Date
14/12/2023

Skype

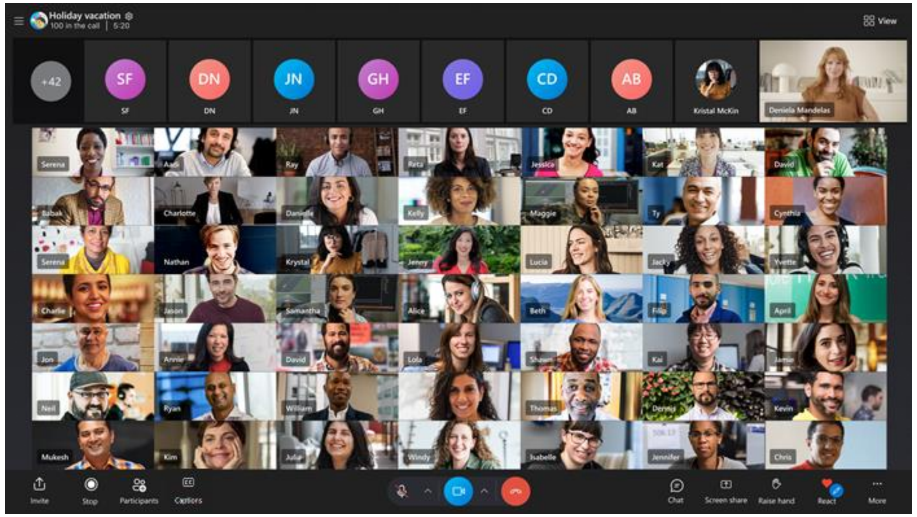
Connects you with anyone, anywhere, anytime.

Babes-Bolyai University
Specialised Protocols In Computer Networks
Lecturer: Sergiu Darabant

Presented by
Anca Alexia Nistor

1. *Introduction*
2. *Skype and the peer-to-peer architecture*
3. *Skype and the centralized Azure-based service*
4. *Skype’s secure communication capabilities*
5. *Skype and encryption*
6. *Skype and voIP*
7. *How does Skype work?*

Skype is a telecommunications application owned by Microsoft, best known for VoIP-based videotelephony, videoconferencing and voice calls.

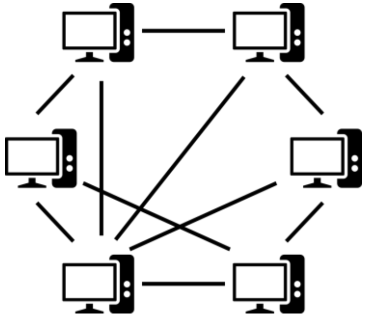


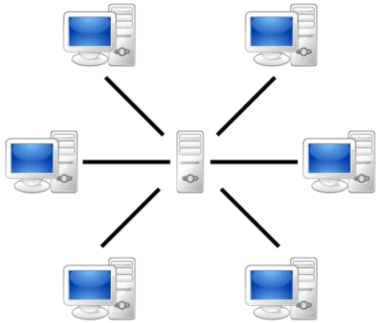
Skype is available on various desktop, mobile, and video game console platforms.

It also has instant messaging, file transfer, debit-based calls to landline and mobile telephones.

Its initial release is 29 August 2003.
Skype originally featured a hybrid peer-to-peer and client-server system.
The name for the software is derived from "Sky peer-to-peer".

Peer-to-peer: devices within the network can act both as clients and as servers to share resources, without the need for a centralized server. (e.g. video calls)
Client-server: the client is a device that requests services or resources from the server. (e.g. login)

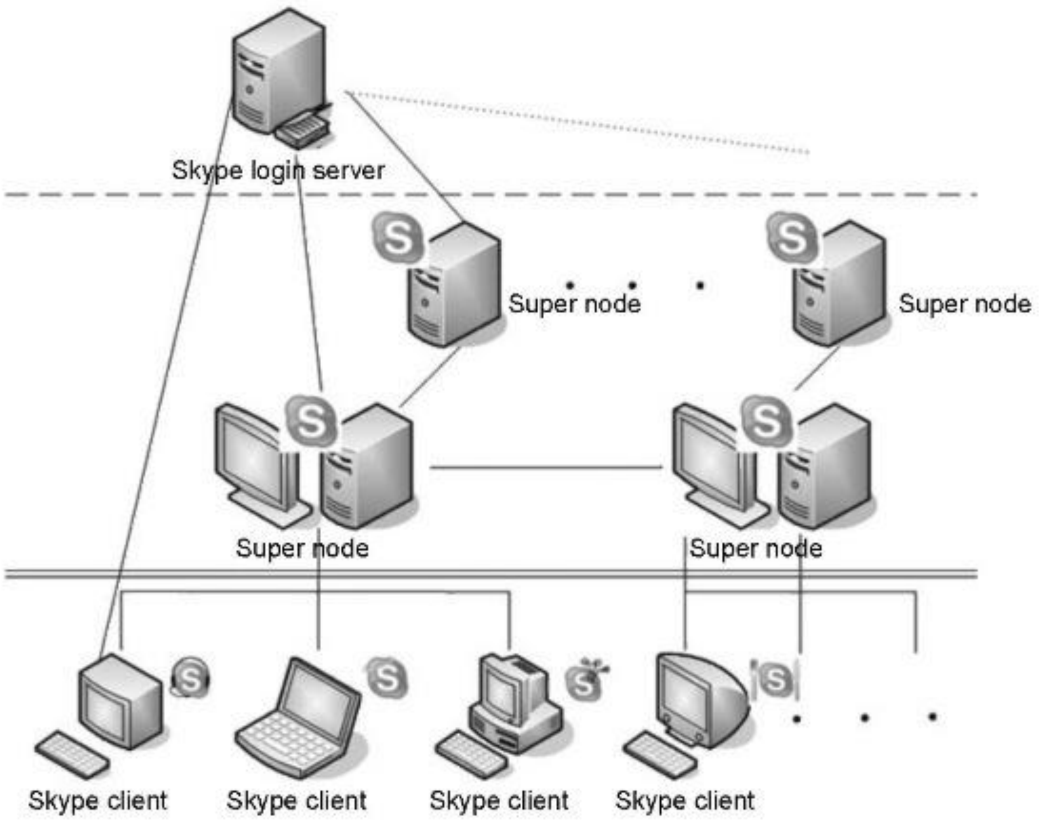




In 2017, it changed from a peer-to-peer service to a centralized Azure-based service: started utilizing Microsoft servers for authentication, call routing, and user management, aiming for improved stability and security.

Skype and the peer-to-peer architecture

Skype was the first peer-to-peer IP telephony network. The network contains three types of entities: supernodes, ordinary nodes, and the login server.



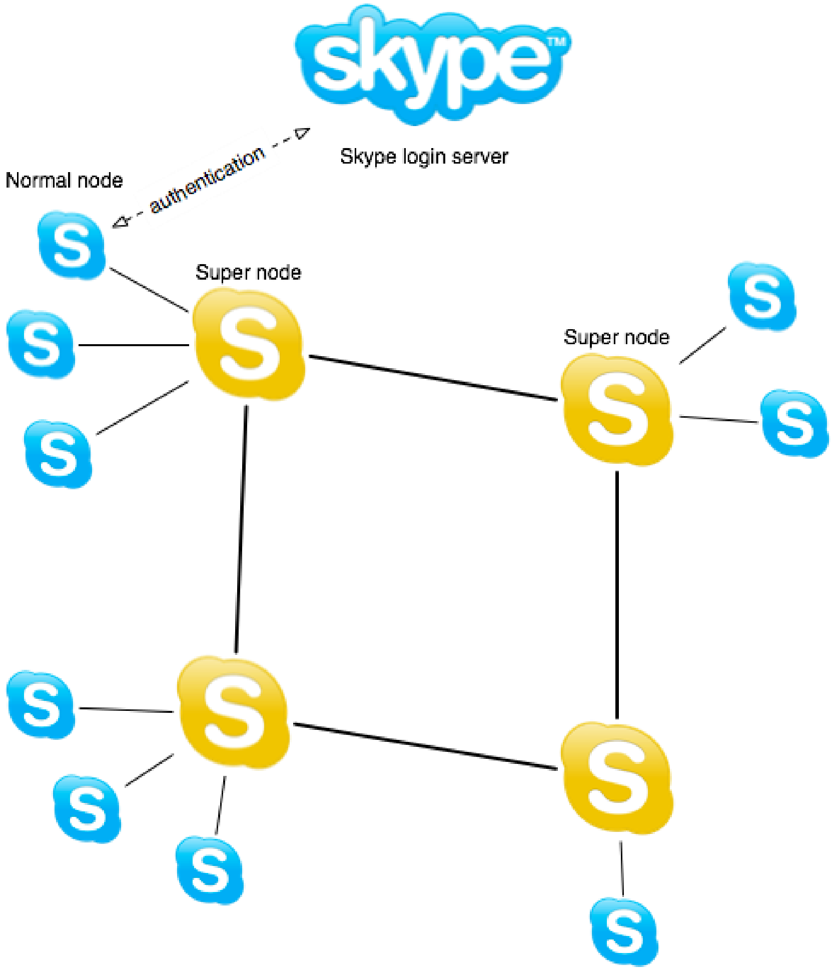
Ordinary nodes:

- regular user devices (computers, smartphones) that run the Skype software and participate in the Skype network
- act as both clients and servers (can initiate connections without relying on a centralized server for every interaction)

Supernodes:

- play a significant role in facilitating connections and managing traffic between ordinary nodes
- act as network hubs or relays
- better connectivity, higher processing power, and more bandwidth
- selected based on specific criteria like network connectivity, available resources, and reliability
- enhance the network's stability, assist with NAT traversal, contribute to the overall functionality

Skype network consists of normal Skype clients and super nodes. Multiple clients can connect to one super node.



The strategy of selecting a Skype super node is not very clear. According to previous studies, if a client has a public IP, sufficient CPU power, memory, and network bandwidth, and stays online for a long time, it is very likely to be selected as a super node.

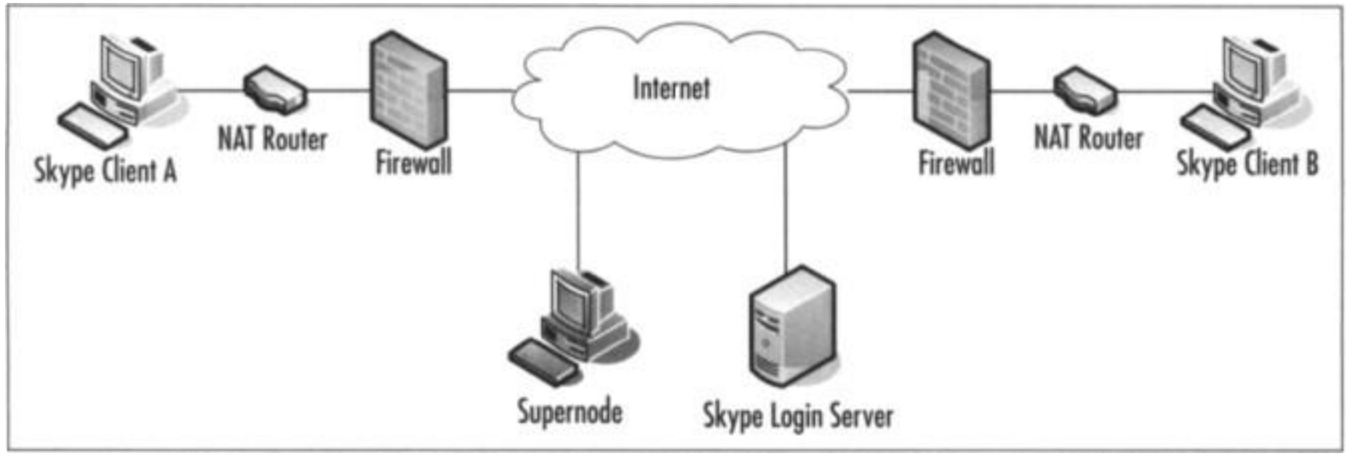
The super nodes still run normal routines as clients, but at the same time, they are connected to each other forming the backbone of the Skype network.

Skype and the centralized Azure-based service

	Peer-to-peer service	Centralized Azure-based service (2017)
Transition overview	Users' devices communicated directly with each other.	Microsoft started utilizing their Azure cloud platform for various Skype services.
Authentication	Skype primarily used P2P connections for user authentication.	Microsoft's servers began handling user authentication, ensuring more centralized control and security in verifying user credentials.
Call routing	Call routing was decentralized and relied on connections between users.	Microsoft's servers started directing connections between users for voice and video calls.
User management	Managing user accounts, contacts, and related functionalities were distributed in the P2P model.	User management was consolidated on Microsoft's servers, providing better control, consistency and management capabilities.

Skype's secure communication capabilities

NAT and Firewall Traversal Skype's NAT and firewall traversal ability ensures that it can work behind almost all kinds of NATs and firewalls.



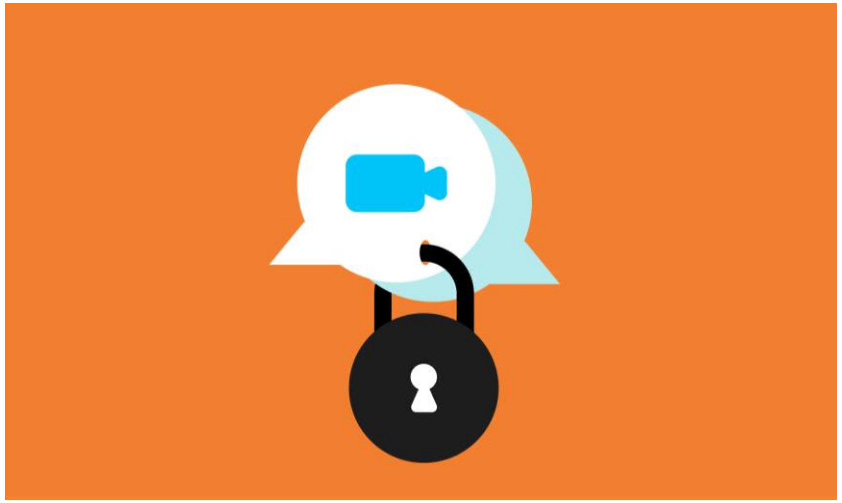
Legend:
NAT: Network Address Translation
STUN: Session Traversal Utilities for NAT
TURN: Traversal Using Relays around NAT
UDP: User Datagram Protocol
TCP: Transmission Control Protocol

It is conjectured that the Skype client uses a variation of STUN and TURN protocols. Moreover, as Skype can use both UDP and TCP as its transport layer protocol, it can easily switch to TCP transition if the UDP flow is blocked by some firewalls.

The website of Skype claims that it uses 256-bit Advanced Encryption Standard (AES) for encryption.

Skype and encryption

All Skype-to-Skype voice, video calls, file transfers, and instant messages are encrypted, providing protection against potential eavesdropping by malicious users.



Regarding instant messages, TLS (transport-level security) encrypts messages between a user's Skype client and the chat service in the cloud. When messages are exchanged directly between two Skype clients, 256-bit Advanced Encryption Standard is employed.

In the case of Skype calls to mobile and landline phones, the segment of the call conducted over the PSTN (ordinary phone network) is not encrypted. For group calls involving two users on Skype-to-Skype and one user on PSTN, the PSTN segment remains unencrypted, while the Skype-to-Skype portion is encrypted.

Voice messages are encrypted upon delivery to the recipient. However, once a voice message is listened to, it transfers from the servers to the local machine of the recipient as an unencrypted file.

Skype and E2EE

End-to-end encryption (E2EE) is a specific type of encryption that provides a higher level of security and privacy by ensuring that the data is encrypted on the sender's device, remains encrypted as it travels through the communication channel (such as the internet), and is then decrypted only on the recipient's device.

This means that the content of the data, whether it's a message, file, or communication, is only accessible to the sender and the intended recipient, and no intermediaries, including service providers or servers facilitating the transmission, can access the unencrypted data.

As of 2018, Skype introduced the "Private Conversation" feature, which allows users to have end-to-end encrypted conversations. This encryption is achieved using a combination of the Signal Protocol and the Double Ratchet Algorithm, which are known for their robust security and privacy features.

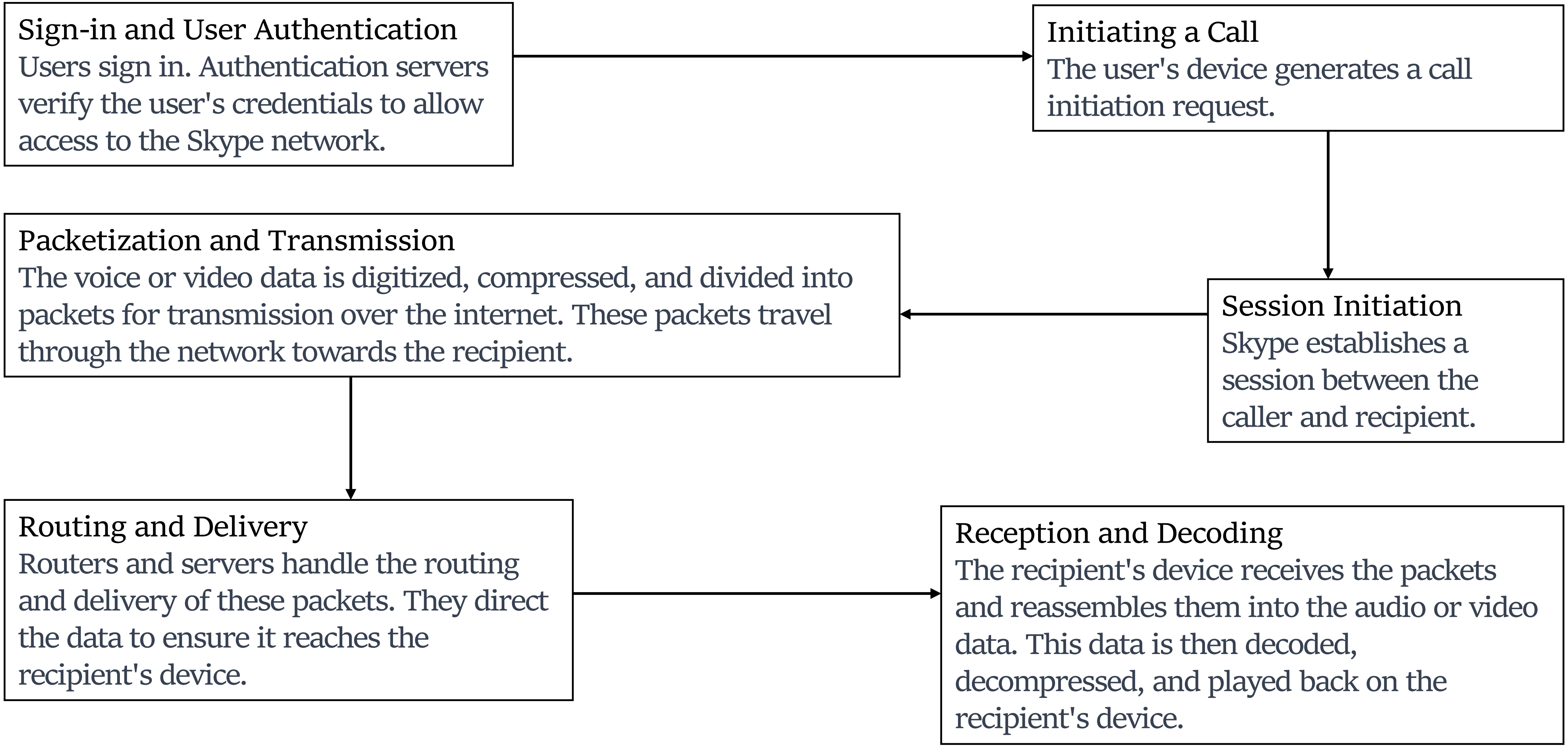
Skype and voIP

The main technology on Skype is voice-over-internet-protocol. This system allows a call to be carried over an Internet connection rather than a phone line.

Unlike a phone service, the Internet doesn't cost more to transfer data around the world than to transfer it to the house next door. This means that Skype can charge much less than phone companies to carry long-distance and international calls, yet still charge enough to make a profit.

VoIP simply converts the sound of voice (and the picture with video calls) into computer data. It reduces the quality of the audio to reduce the data demands. This works in the same way as music file formats such as mp3, meaning that the audio is reduced in quality but not to the point that most callers will notice.

How does Skype work?



Sign-in and User Authentication
Users sign in. Authentication servers verify the user's credentials to allow access to the Skype network.

Initiating a Call
The user's device generates a call initiation request.

Session Initiation
Skype establishes a session between the caller and recipient.

Packetization and Transmission
The voice or video data is digitized, compressed, and divided into packets for transmission over the internet. These packets travel through the network towards the recipient.

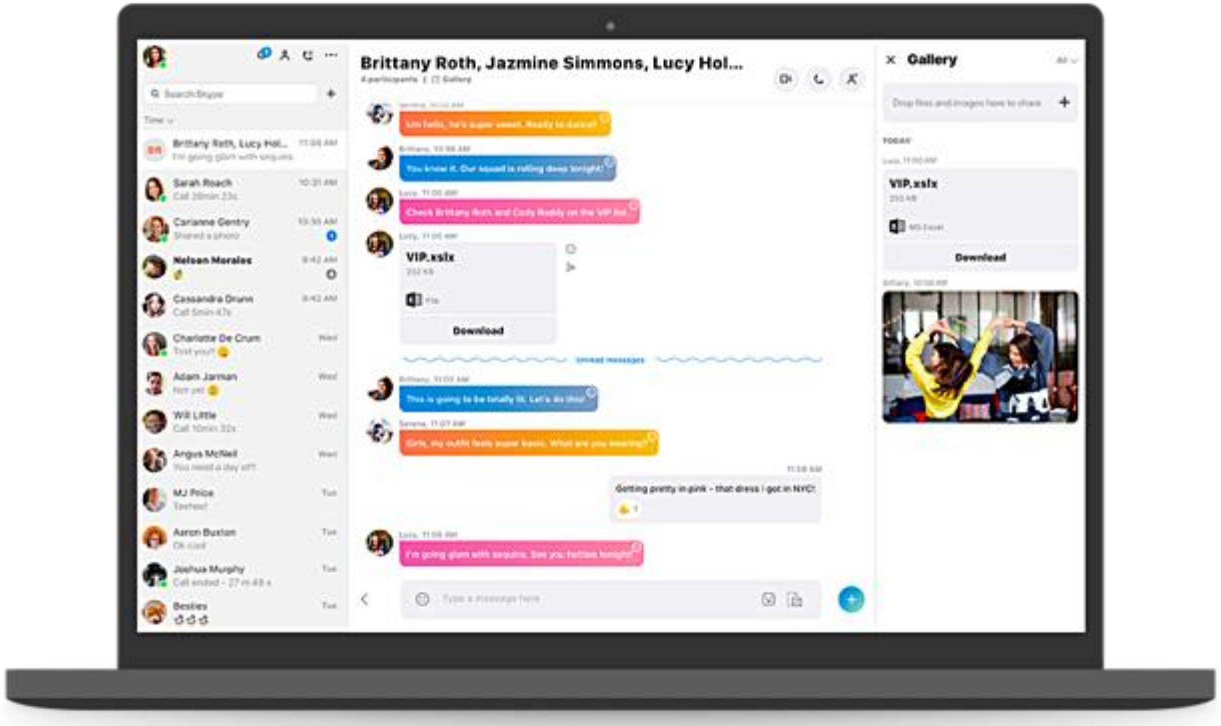
Routing and Delivery
Routers and servers handle the routing and delivery of these packets. They direct the data to ensure it reaches the recipient's device.

Reception and Decoding
The recipient's device receives the packets and reassembles them into the audio or video data. This data is then decoded, decompressed, and played back on the recipient's device.

https://www.skype.com/ro/
https://www.zdnet.com/article/microsoft-starts-testing-end-to-end-encrypted-skype-conversations/
https://www.comparitech.com/blog/information-security/is-skype-safe-and-secure-what-are-the-alternatives/
https://www.theonespy.com/skype-secured-private-conversations-end-to-end-encryption/
https://support.skype.com/en/faq/FA31/does-skype-use-encryption
https://support.skype.com/en/skype/all/privacy-security/
https://security.utexas.edu/consensus/skype
https://secure.skype.com/en/skype-number?intsrc=client-_-windows-_-8.109.0.209-_-.userInfo.GetSkypeNumber&tcg=8fce935a-cb8a-4bea-a169-d39c988e8b85
https://what-when-how.com/voip/skype-overview-voip/
https://en.wikipedia.org/wiki/Node_(networking)
https://en.wikipedia.org/wiki/Supernode_(networking)
https://en.wikipedia.org/wiki/Skype_protocol
https://getvoip.com/library/what-is-voip/
https://www.quora.com/Is-Skype-protocol-really-p2p-or-is-there-a-third-party-server-that-could-possibly-be-keeping-a-record-of-the-communication-going-on
https://dispatch.m.io/skype-for-business-endoflife/
https://en.wikipedia.org/wiki/Skype_protocol
https://en.wikipedia.org/wiki/Peer-to-peer
https://en.wikipedia.org/wiki/Skype
https://en.wikipedia.org/wiki/Skype_Technologies
https://www.lifewire.com/what-is-skype-3426903

Skype is a powerhouse in the world of communication, providing a platform that connects people across the globe. Its range of features makes connecting easy, boosting teamwork, productivity, and bringing folks closer.

THANK YOU! ☺



Serena, 10:55 AM
Um hello, he's super sweet. Ready to dance!

Brittany, 10:58 AM
You know it. Our squad is rolling deep tonight!

Lucy, 11:00 AM
Check Brittany Roth and Cody Reddy on the VIP list.

Lucy, 11:00 AM
VIP.xlsx
232 KB
File
Download

Unread messages

Brittany, 11:03 AM
This is going to be totally lit. Let's do this!

Serena, 11:07 AM
Girls, my outfit feels super basic. What are you wearing?

11:08 AM
Getting pretty in pink - that dress I got in NYC!

Lucy, 11:08 AM
I'm going glam with sequins. See you hotties tonight!