Network Security

IP Security – Part 1

IP Security Overview

- 1994 – **RFC1636**, *“Security in the Internet Architecture”*
- Identified key needs:
  - Secure network infrastructure from unauthorized monitoring
  - Control network traffic
  - Secure end-to-end user traffic using encryption and authentication

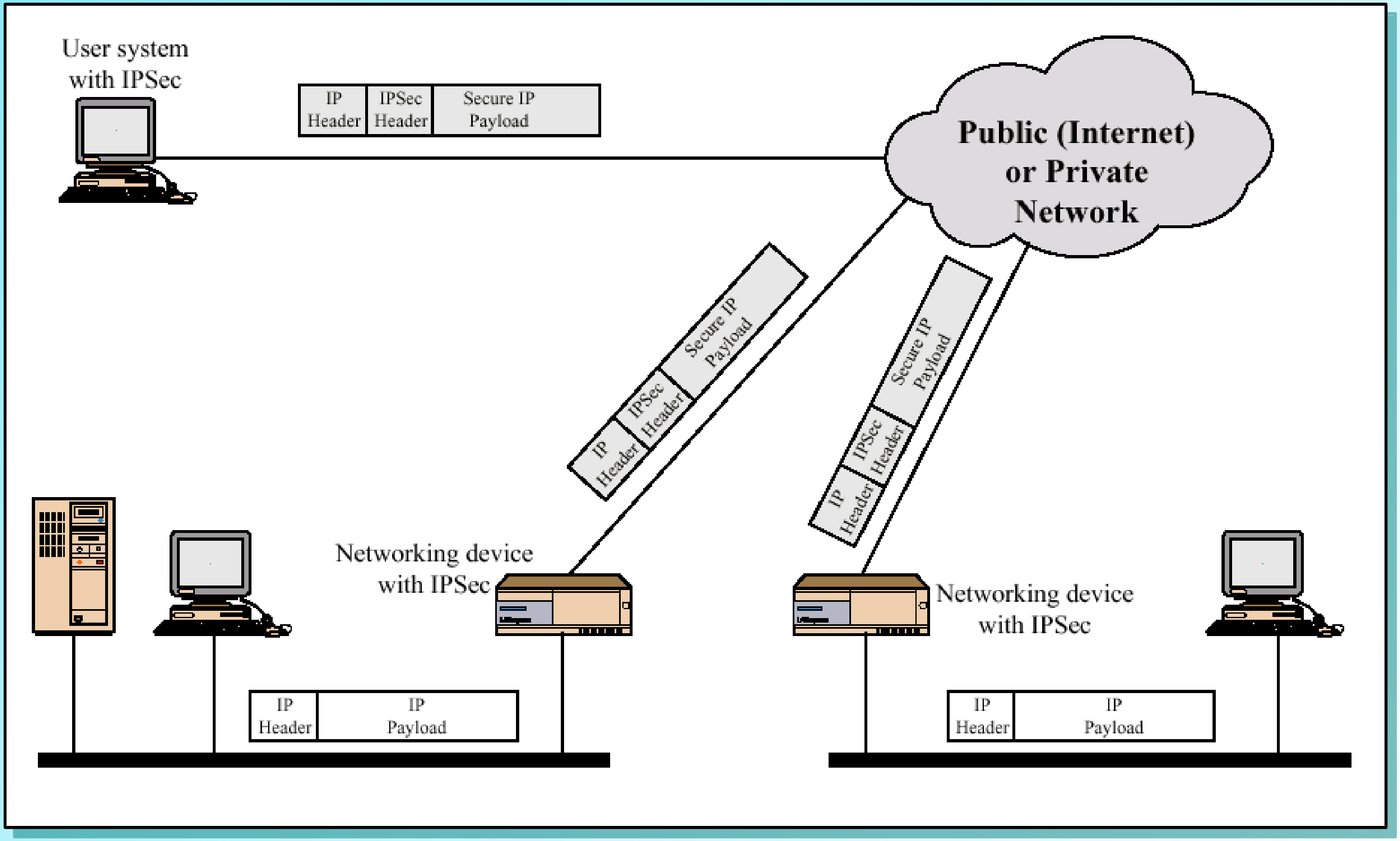
IP Security Overview

- CERT – most serious attacks are IP spoofing and eavesdropping/packet sniffing
- Next generation IP includes authentication and encryption
- **IPv6**
- **IPSec** $\subset$ IPv6
- Available with IPv4

Application of IPSec

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establish extranet and intranet connectivity with partners
- Enhance electronic commerce security

Application of IP Security



Benefits of IPSec

- Strong security for all traffic when crossing the perimeter (assuming it is implemented in a firewall or router)
- IPSec in a firewall is resistant to bypass
- Below the transport layer (TCP, UDP) and transparent to applications
- Transparent to the end user
- Provides security for individual users – offsite workers, VPN

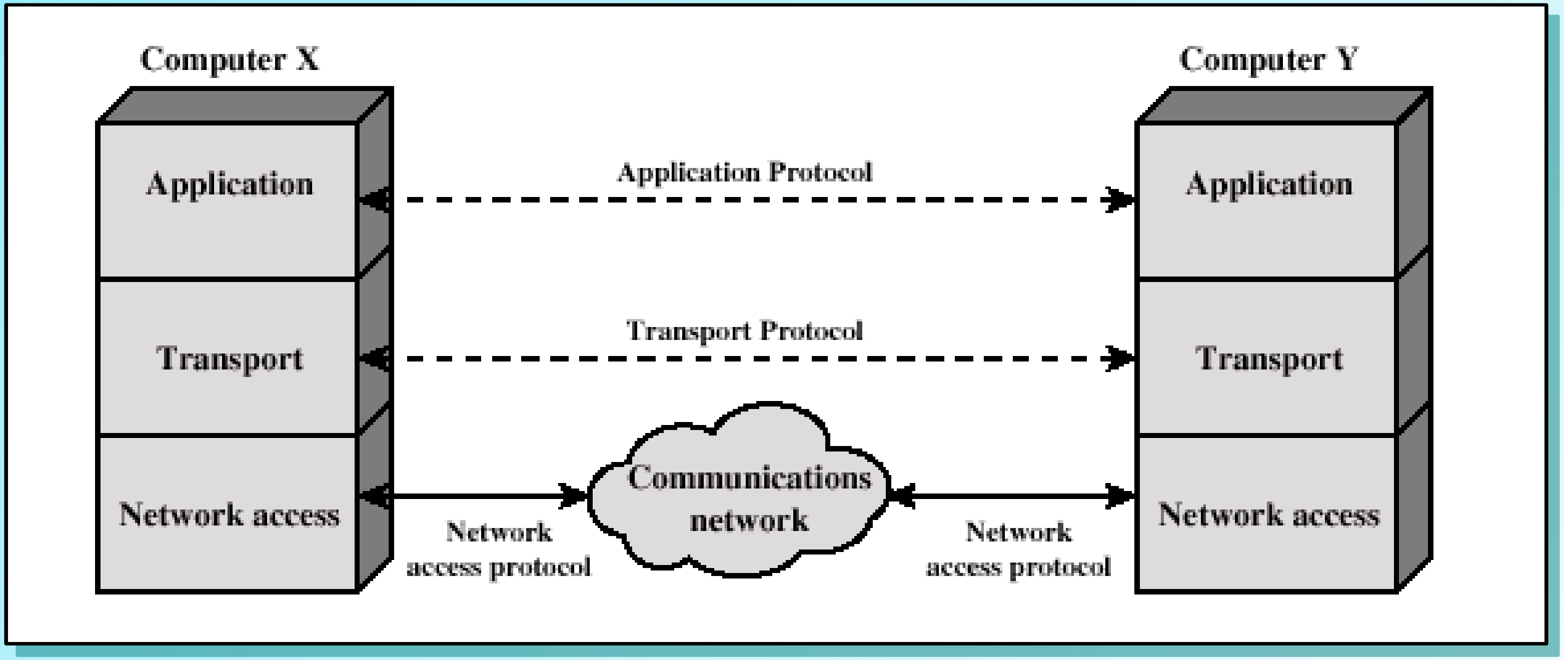
Routing & IPSec

- Router advertisement comes from an authorized router
- Neighbor advertisement comes from an authorized router
- Redirect comes from router to which initial packet was sent
- Routing updates are not forged
- Prevents disruption and diversion of traffic

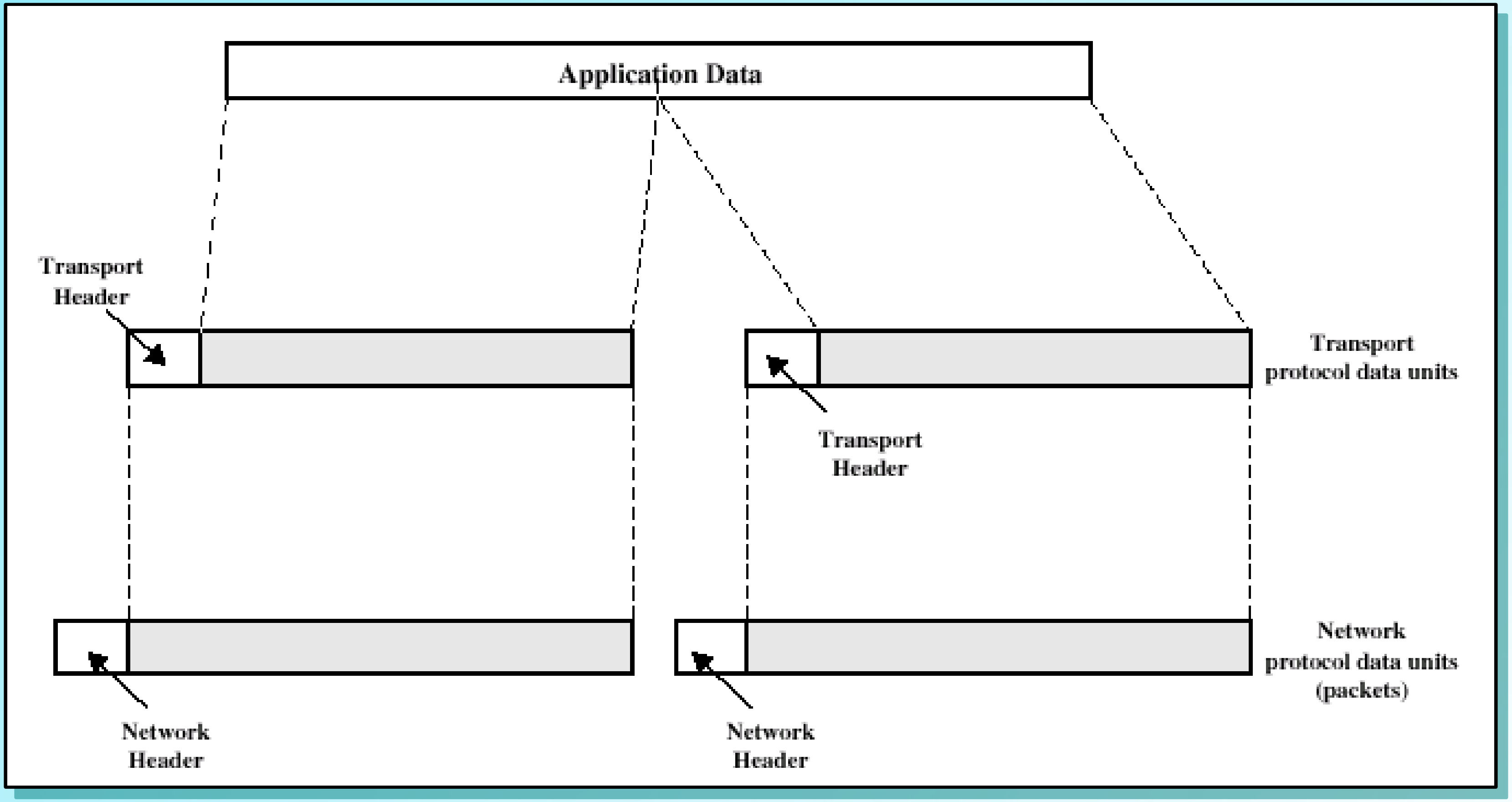
Network Security

Basic Networking – Part A

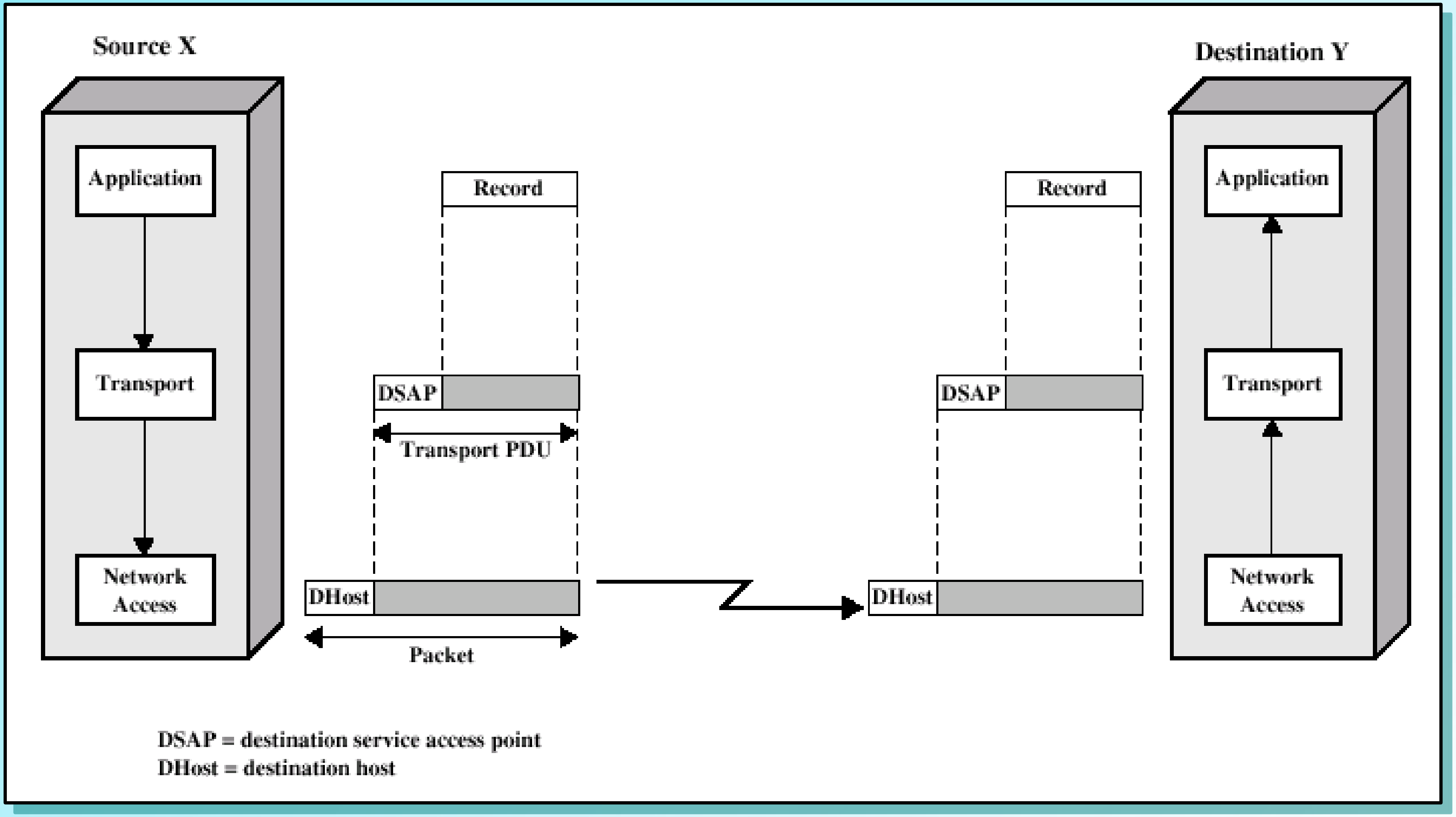
Protocols in a Simplified Architecture



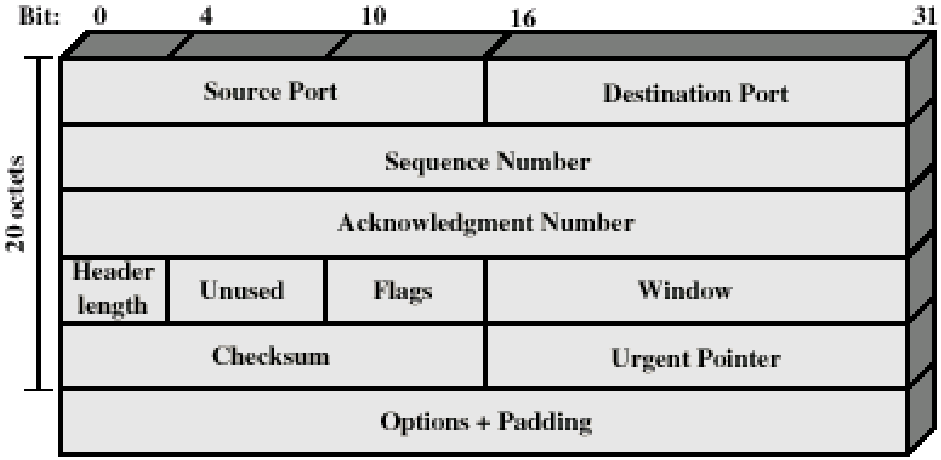
Protocol Data Units



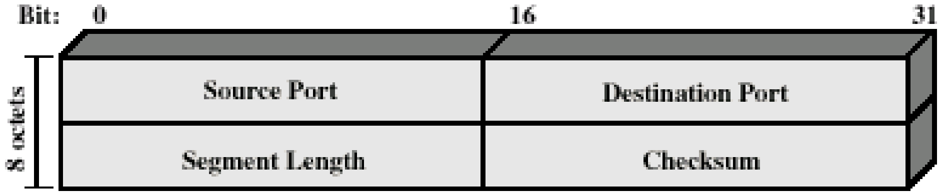
Operation of a Protocol Architecture



TCP and UDP Headers

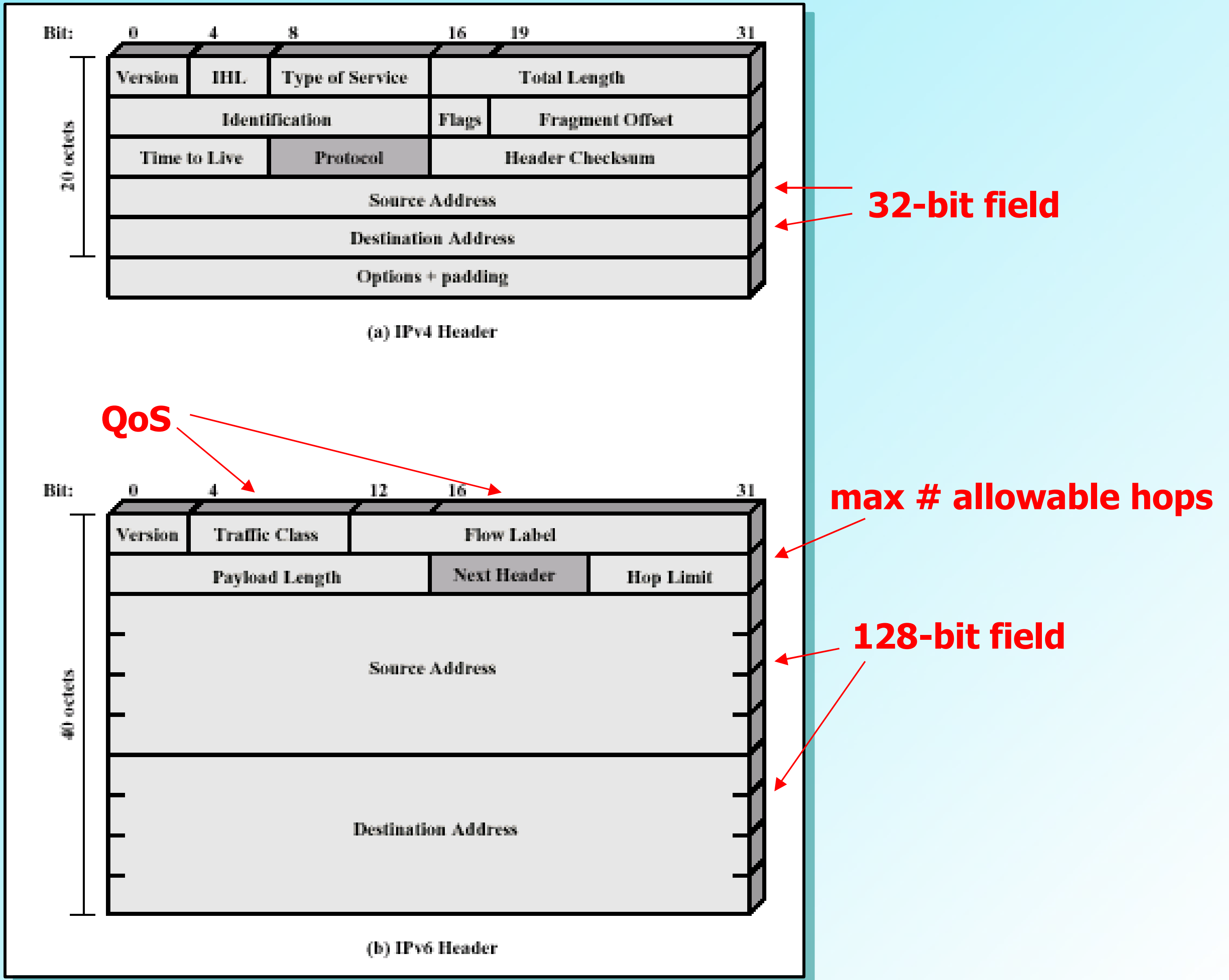


(a) TCP Header



(b) UDP Header

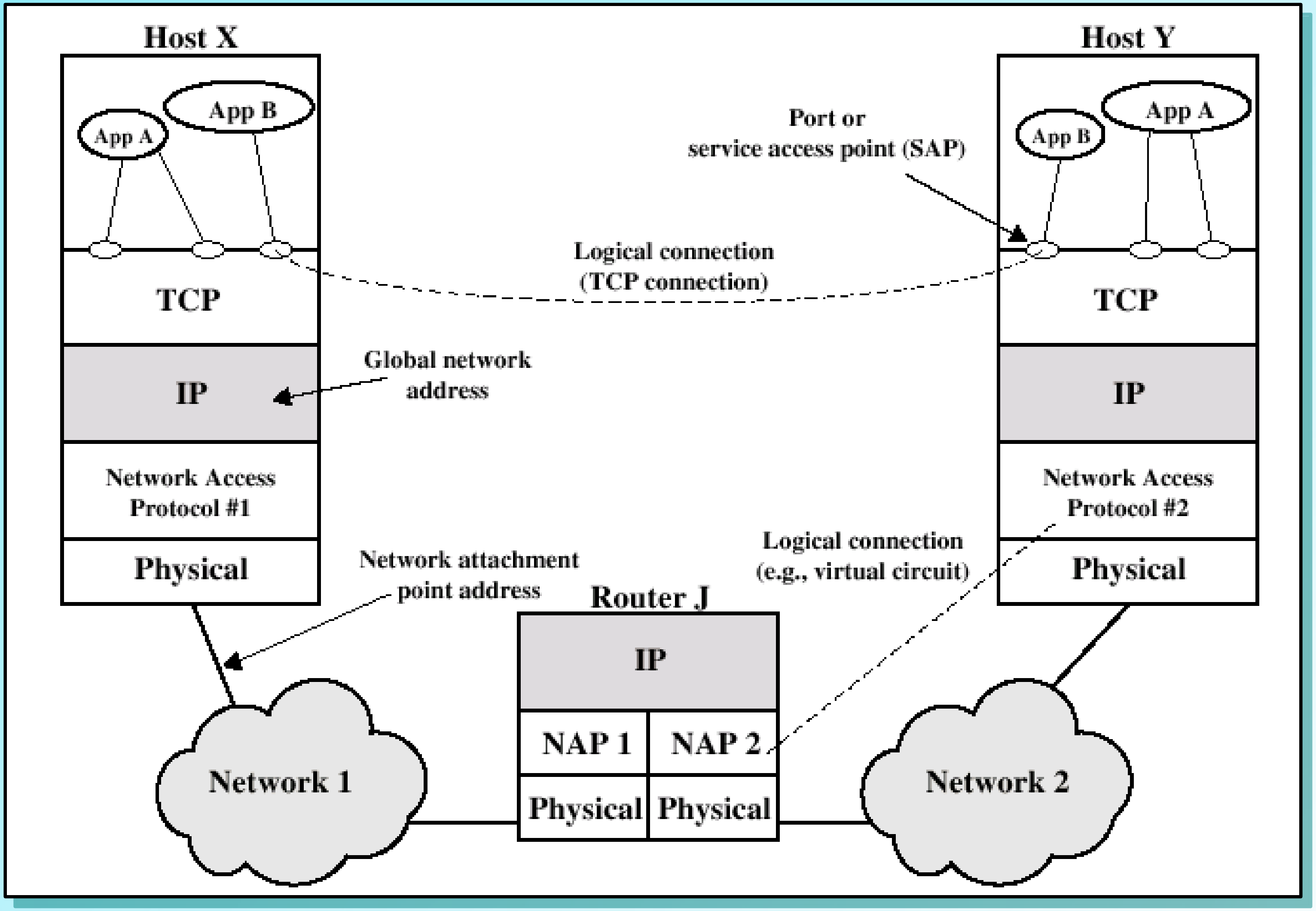
IP Headers



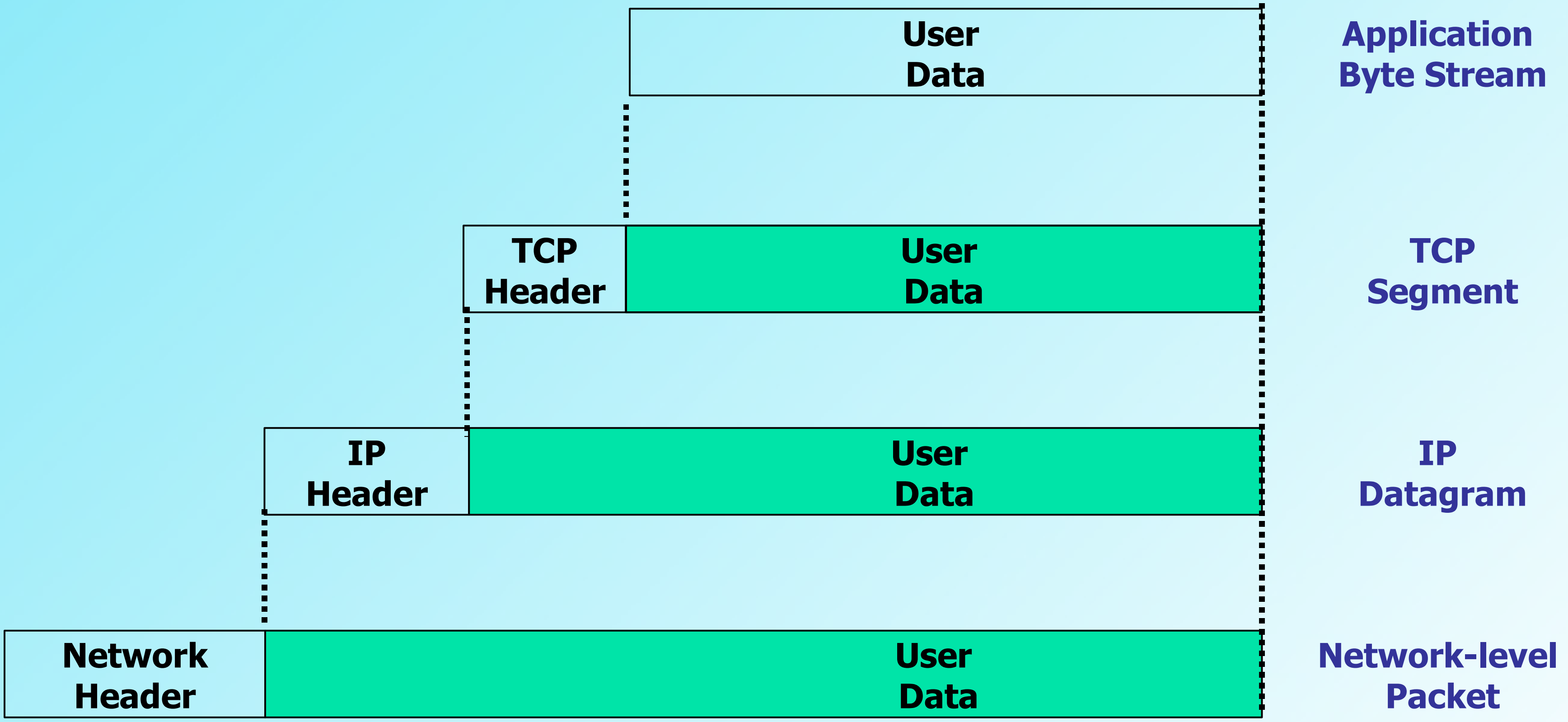
(a) IPv4 Header

(b) IPv6 Header

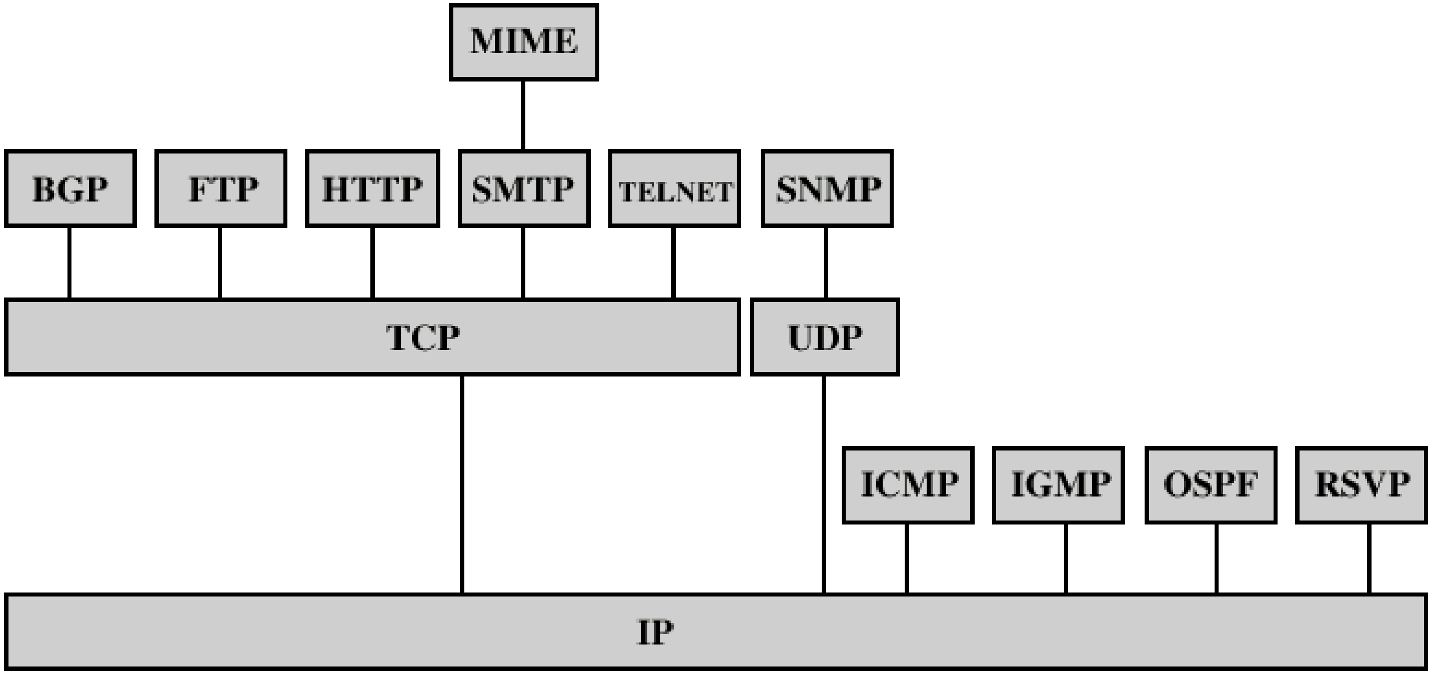
TP/IP Concepts



PDUs in TCP/IP



Some TCP/IP Protocols

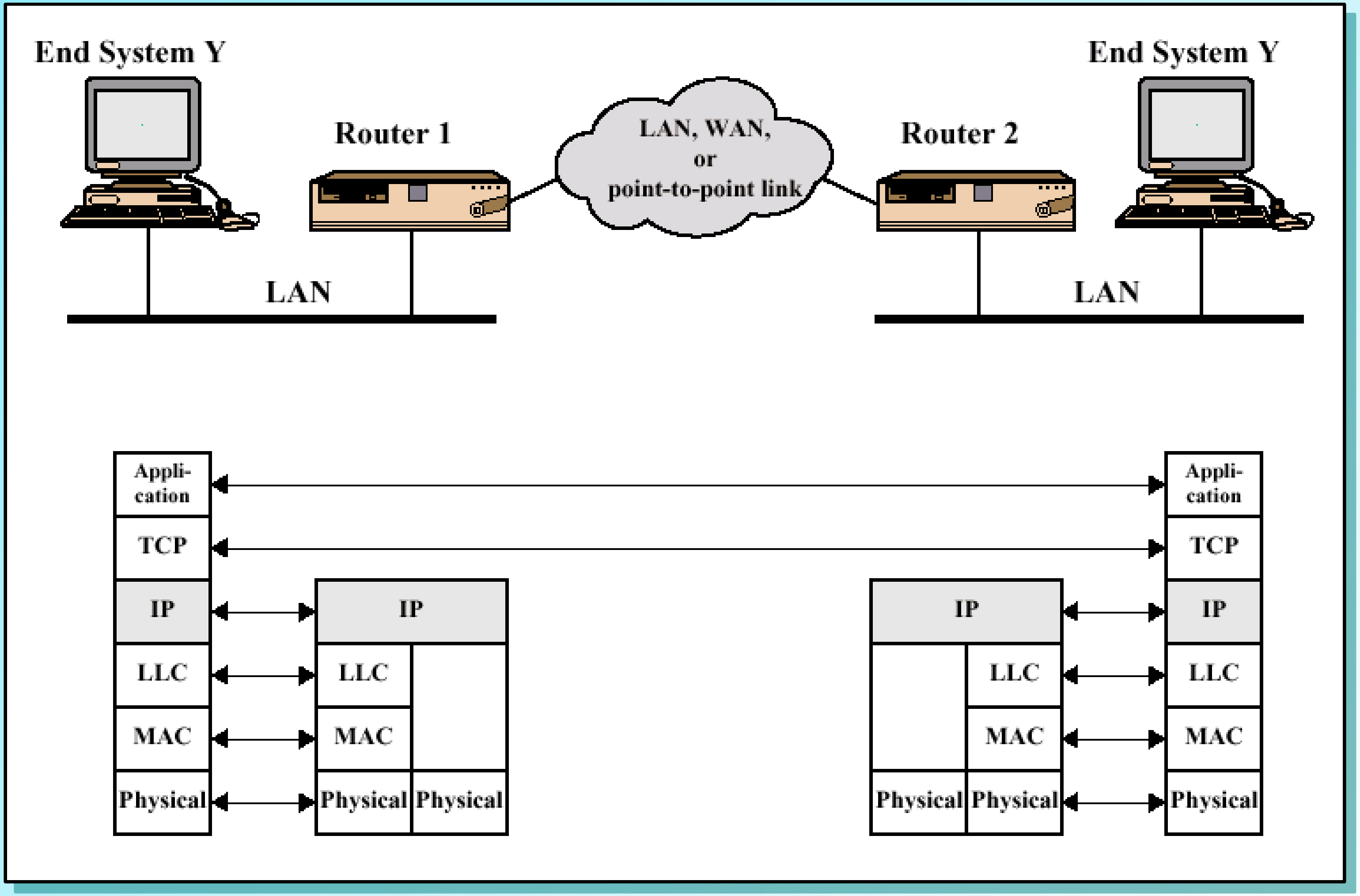


BGP	=	Border Gateway Protocol	OSPF	=	Open Shortest Path First
FTP	=	File Transfer Protocol	RSVP	=	Resource ReSerVation Protocol
HTTP	=	Hypertext Transfer Protocol	SMTP	=	Simple Mail Transfer Protocol
ICMP	=	Internet Control Message Protocol	SNMP	=	Simple Network Management Protocol
IGMP	=	Internet Group Management Protocol	TCP	=	Transmission Control Protocol
IP	=	Internet Protocol	UDP	=	User Datagram Protocol
MIME	=	Multi-Purpose Internet Mail Extension			

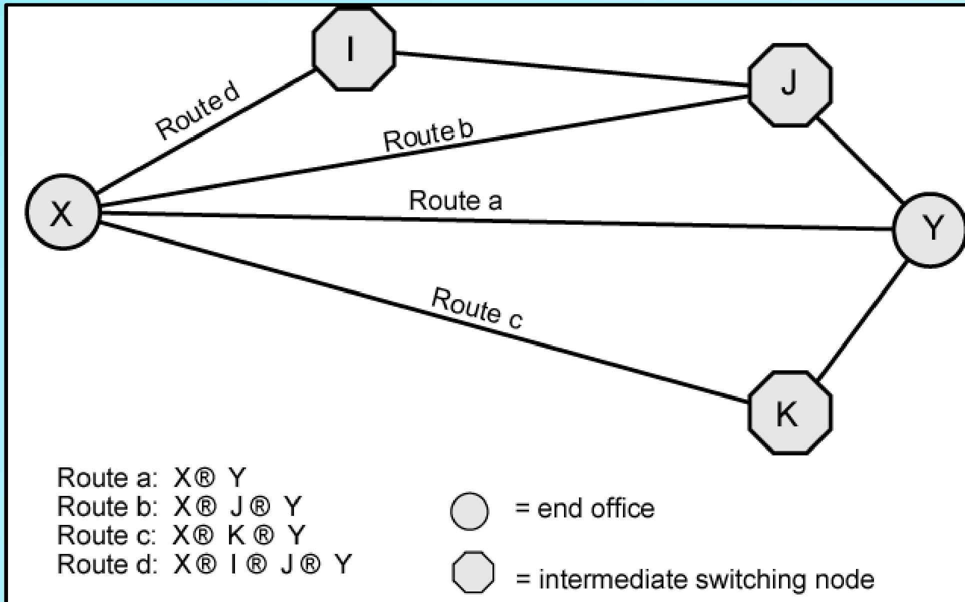
Assigned Port Numbers

Port	Service	Port	Service
7	echo	110	pop3
20	ftp-data	119	nntp
21	ftp	123	ntp
23	telnet	389	ldap
25	smtp	443	https
39	rip	500	isakmp
53	DNS	520	rip2
80	http	1812	radiusauth
88	kerberos	2049	Sun NFS

Configuration of TCP/IP



Alternate Routing Diagram



(a) Topology

Time Period	First route	Second route	Third route	Fourth and final route
Morning	a	b	c	d
Afternoon	a	d	b	c
Evening	a	d	c	b
Weekend	a	c	b	d

(b) Routing table

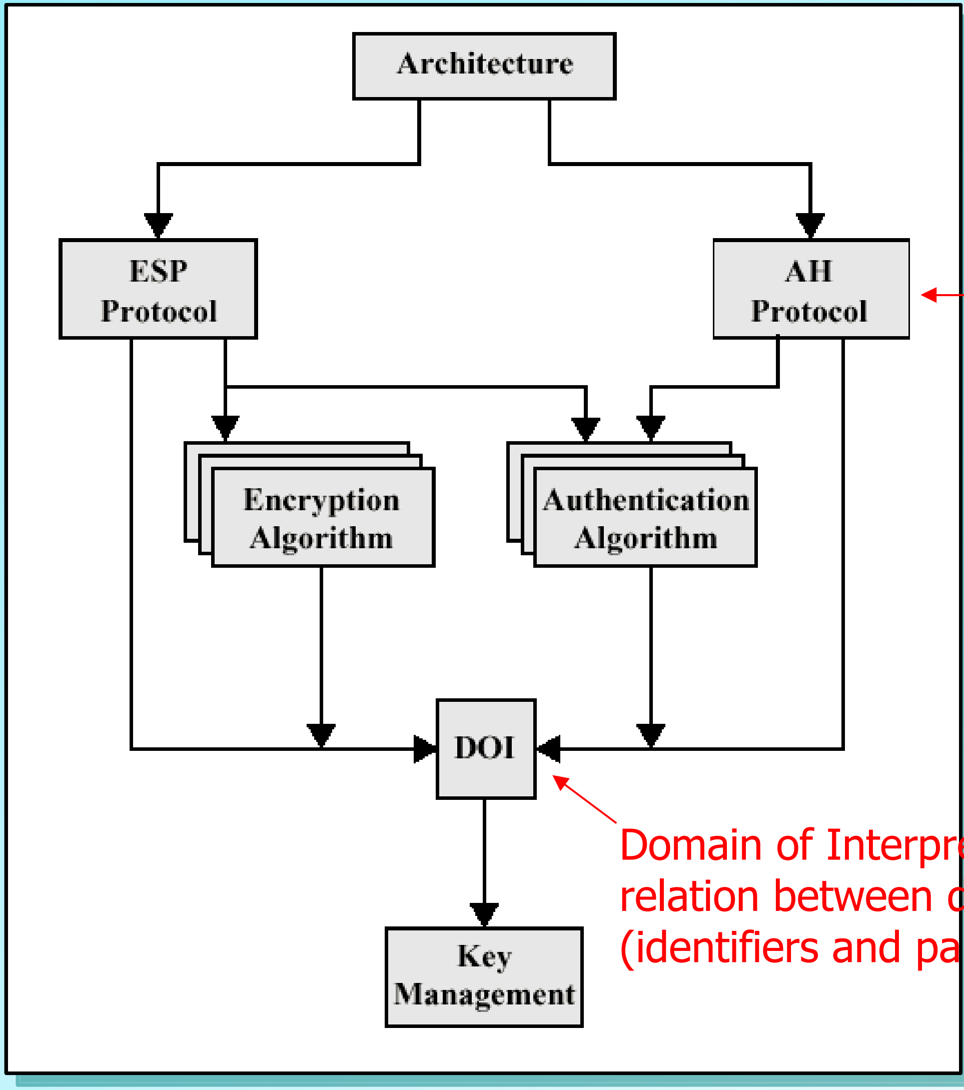
Network Security

IP Security – Part 1

IPSec Documents

- November - 1998
  - RFC 2401 – Overview
  - RFC 2402 – Packet Authentication Extension
  - RFC 2406 – Packet Encryption Extension
  - RFC 2408 – Key Management Capabilities
- *Implemented as extension headers that follow the main header:*
  - Authentication Header (AH)
  - Encapsulating Security Payload Header (ESP)

IPSec Documents



packet format

Domain of Interpretation
relation between documents
(identifiers and parameters)

IPSec Services

- Provides security services at the IP layer
- Enables a system to:
  - Select Required Security Protocols
  - Determine Algorithms To Use
  - Setup Needed Keys

IPSec Services – 2 Protocols

- Authentication protocol – designated by the authentication header (AH)
- Encryption/Authentication protocol – designated by the format of the packet, Encapsulating Security Payload (ESP); it is a mechanism for providing *integrity* and *confidentiality* to IP datagrams
- **AH** and **ESP** are vehicles for access control

IPSec Services

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

two cases

Security Associations

Key Concept:

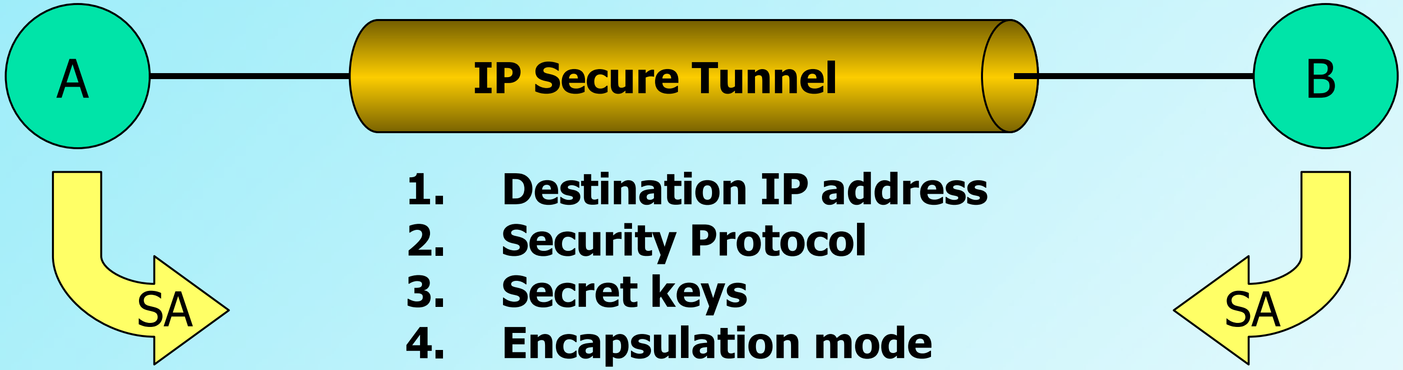
- Security Association (SA) – is a *one-way* relationship between a sender and a receiver that *defines the security services that are provided to a user*
- Requirements are stored in two databases: security policy database (SPD) and security association database (SAD)

Security Associations

Uniquely identified by:

- Destination IP address – address of the destination endpoint of the SA (end user system or firewall/router)
- Security protocol – whether association is AH or ESP. Defines key size, lifetime and crypto algorithms (transforms)
- Security parameter index (SPI) – bit string that provides the receiving device with info on how to process the incoming traffic

Security Associations



1. Destination IP address
2. Security Protocol
3. Secret keys
4. Encapsulation mode
5. SPI

Security Associations

- SA is unidirectional
- It defines the operations that occur in the transmission in one direction only
- Bi-directional transport of traffic requires a pair of SAs (e.g., secure tunnel)
- Two SAs use the same meta-characteristics but employ different keys

Security Association Database

- Each IPSec implementation has a Security Association Database (SAD)
- SAD defines the parameters association (SPI) with each SA
- SAD stores pairs of SA, since SAs are unidirectional

Security Association Database

- Sequence number counter
- Sequence counter overflow
- Anti-replay window
- AH information
- ESP information
- Lifetime of this SA
- IPSec protocol mode – tunnel, transport, wildcard
- Path MTU

Security Policy Database

- Provides considerable flexibility in way IPSec services are applied to IP traffic
- Can discriminate between traffic that is afforded IPSec protection and traffic allowed to bypass IPSec
- The Security Policy Database (SPD) is the means by which IP traffic is related to specific SAs

Security Policy Database

- Each entry defines a subset of IP traffic and points to an SA for that traffic
- These selectors are used to filter outgoing traffic in order to map it into a particular SA

Security Policy Database

- Destination IP address
- Source IP address
- User ID
- Data sensitivity level – secret or unclassified
- Transport layer protocol
- IPSec protocol – AH or ESP or AH/ESP
- Source and destination ports
- IPv6 class
- IPv6 flow label
- IPv4 type of service (TOS)

Security Policy Database

Outbound processing of packet:

1) Compare fields in the packet to find a matching SPD entry
2) Determine the SA and its associated SPI
3) Do the required IPSec processing

Transport and Tunnel Modes

- SA supports two modes:

  Transport – protection for the upper layer protocols

  Tunnel – protection for the entire IP packet

Transport Mode

- Protection extends to the payload of an IP packet
- Primarily for upper layer protocols – TCP, UDP, ICMP
- Mostly used for end-to-end communication
- For AH or ESP the payload is the data following the IP header (IPv4) and IPv6 extensions
- Encrypts and/or authenticates the payload, but *not the IP header*

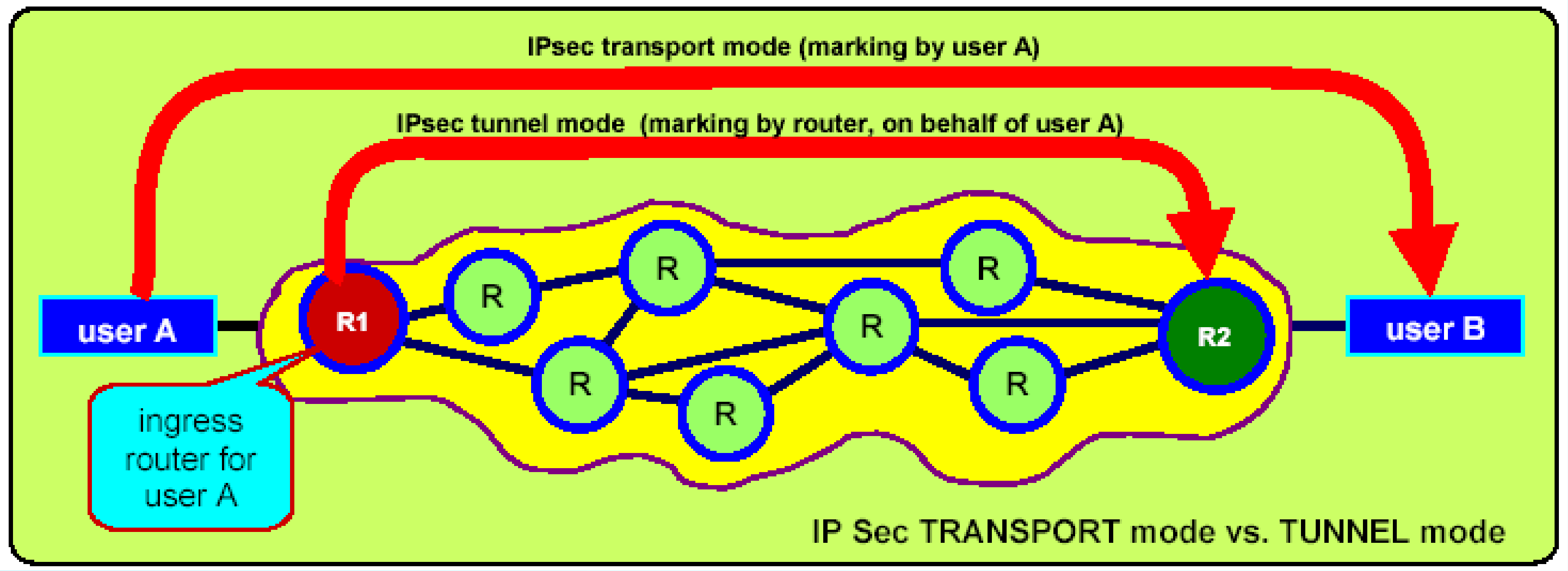
Tunnel Mode

- Protection for the entire packet
- Add new *outer* IP packet with a new outer header
- AH or ESP fields are added to the IP packet and entire packet is treated as payload of the outer packet
- Packet travels through a *tunnel* from point to point in the network

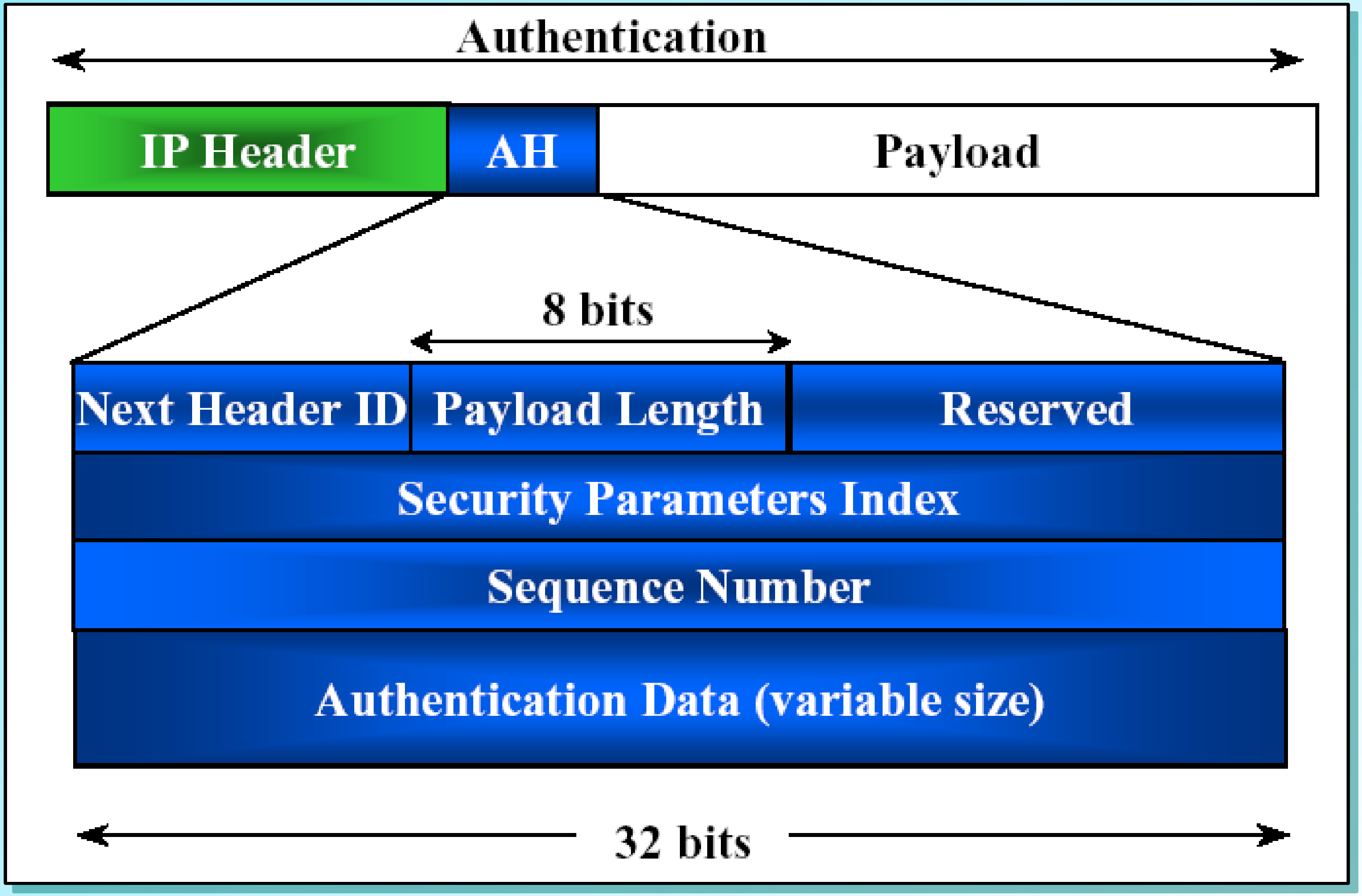
Tunnel and Transport Mode

	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 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 inner IP packet. Authenticates inner IP packet.

Transport vs Tunnel Mode



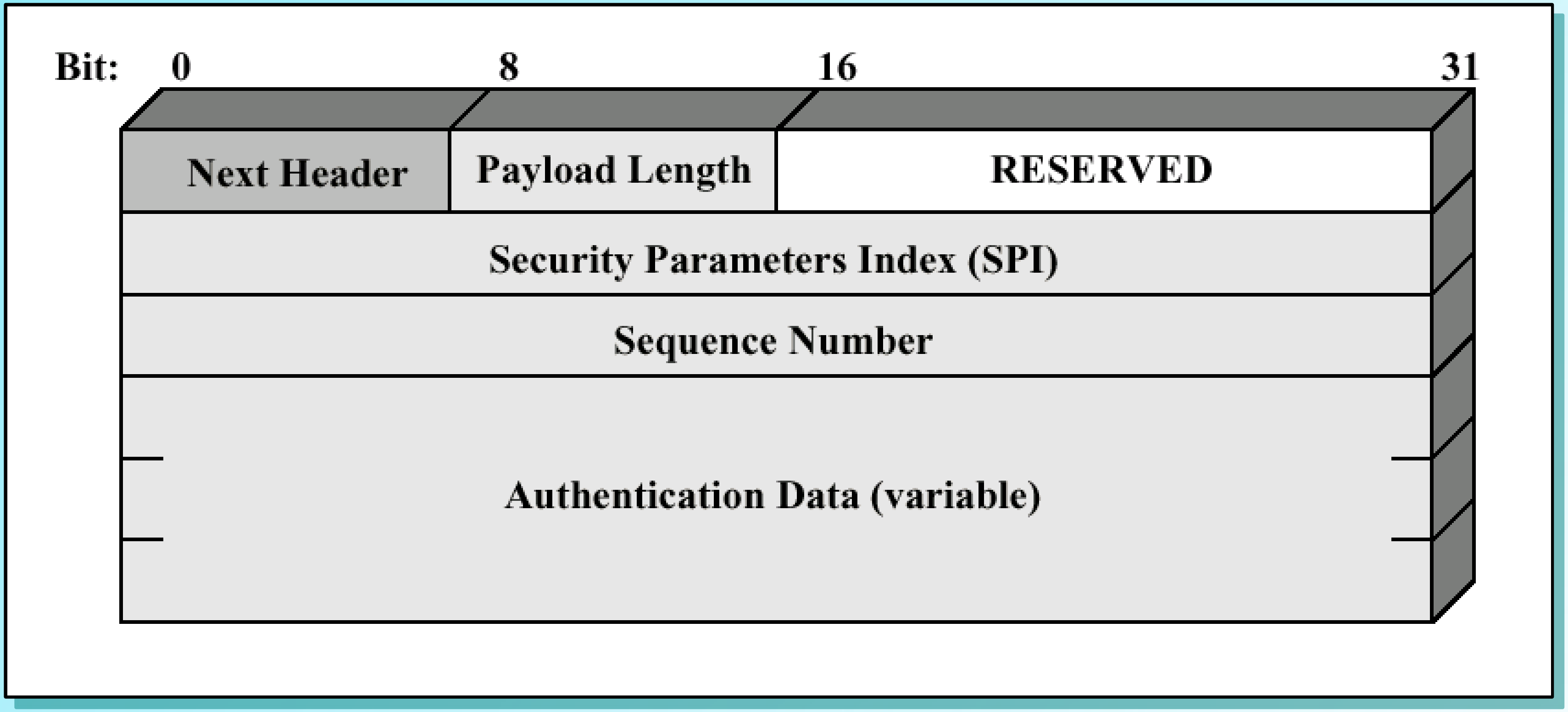
Authentication Header



Authentication Header

- Provides support for data integrity and authentication of IP packets
- Undetected modification in transit is impossible
- Authenticate the user or application and filters traffic accordingly
- Prevents address spoofing attacks
- Guards against replay attacks
- Based on the use of a message authentication code (MAC) so two parties must share a key

IPSec Authentication Header



Authentication Header

- Next header – type of header following
- Payload length – length of AH
- Reserved – future use
- Security Parameters Index – idents SA
- Sequence Number – 32bit counter
- Authentication data – variable field that contains the Integrity Check Value (ICV), or MAC

Anti-Replay Service

- Replay Attack: Obtain a copy of authenticated packet and later transmit to the intended destination
- Mainly disrupts service
- Sequence number is designed to prevent this type of attack

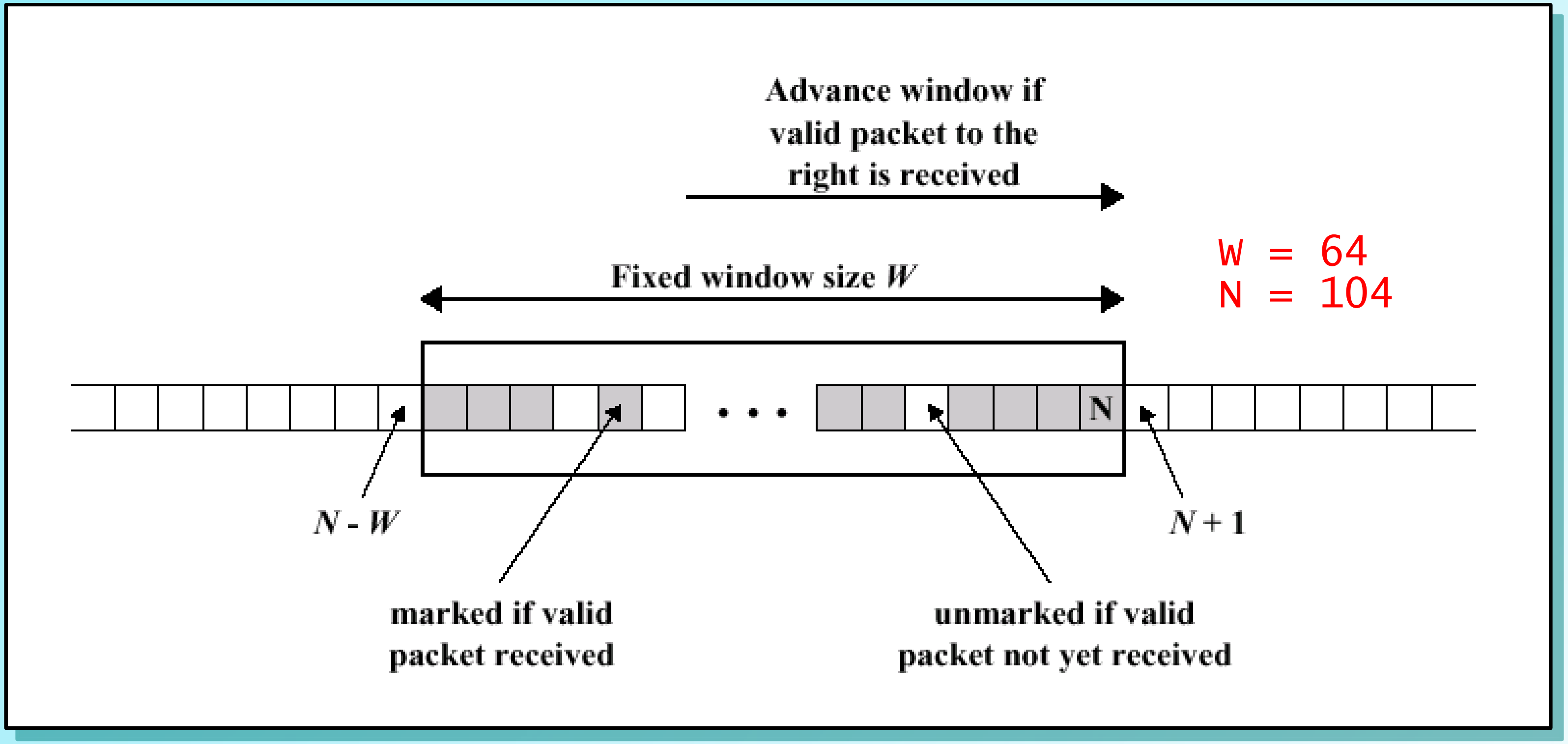
Anti-Replay Service

- **Sender** initializes seq num counter to 0 and increments as each packet is sent
- Seq num < 2^{32}; otherwise new SA
- IP is connectionless, unreliable service
- **Receiver** implements window of W
- Right edge of window is highest seq num, N, received so far

Anti-Replay Service

- Received packet within window & new, check MAC, if authenticated mark slot
- Packet to the right of window, do check/mark & advance window to new seq num which is the new right edge
- Packet to the left, or authentication fails, discard packet, & flag event

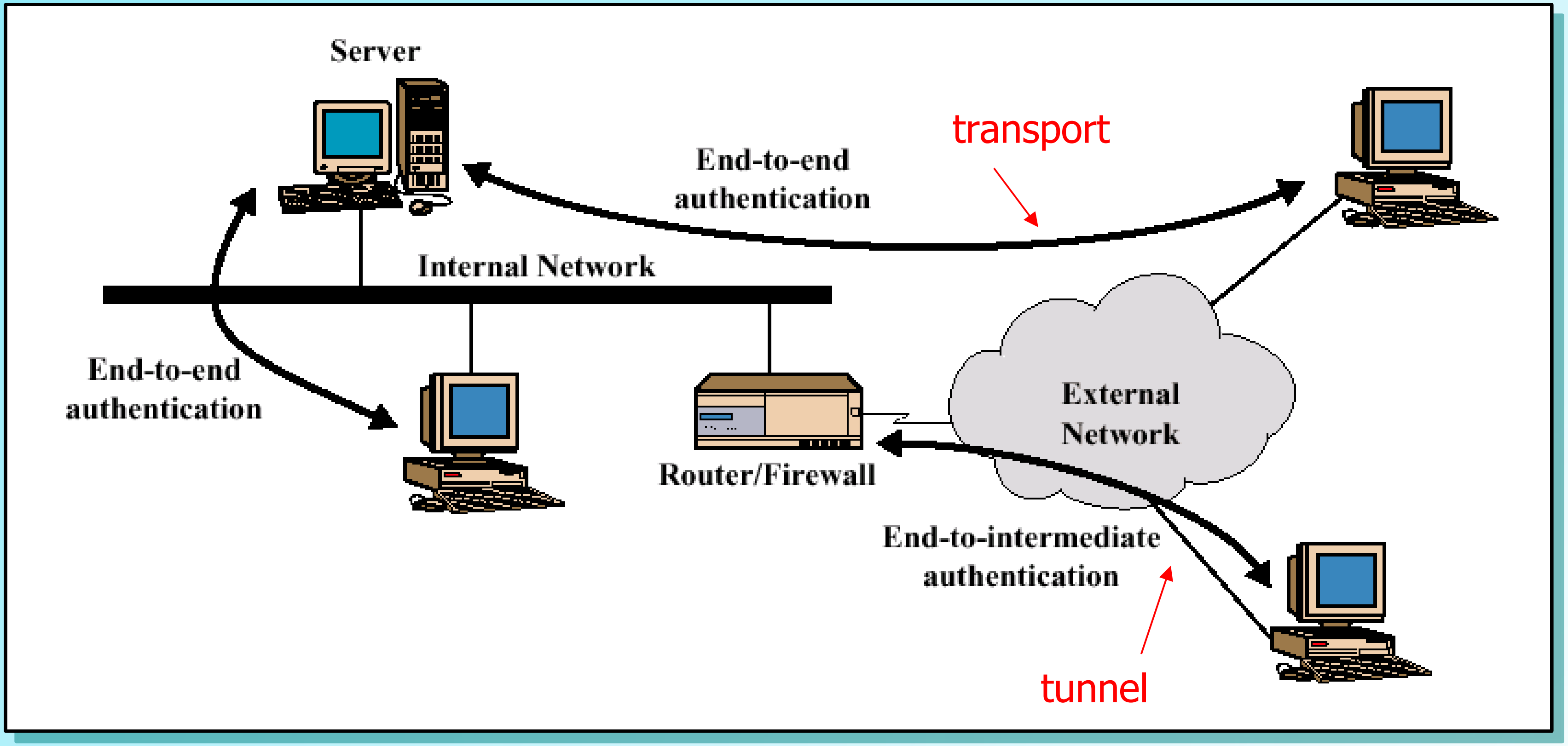
Anti-Replay Mechanism



Integrity Check Value

- Held in the Authentication Data field
- ICV is a Message Authentication Code (MAC)
- Truncated version of a code produced by a MAC algorithm
- HMAC value is calculated but only first 96 bits are used
  - HMAC-MD5-96
  - HMAC-SHA-1-96
- MAC is calculated over an immutable field, e.g., source address in IPv4

End-to-end Authentication



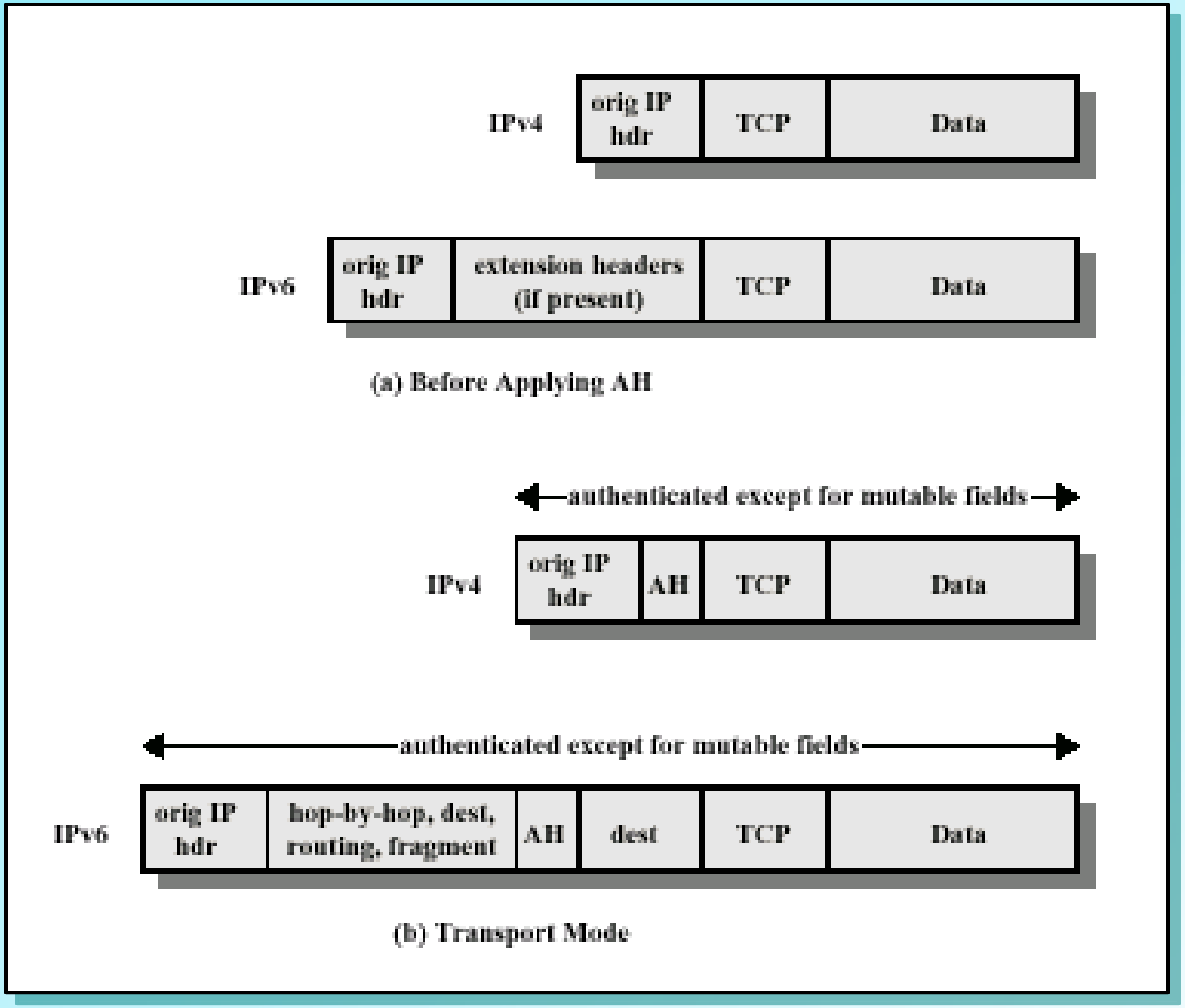
Two Ways To Use IPSec Authentication Service

AH Tunnel and Transport Modes

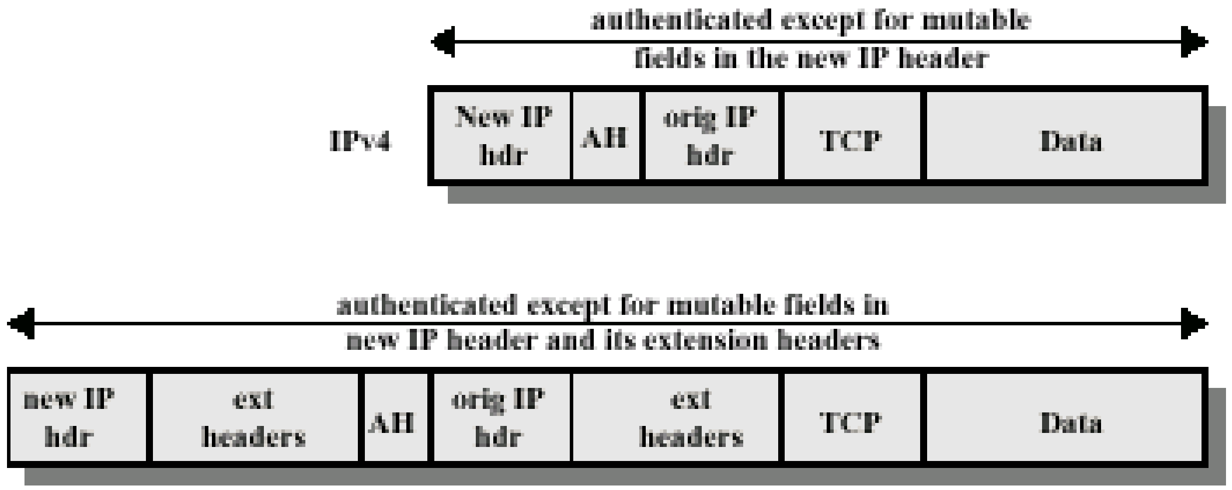
- Considerations are different for IPv4 and IPv6
- Authentication covers the entire packet
- Mutable fields are set to 0 for MAC calculation

What's a mutable field?

Scope of AH Authentication



Scope of AH Authentication



(c) Tunnel Mode

Important URLs

- www.rfc-editor.org - Search for RFC 1636, Security in the Internet Architecture, and other RFCs related to IPSec
- http://en.wikipedia.org/wiki/IPV6 - Great info and links related to IPv6
- http://www.ipv6tf.org/ - This portal has lots of news and info about IPv6

Important URLs

- http://www.ipv6.org/
  Includes introductory material, news on recent IPv6 product developments, and related links.

- www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf
  Very good TCP/IP Tutorial from IBM Redbook Series with a good section (chap. 5) on security

Homework

- Read Chapter Six, Sections 6.1-6.3
- **Mid-Term Exam (take home) will be given next class**
- Submit topic for term paper

Assignment 2

- Obtain PGP software and install it
- Send me an email (vcosta@optonline.net) and your public key

Have A Good Week

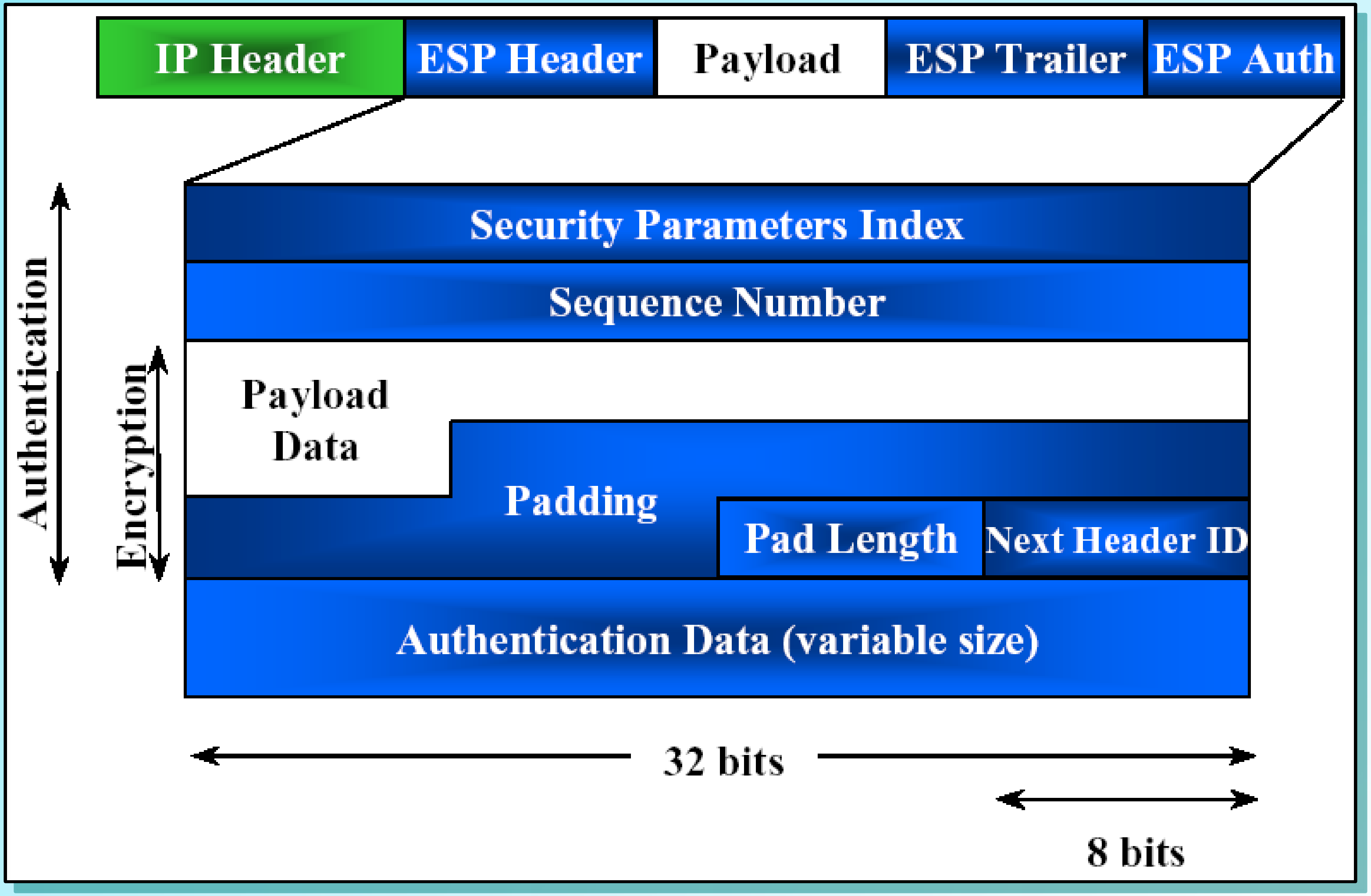
Network Security

IP Security – Part 2

Encapsulating Security Payload

- Provides confidentiality services
- Confidentiality of message contents and limited traffic flow confidentiality
- ESP can also provide the same authentication services as AH

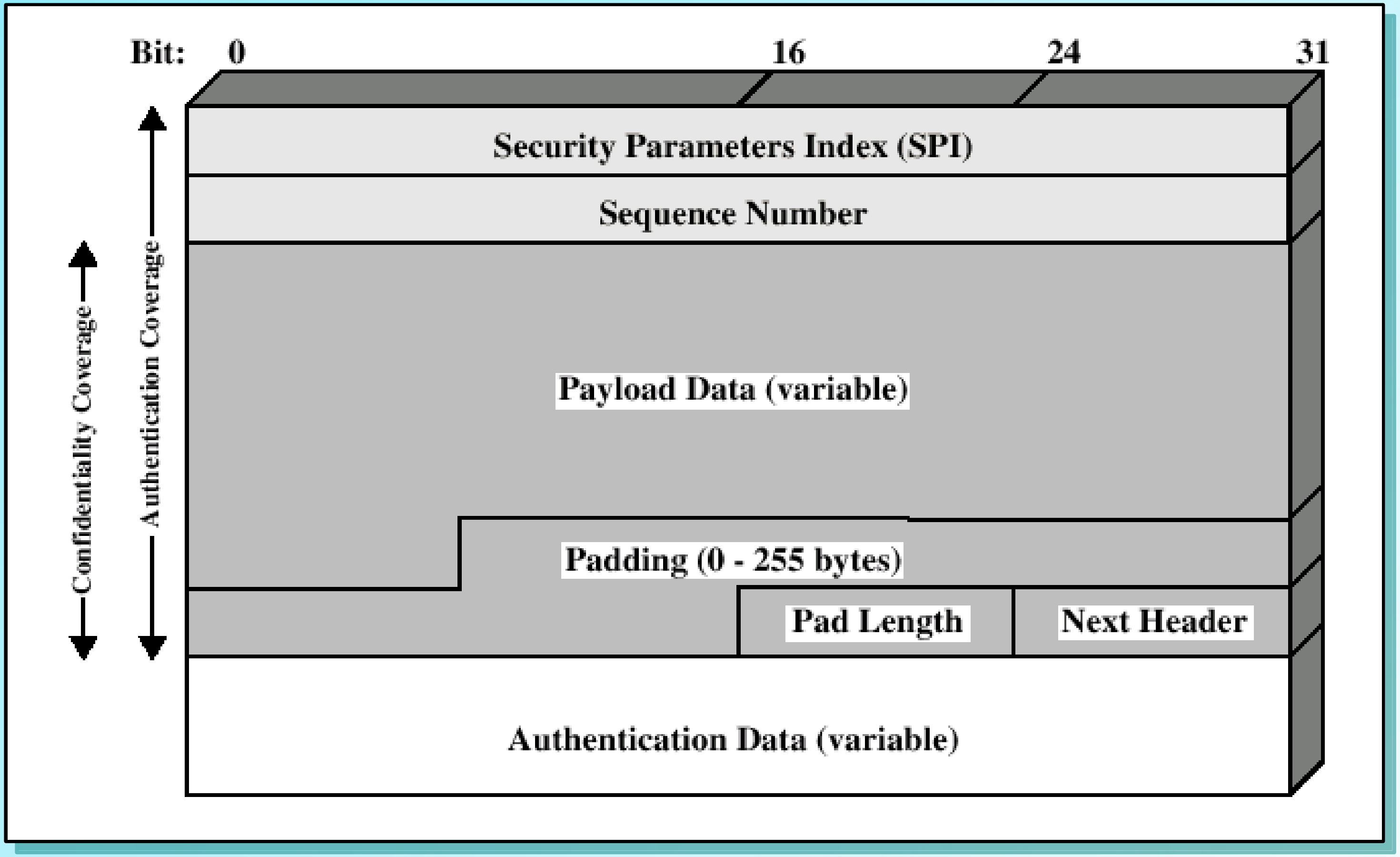
Encapsulating Security Payload



Encapsulating Security Payload

- Security Parameters Index – idents SA
- Sequence Number – 32bit counter
- Payload Data – variable field protected by encryption
- Padding – 0 to 255 bytes
- Pad Length – number of bytes in preceding
- Next header – type of header following
- Authentication data – variable field that contains the Integrity Check Value (ICV)

IPSec ESP Format



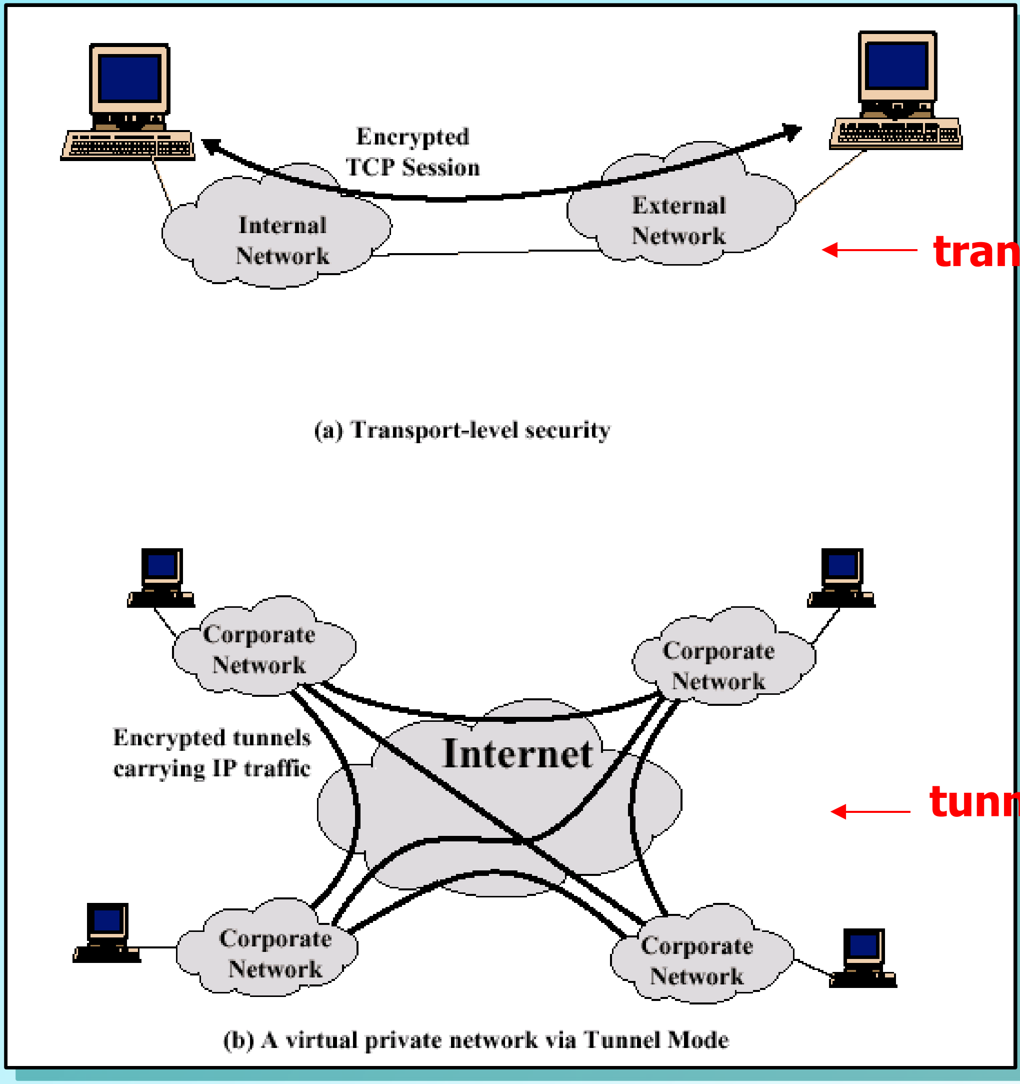
ESP and AH Algorithms

- Implementation must support DES in cipher block chaining (CBC) mode
- Other algorithms have been assigned identifiers in the DOI document
- Others: 3DES, PC5, IDA, 3IDEA, CAST, Blowfish
- ESP support use of a 96bit MAC similar to AH

ESP Padding

- Algorithm may require plaintext to be a multiple of some number of bytes
- Pad Length and Next Header must be right aligned
- Additional padding may be used to conceal actual length of the payload

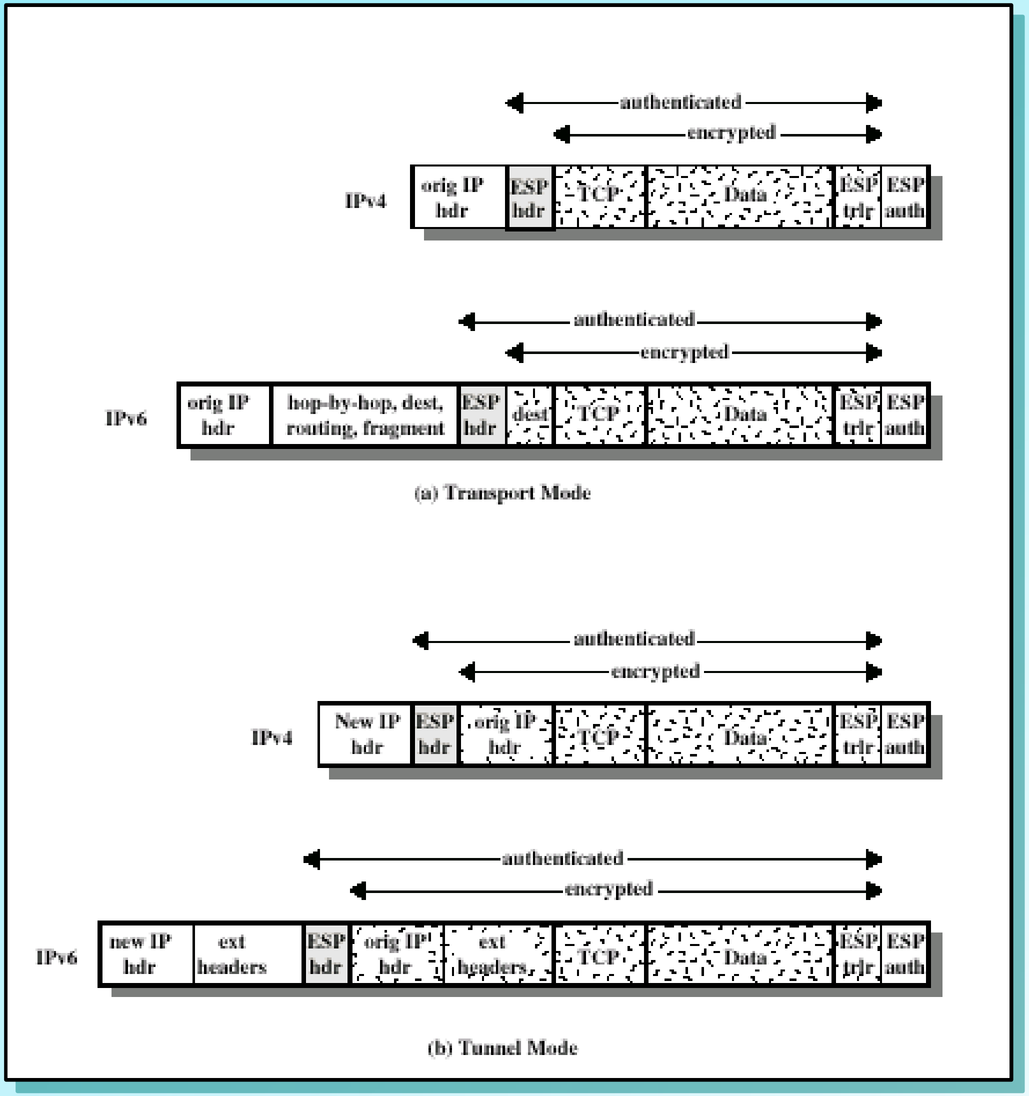
Transport vs Tunnel Mode



transport mode

tunnel mode

Scope of ESP Encryption



Combining SAs

- SA can implement *either* AH *or* ESP protocol, *but not both*
- Traffic flow may require separate IPSec services between hosts
- Security Association Bundle refers to a sequence of SAs
- SAs in a bundle may terminate at different end points

Combining SAs

SAs many combine into bundles in two ways:

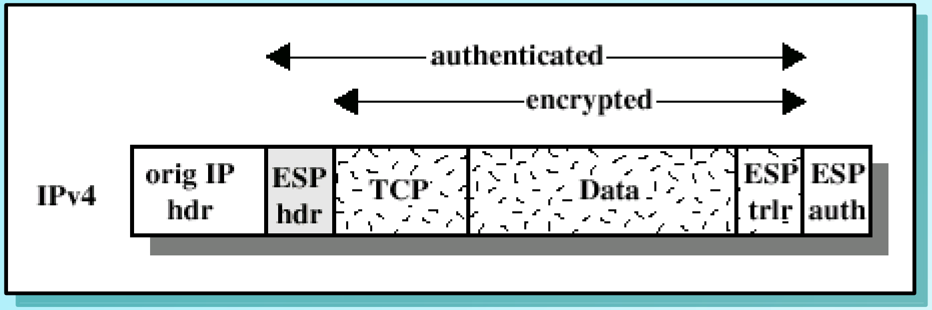
- Transport adjacency – applying more than one security protocol to the same IP packet without invoking tunneling; only one level of combination, no nesting
- Iterated tunneling – application of mutltiple layers of security protocols effected through IP tunneling; multiple layers of nesting

Authentication + Encryption

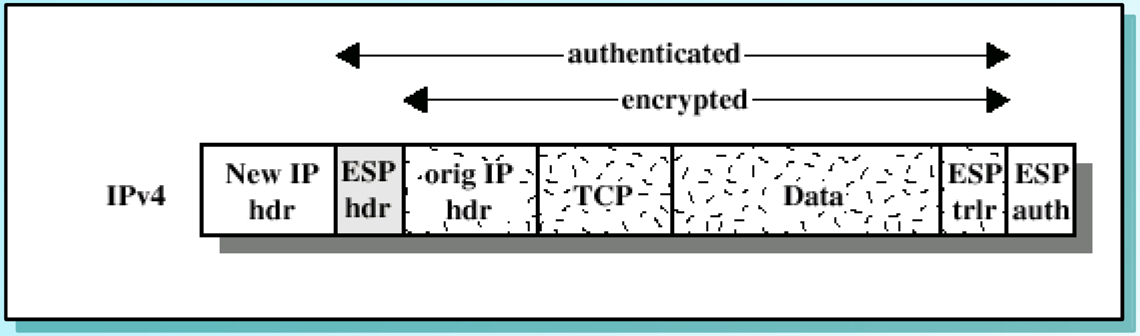
- Several approaches to combining authentication and confidentiality
- ESP with Authentication Option
  - First apply ESP then append the authentication data field
  - Authentication applies to ciphertext rather than plaintext

Authentication + Encryption

- ESP with Authentication Option



Transport Mode



Tunnel Mode

Authentication + Encryption

- Transport Adjacency
  - Use two bundled transport SAs
  - Inner being an ESP SA; outer being an AH SA
  - Authentication covers the ESP plus the original IP header
  - *Advantage*: authentication covers more fields, including source and destination IP addresses

Authentication + Encryption

- Transport-Tunnel Bundle
  - First apply authentication, then encryption
  - Authenticated data is protected and easier to store and retrieve
  - Use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  - *Advantage*: entire authenticated inner packet is encrypted and a new outer IP header is added

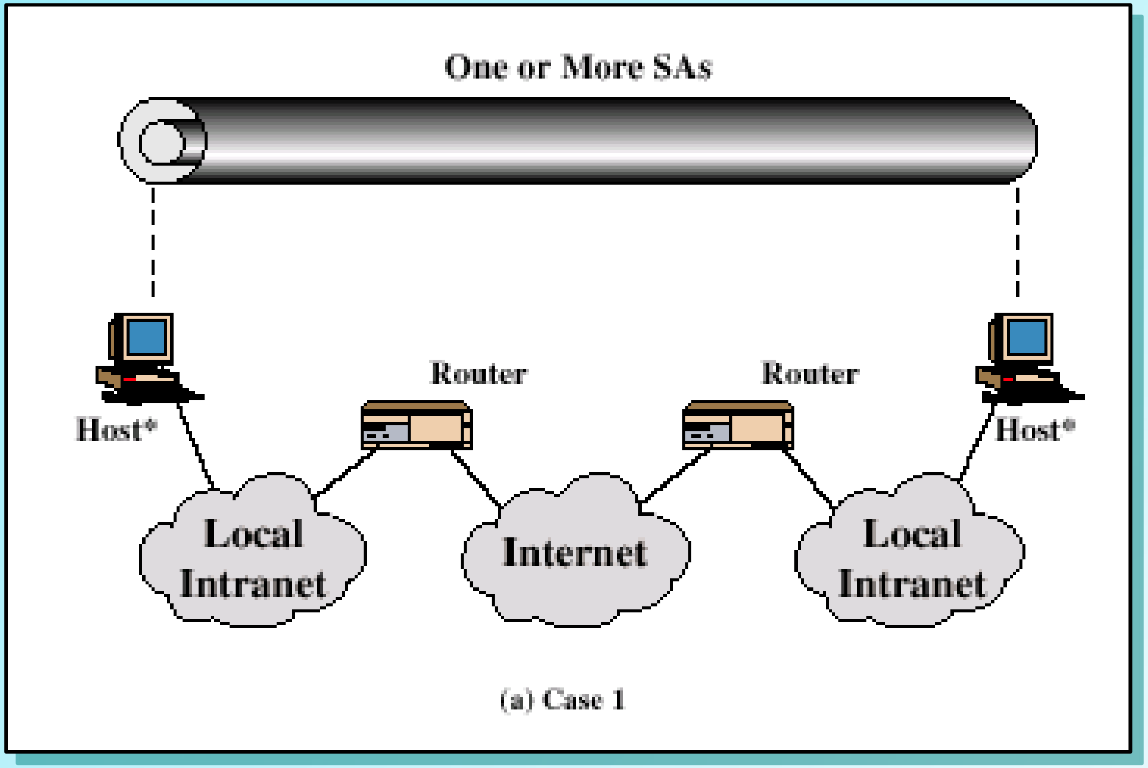
Basic Combinations

- IPSec architecture lists four examples that must be supported in an implementation
- Figures represent the logical and physical connectivity
- Each SA can be either AH or ESP
- Host-to-host SAs are either transport or tunnel, otherwise it must be tunnel mode

Basic Combinations – Case 1

- All security is provided between end systems that implement IPSec
- Possible combinations
  a. AH in transport mode
  b. ESP in transport mode
  c. AH followed by ESP in transport mode (an AH SA inside an ESP SA)
  d. Any one of a, b, or c inside and AH or ESP in tunnel mode

Basic Combinations – Case 1

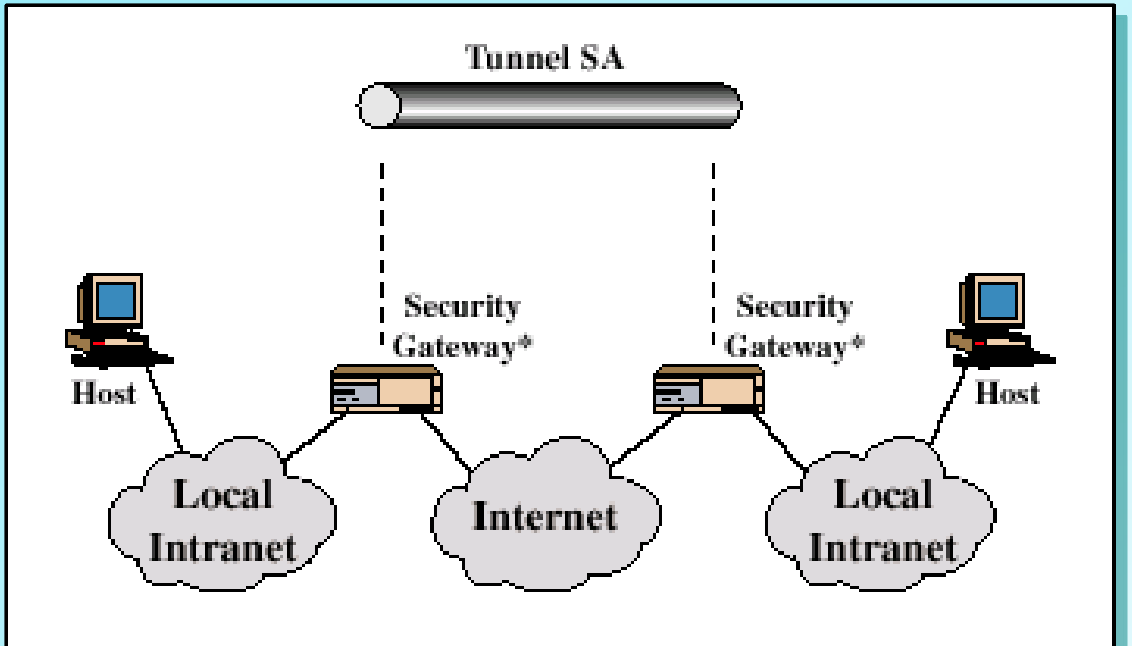


* = implements IPSec

Basic Combinations – Case 2

- Security is provided only between gateways and no hosts implement IPSec
- VPN – Virtual Private Network
- Only single tunnel needed (support AH, ESP or ESP w/auth)

Basic Combinations – Case 2



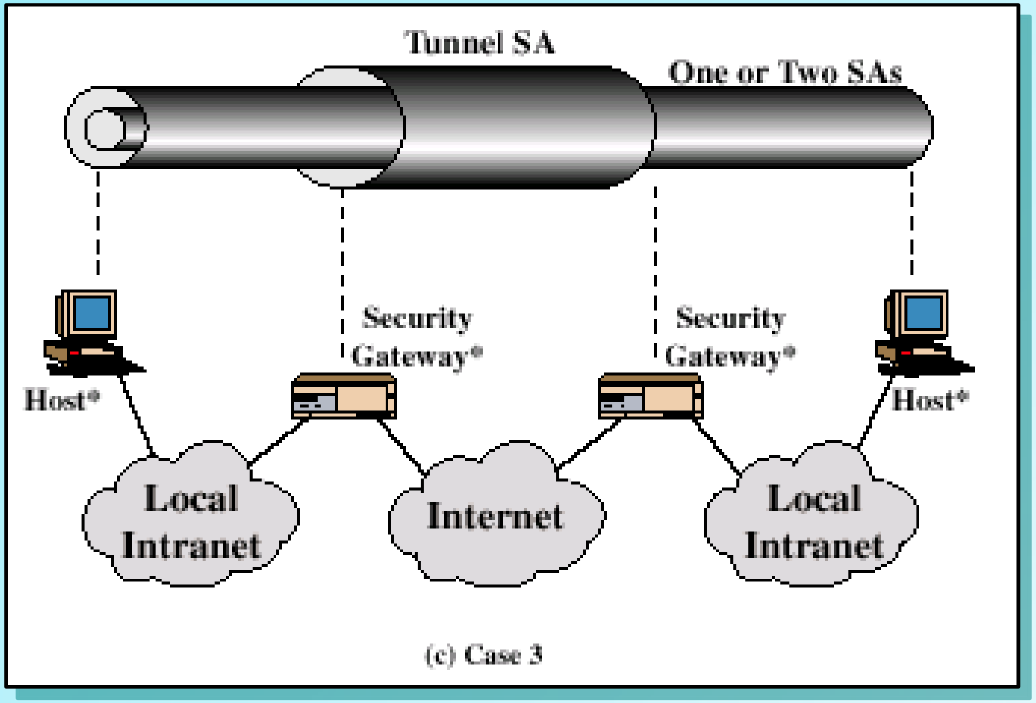
(b) Case 2

* = implements IPSec

Basic Combinations – Case 3

- Builds on Case 2 by adding end-to-end security
- Gateway-to-gateway tunnel is ESP
- Individual hosts can implement additional IPSec services via end-to-end SAs

Basic Combinations – Case 3

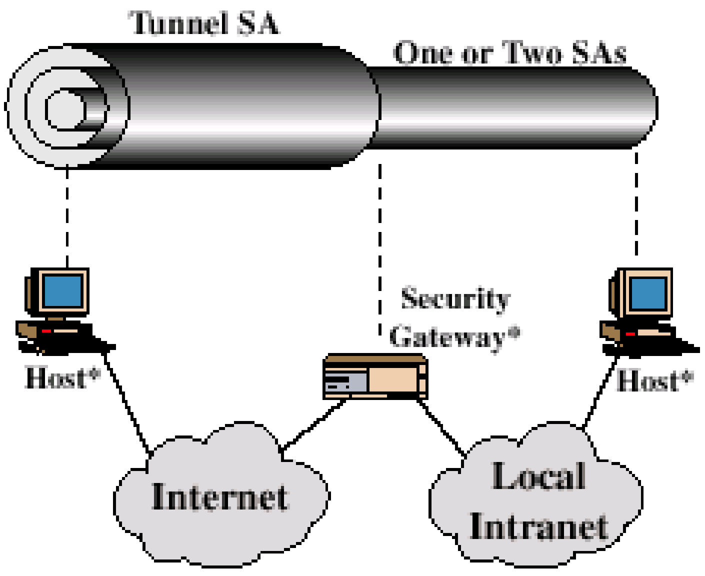


* = implements IPSec

Basic Combinations – Case 4

- Provides support for a remote host using the Internet and reaching behind a firewall
- Only tunnel mode is required between the remote host and the firewall
- One or two SAs may be used between the remote host and the local host

Basic Combinations – Case 4



(d) Case 4

* = implements IPSec

Key Management

- Determination and distribution of secret keys
- Four keys for communication between two applications:
  xmit and receive pairs for both AH & ESP
- Two modes: manual and automated
- Two protocols:
  - Oakley Key Determination Protocol
  - Internet Security Association and Key Management Protocol (ISAKMP)

Oakley Key Determination Protocol

- Refinement of the Diffe-Hellman key exchange algorithm
- Two users A and B agree on two global parameters: q, a large prime number and α, a primitive root of q (see p.68)
- Secret keys created only when needed
- Exchange requires no preexisting infrastructure
- *Disadvantage*: Subject to MITM attack

Features of Oakley

- Employs cookies to thwart clogging attacks
- Two parties can negotiate a group (modular exponentiation or elliptic curves)
- Uses nonces to ensure against replay attacks
- Enables the exchange of Diffie-Hellman public key values
- Authenticates the Diffie-Hellman exchange to thwart MITM attacks

Aggressive Oakley Key Exchange

I → R: CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, $S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

R → I: CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, $S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^y \| g^x \| EHAS]$

I → R: CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, $S_{KI}[ID_I \| ID_R \| N_I \| N_R \| GRP \| g^x \| g^y \| EHAS]$

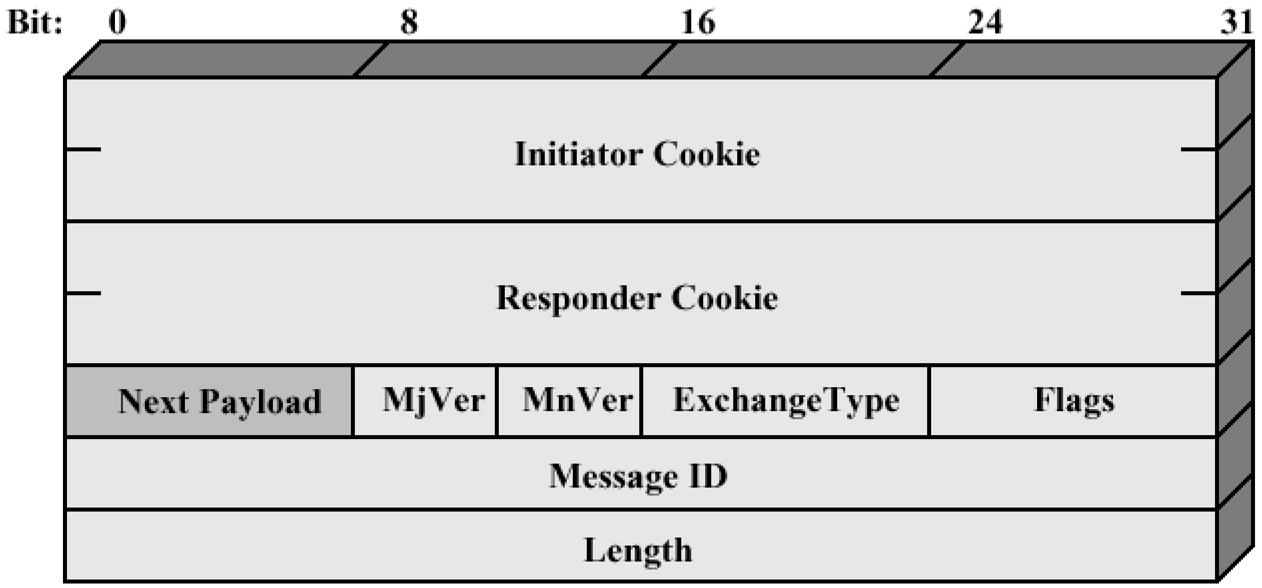
Notation:

I	=	Initiator
R	=	Responder
CKY_I, CKY_R	=	Initiator, responder cookies
OK_KEYX	=	Key exchange message type
GRP	=	Name of Diffie-Hellman group for this exchange
g^x, g^y	=	Public key of initiator, responder; g^{xy} = session key from this exchange
EHAO, EHAS	=	Encryption, hash, authentication functions, offered and selected
NIDP	=	Indicates encryption is not used for remainder of this message
ID_I, ID_R	=	Identifier for initiator, responder
N_I, N_R	=	Random nonce supplied by initiator, responder for this exchange
$S_{KI}[X]$, $S_{KR}[X]$	=	Indicates the signature over X using the private key (signing key) of initiator, responder

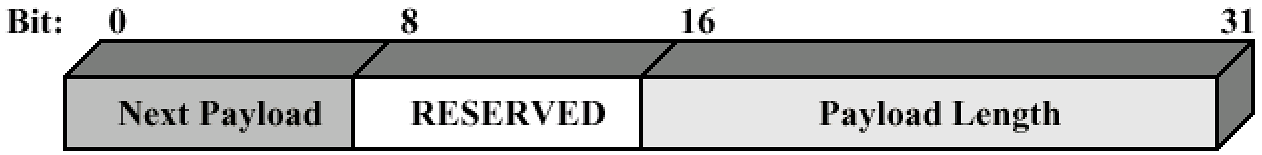
ISAKMP

- Defines procedures and packet formats to establish, negotiate, modify and delete SAs
- Defines payloads for exchanging key generation and authentication data
- Now called IKE

ISAKMP Formats



(a) ISAKMP Header



(b) Generic Payload Header

ISAKMP Payload Types

Type	Parameters	Description
Security Association (SA)	Domain of Interpretation, Situation	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Transform #, Transform-ID, SA Attributes	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Key Exchange Data	Supports a variety of key exchange techniques.
Identification (ID)	ID Type, ID Data	Used to exchange identification information.
Certificate (CERT)	Cert Encoding, Certificate Data	Used to transport certificates and other certificate-related information.
Certificate Request (CR)	# Cert Types, Certificate Types, # Cert Auths, Certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Hash Data	Contains data generated by a hash function.
Signature (SIG)	Signature Data	Contains data generated by a digital signature function.
Nonce (NONCE)	Nonce Data	Contains a nonce.
Notification (N)	DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data	Used to transmit notification data, such as an error condition.
Delete (D)	DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid.

ISAKMP Exchanges

- Provides a framework for message exchange
- Payload type serves as the building blocks
- Five default exchange types specified
- SA refers to an SA payload with associated Protocol and Transform payloads

ISAKMP Exchange Types

Exchange	Note
(a) Base Exchange	
(1) **I → R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R → I:** SA; NONCE	Basic SA agreed upon
(3) **I → R:** KE; ID_I; AUTH	Key generated; Initiator identity verified by responder
(4) **R → I:** KE; ID_R; AUTH	Responder identity verified by initiator; Key generated; SA established
(b) Identity Protection Exchange	
(1) **I → R:** SA	Begin ISAKMP-SA negotiation
(2) **R → I:** SA	Basic SA agreed upon
(3) **I → R:** KE; NONCE	Key generated
(4) **R → I:** KE; NONCE	Key generated
(5)* **I → R:** ID_I; AUTH	Initiator identity verified by responder
(6)* **R → I:** ID_R; AUTH	Responder identity verified by initiator; SA established
(c) Authentication Only Exchange	
(1) **I → R:** SA; NONCE	Begin ISAKMP-SA negotiation
(2) **R → I:** SA; NONCE; ID_R; AUTH	Basic SA agreed upon; Responder identity verified by initiator
(3) **I → R:** ID_I; AUTH	Initiator identity verified by responder; SA established
(d) Aggressive Exchange	
(1) **I → R:** SA; KE; NONCE; ID_I	Begin ISAKMP-SA negotiation and key exchange
(2) **R → I:** SA; KE; NONCE; ID_R; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* **I → R:** AUTH	Responder identity verified by initiator; SA established
(e) Informational Exchange	
(1)* **I → R:** N/D	Error or status notification, or deletion

Notation:
- I = initiator
- R = responder
- * = signifies payload encryption after the ISAKMP header

Internet Key Exchange

- IKE is now at Ver 2 – defined in RFC4306, 12/05
- It works within ISAKMP framework
- Uses Oakley and Skeme protocols for authenticating keys and rapid key refreshment

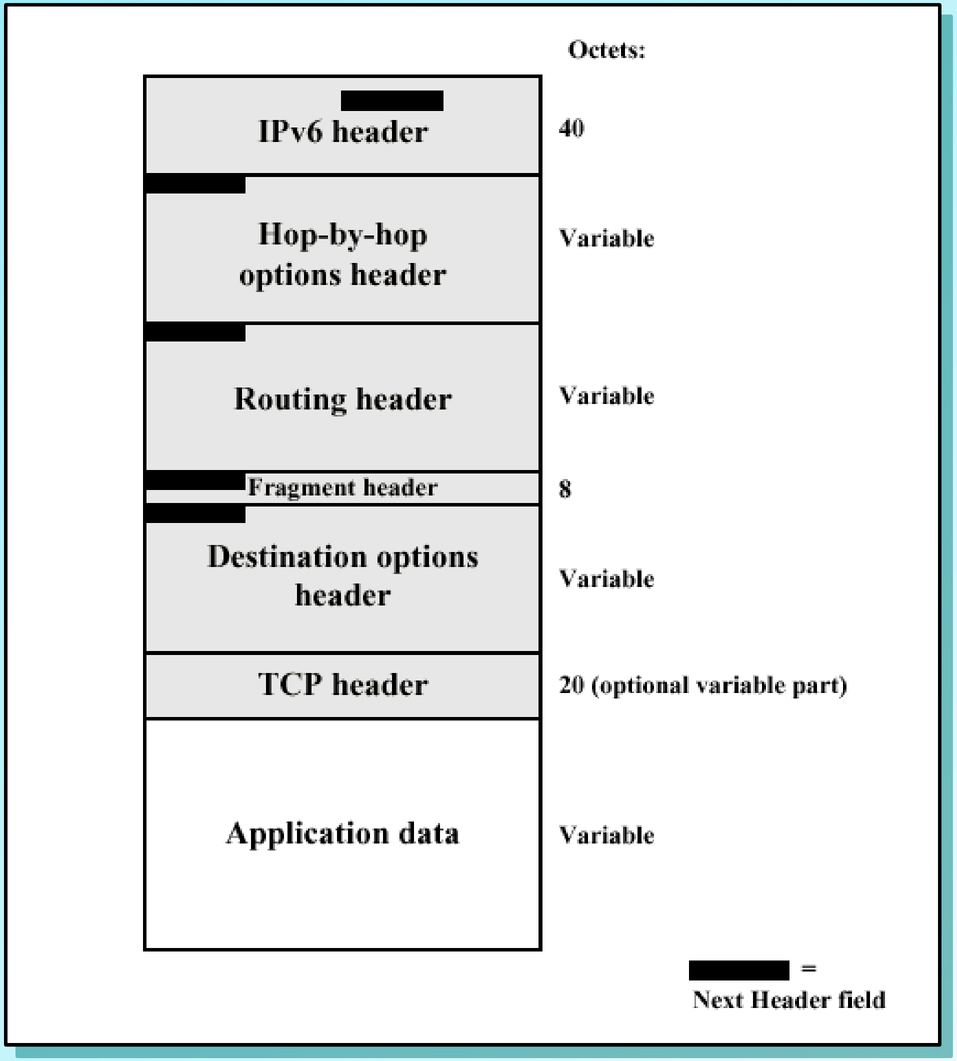
Network Security

Basic Networking – Part B

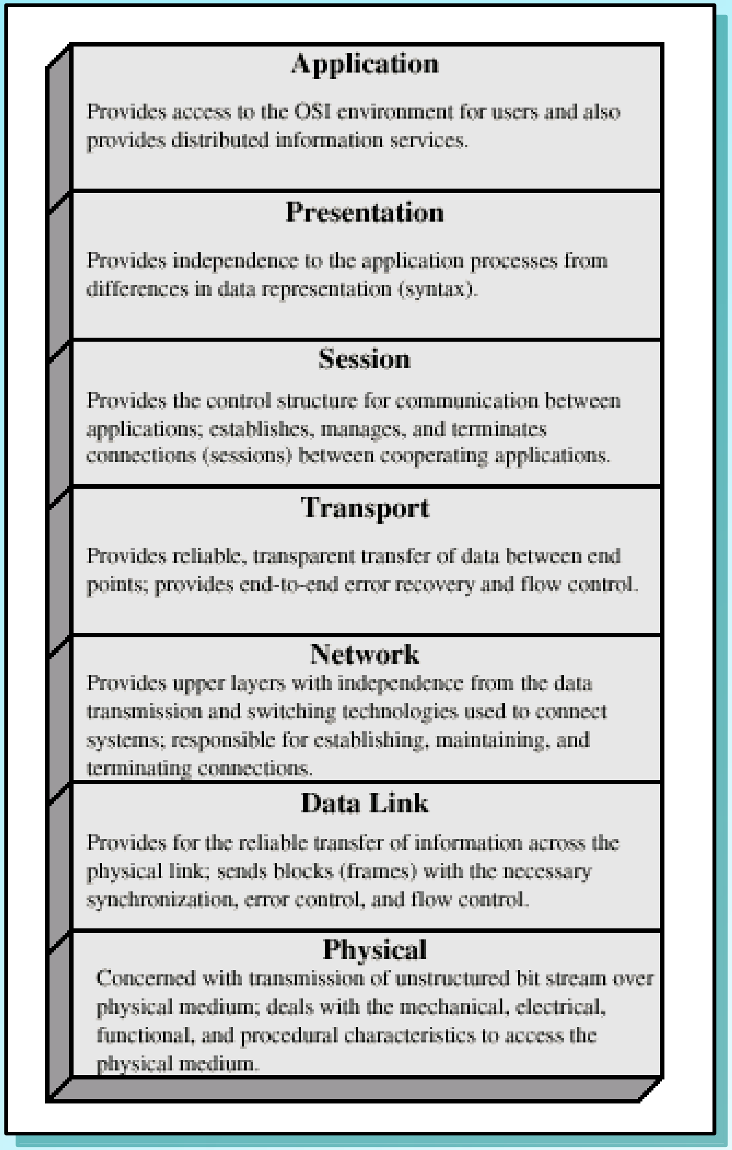
IPv6

- 1995 – RFC 1752 IPng
- 1998 – RFC 2460 IPv6
- Functional enhancements for a mix of data streams (graphic and video)
- Driving force was address depletion 128-bit addresses
- Started in Solaris 2.8, Windows 2000

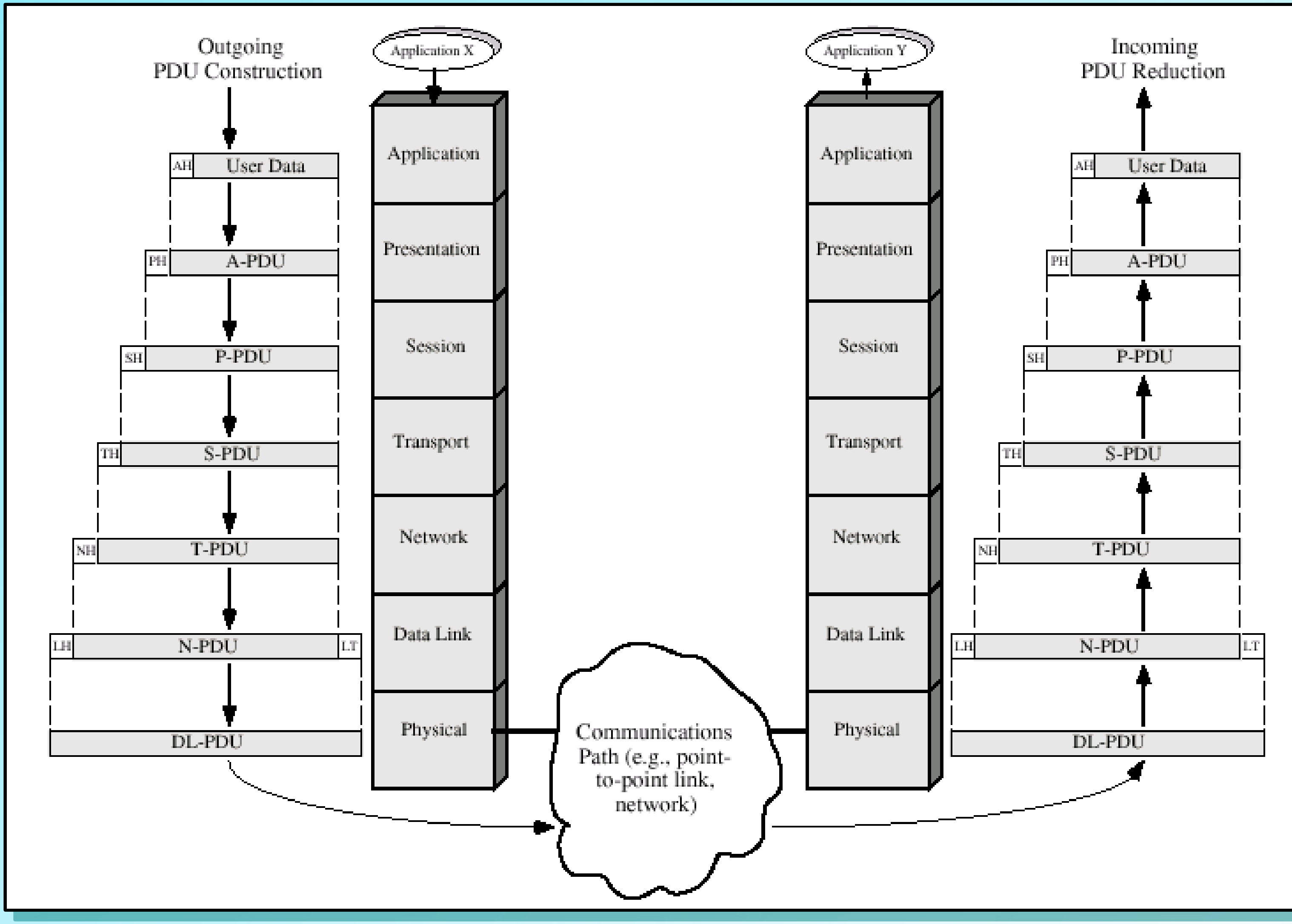
IPv6 Packet w/Extension Headers



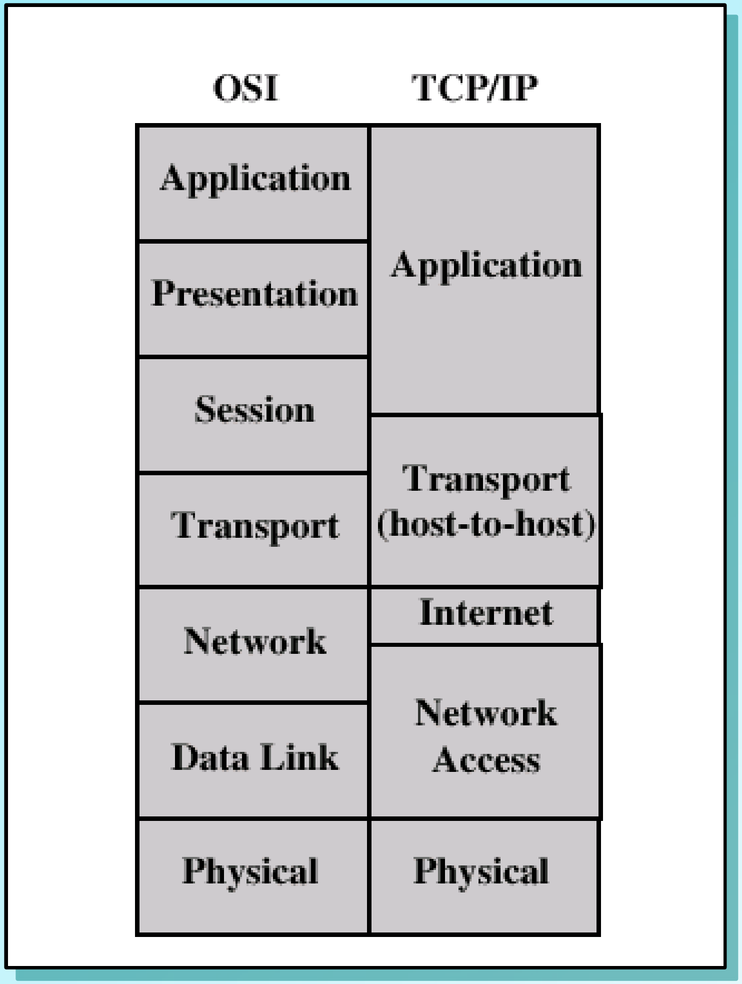
OSI Layers


Application
Provides access to the OSI environment for users and also provides distributed information services.
Presentation
Provides independence to the application processes from differences in data representation (syntax).
Session
Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications.
Transport
Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.
Network
Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections.
Data Link
Provides for the reliable transfer of information across the physical link; sends blocks (frames) with the necessary synchronization, error control, and flow control.
Physical
Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.

OSI Environment



OSI-TCP/IP Comparison

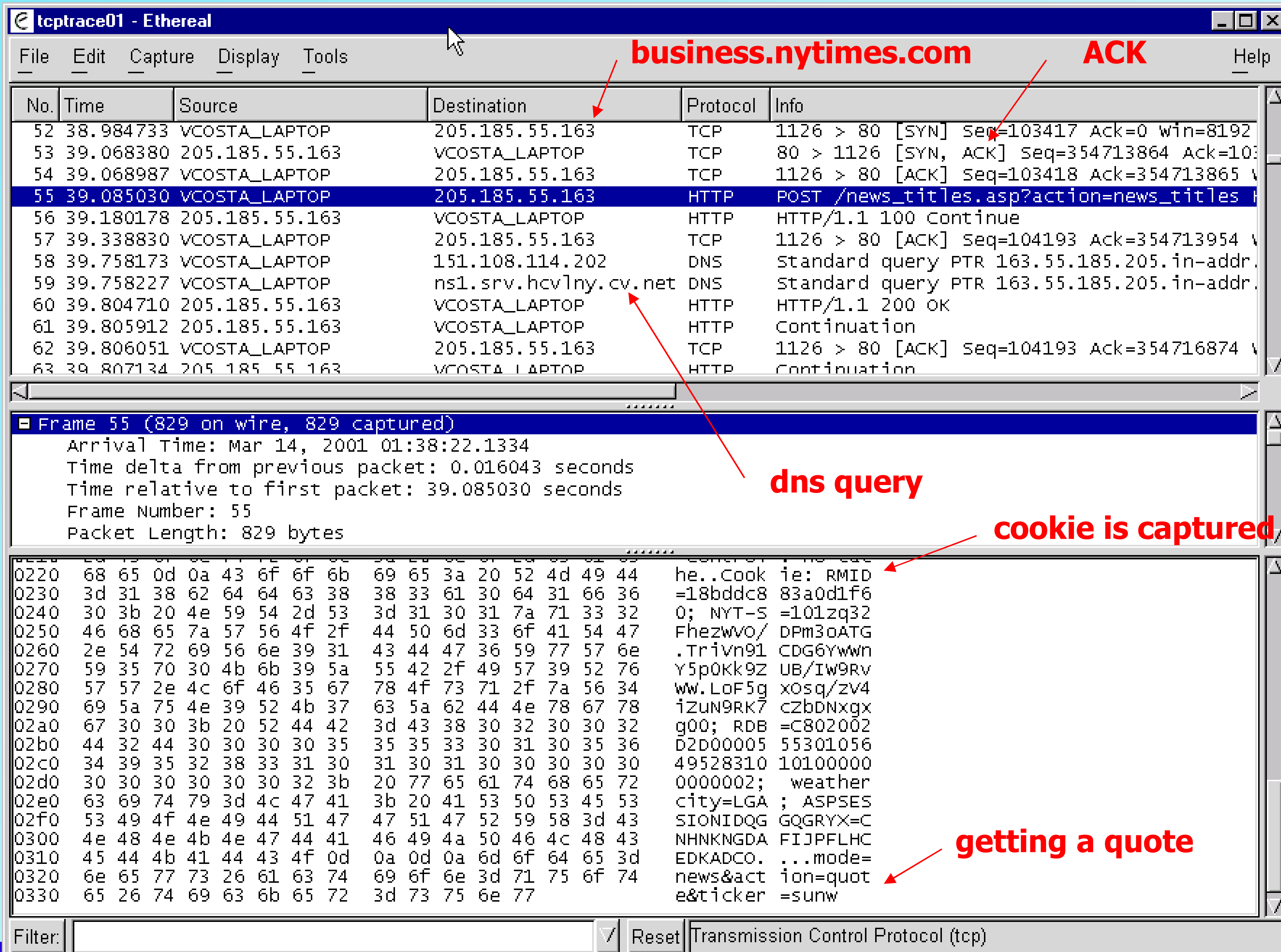


Network Security

IP Security – Part 2

Ethereal

- Ethereal is a free network protocol analyzer for Unix and Windows
- Packet Sniffer - data can be captured "off the wire" from a live network connection
- www.ethereal.com - Everything you ever wanted to know about ethereal
- wiki.ethereal.com - This is the “User's Manual;” also has has a nice “References” section


tcptrace01 - Ethereal
File Edit Capture Display Tools Help
business.nytimes.com
ACK
No. Time Source Destination Protocol Info
52 38.984733 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [SYN] Seq=103417 Ack=0 Win=8192
53 39.068380 205.185.55.163 VCOSTA_LAPTOP TCP 80 > 1126 [SYN, ACK] Seq=354713864 Ack=10
54 39.068987 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=103418 Ack=354713865
55 39.085030 VCOSTA_LAPTOP 205.185.55.163 HTTP POST /news_titles.asp?action=news_titles
56 39.180178 205.185.55.163 VCOSTA_LAPTOP HTTP HTTP/1.1 100 Continue
57 39.338830 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=104193 Ack=354713954
58 39.758173 VCOSTA_LAPTOP 151.108.114.202 DNS Standard query PTR 163.55.185.205.in-addr.
59 39.758227 VCOSTA_LAPTOP ns1.srv.hcvlny.cv.net DNS Standard query PTR 163.55.185.205.in-addr.
60 39.804710 205.185.55.163 VCOSTA_LAPTOP HTTP HTTP/1.1 200 OK
61 39.805912 205.185.55.163 VCOSTA_LAPTOP HTTP Continuation
62 39.806051 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=104193 Ack=354716874
Frame 55 (829 on wire, 829 captured)
Arrival Time: Mar 14, 2001 01:38:22.1334
Time delta from previous packet: 0.016043 seconds
Time relative to first packet: 39.085030 seconds
Frame Number: 55
Packet Length: 829 bytes
dns query
cookie is captured
0220 68 65 0d 0a 43 6f 6f 6b 69 65 3a 20 52 4d 49 44 he..Cook ie: RMID
0230 3d 31 38 62 64 64 63 38 38 33 61 30 64 31 66 36 =18bddc8 83a0d1f6
0240 30 3b 20 4e 59 54 2d 53 3d 31 30 31 7a 71 33 32 0; NYT-S =101zq32
0250 46 68 65 7a 57 56 4f 2f 44 50 6d 33 6f 41 54 47 FhezWVO/ DPm3oATG
0260 2e 54 72 69 56 6e 39 31 43 44 47 36 59 77 57 6e .TriVn91 CDG6YwWn
0270 59 35 70 30 4b 6b 39 5a 55 42 2f 49 57 39 52 76 Y5p0Kk9Z UB/IW9Rv
0280 57 57 2e 4c 6f 46 35 67 78 4f 73 71 2f 7a 56 34 WW.LoF5g xOsq/zV4
0290 69 5a 75 4e 39 52 4b 37 63 5a 62 44 4e 78 67 78 iZuN9RK7 cZbDNxgx
02a0 67 30 30 3b 20 52 44 42 3d 43 38 30 32 30 30 32 g00; RDB =C802002
02b0 44 32 44 30 30 30 30 35 35 35 33 30 31 30 35 36 D2D00005 55301056
02c0 34 39 35 32 38 33 31 30 31 30 31 30 30 30 30 30 49528310 10100000
02d0 30 30 30 30 30 30 32 3b 20 77 65 61 74 68 65 72 0000002; weather
02e0 63 69 74 79 3d 4c 47 41 3b 20 41 53 50 53 45 53 city=LGA ; ASPSES
02f0 53 49 4f 4e 49 44 51 47 47 51 47 52 59 58 3d 43 SIONIDQG GQGRYX=C
0300 4e 48 4e 4b 4e 47 44 41 46 49 4a 50 46 4c 48 43 NHNKNGDA FIJPFLHC
0310 45 44 4b 41 44 43 4f 0d 0a 0d 0a 6d 6f 64 65 3d EDKADCO. ...mode=
0320 6e 65 77 73 26 61 63 74 69 6f 6e 3d 71 75 6f 74 news&act ion=quot
0330 65 26 74 69 63 6b 65 72 3d 73 75 6e 77 e&ticker =sunw
getting a quote
Filter: Reset Transmission Control Protocol (tcp)

Ethereal Etiquette

- Be careful when and where you use this tool
- It makes people nervous
- Use prudence with the information you collect
- **When in doubt, seek permission!**

Other Sniffing Tools

- Ettercap is an open source software tool for computer network protocol analysis and security cracking. It can be used to intercept traffic on a network segment, capture passwords, and conduct man-in-the-middle attacks against a number of common protocols.

- dSniff is a packet sniffer and set of traffic analysis tools. Unlike tcpdump and other low-level packet sniffers, dSniff also includes tools that decode information (passwords, most infamously) sent across the network, rather than simply capturing and printing the raw data, as do generic sniffers like Ethereal and tcpdump.

- AiroPeek was the first Wi-Fi (IEEE 802.11) packet analyzer, or packet sniffer, that provides network engineers with a view of the data traversing a Wireless LAN network. AiroPeek was created in 2001 and its interface was based closely on EtherPeek, another product from WildPackets, Inc. They also have some “free” utilities.

Important URLs

- www.insecure.org/tools.html
  Site has the top 50 security tools
- Nmap is a free software port scanner. It is used to evaluate the security of computers, and to discover services or servers on a computer network.
- EtherApe is a graphical network monitor for Unix. Featuring link layer, ip and TCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Color coded protocols display.
- **Be judicious in the use of these tools!**

Homework

- Read rest of Chapter Six
- **Mid-Term Exam (take home) is due next class**
- *No late submissions*

Spring Fever – Enjoy It!