A REPORT

ON

APPLICATION ARCHITECTURE OF

SUBMITTED TOWARDS THE PARTIAL FULFILLMENT OFINTERNAL

EVALUATION OF SOFTWARE ARCHITECTURE COURSE

BY

Name	PRN
Divya Srinivasan	11030241153
Pooja H. Sheth	11030241163
Priyanka Mangal	11030241167
Victory Abraham	11030241186

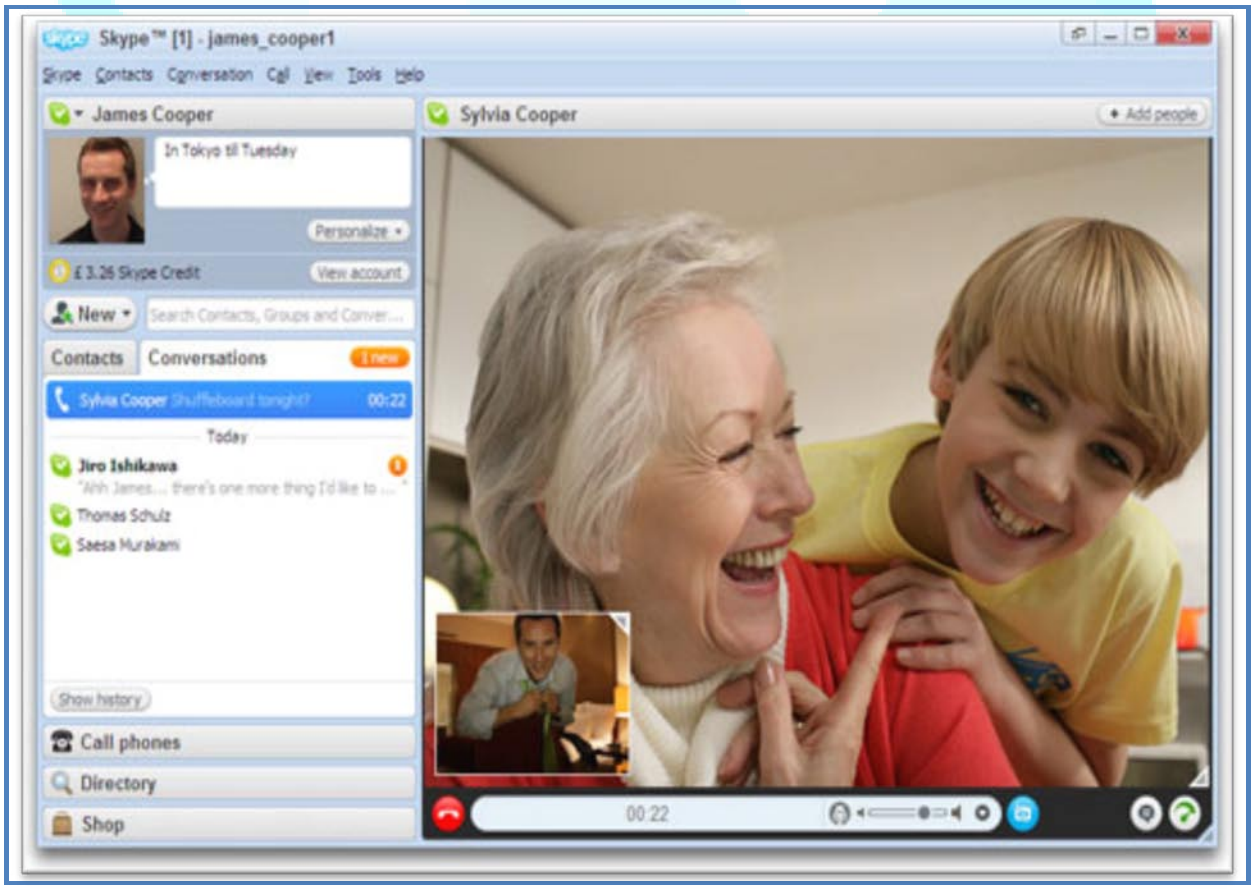
Table of Contents

1. Introduction

Skype is an application that turns a personal computer into a telephone. Skype uses voice over Internet protocol (VoIP) technology, which converts voice signals into data streams that are sent over the Internet and converted back to audio by the recipient's computer.

Although Skype is not the only company that offers VoIP services for consumers, it functions on a P2P (Peer to Peer) model rather than as a centralized application. With the P2P model, users download a piece of software that allows computers to communicate directly with one another, without having to be routed through a central location.

This decentralized model allows Skype to function as a robust, distributed medium for communication. The service allows communication between Skype-equipped devices, which is free, or between a Skype device and a conventional telephone for relatively modest fees. Skype offers features such as voicemail and call forwarding, and the service also now supports video communication.



2. About the Application

Skype was developed by the Danish entrepreneurs behind the KaZaA peer-to-peer file sharing network, and appears to have substantial code in common with the clients and servers developed for that project.

Since Skype was launched in August 2003 it has largely dominated the free Internet telephony application space. Some of the key milestones in Skype's business development are shown on the slide opposite.

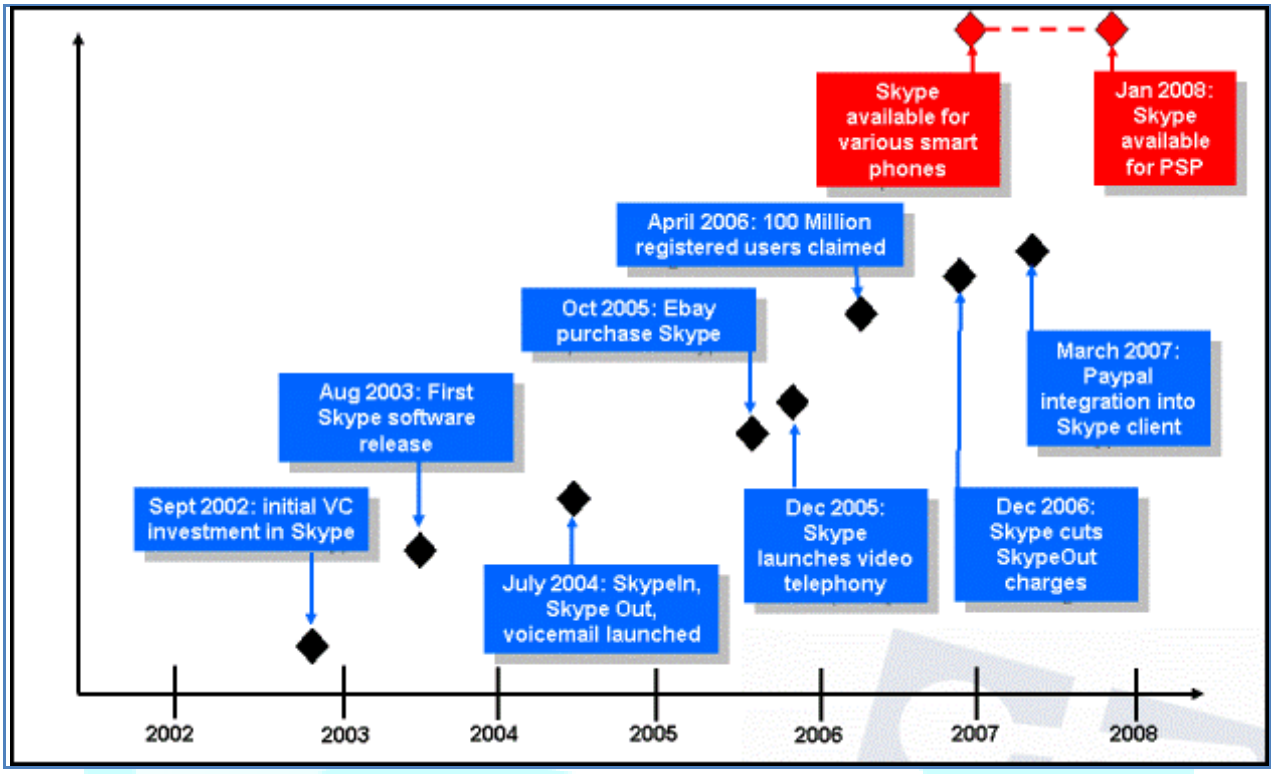
As of January 2008, Skype claim 276 million users accounts. Many of these can be expected to be inactive, and typically users may have more than one account on this (free) service. Annualized revenues of $382 million for 2007 have been reported.

Skype is an instant messaging application, based on the P2P technology. It is estimated that nowadays this program is used by over 200 million users. The popularity of this application is strictly connected with the multitude of possibilities offered by it, as well as the support of some websites, cooperating with this project. In 2005 eBay took over Skype, which resulted in the dynamic and extensive development of this application in the following few years. Although in the recent years appeared many new instant messaging applications, none of them were able to outclass Skype, and only few were able to get close to its level.

The major functions of Skype application are as follows:

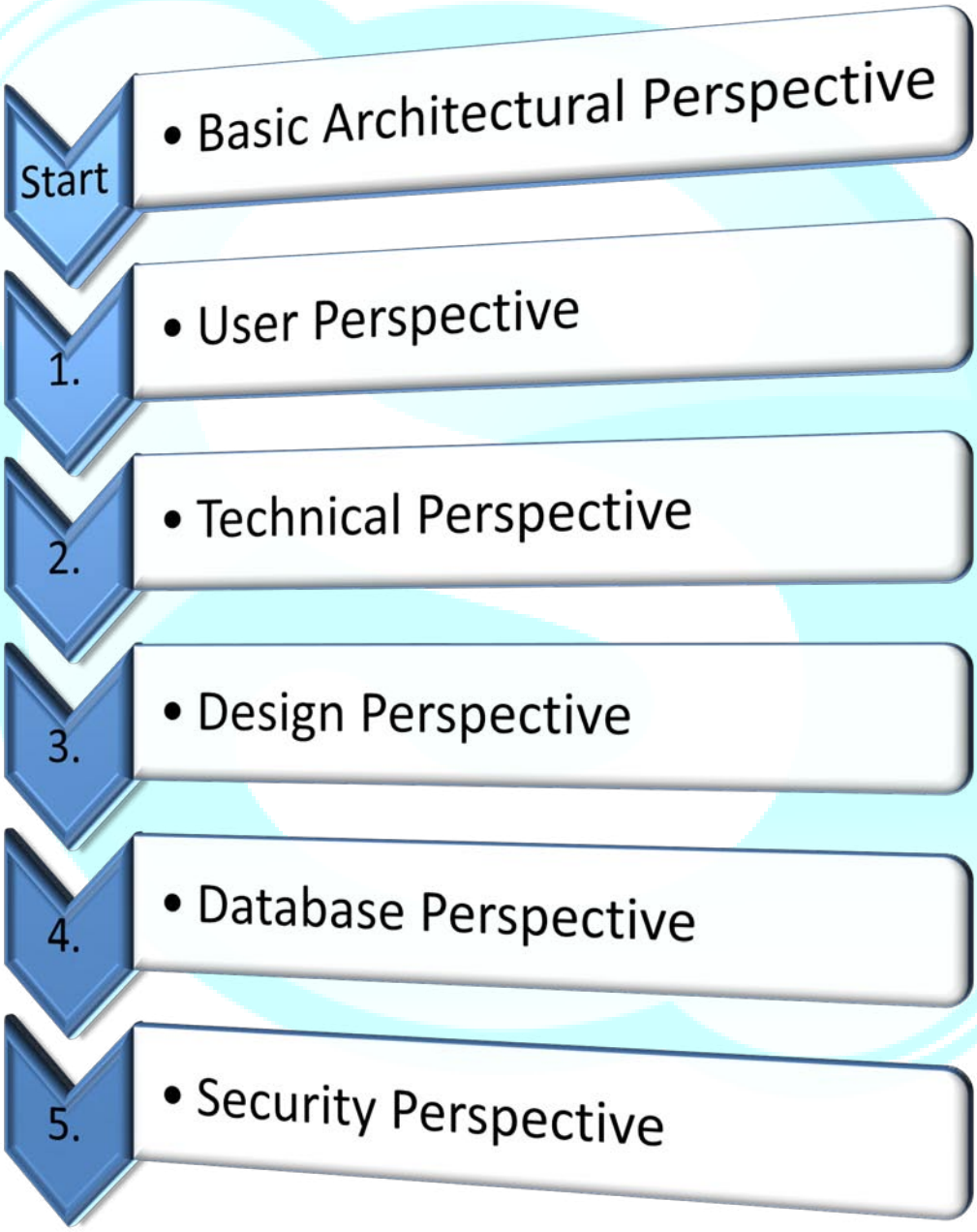
- The main function of this application is a free voice communication between two or more connected users.
- For that, we do not need a super fast Internet connection.
- Additionally, with the use of Skype we can make phone calls to some of the mobile phone and landline networks. However, this function is payable. The phone calls are possible thanks to the Voice over Internet Protocol (VoIP) technology.
- Additionally, we can communicate with other users via the traditional text chat.
- Another important option is the possibility to hold a voice- and videoconferences. The help system and the connection and hardware configuration wizards make this application easy and friendly to even the beginning users. It is also possible to exchange files between users on the contact list.
- Skype is available for Windows operating systems, but not only. Skype 2.0 is also meant for Linux. The only drawback of the Linux version is that the source code of the application is not available, so users cannot develop this application on their own.

An overview of the evolution of Skype



Skype Development

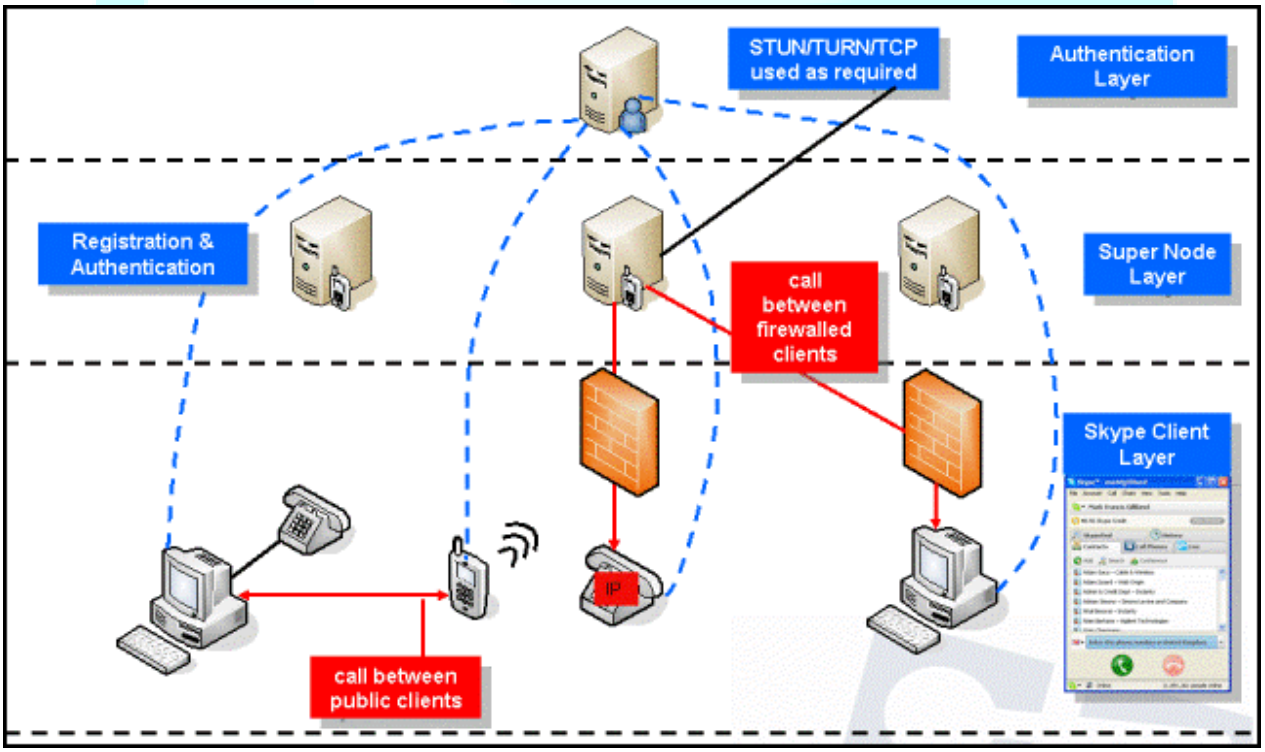
We will be covering the following architectural perspectives along with the basic architectural perspective:



Basic Architecture Perspective:

The Skype architecture includes a central registration server to which all clients register. Unlike most other similar applications and VoIP systems generally, Skype operates on a peer-to-peer, rather than a client-server model, and so buddy lists are managed locally on each machine, and calls are routed via transit nodes only if necessary to circumvent firewalls and NAP/NAPT.

The Skype network consists of conventional nodes and Supernodes, which are themselves Skype endpoints, as well as providing signalling and media proxy services to conventional nodes. Skype applications are provided with a basic set of Supernode addresses when they first register, and maintain a cache of these and additional Supernodes long-term. In common with other VoIP applications, the Skype applications can be adversely affected by firewalls and NAT/NAPT devices.



3. Perspective 1: User

Registered users of Skype are identified by a unique Skype Name, and may be listed in the Skype directory Skype allows these registered users to communicate through both instant messaging and voice chat. Voice chat allows telephone calls between pairs of users and conference calling, and uses a proprietary audio codec. Skype's text chat client allows group chats, emoticons, storing chat history and editing of previous messages. Offline messages were implemented in version 5, but removed after a few weeks without notification. The usual features familiar to instant messaging users — user profiles, online status indicators, and so on — are also included.

3.1 Description:

The Online Number, a.k.a. SkypeIn, service allows Skype users to receive calls on their computers dialed by conventional phone subscribers to a local Skype phone number; local numbers are available for Australia, Belgium, Chile, Colombia, Denmark, the Dominican Republic, Estonia, Finland, France, Germany, Hong Kong, Hungary, Ireland, Italy, Japan, Mexico, New Zealand, Poland, Romania, South Africa, South Korea, Sweden, Switzerland, Turkey, the Netherlands, the United Kingdom, and the United States. A Skype user can have local numbers in any of these countries, with calls to the number charged at the same rate as calls to fixed lines in the country.

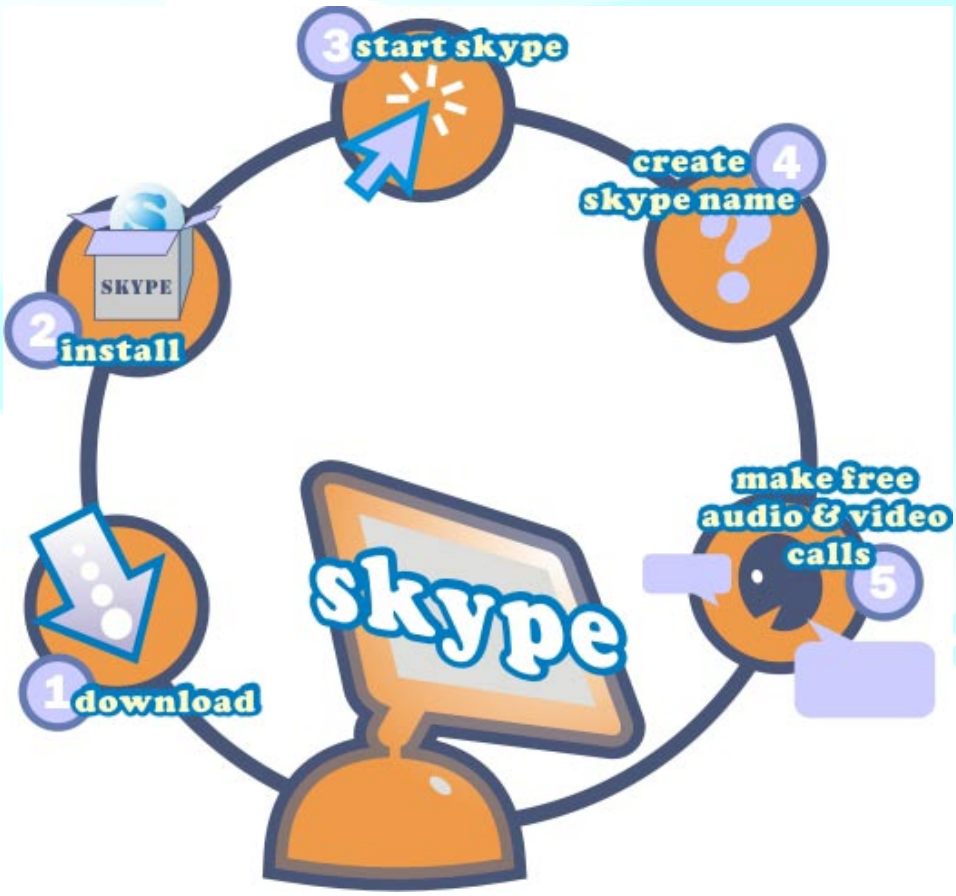
Skype requirements for Windows:

- PC running Windows 2000, XP or Vista. (Windows 2000 users require DirectX 9.0 for video calls).
- Internet connection (broadband is best).
- Speakers and microphone built-in or separate.
- For voice and video calls we recommend a computer with at least a 1GHz processor, 256 MB RAM and of course a webcam.
- For High Quality Video calls you will need a high quality video webcam and software, a dual processor computer and a fast broadband connection (384 kbps).

Skype requirements for Macintosh:

- Mac computer with G4 800 Mhz processor or faster.
- Mac OS X v10.3.9 Panther or later.
- For higher-resolution video a faster processor (Core 2 Duo) and a broadband connection with at least 384kbps upload speeds.
- 512 MB RAM.
- 40 MB free disk space on your hard drive.
- Microphone and speakers or headset.
- Latest drivers for your webcam, for video.
- Internet connection (broadband is best).

3.2 Diagram showing the elements and their relationships



3.3 Elements with their externally observable characteristics

3.3.1 Presence Information

Skype also provides presence information in a very practical way. Presence is the availability and willingness of a person to communicate. For instance, if you find a buddy online ready to communicate, then there is presence. Skype allows you to know, if a buddy is offline, when she is willing to communicate, so you can log back in at that time.

3.3.2 High Quality

People use Skype mainly for the high quality of voice it offers and especially because it offers free PC to PC service. People around the world use Skype for several things: for long-distance mettings with family, friends and loved ones; for remote activity monitoring; for business calls; for long-distance conferences; for cheap calls during travel etc.

3.3.3 Ease of Use

Skype is used in nearly all countries of the world, as it has been developed in view of delivering clear and consistent calls over the Internet. Today, there are many Skype user groups around the world. The largest groups are found in Europe, North America and South East Asia.

3.3.4 Calling

Free Video Calling:

Why just talk when you can see each other face-to-face? Video call your family in Australia, your friends in Spain or your colleagues in Japan, for free. It's the next best thing to being there.Call people all over the world on their phone or mobile from just 0.9c per minute (1c incl. VAT)* using Skype.

Free Skype Calls:

Talk to anyone else on Skype, anywhere in the world, for free with a Skype-to-Skype call. Catch up with your backpacking brother in Asia, check in with your boss away in the US – call any Skype contact for free.

Group Video Calling:

Catch up face-to-face with more people at the same time on a group video call with Skype. Whether you're kicking off a project or showing off the latest addition to the family, it's the next best thing to being there.

Conference Calls:

Talk to more than one person at once. It's free if you're all on Skype.

Voicemail:

Let Skype take a message when you're not free to talk.

Send Files:

Send documents, video clips or photos – any size for free.

Caller ID:

Show it's you when you call a phone number from Skype.

Skype WiFi:

Get online with public WiFi using Skype Credit so you only pay for what you use.

Screen sharing:

Show presentations, photos and more over a Skype call.

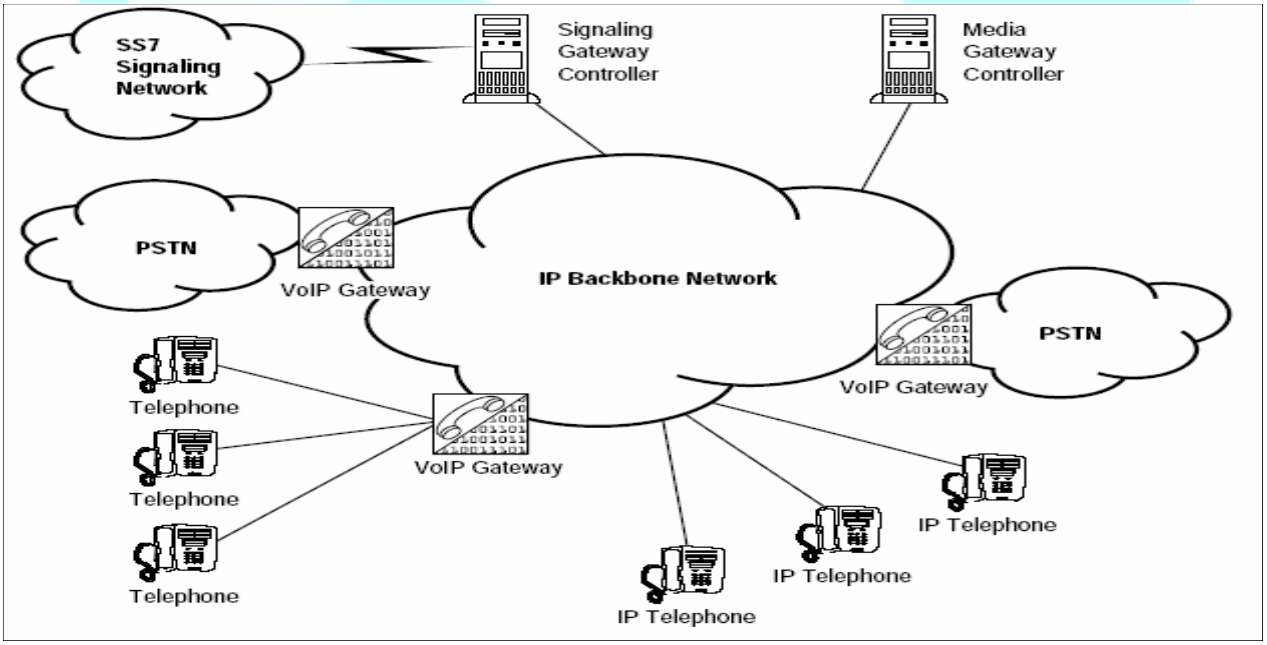
4. Perspective 2: Technical

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.

4.1 Description

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. 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.

4.2 Diagram showing the elements and their relationships



Full Service VoIP Network

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.

4.3 Elements with their externally observable characteristics

4.3.1 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.

4.3.2. 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.

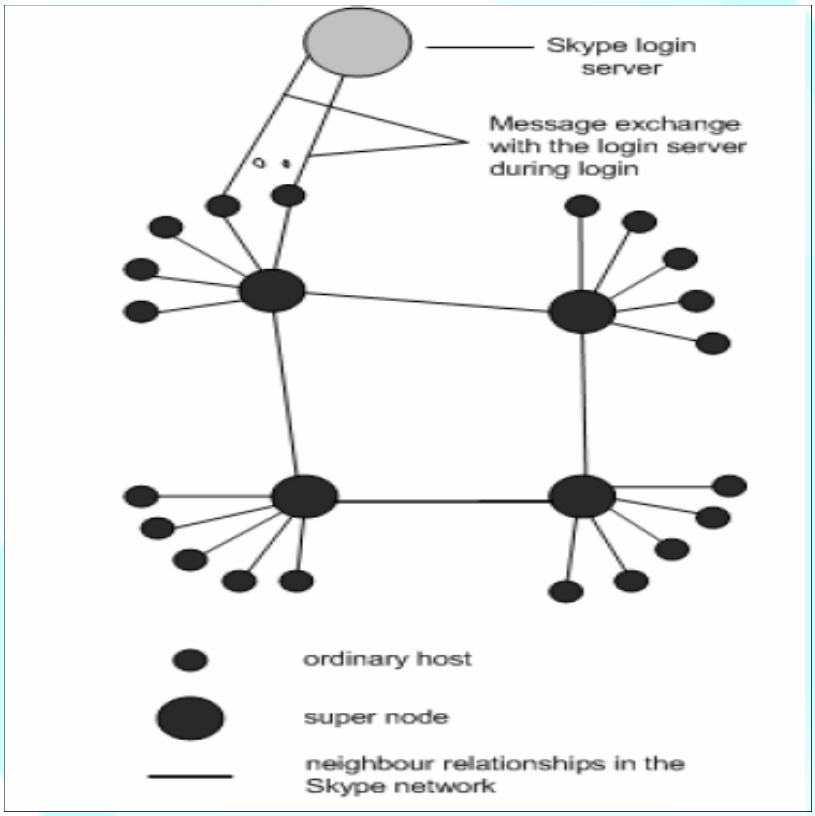
Here is how a VoIP transmission is completed:

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.



Skype Network-Super nodes, ordinary nodes, and the login server.

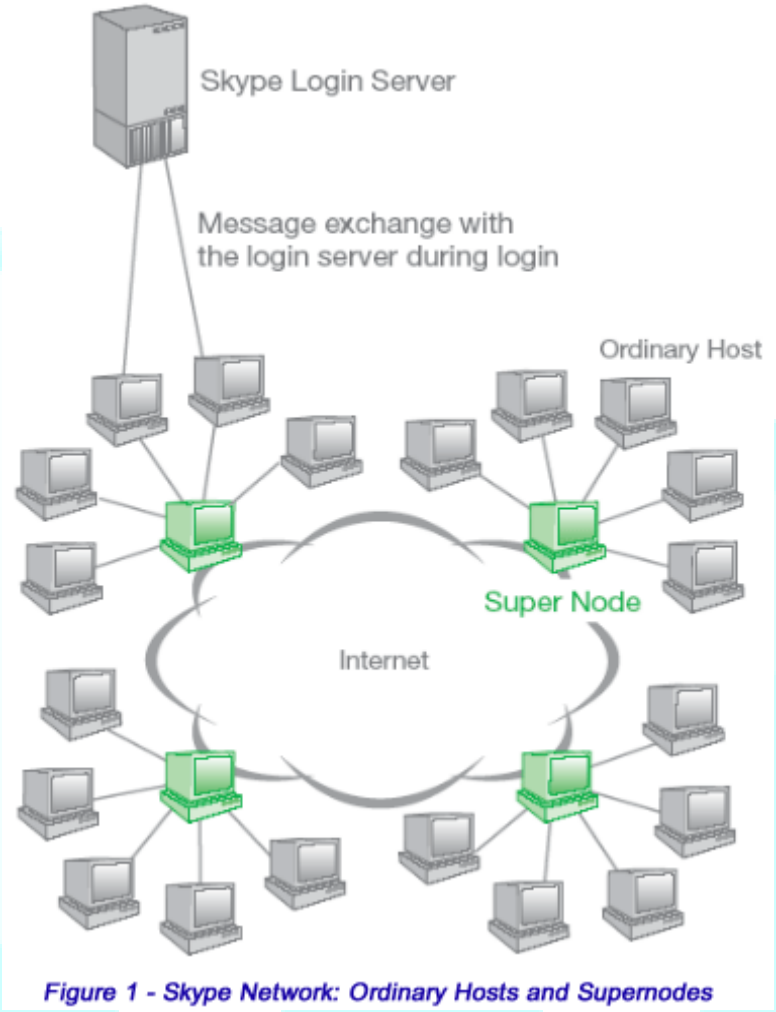


Figure 1 - Skype Network: Ordinary Hosts and Supernodes

4.3.3. 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.

4.3.4. 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.

4.3.5. 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. This table is called alternate node table. It is with these nodes a SC can connect to, if its SN becomes unavailable.

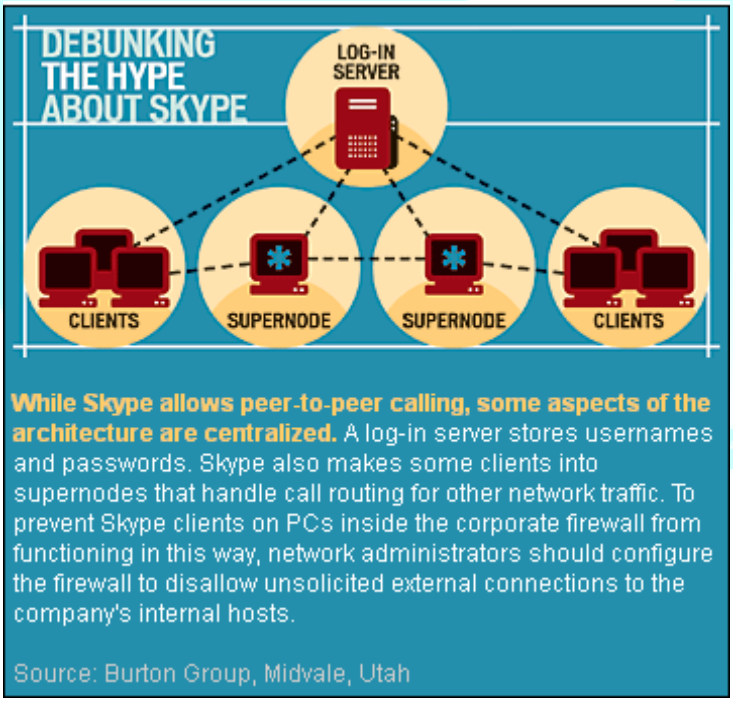
5. Perspective 3: Design

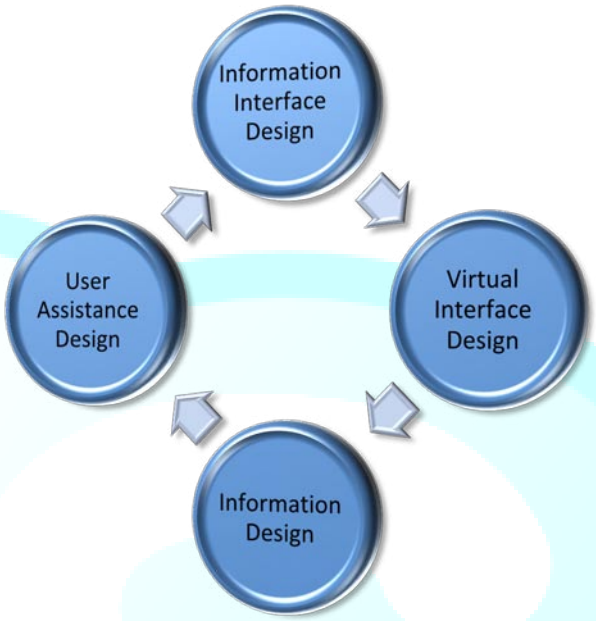
5.1.Description

Since interaction design for Skype plays such a central role in the design of application user experiences, there is much that it encompasses. Good interaction design for Skype will

- effectively communicates the scope and nature of an application's functionality through its primary contexts for interaction, as well as its menus or navigation system
- defines and clearly presents both simple and complex workflows and, thus, facilitates users' tasks
- provides easily discernible opportunities for interactivity through visible affordances, or interactive elements
- defines user interactions that are consistent with best practices or highly intuitable—and, thus, easy to learn—and easy to use
- specifies behaviors that clearly communicate an application's responses to user interactions
- informs users about system state changes
- actively prevents user errors

5.2. Diagram showing the elements with their relationships:





5.3.Elements with their externally observable characteristics

Although information interface design, visual interface design, information design, and user assistance design are also essential aspects of user experience design for skype , all serve supporting roles in the design of applications—that is, they are the means by which designers facilitate interactions, as follows:

5.3.1. Information interface design

An application's information architecture defines its overall structure, with the goal of supporting findability and usability; provides the basis for the application's menus or navigation system; verbally communicates the application's structure through the labeling of its menus or navigation system; and ensures users can easily navigate to related functionality and information from their current context.

5.3.2. Visual interface design

An application's visual interface design visually expresses its hierarchies, groupings, workflows, and affordances—thus, showing users how to interact with the application through effective visual communication; provides iconic representations of the application's objects and actions;

and ensures its user interface is both aesthetically pleasing and accessible to people with color-deficient or low vision.

5.3.3. Information design

An application's information design visually expresses the information the application provides to users—often through charts, graphs, information visualizations, and tabular reports. Another role for an application's information design is to clearly communicate what information users need to provide to accomplish their tasks—typically, by filling out Web forms or editing options in dialog boxes.

5.3.4. User assistance design

An application's user assistance design verbally communicates how users can interact with it—telling users both what to do and how to do it. Interactive user assistance communicates what users should do next when filling out forms. More traditional Help systems should communicate the concepts users must understand to use an application effectively, as well as provide step-by-step instructions for specific tasks.

In application design, the designers who are responsible for information architecture, visual interface design, information design, and user assistance design may be either different people who are specialists in particular aspects of UX design or UX designers who are capable of fulfilling all of these roles.

An application's primary context for interaction should effectively communicate the scope and nature of its functionality—that is, what type of application it is. The virtual contexts that would be most appropriate for an application you're designing depend primarily on the application's type—and to some extent, on the platform for which you're designing it. An application's purpose, features, and the nature of its user experience determine its type, while its overall structure and characteristic frameworks, patterns, affordances, and behaviors express its type. Each virtual context comprises a single screen, Web page, or window. The platform on which an application runs and the size and resolution of its display—otherwise known as an application's form factor—constrain the screen real estate that is available for each of an application's virtual contexts.

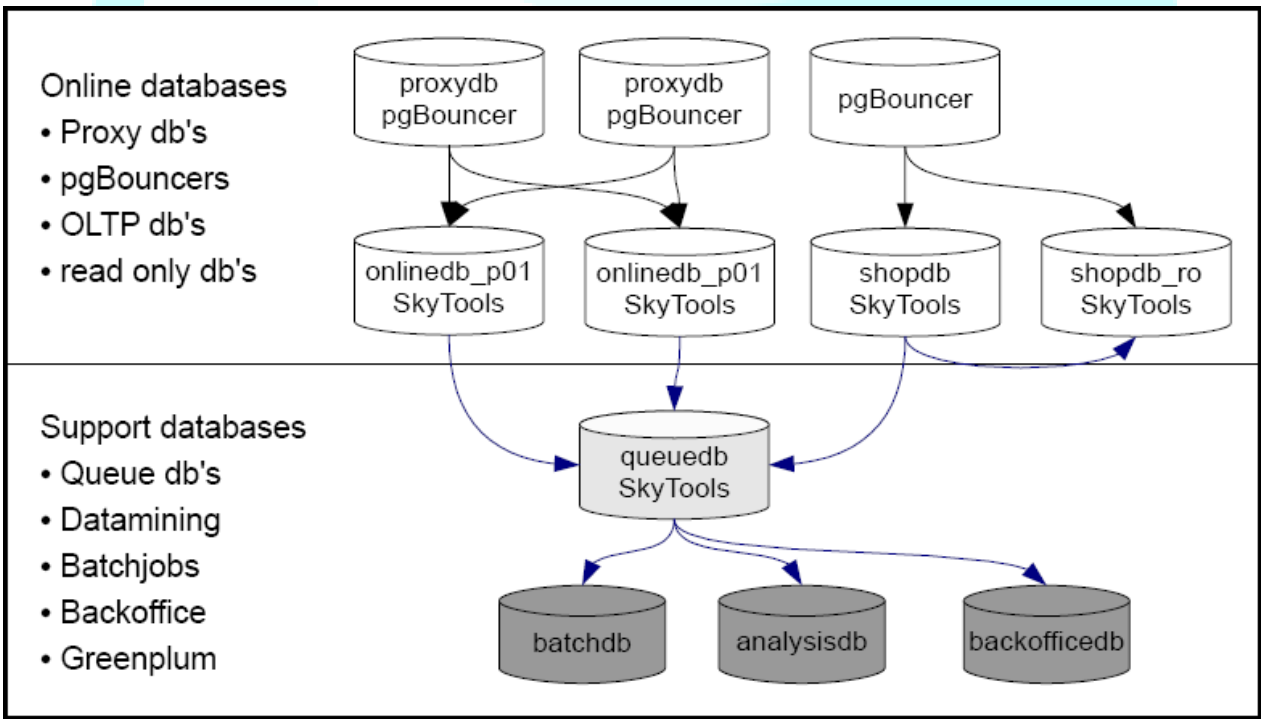
6. Perspective 4: Database Perspective

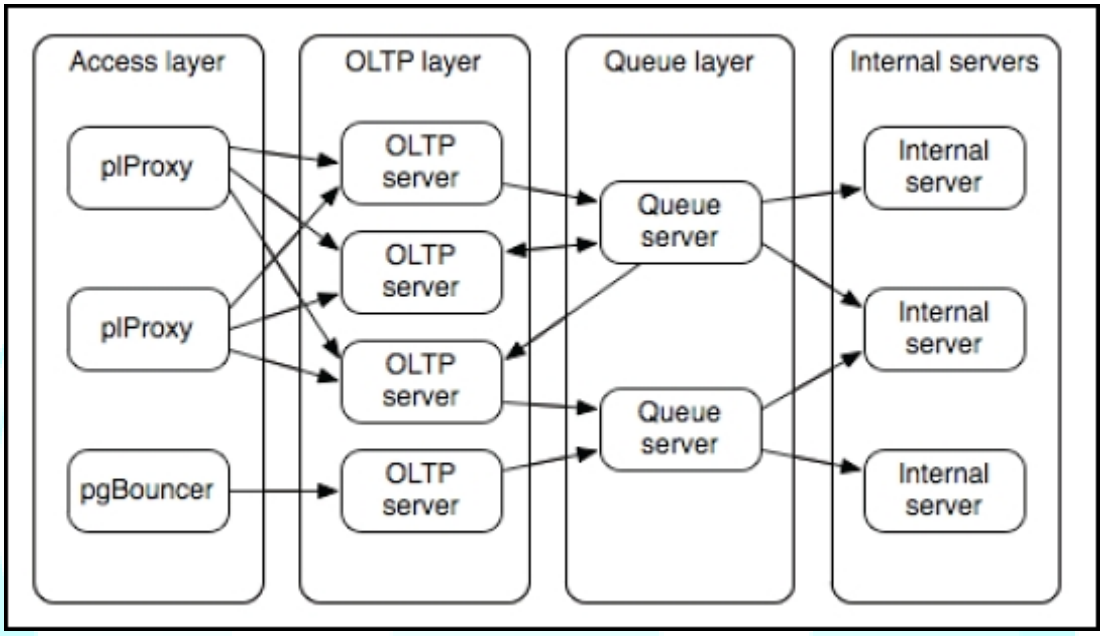
Skype is Communications Company that provides calling and chatting services over internet. Thanks to the fact that a lot of activity goes on in p2p network not everything that user does hits databases.

6.1.Description:

Skype has used PostgreSQL from the beginning for all the OLTP databases. It consists of 100 database servers and 200 databases. The largest OLTP table has several billions of records and the database can handle over 10,000 transactions per second. These databases are used mainly for web store, billing and other centrally provided services. All the access to the database happen through stored procedures.

6.2. Diagram showing the elements and their relationships:



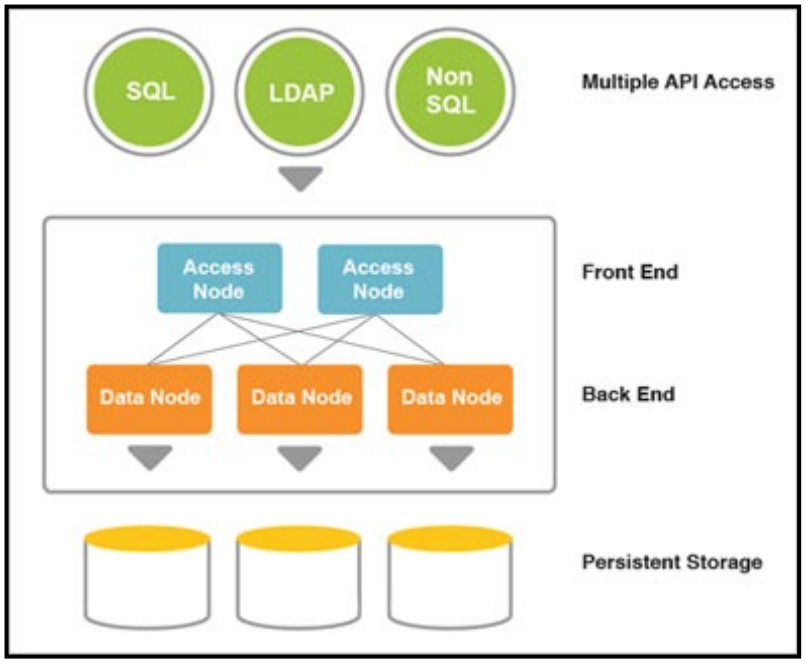


Layers of Databases

The figure above explains how Skype has used these tools to set up Skype database architecture.

It consists of four layers

- Access Layer that provides access to the databases either handling database partitioning (plProxy) or connection pooling (pgBouncer). Is also used for providing transparency for developers
- OLTP Layer where the OLTP databases live
- Queue layer that is responsible for transporting and replicating data between databases within the layers
- Internal servers layer that contains databases for logging, statistics, monitoring, batch processing and ETL purposes

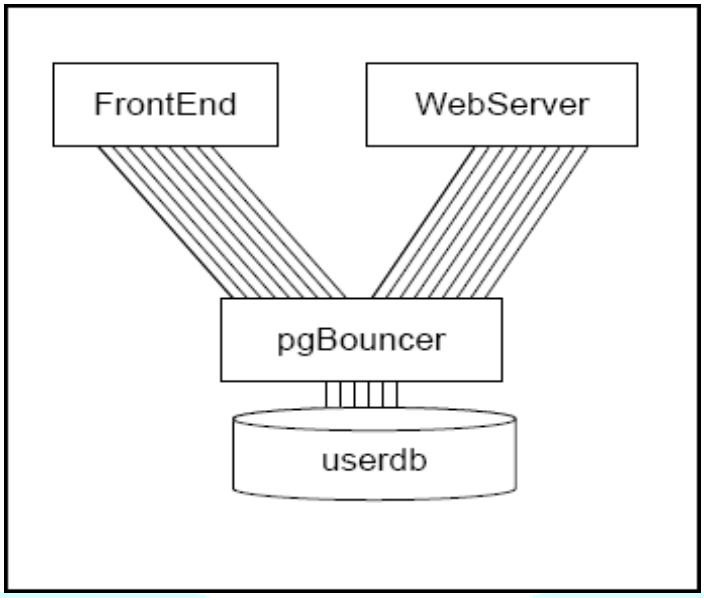

SQL
LDAP
Non SQL
Multiple API Access
Access Node
Access Node
Front End
Data Node
Data Node
Data Node
Back End
Persistent Storage

6.3.Elements with their externally observable characteristics:

There are basically various elements that interact and display various characteristics. These include the ones implicitly present in the architecture as well as the ones explicitly mentioned.

6.3.1. pgBouncer – PostgreSQL Connection pooler

- pgBouncer is lightweight and robust connection pooler for PostgreSQL.
- It reduces thousands of incoming connections to only tens of connections in database.
- Low number of connections is important because each connection uses computer resources and each new connection is quite expensive as prepared plans have to be created each time from scratch.
- We are not using pgBouncer for load balancing.
- Can be used to redirect database calls (database aliases)



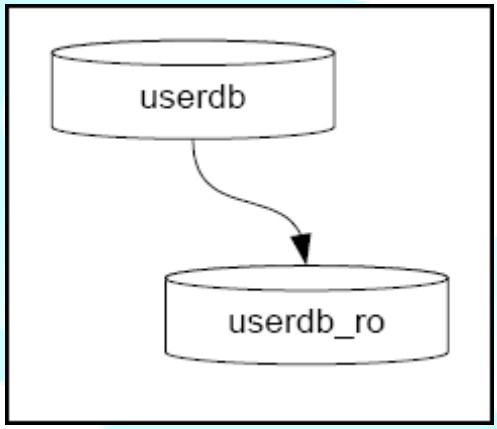
6.3.2. plProxy: Remote Call Language

- PL/Proxy is compact language for remote calls between PostgreSQL databases.
- With PL/Proxy user can create proxy functions that have same signature as remote functions to be called. The function body describes how the remote connection should be acquired.
- plProxy adds very little overhead when used together with pgBouncer.
- On the other hand plProxy adds complexity to development and maintenance so it must be used with care but that is true for most everything.

```
CREATE FUNCTION get_user_email(username text) RETURNS text AS $$
        CONNECT 'dbname=shopdb_ro';
$$ LANGUAGE plproxy;
```

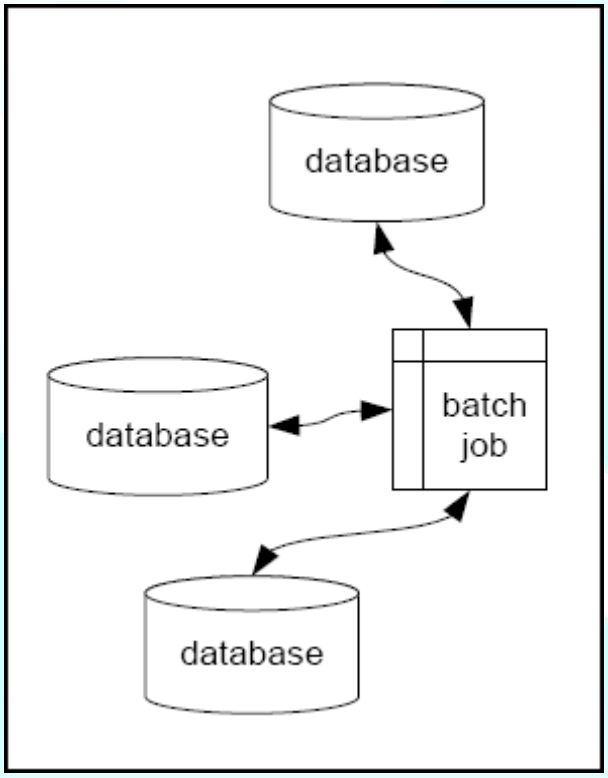
6.3.3. plProxy: Horizontal Partitioning

- We have partitioned most of our database by username using PostgreSQL hashtext function to get equal distribution between partitions.
- When splitting databases we usually prepare new partitions in other servers and then switch all traffic at once to keep our life simple.
- As proxy databases are stateless we can have several exact duplicates for load balancing and high availability.



6.3.4. SkyTools: Package of Database Tools

- Contain most everything we have found useful in our everyday work with databases and PostgreSQL.
- PgQ that adds event queues to PostgreSQL.
- Londiste replication.
- Walmgr for wal based log shipping.
- DBScript framework which provide database connectivity, logging, stats management, encoding, decoding etc for batch jobs. Developers need only to take care of business logic in batch jobs all the rest is handled by batch jobs.
- SkyTools contains tens of reusable generic scripts for doing various data related tasks.



7. Perspective 5: Security Perspective

Skype is the only Internet voice application provider that currently employs strong encryption to protect network traffic. This is because Skype's tight security model is integrally linked to its underlying P2P network architecture. The fact that Skype network traffic is routed through supernodes and may be routed through relay hosts (computers and devices that are not party to a call, IM, or file transfer) means that all Skype network traffic must be automatically encrypted end-to-end to ensure privacy.

As a result, Skype's **network traffic cannot be intercepted and decoded while in transit.** That being said, even though Skype offers a private communication channel, it still runs on mass-market operating systems.
This means that even though Skype network traffic cannot be intercepted and decoded while in transit, when Skype traffic is decrypted on computers that are party to a call, IM, or file transfer, data such as chat logs, and voicemail messages may be vulnerable.

7.1.Description:

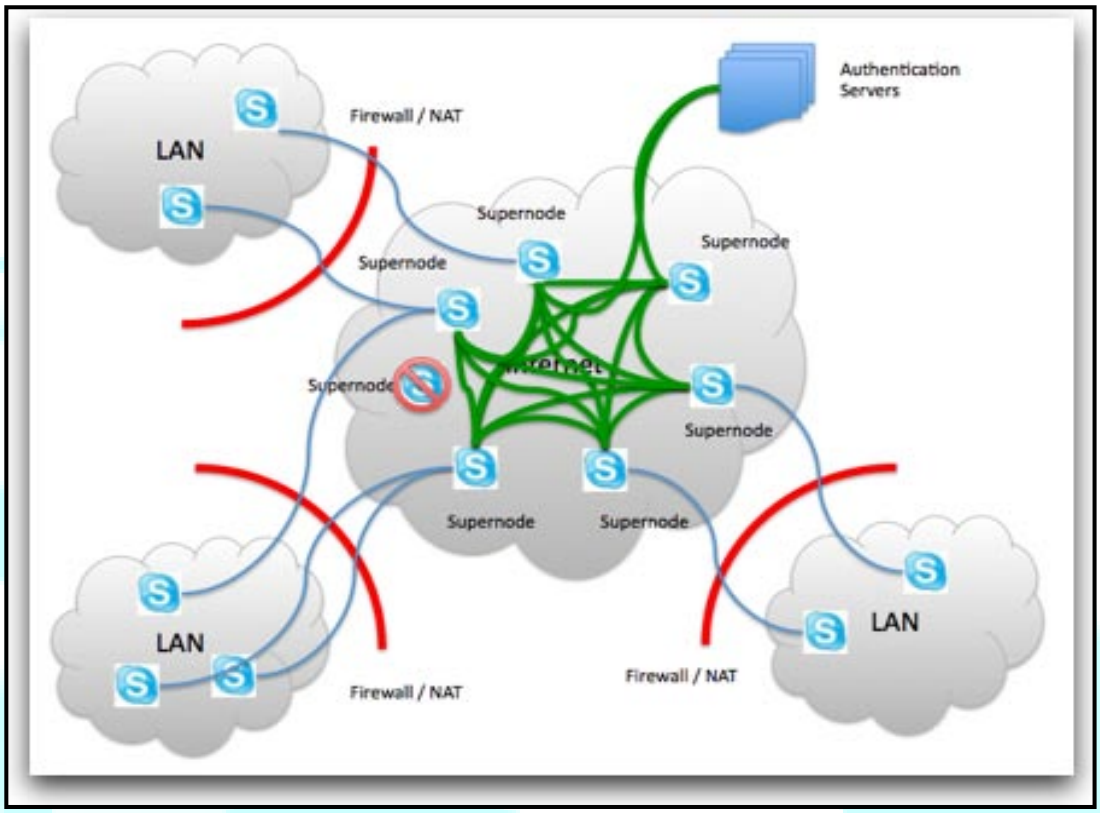
In the context of the security provided by operating system(s) on which the Skype client is installed and running, Skype provides operational level of security or privacy. Therefore, Skype neither provides a secure computing platform in the strictest definition, nor does it offer a secure file storage solution.

By secure computing platform, we mean a computing platform that meets technical criteria about how information is transmitted, received, handled, and stored such that high-value or high-risk transactions can be handled securely.

Skype utilizes a security model that effectively prevents anyone who may have access to a supernode or relay host from interfering with or capturing any part of a Skype communication, even if they are able to collect or sniff network data packets. It also prevents anybody (especially those you consider to be a competitive threat) from installing a computer on the Internet in the theoretical path of incoming and outgoing Skype traffic for the purpose of eavesdropping.

The bottom line is this; although Skype cannot guarantee complete anonymity or secrecy, it does provide transport-layer security to ensure that message content traveling over the Skype network cannot be tapped or intercepted. Skype network traffic and message content will not end up at unauthorized destinations.

7.2. Diagram showing the elements and their relationships:



7.3.Elements with their externally observable characteristics

Skype's security model utilizes a public-key cryptography with signed digital credentials. This enables Skype to validate each user's authenticity. It also reduces the demand for centralized infrastructure.

7.3.1. Skype User Authentication

With public-key/private-key cryptography, one of the keys is made "public" enabling unrestricted distribution. However, the other key remains secret. The two keys are independent but related. Neither of the keys can be used to predict what the other key is. Both keys are needed to complete the handshake that allows a given communication session to complete.

When a Skype user logs in using a Skype name and password, the user's Skype client attempts to connect to a centralized resource; that is, the Skype authentication server. If and when the authentication server validates the connection, it gives the user's Skype client a signed digital credential—signed using a private key which is maintained by Skype Technologies S.A.

The public key required to verify another Skype user's digital credential is maintained in each Skype client. Signed digital credentials are valid for only a limited period of time. In addition, Skype Technologies S.A., periodically renews them to further enhance security.

At the point when a Skype client gets a signed digital credential and can validate its authenticity, the Skype client may (on behalf of a Skype user) present it to other Skype clients. When the authentication process is complete, there is no reason for the recipient to re-verify the authenticity of the caller's credential by checking in with the authentication server or any other piece of centralized infrastructure.

7.3.2. Encryption Handling

Skype relies on a system of public and private keys to ensure the contents of communication are confidential. As stated earlier, all Skype network traffic is encrypted to ensure privacy. This includes all signals used to control the Skype network, as well as communications content; specifically, voice video, text, and data.

The use of strong encryption here means that it is not possible to know what information is traveling in the Skype network among nodes, supernodes, or relay hosts. The cryptographic model behind Skype employs both public-key and symmetric-key cryptography, including the AES algorithm, used in 256- bit integer counter mode. Skype also uses 1,024-bit RSA to negotiate symmetric AES keys. User public keys are certified by the Skype server at login, using 1,536- or 2,048-bit RSA certificates.

At the moment the Skype clients establish a connection (but before an actual voice or video call, text chat, or file transfer begins), each Skype client involved in the session presents digital credential and must agree on an Advanced Encryption Standard (AES) encryption key.

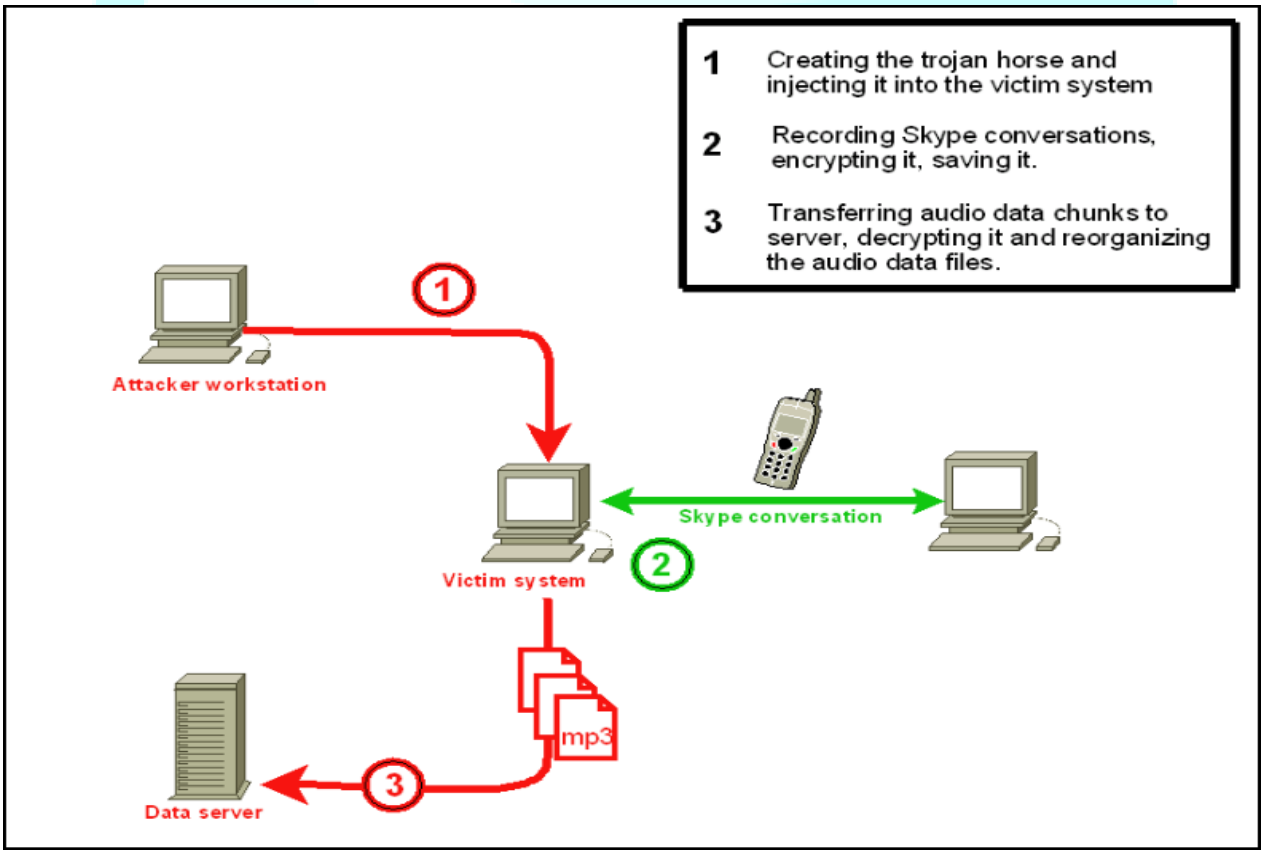
Each Skype client generates half of a 256-bit symmetric key when a connection is established. The keys are exchanged and joined to create a 256-bit session key, which is valid for the life of the session. Every session gets an individual 256-bit key. In the case of a multi-party conference call, multiple simultaneous calls are set up, each with its own session and unique key. The fact that symmetric AES keys are shared enables Skype to be an authenticated channel between any number of valid Skype users.

Skype relies on public-key cryptography to validate signatures on credentials for the purpose of negotiating a symmetric key, then it uses symmetric-key cryptography for secure communication between Skype clients. The combined approach makes the process of establishing transport-layer security among Skype clients efficient.

The public-key cryptographic model enables two things. It permits a Skype client to receive private messages which only it can read, and it lets the Skype client issue signed messages that no one else could have created. No person, organization, nor Skype Technologies S.A., itself has a copy of a key being shared by the parties to a Skype call.

Moreover, there is no sharing or disclosure of keys to any parties other than the pairwise sharing to establish a 256-bit session key. Finally, when a Skype session ends, the keys are discarded. And encryption keys are not disclosed to the Skype user or escrowed to third parties.

7.3.3. Security & File Transfers (Viruses, Trojan Horses, etc.)



The security and file transfers are done securely over the net by not allowing the skype conversation to be decrypted by a third party.

7.3.4. Real-Time File Transfer

A particularly powerful feature of Skype is its capability to enable users to transfer files securely between computers.

On the Microsoft Windows platform, system- and network administrators can turn off the Skype client's file transfer capability by setting a registry key. See Setting Policies via Registry Keys later in this document. The Skype file transfer capability allows a Skype user to send files of up to 2GB to anybody in their contacts list. The intended recipient must meet the following four criteria:

- Has shared contact details (see "Privacy and Sharing Contact Details),
- Has not blocked the sender (see "Blocking Other Skype Users"),
- Is online when the sender initiates the file transfer, and
- Is willing and able to accept the file transfer from the sender.

The Skype client maintains a history of each user's file transfers, those that are sent and received. This list is displayed in the history tab, unless the user clears the list intentionally. The list also shows the origin or destination on the file system of the transferred file.

While Skype's file-transfer capability provides a convenient and secure channel for sending and receiving digital files, along with this newfound capability, comes the risk of inadvertently downloading a file that contains a virus, Trojan horse, or spyware.

So, in much the same way that enterprise users must be thoughtful about opening email attachments or downloading files from the Internet, users must take special precautions when accepting file transfers from other Skype users.
Anti-Virus Shields and Real-time Scanning

All major antivirus software vendors provide anti-virus "shield" capabilities which should be configured to perform real-time scanning. As you recall, all Skype network traffic is encrypted end to end. The Skype client decrypts incoming file transfers only when the user accepts to receive them.

In real-time, as Skype decrypts each file, the anti-virus software on a Skype user's computer will scan it. Therefore, if people in your organization are using or intend to use Skype, it is important to:

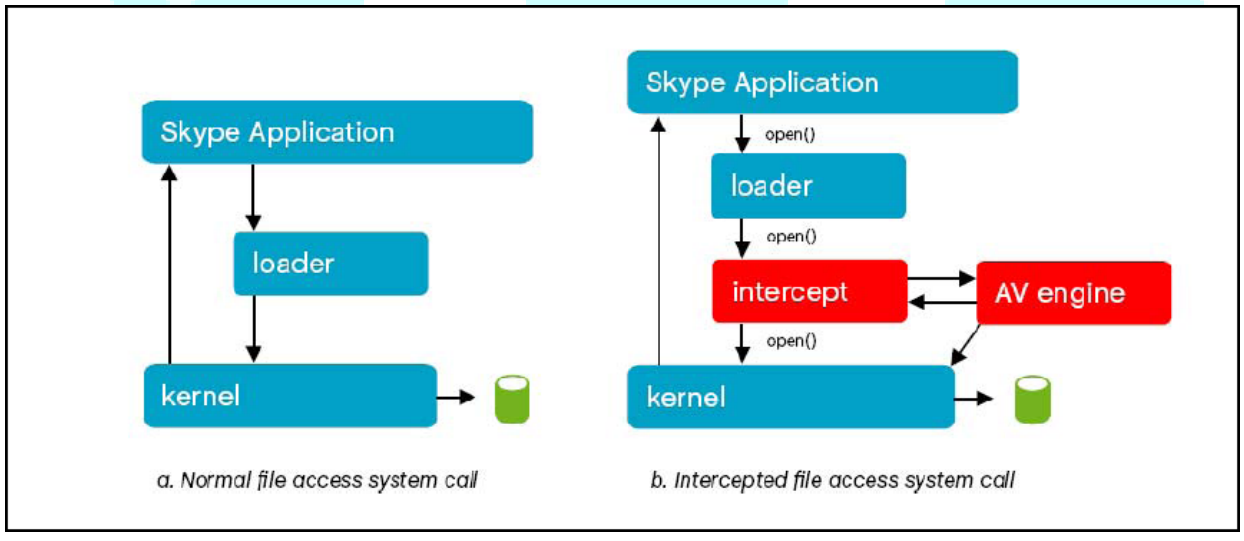
- Configure anti-virus software to scan all incoming files,
- Be vigilant about keeping anti-virus definitions up to date, or
- Turn off the file transfer capability as described later in this document.

Doing these things will prevent your Skype users from inadvertently saving an potentially infected file to the file system (that is, as long as an anti-virus product is running, the virus or Trojan horse is known).
When any software program wishes to read from or write to a file on disk, the application wishing to access the file calls the open() primitive from the kernel to attempt the appropriate access, as is shown in the left panel. When Skype, for instance, reads a file the user wishes to transmit, or when Skype writes the file on the receiving end, the Skype client requests to create, open, read from or write to the file as appropriate.

Antivirus tools make use of the fact that all file access is done through a small number of kernel primitives by employing one of several techniques, depending on the type of operating system in use, to "shim", wrap or intercept all calls to all file access kernel functions.

Therefore, if a user attempts to use Skype to send or receive a file, the antivirus program will detect the attempt to read or write a file containing and deny the Skype client the permission to continue writing.

As is shown in the right-hand panel of figure 6, the antivirus (AV) program inserts itself in the file access chain, which gives it the opportunity to watch for file contents which match known virus signatures.



Real-time Anti-Virus Scanning of File Transfer

8. Conclusion:

Skype is a piece of software that allows people to place both audio and video calls to each other, call ordinary phones and send SMS messages. The company was founded in 2003 and has seen an incredible growth curve since then. We currently have more than 520 million registered users and about 650 employees. Those users generate an average of 210 000 parallel calls about one third of which contain video. These numbers amount to roughly 8% of international calling minutes globally.

Needless to say, this amount of traffic presents unique scalability challenges. For Skype, the main weapon of choice for dealing with those challenges has always been our peer to peer technology. The p2p network (the core of which is implemented in C) is supported by a range of server-based services that are mainly C++ and use Postgre databases with a healthy dose of python thrown in.

9. References:

The following resources and research papers were used to facilitate this research regarding Skype.

http://www.skype.com

http://www.technology-training.co.uk

http://en.wikipedia.org/wiki/Skype_protocol

www.linecity.de/pdf

www.computerworld.com