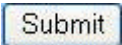
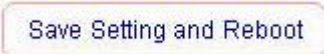


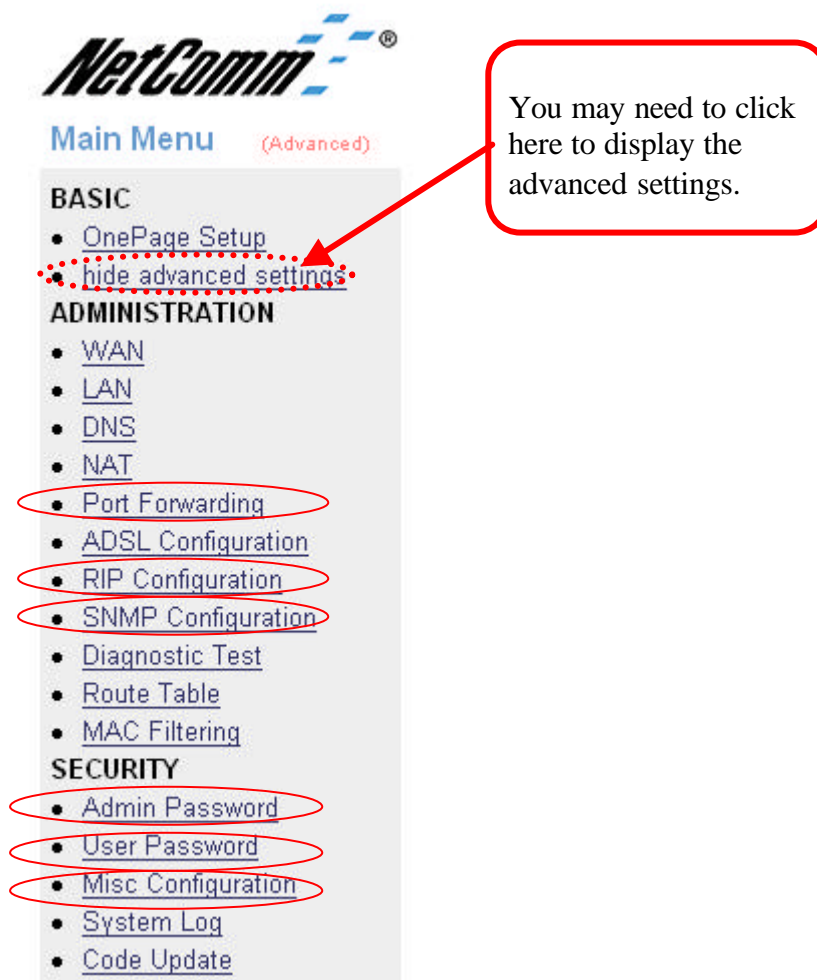
Securing Your NB1300 - Once connected.

There are eleven areas that need your attention to secure your NB1300 from unauthorised access - these areas or features are;

- Physical Security
 - Admin Password
 - User Password
 - SNMP Community Strings (when SNMP is available in your firmware)
 - FTP server
 - HTTP Server
 - DMZ Host
 - Half Bridge mode
 - Port Forwarding
 - Dynamic Routing (RIP Configuration)
 - Telnet
- } These options are all found under 'Misc Configuration'

The features are accessed via the menu item choices shown circled in the screen shot below. Each item is either disabled or changed in it's appropriate page and as always you must click the  button at the bottom of the page. Once you have made all your changes you must then click the  button to commit your changes and reboot the NB1300.

Don't forget you can incorporate all of these settings into an Easy config profile for easier deployment for endusers. See the section on Easy config at the end of the document.



1. **Physical security** - should be considered because if a malicious person has physical access to the unit they can damage it, steal it, reset it to factory defaults or just sabotage it to allow them remote access later on.

Note: Your Admin password can be deleted with physical access.

2. **Administration Password** – Your Admin Password gives you complete control over the NB1300 it should NEVER be left as default because it can allow access from a Web browser, FTP or Telnet service from both your LAN and the Internet. You should change your Administration Password to something complex and involving many UPPER and lower case Characters. The Minimum password length is fixed at eight characters. Some examples of suitable passwords in growing complexity are;

fa11en4you <- mixing words and numbers, replacing letters with numbers.

Buz911B0xzero <- as above but using upper and lower case as well.

SecN@tC0mmwillyou <- The '0' is a zero, the use of '@' instead of 'e'

To change your Admin password choose the 'Admin Password' option on the menu and you will see a screen similar to the one below. Enter your new password twice, once in each field and then click the submit button

Note: For security your password's characters will be replaced with dots so no one can see you type it on the screen.

3. **User Password** – Your User password is used to log-in with the username 'User' this is a restricted account that allows you to view router status but not change anything in the router. However the less information a 'Hacker' can find out about your system the less chance the hacker has of finding an exploit for your system. Depending on your needs you may wish to make the User password as secure as the Admin password or a little easier for regular everyday use.

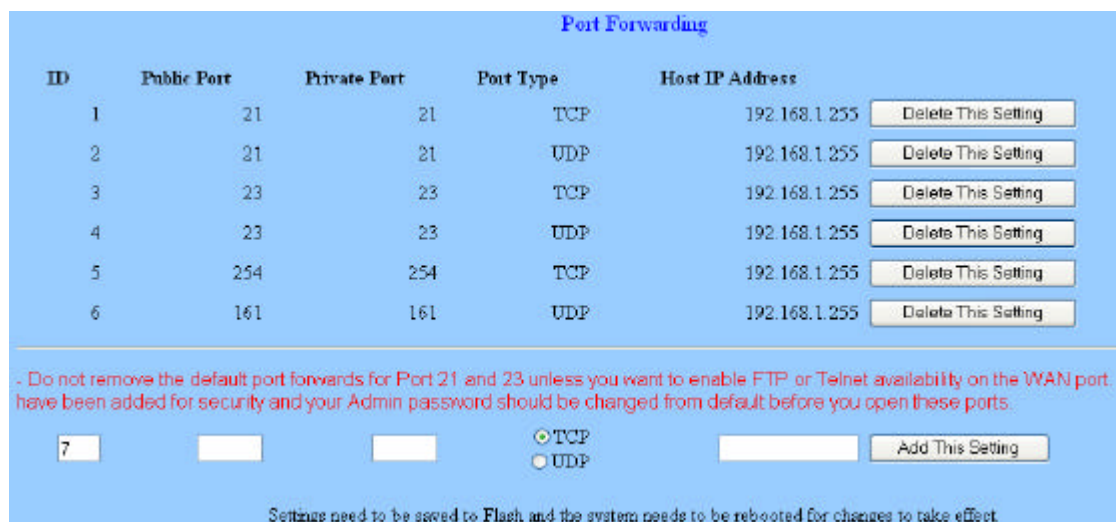
To change your User password choose the 'User Password' option on the menu and you will see a screen similar to the Admin Password screen above. Enter your new password twice, once in each field and then click the submit button.

4. **SNMP** – Simple Network Management Protocol is used to manage devices on networks from a central location. The authentication for SNMP is based on ‘Community Strings’ these are like passwords and should be treated as such when it comes to security. If SNMP is available in your Router (NB1300) you should change all your community strings (both public and private) to more secret names with more complexity. If you wish to block SNMP access from the Internet you should create a dummy port forward for external port 161 as is displayed in the image below for points 5 or 9.
5. **FTP** – The FTP server that is built into the NB1300 is not normally used by the average user and so it should be disabled. This will not affect any FTP services running through the NB1300 but it will prevent local and remote access to the FTP server of the NB1300.

Note: The FTP server is used by NetComm’s Easy Config software to send a pre-configured profile to the NB1300. If you disable FTP you will not be able to use the Easy Config software with the NB1300 until it is reset to factory defaults.

You can leave the FTP server enabled but not vulnerable to access via the WAN port by adding two ‘Dummy dead-end’ port forwards as shown in the screen shot below, with this method you can still use Easy Config to configure the NB1300 locally but FTP via the WAN is blocked.

Note: This security method is automatically incorporated into Firmware versions 5.x.x as shown below.



ID	Public Port	Private Port	Port Type	Host IP Address	
1	21	21	TCP	192.168.1.255	Delete This Setting
2	21	21	UDP	192.168.1.255	Delete This Setting
3	23	23	TCP	192.168.1.255	Delete This Setting
4	23	23	UDP	192.168.1.255	Delete This Setting
5	254	254	TCP	192.168.1.255	Delete This Setting
6	161	161	UDP	192.168.1.255	Delete This Setting

Do not remove the default port forwards for Port 21 and 23 unless you want to enable FTP or Telnet availability on the WAN port. have been added for security and your Admin password should be changed from default before you open these ports.

7 ☒ TCP Add This Setting
☐ UDP

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

6. **HTTP** – The HTTP server built into the NB1300 is used to allow you to view configuration pages via a web browser. You can set the NB1300 to allow this information to be viewed or changed via the LAN or via the WAN (Internet) or both. The Defaults shown here are for Firmware V4.004.1 and they show the access restricted to the LAN. To secure your NB1300 you should have the WAN check box disabled as shown in the screen shot below as this will prevent configuration access from the internet. You can change the port that the service runs on (e.g port 8080 instead of 80) but this means when you

access your NB1300 you will need to include the different port when you type its IP address E.g;

<http://192.168.1.1:8080>

You could disable LAN access but this would prevent you from making further changes or viewing your routers status.

Note: If you block yourself out of your NB1300 you will have to use the Reset button to return to factory defaults.

7. **DMZ Host** – The DeMilitarized Zone Host setting is used to specify the IP address of a computer (Host) that will deal with any data received from the internet that is not a response to an internal computer's request (via NAT). This data would normally be 'dropped' by the NB1300 but if you wish to allow external access to a particular internal computer, this option is used to 'expose' the 'Host' to raw connections from the internet.

The DMZ host feature is most commonly used to allow Internet users access to a Web server or Game server.

To secure your network you should ensure that the DMZ host feature is disabled. If you need to use the DMZ host feature you should ensure the computer with the IP address specified is secured with a firewall.

8. **Half Bridge mode** – This mode allows the NB1300 to work in an 'Unnumbered port' mode which means that you can plug only one computer into your NB1300 and that computer will be assigned the public (internet) IP address as designated by your ISP. In this mode your computer will be directly exposed to the Internet even though the NB1300 is logging into and maintaining a PPP connection to your ISP. This mode should be disabled for security, if you want to use Half bridge mode you should run personal firewall software on your computer.

Miscellaneous Configuration

HTTP server access

☐ All

☒ Restricted

☒ LAN

☐ WAN

Specify IP

Subnet Mask

HTTP server port

FTP server

TFTP server

DMZ

DMZ HOST IP

DHCP Relay

DHCP Target IP

IGMP Proxy

PPP reconnect on WAN access

PPP Half Bridge

Time Server IP

Time Zone

Set to 'Restricted' and tick the 'LAN' box.

Ensure 'WAN' is not ticked.

Set all of these to 'Disabled' if possible.

- 9. Port Forwarding** – This feature is similar to the DMZ host feature listed in step 7 except it allows individual ports on the public Internet IP address to be forwarded to a private IP address. This is most commonly used to allow Internet users to access a Web service on port 80 etc.

To secure your NB1300 you should not have port forwards that are not being used (excluding the FTP dead-end port forwards suggested in point 5). Any port forwards that have been configured should only specify the IP address of

secure computers. Ideally there should be no port forwards accept for “Dummy” port forwards included as factory defaults (port 21, 23, 161 & 254). If you are using older firmware you may wish to add port forwards as shown below.

Note: The ‘Dummy’ Host IP address does not have to be in the same subnet as your NB1300 LAN IP address but it should end in ‘.255’

Port Forwarding

ID	Public Port	Private Port	Port Type	Host IP Address	
1	21	21	TCP	192.168.1.255	Delete This Setting
2	21	21	UDP	192.168.1.255	Delete This Setting
3	23	23	TCP	192.168.1.255	Delete This Setting
4	23	23	UDP	192.168.1.255	Delete This Setting
5	254	254	TCP	192.168.1.255	Delete This Setting
6	161	161	UDP	192.168.1.255	Delete This Setting

- Do not remove the default port forwards for Port 21 and 23 unless you want to enable FTP or Telnet availability on the WAN port have been added for security and your Admin password should be changed from default before you open these ports.

7 ☒ TCP ☐ UDP

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

- 10. Dynamic Routing (RIP)** – RIP is disabled by default, you would only enable RIP if you want your NB1300 to accept information from other LAN routers or if you want it to share it's routing information with other router's. As always the less information a ‘Hacker’ can find out about your system the less chance the hacker has of finding an exploit for your system.

Ensure RIP is disabled if you do not need to use it.

RIP System Wide Configuration

Set to ‘Disabled’ and click submit.

RIP Disabled ▼

Supply Interval Seconds

Expire Timeout Seconds

Garbage Timeout Seconds

Submit

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

11. Telnet – Newer firmware (Release V5.x.x +) now supports Telnet which allows you to manage and configure the NB1300 via a text terminal screen. Externally there are two Telnet ports available;

Port 23 – This is the standard telnet port and it allows full control of the NB1300 in the same way that logging in as ‘admin’ does via Web / HTTP. This port is already blocked in firmware releases that include Telnet.

Port 254 – This port is an extra telnet port that allows minimal monitoring of the ADSL connection, some of the functions are disabled and although it looks like you can reset your NB1300 to factory defaults via this port, this is not true. NetComm recommend you create a dummy port forward for this port number as discussed in Point 9 (Port Forwarding) and shown below.

Port Forwarding

ID	Public Port	Private Port	Port Type	Host IP Address	
1	21	21	TCP	192.168.1.255	Delete This Setting
2	21	21	UDP	192.168.1.255	Delete This Setting
3	23	23	TCP	192.168.1.255	Delete This Setting
4	23	23	UDP	192.168.1.255	Delete This Setting
5	254	254	TCP	192.168.1.255	Delete This Setting
6	161	161	UDP	192.168.1.255	Delete This Setting

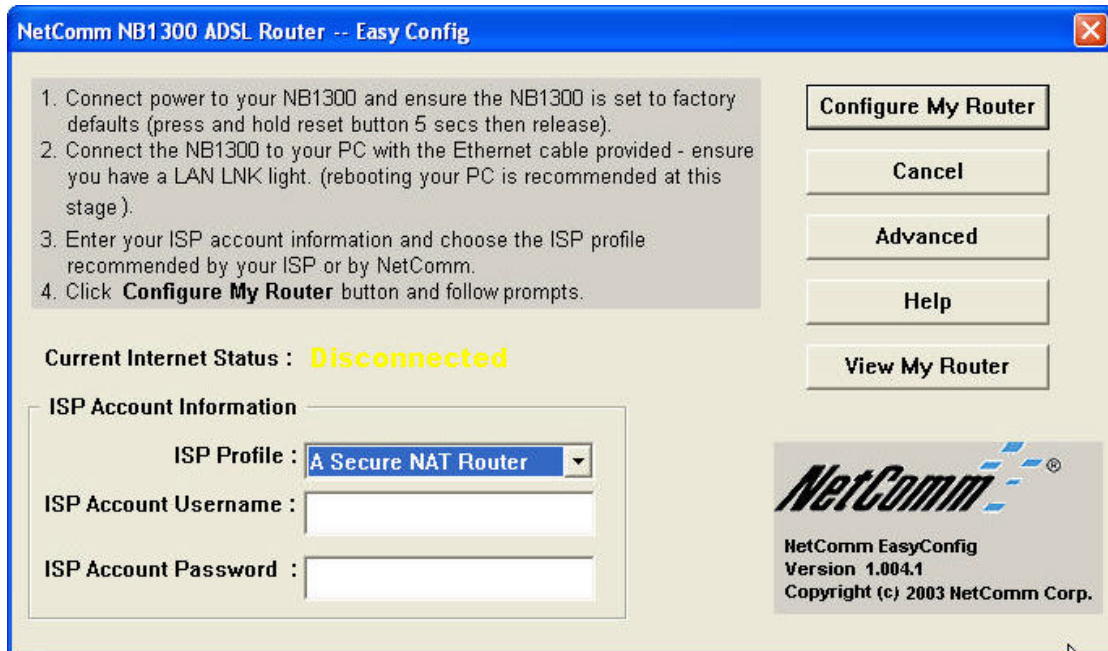
- Do not remove the default port forwards for Port 21 and 23 unless you want to enable FTP or Telnet availability on the WAN port. have been added for security and your Admin password should be changed from default before you open these ports.

☒ TCP
 ☐ UDP

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.

Other Security Measures.

NetComm's Easy Config - You can use NetComm's Easy Config software to easily deploy preconfigured profiles which include all the required ISP and ADSL settings as well as any extra security choices you want. The Easy Config software profile will include settings made to disable services such as FTP.



NetComm's Easy Config even has a feature to "Scramble the Admin Password" to lockout every one, this is offered as a simple tick box in the Advanced area of the Software. Easy config must have LAN FTP access to the unit to deploy your profile but it can be locked out by your profile.



MAC Filters – The NB1300 also has a MAC filtering function, if you wish to restrict which Network Interface Cards (NICs) can use the NB1300 to connect to the internet.

i.e. If you only use 10 computers in your network you may wish to list the MAC addresses of the NIC in just the administration computers as the only devices that can connect to the internet to prevent unwanted internet access by employees.

Resetting to factory defaults

If you forget your passwords, lock out HTTP or FTP access or simply can't remember what IP address you have set the NB1300 on you will probably need to perform a factory defaults reset.

To perform a factory defaults reset you must have physical access to the unit then follow these steps;

1. Make sure the NB1300 is powered on and the RDY light is flashing.
2. Locate the Reset button hole on the back of the unit.
3. Gently press in and hold the button for 5-10 seconds with a suitably thin appliance (E.g. a Pen). 3 seconds after release the RDY light will turn off
4. Watch the RDY light and wait for it to stabilise and start pulsing again.
5. Your router should now be set to factory defaults (192.168.1.1, 'admin' & 'password')

