Skype and JANET

March 2006

Skype: a Definition

UKERNA defines Skype as ‘a proprietary, peer-to-peer resource discovery, directory access, and call signalling protocol.’

Introduction

Skype is a worldwide phenomenon that offers a Voice over IP service based on a free-to-download voice client and a central register of all Skype users. Skype was developed by the originators of, and reuses many of the concepts of, the KaZaa peer-to-peer file-sharing system.

Additional charged-for services are also offered, such as voicemail, SkypeOut (portal to landlines and mobiles) and SkypeIn (a traditional number that a Skype user can be contacted on). Handsets have been manufactured for the use with Skype that can be connected into computers. Skype is also developing a mobile offering as well as bundling video support into the new version of its software.

Skype has developed clients for the Windows, Macintosh, Pocket PC and Linux operating systems, all available for download from their website. Skype states that at the time of writing 254,029,431 users have downloaded a client.

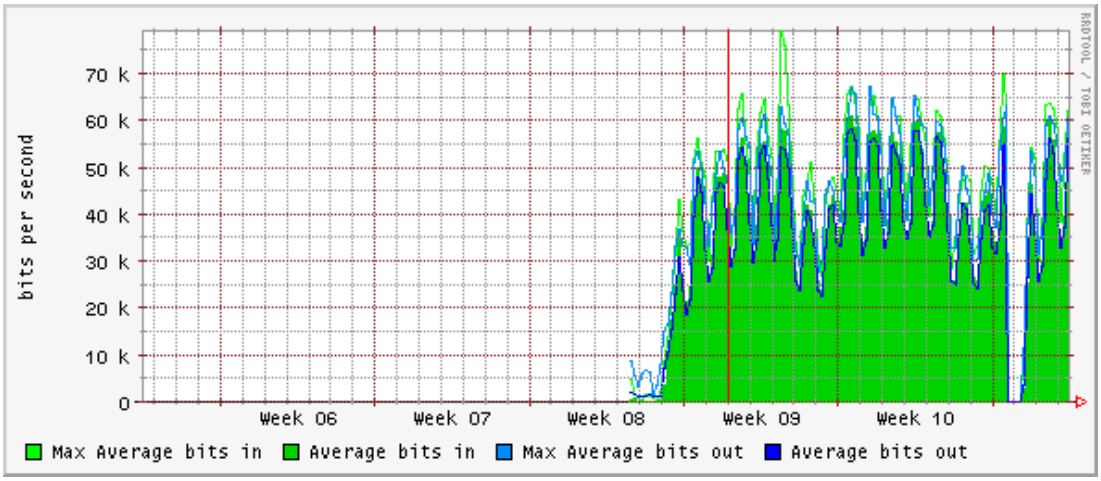
On installing the client, a user is asked for a username and password. If the username has already been claimed then an alternative is offered, ensuring that all usernames are unique. Once the user has logged in, they can locate other users on the central Skype register and take part in an audio call across the Internet. Call quality is generally good, though it can be erratic at times.

The popularity of this software has led UKERNA’s VAG (Voice Advisory Group) to investigate its engineering and any implications for JANET. Two features of Skype – its use of bandwidth and encrypted tunnels – raise particular concerns.

Use of Bandwidth

The Skype system adapts dynamically to the network environment it finds. As with KaZaa, Skype may conclude that the most effective way to route a communication is not directly between the called and calling endpoints, but instead to send the traffic via another Skype client not otherwise involved in the call. An intermediary client used in this way is known as a super-node. Super-nodes are not pre-defined or configured, but are a dynamic feature of the Skype client software. Any Skype client that discovers it is well connected to the Internet is likely to offer itself as a super-node by advertising its connectivity to other Skype users. As a result, a PC that has access to significant bandwidth and runs the Skype client software may handle voice communications to and from clients all over the world, not just those originating or destined for the local user of the PC. Networks with super-nodes may experience large flows of inbound and outbound traffic that have no connection with any local user. A user who installs Skype with the default configuration permits his computer and his organisation’s bandwidth to be used by any other Skype user.

In order to investigate the impact of this behaviour, the Skype client was installed on a PC connected to JANET at a network speed of 1Gbit/s. No calls were made either to or from this PC, nor were any other applications running on it. The graph below shows the network traffic that resulted over a two week basis. It should be noted that the drop in traffic at the end of week 10 resulted from the endpoint shutting down.



Further investigation of this traffic showed that the Skype client, which had apparently decided to act as a super-node, was maintaining between 660 and 690 open connections to different hosts. A snapshot of router flows indicated that in a period of 24 hours the client PC had a total of 319,314 flows to or from it and talked to a total of 38366 different IP addresses. These IP addresses were located in 2763 different network domains (Autonomous System numbers). Clearly even an idle Skype client, if in active call mode (that is, the client is registered with the central register and able to make and receive calls), may generate significant network traffic by acting as a proxy for other Skype traffic.

Although the Skype protocols and behaviour are proprietary, researchers at Columbia University have analysed the traffic from one version of the software to obtain technical details. Their analysis, which is referenced with permission, can be found at:

http://arxiv.org/ftp/cs/papers/0412/0412017.pdf

It has also been reported that placing Skype behind a default deny firewall prevented super-node behaviour while still allowing calls to be made and received using web protocols.

Encrypted Tunnels

A feature of Skype that may be very welcome to its users is that all communications are encrypted end-to-end between the two communicating clients. However, while it may be desirable to prevent telephone conversations being tapped, the encryption also applies to all other Skype activities such as file transfer and chat. This means that any filtering or protection for the user or their PC that is implemented on the organisation's firewall or network will be unable to inspect files or other content transferred to the Skype client. Skype effectively provides an encrypted tunnel through the firewall that could be used for attacks against the client PC and any other networked devices it can connect to in turn. Users and PCs must therefore be able to protect themselves against inappropriate or malicious content including viruses and other malware, or even attacks against the Skype system itself, without any assistance from other systems. Skype also provides a mechanism for third party software to be written and installed within the system: the history of the equivalent function in web browsers suggests that this will be used at least as often by insecure and unwelcome software as by useful applications.

Skype and the JANET Acceptable Use Policy

Two sections of the JANET Acceptable Use Policy may apply to Skype. Section 9.7 of the Policy prohibits:

'deliberate activities with any of the following characteristics:

- wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems; …

- using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)'

Section 11 of the Policy prohibits 'provid[ing] access to JANET for third parties without the prior agreement of UKERNA', but permits a limited amount of such use provided this is regulated by the customer organisation.

Uncontrolled use of Skype, and particularly its bandwidth-hungry super-node behaviour, is likely to breach one or both of these sections.

Managing SKYPE Usage

Skype, like most other network applications, has risks as well as benefits. JANET-connected organisations should therefore consider how they manage Skype – to protect their own network availability and that of others, to ensure that filters for hostile and inappropriate material remain effective and to comply with the JANET Acceptable Use Policy. There are a number of ways in which this can be done:

Local Policy

The organisation may state in its local Acceptable Use Policy that the download and use of Skype is restricted. Use may be banned, or only permitted on hosts that are managed and used in such a way that the risks can be controlled.

User Education

A Skype client can only act as a super-node if it is enabled. Closing the Skype application after use will prevent it becoming a super-node; however, this also means that the client will not be able to receive any incoming calls without prior arrangement. The default installation of Skype is such that it starts and becomes resident as soon as the system is started. It is advisable to change this default behaviour.

Firewall

Organisations may be able to block or restrict the ports used by Skype on a firewall or router. Limiting the total bandwidth that can be consumed by traffic to and from the Skype ports may be effective both in protecting other uses of the network and preventing super-nodes appearing. It should be noted that in some cases the ports used by Skype change when a new software version is released. It has been reported that a Skype client can make and receive calls using only the SSH, Socks, HTTP or FTP ports, but that super-node behaviour does not occur under these restrictions.

Any host on which the Skype client is run should have anti-virus software and security patches installed and kept continually up to date. Anti-virus checking that occurs when files are opened or executed, as well as on disk, is essential. Users must also be made aware of the potential risks of using Skype to themselves, their machines and others.

Finally, Skype is not the only Internet telephony system. Alternatives that are standards-based may prove easier to manage and provide a more predictable service.

Acknowledgements

This document has been jointly created by UKERNA and representation form UCISA-NG

Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Microsoft, NetMeeting and Explorer are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

© The JNT Association 2006

JISC