What is Skype?

Everybody knows!

Skype is a P2P (peer-to-peer) Voice-Over-IP (VoIP) client founded by Niklas Zennström and Janus Friis—also founders of the file sharing application Kazaa (the most downloaded software ever, Skype's 309 million registered users have made more than 100 billion minutes worth of free Skype-to-Skype calls).

Skype is an application that allows free phone calls between computers, and extremely cheap calls to (practically) everywhere on Earth!

Skype (founded in 2002, acquired by eBay in 2005; on September 1st, 2009, a group of investors led by Silver Lake bought 65% of Skype for $1.9 billion) is the fastest growing service in the history of the Internet.

Why is Skype so successful?

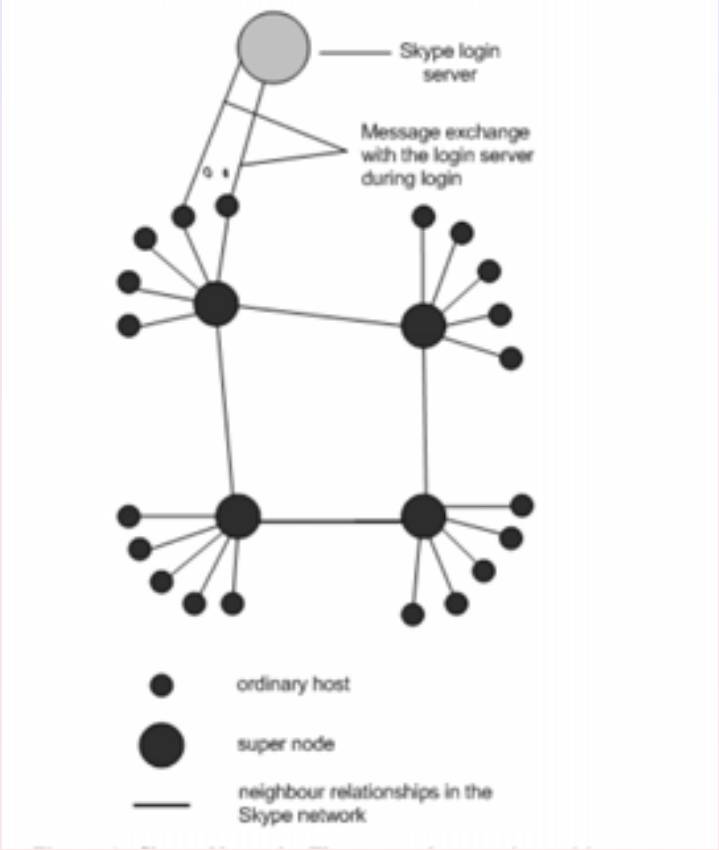
Because:

- it provides better voice quality than anybody else (Skype transmits the full range of human hearing, 20 Hz to 20KHz (compare with the best telephone supporting frequencies in the range 300Hz to 3.4KHz);
- it is reliable and can work almost seamlessly behind NAT's and firewalls;
- it is extremely easy to install and use (probably the most user-friendly application).

How does Skype actually work? 1

Skype network has three types of machines, *all running the same software and treated equally*:

- ordinary host (Skype Client)
- Super Node (SN)
- Skype login server



source: Baset & Schulzrinne, 2004, p.1

How does Skype actually work? 2

A Skype client (SC) (or ordinary host) is the computer of a regular Skype user connected to the network in order to communicate with other users.

An ordinary host connects to a Super Node (SN). Any computer with a public IP and proper hardware configuration can be an SN. An ordinary host must connect to an SN and must register itself with the Skype login server for a successful login.

The Skype login server is the only *central unit* in the whole network. It stores the usernames (Skype Name), e-mail addresses, and respective encrypted representations of passwords of all registered Skype users. There are about 20,000 SN out of many millions of registered Skype users logged on (8,257,048 at 25 May 08 time 09.28; 14, 839,372 at 20 September 2009 time 06.42).

The login process 1

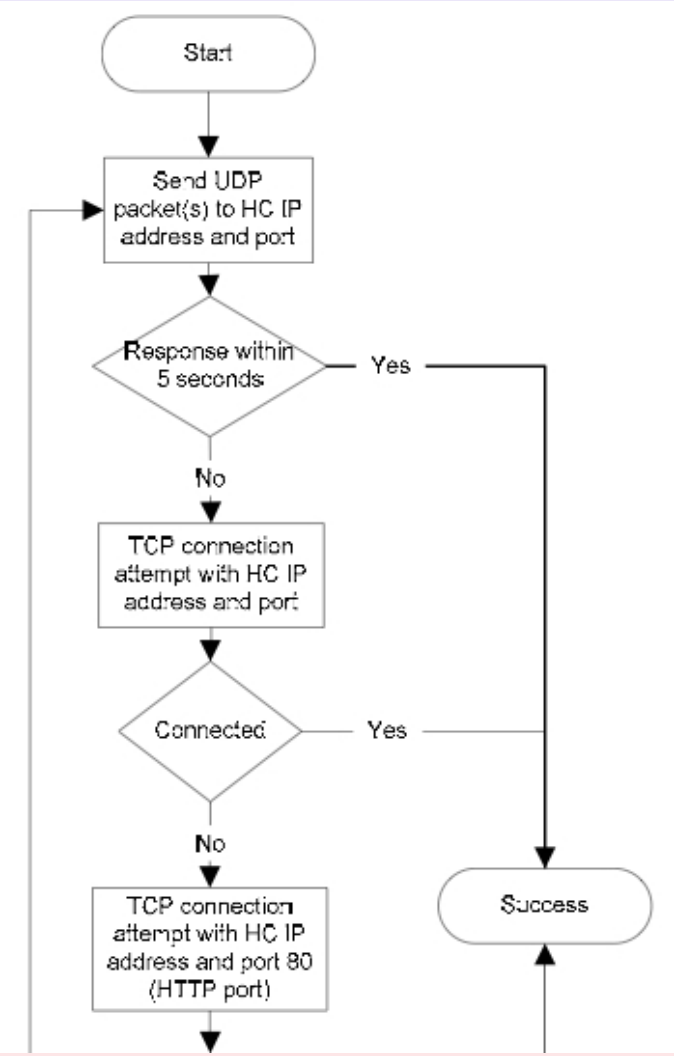
Any SC must connect to an SN, therefore, it maintains a local table that contains the IPs and corresponding ports of SNs—the host cache.

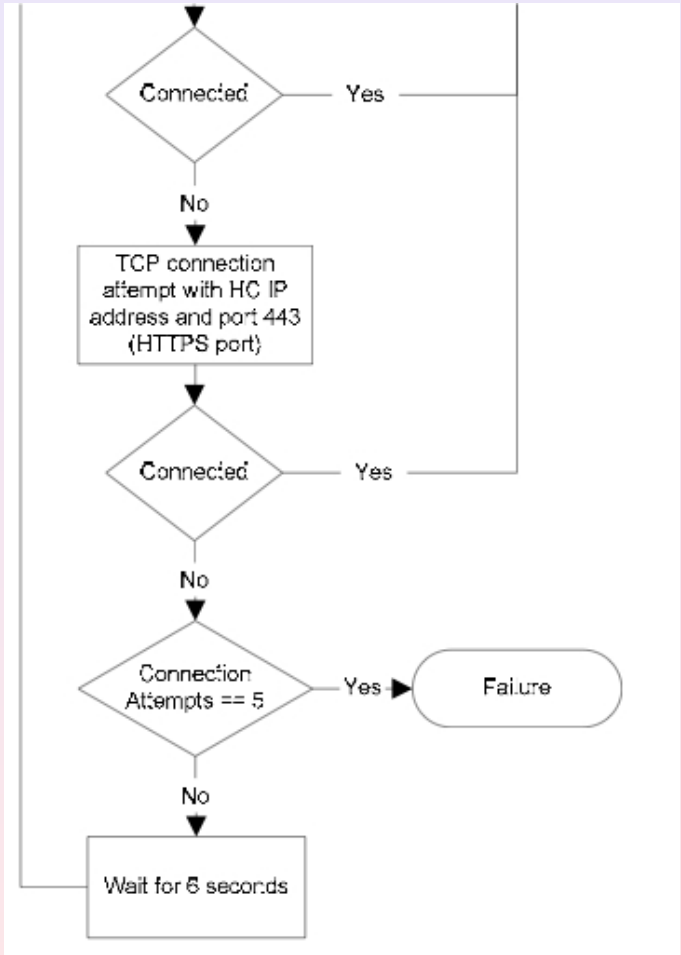
To start-up, SC reads the data from the host cache, takes the first IP (and port) from there, and tries to connect to this SN.

If the connection fails for some reason (e.g. SN is off line), then it reads the next line from the table.

In case it fails to connect to any of the IPs listed, the Skype returns a login error upon start-up. To log in the host cache must contain at least one valid entry—IP address and port number of an online SN.

The login process 2





source: Baset & Schulzrinne, 2004, p.3

Super Nodes 1

SNs (introduced in the third-generation P2P networks) allow

- improved search performance,
- reduced file-transfer latency,
- network scalability,
- and the ability to resume interrupted downloads and simultaneously download segments of one file from multiple peers.

SNs are also responsible for *Global Indexing*, the technology enabling fast searches for other users in the network. Skype guarantees that to find any user registered and logged in during the last 72 hours. Global Indexing allows Skype to build a **reliable** set of services atop a constellation of *unreliable* peers.

Super Nodes 2

The Skype network is self-modifiable.

Almost any computer (which is not behind a firewall) may turn into a SN—*without you even knowing it*. SNs store the *addresses* of up to several hundred SCs, without carrying any voice, text or file-transfer data. In that way, the more SCs come online, the more SNs become available to expand the capacity of the network.

Skype routing

Skype routes the traffic 'intelligently' by choosing the optimum data transfer path. Multiple paths are kept "open" and dynamically Skype chooses the best suited path at the time.

Skype uses either TCP or UDP protocols, hence it *breaks* the whole data stream into separate packets, which can take *different paths* to the end destination where the *final reassembling* is done.

Skype encryption

All Skype communications, voice conversations, text messages, file transfers, are encrypted between the caller and the called party. Encryption is necessary as all calls are routed through the public Internet.

Skype uses Advanced Encryption Standard, known as Rijndel.

Skype uses 256-bit encryption which has a total of 1.1×10^{77} possible keys to encrypt the data in each call or instant message of file transfer. Skype uses 1,536 or 2,048 (for paid services) bit RSA to negotiate symmetric AES keys.

Firewall and NAT 1

Voice-Over-IP (VoIP) was available for years, but has not reached the mainstream market because of the following reasons:

- cheap products do not compare well the standard phones in quality,
- over 50% of residential computers are unable to use the technology because of firewalls and Network Address Translation (NAT) gateway,
- the client needs a lot of technical configuration.

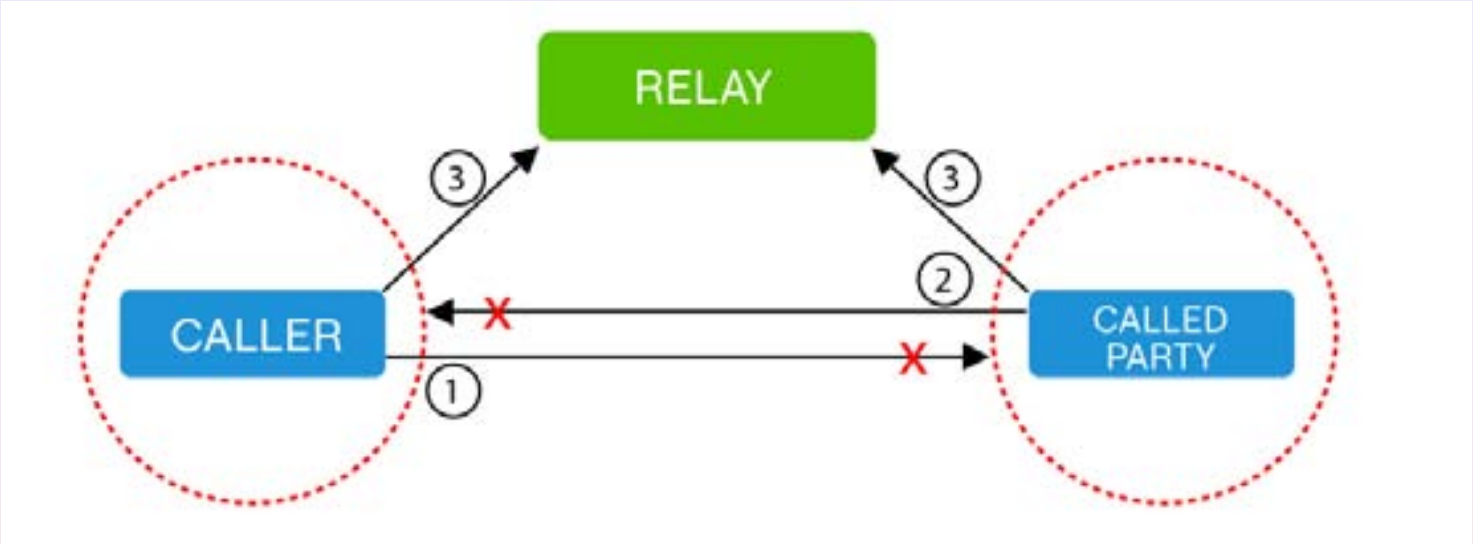
Firewall and NAT 2

If both SCs are on real IP hosts, then the media traffic flows directly between them over UDP. The size of the voice packet is 67B, which is actually the size of UDP payload. One second conversation results in roughly 140 voice packets being exchanged both ways, or 3–16 KBps.

If one of SC or both of them do not have a public IP, then they send voice traffic to another online SN over UDP or TCP.

If both sides are not speaking, voice packets will still be flowing between them. The purpose of these so called silent packages, a form of redundancy, is to keep the connection alive.

Firewall and NAT 3



source: www.skype.com

Skype has implemented a set of NAT traversal techniques which signal to the NAT devices that P2P sessions have been solicited and should be passed. In this way, Skype works behind the majority of firewalls and gateways with no special local configuration.

Not Becoming a Super Node

Three ways to prevent Skype from becoming a SN:

- Beginning with Skype 3.0, an explicit switch is provided in the registry settings to allow the disabling of SN functionality.
- Any computer hosted on a network that is behind a NAT device or restrictive firewall will disable SN functionality.
- Skype clients behind an HTTP or SOCKS5 proxy will not serve as SN.

Skype limitations

Some major limitations of Skype are:

- changing from normal phones to USB phones remains a problem for many users,
- Skype's completely proprietary nature flows against the open source trend (large companies don't appreciate Skype's hidden way of worming through corporate firewalls),
- SNs can generate a significant amount of bandwidth usage, hence some network providers (universities, for example) have banned Skype.

What's next for Skype? 1

- Face competition: VOIP Buster, VOIP Stunt, Gizmo, Free World Dialup, Woize, Xten, Google Talk, etc.
- Continue with improvements in basic technologies and variety and quality of services (fax). For example, screen sharing is getting better making Skype a competitor in the marked o videoconferencing.
- WiFi (short for "wireless fidelity") is becoming more and more popular. The number of cities providing free city-wide WiFi is fast growing. So what?

What's next for Skype? 2

Handheld or other portable wireless devices running Skype become a close substitute for mobile phones: the only difference is that calls are free or at very low rates!
Skype is available on most popular Java-enabled mobile phones from Motorola, Nokia, Samsung and Sony Ericsson: `http://www.skype.com/intl/en/download/skype/mobile`.

Skype is also available in iPhone an iPod touch, directly `http://www.skype.com/download/skype/iphone` or through other applications including Fring, IM+, Nimbuzz, Truphone available from iTunes.

Is growth a problem? Like any P2P network, additional users bring with them their own solution to growth (no more infrastructure is needed).