

# An Analysis of the Peer-to-Peer Internet Telephony Protocol



Salman A. Baset & Henning Schulzrinne  
Department of Computer Science Columbia  
University  
September 15, 2004

Graduate of Dept. of IM  
Wendy Y.F. Wen

# Outline

1. INTRODUCTION
2. KEY COMPONENTS OF THE SKYPE SOFTWARE
3. EXPERIMENTAL SETUP
4. SKYPE FUNCTIONS
5. CONCLUSION

# INTRODUCTION

## INTRODUCTION

COMPONENT

SETUP

FUNCTIONS

CONCLUSION

- ⑤ Skype is a peer-to-peer VoIP client developed by KaZaa.
- ⑤ Capabilities:
  - voice call
  - instant messaging
  - audio conferencing →
  - buddy list
- ⑤ Skype is very similar to the MSN and Yahoo IM applications, however, **the underlying protocols and techniques it employs are quite different.**

## INTRODUCTION

# Skype network

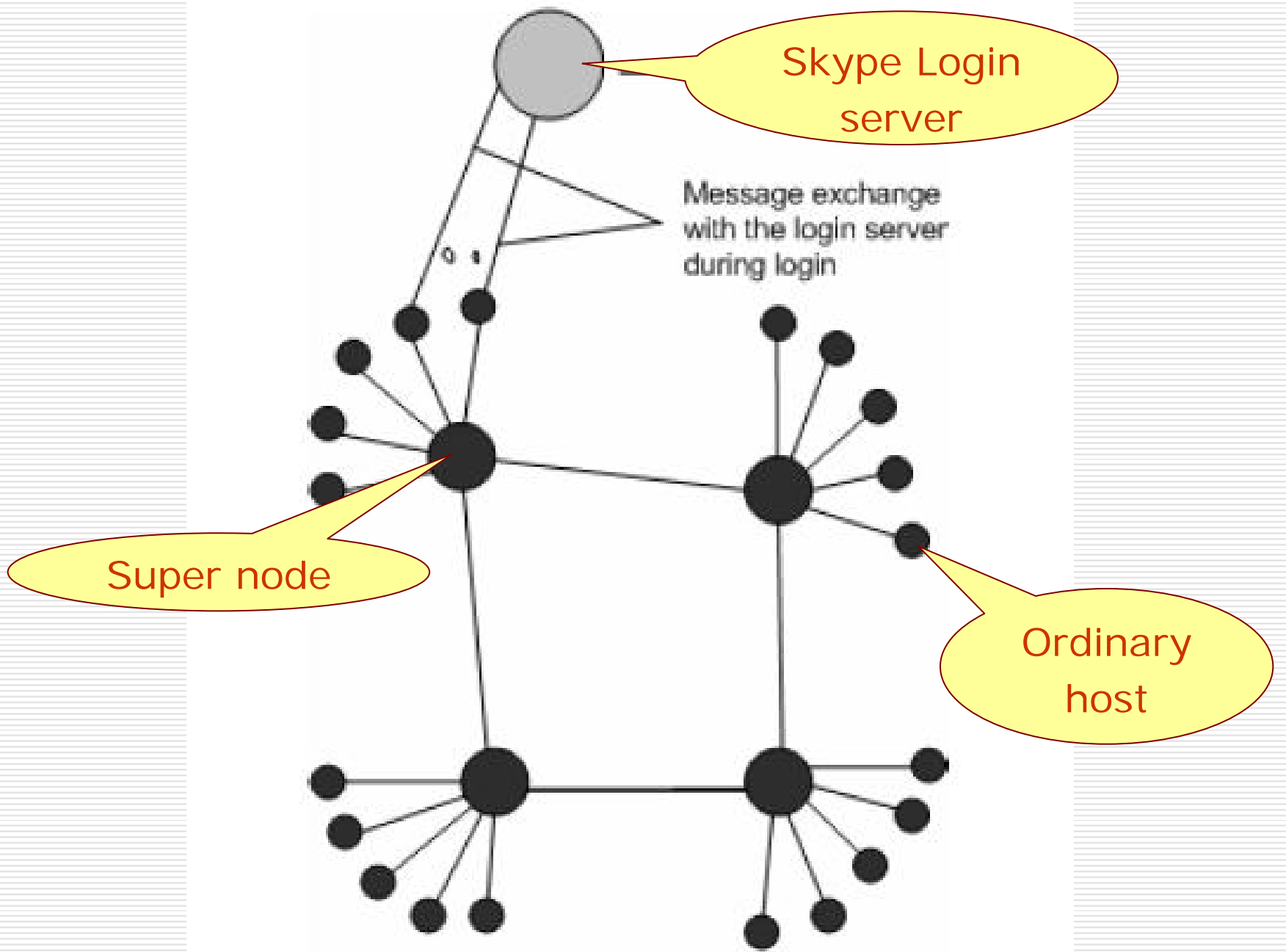
- ③ Skype is an **overlay p2p network**, including two types of nodes:
  - ordinary host (SC)
  - super node (SN)
  
- ③ An SC must connect to a SN and must register itself with the **Skype login server** for a successful login.
  - Skype login server
    - the only one central server
    - username and password
    - user authentication
    - unique Skype login name

COMPONENT

SETUP

FUNCTIONS

CONCLUSION



# KEY COMPONENTS OF THE SKYPE SOFTWARE

# KEY COMPONENTS

1. Ports
2. Host Cache
3. Codecs
4. Buddy List
5. Encryption
6. NAT and Firewall



INTRODUCTION

**COMPONENT**

SETUP

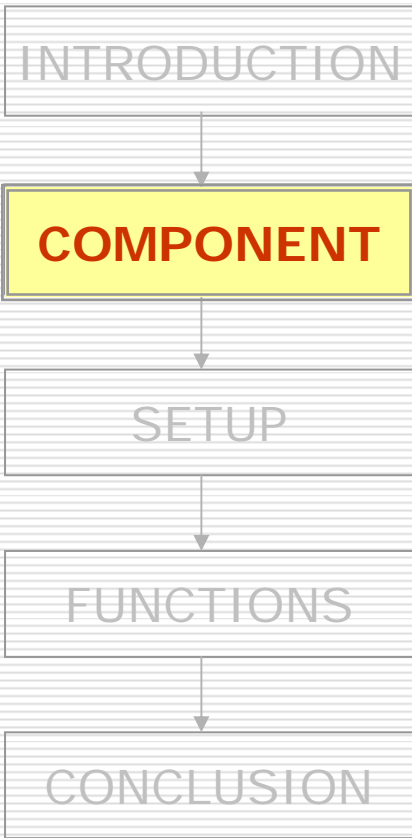
FUNCTIONS

CONCLUSION

# Ports

---

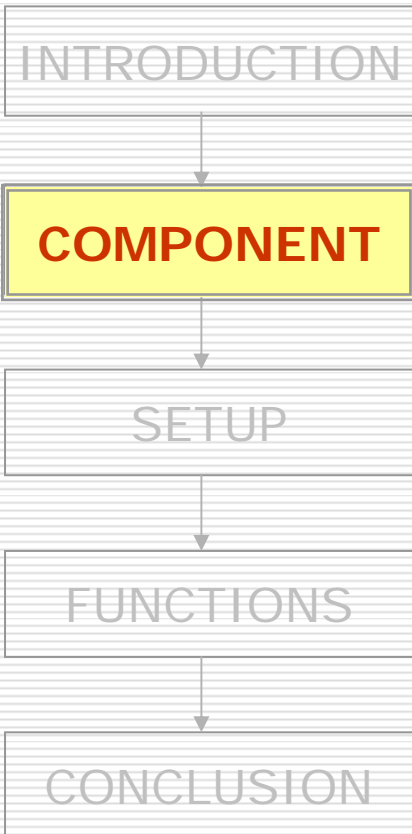
- ❶ A SC opens a TCP and a UDP listening port and randomly chooses the port number upon installation.
- ❷ SC also opens TCP listening ports at port number 80 (HTTP port), and port number 443 (HTTPS port).
- ❸ There is no default TCP or UDP listening port.



## Host Cache (1/2)

---

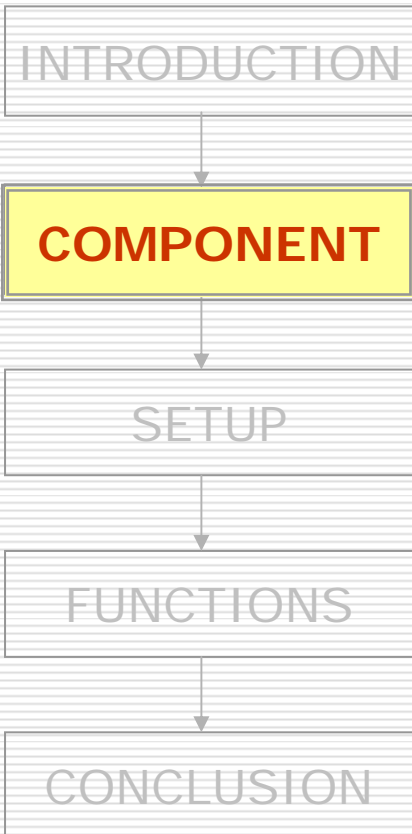
- ❶ HC is a list of SN IP address and port pairs that SC builds and refreshes regularly.
- ❶ At least one valid entry must be present in the HC.
- ❶ A SC stores HC in the Windows registry.



## Host Cache (2/2)

---

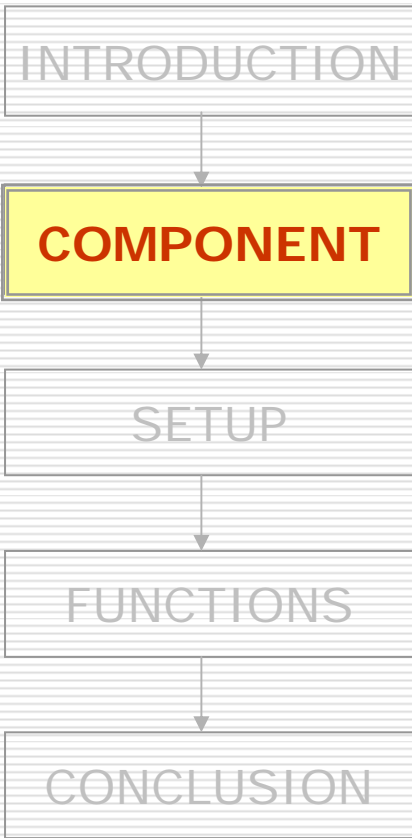
- Ⓢ After running a SC for two days, we observed that HC contained a maximum of 200 entries.
- Ⓢ Chord has a finger table which it uses to quickly find a node.



# Buddy List

---

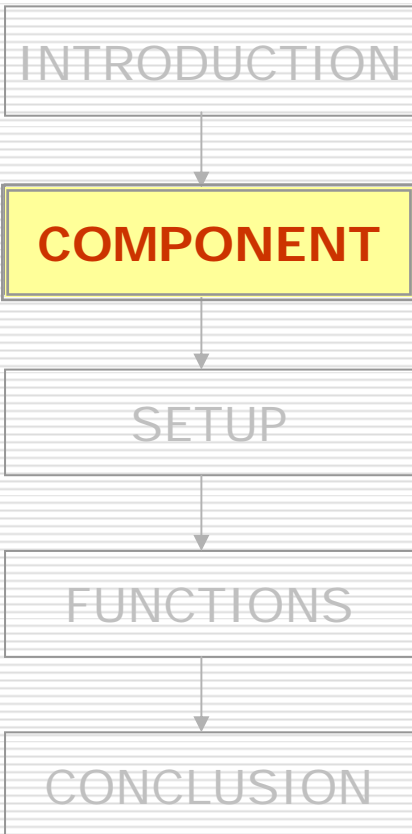
- ❶ Skype stores its buddy information in the Windows registry.
- ❷ The BL is digitally signed and encrypted.
- ❸ The BL is local to one machine.



# Encryption

---

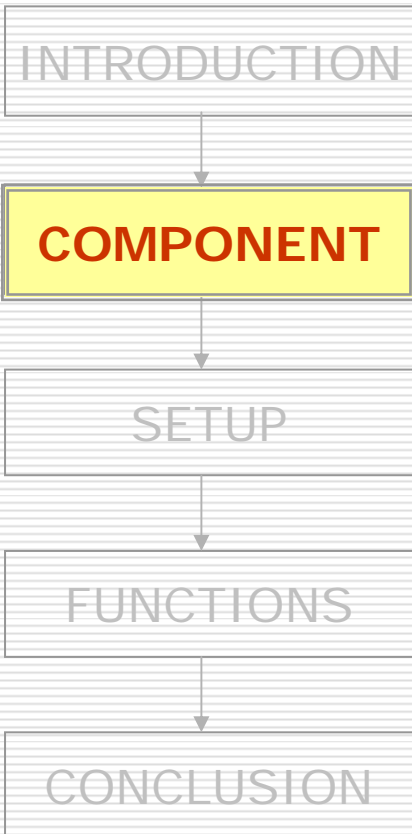
- ❶ Skype uses **256-bit encryption AES**.
  - Which has a total of  $1.1 \times 10^{77}$  possible keys, in order to actively encrypt the data in each Skype call or IM.
- ❷ Skype uses **1536 to 2048 bit RSA to negotiate symmetric AES keys**.
  - User public keys are certified by Skype server at login.



# Codecs

---

- ④ The white paper observes that Skype uses iLBC , iSAC , or a third unknown codec.
  - GlobalIPSound has implemented the iLBC and iSAC codecs and their website lists Skype as their partner.
- ④ We measured that the Skype codecs allow frequencies between 50-8,000 Hz to pass through.
  - **wideband codecs**



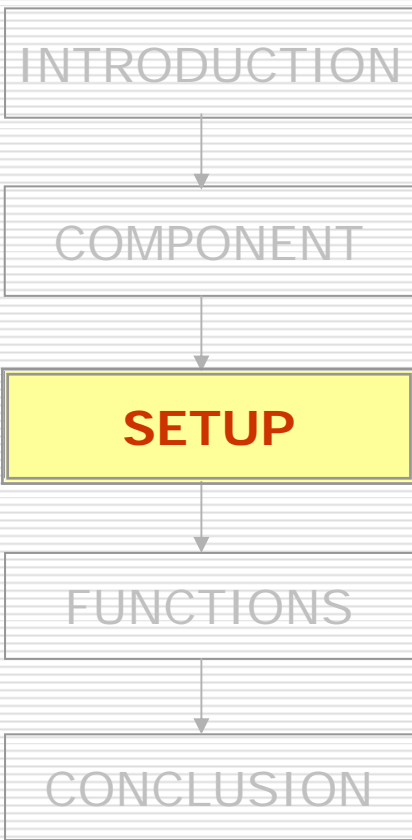
# NAT and Firewall

---

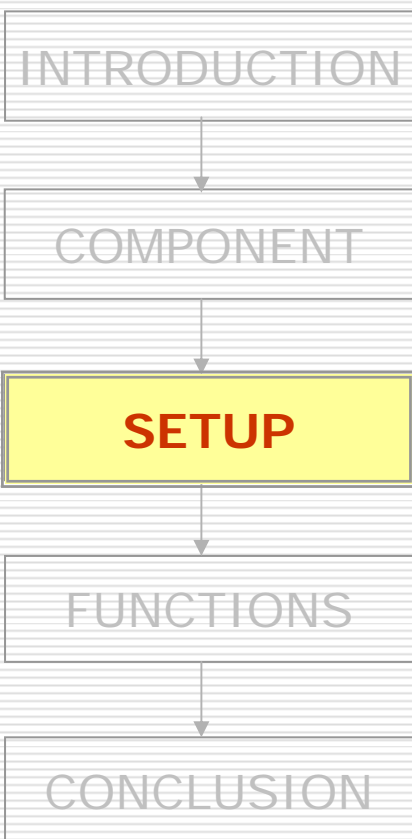
- ⑤ The SC uses a variation of the **STUN and TURN protocols** to determine the type of NAT and firewall it is behind.
- ⑤ A SC cannot prevent itself from becoming a SN.

# EXPERIMENTAL SETUP

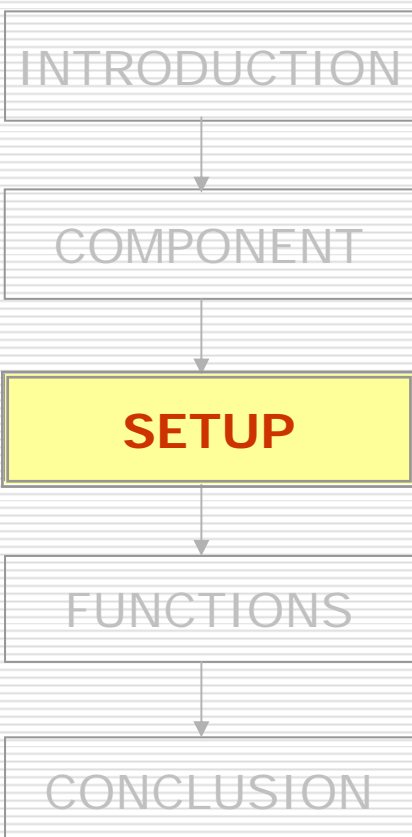




- ❶ Skype version: 0.97.0.6
- ❷ Installed on two Windows 2000 machines:
  1. Pentium II 200MHz with 128 MB RAM
  2. Pentium Pro 200 MHz with 128 MB RAM
- ❸ Each machine had a 10/100 Mbps Ethernet card and connected to a 100 Mbps network.

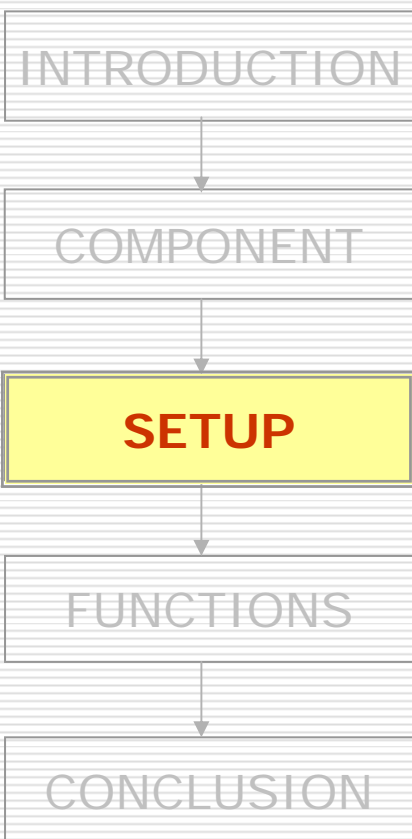


- ⑤ NAT and firewall machines :
  - ran Red Hat Linux 8.0
  - connected to 100 Mbps Ethernet network
  
- ⑤ Ethereal were used to monitor network traffic.
  
- ⑤ NetPeeker were used to control network traffic.



## **S** Three different network setups:

1. Both Skype users were on machines with public IP addresses.
2. One Skype user was behind port-restricted NAT.
3. Both Skype users were behind a port-restricted NAT and UDP-restricted firewall.

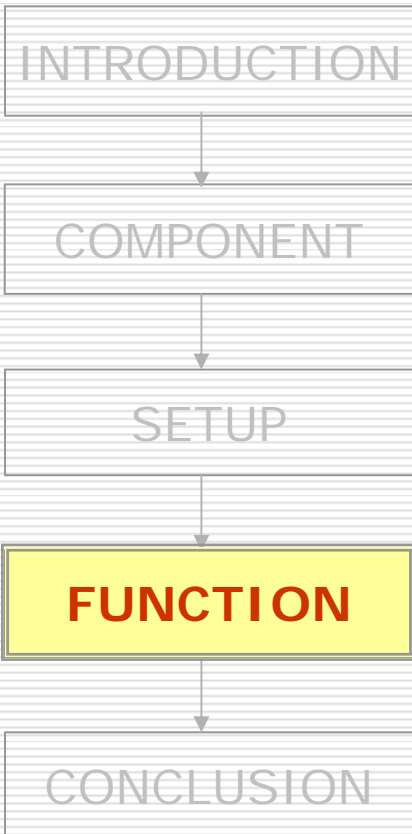


- ❶ For each experiment, the Windows registry was cleared of any Skype entries and Skype was reinstalled on the machine.
- ❷ All experiments were performed between February and April, 2004.

# SKYPE FUNCTIONS

# Skype Functions

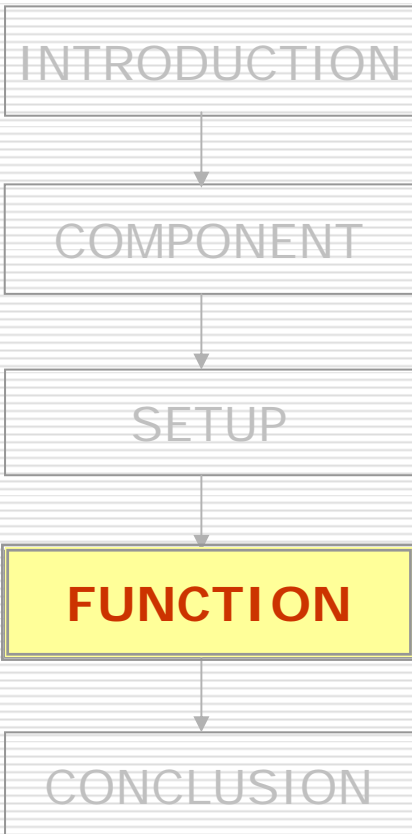
1. Startup
2. Login
3. User Search
4. Call Establishment
5. Call Tear-down
6. Media Transfer
7. Keep-alive Message



# 1. Startup

---

1. After installation, SC sent a HTTP 1.1 GET request to the Skype server (skype.com).
  - The first line of this request contains the keyword 'installed'. ➡
2. Subsequently, a SC only sent a HTTP 1.1 GET request to the Skype server to determine if a new version is available.
  - The first line of this request contains the keyword 'getlatestversion'. ➡

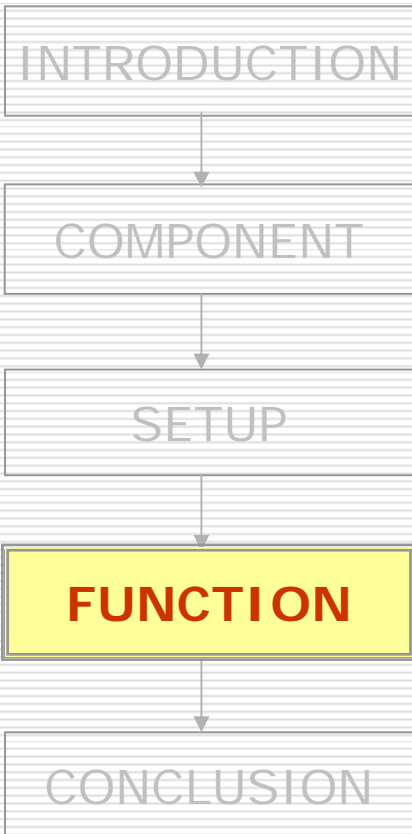


## 2. Login

---


- ⑤ Login is the most critical function to the Skype operation.
  
- ⑤ During this process, a SC would:
  1. authenticate
  2. advertise
  3. determine the type of NAT and firewall
  4. discover online SN

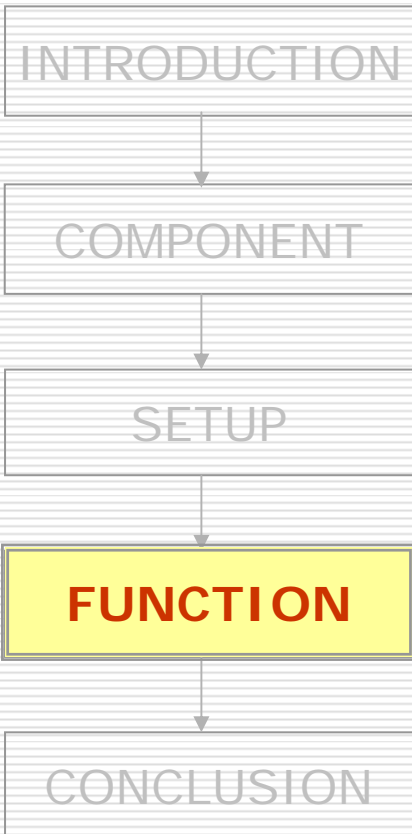




## 2. Login: Login Process (1/2)

---

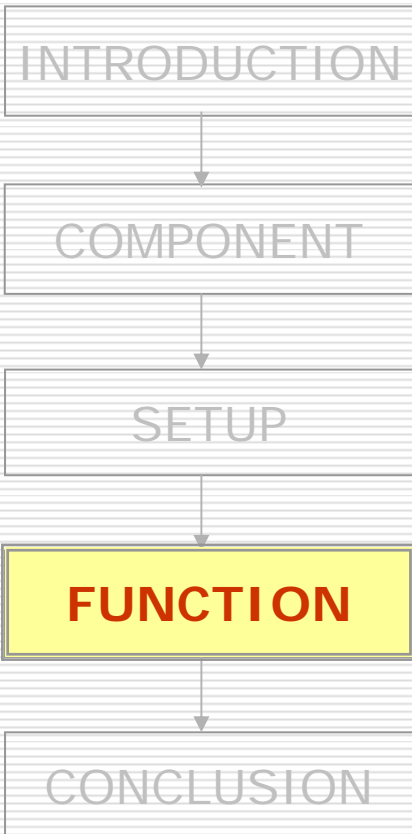
- ⑤ HC must contain **a valid entry** for a SC to be able to connect to the Skype network.
  
- ⑤ To gain useful insights in the Skype login process:
  1. flushing the SC host cache
  2. filling it with only one invalid entry
  3. observing the message flow 



## 2. Login: Login Process (2/2)

---

- ❶ Result of Login Process:
  - 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.

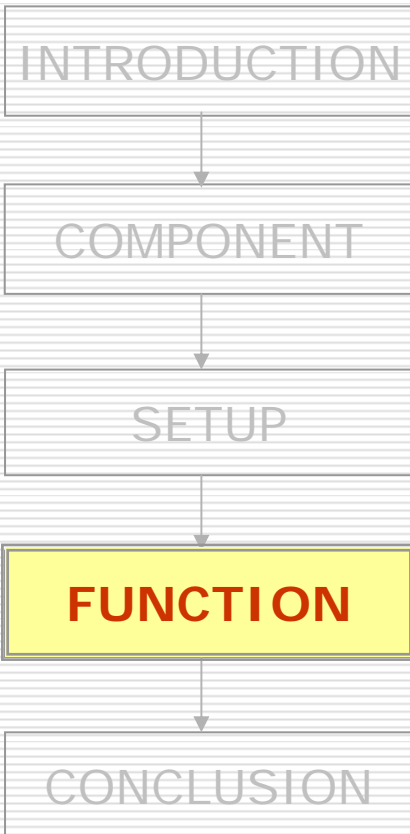


## 2. Login: Bootstrap Super Nodes

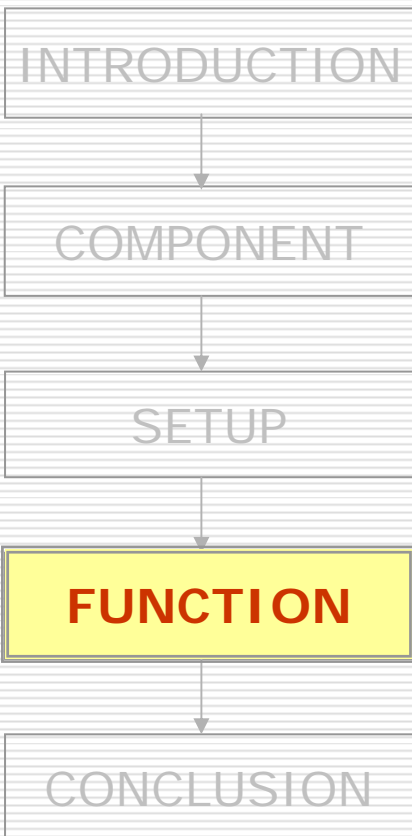
---

- ⑤ After logging in for the first time after installation, HC was initialized with **seven** IP address and port pairs.
- ⑤ We call these IP address and port pairs **bootstrap super nodes**. ➡

## 2. Login: Login Server



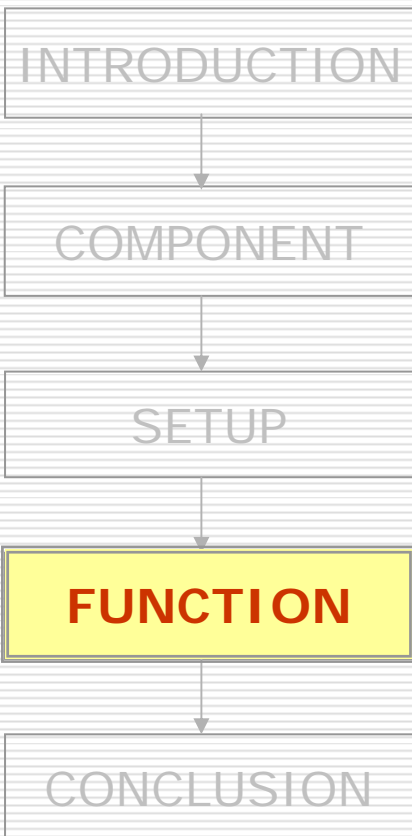
- ③ After a SC is connected to a SN, the SC must authenticate the username and password with the Skype login server.
- ③ The SC always exchanged data over TCP with a node whose IP address was [80.160.91.11](#).
  - We believe that this node is the login server.
- ③ A reverse lookup of this IP address retrieved NS records whose values are [ns14.inet.tele.dk](#) and [ns15.inet.tele.dk](#).
  - It appears that the login server is hosted by an ISP based in [Denmark](#).



## 2. Login: First-time Login Process (1/5)

---

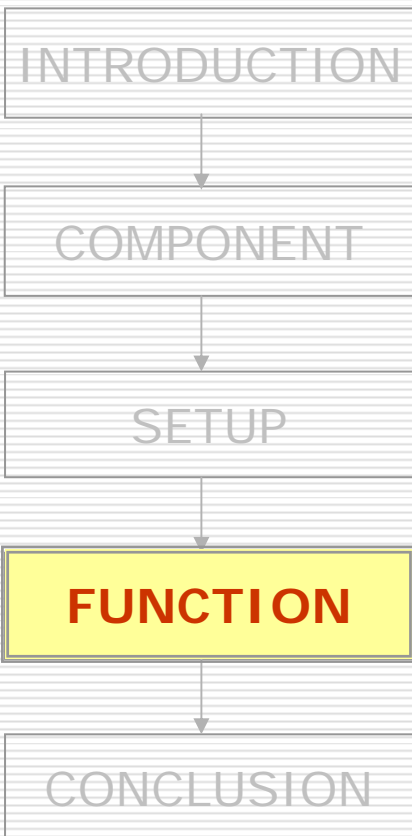
- ⑤ A SC must connect to well known Skype nodes to log on to the Skype network.
  1. sending UDP packets to some bootstrap SN
  2. establishing a TCP connection with the bootstrap SN that responded
  3. exchanging some packets with SN over TCP
  4. establishing a TCP connection with the login server
  5. exchanging authentication information with it
  6. closing the TCP connection



## 2. Login: First-time Login Process (2/5)

---

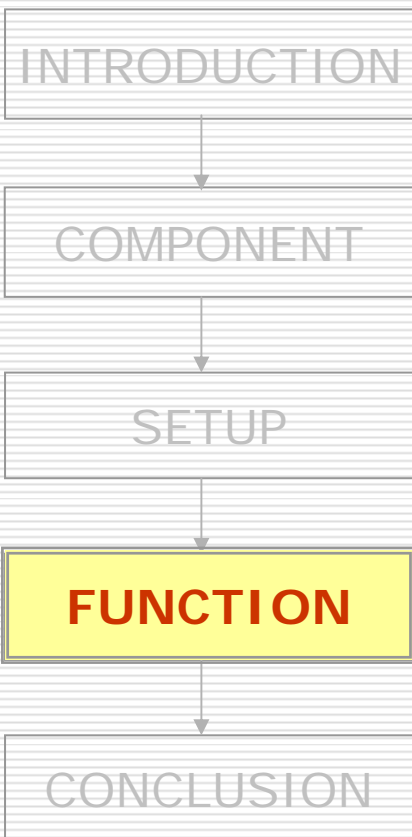
- S** Message flow:
1. on a public IP address ➡
  2. behind a simple NAT ➡
  3. behind a port-restricted NAT and a UDP-restricted firewall ➡



## 2. Login: First-time Login Process (3/5)

---

- ③ Two ways in which a SC can determine at login if it is behind a NAT and firewall:
  1. By exchanging messages with its SN using a variant of the STUN protocol
  2. During login, a SC sends and receives data from some nodes after it has made a TCP connection with the SN
  
- ③ Once determined, the SC stores this information in the Windows registry.

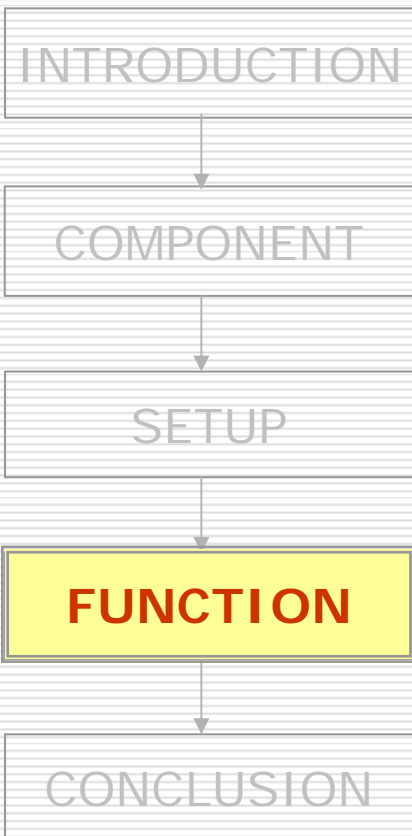


## 2. Login: First-time Login Process (4/5)

---

- ④ SC sends ICMP messages to specific nodes in the Skype network.
  - The reason for sending these messages is not clear.
  
- ④ SC sends UDP packets to 22 distinct nodes at the end of login process,
  - to advertise its arrival on the network.
  - to builds **alternate node table**, a table of online nodes.

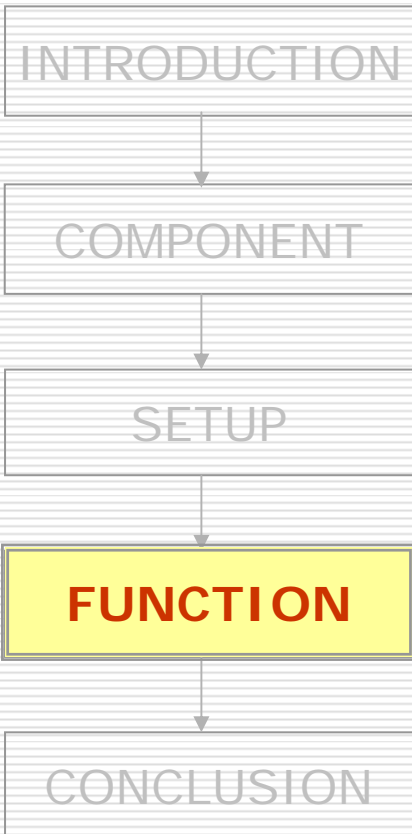




## 2. Login: First-time Login Process (5/5)

---

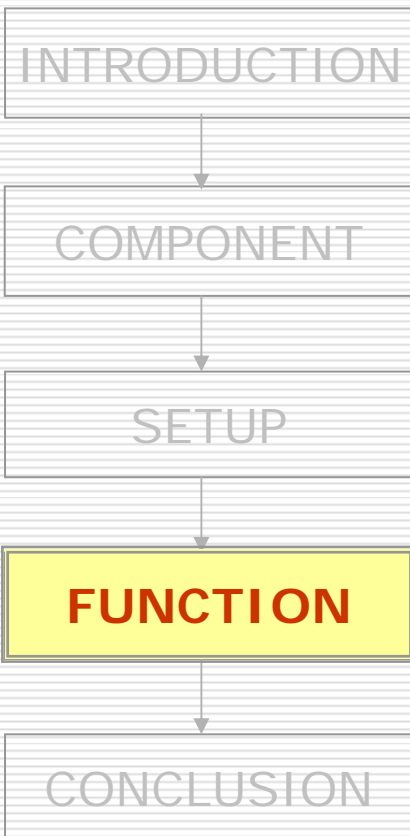
- The time to login on the Skype network,
  - SC with a public IP address and SC behind a port-restricted NAT took about **3-7 seconds**.
  - SC behind a UDP-restricted firewall took about **34 seconds**.



## 2. Login: Subsequent Login Process

---

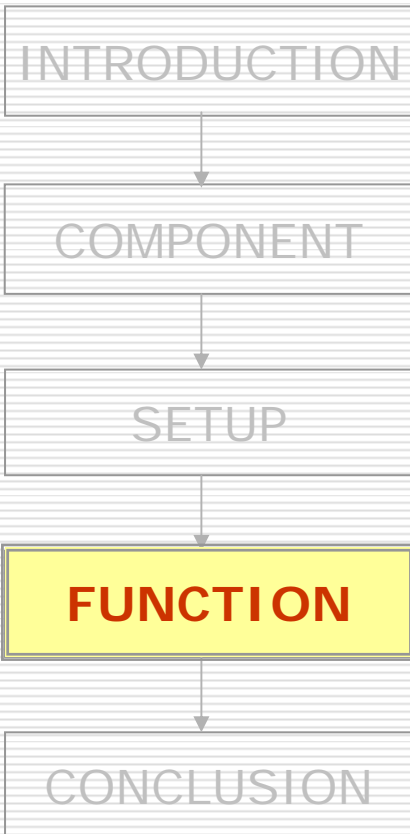
- ⑤ The subsequent login process was quite similar to the first-time login process.
- ⑤ SC used the login algorithm to determine at least one available peer out of the nodes present in the HC.
- ⑤ During subsequent logins, SC did not send any ICMP packets.



### 3. User Search

---

- Skype uses its **Global Index (GI)** (3G P2P) technology to search for a user.
- Search is distributed and is guaranteed to find a user if it exists and has logged in during **the last 72 hours**.

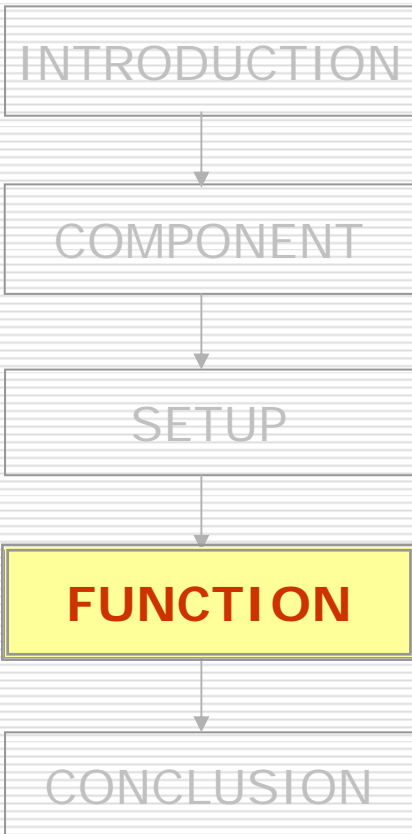


## 3. User Search Process

---




1. SC entered the Skype user id and pressed the find button.
2. SC sent a TCP packet to its SN, and SN gave SC the IP address and port number of four nodes.
3. SC sent UDP packets to four nodes.
4. If SC could not find the user, it informed the SN over TCP.
5. SN now asked it to contact eight different nodes.
6. SC then sent UDP packets to eight different nodes
7. ...

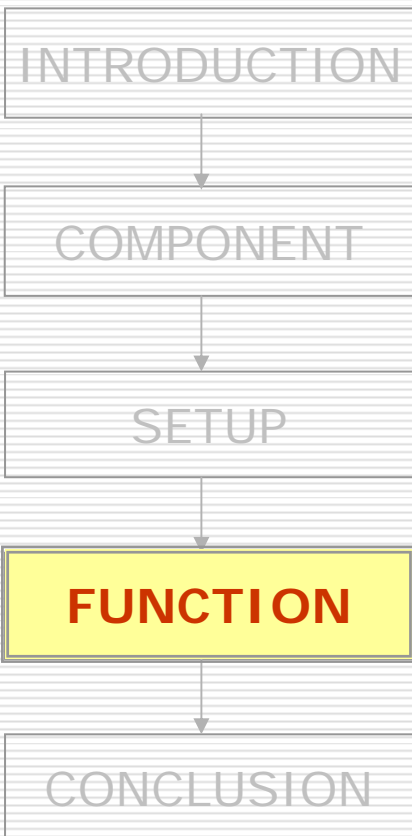
(On average, SC contacted eight nodes. The search took three to four seconds.)



## 4. Call Establishment (1/2)

---

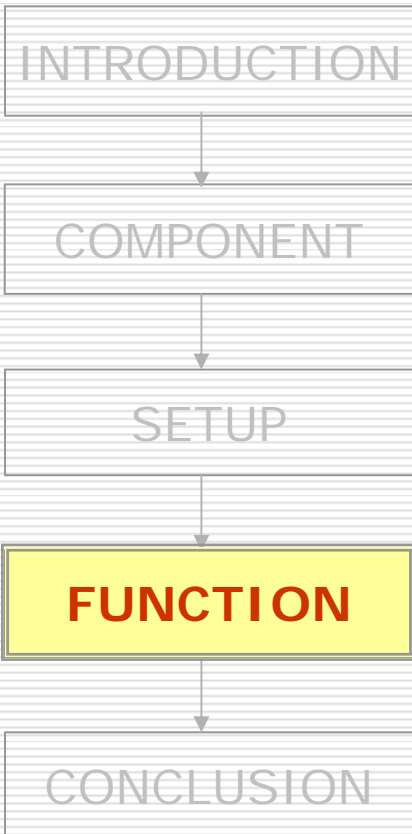
- ⑤ Call signaling is always carried over TCP.
- ⑤ Message flow:
  1. when caller and callee SC are on machines with public IP addresses. 
  2. when caller SC is behind a port-restricted NAT and callee SC is on public IP address. 
  3. when caller and callee SC are behind a port-restricted NAT and UDP-restricted firewall. 



## 4. Call Establishment (2/2)

---

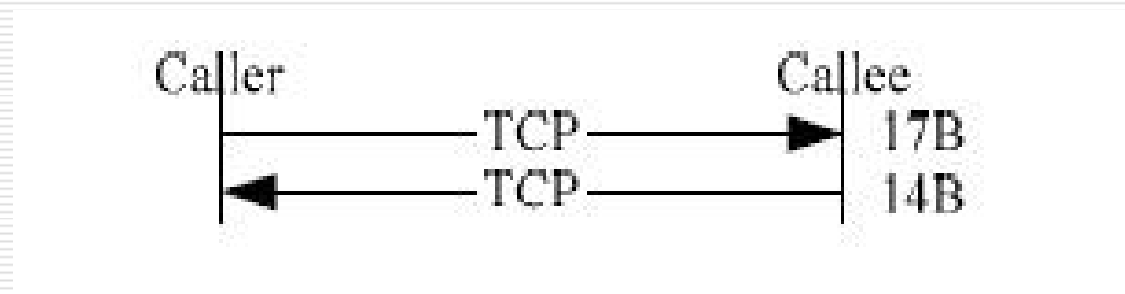
- ⑤ A node, called media proxy, routes the voice packets from caller to callee and vice versa.
  - Advantages:
    1. It provides a mechanism for users behind NAT and firewall to talk to each other.
    2. If users behind NAT or firewall want to participate in a conference, this node serves as a mixer and broadcasts the conferencing traffic to the participants.
  - Disadvantages:
    1. There will be a lot of traffic flowing across this node.
    2. Users generally do not want that arbitrary traffic should flow across their machines.

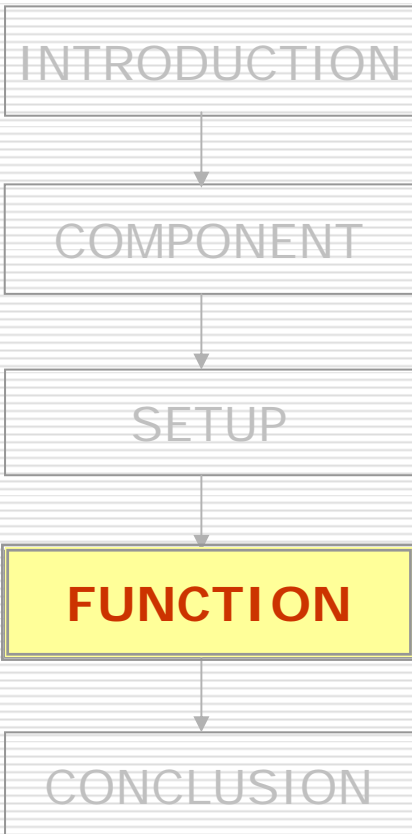


## 5. Call Tear-down

---

- During call tear-down, signaling information is exchanged over TCP between caller and callee.



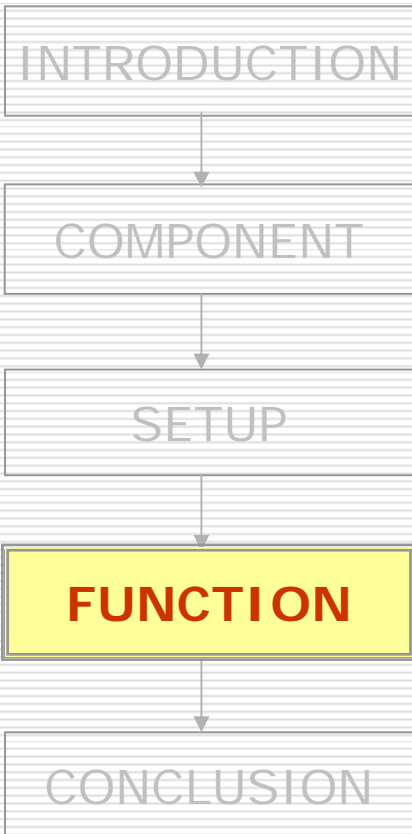


## 6. Media Transfer (1/3)

---

1. Both SC are on public IP address,
  - Media traffic flowed directly between them over **UDP**.
  - Size of voice packet was **67 bytes**.
  - Roughly **140 voice packets** were exchanged both ways in one second.
  - Total bandwidth used for voice traffic is **5 kilobytes/s**.

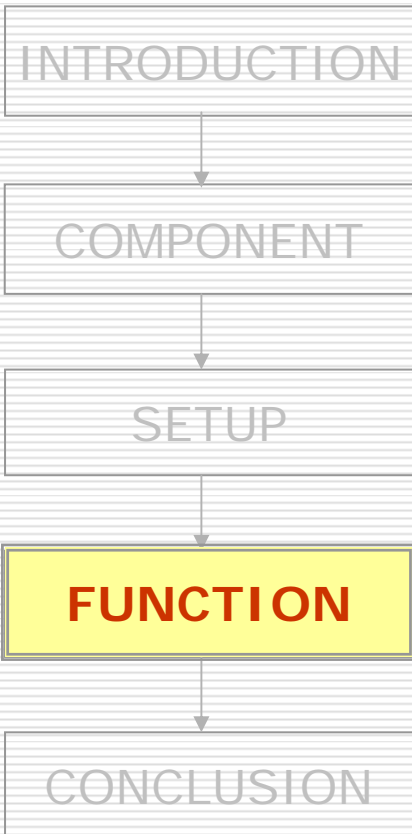




## 6. Media Transfer (2/3)

---

2. Either caller or callee was behind port-restricted NAT,
  - They sent voice traffic to another online Skype node over **UDP**.
  - A node acted as a **media proxy** and forwarded the voice traffic from caller to callee and vice versa.
  - Voice packet size was **67 bytes**.
  - Bandwidth used was **5 kilobytes/s**.



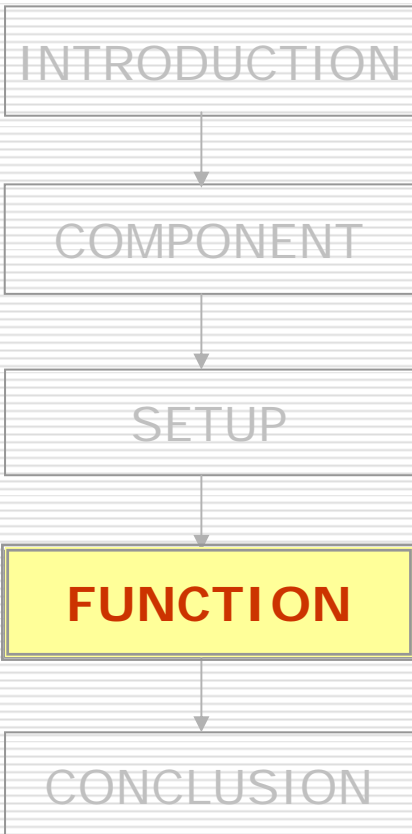
## 6. Media Transfer (3/3)

---

3. Both users were behind port-restricted NAT and UDP-restricted firewall,
  - They sent and received voice traffic over **TCP** from another online Skype node.
  - TCP packet payload size for voice traffic was **69 bytes**.
  - Total bandwidth used for voice traffic is about **5 kilobytes/s**.
  - SC used **TCP with retransmissions**.

## 6. Media Transfer: Silence Suppression

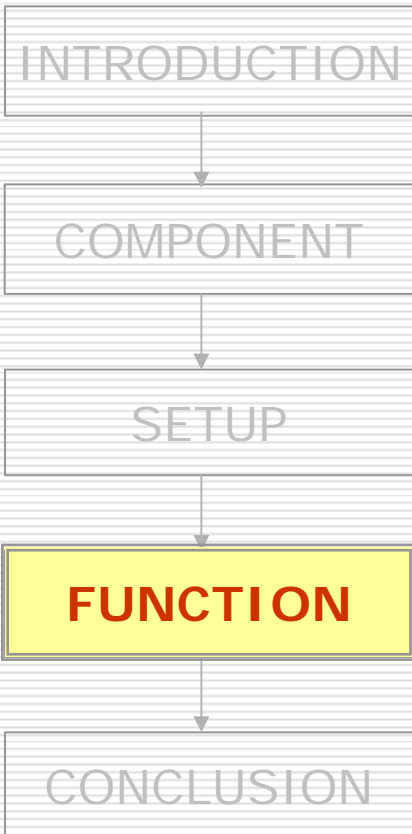
---



- ⑤ No silence suppression is supported in Skype.
  
- ⑤ Transmitting these silence packets has two advantages:
  1. It maintains the UDP bindings at NAT.
  2. These packets can be used to play some background noise at the peer.

## 6. Media Transfer: Putting a Call on Hold

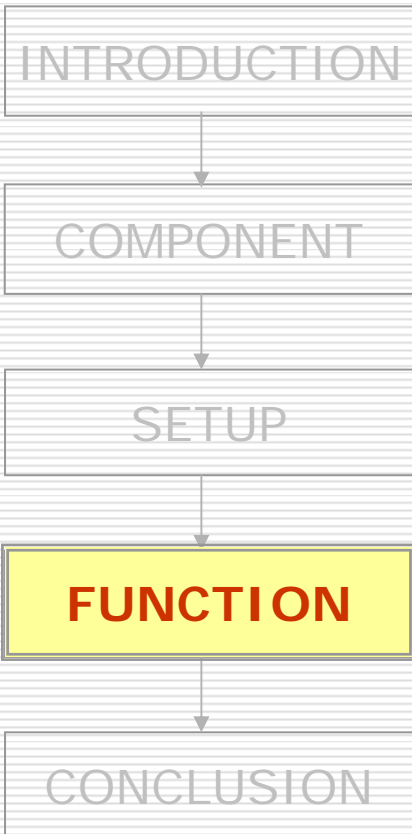
---



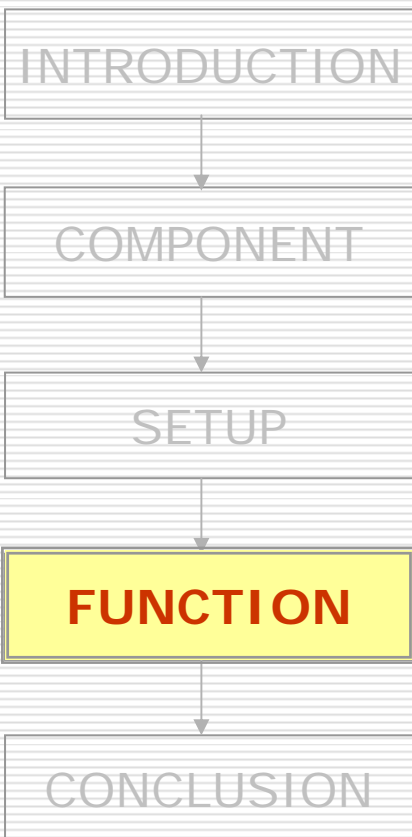
- ❶ Skype allows peers to hold a call.
- ❶ On average, a SC sent **three UDP packets per second** (and **periodic messages over TCP**) to the call peer, SN, or the media proxy when a call is put on hold.

## 6. Media Transfer: Congestion

---



- ⑤ We checked Skype call quality in a low bandwidth environment by using [NetPeeker](#) to tune the bandwidth available for a call.
- ⑤ We observed that uplink and downlink bandwidth of **2 kilobytes/s** each was necessary for reasonable call quality.



## 7. Keep-alive Message

- ③ We observed in for three different network setups that the SC sent a **refresh message** to its SN over TCP every 60s.

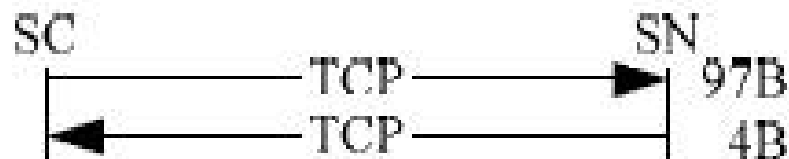
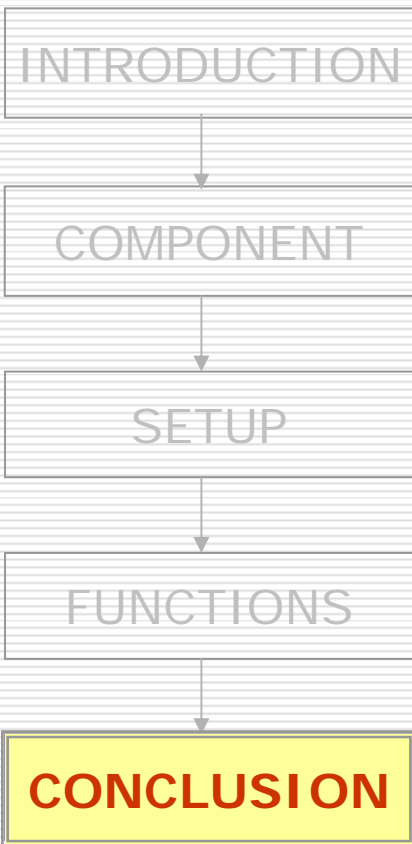


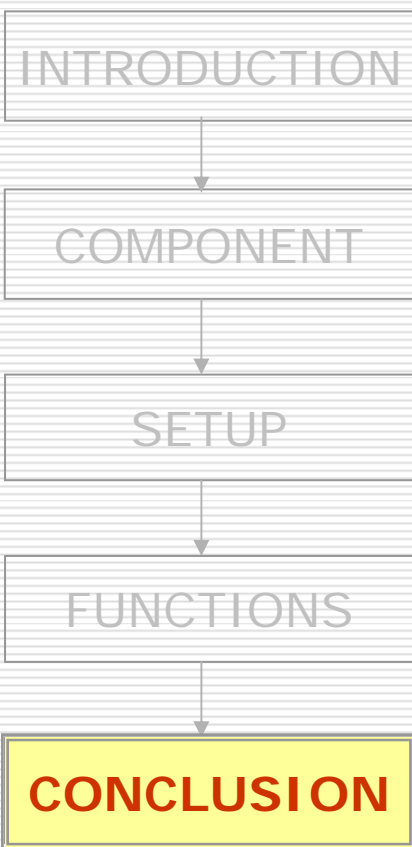
Figure 13. Skype refresh message to SN

CONCLUSION



1. Skype is the first VoIP client based on peer-to-peer technology.
2. Three factors are responsible for its increasing popularity:
  - 1) provideing better voice quality
  - 2) working almost seamlessly behind NATs and firewalls
  - 3) extremely easy to install and use





3. Skype uses TCP for signaling, and both UDP and TCP for transporting media traffic.
4. Skype communication is encrypted.
5. Skype has a central login server.
6. There is no global NAT and firewall traversal server.
7. Skype maintains reasonable call quality at an available bandwidth of 32 kb/s.

# Reference

- ⑤ vSkype-<http://www.festooninc.com/>
- ⑤ Skype-<http://www.skype.com/>
- ⑤ [http://toget.pchome.com.tw/intro/network\\_skype/24075.html](http://toget.pchome.com.tw/intro/network_skype/24075.html)
- ⑤ <http://www.google.com/talk/>
- ⑤ [http://zh.wikipedia.org/wiki/Google\\_Talk](http://zh.wikipedia.org/wiki/Google_Talk)

Thanks for your  
attention

Ⓢ HTTP 1.1 GET request

GET /ui/0/97/en/installed HTTP/1.1

User-Agent: Skype™ Beta 0.97

Host: ui.skype.com

Cache-Control: no-cache

Ⓢ response

HTTP/1.1 200 OK

Date: Tue, 20 Apr 2004 04:51:39 GMT

Server: Apache/2.0.47 (Debian GNU/Linux) PHP/4.3.5

mod\_ssl/2.0.47 OpenSSL/0.9.7b

X-Powered-By: PHP/4.3.5

Cache-control: no-cache, must revalidate

Pragma: no-cache

Expires: 0

Content-Length: 0

Content-Type: text/html; charset=utf-8

Content-Language: en



Ⓢ HTTP 1.1 GET request

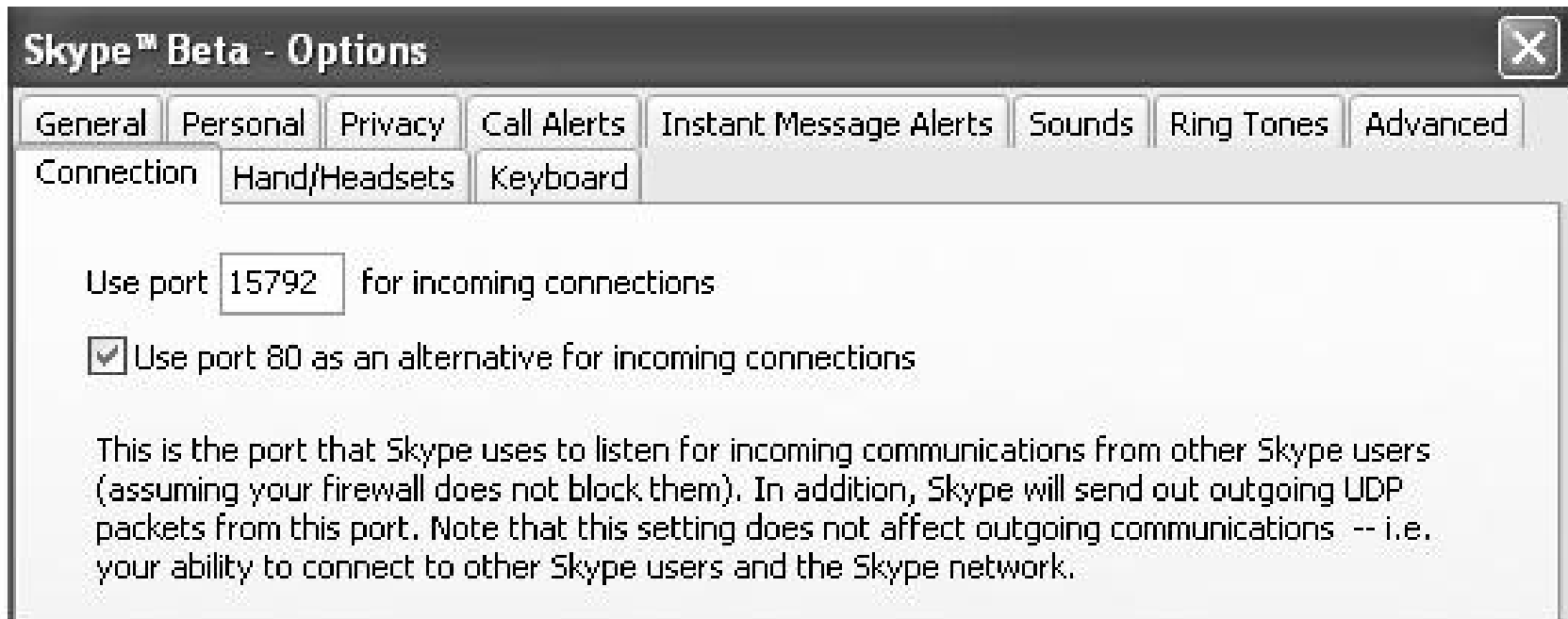
```
GET /ui/0/97/en/getlatestversion?ver=0.97.0.6 HTTP/1.1
User-Agent: Skype™ Beta 0.97
Host: ui.skype.com
Cache-Control: no-cache
```

Ⓢ response

```
HTTP/1.1 200 OK
Date: Tue, 20 Apr 2004 04:51:40 GMT
Server: Apache/2.0.47 (Debian GNU/Linux)
PHP/4.3.5 mod_ssl/2.0.47 OpenSSL/0.9.7b
X-Powered-By: PHP/4.3.5
Cache-control: no-cache, must revalidate
Pragma: no-cache
Expires: 0
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Content-Language: en
2
96
0
```



# Snapshot of HC of SC



# Bootstrap Super Nodes

IP address:port	Reverse lookup result
66.235.180.9:33033	sls-cb10p6.dca2.superb.net
66.235.181.9:33033	ip9.181.susc.suscom.net
80.161.91.25:33033	0x50a15b19.boanxx15.adsl-dhcp.tele.dk
80.160.91.12:33033	0x50a15b0c.albnxx9.adsl-dhcp.tele.dk
64.246.49.60:33033	rs-64-246-49-60.ev1.net
64.246.49.61:33033	rs-64-246-49-61.ev1.net
64.246.48.23:33033	ns2.ev1.net




PChome Online 網路家庭-下載 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)


Google 搜尋 我的最愛 媒體 8 已擷載 檢查 選項 網址(D) http://toget.pchome.com.tw/intro/network\_skype/24075

PChome > Toget 下載 > 網路應用 > Skype工具 > vSkype

請輸入關鍵字 關鍵字搜尋 搜尋 進階搜尋


**vSkype**

版本更新回報



軟體分類：	Skype工具
軟體性質：	Freeware
更新日期：	2005-07-04
最近版本：	beta
作業系統：	Windows 2000
語言界面：	英文
購買金額：	N/A
試用限制：	N/A
原創公司：	<a href="#">SANTA CRUZ NETWORKS</a>

**vSkype — 用Skype多人同時視訊對談**

vSkype不但可讓你用Webcam與朋友直接在Skype中看到彼此的即時影像，更可支援6人同時上線進行語音與視訊的同步會議，不但畫質清晰且佔用的頻寬也不大，相當適合一般ADSL用戶網路環境。此外還可直接傳送電腦桌面或程式的畫面給對方，讓雙方視訊溝通

廣告



KKBOX  
動態歌詞 讓你  
成為K歌王

**CEO Stuart Jacobson says, "vSkype adds two cool new experiences to a Skype user: multi-user video and desktop sharing."**

網際網路 下午 05:43

