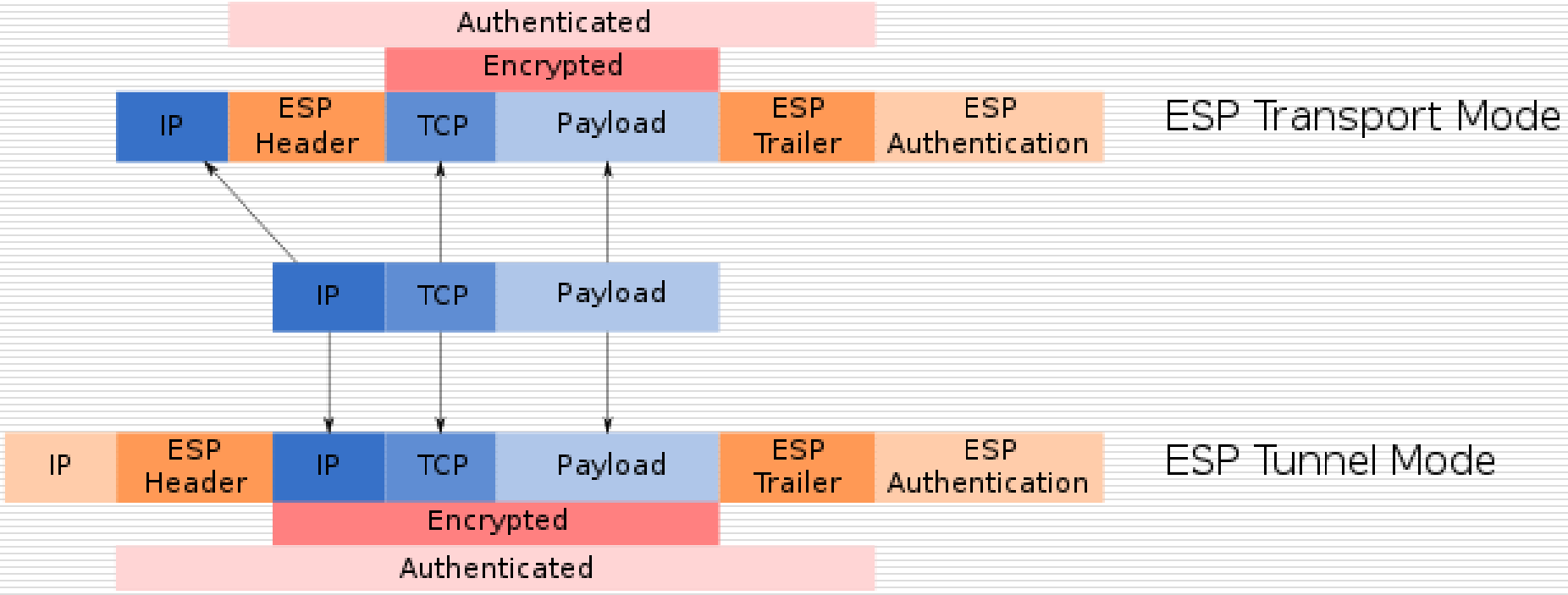
Tunnel Mode ESP

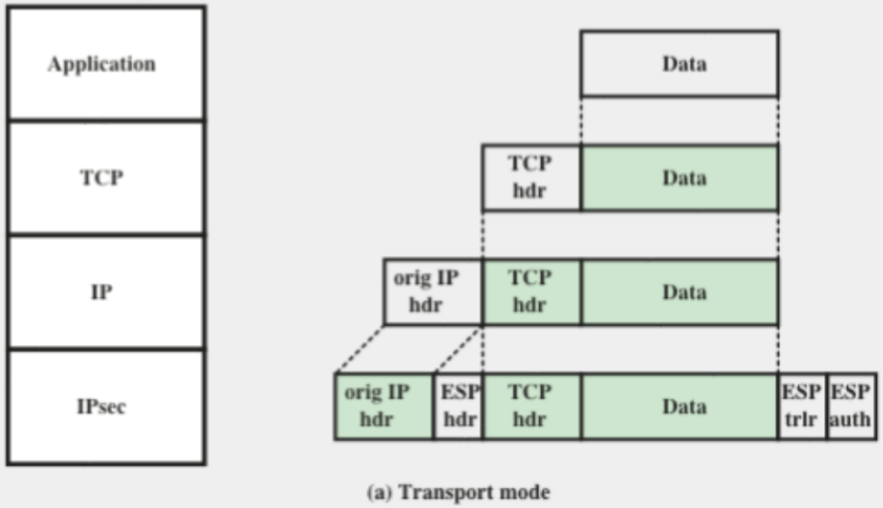




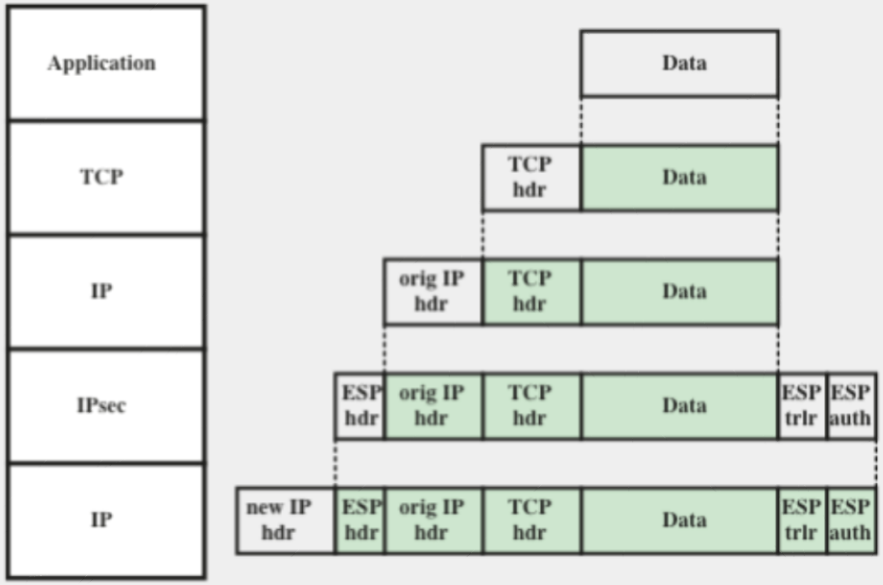


ESP in Tunnel and Transport modes





(a) Transport mode



(b) Tunnel mode

Figure 9.9 Protocol Operation for ESP

ترکیب SAها

- با توجه به اینکه هر SA تنها یکی از سرویس‌های AH یا ESP را پیاده سازی کرده است، برای استفاده از هر دو سرویس باید آنها را باهم ترکیب کرد.

- ترکیب‌های مختلف
  - پیاده سازی IPSec توسط host های متناظر
  - پیاده سازی IPSec توسط gateway ها
  - ترکیب دو حالت بالا

ترکیب SAها

- *Security association bundle*
  - دنباله SAها که با هم ترکیب می‌شوند تا سرویس‌های مطلوب IPSec بدست آید.
  - SA های یک باندل در دو نقطه متفاوت یا یک نقطه مشابه تمام می‌شوند.
  - دو روش ترکیب در یک باندل:
    - Transport adjacency: اعمال بیش از یک پروتکل امنیتی روی یک بسته IP بدون تونل
    - Iterated tunneling: اعمال لایه‌های مختلف امنیتی با استفاده از تونل

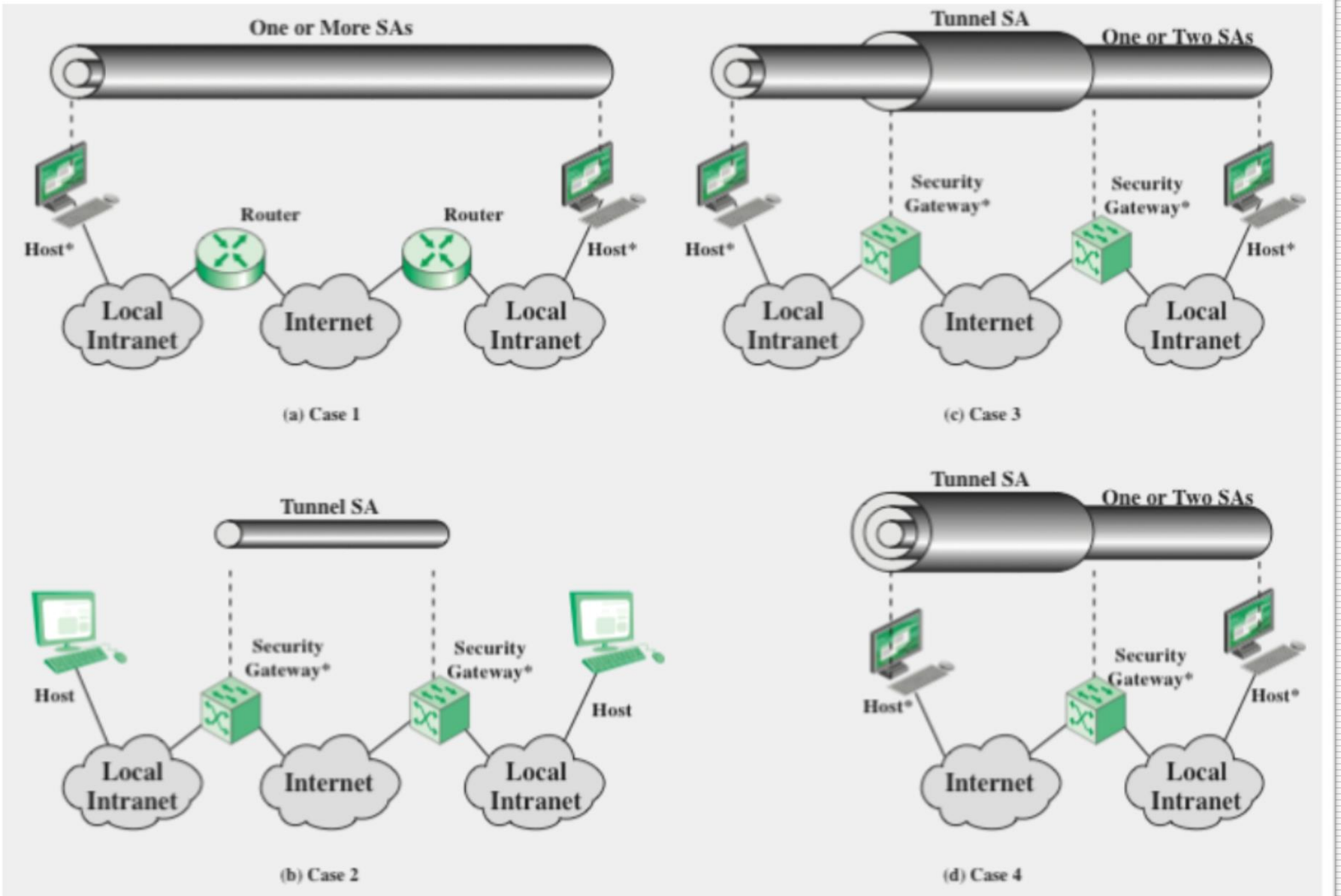


Figure 9.10 Basic Combinations of Security Associations

مدیریت کلید

- عموما به دو زوج کلید، یکی برای AH و دیگری برای ESP نیازمندیم. برای تولید و توزیع این کلیدها به یک مکانیزم مدیریت کلید نیازمندیم.

- دو زوج کلید از این جهت که برای ارسال و دریافت در دو حالت AH و ESP نیازمندیم.

مدیریت کلید

- مدیریت کلید دستی : تنها در سیستم های ایستا و کوچک قابل استفاده است

- مدیریت خودکار :
  - پروتکل اتوماتیک و پیش فرض مدیریت و توزیع کلید IPSec اصطلاحا ISAKMP/Oakley نامیده می شود.

Internet Security Association
and Key Management Protocol

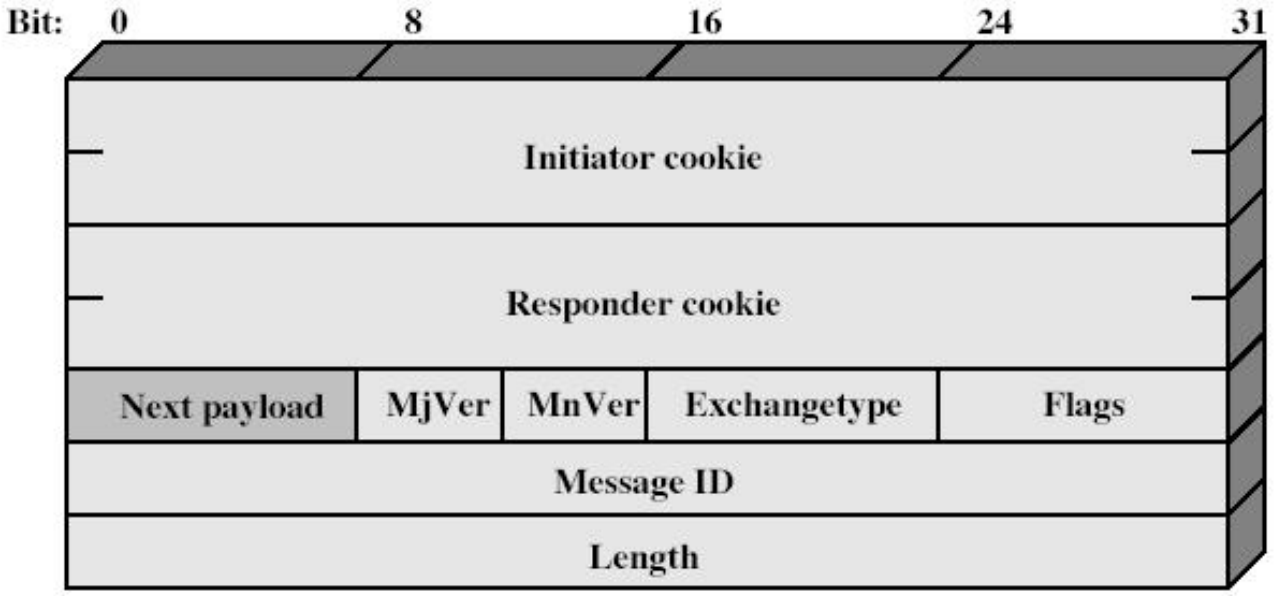
مدیریت کلید

- مدیریت کلید خودکار به نام ISAKMP/Oakley معروف است و شامل دو فاز است
  - پروتکل تعیین کلید Oakley : فرم توسعه یافته پروتکل Diffie-Hellman که ضعفهای آن را برطرف کرده است
    - Clogging Attack: از آنجا که پروتکل دیفی-هلمن سنگین است، منابع قربانی تلف می شود.
      - با استفاده از تعریف مفهومی تحت عنوان Cookie مشکل این حمله را برطرف می کند
    - Man-In-The-Middle-Attack
    - Replay Attack
      - با استفاده از Nonce با حمله های تکرار مقابله می کند.
  - پروتکل مدیریت کلید و SA در اینترنت(ISAKMP)
    - تعریف رویه ها و قالب بسته ها برای برقراری، مذاکره، تغییر یا حذف SA

برای مطالعه بیشتر

- The IPSec Working Group of the IETF. Charter for the group and latest RFCs and Internet Drafts for IPSec:
  - http://ietf.org/html.charters/ipsec-charter.html
- IPSec Resources: List of companies implementing IPSec, implementation survey, and other useful material:
  - http://web.mit.edu/tytso/www/ipsec/index.html

ISAKMP Header & Payload Header



پیوست الف

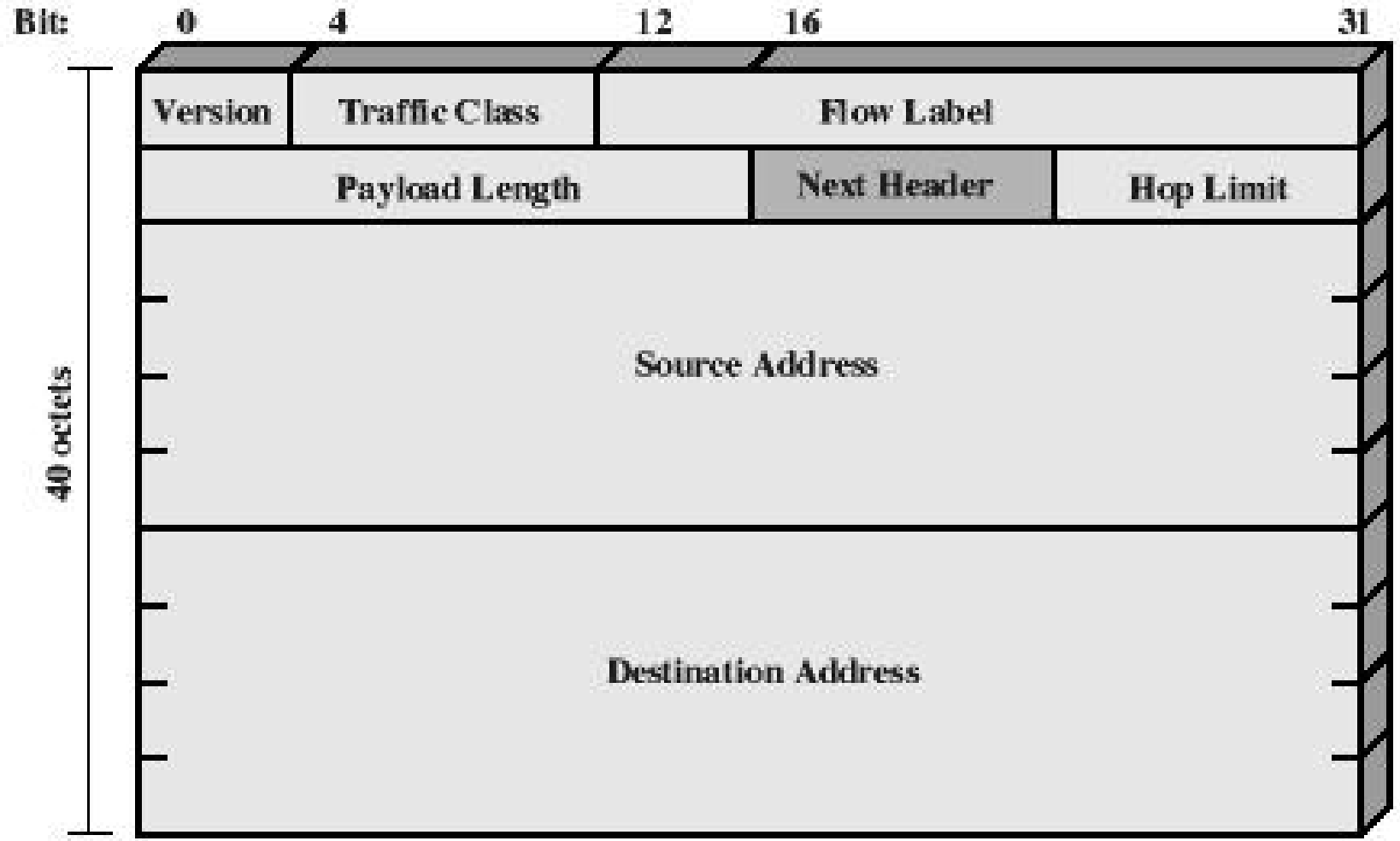
مروری بر IPv6

مرور IPv6

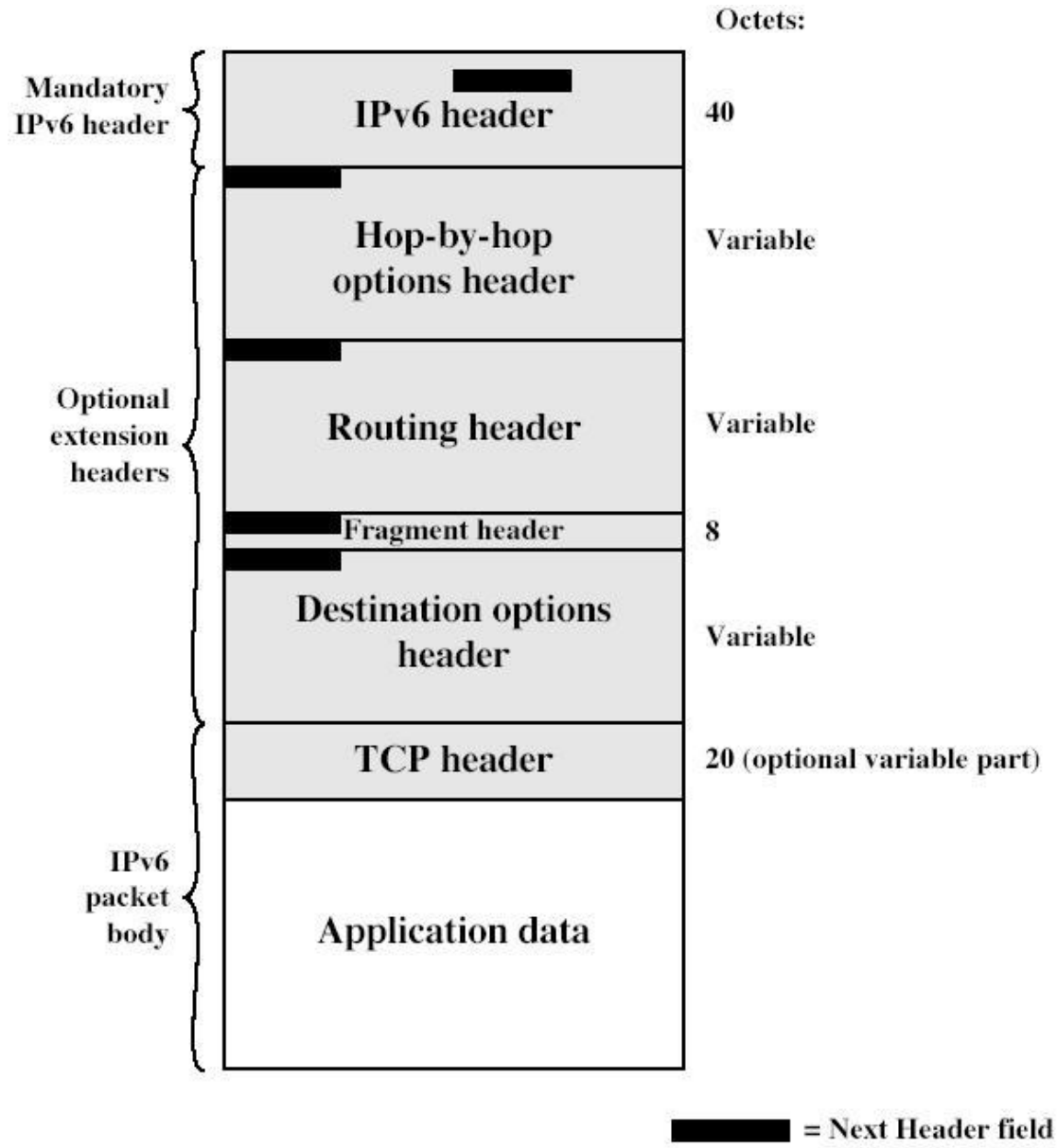
- نسخه ٦ IP عمدتا برای رسیدن به اهداف زیر توسعه یافت:

  - افزودن فضای آدرس دهی : آدرسهای ١٦ بایتی در مقابل آدرسهای ٤ بایتی در IP v4.0
  - سرآیندهای توسعه یافته (Extension Headers)
  - کاهش حجم پردازش در مسیریابها(Routerها)

IPV6


Bit:
0
4
12
16
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
40 octets

IPV6 Extension Headers



مرور IPv6

- سرآیندهای توسعه یافته IPv6.0
  - Hop-by-Hop Options header
    - در صورت نیاز به پردازش hop به hop
  - Routing header
    - مسیریابی توسعه یافته، مثل امکان source routing در IPv4.0
  - Fragment header
    - برای نگهداری اطلاعات بسته های شکسته شده
  - Authentication header : احراز هویت بسته ها
  - Encapsulating Security Header : رمزنگاری بسته ها
  - Destination Options Header :
    - اطلاعاتی که ممکن است توسط گیرنده چک شود