

# Qtel's Guide to a Faster Internet Experience

[www.qtel.com.qa](http://www.qtel.com.qa)



# Contents

Preface

Third Party Modem Configuration

Wireless Security

Impacts of Unsecured Wireless Network

Shared Connection

Peer-to-Peer (P2P) Applications

Worms / Virus Generating Traffic

PC Performance

PC Etiquette

Stay Safe

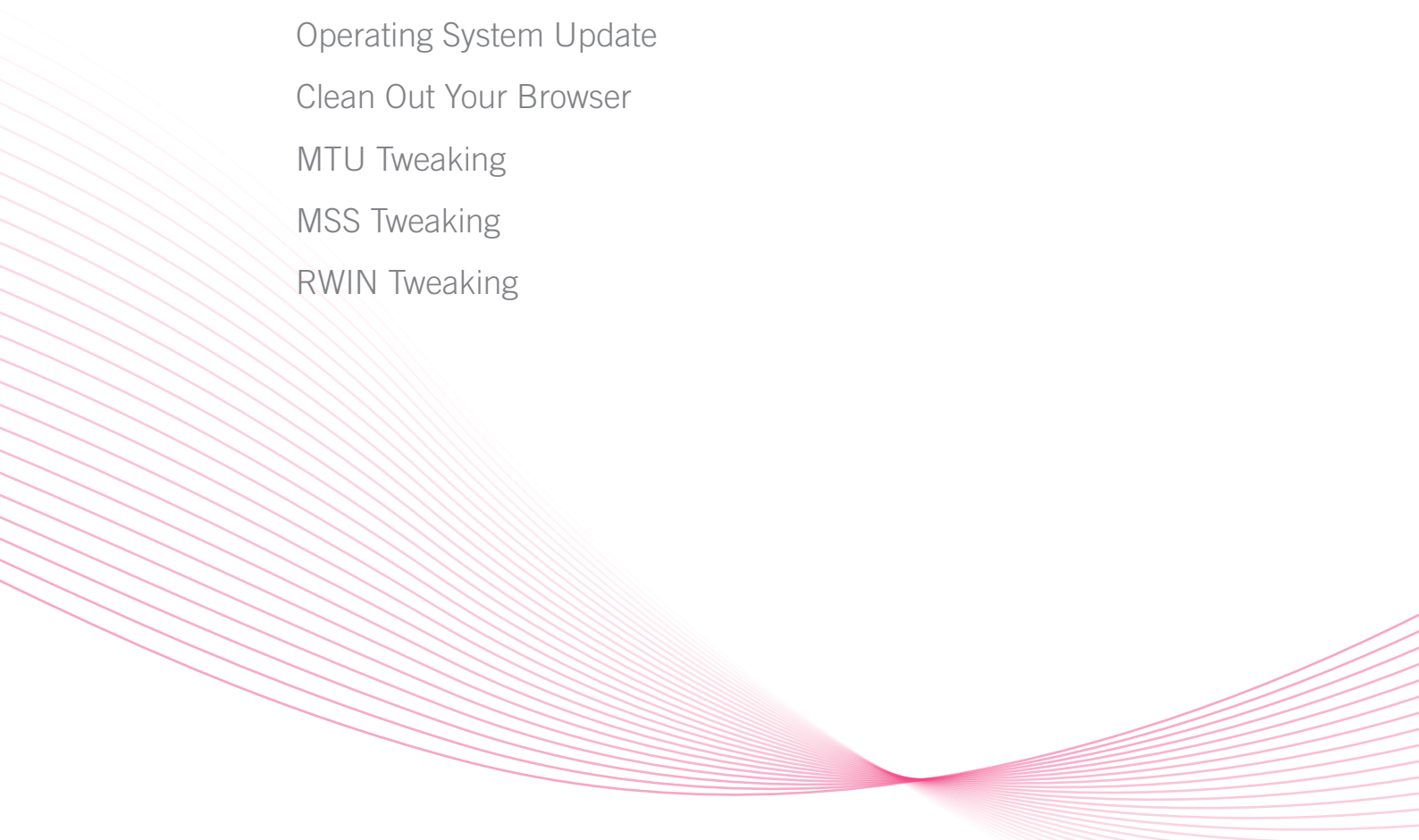
Operating System Update

Clean Out Your Browser

MTU Tweaking

MSS Tweaking

RWIN Tweaking



# Preface

## **What is this manual all about?**

This manual is designed to help customers improve the performance of their home computer, and features a range of hints and tips developed by Qtel's network teams specifically to meet the needs of people in Qatar.

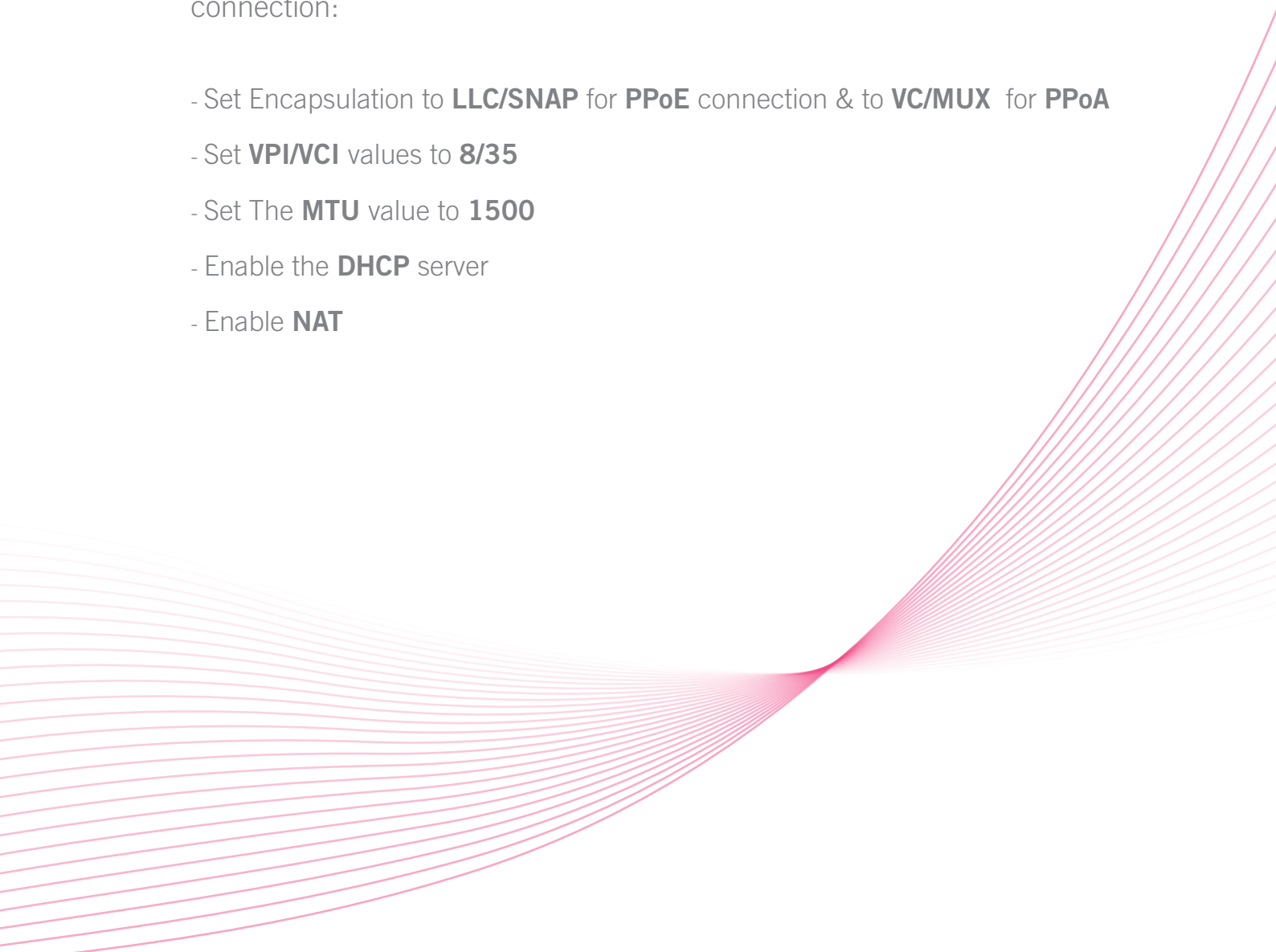
Qtel conducted a wide-ranging analysis Internet performance issues in Qatar in 2008, looking at areas where customers wanted stronger performance. One of the key findings was that, despite Qatar having one of the most robust networks in the region, many customers were not fully benefiting from the full speed and reliability of the available Internet connectivity because of challenges in the customer environment.

As a proactive response to these issues, Qtel has developed this step-by-step guide to tackling issues ranging from configuring a modem correctly, through to cleaning a computer hard drive of malware and infections.

This manual should help you enjoy a faster Internet experience.

# Third Party Modem Configuration

The following are a few points that can be crosschecked for a good connection:

- Set Encapsulation to **LLC/SNAP** for **PPoE** connection & to **VC/MUX** for **PPoA**
  - Set **VPI/VCI** values to **8/35**
  - Set The **MTU** value to **1500**
  - Enable the **DHCP** server
  - Enable **NAT**
- 
- A decorative graphic consisting of numerous thin, parallel red lines that curve and flow from the bottom left towards the top right, creating a sense of motion and depth.

# Wireless Security

## **What does it mean?**

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks.

## **Why is it important?**

Wireless networks are vulnerable in a myriad of ways, some of the most likely problems being rogue access points (APs) and employee use of mobile devices without appropriate security precautions, but malicious hacking attempts and denial-of-service (DoS) attacks are certainly possible as well.

Unlike traditional wired networks in which communications travel along a shielded copper wire pair or optical cable, wireless radio frequency (RF) signals literally traverse the open air. As a result, RF signals are completely exposed to anybody within range and subject to fluctuating environmental factors that can degrade performance and make management an administrative nightmare. Whether authorized or not, wireless access points and their users are subject to malicious activity and employee misuse.

# Impacts of Unsecured Wireless Network

## **Real-time Traffic is Compromised**

- People can see what Web sites you're visiting.
- Login information to unsecured sites (non-SSL) is compromised, along with the content.
- Login information and content from services such as POP3 e-mail accounts and FTP connections is compromised.

## **Network is Open for Others to Connect**

- Your internet connection may be used for sending and/or receiving illegal information
- Others can access any shared files on PCs or servers connected to the network.

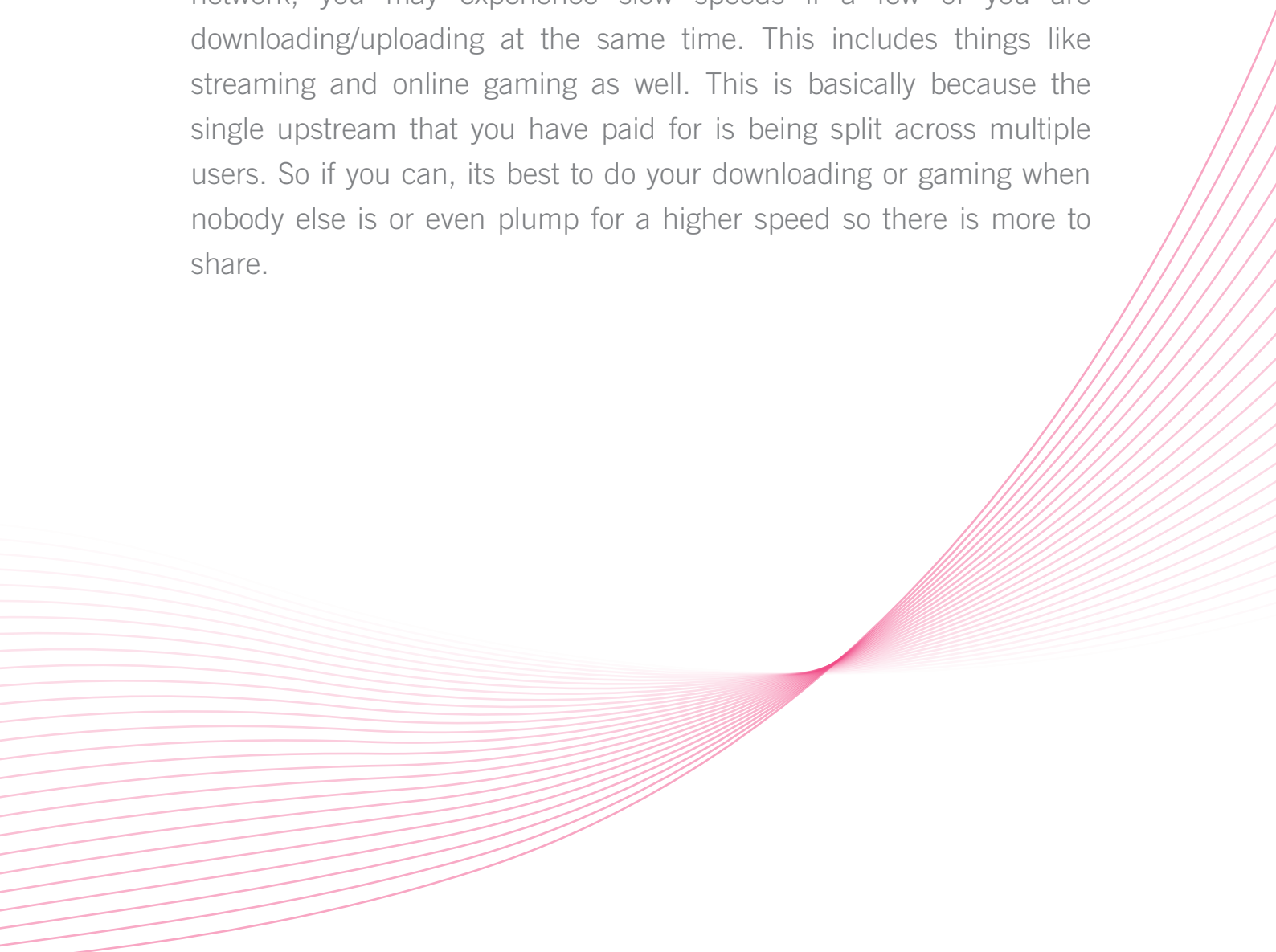
## **Slow Performance**

An ISP (Internet service provider) only provides you with a certain amount of external bandwidth - some maximum number of bits per second that can flow between the LAN (local area network) in your home or small office and the WAN (wide-area network) that we know as the Internet. Activities such as checking email, surfing the Web, transferring files, streaming music and video, and playing multiplayer games will all demand portions of that limited bandwidth. Too many users hogging that bandwidth can easily cause poor performance with those network tasks.

# Shared Connection

(more than one end user scenario)

If you are part of a household where you share your broadband connection with other users, maybe via a wireless router of home network, you may experience slow speeds if a few of you are downloading/uploading at the same time. This includes things like streaming and online gaming as well. This is basically because the single upstream that you have paid for is being split across multiple users. So if you can, its best to do your downloading or gaming when nobody else is or even plump for a higher speed so there is more to share.



# P2P Applications

## How does it Work?

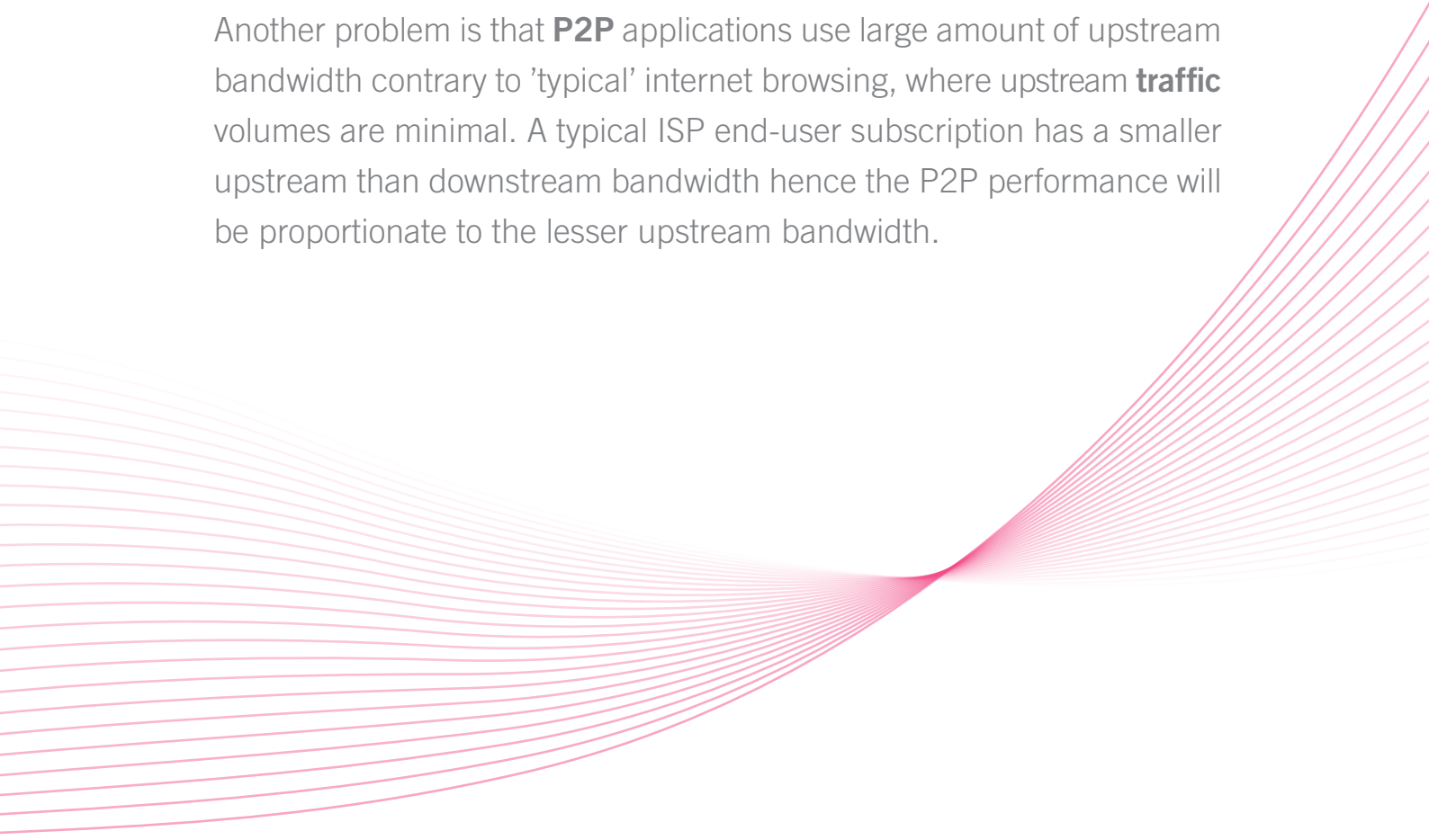
A P2P network does not have the notion of clients or servers but only equal **peer** nodes that simultaneously function as both "clients" and "servers" to the other nodes on the network. This model of network arrangement differs from the client-server model where communication is usually to and from a central server. A typical example of a file transfer that is not P2P is an FTP server where the client and server programs are quite distinct, the clients initiate the download/uploads, and the servers react to and satisfy these requests.

In an unstructured P2P network, if a peer wants to find a desired piece of data in the network, the query has to be flooded through the network to find as many peers as possible that share the data. The main disadvantage with such networks is that the queries may not always be resolved. Popular content is likely to be available at several peers and any peer searching for it is likely to find the same thing. But if a peer is looking for rare data shared by only a few other peers, then it is highly unlikely that search will be successful. Since there is no correlation between a peer and the content managed by it, there is no guarantee that flooding will find a peer that has the desired data. Flooding also causes a high amount of signaling traffic in the network and hence such networks typically have very poor search efficiency.

## Performance Impact

The most common Internet connection offered to end users is a "shared" line. This means that a certain bandwidth, for example 10Mbps, is shared between a group of subscribers. If one or several of these use **P2P** applications, the rest will have less bandwidth for their use. This means that a small number of users "hog" a large portion of the available bandwidth. "Bandwidth Hogging" leads to an unequal situation between users that have identical Internet connection subscriptions.

Another problem is that **P2P** applications use large amount of upstream bandwidth contrary to 'typical' internet browsing, where upstream **traffic** volumes are minimal. A typical ISP end-user subscription has a smaller upstream than downstream bandwidth hence the P2P performance will be proportionate to the lesser upstream bandwidth.



# Worms / Virus Generating Traffic

A **computer worm/virus** is a self-replicating computer program. It uses a network connection to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth.

Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, the amount of network traffic and other unintended effects can often cause major disruption.

Worms spread by exploiting vulnerabilities in operating systems. All vendors supply regular security updates, and if these are installed to a machine then the majority of worms are unable to spread to it. Users need to be wary of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails. Antivirus and antispymware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended.

# PC Performance

## **PC Etiquette**

Refresh the desktop after closing any application. This will remove any unused files from the RAM. Do not set very large file size images as your wallpaper. Do not keep wallpaper at all if your PC is low on RAM (less than 64 MB). Do not clutter your Desktop with a lot of shortcuts. Each shortcut on the desktop uses up to 500 bytes of RAM. Empty the recycle bin regularly. The files are not really deleted from your hard drive until you empty the recycle bin. Delete the temporary internet files regularly. Defragment your hard drive once every two months. This will free up a lot of space on your hard drive and rearrange the files so that your applications run faster.

## **Stay Safe**

Your security program should be set to automatically retrieve updates to protect against malicious programs, like viruses. To check this, open your security program and examine the settings. The option to select automatic updates should be labelled. Set it to update weekly, at least.

## **Operating System Update**

Providing its set up to get them, your computer should be receiving weekly automatic updates from the Microsoft Windows Update website at <http://windowsupdate.microsoft.com>. These updates contain crucial changes to protect your Windows system against security threats.

It will also say whether critical updates are installing properly. Visit the site to view other useful updates for refreshing your computer.

You could look at downloading upgrades to Microsoft Office programs and device drivers – the software that allows your computer to talk to your peripherals like your mouse, printer, camera or webcam.

### **Clean out your browser**

Clear some space on your hard disk and protect your privacy by clearing out your cache and cookies.

These refer to files saved onto your computer when you surf the internet. Both hold details about sites you've visited. They also make surfing the internet quicker.

Click Tools > Internet Options > General tab. Under Browsing history, click Delete. To clear your cache click Delete files. Click Delete cookies to get rid of them too then > OK.

### **MTU Tweaking**

In computer networking, the term MTU refers to the size of the largest packet or frame that a given layer of a communications protocol can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc.). The MTU may be fixed by standards (as is the case with Ethernet) or decided at connect time (as is usually the case with point-to-point serial links). A higher MTU brings higher bandwidth efficiency. For Ethernet, it's 1500 (1514 if you include the MAC header), but may vary depending on the broadband connection or use of VPN.

## **MSS Tweaking**

The **maximum segment size (MSS)** is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the headers must not add up to more than the number of bytes in the maximum transmission unit (MTU). Maximum Segment Size - depends on the protocol, so for any protocol  $MSS = MTU - \text{hdr\_sz}$  (where  $\text{hdr\_sz}$  is the protocol header size).

## **RWIN Tweaking**

The amount of data that can be received before the receiver must ACK. If the sender has sent more than receive window it will stop sending until the receiver ACK's enough packets to bring the amount of outstanding packets back within the receive window. Should be greater than 63000 and not a factor of the MTU value.

