Advanced Networking
Unit 4

-Madhavi Dave

SMTP, POP, IMAP, MIME

Email

- An electronic mail (e-mail) facility allows users to send memos across an internet.
- E-mail is one of the most widely used application services.
- E-mail is also popular because it offers a fast, convenient method of transferring information.
- E-mail accommodates small notes or large voluminous memos with a single mechanism.

Mailbox Names And Aliases

- Users specify recipients by giving pairs of strings that identify the ***mail destination machine name*** and a ***mailbox address*** on that machine.
- The names used in such specifications are independent of other names assigned to machines.
- A mailbox address is the same as a user's login id, and a destination machine name is the same as a machine's domain name.

Alias Expansion And Mail Forwarding

- ***mail forwarding*** software that includes a ***mail alias expansion*** mechanism.
- A mail forwarder allows the local site to map identifiers used in mail addresses to a set of one or more new mail addresses.
- Usually, after a user composes a message and names a recipient, the mail interface program consults the local aliases to replace the recipient with the mapped version before passing the message to the delivery system.
- Recipients for which no mapping has been specified remain unchanged.
- Similarly,the underlying mail system uses the mail aliases to map incoming recipient addresses.

Simple Mail Transfer Protocol (SMTP)

- TCP/IP protocol suite specifies a standard for the exchange of mail between machines.
- The SMTP protocol focuses specifically on how the underlying mail delivery system passes messages across an internet from one machine to another.
- It does not specify how the mail system accepts mail from a user or how the user interface presents the user with incoming mail.
- Also, SMTP does not specify how mail is stored or how frequently the mail system attempts to send messages.

- Communication between a client and server consists of readable ASCII text.
- Although SMTP rigidly defines the command format, humans can easily read a transcript of interactions between a client and server.
- Initially, the client establishes a reliable stream connection to the server and waits for the server to send a ***220 READY FOR MAIL*** message.

- The server responds by identifying itself.
- Once communication has been established, the sender can transmit one or more mail messages, terminate the connection, or request the server to exchange the roles of sender and receiver so messages can flow in the opposite direction.
- The receiver must acknowledge each message.
- It can also abort the entire connection or abort the current message transfer.

Post Office Protocol

- The most popular protocol used to transfer e-mail messages from a permanent mailbox to a local computer is known as version 3 of the ***Post Office Protocol (POP3).***
- The user invokes a **POP3** client, which creates a **TCP** connection to a **POP3** server on the mailbox computer.
- The user first sends a ***login*** and a ***password*** to authenticate the session.
- Once authentication has been accepted, the user client sends commands.

- the computer with the permanent mailbox must run two servers – an **SMTP** server accepts mail sent to a user and adds each incoming message to the user's permanent mailbox, and a POP3 server allows a user to extract messages from the mailbox.

Internet Message Access Protocol

- Version 4 of the ***Internet Message Access Protocol (IMAP4)*** is **an** alternative to POP3 that uses the same general paradigm.
- User can obtain information about a message or examine header fields without retrieving the entire message.
- In addition, a user can search for a specified string and retrieve specified portions of a message.

The MIME Extension For Non-ASCII Data

- Multipurpose Internet Mail Extension
- MIME is defined to allow transmission of non-ASCII data through e-mail.
- MIME allows arbitrary data to be encoded in ASCII and then transmitted in a standard e-mail message.
- The MIME standard specifies that a ***Content-Type*** declaration.

Content Type	Used When Data In the Message Is
text	Textual (**e.g.** a document).
image	A still photograph or computer-generated image
audio	A sound recording
video	A video recording that includes motion
application	Raw data for a program
multipart	Multiple messages that each have a separate content type and encoding
message	An entire **e-mail** message (**e.g.,** a memo that has been forwarded) or an external reference to a message (**e.g.,** an FTP sewer and file name)

MIME Multipart Messages

- MIME multipart content type adds flexibility.
- Subtype **mixed** multipart messages make it possible to include text, graphics, and audio in a single message, or to send a memo with additional data segments attached.
- Subtype **alternative** multipart messages are useful when sending a memo to many recipients.
- Subtype **digest** permits a single message to contain a set of other messages.

Voice And
Video Over IP (RTP)

Audio And Video Transmission And Reproduction

- Audio and video applications are classified as ***real-time*** because they require timely transmission and delivery.
- Because an IP internet is not isochronous, additional protocol support is required when sending digitized real-time data.
- In addition to basic sequence information that allows detection of duplicate or reordered packets, each packet must carry a separate timestamp that tells the receiver the exact time at which the data in the packet should be played.

Real-Time Transport Protocol (RTP)

- The protocol used to transmit digitized audio or video signals over an **IP** internet is known as the ***Real-Time Transport Protocol (RTP).***
- RTP does not contain mechanisms that ensure timely delivery.
- RTP provides two key facilities: a sequence number in each packet that allows a receiver to detect out-of-order delivery or loss, and a timestamp.
- RTP is designed to carry a wide variety of real-time data, including both audio and video, RTP does not enforce a uniform interpretation of semantics.

RTP Control Protocol (RTCP)

- A companion protocol and integral part of RTP is known as RTCP, provides the needed control functionality.
- RTCP allows senders and receivers to transmit a series of reports to one another that contain additional information about the data being tr nance of the n
- RTCP messages are encapsulated in UDP.

Type	Meaning
200	Sender report
201	Receiver report
202	Source description message
203	Bye message
204	Application specific message

IP Telephony And Signaling

- The use of IP as telephonic service in real-time is known as IP telephony or voice over IP.
- Protocol like RTP is needed to transfer a digitized signal across an IP internet correctly.
- A mechanism is needed to establish and terminate telephone calls.
- The telephone industry uses the term signaling to refer to the process of establishing a telephone call.
- The signaling mechanism used in the conventional Public Switched Telephone Network.

- After signaling is complete and a call has been established, the gateway must forward voice in both directions, translating from the encoding used on one side to the encoding used on the other.
- Two groups have proposed standards for **IP** telephony.
- IETF has proposed a signaling protocol known as the ***Session Initiation Protocol (SIP).***

Resource Reservation And Quality Of Service

- The term Quality Of Service (QoS) refers to statistical performance guarantees that a network system can make regarding loss, delay, throughput.
- One of the major arguments against complicated QoS mechanisms arises from improvements in the performance of underlying networks.
- Network capacity has increased dramatically.
- As long as rapid increases in capacity continue, QoS mechanisms merely represent unnecessary overhead.
- However, if demand rises more rapidly than capacity, QoS may become an economic issue.

RSVP

- ***Resource Reservation Protocol (RSVP)*** and the ***Common Open Policy Services (COPS)*** protocol are providing QoS in IP environment.
- QoS cannot be added to IP at the application layer.
- Before data is sent, the endpoints must send a request that specifies the resources needed, and all routers along the path must agree to supply the resources; the procedure can be viewed as a form of signaling.
- Second, as datagrams traverse the flow, routers need to monitor and control traffic forwarding.

- Monitoring, sometimes called **traffic policing**.
- An endpoint uses RSVP to request a simplex flow through an IP internet with specified QoS.
- If routers along the path agree to honor the request, they approve it; otherwise, they deny it.
- If an application needs QoS in two directions, each endpoint must use RSVP to request a separate flow.

FTP: The Major TCP/IP File Transfer Protocol

- File transfer is among the most frequently used TCP/IP applications, and it accounts for much network traffic.
- FTP Features
  - Interactive Access
  - Format (representation) Specification
  - Authentication Control

TFT (Trivial File Transfer Protocol)

- Although FTP is the most general file transfer protocol in the TCP/IP suite, it is also the most complex and difficult to program.
- Many applications do not need the full functionality FTP offers, nor can they afford the complexity.
- FTP requires clients and servers to manage multiple concurrent TCP connections, something that may be difficult or impossible on personal computers that do not have sophisticated operating systems.
- The TCP/IP suite contains a second file transfer protocol that provides inexpensive, unsophisticated service.
- Known as the ***Trivial File Transfer Protocol,*** or ***(TFTP),*** it is intended for applications that do not need complex interactions between the client and server.

- TFTP restricts operations to simple file transfers and does not provide authentication.
- Because it is more restrictive, TFTP software is much smaller than FTP.
- The advantage of using TFTP is that it allows bootstrapping code to use the same underlying TCP/IP protocols that the operating system uses once it begins execution.
- Thus, it is possible for a computer to bootstrap from a server on another physical network.
- Unlike FTP, TFTP does not need a reliable stream transport service.
- It runs on top of UDP or any other unreliable packet delivery system, using timeout and retransmission to ensure that data arrives.

Applications: Internet Management (SNMP)

The Level Of Management Protocols

- In a TCP/IP internet, a manager needs to examine and control routers and other network devices.
- Because such devices attach to arbitrary networks, protocols for internet management operate at the application level and communicate using TCP/IP transport-level protocols.

Standard Network Management Protocol

- The protocol has evolved through three generations.
- Consequently, the current version is known ***as SNMPv3,*** and the predecessors are known ***as SNMPv1*** and ***SNMPv2.***
- The changes have been minor - **all** three versions use the same general framework, and many features are backward compatible.

- Network management protocols specify communication between the network management client program a manager invokes and a network management server program executing on a host or router.
- SNMP takes alternative approach to network management.
- Instead of defining a large set of commands, SNMP casts all operations in a ***fetch-store paradigm***
- The chief advantages of using a fetch-store paradigm are stability, simplicity, and flexibility.

- From a manager's point of view, of course, SNMP remains hidden.
- The user interface to network management software can phrase operations as imperative commands (e.g., ***reboot).***
- Thus, there is little visible difference between the way a manager uses SNMP and other network management protocols.
- In fact, vendors sell network management software that offers a graphical user interface.
- Such software displays diagrams of network connectivity, and uses a point-and-click style of interaction.

SNMP Message Format

- SNMP messages do not have fixed fields.
- Standard ASN.1 encoding. Thus, a message can be difficult for humans to decode and understand.

SNMPv3Message ::=

SEQUENCE {

msgversion INTEGER (0..2147483647),

msgGlobalData HeaderData,

msgSecurityPararneters OCTET STRING,

msgData ScopedPduData

}

New Features In SNMPv3

- The primary changes arise in the areas of security and administration.
- First, SNMPv3 is designed to have both general and flexible security policies, making it possible for the interactions between a manager and managed devices to adhere to the security policies an organization specifies.
- Second, the system is designed to make administration of security easy.

MIB Variables

- SNMP does not specify exactly which data can be accessed on which devices.
- Instead, a separate standard specifies the details for each type of device.
- Known ***as*** a ***Management Information Base (MIB),*** the standard specifies the data items a managed device must keep, the operations allowed on each, and the meanings.
- MIBs have been defined as part of the standards process; they specify more than **10,000** individual variables.

MIB Category

MIB category	Includes Information About
system	The host or router operating system
interfaces	Individual network interfaces
at	Address translation (e.g., ARP mappings)
ip	Internet Protocol software
icmp	Internet Control Message Protocol software
tcp	Transmission Control Protocol software
udp	User Datagram Protocol software
ospf	Open Shortest Path First software
bgp	Border Gateway Protocol software
rmon	Remote network monitoring
rip-2	Routing Information Protocol software
dns	Domain Name System software

MIB Variable Example

MIB category	Includes Information About
system	The host or router operating system
interfaces	Individual network interfaces
at	Address translation (e.g., ARP mappings)
ip	Internet Protocol software
icmp	Internet Control Message Protocol software
tcp	Transmission Control Protocol software
udp	User Datagram Protocol software
ospf	Open Shortest Path First software
bgp	Border Gateway Protocol software
rmon	Remote network monitoring
rip-2	Routing Information Protocol software
dns	Domain Name System software

Structure of Management Information

- The standards that specify MIB variables and their meanings, a separate standard specifies a set of rules used to define and identify **MIB** variables.
- The rules are known as the ***Structure of Management Information (SMI)*** specification.
- To keep network management protocols simple, the SMI places restrictions on the types of variables allowed in the **MIB,** specifies the rules for naming those variables, and creates rules for defining variable types.
- More important, the rules in the SMI describe how the MIB refers to tables of values (e.g., the **IP** routing table).

Internet Security And Firewall Design (IPsec)

Internet Security

- Internet security is difficult because datagrams traveling from source to destination often pass across many intermediate networks and through routers that are not owned or controlled by either the sender or the recipient.
- Source authentication is ***weak*** because it can be broken easily.
- Stronger authentication requires ***encryption.***

- To encrypt a message, the sender applies a mathematical function that rearranges the bits according to a ***key*** which is known only to the sender.
- The receiver uses another mathematical function to decrypt the message.
- Careful choices of an encryption algorithm, a key, and the contents of messages can make it virtually impossible for intermediate machines to decode messages or manufacture messages that are valid.

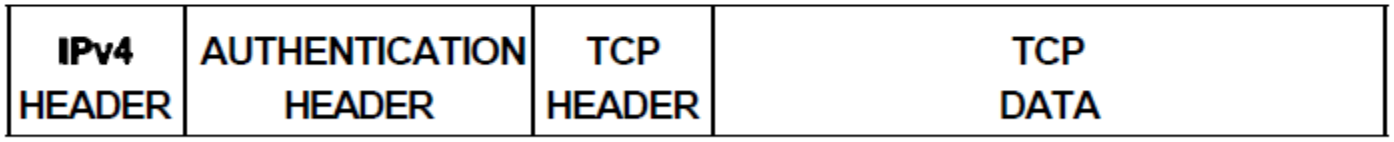
IP Security (IPsec)

- The protocols offer authentication and privacy services at the IP layer, and can be used with both **IPv4** and **IPv6.**
- Instead of completely specifying the functionality or the encryption algorithm to be used, the IETF chose to make the system both flexible and extensible.
- IPsec is not a single security protocol. Instead, IPsec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

IPsec Authentication Header

- Instead of changing the basic datagram header or creating an IP option, IPsec uses a separate ***Authentication Header*** (AH) to carry authentication information.

(a)

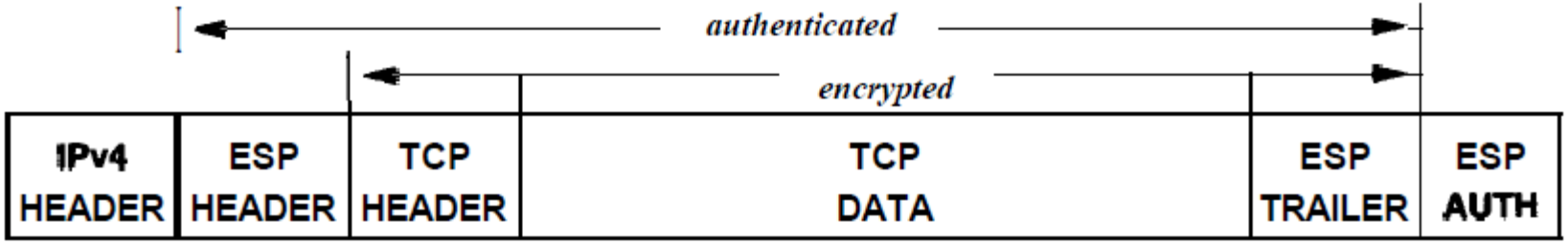


(b)

IPsec Encapsulating Security Payload

- To handle privacy **as** well as authentication, IPsec uses an ***Encapsulating SecurityPayload (ESP),*** which is more complex than an authentication header.

(a)



(b)

Required Security Algorithms

- IPsec defines a minimal set of algorithms that are mandatory.

Authentication	
HMAC with MD5	RFC 2403
HMAC with SHA-1	RFC 2404
Encapsulating Security Payload	
DES in CBC mode	RFC 2405
HMAC with MD5	RFC 2403
HMAC with SHA-1	RFC 2404
Null Authentication	
Null Encryption	

Secure Sockets

- ***Secure Sockets Layer (SSL)*** technology was originally developed by Netscape, Inc.
- As the name implies, SSL resides at the same layer as the socket API.
- When a client uses SSL to contact a server, the SSL protocol allows each side to authenticate itself to the other.
- The two sides then negotiate to select an encryption algorithm that they both support.
- Finally, SSL allows the two sides to establish an encrypted connection.

Firewalls And Internet Access

- A mechanism is needed which can help prevent outsiders from: obtaining information, changing information, or disrupting communication on an organization's intranet.
- Successful access control requires a careful combination of restrictions on network topology, intermediate information staging, and packet filters.

- A single technique known as an internet firewall, has emerged as the basis for internet access control.
- An organization places a firewall at its connection to external networks (e.g., the global Internet).
- A firewall partitions an internet into two regions, referred as ***inside*** and ***outside.***

Firewall Implementation

- A firewall simply blocks all unauthorized communication between computers in the organization and computers outside the organization.
- In practice, the details depend on the network technology, the capacity of the connection, the traffic load, and the organization's policies.

- To operate at network speeds, a firewall must have hardware and software optimized for the task.
- A manager can configure the filter in a router to request that the router block specified datagrams.
- The filters can be used in conjunction with another mechanism to provide communication that is safe, but flexible.

Packet-Level Filters

- ***Packet filter,*** the mechanism requires the manager to specify how the router should dispose of each datagram.
- The term ***packet filter*** arises because the filtering mechanism does not keep a record of interaction or a history of previous datagrams. Instead, the filter considers each datagram separately.
- When a datagram first arrives, the router passes the datagram through its packet filter before performing any other processing.
- If the filter rejects the datagram, the router drops it immediately.

5-tuple

- A 5-tuple refers to a set of five different values that comprise a Transmission Control Protocol/Internet Protocol (TCP/IP) connection.
- It includes a source IP address/port number, destination IP address/port number and the protocol in use.

Stateful firewall

- **Stateful inspection**, also known as dynamic packet filtering, is a **firewall** technology that monitors the state of active connections and uses this information to determine which network packets to allow through the **firewall**
- A **firewall** can be described as being either **Stateful** or **Stateless**.
- **Stateless firewalls** watch network traffic and restrict or block packets based on source and destination addresses or other static values.
- Instead, it evaluates packet contents statically and does not keep track of the state of network connections.

IPv6 Neighbor Discovery

- is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6).
- It operates at the Link Layer of the Internet model , and is responsible for gathering various information required for internet communication, including the configuration of local connections and the domain name servers and gateways used to communicate with more distant systems.
- The protocol defines five different ICMPv6 packet types to perform functions for IPv6 similar to the Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) Router Discovery and Router Redirect protocols for IPv4.