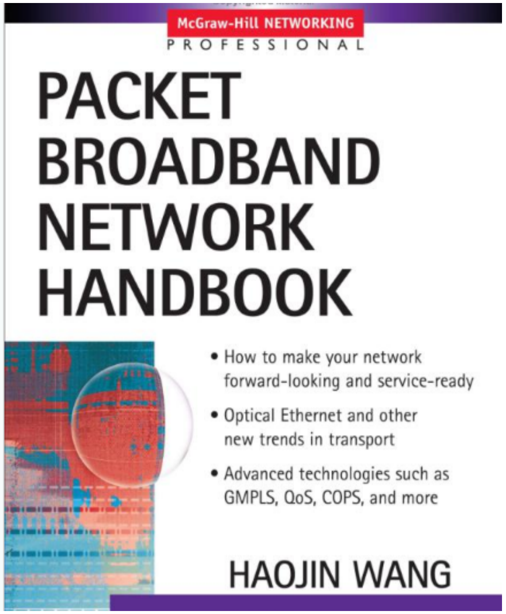
Packet Broadband Network Handbook



Session Initiation Protocol

- SIP is an IETF standard
  - ASCII-based application layer control/signaling protocol
    - Creates, modifies, maintains, and terminates sessions with one or more participating terminals on an IP network
- A session consists of a set of data streams that flow from a sender to one or more receivers
- Carried over both reliable TCP or unreliable UDP layers
- SIP is an alternative protocol and architecture to H.323 for providing multimedia applications over IP networks
- SIP has overwhelming presence over IP networks, far exceeding H.323
- Basic building blocks of the Session Initiation Protocol include
  - Protocol entities
  - Client and server relationship
  - SIP address format
  - Protocol message exchanges and operations

Overview of SIP Protocol

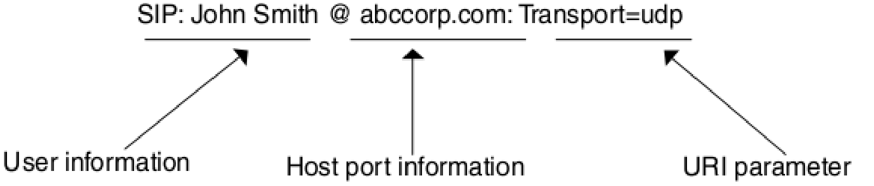
- SIP is a peer-to-peer as well as a client-server protocol
- Peers in a session called user agents (Uas)
- A user agent can function in the following two roles
- User agent client (UAC)—a client application that initiates a SIP request
- User agent server (UAS)—a server application that contacts another user when a SIP request is received & returns a response on behalf of the user
- A SIP endpoint is capable of functioning as both a UAC and UAS
  - But serves only as one or the other during each transaction
  - Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request
- SIP Transaction
  - All the messages exchanged between SIP client and SIP server in a single session
  - Identified by the CSeq sequence number within a single call leg
- SIP Session
  - Set of multimedia senders/receivers, & datastreams flowing b/w senders-receivers
  - Identified by session identifier and for SDP (user name+session ID+ network type+address type+address)

SIP Capabilities

- Establishes session between an originating and target endpoint (i.e., the calling and called parties) only if it determines that a call can be completed
  - Supports midcall changes (addition of another endpoint to a conference call) or changing a media characteristic or codec
- Determines the location of a target endpoint
  - Address resolution, name mapping, call redirection (using location server)
- Determines media capabilities of a target endpoint using Session Description Protocol
  - SIP determines the “lowest level” of common services between the endpoints
- Determines availability of a target endpoint
  - If a call cannot be completed because the target endpoint is unavailable
    - SIP determines the cause if target already on phone or did not answer in the allotted number of rings
    - Returns a message indicating why the target endpoint was unavailable
- Handles the transfer (one end point to another) and termination of calls
  - SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party)
  - Terminates the session between the transferee and the transferring party

Address Format

- SIP Universal Resource Locator (SIP URL) is based on the standard URL with extensions
  - Variety of addresses such as host name, port, Web URL, and email address, among others
- URL included in every message to indicate originator, current destination, and final recipient of a SIP request
- Three major parts: User information, Host port information, and Universal Request Identifier (URI) parameters
  - User information: identifies user involved in the SIP request
    - User name, telephone number, pwd
  - Host port: identifies a host name and a port associated with the host
    - Simple host name, IPv4 address, IPv6 address, domain name etc
  - URI gives flexibility to specify a wide range of parameters
    - Include network transport layer protocol parameter (UDP TCP & SCTP)
    - Additional user parameters IP address, phone, SIP request type; additional host address information



SIP Server

- A SIP server is a software system responsible for serving the requests from SIP clients
  - Provides requested services to the requesting clients
- Three different types of SIP servers

Proxy SIP Server

- A proxy server receives SIP messages and forwards them to the next SIP server or a user agent in the network
  - Provides functions (authentication, authorization, network access control, routing, reliable request retransmission, security)
- Stateless and stateful proxies
- Stateful maintain the status of incoming and outgoing requests
  - Example: multiple-point conference calls
  - Proxy server needs a forking capability
    - Server can fork a request into multiple clients either in parallel or sequential fashion to support applications (conference calls/presence services)
  - Maintains the state information of each leg of the call

SIP Server

Redirect SIP Server

- Provides a client with information about the next hop or hops
  - Message takes to allow the client to contact the next-hop server or UAS directly
- A redirect server does not issue any SIP requests of its own

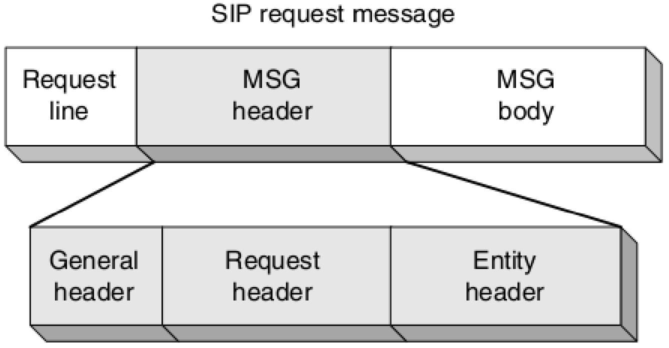
Registrar SIP Server

- Processes requests from SIP clients for the registration of their current locations
- Often co-located with redirect or proxy servers

SIP Messages

Request Messages

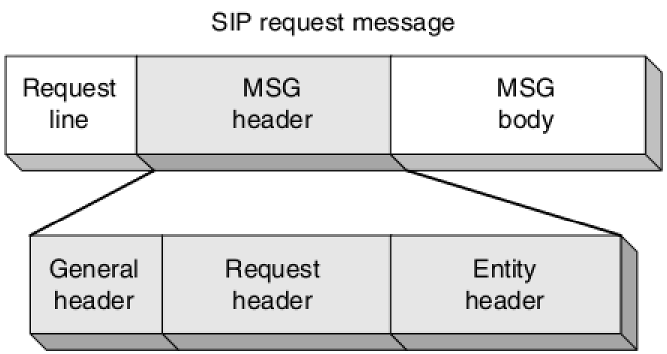
- Total six mandatory request messages (few extension request messages)
  - Request-line: generic information about the request (SIP version, type, request URI)
  - General-header: information generic to both request and response messages
    - Includes fields (call sequence number, call ID, call info, encryption method specification, timestamp, *to address*, *from address*, request path taken so far)
  - Request-header: allows client to pass additional request-specific information to the server
    - Contains fields as priority (urgency), alert-info (alternative call announcement in place of a default ring tone
      - Response-key: encryption key the called party should use in its response
      - Subject: indicates the nature of the call



SIP Messages

Request Messages

- Entity-header: control information or metadata about the message body
- Contains fields
  - Content-disposition: how to interpret the message body
  - Content-length: which indicates the length of the message body
  - Content-encoding: indicates encoded type
  - Content-type: indicates the message content type
- Message-body: contains the contents of the message
  - Format depends on message type (session description using SDP, free text, HTML page, media-specific contents such as audio and video data)



SIP Messages

Request Messages

- Total six mandatory request messages (few extension request messages)

  Call setup and call takedown request messages

  – INVITE: A caller which can be a UAC or SIP server issues an INVITE message to invite the called party to participate in a SIP

    - Address of the called party, media to be used in the call, etc

  – ACK: Allows a client to confirm that it has received the final response to an INVITE request

  – BYE: Allows a client to indicate to the server that it intends to release the call leg

  – CANCEL: Allows a client to cancel an outstanding request such as an INVITE or an ACK request

  Registration-related messages

  – Allows a client to register with a server for address translation service

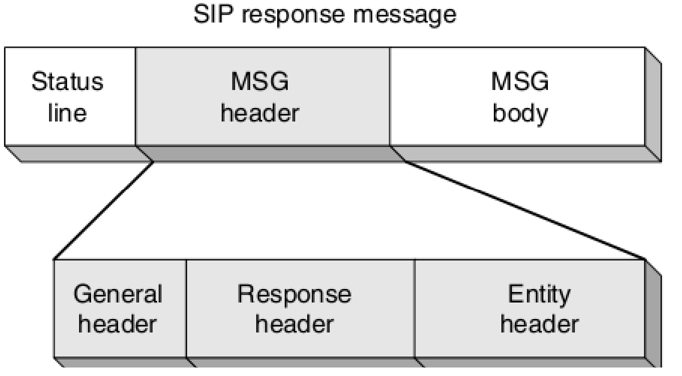
  – REGISTER: Allows a client to bind the address in a request message to one or more URIs where the client can be reached

  – OPTIONS: Allows a client to query the server about its capabilities

SIP Messages

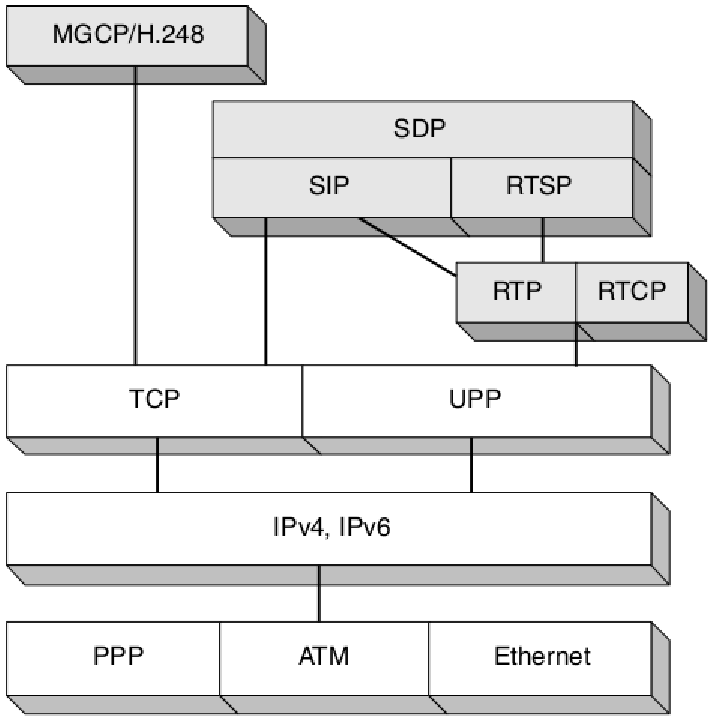
Response Messages

- Allows a server to respond to a request from a client
- Response-header: contains the fields that include
  - Status of the request
  - Reason for the status
  - To and From addressing
  - call ID
  - Information about the server issuing the response, etc
- Response travels the same route as the request



SIP System Architecture

- A set of system components and their interfaces
- Mainly concerned with application layer and transport layer protocols
- SIP and SDP are used for SIP system signaling
- MGCP/H.248 supports interworking with PSTN media gateways
- RTSP is used to provide multimedia session control for applications such as multimedia conference calls



SIP System Architecture

Session Description Protocol

- Allows a client to announce the existence of a multimedia session to other clients.
  - Encapsulated inside the SIP message body
- Each SIP message contains zero or more SDP messages
  - Each SDP message can contain only one session description
    - SDP allows the descriptions of multiple sessions to be concatenated into one SDP message (advanced feature)
- Enables other clients to join in a session (multimedia conference call)
- The information SDP communicates to clients includes
- Session name and purpose
- Time period during which the session is active
- Type of media used for the session
- Other information (address, port, media format needed)

SIP System Architecture

Real-Time Protocol (RTP)

- Real-time transport protocol providing end-to-end delivery services to support real-time-sensitive applications
  - Interactive audio and video
  - VoIP and multimedia applications
- RTP services include
  - Payload type identification   Sequence numbering   Time stamping
- Operates at the transport layer (on top of UDP)
  - Utilize its multiplexing and checksum services
- RTP tailored for real-time applications
  - Timing information in RTP synchronizes and displays audio and video
  - Determines loss or out of order packets
  - Provides data compression
  - Provides auxiliary profile and payload format specifications

SIP System Architecture

Real-Time Protocol (RTP)

- In a multimedia session, each medium is carried in a separate RTP session
- Audio and video travel on separate RTP sessions
- Recipient selectively accepts a particular medium
- RTP does not provide any mechanisms for
- Timely delivery
- Quality-of-service
- In-order delivery
- Must be accompanied by other mechanisms
  - RSVP and TCP to support resource reservation and to provide reliable service

SIP System Architecture

Real-Time Control Protocol (RTCP)

- Monitors the performance of RTP sessions
- Provides the following four services

Performance monitoring

- Provide information to an application regarding the quality of data distribution
- Each RTCP packet contains sender and/or receiver reports that report statistics useful to the application
  - Number of packets sent/lost/interarrival jitter, etc.
- In response, sender may modify its transmission rate based on this feedback
  - Receivers can determine whether problems are local, regional, o global
  - Network managers use information evaluate networks for RTP applications

SIP System Architecture

Real-Time Streaming Protocol (RTSP)

- It operates over RTP over UDP over IP
- Syntax-wise, RTSP is designed to look like HTTP
- Performs three types of operations to users
  - Invites a media server to join a multimedia session
  - Interface a media server to retrieve media data
  - Adds additional media to an active presentation session
- Designed to deliver real-time data content in the form of streaming
- Packet data streaming breaks the data into packets of sizes based on bandwidth available between a client and a server
- Supports playback of the data in real-time fashion
  - When enough packets have been received by the client, the client applications can be playing one packet, decompressing another and downloading the third

SIP System Architecture

RTP source identification

- RTCP carries a transport-level identifier for RTP source
  - Known as the canonical name (CNAME)
  - Used to keep track of the participants in an RTP session
  - Associates multiple data streams from a given participant in a set of related RTP sessions, e.g., to synchronize audio and video streams

RTCP transmission interval adjustment

- Prevents control traffic from overwhelming a network
- Allow RTP to scale up to a large number of session participants
- RTCP has the ability to limit the control traffic to at most 5% of the overall session traffic
- Achieved by adjusting the rate at which RTCP packets are sent as a function of the number of RTP session participants

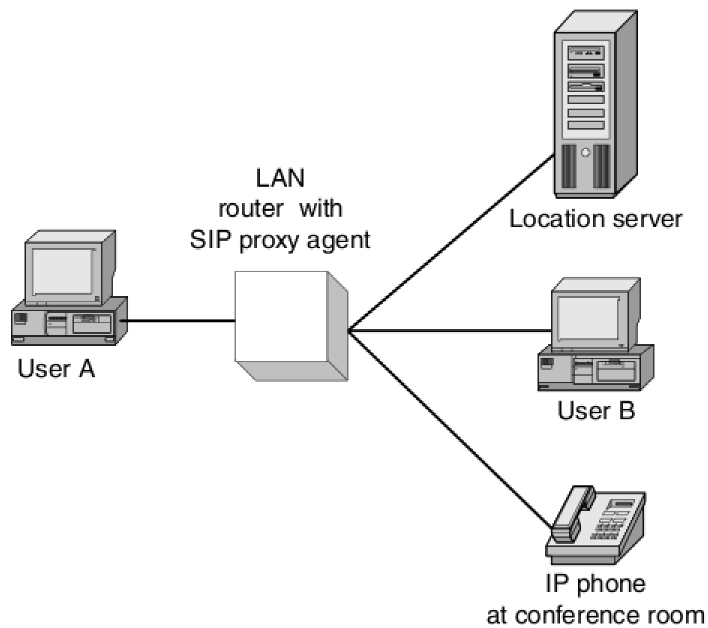
Session control data multicasting (optional)

- Convenient method for multicasting a minimal amount of information to all session participants (e.g., notification)

SIP System Operation Example

1. After user A dials for user B, the SIP UAC at user A’s PC sends an INVITE request message to a SIP proxy server on the LAN

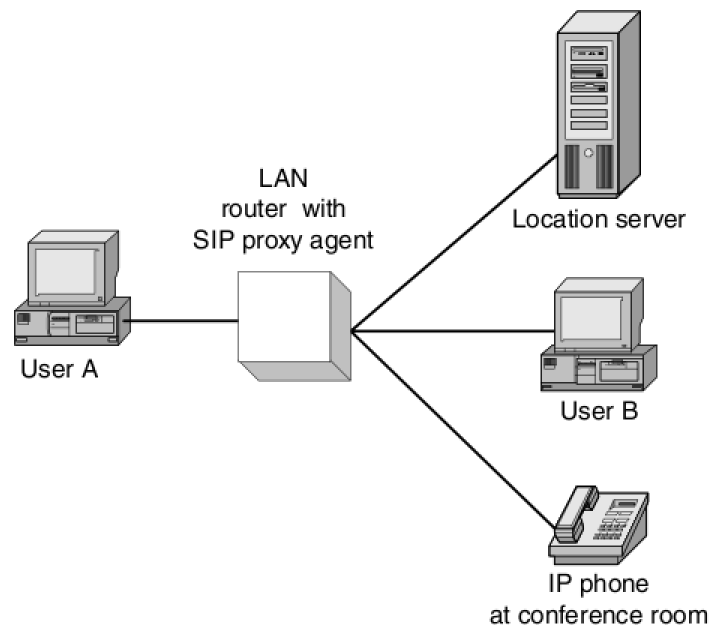
- User B is identified by the email address in the message, and the INVITE message initiates a SIP session



SIP System Operation Example

2. The proxy server sends a request to the location server to get the detailed address of the called party

- The location server sends back a response with the current address of user B
- The location server is either manually configured for the proxy server or can be dynamically discovered by the SIP server the system initialization time

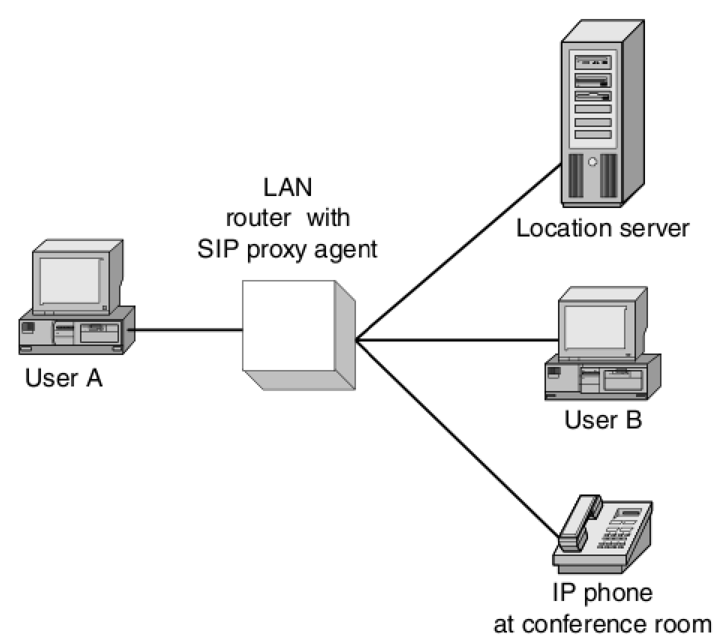


SIP System Operation Example

3. The proxy server initiates another INVITE message with the IP phone number as the to address in the message header on behalf of user A

4. The IP phone in the conference room, after user B picks up the phone, sends a response back to the proxy server

- The proxy server then generates and sends response to user A that contains the OK status of the request

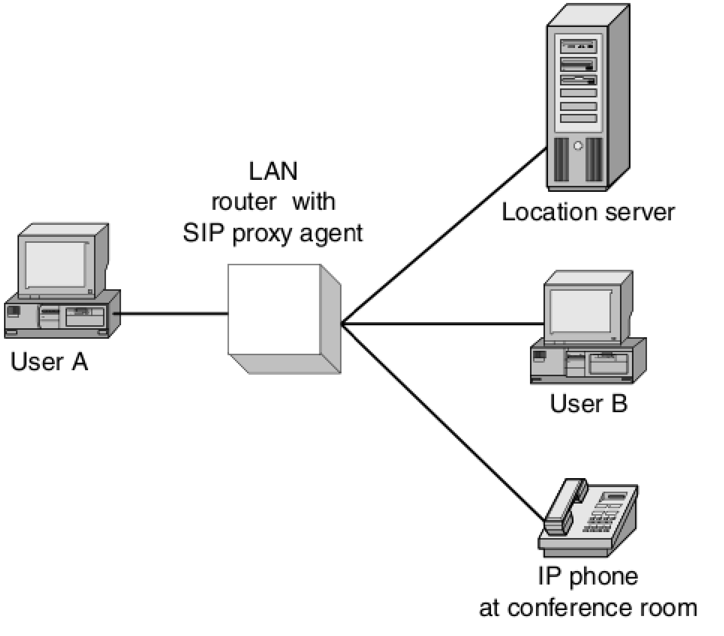


SIP System Operation Example

5. User A then sends an ACK message to acknowledge receipt of the response to the INVITE message and confirms the UPD and RTP ports to be used to carry the phone conversation

- The call setup is then completed after this message

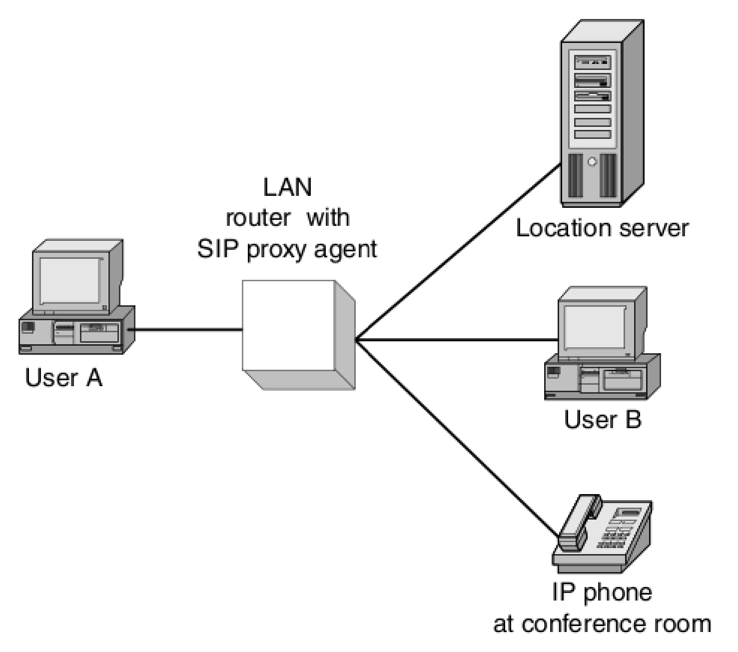
6. The IP packets containing the compressed phone conversation are transmitted between user A's PC and user B's IP phone, using RTP packets over UDP over IP



SIP System Operation Example

7. The UAC at user B's phone issues a BYE request to the server after user B hangs up the phone when the conversation is finished

- The proxy server then issues a BYE request on behalf of the SIP client to the calling party
- The UAC at user A's PC stops transmitting any data to the destination indicated in the BYE message



SIP Supported Services

- Call Processing Language (CPL) server allows users to create simple Internet-based telephony services
- A CPL server is an execution environment that can execute the services created with CPL
- Other types of application server with which a SIP server can interact include LDAP servers, database application servers, or XML servers
- Advanced features
- Call forwarding Call transfer Caller ID
- Three-way calls Call waiting Camp on
- Do-not-disturb Call hold and call return
- Business PBX and centrex services

Billing for SIP Systems

- Traditionally the raw data from which billing data is derived, called call detailed records (CDR) is based on call models
- The better defined the call model, the easier to extract the CDR data
- H.323 call model is largely based on the Q.931 call model, and thus detailed records can be generated with little difficulty
- SIP represents a quite different call model
  - Distributed does not fit well into the established patterns of call models
- To support sustainable business model, new standard billing models need to be established

SIP vulnerabilities

- Registration
- Prevent unauthorized registration modification
- Impersonation of Registration Server
- Prevent attacker from impersonating a valid registration server
- Protecting SIP message bodies
- End-to-End security
- Prevent attackers from interfering with call setup negotiation
- Session security
- Ensuring attackers can not alter sessions
- Protecting SIP headers
- Denial of Service
- Protect against numerous attack strategies that can generate large volume of SIP msgs at target host

Considerations for securing SIP

Entire SIP message can not be encrypted end-to-end

SIP relies on proxies to modify/insert header fields

SIP transport mechanisms are specified on a hop-by-hop basis

User has no control over how proxy server relays request

Firewalls/NATs present major challenges