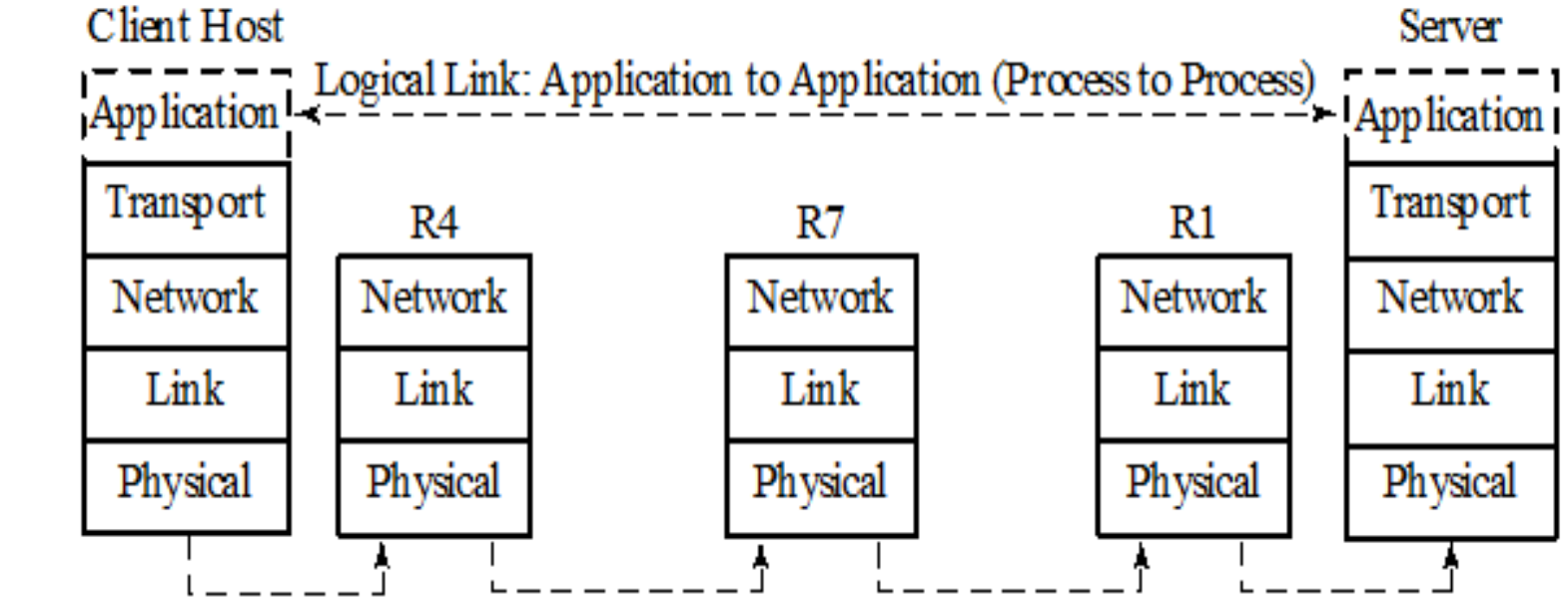
Module 3

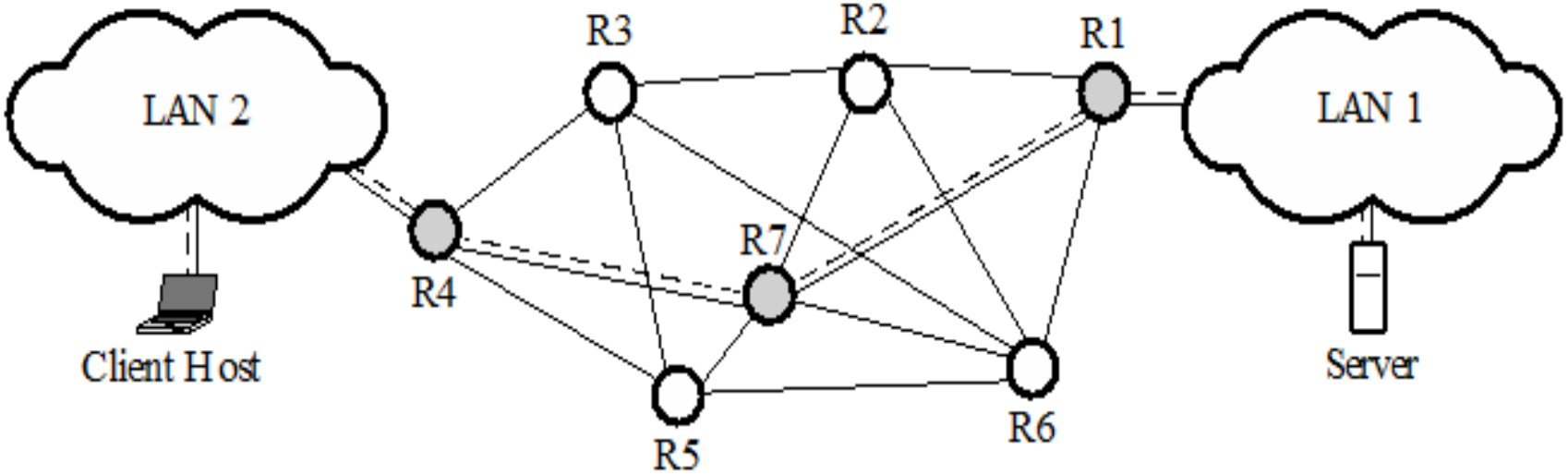
Applications and Network Management

- Application layer overview
- Domain Name System (DNS)
- Remote Login Protocols
- E-mail
- File Transfer and FTP
- World Wide Web and HTTP

Application-Layer Overview

- This provides network services to user applications,
- This provides services such as email, remote access to computers, file transfer, and web etc.
- This has its own software dependencies, i.e. when a new application is developed, its software must be able to run on multiple machines.





Client Server Model

- This provides specific computational services to multiple machines
- A client-host requests services from a server-host.
- Example :remote image processing

Domain Name system

- A domain name is an identification string of a certain network or a network entity.
- Each domain name is identified by one or more IP addresses depending on the size of the domain
- Domain name system - distributed hierarchical and global directory that translates domain names into numerical IP address and vice versa.
- Distributed database system - used to map host names of network domain names to IP addresses

Domain Name System

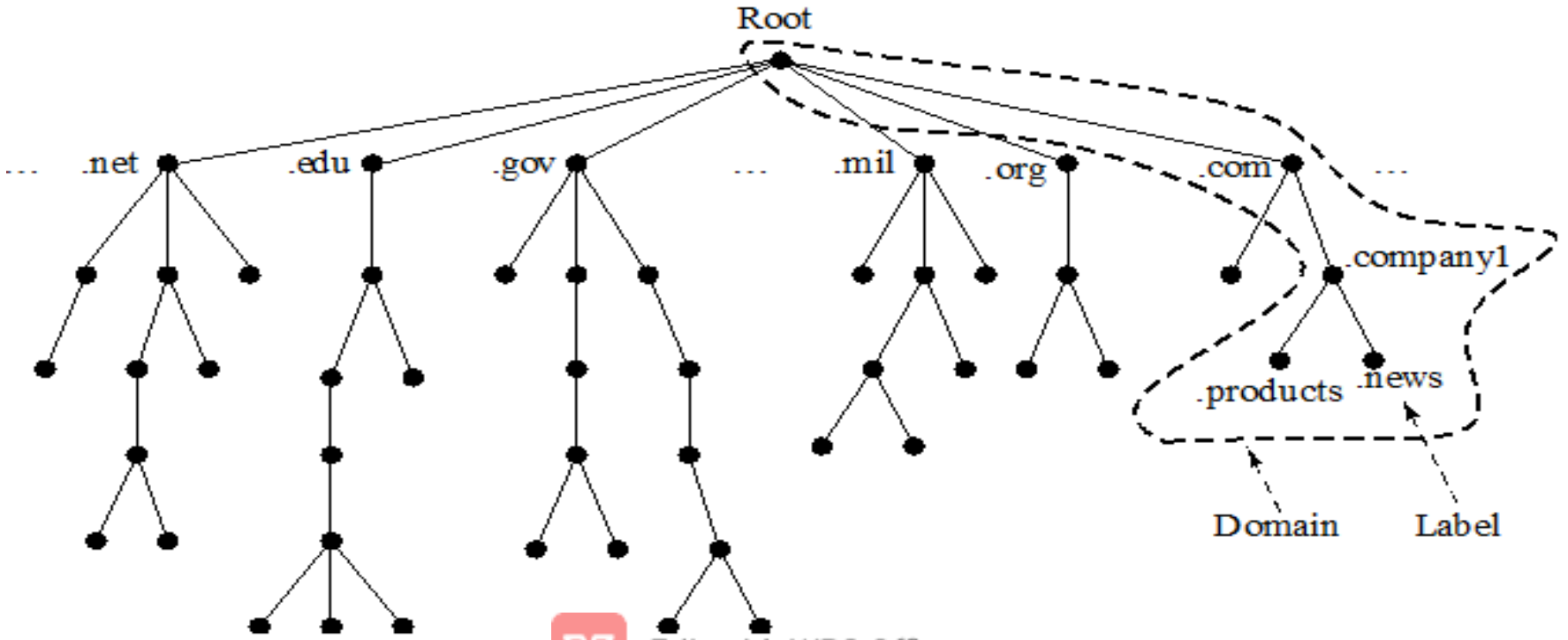
- This is an application-layer protocol
- Follows a tree-based infrastructure – 128 levels starting from level 0.
- all hosts contact DNS to access servers and start connections
- run over either UDP or TCP, however UDP is preferred - fast response
- DNS constructs a query message and passes it to the UDP transport layer without any handshaking
- A UDP header field is attached to the message and resulting segment is passed to the network layer

- Network layer in turn encapsulates the UDP segment into a datagram and this is forwarded to a DNS server
- If the DNS server does not respond – unreliability on the UDP

Domain Name Space

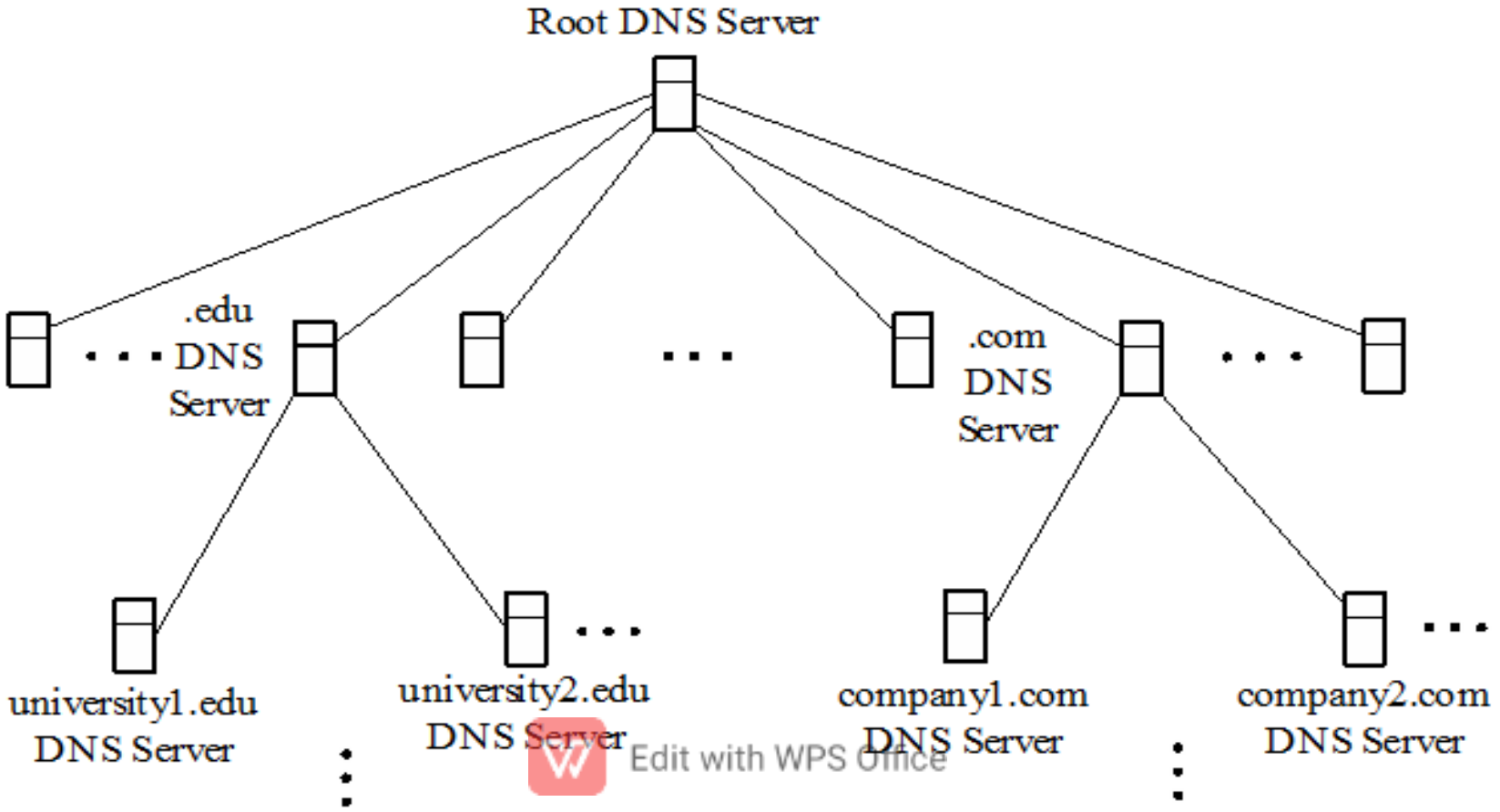
- A network entity with a IP address can be assigned a domain name.
- Unique domain names are selected from the name space and are organized in an hierarchical manner
- Domain Name – Tree based structure with the root at the top
- Each tree can support up to 128 levels starting at level 0 – root
- Each level is comprised of:
  - Nodes
  - Nodes are identified by labels – up to 63 character strings
- Last label of the domain – type of organization; other parts – hierarchy of departments within the organization

- Domain name is a sequence of labels – separated by dots, and is read from the node up to the root
- Domain names can also be defined in a partial manner



DNS servers

- A host sends UDP queries to a DNS server
- Follows a critical infrastructure



Hierarchy of DNS Servers

- A domain name space is divided into sub domains – where each domain or sub domain is assigned a domain name server
- A domain name server has a database – information of every node under that domain
- Each server at any location in the hierarchy can partition part of its domain and delegate the responsibility to another server
- Root server –
  - supervises the entire domain name space
  - Does not contain any information about the domains
  - Maintains references to the servers
  - Distributed all around the world

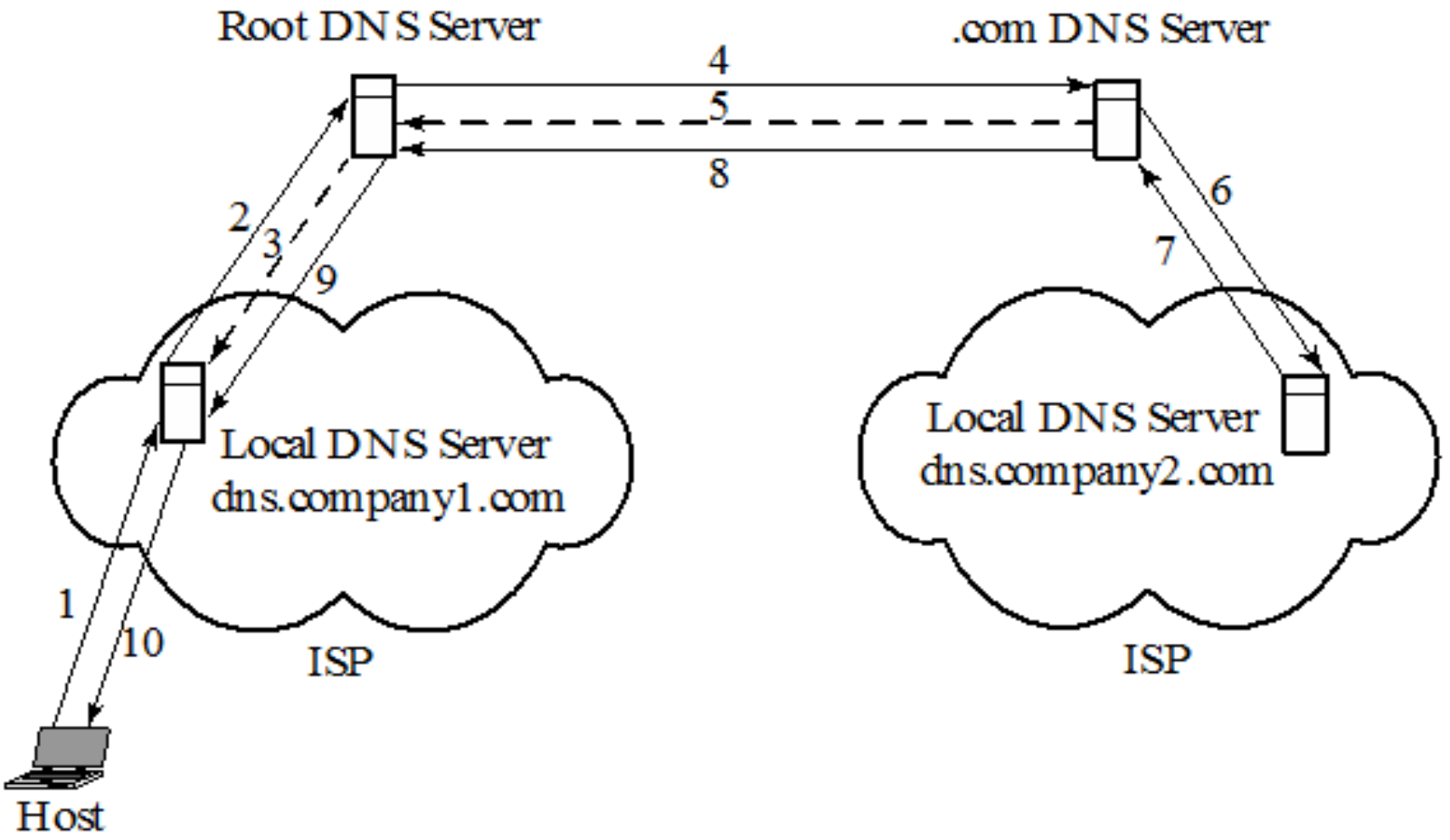
Functions of DNS server

- Finding the address of a particular host.
- Mapping IP addresses to host names.
- Finding an alias for the real name of a host.
- Finding the host type and the operating-system information.
- Naming a host that processes incoming mail for the designated target.
- Delegating a subtree of server names to another server.
- Denoting the start of the subtree that contains cache and configuration parameters, and giving corresponding addresses.

Name/Address Mapping

- Operates based on client/server model
- Client host can send an IP address to a domain name server to be mapped to a domain name
- Steps involved are:
  - Each host need to map an address to a name or vice versa
  - Server finds and releases the requested information back to the host
  - If not found, server delegates the request to other servers or requests for information
  - On receiving the mapping information, host examines it for correctness and then delivers it to requesting process

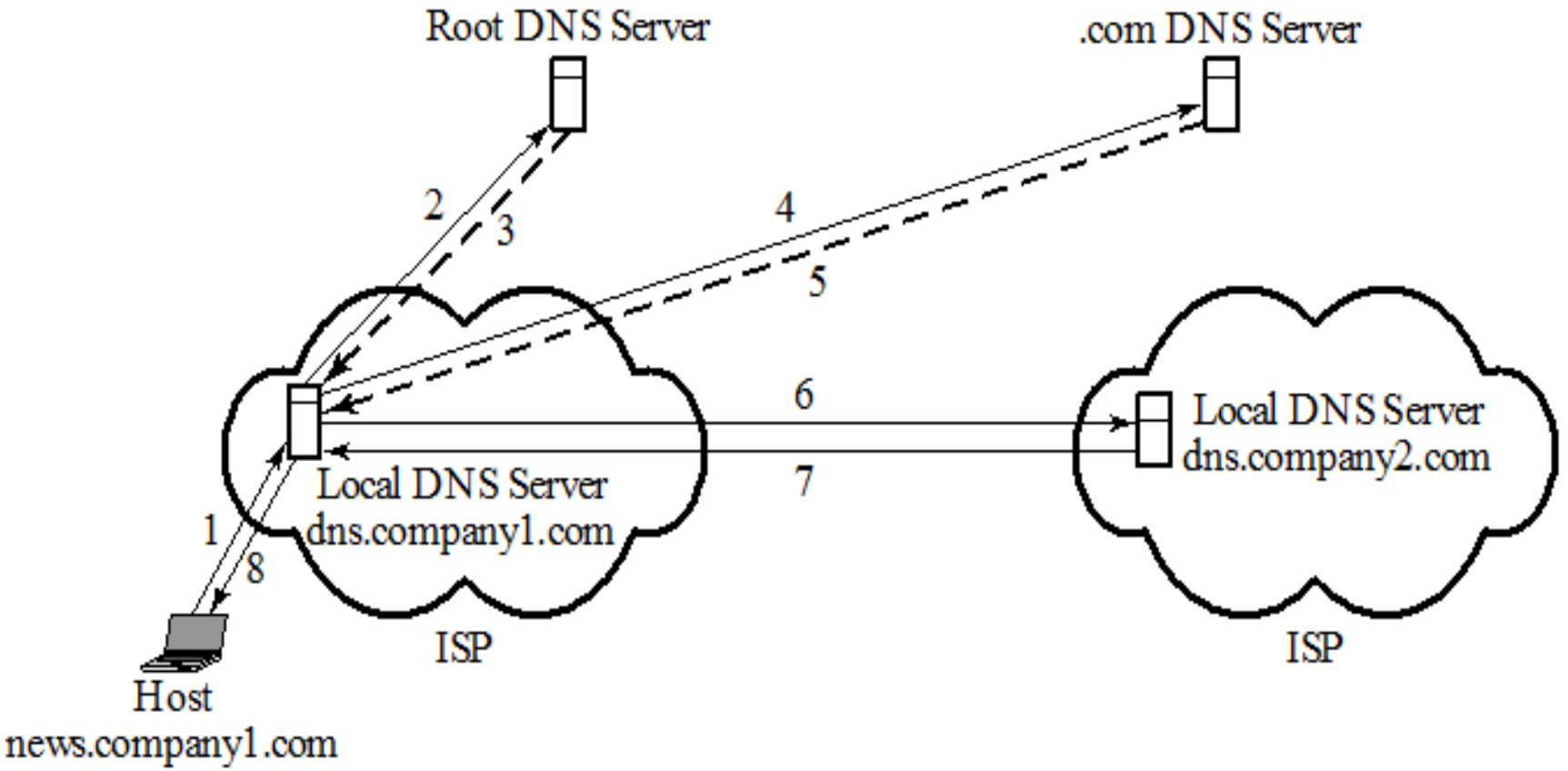
Recursive Mapping



Recursive Mapping

- Client host makes the request to its corresponding DNS server
- DNS server is responsible for finding the answer recursively
- Steps involved:
  - Requesting client host asks for the answer through the local DNS server
  - This server contacts the root DNS server – no information found
  - Root DNS server sends the query to .com server - unsuccessful transaction
  - .com server sends the query to local DNS server – finds the answer
  - The query with the answer is routed back to the origin.
- Local DNS server – where the request initiated – is called as the authoritative server, adds TTL

Iterative Mapping

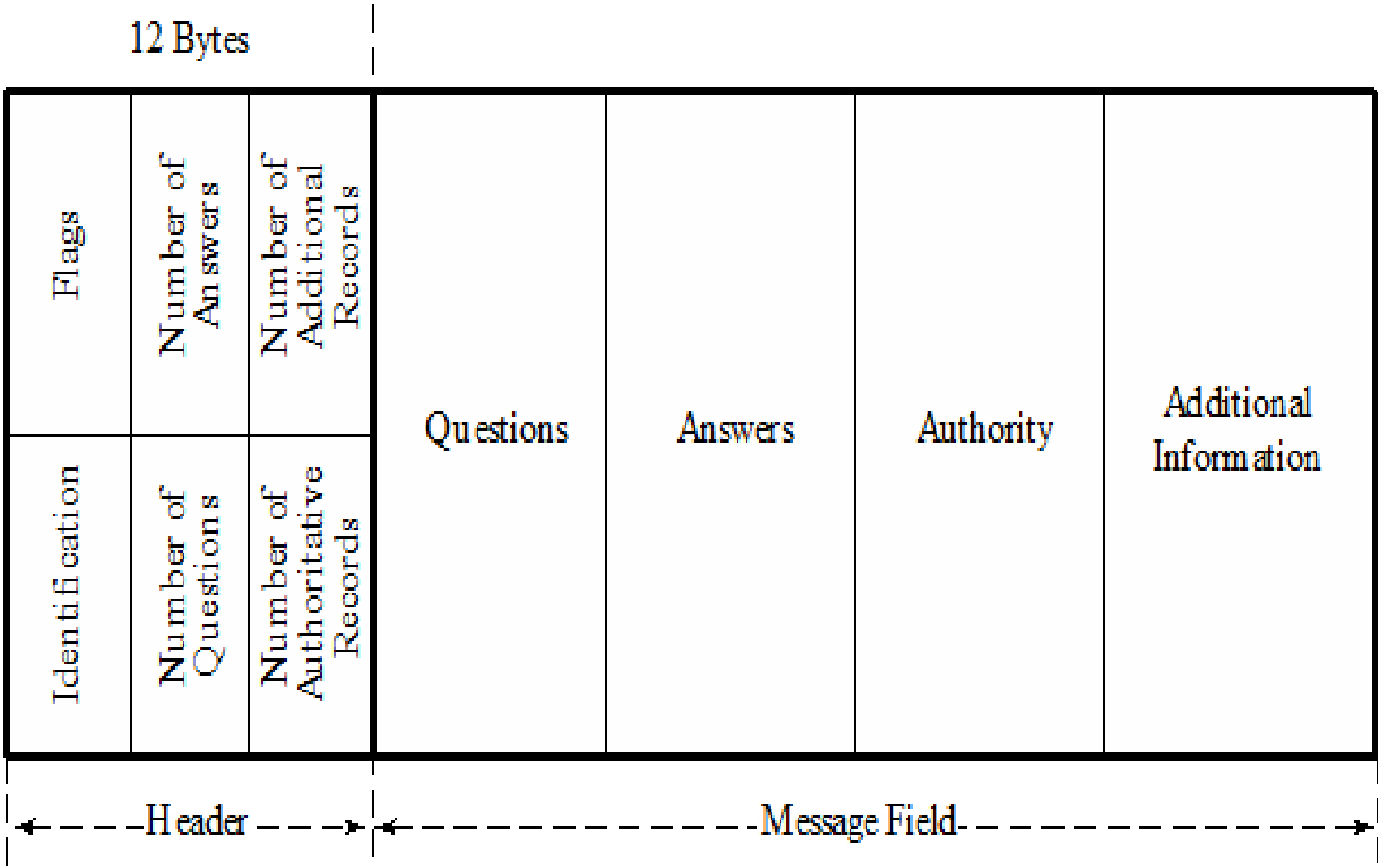


Iterative Mapping

- If the server does not provide the name it returns to the client host
- The host must then repeat the query to next DNS server that may be able to provide the name
- This will continue until the host succeeds in obtaining the name

DNS Message Format

- Communication in DNS is made possible through query and reply messages
- 12 byte header format
- Query message - header + question message
- Reply message – header + question, answer, authority and additional information
- Different fields of the header are:
  - identification field,
  - flags field,
  - number of questions field,
  - number of answers field,
  - number of authoritative records field,
  - number of additional records field



- *Identification*
  - This is used to match the reply with the query.
- *Flags*
  - This represents the type of the message, such as whether mapping is recursive or iterative.
- *Number of questions*
  - This indicates how many queries are in the question portion of the message.
- *Number of answers*
  - This shows how many answers are in the answer field.
- *Number of authoritative records*
  - This consists of the number of authoritative records in the authority portion of a reply message.
- *Number of additional records*
  - These are in the additional information portion of a reply message.
- *Question*
  - This contains one or more questions.
- *Answer*
  - This consists of one or more replies from a DNS server to the corresponding client.
- *Authority*
  - This provides the domain name information about one or more authoritative servers.
- *Additional information*
  - This contains other information such as the IP address of the authoritative server.

Remote Login Protocols

- Using client/server model, a user can establish a session on the remote-machine and then run its applications.
- This application is known as remote login.
- Similar to client server application program which is in need of desired services
- Two protocols:
  - TELNET (Teletype network)
  - Secure Shell (SSH)

TELNET protocol

- TCP/IP standard – used for establishing connection to a remote system.
- This is done by initiating a TCP connection – pass on the details of the application from the user to remote machine
- Logging to remote servers – is based on time sharing where only authorized users with name and password have access

- Properties of TELNET
  - Client-programs are built to use the standard client/server interfaces without knowing the details of server-programs.
  - A client and a server can negotiate data format options
  - Once a connection is established, both ends of the connection are treated symmetrically.
- When a user logs into a remote-server, the client's terminal-driver accepts the keystrokes and interprets them as characters by its operating-system
- Characters are typically transformed to a universal character set called NVT

- The client then establishes a TCP connection to the server
- Texts in the NVT formal are transmitted using a TCP session and are delivered to the operating-system of the remote-server.
- The server converts the characters back from NVT to the local client machine's format
- Using TELNET the clients and servers can negotiate on nonroutine transactions

Secure Shell (SSH) Protocol

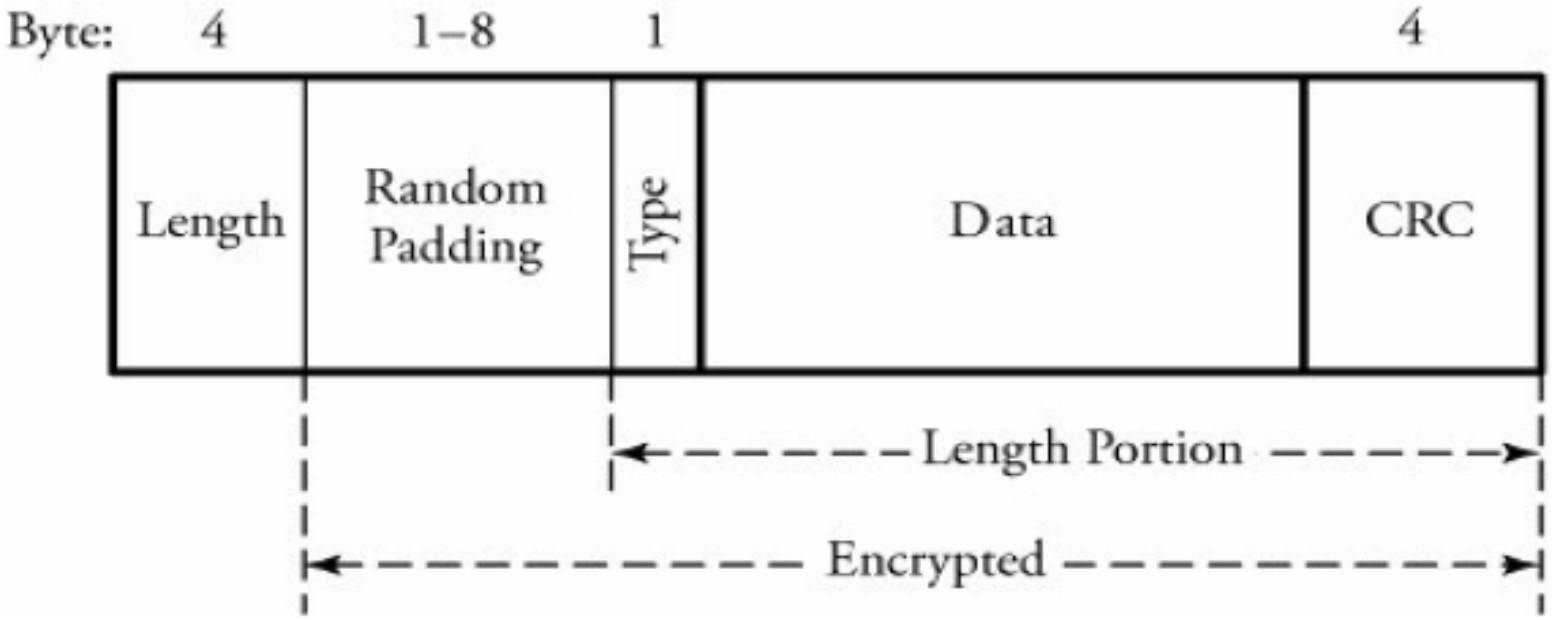
- This is based on UNIX programs.
- TCP for communications.
- More powerful and flexible than TELNET.
- Allows the user to more easily execute a single command on a remote client.
- Advantages compared to TELNET:
  - Security
  - Multiplexing

SSH Security

- Implemented using public-key encryption between client and remote servers
- When a user establishes a connection to a remote server – data transmitted remains confidential
- Implements an authentication process on the messages
- Use of private passwords

SSH Protocol Session

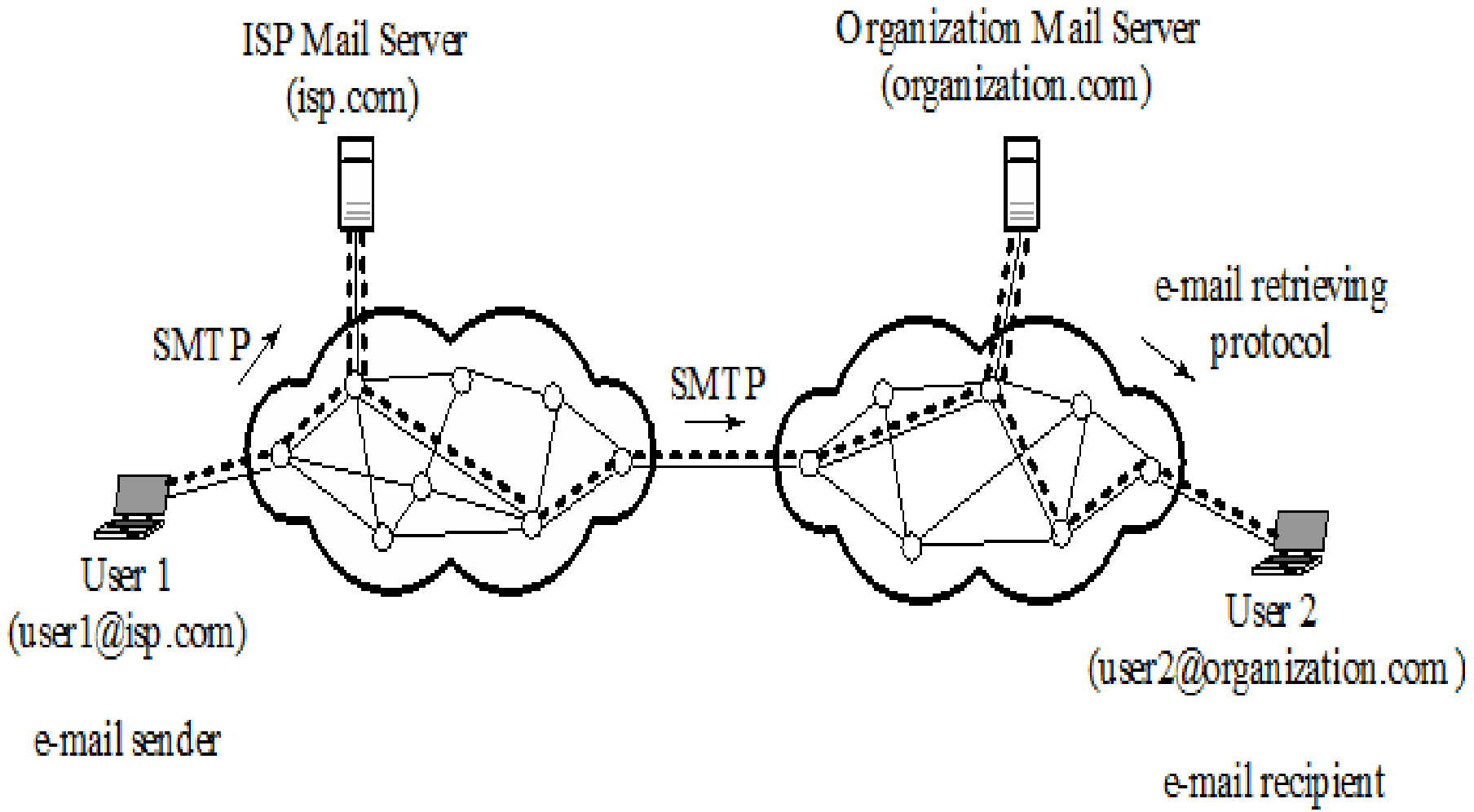
- Server listens to the port that is designated for secure transmissions
- Once the password is submitted, SSH starts a shell for the session
- Several data transfers can be handled simultaneously in the same session



- SSH packet:
  - Length
  - Padding
  - Type
  - CRC

Electronic Mail (e-mail)

- Simple Mail Transfer Protocol
  - SMTP transfers email from the mail-server of a source to the mail-servers of destinations
  - A user-mailbox is a space in the mail-server allocated to the user to keep its email.
  - Push protocol
  - Older than HTTP
  - Limits in the size of e-mail content



Working of SMTP

- User-1 provides user-2's email address(user2@organization.com) and composes its message
- User-1 sends the message to its mail-server(isp.com)
- Server isp.com places the message in its queue.
- SMTP on user 1's mail-server
  - notices the message in the queue and
  - opens a TCP connection with the organization mail-server (organization.com)
- Initial SMTP handshaking takes place between the two servers.
- The message is sent to organization.com's mail-server.
- User-2's mail-server receives the message and then puts it in user-2's mailbox

File Transfer Protocols

- Computer networking application
- FTP is used to transfer files from one host to another host over the internet.
- Files may be typically saved in the servers - user can use FTP to access the server and transfer the file.
- Two file transfer protocols are:
  - FTP
  - SCP

FTP Algorithm

- A user requests a connection to a remote server
- User waits for acknowledgment
- Once connected user has to enter username and password
- Connection is established over a TCP session
- Desired file transfer takes place
- User closes FTP connection

Comparison between FTP and TELNET

- Both are built on client-server paradigm
- Both allow the user to establish a remote connection
- TELNET allows broader access to users than compared to FTP which provides access only to limited set of files

Secure Copy Protocol

- Similar to TELNET but secure
- Supported by a number of encryption and authentication features
- Access of remote information based on username and password details
- Cannot support file transfer between the machines with different internal architectures

World Wide Web

- Application layer software
- Web is a global network of servers linked by a common protocol allowing access to all the connected resources
- Communication in Web is carried through Hypertext Transfer Protocol (HTTP)
- When a client host requests an object – file, the Web server responds by sending the requested object through the browsing tools

- Hypertext
  - Type of text with references or links to other text/additional information which can be immediately accessed by using an available link
- Web page
  - Is a web content consisting of files or images
  - Created using the markup language - HTML
- Web client/browser
  - User agent displaying the requested web page
  - Page styles, scripts and images

- Web server
  - Hardware/software
  - Server side of the web protocols
  - With fixed IP address

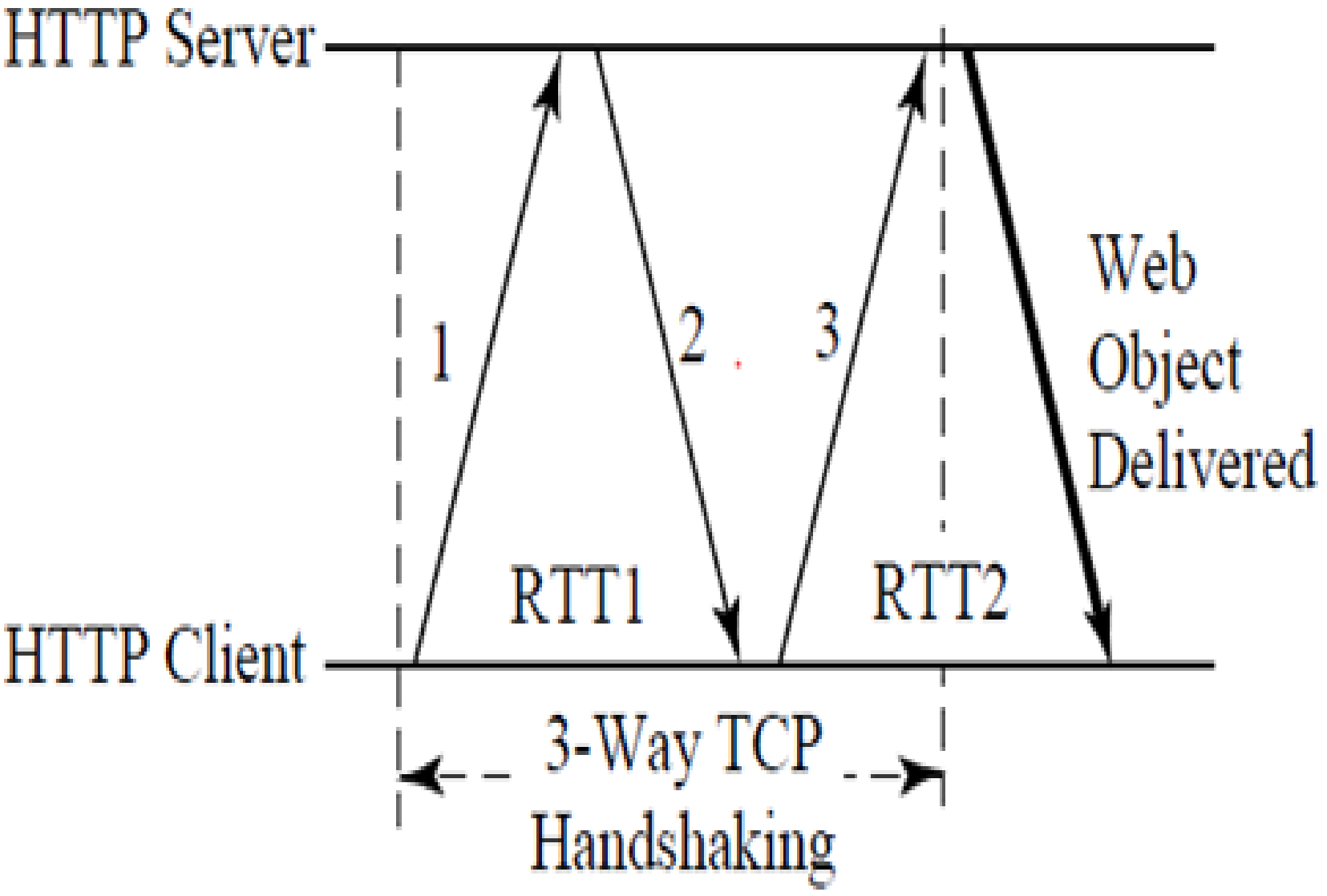
- Uniform Resource Locator
  - Global address of a web page or document or object or resource
  - Application layer address

HTTP

- Web protocol designed to operate at the application layer
- Distributed and collaborative protocol used to exchange or transfer objects and hypertext using hyperlinks
- Based on client/server model – HTTP messages
- HTTP uses TCP rather than UDP, since reliable delivery of web-pages with text is important.

HTTP Algorithm

- Establish a three way handshaking connection – TCP
- Transmit the Requested object by the server
- Terminate the connection - TCP



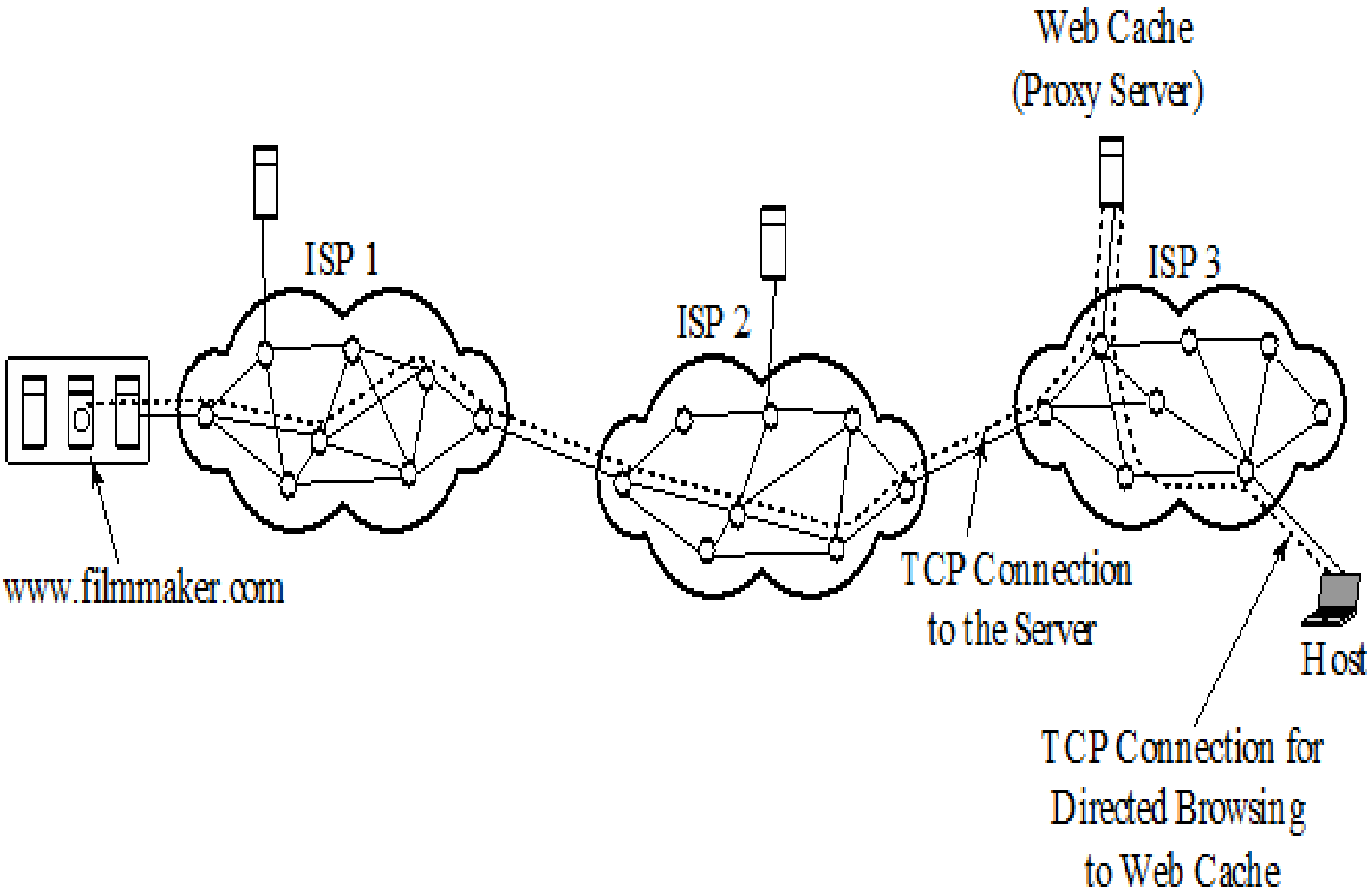
- Client or browser initiates a TCP connection to the server – TCP segment
- Segment leads to the creation of socket at the client – IP address, port number
- Web server – default port number is 80
- Server sends back an ACK – through the newly created socket
- Client sends its HTTP request message along with the URL to the server
- Completion of Three-way handshake, establishment of TCP connection – happens automatically once the user selects the hyperlink on the web page
- Type of HTTP message
  - Request message
  - Response message

Web Caching

- An HTTP request from a user is first directed to the web-cache.
- The web-cache must contain updated-copies of all objects in its defined proximity.
- Two reasons for web caching:
  - To reduce the response-time for a user-request.
  - To reduce traffic on an organization's access link to the Internet

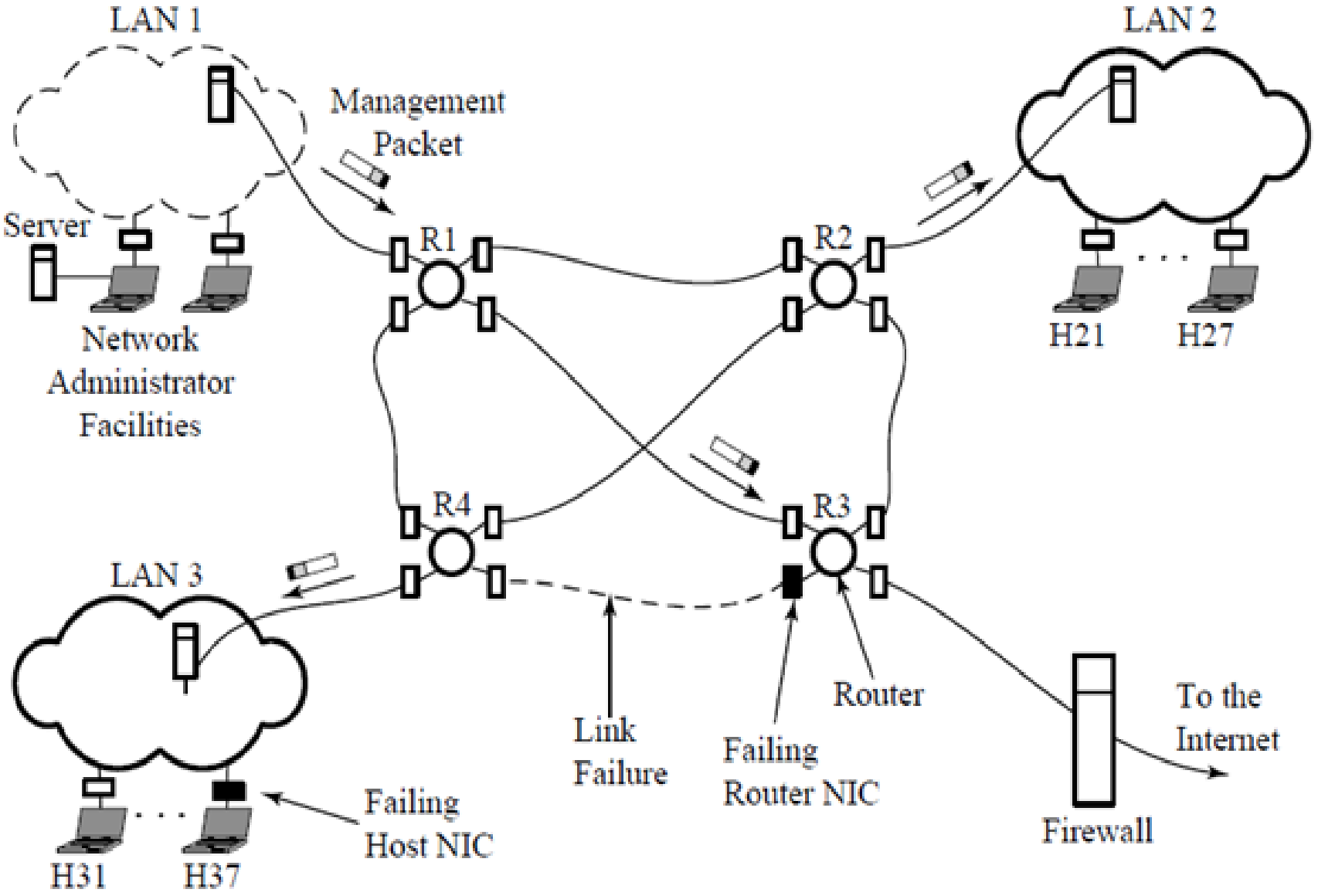
Web Caching Algorithm

- The user-browser makes a TCP connection to the web-cache
- The user-browser transmits its HTTP request to the web-cache.
- If web-cache has a copy of the requested-object,
  - web-cache forwards the object to the user-browser
  - If not, web-cache establishes a TCP connection to the requested-server and asks for the object.
  - Once it receives the object, the web-cache stores a copy of it and forwards another copy to the user-browser.



Network Management

- Monitor, manage and control a network
- The purpose of network management is
  - to monitor, test and analyze the hardware, software and human elements of a network
  - to configure & control those elements to meet the operational performance requirements of the network



Network Management Tasks

- ***QoS and performance management: A network-administrator periodically***
  - monitors & analyzes routers, hosts and utilization of links
  - redirect traffic-flow to avoid any overloaded spots.
- ***Network failure management:***
  - Any fault in a network, such as link, host or router hardware or software outages, must be detected, located and responded to by the network.
- ***Configuration management: This task involves***
  - tracking all the devices under management and
  - ensuring that all devices are connected and operate properly.
- ***Security management: This task is handled through firewall which can***
  - monitor & control access points.
- ***Billing & accounting management: The network administrator***
  - issues all billing & charges to users and
  - specifies user access or restrictions to network resources

Elements of Network Management

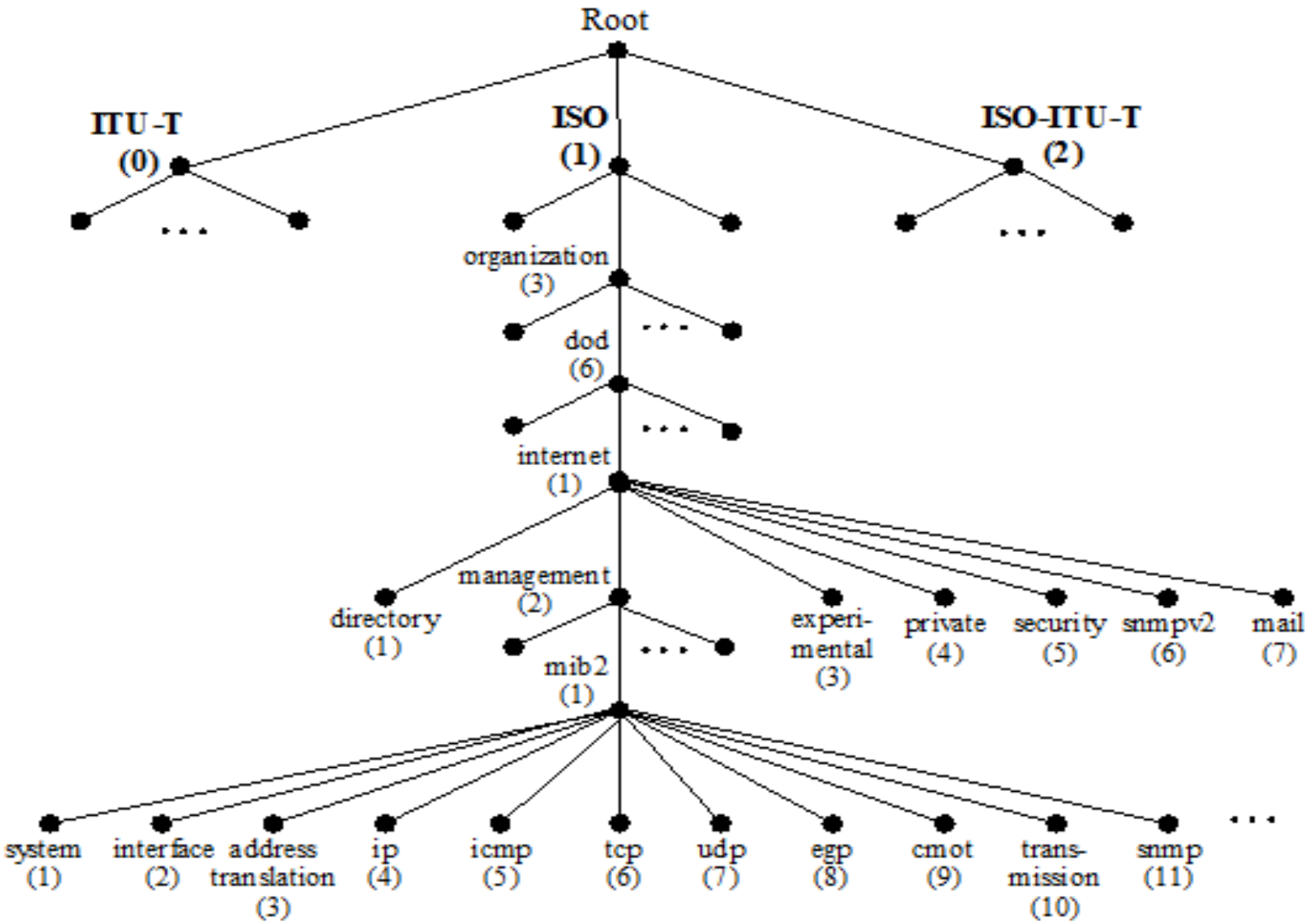
- Network management has three main components:
  - Managing-center consists of the network-administrator and his facilities.
  - Managed-device is the network-equipment that is controlled by the managing-center. The managed-device includes hub, bridge, router, server, printer or modem.
  - Network-management-protocol is a policy between the managing-center and the managed devices.
- An agent is a managed-device such as router, hub or bridge.
- Manager is a network administrative device, such as a management host.

Structure of Management Information

- This is used
  - to define the rules for naming objects and
  - to encode objects in a managed network center
- For ex, Integer32 means a 32-bit integer with a value between -2^31 and -2^(31-1).
- This also provides higher-level language constructs - specify the data type, status and semantics of managed-objects containing the management data.

Management Information Base (MIB)

- This is an information storage medium.
- This contains managed-objects which reflects the current status of the network.
- This also shows relationships among managed-objects.
- Objects
  - are organized in a hierarchical manner and
  - are identified by the ASN.1 object definition language (ASN.1=Abstract Syntax Notation One).
- The hierarchy of object names(known as ASN.1 object identifier) is an object identifier tree in which each branch has both a name and a number
- Network management can then identify an object by a sequence of names or numbers from the root to that object.



- On the root of the object identifier hierarchy are three entries: ISO(International Standardization Organization), ITU-T(International Telecommunication Union Telecommunication) & ISO-ITU-T.
- For ex, the organization(3) branch is labeled sequentially from the root as 1.3

Simple Network Management Protocol

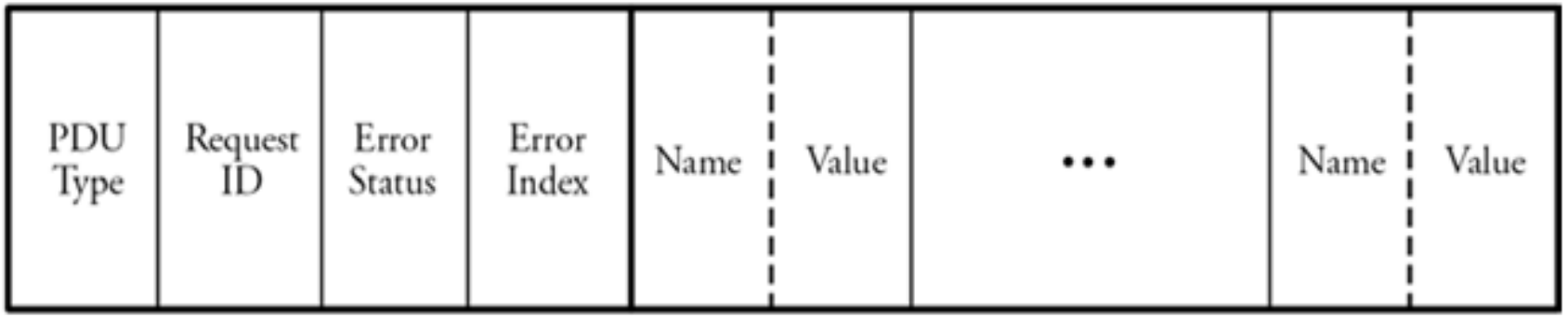
- The purpose of network management is
  - monitor, test and analyze the hardware, software and human elements of a network and
  - then to configure & control those elements to meet operational performance requirements of network
- This runs on top of UDP and uses client/server configuration.
- PDUs(Protocol Data Unit) are carried in the payload of a UDP datagram, and so its delivery to a destination is not guaranteed.
- Managed-devices (such as routers and hosts) are objects, and each object has a formal ASN.1 definition.

- The task of SNMP is to transport MIB information among managing-centers and agents executing on behalf of managing-centers.
- For each managed MIB object, an SNMP request is used to retrieve (or change) it's associated value.
- If an unsolicited message is received by an agent(or when an interface/device goes down),the protocol can also inform the managing-center.

- SNMPv2 has seven PDU's(or messages) as follows.
  - GetRequest: This is used to obtain the value of a MIB object.
  - GetNextRequest: This is used to obtain the next value of a MIB object.
  - GetBulkRequest : This is used to get multiple values, equivalent to multiple GetRequests but without using multiple overheads.
  - InformRequest: This is a manager-to-manager message that two communicating management centers are remote to each other.
  - SetRequest : This is used to set the value of a MIB object.
  - Response: is a reply message to a request-type PDU.
  - Trap: This notifies a managing-center that an unexpected event has occurred.

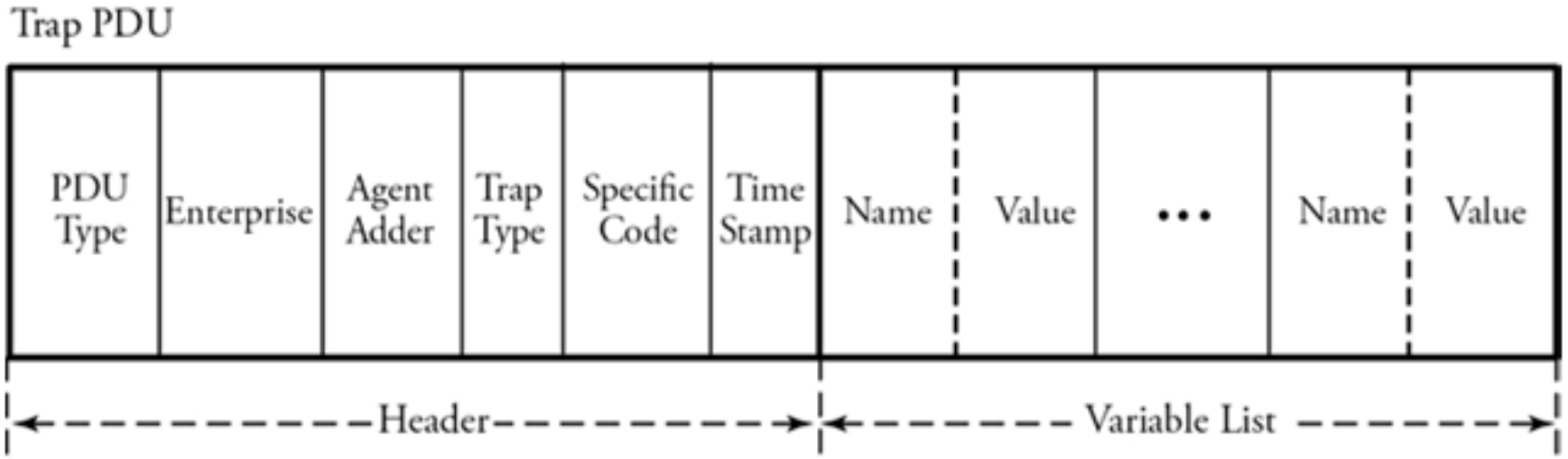
GET or SET PDU format

Get or Set PDU



- PDU type: This indicates one of the seven PDU types
- Request ID: This is used to verify the response of a request.
- Error status: This indicates types of errors reported by an agent.
- Error index: This indicates to a network administrator which name has caused an error

TRAP PDU Format



- Enterprise: This is for use in multiple networks
- Timestamp: This is used for measuring up time.
- Agent address: This indicates address of the managed agent is included in the PDU header.

Module 3

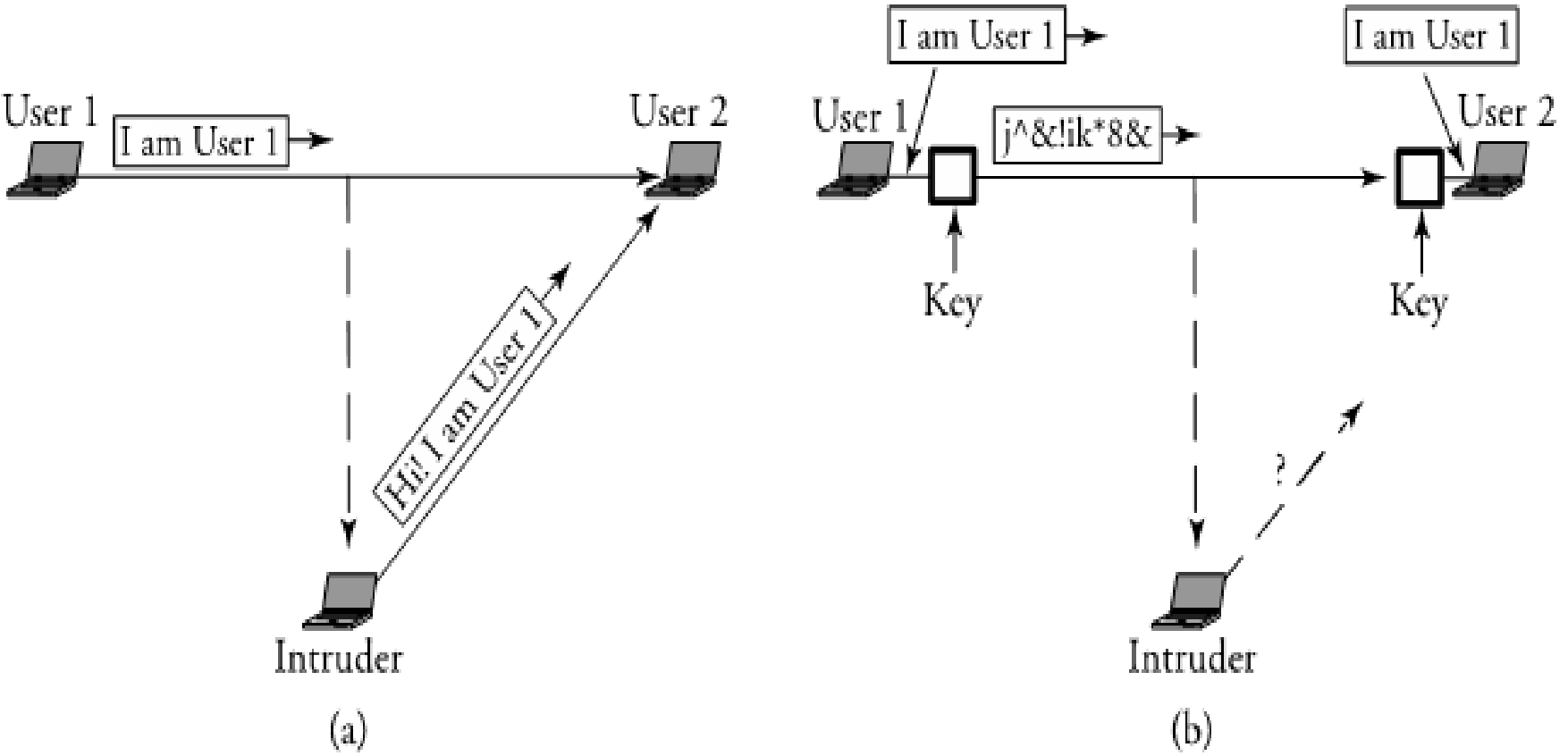
Network Security

- Overview of Network Security
- Overview of Security methods
- Secret Key encryption protocols
- Public Key encryption protocols
- Authentication
- Authentication and Digital Signatures

Overview of Network Security

- Network security is required by the users to communicate on the network

- If medium is insecure then an intruder may intercept, read and modify the transmitted-data from sender to receiver.



In the above figure, user 1 sends a message ("i am user 1") to user 2. Since the network lacks any security system, an intruder can receive the message and change its content to a different message ("hi i am user 1") and send it to user 2. User 2 may not know that this falsified message is really from user 1 – authentication fails.

In the second figure a security block is added to each side of the communication, and a secret key that only users 1 and 2 would know about is included.

Therefore, the message is changed to a form that cannot be altered by the intruder.

Elements of Network Security

- Confidentiality: Information should be available only to those who have rightful access to it
- Authenticity and integrity: The sender of a message and the message itself should be verified at the receiving-point

Threats to Network Security

- Internet infrastructure attacks are broadly classified into 4 categories:
  - DNS hacking
  - Routing table poisoning
  - Packet mistreatment
  - Denial of Service (DOS)

DNS Hacking Attacks

- DNS server is a distributed hierarchical and global directory that translates domain names into numerical IP address.
- DNS is a critical infrastructure, and all hosts contact DNS to access servers and start connections.
- Name-resolution services in the modern Internet environment are essential for email transmission, navigation to web sites, or data transfer. Thus, an attack on DNS can potentially affect a large portion of the Internet.

Types of DNS Attack

- Masquerading attack
- Domain Highjacking attack
- Information Leakage Attack
- Information-Level Attack(Cache Poisoning)

- **Masquerading Attack**
  - The attacker poses as a trusted entity and obtains all the secret information.
  - can stop any message from being transmitted further or
  - can change the content or redirect the packet to bogus servers. This action is also known as a middle-man attack.
- **Domain Highjacking Attack**
  - Whenever a user enters a domain address, he is forced to enter into the attacker's Web site.

- **Information Leakage Attack:** The attacker
  - sends a query to all hosts
  - identifies which IP addresses are not used
  - uses those IP address to make other types of attacks
- **Information-Level Attack(Cache Poisoning)**
  - This forces a server to correspond with other than the correct answer.
  - The hacker tricks a remote name-servers into caching the answer for a third-party domain by providing malicious information
  - redirects traffic to a preselected site.

Routing Table Poisoning

- This is the undesired modification of routing tables.
- This results in a lower throughput of the network.
- Two types of attacks are:
  - link attack
  - router attack.

- **Link Attack**
  - This occurs when a hacker gets access to a link and thereby intercepts, interrupts or modifies routing messages.
  - This act similarly on both the link-state and the distance-vector protocols.
  - If an attacker succeeds in placing an attack in a link-state routing protocol, a router may
    - send incorrect updates about its neighbors or
    - remain silent even if the link state of its neighbor has changed

- Router Attack
  - This may affect the link-state protocol or even the distance-vector protocol.
  - In link-state protocol, if routers are attacked, they become malicious. As a result, routers may
    - add a nonexisting link to a routing table
    - delete an existing link or
    - change the cost of a link.
- In the distance-vector protocol, an attacker may cause routers to send wrong updates about any node in the network, thereby misleading a router and resulting in network problems.

DOS ATTACKS (DENIAL OF SERVICE)

- This is a type of security breach that prohibits a user from accessing normally provided services.
- This can cost the target person a large amount of time and money.
- This affects the destination rather than a data-packet or router.
- They take important servers out of action for few hours, thereby denying service to all users.
- Two types of attacks are:
  - *Single-source: An attacker sends a large number of packets to a target system to* overwhelm & disable it
  - *Distributed: A large number of hosts are used to flood unwanted traffic to a single target.* The target cannot then be accessible to other users in the network.

Packet Mistreatment Attacks

- This can occur during any data transmission.
- A hacker may capture certain data packets and mistreat them.
- The attack may result in
  - Congestion
  - lowering throughput &
  - DOS attacks
- Link-attack causes interruption, modification or replication of data packets. Whereas, a router-attack can misroute all packets and may result in congestion or DOS
- Examples are:

Interruption

•If an attacker intercepts packets, they may not be allowed to be propagated to their destinations.

Modification

•Attackers may succeed in accessing the content of a packet. They can then
•change the address of the packet or
•change the data of the packet
•This kind of attack can be detected by digital signature mechanism.

Replication

•An attacker may trap a packet and replay it.
•This kind of attack can be detected by using the sequence number for each packet.

Malicious Misrouting of Packets

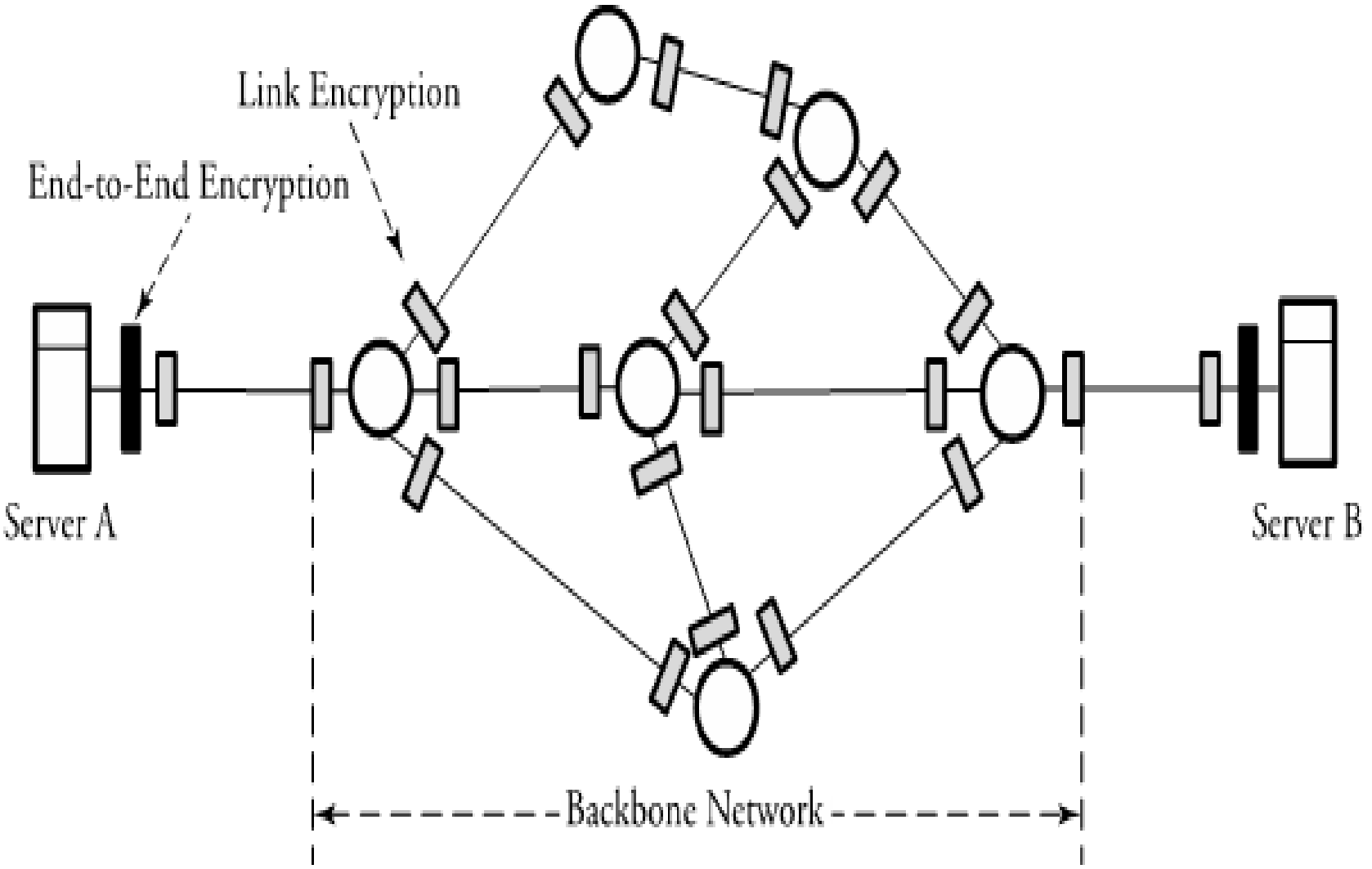
•A hacker may attack a router and change its routing table, resulting in misrouting of data packets.

Ping of death

•An attacker may send a ping message, which is large and therefore must be fragmented for transport.
•The receiver then starts to reassemble the fragments as the ping fragments arrive.
•The total packet length becomes too large and might cause a system crash.

Overview of Security Methods

- Common solutions that can protect computer communication networks from attacks are classified as:
  - cryptographic techniques
  - authentication techniques



Overview of encryption points in a communication network

Cryptographic Techniques

- Cryptography is the process of transforming a piece of information or message shared by two parties into some sort of code.
- The message is scrambled before transmission so that it is undetectable by outside watchers.
- The scrambled-message needs to be decoded at the receiving-end before any further processing.
- The main tool used to encrypt a message M is a secret-key K.
- The fundamental operation used to encrypt a message is the exclusive-OR ($\oplus$)

- Assume that we have one-bit M and a secret-bit K. A simple encryption is carried out using $M \oplus K$.
- To decrypt this message, the second party can detect M by performing the following operation: $(M \oplus K) \oplus K = M$
- In end-to-end encryption, secret coding is carried out at both end systems where as in link encryption, all the traffic passing over that link is secured.
- Two types of encryption techniques are:
  - secret-key
  - public-key encryption
- In secret-key model, both sender & receiver conventionally use same key for an encryption process.
- In public-key model, a sender and a receiver each use a different key.
- The public-key system
  - is more powerful than the secret key system
  - provides better security and message privacy.
- Drawbacks of public-key system:
  - slow speed
  - more complex computationally

Authentication Techniques

- Encryption methods offer the assurance of message confidentiality.
- A networking-system must be able to verify the authenticity of the message and the sender of the message.
- These forms of security techniques are known as authentication techniques.
- Authentication techniques are categorized as
  - authentication with message digest and
  - authentication with digital signature.

Secret Key Encryption Protocols

- This is also called as symmetric encryption or single-key encryption.
- Sender and receiver conventionally use the same key for an encryption process.
- This consist of
  - an encryption-algorithm
  - a key
  - a decryption-algorithm
- The encrypted-message is called ciphertext.
- Two popular protocols are:
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

- shared secret-key between a transmitter and a receiver is assigned at the transmitter and receiver points.
- At the receiving end, the encrypted information can be transformed back to the original data by using
  - decryption algorithm
  - secret key

DES

- Plaintext messages are converted into 64-bit blocks & each block is encrypted using a key.
- key length is 56 bits.
- This consists of 16 identical rounds of an operation
- **Operation of function F()**
  - Out of 56 bits of ki, function F( ) chooses 48 bits.
  - The 32-bit Ri-1 is expanded from 32 bits to 48 bits so that it can be combined with 48 bit ki.
  - F( ) also partitions the 48 bits of ki into eight 6-bit chunks.
  - The corresponding eight chunks of Ri-1 and eight chunks of ki are combined as follows

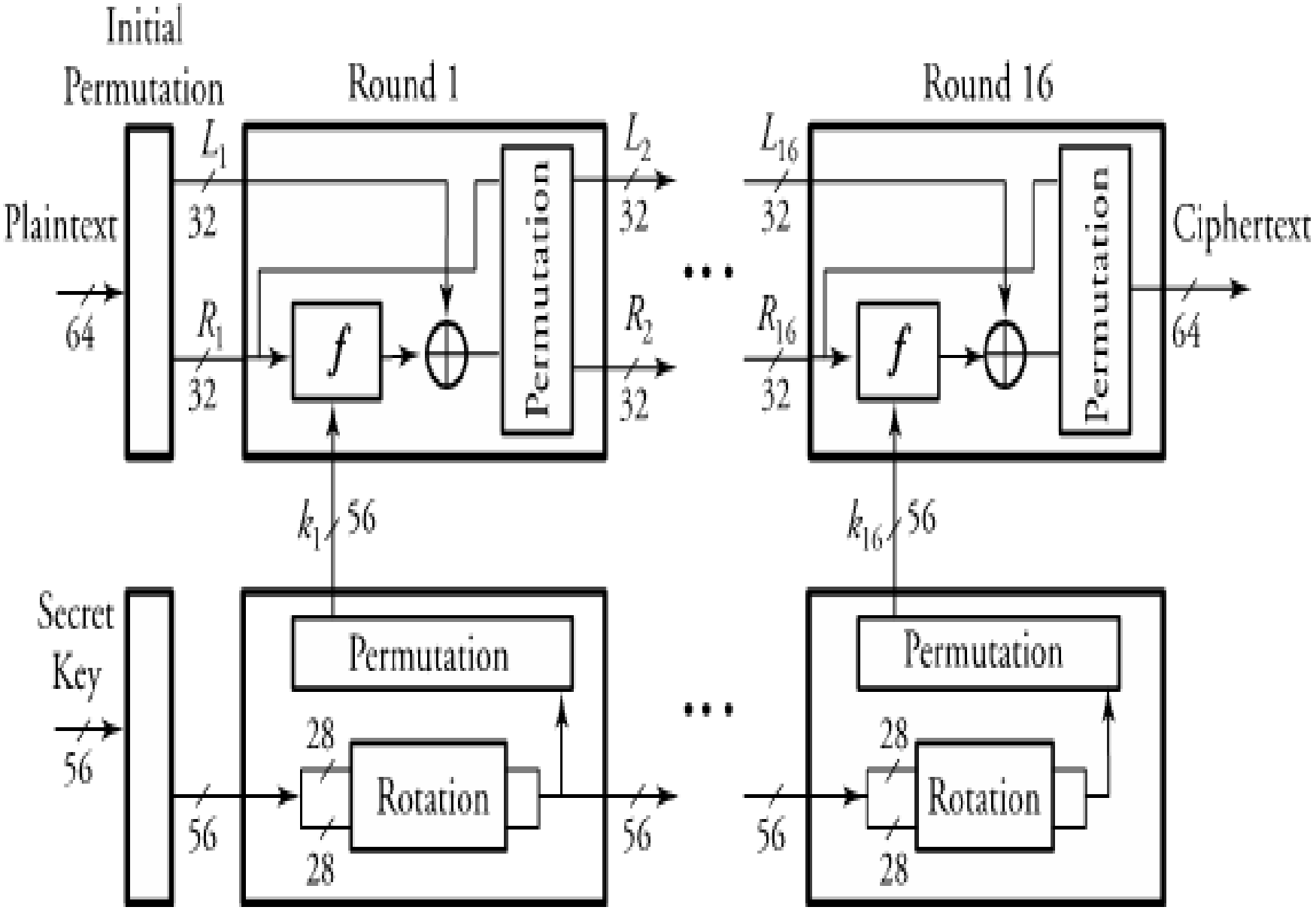
$$Ri=1 = Ri-1 \oplus ki$$

Begin DES Algorithm

1) Initialize. Before round 1 begins, all 64 bits of the message and all 56 bits of the secret key are separately permuted(shuffled).
2) Each incoming 64-bit message is broken into two 32-bit halves denoted by Li and Ri respectively.
3) The 56 bits of the key are also broken into two 28-halves, and each half is rotated one or two bit positions, depending on the round.
4) All 56 bits of the key are permuted, producing version ki of the key on round i.
5) Li and Ri are determined by

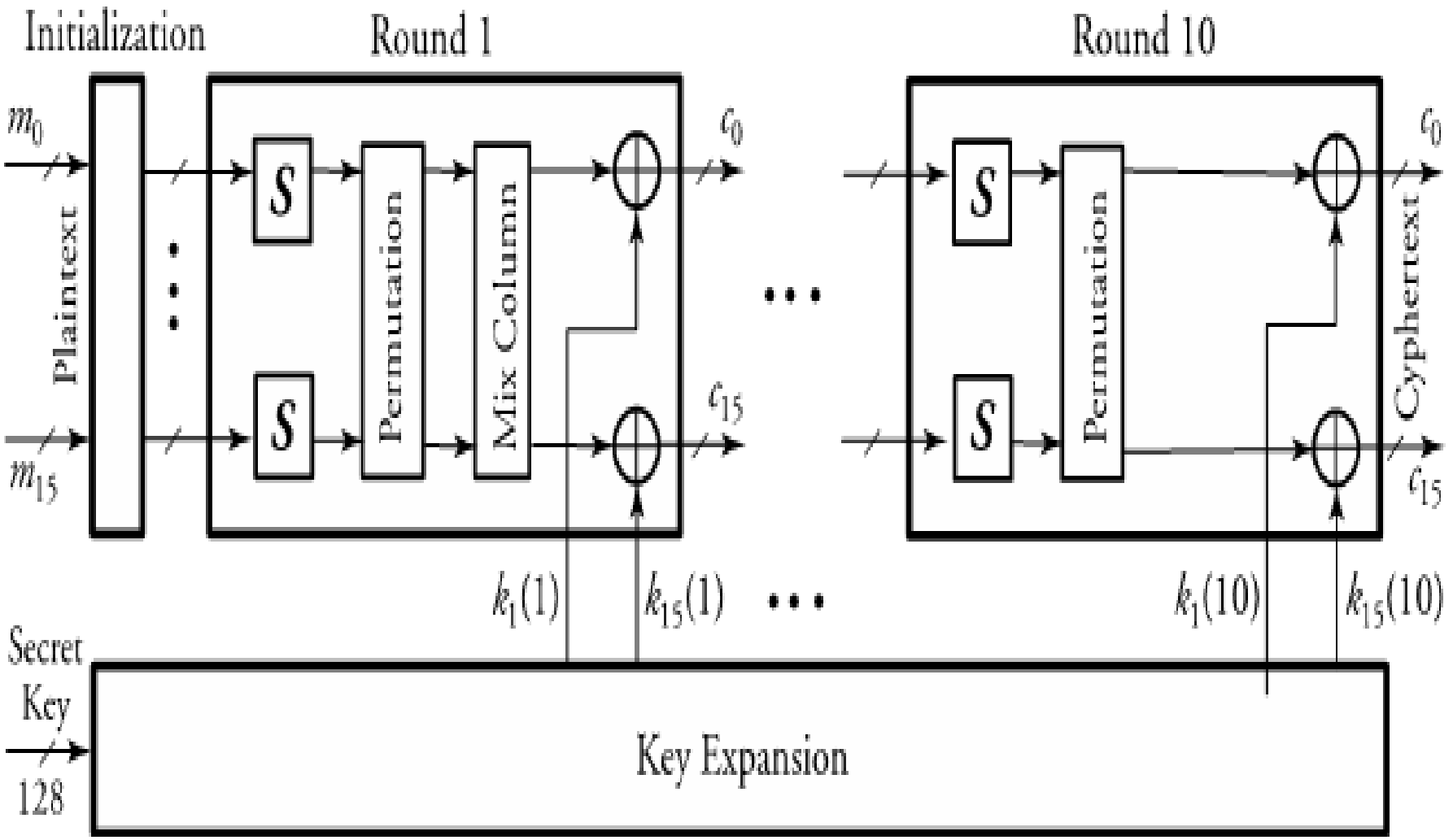
   $Li = Ri\text{-}1$ and $Ri = Li\text{-}1 \oplus F(Ri\text{-}1, ki)$

6) All 64 bits of a message are permuted.



AES

- This has a better security strength than DES (Figure 10.4).
- Message size=128-bit block; Key size=128,192 or 256 bit
- Number of rounds= 10 to 14
- The plaintext is formed as 16 bytes m0 through m15 and is fed into round 1 after an initialization stage.
- In this round, substitute-units(S) perform a byte-by-byte substitution of blocks.
- The ciphers move through a permutation-stage to shift rows to mix-columns.
- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key k0(1) through k15(1).



Overview of the Advanced Encryption Standard (AES) protocol

Public Key Encryption Protocols

- This is also called as asymmetric or two key encryption.
- A sender/receiver pair use different keys.
- This is based on mathematical functions rather than on substitution or permutation.
- Two popular protocols are:
  - RSA protocol
  - Diffie-Hillman key-exchange protocol.
- Either of the two related keys can be used for encryption; the other one for decryption.
- Each system publishes its encryption key by placing it in a public-register & sorts out key as public one.
- The companion key is kept private.

- If A wishes to send a message to B, A encrypts the message by using B's public key.
- At receiving end, B decrypts the message by using its private key.
- No other recipients can decrypt the message, since only B knows its private key.
- The public-key system
  - is more powerful than the secret key system &
  - provides better security and message privacy.
- Drawbacks of public-key system:
  - slow speed
  - more complex computationally

RSA ALGORITHM

- Rivest, Shamir and Adleman (RSA) developed this public key encryption and signature scheme
- Based on intractability of factoring large integers
- Assume that a plaintext m must be encrypted to a ciphertext c.
- This has three phases:
  - key generation
  - Encryption
  - decryption

Key Generation Algorithm

1) Choose two prime numbers a and b and compute n=a.b
2) Find x. Select encryption-key x such that x and (a-1)(b-1) are relatively prime.
3) Find y. Calculate decryption-key y.

x y mod (a-1)(b-1) = 1

4) At this point, a and b can be discarded.
5) The public key = {x, n}
6) The private key = {y, n}

Encryption

1) Both sender and receiver must know the value of n.
2) The sender knows the value of x and only the receiver knows the value of y.
3) Ciphertext c is constructed by

c=m^x mod n

Decryption

1) Given the ciphertext c, the plaintext m is extracted by

m=c^y mod n.

DIFFIE-HILLMAN Key-exchange Protocol

- Two end users can agree on a shared secret-code without any information shared in advance.
- This protocol is normally used for VPN(virtual private network).
- Assume that user-1 wishes to communicate with user-2.

Key Generation Algorithm

1) User-1

→ selects a prime number 'a', random integer number 'x_1',and a generator 'g'

→ creates 'y_1' such that

$$y_1 = g^{x1} \bmod a$$

2) User-2

→ performs the same function and

→ creates y_2 such that

$$y_2 = g^{x2} \bmod a$$

3) User-1 then sends y1 to user-2. Now, user-1 forms its key k_1 using the information its partner sent as

$$k_1 = y_2^{x1} \bmod a$$

4) User-2 forms its key ka using the information its partner send it as

$$k_2 = y_1^{x2} \bmod a$$

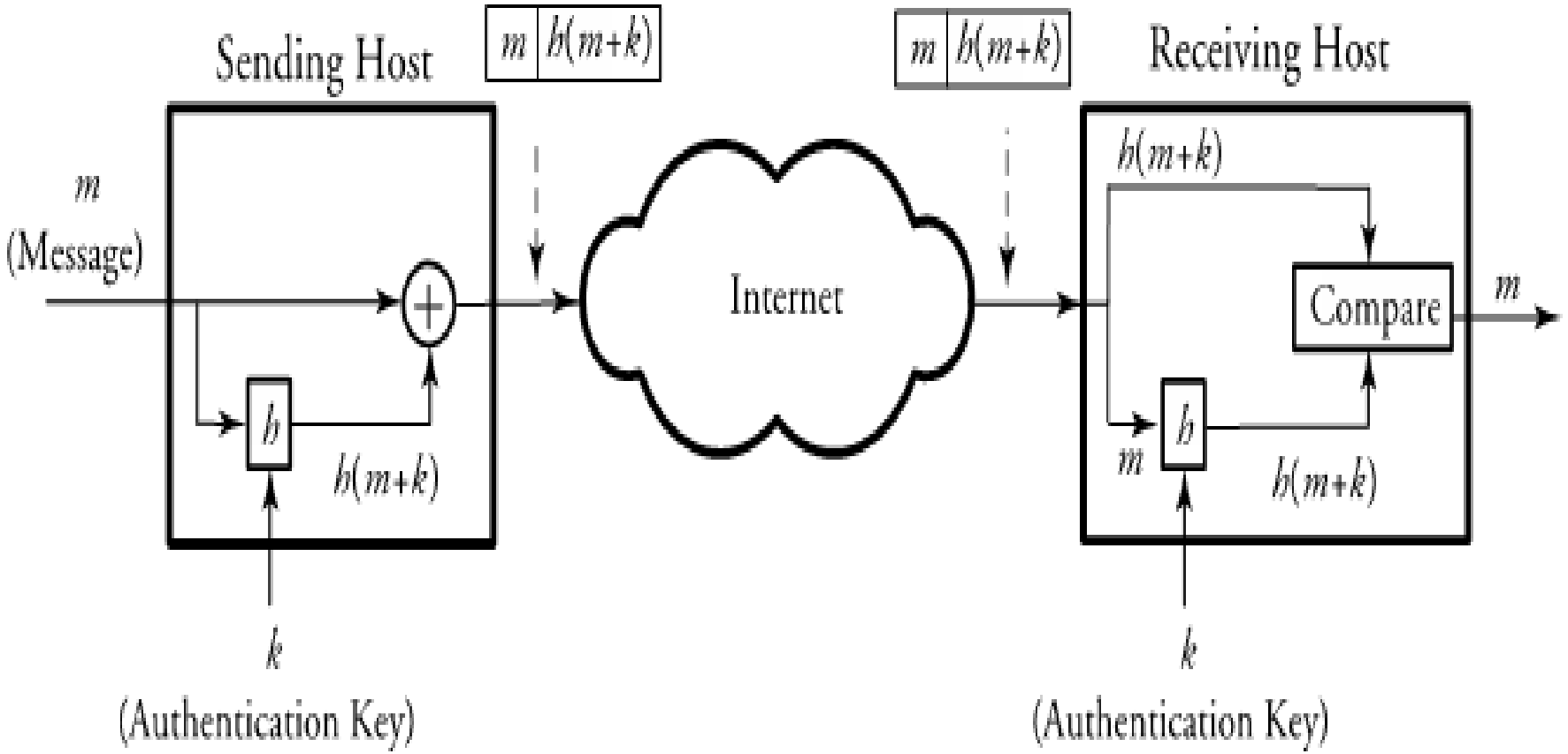
5) The two keys k_1 and k_2 are equal. The two users can now encrypt their messages, each using its own key

Authentication

- Message-authentication verifies the authenticity of both the message-sender and the message-content.
- Message-sender is authenticated through implementation of a digital signature.
- Message-content is authenticated through implementation of a hash function and encryption of the resulting message-digest.
- Hash-function is used to produce a "fingerprint" of a message.
- The hash-value is added at the end of message before transmission.
- The receiver re-computes the hash-value from the received message and compares it to the received hashvalue.
- If the two hash-values are the same, the message was not altered during transmission.
- Once a hash-function is applied on a message m, the result is known as a message-digest h(m).

- The hash-function has the following properties
  - Unlike the encryption-algorithm, the authentication algorithm is not required to be reversible.
  - Given a message-digest h(m),it is computationally infeasible to find m.
  - This is computationally infeasible to find two different messages m1 and m2 such that h(m1)=h(m2).

- Message-authentication can be implemented by two methods:
  - In first method, a hash-function is applied on a message and then a process of encryption is implemented. At the receiver site, the received message-digest is decrypted and the comparison is made between the decrypted h(m) and the message-digest made locally from the received message. compare it with the one made locally at its site for any judgments on the integrity of the message.
  - In second method, no encryption is involved. The two parties share a secret key. Hence, at the receiving site, the comparison is made between the received h(m) and the message-digest made locally from the received message.



Authentication and Digital Signature

- A digital signature on a message is required for the authentication and identification of the right sender.
- RSA algorithm can be used to implement digital signature.
- The message is encrypted with the sender's private key. Thus, the entire encrypted message serves as a
- digital signature.
- At the receiving end, the receiver can decrypt the message using the public key. This authenticates that the packet comes from the right user.

THANK YOU