

## 上网行为管理 协议分析系列

### —— SKYPE 协议分析

**相关主题:** 上网行为管理,PatrolFlow,信息安全网关,带宽管理,流量控制,P2P 控制,BT 下载,邮件监控,IM 控制,游戏监管,聊天监控,内容审计,多链路负载均衡,Web 推送,防火墙,防毒墙

正文内容:

#### 1、概述

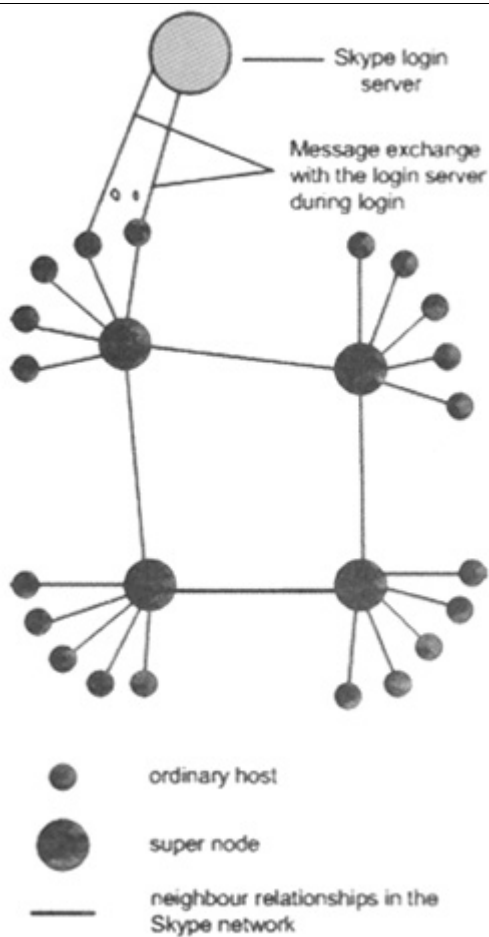
Skype 是由 Kazaa 于 2003 年发明的基于 P2P 技术的 VoIP 客户端，用户可以通过 Skype 通过互联网进行语音和文本的传输。Skype 的通讯协议是不公开的，而且通讯内容是加过密的，哥伦比亚大学的 Baset 和 Schulzrinne 完全在实验的基础上对 Skype 的通讯机制 进行分析，通过分析得出的结论主要有三个：

- (1) Skype 的通话质量较 MSN 和 Yahoo 的即时通信工具要好；
- (2) 可以无缝的在 NATs 和防火墙后使用；
- (3) 安装使用起来非常简单。

#### 2、Skype 的网络结构

Skype 的节点有两种：客户端（ordinary node）和超级节点（super node，SN）。客户端必须链接到超级节点，并且在 Skype 的中央服务器登录。中央服务器保存用户的用户名和密码，完成登录的认证工作。图 1 中的小黑点是客户端，大黑点是超级节点（用于为其它客户端提供登录跳板及广播服务），灰色的点是 Skype 的登录服务器。

Skype 可以看作是一个叠加在互联网之上的网络。与以往 MSN 等 IM 工具最大的不同在于其除了用户登录，其余工作基本不依赖中央服务器。Skype 在穿透防火墙通讯时完全使用了 Peer to Peer，而没用到中央服务器。每一个客户端都维护一个可以到达的主机列表（host cache，HC），包括其 IP 地址和端口号。



### Skype 的网络结构

用户下载安装完 Skype 后，Skype 客户端会发送一段 HTTP 1.1 的请求到中央服务器，告诉它我装完了一个什么样的版本，服务器会返回一个 200 OK 的信息。客户端会进行登录初始化工作，针对三种不同类型的网络情况有三种不同的登录方式：

- (1) 直接有公众网的 IP
- (2) 在内部网，可以通过 TCP 访问外部网络
- (3) 在内部网，但只能通过有限的几个端口（例如 80 和 443）访问外部网络

Skype 在登录的时候会先使用 UDP 请求 HC 中的 IP，如果不行，就用 TCP 请求 HC 中的 IP 及端口，如果还不行。就用 TCP 请求 HC 中的 IP 及 80 端口，如果又不行，就再请求 HC 中的 IP 及 443 端口。如果这时候还不行，那就登录不了了。整个过程中传输的数据量大概在 8k-10k，持续的时间在 3 至 35 秒。

## 3、Skype 的主要组成部分

### 3.1 端口

在 Skype 的连接属性对话框中可以设置监听的端口号，在安装的时候 Skype 会随机的选择一个端口作为监听的端口，这一点与 HTTP 协议等不同，Skype 没有默认的服务端口。同时，它还会打开对 80 和 443 端口的监听。80 是常见的 HTTP 服务默认端口，而 443 则是 HTTPS 服务的默认端口。

### 3.2 主机列表

这里的主机指的是可以提供跳板及广播服务的 SN 的 IP 地址和端口号，这是 Skype 最重要的部分之一，HC 中至少要有一个可用的主机地址和端口号。通常它被存储在注册表里的 HKEY\_CURRENT\_USER/SOFTWARE/Skype/PHONE/LIB/CONNECTION/HOSTCACHE 中。一般情况下，在 Skype 运行两天后，HC 中的 SN 地址及对应的端口号会达到约 200 个。

### 3.3 编解码器

Skype 采用了 iLBC、iSAC 和一个保密的编解码器，能够对 50-8,000 Hz 范围内的语音信号进行编码。Global IP Sound 已经实现了 iLBC 和 iSAC 编解码器，其网站表明了 Skype 是他们的合作伙伴。由此来看 Skype 应该是使用了 Global IP Sound 的编解码器实现的语音通讯。

### 3.4 好友列表

Skype 的好友列表没有保存在服务器上，而是保存在本地的注册表中，并进行了加密。这就使得用户如果更换了另外一台电脑之后需要重新构建好友列表。

### 3.5 加密

Skype 使用 AES (Advanced Encryption Standard) 加密标准，这也是美国政府使用的一个加密标准。Skype 采用了 256 比特加密，可能的密钥有  $1.1 \times 10^{77}$  个。

### 3.6 NAT 与防火墙

Skype 应该是使用了 STUN 和 TURN 协议来检测所处的 NAT 及防火墙环境。Skype 定期的刷新这些信息，这些信息也是存储在注册表中的。与另外一个点对点文件共享系统 Kazza 不同，普通客户端无法阻止自己成为 Super Node (SN)，就是说它随时可能被征用成为别人登录服务和广播服务的提供者，就是类似于 BT 中的种子提供者的角色。

## 4、Skype 的主要功能

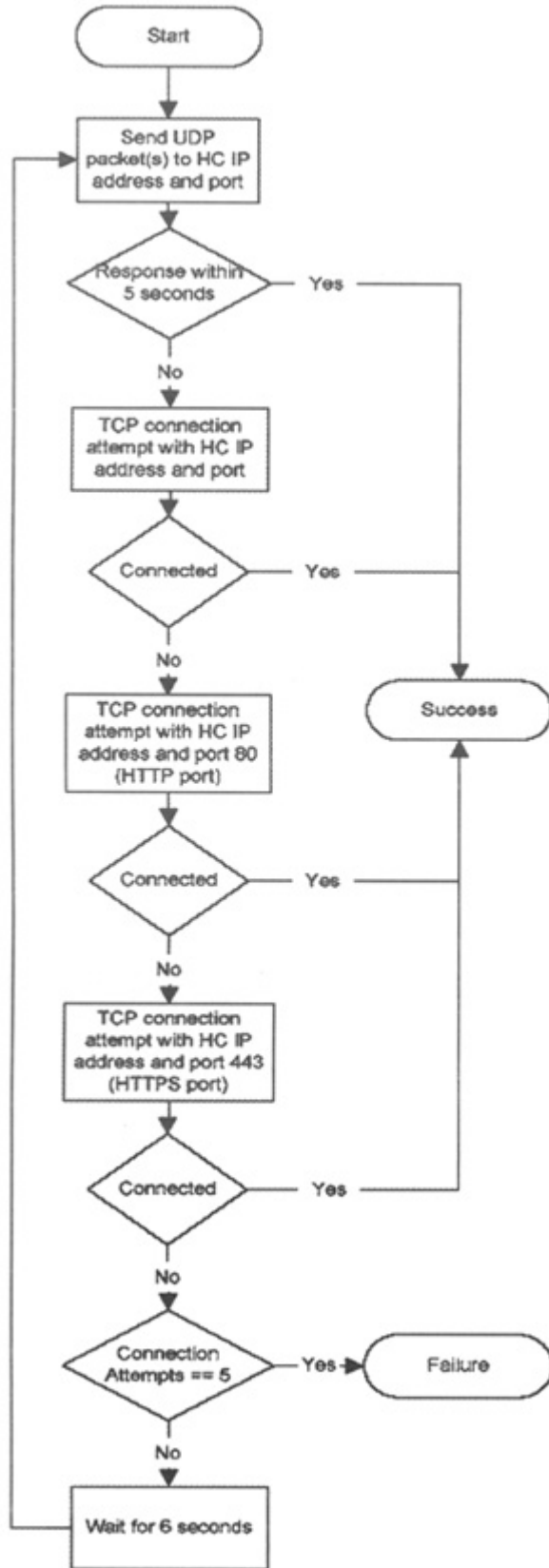
Skype 的功能主要可以分为：初始化，登录，用户搜索，呼叫建立与终止，媒体传输和状态消息。

### 4.1 初始化

第一次安装后，Skype 会发送一段 HTTP 1.1 的请求给中央服务器，包括关键字“installed”以及所装 Skype 的版本号。以后的每次登录 Skype 都会向中央服务器发送一小段包含关键字“getlatestversion”的 HTTP 1.1 请求，检查是否有新版本的 Skype。

### 4.2 登录

登录是 Skype 最重要的功能，如图 2 所示。在这个过程中，Skype 终端到登录服务器上验证用户名密码，广播给在线上的好友及其它节点，检查 NAT 和防火墙的类型，发现拥有公网 IP 地址的在线 Skype 节点，这些新发现的节点被用于在所在 Super Node 无法使用后继续保持本机与 Skype 网络的连接。如果 HC 中所有的节点地址均不可用的话，登录失败。通过分析这些登录失败的过程，我们可以得出一个完整的 Skype 登录过程：



### Skype 的登录过程

先发送 UDP 数据包，如果 5 秒后没有响应，就用 TCP，发送登录请求到目标节点的 80 端口；如果仍然失败，就通过 TCP 发送登录请求到 443 端口，等待 6 秒钟，如果仍然失败就显示无法登录。整个的登录过程可以重复 4 次。连接的对象是保存在本机中 Host Cache 中的节点列表。

#### 4.3 用户搜索

Skype 使用全球索引 (Global Index, GI) 技术进行用户搜索，在 72 小时内登录过的用户，无论是处在公众网还是私有网络中都能找到。客户端可以通过发送 TCP 包向 SC 发送请求，也可以通过 UDP 包向其他 SC 发送查询请求。SC 将结果发回客户端。

#### 4.4 呼叫建立与终止

Skype 采用了 32kbps 的语音编码以保证语音质量，其信令通过 TCP 传递，而语音数据则通过 TCP 和 UDP 进行传输，信令和语音数据使用不同的端口号。Skype 能够向好友列表中的用户发送呼叫请求。为了保证信令传输的可靠性，信令始终是通过 TCP 进行的。如果双方都是在公众网中，有独立的公用 IP，那么主叫用户和被叫用户通过 challenge-response 机制直接进行数据交换。如果有一方位于私有网络或者是防火墙之后，那么私有网络一方需要首先同公众网中的至少一个 SN 建立 TCP 链接，然后由 SN 进行数据转发。如果双方都位于私有网络中，那么双方的数据都需要 SN 进行转发。

#### 4.5 媒体传输和状态消息

如果双方都位于公众网中，双方可以使用 UDP 包直接进行数据交换。Skype 的语音数据包的大小一般是 67 bytes，正好是 UDP 包的净荷。对于 100M bps 的以太网来说，每秒可传送 140 个语音数据包。一般来说，上下行语音传输所需的平均带宽为 5 kbps。如果有其中一方或者双方都位于私有网络中，就需要通过 TCP 同 SN 进行数据交换，由 SC 充当媒体代理服务器的角色，此时一个语音数据包的大小一般为 69 bytes。在可能的情况下，Skype 会优先选择 UDP 协议进行通信。

### 5、结束语

Skype 是第一个利用 P2P 技术进行语音通信的 VoIP 工具，能够提供较好的通话质量。Skype 能够透过防火墙进行无缝通信，安装使用也很简单。随着互联网的不断普及。VoIP 技术已经取得了越来越多的应用。有的运营商甚至开始和 Skype 合作提供语音服务，这是一个新的趋势。如何在新技术不断普及的同时保证运营商在传统通信网络中的核心地位，是一个值得研究的课题。

更多信息请登录 <http://www.byzoro.com>