# DMH remote access

## Table of Contents



UNITRON NV
Frankrijklaan 27
B-8970 Poperinge
België (Belgique, Belgien, Belgium)
RPR Ieper / BTW - BE - 0437.664.097

T + 32(0)57 33.33.63
F + 32(0)57 33.45.24
E-mail: sales@unitrongroup.com
www.unitrongroup.com

Bank (Banque) National: KBC 472-1021801-82 / FORTIS 285-0333147-78
Bank (Banque) International:
(IBAN EURO) BE 25 4721 0218 0182 - BIC (Swift) KRED BE BB
(IBAN USD) BE 45 4721 0218 0889 - BIC (Swift) KRED BE BB
(IBAN CZK) BE 78 4721 0218 0586 - BIC (Swift) KRED BE BB
(IBAN EUR & USD) BE 69 2850 3331 4778 - BIC (Swift) GEBA BE BB

# 1 Remote access description

The key parameters to access a module from the internet are an IP address, a port and a protocol.

Normally the module will be connected to the internet through a router. The router is the gateway between the local network and the internet. The IP address needed for the remote access is the IP address which is obtained by the router from the local ISP. This IP address can be found on the status page of the router or if you have a pc connected to the internet through the router you can surf to a site called http://whatismyipaddress.com/ and there you will find the IP address.

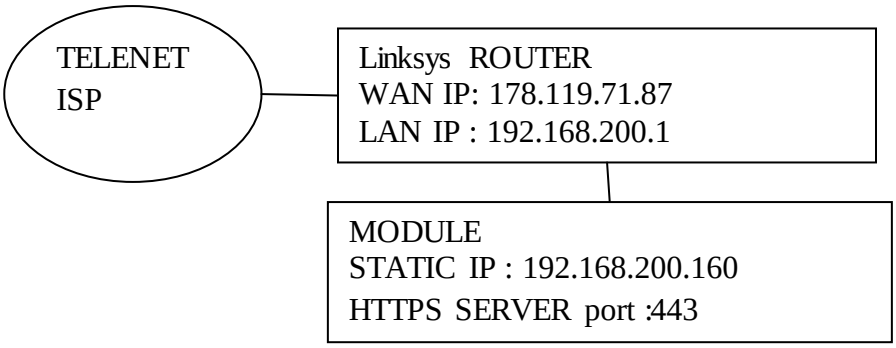
The module contains a secure HTTP webserver this means that all communication between the client's browser and the module is encrypted by using a self-signing certificate, this prevents eavesdropping. The secure HTTP webserver is combined with basic access authentication; the authentication can be enabled or disabled in the webgui. Basic access authentication means that the username and password must be provided once @ the start of the browser session. By default https connections use port 443, when the server is on this port you do not need to specify the port in the address bar of the browser.

When connected to the internet through a router this router should be told to forward all incoming traffic on a specific port to a certain IP address on the internal network, this is called port forwarding and can be done following the manual of the router. When there are multiple modules behind the router each module should be configured with a unique port number for the https server; port numbers allowed in the webgui : port 30 to 40000.

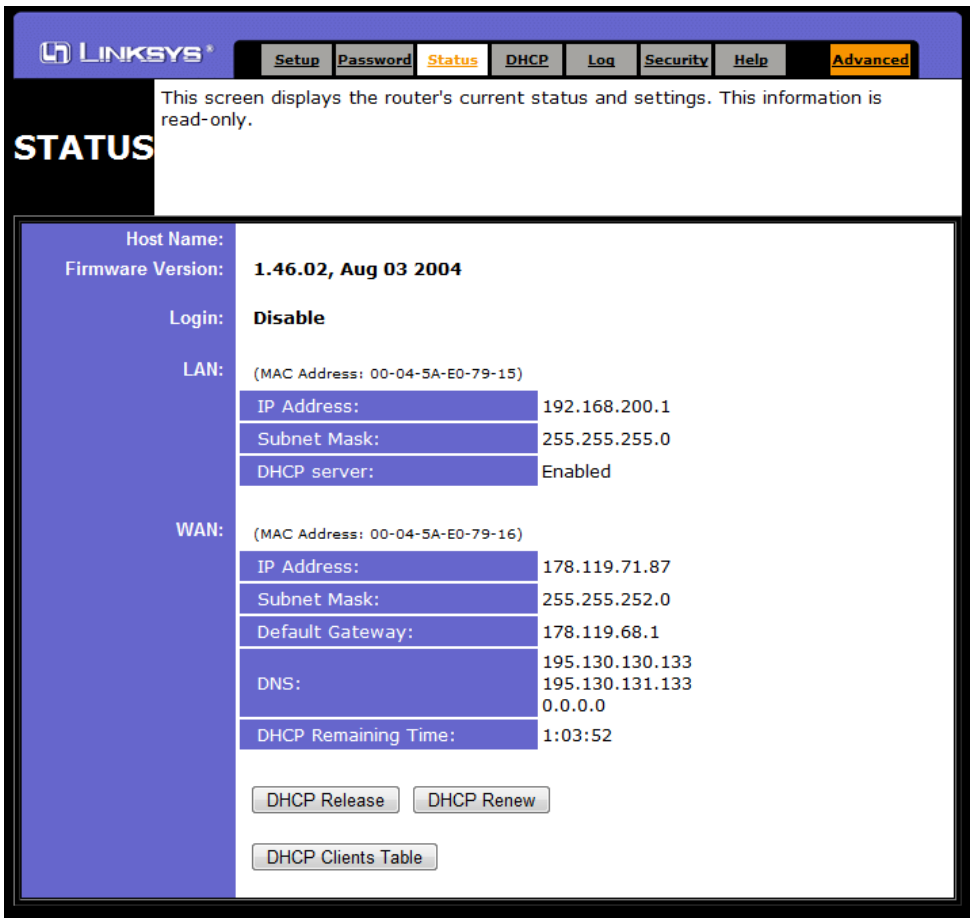
It is best to configure the module with a static IP address when using port forwarding; this is foreseen in the webgui under the global configuration page.

## 1.1 Single module remote access

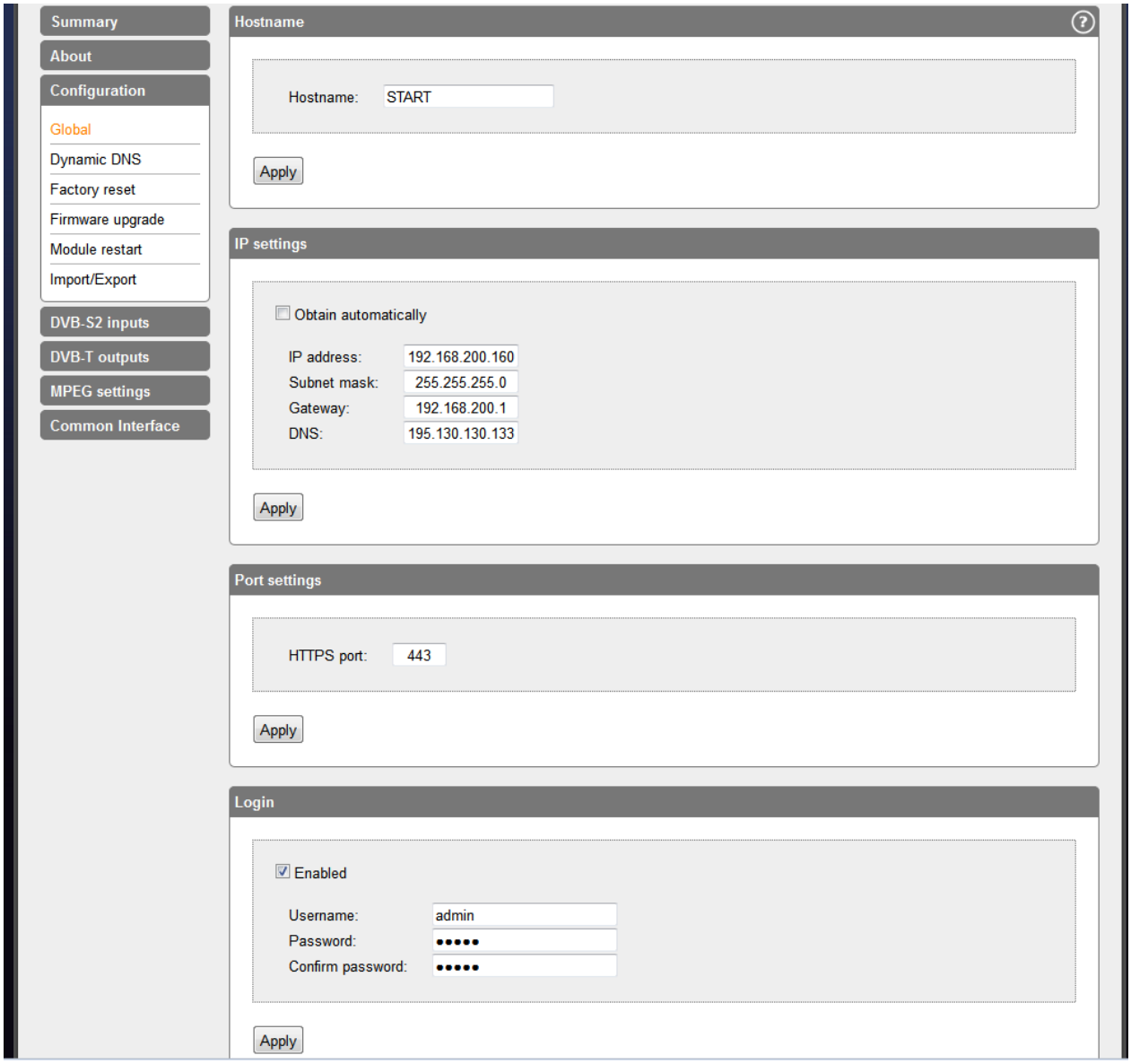
Router connected to the internet, single module connected to the router with static IP address, https server on port 443.
Router configured to forward all incoming traffic on port 443 to the ip address of the module.



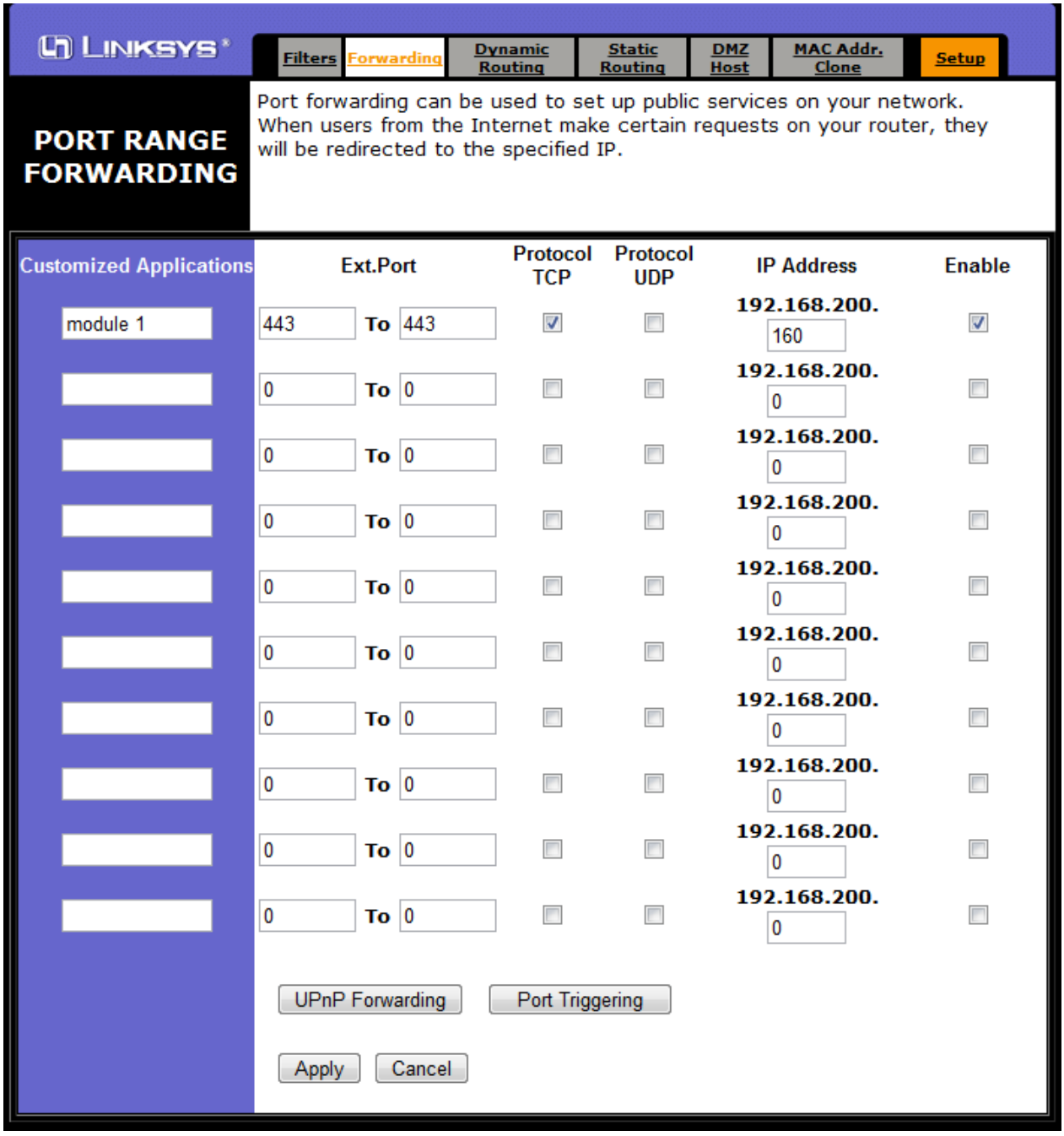

Linksys router status page:



Module config page:



Port forwarding page:

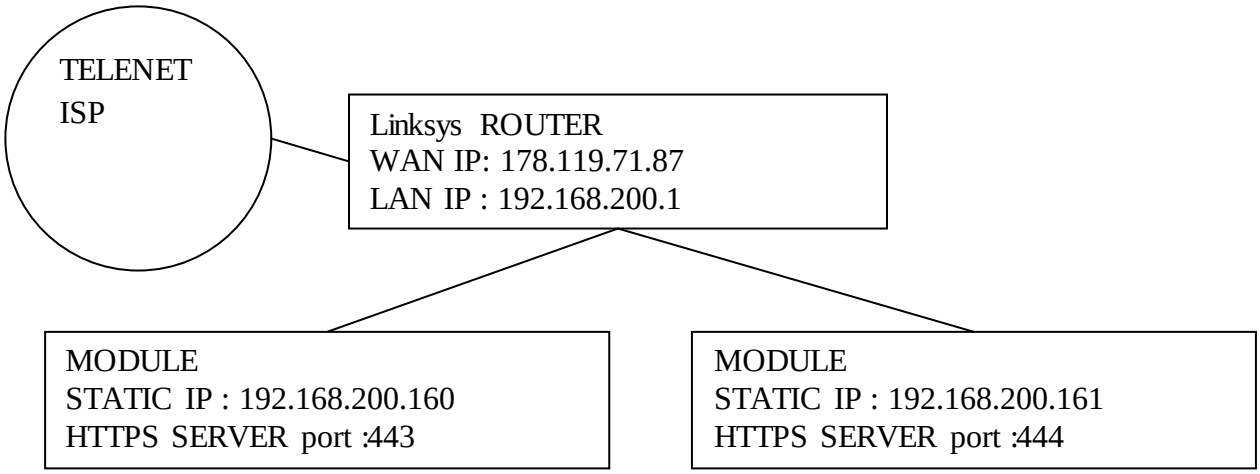



Access from the internet:

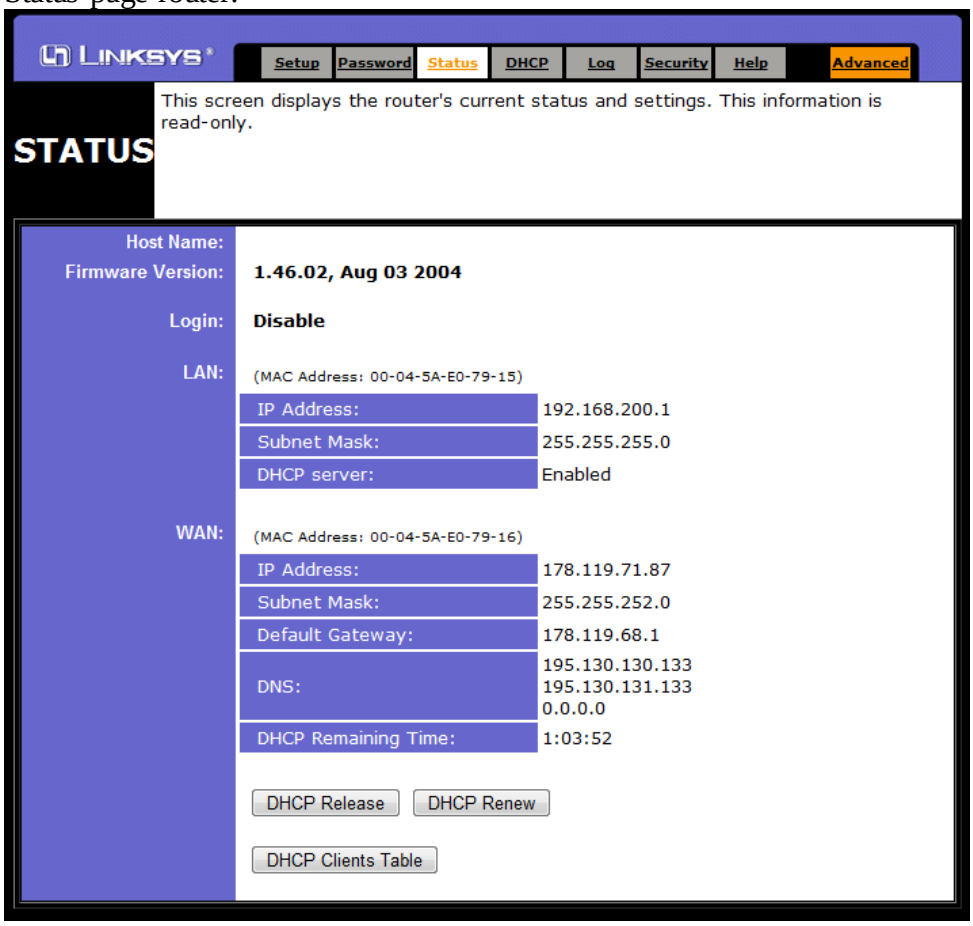
https://178.119.71.87

## 1.2 Multiple modules remote access

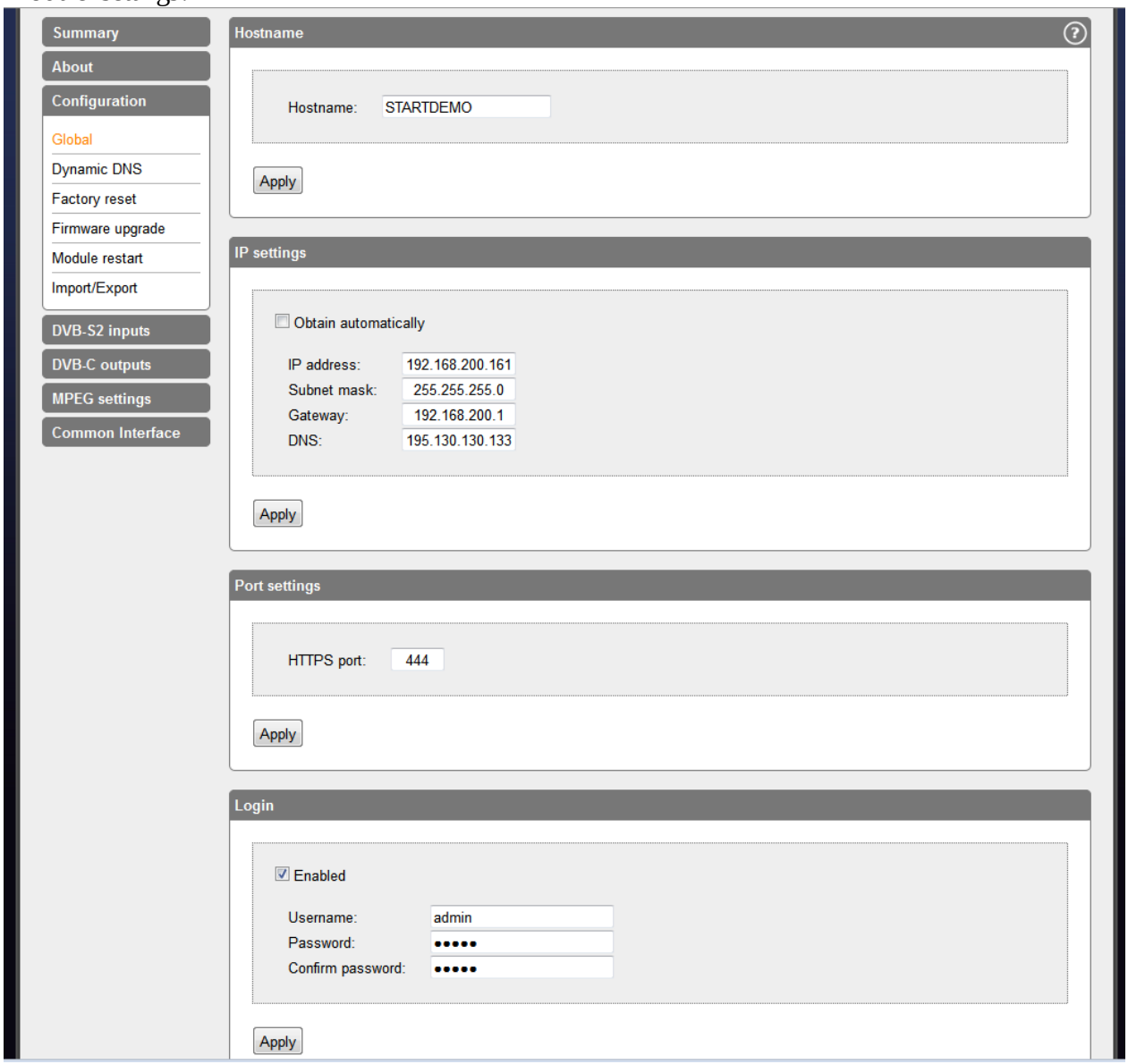
Router connected to the internet, two modules connected to the router with static IP address, https server module 1 on port 443, module 2 on port 444.
Router configured to forward all incoming traffic on port 443 to the ip address of module1 and all incoming traffic on port 444 to the ip address of module 2.



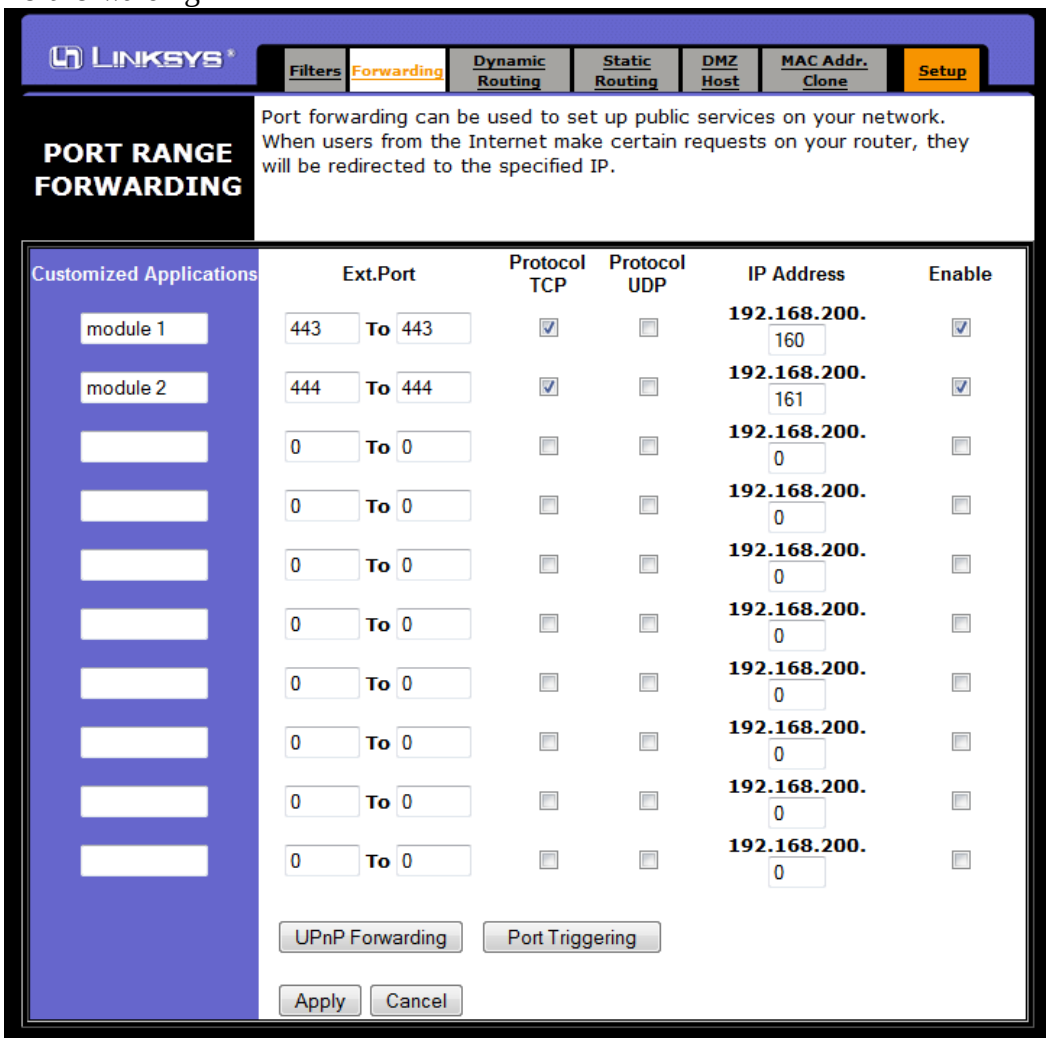

Status page router:



Module settings:



Port forwarding




Remote access:

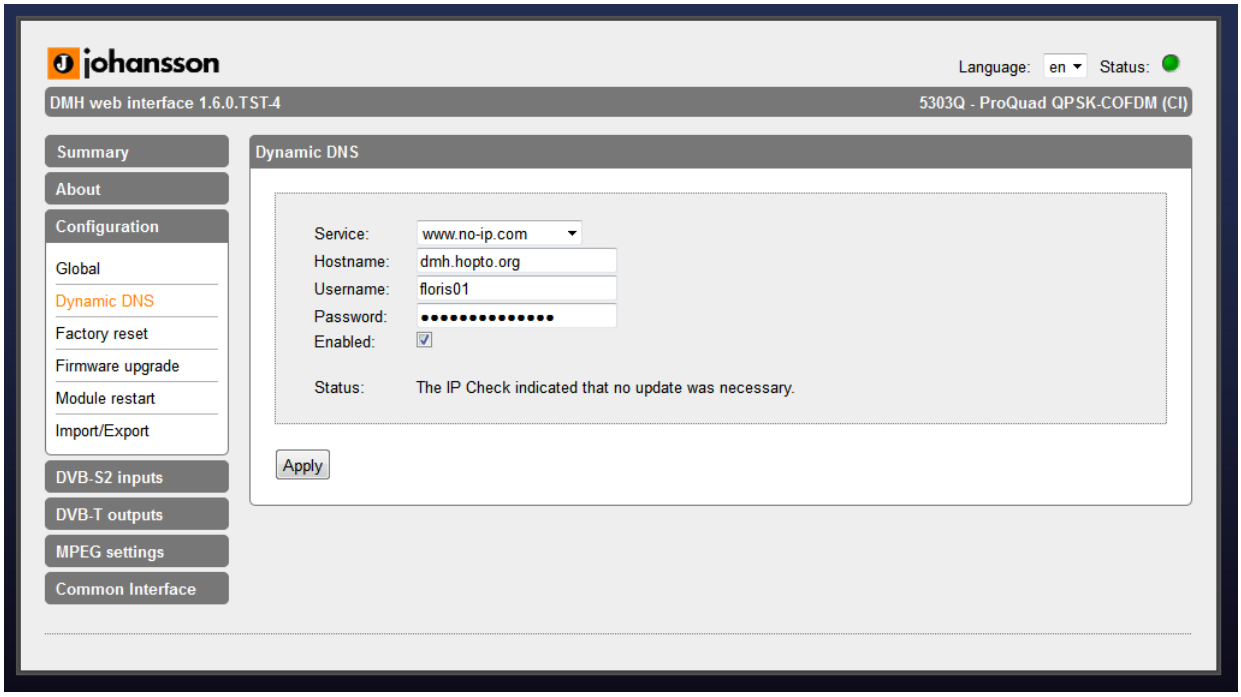
Module 1 : https://178.119.71.87
Module 2 : https://178.119.71.87:444

Module 2 the port is needed in the address because it is operating on a nonstandard https port. As mentioned before all modules need a unique HTTPS port

# 2 Dynamic DNS

As most ISP's work with dynamic IP addresses it could be that the ip address obtained by the router changes in time. This means that the user could lose his access to the module because he doesn't know the new ip address assigned by the ISP. This issue can be solved by using the dynamic dns client built in the module. The user needs to create an account on http://dyn.com or http://www.no-ip.com/ or http://www.dnsomatic.com/ these websites provide a domain name for a certain ip address. Once an account is created the user can link the external ip address of the router to a domain. The user can fill in his account details and the domain name registered for a specific module in the webgui. The module will then check the external ip address every 10 minutes and if necessary (when the external ip changed) update the dns record through the users account. In this case the domain name will always refer to the correct ip address as it will be dynamically updated by the module.

For example: https://dmh.hopto.org refers to https:// 178.119.71.87



# 3 REMARKS/PITFALLS

-Keep in mind that the ip address given by the ISP can change if it is dynamically obtained (see 2 Dynamic DNS).

-Keep in mind that the ip address of the module can change if it is dynamically obtained from the router and when it changes that the port forward settings of the router can become invalid.

-Some ISP's restrict the ports which can be used by the end user example telenet:
http://klantenservice.telenet.be/content/welke-internetpoorten-blokkeert-telenet

-browser warnings due to self-signing certificate:

Self-signed certificates work exactly like a certificate purchased through an SSL Certificate Authority, except that they are NOT signed by a Certificate Authority. Instead they are signed by our module; hence the term "self-signed". That is the only difference. Apart from that, the encrypted connection using a self-signed certificate is as secure as any other SSL connection.
So why do most browsers throw that scary-looking error? The answer lays in the role that certificate authorities play. Certificate authorities perform various checks to see that whoever is purchasing the certificate is who they say they are. Browsers assume that a site that uses an ssl certificate that has been vetted by a certificate authority is safer than a site that does not.

-choose none occupied tcp ports to access the HTTPS server!

-The reactivity of the webgui can be slower when accessing it remotely through the internet. Upload speed of the used internet connection is the limiting parameter. The webgui is a dynamic page which generates traffic when open in a browser.

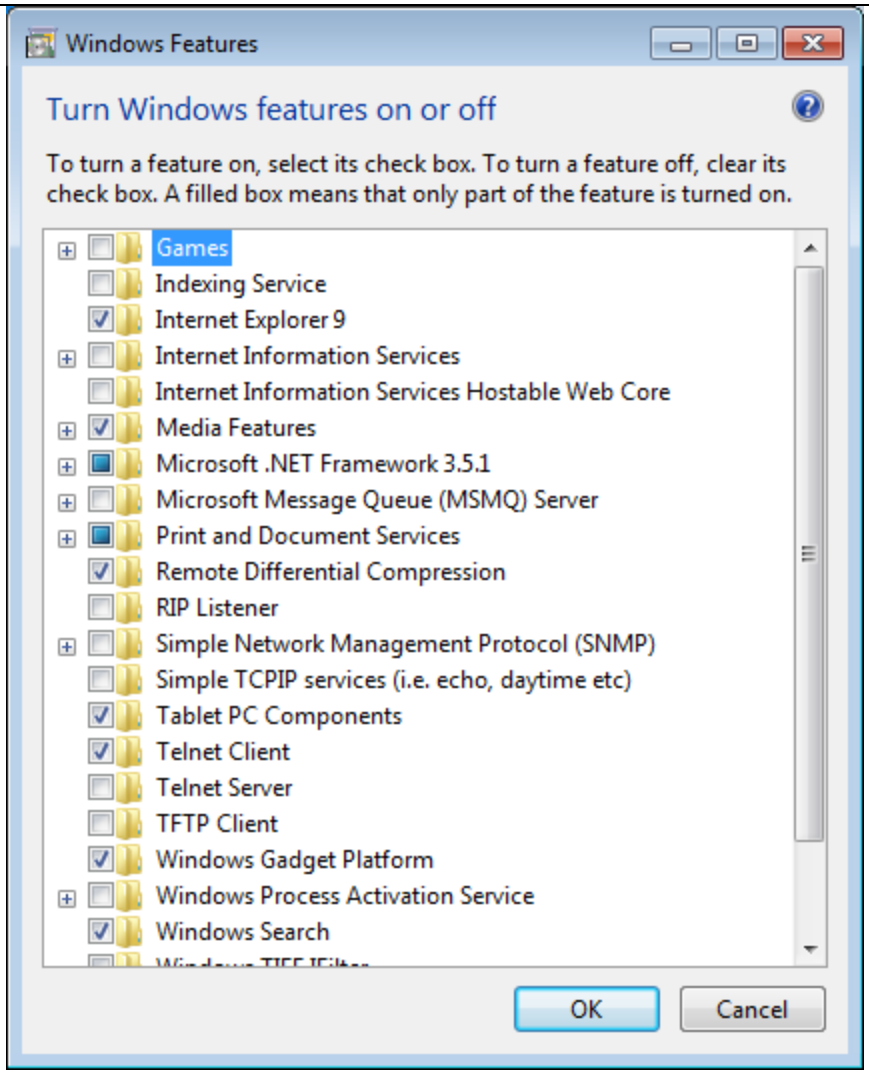
-Firefox is the preferred browser for remote access

-All remote traffic happens over https in the address bar of the browser HTTPS should be typed

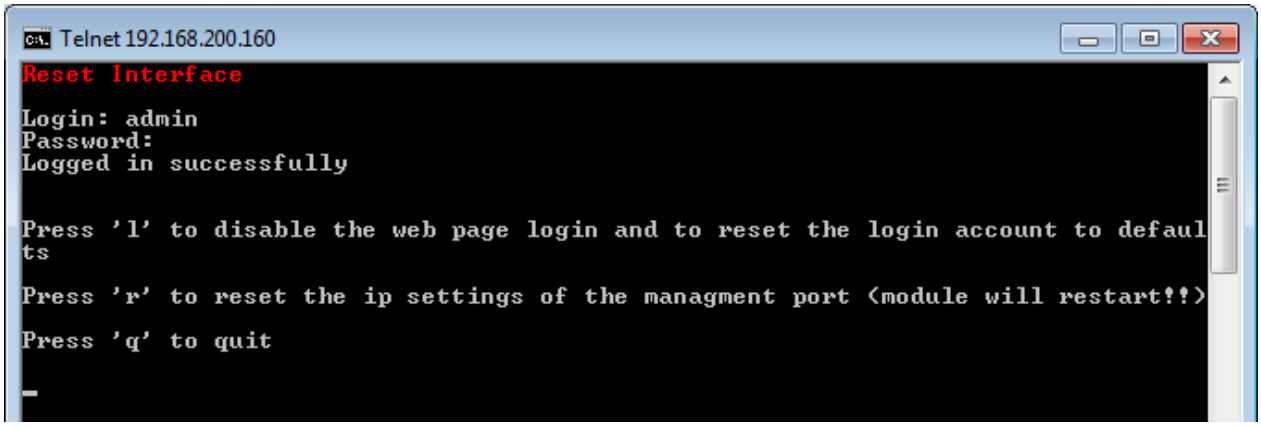
-Users can't use the netbios name to access the device remotely

-forgot username and psw recovery procedure (can only be done when on the local network with the module):

Start telnet session on port 60000 of the module:
telnet is a standard windows command:
go into command line and type "telnet XXX.XXX.XXX.XXX 60000"
XXX.XXX.XXX.XXX stands for the ip address of the module
If telnet isn't installed go to control panel => programs and features => turn windows features on and off and enable the telnet client.




Once client is enabled: telenet XXX.XXX.XXX.XXX 60000
Username: admin
Psw: headend
Follow the instructions on the screen:




When using the r option all ip settings of the management port are ereased this means that the default netbios name is restored (START) and that the module is in auto ip/DHCP mode.