



TheGreenBow IPSec VPN Client

Configuration Guide

Netgear DG834G

Firmware 2.10.22

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Table of contents

| | | |
|-----|--|----|
| 1 | Introduction | 3 |
| 1.1 | Goal of this document | 3 |
| 1.2 | VPN Network topology | 3 |
| 2 | DG834G VPN configuration..... | 4 |
| 3 | TheGreenBow IPSec VPN Client configuration | 5 |
| 3.1 | VPN client Phase 1 configuration | 5 |
| 3.2 | VPN client Phase 2 configuration | 7 |
| 4 | VPN IPSec Troubleshooting | 8 |
| 4.1 | « PAYLOAD MALFORMED » error | 8 |
| 4.2 | « INVALID COOKIE » error | 8 |
| 4.3 | « no keystate » error | 8 |
| 4.4 | « received remote ID other than expected » error | 8 |
| 4.5 | « NO PROPOSAL CHOSEN » error | 9 |
| 4.6 | « INVALID ID INFORMATION » error | 9 |
| 4.7 | I clicked on “Open tunnel”, but nothing happens | 9 |
| 4.8 | The VPN tunnel is up but I can't ping ! | 9 |
| 5 | Contacts..... | 11 |

1. Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a NETGEAR DG834G with firmware 2.10.22

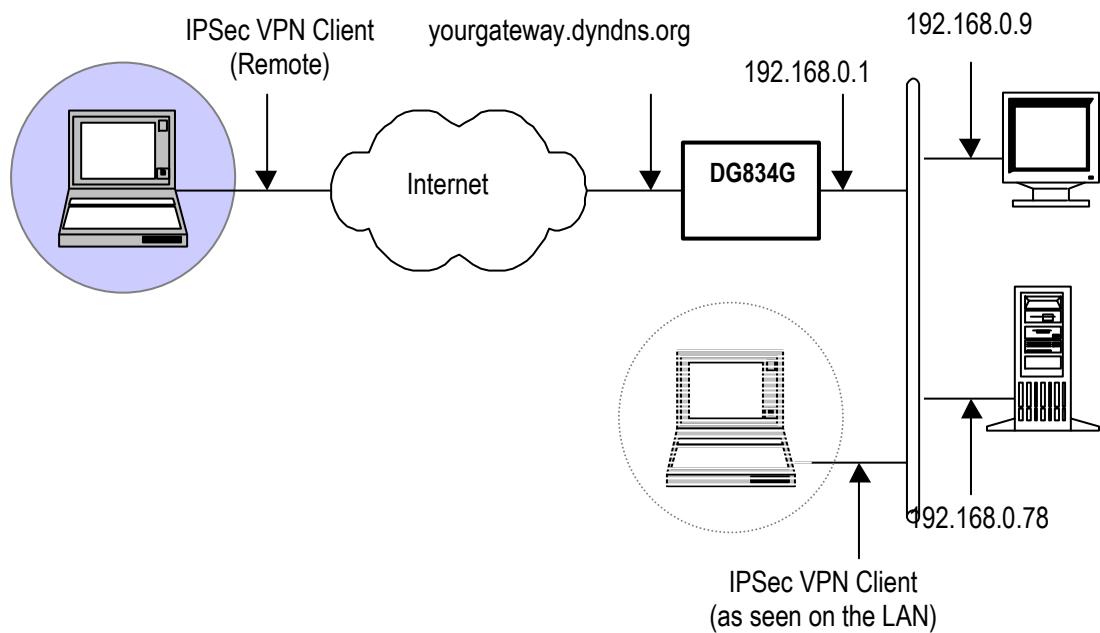


1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the DG834G. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.

A Road Warrior connection also needs to be configured. The following example makes use of these values:

- External IP of the DG834G: yourgateway.dyndns.org (or public IP address)
- IP Subnet behind the DG834G: 192.168.0.0/255.255.255.0



2. DG834G VPN configuration

On the router menu, go to VPN policies, and add a new auto policy

VPN - Auto Policy

General

| | |
|--|---|
| Policy Name | <input type="text" value="client"/> |
| Remote VPN Endpoint | Address Type: <input type="text" value="Dynamic IP address"/> Address Data: <input type="text" value="n/a"/> |
| <input checked="" type="checkbox"/> NetBIOS Enable | |
| <input type="checkbox"/> IKE Keep Alive | Ping IP Address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> |

Local LAN

| | |
|------------|--|
| IP Address | <input type="text" value="Subnet address"/> <input type="button" value="▼"/> Single/Start address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="0"/> Finish address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Subnet Mask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> |
|------------|--|

Remote LAN

| | |
|------------|--|
| IP Address | <input type="text" value="Single address"/> <input type="button" value="▼"/> Single/Start IP address: <input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="10"/> |
|------------|--|

IKE

| | |
|---------------------------|---|
| Direction | <input type="text" value="Responder only"/> <input type="button" value="▼"/> |
| Exchange Mode | <input type="text" value="Main Mode"/> <input type="button" value="▼"/> |
| Diffie-Hellman (DH) Group | <input type="text" value="Auto"/> <input type="button" value="▼"/> |
| Local Identity Type | <input type="text" value="Fully Qualified Domain Name"/> <input type="button" value="▼"/> |
| Data | <input type="text" value="netgear"/> |
| Remote Identity Type | <input type="text" value="Fully Qualified Domain Name"/> <input type="button" value="▼"/> |
| Data | <input type="text" value="thegreenbow"/> |

Parameters

| | |
|---|--|
| Encryption Algorithm | <input type="text" value="3DES"/> <input type="button" value="▼"/> |
| Authentication Algorithm | <input type="text" value="Auto"/> <input type="button" value="▼"/> |
| Pre-shared Key | <input type="text" value="abcdefghijklm"/> |
| SA Life Time | <input type="text" value="28800"/> (Seconds) |
| <input checked="" type="checkbox"/> Enable PFS (Perfect Forward Security) | |

[Back](#)

[Apply](#)

[Cancel](#)

3. TheGreenBow IPSec VPN Client configuration

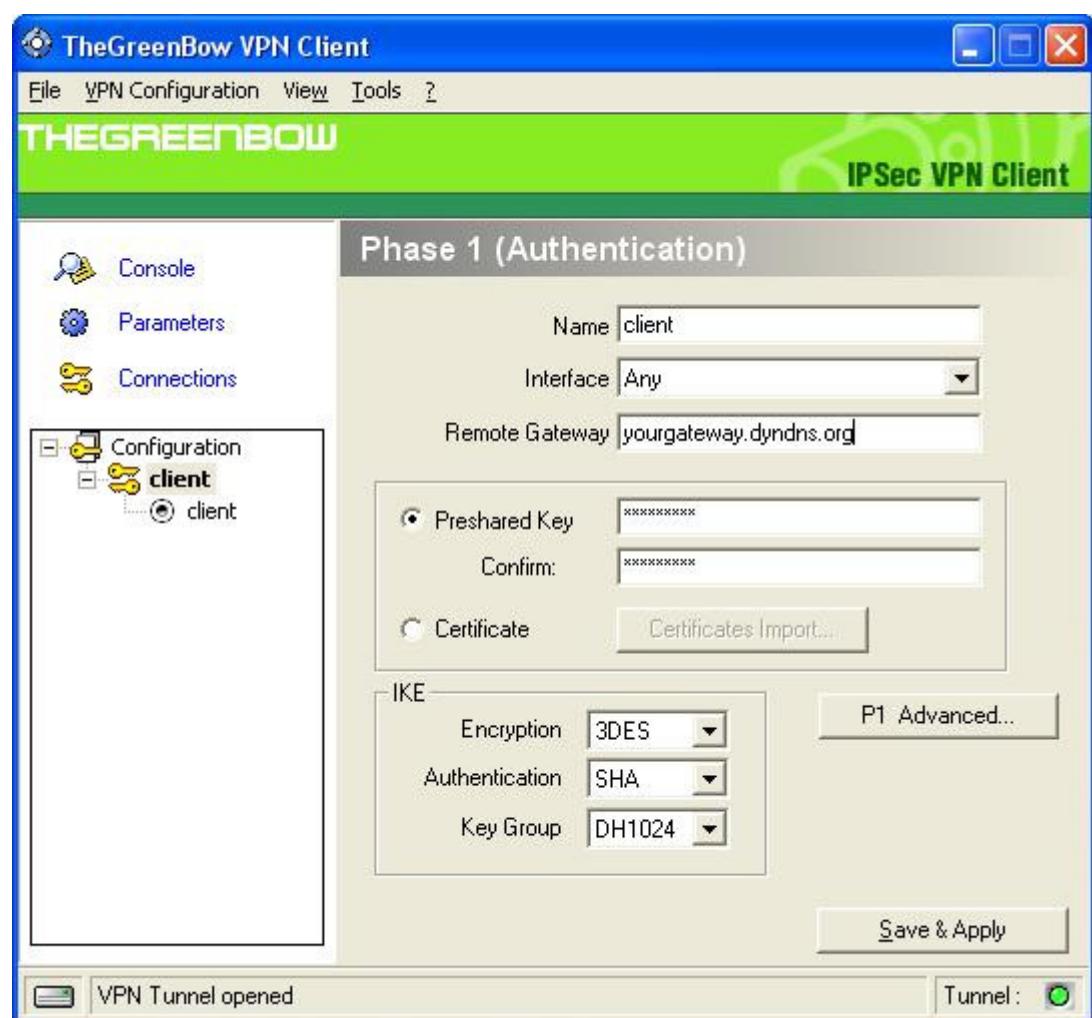
3.1 VPN Client Phase 1 Configuration

Right click on Configuration in TheGreenbow VPN client and select "Add Phase 1".

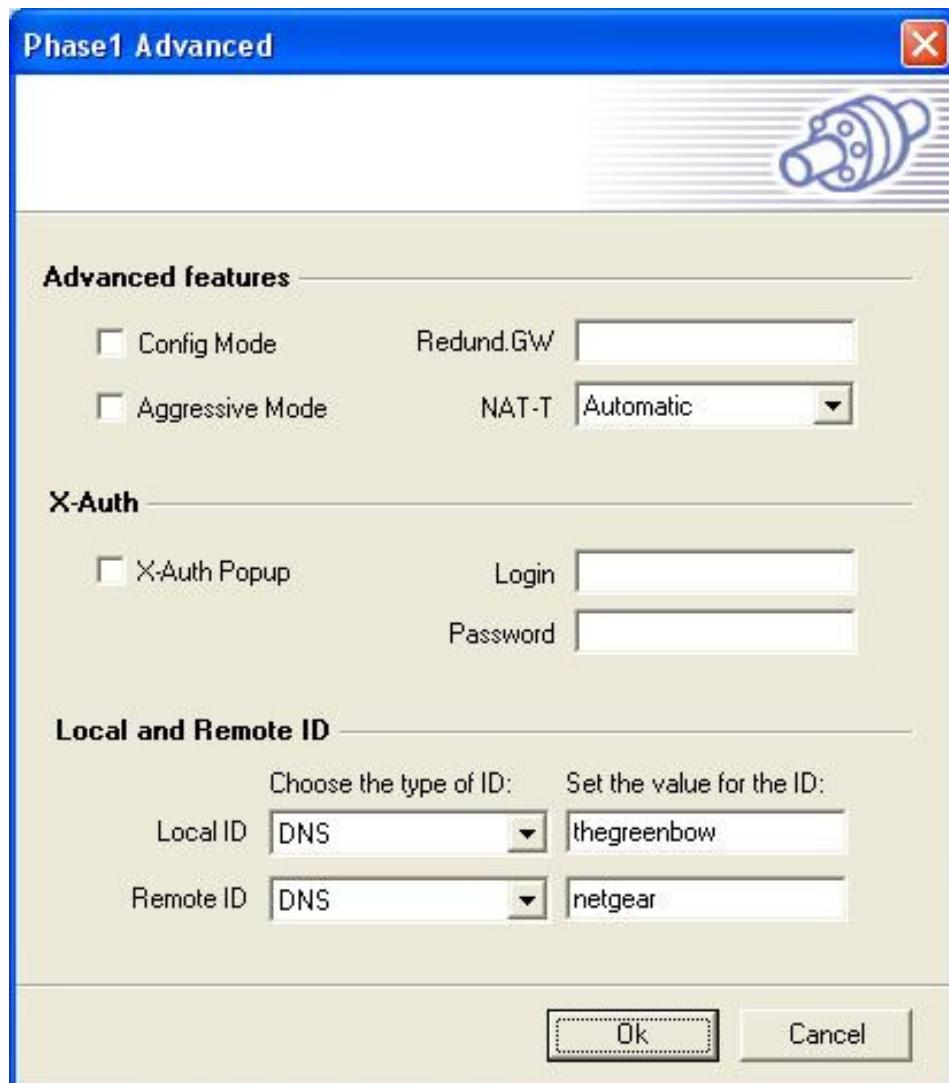
Then select the "new phase 1" screen. The values that need to be changed and entered are displayed here:

The preshared key used in this example is intentionally short. Don't use this key length in a production environment, it must be complex enough for maximum security.

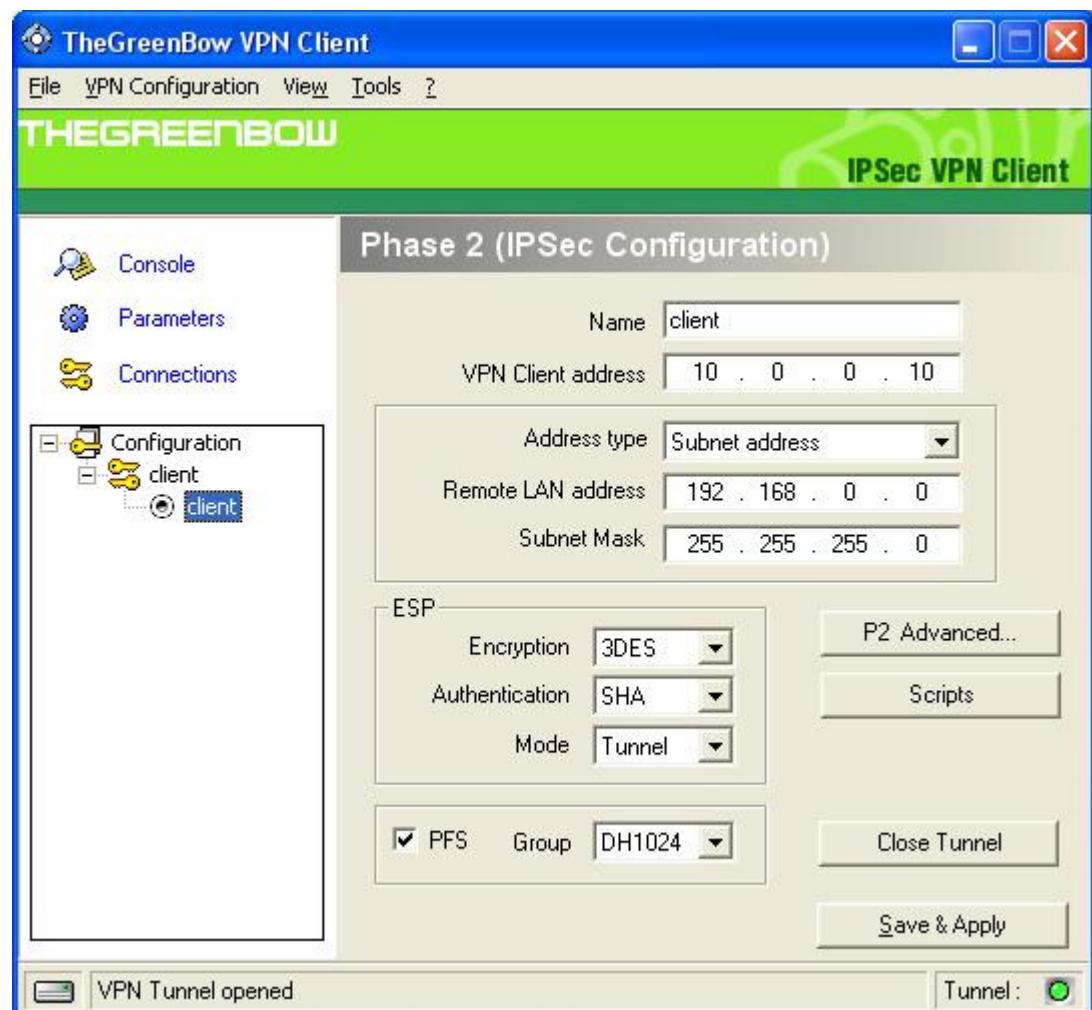
Phase 1 Configuration



Click on “P1 advanced” to enter ID types and values.



3.2 VPN Client Phase 2 Configuration



Phase2 advanced is used to enter alternate dns and/or wins servers addresses .If configured, these addresses will overwrite the current dns and/or wins configuration on the ip stack, once the tunnel is up. The ip stack return to its original state at tunnel normal closure.

4. VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification
type PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

4.2 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification
type INVALID_COOKIE
115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error
```

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

4.3 « no keystate » error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA] [VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY] [NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY] [NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

4.4 « received remote ID other than expected » error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA] [VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY] [NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY] [NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID] [HASH] [NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
```

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

4.5 « NO PROPOSAL CHOSEN » error

```

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA] [VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY] [NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY] [NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID] [HASH] [NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode
[SA] [KEY] [ID] [HASH] [NONCE]
115915 Default RECV Informational [HASH] [NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational [HASH] [DEL]
115915 Default CNXVPN1-P1 deleted

```

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error

```

4.6 « INVALID ID INFORMATION » error

```

122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA] [VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA] [VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY] [NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY] [NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID] [HASH] [NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID] [HASH] [NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode
[SA] [KEY] [ID] [HASH] [NONCE]
122626 Default RECV Informational [HASH] [NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational [HASH] [DEL]
122626 Default CNXVPN1-P1 deleted

```

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

4.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500, UDP port 4500 and protocol ESP (protocol 50).

4.8 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP

| | |
|-------------|---------------------|
| Doc.Ref | tgbvpn_ug_DG834G_en |
| Doc.version | 1.0 –october.2006 |
| VPN version | 4.0 |

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is no “Default gateway” setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install ethereal (<http://www.ethereal.com>) on one of your target computer. You can check that your pings arrive inside the LAN.

5 Contacts

News and updates on TheGreenBow web site : <http://www.thegreenbow.com>

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com