'Network Connectivity Solutions'

Necoso
Het Kasteel 315
7325 PE Apeldoorn
The Netherlands

Phone: +31-(0)55-3601410
Fax: +31-(0)84-7246122
Website: www.necoso.com
E-mail: info@necoso.com

ID1021

Installation manual

The ID1021 is a product from Iolia Datacom B.V. Necoso is the exclusive dealer of Iolia products for Europe

Project	ID1021	**Document ID**	Installation Manual
Customer	<Customer>	**Version**	3.1
Classification	Public	**Status**	Final
Author(s)	Robert Hulsebos	**Date**	21-jun-2008

Summary

This document contains installation instructions and help for engineers that are about to install a <Customer product> with integrated ID1021 internet communications coprocessor from Necoso.

Document History

Version	Date	Author(s)	Description
1.0	04-apr-2002	Robert Hulsebos	First draft version
1.1	11-oct-2002	Robert Hulsebos	Updated for ID1021 firmware v1.5. Added FAQ section.
1.2	13-jan-2003	Robert Hulsebos	Updated for ID1021 firmware v1.6, new BROLIA tool options and new FTP options.
2.0	01-jan-2004	Robert Hulsebos	Updated for firmware v2.1. Necoso version
2.1	15-sep-2006	Robert Hulsebos	Updated for firmware v3.0. Necoso version, new CLI
2.2	04-jul-2007	Robert Hulsebos	Updated for firmware v3.5. Necoso version, new DNS client
3.0	05-may-2008	Robert Hulsebos	Updated for firmware v3.7. Necoso version, new security monitor
3.1	21-jun-2008	Robert Hulsebos	Added FAQs on using telnet and FTP with webbrowser. Add list of public DNS servers.

Document Distribution

Version	Date	To	Company
1.0	04-apr-2002	-major customers-	
1.1	11-oct-2002	-same as previous version-	
1.2	13-jan-2003	-same as previous version-	
2.0	01-jan-2004	-same as previous version-	
2.1	15-sep-2006	-same as previous version-	
2.2	04-jul-2007	-same as previous version-	
3.0	05-may-2008	-same as previous version-	
3.1	21-jun-2008	-same as previous version-	

Table of Contents

Appendices

Table of tables

Table of figures

1 Introduction

This document is an installation guide for engineers who need to install and configure an <Customer product> that is equipped with the ID1021 internet communication coprocessor from Necoso. The ID1021 enables usage of a web browser for configuring/controlling the <Customer product>.

The standard functions of the ID1021 in this solution are:

- to handle the internet protocols that are required for communications over an ethernet network.
- to handle the <Customer> protocol that is required for communications with the <Customer product>.
- present a HTML based user interface to the user that enables him/her to use a standard web browser (e.g. Microsoft Internet Explorer or Netscape Navigator) for configuring/controlling the <Customer product>.

1.1 Scope

This document focuses on ID1021 installation and configurations aspects for the <Customer product> only. For reading ease in the rest of this manual we use the term ID1021 as if it were a standalone device while in fact we mean the ID1021 that is integrated in the housing of <Customer product>.

1.2 Intended audience

This document was intended for installation and service engineers that are responsible for initial installation and/or service to an <Customer product> with ID1021.

1.3 Terms and abbreviations

The table below contains an alphabetical list of the terms and abbreviations used in this document.

Term/abbreviation	Description
API	Application Programming Interface
ARP	Address Resolution Protocol, as specified in RFC 826.
ASCII	American Standard Code for Information Interchange, defines character-set symbols for characters with value in range 0 – 127.
CLI	Command Line Interface
CR	Carriage Return. ASCII character with value 13. (0x0D)
CSMA/CD	Carries Sense Multiple Access with Collision Detect. Physical layer protocol as used with ethernet networks.
DCE	Data Carrier Equipment, one of two possible RS232 device configurations. See also DTE.
DHCP	Dynamic Host Configuration Protocol, as specified in RFC 2131.
DNS	Domain Name Server, as specified by RFC 1034, 1035
DST	Daylight Saving Time
DTE	Data Terminal Equipment, one of two possible RS232 device configurations. See also DCE.
EEPROM	Electronically Erasable Read Only Memory
EFS	Embedded File System
EIA	Electronic Industries Alliance, standardization organization that defines and maintains all kinds of electronics standards. (e.g. RS232 standard for serial communications)
ESA	Embedded Server Application. Application format for ID1021 applications which are permanently active. See also ISA.
Firmware	In-product software, in the context of this document: the

	software that is stored within the boundaries of the ID1021 housing.
FAQ	Frequently Asked questions
FTP	File Transfer Protocol, as specified by RFC 959.
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTML	Hyper Text Markup Language. Format for HTML pages (also called 'web pages'), as specified by RFC 1866.
HTTP	Hyper Text Transfer Protocol. Communication protocol, as specified by RFC 1945, and used by for example a web browser for retrieving a web page from a web server. (HTTP server)
IP	Internet Protocol, as specified by RFC 791
ISA	Internet Server Application. Application format for ID1021 applications that are only active when called upon by the ID1021 HTTP server. See also ESA.
LED	Light Emitting Diode
LF	Line Feed. ASCII character with value 10. (0x0A)
MAC	Medium Access Control
NetBIOS	NetBIOS is a software interface for network access and network device naming, as specified by IBM for PC/AT compatible computers. See also RFC 1001.
ID1021	Internet communications coprocessor from Iolia Datacom B.V.
NVP	Non-Volatile Parameter
PC	Personal Computer
RJ45	Ethernet interface connector of the ID1021.
RFC	Request For Comment. Normally RFC <number> refers to an internet protocol specification document with number <number>. The RFC documents are publicly available and can be downloaded from website *http://www.ietf.org/rfc/* RFC 1880 is an overview document and contains an overview of all available Internet Standards and their most up to data RFCs.
ROM	Read Only Memory
RS485	RS485 serial communications interface standard, as specified by EIA.
RS232	RS232 serial communications interface standard, as specified by EIA. In Europe this standard is sometimes also called V24.
RTC	Real-Time Clock. In this document the ID1021 internal clock that takes care of date & time accounting.
SCI	Serial Communication Interface. Name abbreviation for the serial ports of the ID1021.
SMTP	Simple Mail Transfer Protocol, as specified by RFC 821
TCP	Transmission Control Protocol, as specified by RFC 793.
Telnet	Telnet protocol, as specified by RFC 854.
TTL	Transistor-Transistor Logic
TTY	TeleTYpe – Asynchronous terminal device.
UDP	User Datagram Protocol
URL	Uniform Resource Locator, a string used in HTTP protocol for addressing (network) location of a resource (e.g. HTML page).
UPS	Uninterrupted Power Supply
UTP	Unshielded Twisted Pair. Ethernet cabling standard.
V24	European equivalent for RS232 standard, see RS232.

Table 1: Terms and abbreviations

1.4 References

The following table lists the documents that are referenced in this document.

Reference	Document ID	Version	Description/title
[ID1021]	ID1021 datasheet.PDF	2.0	*ID1021 datasheet, can be downloaded from www.necoso.com*
[RFC1533]	RFC1533.TXT	October 1993	*"DHCP options and BOOTP vendor extensions"*
[RFC1945]	RFC1945.TXT	May 1996	*"Hypertext Transfer Protocol -- HTTP/1.0"*
[ETHERNET20]	Xerox 'Blue Book'	Version 2.0, November 1982	*"The Ethernet - A Local Area Network", by Digital Equipment Corporation, Intel Corporation, Xerox Corporation*
[IEEE802.3]	IEEE standard document P802.3M	1985	*"IEEE Standards for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications"*
[RS232]	TIA/EIA-232	1997	*"Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange"*
[RS485]	TIA/EIA-485	1998	*"Electrical Characteristics Of Generators & Receivers For Use In Balanced Digital Multipoint Systems"*
[NETBIOS]	IBM document 6322916	First Edition, September 1984	*"Technical Reference PC Network"*

Table 2: Referenced documents

1.5 Overview

This document is organized in chapters and (sub)paragraphs. Chapters are used for dividing installation aspects into major aspect groups. Paragraphs and subparagraphs are used to elaborate on details aspects within a specific aspect group.

Chapter 1 introduces this document.
Chapter 2 describes the installation of the ID1021.
Chapter 3 describes the configuration of the ID1021 firmware parameters.
Chapter 4 describes how the ID1021 internal files can be updated.
Chapter 5 describes the Command Line Interface (CLI).
Chapter 6 contains a list of frequently asked questions (FAQs).

2 Installation

2.1 Pre-installation issues

Before installing an ID1021 be aware of the issues mentioned in the next paragraph(s).

2.1.1 Ethernet network issues

1. The ID1021 must be attached to an ethernet network that supports communications over the ethernet at a speed of 10 Mbit.

Explanation: This is required because the ID1021 ethernet interface only supports 10 Mbit ethernet networks. Most modern network equipment (routers, hubs, etc) support both 10 Mbit and 100 Mbit, so usually this is not a problem. However, we have come across some hubs that support 100 Mbit only. Be sure to check that the target network for the ID1021 supports 10 Mbit !

2. The ID1021 supports the DHCP protocol for dynamic acquisition of TCP/IP configuration parameters like IP address, net mask, IP address of default gateway and NetBIOS name. The DHCP server(s) controlling the distribution of these parameters can be either on the same physical network as the ID1021 or on a different network. In latter case it is required that routers in between the ID1021 and the DHCP server(s) support the BOOTP relay agent protocol. If you plan to use the ID1021 DHCP feature and you are not sure about this, please consult your local network administrator.

Explanation: The DHCP protocol uses limited broadcast of BOOTP messages for initial communication between a DHCP client (in our case the ID1021) and a DHCP server. A limited broadcast is normally not passed on to other networks by a router. Exception to this are BOOTP messages if a BOOTP relay agent is active on the router.

Note that support for DHCP can also be switched off if you don't want to use DHCP. (see paragraph 3.1.7 for more details) In that case you don't need to bother about the DHCP issue mentioned above.

2.2 Installation

This manual assumes ID1021is integrated in the housing of the <Customer product> at production time and all required connections between the ID1021 and the <Customer product> have already been made at production time before the housing of the <Customer product> was closed.
The installation of the ID1021 therefore consists only of connecting the ID1021 ethernet interface to the target ethernet network. The ID1021 ethernet interface comes in the form of an industry standard RJ45 UTP connector.

2.2.1 Connecting the ID1021 directly to a PC

This assumes the PC also has an RJ45 UTP interface and the network consists solely of the ID1021 and the PC. (no other devices attached)
In this case a so called '*cross-over cable'* must be used to connect the UTP interface of the ID1021 directly with the UTP interface of the PC.

2.2.2 Connecting the ID1021 directly to an existing intranet or internet

This assumes a network hub/router/switch is available as an intranet/internet access point and has an RJ45 UTP interface, just like the ID1021.
In this case a so called '*patch cable'* must be used to connect the UTP interface of the ID1021 with the UTP interface of the hub/router/switch.

3 Configuration

Before the ID1021 can be used after physical installation first some parameters must be configured to match the target network environment. This chapter describes those ID1021 parameters and shows how they can be configured.

3.1 Non-volatile parameters (NVPs)

The ID1021 contains some user configurable parameters that allow adaptation of the ID1021 behavior to meet the requirements of the installation environment at hand. The parameters are all 'non-volatile', which means that the last values specified for these parameters will be maintained after power off/reset of the ID1021. The values will be re-applied after every next power on or reset of the ID1021 until they are changed again by the user. In this document such parameters are called '*Non-Volatile Parameters'* or NVPs.

Appendix A contains an overview of all NVPs supported by the ID1021 and their factory default values.

3.1.1 Configuring NVP values

Normally the values for the ID1021 NVPs can be viewed / changed using one of the following options:

1. Through ethernet interface, using a telnet application.
2. Through service port interface, using a terminal or PC running a terminal application.

For both options the user interface for viewing / changing the NVP settings consists of a simple ASCII text configuration menu that is output through the respective interface. User input in the form of ASCII commands is input via the same interface.

Any telnet/terminal application capable of the settings listed in Table 3 below will do.

Parameter	Setting	Description
Terminal type	ANSI / VT52 / VT100	Menu is displayed using only ASCII characters and ANSI escape sequences for cursor control and clearing of screen.
Size of emulated terminal display	80 x 25 characters	Bottom line is used for user input. Other lines are used for displaying menu information.
Echo functionality	Local echo should be set off	ID1021 will echo all typed characters.
Character used for 'Enter' function.	ASCII <CR> character (0x0D)	ID1021 will ignore any trailing <LF> character. (0x0A)
Character used for 'Backspace' function.	ASCII <Del> character (0x7F)	ID1021 will erase last typed character by sending ASCII sequence: 0x08 0x20 0x08

Table 3: Communications set up requirements for terminal/telnet application

Configuration of the ID1021 via the ethernet interface is the most convenient as it can be done from any network station or PC that is on the same network as the ID1021. It does not require any additional RS232 cables or a configuration like configuration via the service port. However, it does require knowledge of the IP address of the ID1021.

For first-time configuration this may introduce a problem as the IP address parameters have not been configured yet and are still at their factory default values. And these values may prove to be inappropriate for the network environment at hand. Paragraph 3.1.16 deals with this dilemma and shows how first-time configuration via the ethernet interface is still possible.

In situations were the above mentioned network parameter settings of the ID1021 are unknown the configuration option via the service port can be used as a 'last resort'.

3.1.1.1 Configuring the NVP values via the service port

***Important notes**:*

- *The service port configuration option can only be used when the service port of the ID1021 is made available on the outside of the <Customer product> housing.*
- *Some customers use the ID1021 serial port that is normally used as the service port for other purposes. In this case the configuring the NVP values via the service port is not possible. See also paragraph 3.1.3.*
- *The ID1021 service port signals are by default at TTL voltage level (range 0 .. +5V), not at RS232/V24 level. (range -12 .. +12V) So external level-convertor circuitry must be added if the service port of the ID1021 is to be connected to a serial communications device that requires RS232/V24 levels. (e.g. a PC COM port) Refer to Appendix C for reference circuitry schematics.*

We recommend consulting <Customer> first to see if service port is available for use with <Customer product>.

Configuring the NVP parameters can be done through the service port of the ID1021. It requires a terminal or a PC running a terminal emulation application and a service port cable to connect the service port of the ID1021 with a RS232 port of the terminal or PC. Refer to Appendix D for example of a service port cable.

In this document we assume a PC running the Microsoft Windows XP operating system and use the standard HyperTerminal terminal emulation utility that comes for free with the Microsoft Windows operating system. (*HYPERTRM.EXE*)

HINT: A more user-friendly, GUI based, telnet program that can be downloaded from the internet is Tera Term. Tera Term is an open-source program, so it can be used for free. The website address is http://sourceforge.jp/projects/ttssh2/

HINT: See also paragraph 6.1 for FAQs on the telnet subject.

First we start up the HyperTerminal program:

Start | *Programs* | *Accessories* | *Communications* | *HyperTerminal*

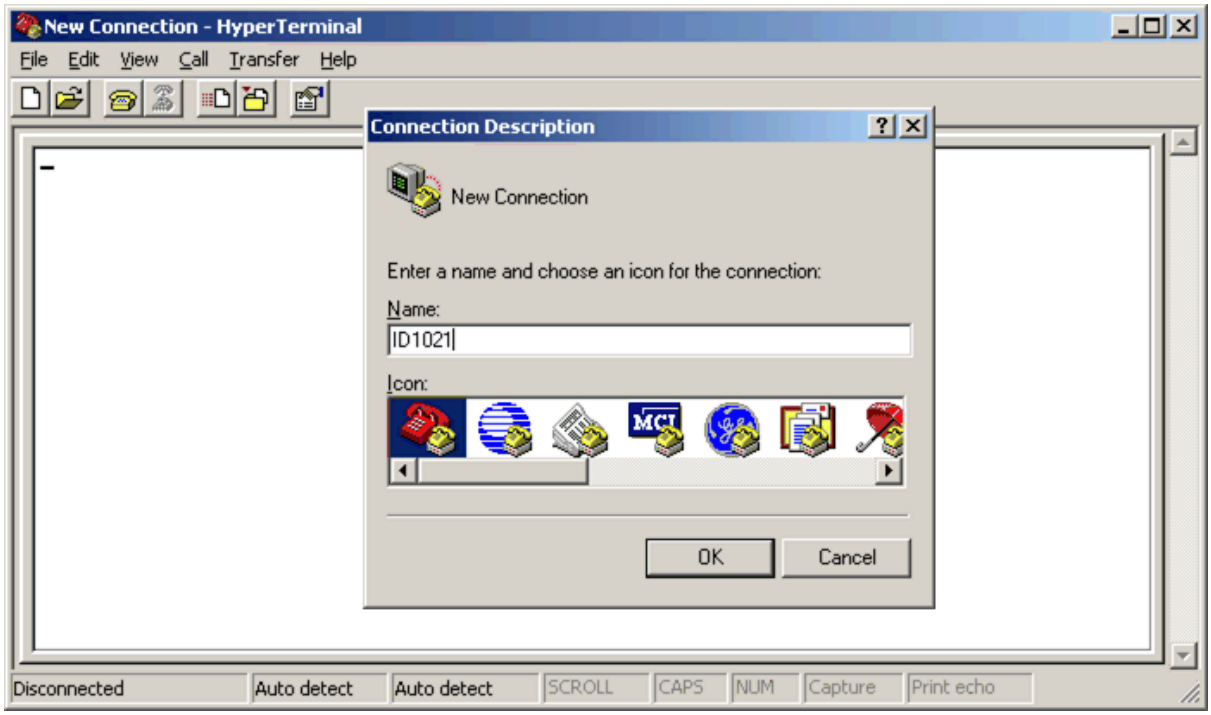


Figure 1: Starting the HyperTerminal program

It prompts us to enter a name for the new connection.
In this example the service port of the ID1021 is attached to the COM1 port of the PC.

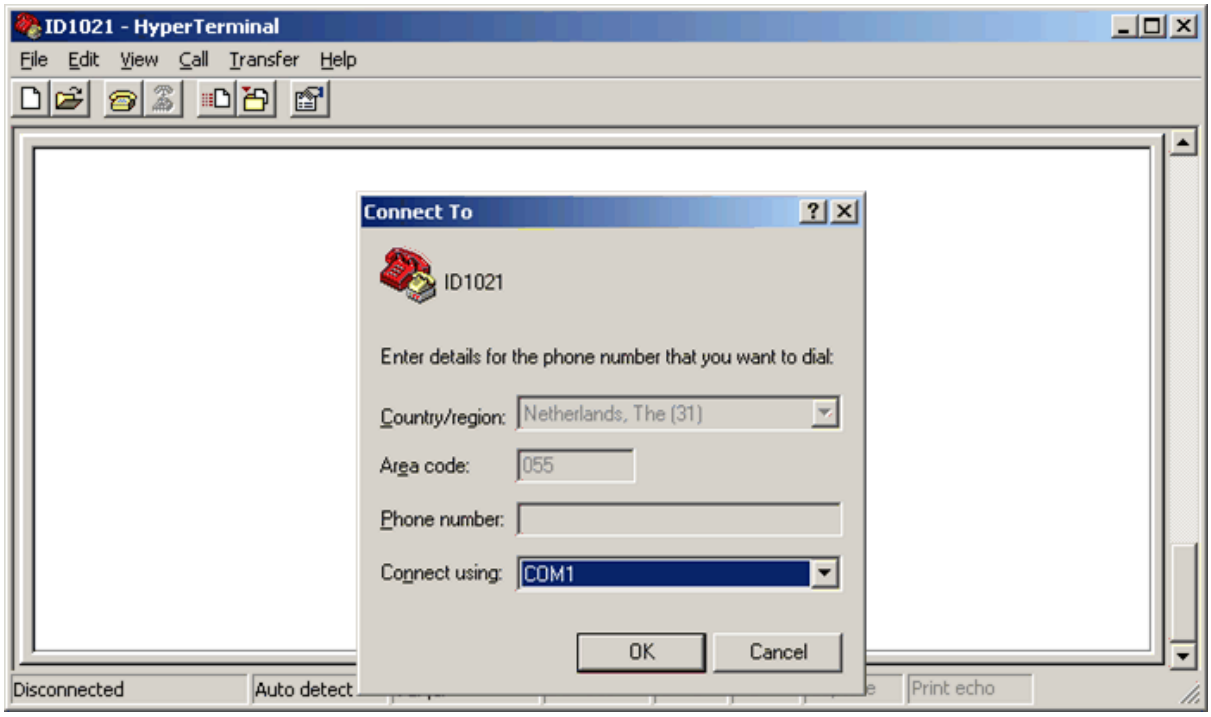


Figure 2: Configuring HyperTerminal program for COM connection (part 1)

Next, we configure the HyperTerminal communications parameters for the communications with the ID1021. Table 4 below specifies the communications set up that is required.

Parameter	Setting	Description
Communications mode	RS-232, asynchronous	See [RS232]

Baudrate	9600 baud	
Character frame	8 data bits, no parity, 2 stop bits	
Hardware/software flow control	-None-	
Inter-character delay	0	Is minimum value.

Table 4: Service port communications setup

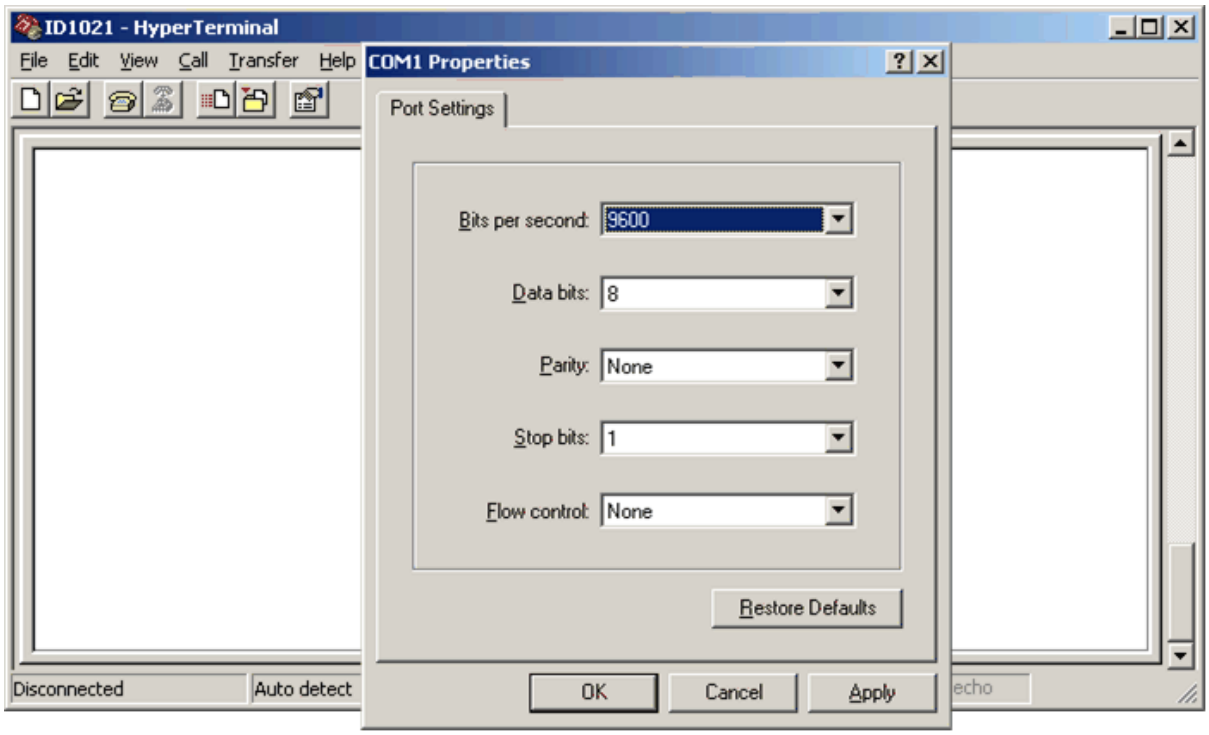


Figure 3: Configuring HyperTerminal program for COM connection (part 2)

The figure below shows the terminal emulation setup. With HyperTerminal it can be accessed via the *File* | *Properties* menu.

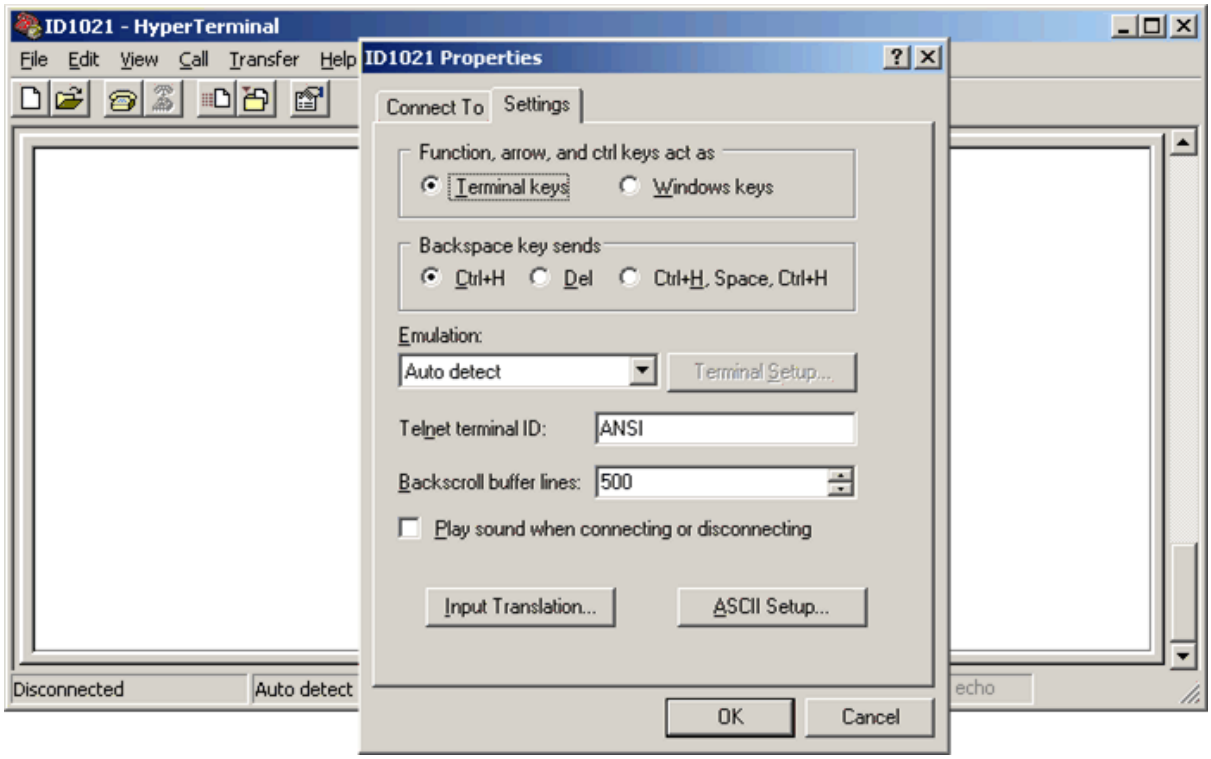


Figure 4: Configuring HyperTerminal program for COM connection (part 3)

Once the configuration is complete we return to the emulation window and press the space bar on the keyboard of the PC to force transmission of the space character (ASCII 20h) to the ID1021. The ID1021 will respond with transmitting the main configuration menu, as displayed in the figure below.

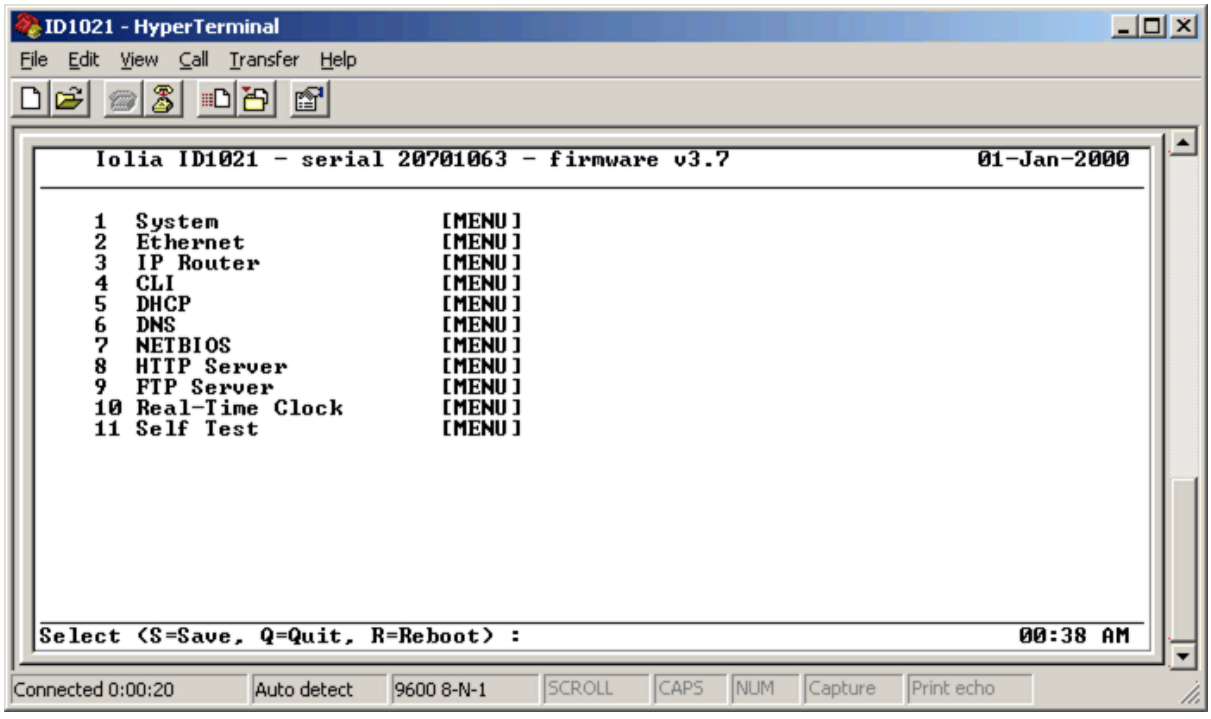


Figure 5: Main configuration menu via service port

Note that if you do not press the space bar you will not see the main configuration menu ! The ID1021 uses the space character as a trigger for setting up a configuration session via the service port.

If you do not see the main configuration menu but still got an empty terminal emulation window, then check the following:

- Is the service port cable attached to the service port of the ID1021 and the correct COM port of your PC or terminal?
- Is the communication setup of the terminal or terminal emulation program as specified in Table 4 ?
- Is the 'Configuration via service port' option enabled? (see paragraph 3.1.3)

If the ID1021 displays the message *'This service is currently in use, please try again later'* then somebody else is already accessing the configuration menu via the ethernet interface. Refer to paragraph 3.1.14 for more information.

If the ID1021 displays the message *'Please logon'* then the access security option for the configuration service is enabled. Refer to paragraph 3.1.13.1 for more information.

3.1.1.2 Configuring NVP values via ethernet interface

Configuring the NVP parameters can be done through the ethernet interface of the ID1021. It requires a PC or workstation that is connected to the ethernet network. And it also requires knowledge of the IP address or NetBIOS name of the ID1021.

In this manual we illustrate configuration of the ID1021 over ethernet using a PC running the Microsoft Windows XP operating system. For setting up a telnet connection we will use the standard HyperTerminal program that comes for free with most of the Microsoft Windows operating systems.

First we start up the HyperTerminal program:

Start | *Programs* | *Accessories* | *Communications* | *HyperTerminal*

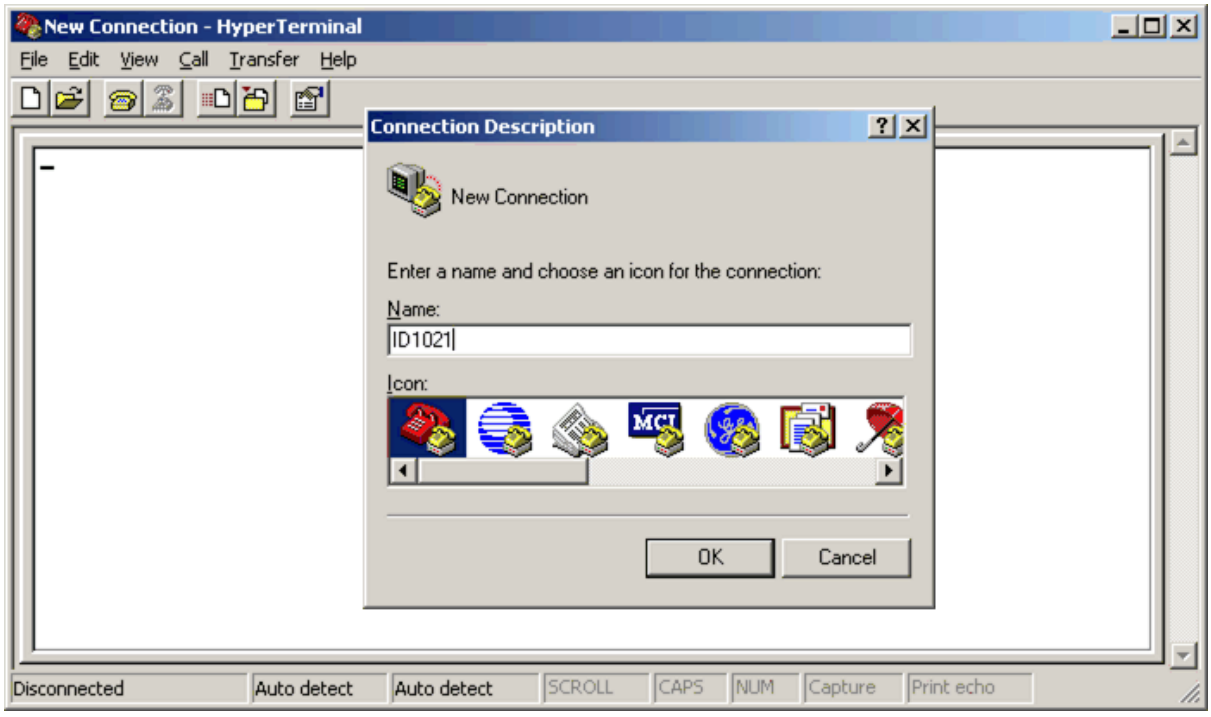


Figure 6: Starting the HyperTerminal program for setting up telnet connection

It prompts us to enter a name for the new connection. In this example we enter the name 'ID1021'.

Next, we must enter the IP address and port number for the connection.

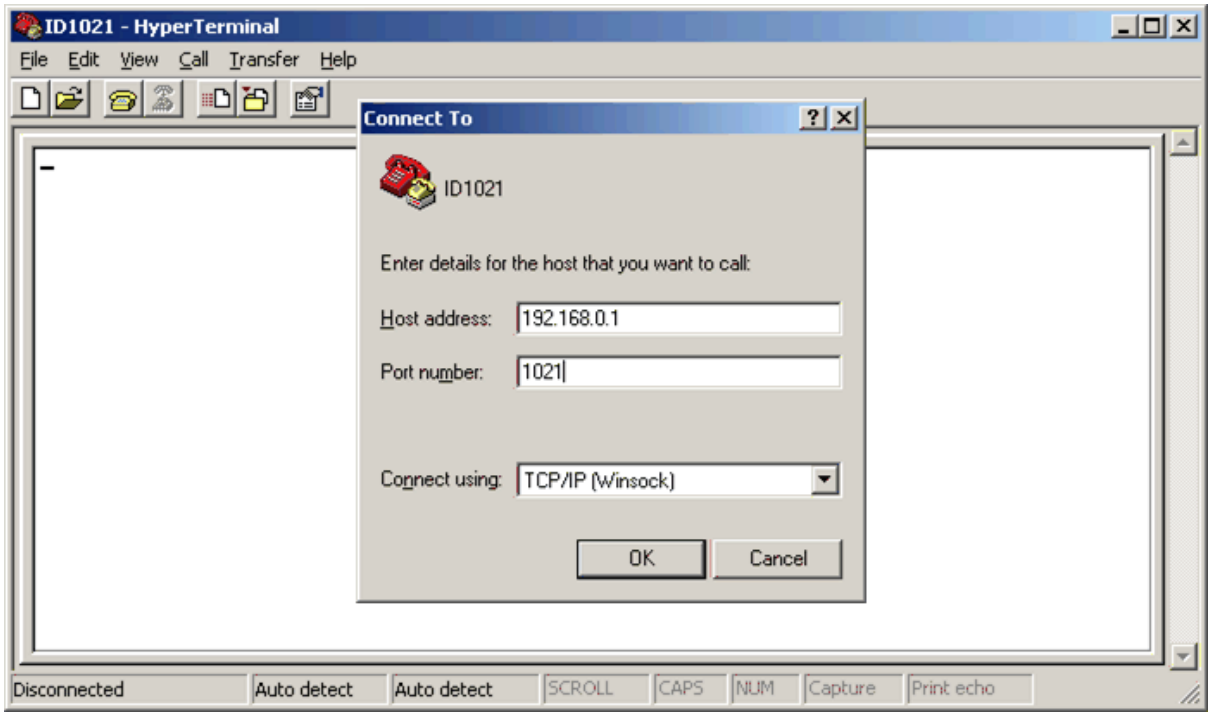


Figure 7: Configuring HyperTerminal program for telnet connection

In this example the IP address of the ID1021 is 192.168.0.1, The TCP port for the configuration menu is port 1021.

After the HyperTerminal program has established a connection with the ID1021 the main configuration menu of will be displayed automatically.

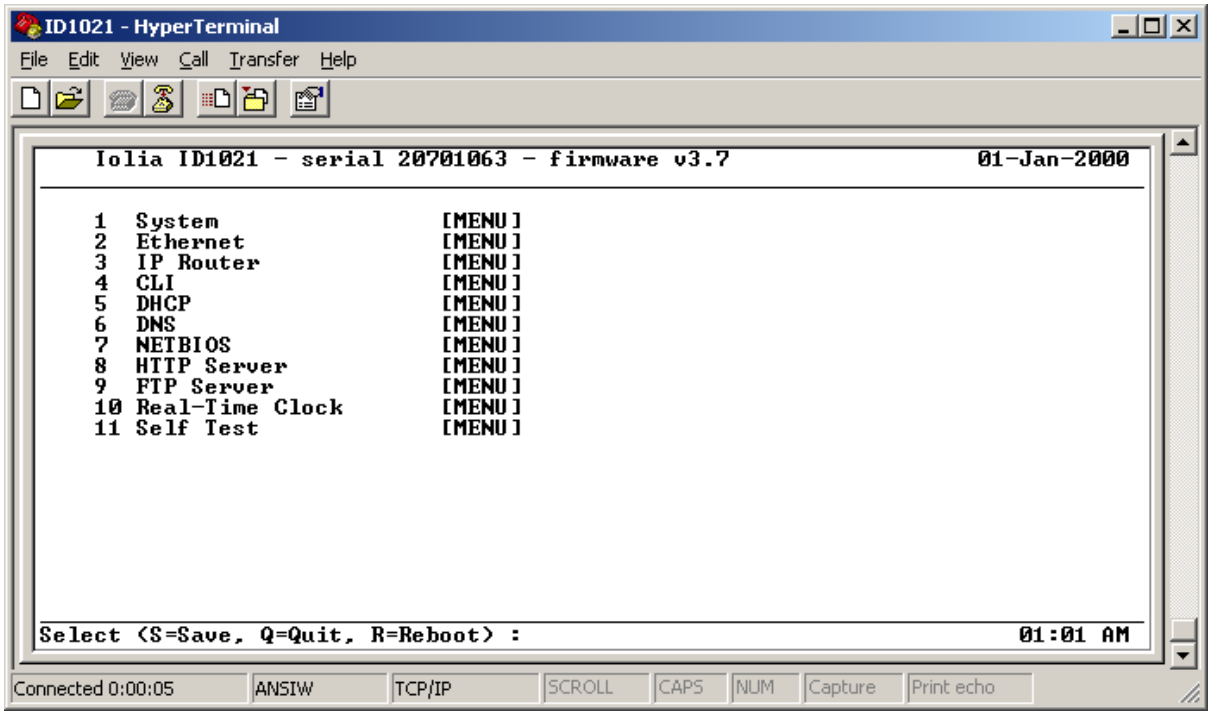


Figure 8: Main configuration menu via ethernet interface

If you see the main configuration menu then you have successfully set up a telnet connection with the ID1021. Please continue reading in paragraph 3.1.2 which will explain the various configuration menu options.

Please note that the main configuration menu that is presented may contain more menu options than the firmware menu options that are listed in the figure above. Additional menu options may be presented by the ESA applications that are active on the ID1021. These application-provided menu options will not be described here, in this chapter, but in the chapters of the respective applications themselves. This chapter only describes only the submenu options that are presented by the ID1021 firmware.

If you do not get the main configuration menu but instead still have some sort of time out error any other error indicating the connection with the ID1021 could not be established, then check the following:

- Is the PC or workstation correctly attached to the ethernet network?
- Is network communications with other devices then the ID1021 working OK?
- Did you set the TCP port for your Telnet program to 1021 as in the figures above? The standard/default TCP port for Telnet is port 23. The ID1021 will not display the configuration menu on this port. Only on port 1021.
- Can the ID1021 be reached over the ethernet network? You can check this by using the 'ping' command with the IP address or NetBIOS name of the ID1021 as a parameter. Please consult the help for the ping command on your PC or workstation for more details about its usage.
- Is the orange LED of the ID1021 ethernet interface on? The orange LED indicates the link status of the ethernet network. It is on if the ID1021 is attached to an ethernet network with a valid carrier. The LED is off when no network is attached or when the network carrier is not present. When attached to a network with valid carrier it will be temporarily off (for 10 ms) if a CSMA/CD collision is detected. If the ID1021 is attached to a network that has a valid carrier then it should be on almost permanently. If it is off then something might be wrong with the ethernet network (cabling).

- Is the green LED of the ID1021 ethernet interface showing any activity? The green LED is used to indicate data traffic on the ethernet network. It is normally on and will be temporarily off (for 100 ms) when data is transmitted/received over the ethernet interface. Pinging the ID1021 should at least result in the green LED to blink a few times.

If the ID1021 displays the message *'Please logon'* then the access security option for the configuration service is enabled. Refer to paragraph 3.1.13.1 for more information.

If the ID1021 displays the message *'This service is currently in use, please try again later'* then somebody else is already accessing the ID1021 configuration menu. Refer to paragraph 3.1.14 for more information.

3.1.2 Using the configuration menu

The figure below shows the main configuration menu of the ID1021.

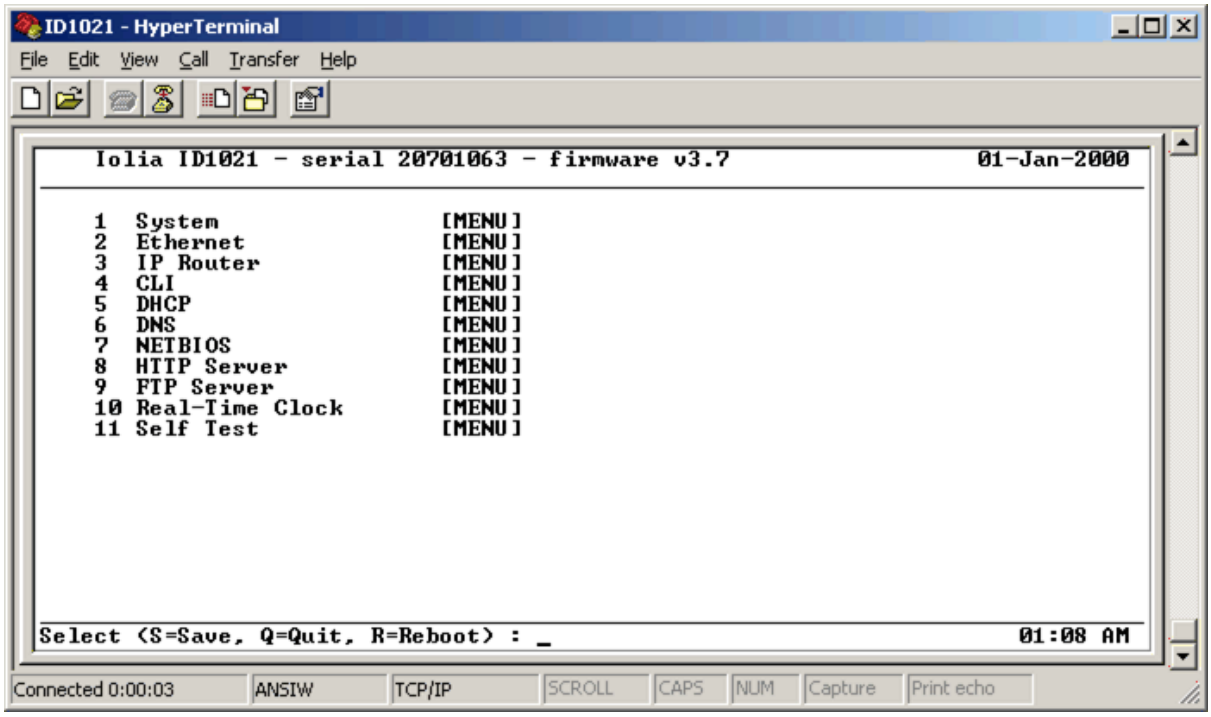


Figure 9: Main configuration menu

At the top line the ID1021 serial number, firmware version and date are displayed. The serial number is the serial number that is printed on the sticker on the ID1021 itself.
At the bottom line the command prompt and the time is displayed.
(date and time according to value of ID1021 real-time clock)

3.1.2.1 Moving through the menu system

The main configuration menu includes a number of sub-menus. Sub-menus are indicated with the text *[MENU].* A sub-menu can be selected by simply entering its number at the command prompt.
For returning from a sub-menu to the higher level main menu just hit the enter key.

3.1.2.2 Changing the value of a parameter

In a sub-menu the parameters for that sub-menu are listed, one parameter per row. At the left most position of a row the number of the parameter and its name are displayed. The current value of the parameter is displayed to the right.

You can select a parameter simply by entering its number. When you select a parameter you will be prompted to enter a new value for the parameter. After entering the new value will be displayed on the menu row for the parameter.

The input format is usually display as part of the command prompt. For parameters with enable/disable characteristics use '0' for 'disable', '1' for 'enable'.

Important note: When ever you change the value of a parameter, the new value for the parameter becomes effective immediately. This allows you to test and evaluate the new value.
However, you must save the ID1021 parameter settings with the 'S' command (is explained in next paragraph) if you want the new value to be permanent. If you do not save the ID1021 parameter settings then the changes you made to the NVPs will be lost after power on or reset of the ID1021.
Exception to this are some of the configuration menu parameters, see paragraph 3.1.3. For security and/or technical reasons the new values for these parameter become effective only after using the 'S' command and rebooting the ID1021

Note also that new values for IP router parameters are effective immediately only for new connections. For example if you change the IP address in the IP Router menu, you're current configuration service connection will not be lost. However, if you quit the current connection (with 'Q' command) and want to set up a new one, then the new IP address must be used.

3.1.2.3 Global commands

The ID1021 supports a few single character commands that can be entered at any command prompt, no matter if you are in the main menu or a sub-menu. These global commands are:

S = Save. Use this command to save the current values for all NVPs so that they can be used again after the next reset or power on of the ID1021. The NVPs are be stored in the NVP file with the name ID1021.INI on drive B of the ID1021. 'Drive B' is the name of the internal disk drive that is emulated by the Embedded File System (EFS) of the ID1021. If no NVP file exists (first-time configuration) then the ID1021.INI file will be created automatically.

R = Reboot. This command forces the ID1021 firmware to reboot itself.

Q = Quit. This command forces the Telnet session to be closed. Only one configuration session can be active at any moment in time. So you must quit the current session if you want to allow another user access to the configuration menu via either the ethernet interface or service port. (see also paragraph 3.1.14)
To avoid a session to be active for ever if a user forgets to quit, the ID1021 implements an inactivity time out mechanism that will automatically close the session after 60 seconds of inactivity, see also paragraph 3.1.15.

3.1.3 System menu

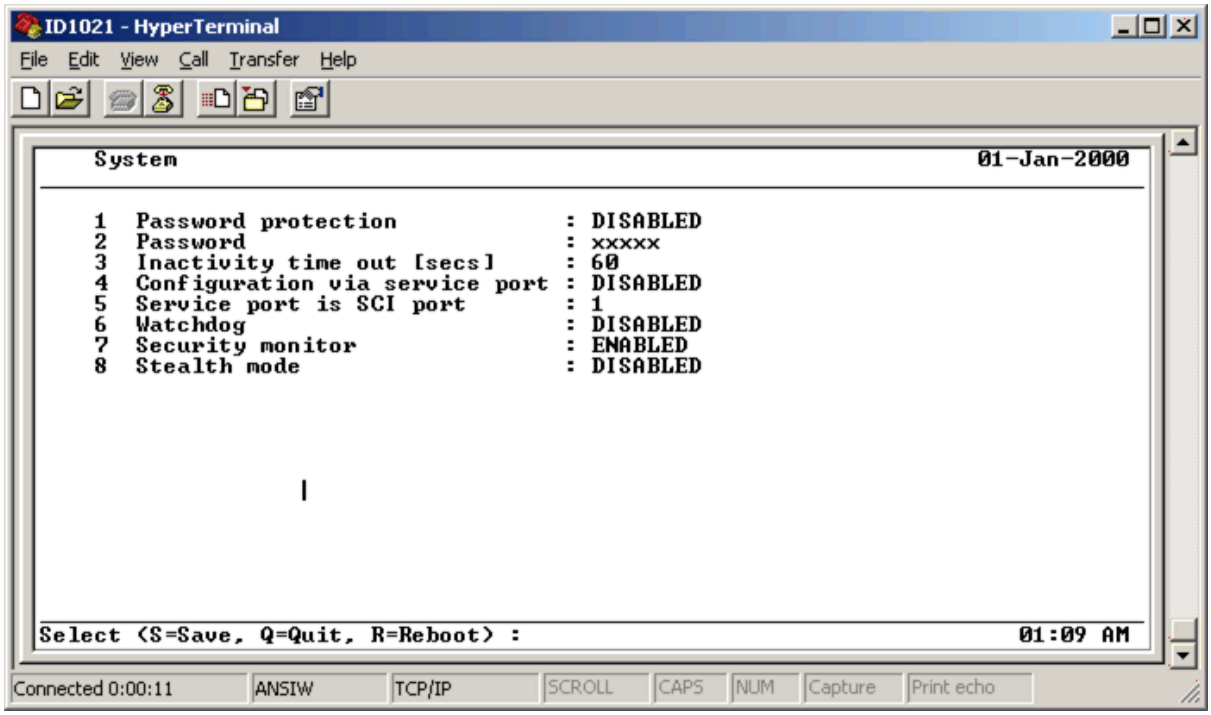


Figure 10: System menu

This menu contains access options for configuration of the ID1021 itself. It includes parameters for enabling/disabling the password protection mechanism. The password itself can also be defined in this menu. It also contains parameters that allow for an alternative interface for the configuration service. (via a serial port interface called 'service port')
The menu contains also an option for enable/disabling the hardware watchdog. The security monitor can also be disabled/enabled from this menu.

Password protection
If you enable this feature then access to the configuration menu will be password protected.
The next time you connect to the ID1021 configuration menu you will be prompted with a logon dialog for entering the password, like in the figure below.

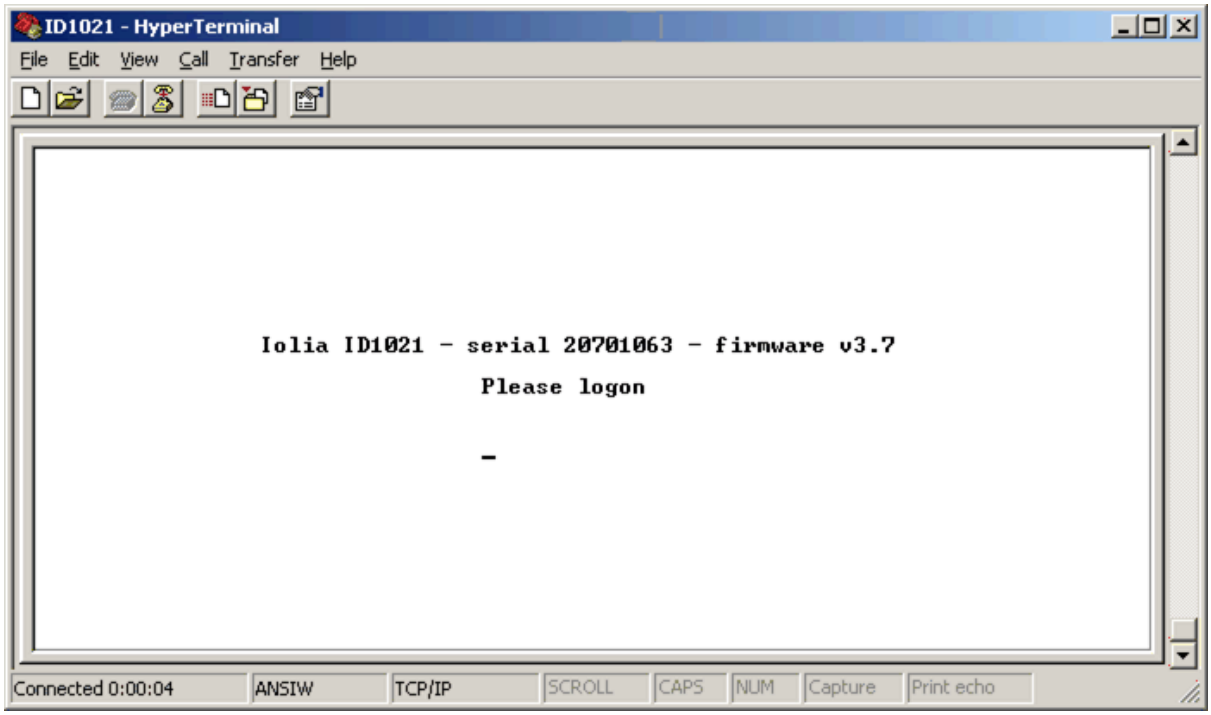


Figure 11: Logon dialog

Only the password needs to be entered. Currently the ID1021 does not support the concept of user name or account name.

Password
This parameter is the actual password for the password protection mechanism.
If you change the password, then you have to enter the new password twice. The second time is for confirmation.

Notes:

- The password protection and password parameter apply for both the service port and the ethernet interface.
- The password parameter is also used by the FTP server, see paragraph 3.1.11.
- The password parameter is also used by the HTTP server, see paragraph 3.1.10.
- The password parameter is also used by the CLI, see paragraph 3.1.11.
- The password parameter is also used for the BROLIA services, see paragraph 3.1.16.1.
- If the password is enabled/disabled than it is enabled/disabled for all interfaces and protocols that use the password.
- The logon dialog does not require entering of a user name like with logon dialogs of other computers or network stations. The system is considered a 'single user' system. For interfaces/protocols that normally enable input of a username (FTP, HTTP) the username that is entered by the user is ignored.
- The factory default password is an empty password. (password of 0 characters long). Which means that you can get access from the logon dialog simply by pressing the <enter> key on your terminal or terminal emulation program.
- Don't forget your password when you specify one, because there is no other way to access the ID1021 than through this logon dialog ! You'll have to return the ID1021 to your supplier if you do forget your password.
- The password parameter is an NVP for which a new setting does not become immediately effective. You must use 'S' command (see paragraph 3.1.2.3) to save all NVPs before the new password will be made active.
- The factory default password is an empty password. If you by accident enabled the logon feature without specifying a password, then try pressing just the <enter> key at the logon dialog.

- The maximum length for the password is 8 characters.
- The password is case-sensitive for all interfaces and protocols.
- Only digits and alphabetical characters may be used for creating a password.
- See also paragraph 3.1.13.1.

Inactivity time out
This parameter specifies the time out time for the inactivity timer of the configuration service. By default it is set to 60 seconds, which is also the minimum value. If the inactivity timer expires then the ID1021 will automatically abort the current configuration session and log off the current user. The inactivity time is automatically restarted each time the user presses a key in the configuration session.

Notes:
- The main purpose of the inactivity timer is to avoid that access to the configuration service is blocked forever if one user forgets to log off or cannot log off because his computer has hung up.
- Another reason is a security reason: the inactivity time out avoids that a password protected ID1021 configuration session is kept 'active' for ever. So unauthorized persons cannot tamper with the ID1021 if the authorized user if called away in the middle of a session and forgets to log off before he leaves his computer.
- See also paragraph 3.1.15.

Configuration via service port
As described in paragraph 3.1.1 the configuration service can also be activated for a serial port called which is then called the 'service port'. The service port can be either one of the two serial ports (SCI0 or SCI1) of the ID1021. If you want to enable this feature then you must set this menu option to enabled. With the 'Service port is SCI port…" menu you option can select which SCI port is to be used for the configuration service.
If you plan to use both ID1021 serial ports for other purposes you must disable the 'Configuration via service port' option.

Notes:
- The service port option coexists with the telnet configuration option. You can use either, but only one at a time – as only one user is granted access to the configuration service at any moment in time, see also paragraph 3.1.14.
- The ID1021 SCI port transmit and receive signals at the host interface of the ID1021 are at TTL level. You cannot directly connect those signals to a COM port of a PC. Converter circuitry (e.g. MAX232 device) will have to used to convert the TTL signal levels of the ID1021 to the RS232 levels of a COM port.

Watchdog
The watchdog is a facility that forces a reset of the ID1021 hardware in case of a software application crash or infinite loop. The reset ensures that the ID1021 will recover from such unintended and erroneous situations and that the ID1021 will remain accessible. This is especially useful when the ID1021 is far and away and human intervention to restart the ID1021 is unwanted/not possible.
By default the ID1021 watchdog is switched off, you can switch it on by enabling the watchdog option.

Backgrounder**:** How does the watchdog work? The watchdog is hardware timer that will expire after 1.7 seconds if it is not serviced by the ID1021 firmware or application. On expiration a hardware reset signal is generated by the timer, forcing the ID1021 to reset itself. Normally the ID1021 firmware and applications service the watchdog periodically, so if everything runs well, the watchdog timer will never expire. However, if an application program crashes or ends up in an infinite software loop then the watchdog will most likely not be serviced any more and a reset is imminent.

Security Monitor
This parameter can be used to disable/enable the Security Monitor. The Security Monitor monitors the communication interface for security events (hacking/sabotage), logs these events and generates alarms, if necessary. See paragraph 3.1.13 for more details about the Security Monitor.

Stealth Mode
This parameter can be used to disable/enable the stealth mode for the ethernet interface. See paragraph 3.1.13.5 for more details.

3.1.4 Ethernet interface menu

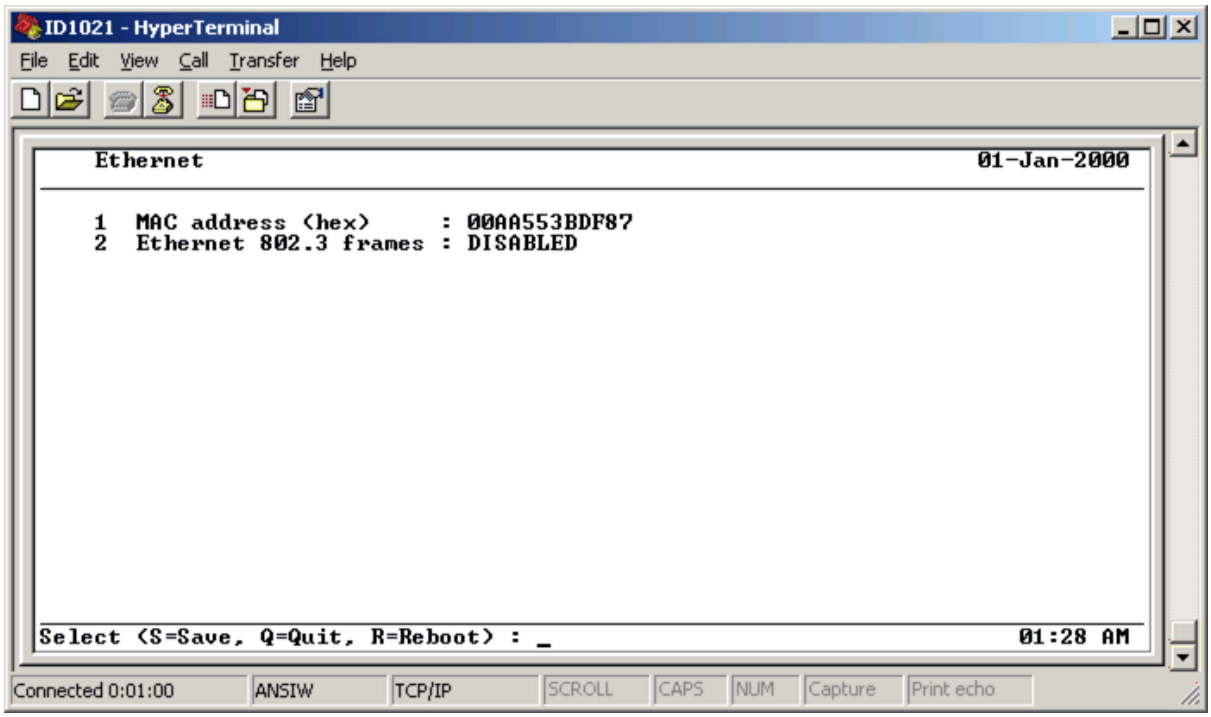


Figure 12: Ethernet menu

This menu contains parameters for the data link layer protocols of the ID1021 ethernet interface.

MAC address
This is the 48-bit unique Medium Access Control (MAC) address of the ID1021. It is sometimes also called 'ethernet address' or 'ethernet hardware address'. The MAC address must be entered in hexadecimal format. Each ID1021 is delivered with a unique default MAC address; refer to paragraph 3.1.16 for more information about how this default MAC address is generated.

Ethernet 802.3 frames
This parameter can be used to force the ID1021 ethernet driver transmitter to use IEEE 802.3 format frames. If set to 'enabled' then the ID1021 ethernet driver will transmit all frames conform the IEEE 802.3 standard. If set to 'disabled' then the ID1021 ethernet driver will transmit all frames conform the Ethernet v2.0 standard. Set this parameter to 'enabled' if the ID1021 is to be installed in a network that supports IEEE 802.3 ethernet framing only.

Notes:

- The IEEE 802.3 frame option applies only for the transmission of ethernet frames. The ID1021 ethernet driver supports seamless reception of both Ethernet v2.0 and IEEE 802.3 frames.
- Refer tot [ETHERNET20] for more information about the Ethernet v2.0 standard.
- Refer tot [IEEE802.3] for more information about the IEEE 802.3 standard.
- On a Windows PC you may need to clean the ARP table after you have changed the MAC address of the ID1021. Otherwise the PC may not be able to find the ID1021 on the network as it will still be using its old MAC address. You can clean the Windows ARP table by opening a command prompt window and enter *ARP –d ** at the command prompt. This will clean all entries in the ARP table. Use *ARP –h* for more information about the ARP command.

3.1.5 IP Router menu

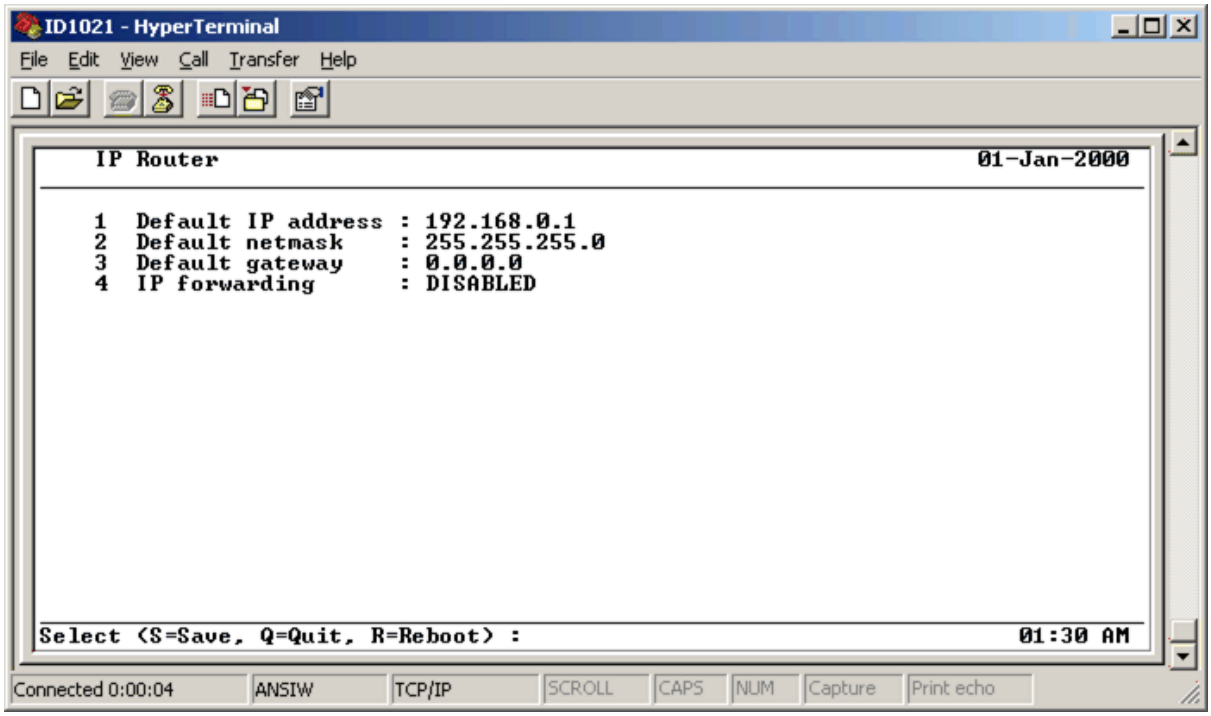


Figure 13: Router Settings menu

This menu includes the IP router parameters for the ID1021.
All parameters are noted in 'dotted-decimal' notation, which is sort of the de-facto standard format for displaying an IP address. Consult your local network administrator if you are not familiar with TCP/IP addressing parameters or if you don't know what the values for these parameters in your installation situation should be.

Default IP address
This is the IP address to be used by the ID1021 for the ethernet interface. For TCP/IP network each device must have a unique IP address.

Default netmask
The netmask is used by the ID1021 as a bit mask for determining the network number part and host number part of an IP address.

Default gateway
This is the IP address of the default gateway host. The default gateway is used by the IP router when it needs to send IP packets to a host that cannot be reached by the ID1021 directly, for example when the destination host is on a different network. The ID1021 sends those packets to the gateway host which then takes care of routing them to the

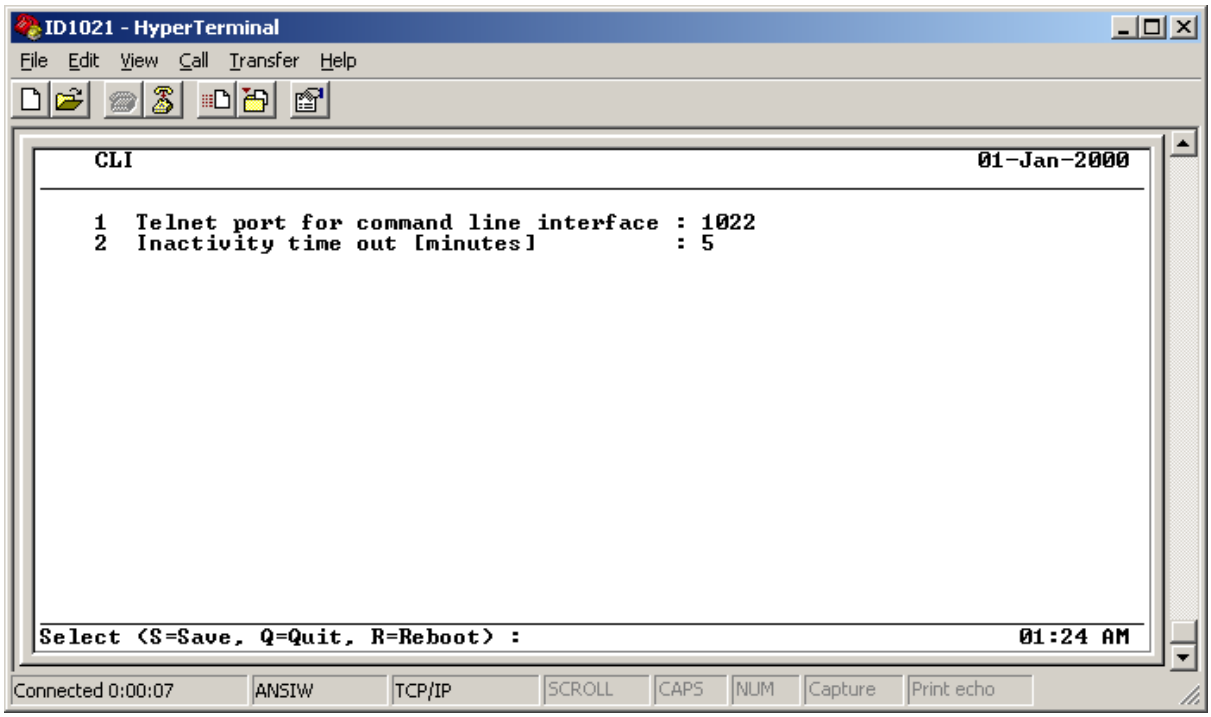
destination host. In case of return packets from the destination host it routes them to the ID1021.

Important note: The parameters in the router menu are only used by the ID1021 in the following situations:
1. DCHP feature is disabled.
2. If DHCP feature is enabled, but retrieval of IP address from DHCP server failed and the 'If fails, apply defaults' option in the DHCP sub-menu is enabled.

Appendix B contains an overall flow diagram that shows which parameter values are used by the ID1021 IP router after power on or reset.

IP forwarding
This option is only required by specific applications that implement their own alternative IP interface. Normally you need not change the setting of this parameter.

3.1.6 CLI menu



The CLI is the Command Line Interface for the ID1021. It enables users to issue commands to the system in a telnet window and returns the results of the executed commands. For more information about the CLI refer to chapter 5.

Telnet port for command line interface
By default the CLI can be found at TCP port 1022. You can use this parameter to specify a different TCP port. When you do, make sure the port is not already in use by other protocols or services of the ID1021. See Appendix E for details on which ports are in use by the ID1021.

Inactivity time out
This parameter specifies the time out time for the inactivity timer of the CLI telnet session. By default it is set to 5 minutes. If the inactivity timer expires then the ID1021 will automatically abort the current CLI session and log off the current user. The inactivity time is automatically restarted each time the user presses a key in the CLI session.

Notes:

- The main purpose of the inactivity timer is to avoid that access to the CLI service is blocked forever if one user forgets to log off or cannot log off because his computer has hung up.
- Another reason is a security reason: the inactivity time out avoids that a password protected CLI session is kept 'active' for ever. So unauthorized persons cannot tamper with the ID1021 if the authorized user if called away in the middle of a session and forgets to log off before he leaves his computer.

3.1.7 DHCP menu

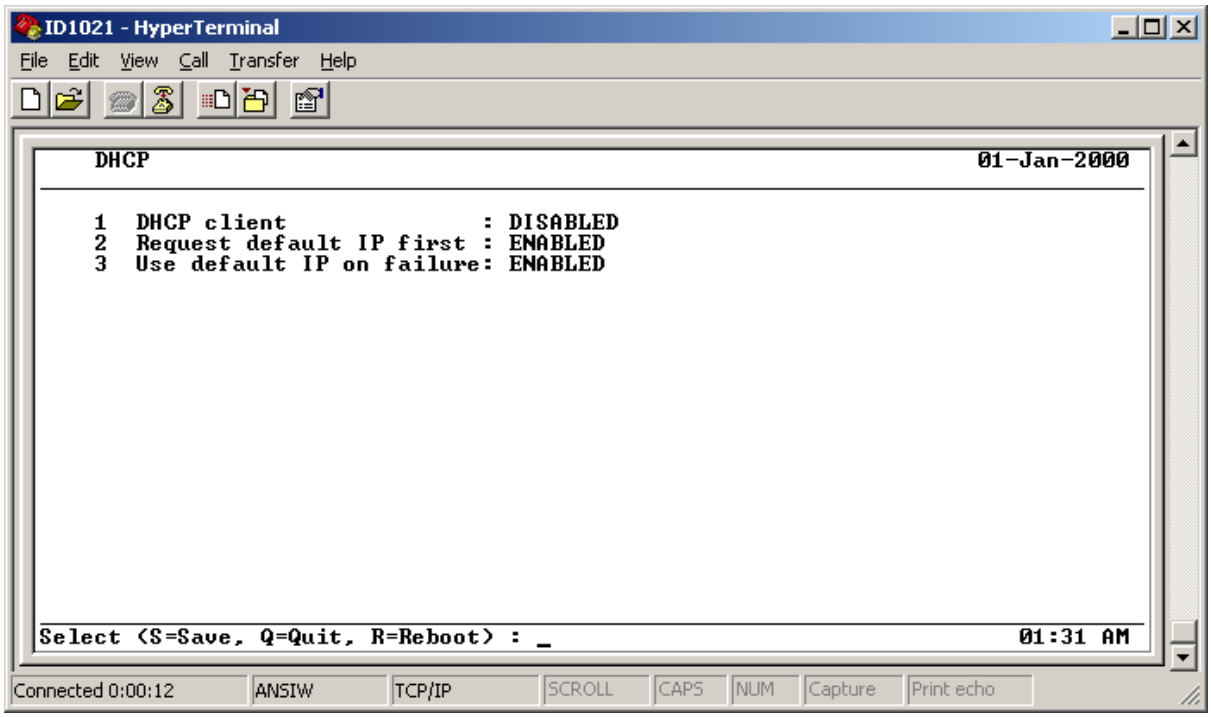


Figure 14: DHCP settings menu

Use this menu to change the DHCP parameter settings for the ID1021.
Getting DHCP to work can be a tricky operation. Consult your network administrator if you are not familiar with the DHCP features that apply for the network where the ID1021 is installed.

DHCP client
With this menu option the ID1021 support for the DHCP protocol can be disabled or enabled. If enabled, then the ID1021 will try and retrieve the IP router parameters (IP address, netmask, default gateway and –optionally- NetBIOS name) from a DHCP host on the ethernet network.

Request default IP first
This menu option tells the DHCP client to try and request the IP address that is installed in the IP Router menu first. The DHCP server may or may not honor this request. There is no guarantee. Set this option to 'enabled' if you must use DHCP but want to use a preferred IP address for the ID1021.

Use default IP address on failure
This menu option tells the DHCP client to use the default IP address that is defined in the IP Router menu if the DHCP fails. This way the ID1021 is still accessible over the ethernet interface, even if retrieving an IP address from a DHCP server does not succeed.

3.1.8 DNS menu

The internet Domain Name System (DNS) associates various information with so called domain names; most importantly, it serves as the "phone book" for the internet by translating human-readable computer hostnames, e.g. *www.example.com*, into IP addresses, e.g. *208.77.188.166*. The DNS is built on a client/server architecture that consists of DNS servers and DNS clients. The DNS servers provide the "phonebook" service. The DNS clients make use of this service.
The ID1021 needs access to domain servers to perform this domain name translations for some of the other internet protocols it supports. The ID1021 fimware therefore implements a DNS client. The DNS menu allows for configuring the DNS client.

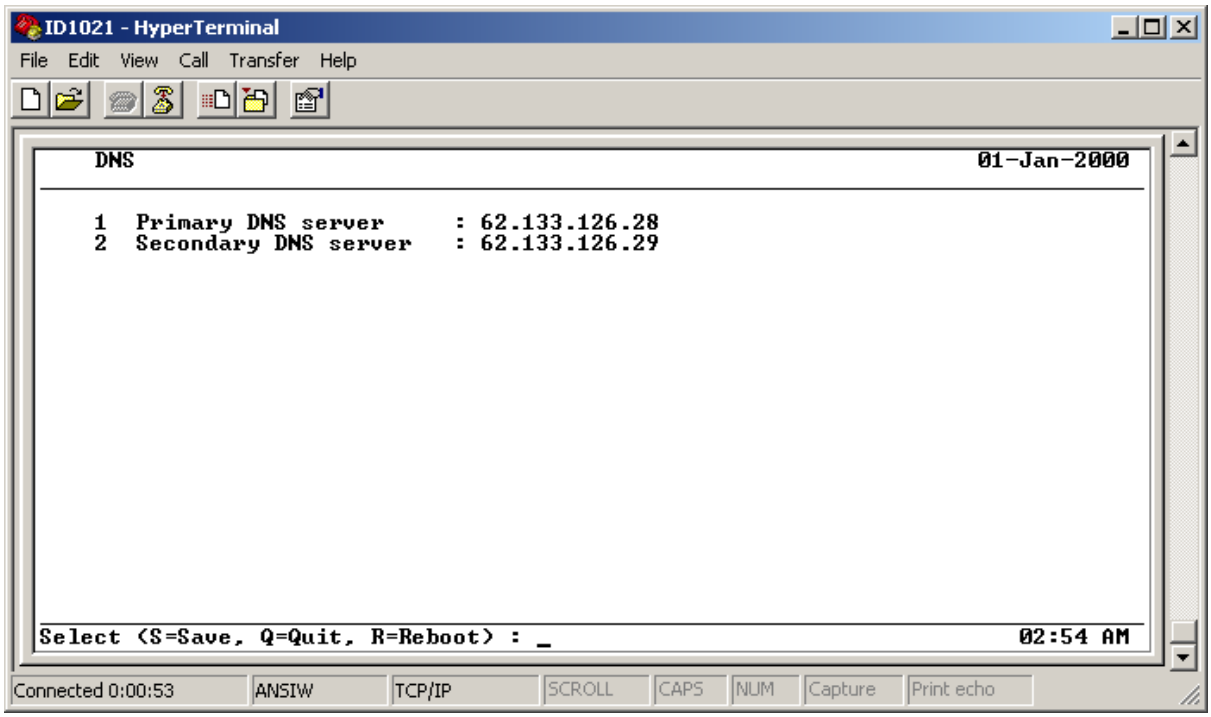


Figure 15: DNS menu

Primary DNS server
This parameter contains the IP address of the primary DNS server that will be used for resolving domain names into IP addresses. See Appendix F for a list of major DNS servers in the Netherlands.

Secondary DNS server
This is the IP address of the secondary or backup DNS server. Normally this server is only used if the primary server is down or too busy.

Note that the DNS client can be disabled by setting both parameters to value 0.0.0.0.

3.1.9 NetBIOS menu

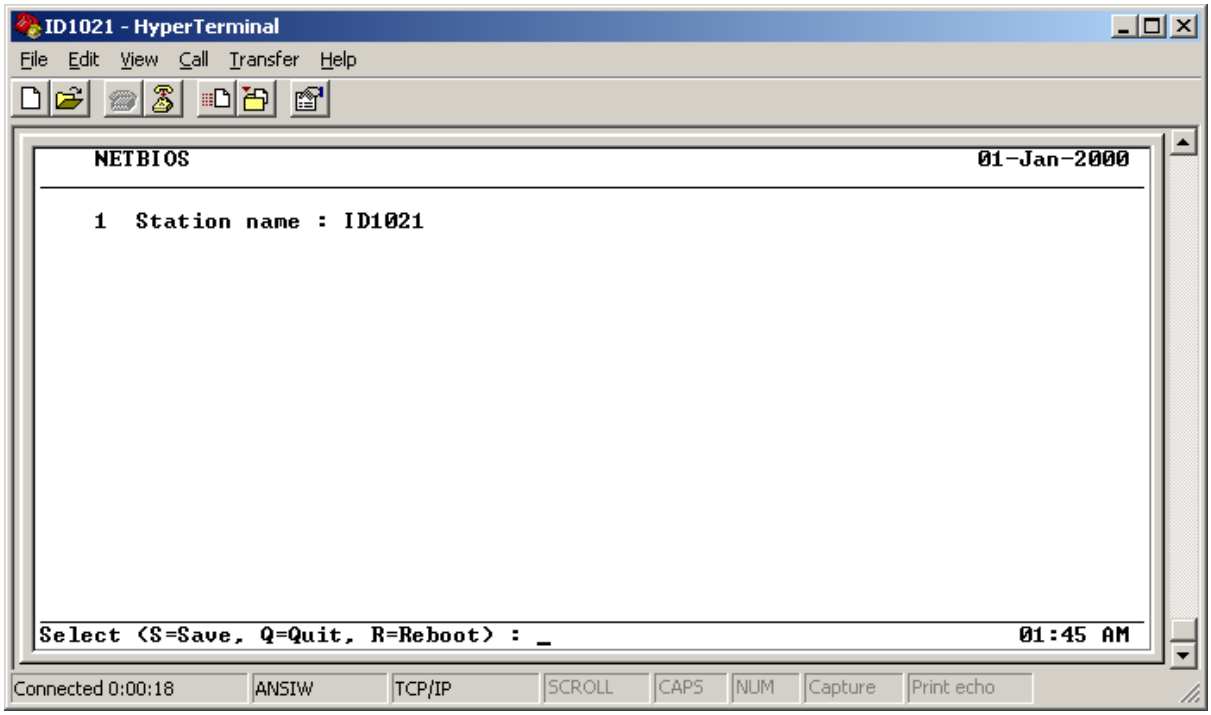


Figure 16: NetBIOS menu

The NetBIOS Settings menu only has one option, the option to specify the NetBIOS station name for the ID1021.

Station name
This is the character string that uniquely identifies the ID1021 for the NetBIOS protocol. The maximum length of the station name is 12 characters. The characters are converted to upper case by the ID1021 firmware. By default there is no station name defined. In the example in Figure 16 above the station name is set to *'ID1021'*.

Notes:
- The station name specified in this menu may be overruled by the name specified by the D*HCP server if support for DHCP is enabled. See paragraph 3.1.7 for more information.

3.1.10 HTTP Server menu

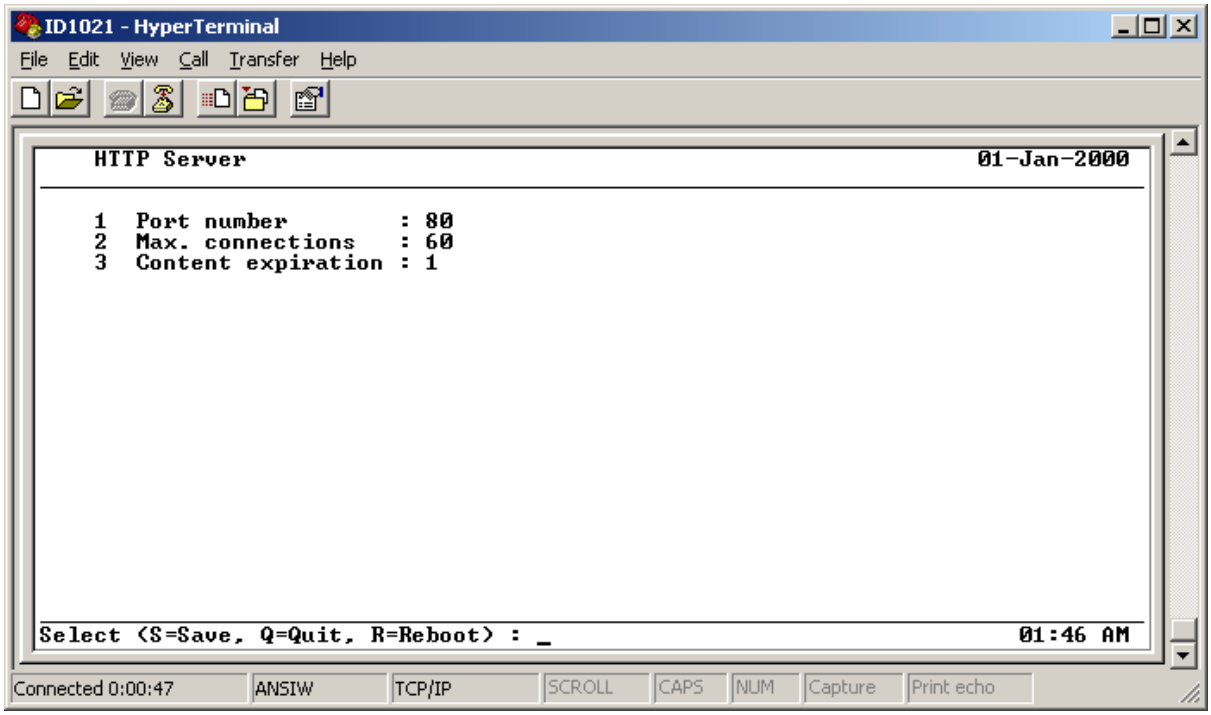


Figure 17: HTTP server menu

This menu allows for configuring the parameters for the HTTP server that is integrated in the ID1021. The HTTP server allows access to the HTML files on the ID1021 internal disk drives using the HTTP protocol, therewith emulating a small web server.

Port number
This is the TCP port number as to be used by the HTTP server for the HTTP protocol. The default/standard port number is 80. Using this option it can be defined to be a different port. When you do, make sure the port is not already in use by other protocols or services of the ID1021. See Appendix E for details on which ports are in use by the ID1021.

Max. connections
This specifies the maximum number of simultaneous connections accessing the HTTP server at any moment in time. Setting it to 0 disables the HTTP server. All users that try to access will get the error message *'Out of connections.'*
Note: For normal use don't set this to a number lower then 10, as one single webpage request from 1 user might require multiple connections. (a web browser might set up one connection for each graphical item in the webpage)

Content expiration
This menu option enables/disables webcontent expiration. If set to 1 then the web content (e.g. JPG, GIF pictures) expires immediately.
If this parameter is set to 0 then the content does not expire. So your webbrowser does not reload it every time. This may come in handy for web pages that never change.

3.1.11 FTP server menu

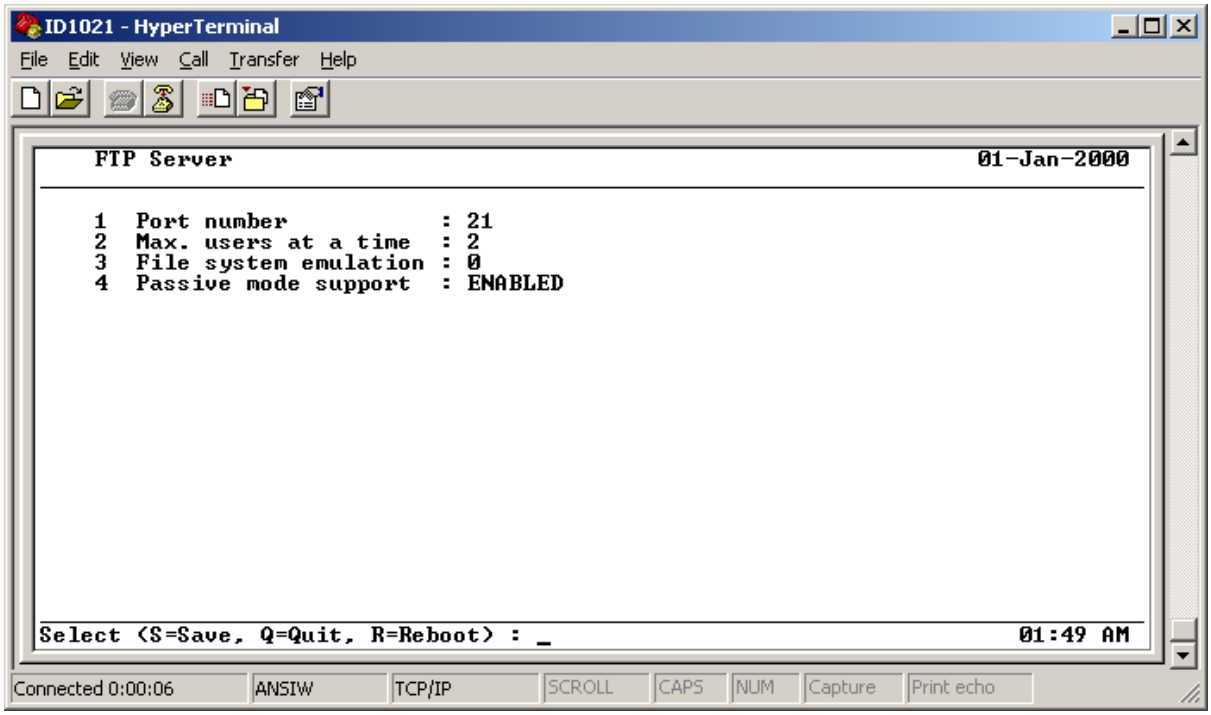


Figure 18: FTP server menu

This menu allows for configuring the parameters for the FTP server that is integrated in the ID1021. The FTP server allows access to all files on the disk drives that are emulated by the Embedded File System (EFS) driver of the ID1021. For its normal operation the FTP server of the ID1021 is not required. It is only needed when the internal ID1021 application software or web content must be updated, see paragraph 4.1.

Port number
This is the TCP port number as to be used by the FTP server for the FTP protocol. The default/standard port number is 21. Using this option it can be defined to be a different port. When you do, make sure the port is not already in use by other protocols or services of the ID1021. See Appendix E for details on which ports are in use by the ID1021.

File system emulation
The FTP server support supports emulation of 2 different file systems for the FTP protocol LIST command. By default (value = 0) the MS-DOS file system is emulated. This emulation may cause problems with FTP clients on other systems (e.g. UNIX, LINUX) that do not support the MS-DOS file system. In that case select the UNIX file system emulation (value = 1).

Passive mode support
For security or other reasons some FTP clients require file transfers to take place in what is called FTP 'passive mode'. Technically speaking this means that the FTP client is responsible for setting up the data connection with the FTP server. In a classic FTP connection, when passive mode is not used, the FTP server is responsible setting up the data connection with the FTP client. For you're convenience passive mode support is enabled by default. If you don't want passive mode file transfers then you can disable passive mode here.

- The user name for an FTP session is currently not used by the ID1021. However, some Windows versions (e.g. Windows XP) require you to specify a non-empty username. Any username will do in that case.

- The UNIX file system emulation supported by the ID1021 is based on the so called *'/bin/ls'* format for directory listings.

3.1.12 Real-Time Clock Menu

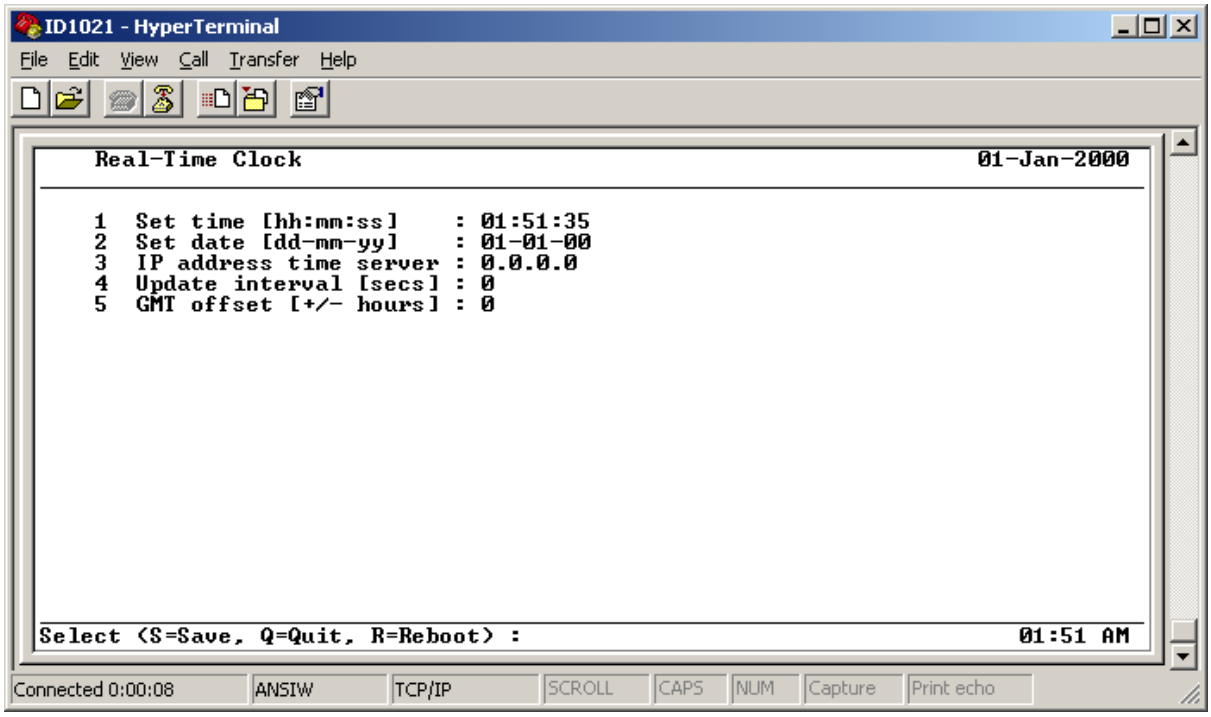


Figure 19: Real-Time Clock menu

The ID1021 supports a Real-Time Clock (RTC) timer for date and time accounting. The RTC timer has a granularity of 1 second. The RTC is not battery backed up and will loose its date & time value if the ID1021 is powered off or reset. In fact after power on or reset the RTC timer will restart with value time = 00:00:00, date = 01-jan-2000. If the RTC value is to be maintained after power down or power glitches, then an uninterrupted power supply (UPS) should be used for the ID1021.
The RTC menu allows for manual setting of date and time as well as for enabling support for a time server for automatic periodic updating of RTC over the (inter)network.

Set time
This option can be used to set the time (hours, minutes, seconds) manually. Note that the RTC is updated immediately after you enter the new time.

Set date
This menu option can be used to set the date (day, month, year) manually. Note that the RTC is updated immediately after you enter the new date.

IP address time server
Use this option to specify the IP address of the a time server for automatic periodic updates of the RTC from that time server. The time server must support the RFC 868 protocol.

Update interval
The update interval is the time between two time queries to the time server mentioned in the description of previous menu option. The interval is specified in seconds. Normally the accuracy of the ID1021 is sufficient to allow for updating only once a day.

GMT offset

This is the offset in hours relative to Greenwich Mean Time (GMT) that should be used in corrections for the time stamp received from a time server. This may be required if the time server is in a different time zone than the ID1021. (remote time server) The offset can be negative as well as positive number of hours

Notes:
- The RTC does not include support for Daylight Saving Time (DST) or automatic world time zone adaptations.
- For automatic updates both the IP address of the time server and the update interval value must be unequal to zero. It will not work if one of them is zero.

3.1.13 Security Monitor

Starting from version 3.7 the ID1021 firmware includes a new module called the 'Security Monitor'. The purposes of the Security Monitor are the following:
1. Provide a uniform mechanism for implementing access security and authentication for the communication interfaces of the ID1021. (ethernet, GSM, serial port)
2. Monitor the communication interfaces of the ID1021 for hacking/sabotage attempts or other irregularities.
3. Log security events and generate alarms for security suspicious situations.
4. Implement a special 'Stealth Mode' that makes the ID1021 less visible on the internet.

User interface of the Security Monitor
The user interface of the Security Monitor is through the CLI. The following new CLI commands are implemented by the Security Monitor:

Command	Parameters	Description
security		Reports security status and statistics.
	reset	Resets security statistics, clear security event list and black list. Resets al active alarms.
	events	Reports all events currently in the security event list.
	blacklist	Reports all entries currently in the black list.

Switching Security Monitor on/off
Although this is not recommended, the Security Monitor can be switched off using a menu option in the configuration menu on port 1021, see paragraph 3.1.3.

3.1.13.1 Access security

The Security Monitor includes a password based access security option that can be enabled through the configuration menu described in paragraph 3.1.3. This access security option forces a user to logon with a password prior to giving him/her access to the main configuration menu. A simple 'logon dialog' is implemented for entering the password, see figure below.

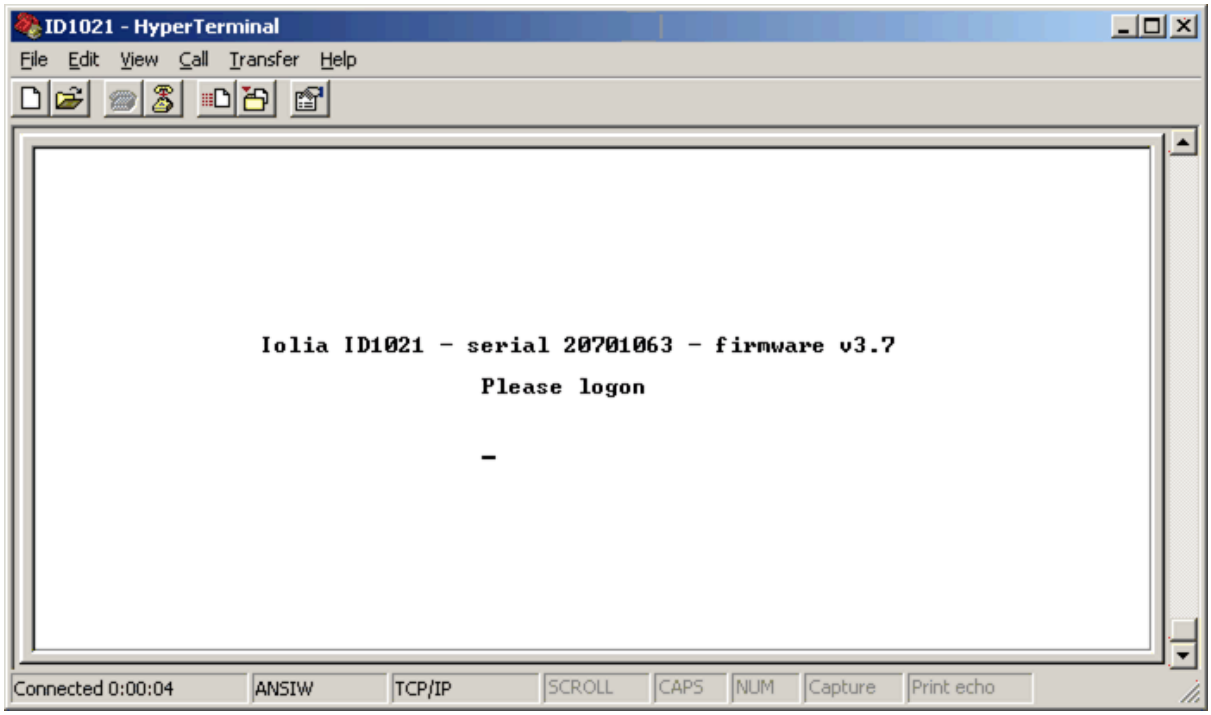


Figure 20: Logon dialog for configuration service

The same password is also used for the FTP server, the HTTP server, the CLI and the BROLIA service. The password dialog might be slightly different for each of the services.

3.1.13.2 Block timer and blacklist

A timer based blocking mechanism is implemented for password based authentication that discourages password guessing/hacking. The mechanism uses a block timer and a black list. In case of incorrect password the connection is forcibly disconnected, a black list record is created for the offending source and a block timer is started for blocking the offending source from further access for a specific period of time. This period of time is initially 10 seconds and is doubled with every next failing authentication attempt until it reaches about the maximum of approximately 12 hours. The table below describes the types of offending sources that are supported by the password authentication mechanism.

Source Type	Interfaces	Protocols	What is blocked ?
IP address	Ethernet, GSM	CLI, Configuration menu, FTP, HTTP, Brolia	Any IP based connection attempt originating from the source IP address
MS-ISDN (GSM phone number)	GSM	SMS	Any SMS message originating from the source MS-ISDN
e-mail address	Ethernet, GSM	SMTP	Any e-mail originating from the source e-mail address
-	Serial port	-	Configuration menu access at serial port

Note that for access through a GSM interface a GSM modem must be attached and special GSM.ESA application must be installed on the ID1021. By default GSM is not supported by the ID1021 firmware.

3.1.13.3 Monitoring the communication interfaces

For detecting sabotage, hacking attempts, and other forms of abuse of the ID1021, the Security Monitor watches over the interfaces and protocols of the ID1021 at various software levels.

3.1.13.4 Logging security events and generating alarms

Suspicious security events detected by the monitor are logged, counted and evaluated. Depending on the type of security event and the number of occurrences, a security alarm may be generated by the Security Monitor.

Security events are logged in a structure called the security event list. Events are added to this list as they occur and may stay on this list for one day at most. The event list is a volatile structure – its contents are lost after power-down or reset of the ID1021.
The contents of the event list can also be cleared manually, by using a specific CLI command.

The Security Monitor supports a number of pre-defined firmware security events as well as an application specific security event that may be used by ESA applications to report their own security issues.

The following table describes all security events and their triggers for alarming.

Event	Trigger for alarm (#occurrences per hour)	Description
Authentication succeeded.	500	Correct password was entered. High number of occurrences may indicate sabotage.
Authentication failed.	500	Incorrect password was entered. May indicate hacking attempt/password guessing in progress.
Packet for not supported ethernet based protocol	100	May indicate sabotage/hacking attempt in progress.
Packet for not supported ARP function	100	May indicate sabotage/hacking attempt in progress.
Packet for not supported ICMP function	100	May indicate sabotage/hacking attempt in progress.
Packet for not supported IP based protocol	100	May indicate sabotage/hacking attempt in progress.
Packet for not supported TCP port	100	May indicate sabotage/hacking attempt in progress. (port scan)
Packet for not supported UDP port.	100	May indicate sabotage/hacking attempt in progress. (port scan)
Socket limit exceeded. (too many open sockets)	1	More than 100 TCP/UDP sockets are open. May indicate sabotage/hacking attempt in progress.
Event limit exceeded. (too many security events)	1	Too many security events. May indicate sabotage/hacking attempts are in progress.
Application specific event.	Defined by application	

How does security alarming work?
The Security Monitor implements counters for counting the security events listed above. An alarm is generated if the number of occurrences of a specific event within one hour exceeds the trigger limit. Note that some security events may generate an alarm immediately. (limit = 1)
ESA applications that register with the Security Monitor for the alarm service are called by the Security Monitor whenever an alarm is generated. These applications can then take appropriate actions, e.g. notify user using e-mail/SMS message, perform self-reset, disconnect from GPRS network, etc. Eventually it's up to the user of the ID1021 to react to a security alarm, evaluate the security situation and take appropriate measures.

Once an alarm has been generated for a specific security event, the alarm remains 'active' until it is cleared by the user. Active alarms will not be generated again automatically when the security event that led to the alarm re-occurs. So human interaction is required. A user can clear all active alarms by forcing an ID1021 reset or by issuing the *'security reset'* command at the CLI command prompt, see below.

It is important to understand that the Security Monitor only detects, signals and administrates security suspicious situations. It does not handle/resolve those situations itself, or take counter measures. Evaluation of the situation at hand and taking further action is up to the user or up to an installed application.

3.1.13.5 Stealth mode

A technique used by hackers is to detect devices on the internet is to send an ICMP echo request packet ('ping') to a range of IP addresses and see which IP addresses respond. Next, a number of connection requests are sent to the responding IP addresses for various TCP and UDP ports. ('port scan') Depending on the ports that accept the connection request, the hacker then tries to determine the type of system he is dealing with, its operating system, and its vulnerabilities.
In order to discourage this kind of scanning the Security Monitor supports a special mode of operation called 'stealth mode'. This mode can be activated using the configuration menu at port 1021, see paragraph 3.1.3.
When stealth mode is active, the ID1021:

- Will no longer respond to ICMP echo packets
- Will no longer respond to connection requests to not supported TCP/UDP ports. Normally the TCP/IP stack should respond with a reject packet here.
- Will no longer respond to connection requests to supported TCP/UDP ports where application or firmware rejects the connection. (e.g. blacklist) Normally the TCP/IP stack should respond with a reject packet here.

In other words, when stealth mode is active the ID1021 is more or less invisible ('stealthy') for those who have no knowledge of the supported protocols and ports.

3.1.14 Multi-user provisions

Theoretically two or more users could access the configuration service menus for changing of NVPs at the same time. For example, one user via the service port, one user via the ethernet interface. To avoid the 'critical-races' and other multi-user aspects which might cause problems on unwanted behavior, the ID1021 implements a simple access control mechanism for the configuration service that allows one user access it via one interface only. Any other user attempting to access the ID1021 configuration menu through no-matter-what interface will get an error message (see figure below) on that interface. The session with the active user will have to end before another user is granted access.

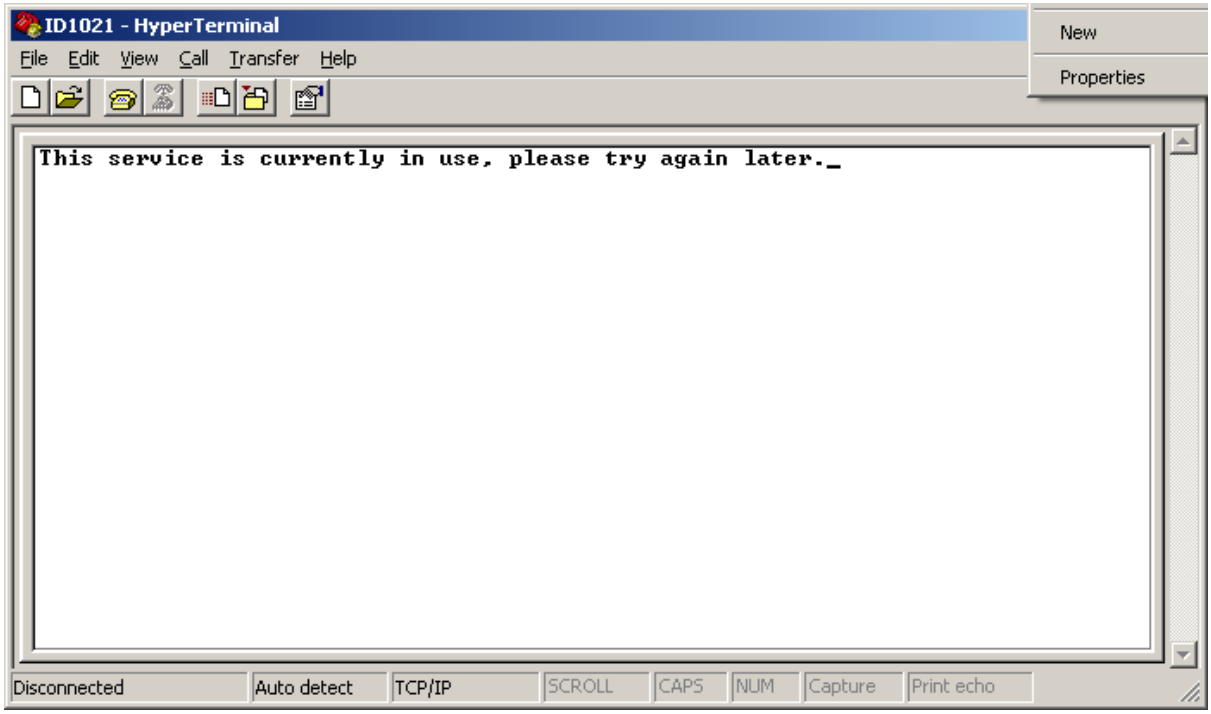


Figure 21: ID1021 configuration menu service already in use by other user

3.1.15 Inactivity time out

For security and access reasons the ID1021 implements an inactivity time out for the configuration menu via the service port and the ethernet interface. If no keystroke is sent to the ID1021 for a (default) period of 60 seconds then the ID1021 will automatically end the active configuration session.

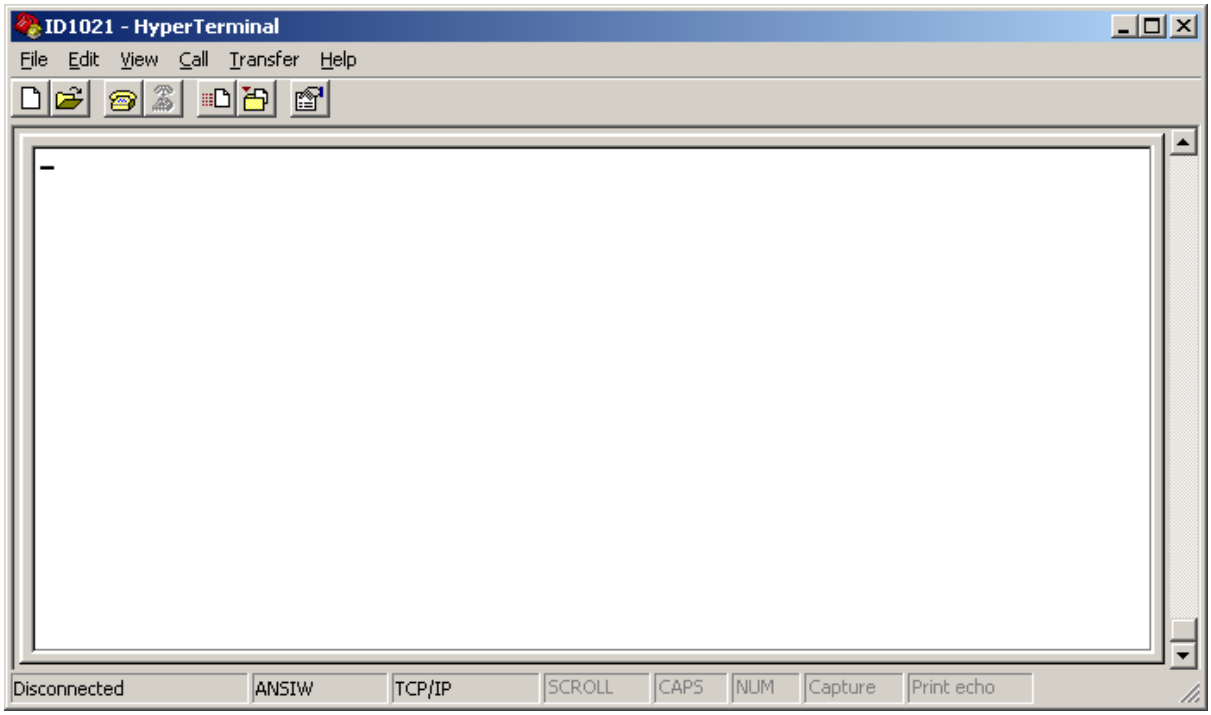


Figure 22: ID1021 has ended configuration session after 60 seconds of inactivity

Notice the 'disconnected' in the lower left corner of the figure above.

The inactivity time out time of 60 seconds is the default value. If you find it too short, you can change it in the configuration menu, see paragraph 3.1.3.

3.1.16 First-time configuration via ethernet interface

When an ID1021 has not been configured before there is no internal NVP file yet and the ID1021 uses the build-in factory default settings for all NVPs. As can be seen in Appendix A the DHCP option is enabled by default. This means that if a new ID1021 is attached to an ethernet network and powered on, it will start to try and find a DHCP server for retrieving an IP address, netmask, default gateway and optionally a NetBIOS name. Now there are two scenarios possible:

1. A DHCP server is present and the retrieval of the above mentioned parameters from the DHCP server is successful. In this case the ID1021 will use the IP address that was leased from the DHCP server and can be reached at this IP address. Usually the DHCP server software contains some kind of user interface that allows you to view the IP addresses that are in use by the DHCP clients. The BROLIA tool can also be used to find the IP addresses of the active ID1021s and may be more convenient as it shows only the detected ID1021 modules, not all other network devices that might also be on the same network. For more information on the BROLIA tool, please refer to paragraph 3.1.16.1.

2. A DHCP server is present and the retrieval of the above mentioned parameters is not successful –or- no DHCP server is present. In this case the ID1021 will revert to the factory default settings for the IP router parameters, which are:

   IP address: 192.168.0.1
   Netmask: 255.255.255.0

   Note that the above parameter settings are fixed, i.e. hard coded in the ID1021 and are the same for *every* ID1021 that is in the factory default configuration state. It is therefore important to configure each ID1021 for its final IP address, netmask and default gateway as soon as possible.
   To avoid IP address conflicts (i.e. multiple use of same IP address) all ID1021 units should be re-configured one after the other, with the other ones in a powered off state. I.e. only one ID1021 with the above mentioned factory default configuration should be powered on at any moment in time.

3.1.16.1 Using BROLIA tool to determine ID1021 network parameters

The BROLIA tool can be used to determine if any ID1021 modules are connected to the network and the IP addresses they are currently using. This may come in handy in situations where DHCP is used and the IP address leased by the ID1021 from the DHCP server is unknown or may vary in time.

If the BRIOLIA tool is run without specifying any command-line options, then it will scan the network for any ID1021 that is currently present and report the serial number, IP address and ethernet (MAC) address for every ID1021 it finds.

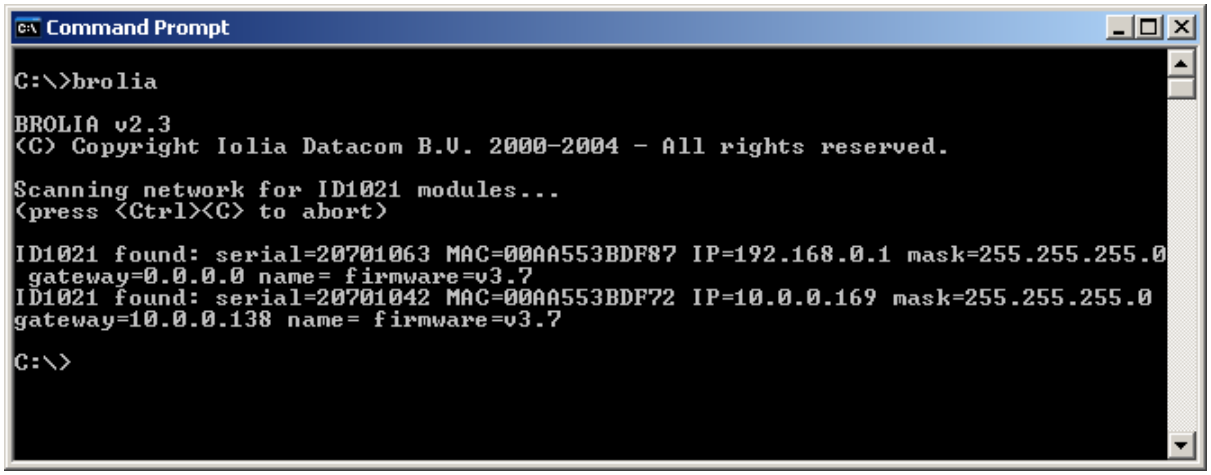


Figure 23: Using the BROLIA tool to detect ID1021 modules on the ethernet network

Additional notes:

- The BROLIA tool will only scan the physical network segment to which the PC is attached that is running the BROLIA tool. It cannot scan any network segments that are behind routers or switches. So only ID1021 modules that are on the same physical network segment will be detected.
- When more then one ID1021 is attached to a network it may be difficult to determine which ID1021 is using which DHCP leased IP address. Normally the unique MAC address of a network device is used as the unique key in a DHCP lease contract. For the ID1021 the factory default MAC address is generated from the serial number of the ID1021 using the following formula:
  1. Convert ID1021 decimal serial number into 32-bit binary serial number.
  2. The most significant 3 bytes of the MAC address are fixed to 0x00, 0xAA, 0x55.
  3. The least significant 3 bytes are the least significant 3 bytes of the 32-binary serial number from step 1.

  Example:

  Serial number ID1021 = 67910084 (decimal) = 0x40C39C4, 3 least significant bytes are 0x0C, 0x39, 0xC4, so default MAC address will be 0x00AA550C39C4 (= 731571304900 decimal)

  So knowing the serial number of the ID1021 – normally it is located on a small sticker on the ID1021 itself – means knowing its MAC address, means knowing its current IP address. (after looking it up in DHCP Server table or with the BROLIA tool)

3.1.16.2 Connecting to the ID1021 for the first time

Now that we know the IP address of the ID1021, how do I connect to it?

If you are using a Windows PC for initial configuration chances are that the network number of the existing network to which the PC and the ID1021 are attached is different from 192.168.0.0. (which is the factory default network number used by the ID1021 if DHCP is not used or fails, see paragraph 3.1.16) Addressing the ID1021 by its default IP address 192.168.0.1 would therefore result in the TCP/IP stack on the PC consulting its default gateway host for addressing the 192.168.0.0 network. As this default gateway most probably does not know a network with this number, communications with the ID1021 will fail.

Now there are three ways to solve this network number mismatch problem:

1. Forcing the ID1021 to use a temporary IP address and netmask, for the configuration session only.

This involves using the BROLIA tool to force the ID1021 to use a temporary IP address and netmask. With 'temporary' is meant that the IP address en netmask settings will be lost after power on or reset of the ID1021. With the temporary address settings the ID1021 can be reached over ethernet and a telnet configuration session can be used to configure the final IP address and netmask and save them. After rebooting the ID1021, the final IP address and netmask will become effective.
Note that this method requires the serial number of the ID1021.

2. Adapting the routing table of the PC

This consist of adding an entry to the IP routing table of your PC that specifies the network the ID1021 is on and how to reach this network. Paragraph xx describes this method in more details for a Windows PC.

3. Adapting the network address of the PC to match that of the ID1021

This involves reconfiguring the TCP/IP address parameters of your PC to match the network number of the ID1021. This is quite rigorous and may influence any other network communications/services that are currently in use on the PC or on the network itself. It is therefore not recommended for configurations where there are more devices on the network then just the PC and the ID1021.

However, it is the fastest and easiest solution for a configuration where there are only 2 devices on the network. (PC and ID1021) Typical example of this is a configuration where an ID1021 is configured with a PC/laptop using a dedicated direct connection with a cross-over UTP cable. For an example of how to adapt the TCP/IP address parameters on a MS-Windows PC, see paragraph 3.1.16.4.

Which method should I use ?

The first method is by far the most convenient one. However, it requires the BROLIA tool and can therefore only be used on systems where the BROLIA tool can be run. (i.e. MS-Windows PCs)
The second method is less rigorous when compared to the third method as it does not require changes to the TCP/IP address parameters of the PC. So we recommend using the first method if possible. If not, then try the second method. Use third method only as a last resort.

3.1.16.3 Forcing the ID1021 to use a temporary IP address and netmask

Important: *If you are unfamiliar with IP addresses, network addresses, netmasks, etc please consult your network administrator and ask him for advice before you start the operations described in this paragraph!*

For this operation the BROLIA tool and the serial number of the ID1021 is required. The serial number is mentioned on the top line of the configuration service main menu (for example, see Figure 9), but also on the ID1021 PCB itself, on a small barcode sticker. (see picture below)

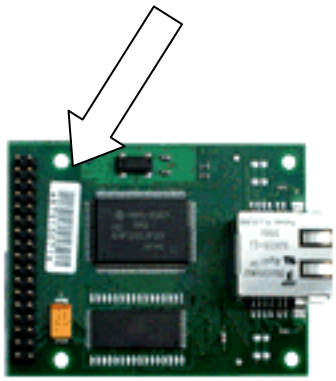


Figure 24: Location of the serial number sticker on the ID1021

It is also required that the system on which you are running the BROLIA tool is attached to the same ethernet network segment as the ID1021. There should not be a router in between them.

Open a command prompt window and enter the following command at the command prompt:

brolia –sxxxxxxxx –iyyy.yyy.yyy.yyy –mzzz.zzz.zzz.zzz -paaaaaaaa

where

xxxxxxxx = the serial number of the ID1021
yyy.yyy.yyy.yyy = the wanted temporary IP address for the ID1021
zzz.zzz.zzz.zzz = the wanted temporary netmask for the ID1021
aaaaaaaa = password for the ID1021

The password option is only required if the password protection option of the ID1021is enabled, see paragraph 3.1.3.

In the example below the ID1021 with serial number 20701063 is forced to IP address 193.0.0.1 and netmask 255.255.255.0.

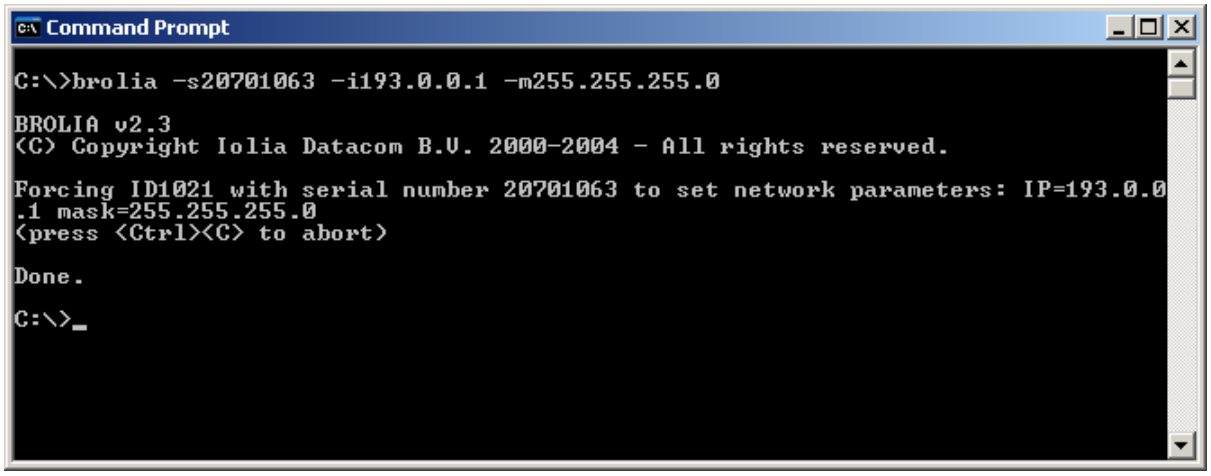


Figure 25: Using BROLIA to force temporary IP address and netmask for the ID1021

The Windows PING tool can be used to verify the result of the BROLIA operation…
(refer to paragraph 3.1.16.6 for more information about using the PING tool)

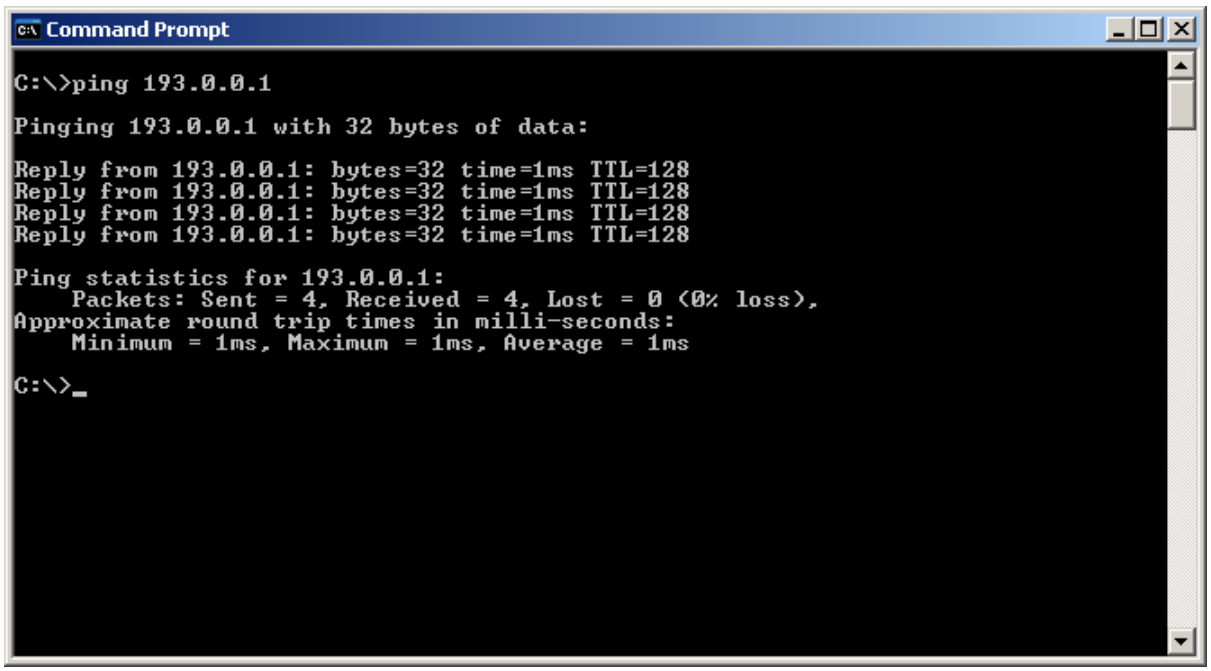


Figure 26: Verifying temporary IP address and netmask with PING tool

… but also the BROLIA tool itself:

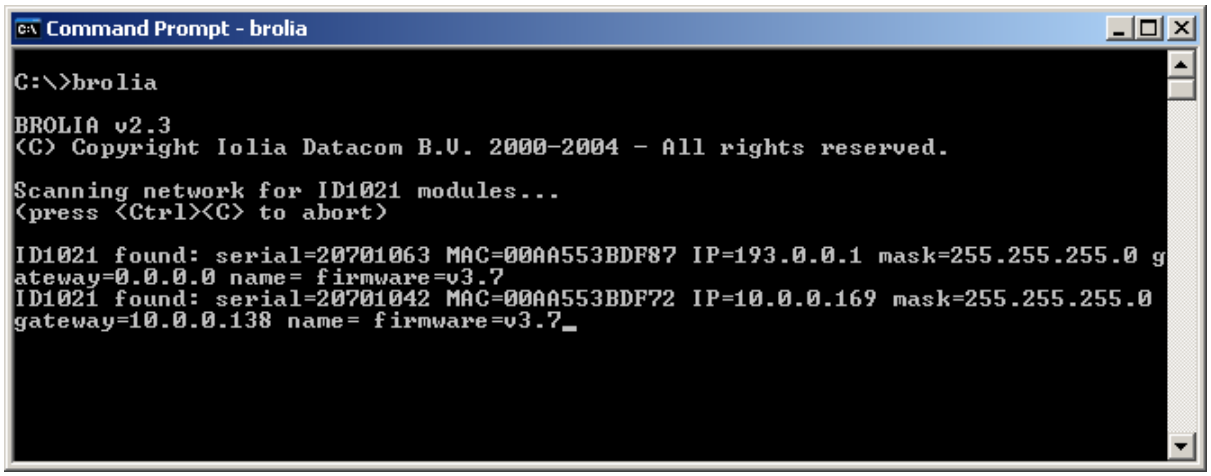


Figure 27: Verifying temporary IP address and netmask with BROLIA tool

Now the ID1021 should be reachable with telnet on port 1021 of its temporary IP address.

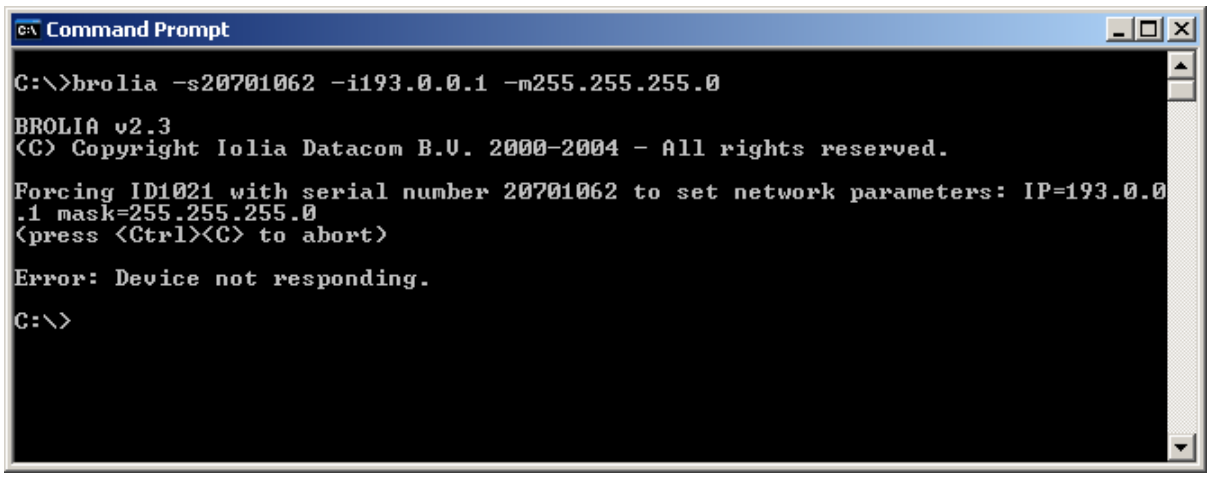


Figure 28: BROLIA failed to force temporary IP address and netmask on ID1021

In the example above BROLIA failed because the serial number of a non-existing ID1021 was specified. If the BROLIA tool did not succeed in forcing the temporary IP address on the ID1021 and instead you got some sort of error like in the picture above, then check the following:

- Is the ID1021 powered on?
- Is the orange LED of the ID1021 ethernet interface on ? The orange LED indicates the link status of the ethernet network. It is on if the ID1021 is attached to an ethernet network with a valid carrier. The LED is off when no network is attached or when the network carrier is not present. When attached to a network with valid carrier it will be temporarily off (for 10 ms) if a CSMA/CD collision is detected. If the ID1021 is attached to a network that has a valid carrier then it should be on almost permanently. If it is off then something might be wrong with the ethernet network (cabling).
- Is the green LED of the ID1021 ethernet interface showing any activity ? The green LED is used to indicate data traffic on the ethernet network. It is normally on and will be temporarily off (for 100 ms) when data is transmitted/received over the ethernet interface. Pinging the ID1021 should at least result in the green LED to blink a few times.
- Are the PC running BROLIA and the ID1021 attached to the same ethernet network segment? Are there any routers in between the PC and the ID1021? There should not be. The BROLIA tool uses ethernet broadcast messages for reaching the ID1021. These messages will not be passed on by a router and therefore this method will fail if the ID1021 and the PC running the BROLIA tool are separated by one or more routers.
- Is a password required for the ID1021 and did you not forget to specify the password option at the command-line?

Notes:

- Use the *-h* command-line option with BROLIA to get more information about the supported command-line options.
- The IP address and netmask settings forced with the BROLIA tool are volatile and will be lost with the next power off or reset of the ID1021.
- The *–g* command-line option with BROLIA can be used to force a the ID1021 to specific gateway address. This is only required if the current gateway address of the ID1021 is conflicting or if the temporary IP address for the ID1021 is to be different network than that of the PC running the BROLIA tool.

3.1.16.4 Adapting the PC network address to match that of the ID1021

Important: *If you are unfamiliar with IP addresses, network addresses, netmasks, etc please consult your network administrator and ask him for advice before you start changing the network address parameters of your PC as mentioned in this paragraph!*

On a PC running Windows XP the network address of the PC can be adapted as follows: Open '*Start* | *Network and Dial-up Connections'*, right-click with mouse on '*Local Area Connection'*. You should get something like this:

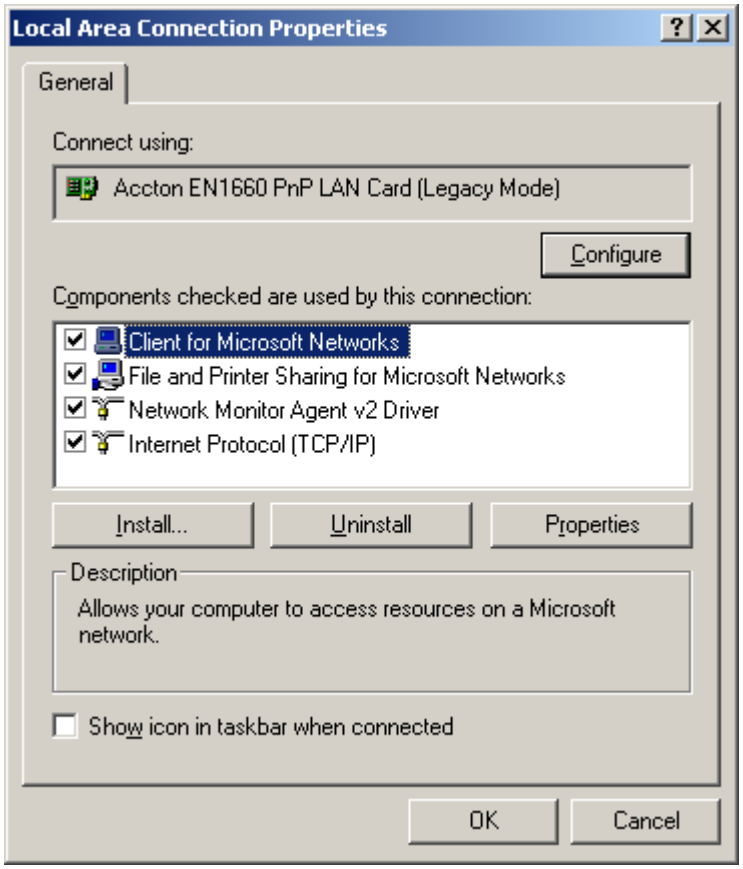


Figure 29: Opening Local Area Connection properties

Select the '*Internet protocol (TCP/IP)'* by clicking on it with the mouse.

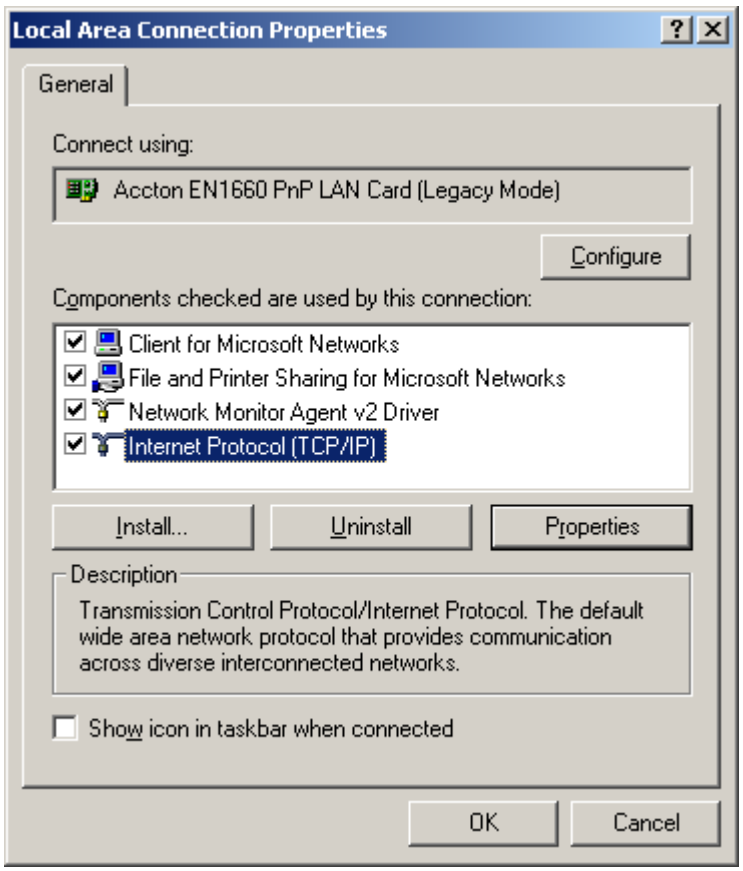


Figure 30: Selecting Internet Protocol (TCP/IP)

Now click on the *'Properties'* button to see its properties and enable editing of the IP address and netmask.

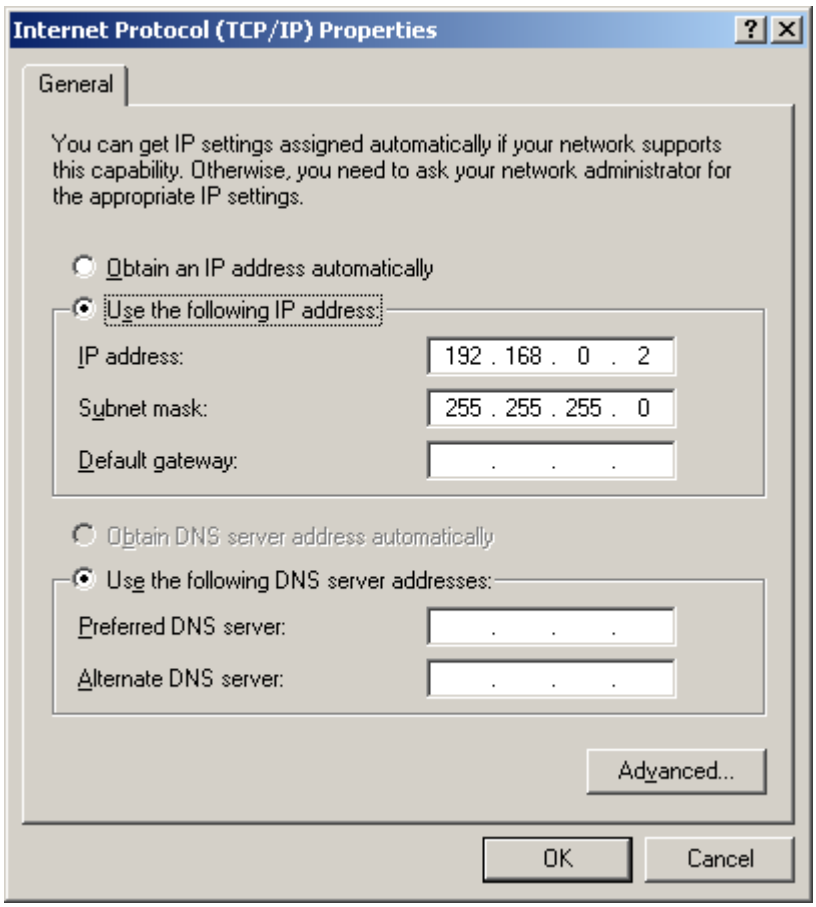


Figure 31: Editing IP address and netmask

Here is where you can adapt the PC's IP address and netmask. When you adapt these parameters make sure:

- The IP address is not exactly the same as the IP address of the ID1021. Only the network part of the IP address should match. You can not have two identical IP addresses on the same network.
- The netmask matches the new IP address type. Usually Windows adapts the netmask automatically when you enter a new IP address, but check it anyway.

In the example above the IP address of the PC is set to 192.168.0.2 and the netmask is set to 255.255.255.0. (= 'class C' network without sub-netting) The network part of the IP address is therefore 192.168.0.0 which that for the ID1021. (which had IP address 192.168.0.1, remember Figure 23)

After you have changed the IP address and netmask of your PC chances are you have to reboot your PC before the new settings will become active.

3.1.16.5 Adapting the routing table of the PC

Important: *If you are unfamiliar with IP addresses, network addresses, netmasks, etc please consult your network administrator and ask him for advice before you start changing the routing table of your PC as mentioned in this paragraph!*

A solution for accessing an ID1021 with network number that differs from that of your PC is to manually add an entry for the ID1021 network number to the IP routing table of the PC. This way, the TCP/IP stack on the PC could resolve the ID1021 network address on its own and communicate with the ID1021 directly. All this thanks to the fact that

most TCP/IP protocol stacks allows for multiple logical networks on the same physical network segment. On a Microsoft Windows PC the routing table of the Windows TCP/IP stack can be manipulated with the ROUTE utility.

Example:

Assuming IP address and netmask of PC are 128.5.0.1 and 255.255.0.0 (= class B network, without sub-netting) then the following command at the Microsoft Windows command prompt would add an entry for the logical network of the ID1021:

route add 192.168.0.0 mask 255.255.255.0 128.5.0.1

This uses the PC's ethernet adapter as a direct gateway to the 192.168.0.0 network, which is the network the ID1021 thinks it is on.
Before you start editing the routing table, make sure the network to add is not already in use. You can check this for example by using the '*print*' command with the ROUTE utility. Also, it is wise to remove the added entry from the routing table as soon as you don't need it any more. This can be done with the 'delete' command of the ROUTE utility.

3.1.16.6 Checking communications with the ID1021 using the PING tool

The PING tool is a standard network test tool that comes for free with many operating systems, including most Microsoft Windows operating systems. It can be used to test network communications with a specific network device. More over, it can be used to test if the target network device is reachable over the network and if it has its TCP/IP stack up and running.
In our case we will use it to test communications with the ID1021.
As with other network tools under MS-Windows we can use either the IP address or the NetBIOS name as a command-line parameter for addressing the ID1021. In the figure below a successful session with the PING tool is shown. As you can see the ID1021 nicely replies to the PING communications requests within a few milliseconds and no packets are lost.

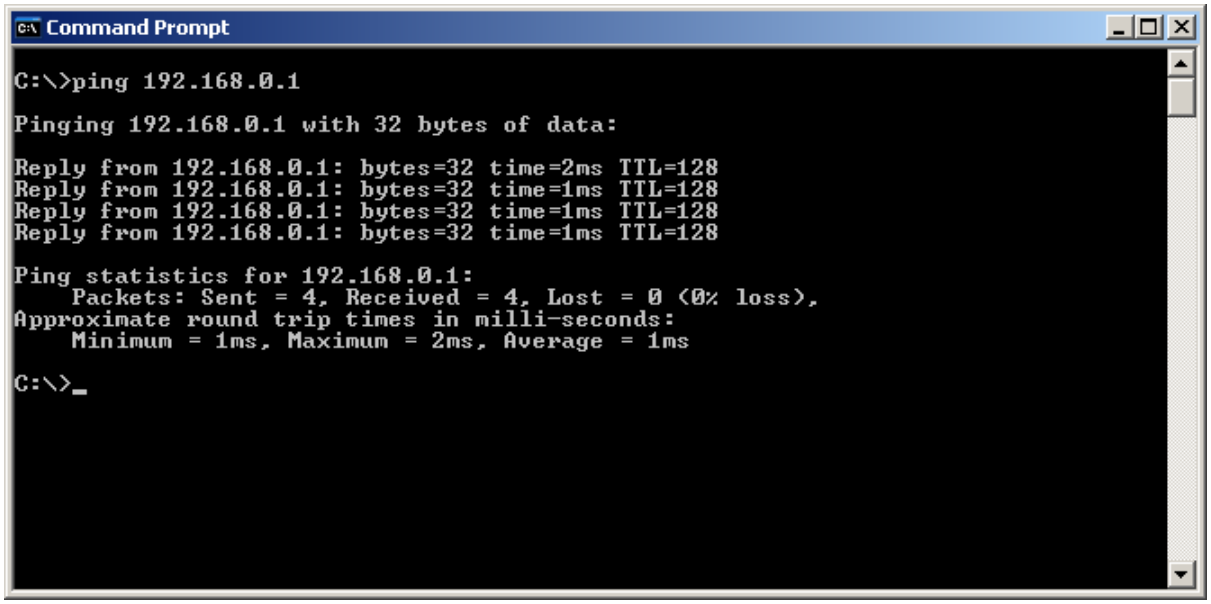


Figure 32: Successful PING session with ID1021

If the ID1021 were unreachable over the network (for whatever reason) you would get something like this:

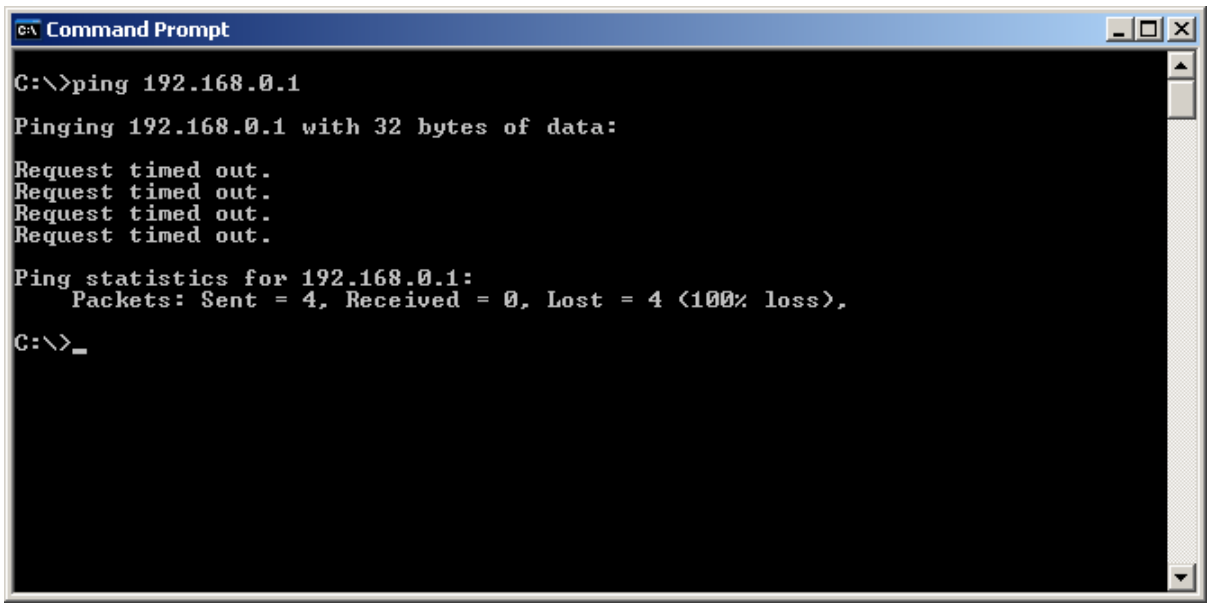


Figure 33: Not successful PING session with ID1021

So the PING tool can be used for verifying the network connection with the ID1021. We recommend the use of the PING tool as the low-level diagnostic tool for investigating network communication problems. If communications with the ID1021 fail at a higher level (FTP, HTTP, Telnet), always try the PING tool first to see if the ID1021 can be reached over the network at all.

Note: If stealth mode is enabled then the ID1021 will not respond to any PING requests, refer to paragraph 3.1.13.5 for details.

3.2 Password protection for HTTP server

Access to the web pages of the ID1021 can be protected against unauthorized use with a simple password protection mechanism. The password used by the HTTP server is the system password, see paragraph 3.1.3.

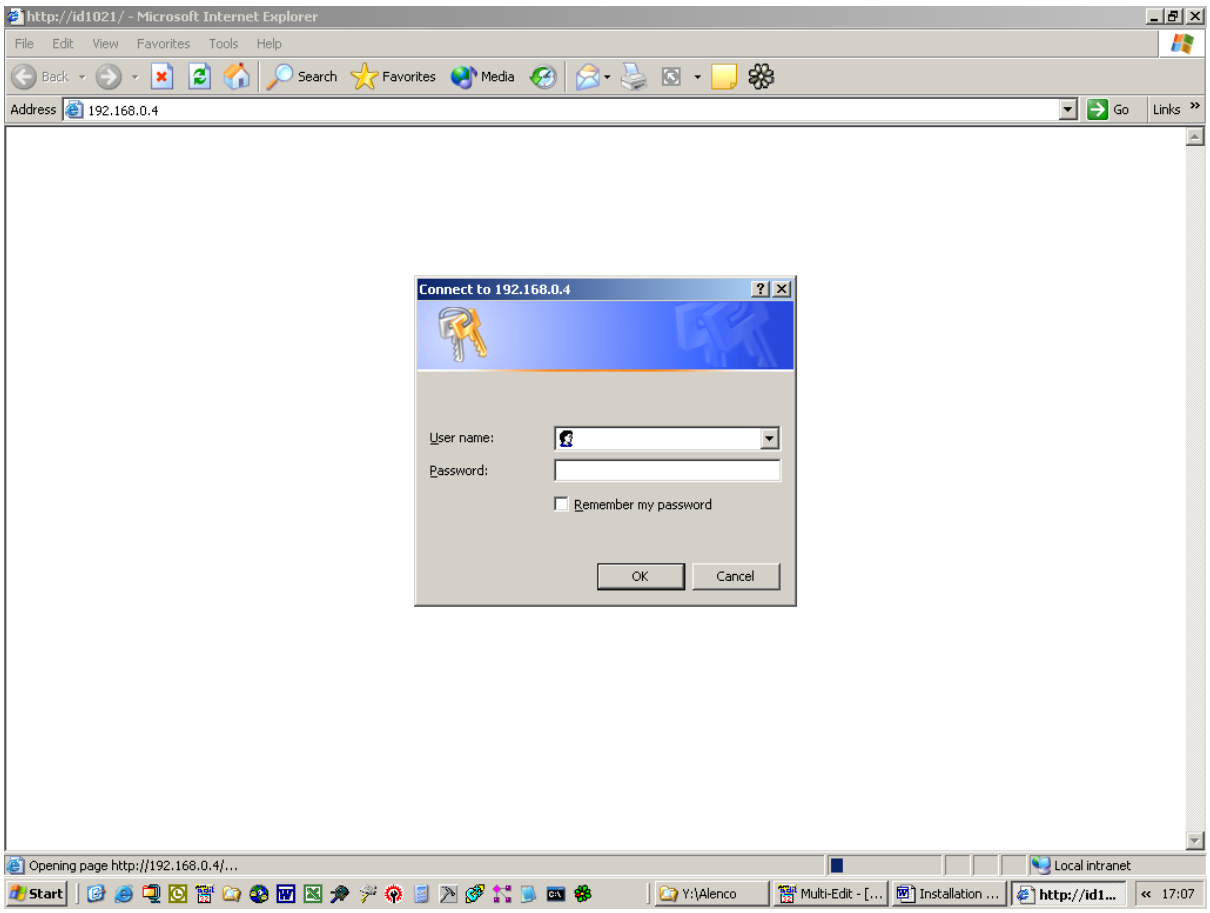


Figure 34: Password dialog window in web browser

If the password mechanism is disabled then the starting web page for the ID1021 will be displayed immediately. (no password dialog window)

Note that a user name is not required for the HTTP server of the ID1021, so you can enter any username you like.

4 Servicing the ID1021

4.1 Updating the files on the ID1021 internal disks

The basic ID1021 data communications functionality is implemented by a set of dedicated software applications and HTML pages, all stored as files on the internal flash disk of the ID1021. Updating the ID1021 applications and HTML pages therefore consists of replacing the existing files on the flash disk with updated ones. In this chapter we will show how the ID1021 internal files can be updated.

The flash disk of the ID1021 is accessible through the integrated FTP server of the ID1021, using the standard File Transfer Protocol (FTP) protocol. The Embedded File System driver of the ID1021 emulates a MS-DOS-alike disk drive with the name 'C:' for the internal flash disk.
The NVPs for the integrated FTP server are described in paragraph 3.1.11.

4.1.1 Setting up connection with ID1021 FTP server

In this manual we illustrate the updating of an ID1021 internal file using a PC running the Microsoft Windows XP operating system. For setting up a FTP connection with the ID1021 we will use the standard FTP program that comes for free with the Microsoft Windows XP operating system. (*FTP.EXE*)

HINT: A more user-friendly, GUI based, FTP program that can be downloaded from the internet is Filezilla. Filezilla is an open-source program, so it can be used for free. The website address is http:/www.filezilla-project.org. Note: For use with the ID1021 you must download the client version of this program, not the server version.

HINT: See also paragraph 6.2 for FAQs on the FTP subject.

For simplicity, we assume that all parameters in the FTP server menu are at their factory default values.

First we start up the FTP.EXE program from a Windows XP command prompt window using the IP address of the ID1021.

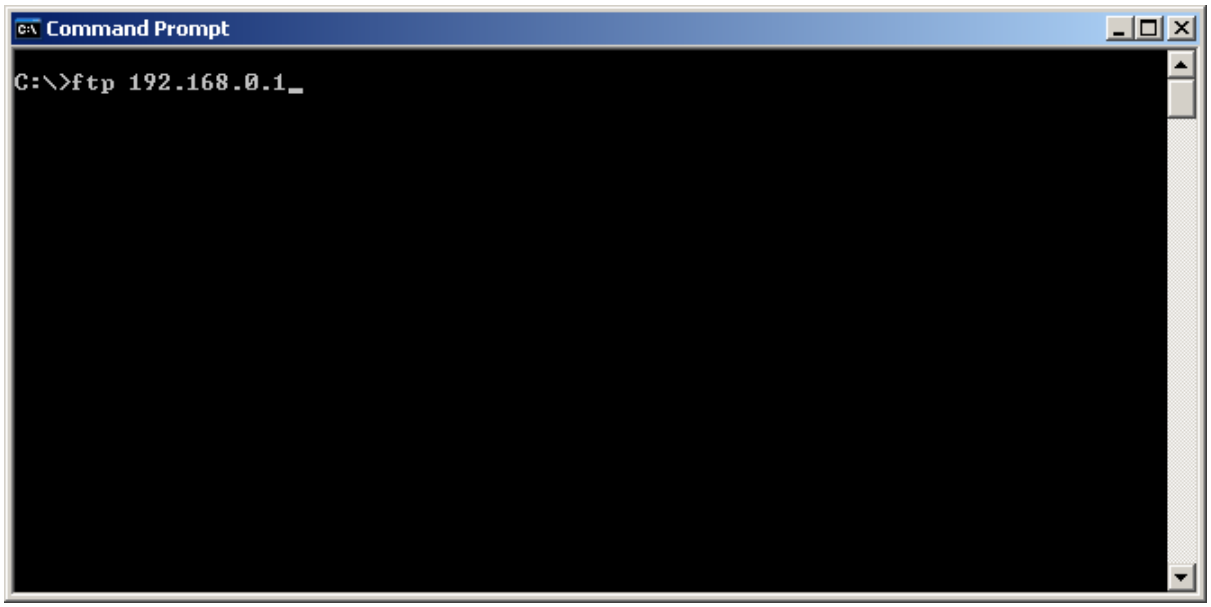


Figure 35: Starting FTP program with IP address

In this example the IP address of the ID1021 is 192.168.0.1. No need to specify TCP port for the FTP server (= port 21), as the FTP program will use port 21 by default.

If the NetBIOS name of the ID1021 is known then we could also start up the FTP program using the NetBIOS name as a command-line parameter.

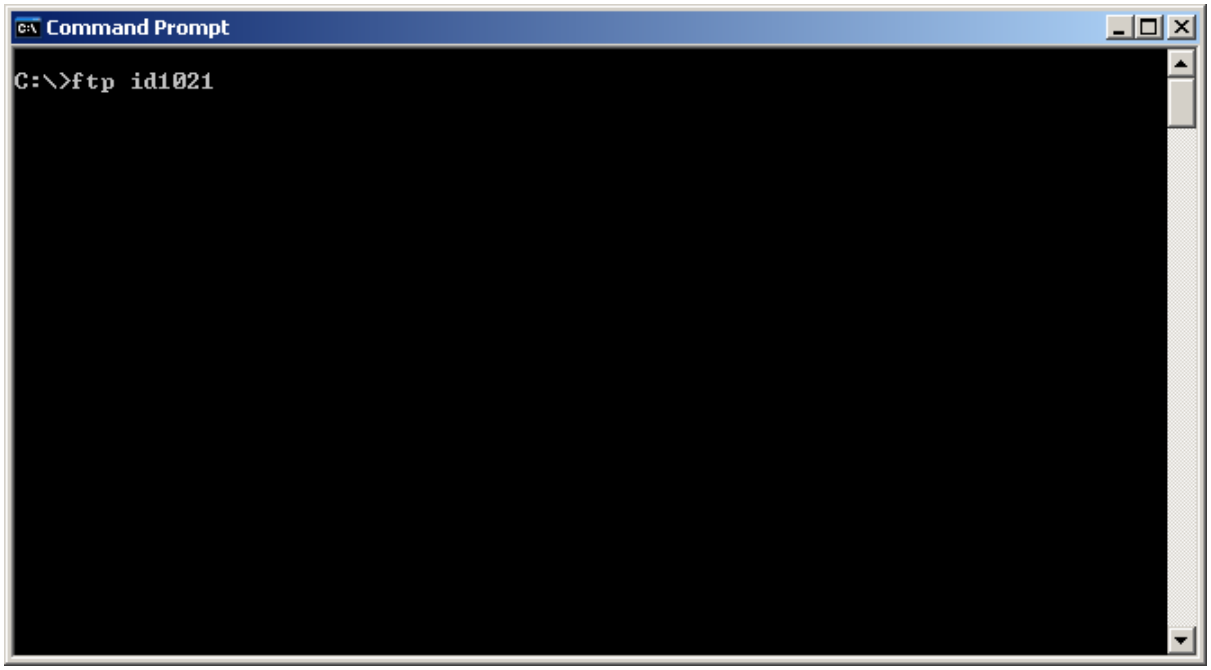


Figure 36: Starting FTP program with NetBIOS name

In the example above the NetBIOS name of the ID1021 is '*id1021*'. The TCP port again is the default port. (port 21, not specified here)

After the FTP program has established a connection with the ID1021, the ID1021 integrated FTP server will report its presence by mentioning its name and version number and prompt you for a user name, as in the figure below.

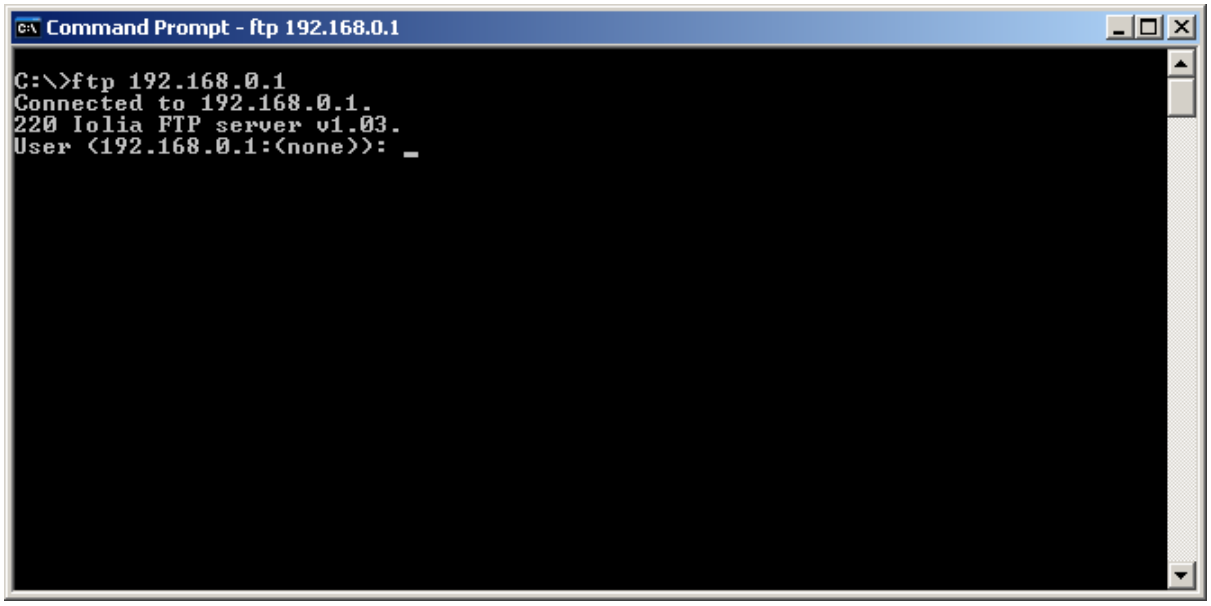


Figure 37: FTP server prompting for a user name

If you get this prompt, then you have successfully established a FTP connection with the ID1021 integrated FTP server. Just press <enter> to bypass the user name prompt. Note that the ID1021 FTP server does not require a user name in an FTP session. With some FTP programs an empty user name is not allowed. In this case any name can be entered. The ID1021 will ignore it.

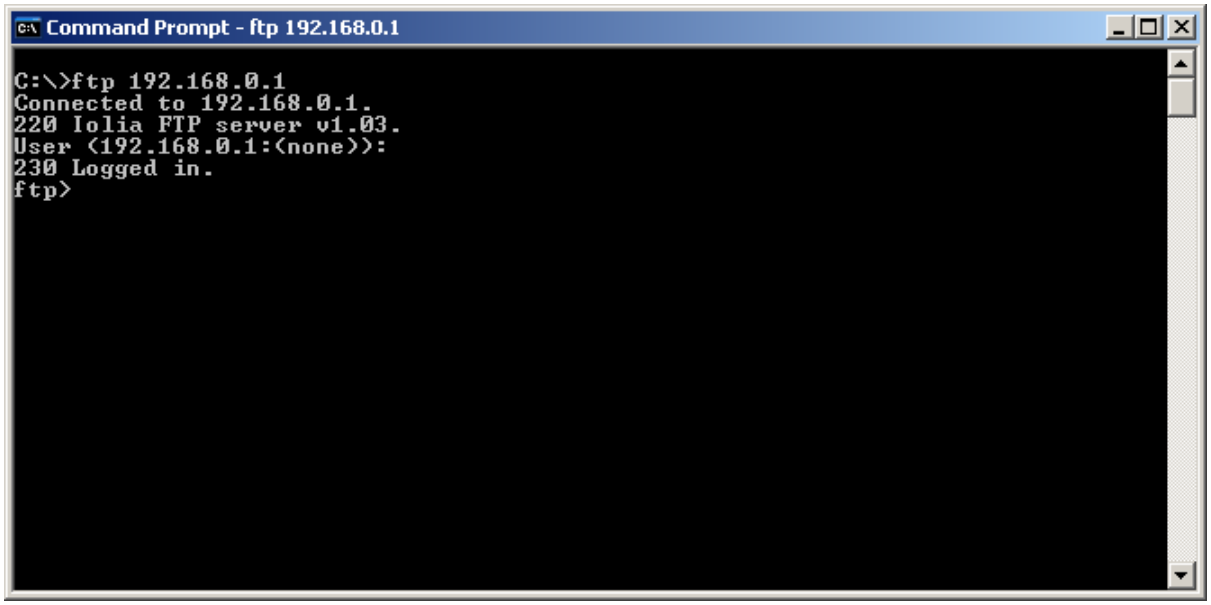


Figure 38: FTP server after successful log in

You should now be logged in to the FTP server and get the *ftp>* command prompt, as displayed in the figure above. If you do get this prompt, please continue reading in paragraph 4.1.2, which will explain the use of the FTP server for updating the ID1021 application in further detail.

If you do not get the above mentioned prompt, but instead some sort of time out error any other error indicating the connection with the ID1021 could not be established, then check the following:

- Is the PC or workstation correctly attached to the ethernet network ?
- Is network communications with other devices then the ID1021 working ok ?
- Are the parameters in the FTP server menu all at their default values ? (see paragraph 3.1.11)
- Can the ID1021 be reached over the ethernet network ? You can check this by using the 'ping' command with the IP address or NetBIOS name of the ID1021 as a parameter. Please consult the help for the ping command on your PC or workstation for more details about its usage.
- Is the orange LED of the ID1021 ethernet interface on ? The orange LED indicates the link status of the ethernet network. It is on if the ID1021 is attached to an ethernet network with a valid carrier. The LED is off when no network is attached or when the network carrier is not present. When attached to a network with valid carrier it will be temporarily off (for 10 ms) if a CSMA/CD collision is detected. If the ID1021 is attached to a network that has a valid carrier then it should be on almost permanently. If it is off then something might be wrong with the ethernet network (cabling).
- Is the green LED of the ID1021 ethernet interface showing any activity ? The green LED is used to indicate data traffic on the ethernet network. It is normally on and will be temporarily off (for 100 ms) when data is transmitted/received over the ethernet interface. Pinging the ID1021 should at least result in the green LED to blink a few times.

If you get an *'421 Service not available…'* error message like in the figure below, then other users are already accessing the ID1021 FTP server and the maximum number of users is exceeded. In this situation you can only get access to the ID1021 FTP server after one or more of the other users log out.

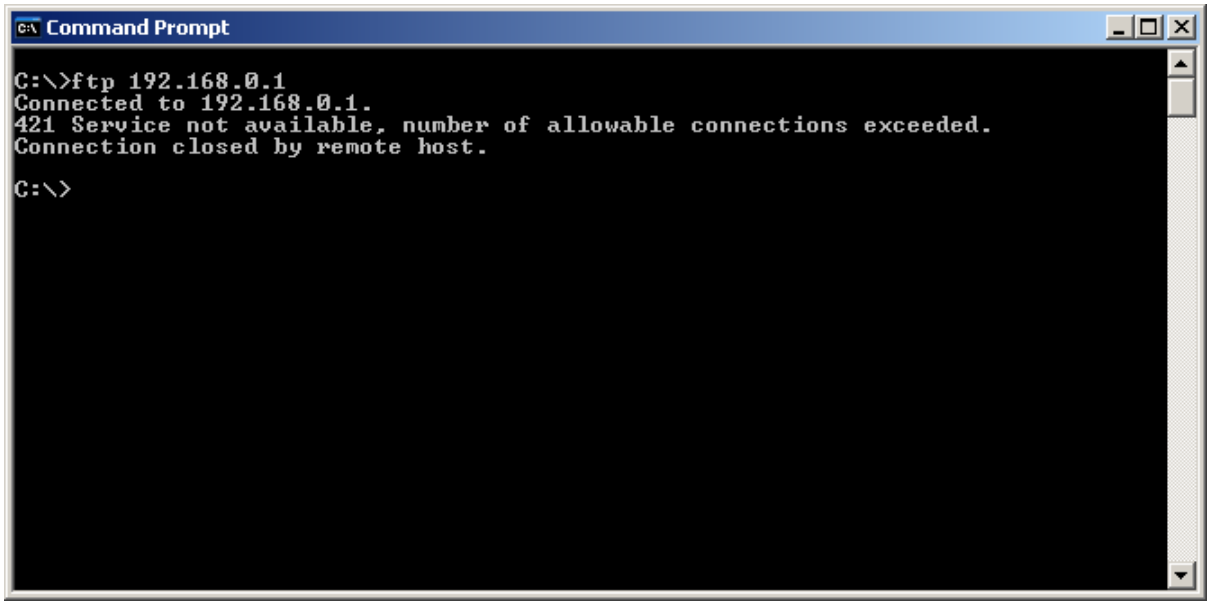


Figure 39: Maximum number of simultaneous FTP users exceeded

If the ID1021 displays the message *'33 1 need password'* prompt like in the figure below, then the password security option for the ID1021 is enabled and you must enter the correct password to gain access to the FTP server. Refer to paragraph 3.1.13.1 for more information about ID1021 access security issues. Note that the user name is not used by the ID1021. Any name may be entered as a user name as long as it is at least 1 character long.

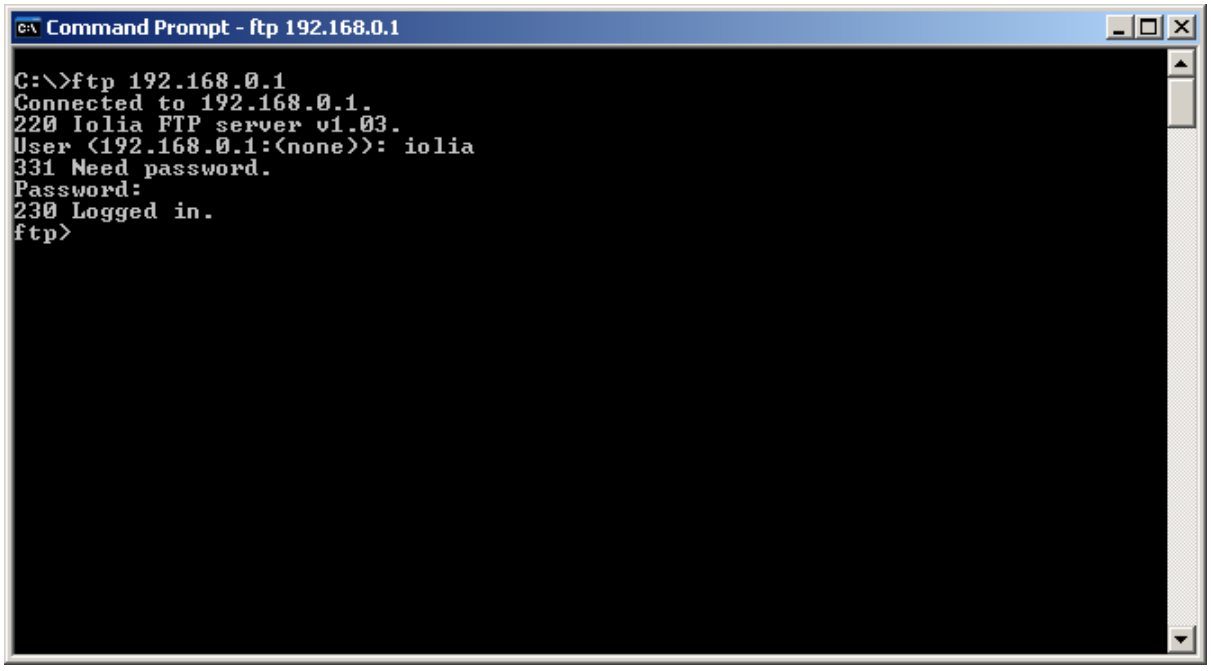


Figure 40: FTP password prompt

4.1.2 Using ID1021 FTP server

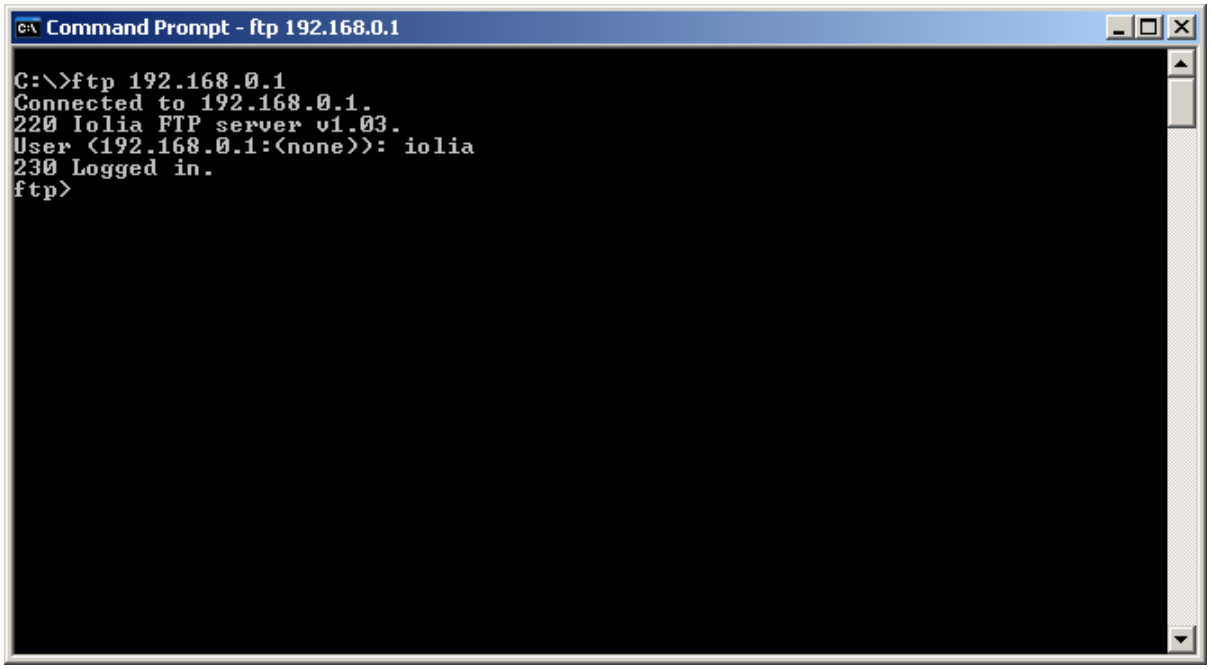


Figure 41: Connected to ID1021 FTP server

Starting point is an established connection with the ID1021 FTP server, see figure above. At this point you can type the '*help*' command to get a list of available commands that are available from the FTP.EXE application.

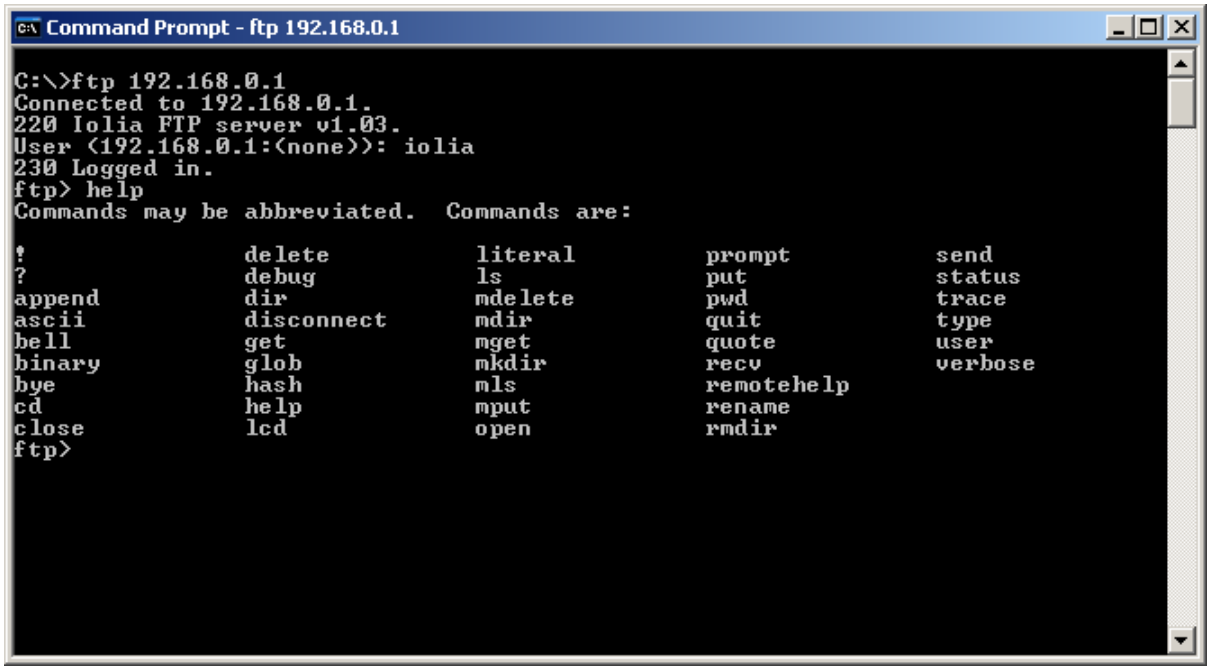


Figure 42: List of available FTP commands

First we use the '*cd*' command to switch to the internal flash disk (= drive C:) of the ID1021.

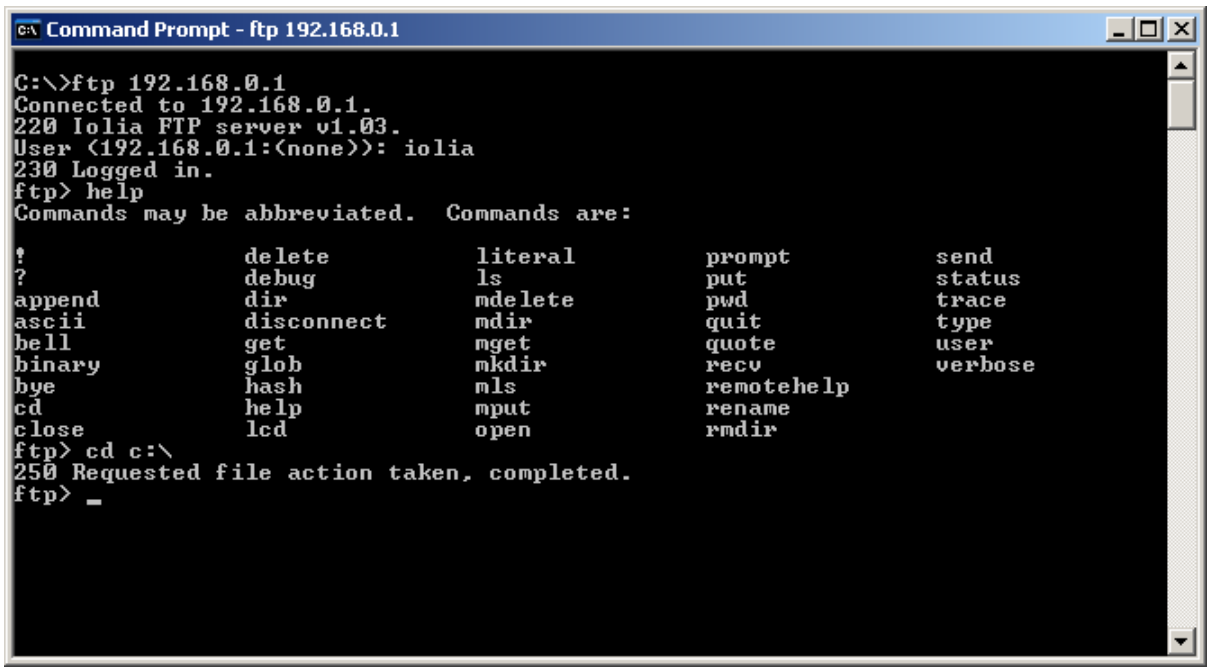


Figure 43: Switching to the internal flash disk of the ID1021

Next, we use the *'dir'* command to view the current contents of the flash disk.

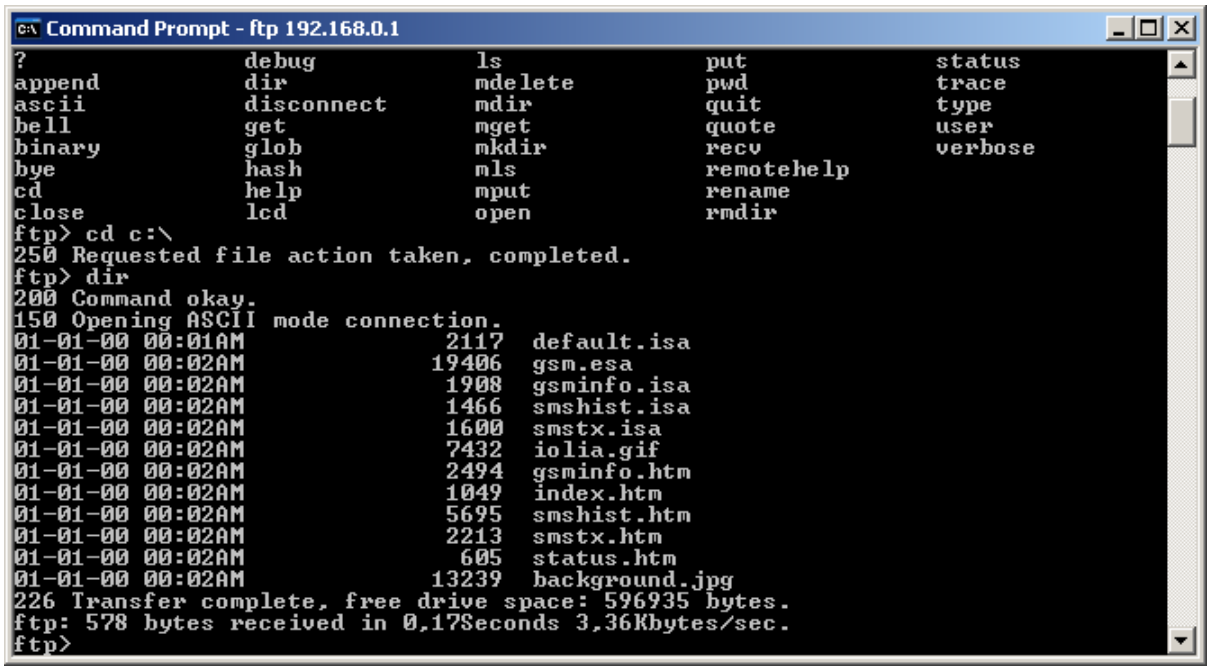


Figure 44: Viewing the contents of the flash disk of the ID1021

There should be a file with the name 'index.htm' on the flash disk. This is the default HTML file that is displayed when no specific page is specified in a HTTP request. Next, we change to the PC directory that contains the updated HTML file. (also with name index.htm)

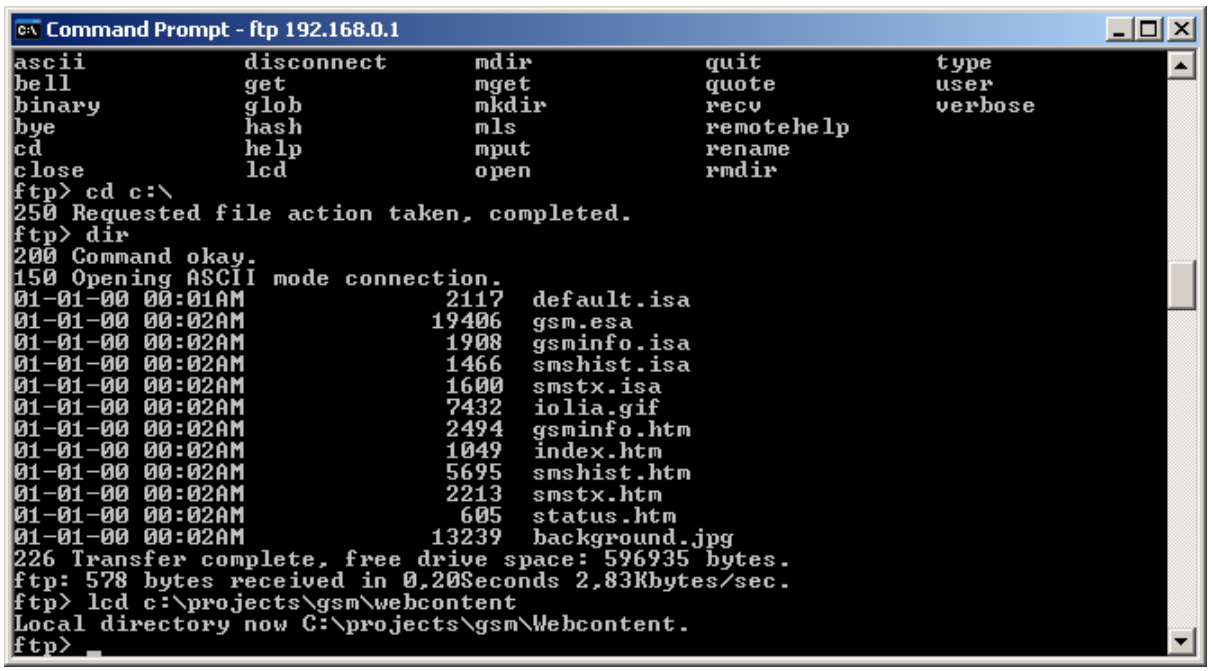


Figure 45: Switching to local directory that contains updated ID1021 application file

In our example this is the PC directory with the name *C:\projects\gsm\webcontent*. We can now use the *'put'* command to overwrite the index.htm on the flash disk with the file in the PC directory.

Important: Currently the ID1021 requires all names of application files to be in lower-case. The ID1021 will not execute any applications from files in with upper-case names. So if you transfer an application file to the ID1021 make sure its original name in the PC directory is in lower-case. The ID1021 will not execute any applications from files in with upper-case names.

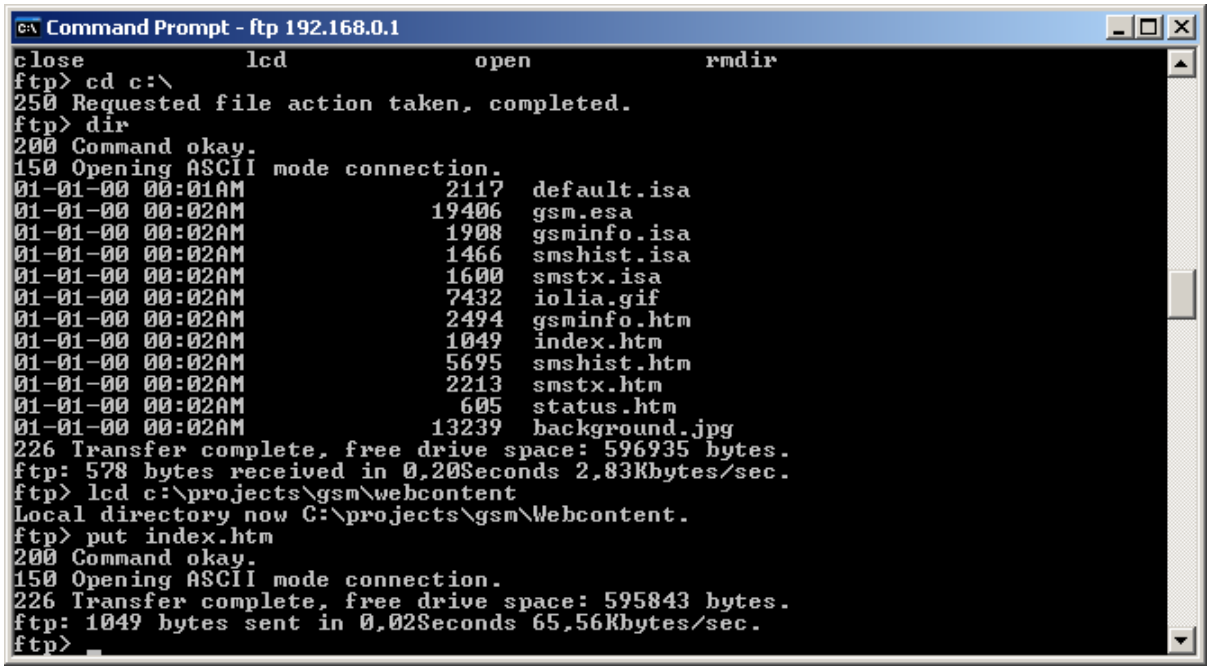


Figure 46: Transferring application file to flash disk

Finally, we use the *'quit'* command to log off from the ID1021 FTP server and close the FTP connection. It will also end the FTP.EXE program and return the Windows command prompt.

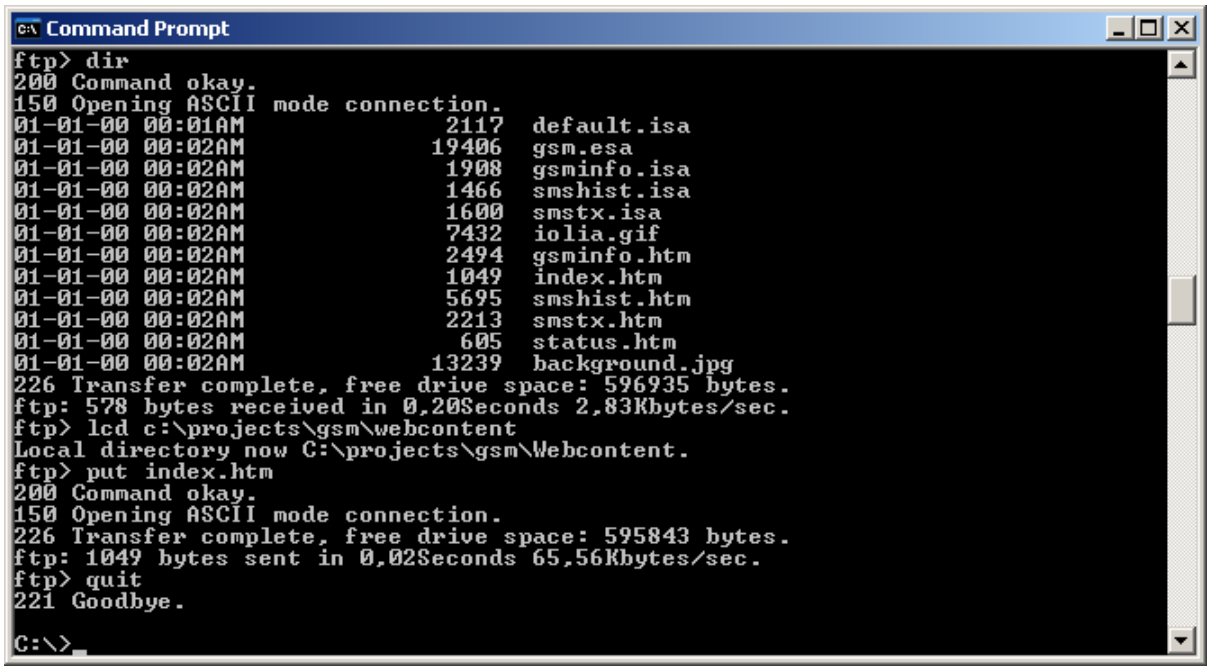


Figure 47: Closing the FTP connection

4.1.3 Additional notes

4.1.3.1 Formatting the flash disk

Due to the block-erase characteristics of the ID1021 internal flash disk and the fact that the Embedded File System driver of the ID1021 does not implement a background-erase mechanism with file backup, the following issues apply: As expected, the mount of free disk space on the flash disk will decrease with each file written to it. However, if a file is deleted from the flash disk, then the disk space that was used by the file is not recovered and added to the pool of free disk space. So, eventually, after many file writes and deletes, flash disk free space will be 0 bytes. At this point the flash disk must be re-formatted to regain the full, original, disk space. It is up to the user to backup the files that must not be lost by transferring them to the Windows PC, and re-write them to flash disk of the ID1021 after formatting. Formatting of the flash disk can be done from within a FTP session using the *'quote'* or *'site'* command:

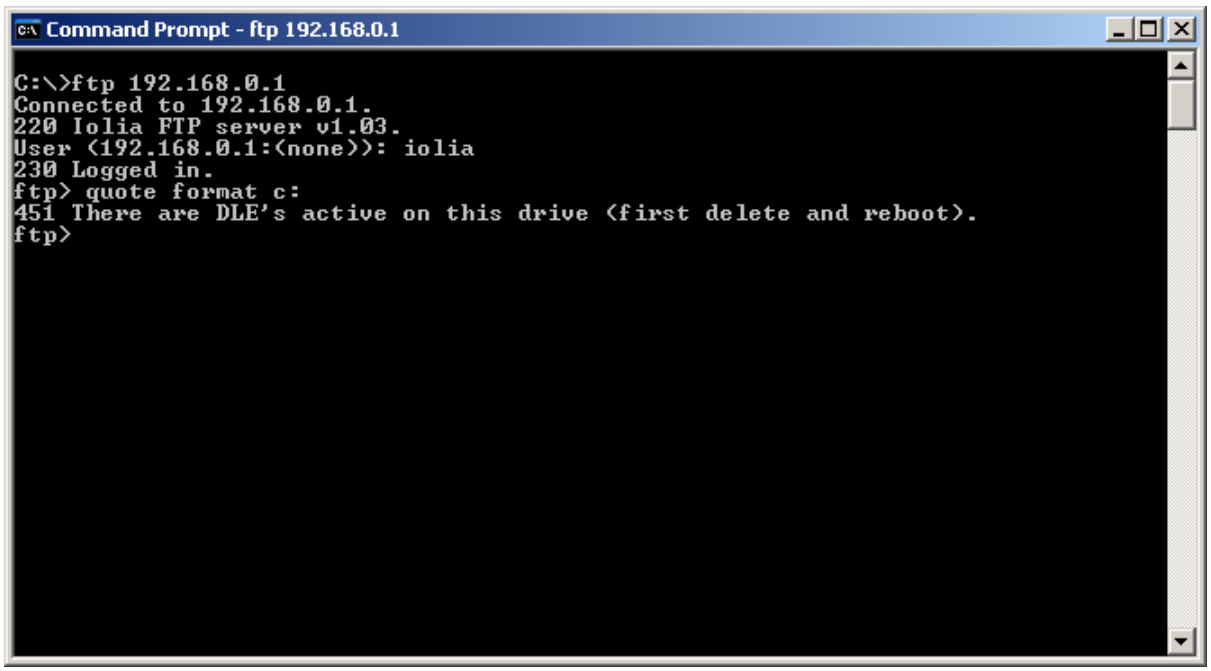


Figure 48: First attempt to format the flash disk

The ID1021 executes ESA applications directly from their location on the flash disk (memory mapped I/O, flash disk is completely within addressable memory space of ID1021 processor). We have to delete the active ESA applications and reboot the ID1021 first, because you execute a program and erase that program's executable image at the same time. That would cause the ID1021 to crash…

Paragraph 4.1.4 contains an overview of other 'quote' commands that are available for the ID1021.

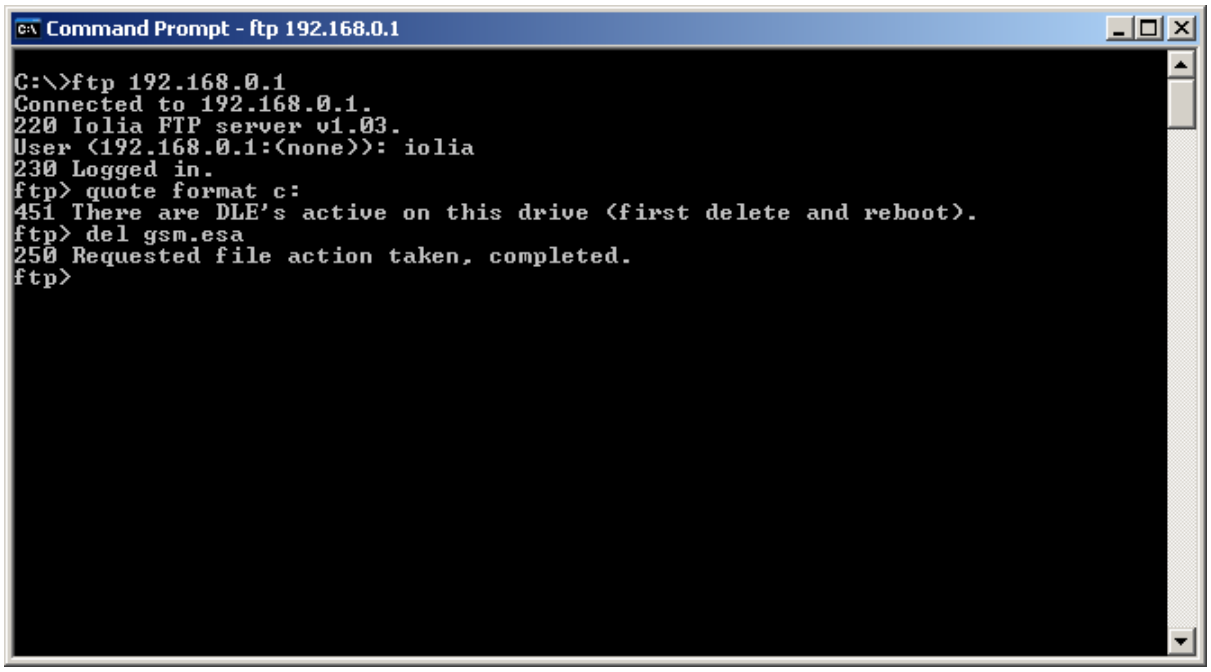


Figure 49: Deleting any ESA application on the flash disk

In this example the only active application is the GSM.ESA application. After removing it we must reboot the ID1021 …

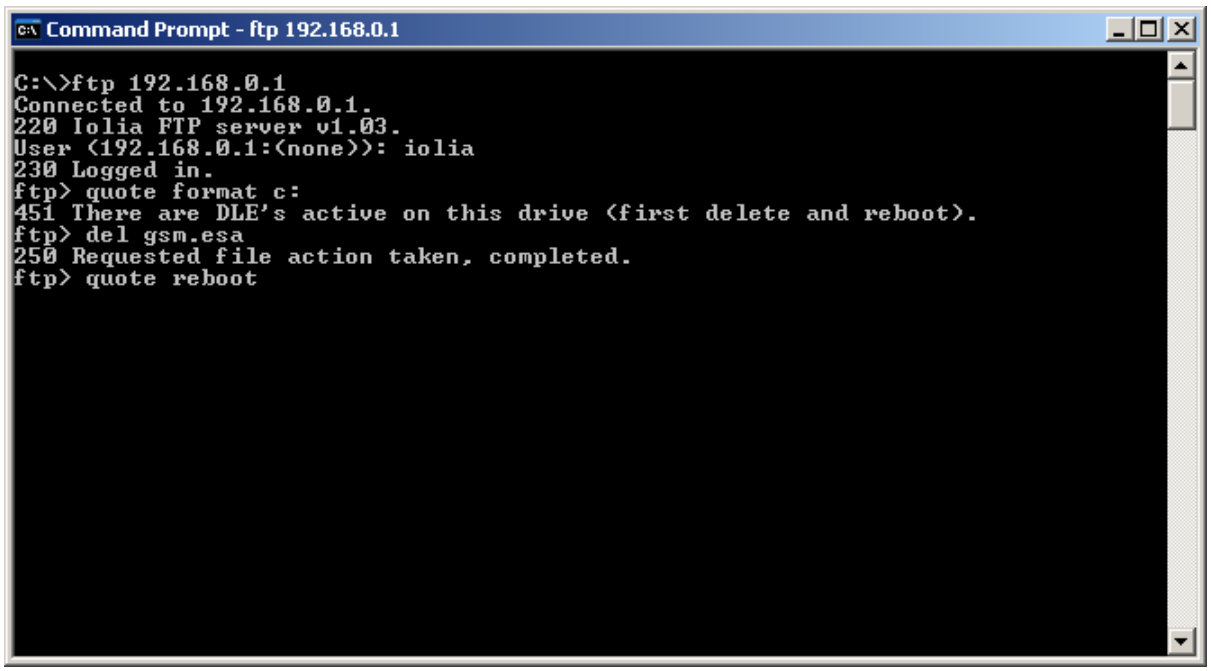


Figure 50: Rebooting the ID1021

…rebooting will cause the FTP connection to be lost…

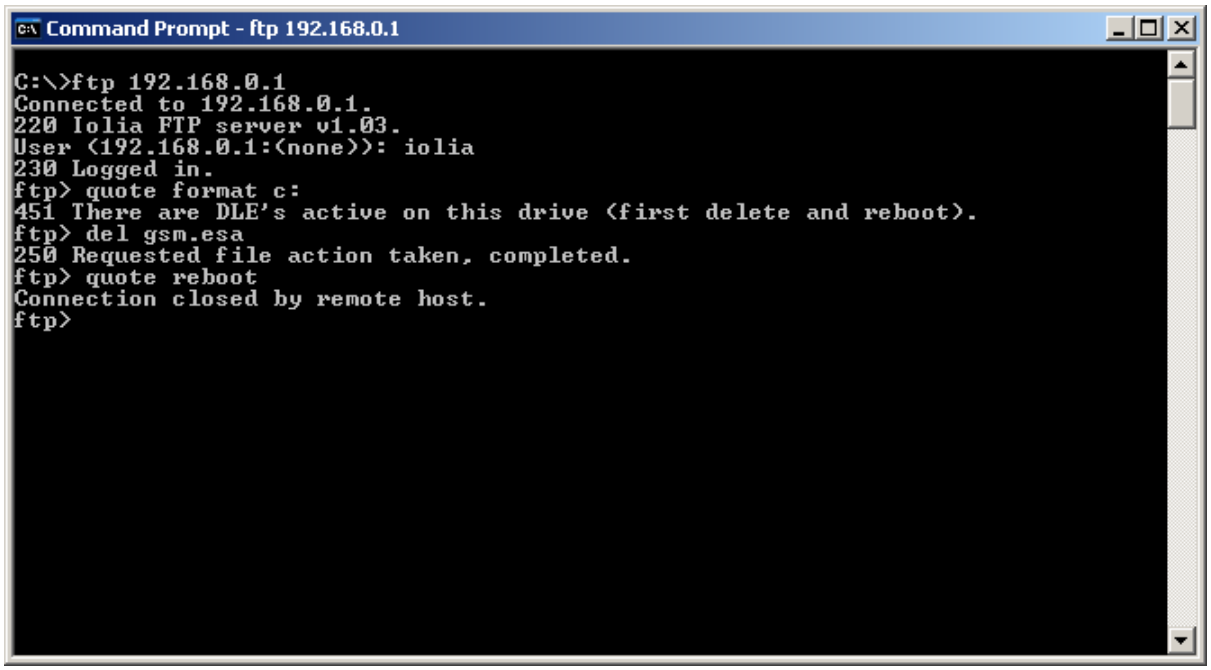


Figure 51: Lost FTP connection with ID1021 after rebooting

… so we must reconnect before we can retry the format operation…

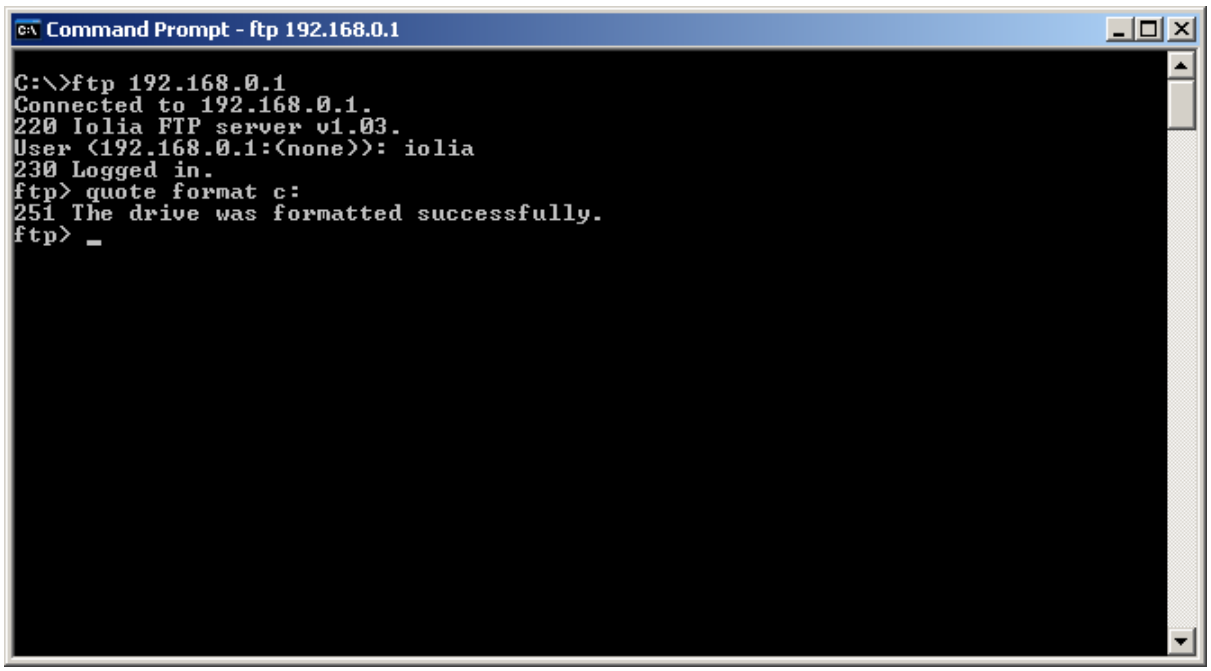


Figure 52: Second attempt to format the flash disk

Now the formatting of the flash disk succeeds. Note that the formatting of the flash disk is a lengthy operation and may take up to one minute.

4.1.3.2 FTP inactivity time out

For security reasons the ID1021 FTP server implements an inactivity time out. If no FTP activity is detected by the FTP server for a period of 60 seconds then the FTP server will automatically close the active FTP session. Unfortunately, with the FTP.EXE program the user at the Windows PC will only notice this when the user issues his next command. (inactivity time out error is reported, see figure below)

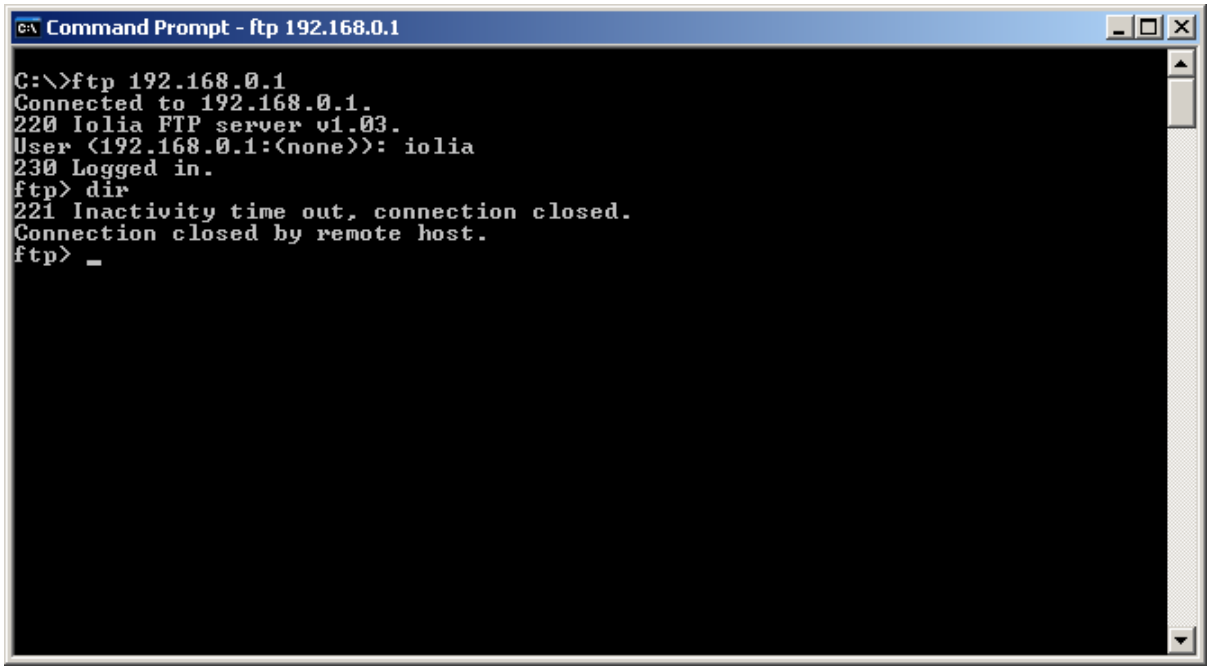


Figure 53: ID1021 FTP server has ended session after 60 seconds of inactivity

4.1.4 Implementation specific FTP sub-commands

The FTP protocol allows the *'quote'* or *'site'* commands to be used to implement application specific sub-commands. The ID1021 firmware uses this feature to implement some ID1021-specific operations, see table below. Note that the sub-commands are identical for both the *'quote'* and *'site'* command. We have noticed that not all FTP clients support both commands. However, chances are that at least one of these two commands is supported by your favorite FTP client.

Sub-command	Example	Description
Format	quote format c:	Formats a specific drive.
Reboot	quote reboot	Reboots the ID1021.
Chkdrv	quote chkdrv c:	Checks the file system on a specific drive of the ID1021.
Chkdle	quote chkdle	Checks integrity of all ISA and ESA applications on drive C: of the ID1021.
Drive	quote drive b:	Switches to a specific ID1021 drive.

Table 5: Implementation specific FTP sub-commands

5 Command Line Interface (CLI)

The CLI is the Command Line Interface for the ID1021. It enables users to issue commands to the system in a telnet session. The CLI returns the results of the executed commands in the form of text messages. ('responses')
By default the CLI service can be found at TCP port 1022. You can use the HyperTerminal program to access the CLI.

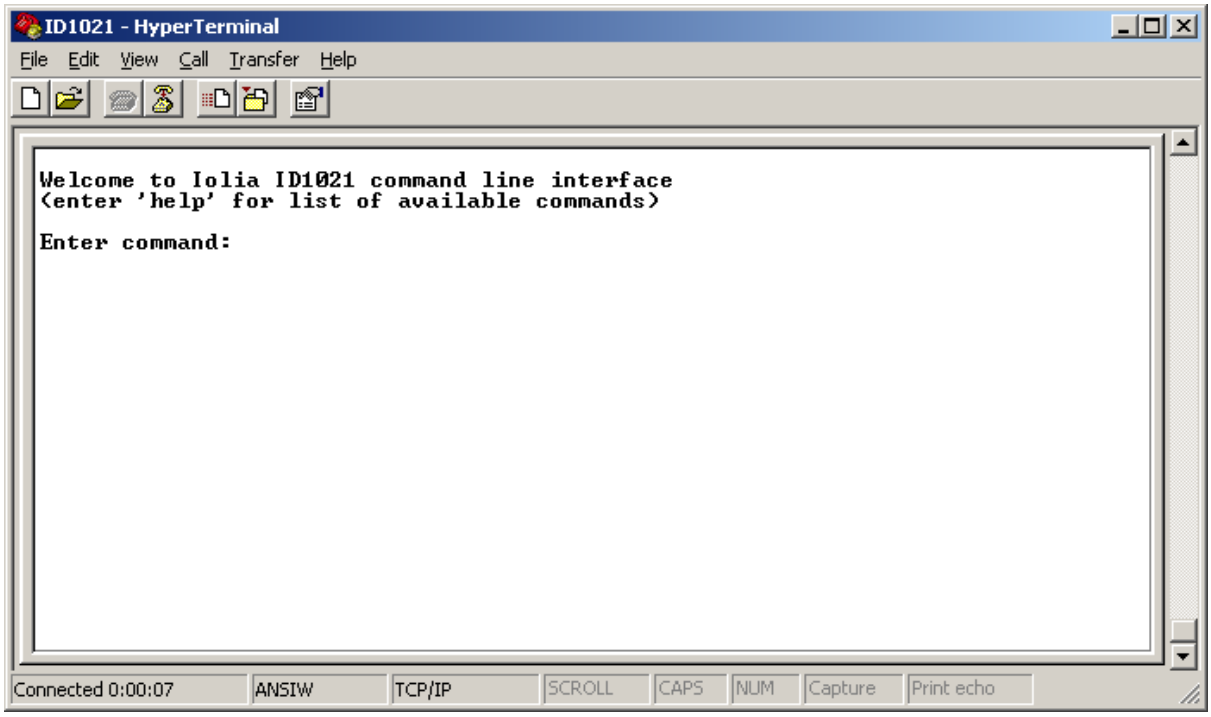


Figure 54: Command Line Interface using HyperTerminal

The CLI implements the following commands:

Command	Parameters	Description
clock		The *'clock'* command without parameter returns the current time & data according to the real-time clock (RTC) of the ID1021.
	<date> <time>	The *'clock'* command with a date & time parameter forces the real-time clock to be update for the specified date & time. The format for the date & time parameters is: <date> = dd-mm-yy <time> = hh:mm:ss
dns		The *'dns'* command without parameter reports information about the contents of the DNS cache.
	clear	Clears the DNS cache.
	rsolve <domain>	Resolves an domain name into IP address and adds a line to DNS cache.
heap		This command returns a text string with information about the current status of the heap. (RAM memory pool)
help		The *'help'* command returns a list of all internal and external CLI commands.
	<command>	Returns help for the specified command.
mem	*<addr>*	Displays the contents of a block of memory starting at the specified address. The *<addr>* parameter must be specified in hexadecimal.
	read <addr> <len>	Reads *<len>* bytes from memory, starting at address *<addr>*
	write <addr> <bytes>	Writes bytes to memory, starting at address *<addr>*. The *<bytes>* parameter is a range of one or more 2-digit hexadecimal bytes, separated from each other by a comma.
	ram <appl>	Displays the RAM memory area for the specified ESA application. The <appl> parameter is the name of the ESA application.
	rom <appl>	Displays the ROM memory area for the specified ESA application.

		The <appl> parameter is the name of the ESA application.
netstat		The *'netstat'* command returns information about the TCP and UDP connections that are currently active in the ID1021. It also reports the current status of the ethernet interface.
nvp	*get <nvp>*	Reports the current value of the NVP with number <nvp>. For an overview of all NVPs, see Appendix A.
	set <nvp> <value>	Sets new value <value> for a NVP with number <nvp>. For an overview of all NVPs, see Appendix A.
	save	Save all current NVP settings to the systems NVP file.
quit		This command quits the CLI and closes the telnet session.
reset		This command forces a reset of the ID1021. (soft reset, same as '*reset soft'* command)
	ethernet	Forces reset of ethernet interface only.
	soft	This command forces a soft reset of the ID1021. (software reset)
	hard	This command forces a hard reset of the ID1021. (watchdog reset)
security		Reports security status en statistics
	blacklist	Reports black list contents.
	events	Reports security events.
	reset	Reset security alarms, counters, event list and black list.
selftest		Forces system selftest and reports the findings of firmware and all participating applications.
serial		Reports the serial number of the ID1021.
uptime		Reports the system uptime, i.e. the number of days, hours, minutes and seconds that elapsed since last system power on or reset.
version		This command lists the version numbers of the firmware, all ESA and all ISA applications.

Table 6: Commands implemented by the CLI

Note that the command must be the first word that is typed on the command line. Commands may be issued in both uppercase of lowercase, the command interpreter is case-insensitive. Commands and parameters for a command must be separated by a single space character.

5.1 Commands added by applications

Apart from the internal commands the CLI supports an API that enables ESA applications to add run-time add commands to the list of supported commands.

You can use the *'help'* command to see what external commands are available and which applications implemented them.

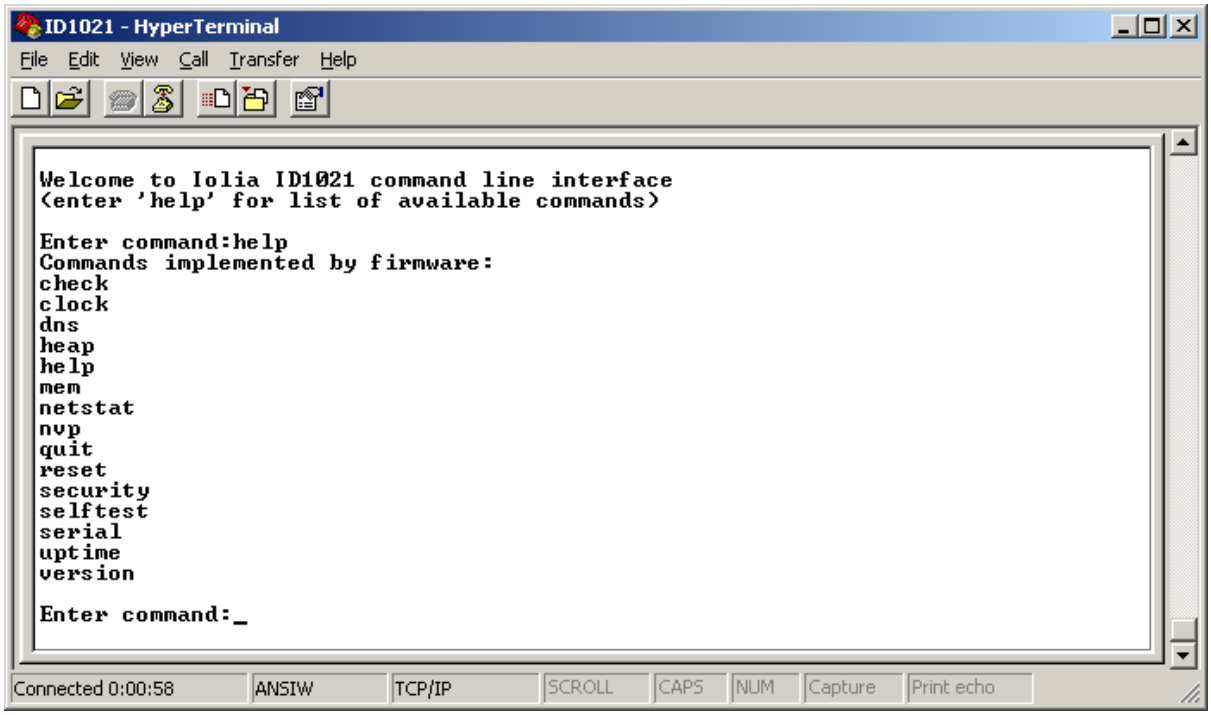


Figure 55: Displaying available commands

5.2 Communication channels added by applications

By default the CLI uses a telnet session on port 1022 to communicate with the user. The CLI supports an API that enables ESA applications to add communication alternatives (additional command channels) for the CLI. This enables the user to use a different option for issuing the same CLI commands.

For example the Necoso GSM.ESA application extends the CLI with a command channel via SMS. So commands can be issues using SMS messages and response texts are received in the form of SMS messages too.
Another example is the Necoso SMTP.ESA application – this application extends the CLI with a command channel via e-mail. So commands can be sent by e-mail and responses are received back in form of e-mail messages too.
Note that these applications are not part of the ID1021 firmware and must be installed on the flash disk of the ID1021 before they can be used. Contact Necoso for more information.

5.3 Password protection for CLI

Access to the CLI can be protected with a password. It is the same password as the password used for protecting the configuration menu of the ID1021.
The password can be defined and enabled/disabled in the system submenu, see paragraph 3.1.3.

6 FAQs

This chapter contains some frequently asked questions (FAQs) about the ID1021.

6.1 Telnet related FAQs

Question: How do I quit the Microsoft telnet (telnet.exe) application?
Answer:. With the Microsoft Telnet application you can quit the telnet session by pressing the key combination <Cntrl> + <]> followed by <q><enter>.

Question: When I use the standard Microsoft telnet application that comes with Windows 2000/Windows XP I get all typed characters displayed on my screen in double. What is wrong ?
Answer:. The ID1021 echoes all typed characters. The telnet application echoes type characters as well. Normally, this can be disabled by pressing <Cntrl> + <]> for telnet command mode followed by entering the '*unset localecho*' command. Unfortunately, due to a bug in the Microsoft telnet application, this does not work. If you are really annoyed by this double echoing of characters try use the HyperTerminal application instead of the standard Windows telnet application. With HyperTerminal disabling local echo does work correctly.

Question: Why do telnet links in a webpage no longer work with IE7?
Answer: This is because Microsoft has removed support for telnet from IE7. You can force it to support telnet again by adding the following key to the Windows registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet\explorer\Main\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]
"iexplore.exe"=dword:00000000

Question: How do I startup telnet client from within the webbrowser for a specific port?
Answer: Example - use the following URL for setting up a telnet session with port 1021 for ID1021 on IP address 192.168.0.1:

telnet://192.168.0.1:1022

Question: The telnet configuration service does not seam to work with the telnet client that comes with Red Hat Linux. The menu is displayed, but I cannot select a sub-menu.
Answer: The Linux telnet application is by default operated in line mode. This must be changed to character mode for the ID1021. Use the *–e* command-line option to define an escape character, for example the ']' character. Use this character to force the telnet command prompt while in a telnet session. Enter '*mode character'* at the command prompt to switch the telnet application to character mode.

Question: Aren't there more user-friendly telnet clients available than the standard Windows provided telnet clients? (telnet.exe, hyperterminal.exe)
Answer: Yes, there are. Check out these free telnet clients:

1. Tera Term: http://sourceforge.jp/projects/ttssh2/
2. PuTTY: http://www.putty.org/

Question: I am using Windows Vista. It seems the telnet.exe application is no longer available?
Answer: The Windows Vista operating system is distributed with its telnet application not installed by default. Microsoft's Telnet: Frequently Asked Questions page describes how to install telnet in your Windows Vista system.

Question: Firefox does not open telnet links – instead I get a prompt to "*launch an external application*" How can I fix this?
Answer: Do the following steps:

1. In the Firefox address bar, type *about:config* [no spaces]
   You will see a list of configuration settings.
2. In the "Filter:" box at the top of this list, type: *telnet*
   You should see:
   network.protocol-handler.warn-external.telnet user set boolean true
3. Double-click on the word "*true*" and it should change to "*false*".

You should now be able to follow links to telnet systems without interruption.

6.2 FTP related FAQs

Question: Aren't there more user-friendly FTP clients available than the standard Windows provided FTP client (ftp.exe)?
Answer: Yes, there are. Check out these free FTP clients:

- FileZilla: http://www.filezilla-project.org/
- AlFTP: http://www.altools.com
- gFTP: http://www.gftp.org (for Linux)

Question: How do I startup FTP client from within the webbrowser for a specific username + password?
Answer: Example - use the following URL for setting up a FTP client with for user 'john' wit password 'secret' on IP address 192.168.0.1:

ftp://john:secret@192.168.0.1

Question: I am using the standard gFTP client that comes with Red Had Linux. It does not support the FTP *'quote'* command. How do I format the flash disk of the ID1021?
Answer:. Use the FTP *'site'* command instead.

Question: I am using the standard gFTP client that comes with Red Had Linux. It does not display any files on the flash disk of the ID1021, but I am sure there are files on it. What is wrong?
Answer: Disable the *'Show all files option'* under File | Options menu of gFTP. If this option is enabled, then the gFTP will use the (non-standard) *–a* option with the FTP LIST. This option is not supported by the ID1021 FTP server and causes the problem.

Question: Is there a FTP add-on for the Firefox webbrowser?
Answer: Yes, it is called FireFTP. Check out this webpage:

https://addons.mozilla.org/en-US/firefox/addon/684

Question: How can I access the various ID1021 drives with FireFTP ?
Answer: For drive C: access specify *'/c:\'* for remote initial directory. For drive B: access specify *'/b:\'* as initial remote directory. (without single-quote characters)

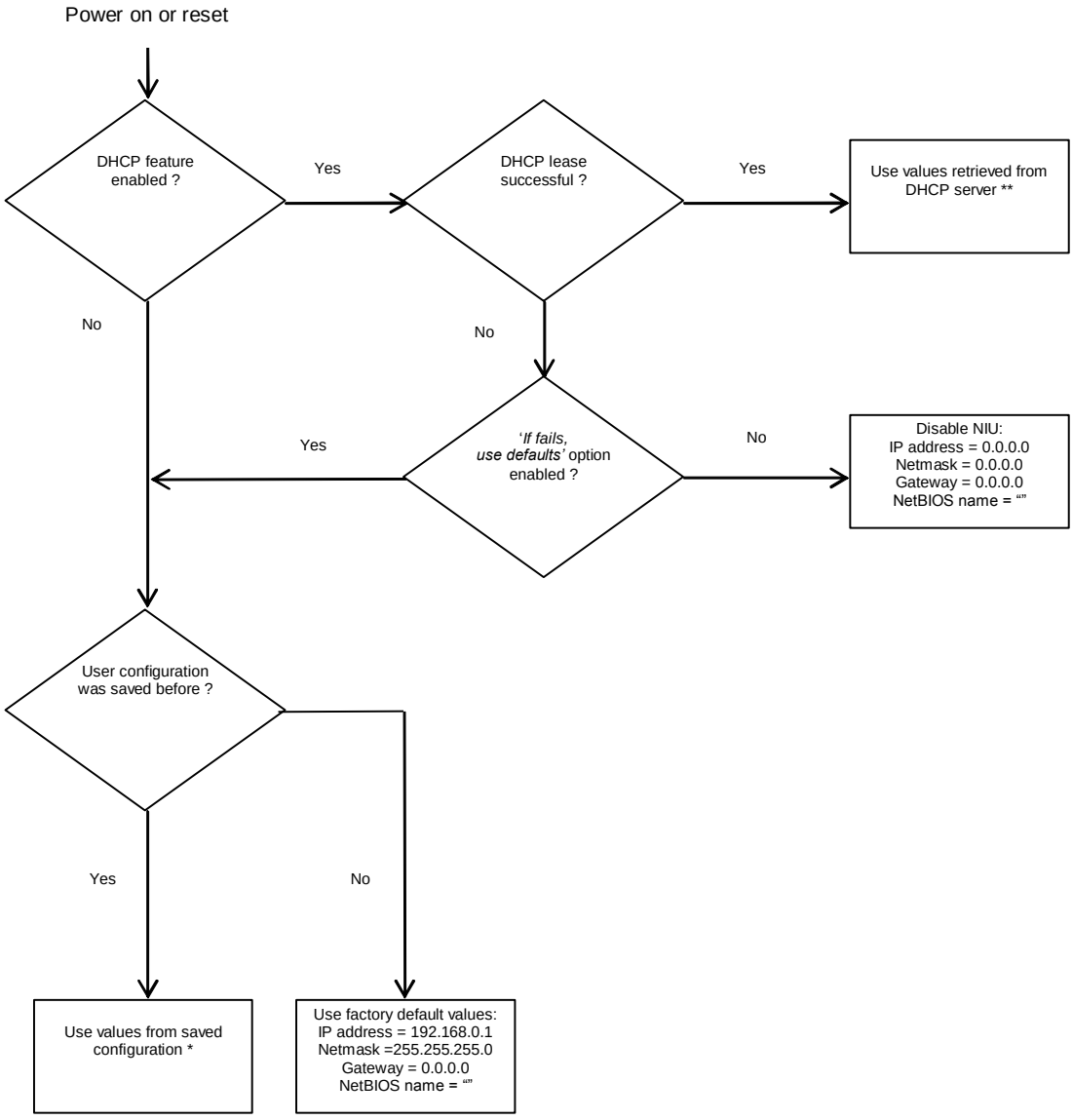
Appendix A - Non Volatile Parameters

FIRMWARE						
NVP number	**Section**	**Name**	**Type**	**Range / possible values**	**Default value**	**Description**
8	System	Password protection	Boolean	0 = disabled 1 = enabled	0	Protection feature for configuration menu.
-	System	Password	String	Between 2 and 8 ASCII characters	<empty string>	Password for protection feature for configuration menu.
9	System	Inactivity time out	Unsigned number	0 - 65535	60	Inactivity time out for configuration menu in seconds.
88	System	Configuration via service port	Boolean	0 = disabled 1 = enabled	0	Configuration menu via serial port.
89	System	Service port	Unsigned number	0 = SCI0, 1 = SCI1	1	Serial port for configuration menu.
16	System	Watchdog	Boolean	0 = disabled 1 = enabled	0	Hardware watchdog that resets system on software hangup.
128	System	Security Monitor	Boolean	0 = disabled 1 = enabled	1	The security monitor watches over all communication interfaces, generates security events and alarms for security suspicious situations.
129	System	Stealth mode	Boolean	0 = disabled 1 = enabled	0	In stealth mode the G2S Bridge does no longer react to specific communication packets to make it self invisible.
6	Ethernet	MAC address	Unsigned number	000000000000h - FFFFFFFFFFFFh	*	MAC address for ethernet interface. Default value is generated from serial number of G2S Bridge.
7	Ethernet	Support for IEEE 802.3 frames	Boolean	0 = disabled 1 = enabled	0	Data link layer support. Will support ethernet 2.0 if 802.3 is disabled.
1	Router	Router IP address	IP address	0.0.0.0 – 255.255.255.255	192.168.0.1	IP address for ethernet interface
2	Router	Router netmask	IP address	0.0.0.0 – 255.255.255.255	255.255.255.0	Netmask for ethernet interface.
3	Router	Router gateway	IP address	0.0.0.0 – 255.255.255.255	0.0.0.0	IP address for gateway server connected to ethernet interface
5	Router	IP forwarding	Boolean	0 = disabled 1 = enabled	0	Forwarding of IP packets to other interface.
112	CLI	CLI port	Unsigned number	0000h – FFFFh	1022	Telnet port for command-line interpreter (CLI)
113	CLI	CLI inactivity time out	Unsigned number	0 - 65535	5	Inactivity time out for CLI session in minutes.
80	DHCP	DHCP client	Boolean	0 = disabled 1 = enabled	0	Support for DHCP protocol for retrieving IP address for ethernet interface.
82	DHCP	Request default IP first	Boolean	0 = disabled 1 = enabled	1	Request router IP address from DHCP server first.
81	DHCP	Router NVP	Boolean	0 = disabled	1	Use router IP address NVP if DHCP failes.

		usage on DHCP failure		1 = enabled		
96	DNS	Primary DNS server	IP address	0.0.0.0 – 255.255.255.255	62.133.126.28	IP address of primary DNS server.
97	DNS	Secondary DNS server	IP address	0.0.0.0 – 255.255.255.255	62.133.126.29	IP address of secondary DNS server.
20	NetBIOS	Host name	String	Up to 12 ASCII characters	<empty string>	Hostname for NetBIOS protocol.
34	HTTP	HTTP Port number	Unsigned number	0000h – FFFFh	80	Port number of HTTP server.
35	HTTP	HTTP Max users	Unsigned number	0 – 255	60	Maximum number of simultaneous HTTP connections.
66	FTP	FTP Port number	Unsigned number	0000h – FFFFh	21	Port number of FTP server.
51	FTP	FTP Max users	Unsigned number	0 – 255	2	Maximum number of simultaneous FTP connections.
68	FTP	File system emulation	Unsigned number	0 = MS-DOS 1 = UNIX (*'/bin/ls'* format)	0	File system emulation for FTP directory listing.
69	FTP	Passive mode support	Boolean	0 = disabled 1 = enabled	1	Support passive mode connections for FTP protocol.
32849	RTC	Time	Time string [hh:mm-ss]	00:00:00 – 23:59:59	00:00:00	Time
32850	RTC	Date	Date string [dd-mm-yy]	01-01-00 – 01-01-36	01-01-00	Date
85	RTC	IP address time server	IP address	0.0.0.0 – 255.255.255.255	0.0.0.0	IP address of remote time server (RFC 868)
86	RTC	Update interval	Unsigned number	0 – 4294967295	0	Interval for updating RTC from time server in seconds. Value 0 means never update.
87	RTC	GMT offset	Unsigned number	-23 ..+23	0	Time zone offset for RTC.
90	Self test	Self test interval	Unsigned number	0 – 4294967295	300	Time interval between two self tests in seconds. If set to 0 then self testing is disabled.
91	Self test	Heap free limit	Unsigned number	0 – 4294967295	13107	Minimum amount of free heap space in bytes. System reset is forced if below this limit.
92	Self test	Heap fragment limit	Unsigned number	0 – 4294967295	117965	Maximum amount of fragmented heap space in bytes. System reset is forced if below this limit.

* Default value varies per ID1021 and is derived from serial number of ID1021.

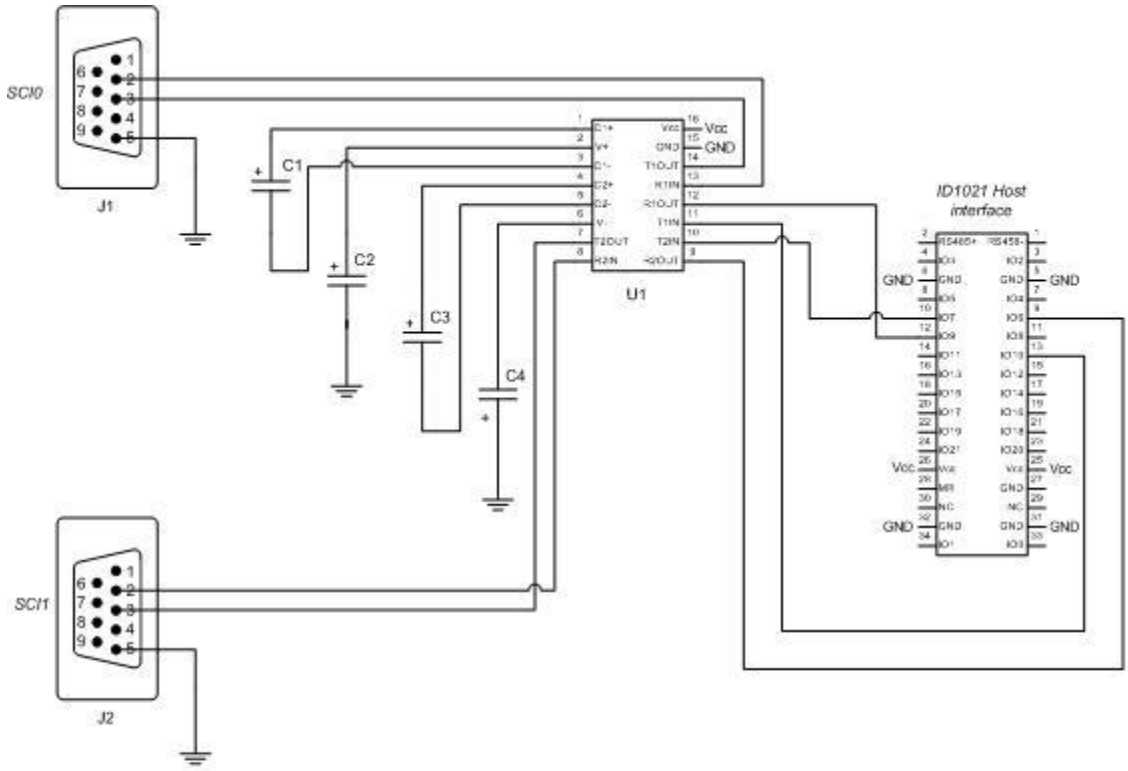
Appendix B - IP router parameter set up after power on or reset



*** As saved with 'S' command from configuration menu, see paragraph 3.1.2.3.**

**** IP address, netmask and address of default gateway are obligatory, NetBIOS name is optional.**

Appendix C - Reference circuitry for service port level conversion



Part list

C1 .. C4 = 10 uF, 25 V
U1 = MAX232 or equivalent IC
J1 ..J2 = Male SUB-D9 connector

Assumptions

Vcc = +5V (+- 5%)
GND = Signal ground
ID1021 host interface - see ID1021 datasheet for details.

Notes

The above schematics allow for either the SCI0 or the SCI1 port to be used as the service port. Both ports are in DTE configuration, so a RS232 cross-over cable must be used when connecting J1 or J2 directly to the COM port of a PC.

Reference circuitry for service port signal level converion
Version 1.0

Appendix D - Reference cable for connecting service port to PC COM port

The table below specifies a cable that can be used to connect the service port of the ID1021 to a COM port of a PC. At the ID1021 side the RS232 level conversion circuitry as specified in Appendix C is assumed.

Cable end for COM port of PC (assuming male sub-D9 connector)		**Cable end for ID1021 side. (assuming male sub-D9 connector)**	
D9 pin number	*Signal Name*	*D9 pin number*	*Signal Name*
2	Receive Data	3	Transmit Data
3	Transmit Data	2	Receive Data
5	Signal Ground	5	Signal Ground

Table 7: Cable for connecting ID1021 service port to PC COM port

As one can see in the table above the cable requires only three wires and is a so called 'cross-over' modem cable. Note that both the ID1021 service port and the PC COM port have a DTE configuration.

Appendix E - UDP and TCP ports user by firmware

The table below lists the UDP ports that are in use by the ID1021 firmware.

UDP	Service	Max sessions	Inactivity time out	Description
137	NetBIOS	n.a.	n.a.	NetBIOS protocol
1021	Brolia	n.a.	n.a.	File transfer protocol. (FTP server)

The table below lists the UDP ports that are in use by the ID1021 firmware.

TCP port	Service	Max sessions	Inactivity time out	Description
21	FTP	2	60 sec	File transfer protocol. (FTP server)
80	HTTP	60	-	Embedded webserver. (HTTP server)
1021	Telnet	1	60 sec	Configuration menu.
1022	Telnet	1	5 minutes	Command-Line Interface (CLI)

Note that applications may also use UPD and/or TCP ports. Please refer to the documentation that comes with the applications.

Appendix F - Major DNS servers in the Netherlands

Provider	Primary DNS	Secondary DNS
12Move	195.241.77.53	195.241.77.54
@Home	212.120.66.204	213.51.129.97
Casema	195.96.96.33	195.96.96.97
Chello	212.83.68.130	212.142.28.66
Dataweb	193.78.237.1	62.166.128.10
Demon	194.159.73.135	194.159.73.136
Dutch Web	82.199.128.11	82.199.128.12
Enertel	195.7.145.2	195.7.146.10
Euronet	194.134.5.5	194.134.0.97
Essent Kabelcom	195.85.130.68	195.85.130.69
Eweka	217.71.121.131	217.71.121.132
Fibre World	213.227.141.10	213.227.130.5
Global-E	212.241.50.200	212.241.50.211
Hacom Datacommunicatie	212.241.34.9	212.241.61.9
HCCNet	62.251.0.6	62.251.0.7
InterBox	217.119.0.250	217.119.4.250
Internet Online	81.17.33.2	
KPN / Direct internet	194.151.228.18	194.151.228.34
KPN / Planet internet	195.121.1.34	195.121.1.66
KPN / GPRS	62.133.126.28	62.133.126.29
Leaseweb	62.212.64.121	62.212.64.122
Multikabel	213.73.255.52	213.73.255.53
Nedstars	80.84.229.237	80.84.229.238
Publishnet	212.241.49.9	193.67.60.10
Qweb	213.196.37.149	213.196.37.13
Solcon	212.45.32.3	212.45.33.3
Surfnet	192.87.106.101	192.87.36.2
Technische Universiteit Eindhoven	131.155.2.3	131.155.2.7
Tiscali	195.241.48.33	195.241.49.33
Trueserver	213.239.128.3	213.239.176.4
Universiteit Leiden	132.229.8.6	132.229.22.2
Universiteit Twente	130.89.1.2	130.89.220.2
UPC	212.142.28.66	212.142.28.67
UUnet	193.67.79.39	193.79.237.39
UwNet / ISD Holland	213.227.141.10	213.227.130.5
Versatel	62.58.62.131	62.58.62.132

PUBLIC DNS SERVERS WORLD WIDE

OpenDNS (www.opendns.com)

- 208.67.222.222
- 208.67.220.220

ScrubIt (www.scrubit.com)

- 67.138.54.100
- 207.225.209.66

OpenNIC (www.opennicproject.org / http://www.opennic.org.uk)

Country	Location	IP Address	Reverse DNS
Australia			
	Queensland	58.6.115.42	ns1.jdcomputers.com.au
	Queensland	58.6.115.43	ns2.jdcomputers.com.au
Ile-De-France			
	Paris	82.229.244.191	ayanami.bikasuishin.org
	Paris	88.191.51.140	matsuri.bikasuishin.org
USA			
	Alaska	216.67.98.38	216-67-98-38.static.acsalaska.net
	Denver, Colorado	216.87.84.209	sourpuss.net
	Denton, Texas	71.170.11.156	static-71-170-11-156.dllstx.dsl-w.verizon.net