VoIP:
Skype and its architecture
Seminar 1

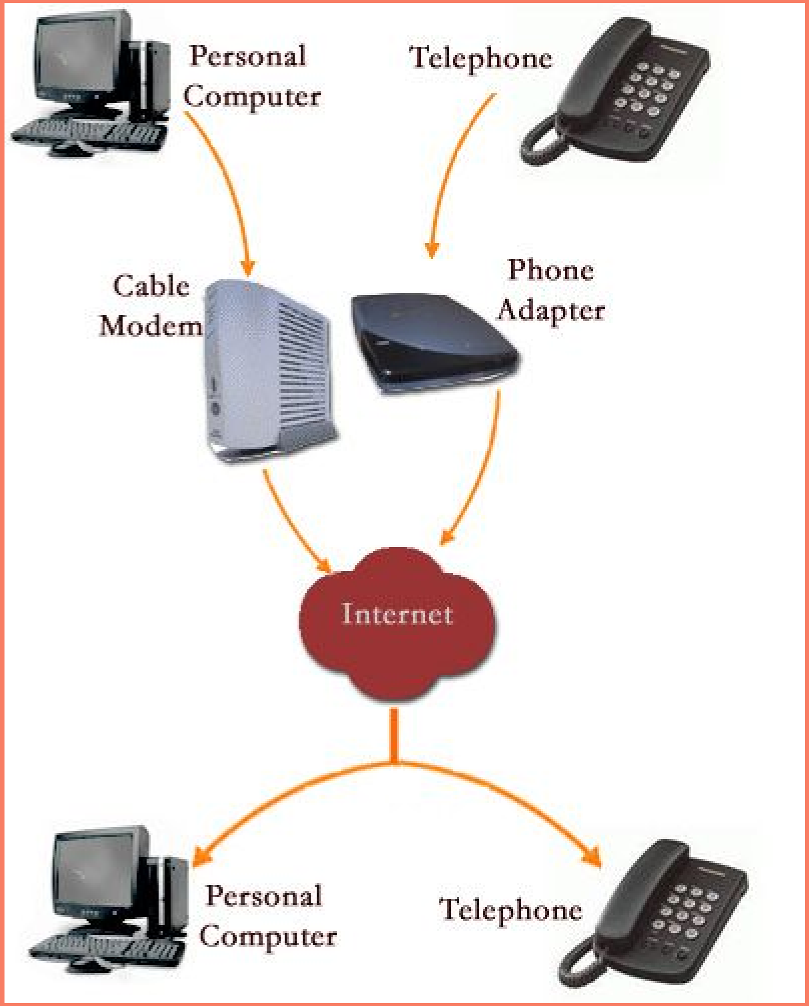
By:

Prateek Arora

Introduction

- VoIP stands for Voice Over Internet Protocol.
- Voice Over IP is a new communication means that let us telephone with Internet at almost null cost.
- More than 30 years ago Internet didn't exist. Interactive communications were only made by telephone at PSTN line cost.
- VoIP works like that, digitalizing voice in data packets, sending them and reconverting them in voice at destination.

Typical VoIP phone



Base architecture

Voice)) ADC → Compression Algorithm →
Assembling RTP in TCP/IP -----
----> |
<---- |
Disassembling RTP from TCP/IP -----
Voice ((DAC ← Decompress. Algorithm ←

Skype

- Skype is a free program that uses the latest cutting edge P2P VoIP technology to bring affordable and high-quality voice communications to people all over the world.
- Peer-to-peer (“P2P”) technology was first widely deployed and popularized by file sharing applications such as Napster and KaZaA.

What is P2P?

- P2P technology allows users to share, search for and download files and involves some direct communication between users or nodes.
- A true P2P system is one where all nodes in a network join together dynamically to participate in traffic routing, processing, and bandwidth intensive tasks that would otherwise be handled by central servers.

Why P2P?

- A true P2P application empowers small teams with good ideas to develop software and businesses that can successfully challenge those of large companies. True P2P, when applied to ripe markets, is known as ***disruptive technology***.
- So P2P telephony became a natural next step where P2P could have a significant disruptive impact and Skype was founded to develop the first P2P telephony network.

Advantages of P2P over traditional SIP based client-server VoIP N/W

1. P2P N/W can **scale indefinitely** without the need for costly centralized resources.
2. P2P N/W **utilize** the **processing** and **networking power** of the **end users** machines since these resources always grow in direct proportion to the network itself.

Advantages (contd.)

3. **Low search time** in P2P N/W.
4. **Low costs** in P2P N/W since by **decentralizing resources**, second generation (2G) P2P networks have been able to virtually eliminate costs associated with a large centralized infrastructure.

Why is Skype better than Net2Phone, ICQ, AIM, MSN, etc.

1. Most voice applications **don't work** well from **behind firewalls and NAT** (Network Address Translation) devices, and nearly all broadband users are behind a NAT or a firewall. Skype lets us do that without compromising security.
2. **High Call Completion Rate**
3. **Superior Sound Quality**
4. **Extremely Easy to Use**
5. **Totally Secure Communications**: Calls are encrypted "end-to-end" and are totally secure.

How does Centralization affects call quality?

- Centralization can overcome some of the call quality issues by routing calls through firewalls or NAT's. However, this brings the cost of running the network to levels approaching that of the existing telecom networks.
- In addition, these **costs scale proportionally with the number of users**. The result is that companies operating such services typically allocate **very little resources** on their servers **per user** which seriously **degrades the call quality**.

Centralization (contd.)

- Since Skype leverage on the resources of the users using Skype, it has allowed Skype to raise the call completion rate and quality in the Skype network to levels exceeding that of POTS (“Plain Old Telephony System”).
- This is all achieved without the need for costly centralized resources.

Description of Skype services

- Skype provides its users with a variety of communications and related services, including the following:
  - Voice calling to another Skype user
  - Voice conference calling
  - Voice calling to traditional telephone lines (SkypeOut)
  - Voice calling from traditional telephone lines (SkypeIn)
  - Chat, providing instant messaging for groups of up to 48 participants
  - Cross-platform file transfer
  - Directory and presence management

- Skype user programs have been built for use on several popular computing platforms, including personal computers running Windows XP, Windows 2000 or Linux, Apple Macintosh computers running Mac OS X and Pocket PCs running Windows Mobile 2003.

How Skype works?

- To provide the most robust and scalable service possible, Skype uses a design called a “**supernode P2P architecture**”, over which all Skype communications are handled.
- Rather than rely on a single big central server to complete calls, Skype software clients directly interact with each other to ensure that the network directory is up to date and that calls are quickly completed.
- Skype users not only use the network as a way to complete calls, their participation in the network helps make the Skype network work.

How Skype works? (contd.)

- Compare it to a **traditional telephone network**, in which **all users** are **connected** to each other through a **hierarchical set of expensive switches** that are set up in **several tiers** in order to allow the completion of **local, regional and long-distance calls**.
- The **supernode P2P architecture** used by Skype **avoids** the **physical connections** needed by the **traditional phone network**.
- The **Skype network** makes this **work because** of its **proprietary Global Index distributed directory**, through which users can find out about each other, place calls, send messages and communicate, all **without using any central servers**.

Supernode P2P architectures

- Supernode P2P architectures have been successfully used by a number of earlier peer-to-peer software applications.
- A **supernode** is a **regular Skype client** that provides a bit of assistance to the Skype network by **handling contact lists** and **helping** out with **call routing**. This service, called the **Global Index function of Skype**, allows Skype to build a reliable suite of services atop a constellation of unreliable peers.
- **Skype's network** can **scale to at least tens of millions of simultaneous users** without foreseeable performance or reliability issues.

What is a Supernode’s duty & eligibility?

- When a Skype client becomes a supernode, it **accepts network connections** from a **small number of other Skype users** for the purpose of **maintaining** the **accuracy** of the **Global Index**.
- Although the **supernode activity** is entirely **transparent** to the user, a Skype client that is **unable to receive inbound network connections** (such as a user behind a NAT or firewall) will **never become eligible** to become a supernode **nor** will it ever be **asked to relay a third party’s traffic**.

How does Skype works across Firewall and NAT?

- Skype’s P2P architecture solves this, allowing calls from users located behind a firewall or a NAT gateway to be transparently routed through the help of a peer that is unfirewalled. This means that anyone can use Skype to make VoIP calls without the need to reconfigure routers or firewalls.
- In business environments, there is no need for a user to demand specialized deployment or operations support for the user client. There is no need to configure ports, gateway names or proxies. In the vast majority of cases, administrators need make no changes to firewall or network configurations.

Call setup

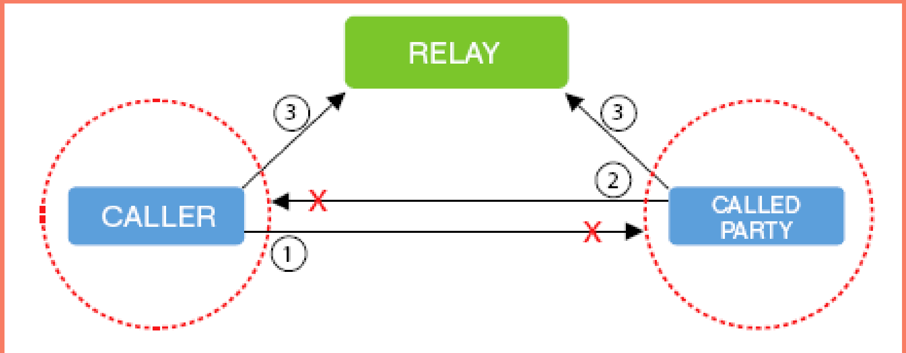


Figure 1-1 Two firewalled Skype users establishing communication

Step 1: When two Skype users wish to communicate with one another, the caller first simply tries to contact the called party directly.

Step 2: If the called party is protected by a firewall, then the called party's computer is asked by the Global Index to connect in the reverse direction back to the caller's computer.

If either of these connections succeeds, then the call is established using a direct connection, providing the most reliable and lowest-latency connection possible between the two parties.

Call setup (contd.)

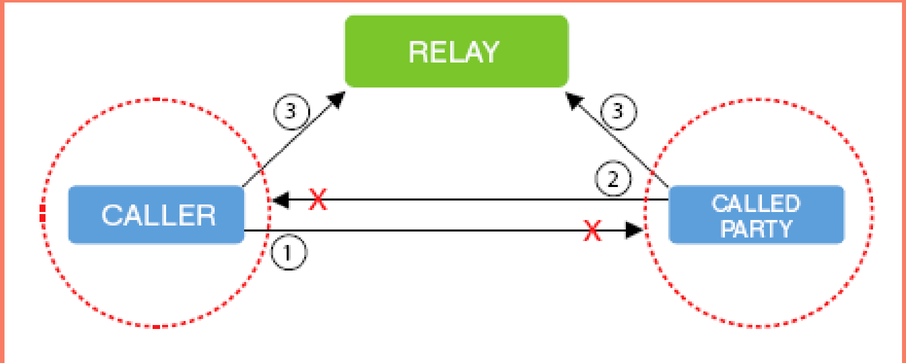


Figure 1-1 Two firewalled Skype users establishing communication

Step 3: If both parties to the call are behind restrictive firewalls, then neither party will be able to reach the other directly. This requires the call to be relayed by a third parties who are reachable by both parties to the call. To do this, a small number of Skype users are selected as relay hosts by the Global Index. In this case, both the caller's and the called party's computers establish a direct link to these relay computers.

Once these connections are established, the caller and called party can communicate because the relay computer will pass data packets between the two parties. One important factor to consider is that even when calls are relayed by third parties, the entire contents of the call, including any voice conversations, text messages or fi le transfers, are encrypted between the caller and the called party.

Reaching outside networks

- One of the difficulties that plagues many VoIP solution is that the call is unable to pass across network boundaries. This problem may arise due to the presence of network address translation (NAT) equipment at the network's boundary or due to restrictive rules put in place on a firewall at the network edge.
- Most networks in use today in homes and offices use NAT to allow easier administration of the network without requiring each network to obtain its own block of scarce network addresses.
- An effective way to set up P2P communications between two computers hosted on private networks — ones behind NAT devices — is to use a technique called "**hole punching**". This is used by Skype.

Skype P2P across NAT

- This technique is widely used by application software communicating using UDP packets and can also be used to establish connections using the more reliable TCP protocol.
- Although the name "**hole punching**" might suggest otherwise, this technique **does not compromise** the **security of private networks** but instead seeks to establish communications by working within the policy framework of most NATs.
- These techniques signal to the NAT devices in the path of a communication that the P2P sessions have been solicited and should therefore be passed.

Protocol used by Skype

- Since the Skype is based on P2P technology, so its developers used a proprietary protocol which they developed.

Proxies & Firewalls

- Skype fully supports SOCKS5 and HTTPS/SSL proxies, including optional authentication. For SOCKS5, the proxy must allow, at a minimum, unrestricted TCP connections to at least port 80, or port 443, or high-numbered ports, meaning those numbered 1024 and higher. For HTTPS/SSL proxies, the proxy must allow unrestricted TCP connections to port 443.
- On Microsoft Windows platforms, Skype uses the proxy settings in Microsoft Internet Explorer to determine what proxy settings, if any, to use. However, the Skype user can set the SOCKS5 or HTTPS/SSL proxy manually, including any needed username and password for proxy authentication.

Skype security

The security properties of Skype services are intended to meet the following objectives:

- **Confidentiality:** The contents of user communications must be accessible only to the
- intended parties and the identity of participants to a communication must be verifiable.
- **Integrity:** User communications must be verifiably authentic. Hence, communications must not be corrupted or modified while in transit.
- **Availability:** Skype services must be available and accessible to legitimate Skype users when needed.

Skype encryption

- All message contents sent between any pair of Skype users is strongly encrypted from end to end. Because Skype communications are sometimes relayed through third parties as part of the NAT traversal process, it’s important that all communications be encrypted from source to destination.
- All communications between any pair of Skype users — consisting of any combination of voice, video, text chat or file transfer — are carried over an encrypted Skype “session layer” that is established between the communicating users before messaging begins.

Skype encryption (contd.)

- At the point of call set-up, the two communicating parties simultaneously exchange signed identification credentials and agree upon a 256-bit encryption key that is used to encrypt the session layer between the parties. Each session is encrypted using the Advanced Encryption Standard (AES) in its AES-256 mode.
- The key established for each Skype session is unique for that session and is neither retained by the user after session termination nor escrowed by Skype or any other party.
- If a Skype user has multiple concurrent open sessions — such as the operation of two or more simultaneous chat sessions — the keys used to encrypt each session will be unrelated to one another.

Conclusion

- Skype is a the first of its kind of P2P based VoIP application, which provides high quality call setup with high call completion rate.
- It is highly secure also because all the calls are encrypted from end to end.

References

- www.google.co.in
- www.skype.com
- http://www.voipreview.org/
- http://www.tldp.org
- http://voip-magazine.com/
- http://telephonyonline.com/voip/metrics/telecom_inte
- http://www.telegeography.com/