PowerGrid DH-10P

Powerline Ethernet Adapter

User’s Manual

Version A1.0. - 2007

260081-00

COMTREND
Leading the Communication Trend

IMPORTANT NOTICE TO THE USER

COMTREND PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IN NO EVENT SHALL COMTREND, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, PROPERTY DAMAGE, PERSONAL INJURY OR LIABILITY, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE, EVEN IF COMTREND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

No part of this manual, including the products and software described in it may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or any means, without the express written permission of COMTREND.

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by COMTREND; or (2) the serial number of the product is defaced or missing.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe. All product and brand names used in this manual are used for identification purposes only and may be the registered trademarks of their respective owners. Windows and the Windows environment are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds in the US and other countries. Linux man pages obtained from the public domain.

This manual provides information to network administrators. It covers the installation, operation and applications of the PLC adapter PowerGrid DH-10P.
The reader reading this manual is presumed to have a basic understanding of telecommunications.

Recycling For The Environment

Never throw your electronic equipment out with household waste. Ask for information from your town council on how to correctly dispose of it, so that it does not damage the environment. Always respect the current legislation regarding waste disposal.

Persons who do not comply are subject to the sanctions and penalties set down in law.

The cardboard box, the plastic contained in the packaging, and the parts that make up the device can be recycled in accordance with regionally established regulations.

The symbol of the container with the cross, which is found on the device means that when the equipment has reached the end of its working life, it must be taken to the recycling centres provided, and that its processing must be separate from that of domestic waste.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY COMTREND. COMTREND ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Copyright

SAFETY PRECAUTIONS

To avoid personal injury and damage to the system:

1. **The principal method to disconnect completely from the electrical power network (mains) is to unplug the equipment itself from the mains socket.**
2. **Never install the unit in wet areas or next to radiators/heaters.**
3. **Never use the unit outside.**
4. **Unplug the unit during severe storms.**
5. **Never open the equipment enclosure.**
6. **The equipment has parts that are not replaceable by the user. In case of failure ask your supplier to repair or replace the damaged unit.**
7. **Never try to repair a damaged unit by yourself.**

Table of Contents

1 Introduction

This document describes the configuration of COMTREND's in-home PLC adapters **PowerGrid DH-10P** with **Spirit 2.2** using the **Web interface**. The scope of this document is to describe the configuration of the available parameters as well as give a basic introduction to their function. It is intended as a guide for configuration only; no advanced description of the functionalities available is given.

The information presented in this document is intended for an audience with some knowledge of data communication and informatics as well as signal processing. Basic understanding of TCP/IP communication, such as IP addressing and the TCP/IP protocol stack, is necessary to fully comprehend the information presented and to perform the configuration steps.

2 How to Use This Manual

The PLC adapters will configure themselves automatically and allow communication between any peripheral equipment (PC, printer, etc.) without any further configuration. We do, however, strongly recommend that some minimum steps are followed to set up a protected home network. As in a wireless network, if no changes are made to the configuration of the equipment in a PLC network, you leave the network open for unauthorised access.

This document can be used to set up a protected in-home PLC network or to configure any of the advanced features available.

2.1 Sections Included in This Document

- **PLC Home Scenarios:** Examples of PLC adapter network scenarios and installation of the PLC adapter.

- **Getting Started with the Adapter:** The most elementary steps to set up a protected in-home network.

- **Advanced Configuration**: Add customized options to your PLC network such as prioritization and multicast configuration, etc.

ALL USERS SHOULD READ THE SECTIONS:

- In-Home Scenarios;
- Getting Started with the Adapter;

The Advanced Configuration section is intended for users who want to add features to improve the performance of the network or add special characteristics to their network.

3 In-Home Scenarios

3.1 Adapter Installation

The installation of the adapter is straightforward; simply plug the adapter into the electrical outlet and connect your PC or any other equipment to it.

However, to optimize the performance of your PLC network you should take care to:

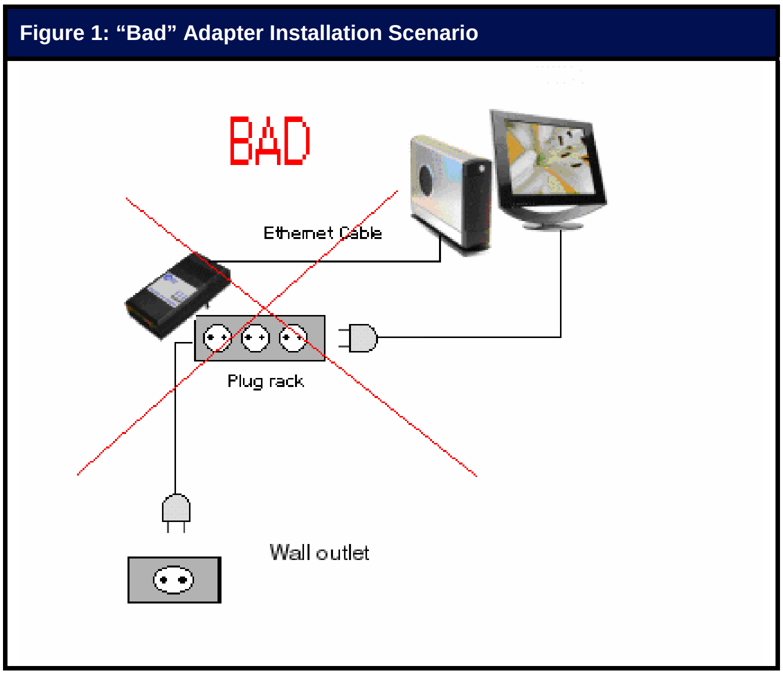
- **Plug the adapter directly into the wall outlet;**
- **Not to use extension cords or power strips with the adapter.**

The following subsections give some examples of recommended and NOT recommended installation scenarios.

3.1.1 “Bad” Adapter Installation Scenario

Figure 1 shows an example of a PLC adapter installation that is **NOT recommended**.

Figure 1: “Bad” Adapter Installation Scenario



Note that the adapter has been plugged into a power strip together with the other electrical appliances.

3.1.2 “Good” Adapter Installation Scenarios

Figure 2 and Figure 3 are examples of **recommended** PLC adapter installations.

Figure 2: Example 1 of a “Good” Installation Scenario

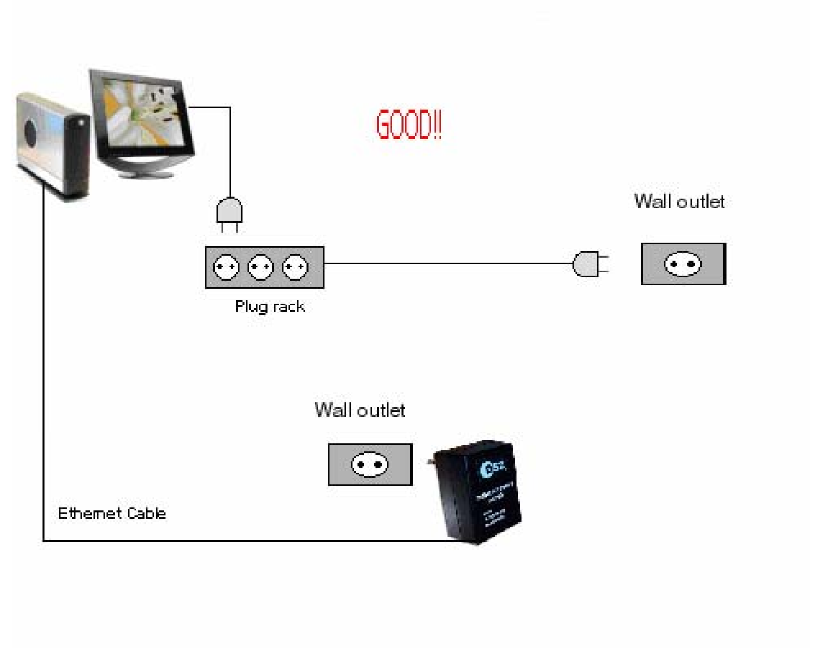
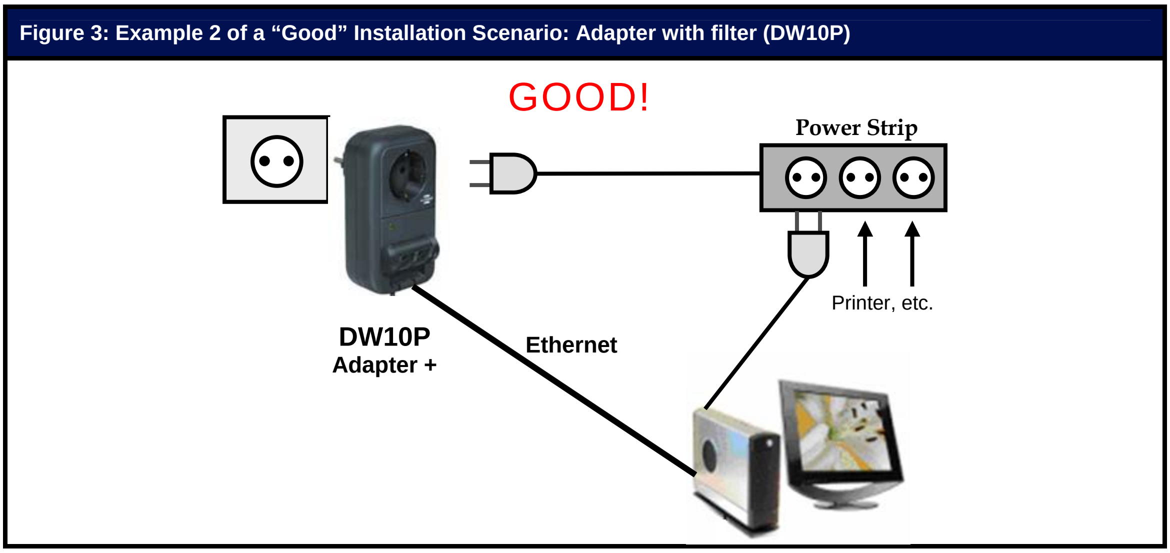


Figure 3: Example 2 of a “Good” Installation Scenario: Adapter with filter (DW10P)



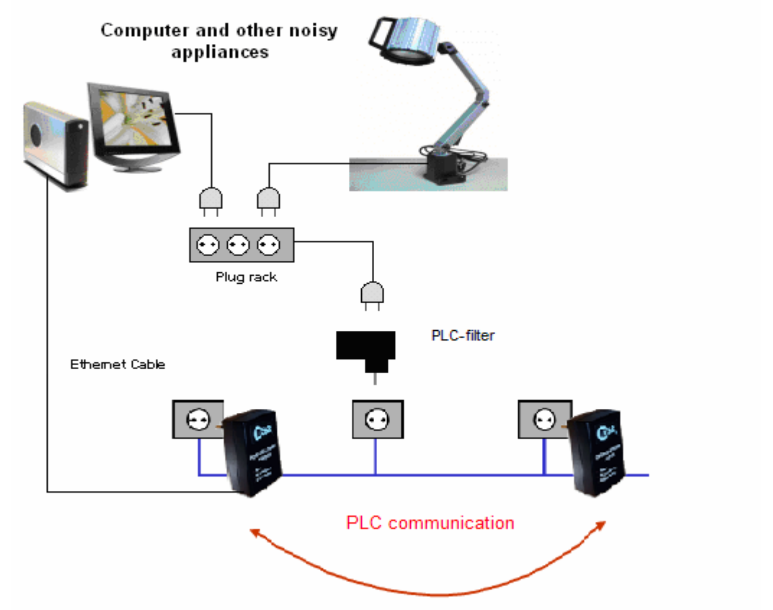
The best installation methods are to use separate plugs for the electrical appliances and the PLC adapters, as illustrated in Figure 2, or to use filtered power strips such as the one shown in Figure 3.

3.2 Using PLC Filters

A PLC filter is a low-pass filter that will only allow the 50/60 Hz mains voltage through; the PLC signal will be blocked as well as "noise" in higher frequencies. Below is an example of when to use such a filter:

- **Filtering noisy appliances**
  The filter can be used to filter the noise produced by electrical appliances. Examples of equipment that might affect the adapter's performance are computer, printer, mobile phone, or any other electrical appliances in general. The noise from these appliances might affect your equipment if plugged in very close to the adapter. An example of how to use the adapter to filter "noisy" appliances can be seen in Figure 4.

Figure 4: PLC Filter



Note that the plug rack is plugged in to the **plc-filter** and not directly in to the wall socket.

3.3 Examples of In-Home Scenarios

Two possible home scenarios are presented as a framework to demonstrate the capabilities of the in-home adapters. The two topologies are presented in Figure 5 and Figure 6.

Figure 5: Data-Only PLC Network

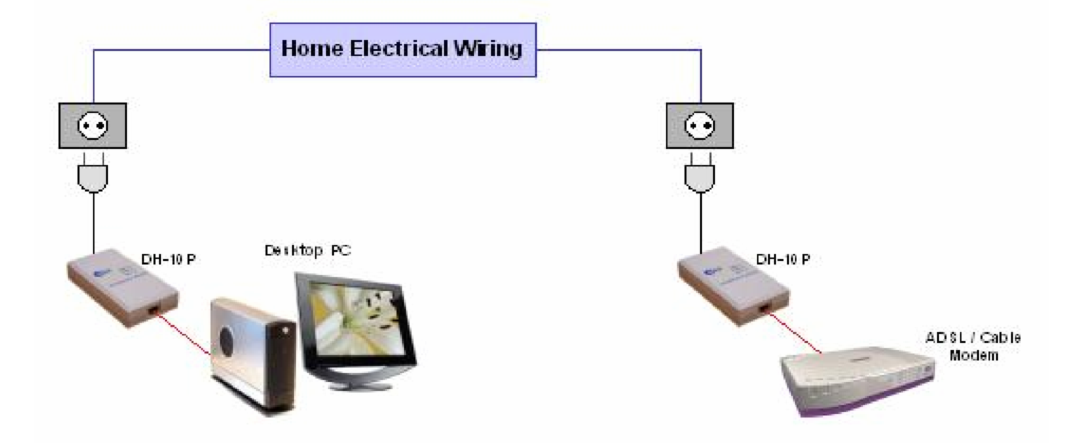


Figure 5 shows a simple PLC solution where two adapters are used to make the Internet access connection available in the electrical outlets of the home. This is a simple network with only two adapters and only data traffic, where CoS probably would not be required.

Figure 6: Mixed Data-Video PLC Network

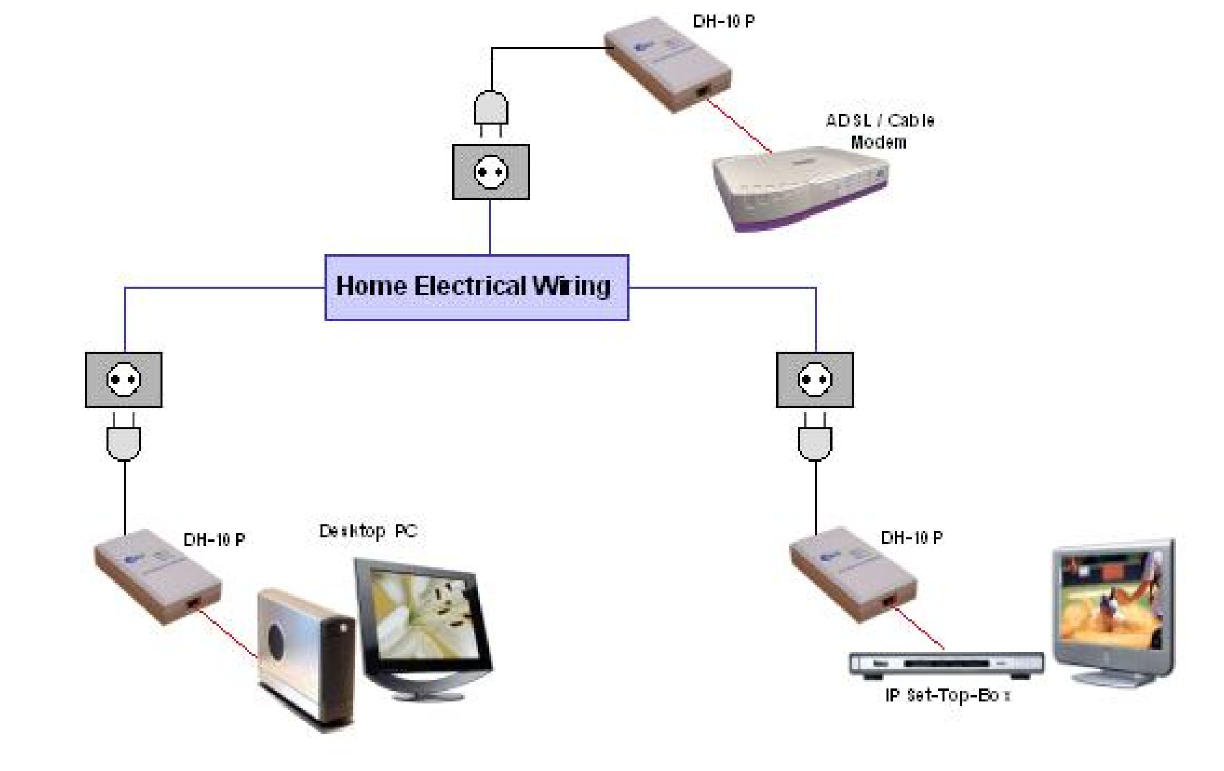


Figure 6 shows a more advanced PLC network with three adapters. Internet access and digital video are delivered through the ADSL/cable line and distributed inside the home using PLC. This network might require some CoS settings to guarantee video quality when the network is congested with data. To configure your network using CoS, please see Section 5.8: *Traffic Classifier*.

Either of these two basic scenarios can be enlarged by adding more adapters, computers, and set-top boxes.

4 Getting Started with the Adapter

4.1 Equipment Necessary for Using the Adapters

- Ethernet cable (as provided with the adapters)
- A PC (with an OS such as Windows, Linux, MacOS or Unix)

Also the following might be needed at some time:

- **FTP (or TFTP) server** (to perform a firmware upgrade)

4.2 Adapter Default Settings

Web Page Password	Enabled (default password: **paterna**)
IP	Static **(10.10.1.69)**
Subnet Mask	255.255.0.0
MAC Mode	Automatic In-Home AV
Service Classifier	Disabled
Traffic Classifier	Disabled
Factory Reset Password	**betera**
Network ID	Public
Encryption	None

4.3 Identifying Adapter Chip Type: DSS9010 or DSS9001

The adapters come with an identification code on the cover. You can tell if the adapter has a DSS9010 or a DSS9001 chip by the part number (PN), as shown below:

PN: A1-6UXX-XXX	DSS9010 chip in a DH10P
PN: A1-7CXX-XXX	DSS9001 chip in a DH10P

4.4 Adapter Configuration Steps

4.4.1 Changing the IP Address of the Adapter

This step is not required when using the L2 tool. For more information about configuring the adapters with the L2 tool please see COMTREND's L2 Configuration Tool User Guide *document.*

All of the adapters are delivered with a static default IP address. It is necessary to change the IP address if you want to access the Web interface of the adapters when two or more units are active in the same network.

Follow the steps below to configure a new IP address for the adapters:

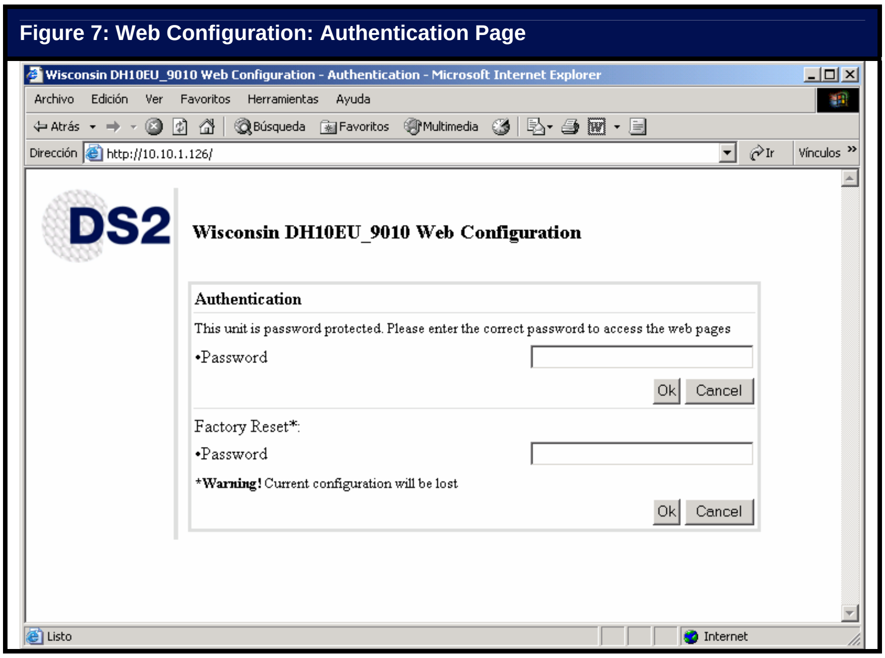
1. Assign the PC an address in the range 10.10.*x.x* and the netmask 255.255.0.0. This is necessary in order to be compatible with the adapter's default settings;

2. Plug in one of the PLC adapters and connect it to the PC using the Ethernet cable provided with the adapter;

WARNING: ONLY PLUG ONE ADAPTER AT A TIME INTO THE WALL OUTLET IF THE IP ADDRESS OF THE ADAPTER HAS NOT BEEN CHANGED FROM THE DEFAULT.

3. Open the Web browser and type the following URL: http://10.10.1.69. A Web page similar to the one in Figure 7 will appear;

Figure 7: Web Configuration: Authentication Page


Wisconsin DH10EU_9010 Web Configuration - Authentication - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://10.10.1.126/
Ir Vínculos
Listo
Internet

Wisconsin DH10EU_9010 Web Configuration

Authentication

This unit is password protected. Please enter the correct password to access the web pages

•Password

Ok Cancel

Factory Reset*:

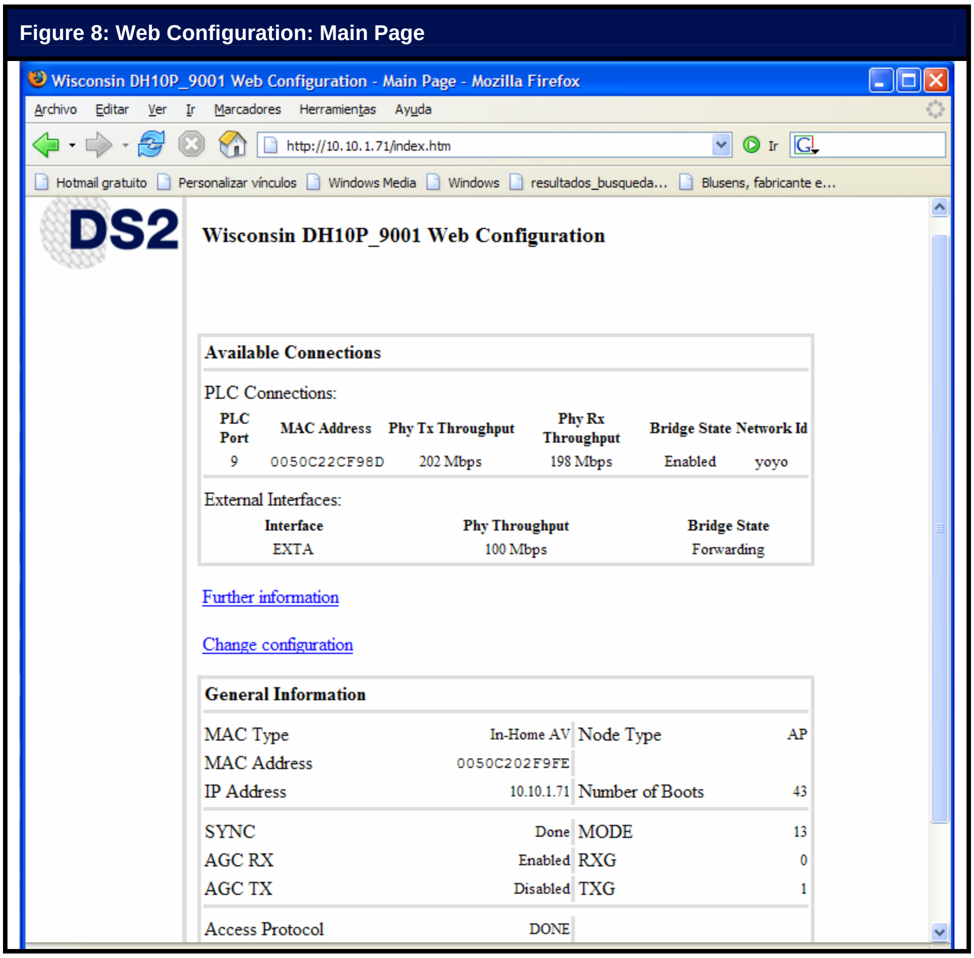
•Password

***Warning!** Current configuration will be lost

Ok Cancel

4. In the *Password* field, type in the default password (**paterna**) and click the *OK* button. A adapter information page similar to the one shown in Figure 8 will appear:

Figure 8: Web Configuration: Main Page


Wisconsin DH10P_9001 Web Configuration - Main Page - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://10.10.1.71/index.htm
Ir
Hotmail gratuito Personalizar vínculos Windows Media Windows resultados_busqueda... Blusens, fabricante e...

Wisconsin DH10P_9001 Web Configuration

Available Connections

PLC Connections:

PLC Port	MAC Address	Phy Tx Throughput	Phy Rx Throughput	Bridge State	Network Id
9	0050C22CF98D	202 Mbps	198 Mbps	Enabled	yoyo

External Interfaces:

Interface	Phy Throughput	Bridge State
EXTA	100 Mbps	Forwarding

Further information

Change configuration

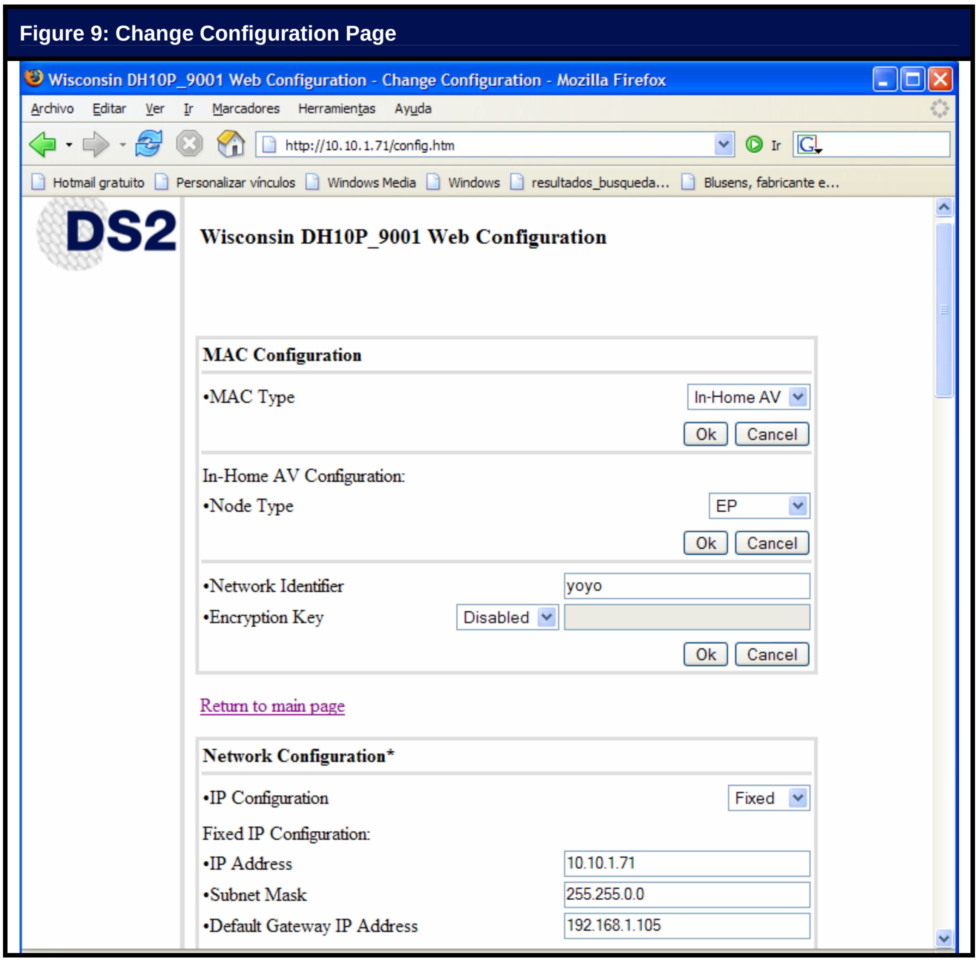
General Information

MAC Type	In-Home AV	Node Type	AP
MAC Address	0050C202F9FE		
IP Address	10.10.1.71	Number of Boots	43
SYNC	Done	MODE	13
AGC RX	Enabled	RXG	0
AGC TX	Disabled	TXG	1
Access Protocol	DONE		

The Main page shows an overview of all visible adapters in the Available Connections section. The connection speeds to any other adapters with direct visibility to the adapter to which you are connected can be seen here. See Section 4.5: *Checking Powerline Network Performance* for more information regarding the PLC Connections menu;

5. Click on *Change configuration* and a new page will appear (Figure 9). This page allows you to change the configuration of the adapter;

Figure 9: Change Configuration Page


Wisconsin DH10P_9001 Web Configuration - Change Configuration - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
http://10.10.1.71/config.htm
Ir
Hotmail gratuito
Personalizar vínculos
Windows Media
Windows
resultados_busqueda...
Blusens, fabricante e...
DS2

Wisconsin DH10P_9001 Web Configuration

MAC Configuration

•MAC Type: In-Home AV

Ok Cancel

In-Home AV Configuration:

•Node Type: EP

Ok Cancel

•Network Identifier: yoyo

•Encryption Key: Disabled

Ok Cancel

Return to main page

Network Configuration*

•IP Configuration: Fixed

Fixed IP Configuration:

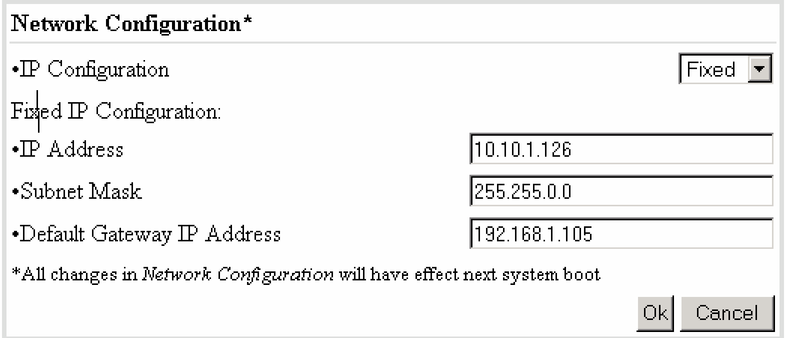
•IP Address: 10.10.1.71

•Subnet Mask: 255.255.0.0

•Default Gateway IP Address: 192.168.1.105

6. In the Network Configuration section, enter the desired IP address, netmask, and gateway for the adapter. An example is shown in Figure 10. (See also the notes on page 12 for more information);

Figure 10: Change Configuration Page: Network Configuration



Network Configuration*

•IP Configuration: Fixed

Fixed IP Configuration:

•IP Address: 10.10.1.126

•Subnet Mask: 255.255.0.0

•Default Gateway IP Address: 192.168.1.105

*All changes in *Network Configuration* will have effect next system boot

Ok Cancel

7. Click the *OK* button to store the values in the memory. Wait for the Web page to refresh;

8. Unplug (or reboot) the adapter, plug in another adapter and go back to Step 2.

NOTES:

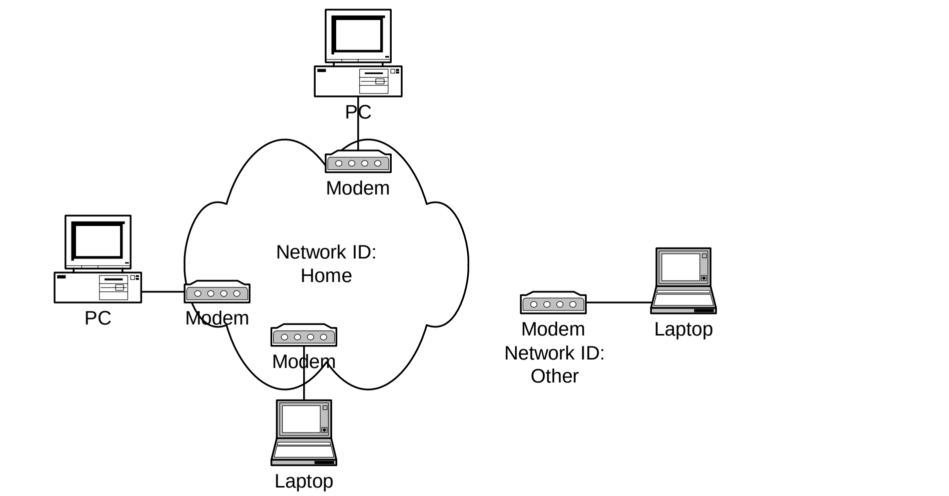
- **Setting the IP:** A different IP must be set for each of the adapters that will work on the same network. Only the PC accessing the configuration page of the adapters must have the same address range as the adapters;
- **Netmask:** The netmask can also be changed, for example to a type C (255.255.255.0) if needed;
- **Gateway IP:** If the adapter is going to be accessed through a router (for example in a large office network) the gateway IP needs to be configured. Otherwise, it can be ignored;
- **Reboot:** The IP change in the adapters will be effective only after a reboot or a power cycle. COMTREND recommends placing a label on each adapter with the IP address assigned to it (see warning below).

WARNING: IF YOU CHANGE THE IP AND SUBSEQUENTLY FORGET IT, YOU WILL NEED THE L2 TOOL TO RESET THE ADAPTER TO ITS ORIGINAL VALUES.

4.4.2 Setting a Network Identifier

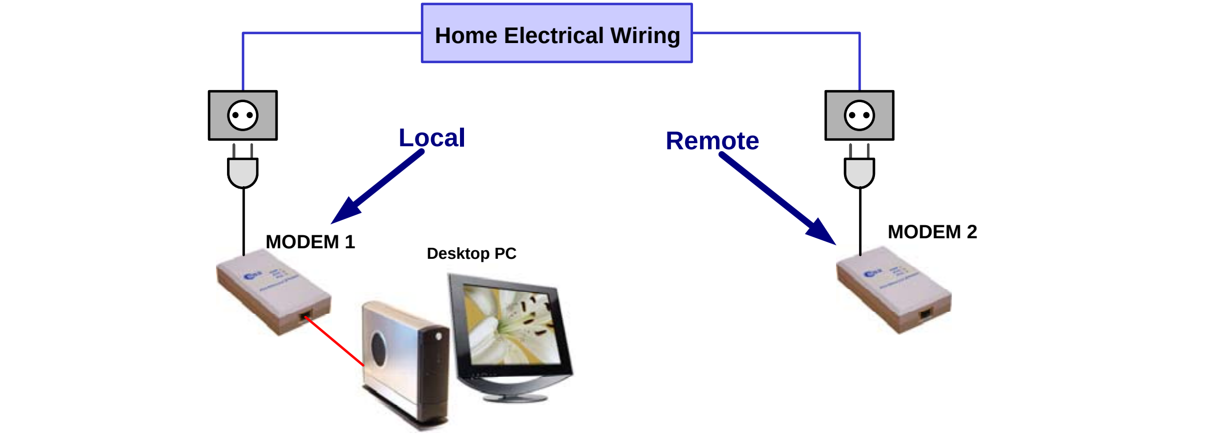
It is strongly recommended to always use a Network Identifier (NID) in your network as this will protect your network from eavesdropping. It is also necessary to specify the NID if you want to set a Fixed AP in your network. The **same NID** will have to be specified in all adapters in the network to allow communication between them. (See Section 5.1: *Changing In-Home AV Node Type* for more information about setting the Fixed AP.)

Figure 11: A Adapter with a Different Network Identifier Cannot Communicate



When changing the NID, please make sure that it is changed in the node(s) connected over the powerline first. When you have changed the NID in one adapter, that adapter will lose connection to the other nodes in the network until they also have the same NID. In the example network seen in Figure 12, the computer is connected to **Adapter 1** and communication with **Adapter 2** is through the powerline. In this network, **Adapter 1** is the **local** node and **Adapter 2** is the **remote** node.

Figure 12: Local and Remote Nodes



Perform the following steps to change NIDs:

1. Plug all adapters into the powerline. Make sure that all powerline adapters are connected. If you are having problems with connectivity between the adapters, please refer to Section 4.5: *Checking Powerline Network Performance*;

2. Connect to the Web page of one of the remote powerline adapters;

3. Go to the Change Configuration menu;

4. In the *Network Identifier* field write the name of choice for your network. Any combination of letters and numbers can be used; for example: COMTRENDpower;

5. Press the *OK* button. At this point you will lose connection to the remote node since the NID has been added but you have not yet set one for the local node;

6. Connect to any remote adapter remaining and repeat Steps 2 through 6;

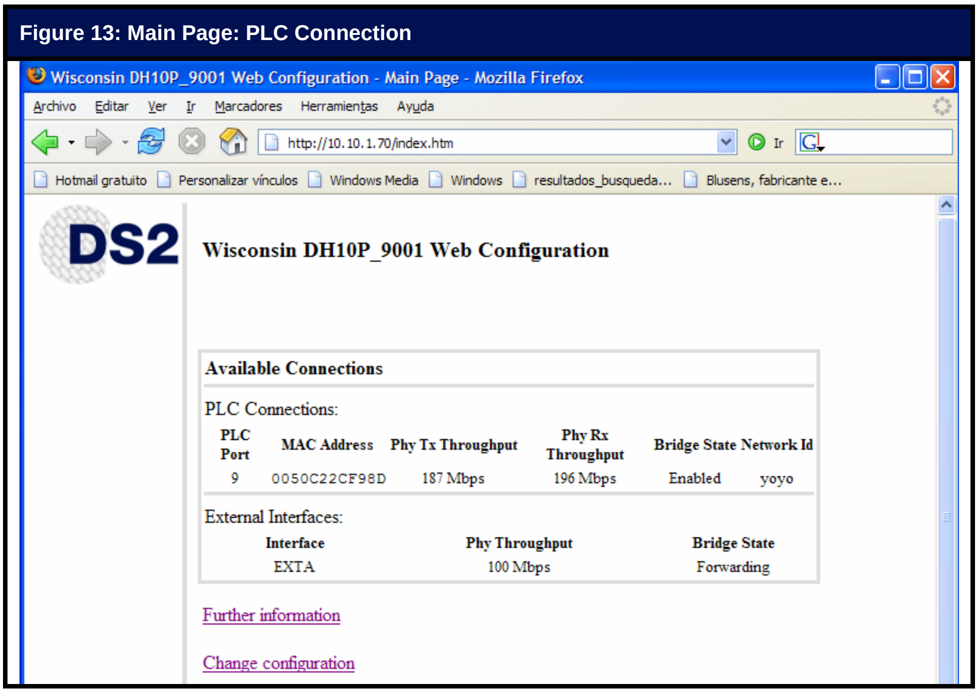
7. Finally connect to the local adapter and repeat Steps 2 through 6.

After you have changed the NID of the local adapter you will recover communication with all of the powerline adapters.

4.5 Checking Powerline Network Performance

In the Main page in PLC Connections section is a list of the MAC addresses of all of the neighbouring adapters that have a connection with the device. This list also indicates the physical throughput in transmission and reception that the device is achieving with each neighbour. The PLC Connections screen is shown in Figure 13.

Figure 13: Main Page: PLC Connection



Wisconsin DH10P_9001 Web Configuration - Main Page - Mozilla Firefox

Wisconsin DH10P_9001 Web Configuration

Available Connections

PLC Connections:

PLC Port	MAC Address	Phy Tx Throughput	Phy Rx Throughput	Bridge State	Network Id
9	0050C22CF98D	187 Mbps	196 Mbps	Enabled	yoyo

External Interfaces:

Interface	Phy Throughput	Bridge State
EXTA	100 Mbps	Forwarding

Further information

Change configuration

The PLC Connection section contains six headers:

PLC Port	An internal value for the adapter to handle the different connections.
MAC Address	The MAC address of the connected adapter.
Phy Tx Throughput	The powerline throughput in Mbps from the local adapter to the remote adapter.
Phy Rx Throughput	The powerline throughput in Mbps from the remote adapter to the local adapter.
Bridge State	When the adapters are up and functioning, there can be two different states: • **Enabled:** A adapter connected to your network. • **Disabled:** A adapter with a different NID than your network without access to your network.
Network ID	The Network ID of your network. Only your local ID will be visible, not the NIDs of other networks.

5 Advanced Configuration

5.1 Changing In-Home AV Node Type

A node can be defined as an End Point (*EP*) or fixed Access Point (*AP*). To change the node, follow the steps below – see also Figure 14 which shows the MAC Configuration Section:

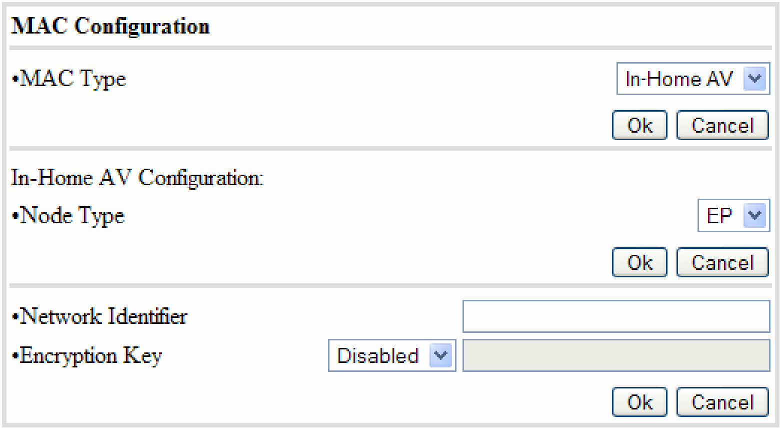
> **WARNING: A NETWORK ID (NID) HAS TO BE SET BEFORE A NODE CAN BE CHANGED TO A STATIC AP. SEE SECTION 4.4.2 FOR INFORMATION ON** *CHYBA! NENALEZEN ZDROJ ODKAZŮ.* **HOW TO SET THE NID.**

1. In the *Node Type* field, select “Fixed AP”;

2. Click the *OK* button. Wait for the Web page to be updated;

3. Verify the changes on the adapter’s main page “http://<ip_address>”.

Figure 14: Change Configuration Page: MAC Configuration Section



MAC Configuration

•MAC Type In-Home AV

Ok Cancel

In-Home AV Configuration:

•Node Type EP

Ok Cancel

•Network Identifier

•Encryption Key Disabled

Ok Cancel

5.2 Setting Advanced Security

Triple-DES (3DES) encryption of the data transmission between adapters can be enabled by specifying an Encryption Key in the *Encryption Key* field in the MAC Configuration section.

Encryption can be configured only if the NID of the adapter is not the public, otherwise malfunctions can occur.

5.2.1 Enabling Triple-DES Encryption

To enable Triple-DES encryption, perform the following steps:

1. Make sure that there is connectivity between the powerline adapters. If you are having problems with connectivity between adapters, please see Section 4.5: *Checking Powerline Network Performance*;

2. Connect to the Web page of one of the **remote** powerline adapters;

WARNING: THE ENCRYPTION KEY SHOULD ALWAYS BE SET IN THE REMOTE ADAPTERS BEFORE BEING CHANGED IN THE LOCAL ADAPTER. PLEASE SEE FIGURE 12 FOR A DESCRIPTION OF LOCAL AND REMOTE ADAPTERS.

3. Go to the *Change Configuration* menu;

4. In the *Encryption Key* field in the MAC Configuration section shown in Figure 14, select ASCII or HEX from the drop down menu and type in the key of your choice for the network. Any combination of letters and numbers can be used if ASCII is selected, for example: 3DESCOMTREND and any hexadecimal digits if HEX is selected, i.e. 355AB6C;

5. Press the *OK* button. At this point you will lose connection to the remote node where 3DES has been enabled since you have not yet set 3DES in the local adapter;

6. Connect to any other remaining **remote** adapters and repeat Steps 2 through 5;

7. Finally, connect to the **local** adapter and repeat Steps 2 through 5;

After you have changed the encryption key of the local adapter, you will recover communication with all of the powerline adapters.

If you want to **disable** 3DES encryption, repeat the same steps above leaving the *Encryption Key* field empty.

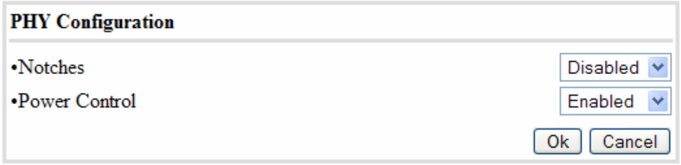
5.3 Configuration of PLC Notches

If the adapter is running in an environment where it can cause interference with amateur radio reception, spectral masking can be enabled. This option, called “notching”, will remove the PLC signal from the frequency bands used by radio amateurs (IARU).

To enable notches for the powerline adapter:

1. Go to the PHY Configuration section of the Change Configuration page (see Figure 15);
2. Click on the drop-down-menu (*Disabled* by default) and select *Enabled*;
3. Click the *OK* button. Wait for the Web page to be refreshed.

Figure 15: Change Configuration Page: PHY Configuration Form (for a DSS9001- or DSS9010–Based Model)



PHY Configuration

•Notches: Disabled

•Power Control: Enabled

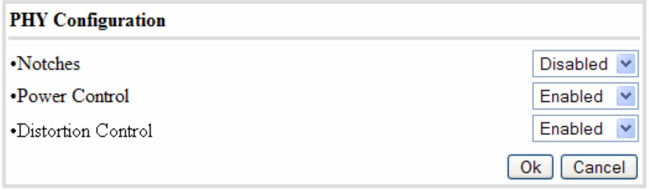
5.4 Power Control

If two or more networks (different Network IDs) are running in the same channel, it is preferable to isolate them. Power Control is a feature that minimizes the transmission power of each adapter based on the measured physical throughput while maintaining a certain level of performance. It is *Enabled* by default as can be seen in Figure 15. Power Control can be disabled by selecting *Disabled* in the pull-down-menu and clicking OK.

5.5 Distortion Control

Some reference designs have an extra parameter, the distortion control. By default the distortion control is enabled; when disabled the power output of the adapter will increase. This power output increase might improve the performance of your PLC connection under certain circumstances, but with the risk of distortion. Distortion will cause the performance (Mbps) of the adapter to drop. Distortion control can be enabled or disabled using the drop-down menu, shown in Figure 16.

Figure 16: Change Configuration Page: PHY Configuration Form (for a DU100 Model)



PHY Configuration

•Notches: Disabled

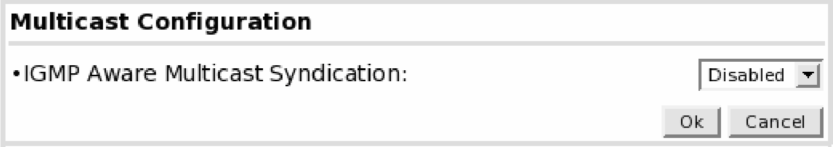
•Power Control: Enabled

•Distortion Control: Enabled

5.6 Multicast Traffic Configuration

The new *IGMP Aware Multicast Syndication* feature included in Spirit 2.0 can be enabled via the form shown in Figure 17. This feature is only available in private networks and end points.

Figure 17: Web Configuration: Multicast Configuration



Multicast Configuration

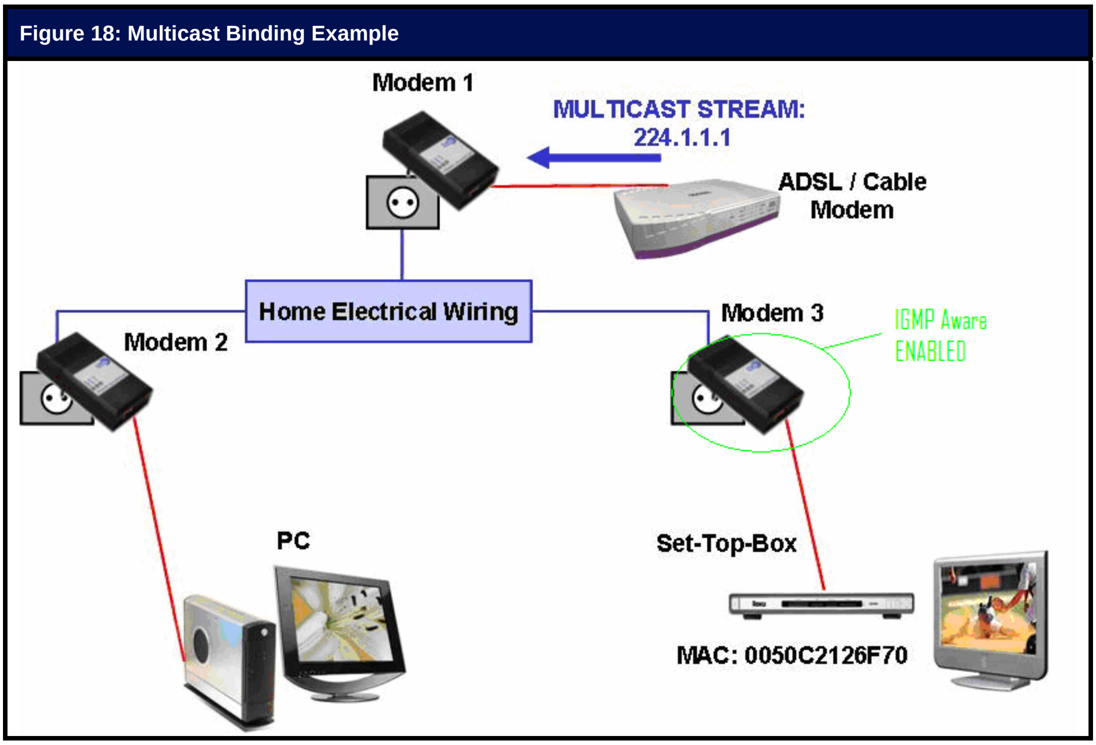
•IGMP Aware Multicast Syndication: Disabled

By default, if IGMP is disabled in every EP, multicast traffic is sent to all devices in the PLC network by duplicating packets.

In the example in Figure 18, a multicast stream using the IP 224.1.1.1 is entering the PLC network from Adapter 1. The intended destination for the multicast stream is only the set-top box connected to Adapter 3. However, the multicast stream will be duplicated and it will reach both Adapter 2 and Adapter 3. This is done by default when IGMP Aware Multicast Syndication is not enabled in Adapter 3. To ensure that only Adapter 3 receives the multicast traffic:

- Enable IGMP Aware Multicast Syndication in Adapter 3 (confirm by clicking OK). If the STB is IGMP snooping compliant (and the provider's network also), Adapter 3 will detect IGMP join messages to a Multicast group from the STB. An internal route will be then be created by the PLC network to carry this Multicast channel directly to the STB.

Figure 18: Multicast Binding Example



5.6.1 Enable IGMP Aware Multicast Syndication

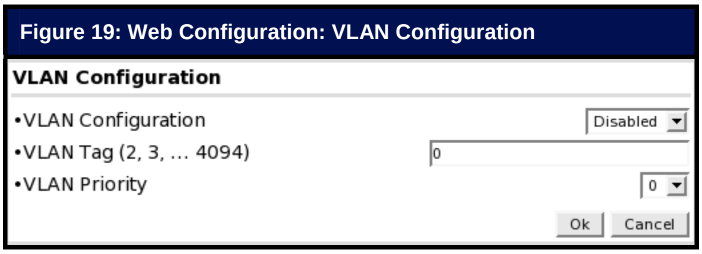
To enable IGMP Aware Multicast Syndication in an EP connected to the STB perform the following steps:

1. A Network ID should have been assigned to the PLC network (see section 4.4.2);
2. The modem connected to the backbone (i.e. Modem 1 from Figure 18 connected to ADSL adapter) should be defined as a Fixed AP (see Section 5.1);
3. Enable IGMP Aware Multicast Syndication in the adapter connected to STB (i.e. Modem 3 from Figure 18) using the specified field in the Webpage interface;
4. Click the *OK* button. Wait for the Web page to refresh.

5.7 VLAN Configuration

The parameters regarding VLAN configuration can be set in the VLAN Configuration section shown in Figure 19. The VLAN can be enabled or disabled using the pull-down *VLAN Configuration* menu. If enabled, the VLAN tag (*VLAN Tag* field) and priority (*VLAN Priority* field) can be configured. See *In-Home Technology Description* document for more information

Figure 19: Web Configuration: VLAN Configuration



VLAN Configuration

•VLAN Configuration Disabled

•VLAN Tag (2, 3, ... 4094) 0

•VLAN Priority 0

5.8 Traffic Classifier

The purpose of the traffic classifier is to prioritize traffic so that bandwidth-sensitive applications such as video or telephony continue to work smoothly even under conditions of network congestion.

5.8.1 Description of the Traffic Classifier, set-up of QoS

The configuration of the QoS is via WEB browser in the part “QoS Configuration”, or via application “PLC Adapter Config Tool” in the part QoS. Accessible possibilities of the rules are in the table, below:

Criterion 1	Criterion 2
Protocol	**Don’t set** – second rule is not use
Origin IP address	**Don’t set** – second rule is not use
Destination IP address	**Don’t set** – second rule is not use
Source TCP port	**Is possible to apply in case** - UDP Protocol or Origin and destination IP address for UDP packets
Destination TCP port	**Is possible to apply in case** - UDP Protocol or Origin and destination IP address for UDP packets
Source UDP port	**Is possible to apply in case** - TCP Protocol or Origin and destination IP address for TCP packets
Destination UDP port	**Is possible to apply in case** - TCP Protocol or Origin and destination IP address for TCP packets

For the rules we can set two priorities: LOW (minimum of throughput) and HIGH (maximum of throughput).

For LOW criteria:

- The LOW rule is not applied when: the traffic doesn’t fulfill the criteria.
- The LOW rule is applied when: the traffic fulfilled the criteria. In this case is the traffic almost suspended.

For HIGH criteria:

- The HIGH rule is not applied when: the traffic doesn’t fulfill the criteria.
- The HIGH rule is applied when: the traffic fulfilled the criteria. In this case, the traffic can to occupy the whole of bandwidth. In case of the VoIP traffic the used bandwidth correspond to the used codec. In case of the FTP traffic can be occupied the whole of bandwidth. In this case is the traffic almost suspended.

5.8.2 Service Classifier Example – Prioritization for VoIP Application nad VNC Server

Criterion 1 (prioritization for the application “VNC Server”)
Protocol – TCP with Port
Origin Port - 5900
Prioritization – High

Criterion 2 (prioritization for outgoing VoIP traffic)
Protocol – UDP
Prioritization – High

This configuration is necessary to do at the PLC adapter near to the PC with the VoIP traffic and installed application “VNC Server”.
In case of prioritization of the incoming VoIP traffic, there is necessary to set rule at the PLC which is on the input side. Most common it is PLC near to the ADSL router. **! In the Criterion 1 will be set Destination Port instead of the Origin Port !**
Rozdílná bude pouze konfigurace u Criterion 1, kde Origin Port nahradí Destination Port s hodnotou 5900.

Basically, The QoS criteria are set on the outgoing direction. And there are used source and destination parameters (e.g. IP address and Port).

.

5.9 Setting the Password for Access to the Web Application

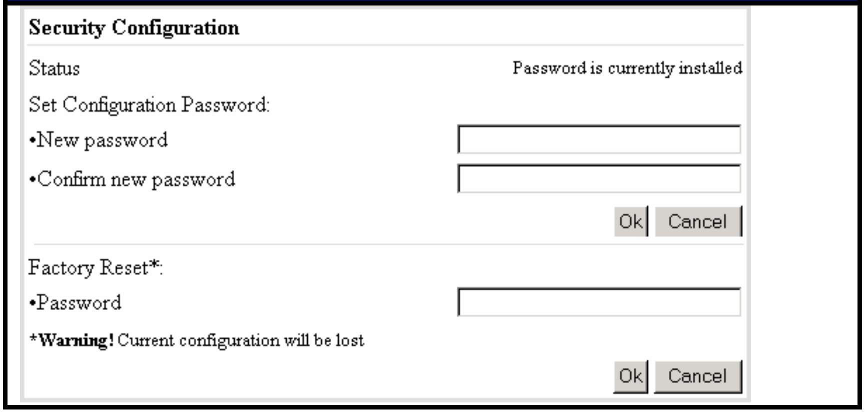
The Web application password restricts access to the configuration page. When attempting to access the configuration Web page of the adapter, you will be prompted for a password. To configure a password for the Web application, go to the Security Configuration form, shown in Figure 20 and:

1. Specify the password in the *New Password* and *Confirm New Password* fields;

2. Click the *OK* button. Wait for the Web page to refresh.

It is now necessary to enter the password to access the configuration page.

Figure 20: Change Configuration Page: Security Configuration Form



Security Configuration

Status Password is currently installed

Set Configuration Password:

•New password

•Confirm new password

Factory Reset*:

•Password

***Warning!** Current configuration will be lost

The password can be **disabled** by leaving the two fields, *New Password* and *Confirm New Password*, empty and pressing the *OK* button. The message “*No password installed*” will be shown in the security configuration form.

5.10 Factory Reset – Resetting the Adapter to Default Values

The factory reset will return the adapter to the original configuration (as described in Section 4.2). A *remote factory reset can also be done using the L2 tool; for more information please see COMTREND's* L2 Configuration Tool User Guide *document.*

A specific password is required to perform a factory reset. The password is ***betera***.

To perform a factory reset, type the password in the *Factory Reset* field and click the *OK* button. Wait for the Web page to refresh.

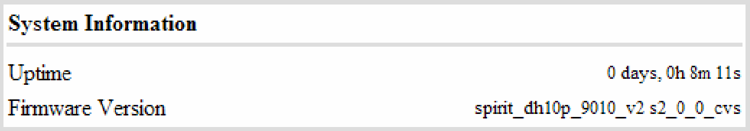
5.11 Firmware Upgrade

To upgrade the adapter's firmware, an FTP server must be running on the computer. COMTREND recommends a freeware tool called *Quick 'n Easy FTP Server*. This tool can be downloaded at the following address: http://www.pablosoftwaresolutions.com/.

5.11.1 Checking Firmware Installed

To verify the current firmware installed in your adapter go to the *Further Information* page, as shown in Figure 21. The current firmware installed is specified in the System Information section at the top of the page.

Figure 21: Further Information Page: System Information



System Information

Uptime	0 days, 0h 8m 11s
Firmware Version	spirit_dh10p_9010_v2 s2_0_0_cvs

The firmware version field consists of the platform type, the chip type, the clock speed and the flash size as well as the version. The format used is:

spirit_*<platform>*_*<chip_type>*_"*<clock_speed>*_""<hw version>-"*<version>*_cvs"

Platform Types	**du100** **dh10p**
Chip Types	**9001** **9010**
Clock Speed (**ONLY DU100**)	**80 MHz** **160 MHz**
HW version	**None (version by default)** **v<number>**

The characteristics of the firmware adapter shown in Figure 21 (*spirit_dh10p_9010_v2_s2_0_0_cvs*) are:

Platform Type	dh10p
Chip Type	9010
HW version	V2
Firmware Type	2_0_0
Clock Speed (**ONLY DU100**)	When not specified it is 160 MHz. clkint80 → 80 MHz

5.11.2 Selecting Firmware File for Upgrade

The firmware files for the upgrade have the same format as the file specified in the *System Information* section. The only difference is that the firmware files have an extra parameter for selecting the type of upgrade. An example of a firmware file is:

spirit_dh10p_9010_v2-s2_0_17_cvs_remote_app.ftp

Note that only files ending with **ftp** can be used to upgrade the adapter through the Web page.

The last parameter, in the example above, "remote_app" specifies the type of upgrade file. There are three different possibilities for an upgrade through the Web page:

app	Firmware only
loader	Boot loader only
config	Factory settings only

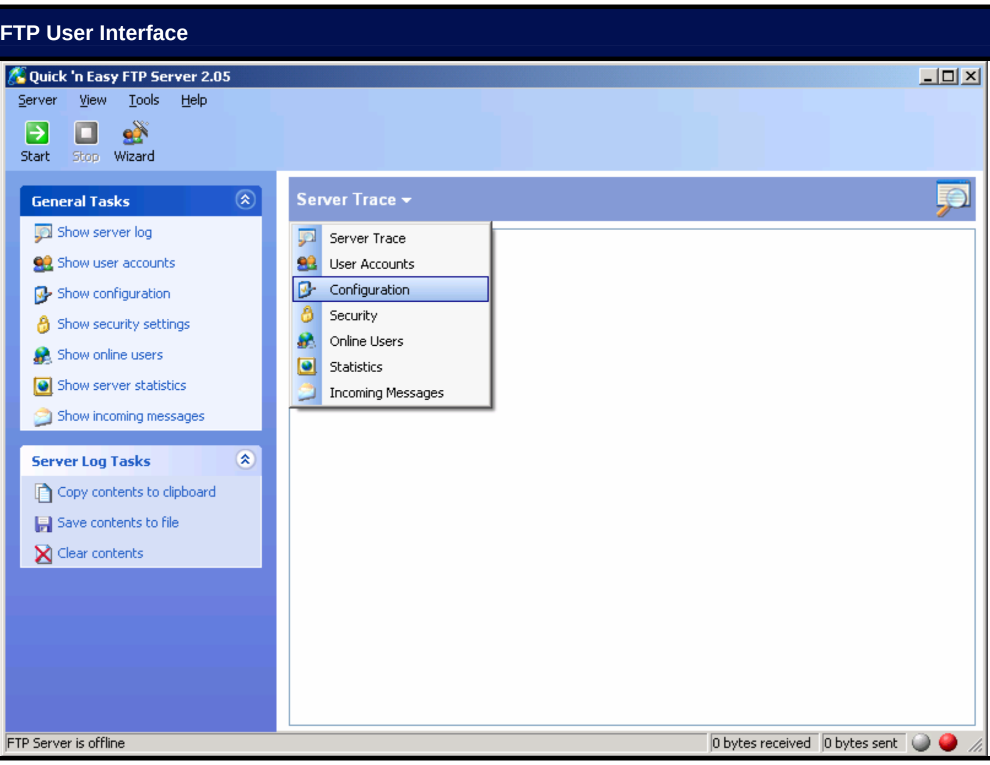
When upgrading the adapter's firmware, you will have to specify the type of upgrade you wish to perform.

5.11.3 Performing a Firmware Upgrade

Follow the steps below to upgrade the adapter’s firmware:

1. Open the *Quick ‘n Easy FTP Server* (see Section 5.11). This application has the GUI shown in Figure 22;

Figure 22: FTP User Interface



FTP Server is offline | 0 bytes received | 0 bytes sent

2. Place the image file in the directory specified in the *Configuration* section or change it to point to the location where the image is stored;

3. Open the Web browser and enter the IP of the adapter to be upgraded;

4. When the page opens, click *Change configuration*;

5. Go to the *Firmware Update* section and specify the upgrade parameters (as shown in Figure 23):

    a. Specify the desired upgrade type in the *Flash Section* drop-down menu:

    - Firmware
    - Loader
    - Factory settings

    b. In the *Upgrade Protocol* drop-down menu, select *FTP*.
    c. Enter the IP address of the PC with the installed FTP server in the *Server IP Address* field.
    d. Specify the name of the firmware image file in the *File Name* field.

WARNING: CONFIRM THAT THE PLATFORM AND CHIP ARE THE SAME AS THAT OF THE FIRMWARE ALREADY INSTALLED. INSTALLING AN INCORRECT FIRMWARE TYPE MAY CAUSE THE ADAPTER TO MALFUNCTION.

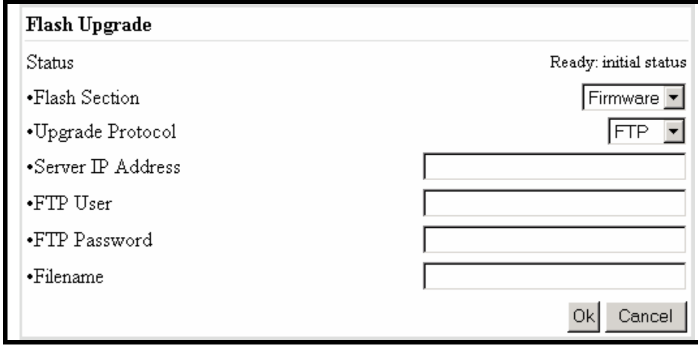
6. Click OK to start the process. Progress information is shown on the Web page every 30 seconds. This process may take up to five minutes. To refresh the Web page more frequently use the refresh button of your Web browser;

7. The adapter will first download the file and then calculate the CRC;

8. If the CRC is correct, the *Hardware Reset* button will be highlighted;

9. Reset the adapter. The adapter must be reset for the new firmware to run.

Figure 23: Change Configuration Page: Firmware Update Form



Flash Upgrade

Status	Ready: initial status
•Flash Section	Firmware
•Upgrade Protocol	FTP
•Server IP Address	
•FTP User	
•FTP Password	
•Filename	

6 Appendix A: Optimizing TCP throughput in Windows

By default, Windows are optimized for Ethernet connections. As with ADSL or cable adapters, you will not achieve maximum TCP performance with the PLC adapter unless you apply some changes to the default maximum TCP window size of your operating system (OS). In order to achieve maximum throughput performance in a PLC network some changes are necessary in the OS register. Please follow the steps below to apply the required changes to your Windows OS.

It is necessary to make the changes on all computers connected to the PLC nodes for the changes to affect your network TCP performance.

For Windows 2000/XP:

1. Open a new "Notepad" document (in the Programs – Accessories menu);

2. Select the text in Figure 24 and copy it to the Notepad document;

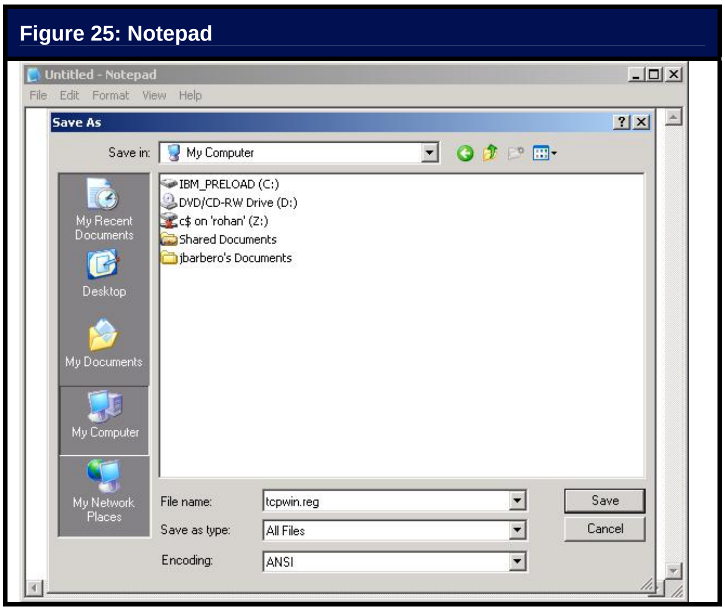
Figure 24: tcpwin.reg

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpWindowSize"=dword:00020000
"GlobalMaxTcpWindowSize"=dword:00020000
"Tcp1323Opts"=dword:00000003
```

3. Select "Save As…" and in the window that opens change the *Save as type* from "Text document" (*.txt) to "All Files" as shown in Figure 25;

Figure 25: Notepad



File name: tcpwin.reg

Save as type: All Files

Encoding: ANSI

4. In the *File name* field write "tcpwin.reg" and click on *Save*;

5. Double click on the new file created, *tcpwin.reg*;

6. A pop-up window will appear asking if you want to write in the register; click OK;

7. Reboot the computer for the changes to take effect.

The system is now optimized for transmission of TCP over networks with slightly higher latencies than Ethernet. The maximum TCP window size has been changed to 128 KB.

7 Abbreviations

The following is a list of abbreviations used in this manual.

ADSL	Asymmetrical Digital Subscriber Line
AP	Access Point
CoS	Class of Service
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
EP	End Point
FTP	File Transfer Protocol
GUI	Graphical User Interface
IARU	International Amateur Radio Union
IGMP	Internet Group Management Protocol
MAC	Media Access Control
NID	Network ID
OS	Operating System
PLC	Powerline Communications
STB	Set Top Box
TCP	Transmission Control Protocol
TFTP	Trivial FTP
TOS	Type of Service
UDP	User Datagram Protocol
VLAN	Virtual LAN