SIP – Session Initiation Protocol, project report for the course Datakommunikation och distribuerade system

Contents

Chapter 1

Introduction

Until the mid 1990 the telecommunication companies provided most of our communication needs. Today the picture is totally different. There is a need of new kind of networks to handle the communication. These will be primarily based on IP technology this also mean that a wide spectra of new services will show up and SIP could be a solution to handle many of the new challenges that will arise.

Session Initiation Protocol is a text based protocol similar to HTTP and SMTP. It was developed in the mid 1990 by IETF, who develops and promotes standards on Internet, and Multiparty Multimedia Session Control (mmusic), who develops protocols to support Internet teleconferencing and multimedia conferencing.

1.1 SIP is still under development

The Session Initiation Protocol working group are people that continue the development of the protocol. The working group will for example develop proposed extensions that comes from new requirements. The SIP Working group is charged with being the guardian of the SIP protocol for the Internet, and therefore should only extend or change the SIP protocol when there are compelling reasons to do so.[1]

The Session Initiation Protocol Project INvestiGation (SIPPING) is another working group. Group is chartered to be a filter in front of the SIP group. This working group will investigate requirements for applications of SIP. To know what has to be extended the group documents the use of SIP for applications related to multimedia and telephone.

Chapter 2

Overview of the protocol

SIP is an application-layer protocol that can establish, modify and terminate multimedia sessions or calls. SIP started as a real time communication protocol for voice over IP but has later on been expanded with new features such as video. It has been considered by some people to be the successor to H.323 which is a protocol recommendation to provide audio-visual communication sessions on any packet network and is used in different real-time communication among others "net meeting".[5]

SIP provides 5 services for establishing and terminating a session:

User location: determination of the end system to be used for communication;

User availability: determination of the willingness of the called party to engage in communications;

User capabilities: determination of the media and media parameters to be used;

Session setup: "ringing", establishment of session parameters at both called and calling party;

Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

[3]

SIP should not, however, be seen as the protocol that manages to establish the entire session including the streaming of data. It rather relies on other IETF protocols including RTP and RTSP. Besides the services provided SIP is responsible for providing security services such as denial-of-service prevention, authentication, integrity protection and encryption.

2.1 Capabilities

The following list shows some examples of what SIP is capable of:

Add / Drop media: SIP supports to add and drop media during a session. This means that if a A speaks to B over also using video stream over an established connection, can turn off the video and continue speaking. After a while they decide that want to turn it on again and do so, all this during the same session.

Find me / follow me: SIP gives the opportunity to be registered at different locations at the same time. This mean that if an incoming audio INVITE message arrives all devices will ring at the same time and stops ringing when one of the devices answers the incoming call. It is also possible to register with a video device during an audio call to be able to extend the cal with a video stream.

Presence and instant messaging: The SIMPLE working group of IETF the leading candidate to fulfill the requirements of IMPP.

Conferencing and distance working: Support for conference and distance working. This could be a teacher providing distance learning support to students spread around the country.

Multi party gaming: SIP can also support audio and video feed during multiplayer games. This could be taken care of either by the game itself or via some extra software.

2.2 Components of SIP

SIP is a peer-to-peer protocol. These peers are called User Agents. A UA can be either a User Agent Client, which is the application that initiates the SIP requests, or it can be a User Agent Server, which is a server application that returns a response initiated by the UAC.

2.2.1 SIP Client

Phones acts as either a UAS or UAC. Both SIP-capable phones and Software phones are able to initiate a request and respond to requests.

Gateways provide many translation services between different endpoints and terminal types. For instance a gateway to PSTN.

2.2.2 SIP Server

Proxy server is a device that receives SIP requests from the client and then redirects them to the appropriate server. It is also responsible for authentication, authorization, network access control, routing and security.

Redirect server responds to Client with which hops the UAC should take in order to speak to the UAS.

Registrar server is responsible for registration of UACs current location.

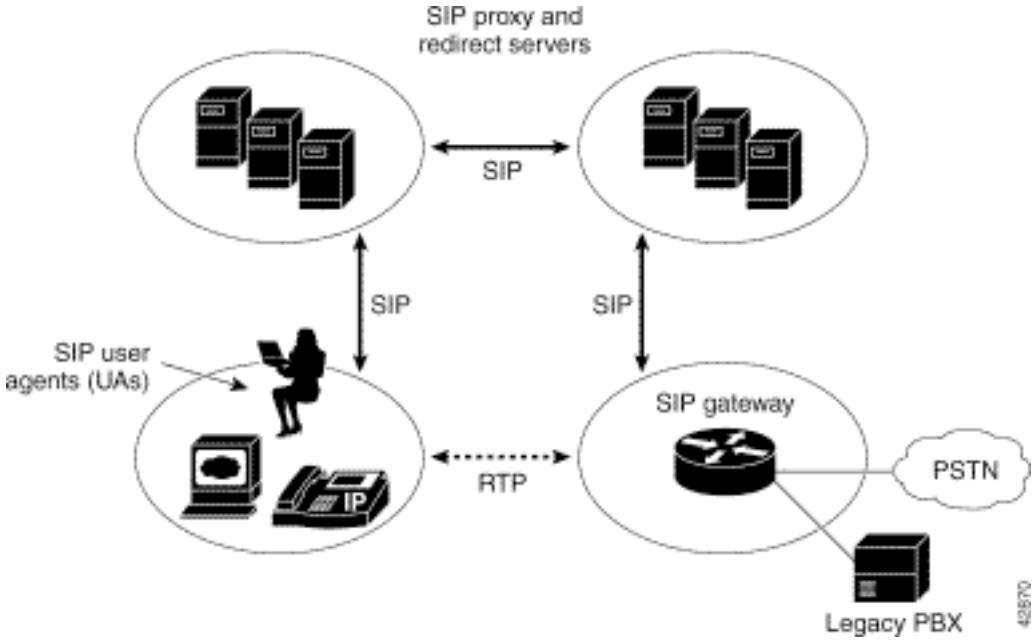

Figure 2.1: This figure shows different components of SIP, their roles and how they interact with each other.

Chapter 3

Overview of the operation

Two persons A and B wants to communicate over the Internet (an IP network). Part of this can be done using SIP. Both parties that are going to communicate use a user agent which is some sort of software. This software enables communication between A and B. The software can be installed in a PC or some other device such as a mobile device.

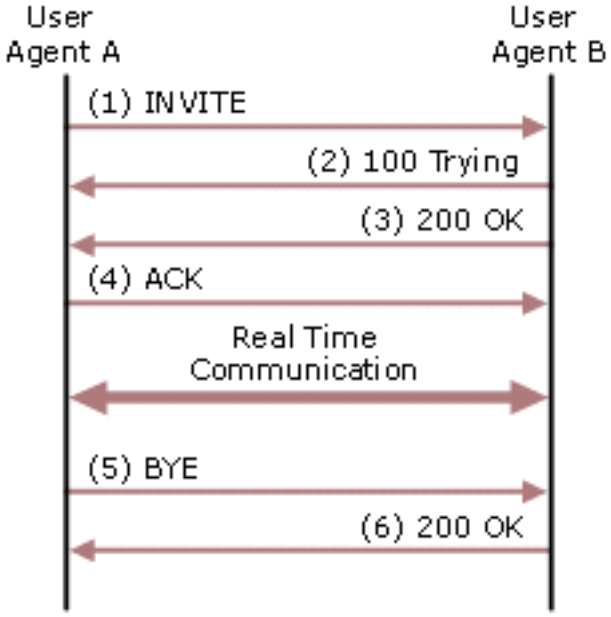

Figure 3.1: This figure represents the call flow for initiated calls by the user agents

Lets say that A wants to speak with B. The first thing A will do is to send a message to B on the standard SIP port (5060). This message is called INVITE message and it contains information about what media that can be used. When B who is listening on the SIP port is receiving the INVITE message he responds by sending back a message containing the type of media that B prefer. When A finally responds to B with an ACK message both parties know what type of media that will be used and what bandwidth they can use, they are have also been aware of each others IP and what ports that will be used for the communication. When booth parties have received their ACK:s the start to communicate with each other over the decided ports. This is often done by using the RTP

(real-time protocol) but some other transport protocol can also be used. Sometimes one of the communicating parts wants to change the media during communication this can be done by sending additional SIP messages. When communication is done either A or B send a BYE message to end the session and when this I received bye the part on the other side the session is closed.

The following encoded message is an example of what an INVITE-message might look like:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

The datagram protocol UDP is often used during these sessions but also other protocols can be used but these are optional. Due to that UDP is an unreliable protocol SIP can handle retransmission itself.

3.1 SIP addressing

SIP addresses are expressed as URI which contain the URL of participating parties. The basic form in which URLs are expressed is: `sip:user@foo.com`

However the URL can also contain all the parameters used to establish a call. For instance `tel:+358-555-1234567;postd=pp22` becomes `sip:+358-555-1234567;postd=pp22@foo.com;user=phone` which means that we want to establish a call to someone with a global phone-number. Using standard URL in SIP implies that a DNS must be used to map domain names and hosts into IP numbers. This is an important aspect due to the integration between other web based technologies.

Chapter 4

Integration with PSTN

Setting up communication between two clients on the Internet (or IP network) using SIP may not be so difficult but what about if a person on the Internet wants to speak with some other person who is not on the network? What if the person is on the public switched telephone network?

The PSTN (public switched telephone network) is the circuit-switched telephone network which people around the world uses when they do a "ordinary" phone call. The PSTN is big, there are still over 200000000 people using this. There are other switched telephone networks also but they are often separated such as military networks and corporation networks.

So let us go back to the problem. Two persons A and B wants to speak with each other. Person A is sitting on the Internet while person B is sitting on the PSTN. Since they are sitting on two different networks which speak different languages they cant communicate. The solution to this is to use an adapter that converts the signals from PSTN to fit into the Internet and vice versa this device is called gateway. The first SI message sent to start the session can look like the message above e.g;
`sip:+358-555-1234567;postd=pp22@foo.com;user=phone`

4.1 ENUM

One problem that arises when a client on a PSTN wants to call to another client on a IP network is how to get in contact with this person (the caller can only use digit keys). The answer to this question is ENUM. By creating a global directory which maps to SIP addresses or email etc. Support for E.164 numbering in DNS (ENUM) allows SIP clients and servers to send and receive phone numbers in place of SIP URI:s in messages and to route them as usual. The E.164 number queries are formed as a reversed dot separated number to which the string `.e164.arpa` is added. E.g. the number +046317721010 becomes after the conversions `0.1.0.1.2.7.7.1.3.6.4.e164.arpa`

DNS and ENUM helps an ingress gateway to resolve the SIP address from a E.164 number so it then can reach the target.

4.2 FORKING

SIP proxy server offers forking. This means that they have the capability to forward incoming messages to several different receivers. This can be to a phone and at the same time also to a web camera and a desk computer or lap top. The proxy server then checks the answer and makes sure that only one device will answer so that the asking client gets a single stream back.

4.3 Virtual private network

Because of the use of indirection capabilities of SIP, ENUM and DNS virtual private networking is made easy to handle and develop. A single SIP proxy server can provide address mapping and forwarding services for a remote location making it look like people are on the same domain but they actually are not.

Chapter 5

SIP and security

SIP deployment in a IP network is exposed to a large variety of different threats for example ID and Internet. ID: Displaying the right ID of a caller is a legal requirement for the phone companies, What happens if someone fakes their ID? Internet The main reason why Internet is not safe is that there has never been enough safeguards and equipment to keep a network totally safe on the Internet.

A SIP-based network will face two different threats. These are internal and external threats. The external threats are attacks launched by an aggressor who is not participating in the actual SIP-based communication. The external threats arises when the information crosses boundaries / networks which involves a third-party or untrustworthy networks.

The other threat is the internal threat. This is often a threat launched by a SIP-session participant. Because a SIP-session participant is launching the attack the participant can no longer be trusted. Because the network is protected by firewalls and so on one donâĂŹt expect attacks from the inside and therefore these attacks are more complex and it is much more difficult to find the source of the attack.

Denial of Service attacks: The attack means that by sending lot of strange, malformed or other types of packets to a server or gateway this computer can stop responding. Solution: Configuring of devices. i.e. stop specific packets.

Eavesdropping: An attacker can get hold of the information transmitted to the other side. *Solution: Encrypted traffic prevents this kind of attack. E.g. Secure RTP*

Packet spoofing: An attacker pretends to be another by sending fake packets. *Solution: Send address authentication between call participants.*

Replay attacks: Retransmission by an attacker of an earlier sent message. *Solution: Encrypt and sequence messages; in SIP this is offered at the application-protocol level by using CSeq and Call-ID headers.*

Message integrity: A message received may not be the same message that was sent in the first place. An attacker could have changed the content in the message during the transmission. *Solution: Authenticate messages.*

SIP offers different security mechanisms for end-to-end and hop-by-hop encryption of sensitive information such as header fields and the message body. Many of these features are included in the SIP such as different methods and variations of HTTP authentication

or secure attachments. Transport and / or network-layer security encrypts SIP signalling traffic, guaranteeing message confidentiality and integrity. One example of a popular security mechanism that provides transport layer security is IP-Sec (IP Security).

Chapter 6

The future of SIP

Due to it's openness based on IETF standards, SIP has quickly gained acceptance by many communications equipment manufacturers and software companies. It's text-based message format and flexible addressing via commonly used URL makes it ideal for future development. Because SIP uses the building blocks of the Internet it can be easily implemented in any device that support the TCP/IP-protocol suite. The current development of SIP-based devices and software clearly states that SIP will be the major technology providing all communication, including; video and audio conferencing, presence notification. SIP integration of the these features into a one package will hopefully provide us with only one SIP-URL in order to make phone-call or have a video conference or chat. This will hopefully eliminate the need of using different technologies for using these services.

Appendix A

Glossary

SIP Session Initiation Protocol.

IETF Internet Engineering Task Force

RTP Real-Time Protocol

RTSP Real-Time Steaming Protocol

SIMPLE Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions

TCP Transport Control Protocol

UDP User Datagram Protocol

IP Internet Protocol

IMPP Instant Messaging and Presence Protocol

URI Uniform Resource Identifier

PSTN Public Switched Telephone Network

DNS Domain Name System

SMTP Simple Mail Transfer Protocol

VPN Virtual Private Networking

IPsec Internet Protocol Security

ENUM Electronic Numbering

MMUSIC Multiparty Multimedia Session Control

UAC User Agent Client

UAS User Agent Server

Bibliography

[1] A. Mankin, S. Bradner, R. Mahy, J. Ott, B. Rosen *Change Process for the Session Initiation Protocol*, RFC 3427, December 2002

[2] Handley, H., Schulzrinne, H., Schooler, E. and J. Rosenberg, *SIP: Session Initiation Protocol*, RFC 2543, March 1999.

[3] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, June 2002.

[4] *Microsoft Real-Time Communications: Protocols and Technologies*, <http://www.microsoft.com/technet/prodtechnol/winxppro/plan/rtcprot.mspx>

[5] Wikipedia, *Session Initiation Protocol* <http://en.wikipedia.org/wiki/Session_Initiation_Protocol>

[6] IPTEL.ORG, SIP and PSTN connectivity <http://www.iptel.org/ser/doc/presentations/ripe46-eof-enum-sip-pstn.pdf>

[7] Cisco Systems, *Security in SIP-Based Networks*, <http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae4

[8] Cisco Systems, *Overview of the Session Initiation Protocol*, http://www.cisco.com/univercd/cc/td/doc/product/voice/sipsols/biggulp/bgsipov.htm