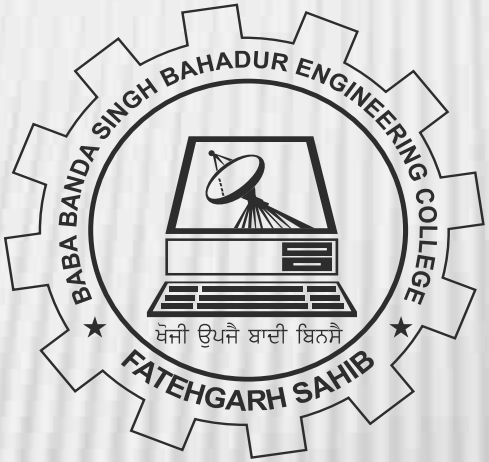
COMPUTER NETWORKS - II
(BCSE1-520)

B.Tech(CSE)
Semester: 5th
(Session – July-Dec, 2019)



Department of Computer Science & Engineering
Baba Banda Singh Bahadur Engineering College
Fatehgarh Sahib -140407, Punjab, India

NETWORK SECURITY

Fundamentals of Network Security

Basics of IPv6

IPsec: overview of IPsec

IP and IPv6

Authentication Header (AH)

Encapsulating Security Payload (ASP)

FUNDAMENTALS OF NETWORK SECURITY

- Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.
- Network security is mostly achieved through the use of cryptography, a science based on abstract algebra.

SERVICES PROVIDED BY NETWORK SECURITY

- **Network security can provide one of the five services:**
- services related to the message exchanged using the network:
  - 1) message confidentiality,
  - 2) integrity,
  - 3) authentication, and
  - 4) nonrepudiation
- service related to entity:
  - 5) entity authentication or identification.

MESSAGE CONFIDENTIALITY

- Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.
- For Example, When a customer communicates with her bank, she expects that the communication is totally confidential.
- Techniques: symmetric-key cryptography or asymmetric key cryptography

MESSAGE INTEGRITY

- Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously.
- As more and more monetary exchanges occur over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000.
- The integrity of the message must be preserved in a secure communication.
- Encryption and decryption provide secrecy, or confidentiality, but not **integrity.**
- **Techniques:** Document and Fingerprint, Message and Message Digest (using Hash Function), Digital Signature

MESSAGE AUTHENTICATION

- Message authentication is a service beyond message integrity.
- In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.
- Techniques: MAC (message authentication code), Digital Signature

MESSAGE NONREPUDIATION

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver.
- For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.
- Techniques: Digital Signature

ENTITY AUTHENTICATION

- In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example).
- For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.
- Techniques: Passwords, Challenge-Response, Digital Signature,

BASICS OF IPV6

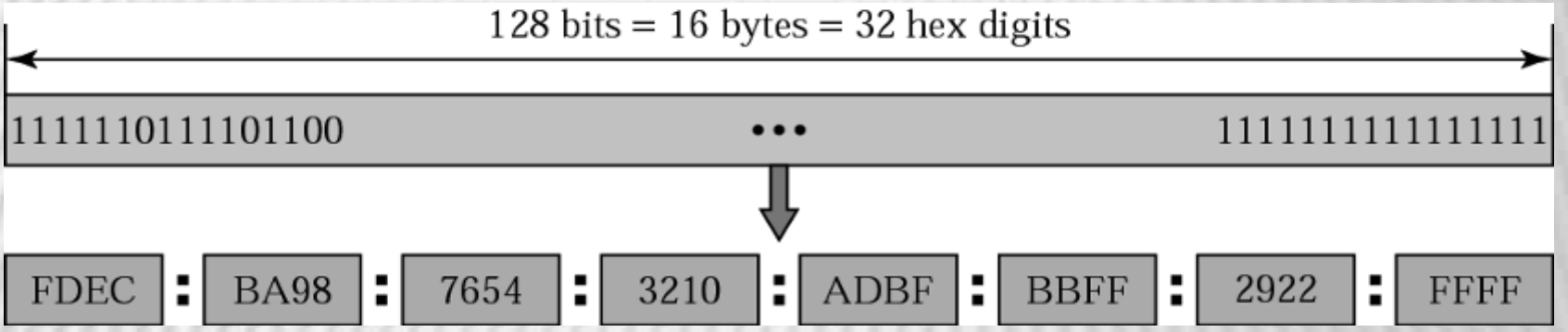
- The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPv6 (IP version 6).
- In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation.
- These addresses are referred to as IPv6 (IP version 6) addresses.

- Despite all short-term solutions, such as classless addressing, Dynamic Host Configuration Protocol (DHCP), and NAT, address depletion is still a long-term problem for the Internet.
- This and other problems in the IP protocol itself, such as lack of accommodation for real-time audio and video transmission, and encryption and authentication of data for some applications, have been the motivation for IPv6.

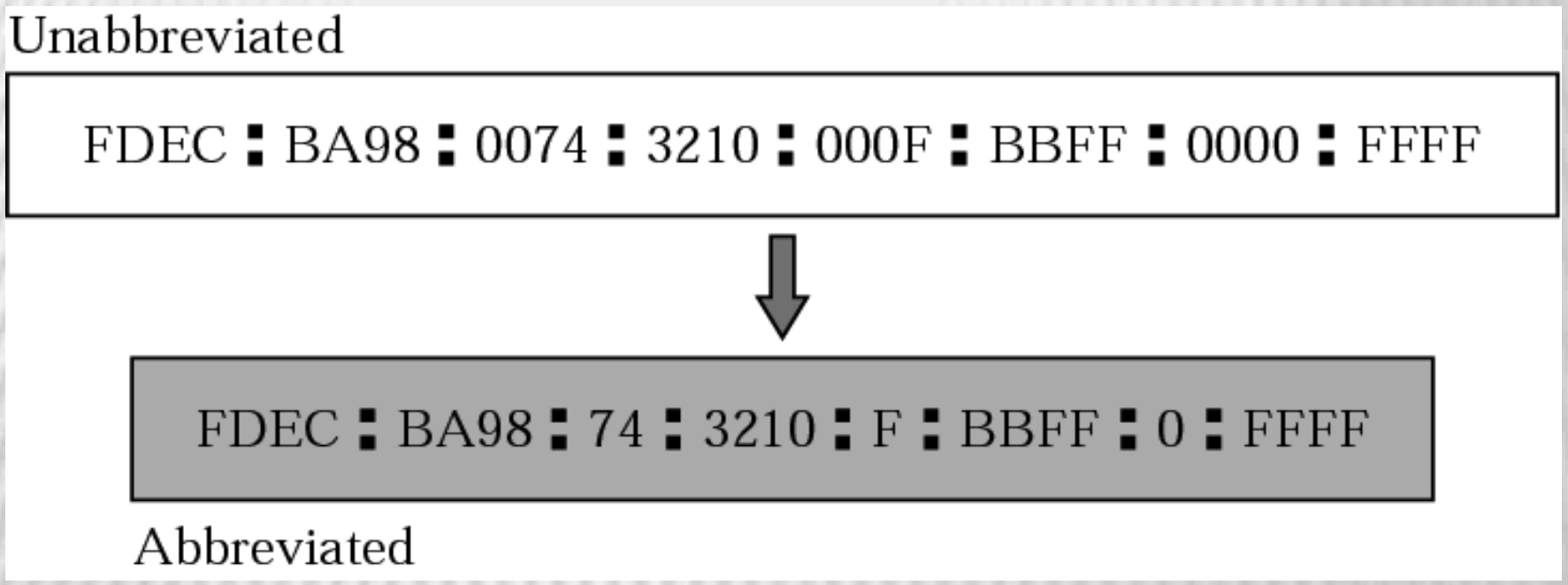
IPV6 ADDRESS STRUCTURE

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.
- *Hexadecimal Colon Notation*
  - To make addresses more readable, IPv6 specifies hexadecimal colon notation.
  - In this notation, 128 bits is divided into eight sections, each 2 bytes in length.
  - Two bytes in hexadecimal notation requires four hexadecimal digits.
  - Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon

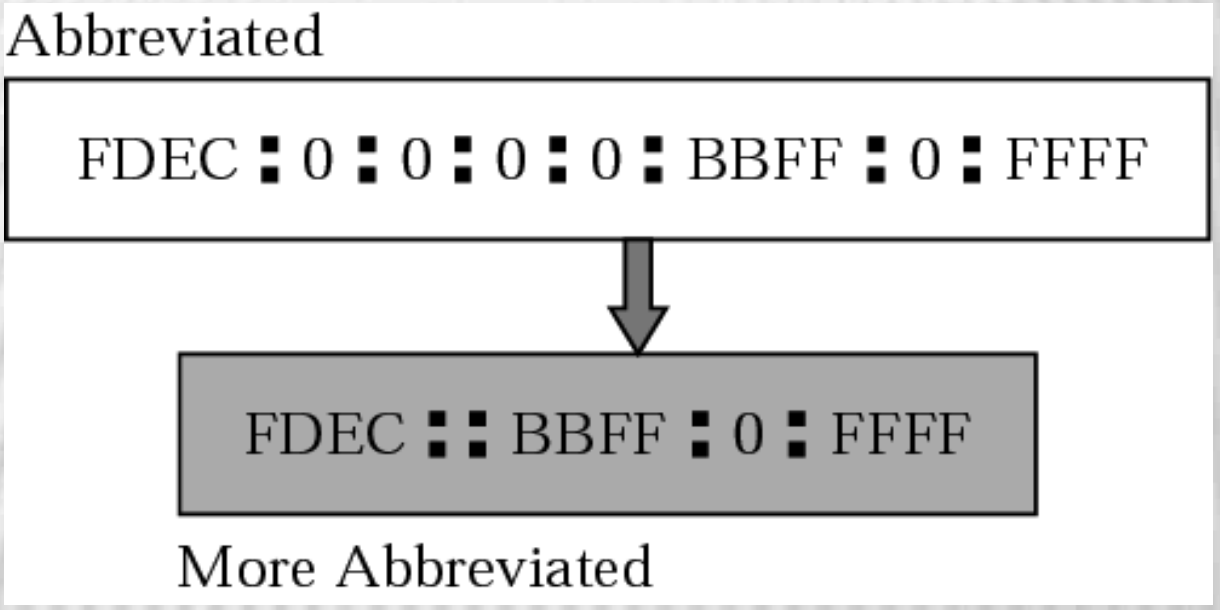
IPV6 ADDRESS



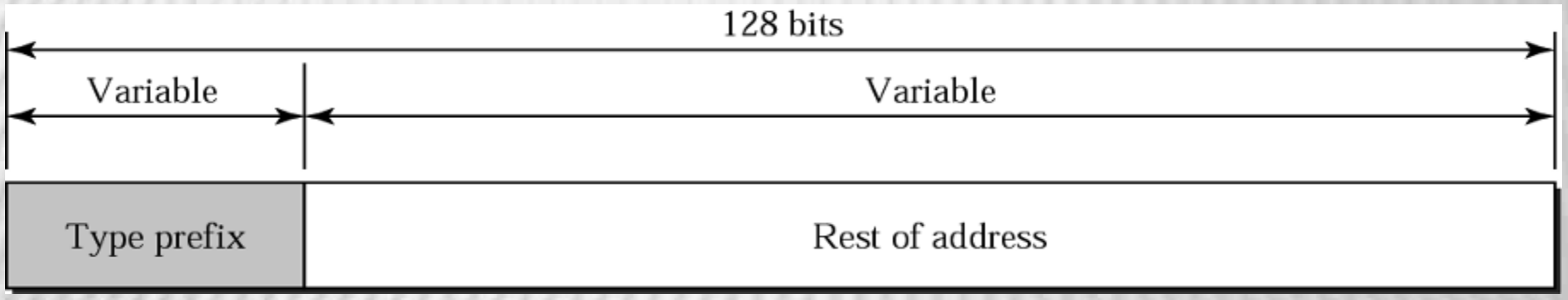
ABBREVIATED ADDRESS



- *Abbreviated address with consecutive zeros*



ADDRESS STRUCTURE



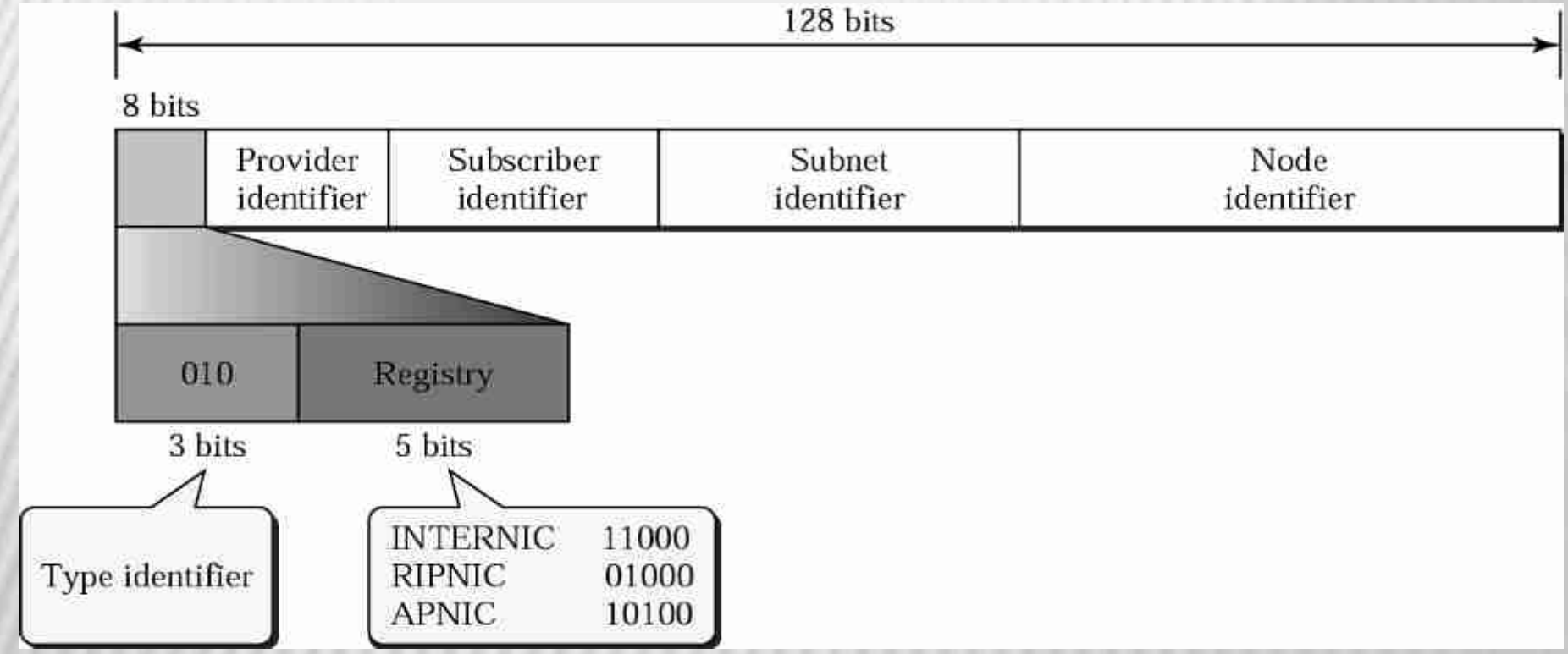
ADDRESS SPACE

- IPv6 has a much larger address space; 2power128 addresses are available.
- The designers of IPv6 divided the address into several categories.
- A few leftmost bits, called the *type prefix, in each address define its category.*
- *The type prefix is variable in length, but it is* designed such that no code is identical to the first part of any other code.
- In this way, there is no ambiguity; when an address is given, the type prefix can easily be determined.

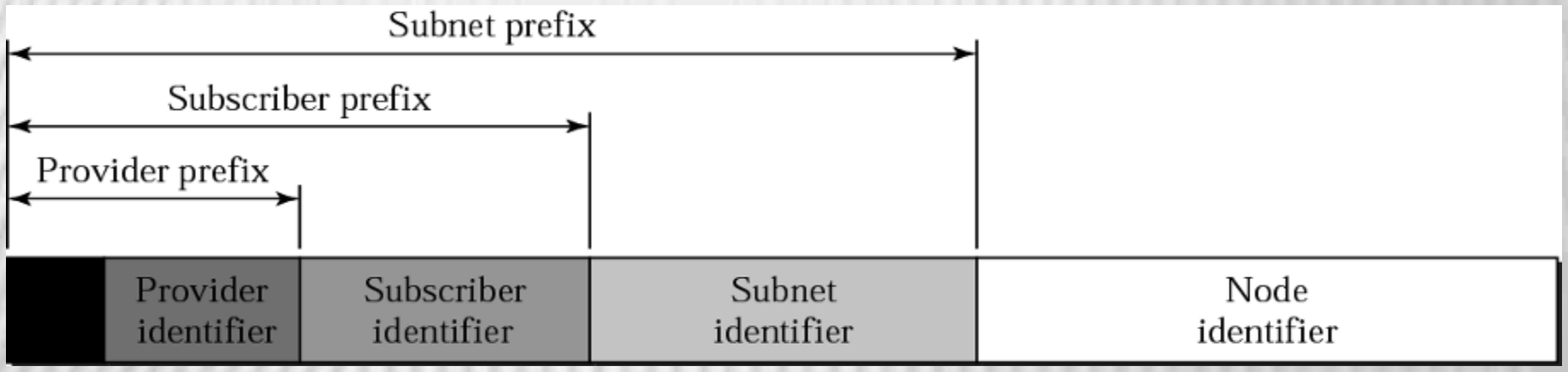
TYPE PREFIXES FOR IPV6 ADDRESSES

Type Prefix	*Type*	*Fraction*
010	**Provider-based unicast addresses**	**1/8**
011	Reserved	1/8
100	Geographic unicast addresses	1/8
101	Reserved	1/8
110	Reserved	1/8
1110	Reserved	1/16
1111 0	Reserved	1/32
1111 10	Reserved	1/64
1111 110	Reserved	1/128
1111 1110 0	Reserved	1/512
1111 1110 10	Link local addresses	1/1024
1111 1110 11	Site local addresses	1/1024
1111 1111	Multicast addresses	1/256

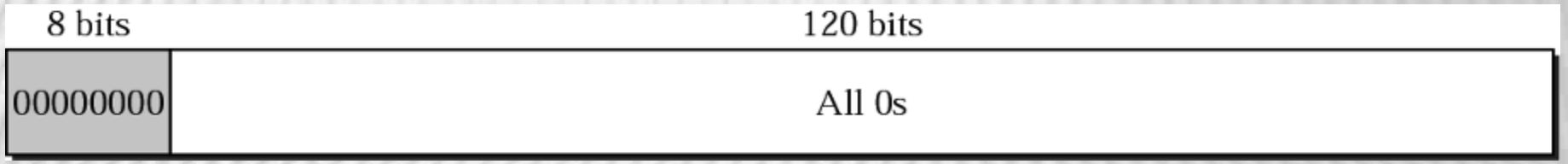
PROVIDER-BASED ADDRESS



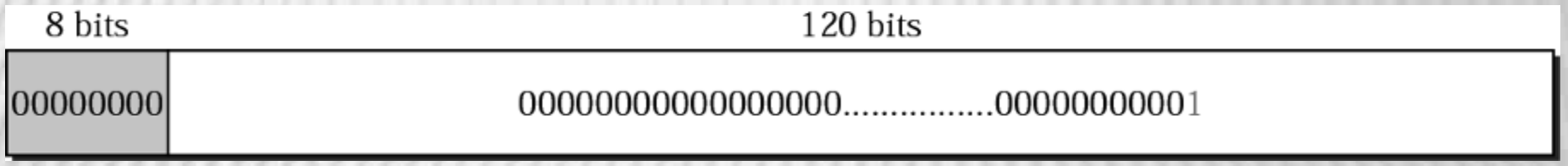
ADDRESS HIERARCHY



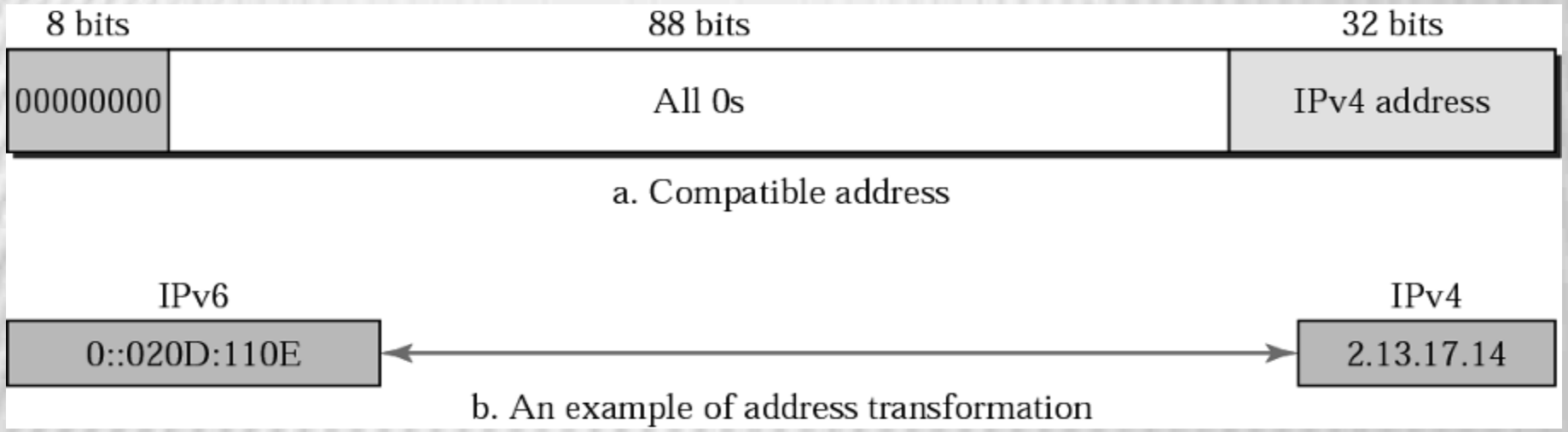
UNSPECIFIED ADDRESS



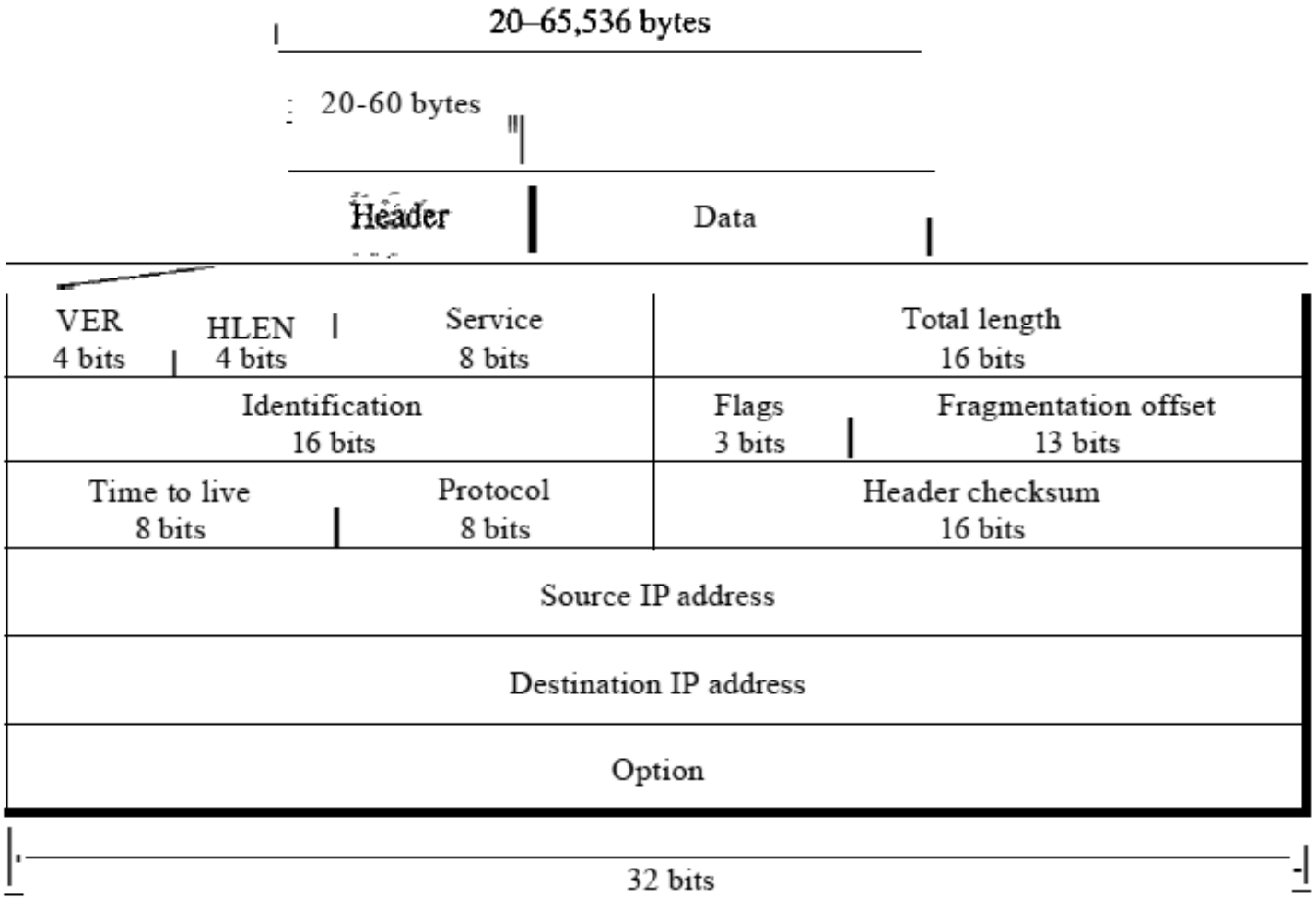
LOOPBACK ADDRESS



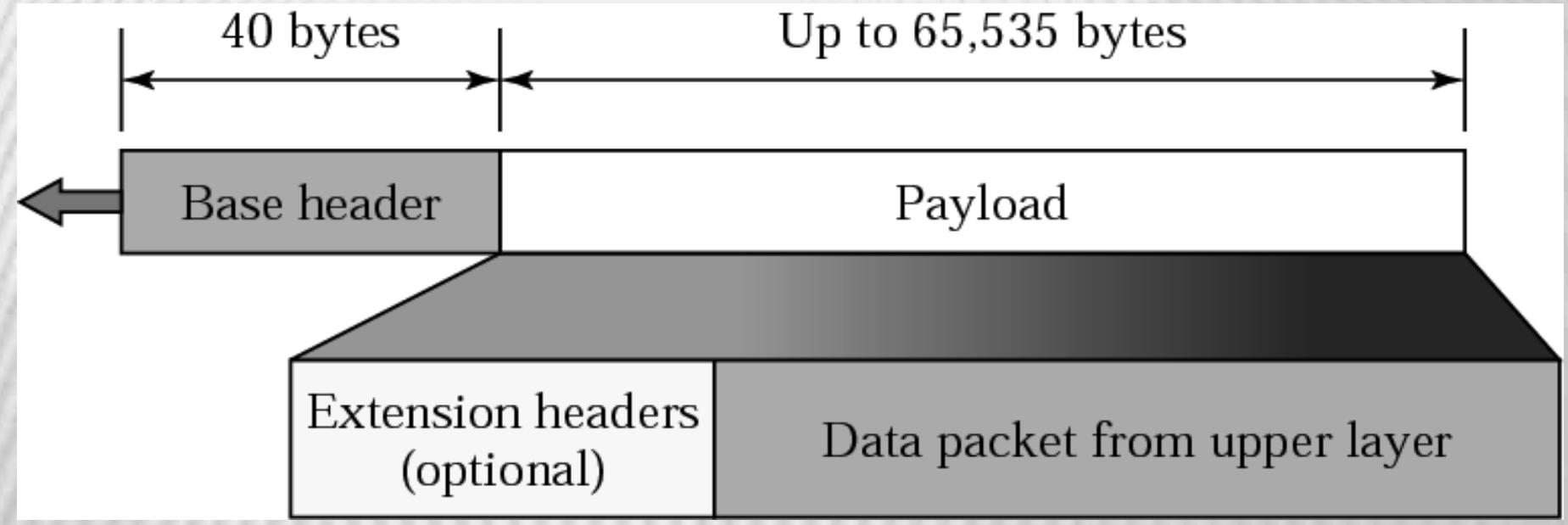
COMPATIBLE ADDRESS



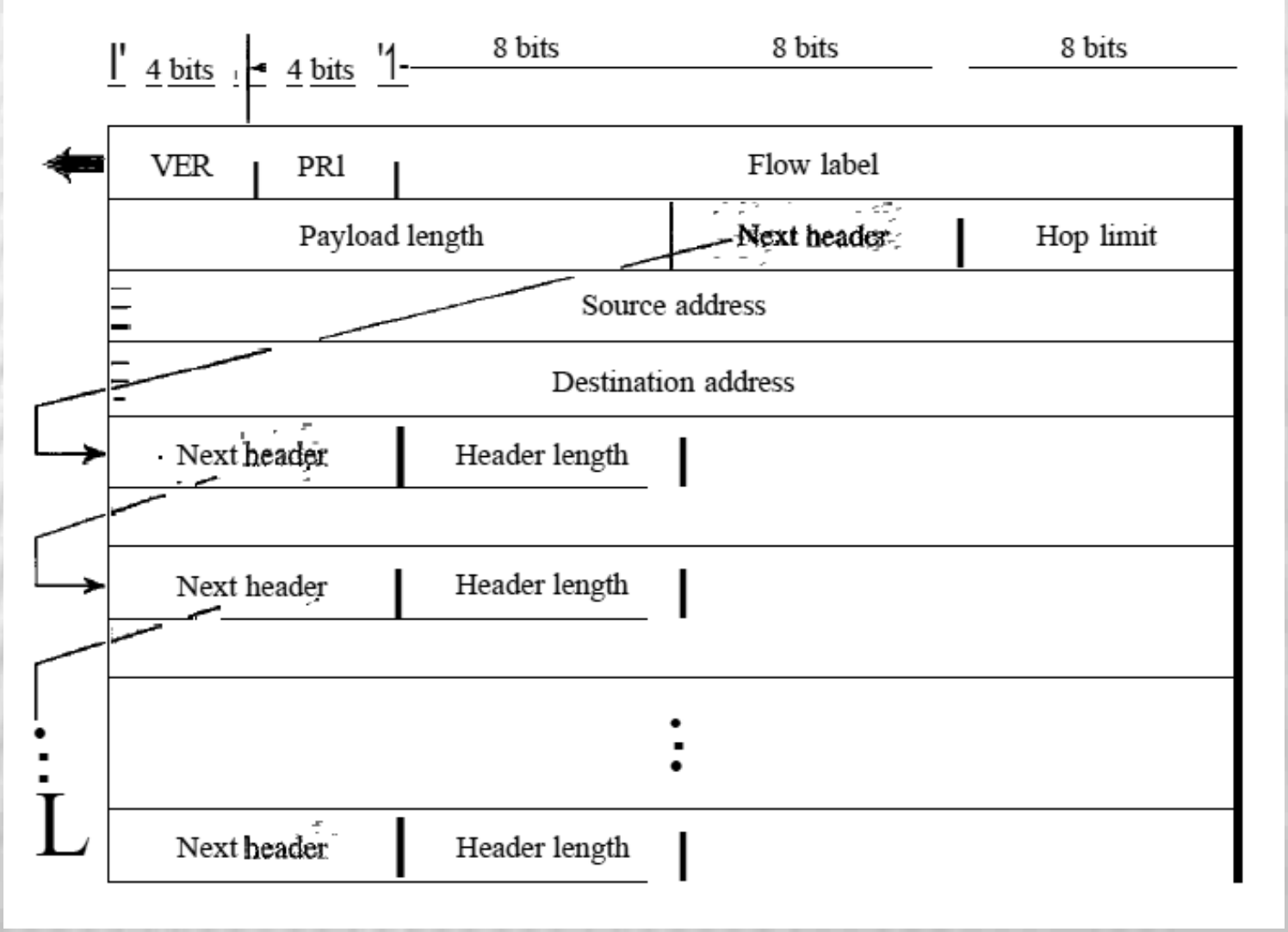
IPV4 DATAGRAM FORMAT



IPV6 DATAGRAM



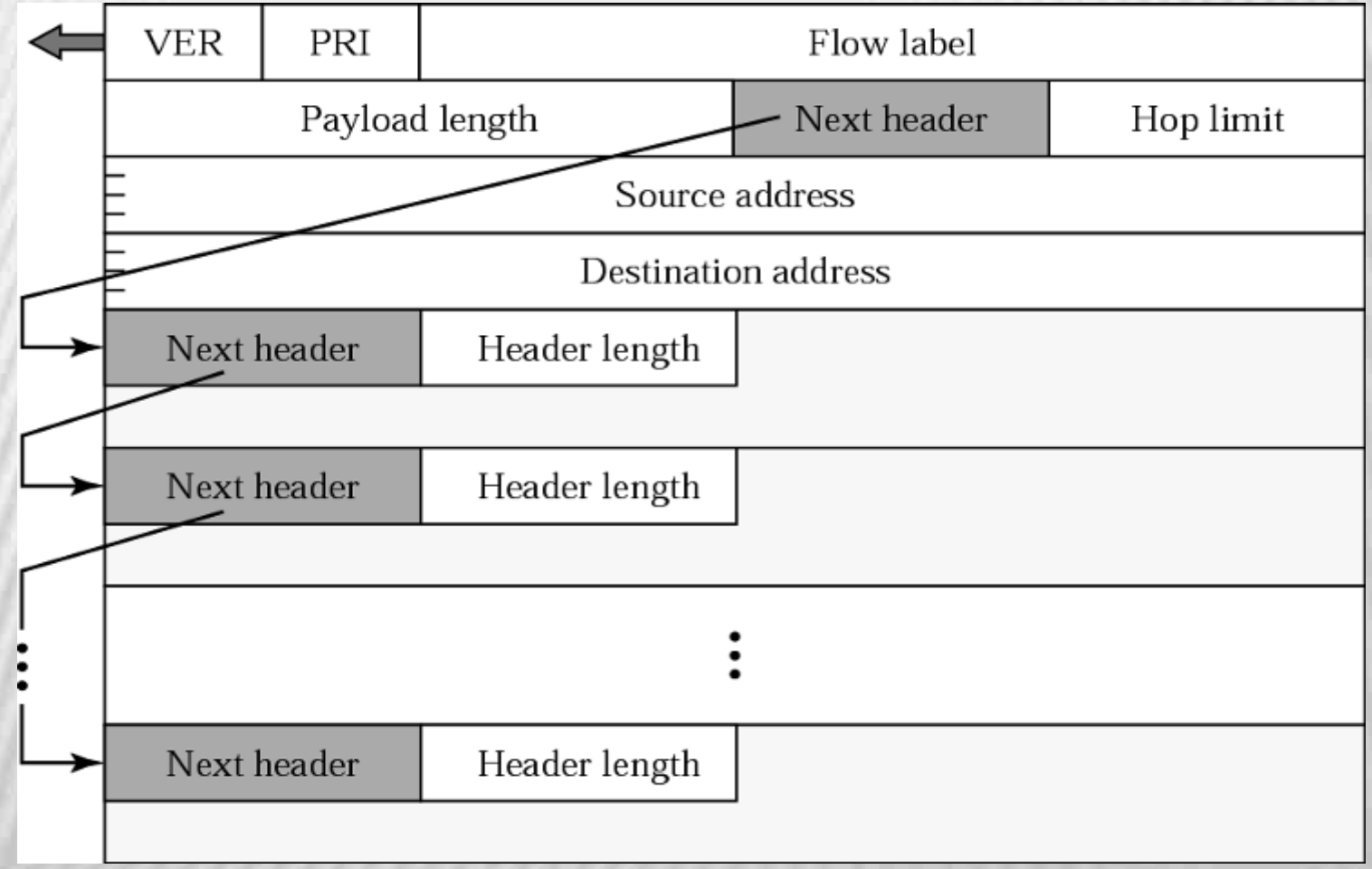
IPV6 DATAGRAM FORMAT



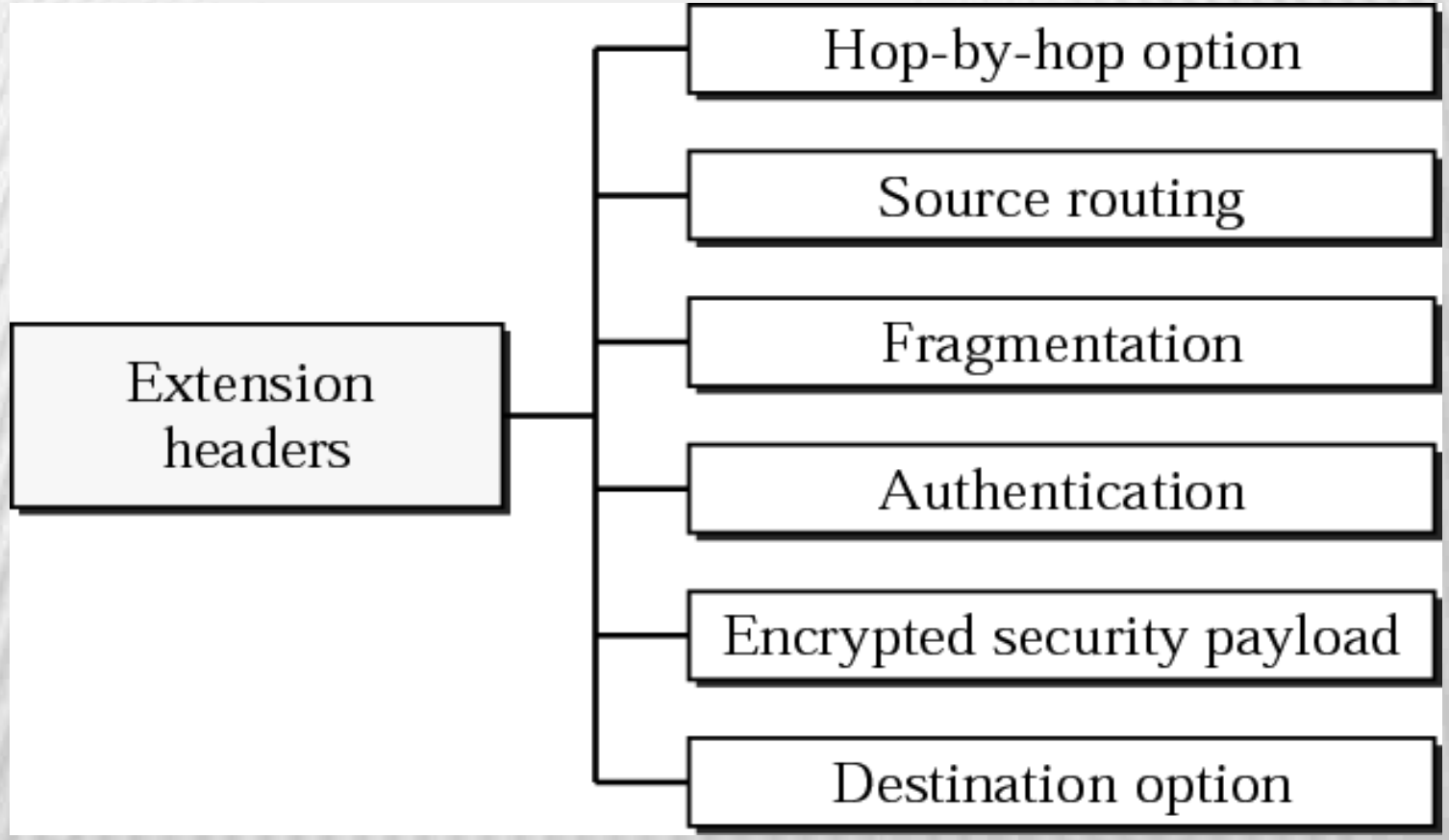
NEXT HEADER CODES

Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (No next header)
60	Destination option

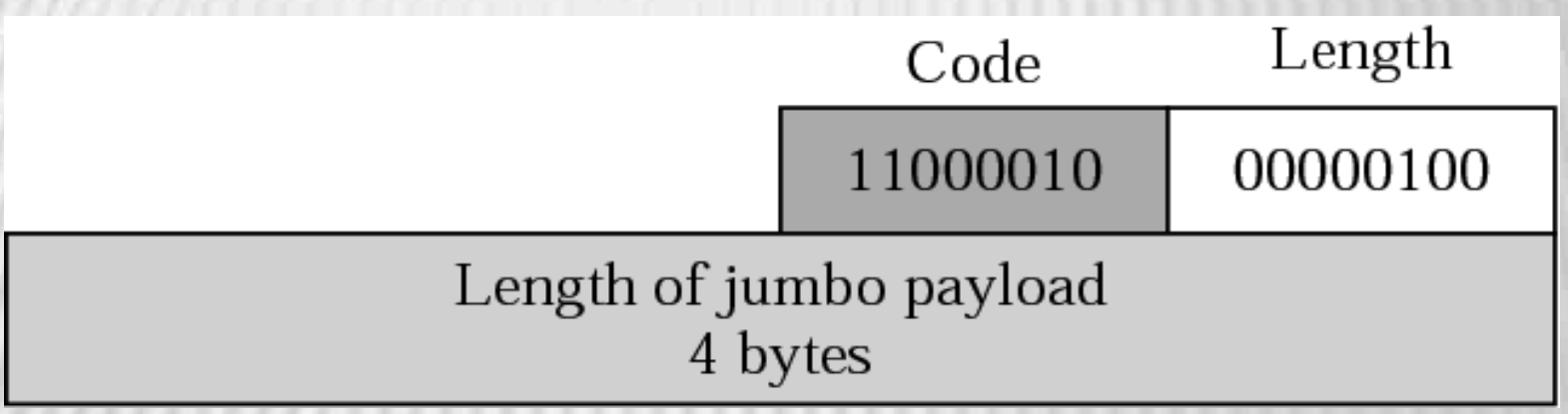
EXTENSION HEADER FORMAT



EXTENSION HEADER TYPES



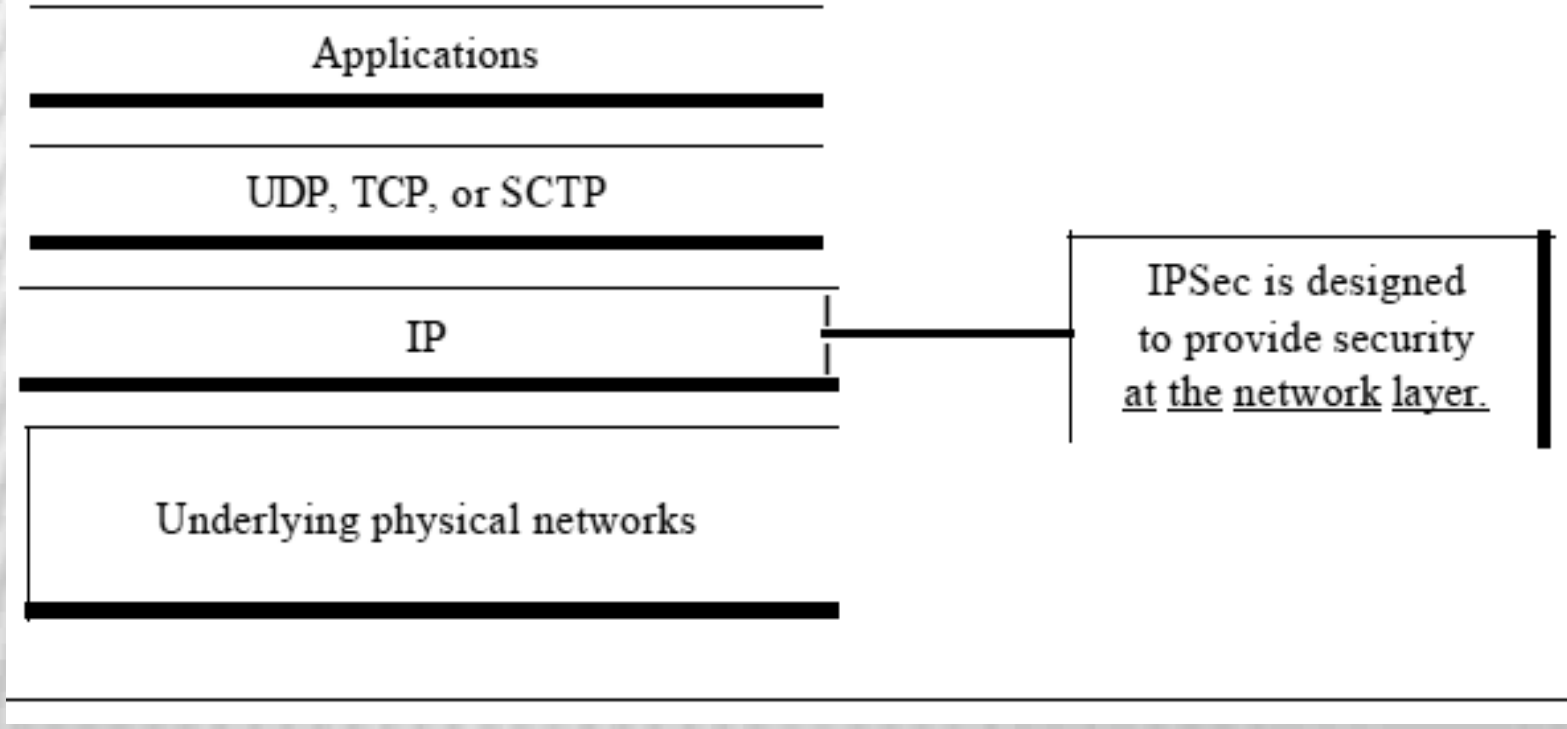
JUMBO PAYLOAD



IPSEC

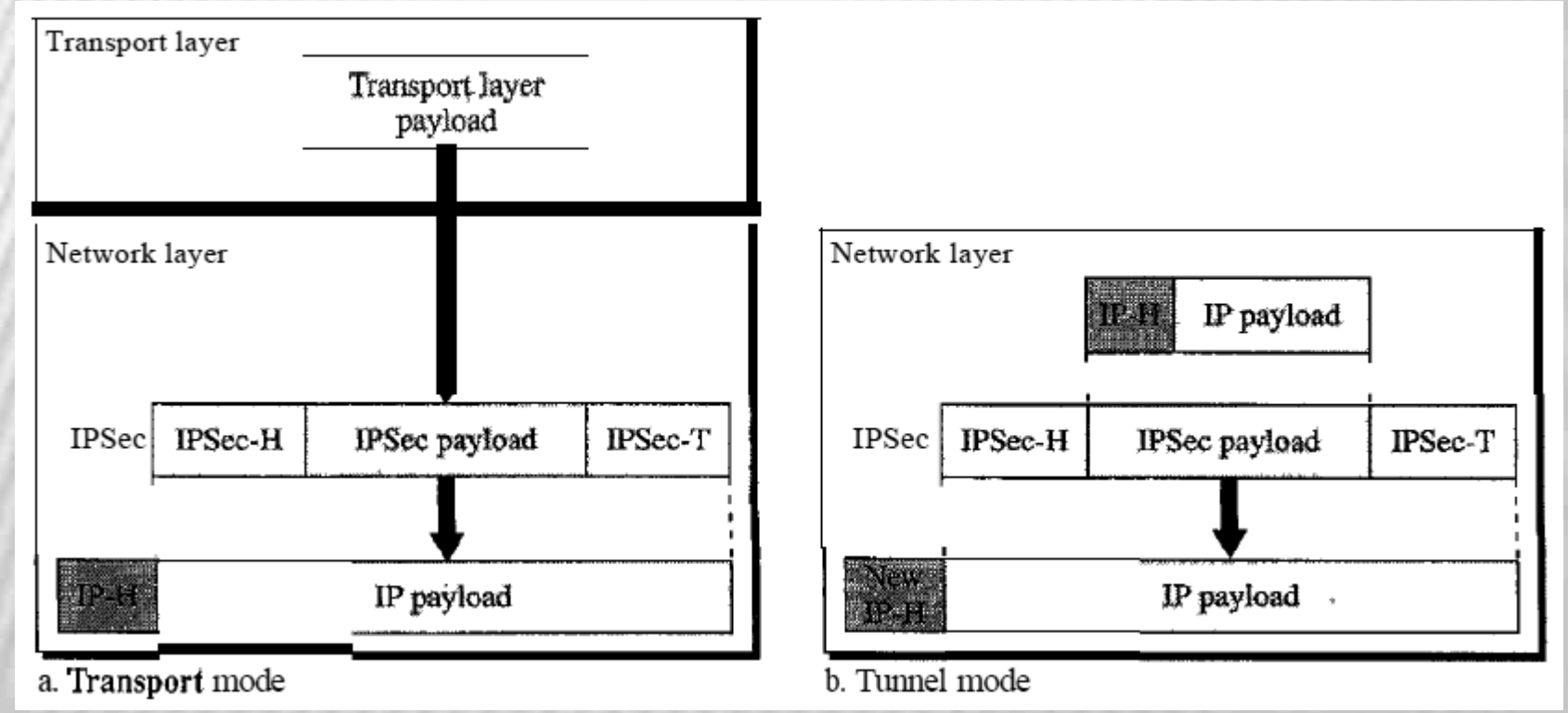
- IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- IPSec helps to create authenticated and confidential packets for the IP layer.

TCPIIP protocol suite and IPSec



TWO MODES

- IPSec operates in one of two different modes: the transport mode or the tunnel mode

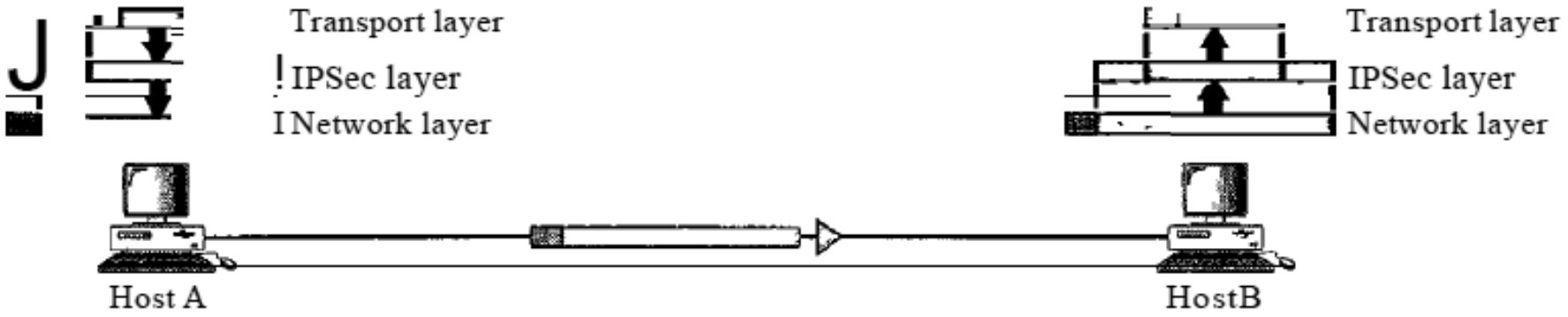


TRANSPORT MODE

- In the transport mode, IPSec protects what is delivered from the transport layer to the network layer.
- In other words, the transport mode protects the network layer payload, the payload to be encapsulated in the network layer.
- Note that the transport mode does not protect the IP header.
- In other words, the transport mode does not protect the whole IP packet; it protects only the packet from the transport layer (the IP layer payload).
- In this mode, the IPSec header and trailer are added to the information coming from the transport layer.
- The IP header is added later.

- The transport mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.
- The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.
- **IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.**

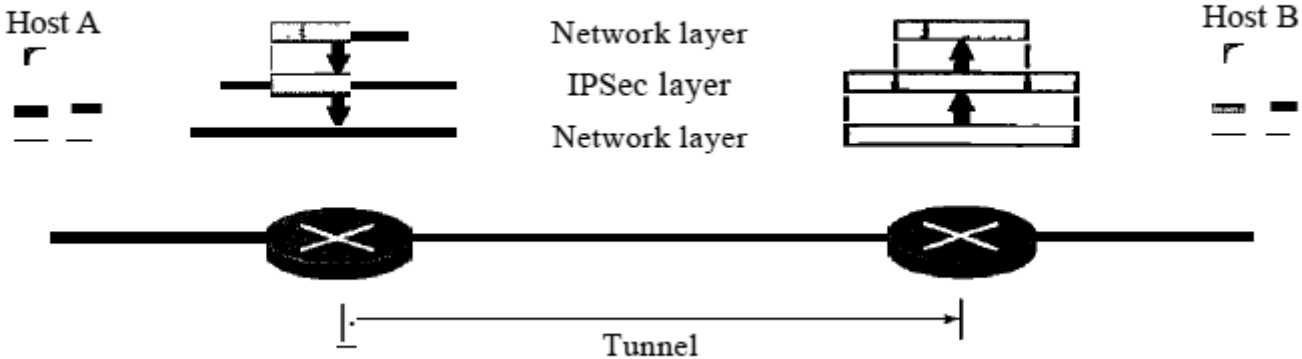
Transport mode in action



TUNNEL MODE

- In the tunnel mode, IPSec protects the entire IP packet.
- It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.
- The new IP header, as we will see shortly, has different information than the original IP header.
- The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host.

Tunnel mode in action



- In other words, we use the tunnel mode when either the sender or the receiver is not a host.
- The entire original packet is protected from intrusion between the sender and the receiver.
- It's as if the whole packet goes through an imaginary tunnel.
- **IPSec in tunnel mode protects the original IP header.**

TWO SECURITY PROTOCOLS

- IPSec defines two protocols to provide authentication and/or encryption for packets at the IP level-
  - Authentication Header (AH) Protocol and
  - Encapsulating Security Payload (ESP) Protocol

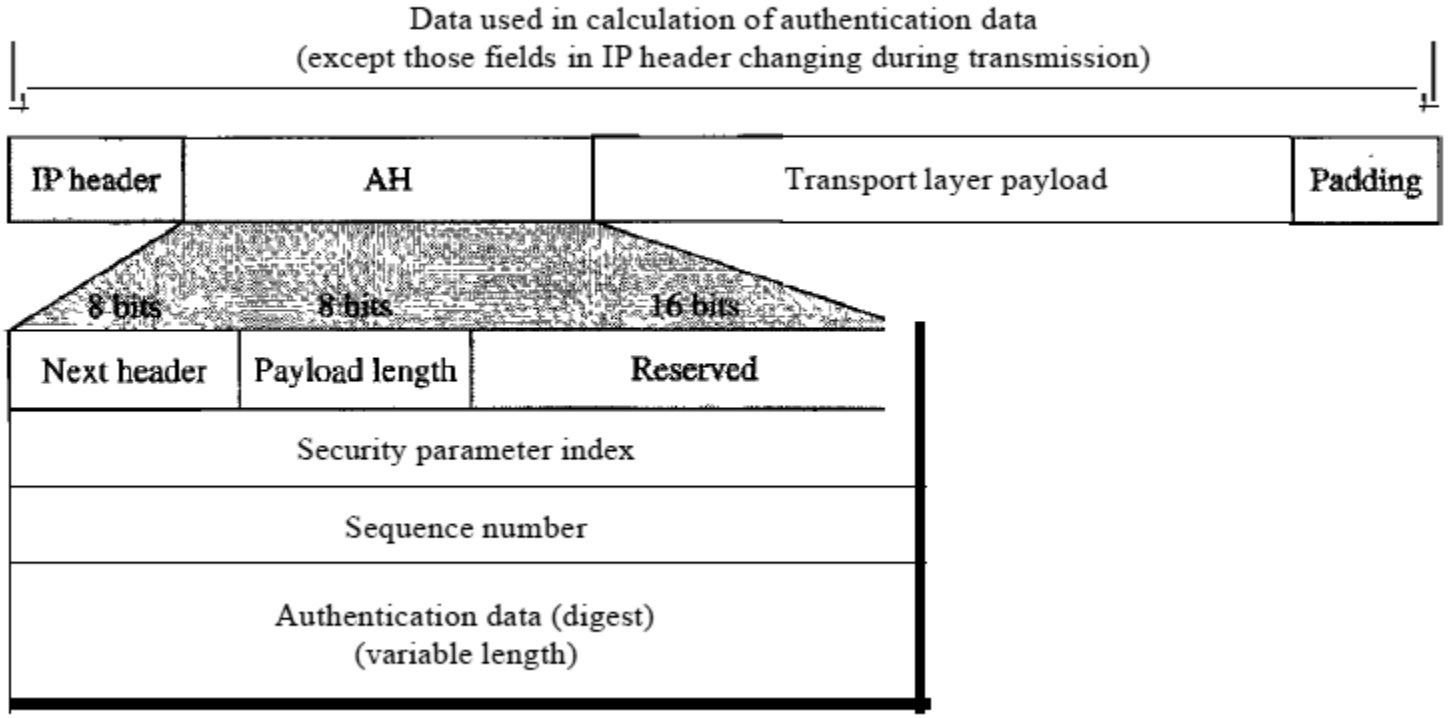
AUTHENTICATION HEADER (AH)

- The Authentication Header (AH) Protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
- The protocol uses a hash function and a symmetric key to create a message digest; the digest is inserted in the authentication header.
- The AH is then placed in the appropriate location based on the mode (transport or tunnel). Figure shows the fields and the position of the authentication header in the transport mode.
- When an IP datagram carries an authentication header, the original value in the protocol field of the IP header is replaced by the value 51.
- A field inside the authentication header (the next header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram).
- **The AH Protocol provides source authentication and data integrity, but not privacy.**

- The addition of an authentication header follows these steps:

1. An authentication header is added to the payload with the authentication data field set to zero.
2. Padding may be added to make the total length even for a particular hashing algorithm.
3. Hashing is based on the total packet. However, only those fields of the IP header that do not change during transmission are included in the calculation of the message digest (authentication data).
4. The authentication data are inserted in the authentication header.
5. *The IP header is added after the value of the protocol field is changed to 51.*

Authentication Header (AH) Protocol in transport mode



A brief description of each field follows:

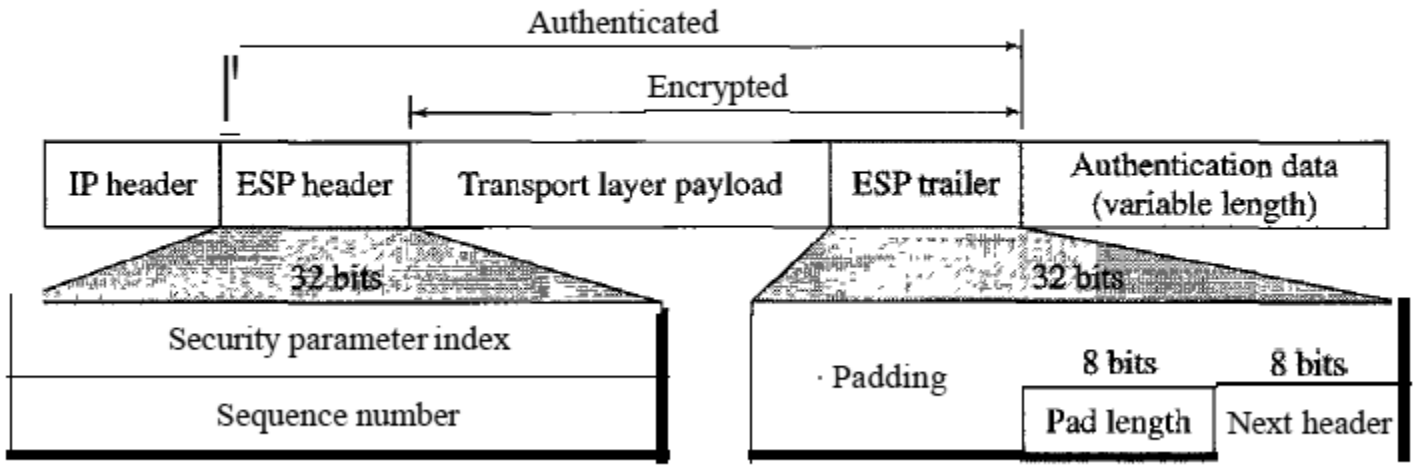
- **Next Header**
  - The 8-bit next-header field defines the type of payload carried by the IP datagram (such as TCP, UDP, ICMP, or OSPF).
  - It has the same function as the protocol field in the IP header before encapsulation.
  - In other words, the process copies the value of the protocol field in the IP datagram to this field. The value of the protocol field in the new IP datagram is now set to 51 to show that the packet carries an authentication header.
- **Payload Length**
  - The name of this 8-bit field is misleading.
  - It does not define the length of the payload;
  - it defines the length of the authentication header in 4-byte multiples, but it does not include the first 8 bytes.
- **Security Parameter Index**
  - The 32-bit security parameter index (SPI) field plays the role of a virtual-circuit identifier and is the same for all packets sent during a connection called a security association (discussed later).

- **Sequence number**
  - A 32-bit sequence number provides ordering information for a sequence of datagrams.
  - The sequence numbers prevent a playback.
  - Note that the sequence number is not repeated even if a packet is retransmitted.
  - A sequence number does not wrap around after it reaches 232; a new connection must be established.
- **Authentication data**
  - Finally, the authentication data field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit (e.g., time-to-live)

ENCAPSULATING SECURITY PAYLOAD (ESP)

- The AH Protocol does not provide privacy, it provides only source authentication and data integrity.
- IPSec later defined an alternative protocol that provides source authentication, integrity, and privacy called Encapsulating Security Payload (ESP).
- ESP adds a header and trailer.
- Note that ESP's authentication data are added at the end of the packet which makes its calculation easier.

Encapsulation Security Payload (ESP) Protocol in transport mode



- When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50.
- A field inside the ESP trailer (the next-header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram, such as TCP or UDP).
- The ESP procedure follows these steps:
  - 1. An ESP trailer is added to the payload.
  - 2. The payload and the trailer are encrypted.
  - 3. The ESP header is added.
  - 4. The ESP header, payload, and ESP trailer are used to create the authentication data.
  - 5. The authentication data are added to the end of the ESP trailer.
  - 6. The IP header is added after the protocol value is changed to 50.

- The fields for the header and trailer are as follows:
  - **Security parameter index.** The 32-bit security parameter index field is similar to that defined for the AH Protocol.
  - **Sequence number.** The 32-bit sequence number field is similar to that defined for the AH Protocol.
  - **Padding.** This variable-length field (0 to 255 bytes) of 0s serves as padding.
  - **Pad length.** The 8-bit pad length field defines the number of padding bytes. The value is between 0 and 255; the maximum value is rare.
  - **Next header.** The 8-bit next-header field is similar to that defined in the AH Protocol. It serves the same purpose as the protocol field in the IP header before encapsulation.
  - **Authentication data.** Finally, the authentication data field is the result of applying an authentication scheme to parts of the datagram. Note the difference between the authentication data in AH and ESP. In AH, part of the IP header is included in the calculation of the authentication data; in ESP, it is not.
- **ESP provides source authentication, data integrity, and privacy.**

INTERNET KEY EXCHANGE (IKE)

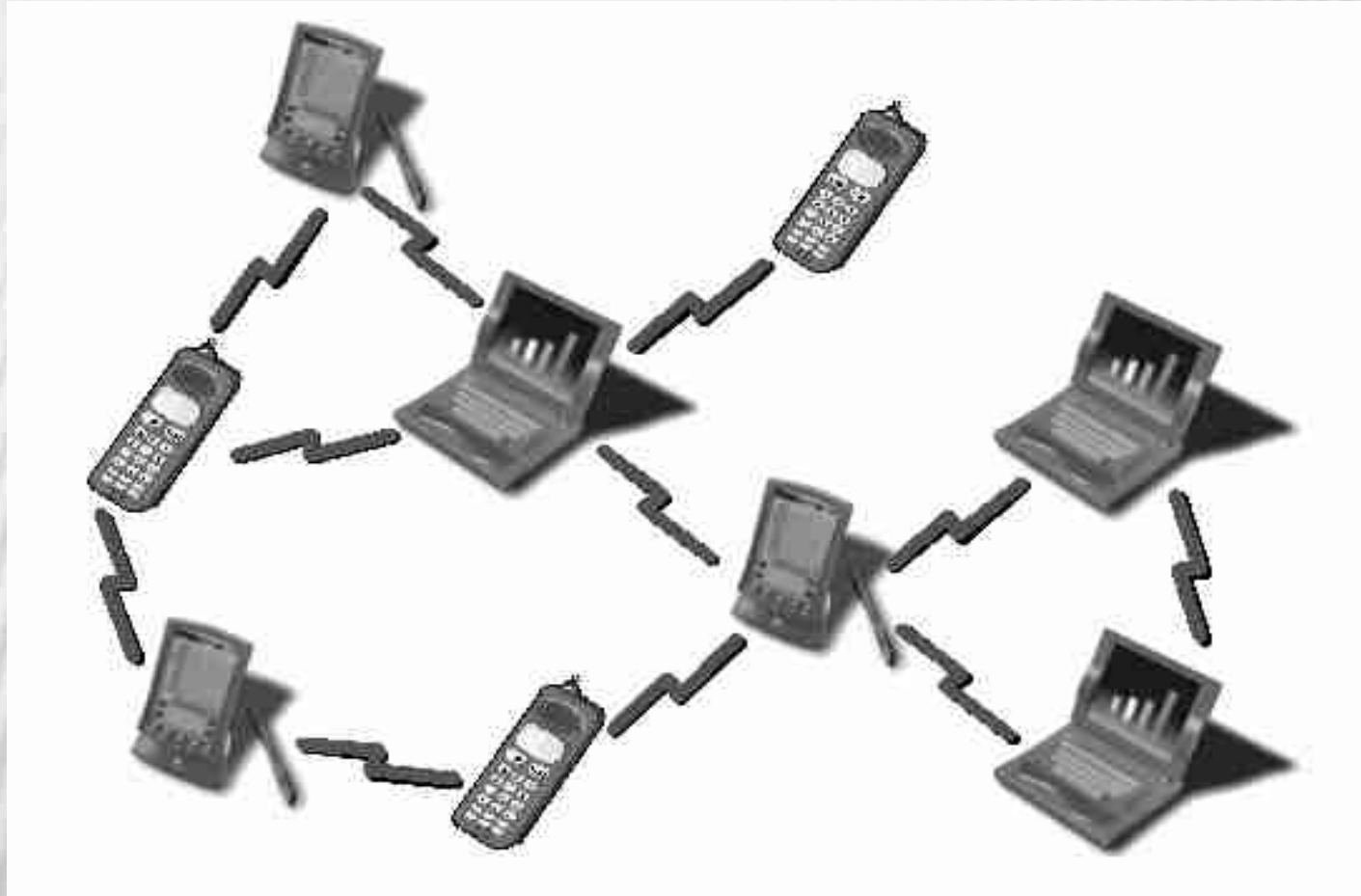
- History
- Photuris
- Simple Key-management for Internet Protocols (SKIP)
- IKE Phases
- IKE Encoding

ADHOC NETWORKS

- Features
- Adantages and Applications
- Adhoc versus Cellular Networks
- Network Architecture
- Protocols: MAC Protocols, Routing Protocols, Technologies

DEFINITION

- An Ad-hoc network is a local area network or some other small network, especially one with wireless devices, in which some of the network devices are the part of the network only for the duration of a communications session.
- Ad-hoc Network is a collection of mobile wireless nodes forming a network without the aid of any infrastructure or centralized administration, where nodes having limited transmission range act as a routers.
- A network without any base stations “infrastructure-less” or multi-hop. A collection of two or more devices equipped with wireless communications and networking capability infrastructure network. It supports anytime and anywhere computing.



TYPES OF AD HOC NETWORKS

- MANET
- WSN
- WMN
- VANETs

PRINCIPLE

- The principle behind ad hoc networking is multi-hop relaying in which messages are sent from the source to the destination by relaying through the intermediate hops (nodes).
- In multi-hop wireless networks, communication between two end nodes is carried out through a number of intermediate nodes whose function is to relay information from one point to another.
- In the last few years, efforts have been focused on multi-hop "ad hoc" networks, in which relaying nodes are in general mobile, and communication needs are primarily between nodes within the same network.

FEATURES

- Dynamic topology
- Variability of the radio channel
- Do not require network infrastructure
- Using multi-hop communications
- Limited bandwidth
- Allows new network devices to be quickly added.
- Each user has a unique network address that is recognized as the part of the network.
- Collection of nodes that do not rely on a predefined infrastructure
- Auto-configurable network and Self organizing
- Nodes are mobile and hence have dynamic network topology.
- Nodes in ad-hoc networks play both the roles of routers and terminals.
- Routing protocol required

EXAMPLES

- Classroom
  - Ad hoc network between student PDAs and workstation of the instructor
- Large IT campus
  - Employees of a company moving within a large campus with PDAs, laptops, and cell phones
- Moving soldiers with wearable computers
  - Eavesdropping, denial-of-service and impersonation attacks can be launched
- Shopping mall, restaurant, coffee shops
  - Customers spend part of the day in a networked mall of specialty shops, coffee shops, and restaurants

ADVANTAGES

- No expensive infrastructure must be installed
- Independence from central network administration
- Use of unlicensed frequency spectrum
- Self-configuring, nodes are also routers
- Self-healing through continuous re-configuration
- Scalable: accommodates the addition of more nodes
- Flexible: similar to being able to access the Internet from many different locations
- Quick distribution of information around sender
- Use of ad-hoc networks can increase mobility and flexibility, as ad-hoc networks can be brought up and torn down in a very short time.

- Ad-hoc networks can be more economical in some cases, as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes.
- Because of multi-hop support in ad-hoc networks, communication beyond the Line of Sight (LOS) is possible at high frequencies.
- Multi-hop ad-hoc networks can reduce the power consumption of wireless devices. More transmission power is required for sending a signal over any distance in one long hop than in multiple shorter hops
- Reduced interference levels, increases spectrum reuse efficiency, and makes it possible to use unlicensed unregulated frequency bands(Because of short communication links radio emission levels can be kept low).

DISADVANTAGES

- Each node must have full performance
- Throughput is affected by system loading
- Reliability requires a sufficient number of available nodes. Sparse networks can have problems
- Large networks can have excessive latency (high delay), which affects some applications

APPLICATIONS

- Military Applications
  - Establishing communication among a group of soldiers for tactical operations
  - Coordination of military object moving at high speeds such as fleets of airplanes or ships
  - Requirements: reliability, efficiency, secure communication, and multicasting routing,
- Collaborative and Distributed Computing
  - Conference, distributed files sharing
- Emergency Operations
  - Search, rescue, crowd control, and commando operations
  - Support real-time and fault-tolerant communication paths
- Personal Area Networks (PANs)
- Environmental monitoring
  - used to predict water pollution or to provide early a natural catastrophe warning.
- Peer to Peer Networks

- Disaster recovery
- Battlefield
- 'Smart' office

Rapidly deployable infrastructure

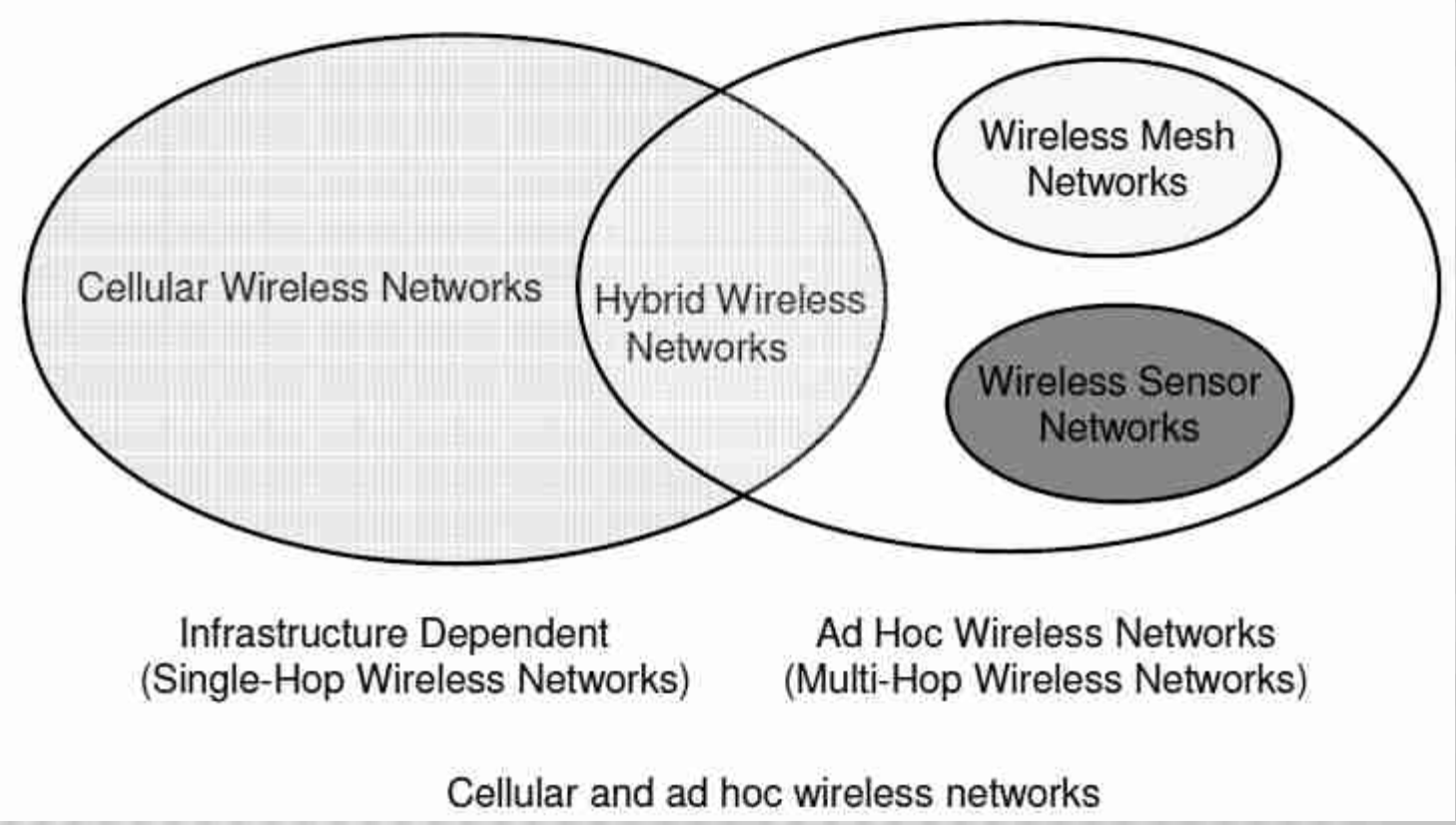
- Wireless: cabling impractical
- Ad-Hoc: no advance planning

Backbone network: wireless IP routers

- Network of access devices
  - Wireless: untethered
  - Ad-hoc: random deployment
- **Edge network**: Sensor networks, Personal Area Networks (PANs), etc.

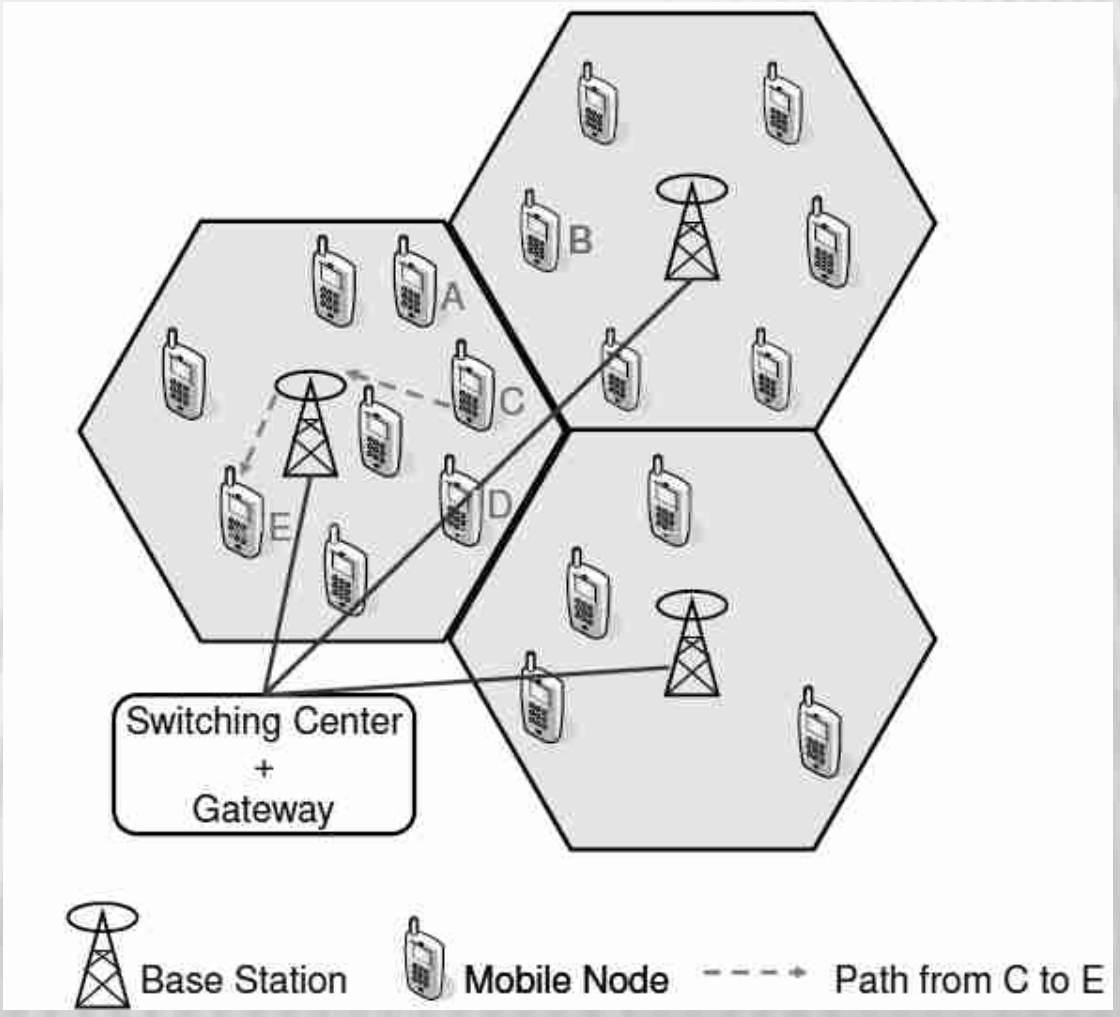
ADHOC VS CELLULAR NETWORKS

- Ad Hoc Networks
- multi-hop radio relaying and without support of infrastructure
  - Wireless Mesh Networks
  - Wireless Sensor Networks
- Cellular Wireless Networks
- infrastructure dependent network



Cellular and ad hoc wireless networks

CELLULAR NETWORK

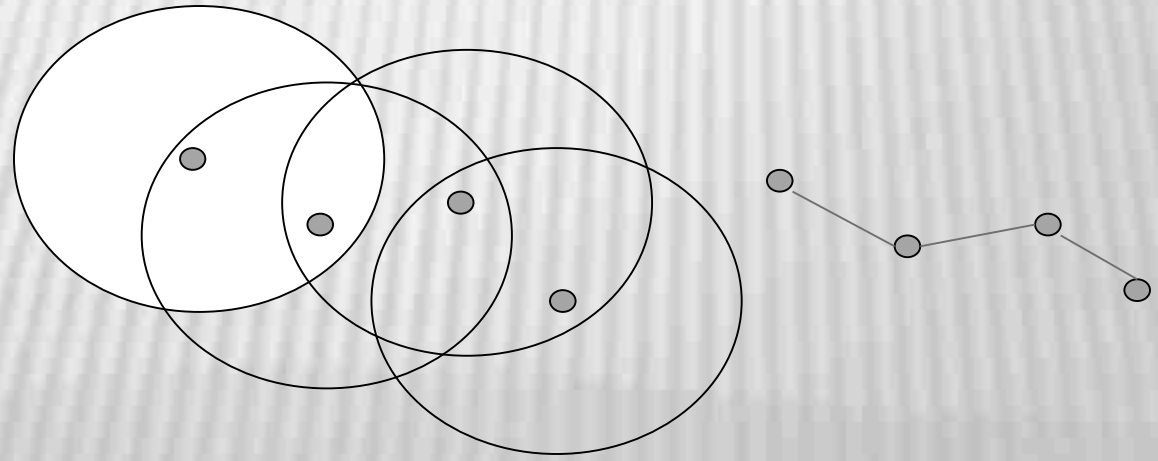


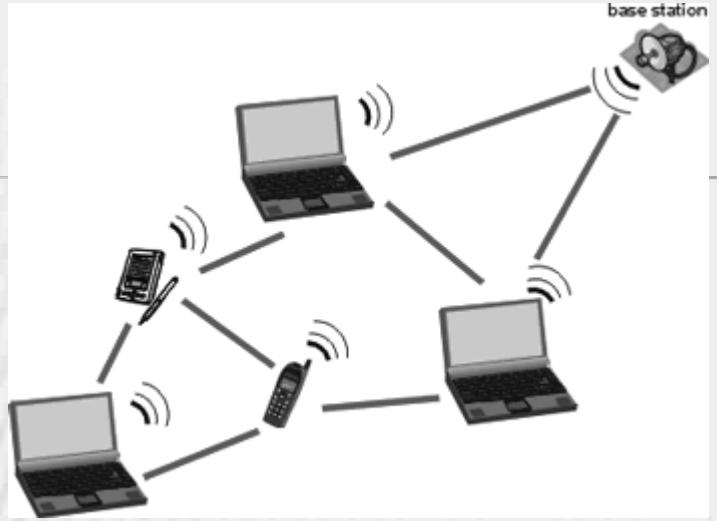
SINGLE HOP COMMUNICATION (CELLULAR NETWORKS)

- Single hop wireless connectivity to the wired world
  - Space divided into cells
  - A base station is responsible to communicate with hosts in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station

MULTI HOP COMMUNICATION (ADHOC NETWORKS)

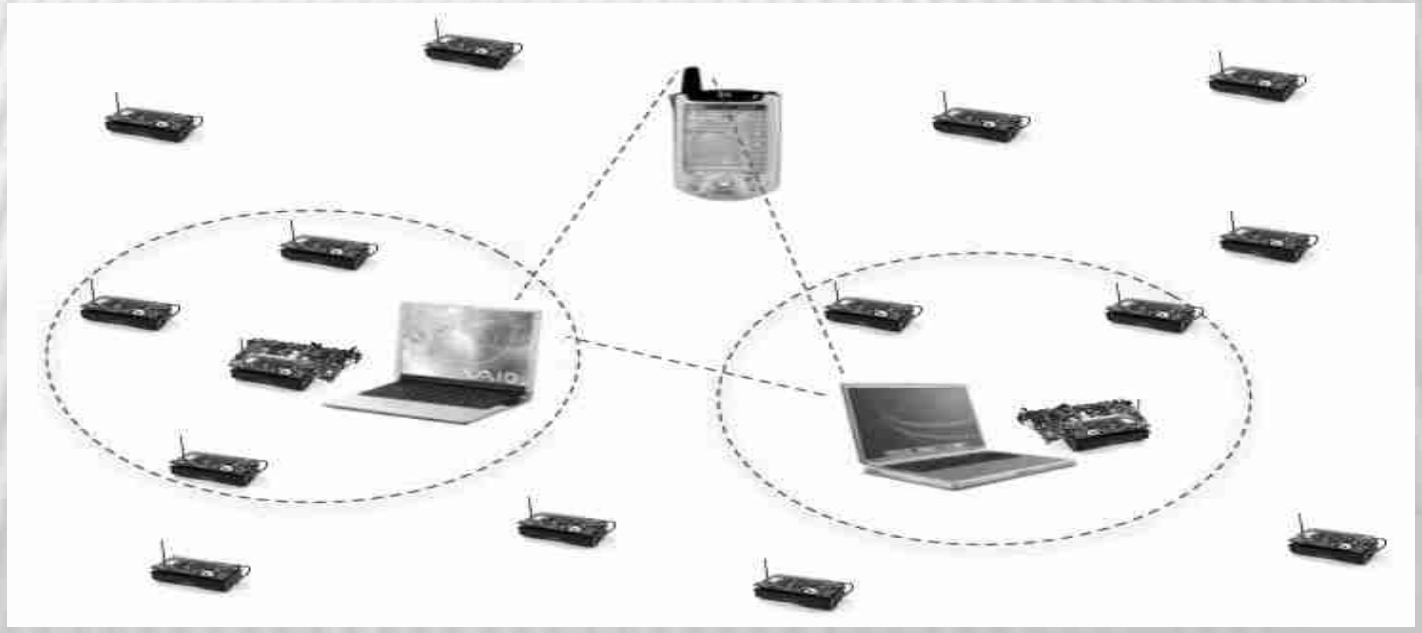
- May need to traverse multiple links to reach destination
- Mobility causes route changes





Single hop
Architecture

Multi hop
Architecture



DIFFERENCES BETWEEN AD-HOC WIRELESS NETWORKS AND CELLULAR NETWORKS

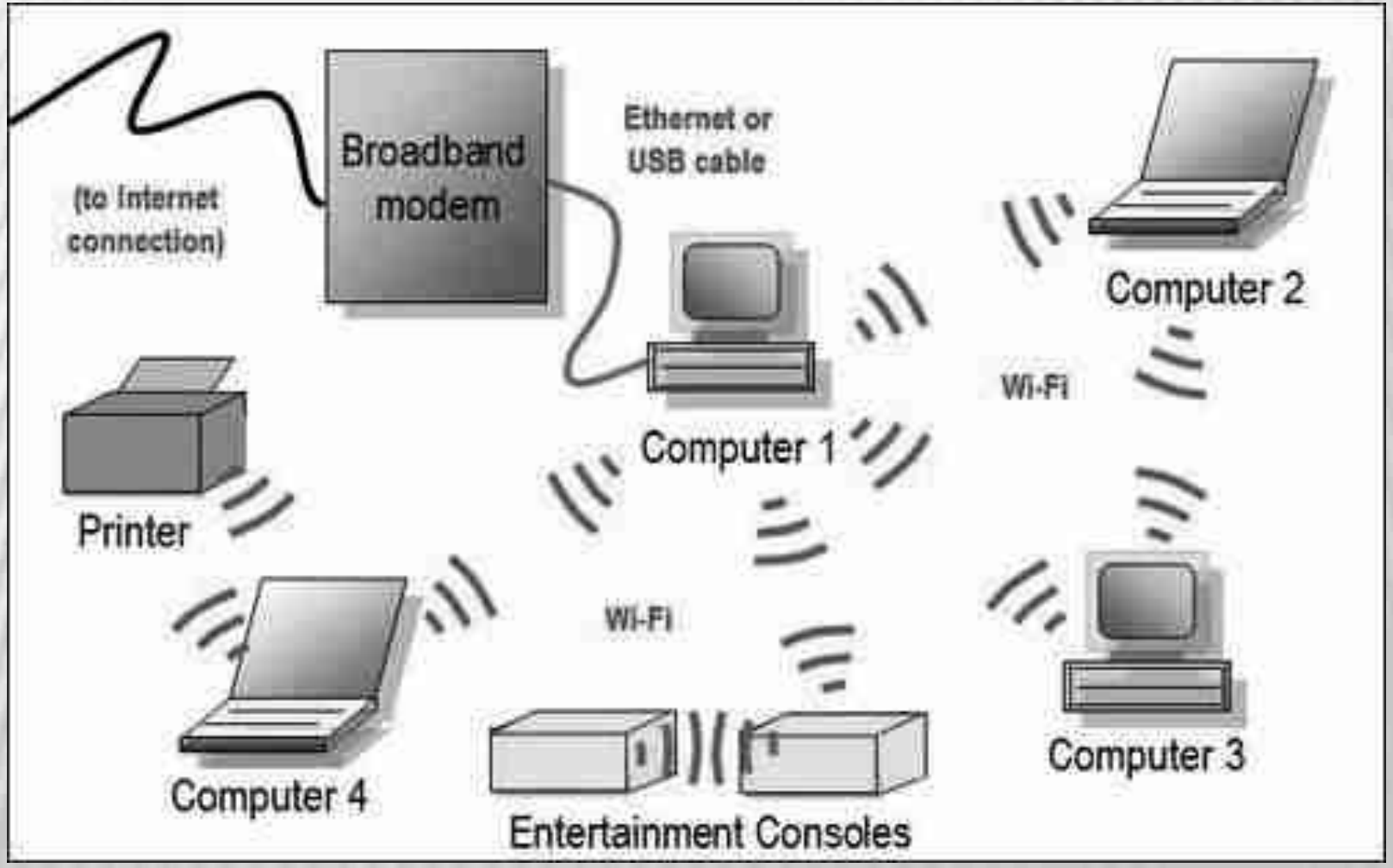
Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequency path break due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism

Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sector	Application domains include battlefields, emergency search and rescue operation, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capacity)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Man aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

NETWORK ARCHITECTURE

- There are two architectures available: **standalone** (Ad Hoc Mode) and
- **centrally coordinated** (Infrastructure Mode)

STANDALONE ARCHITECTURE (AD HOC MODE)

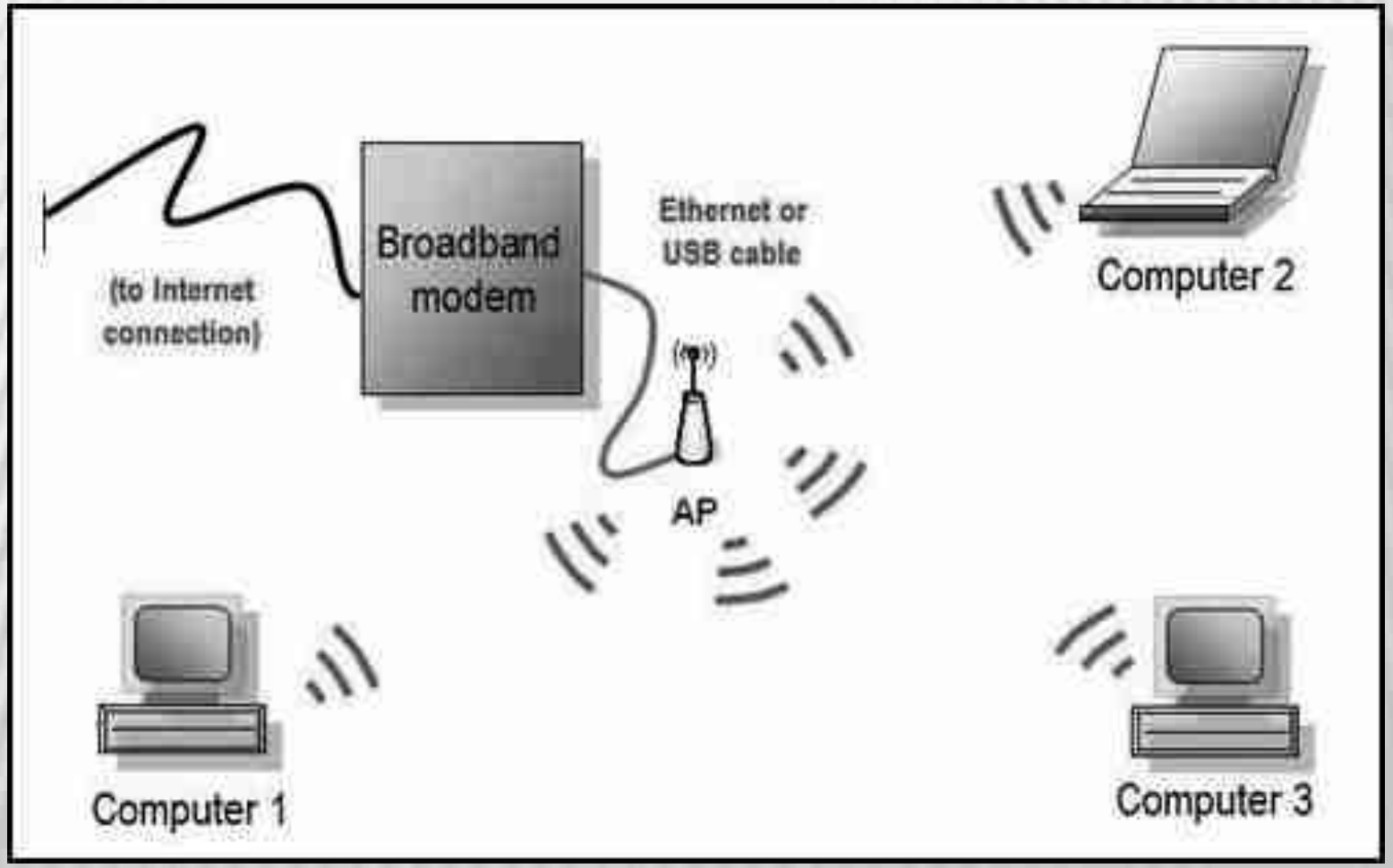


- By using ad hoc mode, all devices in the wireless network are directly communicating with each other in peer to peer communication mode.
- No access point (routers/switches) is required for communication between devices.
- For setting up ad hoc mode, we need to manually configure the wireless adaptors of all devices to be at ad hoc mode instead of infrastructure mode, and all adaptors must use the same channel name and same SSID for making the connection active.

- Ad hoc mode is most suitable for small group of devices and all of these devices must be physically present in close proximity with each other.
- The performance of network suffers while the number of devices grows.
- Disconnections of random device may occur frequently and also, ad hoc mode can be a tough job for network administrator to manage the network.
- Ad hoc mode has another limitation is that, ad hoc mode networks cannot bridge to wired local area network and also cannot access internet if without the installation of special gateways.
- However, Ad hoc mode works fine in small environment. Because ad hoc mode does not need any extra access point (routers/switches), therefore it reduces the cost.
- Ad hoc can be very useful as a backup option for time being if network based on centrally coordinated wireless network (infrastructure mode) and access points are malfunctioning.

- An ad hoc mode uses the integrated functionality of each adaptor to enable wireless services and security authentication.
- The characteristics of an Ad hoc wireless network are listed as below:
  - All access points in the network operate independently and has own configuration file.
  - Access point is responsible for the encryption and decryption.
  - The network configuration is static and does not respond to changing network conditions.

CENTRALLY COORDINATED ARCHITECTURE (INFRASTRUCTURE MODE)



- The other architecture in wireless network is centrally coordinated (infrastructure mode).
- All devices are connected to wireless network with the help of Access Point (AP).
- Wireless APs are usually routers or switches which are connected to internet by broadband modem.
- Infrastructure mode deployments are more suitable for larger organizations or facility. This kind of deployment helps to simplify network management, and allows the facility to address operational concerns. And resiliency is also assured while more users can get connected to the network subsequently.
- The infrastructure mode provides improved security, ease of management, and much more scalability and stability. However, the infrastructure mode incurs extra cost in deploying access points such as routers or switches.

- An infrastructure mode wireless network has the characteristics as below:
  - The wireless centralized controller coordinates the activity of access point.
  - The controller is able to monitor and control the wireless network by automatically reconfiguring the access point parameters in order to maintain the health of the network.
  - The wireless network can be easily expanded or reduced by adding or removing access points and the network can be reconfigured by the controller based on the changes in RF footprint.
  - Tasks such as user authentication, fault tolerance, control of configuration, policy enforcement and expansion of network are done by the wireless network controller.
  - Redundant access points can be deployed in separate locations to maintain control in the event of an access point or switch failure.

INTERNET KEY EXCHANGE (IKE)

SECURITY ASSOCIATION

- An IPsec security association (SA) is a cryptographically protected connection.
- Associated with each end of the SA is a cryptographic key and other information such as the identity of the other end, the sequence number currently being used, and the cryptographic services being used (e.g., integrity only, or encryption + integrity, and which cryptographic algorithms should be used).
- The SA is considered unidirectional, so a conversation between Alice and Bob will consist of two SAs, one in each direction.

- The IPsec header includes a field known as the SPI (SECURITY PARAMETER INDEX) which identifies the security association, allowing Alice to look up the necessary information (such as the cryptographic key) in her SA database.
- The SPI value is chosen by the destination (Bob), so it would seem as though the SPI alone should allow Bob to know the SA, since Bob can ensure that the SPI is unique with respect to all the sources that Bob has SAs with.
- But it is possible for Bob to also be receiving multicast data, in which case Bob would not have chosen the SPI, and it might be equal to one that Bob already assigned.
- Therefore the SA is defined by both the SPI and the destination address. (The destination address of a packet received by Bob will be Bob for unicast, or a group address if it's multicast.)
- Furthermore, IPsec allows the same SPI values to be assigned to different SAs if one SA is using AH and one is using ESP, so the SA is defined by the triple <SPI, destination address, flag for whether it's AH or ESP>.

SECURITY ASSOCIATION DATABASE

- A system implementing IPsec keeps a security association database.
- When transmitting to IP destination X, the transmitter looks up X in the security association database, and that entry will tell it how to transmit to X, i.e., it will provide the SPI, the key, the algorithms, the sequence number, etc.
- When receiving an IP packet, the SPI of the received packet is used to find the entry in the security association database that will tell the receiver which key, sequence number, etc., to use to process the packet.

WHAT IS IKE?

- The Internet Key Exchange (IKE) protocol is a key management protocol standard, which is used in conjunction with the IPsec standard, for doing mutual authentication and establishment of a shared secret key to create an IPsec Security Authentication (SA).
- It is described in RFC 2409.
- IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.
- IPsec security associations (SAs) must exist in order for IPsec to protect network traffic.
- IKE manages those SAs on behalf of IPsec, and automatically negotiates protection policies between IPsec peers.

- IKE is a hybrid protocol based on the Internet Security Association and Key Management Protocol (ISAKMP), described in RFC 2408.
- The IKE protocol implements parts of two other key management protocols–-Oakley, described in RFC 2412, and SKEME.
- The protection policy within SAs is negotiated and established with the help of the ISAKMP protocol, and keying material (session keys for encryption and packet authentication) is agreed on and exchanged with the use of Oakley and SKEME protocols.

- The intention of IKE is to do mutual authentication using some sort of long term key (pre-shared secret key, public signature-only key, or public encryption key), and establish a session key.
- In addition to variants necessitated by having different types of keys, there are variants depending on what features you want (e.g., hiding endpoint identifiers, or the ability to negotiate cryptographic algorithms rather than having them chosen by the initiator), trading off those features against extra messages.

KEY TERMS IN IKE

ISAKMP

- The Internet Security Association and Key Management Protocol is a protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.
- ISAKMP is implemented according the latest version of the "Internet Security Association and Key Management Protocol (ISAKMP)" standard.
- ISAKMP establishes a secure management session between IPsec peers, which is used to negotiate IPsec SAs.
- ISAKMP provides the means to authenticate the remote peer, cryptographically protect the management session, exchange information for key exchange, and negotiate all traffic protection parameters using configured security policies.
- Therefore, the goal of ISAKMP is the establishment of an independent security channel between authenticated peers in order to enable a secure key exchange and the negotiation of IPsec SAs between them.

OAKLEY

- A key exchange protocol that defines how to derive authenticated keying material.
- Oakley is originally a free-form protocol that allows each party to proceed with the exchange at its own speed. IKE borrowed this idea from Oakley, and defines the mechanisms for key exchange in different modes over the IKE (ISAKMP) session.
- Each protocol produces a similar result—an authenticated key exchange, yielding trusted keying material used for IPsec SAs.
- Oakley, within IKE, determines AH and ESP keying material (authentication and encryption session keys) for each IPsec SA automatically, and by default uses an authenticated Diffie-Hellman algorithm to accomplish this.

- **SKEME**
  - A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.
- **Diffie-Hellman algorithm**
  - Diffie-Hellman algorithm was discovered in 1976 by Whitfield Diffie and Martin Hellman.
  - It gets its security from the difficulty of calculating the discrete logarithms of very large numbers.
  - The Diffie-Hellman algorithm is used for secure key exchange over insecure channels and is used a lot in modern key management to provide keying material for other symmetric algorithms, such as DES or keyed- MD5 (HMAC).

HISTORY OF IKE

- While SKIP and Photuris proponents were fighting with each other, ISAKMP (Internet Security Association and Key Management Protocol, RFC 2408) emerged, a gift to the IETF from the NSA.
- ISAKMP wasn't a protocol but was a framework in which fields could be exchanged to create a protocol.
- It is specified as running over UDP rather than TCP, and is woefully underspecified on issues such as what happens when messages get lost.
- Given how thrilled IETF usually is at anything having to do with the NSA, and given how ISAKMP didn't actually do anything, it was astonishing that the IETF embraced it and decided that IPsec would somehow have to operate within the ISAKMP framework.
- Adopting ISAKMP gave an excuse not to adopt either SKIP or Photuris, because once the requirement of working with ISAKMP was assumed, neither protocol met that requirement.

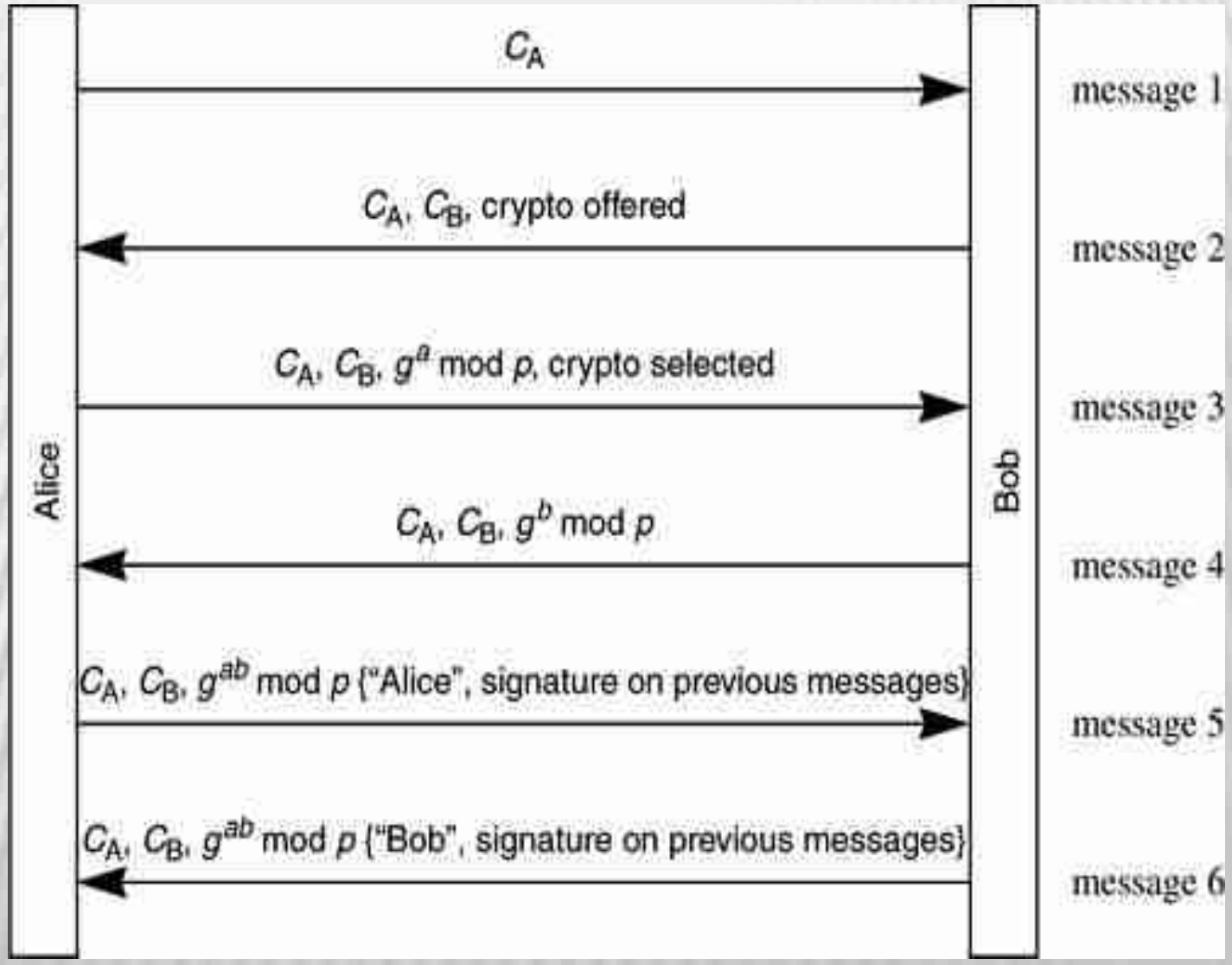
- Another document was written, supposedly as a protocol that would work within the ISAKMP framework, and that was called OAKLEY (RFC 2412).
- Another proposal was SKEME.
- Then IKE (RFC 2409) was written, crediting ideas from OAKLEY and SKEME, and using ISAKMP syntax.
- But even at that it was incomplete, and there's another document, The Internet IP Security Domain of Interpretation for ISAKMP (RFC 2407) that defines a lot of the fields.
- ISAKMP's idea of a domain of interpretation (DOI) is that a DOI specifies a particular use of ISAKMP, and the intention is that for each DOI value there would be a specification that would define what all the parameters mean for that DOI value.
- So you need RFCs 2407, 2408, and 2409 in order to know how to implement IKE.

- The distinction between IKE and ISAKMP is very confusing.
- Probably the best way to think of it is that IKE is a profiling (i.e., defining fields, choosing options) of ISAKMP, but it isn't that straightforward.
- The impression is that the IKE authors attempted to make their document self-contained but ran out of energy and deferred to the ISAKMP spec for encodings.
- The terms tend to be used inconsistently, adding to the confusion.
- For instance, a direct quote from the IKE spec (RFC 2409):

  While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.

PHOTURIS

- Photuris was one of the two main candidates for this piece of IPsec (the other being SKIP).
- Photuris was basically a signed Diffie-Hellman exchange, with identity hiding by first doing an anonymous Diffie-Hellman, and using an initial stateless cookie.
  - Alice transmits C_A, which Photuris calls a cookie, but it's not for the same purpose as Bob's stateless cookie C_B.
  - C_A is just a way for Alice to keep connection attempts separate, in case she is initiating multiple simultaneous connections to Bob.
  - Messages 3 and 4 consist of the Diffie-Hellman exchange, and the resulting Diffie-Hellman key is used to encrypt the identities in messages 5 and 6.
  - In addition to the identities, the signatures on the previous messages are sent in message 5 and 6.


Alice
Bob
C_A
message 1
C_A, C_B, crypto offered
message 2
C_A, C_B, g^a mod p, crypto selected
message 3
C_A, C_B, g^b mod p
message 4
C_A, C_B, g^{ab} mod p {"Alice", signature on previous messages}
message 5
C_A, C_B, g^{ab} mod p {"Bob", signature on previous messages}
message 6

- This is somewhat simplified.
- There's also crypto parameter negotiation, and choosing of SPI values for each direction. SPI identifies the SA.
- C_B is for denial of service protection.
- It is desirable for Bob to be stateless until message 3 (when he knows that Alice can return a valid cookie).
- The only way he can do this is to reuse his Diffie-Hellman secret number b for many connections.
- But if he always uses the same b, perfect forward secrecy will be lost.
- Therefore he should change his b periodically.

SIMPLE KEY-MANAGEMENT FOR INTERNET PROTOCOLS (SKIP)

- SKIP (Simple Key-Management for Internet Protocols) has some interesting ideas, and was at one point widely deployed.
- SKIP uses long term Diffie-Hellman public keys (e.g., $g^a \bmod p$).
  - Assuming Alice knows Bob's public key ($g^b \bmod p$), and her own private key (a), then she can compute $g^{ab} \bmod p$, the shared secret between herself and Bob, thus establishing a session key in zero messages!
  - If they don't already know each other's public keys, they would have to send each other certificates, or retrieve certificates from a directory, in which case it wouldn't be zero messages, of course.

- It's bad cryptographic practice to use a key for encrypting a lot of data.
- So SKIP doesn't use the shared key $X = g^{ab} \bmod p$ for encrypting the data.
- It only uses it for encrypting the data encryption key.
- Each packet of data is encrypted with some key S, and has a SKIP header that contains X{S}.
- You could use the same S for many packets, and would be able to tell efficiently (without needing to decrypt X{S}) that the key was still S because the header would start with the same value of X{S}. Or you could change the key on every packet.
- The SKIP designers really liked this feature because it somewhat got around the 40-bit key limit imposed at that time by the U.S. government.
- Although S was only 40 bits, if a conversation involves breaking 1000 Ss, then an attacker had 2^{50} amount of work to do to decrypt an entire conversation.

- Later SKIP was modified in order to meet some of the objections of the IPsec working group.
- Perfect forward secrecy was added, which meant periodically doing more Diffie-Hellman exchanges, and the data packet format used AH and ESP, which added more complexity since SKIP's idea of including X{S} in each packet was not all that well-suited to being encoded with AH and ESP.
- Although widely deployed before IKE, once IKE was standardized most deployments migrated to IPsec.

IKE PHASES

- IKE defines two phases.
- Phase 1 does mutual authentication and establishes session keys.
- It is based on identities such as names, and secrets such as public key pairs, or pre-shared secrets between the two entities.
- Then using the keys established in phase 1, multiple phase-2 SAs between the same pair of entities can be established.
- The phase-1 exchange is known as the ISAKMP SA, or sometimes it is referred to as the IKE SA.
- An ESP or AH SA would be established through phase 2.

- Why not just establish an ESP or AH SA in a single exchange and not bother with a separate phase 2?
- It would certainly be simpler and cheaper to just set up an SA in a single exchange, and do away with the phases, but the theory is that although the phase-1 exchange is necessarily expensive (if based on public keys), the phase-2 exchanges can then be simpler and less expensive because they can use the session key created out of the phase-1 exchange.
- This reasoning only makes sense if there will be multiple phase-2 setups inside the same phase-1 exchange.

- Here are some arguments people give for the two phases:
  - The ISAKMP designers assumed ISAKMP would be used by more than just IPsec, and in addition to setting up IPsec (e.g., AH, ESP) SAs, it might be used to establish SAs for other protocols.
  - The IETF even assigned values for DOI for some routing protocols such as RIP and OSPF, but never wound up designing exchanges for them.
- And indeed since those protocols run on top of IP, they didn't need their own protocol. They could use IPsec.
- Some people advocate setting up different SAs for different traffic flows (conversations).
  - In that case, a firewall-to-firewall link might require many SAs, one perhaps for each source/ destination/port pair.
  - Even if the SA is end-to-end, there might be multiple processes on one machine talking to processes on the other.

- The concern is that there might be security weaknesses if different flows used the same key.
- Indeed such a weakness was discovered if the SA used encryption only (no integrity protection).
  - Imagine two machines M_1 and M_2 with an SA over which traffic for many source/destination pairs flows.
  - The source/destination pairs might be applications on M_1 and M_2, or M_1 and M_2 might be firewalls forwarding traffic from one portion of the net to machines on another portion of the net.
  - Suppose there are conversations between A and B, and between C and D that go through the M_1-M_2 SA.
  - If C wants to decrypt a packet sent by A to B, then it can record an encrypted packet between A and B, and between C and D, and splice the first encrypted part (the part that contains the source and destination) from the C-D packet onto the A-B encrypted packet, and forward the packet to M_2.
  - M_2 will decrypt the spliced packet, deliver the decrypted data from the A-B packet to D (because the initial portion of the packet was spliced from a packet that indicated M_2 should forward the packet to D).

- This is not an issue if integrity protection is used, because the spliced packet would not pass the integrity check, and there is no excuse for ever using encryption without integrity protection.
- But because of this bug with multiplexing flows over an encryption-only SA, some people think it is safer not to multiplex flows over an SA.
- Without multiplexing flows, there might then be many SAs between the same pair of machines

- Key rollover is cheaper using phase 2 rather than restarting the phase-1 connection setup.
- You can set up multiple connections with different security properties, such as integrity-only, encryption with a short (insecure, snooper-friendly) key, or encryption with a long key.
- We disagree with this since it would seem logical to use the strongest protection needed by any of the traffic for all the traffic rather than having separate SAs in order to give weaker protection to some traffic.
- There might be some legal or performance reasons to want to use different protection for different forms of traffic, but this should be a relatively rare case not worth optimizing for.
- A cleaner method of doing this would be to have completely different SAs rather than multiple SAs loosely linked together with the same phase-1 SA.

BIBLIOGRAPHY

S. No.	Title of Books	Author	Publication
1.	Wireless Communications: principles and practices (2nd Edition)	Theodore S. Rappaport	Pearson Education
2.	Network Security (2nd Edition)	Charlie Kaufman, Radip Perlman, Mike Speciner	PHI
3.	Wireless and Mobile Networks: concepts and protocols	Sunilkumar S. Manvi, Mahabaleshwar S. Kakkasageri	Wiley India
4.	Computer Communications and Networking Technologies	Michael A. Gallo & William M. Hancock	Cenage Leraning
5.	An Engineering Approach to Computer Networking	S. Keshav	Pearson Education
6.	Computer Networks	Mayank Dave	Cenage Learning