

Telegesis™	 <b>SILICON LABS</b>	TG-APP-Internet-101
ETRX2, ETRX35x		Application Note

Telegesis™ is a trademark of Silicon Laboratories Inc.

## **ETRX2 and ETRX357 Wireless Mesh Networking Modules**

### **Application Note – Accessing Modules over the Internet**



## Table of Contents

1	INTRODUCTION.....	3
2	OBSTACLES.....	3
3	CONFIGURING A GATEWAY .....	4
4	COMMUNICATING WITH THE EAP.....	9
5	OUTGOING CONNECTIONS FROM AN EAP.....	9
6	WARNING.....	12

## 1 Introduction

The serial port of the ETRX2 and ETRX357 modules can be connected to an Ethernet network via a suitable adaptor such as a Lantronix XPort Direct+, which is the basis of the EAP-E device. It is then simple to communicate with the module, either using a HyperTerminal connection directly to its IP address or by using the Lantronix COM Port Redirector to map the IP address to a virtual COM port.

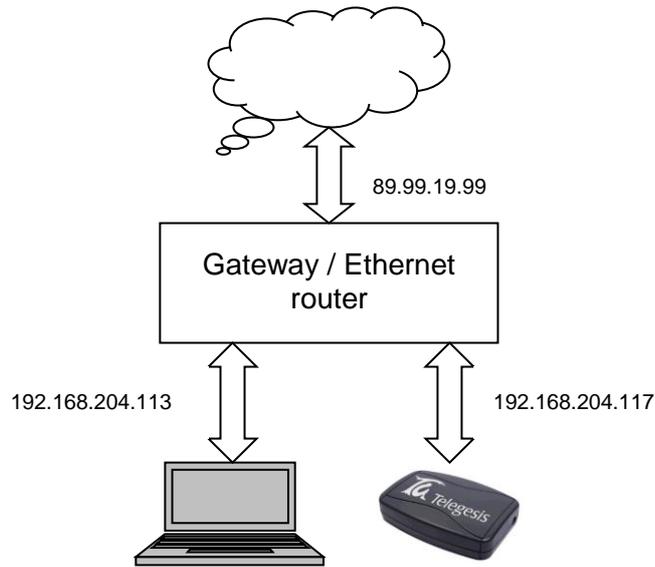
This is straightforward on a local sub-net, but it is less clear how to achieve this over longer range. This note describes the general principles of configuring a gateway such as a broadband router so that a local PC can connect to a remote EAP and open a TCP connection. Aspects such as firewall security and creating a web server are beyond the scope of this note, which just details the first steps in forming a simple connection from a PC to a remote EAP. It gives examples using a typical domestic gateway device (a Thomson ST546) but others will be similar.

This application note was originally written with regard to the EAP-E Ethernet Access Point which is now obsolete, but the same principles apply to its replacement, the Communications Gateway.

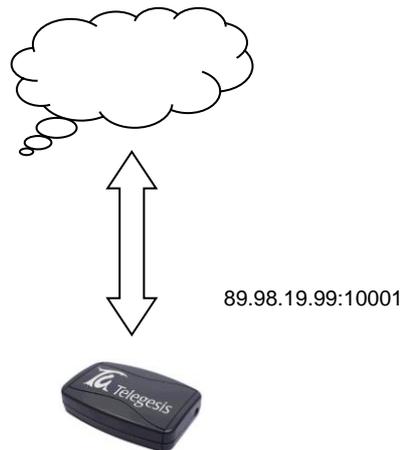
## 2 Obstacles

Gateway devices use Network Address Translation (NAT) to hide the local network from public view. Local devices acquire an IP address from the gateway/router which are typically 192.168.x.x for a private network, but the gateway translates this to its own address assigned by the Internet Service Provider. In this way the gateway can provide a firewall which hides the local devices and only allows incoming packets in response to an outgoing request, and it allows multiple PCs to access the Internet while the ISP only has to provide a single IP address.

The difficulty is then that an EAP gets an IP address from the gateway but a remote user has no way of connecting to it directly. A solution is to drill a hole in the gateway's firewall by using port forwarding (or port mapping). In this way, packets addressed to a specific port or range of ports of the gateway are always routed to the EAP. A remote user then just needs the IP address of the gateway and the relevant port number.



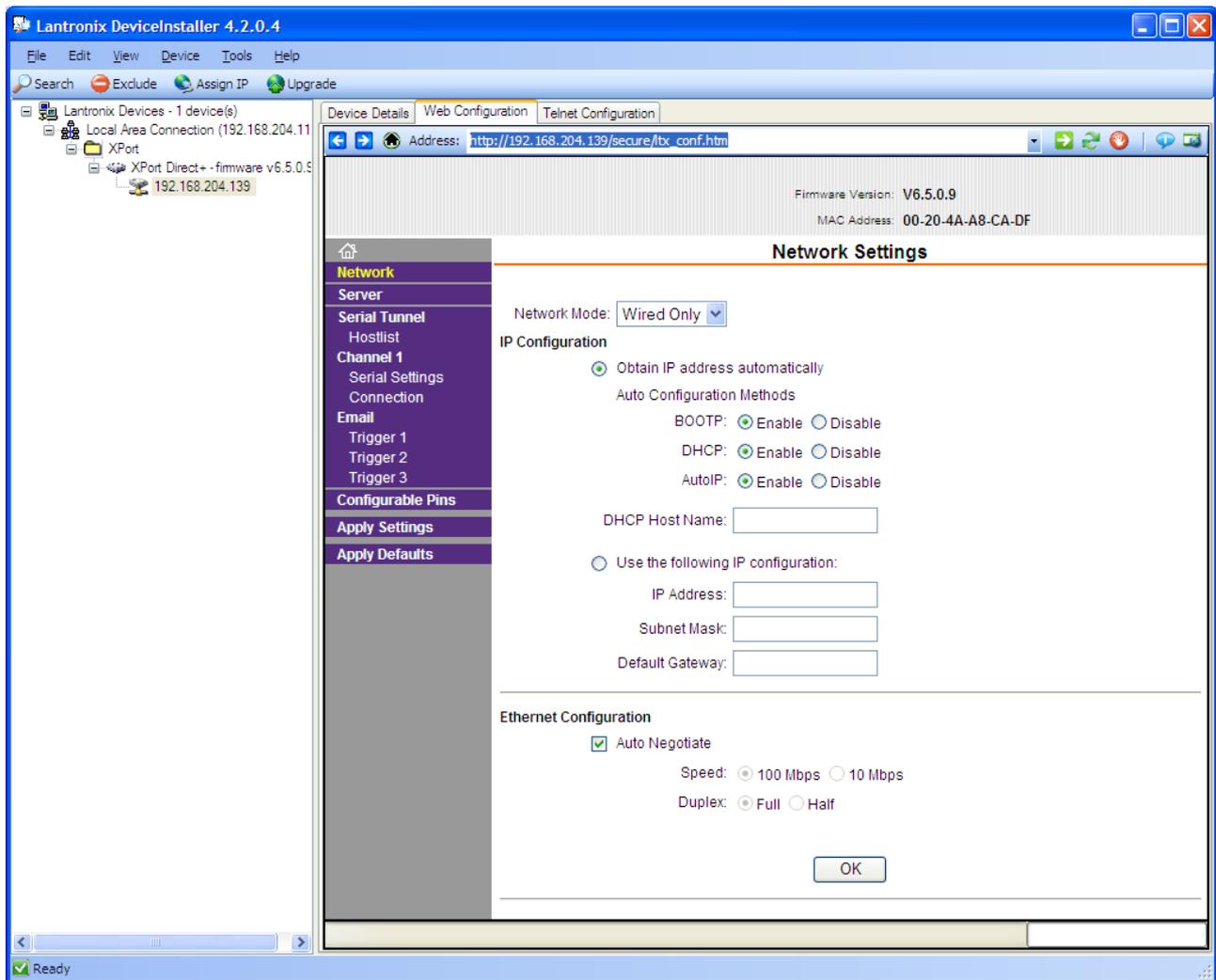
**1. Network devices with example addresses**



**2. EAP after port mapping**

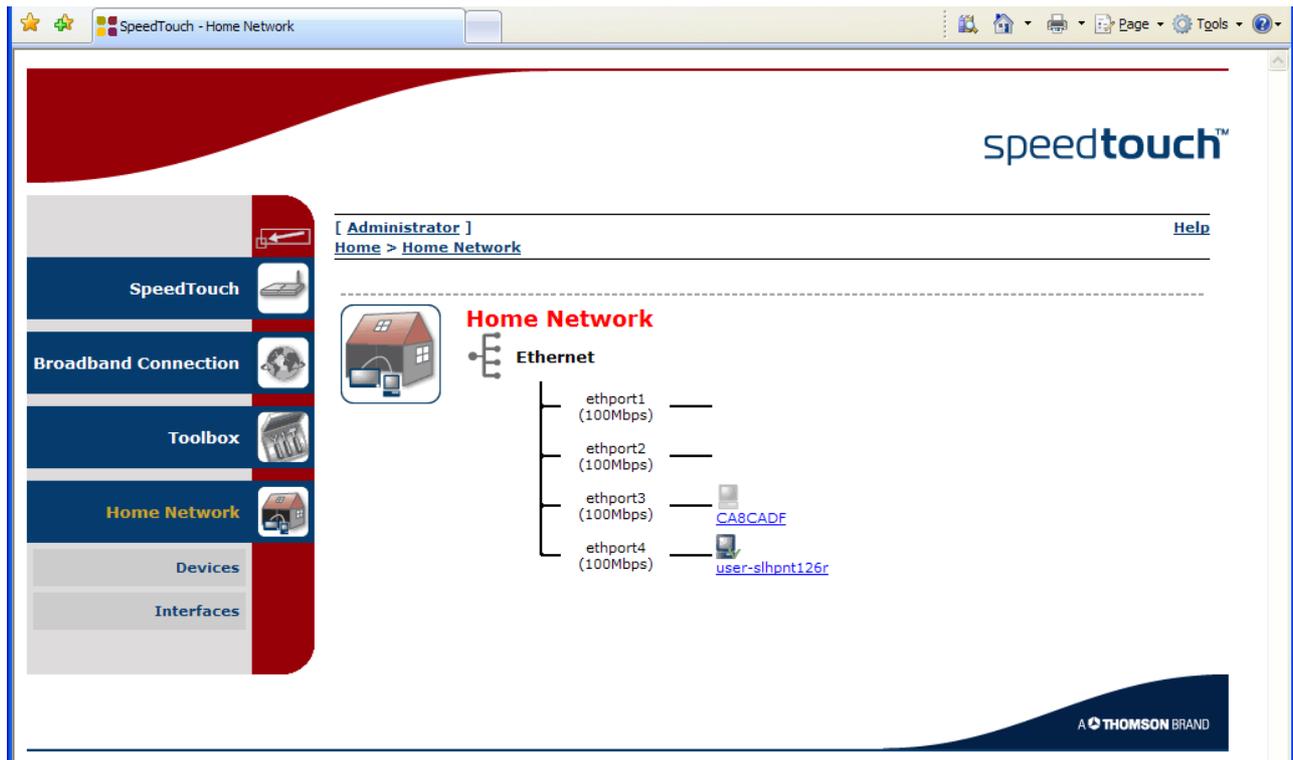
**3 Configuring a gateway**

First it is necessary to know the local IP address and port number of the EAP. The standard port number is 10001 for a Lantronix XPort Direct+. The EAP is usually configured to use DHCP and will acquire its IP address from the gateway/router, and it is important to ensure that this does not change. The address can often be obtained from the maintenance web pages of the router, which often allows you to fix the address. Otherwise the EAP can be configured to use static IP addressing; the Lantronix Device Installer tool is the easiest to use since it can discover the devices and report their IP address. It allows you to change the device settings via Telnet or a web browser, and the web page for the address settings look like this:



### 3. EAP address settings

The exact procedure for setting up port mapping on your gateway depends on the model, but it will usually start by accessing the maintenance pages from a web browser. For example, a particular Thomson gateway displays a map of the local network:

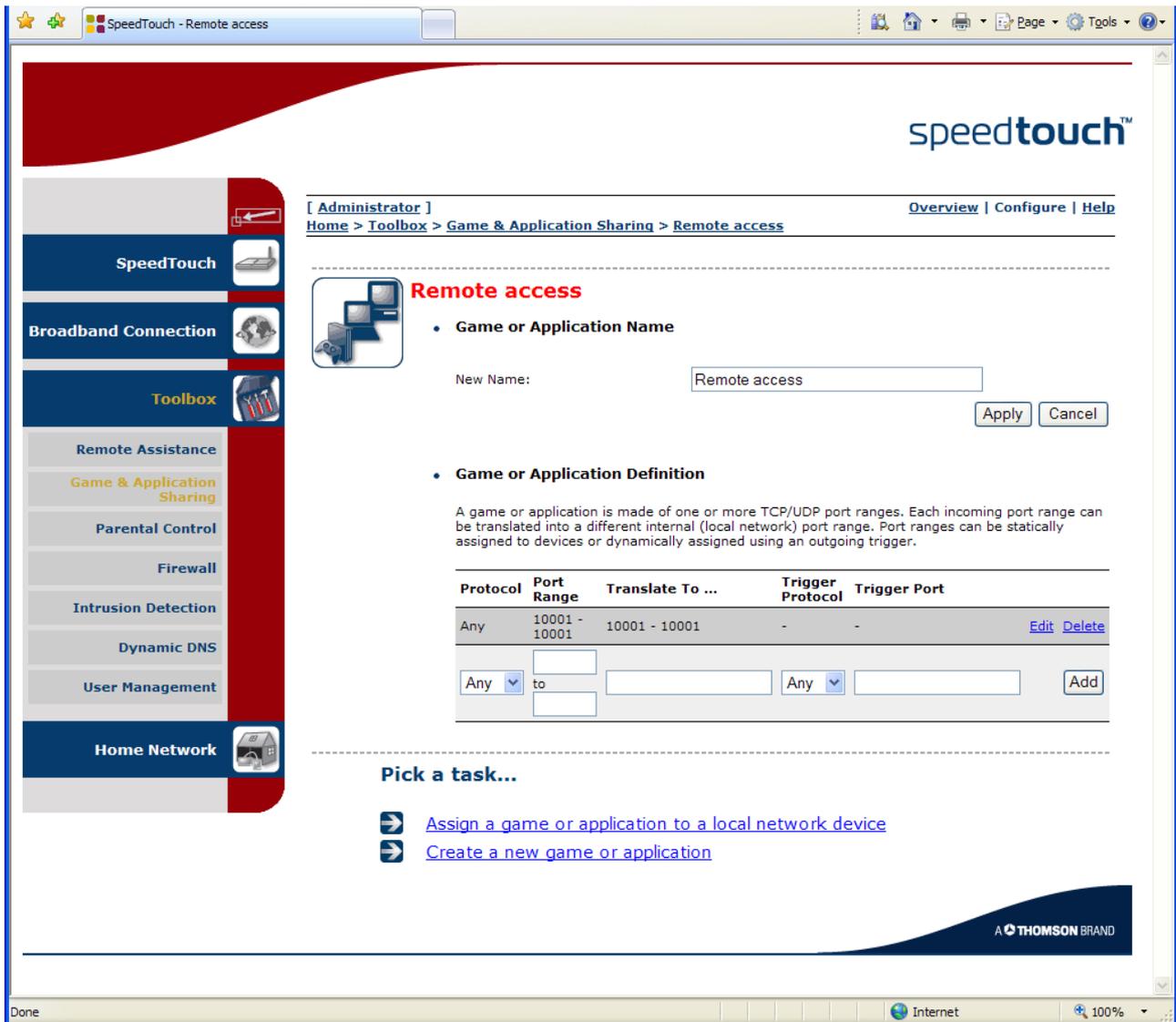


#### 4. Local network map

It has assigned the name CA8CADF to an EAP based on the MAC address of the Lantronix module. Clicking on that device icon brings up all the relevant information including its IP address.

Port forwarding may be described in different ways such as “Port Mapping”, “Gaming” or “Application Sharing” but the end result is the same. There is likely to be a predefined set of mapping rules for various applications but it is simpler to add a new one. There will be typically three stages to this:

1. Create a new rule and give it a name
2. Define the mapping rule for the port or range of ports. Port 10001 is not used very much on the Internet so it should be safe to retain the same port number on the public and private sides of the gateway. On the Thomson example there is a form to define the port mapping (the map in this instance has already been defined; this is the page to edit it but it is essentially the same):



**speedtouch™**

[ Administrator ] [Overview](#) | [Configure](#) | [Help](#)  
[Home](#) > [Toolbox](#) > [Game & Application Sharing](#) > [Remote access](#)

### Remote access

- Game or Application Name**  
 New Name:
- Game or Application Definition**  
 A game or application is made of one or more TCP/UDP port ranges. Each incoming port range can be translated into a different internal (local network) port range. Port ranges can be statically assigned to devices or dynamically assigned using an outgoing trigger.

Protocol	Port Range	Translate To ...	Trigger Protocol	Trigger Port
Any	10001 - 10001	10001 - 10001	-	-

to

**Pick a task...**

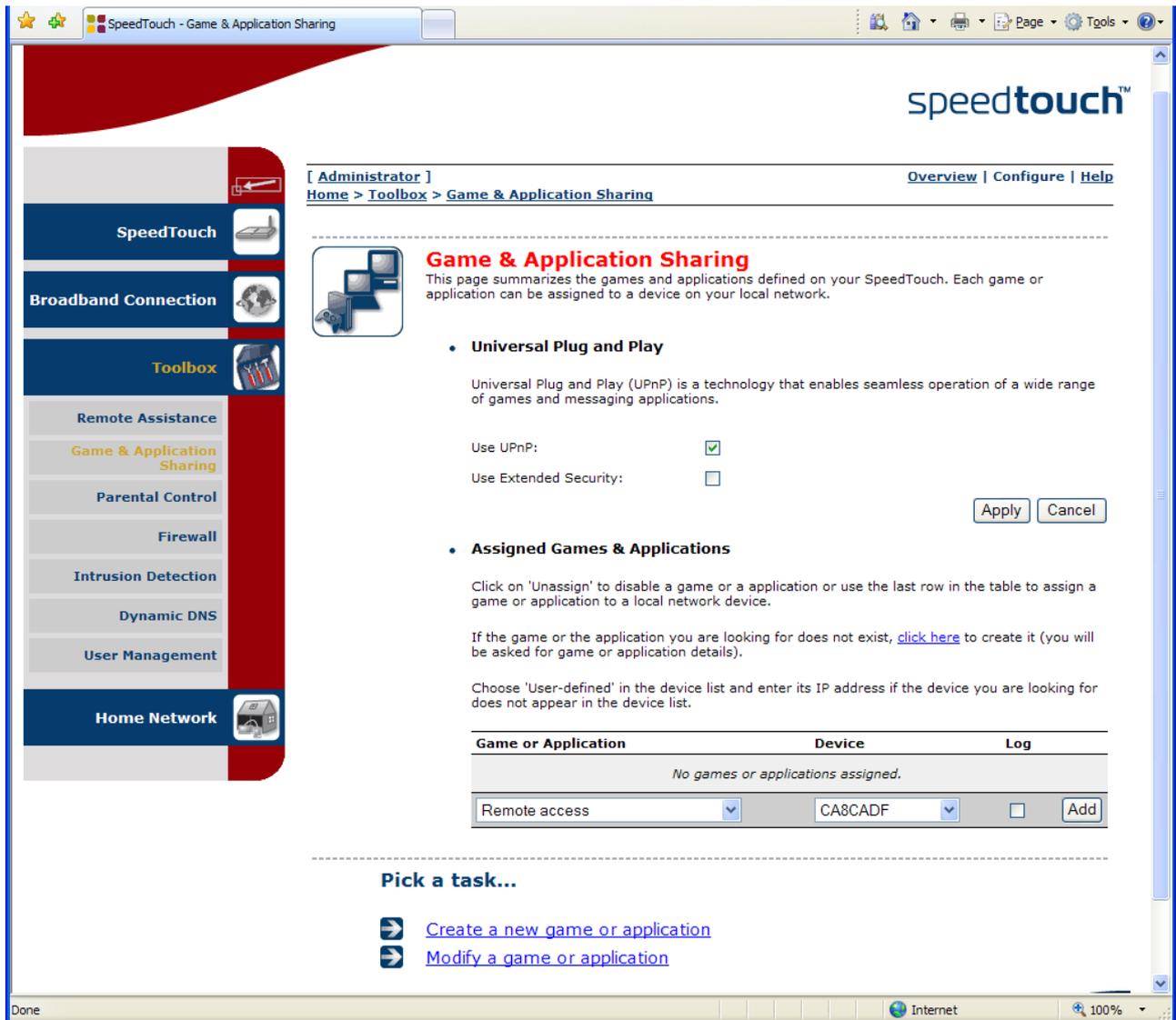
- [Assign a game or application to a local network device](#)
- [Create a new game or application](#)

A THOMSON BRAND

### 5. Port mapping rule

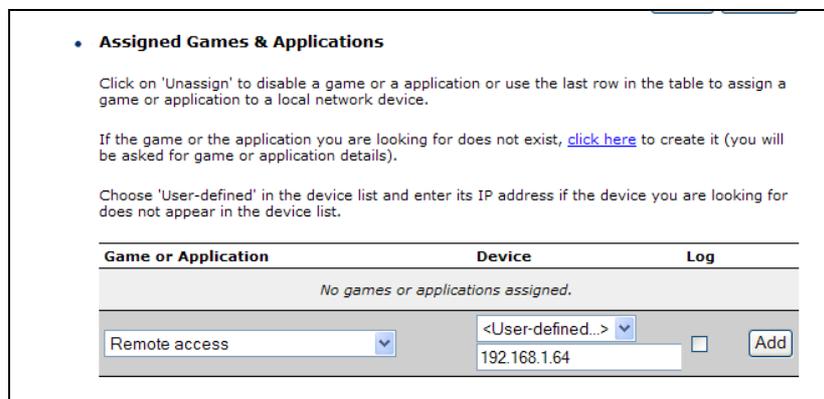
At this stage the mapping rule is not assigned to any particular device.

3. Define the local device to which the rule applies. This will involve selecting it from a list of discovered devices (figure 6) or by typing in the EAP's IP address (figure 7):



The screenshot shows the SpeedTouch web interface for Game & Application Sharing. The left sidebar contains navigation options: SpeedTouch, Broadband Connection, Toolbox, Remote Assistance, Game & Application Sharing (highlighted), Parental Control, Firewall, Intrusion Detection, Dynamic DNS, User Management, and Home Network. The main content area is titled "Game & Application Sharing" and includes a description, a "Universal Plug and Play" section with a checked "Use UPnP" option, and an "Assigned Games & Applications" section. The table in this section is currently empty, showing "No games or applications assigned." Below the table is a form with a dropdown for "Game or Application" (set to "Remote access"), a dropdown for "Device" (set to "CA8CADF"), and an "Add" button.

**6. Assign rule to a discovered device**



This close-up shows the "Assigned Games & Applications" section. It contains the same text and table as the screenshot above. In this view, the "Device" dropdown is set to "<User-defined...>" and the text input field below it contains the IP address "192.168.1.64". The "Add" button is visible to the right of the input field.

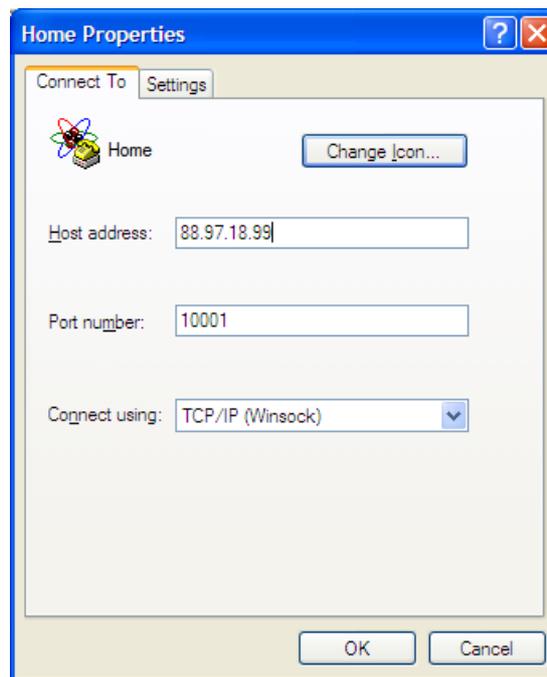
**7. Assign rule to an IP address**

Finally, note the IP address that the gateway uses on its public side. This is unlikely to change over a few days, but you could use a dynamic DNS service to track the changes. Consult the manual of your gateway for more details.

You should now be ready to access the EAP from the outside world.

## 4 Communicating with the EAP

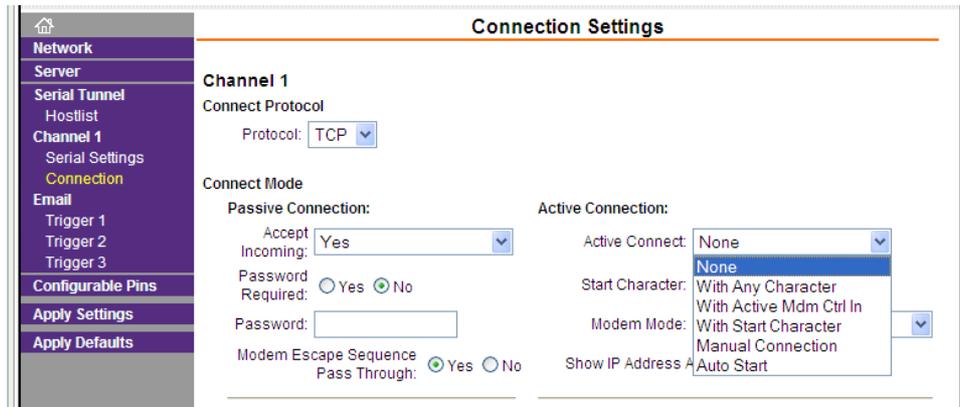
Telegesis Terminal may be suitable as the latest version can access IP addresses. HyperTerminal works if you have it on your machine (for some reason Microsoft dropped it after Windows XP), otherwise use your favourite terminal application or a basic tool such as Telnet. In HyperTerminal, start by creating a new connection and enter the connection data:



The host address is obviously the public IP address of your gateway. The connection should then open automatically and you can type in the commands appropriate to the ZigBee firmware – the AT command set of the R3xx firmware for example, or start receiving data from a device programmed to transmit automatically.

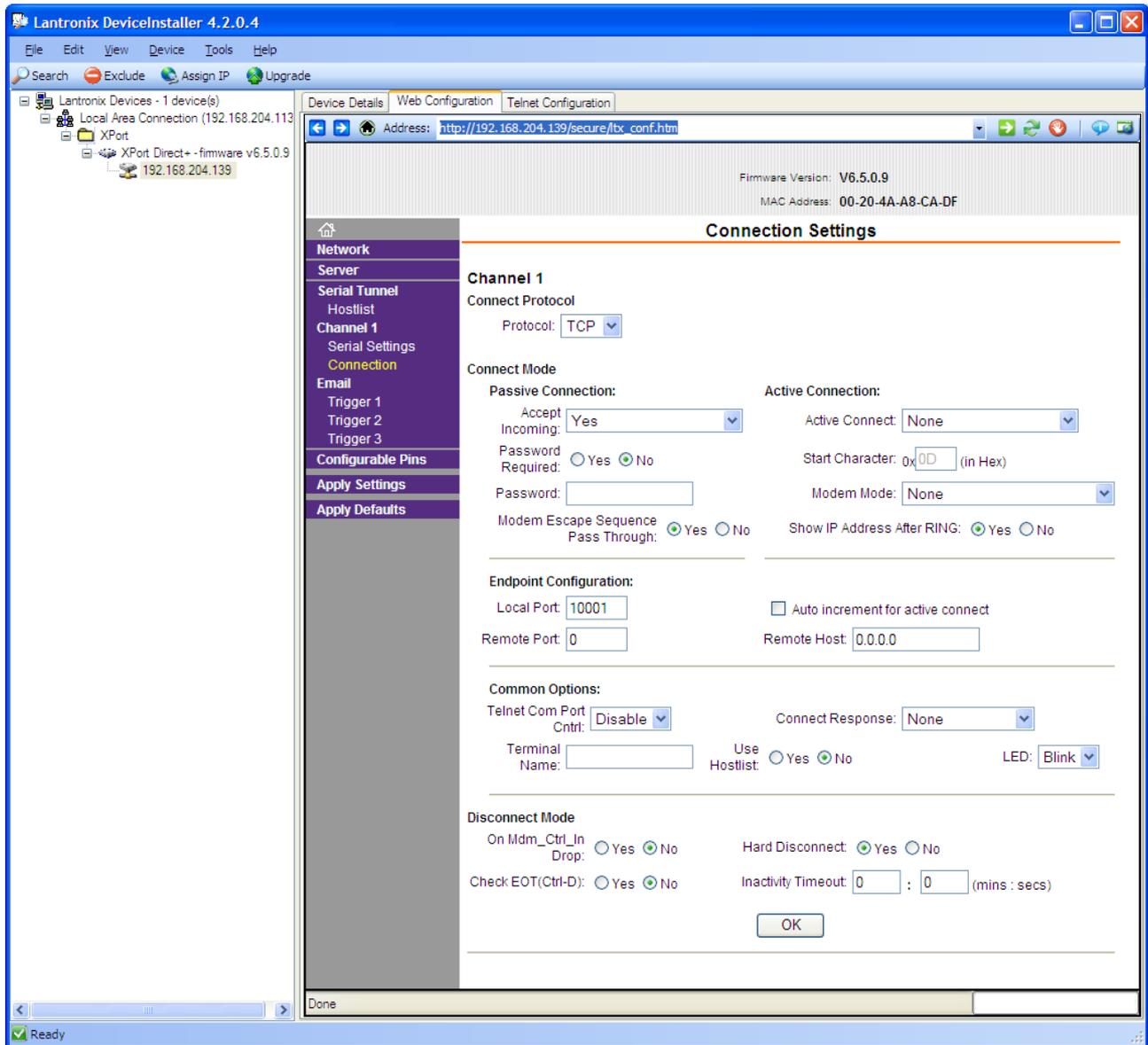
## 5 Outgoing connections from an EAP

The Lantronix Direct+ module by default accepts any incoming request for a connection, but is otherwise idle. Instead, you can set it to open a connection when it starts up:



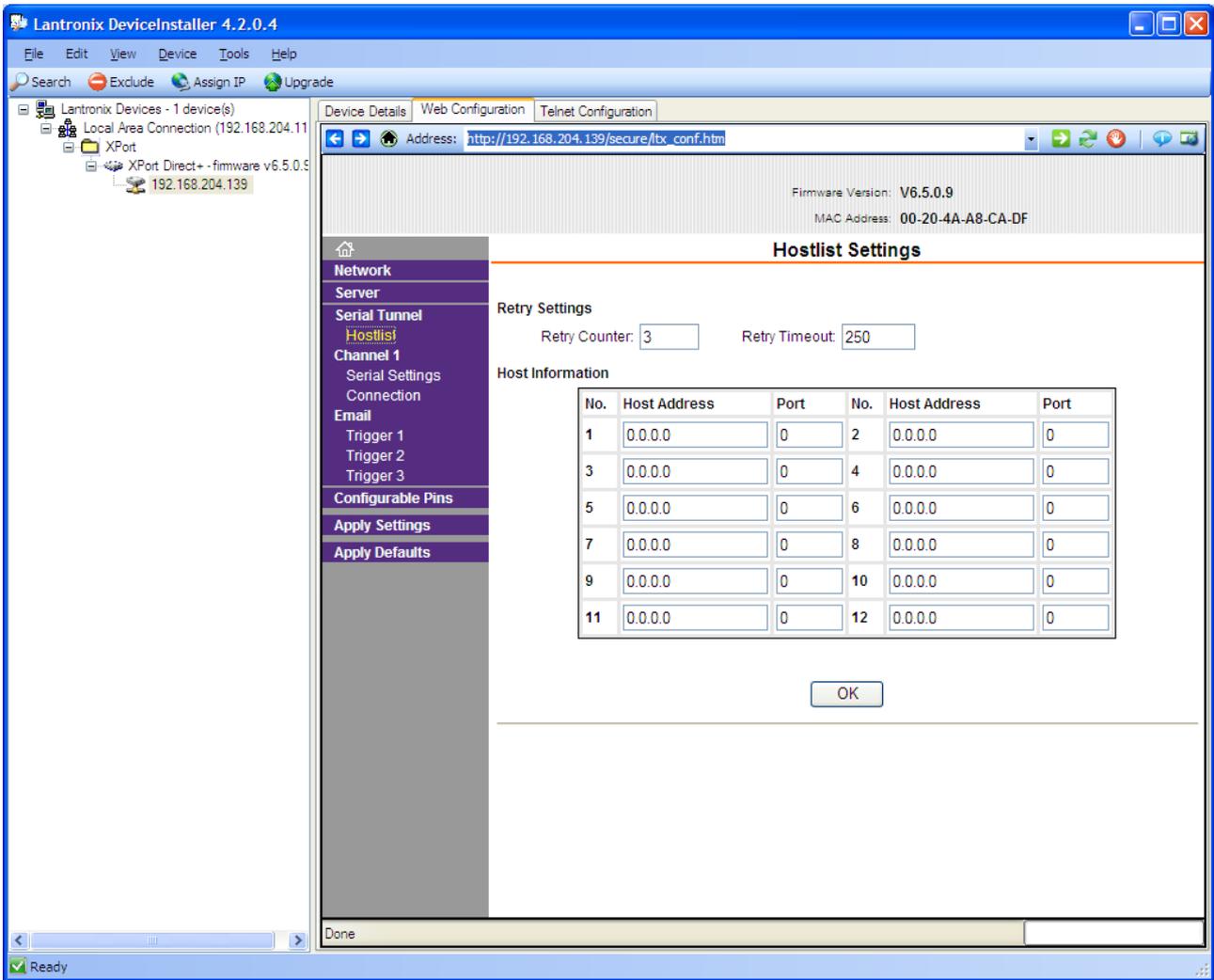
### 8. Opening an automatic connection

This connection can be a single address, listed here as "Remote host":



### 9. Ethernet connection settings

Alternatively you can create a hostlist and the EAP will connect to the first available address:

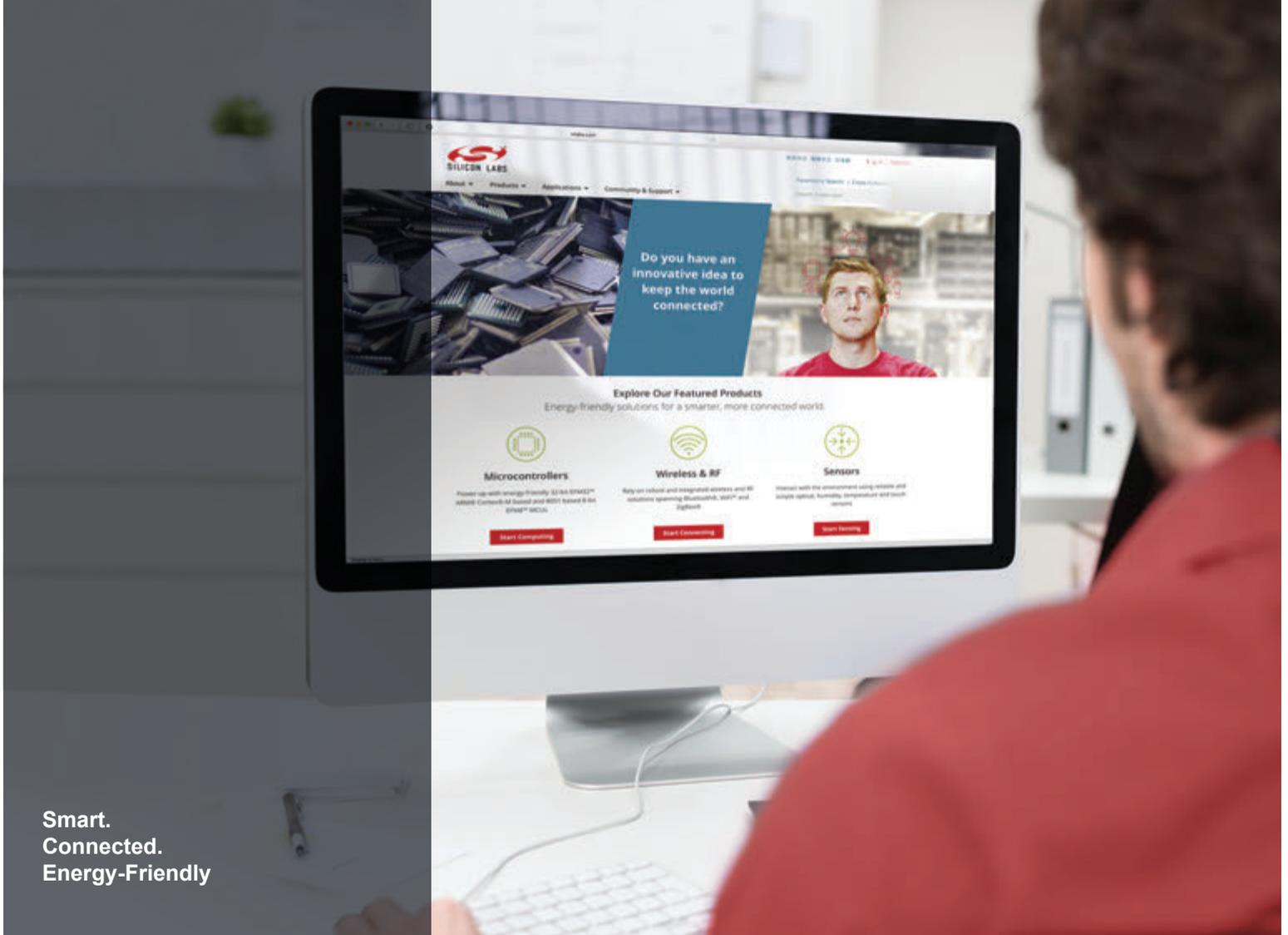


### 10. Hostlist

Consult the latest user guide for the full details, which is currently downloadable from [www.lantronix.com/support/downloads/?p=XPORTDIRECTPLS](http://www.lantronix.com/support/downloads/?p=XPORTDIRECTPLS)

## 6 Warning

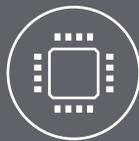
Putting a hole in your gateway’s firewall has possible security implications which are outside the scope of this note. A malicious port scanner could exploit this hole, but it would only be able to access the EAP unit. There may be critical ZigBee systems where this is not acceptable, but this note is only an introduction to setting up a simple link.



Smart.  
Connected.  
Energy-Friendly



**Products**  
[www.silabs.com/products](http://www.silabs.com/products)



**Quality**  
[www.silabs.com/quality](http://www.silabs.com/quality)



**Support and Community**  
[community.silabs.com](http://community.silabs.com)

**Disclaimer**

Silicon Laboratories intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Laboratories products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Laboratories reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Laboratories shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System without the specific written consent of Silicon Laboratories. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Laboratories products are not designed or authorized for military applications. Silicon Laboratories products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

**Trademark Information**

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR®, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISModem®, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress® and others are trademarks or registered trademarks of Silicon Laboratories Inc. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.



**SILICON LABS**

Silicon Laboratories Inc.  
400 West Cesar Chavez  
Austin, TX 78701  
USA

<http://www.silabs.com>