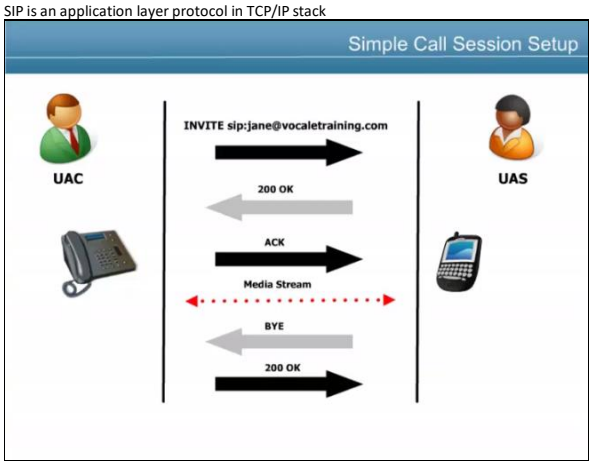
-Chapter 1 - Core SIP (Session Initiation Protocol)

User benefits – more services, low cost - SIP is based in text, client server mode (request, response), RFC 3261 - SIP is an application layer protocol

SIP – Signaling Protocol, Controls Multimedia Sessions, Establish user Presence, Locate Users (SIP Mobility), Setup Modify and Tear Down Sessions.

SIP is an application layer protocol in TCP/IP stack



SIP Components:

User Agents b2bua

-UAC (Initiates a call, 1 Invite, 3 ACK) – SIP entity that generates requests

-UAS (Receives call, 2 OK) – SIP entity that receive requests and generates responses.

Registrar Servers – UA use to register current location on a network

-When UA Registers tells registrar about features capabilities (RFC 3840)

Proxy Servers – assists in the discover and setup between UA, updates Location Server

-Forward request to the next server, interpret message and if necessary rewrite

3 types of Proxy servers:

-*Stateful* – keeps state information for the entire duration of a SIP session, used when extra services used (CF busy or NA)

-*Stateless* – keeps no state information when helped out a UA forgets everything about the transaction. Used for high load.

-*Transaction Stateful* – keeps all state information on all transaction that are pending, once session is established the proxy forgets the state information.

-*"Super Stateful"* – can use the Record-Route header in SIP messages in order to be kept on the signaling path of all subsequent exchanges, useful for supplying billing information

-It's possible also to set up the proxy server to act as a Stateless proxy for some calls, Stateful for others and even as a redirect based on criteria.

-Can "fork" request to multiple location registrations

-Used to be the only one allowed to leave the corporate network, can be used as the corporate firewall. (DHCP option 120)

Redirect Servers – forward information to UA doesn't involve in the call setup, just forward information to initiator of call.

Location Servers – contains the registered location, is used by the redirect or proxy servers, the components are:

-DB – updated by location and registrar servers, components can run in same server, and an external DB as AD

- DNS servers

SIP Gateways – translate signaling (probably media) to communicate legacy devices

RFC (Request For Comments) is sent to IETF

1 Proposed Standard -> 2 Draft Standard -> 3 Internet Standard

URI (Uniform Resource Identifier) – string that identifies some kind of resource (someone@domain.com) the main types are:

1) Services – example conferencing unit 2) Device 3) User – something static goes to business card (is also known as AOR Address Of Record)

URL (Uniform Resource Location) – URI form that also tell how to reach the resource (http://www.google.com)

SIP addressing

user@domain -> user = name, telephone host = domain, IP

SIP Messaging

Is based on request and responses, authorization and encryption can be used.

SIP Request – consist of a Request Line, several headers, and empty line and a message body

Request Line – Three Elements: Method, request URI and Protocol

Methods:

- INVITE – initiates a call, can also be used for session modification.
- ACK – used to respond to the 200 OK result of an initial Invite (including re-Invites), SIP Method that doesn't get a response
- BYE – termination of a call or session
- CANCEL – cancel pending request
- REGISTER – register used by the UA, binding Agent URI to an AOR, so SIP Server knows the location of UA
- OPTIONS – used to find out what UA media capabilities are, but not set up a session.
- INFO – used for communicating mid-session signaling info
- PRACK – provisional ACK used only to a 1xx style response, useful when Invite had no SDP body, it includes the relevant SDP detail. RFC 3262
- SUBSCRIBE – used to request notification of an event or set of events at a later time (example, request notification when IM Presence change details)
- NOTIFY – used to notify an event that was requested by an earlier SUBSCRIBE, used also to notify MWI.
- REFER – used to transfer calls and also contact external resources
- UPDATE – allows client to update parameters of a session (has no impact on the state of dialog)
- SERVICE – carry SOAP message as its payload
- BENOTIFY – Best Effort Notify, used by Microsoft
- COMET – used to confirm that conditions to make the connection have been met such as QoS requirement
- MESSAGE – allows transfer of IM where requests will normally carry the IM content in the request body.

Request URI contains the next hop in the path. Only the UA that originated the INVITE can send an ACK for a final successful response.

SIP Response – consist of a status line, several headers an empty line and a message body

Status Line has 3 elements: protocol version, status code and a reason phase.

Response Codes are made up of 3 digits, first digit indicates the class of the response and the other 2 digits are used to represent the "reason phrase"

• 1xx – Informational response, request was received and is still being processed.	**Provisional Response**
• 2xx – success reponse, action was received, understood and accepted.	
• 3xx – redirection response, further action needs to be taken in order to complete the request.	
• 4xx – client error response	**Final Response**
• 5xx – server error response	
• 6xx – global error response	

Analyze SIP Header Invite

Header – indicates method type

*Via – show layer 4 transport protocol to use, IP/Port the response must be send back to, branch is a unique id for transaction, rport = security, store all the proxies that handle the request, is used for detecting loops

*From – shows details of the caller and callers SIP URI

*To – details of the called party (usually contains the public address of the destination party)

*Call-ID – Globally unique ID for this particular dialog

*CSeq – used to identify an order transactions

*Max-Forwards – Limit the number of proxies or gateways (70 is default)

Contact – shows SIP URI that can be used to contact this Agent with subsequent request

User-Agent – Model of software/hardware used

Accept – Application/SDP

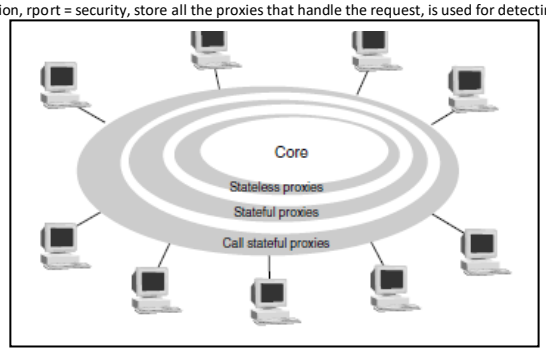
Allow – set of methods supported

Allow-Events – details some basic events that UA supports

Session-Expires – session interval for a SIP call

Content-Type – describes the body contet

Content-Length – length of the SDP body in bytes



ACK – used to acknowledge the reception of a final response to an INVITE

INVITE is the only method that uses 3 way handshake

CANCEL doesn't have effect a transaction once a final response has been sent. Proxy Servers can only ACK non successful final responses. Successful Responses are always ACKed by the UA initiating the INVITE

SIP is designed for stateless server at the core. After an INVITE all subsequent requests (except ACK and CANCEL) contains a CSEQ which is the result of increment by ONE the CSEQ of the original requests

Header remains the same during the session.

Analyze Header 200 OK

Via – inserted by servers into requests to detect loops and to allow responses to find their way back to.

From – same Invite

To – same Invite

CSeq – same

User-Agent – Agent used

Call-ID – same as Invite

Call-Info – additional information for the called party

Contact – same as Invite

Allow-Events – basic events supported

Allow – Set of methods allowed

Session-Expires – session interval

Record-Route – are inserted by the proxy to force future requests in this dialog to be routed though proxy

Content-Type – body content

Content-Length – Length of the SDP body

Via, From, To, Call-ID and CSeq are copied exactly from Request

Session Description Protocol (SDP)

RFC 4566

Handles the session negotiation process within a SIP transaction, carried as the message body of a SIP request.

SDP offer is made in an Invite request detailing characteristics that define the proposed media session.

MIME is used to define what is the body of a SIP message.

V – protocol information

O – Owner username

S – session name field

C – Connection information

T – Time

M – Media

Session can be modified by changing session parameters through SDP with methods such as re-Invite (CSeq is incremented) or Update

Hold
Re-Invite is sent to put on hold

- Sender send:
  - c=IN IP4 0.0.0.0
  - a=sendonly
- Receiver send:
  - a=recvonly

Re-Invite is sent to continue the conversation

- Sender send:
  - c=IN IP4 x.x.x.x
  - a=sendrecv
- Receiver send:
  - a=sendrecv

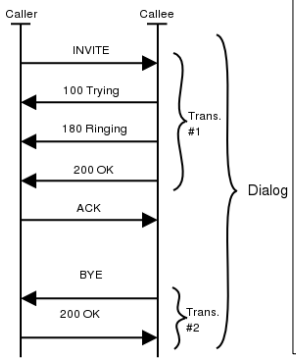
RFC 2543 – old way to put on hold setting the connection to c=0.0.0.0 (RTCP and IPv6)
RFC 3264 – new way to put on hold extends options available and discourages the use of c=0.0.0.0, some devices support both RFCs
Re-Invite uses the same Call-ID and increments CSeq
A retransmitted Invite uses the same Call-ID and same CSeq.
SIP Mobility
SIP support user mobility by proxying and redirecting request to users current location, user must register current location.
Call forking Parallel – invites will be sent to both devices, proxy send a cancel
Call forking Sequential – proxy receives a 302 (Moved)
Dialogs CallID, Local tag, remote tag
Transaction
Branch = z9hG4bK
MIME (Multipurpose Internet Mail Extensions)
MIME was defined to provide a way of attaching different document/file types to email messages.
SIP body are only meaningful to UA, message bodies can be encrypted end to end without losing any functionality.

VIA
Each element in the call path adds its own details in form of another VIA record.
These elements are removed at each hop on the way back in the Response.
Via Elements can be Hidden (Encrypted) – Record-Route elements cannot.
Via headers are used by proxies to see if any Looping has occurred.
Record route and Route keep in the route to proxies.
SIP entities treat INVITES and ACK in different ways than other methods as they are part of an 3 way handshake
Loose routing RFC 3261 lr
Strict routing RFC 2543
Routing request where to send it

1) Route
2) Contact (if there is no Route)
3) From (if there is no Contact)

SIP and B2BUA
Acts as a Server and Client.
Centralized management
PBX Call Management features
Billing functionality
Call Conferencing facilities
Ability to hide the network as Private IP address scheme
Ability to connect two different signaling networks
Implement and enforce policies
Manage Security and NAT issues

Notes:
If a transaction was initiated by an INVITE request then the same transaction also includes ACK, but only if the final response was not a 2xx response. If the final response was a 2xx response then the ACK is not considered part of the transaction. As we can see this is quite asymmetric behavior--ACK is part of transactions with a negative final response but is not part of transactions with positive final responses.
SIP entities that have notion of transactions are called stateful.



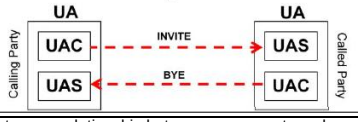
SIP Messages

- Message types: request, response
- Message format: ASCII-based, similar to HTTP
  - Formatted according to RFC 822 "Standard for the format of ARPA Internet text messages"
- Message syntax: [RFC 3261]
  - Start-Line: Request-line (for request), Status-line (for response)
    - Request-line: method request-URI SIP-Version
    - Status-line: SIP-Version Status-Code Reason-Phrase
  - Message Header: additional message information (Via, To, From)
  - Message Body: type of session to be established
    - SIP uses Session Description Protocol (SDP) to characterize a media session
    - SDP is included in the Message Body

Dialog identifiers consist of three parts, Call-Id, From tag, and To tag
Record routing according to RFC2543 rewrote the Request-URI. That means the Request-URI always contained URI of the next hop (which can be either next proxy server which inserted Record-Route header field or destination user agent). Because of that it was necesarry to save the original Request-URI as the last Route header field. This approach is called strict routing.
Loose routing, as specified in RFC3261, works in a little bit different way. The Request-URI is no more overwritten, it always contains URI of the destination user agent. If there are any Route header field in a message, than the message is sent to the URI from the topmost Route header field. This is significant change--Request-URI doesn't necessarily contain URI to which the request will be sent. In fact, loose routing is very similar to IP source routing.

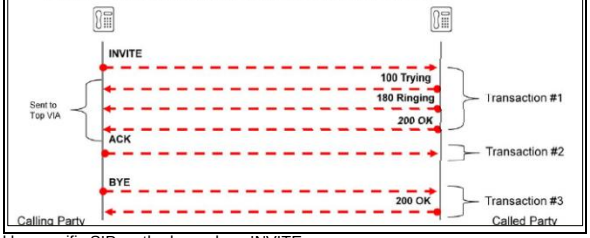
SIP Infrastructure

- User Agent (UA)
  - Is an IP endpoint participating in a session
  - Acts as both a user agent client or user agent server
- User Agent Client (UAC)
  - Is a logical entity that creates a new SIP request, and then uses the client transaction state machinery to send it
- User Agent Server (UAS)
  - Is a logical entity that generates a response to a SIP request
- The role of UAC and UAS lasts only for the duration of a transaction



Transaction

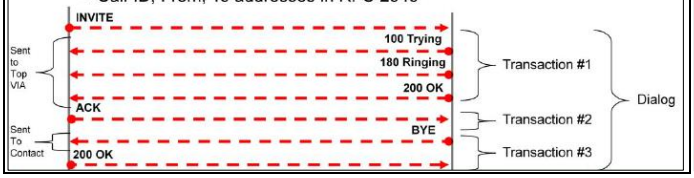
- A SIP transaction consists of a single request and any responses, including provisional and final, to that request.
  - Request sent by a client to a server
  - Responses to request (provisional & final) sent to top VIA field location
  - With exception of ACK on INVITE with 2xx response



Dialogs represent a peer-to-peer relationship between user agents and are established by specific SIP methods, such as INVITE.

Dialog

- Dialog is a peer-to-peer association between communicating SIP endpoints that persists for some time
- Dialogs are established by dialog creating transactions
  - Not all transactions create dialogs
  - A transaction may belong to exactly one dialog
- SIP messages carry enough state to identify the dialog
  - Dialogs are identified by portions of a message:
    - Call-ID, From, To tags in RFC 3261
    - Call-ID, From, To addresses in RFC 2543



Address-of-Record (AOR)

- AOR Is a SIP (or SIPS) URI that points to a domain with a location service that can map the URI to another URI where the user might be available
  - Typically the location service is populated through registrations
  - The URI of an AOR is different from the request-URI of a SIP message
    - Request-URI is associated with a particular device or UA
    - URI of an AOR is associated with a user
- An AOR is frequently thought of as the "public address" of the user
  - Represents an identity of the user, generally a long-term identity, and does not have a dependency on any device
  - Users can move between devices or even be associated with multiple devices at one time while retaining the same AOR

Back-to-Back User Agent (B2BUA)

- B2BUA is a logical entity
  - Receives a request and processes it as a UAS
  - Generates requests as a UAC in order to determine how the request should be answered
- Unlike a proxy server, a B2BUA
  - Maintains dialog state
  - Must participate in all requests sent on the dialogs it has established
  - Supports complete topology hiding
- The Net-Net SD can operate as a B2BUA and an edge proxy
  - The Net-Net SD, by default, operates as a B2BUA

The lowest layer of SIP is its syntax and encoding. -> Backus-Naur Form grammar (BNF)
The second layer is the transport layer.
The third layer is the transaction layer.
The layer above the transaction layer is called the transaction user (TU).

User agents contain a transaction layer, as do stateful proxies.
Stateless proxies do not contain a transaction layer.

The transaction layer has a client component (referred to as a client transaction) and a server component (referred to as a server transaction)
For a UAC, these rules govern the construction of a request; for a UAS, they govern the processing of a request and generating a response.
A dialog is a peer-to-peer SIP relationship between two user agents that persists for some time.
The INVITE method is the only way defined in this specification to establish a dialog.
A session is a collection of participants, and streams of media between them, for the purposes of communication.
Spiral is not an error condition, unlike a loop.
Stateful Proxy: A logical entity that maintains the client and server transaction state machines defined by this specification during the processing of a request, also known as a transaction stateful proxy. A (transaction) stateful proxy is not the same as a call stateful proxy.
User Agent (UA): A logical entity that can act as both a user agent client and user agent server.
UAC and UAS procedures depend strongly on two factors. First, based on whether the request or response is inside or outside of a dialog, and second, based on the method of a request.
A valid SIP request formulated by a UAC MUST, at a minimum, contain the following header fields: To, From, CSeq, Call-ID, Max-Forwards, and Via; all of these header fields are mandatory in all SIP requests.
The CANCEL request, as the name implies, is used to cancel a previous request sent by a client. Specifically, it asks the UAS to cease processing the request and to generate an error response to that request.
CANCEL has no effect on a request to which a UAS has already given a final response.

Chapter 3 – SIP, the PSTN and SIP-T
ITSP – Internet Telephony Service Provider
SIP to PSTN Call Flow

Invite	Setup (IAM)
183 Session Progress	Alerting (ACM)
180 Ringing	Alerting (ACM)
200 OK (Response to IAM)	Answer (ANM)
480 Temp Unavailable	Release Circuit (RLC)
BYE	Release (REL)
CANCEL	Release (REL)
181 Forwarding	Alerting (CPG)
4xx, 5xx, 6xx	Release (REL)
200 OK (Response to bye)	RLC

ISUP = Integrated Services Digital Network User Part
IAM = Initial Address Message
NPI = Numbering Plan Indicator

Early Media – is used to overcome a few problems that arise due to two different systems such as SIP and PSTN, is not required on standard PSTN calls, gives the opportunity to replace ringing media with corporate messages or other instructions for the caller before they get to speak to a real person, also allows Busy Tone and other Announcements to be played to the Caller even though the called phone has not been picked up.
Clipping is a problem where if a person using a PSTN phone answers their phone and starts talking, without Early Media the SIP phone that is calling them will miss the first part of the conversation as it hasn't received a 200 OK message to enable it to set up the RTP media path.
Early offer – Invite with SDP (codec choices)
Delayed offer – Invite with no SDP

SIP Gateways
SIP/PSTN gateways convert signaling and media conversion between SIP and PSTN.

SIP/SDP	ISDN/ISUP
RTP/RTCP	TDM

TRIP (Telephone Routing over IP) and Gateway Location
When looking to call a device that doesn't have a SIP URI (PSTN phone), calls needs to be routed to a gateway. When multiple gateways are involved supporting multiple ranges of E.164 telephone numbers it's important to route the calls to the correct gateway. TRIP intents to make it easy by advertising the phone numbers that gateway supports (using the Location Servers), it's a "protocol independent", is based on BGP (Border Gateway Protocol).

SIP-T and PSTN Bridging
SIP-T is used to describe PSTN-SIP, SIP-PSTN, PSTN-SIP-PSTN (SIP Bridging), Legacy-SIP-Legacy, used for LD calls, must provide translation between protocols and provide feature transparency across PSTN to SIP to PSTN interconnections.
ISUP messages has to be interrogated because some information that helps to route the SIP messages are built into the SIP Headers whilst other information are included as MIME message body.
SIP INFO is another SIP-T approach or method that is used for in-call ISUP signaling across an IP network.
SIP-I (SIP with encapsulated ISUP) another approach developed by the ITU its supported on most manufacturer gateways/softswitches/SBCs and is "more accurate" and generally preferred over SIP-T.
When privacy is requested by the PSTN the originated number is shown as unknown (anonymous).

- **SIP-T** or **SIP for Telephones** is a framework that can enable SIP networks to carry legacy telephone signals across an IP based network to another legacy network. This would have a dramatic effect on long distance call charges which is great for end users but of course there are technical issues that need to be addressed
- The legacy SS7 **ISUP** messages have to be interrogated by the SIP/PSTN gateway and then the information that will help SIP proxies to route the SIP message is built into the SIP header whilst other ISUP information added as a MIME message body. To ensure that the body is closed to 'unwanted' parties snooping on the network it can be encrypted and this is discussed in the security module of this course
- SIP INFO is another SIP-T approach or method that is used for in-call ISUP signaling across an IP network.
- In essence SIP-T must provide translation between protocols and provide feature transparency across PSTN to SIP to PSTN interconnections.
- http://www.rfc-editor.org/bcp/bcp63.txt

SIP-I

(SIP with encapsulated ISUP)

Is another (similar) approach that was developed by the ITU (not the IETF for SIP-T). It's supported on most manufacturer gateways / Soft switches and SBC equipment and is 'more accurate' and generally preferred over SIP-T

SIP and DTMF

- Inband -> is transmitted in the same RTP, some tones will be heard by parties in a conversation, codec compressions may make tones unintelligible, G711 is good, compress codecs will make tones bad
- RFC2833 – RFC used
  - out of band, makes DTMF into own RTP packets, compression survive digit 1 rtp event in wireshark
  - RFC 4733 – supersedes RFC 2833
  - new RFC 4734
- SIP Info – method is used to carry session control along the SIP signaling application/dtmf-relay

Chapter 4 – SIP and VoIP
Packet switching – better utilization than traditional dedicated circuits
RFC 3261 – "all SIP elements MUST implement UDP and TCP. SIP elements MAY implement other protocols"
RFC 2543 – implemented SIP in UDP but TCP is being used more and more as it has the ability to break up messages, re-assemble them at the destination and cope with packet loss with retransmissions.

Codec	Description	MOS	RTP/AVP Payload Type

G711u-law	Uncompressed codec for calls in North America and Japan	4.3	0
G711a-law	Uncompressed version of u-law codec for calls to areas other than North America and Japan	4.3	8
G729a	This codec produces compressed voice by using a special model called Code Excited Linear Prediction (CELP). Sample rate of 8Kb/s	3.7	18
G723	This is a codec that compresses voice and uses Voice Activity Detection	3.9	4
G722	In its G722.2 variant this codec can adapt its sampling rate in reaction to network congestion. The less congestion the higher quality of the samples. It also samples at 16Khz to produce a superior quality to other codecs.	4.3	9
iLBC	Internet Low Bit Rate Codec is a relatively new codec designed to work well over the Internet.	3.8	Dynamic

Wideband HD codecs
G722
G722.1
G722.2
AMR-WB
Speex
RTAudio
SILK

RTP is designed to support "real-time" traffic such as video and voice, runs only over UDP, doesn't provide guarantee timely delivery of the payload, or quality over the service guarantee, it does rely on lower layer protocols to provide these extra services. It can work with both unicast and multicast applications, provides services that:

- Payload type identification
- Sequence numbering
- Timestamps
- Delivery information

RTCP – can be used alongside RTP in order to provide information on the session and the participants, the types of RTCP packets are:

- SR – Sender Report, shows stats on transmission and reception for the participants in the session that are actively sending data.
- RR – Receiver Report, shows stats from participants that are not actively sending data in the session.
- SDES – Source Description items including identifying information such as CNAME and allows the binding of SSRC value with an actual id of the user.
- GOODBYE – end of participation in a session
- APP – this denotes Application specific functions that will effect/interact with the session
- XR – RTCP extension, can provide a rich set of data voice management (if implemented in VoIP devices) RFC 3611

RCTP Protocol measures VoIP quality using these following key metrics:

- Packet loss and discard rate and distribution of lost and discarded packets
- Round-trip delay
- Signal, noise and echo
- Call quality in terms of estimated R factor or MOS
- Configuration data such as jitter buffer size and configuration, and the type of packet-loss concealment algorithm in use

RTCP uses RTP port + 1

Quality of Services

Best quality

- One way end to end voice delay should be no more than 150 ms ping –l 218 x.x.x.x or ping –s (linux)
- No more than 30 ms jitter no more than 5%

Routers insert more delay Packet loss means a voice packet was sent, lost in transit and never received (less than 5%)

TOS and DiffServe

TOS = 3 bits (5) DSCP = 6 bits (46)

Chapter 5 – SIP Security

Authentication and Authorization

Proxy Authentication – when user needs to be authenticated proxy responses with a 407, sending a string nonce, user encrypt the password using nonce and MD5, and send back the invite including the hash with the password encrypted, it's decrypted by the server.

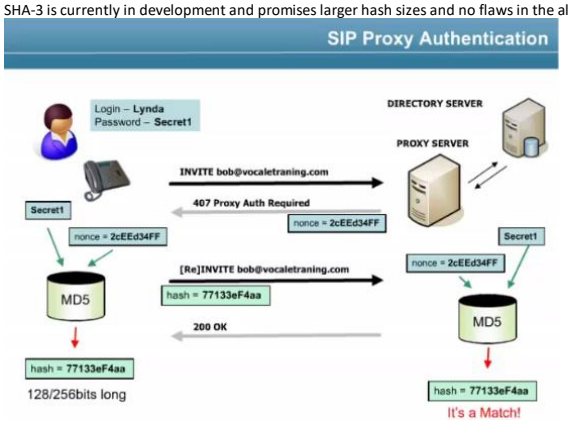
401 unauthorized is a response to register messages

Once authentication has been made, authorization will determine what an authenticated person can do.

128 bit MD5 mechanism is proven to flawed.

SHA-1 at 160 bits is a little more secure but has issues, hence the development of SHA-2 that can produce hash sizes of up to 512 bits.

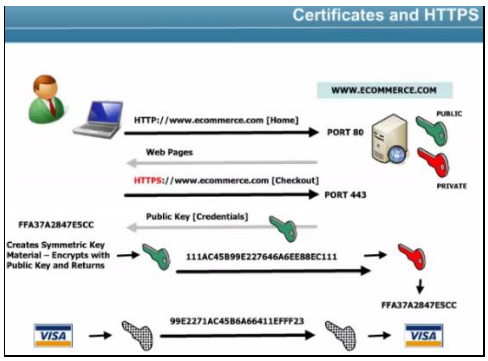
SHA-3 is currently in development and promises larger hash sizes and no flaws in the algorithm.

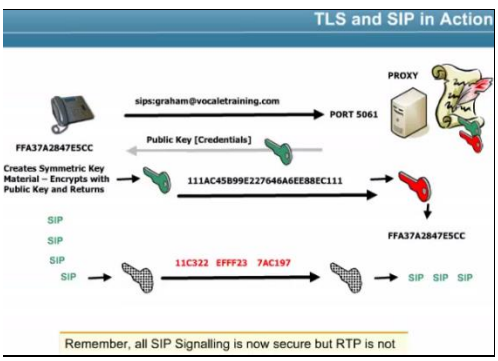


Encryption

There are many types of malicious attacks:

- VoIP interception, modification and replay
- Conversation eavesdropping
- Dictionary attacks
- Telephone number harvesting
- DOS and DDOS attacks
- SPIT and SPAM
- Flood attacks





Certificate authorities manages the certificates for some companies.

SIP with TLS only secures signaling, but no audio or other media, SRTP needs to be used to encrypts audio.

SSL (Secure Sockets Layer) first introduced via the Netscape browser, v3 introduced certificate support and SHA-1 support (http, ftp, smtp use it).

TLS has replaced SSL, RFC 5246 TLS 1.2
TLS is based on a shared secret known only to the server and the client, ensure that all SIP signaling messages are encrypted, work on an end to end basis where all systems between the UAs must support TLS or the call will fail. Can work on a hop by hop basis but this requires a new TLS session established between each point on the network.

If security/encryption along the whole path is needed to the end destination the use the sip address type of sips:
Crypto - RFC 4568
RFC 4474 – Caller ID Identity
RFC 6347 and 5763 – DTLS/SRTP
S/MIME (Secure Multipurpose Internet Mail Extensions) – was developed so emails can be encrypted and also digitally signed for proof of sender (only the sender needs a certificate and associated encryption keys) (for email encryption both sender and recipient require certificates), SIP has adopted S/MIME standard to enable it to encrypt SDP body parts to ensure information privacy, SIP headers are encrypted using TLS.
sRTP can generate encryption keys between two UA without the need of a certificate authority.
IPSec is a heavyweight solution as it requires a PKI to be in place:

- Adds a lot of overhead in the encapsulation process
- Is tended to be implemented in a lot of VPN

Attacks and responses
Attacks

- DOS – systems send vast numbers of SIP INVITE to a UA or Server, the system hangs or shuts down, denying service to the users.
- DDOS – Destributed Denial of Service occurs when there are multiple focused external attacks on a SIP gateway
- Call Pattern Tracking – find out who is making calls to whom, when and for how long, helps to build up a call profile for a user or even a company.
- ARP Poisoning – fools using MAC address so host in a conversation thinks they are talking to the correct MAC.
- Interjection/Modification – occurs when an unknown 3rd party intercepts SIP signaling, makes changes or even adds to the SIP messages and forwards messages on
- Directory Harvest for SPIT – using whois, DNS and google to "Directory Harvest" telephony numbers that can be used to send unsolicited VoIP messages to. SPIT is the IP Telephony variant of SPAM.
- Hacking – describe attacks on a network server or end device. Hacking starts by "footprinting" the network to check for vulnerabilities then use tools to exploit them.
- Spoofing – modify packets so that the recipient thinks you are someone else, can modify MAC, IP, extensions, etc
- Eavesdropping – voice capture for playback, building directory numbers for a SPIT attack and also Call Pattern Tracking.
- Capture + Replay – capture for playback

Responses

- Firewalls – prevent attacks, closing unneeded ports and providing a barrier to TCP/UDP port scans, apply security policies to control incoming/outgoing traffic.
- SIPS – by using sips, your sip UA is requesting a Secure session, preventing capture, spoofing, interjection and modification.
- Authentication – if a SIP device is not authenticated with a Proxy or other SIP server then it cannot communicate.
- Authorization – determines what an authenticated SIP UA can do, this also prevents rogue SIP devices from accessing services that you want to keep locked down.
- Anti-Harvesting - ensure that your DNS has secure Zone transfers to know devices.
- VLAN Port Security – ARP Poisoning and MAC spoofing is possible as any device can register its MAC address with a LAN switch, use switch port security.
- PKI – is the foundation of securing all SIP signaling and other network traffic, try to use certificate authority such as VeriSign.
- TLS, SRTP and IPSec – TLS secures sip messages, Secure RTP media streams, SBCs can break end to end security. IPSec encrypts all traffic regardless of the type of traffic, it needs PKI.

RFC 4475 – SIP torture test messages
Ethical Hacking

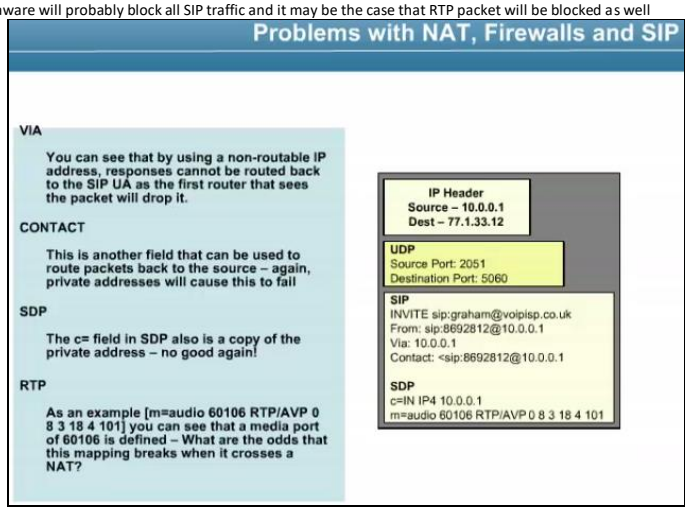
- Capture conversation
- SIP vicious
- Cain
- HoverIP – port scanning
- SIPScan
- SIPtap

NIST National Institutes of Standards and Technology

- Separate your networks, public and private, voice and data
- Use an ALG firewall or SBC
  - STUN doesn't work with a Symmetric NAT
  - TURN works but is limited to a single UA behind NAT
  - ICE is good but can take time to call setup and not all devices are compatible with ICE yet
  - UPnP not good with multiple NAT but fine for Home use
- Use strong authentication such as SHA-1 or MD5
- Use TLS end to end encryption or even an IPSec connection
- Don't use softphone in a security sensitive network as the PC runs on usually vulnerable OS attack

Chapter 6 – Firewall NAT and SBC

- Private addressing on the internal network can cause problems when using SIP through a NAT.
  - Full-cone NAT
    - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
    - Any external host can send packets to iAddr:iPort by sending packets to eAddr:ePort.
  - Restricted Cone
    - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
    - An external host (hAddr:any) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:any. "Any" means the port number doesn't matter.
  - Port Restricted
    - Like an address restricted cone NAT, but the restriction includes port numbers.
    - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
    - An external host (hAddr:hPort) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:hPort.
  - Symmetric
    - Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port, if the same internal host sends a packet even with the same source address and port but to a different destination, a different mapping is used.
    - Only an external host that receives a packet from an internal host can send a packet back.
- NAPT introduces another set of problems
- SIP has a firewall to content with
  - Corporate and personal firewall are placed at the edge of the network acting as a perimeter device that can permit traffic leaving and entering based on a set of policies or rules
  - Usually all traffic originating from within a network is allowed out and traffic from outside is allowd in (in response to request from the private network). HTTP and SMTP usually is allowed to enter into the network
  - Firewalls that are not SIP aware will probably block all SIP traffic and it may be the case that RTP packet will be blocked as well



Problems with NAT are caused because of the hostile environment made for the lack of standardized behaviors and controls in NATs.
Solutions

- STUN (Simple Transversal of UDP)

- How it works:
  - allow to communicate across NATs, before making calls client contacts STUN SERVER to find out the external IP Address that is using, on port 3489. That way when sending the messages clients can get back to the originating client.
  - Also use the IP/Port details in its register to the registration server to keep the appropriate firewall ports open.
  - rport entry overrides the dst port when SIP messages are returned to the client behind NAT as it is what STUN can see.
  - rport is filled in by the proxy or UAS
- problems:
  - STUN doesn't work behind symmetric NAT as new IP/Port mappings are created for each session
  - If firewalls are configured to drop UDP packets it will fail
  - UDP is not connection oriented so firewalls may close port pinholes causing session to fail
  - Multiple NAT can have problems

- TURN (Traversal Using Relays around NAT)
  - Operates similar to STUN, but it can also relay RTP streams as well as SIP messages (both are proxied)
  - Works with both UDP and TCP, so TCP can be used to ensure sessions stay open.
  - TURN works with symmetric NAT
  - TURN must have an Internet Facing address
- ICE (Interactive Connectivity Establishment)
  - ICE UA make a series of connectivity check in order to discover which is the set of IP address that will be guaranteed to work.
  - Loos at all of its local addresses and then queries its STUN and TURN server to collect more addresses it can be reached.
  - Then it starts its own STUN service, passes a copy of the IP Addresses to it and then sends all of the collected IP address to the destination device
  - The destination responds by sending a STUN request to each IP address with initiates a STUN reply back to the destination client with details of each IP address that worked.
  - The STUN device then sends a final notification back to the destination device to confirm the connection details
  - ICE RFC 5245
  - Will take time to enable ICE clients, good news is that actual devices may only need software upgrade or patch
  - Due to chaotic implementation of NATs it could take a while to implement ICE
  - As it checks for the best IP/Port combination to use it delays the call set up time
- UPnP
  - The protocol running on the SIP device queries the firewall/NAT directly for the external public address and port numbers
  - SIP device rewrites private addresses as usual in the sip message and SDP body with the public address
  - UPnP is supported by the majority of manufacturers
- RTP Problem
  - When caller inside send the rtp packet the firewall cannot know which port is going to be used so the response can be blocked
  - When caller outside send the rtp packet the firewall cannot know which port is being used for audio so the response can be blocked
  - Solving the RTP problem
    - Rtp are dynamically allocated
    - Firewall don't know these details
    - Opening more firewall ports is not an option
    - Symmetric RTP
      - The audio is sent to the port used for signaling as it is already opened
    - Media Proxy
      - The SIP devices register in the media proxy and forward the registration to the registration server as it was the SIP device
    - ALG (Application Level Gateway)
      - Is not unlike a Media Proxy
      - Can sit inside a DMZ controlled by the firewall
      - All sip and rtp packets are sent to the ALG
      - Works with NAT by changing the SDP body of the SIP
      - Can be software that is embedded on the firewall
    - SIP Aware Firewall
      - Rewrites the ports used to send the audio
    - SBC
      - Control billing
      - Ensure QoS
      - Apply usage policies
      - Apply security policies
      - Firewall/NAT issues
    - SBC Enterprise
      - Act as an ALG
      - Codec Conversion
      - TLS, SRTP and/or IPSec
      - Remote SIP devices
      - Benefits
        - Hide ip addressing
        - Apply CAC
        - Apply security policies
        - Apply QoS settings
        - Billing services
        - Scalate to 100,000 connections

SBC offers:
- DoS prevention
- DoS protection
- Access control
- Topology hiding
- VPN separation
- Fraud prevention
- Monitoring and reporting
- QoS
- Normalization
- Optimization

Chapter 7 – SIP Trunking

SIP Trunking – IETF defines as a virtual SIP entity on a server constrained by a predefined set of policies and rules that determine how to process requests. It's a logical connection from a PBX at a customer site to an Internet Telephony Service Providers (ITSP). Least Cost Routing (LCR)

SIP Trunks and MPLS

MPLS – is a mechanism in high-performance telecommunications networks which directs and carries data from one network to the next. MPLS makes it easy to create "virtual links" between distant nodes.

Impresion 30:46

MPLS Benefits
- Cheaper than other services
- QoS ensure great performance
- Disaster recovery, can switch to redundant circuits very quickly
- Better performance
- Future proofing

MPLS
DSL
ADSL
SDSL

SBCs
- Gives control
- Backup
- Interoperability
- QoS Settings
- Protocol Conversion (Lync only works with TCP)
  - Refer problems with SBC a re-Invites generates a new call
  - Refer RFC 3515
  - Transfers with ITSP RFC 5589

Enterprise PSTN identities
- DID sent to outside calls
- Enterprise name or even the caller name
- SIP PBX must be able to receive DID numbers to connect the correct UA

P-Asserted identity field

Allows an enterprise a common enterprise number to be called arties yet also provides an identity for the caller to be used for other services provided by the ITSP such as Application, Messaging, Presence, etc. This is the preferred method for managing identities. RFC 3325 P-Asserted to be removed when forwarding out of a "trusted domain".

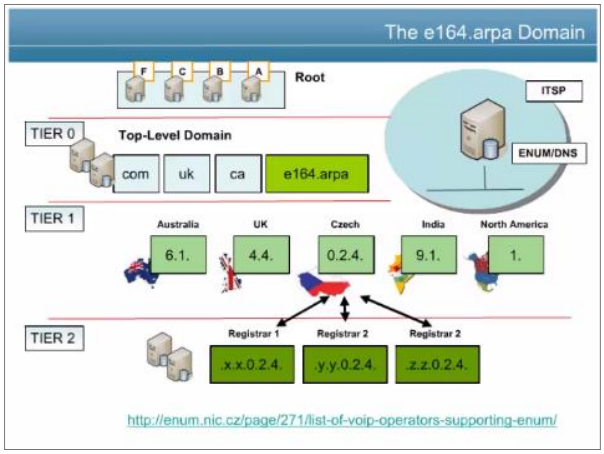
P-Preferred is a way in which a SIP UA can suggest which SIP URI (out of a few) to be used when populating the P-Asserted field. Updated 3325 RFC 5876

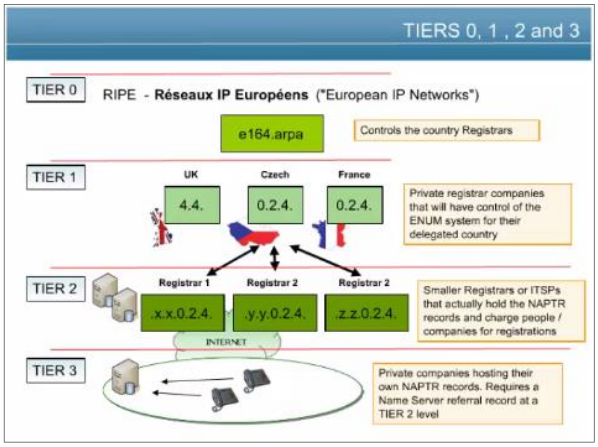
SIP Trunking troubleshooting and Interops
- SIP Trunks fail to initialize – spelling domain names, accounts and password, router ip address , firewall, DNS, FQDNS
- 403 Forbidden – Password problem
- 407 Proxy Authentication Required – Authentication needed
- Call Quality – Bandwidth, SLA.
- One-Way Audio – Firewall issue
- SIP trunks keep dropping – not getting keep alive
- Alternative ITSP – Known working ITSP to validate routes

Chapter 8 – ENUM DNS VoIP peering
E.164 is the International numbering plan for Public Telephone Systems, was developed by the ITU.
It has 3 parts up to 15 digits in total: CONTRY CODE National Destination Code Subscriber Number

Telephone **Nu**mber **M**apping (ENUM) relates to a set of protocols that map E.164 telephone numbers into domain names. Enables corporate VoIP islands to connect to PSTN and to each other easily.
Telephone Numbers are stored on DNS servers as NAPTR (Naming Authority Pointer) records, for example:
+4421216236776 -> 6.7.7.6.3.2.6.1.2.1.2.4.4.e164.arpa

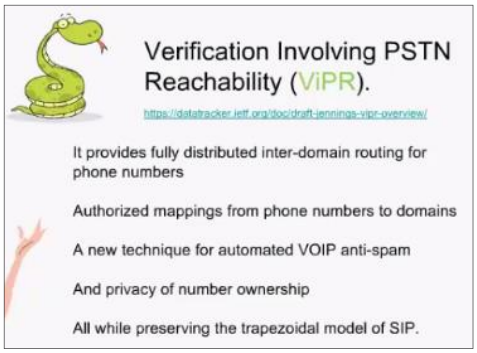
Enum look up to DNS ENUM uses the DNS infrastructure, 13 root servers (.com .mx etc)

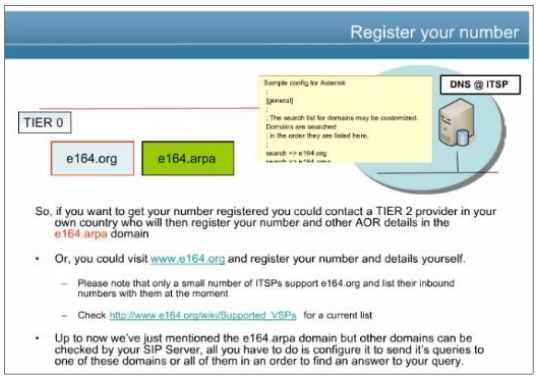


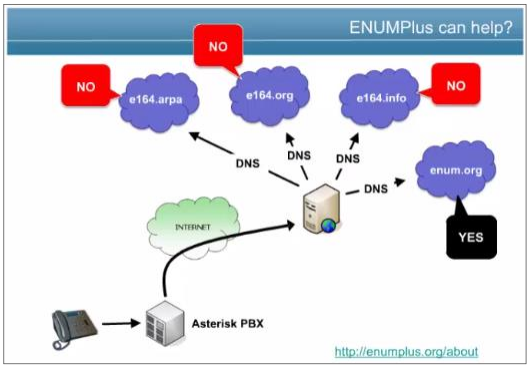


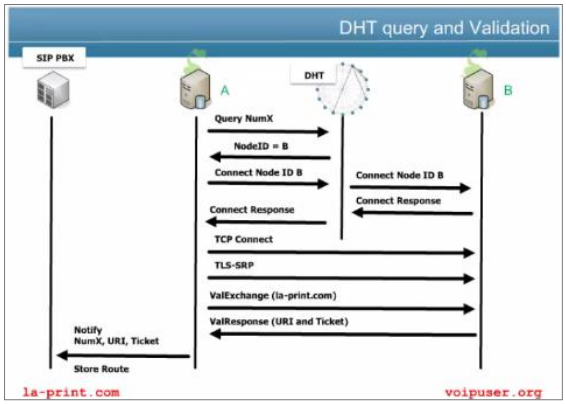
MARTINI
Multiple AoR reachabiliTy InformatioN Indication

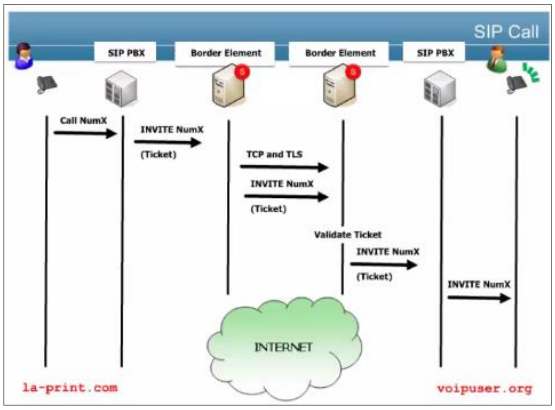
Public ENUM
Private ENUM
Operator

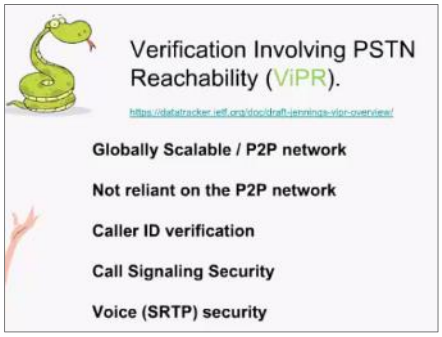






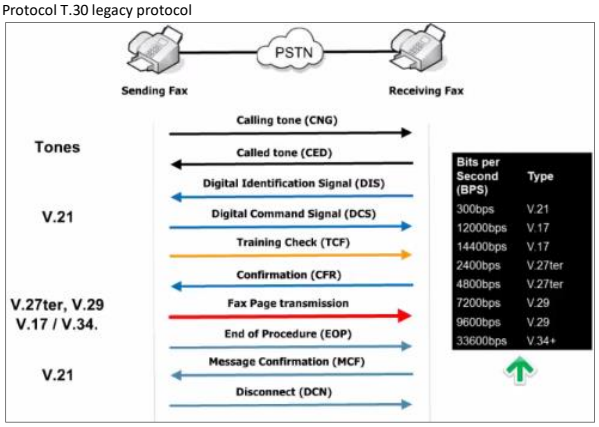






Chapter 9 – SIP and FoIP

Protocol T.30 legacy protocol

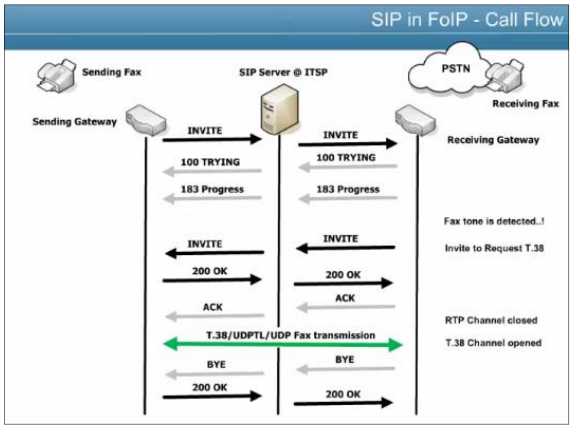


3 FAX IP protocol:

- G711 Pass through -> uses g711, faster than t38, sensitive to delay, packet loss jitter, SRTP
- T.37 tiff, email (aka store and forward) needs fax and email servers, not in real time, no receipt
- T.38 standard for real time, resolves issues with g711 (packet loss), receipt, less BW

T38 capabilities RFC 3407

UDPTL – Aplication Layer for T.38



Chapter 10 – SIP and UC

Instant Messaging and Presence Protocol (IMPP) CPP several RFC

SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions)

XMPP

Extensible Messaging and Presence Protocol

XMPP simplier than SIP/SIMPLE

SIMPLE is a complete protocol for IM/Presence/Voice/Video/Text

Conferencing

Focus is conferencing server