Skype VoIP service- architecture and comparison

Hao Wang
Institute of Communication Networks and Computer Engineering
University of Stuttgart
Mentor: Dr.-Ing. S. Rupp

ABSTRACT

Skype is a peer-to-peer (P2P) overlay network for VoIP and other applications, developed by KaZaa in 2003. Skype can traverse NAT and firewall more efficiently than traditional VoIP networks and it offers better voice quality. To find and locate users, Skype uses "supernodes" that are running on peer machines. In contrast, traditional systems use fixed central servers. Also Skype uses encrypted media channel to protect the dada. The main contribution of this article is illustrating the architecture and components of Skype networks and basically analyzing key Skype functions such as login, NAT and firewall traversal. Furthermore, it contains comparisons of Skype networks with VoIP networks regarding different scenarios. On that basis it reveals some reasons why Skype has much better performance than previous VoIP products.

Keywords

Voice over IP (VoIP), Skype, Peer-to-peer (p2p), Super Node (SN)

1. Introduction

It is expected that real-time person-to-person communication, like IP telephony (VoIP), instant messaging, voice, video and data collaboration will be the next big wave of Internet usage. VoIP refers to technology that enables routing of voice conversations over the Internet or any other IP network. Another technology is peer-to-peer, which is used for sharing content like audio, video, data or anything in digital format. Skype is a combination of these two technologies. It has much better performance by making use of advantages of both technologies. In the first part of this article is a brief introduction to VoIP, including the network architecture and the function of main components. Followed is the description of p2p network and its generations. It discards the "client/server" concept; instead it uses equal peer nodes to accomplish required functions. In addition, Skype network is introduced, which also displays the architecture and the components. The difference between VoIP and Skype networks is very clearly.

Because of this essential distinction in network architecture, VoIP products and Skype execute differently to fulfill the same task such as user search, signaling and NAT/ Firewall traversal. User search is a challenging problem in p2p networks due to the decentralized directory, while in VoIP networks it is not difficult because of the existence of the centralized server. But latter is less scalable and may have the "one point failure" problem if there is no replication mechanism. NAT/ Firewall traversal is a troublesome issue in both networks. Skype studies the mechanisms used in VoIP and changes one of them to adapt the requirement in p2p networks. In part four of the article, these two scenarios are carefully discussed.

Skype shows that signaling, the most unique property of traditional phone systems, can now be accomplished with self organizing P2P networks. How Skype handle this question is also discussed in part four. Another two important issues, Codec and security, are discussed at last. Skype integrates advanced technologies to ensure these two functions.

2. Background knowledge of VoIP

VoIP is a generic term that refers to all types of voice communication using Internet Protocol (IP) technology instead of traditional circuit switched technology. This includes use of packet technologies by telecommunications companies to carry voice at the core of their networks in ways that are not controlled by and not apparent to end users. The major signal protocols used now are H.323 and SIP [1], and the protocol used to data transfer is Real-time Transport Protocol.

The major components of a VoIP network are very similar in functionality to that of a circuit-switched network. VoIP networks must perform all of the same tasks that the PSTN does, in addition to performing a gateway function to the existing public network. Although using different technology and approach, some of the same component concepts that make up the PSTN also create VoIP networks. As shown in figure 1, there are three major pieces to a VoIP network.

Media Gateways

Media gateways are responsible for call origination, call detection, analog-to-digital conversion of voice, and creation of voice packets (CODEC functions). In addition, media gateways have optional features, such as voice (analog and/or digital) compression, echo cancellation, silence suppression, and statistics gathering. The media gateway forms the interface that the voice content uses so that it can be transported over the IP network. Media gateways are the sources of bearer traffic. Typically, each conversation (call) is a single IP session transported by a Real-time Transport Protocol (RTP) that runs over UDP. Media gateways exist in several forms. For example, media gateways could be a dedicated telecommunication equipment chassis, or even generic PC running VoIP software.

Media Gateway Controllers

Media gateway controllers house the signaling and control services that coordinate the media gateway functions. Media gateway controllers could be considered similar to that of H.323 gatekeepers. The media gateway controller has the responsibility for some or all of the call signaling coordination, phone number translations, host lookup, resource management, and signaling gateway services to the PSTN (SS7 gateway). The amount of functionality is based on the particular VoIP enabling products used. In a scalable VoIP network, the role of a controller is divided into signaling gateway controller and media gateway controller. For calls that originate and terminate within the domain of the VoIP network, only a media gateway controller might be needed to complete calls. However, a VoIP network is frequently connected to the public network. A signaling gateway controller is used to directly connect to the SS7 network, while also interfacing to the VoIP network elements. This signaling controller would be dedicated to the message translation and signaling needed to bridge the PSTN to the VoIP network.

IP Network

The VoIP network can be viewed as one logical switch. However, this logical switch is a distributed system, rather than that of a single switch entity; the IP backbone provides the connectivity among the distributed elements. Depending on the VoIP protocols used, this system as a whole is sometimes referred to as a softswitch architecture.

Here is how a VoIP transmission is completed:

Step 1: Because all transmissions must be digital, the caller’s voice is digitized. This can be done by the telephone company, by an Internet service provider (ISP), or by a PC.

Step 2: Next using complex algorithms the digital voice is compressed and then separated into packets; and using the Internet protocol, the packets are addressed and sent across the network to be reassembled in the proper order at the destination. Again, this reassembly can be done by a carrier, and ISP, or by one's PC.

Step 3: During transmission on the Internet, packets may be lost or delayed, or errors may damage the packets. Conventional error correction techniques would request retransmission of unusable or lost packets, but if the transmission is a real-time voice communication that technique obviously would not work, so sophisticated error detection and correction systems are used to create sound to fill in the gaps.

Step 4: After the packets arrive at the destination, the transmission is assembled and decompressed to restore the data to an approximation of the original form.

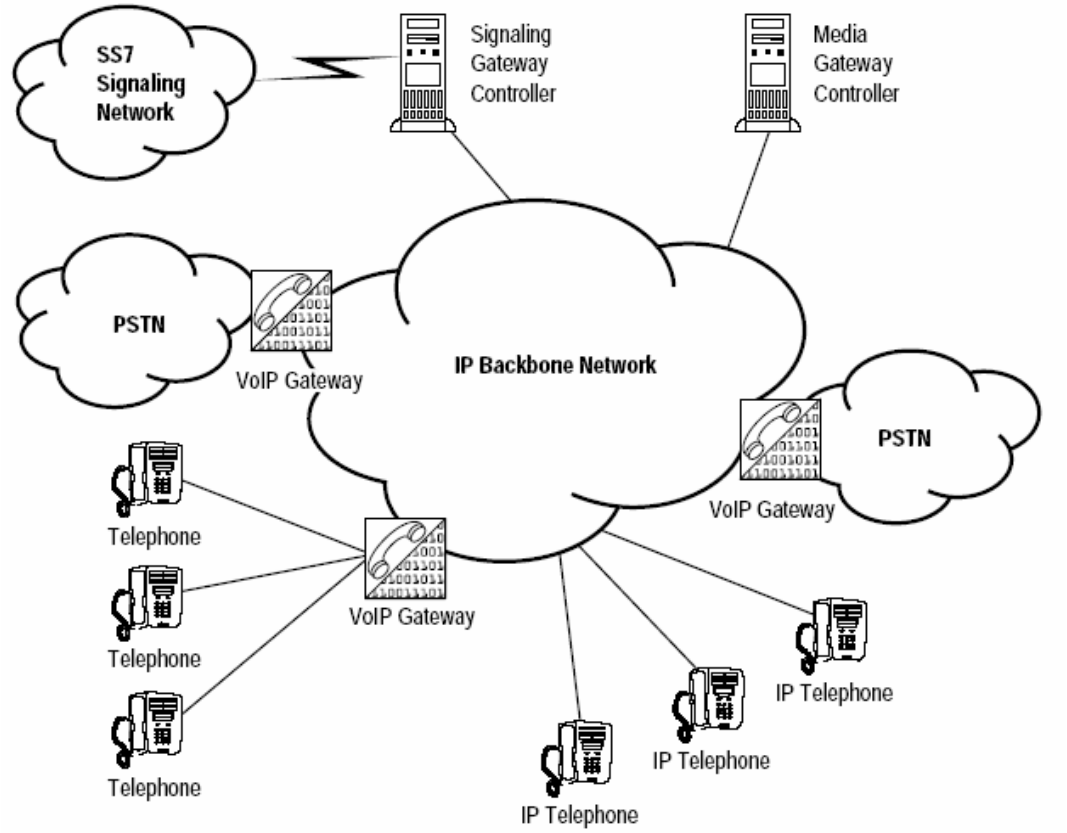

Figure 1. Full Service VoIP Network

3. Skype: A P2P VoIP Service

3.1 What is peer-to-peer

A peer-to-peer (or P2P) computer network is a network that relies on computing power at the edges (ends) of a connection rather than in the network itself. A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server. An important goal in peer-to-peer networks is that the bandwidth of all clients can be used, so the total bandwidth - and usually the available download bandwidth for the average user - grows with the number of nodes, instead of all clients having to share the bandwidth of one server, where adding more clients could mean slower data transfer for all users. There are three generations of peer-to-peer networks: First generation had a centralized file list, like Napster. In the centralized peer to peer model, a user would send a search to the centralized server of what they were looking for, i.e. song, video, movie. The server then sends back a list of which peers have the data and facilitates the connection and download. Second generation, by electing some nodes which had more capacity as indexing nodes, and having

lower capacity nodes branching off from them, allowed for a network which could scale to a much larger size. Also included in the second generation are distributed hash tables, which solve the scalability problem by electing various nodes to index certain hashes (Which are used to identify files), allowing for fast and efficient searching for any instances of a file on the network, though they are with their own drawbacks, such as stale hosts and network splits. Third generation of peer-to-peer networks are those which have anonymity features built in.

3.2 Skype

Skype is a peer-to-peer internet telephony (VoIP) network, founded by Niklas Zennström and Janus Friis, the creators of Kazaa [2]. The network is provided by all combined users of the free desktop software application. Skype users can speak to other Skype users for free, call traditional telephone numbers for a fee (SkypeOut), receive calls from traditional phones (SkypeIn), and receive voicemail.

The main difference between Skype and other VoIP clients is that it operates on a peer-to-peer model rather than the more traditional server-client model. The Skype user directory is entirely decentralized and distributed among the nodes in the network, which means the network can scale very easily to large sizes without a complex and costly centralized infrastructure. Skype also routes calls through other peers on the network, which allows it to traverse NATs and firewalls, unlike most other VoIP programs (notably those based on the SIP protocol). This, however, puts extra burden on those who connect to the Internet without NAT, as their computers and network bandwidth may be used to route the calls of other users. The selection of intermediary computers is fully automatic, with individual users having no option to disable such use of their resources.

Based on reverse engineering of Skype [3] by S. Baset and H. Schulzrinne at Columbia, there are two types of nodes in this overlay network, ordinary hosts and super nodes (SN). An ordinary host is a Skype application that can be used to place voice calls and send text messages. A super node is an ordinary host's end-point on the Skype network. Any node with a public IP address having sufficient CPU, memory, and network bandwidth is a candidate to become a super node. An ordinary host must connect to a super node and must register itself with the Skype login server for a successful login. Although not a Skype node itself, the Skype login server is an important entity in the Skype network. User names and passwords are stored at the login server. User authentication at login is also done at this server. This server also ensures that Skype login names are unique across the Skype name space. Figure2 illustrates the relationship between ordinary hosts, super nodes and login server. Apart from the login server, there is no central server in the Skype network. Online and offline user information is stored and propagated in a decentralized fashion and so are the user search queries.

4. Comparison of different scenarios between Skype and VoIP

In order to demonstrate the differences between Skype and VoIP, six scenarios are chosen to be compared in detail.

4.1 *Login*

In VoIP a client may only have to authenticate its user name and password with login server. While in Skype Login is perhaps the most critical function to the Skype operation. It is during this process a SC authenticates its user name and password with the login server, advertises its presence to other peers and its buddies, determines the type of NAT and firewall, and discovers online Skype nodes with public IP addresses. Below is further study of Skype login process [3].

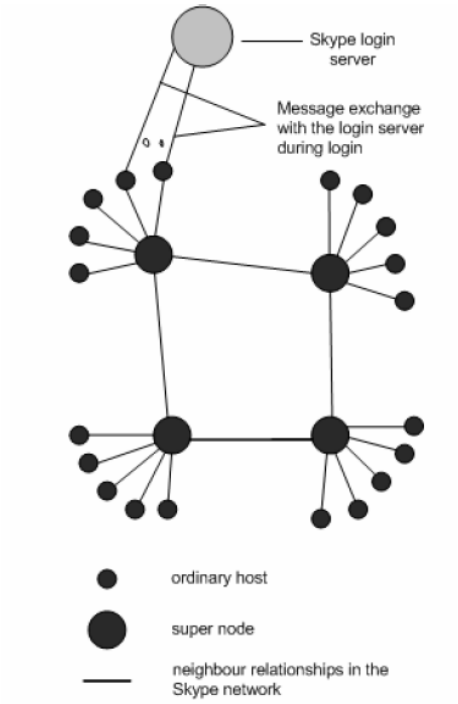

Figure 2. Skype Network. Super nodes, ordinary nodes, and the login server.

Login Process

When SC was run for the first time after installation, it sent a HTTP 1.1 GET request to the Skype server (skype.com). The first line of this request contains the keyword 'installed' .During subsequent startups, a SC only sent a HTTP 1.1 GET request to the Skype server (skype.com) to determine if a new version is available.

The host cache (HC) is a list of super node IP address and port pairs that SC builds and refreshes regularly. The HC must contain a valid entry for a SC to be able to connect to the Skype network. If the HC was filled with only one invalid entry, SC could not connect to the Skype network and reported a login failure. SC first sent a UDP packet to this entry. If there was no response after roughly five seconds, SC tried to establish a TCP connection with this entry. It then tried to establish a TCP connection to the HC IP address and port 80 (HTTP port). If still unsuccessful, it tried to connect to HC IP address and port 443 (HTTPS port). SC then waited for roughly 6 seconds. It repeated the whole process four more times after which it reported a login failure. It is observed that a SC must establish a TCP connection with a SN in order to connect to the Skype network. If it cannot connect to a super node, it will report a login failure. Most firewalls are configured to allow outgoing TCP traffic to port 80 (HTTP port) and port 443 (HTTPS port). A SC behind a firewall, which blocks UDP traffic and permits selective TCP traffic, takes advantage of this fact. At login, it establishes a TCP connection with another Skype node with a public IP address and port 80 or port 443.After a SC is connected to a SN, the SC must authenticate the user name and password with the Skype login server.

NAT and Firewall Determination

SC is able to determine at login if it is behind a NAT and firewall. There are maybe at least two ways in which a SC can determine this information. One possibility is that it can determine this information by exchanging messages with its SN using a variant of the STUN [4] protocol. The other possibility is that during login, a SC sends and possibly receives data from some nodes after it has made a TCP connection with the SN. Once determined, the SC stores this information in the Windows registry. SC also refreshes this information periodically. It is not clear on how often a SC refreshes this information since Skype messages are encrypted.

Alternate Node Table

Skype is a p2p client and p2p networks are very dynamic. SC, therefore, must keep track of online nodes in the Skype network so that it can connect to one of them if its SN becomes unavailable. SC sends UDP packets to 22 distinct nodes at the end of login process and possibly receives a response from them if it is not behind a UDP-restricted firewall. SC uses those messages to advertise its arrival on the network. Upon receiving a response from them, SC builds a table of online nodes. This table is called alternate node table. It is with these nodes a SC can connect to, if its SN becomes unavailable.

4.2 User Search

Usually in SIP caller will search the users by asking the SIP server .In case a callee may keep changing its position with time, these locations can be dynamically registered with the SIP server. When the SIP server is queried about the location of a callee, it returns a list of possible locations. A Location Server in the SIP system actually generates the list and passes it to the SIP server.

Skype uses its Global Index (GI) [4] technology to search for a user. Skype claims that search is distributed and is guaranteed to find a user if it exists and has logged in during the last 72 hours. Due to Skype is not an open protocol and its messages are encrypted, it is not possible to trace Skype messages beyond a SN. Nevertheless, according to Henning Schulzrinne' study [3], below are search message flows for the three different network setups.

For SC on a public IP address, SC sent a TCP packet to its SN. It appears that SN gave SC the IP address and port number of four nodes to query, since after that exchange with SN, SC sent UDP packets to four nodes. If it could not find the user, it informed the SN over TCP. It appears that the SN now asked it to contact eight different nodes, since SC then sent UDP packets to eight different nodes. This process, illustrated in figure 3, continued until the SC found the user or it determined that the user did not exist. On average, SC contacted eight nodes. It is not clear on how SC terminates the search if it is unable to find a user.

A SC behind a port-restricted NAT exchanged data between SN, and some of the nodes which responded to its UDP request during login process. The message flow is shown in Figure 4. 'B' stands for bytes and 'N' stands for node. UDP packets were sent to N1, N2, N3, and N4 during login process and responses were received from them. Message size corresponds to payload size of TCP or UDP packets.

A SC behind a port-restricted NAT and UDP-restricted firewall sent the search request over TCP to its SN. SN then performed the search query and informed SC of the search results. Unlike user search by SC on a public IP address, SC did not contact any other nodes. This suggests SC knew that it was behind a UDP-restricted firewall.

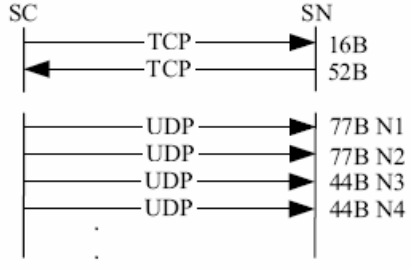

Figure 3. Message flow for user search when SC has a public IP address. 'B' stands for bytes and

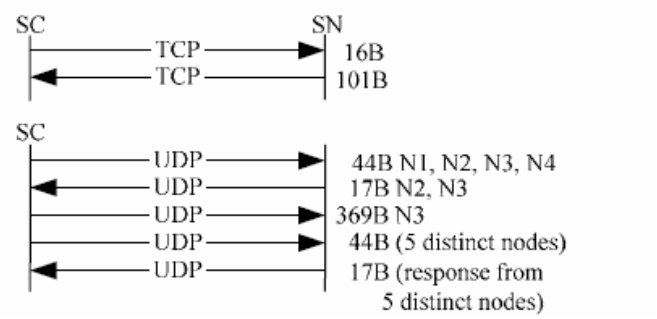

Figure 4. Message flow for user search when SC is behind a port-restricted NAT.

Also the experiment performed by Henning Schulzrinne shows that the SC performs user information caching at intermediate nodes.

A conjecture based on the message flows above is that Skype perhaps use Chord [6]-like hash-based methods, combined with traditional blind searching techniques. SN acts like a search proxy for SC and caches searched results.

4.3 NAT and Firewall

When connecting a PC to the Internet, it is imperative to safeguard the system from hacker attacks and other unwanted accessibility. A firewall protects the PC by rejecting attacks and illegal data packets, allowing only approved traffic. On a local area network (LAN), where several PCs or other equipment is connected, it is common to have private IP addresses on the LAN and a single common public IP address to the Internet. This is called NAT (Network Address Translation) and is often an integrated part of the firewall. Firewalls and NATs are designed for data traffic that is initiated from the inside of the private network. If instead the data traffic is initiated from the outside, and even worse, must reach a specific user on the private network, serious problems will occur.

Normally three workarounds [7] are suggested to solve the Firewall and NAT traversal issues for Voice over IP. The first method is NAT port forwarding, either by manual configuration or via UPnP (Universal Plug and Play) .Second, the STUN protocol enables a client to discover whether it is behind a NAT, and to determine the type of NAT. Third, the ALG (Application Layer Gateway) processes the signaling and media streams so it can modify the signaling to reflect the public IP addresses and ports being used by the signaling and media traffic.

In contrast to traditional approaches, schemes used in Skype are natural and elegant, involving little management structure and overhead. As described in Login process, SC uses a variation of typical schemes such as STUN to determine the type of NAT and firewall it is behind. SC refreshes this information periodically. This information is stored, e.g., in the Windows registry. Then Skype uses a peer relay to connect clients behind NATs or use a TCP tunnel to a peer relay to bypass a UDP blocking firewall.

4.4 Call Establishment and Teardown

Again the process in SIP is used as example here to illustrate the scenario in VoIP. First we should know callers and callees are identified by SIP addresses (URI). Suppose caller is Alice with IP_A and callee is Bob with IP_B under bob@uni-stuttgart.de. If Alice knows Bob is at IP-B, she can directly send a SIP INVITE message to Bob .But, Alice usually does not know IP-B, and she will look it up using bob@uni-stuttgart.de. She does so by sending the INVITE message to her SIP Proxy , which in turn forwards the INVITE message to the SIP

Registrar. The SIP Registrar then forwards the message to Bob's machine. The SIP proxy uses DNS to find the SIP registrar of Bob .The response from Bob traverses the reverse route that the INVITE traversed. After they agree on how they should encode their audio and transport the stream, the connection is established and they can start the conversation.

In the case of Skype, call establishment for the three network setups as described before are considered .It is important to note that call signaling is always carried over TCP. For users that are not present in the buddy list, call placement is equal to user search plus call signaling. Thus, call establishment for the case where callee is in the buddy list of caller is discussed.

If both users are on public IP addresses, online and are in the buddy list of each other, then upon pressing the call button, the caller SC establishes a TCP connection with the callee SC. Signaling information is exchanged over TCP. The initial exchange of messages between caller and callee indicates the existence of a challenge-response mechanism. The caller also sends some messages over UDP to alternate Skype nodes, which are online Skype nodes discovered during login.

In the second network setup, where the caller is behind port restricted NAT and callee is on public IP address, signaling and media traffic do not flow directly between caller and callee. Instead, the caller sends signaling information over TCP to an online Skype node which forwards it to callee over TCP. This online node also routes voice packets from caller to callee over UDP and vice versa.

For the third setup, in which both users are behind port restricted NAT and UDP-restricted firewall, both caller and callee SC exchange signaling information over TCP with another online Skype node. Caller SC sends media over TCP to an online node, which forwards it to callee SC over TCP and vice versa.

During call tear-down, signaling information is exchanged over TCP between caller and callee if they are both on public IP addresses, or between caller, callee and their respective SNs. For the second and third network setups, call tear down signaling is also sent over TCP.

4.5 Media Transfer and Codecs

Media Transfer

H.323 and SIP are only the signaling protocols. Audio data is carried by RTP [8] (Real-time Transport Protocol). The RTP protocol provides features for real-time applications, with the ability to reconstruct timing, loss detection, security, content delivery and identification of encoding schemes. The media gateways that digitize voice use the RTP protocol to deliver the voice (bearer) traffic. For each participant, a particular pair of destination IP addresses defines the session between the two endpoints, which translate into a single RTP session for each phone call in progress.

Again three network setups in Skype are discussed. First, if both Skype clients are on public IP address, then media traffic flows directly between them over UDP. Second, if either caller or callee or both were behind port-restricted NAT, they sent voice traffic to another online Skype node over UDP. That node acted as a media proxy and forwarded the voice traffic from caller to callee and vice versa. At last, if both users are behind port-restricted NAT and UDP-restricted firewall, then caller and callee send and receive voice traffic over TCP from another online Skype node. The Skype protocol seems to prefer the use of UDP for voice transmission as much as possible. The SC will use UDP for voice transmission if it is behind a NAT or firewall that allows UDP packets to flow across.

Codecs

Voice communication is analog, while data networking is digital. The process of converting analog waveforms to digital information is done with a coder-decoder. There are many ways an analog voice signal can be transformed, all of which are governed by various standards. The process of conversion is complex and beyond the scope of this paper. Suffice to say that most of the conversions are base on pulse coded modulation (PCM) or variations. In addition to performing the analog to digital conversion, Codecs compress the data stream, and provide echo cancellation. Compression of the represented waveform can lead to bandwidth savings. Another way to save bandwidth is the use of silence suppression, which is the process of not sending voice packets between the gaps in human conversations.

Global IP Sound [9] provides voice processing software to Skype. Skype automatically selects the best codec depending on the connection. All solutions are designed specifically for use on packet networks:

- No inter-frame dependency
- Multiple description coding
- Variable bit-rate

It should be known that no silence suppression is supported in Skype. Henning Schulzrinne observed that when neither caller nor callee was speaking, voice packets still flowed between them. Transmitting these silence packets has two advantages. First, it maintains the UDP bindings at NAT and second, these packets can be used to play some background noise at the peer. In the case where media traffic flowed over TCP between caller and callee, silence packets were still sent. The purpose is to avoid the drop in TCP congestion window size, which takes some RTT (round-trip time) to reach the maximum level again.

4.6 Security

Security in VoIP

Security, especially in a converged voice and data network, is a high priority. Proper mechanisms are needed to protect the voice communications elements and to prevent unauthorized users and hackers from accessing the network. Basically there are two major solutions for achieving some degree of protection goals: IP security [10] is one solution on network layer that can be applied for securing IP Telephony networks; on higher layers (transport and application layer) , a firewall may provide different security services depending on the layers on which it has functionality: network, transport or application layer.

Security in Skype

Skype is encrypted end-to-end because it uses the public Internet to transport voice calls and text messages and sometimes these calls are routed through other peers. Skype encryption ensures that no other party can eavesdrop on call or read instant messages. As claimed on Skype's homepage, Skype uses AES (Advanced Encryption Standard) to protect sensitive information. Skype uses 256-bit encryption in order to actively encrypt the data in each Skype call or instant message. Skype uses 1024 bit RSA to negotiate symmetric AES keys. User public keys are certified by the Skype server at login using 1536 or 2048-bit RSA certificates.

This scenario is supposed like this: before A wants to send message to B, A sends its certification which is encrypted with Skype server's private key to B first. B can decrypt the certification and read the public key of A. Then A encrypts AES key with its private key and sends it to B. While B knows A's public key, he can read the AES key and use it to transfer messages with A.

5. Conclusion

Skype is a successful combination of several technologies with high potential as it has many advantages compared to traditional VoIP: much better voice quality, ability to traverse the NAT and firewalls, encrypted media channel, ability to scale up to handle large-scale connection-oriented real-time services such as voice, etc. However Skype's achievement is because that on the basis of p2p overlay networks, it makes use of several great technologies and integrates them very skillfully. For instance, Skype possibly uses a variant of the STUN (discuss in part 4.1) to determine the NAT and firewall it is behind.

The p2p networks have a flat architecture, and avoid employing central components. This results to that there are heavy software based DSP operations at Skype clients, including codecs, mixer and fancy echo cancellation. However it will make the person-to-person communication easier, which is the original purpose of the Internet.

Compared to previous p2p networks which focused on content such as file sharing, Skype puts the attention on communications. In this way, Skype has shown, or at least suggested that p2p networks can accomplish the signaling function and P2P overlay networks can handle large-scale connection-oriented real-time voice services.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: session initiation protocol. RFC 3261, IETF, June 2002.

[2] http://www.kazaa.com/us/index.htm

[3] Salman A. Baset and Henning Schulzrinne
An Analysis of the Skype Peer-to-Peer Internet Telephony protocol. cs.NI/0412017, arXiv, 5 Dec 2004

[4] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). RFC 3489, IETF, Mar. 2003.

[5] Global Index (GI): http://www.skype.com/skype_p2pexplained.html

[6] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In Proc. ACM SIGCOMM (San Diego, 2001).

[7] Rosenberg, Mahy, Sen, NAT and Firewall Scenarios and Solutions for SIP.
draft-rosenberg-sipping-nat-scenarios-00, IETF Draft, November14, 2001.

[8] Rakesh Arora, Voice over IP : Protocols and Standards. Student reports, CSE of Ohio-state University. November, 1999. http://www.cse.ohio-state.edu/~jain/cis788-99/voip_protocols/

[9] Global IP Sound. http://www.globalipsound.com/partners/

[10] Andon Batchvarov , Security Issues and Solutions for Voice over IP compared to Circuit Switched Networks. Seminar Advanced Communication Services (ACS), 2004 , University of Stuttgart

[11] Skype FAQ. http://www.skype.com/help_faq.html

[12] Lecture slides: Computer Networks by Professor H. T. Kung, Harvard University
http://www.eecs.harvard.edu/cs143

[13] Solving the Firewall and NAT Traversal Issues for Multimedia Services over IP.
Newport Networks Systems Inc. www.newport-networks.com/cust-docs/910033-nat-wp.pdf

[14] White Paper: Voice over IP Solutions by Juniper Networks, Inc.
www.juniper.net/solutions/ literature/white_papers/200011.pdf

[15] Cisco − VoIP Traversal of NAT and Firewall, Cisco Systems, Inc.
voip-itec.tamu.edu/files/reference/voip-nat.pdf