

## Thomson Gateways and UPnP

**Date:** April 2007

**Version:** v3.0

---

**Abstract:** This application note provides technical information on UPnP support in Thomson Gateway products. First, a general introduction will explain what UPnP is exactly. Secondly, the Internet Gateway Device concept as defined by the UPnP working group is made clear. Finally, support in the Thomson Gateway product range is presented as well as support in operating systems like Windows XP and how they work together.

**Applicability:** This application note applies to all THOMSON DSL Gateways and Routers.

**Updates:** THOMSON continuously develops new solutions, but is also committed to improving its existing products.

For more information on THOMSON's latest technological innovations, documents and software releases, visit us at <http://www.thomson-broadband.com>

<b>1</b>	<b>Universal Plug and Play: Introduction .....</b>	<b>3</b>
1.1	<b>The Concept .....</b>	<b>3</b>
1.2	<b>UPnP Model and Mechanism .....</b>	<b>4</b>
1.3	<b>UPnP AV .....</b>	<b>6</b>
<b>2</b>	<b>UPnP and Network Address Translation (NAT).....</b>	<b>7</b>
2.1	<b>The Concept .....</b>	<b>7</b>
2.2	<b>Problems Encountered by NAT .....</b>	<b>8</b>
2.3	<b>Solution: NAT Traversal .....</b>	<b>9</b>
<b>3</b>	<b>UPnP Support in Operating Systems .....</b>	<b>10</b>
<b>4</b>	<b>Using UPnP with the Thomson Gateway .....</b>	<b>11</b>
4.1	<b>Windows ME.....</b>	<b>11</b>
4.2	<b>Windows XP .....</b>	<b>12</b>
4.2.1	Control and Eventing .....	14
<b>5</b>	<b>UPnP and Security .....</b>	<b>17</b>
<b>6</b>	<b>UPnP Tweaking via the CLI.....</b>	<b>19</b>
6.1	<b>UPnP CLI Commands .....</b>	<b>19</b>
6.1.1	system config upnp enabled/disabled .....	19
6.1.2	upnp config .....	20
6.1.3	upnp list.....	20
6.2	<b>CLI Tracing .....</b>	<b>21</b>

# 1 Universal Plug and Play: Introduction

## 1.1 The Concept

### What is UPnP?

The term UPnP brings to mind the well-known Plug and Play concept. Plug and Play was launched a few years ago to help users **install** and **configure** computer peripherals such as printers and web cams without any hassle. The idea is: just plug in the device, and it is ready to use.

UPnP now extends the Plug and Play concept to the **networking** environment. UPnP is designed to automate the installation and configuration of a (small) network as much as possible. This means that UPnP capable devices can join and leave a network without any effort of a network administrator. As a matter of fact, for the small networks that typically exist in the residential home or SOHOs, there is mostly no knowledgeable administrator.

Moreover, UPnP capable devices can offer the user **services** and inform him about them, making it easy to benefit from these services. In addition, controlling these devices can be automated. Should manual control still be preferred, this is conveniently possible from a single location.

### Examples: UPnP in Your Home

Let's take a look at a few examples.

If a UPnP **printer** is connected to the network:

- > It is automatically installed with the proper drivers (part of the normal Plug and Play feature).
- > It broadcasts its presence and makes itself accessible throughout the network without further hassle.

So Dad's new colour printer in Dad's study will simply pop up on the computer screen in his son Pete's room, ready to print his homework.

Other networking areas, such as **home entertainment**, can benefit from UPnP as well:

- > As Mum is changing her clothes after a hard day's work, she gets intrigued by the cooking program on the (UPnP enabled) bedroom TV.
- > With the UPnP TV remote control, she starts the living room video recorder to record the program that is on her TV screen.
- > With the same remote control, she puts an entry in Dad's computer calendar with a hint about the sumptuous recipe.
- > The doorbell rings, so she quickly switches to the front door web cam to check out who is there. This is possible from any UPnP enabled TV in the house.

## 1.2 UPnP Model and Mechanism

### UPnP Model

The UPnP model is based on Devices and Control Points:

> **Devices:**

- Offer services and may contain further devices with additional services.
- Record their state in a set of state variables.

> **Control Points:**

- Make use of the services offered by the devices.
- Control the devices with defined actions that change the state of the device and control the service it is offering.

In the example above, the printer offers its printing services to control point PC's throughout the network. Likewise, the web cam is a UPnP device, offering a monitoring service to the TVs that act as control points.

To make all this happen, Universal Plug and Play mainly uses proven techniques and well known standards such as TCP/IP, DHCP, XML, ... These can be run by any operating system and implemented in any programming language, which makes the concept universal.

### UPnP Mechanism

There are 6 different steps in the UPnP mechanism:

**1 Addressing**

Addressing is the process through which control points and devices **obtain a network address**. They first try to obtain an IP address from a DHCP server; if none is available, an AutoIP (or APIPA) address in the 169.254 subnet is randomly chosen (and tested for uniqueness on the LAN).

**2 Discovery**

Discovery allows control points to **find devices** that are of interest to them.

- When control points enter the network, they broadcast search packets to look for devices and/or services, either in general or of a specific type. Devices featuring the appropriate services/subdevices can then respond.
- Similarly, UPnP devices will advertise their presence on the network at regular intervals. Control points listen for these advertisement packets or discovery packets to detect new devices and their capabilities as they become present on the network.
- UPnP devices leaving the network also send notifications that their services will no longer be available.

**3 Description**

The discovery packets sent out by the devices refer the control points to a location where they can retrieve a Device Description Document (DDD). This DDD contains:

- A summary of the device's embedded devices and a list of services.
- A URL for the so called Service Control Protocol Definition (SCPD). This SCPD describes how the control points can make use of the services offered by the device.
- Control and Eventing URLs: these are the URLs to which the control points have to send commands in order to configure the UPnP device and make use of the device's services.
- A URL for presentation (see step 6).

### **4 Control**

Control allows control points to send commands to devices. As mentioned before, the URL to which these commands are sent, is specified in the DDD.

### **5 Eventing**

Eventing allows control points to track state changes in devices. Control points first subscribe to the appropriate service. Subsequently, any state changes in the device's service are sent as events to the subscribed control points to keep them up to date.

### **6 Presentation**

Control points can optionally display a user interface for devices. The URL for presentation is specified within the DDD. The presentation page shows an HTML-based user interface so that a user can consult and/or consult the device's status. As such, presentation is complementary to control and eventing.

## **The Internet Gateway Device (IGD)**

The Internet Gateway Device (IGD) is the UPnP device in the UPnP network that provides access to the Internet. UPnP control points throughout the house will use the IGD services to transparently connect to and disconnect from the Internet.

All kinds of devices can be an Internet Gateway device: DSL modems and routers, POTS modems, cable modems and Ethernet routers.



The IGD standard was defined by the Internet Gateway Working Committee, a committee that was established by the UPnP. This Forum is the standardization body for UPnP. Apart from the IGD Working Committee, it has defined other working committees (WC) that each concentrate on a certain type of device and services: Home Automation and Security, Audio/Video, Imaging and Print, Camera, ...

## 1.3 UPnP AV

### What Is UPnP AV?

The UPnP AV standard is built on top of UPnP, and is designed to connect and control audio-video devices in a peer-to-peer IP network:

- > As with UPnP, the network is independent of operating systems and architectures, and uses open Internet protocols. Wireless connection to this network is possible.
- > Users can store, archive, and play digital content on the networked devices. Content can be audio and video material, text, graphics, photography, paintings or other artwork. The devices range from anything like TVs, DVD players, AV receivers, to MP3 players, printers and PCs.

### UPnP AV Model

Similar to UPnP, the UPnP AV model is also based on devices and control points. In UPnP AV, the device can be either a “media server” (such as a PC) or “media renderer” (such as a CD player, television, or VCR), and the control point can be a part of either of those elements or separate from them. As a result, there is a wide variety of use scenarios.

For example, users can direct audio content from the PC’s hard drive to be played on a stereo, or they can play audio content from a TV on a stereo. There’s no restriction on what or where the control point is because the UPnP AV standard defines only the feature set for the media server and media renderer. The control point simply has to take advantage of the instructions defined for the various devices.

In UPnP AV, the role of the control point is to find content, configure devices, and transfer data. The control point:

- > Discovers audio/visual devices on the network,
- > Locates the content selected by the user,
- > Determines a common transfer protocol and media format,
- > And initiates and controls the transfer to the renderer, including instructions on how the content is to be rendered (brightness, contrast, colour levels, volume, and so on) and how the content should flow (play, stop, pause, seek, next, previous).

## 2 UPnP and Network Address Translation (NAT)

### 2.1 The Concept

#### What Is Network Address Translation and Why Do We Need It?

One of the problems of the Internet today is the shortage of IP addresses. When the Internet Protocol (IP) was conceived in the early 70s, every computer was given an IP address to be able to identify it when sending IP traffic. However, the number of IP hosts has grown tremendously over the years and the address space is almost completely used. A new version of IP (IPv6) will solve this problem, but the transfer to IPv6 of each of the billions of computers on the Internet will not happen overnight.

To alleviate the problem in the meantime, the idea of NAT was introduced. NAT stands for Network Address Translation and is a mechanism that multiplexes a multitude of (private) IP addresses onto a single (public) IP address. In other words: each device in a private network has its own private IP address. Communication with the public network, however, is established via 1 device that uses 1 public IP address. Since the private IP addresses are confined to specific, private realms, they can be reused in each of these private realms; only the public IP addresses need to be unique in the public domain. As a result, a number of private IP hosts can share a single public IP address on the Internet.



As a matter of fact, the address multiplexing mechanism described is called NAPT and stands for Network Address Port Translation. Other kinds of address translation exist also, e.g. in which only a one-to-one address mapping is done. We will use the more general name NAT in the remainder of this text to indicate NAPT.

#### Network Address Translation in the UPnP Network

In a UPnP network, the Internet Gateway Device has a Network Address Translation engine. This means that all the devices in the UPnP network use private IP address for the communication amongst each other. To communicate with the Internet, the IGD generates translates all these private IP addresses to one public address.

## 2.2 Problems Encountered by NAT

### IP Addresses and Ports Embedded in the Payload

NAT is not a simple thing to do, though, as each IP packet needs to be translated: in upstream direction, the private IP address/port in the IP header is replaced with the public IP address/port (and vice versa in downstream direction).

This can be a problem because some applications (need to) embed additional information about the IP address/port in the payload of the IP packet, and the NAT engine in the IGD has no way of knowing where exactly the IP address/port is mentioned in the IP payload.

To solve this issue, Application Level Gateways (ALGs) have to be written which will scan the IP packets' payloads for the IP address/port and replace it. Such an ALG program has to be written for each application that embeds IP address/port information in an IP packet. This often means that the application is released to the public for quite a while already, before NAT routers start supporting them through an appropriate ALG.

### Forwarding Unsolicited Packets

A second issue is that the NAT engine cannot find out where to forward inbound packets to if these packets are unsolicited. For example, if a web server is on the LAN, packets coming in from the WAN (Wide Area Network) on port 80 (the HTTP port) should be forwarded to this web server. This forwarding information needs to be explicitly configured on the NAT engine on the IGD.

In the next paragraphs we will see how UPnP can help resolve the two issues described above: the NAT ALG problem and the configuration of a NAT engine for incoming connections.

## 2.3 Solution: NAT Traversal

### What Is NAT Traversal?

NAT Traversal counters the NAT problems mentioned above in two ways:

- > Detection of the Public IP
- > Port Mappings for Services

### Detection of the Public IP

The problems described above can be solved if the applications are able to find out the public IP address and immediately embed this address in the IP packet's payload along with the IP address information that they need to embed.

This is exactly one of the services that is provided by a UPnP Internet Gateway Device. A control point can retrieve the public IP address used by the IGD from the IGD. Applications residing on the control point can then embed this IP address in their payload. This will render the complex ALG mechanism superfluous.



Please note that, for NAT Traversal to work, the application needs to make use of the UPnP API (Application Programming Interface) in Windows or embed its own API. MSN Messenger and a large number of games are examples of such UPnP enabled applications.

For example MSN Messenger (the application) can use the UPnP API in Windows XP (the Control Point) to retrieve the public IP address from the Thomson Gateway (the IGD) and embed it in the SIP messages to set up a video session.

### Port Mappings for Services

The second benefit of UPnP NAT Traversal has to do with configuring services on your LAN. For example, if you want to deploy a small web server or FTP server on your LAN, the appropriate ports (either 80 or 21 respectively) need to be configured on the NAT IGD. The NAT IGD can only know where it should forward the incoming packets from the Internet to, if there is an explicit mapping to the internal host that is running the web or FTP server.

With UPnP, this mapping on the NAT IGD becomes easy. We will see how to do this in the next chapters.

## 3 UPnP Support in Operating Systems

### Microsoft Windows

Both Windows ME and Windows XP support UPnP inherently.

- > UPnP support in Windows ME is restricted to IGD discovery and presentation.
- > UPnP support in Windows XP is more elaborate and includes NAT Traversal functionality.

By default, previous versions of Windows don't have inherent UPnP support. However, you can enable UPnP control point support on Windows 98/98SE/ME similar to the Windows XP support by using the "Network Setup Disk" from Windows XP. For games, this can be done installing DirectX 8 & 9.



The "Network Setup Disk" is a floppy disk that makes it easy to build a small home network. The instructions on how to make such a disk can be found in the Windows XP help pages (type "Network Setup Disk").

Further on, we will go deeper into the specifics of Windows XP and how it interacts with an IGD in general and the Thomson Gateway in particular.

### Mac OS

So far, Apple has not announced support for Universal Plug and Play.

### Linux

Currently, there are no distributions of Linux that come with UPnP control points. However, a free SDK for UPnP under Linux is available from Intel. Some other companies also offer a commercial Linux UPnP package.



More information on these can be found on the UPnP web site: <http://www.upnp.org/>.

## 4 Using UPnP with the Thomson Gateway

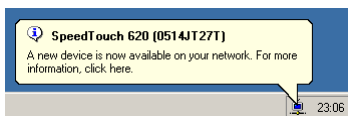
The Thomson Gateway supports the full UPnP Internet Gateway Device standard. It was certified as such by the UPnP Implementers Corporation (UIC, <http://www.upnp-ic.org>) and awarded the UPnP certification mark.



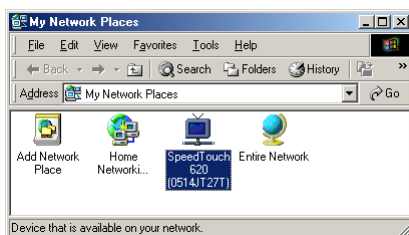
We will now see how the Thomson Gateway IGD interacts with Windows and how to benefit from the Thomson Gateway UPnP features.

### 4.1 Windows ME

Windows ME only supports discovery and presentation. This means that if a UPnP device is attached to the network, a pop-up message box will announce its presence on the network.



More specifically for an IGD, an icon will appear in **My Network Places**.



- > Double-click the icon to show the presentation page.

In the case of the Thomson Gateway, this is the normal web interface, which can also be accessed by typing the Thomson Gateway's IP address (by default this is 192.168.1.254) in a web browser window or simply <http://dsldevice.lan>.

-Or-

- > Right-click the icon and select **Properties** to show general information like the name, manufacturer, ...

## 4.2 Windows XP

### Discovery

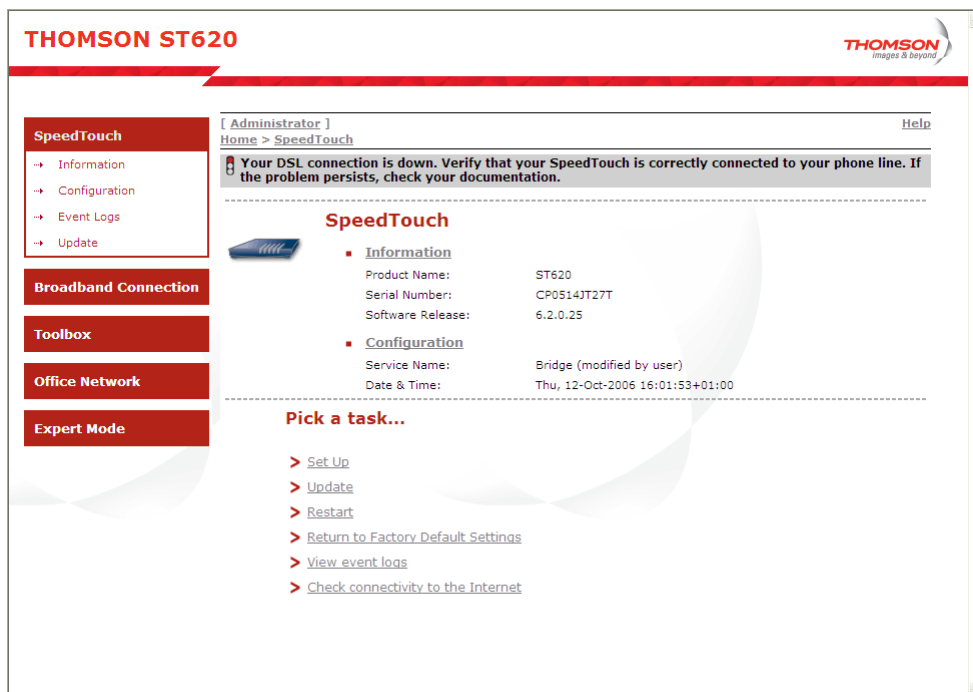
Windows XP features more comprehensive UPnP support. Similar to Windows ME, a pop-up window announces the presence of a new UPnP device as soon as it is discovered in the network.

### IGD Icon

When an IGD is discovered in the network, an icon will appear in **My Network Places**.

- > Double-click the icon to show the presentation page.

In the case of the Thomson Gateway, this is the normal web interface, which can also be accessed by typing the Thomson Gateway's IP address (by default this is 192.168.1.254) in a web browser window or simply <http://dsldevice.lan>.



-Or-

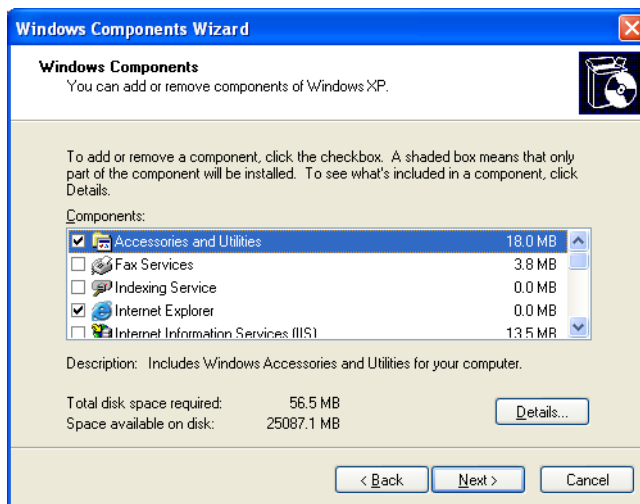
- > Right-click the icon and select **Properties** to show general information like the name, manufacturer, ...

### Other UPnP devices

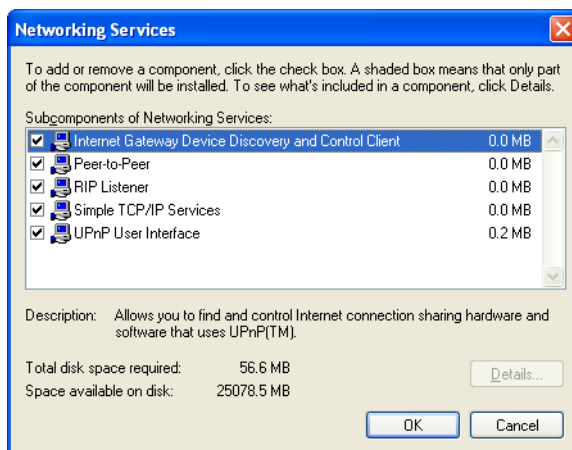
UPnP devices other than the IGD do not appear by default in **My Network Places** on Windows XP.

To see the icon of the other UPnP devices in **My Network Places**:

- 1 Open the Windows Start Menu and click (**Settings >**) **Control Panel**.  
The **Control Panel** appears.
- 2 Double-click **Add or Remove Programs**.  
The **Add or Remove Programs** window appears.
- 3 Click **Add/Remove Windows Components** in the left navigation pane.  
The **Windows Components Window** appears.



- 4 Select the **Networking Services** check box.
- 5 Click **Details**.  
The **Networking Services** window appears.



- 6 Select **UPnP User Interface**.
- 7 Click **OK** to save your changes.

## 4.2.1 Control and Eventing

### Control and Eventing: Connecting and Disconnecting

When an IGD is discovered, an Internet Gateway icon will appear in the **Network Connections** window.



Open the **Network Connections** window via **Start** menu > **Settings** or via the **Control Panel**.

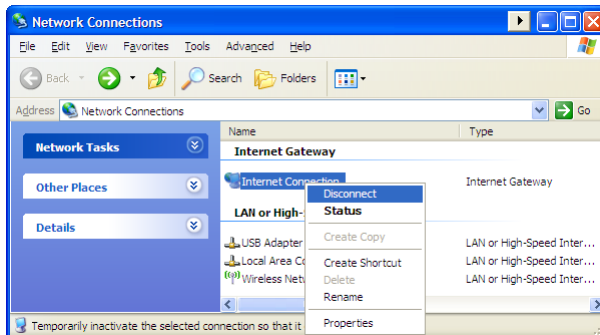
- > To connect the local network to the Internet, double-click this icon. This will set up a routed PPP connection to the Internet starting from the Internet Gateway.



It is important to note that the connection to the Internet is set up from the Internet Gateway; as a consequence, the Thomson Gateway IGD acts as a NAT router.

The Thomson Gateway also supports many other connection models, like Bridging, or PPTP-PPPoA relay. However, UPnP and the IGD functionality may not be (fully) supported in these connection models.

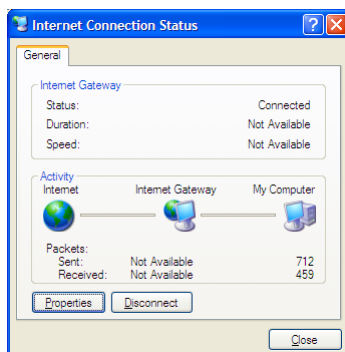
- > To disconnect the IGD, right-click the IGD icon and select **Disconnect** from the menu.



Thanks to this feature, you don't have to surf to the web interface of the Thomson Gateway each time you want to connect to or disconnect from the network.

### Control and Eventing: Status

When the local network is connected to the Internet, double-click the Internet Gateway icon in the **Network Connections** window to check the status: how long has the device been connected and what is the connection speed (downstream).



The figures in the lower left-hand corner of the **Internet Connection Status** window indicate the traffic on the xDSL line (totality of all hosts connected to the IGD). The figures at the right indicate the number of bytes sent and received between this computer and the Internet Gateway only. On a live connection these will be running up steadily.

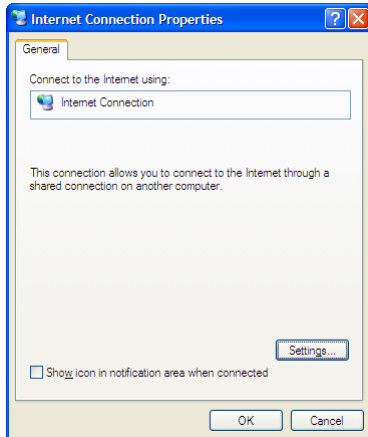
### Control and Eventing: NAT Traversal

You can access the NAT Traversal of the IGD via the Internet Connection Status window or via My Network Places. Since Windows only supports UPnP IGDs that do NAT routing, this feature is quite important.

- 1 Click the **Properties** button in the **Internet Connection Status** window.

-Or-

Right-click the IGD icon in **My Network Places** and select **Properties**

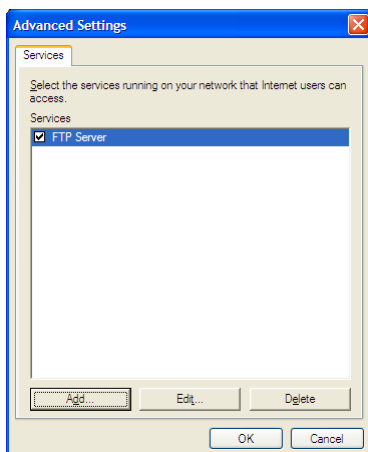


- 2 Click the **Settings** button to see the list of NAT port mappings.

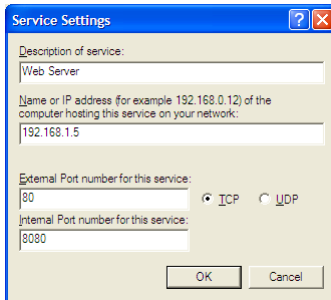


What are NAT port mappings? As explained before, a NAT router will translate a host's internal (private) IP address and port to the IGD's external (public) IP address and port and vice versa. To keep track of all the different translations, the internal and external IP/port pairs are recorded in so called port mappings.

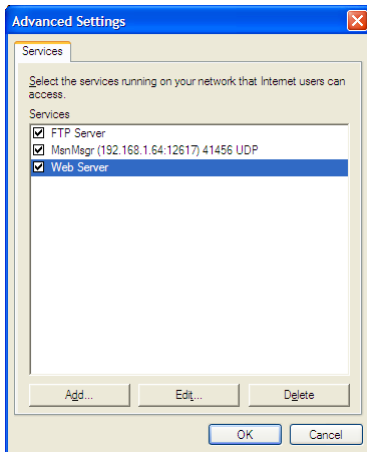
The screenshot below shows a port mapping for an FTP server that is already configured, i.e. externally incoming packets with destination port 21 will be forwarded to the host specified in this mapping.



- 3 Click **Add** to configure a mapping for a web server: all packets coming in on port 80 will be forwarded to the host with IP address 192.168.1.5 on port 8080.



Additionally, UPnP enabled applications like MSN Messenger can automatically reserve incoming ports. In the screenshot below, we can see how Messenger has made port mappings for two external ports to enable external hosts to set up voice and video sessions to internal host with IP address 192.168.1.64.



This is truly NAT Traversal: no user intervention is needed to make applications work transparently with a NAT router.

## 5 UPnP and Security

### UPnP Features

To summarize what has been explained in the previous chapters, a UPnP Internet Gateway Device allows you to:

- > Connect/disconnect the Internet connection,
  - > Create NAT entries,
  - > Get statistics about the Internet connection,
- from a remote interface.

### Risks and Solutions

In a multi-user environment, one can easily imagine the disturbance that can be generated by people playing with the connect/disconnect functionality. But if you simply disable UPnP, users cannot enjoy the benefits of the UPnP-aware application to establish a connection to the Internet without any need for manual configuration (e.g. Messenger, DirectX based software, Xbox live, the list is increasing every day).

In order to let the end user choose his operating mode, the following UPnP configuration types are available from the Thomson Gateway web interface:

- > **Full** - UPnP is enabled without any restrictions. Control points have the ability to connect/disconnect the connection services, and to create NAT entries.
- > **Extended Security** (default setting) - UPnP is enabled with the following limitations:
  - Write mode option "NAT only": only NAT actions are allowed remotely (i.e. creation, deletion). The gateway cannot be connected/disconnected via UPnP.
  - Safe NAT option "enabled": A control point can only create NAT entries for himself onto the gateway device (e.g. not possible to open a door towards an other device available inside the LAN).
- > **Off** - UPnP is disabled on your Thomson Gateway.

## Configuration via the Thomson Gateway Web Pages

Proceed as follows:

- 1 Open a web browser, and browse to <http://192.168.1.254>.  
The Thomson Gateway web page appears.
- 2 In the **Toolbox** menu, click **Game & Application Sharing**.  
The **Game & Application Sharing** page appears.
- 3 In the upper right-hand corner, click **Configure**.  
The Configuration options appear.



### Game & Application Sharing

This page summarizes the games and applications defined on your SpeedTouch. Each game or application can be assigned to a device on your local network.

#### ■ Universal Plug and Play

Universal Plug and Play (UPnP) is a technology that enables seamless operation of a wide range of games and messaging applications.

Use UPnP:

Use Extended Security:

Apply Cancel

#### ■ Assigned Games & Applications

Click on 'Unassign' to disable a game or a application or use the last row in the table to assign a game or application to a local network device.

If the game or the application you are looking for does not exist, [click here](#) to create it (you will be asked for game or application details).

Choose 'User-defined' in the device list and enter its IP address if the device you are looking for does not appear in the device list.

Game or Application	Device	Log
<i>No games or applications assigned.</i>		
ABC (Another BitTorrent Client)	edgmd0505016	<input type="checkbox"/> Add

- 4 Under **Universal Plug and Play**, select:
  - The **Use UPnP** check box to enable UPnP.
  - The **Use Extended Security** check box to enable Extended security.
- 5 Click **Apply** to save your changes.

## 6 UPnP Tweaking via the CLI

The Thomson Gateway is a highly flexible device: it allows you to tailor its features to your specific needs. This is also true for UPnP support.

Tweaking the Thomson Gateway UPnP support can be done from the CLI (Command Line Interface), which can be accessed by setting up a telnet session to the Thomson Gateway. For example, in Windows, open the **Start > Run** box and just type `telnet 192.168.1.254`.



The Thomson Gateway default IP address is 192.168.1.254. If you or your service provider has changed this, please use the appropriate IP address.

### 6.1 UPnP CLI Commands

The following table summarizes how UPnP support in the Thomson Gateway can be tailored to your own needs.

Command	Comment
<code>system config upnp enable/disable</code>	Enable/Disable the UPnP functionality in the Thomson Gateway
<code>upnp config</code>	Configure UPnP parameters (Maxage, Defcservice, Writemode, Safenat, Preferredaddress)
<code>upnp flush</code>	Flush the UPnP configuration (parameter values return to default values)
<code>upnp list</code>	List the UPnP services that are offered by the Thomson Gateway

#### 6.1.1 system config upnp enabled/disabled

This command will start/stop UPnP functionality in the Thomson Gateway altogether. If stopped, no IGD is advertised, and none of the functionality described in this document will be accessible.

## 6.1.2 upnp config

### upnp config maxage

The maxage parameter (in seconds) allows configuring how often the Thomson Gateway sends the notification messages to advertise its presence as an IGD on the network. Setting this parameter to a low value will increase the number of packets over time sent on the network, but will make the state of the device more up to date. Entering the command without a value allows checking the currently configured value (by default 1800).

### upnp config defcservice

In case there are several connection services configured on your Thomson Gateway, the defcservice parameter allows you to configure which connection should be considered the default.

### upnp config writemode full/natonly/readonly

As explained in the chapter about UPnP and Security, the Thomson Gateway integrates a set of rules to limit the remote access from UPnP. In case the write mode is set to:

- > **Full:** the host will accept all the UPnP SET and GET actions (retrieve the status of the device, configure NAT entries and connect /disconnect the WAN services),
- > **Natonly:** GET and NAT related SET actions are processed others will be refused,
- > **Readonly:** the control point will only be able to retrieve information from the Thomson Gateway, all the SET will be refused.

### upnp config safenat enabled/disabled

To enhance security, an extra level can be enabled to avoid any suspicious NAT actions via the UPnP interface to be accepted. In case enabled, any NAT creation/deletion request for an LAN side IP address different from the source IP of the UPnP message will be discarded (e.g. a NAT create from IP=192.168.1.10 for Inside\_Addr=192.168.1.15 will be refused, but a NAT create from IP=192.168.1.10 for Inside\_Addr=192.168.1.10 will be granted).

### upnp config preferredaddress

The Thomson Gateway embeds a complex mechanism to determine the best IP address to advertise with in case several IP addresses are configured on your device. As all automatic configurations, it might be that in very specific network configurations the automatically selection is not fitting your specific requirements. The preferred address can be used to overrule the automatic selection.

## 6.1.3 upnp list

This command lists the devices and services that are currently advertised by the Thomson Gateway (e.g. it can be checked here whether a PPP connection is properly configured and thus advertised as a PPP service).

## 6.2 CLI Tracing

### What Is CLI Tracing?

Via the CLI, you can trace what your UPnP Internet Device Gateway is doing.

- 1** Open the CLI.
- 2** Press CTRL + Q.

An overview appears of the actions performed by the gateway.

## Visit us at:

[www.thomson-broadband.com](http://www.thomson-broadband.com)

## Coordinates

THOMSON Telecom  
Prins Boudewijnlaan 47  
B-2650 Edegem  
Belgium

E-mail: [documentation.speedtouch@thomson.net](mailto:documentation.speedtouch@thomson.net)



## Copyright

©2007 THOMSON. All rights reserved.

The content of this document is furnished for informational use only, may be subject to change without notice, and should not be construed as a commitment by THOMSON. THOMSON assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. The information contained in this document represents the current view of THOMSON on the issues discussed as of the date of publication. Because THOMSON must respond to changing market conditions, it should not be interpreted to be a commitment on the part of THOMSON, and THOMSON cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. THOMSON MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.