Technical Support
Bulletin Nr. 21 – **Web&Lan**Adapter

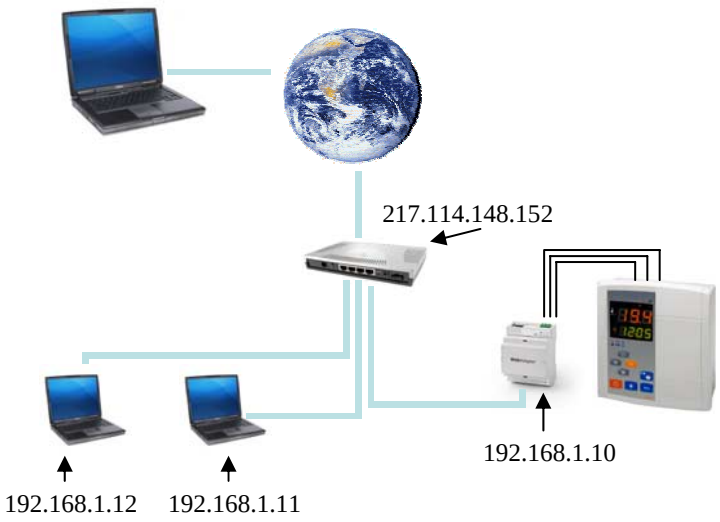
Contents

- *Connecting the **Web**Adapter to the network*
- *Connecting from a terminal outside the private LAN*
- *Settings on the server or router*
- *Connecting from a terminal within the private LAN*
- ***Lan**Adapter*
- ***Lan**Adapter within a local network*
- *Glossary*

Connecting the **Web**Adapter to the network

The **Web**Adapter interface makes it possible to transpose the information on a single Eliwell controller into HTML format so that it can then be viewed using a browser such as Internet Explorer 6 and later versions, or Firefox 1.5.
The interface connects to the controller by means of Eliwell Protocol or ModBus-RTU on an RS485 or TTL type physical bus, and interacts with the PC by means of TCP\IP protocol with an Ethernet or Wi-Fi type physical connection.
Two distinct types of connection to the **Web**Adapter object are dealt with hereinafter, depending on whether the user accesses the network from a terminal outside the LAN or from a terminal within it.

Fig. 1

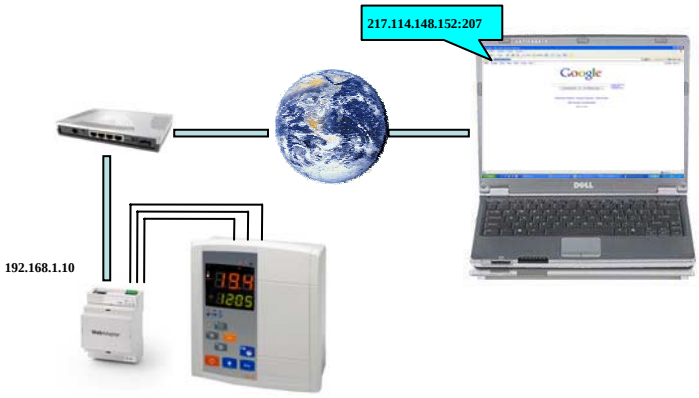


Eliwell Controls s.r.l.
Via dell'Industria, 15 • Zona Industriale Paludi • 32010 Pieve d'Alpago (BL) ITALY
Telephone +39 0437 986 111 • Facsimile +39 0437 989 066
Technical helpline +39 0437 986 300 • E-mail techsuppeliwell@invensyscontrols.com
www.eliwell.it

© Eliwell Controls s.r.l. 2007 All rights reserved.

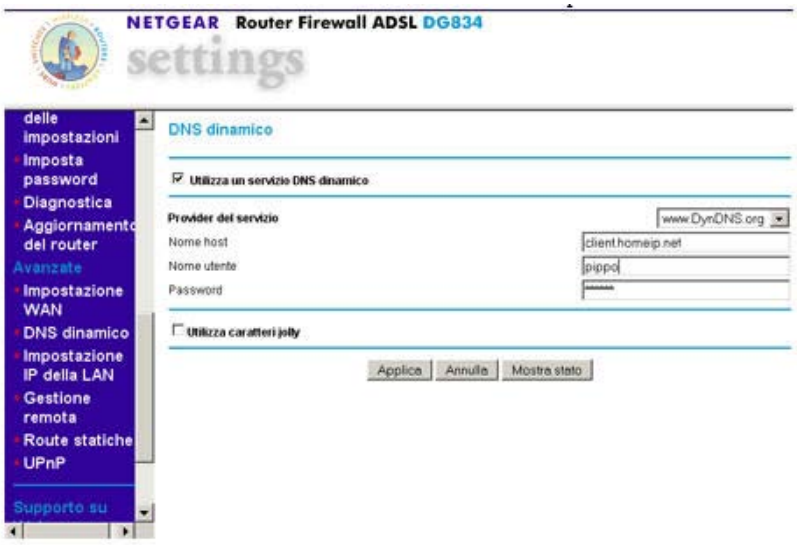
Connecting from a terminal outside the private LAN

1. If you need to connect from an external terminal, you need to know the public address of the router or server. The IP address can be static (case "a") or dynamic (case "b").
    a. In the first case, the user rents an internet connection with static IP address (public IP), so as to be the exclusive owner of it and to be always reachable at it. This type of address assignation is applicable regardless of whether the access point to internet is a server (a PC), or a modem\router.



To gain access from an external terminal, simply type in the public IP address followed by the port assigned in the NAT (see point 2) as shown in the figure.

    b. In the second case, the user has an internet connection with dynamic IP, which is assigned randomly by the DHCP server at each connection, for a limited period of time. This means that the address changes over time and the **Web**Adapter is therefore unreachable. To solve this problem, it is possible to have recourse to a DDNS server that provides a re-routing service, e.g. www.no-ip.com.
    The DDNS server makes it possible to have a public name (e.g. mioWebAdapter.no-ip.com), which is re-routed automatically to the temporarily assigned dynamic IP address.
    Two different conditions exist depending on whether access to internet is via a server (a PC) or directly through a modem\router.
        i. In the first situation, the DDNS service provider supplies a programme to be installed in the server.
        ii. In the second situation, no server is present, but a modem\router instead. In this case, it is necessary to ensure that your router supports the DDNS service. It is therefore necessary to sign up to an account for the service indicated by the manufacturer and set the username and password assigned to the account in the modem/router. The modem/router will then transmit the current dynamic IP to the DDNS server. The configuration page of the Netgear DG834 modem\router is shown below.



In both of the above cases, the access point to the private LAN can be reached through the username registered on the DDNS server.
e.g. mioWebAdapter.no-ip.com



Settings on the server or router

2. Once the access point to the private LAN is defined, it is necessary to assign an IP within the network to the **Web**Adapter device and couple it with a free TCP port by means of the NAT service (e.g. 207). All incoming requests addressed to this port will be re-directed to the device inside the LAN. There are two ways of assigning the IP address inside the LAN to the **Web**Adapter. The first is to assign it by means of the respective configuration pages, by manually assigning it a valid address that is coherent with the IP screen used by the LAN. The second way is to require the controller to request from the DNS server a valid IP assigned by means of the DHCP server. The IP address assigned by the DHCP must be fixed and associated with the mac address of the **Web**Adapter device.

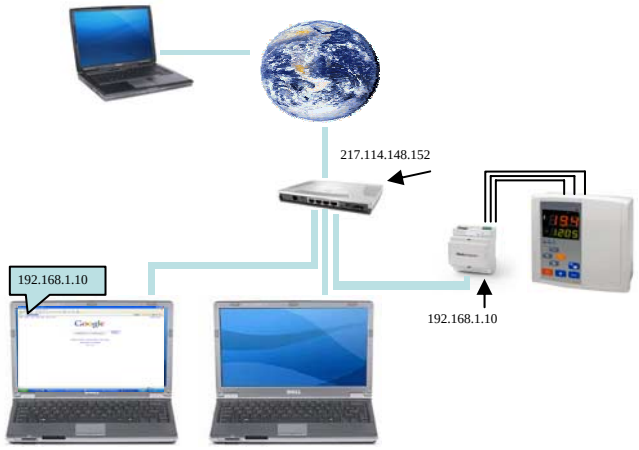
Connecting from a terminal within the private LAN

It is also possible to access the **Web**Adapter from a computer that belongs to the same LAN. To do this, it is sufficient to know the address(es) assigned within the same network to reach the object.

Two distinct cases exist, according to how the IP address is assigned to the **Web**Adapter.

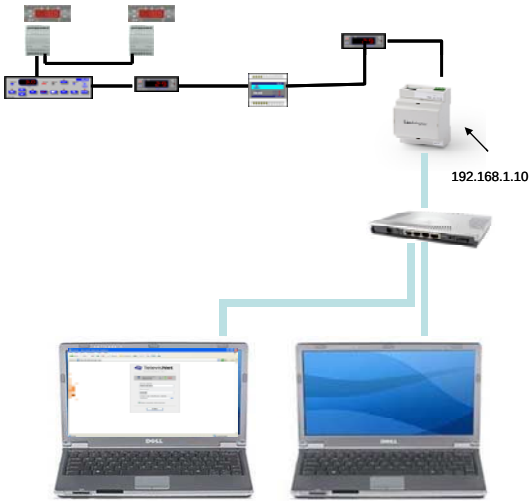
1. In the first case, the address is fixed in the configuration of the same **Web**Adapter. The assigned address must be coherent with the addresses screen in use in the LAN. If a server is present, ask the network administrator; in the case of a router, check on the router's configuration pages.
2. In the second case, the **Web**Adapter is asked to request the IP address from the DNS server, which is assigned by the DHCP server. Regardless of whether there is a network server or a simple router, it is necessary to configure these so that they associate a fixed IP address to the Mac Address of the network device.

The device(s) can be reached from any PC belonging to the LAN, simply by typing in the IP address of the desired object in the browser.



Lan*Adapter*

The **Lan**Adapter device makes it possible to interface a network of communicating controllers by means of Eliwell or Modbus protocol on an RS485 network (homogeneous networks only) with a LAN, with either an Ethernet or a Wi-Fi connection. It is therefore possible to locate the computer that handles the acquisitions in a different place from the physical network made up of the controllers.



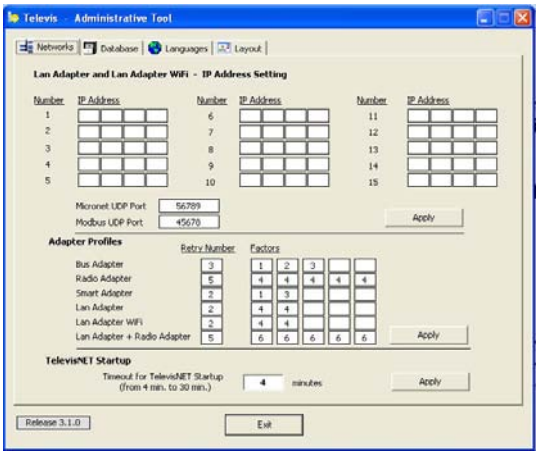
LanAdapter within a local network

Let us suppose that we have a LAN at our disposal in a building. With this configuration it is possible to have the host PC of the televis in one department (such as management) and have the controllers in the sales area. Without having to reach the area to be managed via the RS485 data bus, we use the LAN. Connection is made through the first connection point to the local network, regardless of whether this is an ethernet socket or an access-point.

It is possible to have up to 15 **Lan**Adapter devices even if they are not homogeneous, i.e. a mix of Ethernet and Wi-Fi versions, but it is permissible to use only wired instruments connected to these interfaces. The radiofrequency option downstream of a **Lan**Adapter is not permissible.

It is necessary to fix an IP address for each **Lan**Adapter. This can be assigned by means of the configuration pages of the device itself, or assigned by the DNS server and linked with the Mac Address in the DHCP server.

As soon as the IP address of the various controllers is known and coherent with the screen to the user, it is necessary to go into the Administrative Tool (Programmi\Eliwell\Administrative tool) and set the IP addresses present in the LAN.



By activating the Televis, the programme will recognise the connected interfaces. At least one of these must be a classic PC interface with USB or serial connection, in which the licence bluecard is inserted (valid up to version 03.01.00 of the programme. Contact assistance in the case of more recent versions).

Glossary

UDP – A connection-less data transport protocol. This transfers data packets to the recipient, but does not guarantee their arrival. The only error control is a checksun. This does not manage the start, duration or end of the connection. Useful for rapid transmissions in which the loss of packets is tolerable.

TCP – A data transport protocol. Much more reliable than UDP, this guarantees the arrival of data packets at their destination. In the event of a loss, it is capable of asking the sender for the missing packet and reorganising the information sent. Useful for exchanging data between two applications. Manages the start, duration and end of the communication and also controls data flow and network congestion.

DNS – Domain Name System is a service which enables you to associate an alphanumeric name to an IP address expressed in numerical format.

DDNS – The Dynamic Domain Name System makes it possible, by means of a third site, to resolve the IP address, and associate it with a name, even if the IP continues to change. For example, a PC to which a dynamic IP address is assigned, by means of the DHCP service, can always be reached simply by knowing the name of the machine. The PC in question is registered in a site that offers the DDNS service, such as www.no-ip.com and, by means of a programme that is installed, each time the IP address is changed, the PC informs the host server. The current IP address is thus always associated with the name of the machine.

DHCP – Dynamic Host Configuration Protocol is a protocol used for temporarily and unequivocally assigning an IP address to calculators and making it part of a sub-network in which it is reachable. This automatic service thus makes it possible to optimise the management of assigning addresses and their availability.

NAT - Network Address Translation is a technology with which it is possible to re-route the individual internal PCs from and to the user of a private network. NAT technology can be applied both in output and input and brings two major advantages. The first is that it reduces the number of public addresses, and the second is that it keeps the IP addresses of the internal network private, thus increasing security. It can be divided into SNat and DNat according to whether the modified IP address is the source or destination address.

Let us look at the first case (SNat) in which a PC asks to open a connection session with an external IP address, presumably an internet site. The PC contacts the NAT server, which keeps track of the connection and replaces the source IP with its own. The Web server will thus think it is connected not with the requesting PC but with the NAT server. In response, the IP is returned to the origin and sent to the requesting PC.

The second case, also seen as Port Forwarding, makes it possible to open a TCP or UDP port, and at each connection to the NAT IP address in the specific port, the request is re-directed to a specific internal IP.

Mac address: This is a physical address assigned unequivocally to any network device, whether wired or wireless, manufactured worldwide.

DISCLAIMER

This document is the exclusive property of Eliwell and may not be reproduced or circulated unless expressly authorized by Eliwell. Although Eliwell has done everything possible to guarantee the accuracy of this document, it declines any responsibility for damage arising from its use. The same applies to any person or company involved in preparing and writing this document.
Eliwell reserves the right to make changes or improvements at any time without notice.