How To | Configure A Router As A UPnP Internet Gateway Device With A Windows® XP® Machine As A UPnP Control Point

Introduction

This How To Note describes how to configure your router as a UPnP Internet Gateway Device (IGD), and provides a configuration example for setting up UPnP components. This note also outlines how to configure your Windows® XP® machine as a UPnP control point.

Note: This How To Note describes the Allied Telesis implementation of InternetGatewayDevice:1 Device Template Version 1.01 for Universal Plug and Play Version 1.0. Although every effort has been made to comply with the Internet Gateway Device:1 Device Template Version 1.01 Standardized DCP, this implementation has not been certified by the UPnP Implementers Corporation.

Which products and versions does it apply to?

This document applies to the following Allied Telesis routers:

- AR720 and AR740 routers, running software release 2.6.4 or later
- other AR700 series routers, running software release 2.7.1 or later
- AR400 series routers, running software release 2.7.1 or later

Related How To Notes

You may also find the following How To Note useful:

- *How To Configure UPnP*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

What is Universal Plug and Play (UPnP)?

Universal Plug and Play (UPnP) is an architecture that allows for dynamic connectivity between devices on a network. Devices may dynamically add themselves to a network without the need for user intervention or configuration.

A UPnP-enabled device may obtain an IP address, advertise its capabilities, learn about other connected UPnP devices and then communicate directly with those devices. The same device can terminate its connection cleanly when it wishes to leave the UPnP community. The intent of UPnP is to support zero-configuration, "invisible" networking of devices including intelligent appliances, PCs, printers and other smart devices using standard protocols.

UPnP also supports the functionality of NAT Traversal. This is a solution to the real-time communication problem for peer-to-peer applications such as instant messaging running behind the NAT-enabled Firewall.

Firewall and Network Address Translation (NAT)

A firewall is a security device that protects the internal network by preventing unsolicited access from the outside. Due to the scarcity of IPv4 addresses, Network Address Translation (NAT) provides a means to allow multiple computers or devices on a private network to share a single, globally routable IPv4 address.

Although firewall and NAT provide benefits for internal or private networks, they also cause problems for applications that need a public IP address and unique port number for each session, where the session setup is initiated by the external client.

For example, instant messaging applications such as Windows Messenger use the Session Initiation Protocol (SIP) for setting up voice/video sessions with a remote peer. The Windows Messenger client in the internal network embeds the private address assigned to it, and the dynamic port information in the SIP message, when sending the SIP invitation to the remote peer. However, the address and port information embedded in the SIP message are not NAT-ed and hence they are invalid for the remote peer to contact the internal client.

UPnP Internet Gateway Device and NAT Traversal

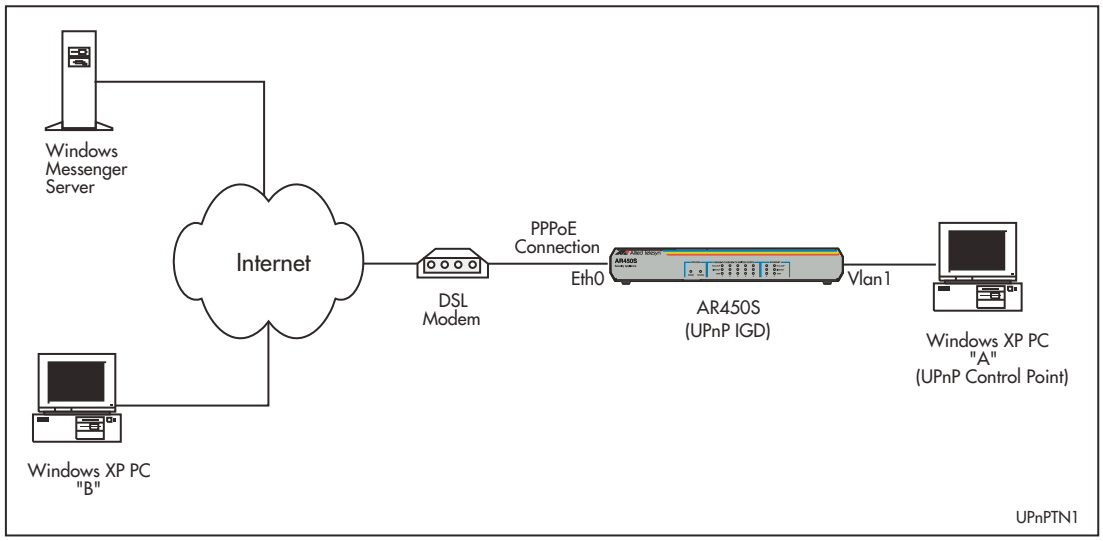
The UPnP Internet Gateway Device (IGD) addresses the issues caused by the firewall and NAT by providing support for NAT Traversal. The IGD can be detected and controlled using UPnP protocols by the control point in the UPnP networking infrastructure. A UPnP-enabled application client can determine if a firewall and/or NAT device is present, learn the translated IP address and configure port mappings in the IGD.

For example, Windows Messenger (the UPnP enabled client) in Microsoft® Windows® XP (the UPnP control point) can use the NAT Traversal API to discover whether it is behind a NAT device. If so, it can retrieve the translated address and configure port mappings to be used in the UPnP-enabled gateway device (UPnP IGD) and use this information in the SIP message for setting up a voice/video session with the remote peer. This allows the Window Messenger peer to run a real-time communication session by using valid addressing.

Configuration Example

This example describes how to configure an AR450S router as an Internet Gateway Device (IGD) for UPnP. This support is an Allied Telesis implementation of InternetGatewayDevice:1 Device Template Version 1.01 for Universal Plug and Play Version 1.0. The following sections describe how to configure the AR450S router and Windows XP as UPnP components.

In the following figure, Windows XP (UPnP control point) "A" is in the local private network behind the AR450S router which is a UPnP supported IGD and has firewall and NAT enabled. Windows Messenger clients "A" and "B" are peers for the voice/video conferencing session. It is assumed that "B" is directly connected to the Internet and does not use a gateway device with firewall and NAT.



Configuring an AR450S router as an IGD for UPnP

The following is an example configuration setup for the AR450S router as an Internet Gateway Device using a PPPoE connection to the Internet. In this example, the Control Point "A" is connected to the router via the VLAN port and is assigned an IP address by the router using DHCP.

```
set system name=AR450
create ppp=0 over=eth0-ANY iprequest=on
enable ip
enable ip remote
enable ip dnsrelay
add ip interface=ppp0 ip=0.0.0.0 mask=0.0.0.0
add ip interface=vlan1 ip=192.168.1.1
add ip route=0.0.0.0 mask=0.0.0.0 interface=ppp0 next=0.0.0.0
enable upnp
enable firewall
create firewall policy=UPnP1
set firewall policy=UPnP1 upnp=enabled
```

```
# Allow the firewall to forward pings for testing purposes
enable firewall policy=UPnP1 icmp_forwarding=ping

add firewall policy=UPnP1 interface=vlan1 type=private upnptype=lan

add firewall policy=UPnP1 interface=ppp0 type=public upnptype=wan

add firewall policy=UPnP1 nat=enhanced interface=vlan1
   gblinterface=ppp0

enable dhcp

create dhcp policy=base lease=7200

add dhcp policy=base subnet=255.255.255.0

add dhcp policy=base router=192.168.1.1

add dhcp policy=base dnsserver=192.168.1.1

create dhcp range=office policy=base ip=192.168.1.2 number=16
```

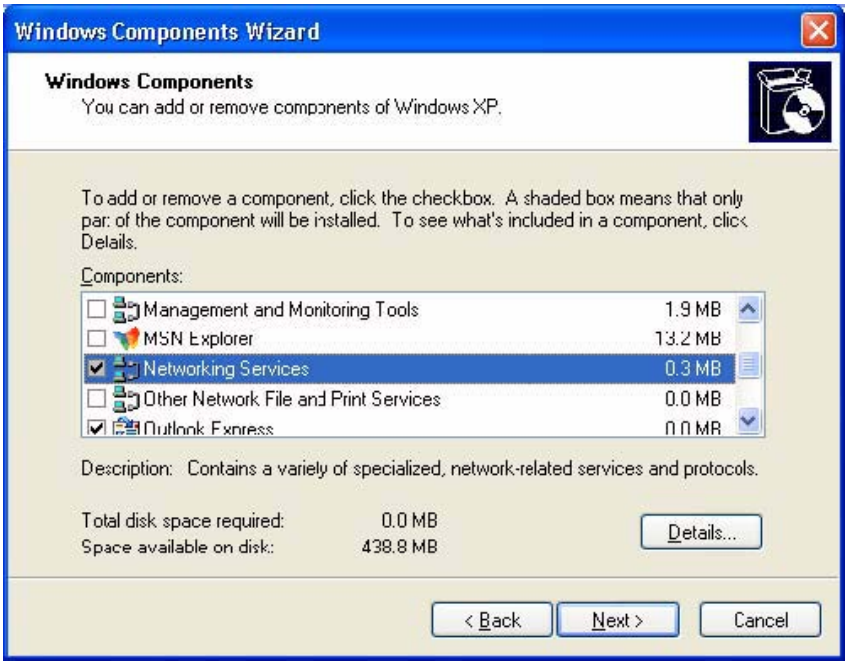
Configuring Windows XP as a UPnP Control Point

Windows XP has native support for UPnP as a control point. In this example, PC A is running Windows XP Home Edition with SP1 and Windows Messenger client version 4.7 (4.7.2009).

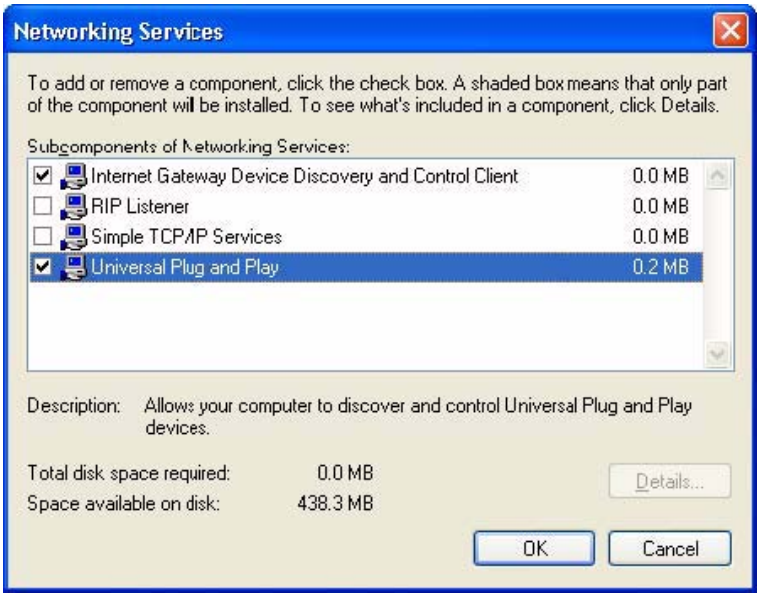
1. Install the UPnP component of the Networking Services

By default, the UPnP client is not installed in Windows XP. To install the UPnP component, follow these steps:

1. Click **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the **Components** list, click **Networking Services**, then click **Details**.



5. Select the **Universal Plug and Play** check box. The **Internet Gateway Device Discovery and Control Client** check box should already be selected.



Note: In order for the UPnP capability to function properly, make sure both **Internet Gateway Device Discovery and Control Client** and **Universal Plug and Play** are selected.

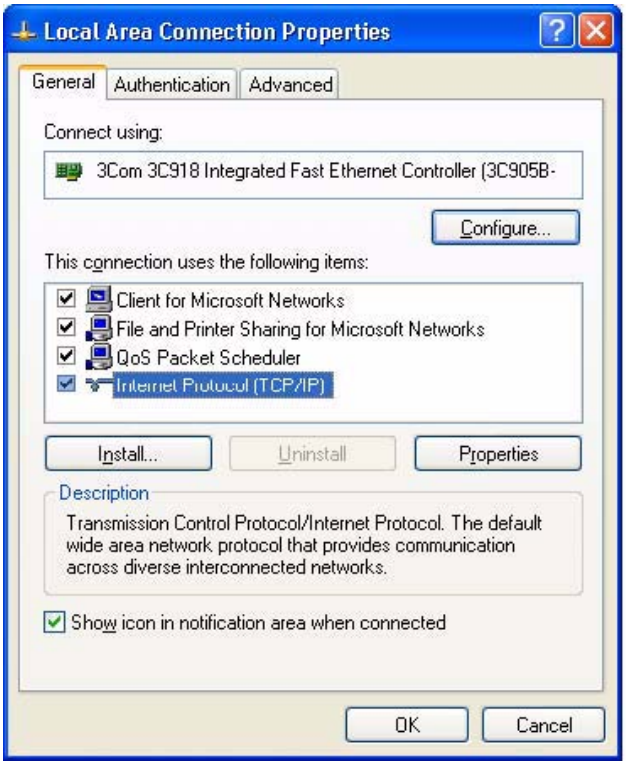
6. Click **OK**.
7. Click **Next**, then click **Finish**.

2. Configure the Local Area Connection

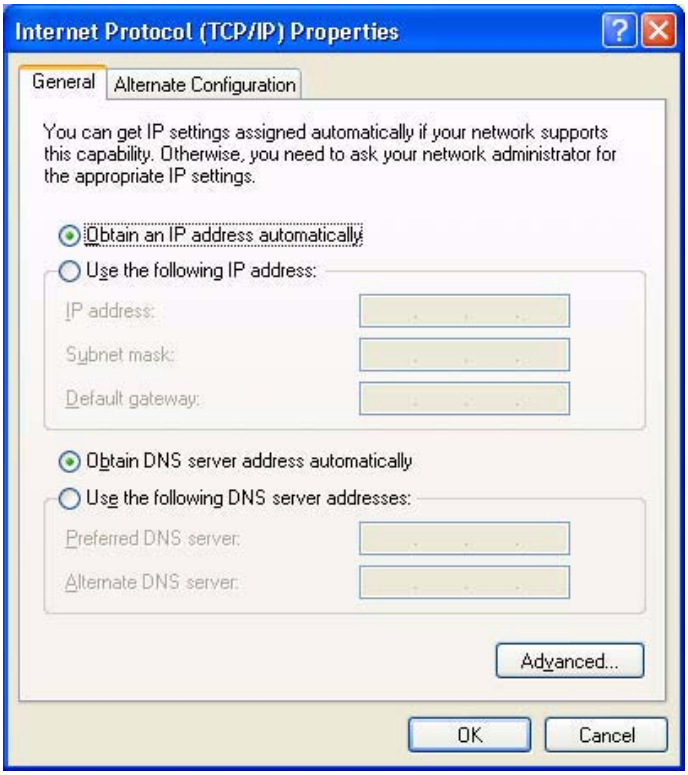
The following steps show how to configure the TCP/IP settings:

1. Click **Start > Control Panel**.
2. Double-click the **Network Connections** icon.
3. Right-click the **Local Area Connection** icon and choose **Properties** from the shortcut menu.

4. In the **Local Area Connection Properties** window, double-click **Internet Protocol (TCP/IP)**.



5. In the **Internet Protocol (TCP/IP) Properties** window, select the radio buttons **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



6. Click **OK**.

Device Discovery and Device Presentation

This section provides more information on device discovery and device presentation. It is assumed that you have carried out the configuration described previously.

When Windows XP discovers a UPnP supported device, a balloon message is displayed on the taskbar area announcing that a new UPnP device has been found. The balloon message only appears the first time the device is discovered.

An **AR450 Internet Gateway Router** icon is shown in the **My Network Places** window.

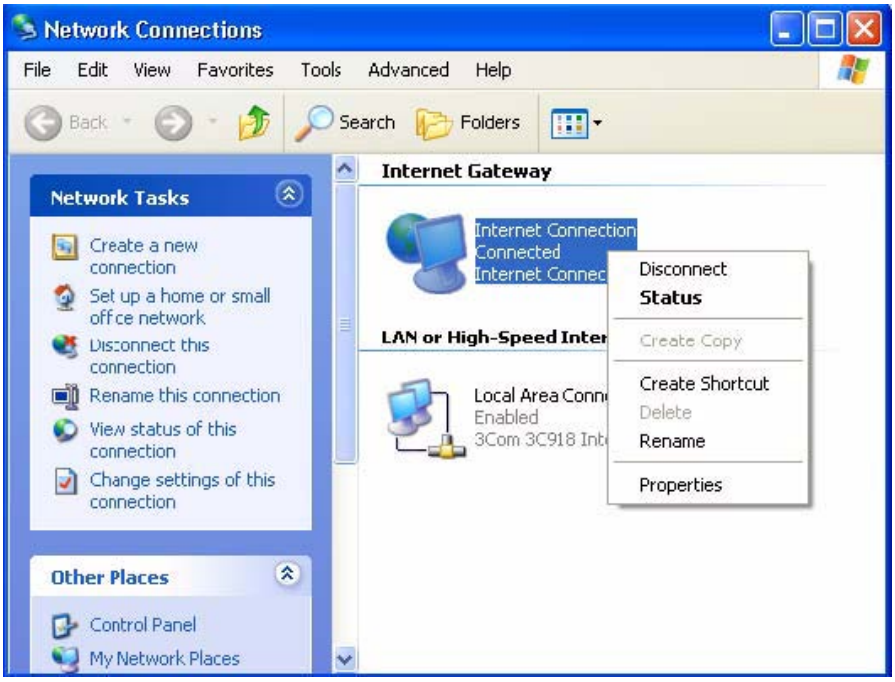
- To see its properties, right-click the **AR450 Internet Gateway Router** icon and select **Properties** from the short-cut menu. This opens the **AR450 Internet Gateway Router Properties** window.

- To access the router's Graphical User Interface (GUI), double-click the **AR450 Internet Gateway Router** icon in the **My Network Places** window. Enter your **User name** and **Password**.

Windows XP Control: Connect, Disconnect, Status

An **Internet Gateway** icon will be shown in the **Network Connections** window.

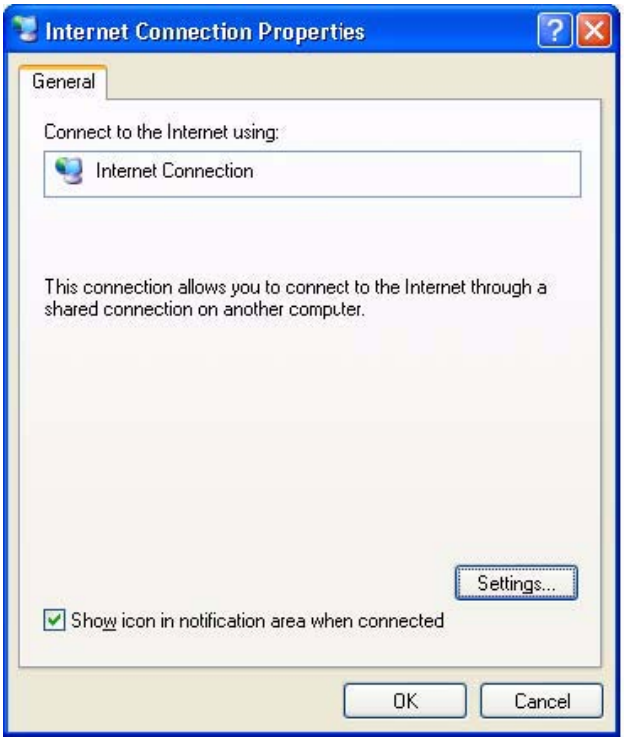
- To disconnect the Internet connection, right-click the **Internet Gateway** icon and select **Disconnect** from the short-cut menu.



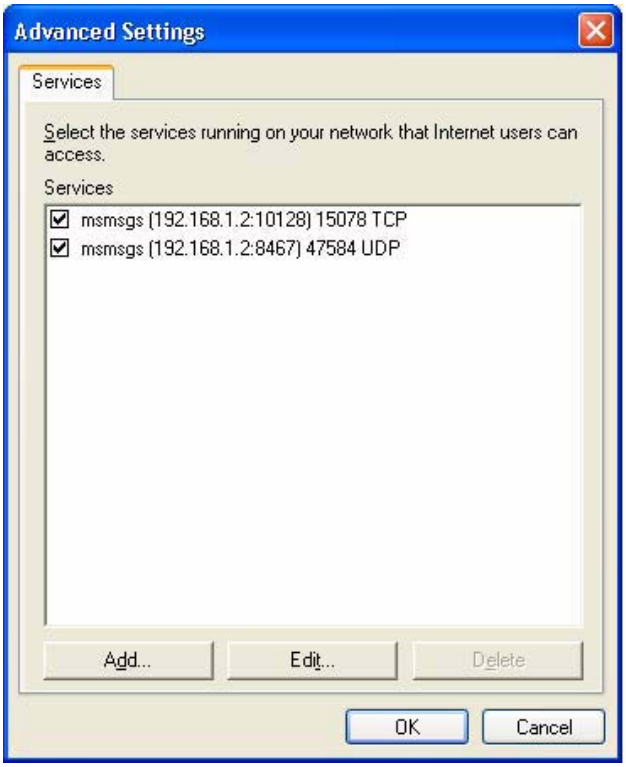
- To reconnect the Internet connection, right-click the **Internet Gateway** icon and select **Connect** from the short-cut menu.
- To see the status of the connection, right-click the **Internet Gateway** icon and select **Status** from the short-cut menu. This opens the **Internet Connection Status** window.

Windows XP Control: NAT Traversal

1. Right-click the **Internet Gateway** icon and select **Properties** from the shortcut menu. This opens the **Internet Connection Properties** window.

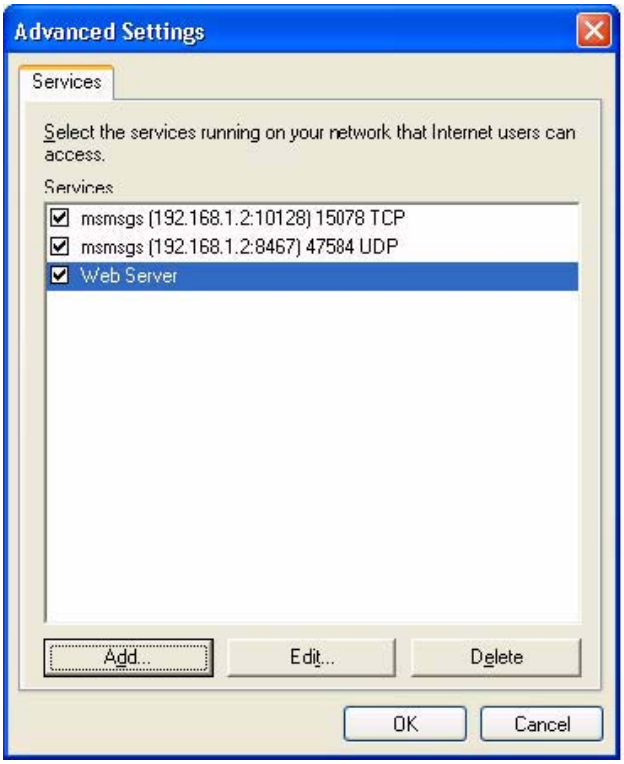


2. Click the **Settings** button. This opens the **Advanced Settings** window. The following screen capture shows that two port mappings have been added by the Windows Messenger. This is the NAT Traversal functionality—port mappings are automatically added without user configuration.



3. You can add more port mappings by clicking the **Add** button on the **Advanced Setting** window. The following figure shows how to add a port mapping for a Web server.

4. Click **OK**. The following figure shows the port mapping for the Web Server is successfully added.



Using Windows Messenger for Videoconferencing

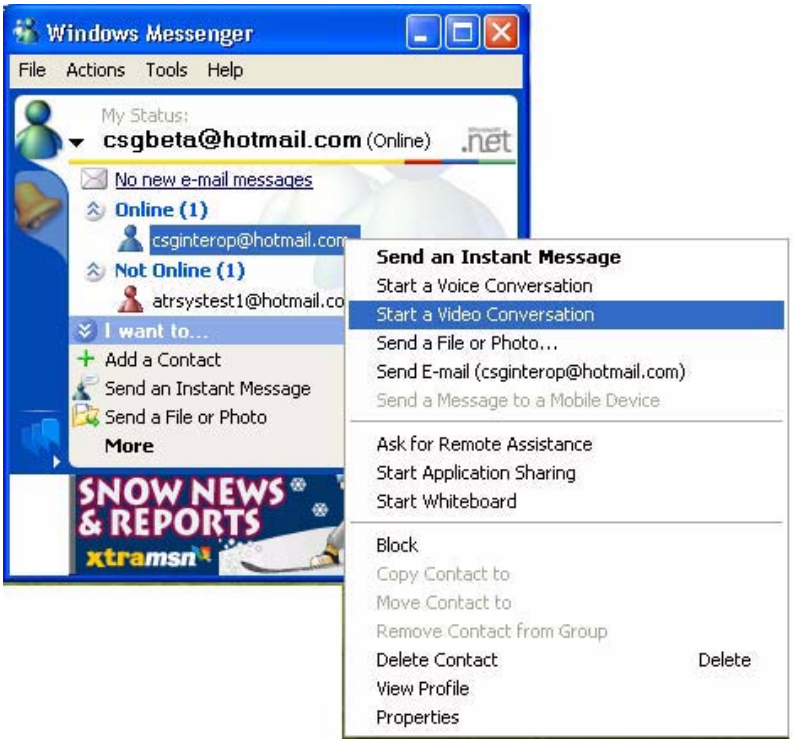
With UPnP support, the user of the Windows Messenger behind the firewall/ NAT device will be able to connect the peer for voice and video conferencing.

The following steps show how to communicate with peers for Windows Messenger videoconferencing.

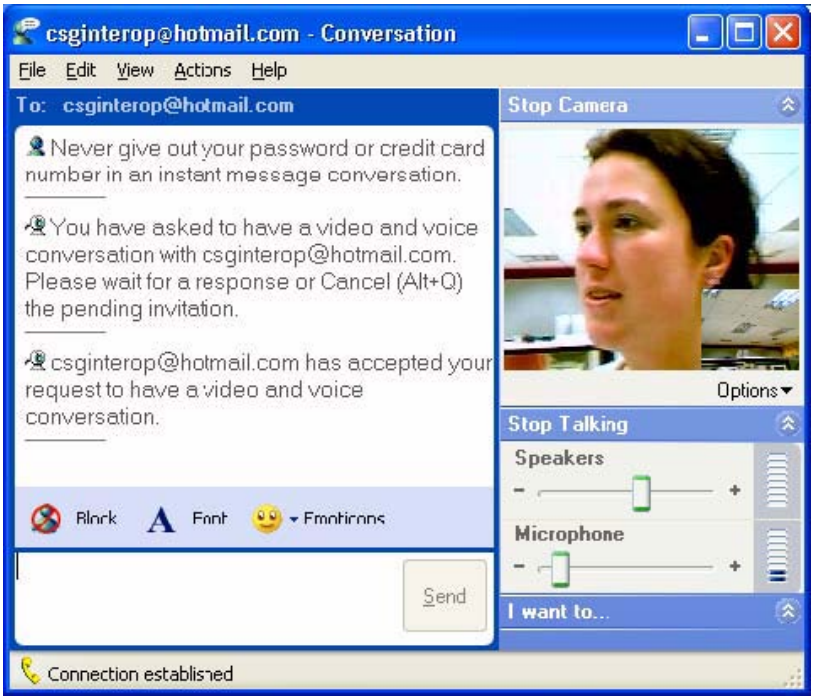
1. Double-click the **Windows Messenger** icon in the status area of the task bar. If Windows Messenger is not running, click **Start > All Programs**, and then click **Windows Messenger**.

2. Click **Click here to sign in** and sign in.

3. Right-click a contact who you want to communicate with who is online. Click **Start a Video Conversation** from the short-cut menu.



4. Once your contact has accepted your invitation, the video conversation session starts.



USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

C613-16001-00 REV B