

www.vskom.de

User Manual NetCom PRO/WLAN

Edition: April 2012



Tel: +49 40 528 401 0

Fax: +49 40 528 401 99

Web: www.visionsystems.de

Support: service@visionsystems.de

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2009-2012 Vision Systems. All rights reserved. Reproduction without permission is prohibited.

Trademarks

VScom is a registered trademark of Vision Systems GmbH. All other trademarks and brands are property of their rightful owners.

Disclaimer

Vision Systems reserves the right to make changes and improvements to its product without providing notice.

Vision Systems provides this document “as is”, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Vision Systems reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Vision Systems assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contents

1	Overview	11
2	Introduction	11
2.1	About this Manual	11
2.2	Features	12
2.3	Product Specifications	12
2.3.1	Common characteristics	13
2.3.2	Device specific Characteristics	14
2.3.2.1	NetCom 113 PRO	14
2.3.2.2	NetCom 411 PRO	14
2.3.2.3	NetCom 413 PRO	15
2.3.2.4	NetCom 811 PRO	16
2.3.2.5	NetCom 813RM PRO (19")	17
2.3.2.6	NetCom 1611RM PRO (19")	17
2.3.2.7	NetCom 1613RM PRO (19")	18
2.3.2.8	NetCom 123 WLAN	19
2.3.2.9	NetCom 423 WLAN	20
2.3.2.10	NetCom 823RM WLAN (19")	21
2.4	Packing List	22
3	Hardware Description	23
3.1	Serial Port Configuration	23
3.2	Signal Assignment	24
3.3	RS 422/485 Electrical Configuration	24
3.3.1	Termination Resistors	25
3.3.2	BIAS Function	25
3.4	Serial Port Simple Settings	25
3.5	Network	26
3.5.1	WLAN Configuration	26
3.5.2	WLAN Antenna	26
3.5.3	Ethernet	26
3.6	Power Supply	27
3.6.1	Terminal Block Power	27
3.6.2	AC Power Plug	27
4	Windows Virtual COM Driver	28
4.1	Installation Procedure	28
4.1.1	Start the Installation Wizard	28
4.1.2	Find and Configure NetCom Devices	31
4.1.2.1	Configure IP Parameters	31
4.1.2.2	Configure Firewall	33
4.1.3	Install Drivers	33
4.2	Verify the Installation	35
4.3	Update the Drivers and Tools	36
4.4	Configuration of the Virtual COM Driver	36
4.4.1	Configure the Serial Ports	37
4.4.2	Performance Issues	38

4.4.3	Network & Misc Properties	40
4.4.4	Remote Settings Properties	42
4.4.5	Installation of NetCom Servers	44
4.4.5.1	Changing the Installation	45
4.5	Uninstall the Drivers and Tools	46
5	Configure with NetCom Manager	48
5.1	Starting NetCom Manager	49
5.2	NetCom Server Settings – Info	50
5.3	NetCom Server Settings – Ports	51
5.4	NetCom Server Settings – Firewall	52
5.5	NetCom Server Settings – Options	53
5.6	Manual Detection/Installation of a NetCom	54
5.7	Firewall Traversal Configuration	54
5.7.1	SOHO Firewall example	54
5.7.2	SOHO Virtual Servers	55
5.7.3	NetCom Detection through SOHO Firewall	55
5.7.4	Serial Ports through SOHO Firewall	56
5.7.5	DMZ and Virtual Servers	57
5.8	NetCom Helper Service	57
5.8.1	Configure Helper Service	57
5.8.2	Detection and Priority	58
5.8.2.1	Broadcast Search	58
5.8.2.2	DNS based Search	58
5.8.2.3	DNS based Firewall Configuration	59
5.8.3	Changed IP Address	59
5.8.3.1	Broadcast Domain	59
5.8.3.2	Internal DNS	60
5.8.3.3	Internet	60
5.8.4	Polling Period	60
5.9	Dynamic IP Address and OpenVPN™	61
6	Configure the Operation Modes	62
6.1	Accessing the Configurations	62
6.1.1	Web Browser Configuration	62
6.1.2	Telnet Configuration	63
6.1.3	Serial Configuration	65
6.2	NetCom Configuration Options	65
6.2.1	Server Configuration	65
6.2.1.1	Server Info	66
6.2.1.2	Server Parameter	67
6.2.1.3	Wireless Parameter	70
6.2.1.4	Encrypted Communication	71
6.2.1.4.1	Generating strong keys	75
6.2.1.5	Authentication	75
6.2.1.6	Date & Time	76
6.2.1.7	Save	77
6.2.2	Serial Port Configuration	78
6.2.2.1	Serial Settings	79
6.2.2.2	Transfer Settings	82

6.2.2.2.1	Driver Mode	82
6.2.2.2.2	TCP Raw Server	83
6.2.2.2.3	TCP Raw Client	84
6.2.2.2.4	Null Modem Tunnel	85
6.2.2.2.5	TCP Advanced Settings	87
6.2.2.2.6	UDP Data Transfer	89
6.2.2.2.7	IP-Modem	90
6.2.2.2.8	Print Server Function	91
6.2.2.2.9	PPP Network Configuration	92
6.2.2.3	Save	94
6.2.3	NetCom Tools	95
6.2.3.1	Ping	96
6.2.3.2	Statistics	96
6.2.3.3	Netstat	97
6.2.3.4	Wireless	100
6.2.3.5	Firmware	101
6.2.3.6	Save and Load Configuration	101
6.2.3.7	Logging and Debug	102
6.2.3.8	Save	103
6.2.4	Reboot	103
6.2.5	Save&Exit Menu	103
6.2.5.1	Save Parameter	103
6.2.5.2	Exit	104
6.2.5.3	Reboot	104
6.3	Erase Configuration of NetCom	104
7	IP Modem Function	106
7.1	Some possible Scenarios	106
7.2	Serial Signals and Cables	106
7.3	Operation Modes by IP Modem	107
7.4	Hayes Commands	107
7.4.1	AT command set	108
7.4.1.1	Standard AT-Commands	108
7.4.1.2	Extended AT-Commands	108
7.4.1.3	Non-AT commands	109
7.4.2	S-Registers for Configuration	109
7.4.3	Sample Commands used by Windows	109
7.5	Description of AT-Commands	109
7.5.1	AT D (dial)	110
7.5.2	AT O (online / data mode)	110
7.5.3	AT A (answer call)	110
7.5.4	AT B (modulation) [ATB1]	110
7.5.5	AT E (echo) [ATE1]	111
7.5.6	AT Q (quiet) [ATQ0]	111
7.5.7	AT V (verbose) [ATV1]	111
7.5.8	AT H (hangup) [ATH0]	111
7.5.9	AT I(n) (information) [ATI0]	111
7.5.10	AT S (setup)	112
7.5.11	AT L (loudness)	112

7.5.12	AT M (speaker)	112
7.5.13	AT N (auto baud) [ATN0]	112
7.5.14	AT Z (reset)	112
7.5.15	AT &F (factory settings) [AT&F0]	113
7.5.16	AT &C (DCD configuration) [AT&C1]	113
7.5.17	AT &S (DSR configuration) [AT&S0]	113
7.5.18	AT &D (DTR configuration) [AT&D2]	113
7.5.19	AT &K (handshake) [AT&K3]	114
7.5.20	AT \Q [AT\Q3]	114
7.5.21	AT &V (view profile)	114
7.5.22	AT &W (save profile)	114
7.5.23	AT &Z (save destination)	114
8	Print Server Operation	115
8.1	Printer Queue	115
8.2	Printer Reset	115
8.2.1	Init String Definition	115
8.2.1.1	ASCII Text	116
8.2.1.2	ASCII Control Codes	116
8.2.1.3	Numeric Codes	116
8.2.1.4	Modem Control Signals	116
8.2.1.5	Timing Options	116
8.2.2	Reset Example	116
8.3	Operation in Windows®	117
8.3.1	Add a New Printer	117
8.3.1.1	Create new printer port	117
8.3.1.2	Name the new Printer Port	118
8.3.1.3	Configure the Printer Port	119
8.3.1.4	Install Printer Driver	119
8.3.2	Modify an Existing Printer	119
8.3.2.1	Open the properties	119
8.3.2.2	Add the Print Server Port	120
9	OpenVPN™ Encryption	121
9.1	OpenVPN™ Installation	121
9.2	NetCom OpenVPN Configuration	122
9.3	OpenVPN™ Configuration	123
9.3.1	OpenVPN Configuration File	123
9.3.2	Start OpenVPN™ by Context-Menu	124
9.3.3	Start OpenVPN™ by Command line	125
9.3.4	Start OpenVPN™ as Windows Service	126
9.4	OpenVPN™ without Encryption	127
9.5	Reconfigure Virtual Serial Ports for OpenVPN™	127
10	PPP Network for Dial-In and -Out	128
10.1	PPP User Accounts	128
10.1.1	PPP Accounts for Dial-In	128
10.1.2	PPP Accounts for Dial-Out	128
10.2	PPP Hardware	129
10.2.1	PPP Modem Commands	129

10.2.2	PPP Null Modem Configuration	129
10.3	PPP Networks	130
10.3.1	PPP Client	130
10.3.2	PPP Server	130
11	TCP/IP Description	131
11.1	Recommended Settings	131
11.1.1	Static Configuration	131
11.1.2	DHCP Configuration	131
11.1.3	Automatic Configuration (APIPA)	132
11.1.4	Other Configuration	132
12	Troubleshooting Guide	133
13	Glossary of Terms	136
14	History	139

List of Figures

1	NetCom 113 PRO Top, Front and Rear Side	14
2	NetCom 411 PRO Top and Front Side	15
3	NetCom 413 PRO Top and Front Side	15
4	NetCom 811 PRO	16
5	NetCom 813RM PRO	17
6	NetCom 1611RM PRO Front side	17
7	NetCom 1611RM PRO Front side	18
8	NetCom 123 WLAN Top and Front Side	19
9	NetCom 423 WLAN Top and Front Side	20
10	NetCom 823RM WLAN Front Side	21
11	NetCom 823RM WLAN Rear Side	21
12	Connector DB9 male	24
13	RS 422/485 Option Jumper	25
14	Master Switch Standard Configuration	25
15	Power Terminal Block	27
16	AC Power input	27
17	Installation Wizard	28
18	NetCom Driver Installation	29
19	Start Driver Installation	30
20	Copy Driver Files	30
21	Discover and Select NetCom Devices for Installation	31
22	NetCom in Manager	31
23	Define NetComs IP Configuration	32
24	DNS Name for NetCom Server	32
25	Sending Parameters to a NetCom	33
26	Virtual Com Ports installing	33
27	New Hardware Wizard	34
28	Install drivers for the serial ports	35
29	VScom drivers in the Start Menu	35

30	NetCom in Device Manager	36
31	NetCom Manager NT	36
32	NetCom COM Port Serial Settings	37
33	NetCom COM Port Performance Settings	38
34	NetCom COM Port Network/Misc Properties	40
35	NetCom COM Port Remote Settings Properties	42
36	Select NetCom to install	44
37	Excluded NetCom	44
38	NetCom Manager Ports View	45
39	Reconfigured NetCom found	45
40	Replaced NetCom found	46
41	Uninstall NetCom Drivers via Control Panel	46
42	Uninstall NetCom Drivers in Start Menu	47
43	Remove, Repair	47
44	NetCom Manager	48
45	NetCom Manager in Start Menu	48
46	NetCom Manager Servers Panel	49
47	NetCom Manager Server Settings - Info	50
48	NetCom Manager Server Settings - Ports	51
49	NetCom Manager Server Settings - Firewall	52
50	NetCom Manager Server Settings - Options	53
51	NetCom Manager Port Configuration for Driver	56
52	NetCom Helper Service	58
53	Enter Qualified Domain Name	58
54	Configuration Menu in Web Browser	63
55	Request to Reboot in Web Browser	63
56	Password Request in Telnet	64
57	Select Terminal Type in Telnet	64
58	Main Menu of Configuration Console in Telnet	64
59	Server Information	66
60	Server Parameter Web Interface	67
61	Server Parameter Telnet Interface	68
62	Ethernet Operation by Software	69
63	Wireless Parameter	70
64	Wireless Encryption Modes	71
65	OpenVPN Network Parameter	72
66	OpenVPN Encryption grades	73
67	OpenVPN Key Management in Web Browser	73
68	Sample OpenVPN Key in Telnet	74
69	Use new Key in Telnet	74
70	Access Authentication	75
71	Date & Time Retrieval Options	76
72	Port Page Selection in Web Browser	78
73	Port Selection in Telnet	78
74	Serial Settings	79
75	Operation Mode by Software	80
76	Advanced Flow Control	81
77	Serial Port Mode Selection	82
78	Driver Mode parameters	83

79	TCP Raw Server parameters	84
80	TCP Raw Client parameters	85
81	Null Modem Tunnel	86
82	TCP Advanced Settings	88
83	UDP Data Transfer	89
84	IP-Modem	90
85	Print Server Configuration	91
86	PPP Configuration	93
87	Ping and Response in Web Browser	96
88	Ping and Response in Telnet	96
89	Statistics Port Selection	97
90	Port Statistics	97
91	Start Netstat	98
92	Netstat Sample Output	98
93	WLAN Scan	100
94	WLAN Scan Output	100
95	Firmware Upload	101
96	Save and Load Configuration in Web Browser	102
97	Syslog & Debuglog Parameters	102
98	Menu Save modified Parameters in Telnet	103
99	Menu Exit from Configuration in Telnet	104
100	Exit and Reboot in Telnet	104
101	Add a printer	117
102	Select Printer Port	117
103	Create Printer Port	118
104	Name-Properties of Print Server Port	118
105	Mode-Properties of Print Server Port	119
106	Select Port for Printer	120
107	Add Printer Port	120
108	OpenVPN Installation Wizard	121
109	OpenVPN Installable Components	121
110	Installing TAP-Win32 Adapter	122
111	OpenVPN Network Adapter	122
112	OpenVPN Configuration File	123
113	Context-Menu of OpenVPN™	124
114	OpenVPN Connection is active	125
115	OpenVPN by Command line	125
116	OpenVPN as Windows Service	126
117	Start OpenVPN Service	126
118	Service Options	126
119	Startup Types	127
120	Null Modem Connections	129

List of Tables

1	Specifications, common	13
2	Characteristics of NetCom 113 PRO	14
3	Characteristics of NetCom 411 PRO	14

4	Characteristics of NetCom 413 PRO	15
5	Characteristics of NetCom 811 PRO	16
6	Characteristics of NetCom 813RM PRO	17
7	Characteristics of NetCom 1611RM PRO	17
8	Characteristics of NetCom 1613RM PRO	18
9	Characteristics of NetCom 123 WLAN	19
10	Characteristics of NetCom 423 WLAN	20
11	Characteristics of NetCom 823RM WLAN	21
12	Switch Configurations	23
13	Signal Assignment DB9 male	24
14	RS 422/485 Jumper Configuration	25
15	LED Function	27
16	SOHO Firewall Pass-Through	55
17	IP Modem cable	107
18	IP Modem Standard AT Commands	108
19	IP Modem Extended AT-Commands	108
20	IP Modem S-Registers for Configuration	109
21	IP Modem Sample Dials	110
22	IP Modem virtual Modulation	111
23	IP Modem Responses	111
24	IP Modem Information Responses	112
25	IP Modem DTR Configuration	113

1 Overview

The NetCom PRO Serial Device Servers are designed to remotely operate serial ports over networks. The network interface is implemented as 100 Mbit/s Fast Ethernet with Auto-MDI(X). The subfamily of NetCom WLAN Serial Device Servers provide a second network interface as WLAN (as of 802.11g) with 54Mbit/s transfer rate.

The transport is implemented via TCP/IP and UDP protocols. Therefore control is available via WLAN, Ethernet, Intranet and Internet. All communication with the NetCom PRO Servers may happen encrypted with strong algorithms on all interfaces.

The supplied driver software implements virtual serial ports, which hide the network transfer from your applications. Software applications using standard COM ports need no change to operate via NetCom through the virtual serial ports.

2 Introduction

This manual covers several different models of NetCom PRO devices, in particular the Wireless operating devices of the PRO series. In general the operation is the same on all models, except where explicitly noted otherwise.

The devices come with a steel case well suited for industrial environments.

The NetCom PRO supports high serial speeds up to 3.6 Mbps. All serial ports provide communication via the common RS 232 mode (up to 500 kbps). The NetCom PRO servers with a '13' in their name (and the PRO WLAN servers) also offer the industrial RS 422 and RS 485 configuration (up to 3.6 Mbps). In RS 485 mode the NetCom may use the Automatic Receive Transmit (ART) control logic to follow the RS 485 specifications for transmitting data. No special code is necessary to be implemented in your software applications.

2.1 About this Manual

This manual covers many configuration options of the NetCom PRO Serial Device Servers. The vast majority of these are set by software, sometimes in alternative methods. To emphasize these in the text, special character styles are used.

Bold Typewriter is used for the names of configuration options or buttons, as they are displayed in menus or dialogs.

Typewriter denotes names of special values for multiple-choice parameters. Such values may appear in drop-down lists or as radio buttons.

The version of the firmware described in this manual is 2.6.4, covered together with driver 1.5.12.0.

2.2 Features

- Single power supply
DC 9-30V, 200-600 mA@12V
AC 100-240V 47-63Hz, 25VA
- Wireless LAN 802.11b/g for 54Mbit/s on WLAN models
- Ethernet 10/100BaseTx/Auto-MDI(X) for auto-configuration
- Three way serial port interfaces: RS 232, RS 422 and RS 485
- Max. 3.686.400 bps, half- and full-duplex
- TCP/IP configuration fixed or by DHCP
- Easy remote configuration via SNMP
- Drivers for Windows™ and Linux operating systems
- Documented interface for every networked operating system

2.3 Product Specifications

Most of the hardware characteristics are common for all models. However some must differ from model to model, they are shown in dedicated sections. Some models are restricted to RS 232, others do not have a WLAN connection.

2.3.1 Common characteristics

Processor	ARM9 (KS8695P)	
Memory	16MB SDRAM	
	2MB Flash	
WLAN antenna	SMA-reverse	
Ethernet connector	RJ45 10BaseT/100BaseTx	
Protocols	TCP/IP, UDP, SNMP, DHCP, ICMP, ARP, Telnet, RTelnet, HTTP	
Serial Speed	1 bps up to 3.69 Mbps ¹	
Parity	None, Even, Odd, Mark, Space	
Data bits	5, 6, 7, 8	
Stop bits	1, 2 (1.5 with 5 data bits)	
	RS 232	TxD, Rx D, RTS, CTS, DTR, DSR, DCD, RI, GND
	RS 422	Tx+/Tx-, Rx+/Rx-, GND
	RS 485 4-wire	
Serial signals	RS 485 2-wire	Data+/Data-, GND
Serial connector	DB9 male (similar to PC)	
Serial operation	RS 232, RS 422/485 configured by DIP switch or by software	
Management	Serial console, Telnet, Web browser, SNMP	
Driver software	Windows Vista/2003/XP/2000, Windows NT, Linux (Fixed TTY)	
Management software	Driver installation and configuration program, Management console	
Operating temp.	0° to 55°C	
Approval	CE, FCC	

Table 1: Specifications, common

Note 1: Serial bitrates above 500 kbps may cause problems when used with RS 232. It requires short cables with low capacity, to reduce load on the serial signals. When using RS 422 or RS 485 there is no problem using maximum bitrates.

2.3.2 Device specific Characteristics

2.3.2.1 NetCom 113 PRO One port.

Power Requirement	DC 9V to 30V, 300 mA@12V
Power Connector	Terminal Block (3.6.1)
Serial Ports	1×RS 232, RS 422/485
Dimensions	73×115×27 mm ³ (W×D×H) 101×121×27 mm ³ with connectors
Weight	250 g

Table 2: Characteristics of NetCom 113 PRO



Figure 1: NetCom 113 PRO Top, Front and Rear Side

This is the NetCom 113 PRO with the serial connector and the configuration switches. The rear side holds the power connector, Reset hole and the Ethernet RJ45.

2.3.2.2 NetCom 411 PRO Four Ports.

Power Requirement	DC 9V to 30V, 400 mA@12V
Power Connector	Terminal Block (3.6.1)
Serial Ports	4×RS 232
Dimensions	169×93×29 mm ³ (W×D×H) 169×99×29 mm ³ with connectors
Weight	500 g

Table 3: Characteristics of NetCom 411 PRO



Figure 2: NetCom 411 PRO Top and Front Side

This is the NetCom 411 PRO with the serial connectors and the LEDs. The hidden rear side holds the power connector, Reset hole, the Ethernet RJ45 and the configuration switches.

2.3.2.3 NetCom 413 PRO Four Ports.

Power Requirement	DC 9V to 30V, 400 mA@12V
Power Connector	Terminal Block (3.6.1)
Serial Ports	4×RS 232, RS 422/485
Dimensions	169×93×29 mm ³ (W×D×H) 169×99×29 mm ³ with connectors
Weight	500 g

Table 4: Characteristics of NetCom 413 PRO



Figure 3: NetCom 413 PRO Top and Front Side

This is the NetCom 413 PRO with the serial connectors and the LEDs. The hidden rear side holds the power connector, Reset hole, the Ethernet RJ45 and the configuration switches.

2.3.2.4 NetCom 811 PRO Eight Ports.

Power Requirement	AC 100V to 240V, 47-63Hz, 25VA
Power Connector	Terminal Block (3.6.1)
Serial Ports	8×RS 232
Dimensions	171×94×46 mm ³ (W×D×H) 193×99×47 mm ³ with connectors
Weight	1350 g

Table 5: Characteristics of NetCom 811 PRO



Figure 4: NetCom 811 PRO

This is the NetCom 811 PRO with the LEDs and the serial connectors. The rear side holds the power and the Ethernet connector as well as the Master configuration DIP switch. The Reset pin is located on the hidden right side.

2.3.2.5 NetCom 813RM PRO (19") Eight Ports.

Power Requirement	AC 100V to 240V, 47-63Hz, 25VA
Power Connector	AC Power plug (3.6.2)
Serial Ports	8×RS 232, RS 422/485
Dimensions	258×149×45 mm ³ (W×D×H) 278×155×46 mm ³ with connectors
Weight	1350 g

Table 6: Characteristics of NetCom 813RM PRO



Figure 5: NetCom 813RM PRO

This is the NetCom 813RM PRO with the Ethernet connector and the LEDs, the serial connectors and the Reset pin (in the lower right). The brackets for 19" mounting shall be attached left and right to the case. This rack mount option is part of the shipment. The rear side holds the power connector and the Master configuration DIP switch.

2.3.2.6 NetCom 1611RM PRO (19") Sixteen Ports.

Power Requirement	AC 100V to 240V, 47-63Hz, 25VA
Power Connector	AC Power plug (3.6.2)
Serial Ports	16×RS 232
Dimensions	258×149×45 mm ³ (W×D×H) 278×155×46 mm ³ with connectors
Weight	1450 g

Table 7: Characteristics of NetCom 1611RM PRO



Figure 6: NetCom 1611RM PRO Front side

This is the NetCom 1611RM PRO with the Ethernet connector and the LEDs, the 16 serial connectors and the Reset pin (in the lower right corner). The hidden rear side holds the power connector and the Master configuration DIP switch.

Not shown here are the mounting angles for a 19" rack.

2.3.2.7 NetCom 1613RM PRO (19") Sixteen Ports.

Power Requirement	AC 100V to 240V, 47-63Hz, 25VA
Power Connector	AC Power plug (3.6.2)
Serial Ports	16×RS 232, RS 422/485
Dimensions	258×149×45 mm ³ (W×D×H) 278×155×46 mm ³ with connectors
Weight	1450 g

Table 8: Characteristics of NetCom 1613RM PRO



Figure 7: NetCom 1611RM PRO Front side

This is the NetCom 1613RM PRO with the Ethernet connector and the LEDs, the 16 serial connectors and the Reset pin (in the lower right corner). The hidden rear side holds the power connector and the Master configuration DIP switch.

Not shown here are the mounting angles for a 19" rack.

2.3.2.8 NetCom 123 WLAN One Port.

Power Requirement	DC 9V to 30V, 300 mA@12V
Power Connector	Terminal Block (3.6.1)
Serial Ports	1×RS 232, RS 422/485
Dimensions	73×115×27 mm ³ (W×D×H) 101×121×27 mm ³ with connectors
Weight	250 g

Table 9: Characteristics of NetCom 123 WLAN



Figure 8: NetCom 123 WLAN Top and Front Side

Here showing NetCom 123 WLAN with the antenna, the serial connector and the configuration switches. The hidden rear side holds the power connector, Reset hole and the Ethernet RJ45.

2.3.2.9 NetCom 423 WLAN Four Ports.

Power Requirement	DC 9V to 30V, 400 mA@12V
Power Connector	Terminal Block (3.6.1)
Serial Ports	4×RS 232, RS 422/485
Dimensions	169×93×29 mm ³ (W×D×H) 169×99×29 mm ³ with connectors
Weight	500 g

Table 10: Characteristics of NetCom 423 WLAN



Figure 9: NetCom 423 WLAN Top and Front Side

Here showing NetCom 423 WLAN with the antenna, the serial connectors and the LEDs. The hidden rear side holds the power connector, Reset hole, the Ethernet RJ45 and the configuration switches.

2.3.2.10 NetCom 823RM WLAN (19") Eight Ports.

Power Requirement	AC 100V to 240V, 47-63Hz, 25VA
Power Connector	AC Power plug (3.6.2)
Serial Ports	8×RS 232, RS 422/485
Dimensions	258×149×45 mm ³ (W×D×H) 278×155×46 mm ³ with connectors
Weight	1350 g

Table 11: Characteristics of NetCom 823RM WLAN



Figure 10: NetCom 823RM WLAN Front Side

Here showing NetCom 823RM WLAN with the Ethernet connector and the LEDs, the serial connectors and the Reset pin (in the lower right). Also visible is the WLAN antenna from the rear side.



Figure 11: NetCom 823RM WLAN Rear Side

The rear side holds the power connector and the Master configuration DIP switch. This image also shows the front side with the 19" mounting angles. This rack mount option is part of the shipment.

2.4 Packing List

- NetCom PRO or NetCom WLAN Serial Device Server
- Power supply 12V 1A for DC Models NetCom 113 PRO, 123 WLAN, 411 & 413 PRO, 423 WLAN and 811 PRO
- Power cord for AC Models NetCom 813RM PRO, 823RM WLAN, 1611RM PRO and 1613RM PRO
- WLAN Antenna for NetCom WLAN Models
- Mounting angles for 19" models
- CD-ROM with driver and configuration software
- Quick Installation Guide

3 Hardware Description

This section focuses on the options provided by the hardware of NetCom PRO Serial Device Servers

3.1 Serial Port Configuration

The serial ports in the NetCom Devices follow the specifications of RS 232. It is also possible to use the serial port in RS 422 or RS 485 mode. This is defined by a set of DIP switches or by software. Here is a list of the available modes and the switch settings.

Warning: a bad configuration may cause serious damage in the NetCom or the connected device.

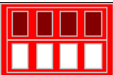
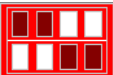

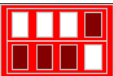
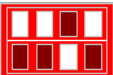
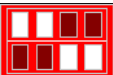
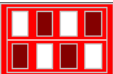
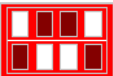
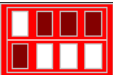
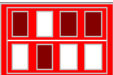
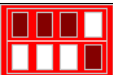
	Line Mode, Comment	S1	S2	S3	S4	Switch Positions
RS 232	Configuration via serial port	Off	Off	Off	Off	
RS 232	Data communication	Off	Off	On	On	
RS 422	Data communication	Off	On	On	On	
RS 485 by ART	4 wire Full Duplex	On	On	On	Off	
- " -	2 wire Half Duplex with Echo	On	On	Off	On	
- " -	2 wire Half Duplex no Echo	On	On	Off	Off	
RS 485 by RTS	4 wire Full Duplex	On	Off	On	Off	
- " -	2 wire Half Duplex with Echo	On	Off	Off	On	
- " -	2 wire Half Duplex no Echo	On	Off	Off	Off	
	Selected by Software	Off	On	Off	Off	
	Factory settings	Off	Off	Off	On	

Table 12: Switch Configurations

'Configuration via serial port' is only effective on port 1 of the NetCom Server.

ART is the Automatic Receive Transmit control. In RS 485 this is the recommended option. The NetCom performs the required activation and disabling of the RS 485 transmitter by an internal automatic.

The Master DIP switches configure all serial ports of a NetCom to the same operation mode. If different modes are desired, the switch must be set to «Selected by Software», and the configuration may be done via Serial Port, Telnet, Web browser or SNMP.

Factory Settings are restored on next Power-Up/Reset of the NetCom Server.

3.2 Signal Assignment

It is of course important to know the exact location of the serial signals in the configured mode. Here is the table for the DB9 male connector. For RS 232 the assignment is the same as on any PC (Com1/2).

Pin	RS 232	RS 422/485 4-wire	RS 485 2-wire
1	DCD	Tx- (A)	Data- (A)
2	RxD	Tx+ (B)	Data+ (B)
3	TxD	Rx+ (B)	
4	DTR	Rx- (A)	
5	GND	GND	GND
6	DSR		
7	RTS		
8	CTS		
9	RI		

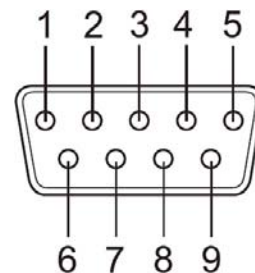


Figure 12: Connector DB9 male

Table 13: Signal Assignment DB9 male

Please note the GND signal in RS 422 and RS 485 modes. This signal must also be connected between the serial devices. So in reality there is neither a 2-wire nor a 4-wire connection. With the exception of very special configurations, a serial cable without GND violates the specifications for RS 422 and RS 485.

3.3 RS 422/485 Electrical Configuration

In typical RS 422 and RS 485 installations certain electric conditions have to be configured. Simply connecting cables is not enough to fulfill the specifications of RS 422 and RS 485.

For ease of installations the NetCom PRO Serial Device Servers provide these functions for often used parameters. They are activated by placing certain jumpers, internal of the NetCom PRO. There is one block of jumpers near each serial port. Place a connection cap to activate the function.

Pins	Function of Signals
1-2	Place 120Ω to terminate $Tx\pm$ (Data \pm in RS 485 2-wire)
3-4 5-6	Add BIASing function to $Tx\pm$ (mostly required for RS 485 2-wire modes)
7-8	Place 120Ω to terminate $Rx\pm$
9-10 11-12	Add BIASing function to $Rx\pm$

Table 14: RS 422/485 Jumper Configuration

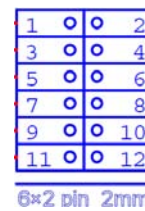


Figure 13: RS 422/485 Option Jumper

Warning: All jumpers are unconnected by default. This is important for use in RS 232 mode. Never close any jumper, otherwise communication errors or damage of devices is possible.

3.3.1 Termination Resistors

The use of long communication lines in RS 422 and RS 485 mode require the installation of termination resistors. These must match the impedance of the cable. Typical cables in Twisted-Pair configuration have an impedance of about 120Ω . In RS 422 this resistor has to be placed at the far end from the sender, in RS 485 the typical configuration requires one resistor at each end of the cable.

3.3.2 BIAS Function

RS 485 requires a BIAS option for the communication lines. This will guarantee stable electrical levels on the cables, even at times when no station is transmitting data. Without BIAS there will be noise on the cable, and sometimes receivers can not detect the first characters of a beginning communication.

3.4 Serial Port Simple Settings

There is one set of 4 Dip switches to configure the operation mode of the NetCom PRO Device. This switch is the Master configuration for each serial port. All ports operate in the same mode, unless the DIP switches configure for software setting. Before connecting a serial device, the serial port configuration must be completed.

Warning: a bad configuration may cause serious damage in the NetCom or the connected device. To avoid these problems, it is recommended not to connect a device to the serial ports in the first installation. The serial ports should be configured for RS 232. This is done by setting the DIP switches like this example.

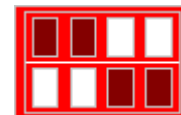


Figure 14: Master Switch Standard Configuration

3.5 Network

The NetCom PRO connects to Ethernet, while the NetCom WLAN may use either WLAN or Ethernet at customers choice. By factory settings both interfaces are enabled, and the priority is set for Ethernet (i.e. via cable). If no cable is connected here, the Wireless interface is active. Otherwise the server communicates via Ethernet. Both interfaces use the same MAC Address and IP Address, to allow for seamless fail-over from cable to wireless operation. The NetCom WLAN Servers do not perform a DHCP request when the WLAN interface becomes active.

3.5.1 WLAN Configuration

The pre-defined operation mode is ad-hoc, which means you do not need an Access Point to get access to the NetCom. Any computer with WLAN equipment may contact the NetCom WLAN. The configuration of the NetCom WLAN is done with the tools described later. This is the most easy way of installation.

However the Ad-hoc mode is not encrypted by definition of the IEEE 802.11 standard. As one result any station can read the data transferred to the NetCom WLAN. This also includes the passwords. Further in case of problems, it is harder to find the source of the problems. Therefore the recommended method is to use the Ethernet connector for the first configuration. Or in case of doubt, use the first serial port to configure the NetCom.

The configuration of the WLAN parameters should follow in a later step. This is especially the case, if encryption or certain other parameters require special configuration.

3.5.2 WLAN Antenna

The connector used for the WLAN Antenna is known as SMA-Reverse. This is a standard type to allow for simple connection of different equipment. Just fit the supplied antenna by carefully screwing it to the connector. You are free to connect a cable and a different antenna of your choice, as long as it is designed for WLAN. When the NetCom WLAN detects an operational WLAN it can connect to, the Blue LED lights.

3.5.3 Ethernet

The connector for Ethernet is the usual RJ45. Simply connect it to your (switching) Hub. Because the Ethernet has Auto-MDI(X) function, a direct cable or a cross-over cable may both be used.

When the connect is done the Link LED on NetCom PRO (yellow) will light. When data traffic occurs on the network, this LED will blink. It depends on your network whether a 100Mbit or a 10Mbit connect will be established. A 100Mbit net causes the Speed LED on NetCom PRO (green) to light, otherwise it will remain dark.

Red LED	Yellow LED	Green LED	Status
Off	–	–	Device off, no power
On	Off	Off	No connection
On	On	Off	10Mbit connection established
On	Blink	Off	10Mbit data transfer (traffic)
On	On	On	100Mbit connection established
On	Blink	On	100Mbit data transfer (traffic)

Table 15: LED Function

3.6 Power Supply

The NetCom PRO device is powered by a single 9-30V power supply. It requires 200 mA up to 1500 mA of current, depending on the device type and voltage supplied. A suitable power supply adapter is part of the packaging. Connect the cable to the power jack (Terminal Block) at the rear side of NetCom PRO, and put the adapter into the socket.

You may connect a power supply of your choice, providing the technical requirements are met.

For the 19" devices of course just plug the power cord into the socket, the NetCom accepts 100V to 240V AC, 47 to 62Hz. The Power LED on NetCom (red) will light.

3.6.1 Terminal Block Power

The Terminal Block power connector receives positive voltage on the right (V+) pin. The center (V-) pin connector is negative, which is connected to GND and the case. GND is the same as Field GND (FG), so the standard adapter does not connect to this pin.

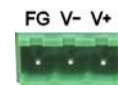


Figure 15: Power Terminal Block

3.6.2 AC Power Plug

AC power is provided by a standard cable. Protective Earth connects to the case.



Figure 16: AC Power input

4 Windows Virtual COM Driver

This chapter covers the use of NetCom Devices via Virtual Com Ports installed by the supplied driver software for Windows. Sections 4.1 to 4.3 describe in details the process of driver installation and removal, as well as updating. This first part here is for quick installation, so only the common options are covered.

Section 4.4 provides the details of NetCom Manager and also the options available with the Virtual Com Ports.

4.1 Installation Procedure

Before starting installation, it is essential to have an IP configuration ready for the NetCom Device to install. You may read the TCP/IP Description (section 11) below. The default configuration is based on DHCP, which is fine in many networks. If in doubt, please ask your Network Administrator for help. Further it is assumed the network access is functional. It is recommended to use Ethernet via Hub or Cross-Over cable for configuration.

The following description is based on Windows XP Professional, with Service Pack 2 installed. The installation on other configurations of Windows is similar. The installation of drivers is described first. This is followed by a procedure to verify a correct installation. The last part of this section is about the uninstall or update processes of drivers and tools.

Drivers are provided for Windows NT, Windows 2000 up to Windows 7, Windows Server 2000 up to 2008 R2. The x86 and x64 Editions have separate drivers.

The drivers use the IP Address of NetCom Servers to operate. So the configuration of the device should avoid to change that over time. This is either done via a static IP Address, or by proper configuration of the DHCP server. In the second case the DHCP server shall recognize the NetCom by its MAC Address, and assign the same IP Address each time the device sends a request. All available DHCP Server products provide such a function, even in SOHO routers.

4.1.1 Start the Installation Wizard

This is the Installation Wizard, it is named VSNSETUP.EXE^{ab}. You'll find it on the CD-ROM shipped with the NetCom PRO, in the directory responsible for your operating system. The drivers are also available on the Internet, in the latest version. Start this program to install the drivers.

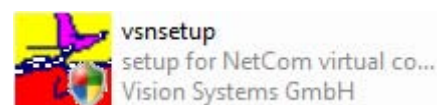


Figure 17: Installation Wizard

^aVSNSETUPA64.EXE in x64 Editions of Vista and Windows XP

^bVSNSTUNT.EXE in Windows NT



Figure 18: NetCom Driver Installation

The installation program offers three different ways of installation. The first option is the most common used function, a **Complete Installation**. All driver files and tools are copied to the Windows system, and installed in the Start Menu. Further the drivers are installed in the system, and the network is searched for available NetCom. The serial ports on these devices are installed as Virtual Com Ports in the system.

The second option will **Install Tools and Drivers**. However the network is not searched for NetCom Devices. And of course no serial ports are installed in the system. This function is designed to prepare a computer for use of NetCom Virtual Com Ports, but the final installation shall be skipped for some reasons. For example the computer shall be shipped to a customer, and the final installation shall happen there.

Finally the third option is to **Install Tools only**, no drivers. At time of writing these tools are the NetCom Manager, as well as the uninstall and repair functions. This function should be selected when the use of Virtual Com Port drivers is not intended. The NetCom Devices may be used in many different operation modes covered later (6).

There are also some Hyperlinks, opening access to more recent driver versions.

This part of the manual documents the **Complete Installation**, so click this option.

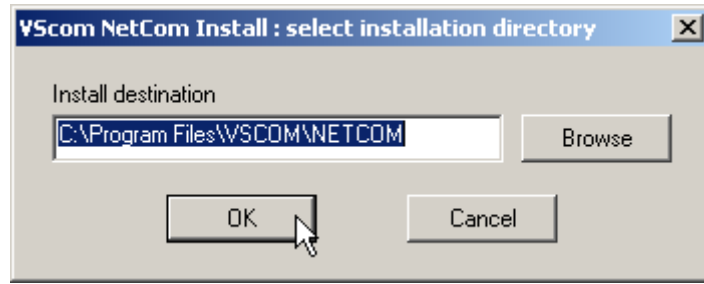


Figure 19: Start Driver Installation

A target folder for a file copy is requested. The tools and driver files are installed here. The tools will appear in the Start Menu, so a sub-folder of your Program Files is suggested. Just click the OK button.



Figure 20: Copy Driver Files

Some files are copied to your hard disk, this is the usual process similar to other Windows installations. The upper bar increases with the progress of each step performed in the installation process. The lower bar illustrates each step performed until full installation is finished.

4.1.2 Find and Configure NetCom Devices

When all files are copied, the NetCom Manager¹ program is started. This searches for all NetCom Devices on your network.

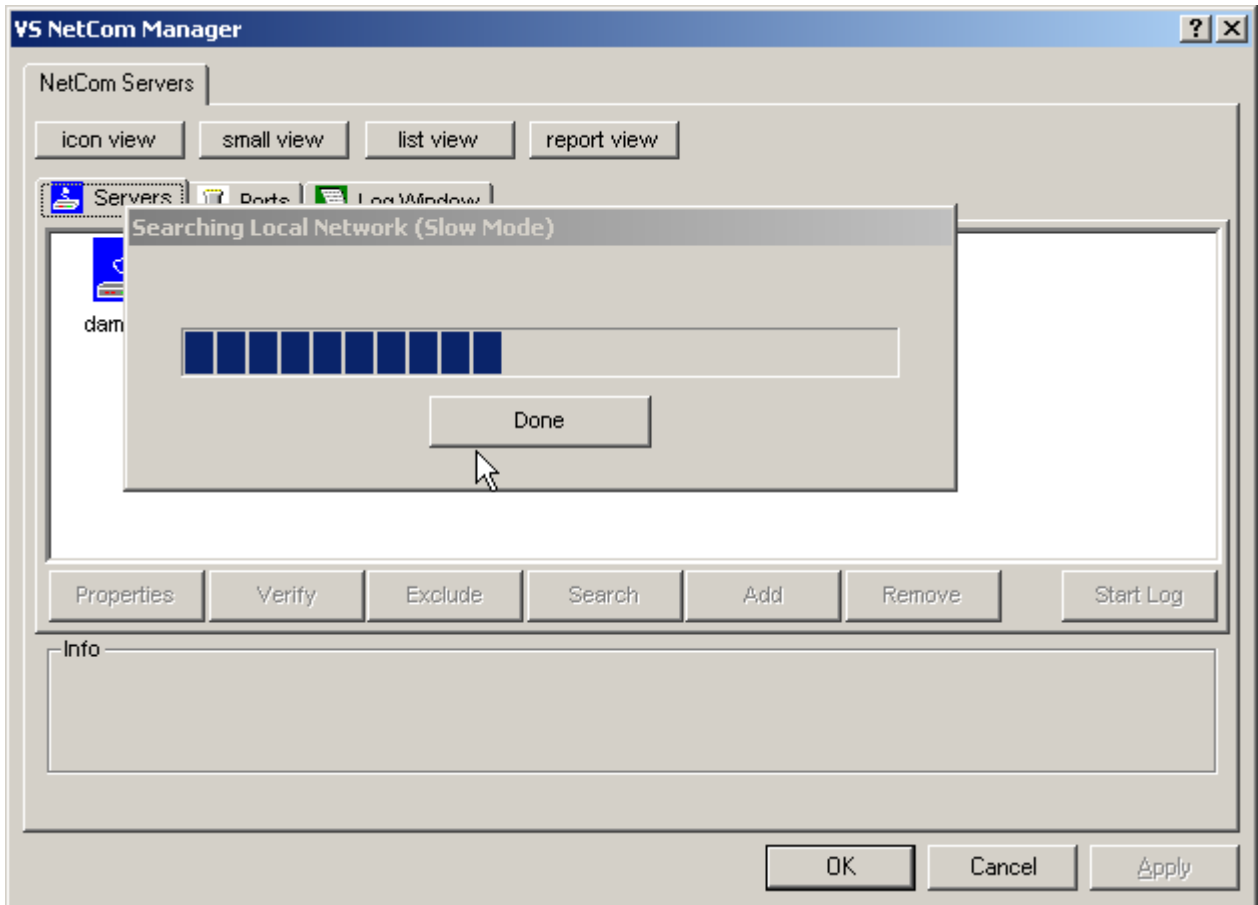


Figure 21: Discover and Select NetCom Devices for Installation

After short time the search process is finished. All discovered NetCom are listed. In your very first installation of NetCom Devices and Drivers you should connect only one NetCom to your network. This single Device is listed here. Identify it by comparing the serial number shown in the NetCom Manager.



Figure 22: NetCom in Manager

4.1.2.1 Configure IP Parameters As mentioned above, it is important to configure the NetCom to operate in your network. In many networks this is done by a special server (DHCP). Please ask your Network Administrator for information. If you need to define parameters manually, double-click the devices icon.

¹This program is covered in detail in 4.4. For now follow the minimum steps.

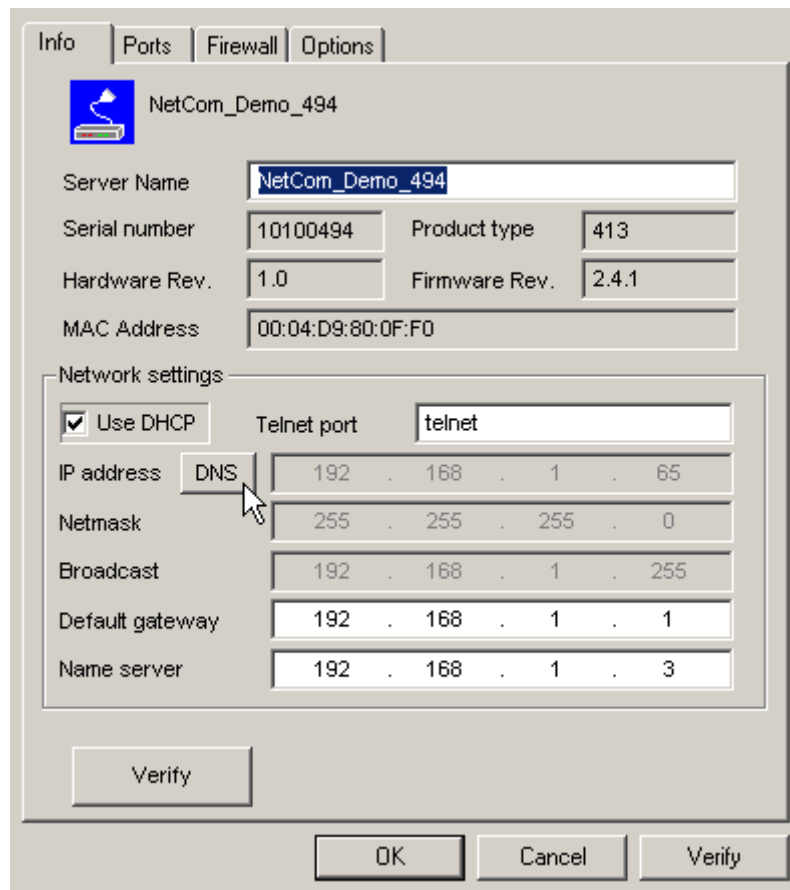


Figure 23: Define NetComs IP Configuration

This panel opens. Deselect the Option of **Use DHCP**, and place your parameters as **IP address**, **Netmask** and **Broadcast**. Click on the **OK** button. Since driver version 1.5.6 you may also enter a **DNS** name instead of the IP Address.

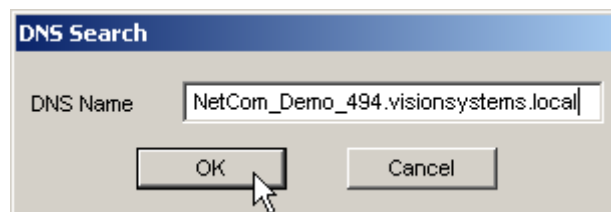


Figure 24: DNS Name for NetCom Server

Click the **DNS** button, and enter the Qualified Domain Name defining the NetCom Server. Your Administrator will provide you with it. This name is translated to an IP Address and used by the driver.

When all parameters of the configuration are set, click the **OK** button. This will update the configuration of the NetCom , the new parameters are sent to the device.

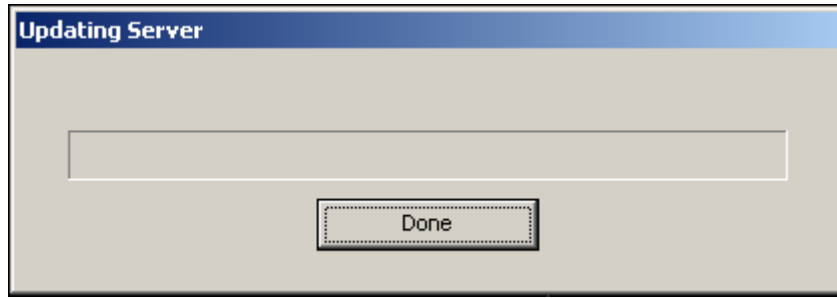


Figure 25: Sending Parameters to a NetCom

4.1.2.2 Configure Firewall As you will notice in figure 23 the driver may also operate by traversal of a Network Firewall. This requires a special configuration, which is skipped here. Please read in detail in section 5.6 on page 54. For now proceed with the standard installation.

4.1.3 Install Drivers

You are now back in the NetCom Manager. Click the **OK** button, the installation continues. Windows detects the serial ports on the fresh NetCom as new Hardware. All new Virtual Com Ports are installed without manual intervention by the user.

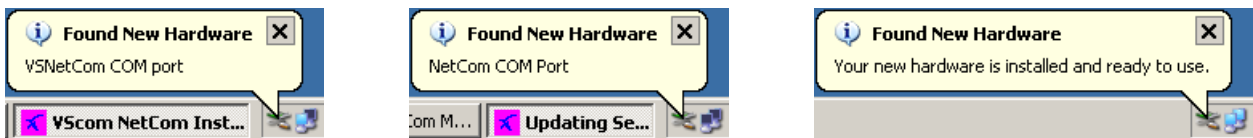


Figure 26: Virtual Com Ports installing

However using early driver versions or certain configurations of Windows, the system may request certain actions by the user. You may be asked about to get latest drivers.



Figure 27: New Hardware Wizard

Automatic searching of Windows Update website will take quite a long time. So select the third item, and click on **Next**. This question neither appears on Windows XP prior to SP2, nor on any previous Windows version.

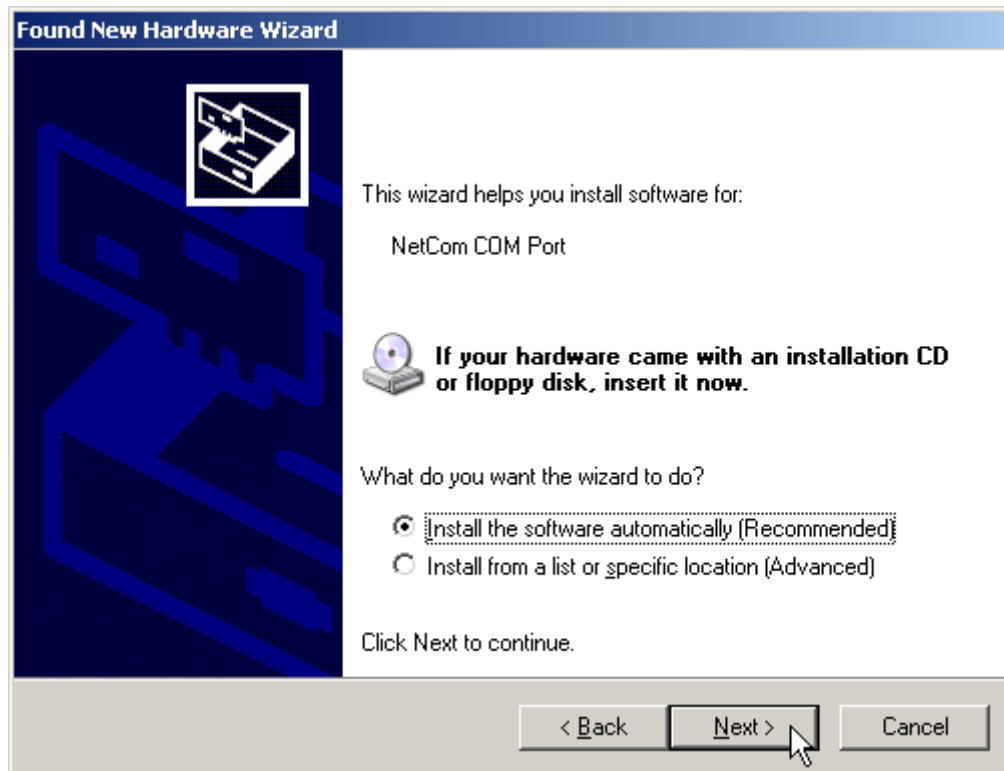


Figure 28: Install drivers for the serial ports

The pre-selected automatic installation is fine, just click on **Next**. The driver files are already copied to your hard disk. Now Windows installs them in the system directory. To **Finish** the installation click on that button as it appears. If the system can not detect the drivers, use the second option. Add the folder as given in figure 19 to the search, then the system will detect suitable driver files.

These latest steps happen for each serial port on the NetCom Device. Just repeat the procedure, until all ports are successfully installed. Windows will show you this. In most situations it is not required to reboot the system. Of course you can do that now, to test the drivers.

4.2 Verify the Installation

In the Start Menu you'll find the new program group "VScom NetCom". The installed programs are the NetCom Manager, the Driver Repair program and an option for uninstallation. This group is not installed on Windows NT.



Figure 29: VScom drivers in the Start Menu

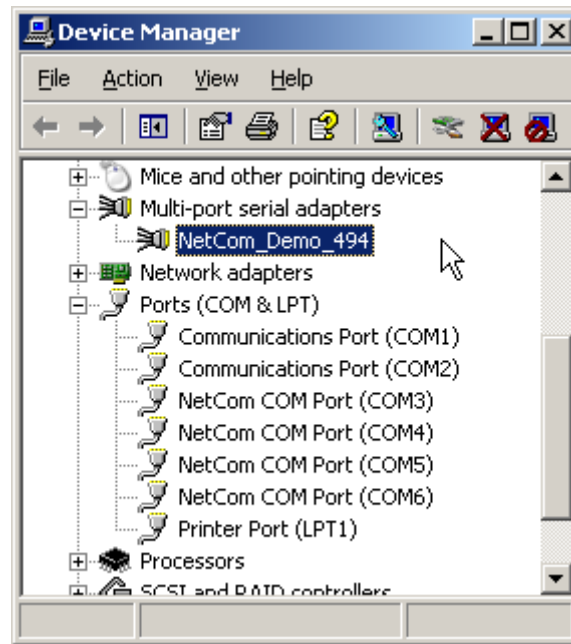


Figure 30: NetCom in Device Manager

In the Device Manager the serial ports are listed in the usual section **Ports**. Additionally there is the device class **Multi-port serial adapters**^a. All installed NetCom Devices are listed herein. The available options are described later.

On Windows NT there is no Device Manager. You'll find the serial ports listed in the Control panel in the Ports applet. To configure the NetCom and special port options, there is a new applet named NetCom Manager.



Figure 31: NetCom Manager NT

^aIn drivers up to version 1.5.6 this was 'VScom Virtual Com'

4.3 Update the Drivers and Tools

As suggested by figure 43 the Installation Wizard offers an option to **Update** the drivers to a new version. Windows itself also offers an option to update the drivers of installed devices. Although this is a functional option, the correct operation of the NetCom drivers depends on a common version for all drivers. The secure way to perform such an update is to run the Installation Wizard. All driver files are replaced by later versions simultaneously, and all configuration data (Com number, special port configurations, ...) is preserved.

Because several internal configurations of drivers have changed from version 1.5.6 to 1.5.8, the option of **Update** is not available in this situation. The only way of update is to Uninstall the current version, and install the new. Such a situation will be very rare.

4.4 Configuration of the Virtual COM Driver

If properly configured, the serial ports of the NetCom Devices appear as Virtual Com Ports in your computer. The "virtual" means, in the computer is no real hardware related to the serial port,

however the driver offers the full functionality of a serial port to the system. The interface used by the driver is VCOMM, which in turn is supported by the Windows API. So Windows does not see a difference to Com1, and also no application should detect the change.

When the serial ports are installed by the Virtual Com driver software, any application may use them. In the Device Manager they appear as **NetCom COM Port** (figure 30). Without special tests a program does not see a difference between Com1 and the virtual Com7. For example the HyperTerminal program has no problem to communicate through these Virtual Com. And this situation is common amongst most programs.

4.4.1 Configure the Serial Ports

A typical application selects a serial port, and opens it. After that it performs the standard configuration of bits per character, parity settings and number of stop bits. Also the flow control (handshaking) is defined by the application. Windows sends these requests to the port driver, and this driver sends the requests to the serial port on the NetCom.

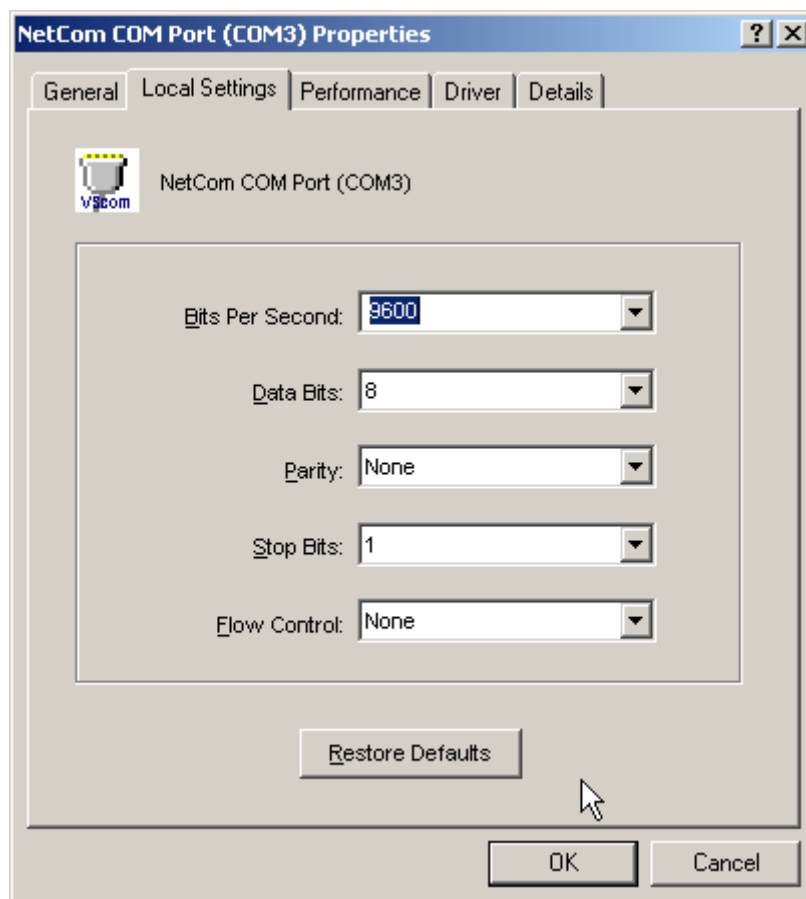


Figure 32: NetCom COM Port Serial Settings

The same parameters may be pre-configured in the Device Manager. This is done via the **Properties** of the **NetCom COM Port**. In the **Local Settings** tab these standard parameters are defined. Since most programs configure these parameters by themselves, the values are very rarely used. A typical situation is a serial printer attached to this virtual port.

As usual this behaves different in Windows NT. There is no Device Manager. To change these standard parameters, open the **Ports** applet in the Control Panel. However it is suggested you open the new **NetComManager** applet instead. Change to the **Ports** view as in figure 38. Double-click on the small icon at the left side. In this dialog go to the **Local Settings** tab, as seen above.

4.4.2 Performance Issues

Operation through the network causes some extra time, which is approximately 5 Milliseconds. For comparison, with a port internal to the computer this time may be just some 100 Microseconds. This added time has an impact on reaction times. Some data protocols may be sensible. A lot of configurations are possible to compensate for this. But these have an effect on the sheer data throughput of the virtual serial port.

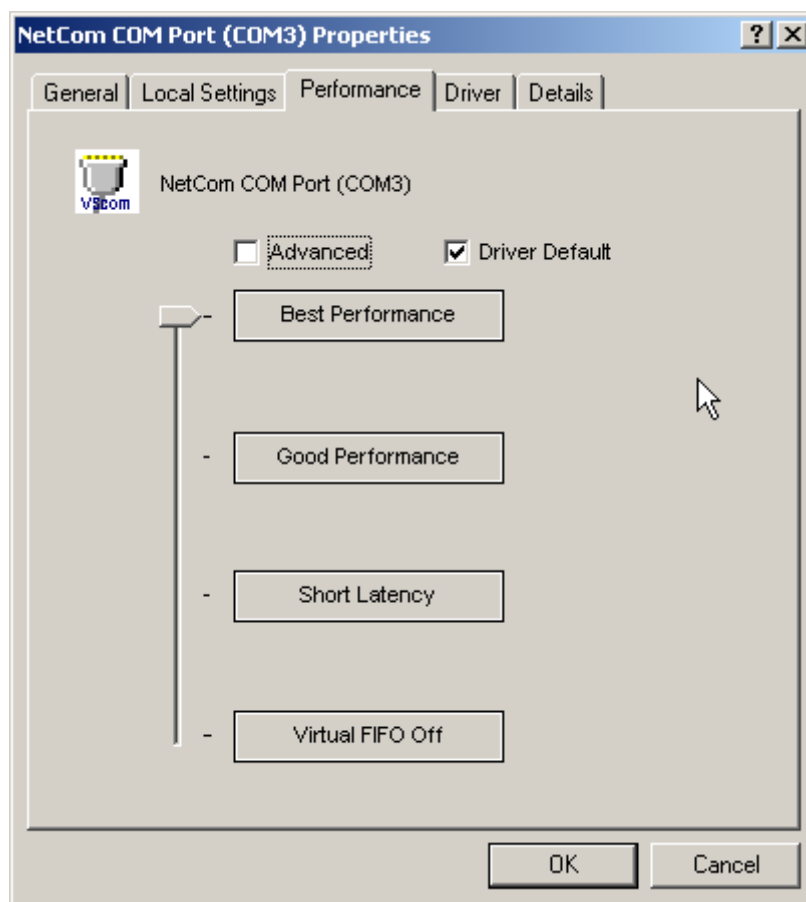


Figure 33: NetCom COM Port Performance Settings

Consequently the configuration starts on the **Performance** tab. There are four already defined sets of parameters.

Best Performance is the default configuration. The driver software and the NetCom communicate with big data blocks. As a result a reaction on short events on the serial port is somehow delayed. For applications operating with short data blocks, and waiting

for short answers this is not optimal. It causes transmission delays, called Latency.

Good Performance uses smaller blocks. The Latency may be reduced a little bit, depending on the application. But the impact on the data throughput is small.

Short Latency mimics a 16C550 with full FIFO enabled, but no network timeouts will occur. This means the block size is 16, quite small for network operations.

Virtual FIFO Off simulates a deactivated FIFO, which is the fastest setting in terms of latency. The port is configured as if the FIFO is off, buffers are configured to never wait for a timeout, hence gaining in best reaction times. The FIFO buffers are not deactivated in reality, they are still used to prevent data loss.

Driver Defaults returns to the standard settings when enabled.

Advanced opens access to detailed configuration of the operation parameters.

4.4.3 Network & Misc Properties

When you use the **Advanced** checkbox on the **Performance** tab, the **Network/Misc** tab opens automatically.

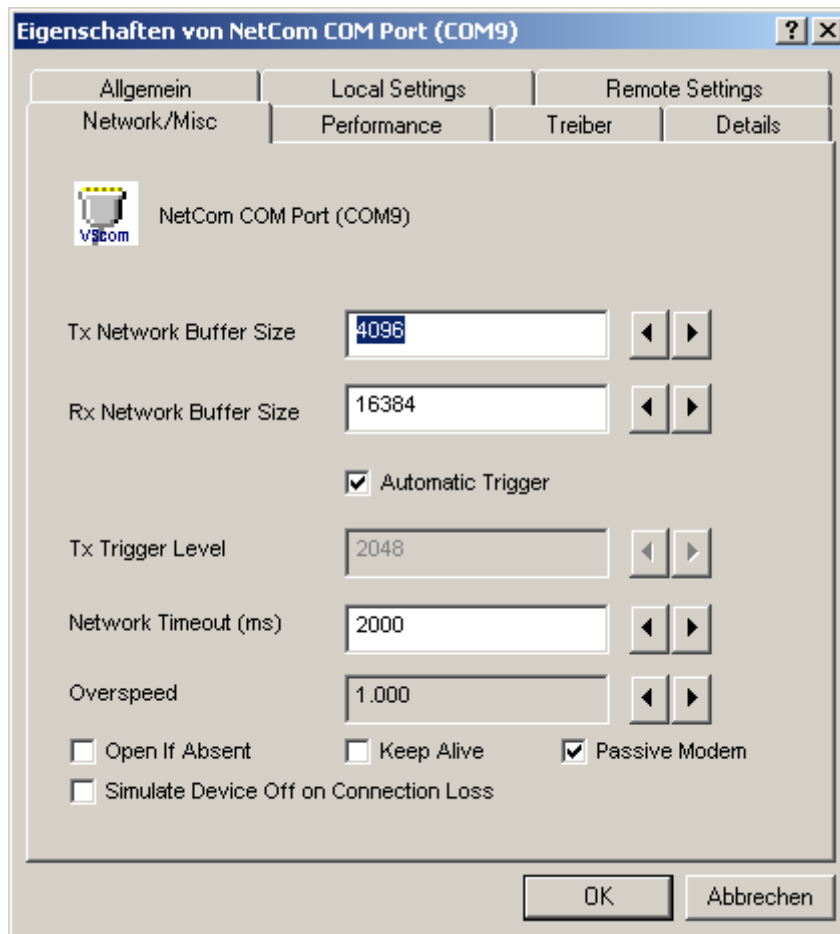


Figure 34: NetCom COM Port Network/Misc Properties

The parameters on this tab control the operation of the driver software on the computer.

Tx Network Buffer Size: If the application sends small chunks of data to the driver, these are buffered to send them in one large packet. This parameter defines the size of the buffer. And also the maximum packet size sent to the serial port by the driver software.

Rx Network Buffer Size: This is the size of the buffer to receive data from the NetCom.

Automatic Trigger: based on internal rules, this checkbox selects a best practice value for **Tx Trigger Level**. Deactivate it to control that parameter manually.

Tx Trigger Level: Controls the time when data is sent to the NetCom. If the Tx buffer holds at least this amount of data, the driver

immediately sends them. If there is less data, the driver may use a timeout to determine when to send them.

NetworkTimeout (ms): This is the timeout.

Overspeed: This is a special option, not really related to network communication. There are old applications, limited in the maximum speed. With Overspeed you define a multiplier. The baudrate requested by the application is multiplied with this factor. The result is sent to the NetCom to configure the serial port. E.g. the application may be limited to 38,400 bps, but there is a modem capable of 230,400 bps on the serial port. Set Overspeed to a value of 6.000, and configure the application to use 38,400 bps.

Open If Absent: The NetCom may be used from a computer with a Dial-Up connection. When this option is used, the driver will delay the connection to NetComs serial port. Even when an application opens the port and configures the parameters, no command is sent. The connection is established when data is sent to the NetCom, or when status information is requested.

Keep Alive: This option will periodically send control information to the NetCom to check if the connection is still operational. As a second effect a Dial-Up connection will not automatically close.

Passive Modem: This option controls how often the driver retrieves Modem status information from the NetCom. If activated, the driver never asks for the modem status. Instead the NetCom informs the driver of any changes. If an application frequently requests the Modem status, it gets the last value received. On slow networks like the Internet this option is recommended. If inactive, the driver software retrieves the Modem status from the NetCom serial port each time the application requests it, but with a maximum frequency of 10 per second. If the latest retrieved information is not older than 100 milliseconds, this value is returned.

Simulate Device Off on Connection Loss: When this option is enabled, the NetCom driver does not attempt to preserve transmitted data. If on a normal serial port the connected device is switched off, all data sent to this device gets lost. NetCom simulates this behavior. All data sent from the application to the driver is discarded, when the TCP connection to the NetCom is lost. The NetCom driver attempts to re-establish the connection in regular intervals. When the NetCom is available again, data may be transferred from then on.

4.4.4 Remote Settings Properties

The other panel created by activating the **Advanced** checkbox on the **Performance** tab, is the **Remote Settings** tab.

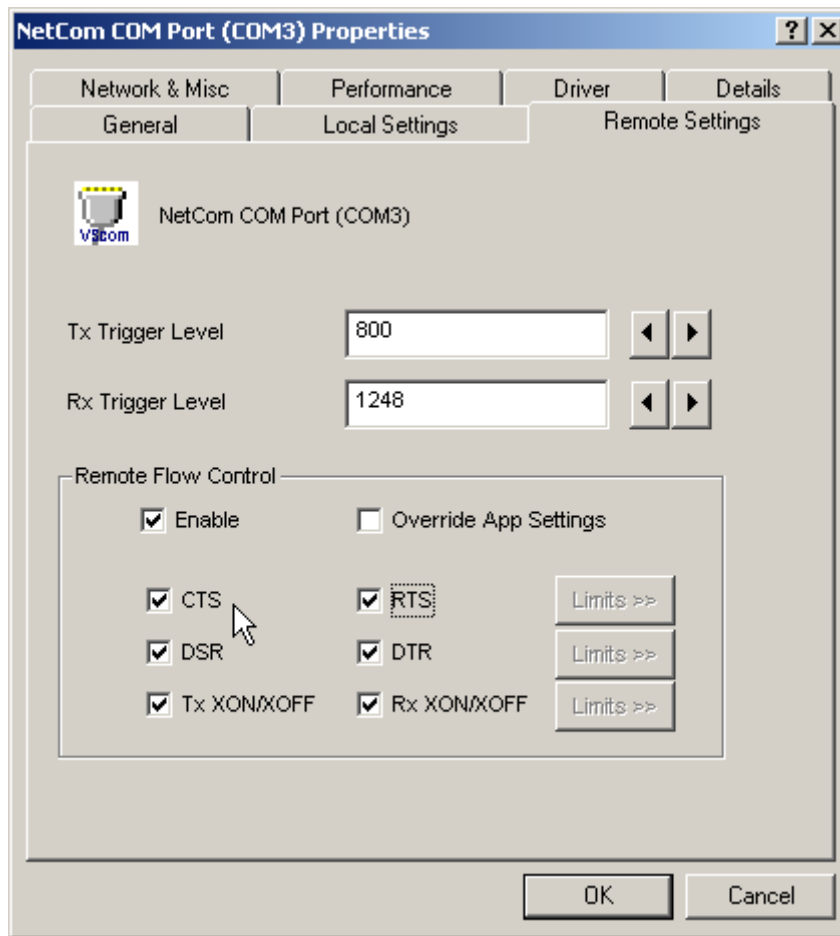


Figure 35: NetCom COM Port Remote Settings Properties

The parameters on this tab control the operation of the serial port on the NetCom Device. They are defined and activated by the driver software.

Tx Trigger Level: The serial port on the NetCom Device buffers data for transmission to external devices. If the amount of data in this buffer drops below this level, the NetCom is capable to receive new data. It will send a related event to the driver software.

Rx Trigger Level: When the serial port has received this amount of data, these are sent to the driver on the connected computer. If the amount is less than this, the NetCom applies a timeout of about 5 character times. This means the timeout varies with the serial transmission speed.

The **Remote Flow Control** panel signals the NetCom to perform the handshake on its own. This is necessary, because the network delay of some milliseconds is too long for reliable operation in many situations.

Enable: The configuration shown here is active, when the pre-defined performance levels are used. When using the ‘Advanced’ option, Remote Flow Control is completely disabled. Enable as required. While it is best practice to configure as figure 35, you can disable certain events here.

CTS, DSR, Tx XON/XOFF: these control the output of data to the serial port.

RTS, DTR, Rx XON/XOFF: used to stop transmission from the connected device.

An application has the option to use any combination of these methods at the same time. The command to use them is transferred to the NetCom. For example, if the port is configured to use Hardware Flow Control, the NetCom will control the RTS line, and observe the CTS line. If requested, any of these methods may be unchecked. In that case the driver software on the computer will control the lines.

Override App Settings: In rare situations it is necessary to ignore the applications configuration. Check this box, and select the Flow Control functions to use with the device.

Limits: These buttons are prepared for future software versions.

4.4.5 Installation of NetCom Servers

This section of the manual covers the correct installation of the drivers and serial ports. Please do a quick review of the section 4.1, before reading further. As of the time of writing, the current driver is version 1.5.12.0

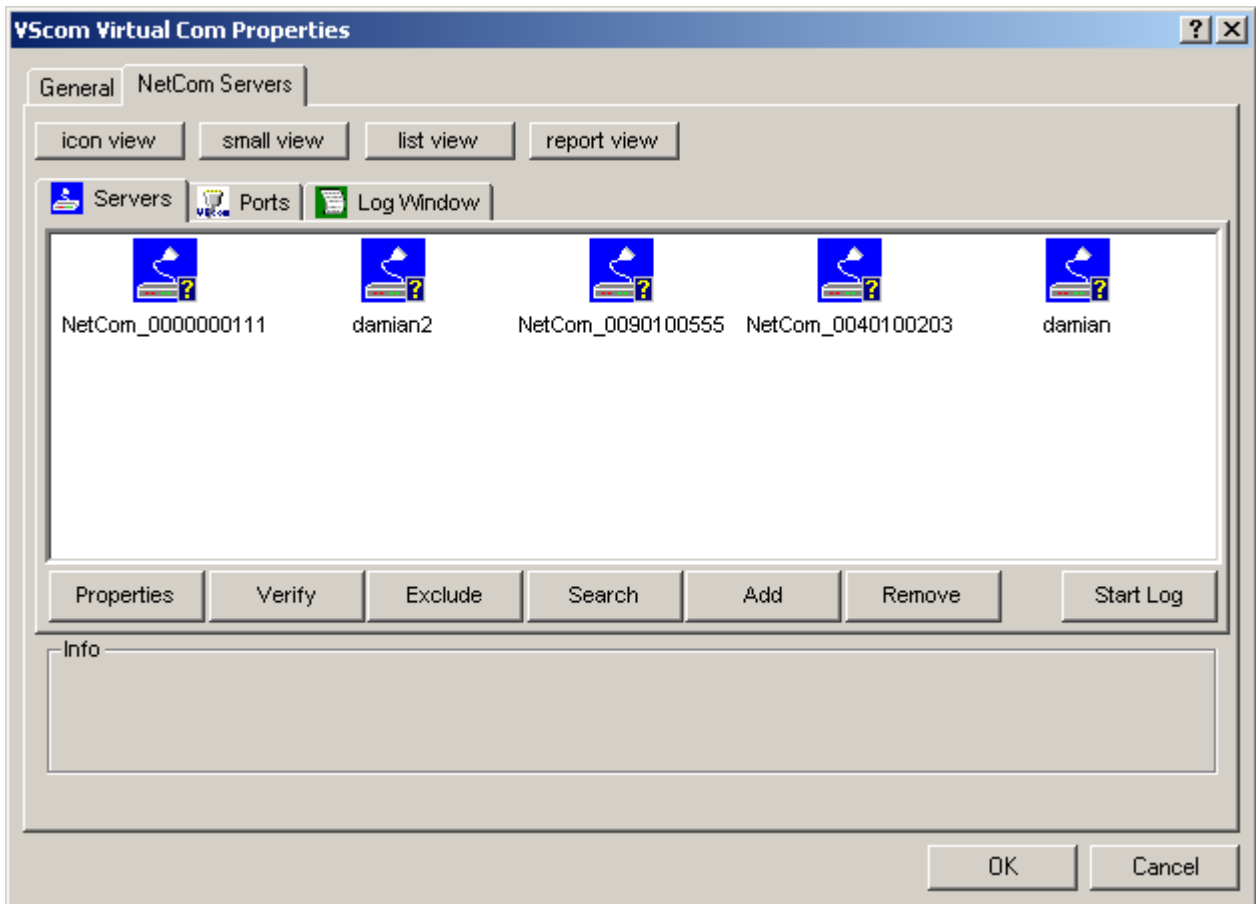


Figure 36: Select NetCom to install

The NetCom Manager program is started by the Installation Wizard. Often there are more than only one NetCom listed. And sometimes not all of them are to be used on this specific computer.

The **Exclude** button is used for that purpose. Select a NetCom Device, and click on that button. The driver will later ignore this NetCom, when installing and operating the serial ports. The Icon changes to olive color.

In figure 36 above you'll notice yellow questions marks at each icon. These appear when the NetCom is not already installed for the Virtual Com driver. It may also appear, if you open NetCom Manager without administrative privileges. If the mark changes to a red exclamation mark, the NetCom is non functional. It may be without power, the network may be broken, or the device is completely removed. Or the NetCom Manager is still without administrative privileges. To clear the display in NetCom Manager just select that NetCom and use the **Remove** button.



Figure 37: Excluded NetCom

If a NetCom has not been operational when the Manager program was started, it is either displayed with the exclamation mark, or not displayed at all. You may make it operational by connecting it now. To install it, use the button **Search** to find it in the network. Or **Add** it manually with that button (section 5.6).

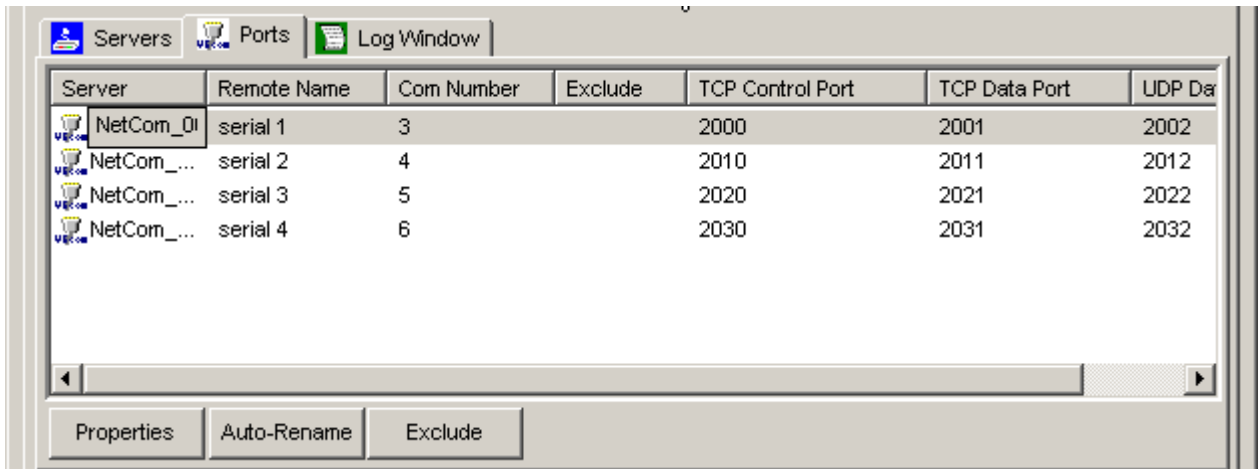


Figure 38: NetCom Manager Ports View

Similarly you may exclude certain ports on a specific NetCom Server from installation as a Virtual Com port.

These are the special options used while installing the driver software. At any time after installation the configuration may be changed by the NetCom Manager program. This may result in serial ports appearing in or vanishing from the system.

4.4.5.1 Changing the Installation There are common situations, when the current configuration needs a change. In the first case the NetCom has been moved to a different location, or the logical structure of the network has changed. It may happen the IP Address of NetCom is also changed. Either by Automatic (DHCP), or manually via a different interface like the Web browser. Because of the changed address the driver does not find the serial port to contact.

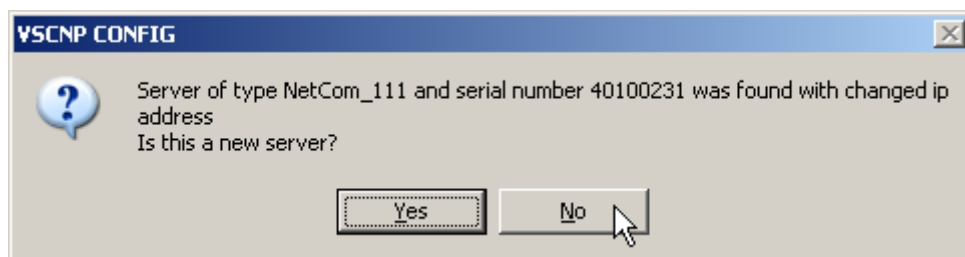


Figure 39: Reconfigured NetCom found

Now open the NetCom Manager. It will re-detect the devices. In this process the Manager finds the already installed NetCom, but with a new configuration. Then the Manager requests interaction from the user. This question here assumes the NetCom shall be installed from scratch. This will produce a Com port with a new number. If just a reconfiguration has occurred, click on **No**. When

you do that, the parameters of the installed Virtual Com Port are changed to contact the same serial ports on a new network address.

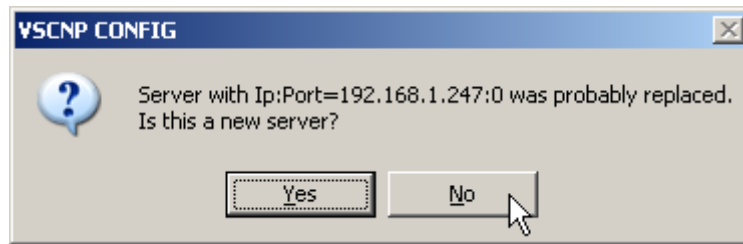


Figure 40: Replaced NetCom found

The second case occurs, when a NetCom is replaced by another device. This new device shall have the same configuration, especially the same IP Address. When you start the NetCom Manager, it will detect a new device with parameters already in the database. So a similar question appears. An installation of a new serial port is assumed again. If the device shall replace the old one, click on the **No** button.

In general the driver software and the NetCom Manager identify the NetCom Devices by the combination of IP Address and serial number. If one of these is changed, the above requests appear.

4.5 Uninstall the Drivers and Tools

To completely uninstall the NetCom Drivers and files, there are three methods. The usual way is to use the **Add/Remove Programs** applet in the Control Panel, and remove the NetCom Drivers. This will start the NetCom uninstallation program.

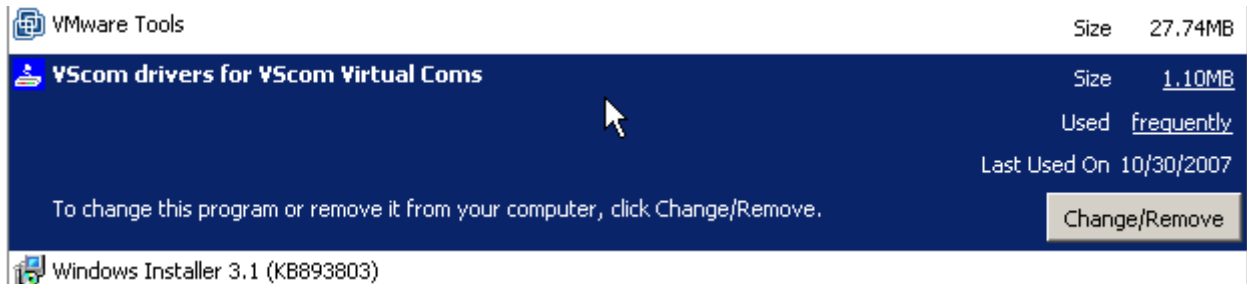


Figure 41: Uninstall NetCom Drivers via Control Panel

As a second way you may start the Uninstall program in the start menu. The third method is to start the Installation Wizard again from CD-ROM or the installation directory.

The Wizard will detect the drivers on the system. You have the options to **Repair** the current installation, or to **Remove** the installed drivers. Since the Installation Wizard is of the same version as the installed drivers, the option of **Update** is not available.



Figure 42: Uninstall NetCom Drivers in Start Menu

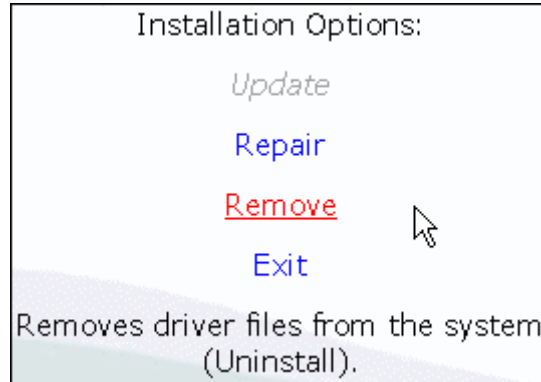


Figure 43: Remove, Repair

A **Repair** replaces the driver files on the system with those in the installation package. Since this is the same versions, the files should also be the same. If anything is damaged in the installed drivers, the Repair process will correct the problems.

As expected the **Remove** process will uninstall drivers and tools from the system. The drivers are removed from the configuration and also completely deleted from the System drive. This happens with any configuration data also. Afterward the system is available for a clean installation.

5 Configure with NetCom Manager

Shipped with the NetCom Devices there is a versatile program for Windows Operating System, named NetCom Manager. This program shall detect, manage and configure the NetCom Devices in your network. You can start it by several ways. First of all it is stored on the CD-ROM, named NETCOMMGR.EXE²³. It is possible to start it directly from the CD-ROM.

See this Icon. When the Virtual Com Drivers are installed, there are more options to run the program. In Windows NT the same Icon appears in the Control Panel, to start the NetCom Manager program.



Figure 44: NetCom Manager

Also the process of installing the drivers created a new program group in the Start Menu.

This section of documentation focuses on management of the NetCom Devices. The options to configure driver-specific parameters of the serial ports are skipped here. This includes some buttons and panels. They are described in total in section 4.4, in the documentation of the drivers and panels.

While in the configuration process, a click on a button or a double-click on an item opens properties or other options. In many situations, a right-click with the mouse opens context-sensitive options. Just try it out. The NetCom Manager is designed to help configure driver options. So for very detailed configuration of a NetCom, it is better to use the Web browser interface, or do it via Telnet as described in section 6. Here are the options.



Figure 45: NetCom Manager in Start Menu

²NETCOMMGRA64.EXE in x64 Editions of Windows

³NETCOMMGRNT.EXE on Windows NT

5.1 Starting NetCom Manager

When NetCom Manager is started, it will ‘Search’ the NetCom in your LAN by SNMP. This process may take up to 30 seconds. The devices in a LAN are typically found in the first seconds. If this is enough for you, you can stop the search by click on the ‘Done’ button.

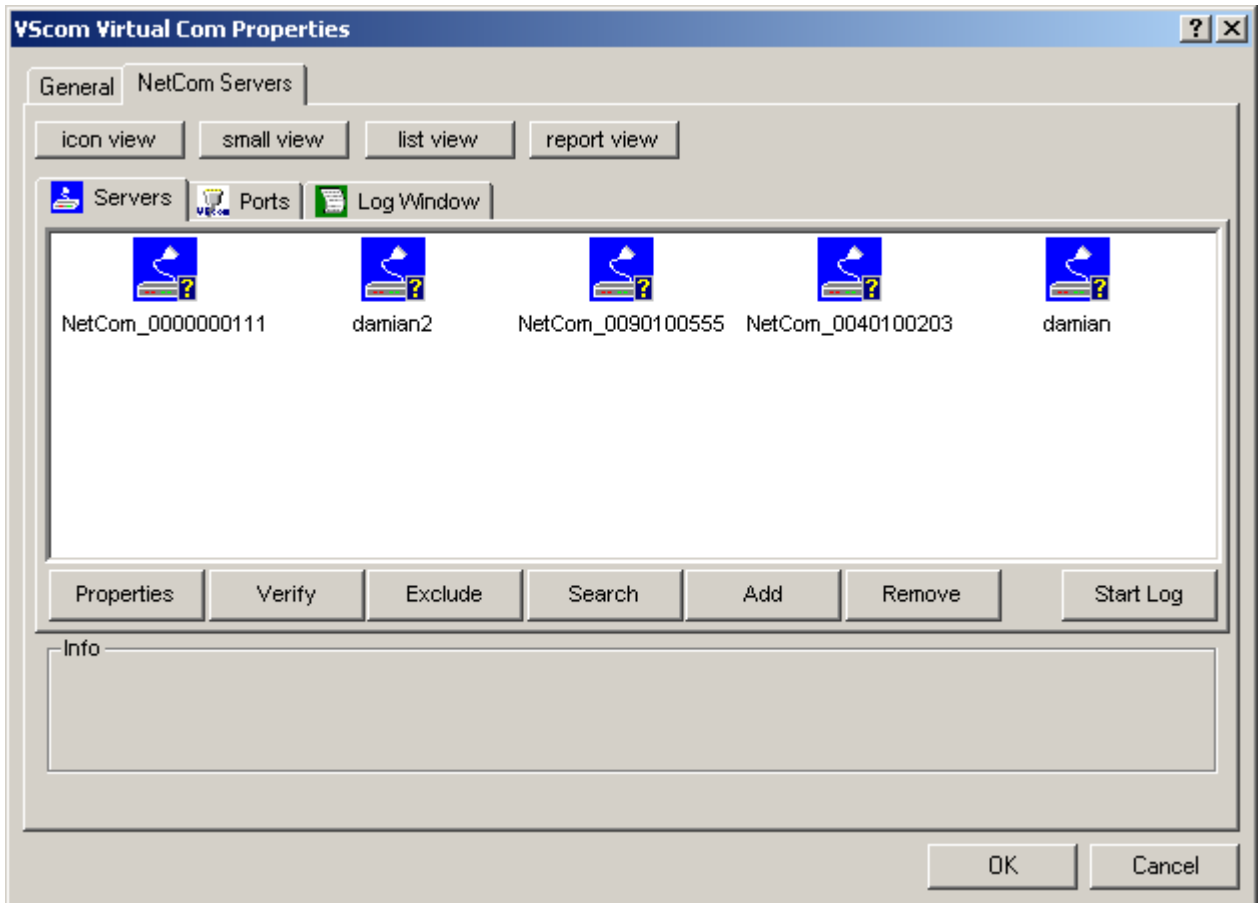


Figure 46: NetCom Manager Servers Panel

The NetCom are listed here in the **Servers** panel. Since the **Search** uses broadcast mechanisms, the range is limited. If you have Routers in your network, or you contact some NetCom via Internet, you must **Add** them manually (section 5.6). Enter the network parameters to access the NetCom.

Select a NetCom, and click on the **Properties** button, double-click the Icon, or use a right click. Using **Verify** the NetCom Manager contacts the NetCom to check if it is properly configured and online. **Exclude** is only useful in conjunction with the Virtual Com Drivers, so skipped here. **Search** repeats the search from the program start, and may be used at any time. **Remove** removes a NetCom server from this list. This option is most often used to clear old data from the drivers database. For monitoring purposes you may select a NetCom, and **Start Log** for this. It may be done for several Devices at the same time. The output is visible in the **Log Windows** panel.

5.2 NetCom Server Settings – Info

As described above, open the **Properties** of a NetCom Device. The Server Settings start with the **Info** panel. Configure the options as your network requires.

The screenshot shows the 'Info' tab of the NetCom Manager interface. The device is identified as 'NetCom_Demo_494'. The 'Network settings' section is active, with 'Use DHCP' checked. The IP address is 192.168.1.65, Netmask is 255.255.255.0, Broadcast is 192.168.1.255, Default gateway is 192.168.1.1, and Name server is 192.168.1.3. The Telnet port is set to 'telnet'. A mouse cursor is hovering over the 'DNS' label next to the IP address field.

Figure 47: NetCom Manager Server Settings - Info

The **Server Name** is just for information. As factory setting it includes the serial number of the device. You may change it to any string (of ASCII characters), since there is no functionality related to the name. This name is listed in the Server panel of NetCom Manager. The next parameters are fixed, and displayed for information only.

The **Telnet port** allows to configure this NetCom via Telnet. The value is a TCP port number. Factory setting is 23, the standard port for Telnet protocol. By default the NetCom is set to **Use DHCP** for automatic configuration of IP parameters. This is the suggested method. However there are several situations where this option can not be used. In this case deactivate it. When inactive, other parameters may be changed. The basic parameters **IP address** and **Netmask** are mandatory. Instead of an IP Address you may enter a **DNS** name. The NetCom Manager will resolve that name to the actual IP Address.

If address or netmask are changed, the NetCom Manager calculates a matching address for **Broadcast**. You may also change this address. The DHCP option will also configure the **Default gateway** and the **Name server**. Without DHCP you must enter these parameters by yourself, enter 0.0.0.0 if they are not used.

5.3 NetCom Server Settings – Ports

The **Ports** panel lists all serial ports of a NetCom. Some of the options are driver related, e.g. the **Com Number**. Each serial port may operate via two TCP ports.

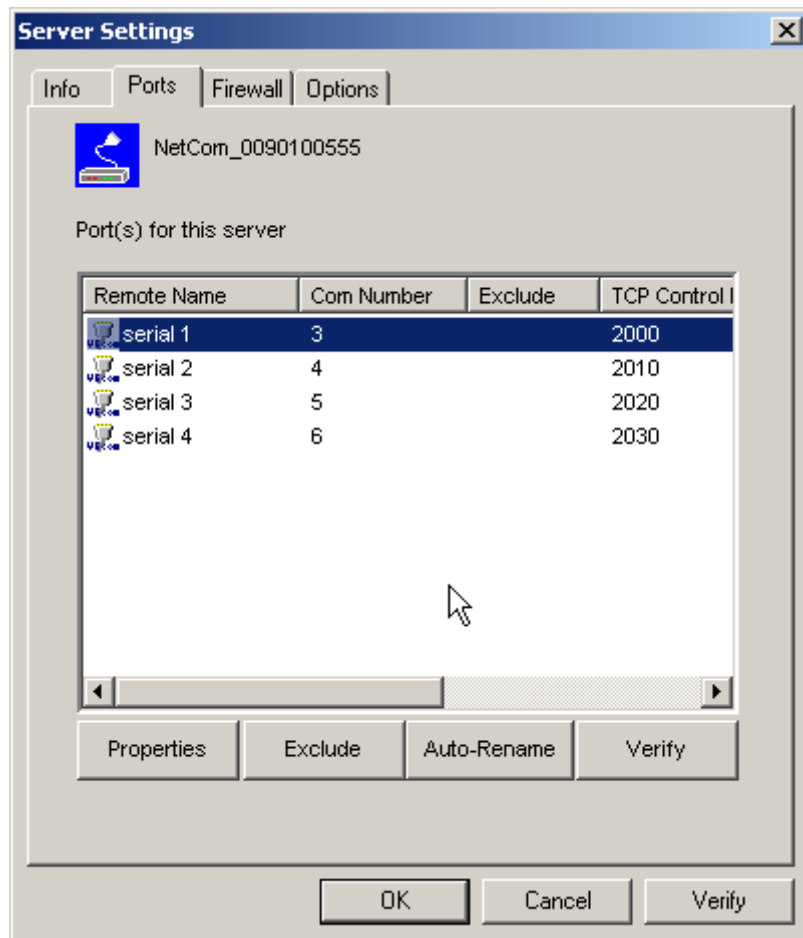


Figure 48: NetCom Manager Server Settings - Ports

The **TCP Control Port** is used in the Virtual Com Driver mode, and also in Null-Modem Tunnel. If Driver mode is not desired, this parameter is ignored almost always.

The **TCP Data Port** is used to transmit data to and from the serial port. Use the default, or change the value to the settings required for your network.

There is also a **UDP Data Port**, used in packet data transfer. You can not switch the NetCom to UDP mode with the Manager. But if it is already in this mode, you can change this basic parameter.

5.4 NetCom Server Settings – Firewall

Many networks use a Firewall to protect the stations in the network from other networks, including the Internet. In some situations the contact to a NetCom must pass through such a Firewall configured for NAT (Network Address Translation, section 13).

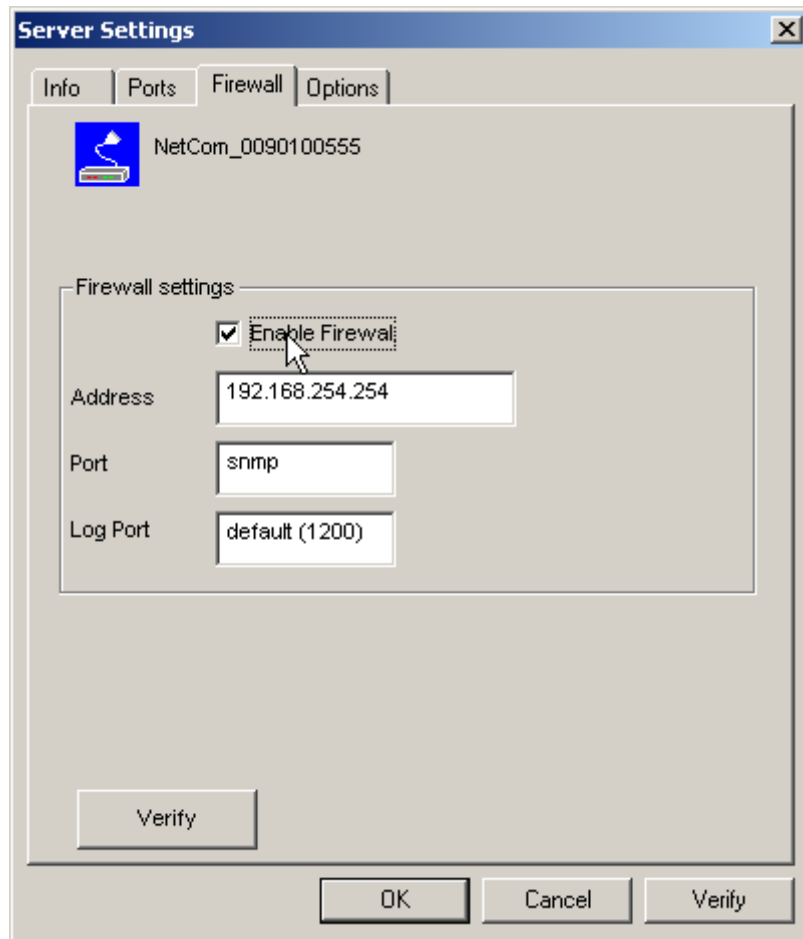


Figure 49: NetCom Manager Server Settings - Firewall

To do this you must **Enable Firewall**, and enter the **Address** of the Firewall. The address may be the IP Address, or the Qualified Domain Name (DNS).

The Manager configures a NetCom via SNMP, which uses UDP. The Firewall must have a special **Port** to receive those data, and to transfer it to the internal network. Enter this port here.

The same scheme applies to the logging option. When logging is active a NetCom listens on port 1200 for logging connections. The Firewall must also have a special **Log Port** to receive this connection, and to transfer it to the NetCom.

The NetCom does not need any configuration to operate in a Firewall protected environment. This configuration here is for installation of the drivers. There is a Firewall tutorial section later in this manual (5.7).

5.5 NetCom Server Settings – Options

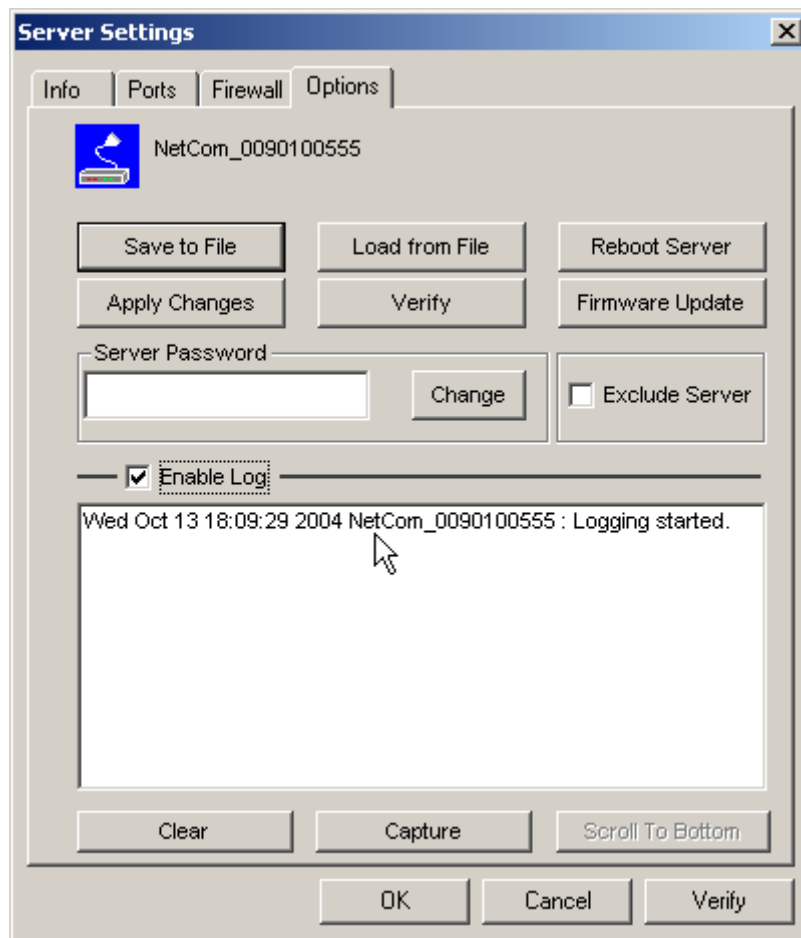


Figure 50: NetCom Manager Server Settings - Options

This Panel is available since software version 1.4.8.0, in this enhanced version. A **Save to File** of the configuration is available, as well as the opposing **Load from File** of this data. But this function is dedicated for the most basic parameters only. It is highly recommend to use the option to Save and Load the configuration via the Web Browser (paragraph [6.2.3.6 on page 101](#)).

You can also **Reboot** the NetCom. This may be useful, e.g. if an old connection blocks access to the NetCom.

The button **Apply Changes** commits all parameter settings done so far to the NetCom. And the **Verify** checks the current settings by reloading the status from the NetCom to the Manager program.

When you want to install a **Firmware Update**, use this button. But this option is designed for old firmware versions. It may operate with your device, it is still available for compatibility. But it is highly recommended to use the option via the Web Browser (paragraph [6.2.3.5 on page 101](#)).

The NetCom may be protected for access, in this case you must place the current **Server Password** in the dialog. The option to change the password is reserved for a future extension. **Exclude Server** is related to the Driver installation only.

You may **Enable Log** to see events at the NetCom, for monitoring. If enabled, the log will also appear in the central **Log Window**. At any time it's possible to **Clear** the log, or **Capture** the data to a file.

5.6 Manual Detection/Installation of a NetCom

Sometimes the NetCom Device Server can not be detected by the automatic in the NetCom Manager. To detect and configure devices the protocol SNMP is used. The detection is done by sending out a broadcast on all available network interfaces of your computer. This SNMP broadcast is realized as an Ethernet broadcast. Such a broadcast is only transmitted through Hubs and Switches. When there is a Router between the computer and the NetCom, probably the broadcast is not transmitted further. This is especially the situation when the NetCom is located somewhere via Internet, but also in big networks of some companies. If this is the case, the detection has to be done manually. Refer to figure 36 and **Add** the NetCom by use of the button. Enter the IP Address of the NetCom in the NetCom Manager Server Settings, and click the button **Verify**. Since now the IP Address of the NetCom is known, the NetCom Manager sends a request directly to this target, instead of a broadcast. This directed SNMP request is transported, even by Routers. The NetCom sends the normal reply, giving all required information to the NetCom Manager. Now it is possible to configure all options as usual. Also the drivers for virtual serial ports are installable now.

Please note, the drivers require to have the IP Address. They can not operate using a DNS name, because the driver can not perform a DNS name resolution. If your NetCom is located on a dynamic IP Address (e.g. on a Dial-Up connection with 24 hours disconnection), you need to reconfigure the driver installation, when the IP Address has changed. There is a NetCom Helper Service 5.8 for assistance.

5.7 Firewall Traversal Configuration

There are more difficult situations with a Firewall between the NetCom and the NetCom Manager. Many Firewalls protect the internal LAN by using the feature of NAT (Network Address Translation, 13). In this situation the IP Address of the internal device is not visible on the Internet. Only the Firewall can be contacted via its public IP Address. The NetCom Manager and the driver software for the virtual serial ports can handle such setups. But this requires certain configurations.

An easy-to-use alternative is provided with the NetCom PRO models. This implements a VPN to the NetCom PRO, which makes Firewall configuration quite easy.

5.7.1 SOHO Firewall example

The most easy situation for such a setup is by using a very simple SOHO Router as the Firewall. This configuration will show the principle of the technical details. Those principles can be transferred very easy to the configuration of more complicated installations.

On the SOHO Router there is only one public IP Address on the external side, and typically 254 internal private IP Addresses for the LAN side. These internal addresses may be assigned by DHCP or static. Such Routers offer a feature typically named "DMZ", which in fact is only a single exposed

host. It is recommended not to use the "DMZ" for several reasons, some of them are security related. Especially it is recommended not to configure a NetCom as the DMZ host.

5.7.2 SOHO Virtual Servers

The Router also offers "Virtual Servers" (here named ViServ for short), which is the option required for NetCom installation. These ViServ operate by a technique called PAT (Port Address Translation, 13). Certain data addressed to the public IP Address of the Router are forwarded to the internal private address of the NetCom. This way the NetCom can be contacted via the public IP Address of the Router.

First you need to configure the Router for some ViServs. As the absolute minimum there is one ViServ for the NetCom device itself, and another two ViServs for each serial port of the NetCom. Those ViServs are to be configured for TCP or UDP transmissions. Please read in the manual of your Router how to do that. You need a port for the external interface, and an IP Address plus a port for the LAN side. The LAN IP Address is of course that of the NetCom. As an example the most easy device is a NetCom 113 PRO. The internal port for SNMP is 161 for UDP. The serial port requires ports 2000 and 2001 for TCP.

Function	External port	Internal port
SNMP	8161/UDP	161/UDP
Control	9000/TCP	2000/TCP
Data	9001/TCP	2001/TCP

Table 16: SOHO Firewall Pass-Through

Configure your Router for these example ViServs, and use the internal IP Address of the NetCom for the targets. Connect the NetCom to your LAN. Now you are ready for a very first test. Use Telnet to connect to the Data port of the NetCom serial port. Open a console (DOS Box) and type the command

```
Telnet <Routers-IP-Address> 9001
```

You will be connected to the serial port. Every character you type is sent out of the serial port, and every received data is shown on your screen. The serial parameters are pre-configured in your NetCom.

5.7.3 NetCom Detection through SOHO Firewall

Now open the NetCom Manager as in section 5.6 above, and click the **Add** button. You again get the NetCom Manager Server Settings dialog. But now you have to select the panel named **Firewall** (see figure 49).

Check the Option **Enable Firewall**, and enter the IP Address of the Router in the **Address** field. In the field **Port** enter the target port for the SNMP configuration. From the Virtual Server example above this is port 8161. Since there is no configured ViServ for Logging, ignore this field. Click the button **Verify** to have the NetCom Manager contact the Router. This is a directed request, so there is no problem with broadcasts. The Router will transfer the request to UDP-Port 161 on the NetCom, which is the port for SNMP. The NetCom will answer the request, and send it out to

your computer. The NAT function in the Router will replace the source IP of the data by its own public value, so the NetCom Manager will see the answer come from the Router. The NetCom Manager is satisfied with this data.

Some ISP will block the SNMP protocol, which typically means they do not transport data for 161/udp to their customers (this is the first reason why port 8161 was used in the example).

This answer brings every required information about the NetCom, including its *internal* IP Address. Select the panel of NetCom Manager Server Settings to verify the information, but do not make any changes here. Changing the configuration may disconnect the NetCom from the protected LAN.

5.7.4 Serial Ports through SOHO Firewall

Now the NetCom is available in the NetCom Manager, but still the serial ports are not usable. The information of the TCP-ports for the ViServ related to the serial port is still missing. In the NetCom Manager Server Settings select the NetCom Manager **Ports** Panel. In this panel select one serial port, in this example of NetCom 113 PRO there is only one serial port. Click the **Properties** button to open the configuration of the port.

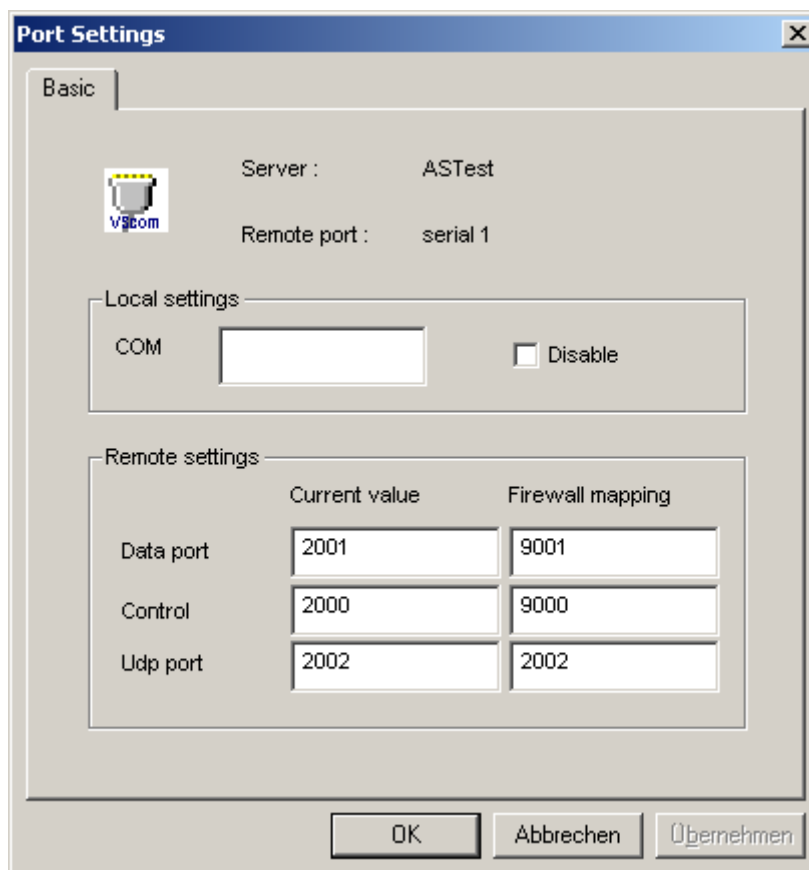


Figure 51: NetCom Manager Port Configuration for Driver

Since the Firewall function is enabled, the parameters for **Firewall mapping** are available for editing. Enter the ports defined in the Router, 9001 and 9000 in this example. Please note, so far there is no number for the Virtual Com Port available. The driver is not installed in this

moment, and Windows does not know about the available hardware. This will happen later in the installation. Click the **OK** button, and proceed with the driver installation as already described.

5.7.5 DMZ and Virtual Servers

Why is it recommended not to use the DMZ function of the Router? There are two reasons. The first one is simple, only one device in the LAN can be defined as the DMZ target. The DMZ is implemented as "Send all IP data targeted for the Router to the DMZ station, unless there is a specific rule for a different target". When a second NetCom shall be installed on the LAN, the Virtual Servers have to be configured anyway.

The second reason is the security. Using the "DMZ" option the Firewall in the Router becomes transparent. All data from outside is transferred to the LAN, including all malicious data. In general this is not an especially smart idea.

5.8 NetCom Helper Service

In certain situations users of VScom NetCom Serial Device Servers come to the problem of dynamic IP Addresses. This typically happens when the NetCom is used over Internet, using an ADSL or cable Modem connection. At certain times (e.g. every 24 hours) the NetCom is disconnected from the Internet. When it is re-connected, it will receive a new IP Address, which is different than before.

The NetCom Driver for Windows installs the serial ports on the NetCom Servers as virtual local Com Ports in the system. They are seen in the Device Manager, and standard applications like Hyper Terminal have a seamless access to the connected serial devices. To perform this task the driver uses the IP Address of the NetCom Server. On the established TCP connections the driver exchanges serial data, commands and status information.

When the IP Address of the NetCom has changed, the driver attempts to contact the old IP Address, which will fail. So the virtual Com Port is not usable any longer. Up to driver version 1.5.5 users have to use the NetCom Manager to reconfigure the driver.

Since the driver version 1.5.6 there are more options. The software installs a so-called Helper Service on the system. This service monitors the configured NetCom Servers, and detects the changed IP Address. The driver is reconfigured to use the new IP Address, so the port is usable again. This all happens without specific user interaction.

5.8.1 Configure Helper Service

The NetCom Helper Service is configured via NetCom Manager. There is a new Register card. In the upper part users **Enable** the Helper Service, and they also configure the **PollingPeriod** (i.e. frequency). If the Helper Service is disabled, it is also stopped in the system; it does not consume any system resources. Of course it does not provide any help when disabled. The **PollingPeriod** is given in seconds. When the interval has passed, the configuration of the NetCom Servers is checked.

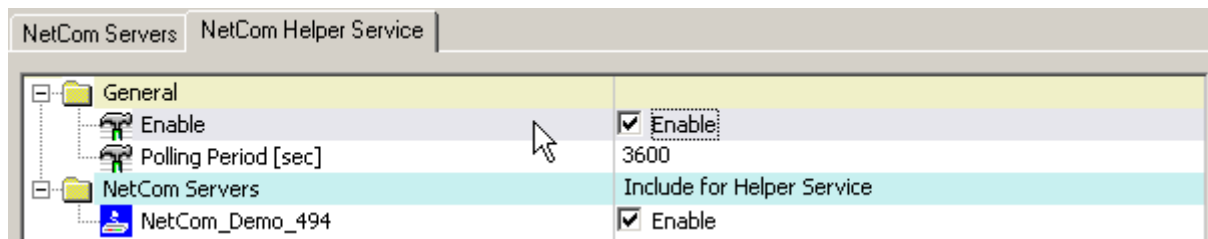


Figure 52: NetCom Helper Service

The lower part in the new panel lists all NetCom Servers available in the system configuration. The user must decide which of those shall be monitored (**Enable**). At the regular intervals as configured above the NetCom Server is checked. The Helper Service attempts to connect to the NetCom Server, and verifies the parameters. If the verification fails, the Service uses several methods to find and identify the NetCom Server.

5.8.2 Detection and Priority

The NetCom Helper Service has two basic methods to detect and identify a NetCom Server. The first method is the broadcast search on the network, the new method is DNS based. The DNS method has two variants, with or without firewall configuration. The reasons for changing IP Addresses or the methods to use are discussed later.

5.8.2.1 Broadcast Search The method of broadcast search is the same method as used in the NetCom Manager. A broadcast request is sent to the local network, and the NetCom Servers reply to this. The NetCom Manager lists them for configuration.

This method is used by the NetCom Helper Service also. A NetCom Server is identified by MAC-Address and Serial Number. These two parameters are fixed, customers can not change them. If a NetCom Server is found with a changed IP Address, the driver configuration is updated.

5.8.2.2 DNS based Search In driver versions up to 1.5.5 the NetCom Server has been configured by its IP Address. This is still the standard situation in later driver versions. However the Info Panel of Server Properties is modified (see figure 47). You may enter a Qualified Domain Name instead of the IP Address.

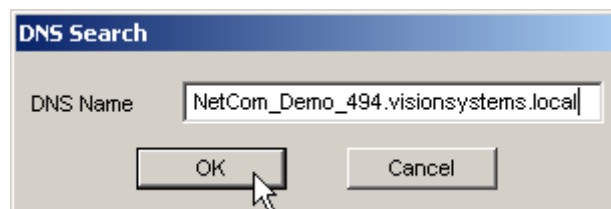


Figure 53: Enter Qualified Domain Name

The name is resolved, i.e. translated to the current IP Address associated with the name. This IP Address is configured in the driver, and the DNS name is also saved there.

In a local company network this may not be an especially useful option. But when the NetCom Server is used via the Internet, this is the standard situation for most applications.

DNS is used when the NetCom is not a part of the local network broadcast domain. As a consequence it is not detectable via the broadcast method described above. Provided there is a reliable DNS service available, now it is more easy to install a NetCom in the system. Please read about the Manual Detection/Installation of a NetCom in section 5.6.

The NetCom Helper Service regularly checks if the NetCom Server is still available on the known IP Address. If the attempt for contact fails, the Helper Service uses DNS to find the new IP Address of the NetCom Server. This new IP Address is used for future operation.

5.8.2.3 DNS based Firewall Configuration The NetCom Servers do not manage an Internet Connection on their own. But it is possible to have a NetCom Server on a public IP Address, when the Internet Connection is managed by Routers. More often the NetCom Server connects to a private LAN, and has a private IP Address. The Internet Connection is managed by a Router, which also acts as a Firewall. This Router uses NAT/PAT to make the NetCom Server available via Internet. Please read about this in section 5.7.

When the Firewall Configuration is activated for access to the NetCom, it has been possible to enter the DNS name of the NetCom Server in previous versions of the driver. Precisely it was the DNS name of the Router. This name has been resolved at the time of configuration, and has been stored for later use. Now the NetCom Helper Service monitors the DNS name to connect to the NetCom Server. If the connect fails, the DNS name is resolved again. The new result is used in the driver. The driver can again contact the firewall to get access to the NetCom and the serial ports.

5.8.3 Changed IP Address

There are several configurations with changed or regularly changing IP Addresses. This is a rough overview.

5.8.3.1 Broadcast Domain The broadcast domain is part of a local network. In typical SOHO networks the domain covers the entire network. The broadcast domain is typically limited by Routers. Broadcasts are transmitted between computer and NetCom Server, if there are only Switches/Hubs or WLAN Access Points on the way between those two.

Usually the IP Addresses in a local network are static. This is also the situation when there is a DHCP server, and all clients use this. If the server is configured properly, it will provide the same IP Address to a certain station again and again. It does so, because the stations are identified by their unique MAC-Address.

A changed IP Address may occur because the network is re-organized, combined with a reconfiguration of the DHCP server. In most cases however it is simply because the station has been switched off for a comparably long time. So the DHCP server forgot about the station, and provided the IP Address to a different target.

5.8.3.2 Internal DNS If the company network becomes larger, it will also use some Routers. For organization the network is grouped in subnets. As mentioned above, typically the broadcasts are blocked by Routers, so the broadcasts only cover a single subnet. To contact stations in other subnets the IP Address of the target is required. Usually this is provided by a DNS server. This server may co-operate with a DHCP server.

A usual cause for a changed IP Address in the NetCom Server is a connection to a different subnet. It will have a different IP Address there, but the DNS server should know about the new address.

5.8.3.3 Internet Some ISP disconnect the customers stations from the Internet in regular intervals, e.g. every 24 hours. If the station is configured for immediate re-connect, it will get a new IP Address. This station can notify a Dynamic DNS service, so this will resolve to the new address. This is typically combined with a SOHO Firewall/Router.

5.8.4 Polling Period

The last matter to check about is a suitable Polling Period for the NetCom Helper Service. The standard value is 3600 seconds, i.e. one hour. With this configuration a change in the address is noticed up to 60 minutes later. When the change occurs just before the Helper Service checks the connect, it will be recognized very soon, if the check happens just after the change, it will require the maximum time.

Usually an installation requires to have changes detected very soon, but this is not possible on networks. The NetCom Server has no feature to contact all clients, and notify them of a changed configuration. This is because the NetCom Server can not manage a possibly huge list of client computers.

So the Helper Service is installed on the client computers. If there are a lot of clients, very frequent polls cause a high load. For one side on the network, but most important on the NetCom Server. The best choice for a suitable polling interval depends on the usage period of the client computer. If it is unused for some hours per day (over night), it will detect a change at least the next morning. Provided the change happens over night.

If the NetCom Server uses an Internet connection with regular disconnects, it is a good idea to configure those disconnects to times of inactivity of the clients.

For manual detection of changes it is possible to restart the NetCom Helper Service. Controlling a service requires administrative privileges on the Windows system. A restricted user account can not do this. Restricted users use the Polling Period configured by the system Administrator.

5.9 Dynamic IP Address and OpenVPN™

Since Firmware version 2.2 there is a different method to provide a tunnel to the NetCom. The option of Encryption uses a Virtual Private Network (VPN) based on a single TCP connection between the NetCom and a client computer. Regardless of strong encryption or even weak as not encrypted, here the key point is the single TCP connection. It is more simple to provide a Firewall configuration for a single connection, so the Router Firewall is more easy to set up.

The network link established by OpenVPN™ requires to have a target address and a port number. Since the basic TCP connection is activated by the `openvpn.exe` program, there is the freedom of using a DNS name for the target device.

With a Dynamic IP Address for the NetCom site, one of the several Internet services for Dynamic DNS (DDNS) may help. It is even relatively simple to construct an own version. Using this service the `openvpn.exe` program gets the IP Address of the Firewall Router, and will establish the link. When the IP Address changes (after 24 hours), the connection first gets lost. OpenVPN™ will continuously attempt to connect again. When the new IP Address is known via DDNS, the network link is re-established. The NetCom is available again, because the IP Address on the OpenVPN™ link did *not* change. Even when a serial port has been open, the function will continue seamlessly.

6 Configure the Operation Modes

The NetCom Devices are often used without the installation of a driver software. Customer applications contact the NetCom directly, using network functions. These setups require independent configuration of the NetCom Device and the serial ports. There are five ways to do this configuration. The NetCom offers a Web browser interface, configuration via serial port, via Telnet and also via SNMP. This SNMP option is not covered in this manual, please see separate documentation. The NetCom Manager program for Windows is already explained above.

The access to the NetCom via web interface or Telnet are done via a TCP/IP connection between the computer and the NetCom. So users need the IP Address of the NetCom. The most easy way to retrieve this information is the NetCom Manager program (section 5). Start it, and open the Info Panel (figure 47) of the NetCom Server you want to configure. This panel displays the current IP Address of the NetCom. Do not change the parameters, just write down the value.

The default configuration of a NetCom is for use of a DHCP server. When such is not available, the IP Address defaults to 192.168.254.254. When the IP Address of the NetCom is not in final state, leave the NetCom Manager open while doing the first configuration of the NetCom Server. But in general the software may be closed as soon as the IP Address is known.

6.1 Accessing the Configurations

Here the manual shortly explains the different methods to get access on the parameters of a NetCom. These parameters are the same, independent from the method for configuration. So the options are described later.

The configuration is accessible via web browser, a Telnet software with VT100/VT52 emulation, or via a Terminal emulation connected to the first serial port of the NetCom .

6.1.1 Web Browser Configuration

Open your favorite web browser, and enter the IP Address as the target location. To avoid any confusion you should precede it with `http://`, so your browser has definite target information. Most browser programs do not need that. Your browser must not suppress images.

If the NetCom is password protected, you must enter this now. Leave the user name empty, just type the password.

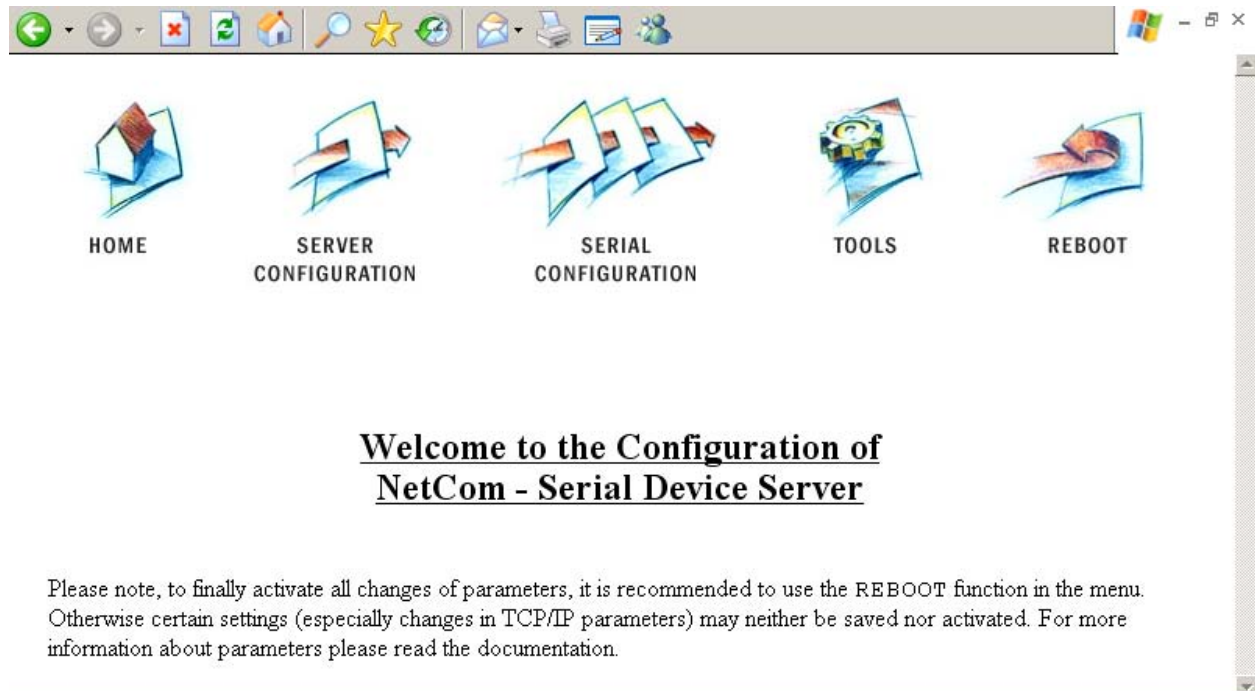


Figure 54: Configuration Menu in Web Browser

The NetCom welcomes you with its "Home" screen. To access the different options of configuration, the images above function as a link. In many menus you'll see a blue question mark. This is a symbol for help. When clicked a short explanation pops up, informing about the function of this parameter. Some other settings require a reboot to save and activate them. Whenever this situation occurs, the NetCom requests a REBOOT.

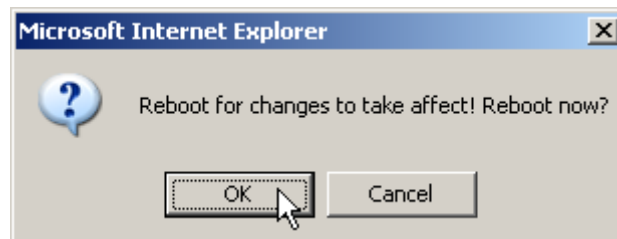


Figure 55: Request to Reboot in Web Browser

It is done like this here, you may reboot then, or do that later when the configuration is finished.

6.1.2 Telnet Configuration

Start your Telnet software with the IP Address of the NetCom as the parameter. In most configurations you use the standard port for Telnet, so you omit this parameter. As an example this is the command-line in Windows, which you may enter in Start⇒Run, or in a console (DOS box).

```
C:\Windows\System32>Telnet 192.168.254.254 23
```

For completeness the port is shown in this command. Enter the configured parameter when the port is different. If the NetCom is password protected, you need to enter the password right now.

```
Please enter your password: ■
```

Figure 56: Password Request in Telnet

When connected to NetCom you must define the type of terminal used. Most Telnet software includes an emulation of a VT100 terminal, so choose this option. Also choose this option for an ANSI emulation.

```
Please choose your terminal type (1:VT100 2:VT52 [1]): 1
```

Figure 57: Select Terminal Type in Telnet

The configuration with Telnet is menu-driven.

```
+----- NetCom - 123 WLAN V2.4.1 -----+
|  ServerConfig      SerialPorts      Tools      Save&Exit      |
+-----+

Server configuration settings

----- h=HELP -----
```

Figure 58: Main Menu of Configuration Console in Telnet

This is the start point for configuration. **ServerConfig** has all options to configure the NetCom device itself, including the IP-Parameters to access it. **SerialPorts** defines settings related to the serial port. **Tools** has some utilities like PING or displays statistics. In **Exit** you may leave the menu or reboot the NetCom . At any time you can get a short hint by typing "H" for help.

Use the cursor keys to select the parameter you want to change. Hit <Enter> to edit them. Type the new value, or select provided options. Use <Esc> to leave a parameter or menu. Please check the configuration of your Telnet, if there are any problems.

6.1.3 Serial Configuration

In some situations it may be impossible to get network access to the NetCom Device. If this happens (e.g. by an accidentally misconfiguration), neither Telnet, nor the web interface is functional. It may be even impossible to use the NetCom Manager program.

In this case you must connect to the NetCom via the serial port. Disconnect any serial cable from NetCom. Set the DIP Switches to "RS 232 Configuration" (all switches to Off, section 3.1). Then connect the NetCom with your computer using a Null Modem cable. If your NetCom is an old model with a connector DB9 female, attach the supplied Null-Modem Adapter to the port first. Or connect your computer to the female connector with a straight-through cable.

Open any serial terminal program (Hyper Terminal, minicom, PuTTY⁴, ...), select 38400 bps, 8 Bit, No Parity as configuration. Set your terminal to emulate a VT100 (recommended, but VT52 is also possible), including the Arrow keys.

Then power on the NetCom. When connected to NetCom you must define the type of terminal used (VT100 or VT52), and optionally provide the password. This is the same configuration option as described above at 6.1.2, so follow the instructions for Telnet.

When the configuration is done, change the DIP Switches back to normal operation. Later configurations can be done by web interface or Telnet. Of course this requires to have a functional IP configuration defined.

6.2 NetCom Configuration Options

Some of the menus are very long, especially on the web interface. These are divided in their logical sections throughout this document. Each section shortly mentions the way to access the parameters. Short screen shots show the typical display when configuring the NetCom. Usually the web interface is shown on top, and the terminal interface (Telnet, serial port) is shown below; a horizontal line divides the two. On few occasions the two screen shots are displayed side by side, with the web interface to the left and the terminal interface to the right; then divided by a vertical bar.

6.2.1 Server Configuration

In your web browser click on the Icon of "SERVER CONFIGURATION", the browser opens the basic server information, the server parameters related to the IP-configuration, the parameters for Wireless communication, the section for encrypted communication, Password settings, and finally the configuration for date and time.

In Telnet the **ServerConfig** offers the IP parameters, Wireless and encrypted configuration, Password settings, configuration for date and time, as well as basic server information.

⁴Download PuTTY from putty.org

6.2.1.1 Server Info

Web: menu “SERVER CONFIGURATION”, section “Server Info”.

Telnet: “ServerConfig”, option “Info”

Server Info	
Server Type	423 WLAN
Software Version	2.4.1
Hardware Version	1.0
Serial Nr.	0210100424
UpTime	3 day(s) 02:05:32
Contact ?	<input type="text" value="<unset>"/>
Location ?	<input type="text" value="<unset>"/>

<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; padding: 2px;">ServerConfig</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">+-----+ Parameter Wireless OpenVPN Authentication Date & Time Info +-----+</td> </tr> </tbody> </table>	ServerConfig	+-----+ Parameter Wireless OpenVPN Authentication Date & Time Info +-----+	<table style="width: 100%;"> <thead> <tr> <th colspan="2" style="text-align: center; padding: 5px;">Server Info</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Server Type</td> <td style="padding: 5px;">423 WLAN</td> </tr> <tr> <td style="padding: 5px;">Software Version</td> <td style="padding: 5px;">2.4.1</td> </tr> <tr> <td style="padding: 5px;">Hardware Version</td> <td style="padding: 5px;">1.0</td> </tr> <tr> <td style="padding: 5px;">Serial Nr.</td> <td style="padding: 5px;">0010100454</td> </tr> <tr> <td style="padding: 5px;">UpTime</td> <td style="padding: 5px;">3 day(s) 02:10:17</td> </tr> <tr> <td style="padding: 5px;">Contact</td> <td style="padding: 5px;">[<unset>]</td> </tr> <tr> <td style="padding: 5px;">Location</td> <td style="padding: 5px;">[<unset>]</td> </tr> </tbody> </table>	Server Info		Server Type	423 WLAN	Software Version	2.4.1	Hardware Version	1.0	Serial Nr.	0010100454	UpTime	3 day(s) 02:10:17	Contact	[<unset>]	Location	[<unset>]
ServerConfig																			
+-----+ Parameter Wireless OpenVPN Authentication Date & Time Info +-----+																			
Server Info																			
Server Type	423 WLAN																		
Software Version	2.4.1																		
Hardware Version	1.0																		
Serial Nr.	0010100454																		
UpTime	3 day(s) 02:10:17																		
Contact	[<unset>]																		
Location	[<unset>]																		

Figure 59: Server Information

Information about the selected NetCom is displayed as “Server Info”. Starting with the **ServerType**, this is the model of the NetCom, followed by the **SoftwareVersion** and **HardwareVersion**. This will give a rough overview, which features are implemented, or need an upgrade of the firmware. The **SerialNr.** is important to identify the device you are configuring right now. For further information the **UpTime** is listed.

Contact and **Location** are user-defined information. They may later help to find the device in the installation, and the person responsible for management. The Administrator may provide some contact information here.

Contact defines a person to contact for help, e.g. "Mrs. Jane Doe, 555-HELP". **Location** is the physical place of the NetCom, e.g. "CeBIT Hall 12, Service Box IX.a". These data are restricted to ASCII characters.

6.2.1.2 Server Parameter

Web: menu “SERVER CONFIGURATION”, section “Server Parameter”.

Telnet: “ServerConfig”, option “Parameter”

The **Server Parameter** allow configuration of the NetComs name and of course all parameters in IP-settings. The **Server Name** is used as general information, e.g. in the NetCom Manager program. On a NetCom WLAN you may choose the network **InterfacePriority** as Cable, Wireless or both (priority Cable,Wireless or Wireless,Cable).

Server Parameter	
<u>Warning: for changes like network settings the server must be rebooted</u>	
Server Name ?	<input type="text" value="NetCom_0210100424"/>
MAC Address	<input type="text" value="00:04:D9:80:3A:9D"/>
Options ?	<input type="text" value="auto"/>
Interface Priority ?	<input type="text" value="Cable, Wireless"/>
DHCP ?	<input type="text" value="Disabled"/>
IP Address ?	<input type="text" value="192.168.1.243"/>
Netmask ?	<input type="text" value="255.255.255.0"/>
Broadcast ?	<input type="text" value="192.168.1.255"/>
Gateway ?	<input type="text" value="192.168.1.1"/>
DNS ?	<input type="text" value="192.168.1.3"/>
Domain ?	<input type="text" value="visionsystems.de"/>
ConfigPort ?	<input type="text" value="23"/>
PrintServerPort ?	<input type="text" value="515"/>
KeepAlive ?	<input type="text" value="Off"/>
KeepAliveInterval ?	<input type="text" value="0"/>

Figure 60: Server Parameter Web Interface

ServerConfig		Server Parameter	
Parameter		Server Name	[NetCom_0051100021]
Wireless		MAC Address	00:04:D9:80:00:14
OpenVPN		Options	auto
Authentication		Interface Priority	Cable, Wireless
Date & Time		DHCP	Enabled
Info		IP Address	192.168.1.81
		Netmask	255.255.255.0
		Broadcast	192.168.1.255
		Gateway	192.168.1.1
		DNS	192.168.1.3
		Domain	netcom.vicom.com.tw
		ConfigPort	[23]
		PrintServerPort	[515]
		KeepAlive	Off
		KeepAliveInterval	[0]

Figure 61: Server Parameter Telnet Interface

The **Options** first implemented in firmware version 2.6.4 define the operation mode of the Ethernet Interface. The details are explained below.

Manual changes of IP parameters are only available with **DHCP** set as **Disabled**. When DHCP is not used, enter **IP Address** and **Netmask**, as well as the **Broadcast** address. **Gateway** is required, if there are Routers in the network. **DNS** is used to access other stations by name. The **ConfigPort** is used to access the NetCom for administration via Telnet. It is suggested to use the standard value for Telnet, TCP port number 23. However it may be changed for different purposes. This does not change the function of the Telnet menus.

Firmware version 2.2 introduces the new function as Print Server. The TCP Port defined by RFC1194 (mostly referred to as »Line Printer Daemon«) is 515, under certain circumstances you may change the **PrintServerPort**. More about Print Server function at the configuration of the serial ports ([6.2.2.2.8 on page 91](#)).

KeepAlive is an intrinsic function of the TCP/IP protocol. If used it causes network traffic, traditionally intended to prohibit automatic shut-down of Dial-Up network equipment. In a LAN this traffic usually is not a problem. If this function is **On**, you must define a **KeepAliveInterval** given in seconds. As a side effect of the traffic network problems are detected earlier. NetCom has a better chance to react on network problems, or failed hosts. Even dropping an old connection may be useful in certain environments. It is suggested to activate this function when using RAW TCP communication ([6.2.2.2.2](#), [6.2.2.2.3](#)), with an interval of about 180 seconds.

The **Options** for Ethernet allow to control the network operation mode by configuration, overriding the automatic negotiation of the hardware.

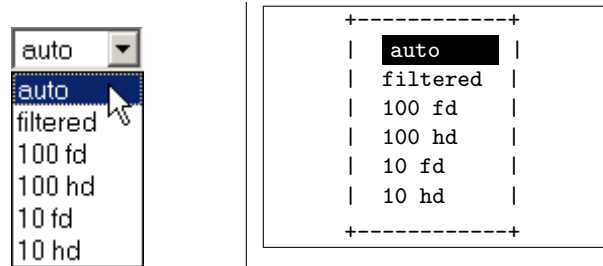


Figure 62: Ethernet Operation by Software

auto is the standard operation. The Ethernet port automatically detects the capabilities of the connected device, and adjusts to the best possible communication.

filtered is not recommended. Useful in certain networks, activate on explicit instruction.

100 fd configures for communication at 100 Mbit/s in Full Duplex mode. This is best possible, and usually configured without special configuration.

100 hd configures for communication at 100 Mbit/s in Half Duplex mode. Normally not advised, used if the automatic detection fails.

10 fd configures for slow communication at 10 Mbit/s in Full Duplex mode. For connection to old network hardware, if this is not detected.

10 hd configures for slow communication at 10 Mbit/s in Half Duplex mode. For connection to very old network hardware, like Thin or Yellow cable. Not recommended.

6.2.1.3 Wireless Parameter

Web: menu “SERVER CONFIGURATION”, section “Wireless Parameter”.

Telnet: “ServerConfig”, option “Wireless”

This section is of course only available on the NetCom WLAN class of devices. To operate a Wireless device, a lot of parameters are required. The configuration in the NetCom is reduced to a small set of them, for ease of configuration.

Wireless Parameter

Chipset	Ralink RT2561T
SSID	NetCom_0210100432
OperationMode	Ad-hoc
WirelessMode	11 b+g
CountryRegion	ETSI (1-13)
Channel	7
Encryption Type	WPA2
Encryption Key
RTSThreshold	2312
FragmentationThreshold	2312

<pre> ServerConfig +-----+ Parameter Wireless OpenVPN Authentication Date & Time Info +-----+ </pre>	<pre> Chipset Ralink RT2561T SSID [NetCom_0000123456] OperationMode Ad-hoc WirelessMode 11 b+g CountryRegion ETSI (1-13) Channel 7 Encryption Type Off Encryption Key [empty] RTSThreshold [2312] FragmentationThreshold [2312] </pre>
--	---

Figure 63: Wireless Parameter

The **Chipset** is provided as a read-only parameter. This defines the hardware base for the WLAN functions. The first models of NetCom WLAN used the RT2560. Current models are equipped with RT2561T, which provides the additional WPA2 encryption. Later models may have different hardware, possibly providing more WLAN functions.

SSID is the «Service Set Identifier». This is used to get access to radio cells established by an Access Point. By default it is used as identification in Ad-hoc mode, and built from the serial number. This means it is the same as the default NetComs name.

The **OperationMode** is selectable as **Ad-hoc** for a direct connection from wireless stations to other stations, and also as **infra** to select the «Infrastructure Mode». The second mode is required to connect to an Access Point. Other wireless stations such as a PC or Laptop use the Access Point to transfer the data to the NetCom.

The **WirelessMode** is available as 11b and 11b+g. It may be necessary to use the restriction of 11b when compatibility problems with other clients occur.

WLAN as of IEEE 802.11b/g defines fourteen possible channels (i.e. predefined frequencies) to use with WLAN devices. Some of these frequencies are restricted in some countries. Please check with your local regulations for the channels you are entitled to use. This manual is just informative, it is in no way a reproduction of local regulations. The available **CountryRegion** values are FCC(1-11) for North America, ETSI(1-13) for Europe in general, SPAIN(10-11), FRANCE(10-13) and MKK(14) in Japan. Late information indicate even in Spain and France the full range of ETSI is now legal; check yourself. In Infrastructure Mode the NetCom adapts to the configuration of the Access Point. Be sure to have the correct Country/Region to match the parameters of the Access Point. The Access Point must broadcast the SSID, otherwise the NetCom will not contact it.

The **Channel** is used in Ad-hoc mode. Depending on the Country Region the selection is restricted. In Infrastructure Mode this value is defined by the Access Point.

EncryptionType defines the encryption of the radio transmission. It may be Off, WEP, WPA-PSK/TKIP or WPA2.

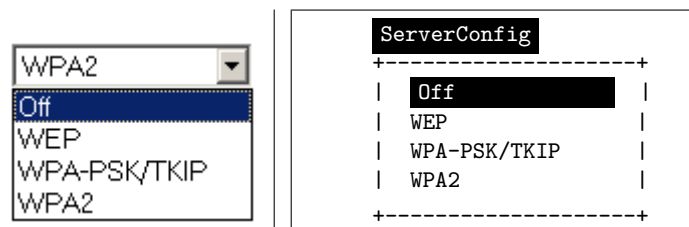


Figure 64: Wireless Encryption Modes

The WEP encryption may use 40 or 104 bit keys, sometimes also named WEP40/64 or WEP104/128. Which of this is required is defined by the **EncryptionKey** Parameter. This key may be entered as ASCII characters, or as hexadecimal for a binary key. A string with 5 characters results in WEP40 using an ASCII key. Using 10 characters as key defines this key as also WEP40, but with a binary key in hexadecimal notation. Likewise a 13 character string is WEP104 with ASCII, and 26 characters select WEP104 with a binary key.

WPA Encryption is available using TKIP cypher. The key is PSK (a Pre-Shared Key) and must be installed on all stations. An ASCII key consists of 8 to 63 characters, a binary key are 32 bytes in hexadecimal (64 characters) notation.

WPA2 Encryption is provided in firmware version 2.6, the cypher is AES. The key is similar as with WPA, i.e. 8 to 63 characters, or 32 bytes.

It is recommended to use WPA/WPA2 with a binary key, generated from random data. As with all encryption options a strong key is required for protection. [6.2.1.4.1 on page 75](#) provides a little help and background information.

RTSThreshold and **FragmentationThreshold** are low level WLAN parameters. They should match the configuration in the Access Point. Higher values result in better data throughput. But when transmission errors occur, the impact is dramatic. In this case lower values provide better security and better performance. The configured values shall match those configured in the Access Point.

6.2.1.4 Encrypted Communication

Web: menu “SERVER CONFIGURATION”, section “OpenVPN Parameter”.

Telnet: “ServerConfig”, option “OpenVPN”

Firmware version 2.2 introduces a way for encrypted communication with the NetCom PRO Serial Device Server. This function establishes an encrypted VPN tunnel between your computer and the NetCom. All communication to the NetCom uses this new connection. No application requires a change of operation or source code, but seamlessly gets the advantages of Encryption. This may be especially useful to get secure communication via an otherwise insecure Wireless LAN.

To build this tunnel NetCom uses the Open Source product OpenVPN™ (<http://openvpn.net>). This section is about the configuration of the parameters on the NetCom side. The function and the configuration of OpenVPN™ is described with more details later in section 9 on page 121 of OpenVPN™ Client installation.

OpenVPN Parameter

OpenVPN ?	<input type="text" value="Disabled"/>
TCP Port ?	<input type="text" value="1194"/>
IP Address ?	<input type="text" value="192.168.127.254"/>
Netmask ?	<input type="text" value="255.255.255.0"/>
Broadcast ?	<input type="text" value="192.168.127.255"/>
Max.Clients ?	<input type="text" value="8"/>
Cmd.Line Params (Server) ?	<input type="text"/>
TCP Port (Destination) ?	<input type="text" value="1194"/>
IP Address (Destination) ?	<input type="text" value="0.0.0.0"/>
Cmd.Line Params (Client) ?	<input type="text"/>
Encryption ?	<input type="text" value="AES-256-CBC"/>
Logging ?	<input type="text" value="Off"/>

Configuration-Settings of the Encryption-Key

ServerConfig																															
+-----+																															
Parameter																															
Wireless																															
OpenVPN																															
Authentication																															
Date & Time																															
Info																															
+-----+																															
	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">OpenVPN</td> <td style="width: 50%;">Disabled</td> </tr> <tr> <td>TCP Port</td> <td>[1194]</td> </tr> <tr> <td>IP Address</td> <td>[192.168.127.254]</td> </tr> <tr> <td>Netmask</td> <td>[255.255.255.0]</td> </tr> <tr> <td>Broadcast</td> <td>[192.168.127.255]</td> </tr> <tr> <td>Max.Clients</td> <td>[8]</td> </tr> <tr> <td>Cmd.Line Params (Server)</td> <td>[]</td> </tr> <tr> <td>TCP Port (Destination)</td> <td>[1194]</td> </tr> <tr> <td>IP Address (Destination)</td> <td>[0.0.0.0]</td> </tr> <tr> <td>Cmd.Line Params (Client)</td> <td>[]</td> </tr> <tr> <td>Encryption</td> <td>None</td> </tr> <tr> <td>Logging</td> <td>Off</td> </tr> <tr> <td></td> <td style="text-align: center;">[Generate Key]</td> </tr> <tr> <td></td> <td style="text-align: center;">[Upload Key]</td> </tr> <tr> <td></td> <td style="text-align: center;">[Stored Key]</td> </tr> </table>	OpenVPN	Disabled	TCP Port	[1194]	IP Address	[192.168.127.254]	Netmask	[255.255.255.0]	Broadcast	[192.168.127.255]	Max.Clients	[8]	Cmd.Line Params (Server)	[]	TCP Port (Destination)	[1194]	IP Address (Destination)	[0.0.0.0]	Cmd.Line Params (Client)	[]	Encryption	None	Logging	Off		[Generate Key]		[Upload Key]		[Stored Key]
OpenVPN	Disabled																														
TCP Port	[1194]																														
IP Address	[192.168.127.254]																														
Netmask	[255.255.255.0]																														
Broadcast	[192.168.127.255]																														
Max.Clients	[8]																														
Cmd.Line Params (Server)	[]																														
TCP Port (Destination)	[1194]																														
IP Address (Destination)	[0.0.0.0]																														
Cmd.Line Params (Client)	[]																														
Encryption	None																														
Logging	Off																														
	[Generate Key]																														
	[Upload Key]																														
	[Stored Key]																														

Figure 65: OpenVPN Network Parameter

Of course **OpenVPN** may be **Disabled**, active as **Server** or in the combined **Server-Client** mode. When the function is active, the NetCom is virtually invisible on the IP Address defined in "Server Parameter" (6.2.1.2). It will still answer on ICMP, and also the Logging function is available for trouble shooting. But there is only one connection accepted by the NetCom, to the **TCP Port** defined for OpenVPN™.

Nothing more is available for security reasons.

The **IP Address** is the local address on the VPN, it should be a private address ([RFC 1918](#)). This VPN also has a **Netmask** and a **Broadcast** address, this is similar to the configuration of the "Server Parameter". The Limit of **Max.Clients** specifies how many stations may establish simultaneous connections to the NetCom; it does not limit the number of installed clients.

The field of **Cmd.Line Params (Server)** is available since Firmware version 2.6.2, and accepts commandline parameters to openVPN in server mode. Users with deep knowledge about openVPN may add special configuration here, The content is not checked by the firmware, so check many times for avoiding a malfunction.

If **OpenVPN** is configured for **Server-Client** mode, it will establish a connection to a given Server, e.g. another NetCom PRO. The **TCP Port** and the **IP Address** of the Destination are required.

The field of **Cmd.Line Params (Client)** is available since Firmware version 2.6.2, and accepts commandline parameters to openVPN in client mode. Users with deep knowledge about openVPN may add special configuration here, The content is not checked by the firmware, so check many times for avoiding a malfunction.

If **Logging** is **On**, NetCom sends the messages of OpenVPN™ to the standard debug log output.

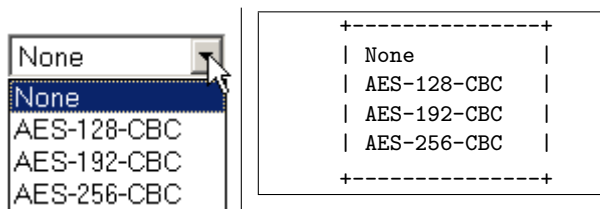


Figure 66: OpenVPN Encryption grades

Different grades of **Encryption** are available, from no encryption at all to AES with a 256 bit key. Select the required grade of security, and open the "Configuration-Settings of the Encryption-Key" to open a window for the parameters.

The management of encryption keys behaves different in a web browser or by Telnet.

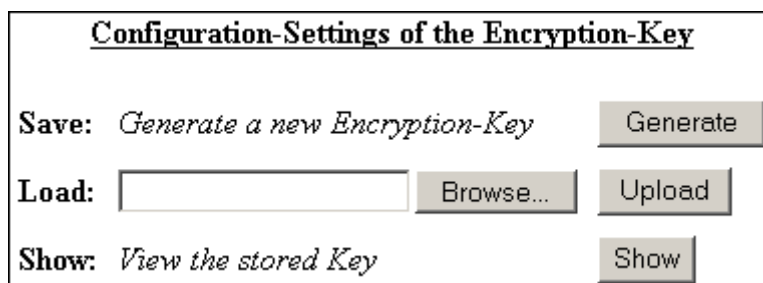


Figure 67: OpenVPN Key Management in Web Browser

This window is for key management. The NetCom allows to **Generate** a new key from Pseudo Random Data. This key is displayed in the browser window. Depending on the configuration of your Web browser, it will attempt to immediately save the key to a file on your disc. Since the Internet Explorer also shows this behavior, the Firmware suggests a file extension of ".cfg" instead of ".key". Windows may react crazy on "key"-files. Please also note, this fresh new key is only displayed/saved. The configuration of the NetCom has not changed.

To use this new key on the NetCom, you must load it to the NetCom. Select the file containing the key data, and **Upload** it to the NetCom. This may be any key, regardless of the source.

Instead of loading a new key to the NetCom, it is possible to **Show** the key currently used. Again some browsers including Internet Explorer directly attempt to save the key.

The Telnet menu (figure ??) provides three Options for key management. **Generate** a new key from Random Data⁵, it is displayed in the terminal window. Depending on your terminal program, you need to have the logging capability active to save the data, or on other programs you may directly save the screen content. Here is a sample key displayed.

```
# Please copy this key into a new text file.
-----BEGIN OpenVPN Static key V1-----
0f3fc3d7d1d22d5b3ba1e498d27338c7
f8bf452edf484fae209d657b8cabfc58
9d2edb0c84eae68a65d6e93cda961775
1dbf8a7c38a73c9bc5f1a1ce0e0e0729
72b297945d6e0482a84f2397ab5ba8e6
00069892f0e41b8ab4a511d42ca6405c
8348f40652d8045962e8c0bcfc4c2b91
0ee7772be2b54ed0c0574acd9643d3b5
05a260ed54bd3ba730d12863b4f3df5a
4207b90562c6c7a9c27febabf6e0aa69
ebd04188729eed159c48a94a3da4a30e
7411c4ca2fca8afa365c535877dc00a5
306ddab341b0bf5b325be68b849294a5
47b69cc493aaf2329675f63953715952
558190b8964caf707b59801115413059
ea4b955d8f97263c233d280e032ba83e
-----END OpenVPN Static key V1-----
```

Figure 68: Sample OpenVPN Key in Telnet

Please note, this fresh new key is on the display only. The configuration of the NetCom has not changed. When you exit this display with the <ESC> key, you are asked whether you want this key as the new key in your NetCom.

```
+-----+
| Should the generated key be stored as your new secret key? |
|                               Yes  No  |
+-----+
```

Figure 69: Use new Key in Telnet

⁵Actually from a PRNG (Pseudo Random Number Generator)

Select **Yes** to use this new key on the NetCom.

As an alternative you may **Upload** any key to the NetCom, regardless of the source. This way you have your Telnet/Terminal software to send the key as an ASCII file. Check your documentation on how to do it. With Hyper Terminal you may just paste the text into the window.

Instead of loading a new key to the NetCom, it is also possible to **Show** the key currently stored on the NetCom.

6.2.1.4.1 Generating strong keys As seen the OpenVPN function allows to generate a new key on the NetCom. The result may be used to get a new binary key for Wireless and other Encryption. Just generate the key, *but do not store it*. Copy 64 (26/10) hexadecimal characters from the middle area, and place them on one line. This is at least better as typing 'something' on the keyboard.

Binary random data has 8 random bits per byte. In contrast ASCII characters only have 7 bits, but these aren't pure random. Only 94 characters from ASCII are printable, but usually they are not selected by random. Playing monkey on the keyboard generates a small set of characters. This is equivalent to 4 random bits per character, or even less. Selecting every 11th bit from a given text may look better, but also this is not random.

6.2.1.5 Authentication

Web: menu "SERVER CONFIGURATION", section "Authentication".

Telnet: "ServerConfig", option "Authentication"

Authentication

Security Settings

Password: ?
Retype Password:

PPP Server Authentication

Accounts ?

<pre> ServerConfig +-----+ Parameter Wireless OpenVPN Authentication Date & Time Info +-----+ </pre>	<div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;">Security Settings</p> <p>Password [empty]</p> <p style="text-align: center;">PPP Server Authentication</p> <p>Accounts [name:pass,name2:pass2]</p> </div>
---	---

Figure 70: Access Authentication

The Security Settings define a **Password** to restrict access to the configuration of NetCom. The password is not shown while typing it. To protect against accidental mistyping, you must type the Password twice.

The "PPP Server Authentication" provides a list of **Accounts**, which are usable to Dial-In to the NetCom. For background information about this feature please consult section 10. The list consists of accounts, separated by comma. Each account is a pair of username and password, separated by a colon. This list is valid for all serial ports.

6.2.1.6 Date & Time

Web: menu "SERVER CONFIGURATION", section "Date and Time Settings".

Telnet: "ServerConfig", option "Date & Time"

It may be helpful to have a correct time setting in the NetCom. You may manually enter the time here. Please note, there is no real time clock with a battery backup in the NetCom. When the NetCom is restarted, the time is lost. Retype the value of **Date & Time** for manual setting. The format is DD-MM-YYYY HH:MM:SS UTC+/-TZ (Time Zone).

Date and Time Settings

Date & Time ?

Simple Network Time Protocol

State ?

Mode ?

Interval ?

Server ?

ServerConfig

```

+-----+
| Parameter |
| Wireless  |
| OpenVPN   |
| Authentication |
| Date & Time |
| Info      |
+-----+
                
```

Date and Time Settings

Date & Time [01-01-1970 00:17:33 UTC+0]

Simple Network Time Protocol

State Off

Mode DHCP

Interval [1800]

Server []

Figure 71: Date & Time Retrieval Options

It is possible to configure NetCom for automatic time retrieval via SNTP.

The **State** field has three possible settings:

- **Off**: disables automatic time retrieval.
- **Startup**: NetCom gets the time at reset or power on.
- **Interval**: NetCom repeats to retrieve time.

The parameter **Mode** is used to find the definition of the Time Server. It may be defined direct, or by DHCP⁶.

The **Interval** in seconds instructs the NetCom to regularly check for an update of the internal time settings. The Time **Server** may be given by IP Address or by name. A name of course requires a configured DNS server⁷.

6.2.1.7 Save

Web: menu “SERVER CONFIGURATION”, at bottom.



At the bottom of the web page below all the options there is the button **Save**. This will store all configurations done here in the NetCom. Selecting a different configuration section from the menu may discard all changes done. For many configuration changes the NetCom requires a reboot to proceed, especially if the IP parameters have been updated.

The Telnet section has a separate menu for saving configurations, described later.

⁶DHCP has to be active in the Server Parameter [6.2.1.2](#)

⁷see at Server Parameter [6.2.1.2](#)

6.2.2 Serial Port Configuration

In your web browser click on the Icon of “SERIAL CONFIGURATION”. This is a huge menu in the web browser. Each serial port of the NetCom is listed in a separate Column. A maximum of four serial ports is shown. Select the appropriate group of ports.

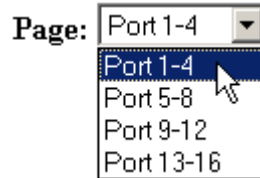


Figure 72: Port Page Selection in Web Browser

The top half of the parameters titled “Serial Settings” is directly related to common serial configurations. The bottom half titled “Transfer Settings” configures the operation mode of NetCom on the network. Each serial port is configured separately, there is no setting shared between ports.

In the Telnet menu select “SerialPorts” in the Main Menu, and directly select the serial port to configure.

The settings available in this menu are by port. Therefore, first the port to configure has to be chosen.

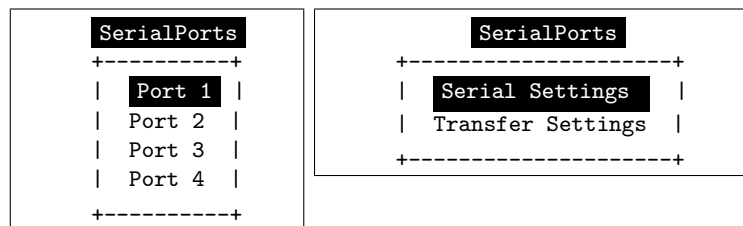


Figure 73: Port Selection in Telnet

Just select the port by placing the cursor, and then press <Enter>. The next option is to configure the **Serial Settings** or the **Transfer Settings**.

6.2.2.1 Serial Settings

Web: menu “SERIAL CONFIGURATION”, column “Port N”, “Serial Settings”.

Telnet: “SerialPorts”, select “Port N”, “Serial Settings”

The NetCom devices allow to operate in RS422/485 modes. This is configured by the Master DIP switches or by software, **PortType (current)** displays the current setting.

Port 1	
PortType (current)	rs232
DefaultModel	16950
MaxBaudrate	921600
PortType ?	rs232
Model ?	16950
Baudrate ?	57600
Manual ?	1843200
FlowType ?	None
DataBit ?	8
Parity ?	None
StopBit ?	1
RxFifoLength	1024
RxTriggerLevel ?	224
TxFifoLength	1024
TxTriggerLevel ?	800

Serial Settings	
Port Nr.	1
PortType (current)	rs232
MaxBaudrate	921600
PortType	rs232
Model	16950
Baudrate	38400
Manual	110
FlowType	None
DataBit	8
Parity	None
StopBit	1
RxFifoLength	2048
RxTriggerLevel	[1248]
TxFifoLength	2048
TxTriggerLevel	[800]

Figure 74: Serial Settings

If the DIP switches are set for «Selected by Software», the mode of operation is chosen by the **PortType** parameter with following selections:

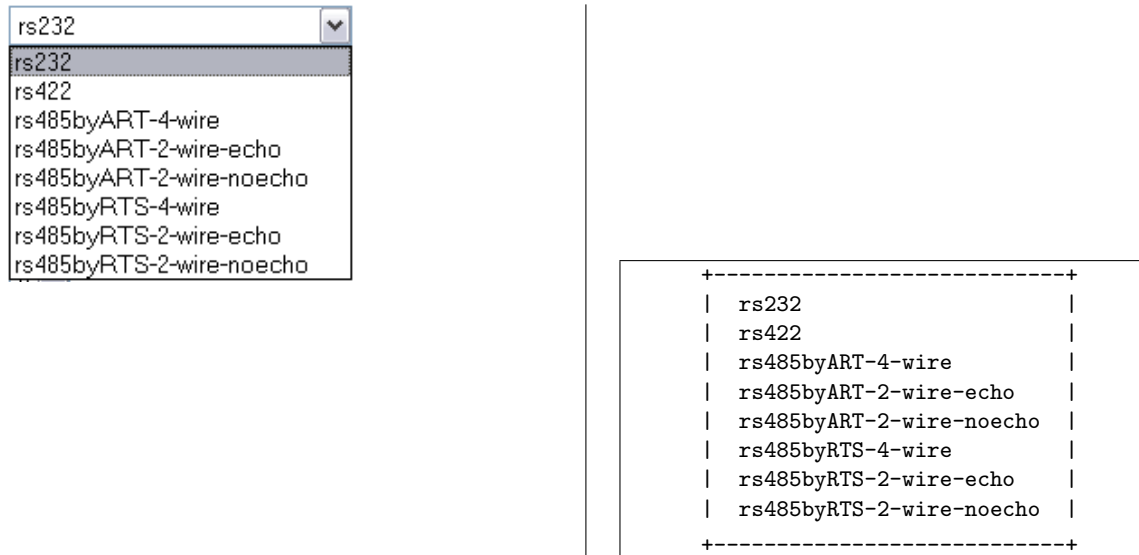


Figure 75: Operation Mode by Software

These are the same modes as available by configuration of DIP Switches. Using software configuration each port is functional independent from other ports. This is the only way to have different operation modes on a multi-port NetCom.

The serial ports are based on enhanced UARTs, the Model and maximum speed are also displayed. The current UART **Model** may be virtually changed to a less advanced type. In some situations it may be desirable to deactivate the FIFO memory, or some other options.

When the NetCom is used via the Virtual Com Driver mode, the following serial parameters are controlled by the application which opened the serial port. However certain installations use a different operation without Driver mode. Then the serial parameters must be defined via this configuration section.

The **Baudrate** may be selected in a drop-down list of common values, or entered manually. If **Manual** is selected in the list, the value in the respective field is used to transmit data. NetCom checks if the configuration is possible, and warns otherwise. Note: The **MaxBaudrate** shown is kind of safe settings. It is achievable in RS 232-Mode with proper cabling. However, the NetCom may operate in RS 422 or RS 485 configuration. These are much less sensitive for noise. It is possible to configure a baudrate of four times the MaxBaudrate, usually 3.686.400 bps. **DataBit** per character, **Parity** and **StopBit** are quite usual parameters. The **FlowType** is available as standard configuration. But there is also the option of **Advanced Configuration**.

Advance		
	On	Off
AutoCTS	<input checked="" type="radio"/>	<input type="radio"/>
AutoRTS	<input type="radio"/>	<input checked="" type="radio"/>
AutoDSR	<input type="radio"/>	<input checked="" type="radio"/>
AutoDTR	<input type="radio"/>	<input checked="" type="radio"/>
AutoTxXOnXOff	<input checked="" type="radio"/>	<input type="radio"/>
AutoRxXOnXOff	<input type="radio"/>	<input checked="" type="radio"/>

FlowType Configuration	
Port Nr.	1
AutoCTS	off
AutoRTS	off
AutoDSR	off
AutoDTR	off
AutoTxXOnXOff	off
AutoRxXOnXOff	off

Figure 76: Advanced Flow Control

This gives very specific control to the user. NetCom can generate Events on RTS, DTR or as XON/XOFF, when the serial receive buffer is filled/emptied. These will inform the connected device to stop or continue the transmission. The NetCom will also respect the state of CTS, DSR or XON/XOFF when sending data to the connected serial device.

The **RxTriggerLevel** defines when NetCom sends the received data to the host. If the amount of data is this high, the data is sent. It does not matter if there is still data coming on the serial line. If less data is received, the NetCom waits some time for further data, before sending the buffer. When this parameter is reduced to '1' obviously all data is sent right when it has been received. The **TxTriggerLevel** operates similar for the transmission. If the defined amount is received from the network, the NetCom does not accept more data to transmit. These options reduce latency times, by increasing the network traffic.

6.2.2.2 Transfer Settings

Web: menu “SERIAL CONFIGURATION”, column “Port N”, “Transfer Settings”.

Telnet: “SerialPorts”, select “Port N”, “Transfer Settings”

The Transfer Settings allow different operation modes. They are selected by the basic **Mode** setting. Depending on the current mode, only some of the many parameters are useful. The web configuration hides those parameters without function.

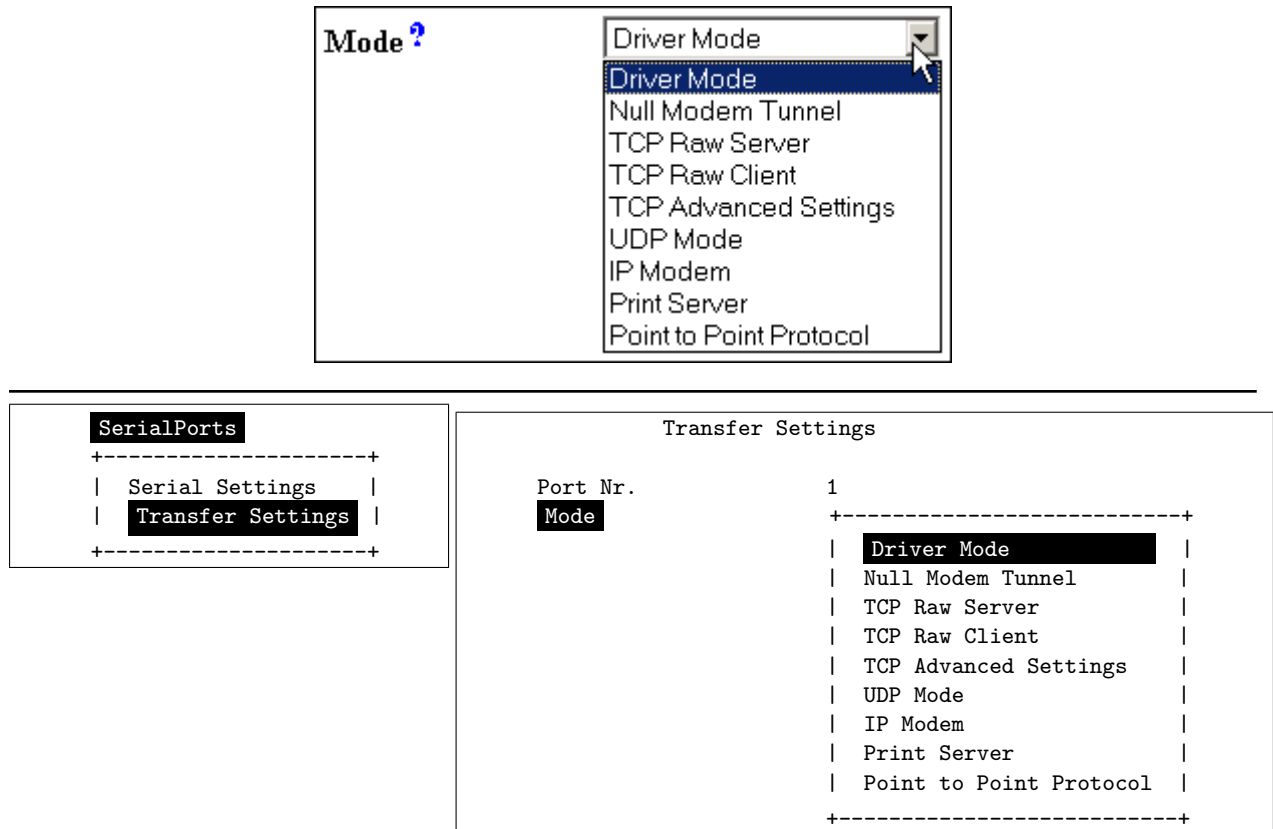


Figure 77: Serial Port Mode Selection

The following paragraphs explain these operation modes as well as their parameters and configuration in detail.

6.2.2.2.1 Driver Mode Only very few parameters have a function in Driver Mode. NetCom is operating as a Server in TCP mode, it accepts two connections per serial port. This mode is required when the driver software for Virtual Com Ports shall be used.

Mode ?	Driver Mode
TCP Port(Control) ?	2000
TCP Port(Data) ?	2001
KeepAliveMode ?	On Connect
KeepAliveInterval ?	0

Mode	Driver Mode
TCP Port (Control)	[2000]
TCP Port (Data)	[2001]
KeepAliveMode	On Connect
KeepAliveInterval	[0]

Figure 78: Driver Mode parameters

The first connection is used to transmit the serial data, this is the **TCP Port (Data)**. And the other is used to transmit control information, **TCP Port (Control)**. This control connection includes the configuration of the serial port, as well as signals for changed Modem Status lines. This mode is required when the serial port is operated via the Virtual Com Driver, it is the default.

In Driver Mode the NetCom accepts only one client per serial port. An attempt to connect a second client is actively refused. This is required to avoid confused configurations and data on the serial port.

The NetCom can monitor an open connection. This is controlled by the **KeepAliveMode**, which has three settings: **Off**, **On Connect** and **Polling**.

- **Off**: never send KeepAlive packets.
- **On Connect**: when a client is trying to connect to the server and there was a connection before, the server checks if the first connection still exists. If it does not exist anymore, the server accepts the new connection.
This option is the default configuration.
- **Polling**: the server checks in **KeepAliveInterval** (seconds), if a connection still exists.

If the network connection between client and NetCom seems to be unstable, the configuration of **Polling** may be desired. This way the NetCom may detect when the connection got lost. When the NetCom detects a lost connection, this is discarded, so the NetCom is available for other clients. Disabling the check is not recommended.

6.2.2.2.2 TCP Raw Server As Raw Server the NetCom operates very simple. It only waits for incoming data connections in Raw IP mode. In contrast to the Driver Mode no driver software needs to be installed on client computers, this mode operates directly on the TCP/IP stack in

the operating system. The parameters of the serial port are defined on the NetCom, as given above (3.1).

Mode ?	TCP Raw Server
TCP Port(Data) ?	2001
Max.Clients ?	1
Password ?	
Retype Password:	

Mode	Raw Server
TCP Port(Control)	[2000]
Max.Clients	[1]
Password	[*****]

Figure 79: TCP Raw Server parameters

Compared to the Driver Mode only the data connection is defined by the **TCP Port(Data)**. The **Max.Clients** parameter allows for more than one connection to the NetCom at a time. If the number is raised, it is the responsibility of the customer to ensure correct operation. There is no special Keep Alive option, the global parameters from section 6.2.1.2 apply.

Firmware version 2.2 added the option of additional protection by **Password**. When a password is configured, the NetCom sends the question "Password: " to the client. The user (his application) must first send the password, followed by a <CR> character. The password is not echoed to allow usage with Telnet on a Monitor.

6.2.2.2.3 TCP Raw Client Also as Raw Client the NetCom requires very few parameters. The client computer operates via the TCP/IP stack as in 6.2.2.2, but now this computers waits for incoming connections opened by the NetCom. Using this mode several NetCom may connect to the same server software installation. The parameters of the serial port are defined on the NetCom, as given above (3.1). When the client computer is another NetCom in TCP Raw Server mode, this will virtually connect the devices attached to the serial port.

Mode ?	TCP Raw Client
Destination ?	
Connect ?	Triggered
ShortHoldTime ?	0

Mode	Raw Client
Destination	[192.168.1.5:2001]
Connect	Triggered
ShortHoldTime	[0]

Figure 80: TCP Raw Client parameters

Under certain conditions the NetCom establishes a Raw TCP connection to a pre-defined **Destination**. Since version 2.0 of the NetCom Firmware the Destination can hold multiple hosts as targets for a connection. They are entered as a comma separated list of DNS names or IP Addresses. Each destination will have a TCP port number, separated by a colon. Instead of a single IP Address or DNS name, a range of IP Addresses is also valid. This range must be followed by the TCP port number, as in 192.168.254.12-192.168.254.17:2077.

The parameter **Connect** defines if NetCom uses the connections as **Permanent**, **Triggered** or by **DSR**. With **Permanent** the NetCom attempts to open the connection as soon as it is available. In **Triggered** mode any activity on the serial ports establishes the connection, inactivity of longer than the **ShortHoldTime** cause NetCom to close the connection. With **DSR** the TCP-connections follow the state of the DSR signal at the NetCom serial port. When it becomes active they are established, until DSR becomes inactive. At that moment the connections are dropped.

6.2.2.2.4 Null Modem Tunnel This operation mode is intended to build a long virtual Null Modem Cable between the serial ports of two NetCom. This mode is symmetric, both NetCom operate as server and as client at the same time. The parameters of the serial port are defined on the NetCom, as given above (3.1).

Mode ?	Null Modem Tunnel ▾
Server	
TCP Port(Control) ?	2000
TCP Port(Data) ?	2001
Client	
Destination ?	
TCP Port(Control) ?	2000
TCP Port(Data) ?	2001
Connect ?	Triggered ▾
ShortHoldTime ?	0
KeepAliveMode ?	On Connect ▾
KeepAliveInterval ?	0

Mode	Null Modem Tunnel
Server	
TCP Port(Control)	[2000]
TCP Port(Data)	[2001]
Client	
Destination	[]
TCP Port(Control)	[2000]
TCP Port(Data)	[2001]
Connect	Triggered
ShortHoldTime	[0]
KeepAliveMode	On Connect
KeepAliveInterval	[0]

Figure 81: Null Modem Tunnel

This is a mixed mode, requiring parameters for server function and for the client part. The NetCom operates as a server while accepting connections in Driver Mode (6.2.2.2.1). If there is no current connection, the NetCom may establish a connection as a client. This is also a special connection, using the Driver Mode protocol. NetCom will not only transmit serial data in both directions, it will also pass information about the current settings of the Modem Status lines. And it will itself set the Modem Control lines as required by the other host. The CTS is connected to the RTS of the partner, and DSR connects to DTR. Since this operation requires another NetCom to accept the connection, both NetCom together operate as a long Null-Modem cable. The data is sent via a tunnel through the network.

The configuration as **Server** (top part) requires the same parameters as the Driver Mode, hence **TCP Port(Control)** and **TCP Port(Data)**. Also the **KeepAlive** function operates the same.

The configuration as **Client** (bottom) first requires a destination. Here it is given by name, but a direct IP Address may be more usual. On the destination there is also a **TCP Port(Control)** and **TCP Port(Data)** to accept the connect of the NetCom.

The **Connect** methods are the same as with the TCP Raw Client mode. So connections to the partners are permanent, last until there is no activity for a given time, or they are controlled by the DSR signal.

Attention: You *must not* configure both NetCom with a **Connect** option configured as **Permanent**. This will result in each of them attempting to contact the other at the same time. Both NetCom will reject the connect, because they are already busy establishing a connect of their own. Instead create an asymmetric configuration: either use one of the NetCom in Driver Mode, or configure it with an empty Destination parameter. Or consider to have a connection on demand, i.e. use the **Triggered** option.

6.2.2.2.5 TCP Advanced Settings All of the above operation modes are special configurations for options. In some situations none of the pre-defined modes fit the customers needs. When this is the case, the TCP Advanced Settings offer the configuration of any Transfer parameter. Unusual combinations of Modes are possible with this, also standard modes with unusual parameters.

Mode ?	TCP Advanced Settings ▾
Server ?	Off ▾
TCP Port(Control) ?	0
TCP Port(Data) ?	2001
Max.Clients ?	1
Client ?	On ▾
Destination ?	
TCP Port(Control) ?	0
TCP Port(Data) ?	0
Connect ?	Triggered ▾
ShortHoldTime ?	0
KeepAliveMode ?	On Connect ▾
KeepAliveInterval ?	0

Transfer Settings	
Port Nr.	1
Mode	TCP Advanced Settings
Server	On
TCP Port(Control)	[2000]
TCP Port(Data)	[2001]
Max.Clients	[1]
Client	Off
Destination	[]
TCP Port(Control)	[2000]
TCP Port(Data)	[2001]
Connect	Triggered
ShortHoldTime	[0]
KeepAliveMode	On Connect
KeepAliveInterval	[0]

Figure 82: TCP Advanced Settings

The NetCom usually acts as a network server. This means it accepts incoming connections. The most used Driver Mode is one example. The NetCom detects which mode to use. When the Data-Port is opened first, then the NetCom operates in TCP Raw Server mode, with respect to **Max.Client**. When the Control-Port is opened first, the NetCom expects a second connection on the Data port, to operate in Driver Mode for one client only.

The NetCom can also operate as a network client as seen in TCP Raw Client mode. This is enabled by setting **Client** to **On**. As a client it requires the same parameter as for the specialized modes. When the **TCP Port(Control)** is defined (not zero), the NetCom will operate as a client for Driver Mode, as in Null Modem Tunnel. The destination is the target address or DNS name.

Otherwise the NetCom operates in TCP Raw Client mode when it establishes a connection. The syntax for multiple destinations applies then.

The remaining parameters are explained in the client mode descriptions.

The TCP Advanced Settings allow for flexible usage of the NetCom, when **Server** and **Client** modes are **On** at the same time. If no connection is active with the NetCom, it accepts incoming connections, i.e. it operates as server as long as the connections are held. Without a connection a Trigger event defined in **Connect** cause the NetCom to establish a connection to the defined target. So the NetCom is a client at that time.

6.2.2.2.6 UDP Data Transfer UDP is an Internet Protocol, which does not define a connection, it sends data in single packets instead of a stream. There is no extra return data to signal a successful transmission. As a side effect data may be sent and received faster than with TCP/IP. The UDP mode is available as a function since the version 1.4 of the NetCom firmware.

Mode ?	UDP Mode
UDP Port(Local) ?	2002
Destination ?	
UDP Port(Dest) ?	2002
UDP MaxPacketSize ?	1458
UDP Timeout ?	0
UDP Trigger ?	

Mode	UDP Mode
UDP Port(Local)	[2002]
Destination	[]
UDP Port(Dest)	[2002]
UDP MaxPacketSize	[1458]
UDP Timeout	[0]
UDP Trigger	[]

Figure 83: UDP Data Transfer

This protocol requires a **UDP Port(local)** for listening to incoming data. Other stations on the network send their data to this port. The **Destination** host is configured by IP Address or name, plus the target **UDP Port(Dest)**. Please compare with the parameters for TCP Raw Server and Client Modes. The parameters to configure the UDP Mode are similar to a mixture of these modes. A UDP Broadcast is sent, if the destination address is the broadcast Address, see section 6.2.1.2 above.

Since there is no connection, data can not be sent in a stream. UDP uses packages. There are several ways to define the content for a package.

UDPMaxPacketSize is a limit for the size of UDP packets. When the amount of data received on the serial port reaches this limit, the UDP Frame is assembled and sent to the destination.

UDPTimeout defines when the NetCom sends the received data as a UDP Frame. If the reception of serial data is interrupted for this time (in milliseconds), the data sampled so far is sent to the destination. A value of zero causes all data to be sent immediately, use “-1” to disable the function of timeout trigger.

UDPTrigger defines a sequence of characters. As soon as this sequence is detected in the received data, all data up to the end of this Trigger is sent to the destination. In most situations such a Trigger includes control or other special characters. Enter them numeric: as \xHH where HH is the hexadecimal code of the character, or as \OOO where OOO is the octal code of the character. The backslash itself must be doubled as \\.

6.2.2.2.7 IP-Modem The serial port of a NetCom may mimic (emulate) a serial modem. There is the separate section 7 defining this functionality. Here are the basic network parameters only.

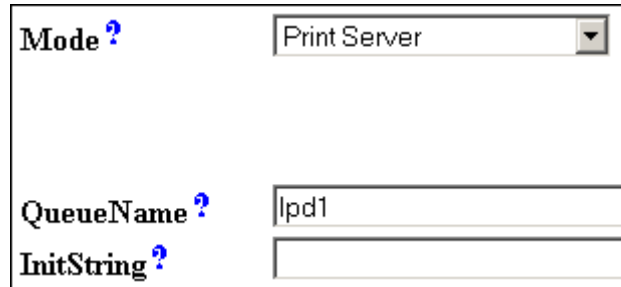
Mode	IP Modem
TCP Port(Data)	[2001]
Destination	[]
IP Modem Config	[]

Figure 84: IP-Modem

A serial modem accepts connections from a phone line, while an IP Modem accepts connections from the network, in this case via TCP/IP. The TCP port for this is defined as the **TCP Port (Data)**, similar to TCP Raw Server mode. This is the only parameter required to set here.

All other values are normally defined by AT-commands via the serial port. However for short, **Destination** allows for up to four predefined targets, available with special Dial commands. The **IP Modem Config** is known as the Init String in standard modems.

6.2.2.2.8 Print Server Function The NetCom firmware version 2.2 introduces the function as a Print Server according to RFC1179, also called a »Line printer daemon«. A print server is accessed through its IP Address via one specified TCP Port (see section 6.2.1.2). Data is handled in distinct queues, each with a certain name. Each queue is handled by a certain serial port, and the data is sent to the serial printer attached to this port.



Mode ? Print Server

QueueName ? lpd1

InitString ?

Port Nr.	1
Mode	Print Server
QueueName	[lpd1]
InitString	[]

Figure 85: Print Server Configuration

Each serial port configured for Print Server operation has its separate **QueueName**. The default value is »lpd« plus port number. The **InitString** is a special feature of NetCom. This string is sent to the serial printer at the beginning of the next queued print job. The definition is in section 8.2.1 on page 115.

6.2.2.2.9 PPP Network Configuration The NetCom firmware version 2.4 offers the network access via PPP(13) over the serial ports of the NetCom. This function is not designed to allow routing of information from one station to another, passing the NetCom. It provides access to the NetCom and its internal functions via means of PPP network.

The serial port of the NetCom may operate as a PPP Server, i.e. it will accept incoming calls (Dial-In). However as a Client it may also establish PPP connections by itself (Dial-Out). This section here just explains how to configure the NetCom for the operation. The technical information about the required parameters is given in section 10.

Mode ?	Point to Point Protocol
Mode ?	Client
Dynamic Addresses ?	Enabled
Idle Timeout ?	0
Modem Mode ?	Modem
Default Route ?	Disabled
Server	
Local IP Address ?	10.1.1.1
Remote IP Address ?	10.1.1.2
Client	
Username ?	user1
Password ?	passwd1
Dial String ?	ATDT
Modem Init-String ?	
Local IP Address ?	10.1.0.1
Remote IP Address ?	10.1.0.2
Netmask ?	255.255.255.0

```

Port Nr.          1
Mode            Point to Point Protocol

Mode              Client-Server
Dynamic Addresses Enabled
Idle Timeout      [0 ]
Modem Mode        Modem
Default Route     Disabled

Server
-----
Local IP Address  [10.13.1.1]
Remote IP Address [10.13.1.2]

Client Configuration on the next Site

Client
-----
Username          [user13      ]
Password          [passwd13    ]
Dial String       [ATDT        ]
Modem Init-String [             ]
Local IP Address  [10.13.0.1]
Remote IP Address [10.13.0.2]
Netmask           [255.255.255.0]
    
```

Figure 86: PPP Configuration

The serial port may operate in the combined PPP **Mode** of **Client-Server**, or the operation may be restricted to only one of those two. With **Dynamic Addresses** as **Enabled** the NetCom accepts the Assignment of an IP Address from a PPP Server. The NetCom operates as PPP Client to use this. When this option is **Disabled**, fixed addresses are predefined below.

When no data has been sent for the **Idle Timeout** (in seconds), the PPP-Link will be closed. Use the value zero to disable the timeout.

The serial port may operate via a real Modem (analogue, ISDN, GPRS, ...), or via a Nullmodem cable. A Nullmodem cable only partially emulates the functions of a Modem. The **Modem Mode** parameter selects the different ways of operation.

The PPP-interface may have the **Default Route** function on the PPP-Link as **Enabled** or **Disabled**.

When the serial port is operating as a PPP Server, it will require a **Local IP Address** for its end of the PPP-Link. Likewise the **Remote IP Address** is assigned to the connected station, if this requests such.

The client part of configuration is directly visible in the web browser interface. Via Telnet or serial port use the Left- and Right-keys to change between Server and Client parameters.

When the serial port is operating as a PPP Client, there is of course a PPP Server to contact to. To get access to this Server the NetCom will use an account on the server. The accounts consists of a **Username** and a **Password**, which are configured in the NetCom. This account is used by this serial port only, other serial ports on the NetCom require separate account configuration.

PPP operates via an operational serial connection. To open this connection a real Modem must dial to the target modem first. This will require a phone number for the target. Instead of only configuring the phone number, the NetCom accepts a complete **Dial String**. This string contains the phone number, but also may have certain commands to the Modem.

Likewise a real Modem may require special configuration prior to operate for PPP. This initialization is provided by the **Modem Init-String**.

When the PPP-Link is established, the NetCom may accept the assignment of an IP Address from the server. If this feature is **Disabled**, or the server does not provide the address, the NetCom uses the **Local IP Address** for its own end of the PPP-Link.

The **Remote IP Address** is used together with the **Netmask**. They define a network route for IP data frames. The NetCom uses these parameters to decide whether a certain communication shall use the PPP-Link or a different network interface.

6.2.2.3 Save

Web: menu "SERIAL CONFIGURATION", at bottom.

A rectangular button with a thin border and the word "Save" centered inside.

Again at the bottom of the web page below all the serial port options there is the button **Save**. This will store all configurations done for the current group of serial ports. Selecting a different group of ports or another configuration section from the menu may discard all changes done.

6.2.3 NetCom Tools

Several tools for system status, checks and debugging are available in the Firmware. The available tools are:

- The Ping utility to check if a station is available.
- Statistic information for each serial port.
- The Netstat utility to monitor used TCP connections.
- The option to detect WLAN devices in the proximity (NetCom WLAN only)
- The option to update the firmware.
- Saving of Configuration to / Loading from a file (web browser only).
- Information logging by Syslog function and a DebugLog via TCP/IP.

In your web browser click on the Icon of “TOOLS”, the browser opens the list of available tools. In Telnet the “Tools” menu provides a list of the tools.

6.2.3.1 Ping

Web: menu “Tools”, section “Ping”.

Telnet: “Tools”, option “Ping”.

Enter the **IP Address** or the name of a station in the field. In the web browser click the **Ping** button, hit the <Enter>-key via Telnet. The network connection is checked by sending ICMP Echo Request data packages.

```

PING 127.0.0.1 from 192.168.1.87 : 44 (72) bytes of data
52 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=1.560 msec
52 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=1.542 msec
52 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=1.542 msec
back

```

Figure 87: Ping and Response in Web Browser

```

PING 127.0.0.1 from 192.168.1.243 : 44 (72) bytes of data.

52 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=< 10 ms
52 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=< 10 ms
52 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=< 10 ms
52 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=< 10 ms

```

Figure 88: Ping and Response in Telnet

If the target responds, the network between the NetCom and the target is operational. The time required for an echo depends on the speed of the network. In a typical Ethernet this is only very few Milliseconds, while it can be several seconds throughout the Internet.

Via Telnet use the <Esc>-key to stop the Ping function.

6.2.3.2 Statistics

Web: menu “Tools”, section “Statistics”.

Telnet: “Tools”, option “Statistics”.

The Statistics are presented on a by-port base. So you first select the serial port, and then you get the information about modem status and control. Also the amount of data transferred is shown.

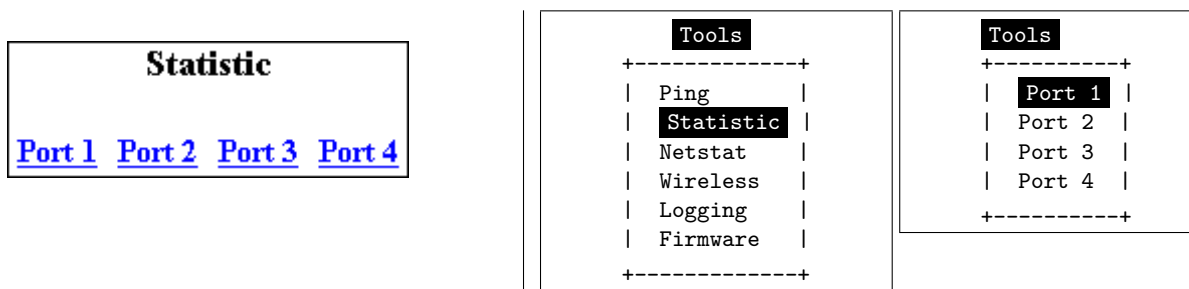


Figure 89: Statistics Port Selection

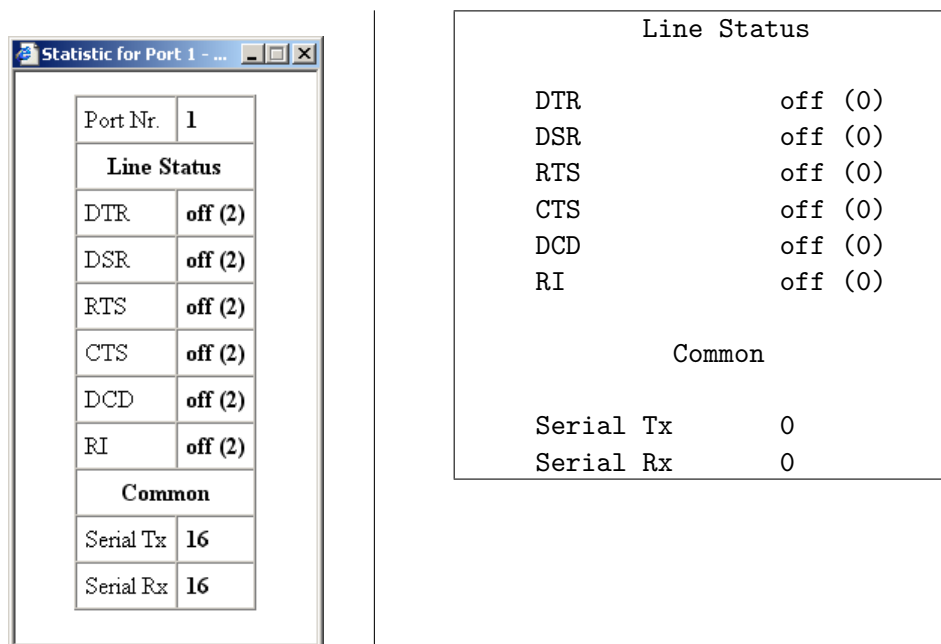


Figure 90: Port Statistics

The statistics window⁸ reports the state of the modem status and control signals. Further the NetCom counts the number of status changes on the modem control- and status-signals, since the NetCom has been started. The number of characters sent and received is shown at the bottom.

6.2.3.3 Netstat

Web: menu “Tools”, section “Netstat”.

Telnet: “Tools”, option “Netstat”.

Netstat is a common tool to display the actual status of network connections. It may be used to monitor the actual status of the NetCom. This is a standard tool for network debugging.

⁸The web browser opens a separate window for each port selected

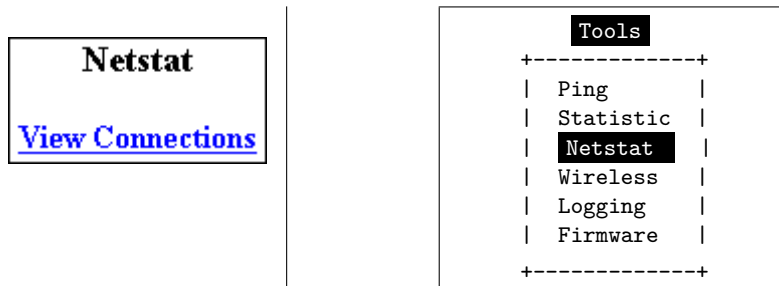


Figure 91: Start Netstat

Proto	Local Address	Foreign Address	State
tcp	0.0.0.0:23	0.0.0.0:0	LISTEN
tcp	0.0.0.0:80	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2000	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2001	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2010	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2011	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2020	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2021	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2030	0.0.0.0:0	LISTEN
tcp	0.0.0.0:2031	0.0.0.0:0	LISTEN
tcp	192.168.1.243:80	192.168.1.42:1280	TIMEWAIT
tcp	192.168.1.243:80	192.168.1.42:1281	ESTABLISHED
udp	0.0.0.0:161		
udp	0.0.0.0:19970		
udp	192.168.1.243:32331		

1/1	Proto	Local Address	Foreign Address	State
	tcp	0.0.0.0:23	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:80	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2000	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2001	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2010	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2011	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2020	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2021	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2030	0.0.0.0:0	LISTEN
	tcp	0.0.0.0:2031	0.0.0.0:0	LISTEN
	tcp	192.168.1.98:23	192.168.1.42:3665	ESTABLISHED
	udp	0.0.0.0:161		
	udp	0.0.0.0:33320		
	udp	192.168.1.98:10397		

Figure 92: Netstat Sample Output

A 'Foreign Address' of "0.0.0.0" is listed when NetCom is waiting for an incoming connection (LISTEN mode). If the value is not "0.0.0.0", the connection is either active (ESTABLISHED) or already closed (TIMEWAIT).

In the web browser you may **Update** the Netstat output.

Via Telnet the output may not fit on the screen, then the display will start with "1/2" in the first line. Or even more for a long list. You may change to a different page by using the Page Up/Down

keys in your Telnet. The display is refreshed in an interval of some seconds. Use <Esc>-key to return to the menu.

6.2.3.4 Wireless

Web: menu “Tools”, section “Wireless”.

Telnet: “Tools”, option “Wireless”.

When Wireless communications is intended, it is useful to see a list of possible partner stations on the WLAN. This function is available in many driver packages for Windows, and also in the NetCom WLAN Serial Device Servers. This function is often referred to as »Range Scan«.

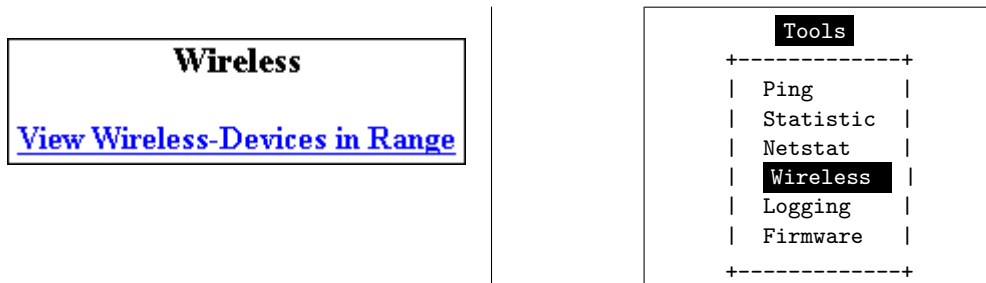


Figure 93: WLAN Scan

On the NetCom WLAN it will open a separate browser window with the results. An example of this is shown below. Telnet displays the results.

Wireless-Devices in Range Update					
Act	MAC	SSID	Channel	Mode	Enc
X	86:73:F6:22:E1:BA	NetCom_0210100462	7	Ad-Hoc	
X	A6:E8:9E:BE:7D:86	NetCom_0210100444	7	Ad-Hoc	
X	00:0F:B5:66:CF:56	NETGEAR	11	Managed	X
Current Rate: 11Mb/s					

Act	MAC	SSID	Ch	Mode	Enc
X	86:73:F6:22:E1:BA	NetCom_0210100444	7	Ad-Hoc	
	A6:E8:9E:BE:7D:86	NetCom_0230100152	7	Ad-Hoc	
X	00:0F:B5:66:CF:56	NETGEAR	11	Managed	X
Current Rate: 11Mb/s					

Figure 94: WLAN Scan Output

This example lists two other NetCom WLAN configured for Ad-Hoc communication on channel 7. Both do not use encryption. There is also an Access Point (listed as **Managed**), of course in Infrastructure-mode. To connect to this AP the NetCom WLAN must use encryption.

Since the NetCom WLAN itself is in Ad-Hoc mode, the communication is limited to the 802.11b, which results in 11Mb/s as raw transmission speed. Further the encryption is limited to the WEP methods.

In Telnet the display is updated automatically when some information changes. Most noticeably this will be the Act-ivity sign.

6.2.3.5 Firmware

Web: menu “Tools”, section “FirmwareUpdate”.

Telnet: “Tools”, option “Firmware”.

To upload a new version of the firmware, put the name of the file in the field. Your web browser will allow to search for the file. Click on the **Update** button, and your browser will upload the file to the NetCom.

FirmwareUpdate

Warning: All connections get closed
and the server reboots after updating

Tools

```

+-----+
| Ping   |
| Statistic |
| Netstat |
| Wireless |
| Logging |
| Firmware |
+-----+

```

Firmware Update

[2400]

[Start Update]

Figure 95: Firmware Upload

Via Telnet the option to upgrade the Firmware of NetCom is different. The upload of the data is either done via the current channel (i.e. the serial or Telnet connection). Or independently via a separate TCP/IP connection. The **Update Port** parameter defines this second connection, the NetCom waits for a TCP connection on this port. The Firmware is sent coded in base64 (a special text format), via very simple programs like a second Telnet session, or similar tools. Terminal software by serial configuration may just use the “Send Textfile” function.

While uploading the file it is checked by NetCom. If it is a valid content, it is stored in the Flash Memory. When the upload is finished, NetCom will Reboot.

6.2.3.6 Save and Load Configuration

Web: menu “Tools”, section “Configuration File”.

Via web browser it is possible to save the actual configuration to a text file. Of course it is also possible to load the saved configuration into a NetCom.

Configuration File		
Save:	Save the Configuration Parameters in a File	<input type="button" value="Download"/>
Load:	<input type="text" value="cuments\NetCom423.cfg"/> <input type="button" value="Browse..."/>	<input type="button" value="Upload"/>

Figure 96: Save and Load Configuration in Web Browser

This may be very useful when configuring several NetCom of the same type. Configure one device, and save the file. Change the configuration file for the necessary parameters, and upload the modified version to the next model.

6.2.3.7 Logging and Debug

Web: menu “Tools”, section “Syslogging”.

Telnet: “Tools”, option “Logging”.

The NetCom has two options of Logging. There is the standard Syslog, and a second option of logging via Telnet.

Syslogging	
Syslog ?	<input type="button" value="On"/>
Destination ?	<input type="text" value="syslog.vicom.de"/>
Facility ?	<input type="text" value="1"/>
Debuglog ?	<input type="button" value="On"/>
Debug Port ?	<input type="text" value="1200"/>

Tools	Logging
<pre> +-----+ Ping Statistic Netstat Wireless Logging Firmware +-----+ </pre>	<pre> Syslog Off Destination [] Facility [1] Debuglog Off Debug Port [0] </pre>

Figure 97: Syslog & Debuglog Parameters

The **Syslog** function may of course be **Off** or **On**. In the **On**-state the NetCom sends all the log information to a computer defined by **Destination**. A special software often called Syslog Daemon

has to receive these data. The Option of **Facility** is a criteria for the Daemon how this will organize the data received from the NetCom.

In contrast for **Debuglog** the NetCom behaves as the server. When this option is **On** the NetCom waits for incoming TCP connections to the configured **Debug Port**. The NetCom sends all logging information via this connection. For manual use a software like Telnet is suitable, especially if it has the option to save all received data.

6.2.3.8 Save

Web: menu “Tools”, at bottom.



As usual at the bottom of the web page below all the options there is the button **Save**. This will store the configurations done for Logging (6.2.3.7).

6.2.4 Reboot

Web: menu “REBOOT”.

In your web browser, click the Icon of **REBOOT** to restart the NetCom firmware.

Attention: This option will discard all configuration changes, unless they have explicitly been saved. Naturally it will also disconnect all other clients using serial ports or the Telnet configuration menu.

6.2.5 Save&Exit Menu

This section of configuration is only available via the terminal interface, i.e. via Telnet or serial port. Modifications in the configuration of the NetCom are not active, until they are explicitly saved to the Flash Memory of NetCom. This menu also allows to discard all changes, and even to restart the firmware.

6.2.5.1 Save Parameter

Telnet: “Save&Exit”, option “Save Parameter”.

When some changes are done, these modified settings should be saved. A confirmation is requested before doing this.

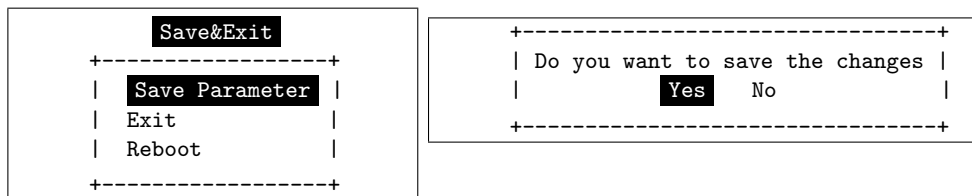


Figure 98: Menu Save modified Parameters in Telnet

The Telnet interface is still active when this operation is finished.

6.2.5.2 Exit

Telnet: “Save&Exit”, option “Exit”.

You will not be surprised, when you leave the menu by selecting this option. If you made any changes of parameters, you must confirm to save these.

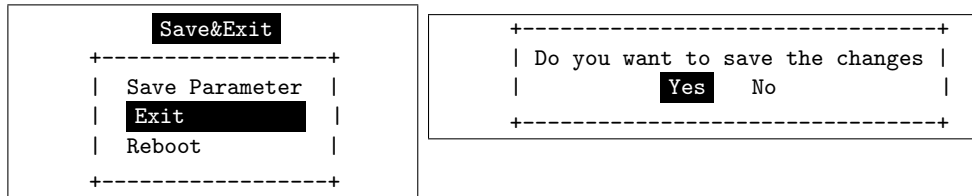


Figure 99: Menu Exit from Configuration in Telnet

The NetCom terminates the Telnet interface when this operation is finished, even when the modifications are not saved to Flash Memory.

6.2.5.3 Reboot

Telnet: “Save&Exit”, option “Reboot”.

Users may restart the firmware of the NetCom. Modified configurations are activated by the restart process. Such a restart is necessary for some changes like IP configuration, others do not require a restart.

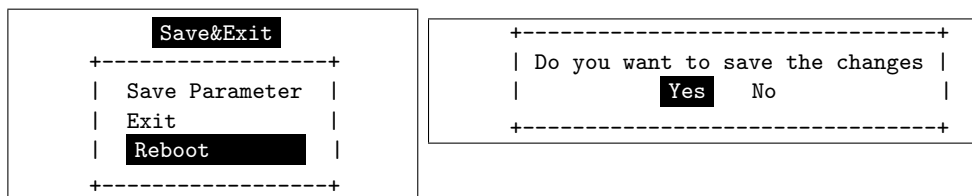


Figure 100: Exit and Reboot in Telnet

Also here, if parameters are changed during the session, confirmation for saving them is requested. Of course the Telnet configuration is closed, because all TCP connections are terminated by the reboot process.

6.3 Erase Configuration of NetCom

Sometimes it is required to clear any configuration done, and go back to the Factory Settings. Users might think this is possible with the Reset button. It is not done this way. The Reset button is just a way to restart the NetCom without removing the power.

To make a clean configuration the DIP switches must be configured to the pattern of "Factory settings". Refer to Section 3.1 or to the table on top of the NetCom case. When this pattern is chosen, the NetCom has to be restarted, by power off or by using the Reset button. This is for security. When changing a DIP configuration, the 'Factory settings' might appear by accident. So the NetCom requires to be restarted with this DIP pattern active to avoid accidental damage of the configuration. While restarting, the NetCom erases the current configuration, and replaces

the parameter with the default values. When this is finished, the Power LED blinks once. Do not power off or reset the NetCom before this blink is seen.

The Ethernet cable should not be connected, because the NetCom uses DHCP in factory configuration. Without an Ethernet cable it does not attempt to find a DHCP server, which makes a faster reboot process.

7 IP Modem Function

The Firmware offers the function of IP Modem. Used in this mode, the serial port of the NetCom emulates a standard serial modem. Basically this means the NetCom will

- a) answer to AT-commands on the serial port
- b) establish a connection to a destination
- c) inform the connected serial device of the connection
- d) accept a TCP connection, and inform the serial device of that event

For connections the NetCom will use a TCP connection. This differs from a normal telephone line, so there will be some modifications in the behavior. The target is an IP Address, not a phone number. Also for hardware reasons the automatic baudrate detection used in today serial Modems is not available. However this is not a problem at all, the IP Modem can be installed in Windows as a Standard 33600bps Modem. There is an INF-file for ease of installation.

7.1 Some possible Scenarios

1. The customer has a remote management installation, operating via telephone line. These lines may be in-house or through public phone systems to other destinations. The customer wants to reduce costs for these lines, management and possibly hardware, using the Intra- or Internet.
2. The customer wants to contact several stations from a central server. Because of frequent target changes he does not want to define the target by a Virtual Com Port.
3. Remotely distributed devices contact a central system by Modem. This is the reverse of option 1.
4. A computer without Network access shall have at least limited control on the connections established by a NetCom.
5. Old fashioned BBS installations become accessible via Internet. The typical multi-modem box is replaced by a NetCom Server with multiple ports configured for IP Modem operation.

7.2 Serial Signals and Cables

A real modem provides the same signals as the serial port of a PC. However, where a signal is an output on the PC, it is an input to the modem, and vice versa. So in the NetCom the emulation of a modem must be incomplete. By exchanging RxD and TxD the data connection is fine, the same happens for handshaking signals RTS and CTS. The DTR of the PC is connected to DSR of NetCom, this is simple. The RI may be ignored, some connectors for serial ports also do that.

However a real modem provides DSR and DCD to the PC. There is only the DTR left on NetCom to serve these signals. In most configurations the NetCom-DTR serves as the DCD to the computer.

The cable must provide a DSR to the PC then, e.g. by shortcut to the PC-DTR. In some configurations the NetCom-DTR must serve as the DSR. This is configurable by a command.

The recommended cable connects as shown in this table. Please note, this installation does not use the simply crossed signals. Especially the DSR of the PC is internally connected to the DTR of the PC.

DB9m	PC		IP-Modem	DB9m	DB9f
3	TxD	——	RxD	2	3
2	RxD	——	TxD	3	2
7	RTS	——	CTS	8	7
8	CTS	——	RTS	7	8
6	DSR	PC-DTR (internal loop-back)			
4	DTR	——	DSR	6	4
1	DCD	——	DTR	4	6
5	GND	——	GND	5	5

Table 17: IP Modem cable

The limitation of signals is a restriction in function, compared to real world serial modems. Since most installations do not require the full availability of all signals, the required subset can be selected.

7.3 Operation Modes by IP Modem

The function of IP-Modem may be configured port by port. On a NetCom with a single port there is no much of a difference. However a NetCom with more serial ports operates each port independently. In the following sections of this manual the phrase "serial port of a NetCom, configured to operate as IP Modem" is replaced by "IP Modem" for brevity.

Two basic operation modes are available. The first and default mode is Modem-to-Modem. This requires a serial port of a NetCom configured as IP Modem on both ends of the connection. When one IP Modem dials the other, the connection is established on the TCP level. Directly afterward both IP Modems negotiate to ensure they are a real NetCom IP Modem and are free for connection. If successful both issue a "CONNECT ..." response to the serial connected devices. This is convenient for the customer to understand. The CONNECT may report some parameters, e.g. the minimum serial speed used by both Modems. These extra parameters are not implemented so far.

The other mode is named as Modem-to-Host. The destination is any software, which opens a TCP port for Listen mode. It may be a second NetCom configured for TCP Raw Server Mode. It may also be the customers application, running on a certain computer. This mode offers less features.

7.4 Hayes Commands

The IP Modem operates with a command set similar to those in real Modems. All of the commands start with the character sequence AT.

7.4.1 AT command set

The following table lists many standard commands (in alphabetical order). The AT is omitted for brevity. The discussion of the functions is below the tables in section 7.5 below.

7.4.1.1 Standard AT-Commands

These commands are based on the old Hayes Modem.

AT	Hayes-Standard	IP Modem Function
A	Answer Call	Accept a connection
Bn	ITU-T modulation	Define some modem operation modes
Dnnn	Dial connection, basically phone number as nnn	Connect to the target system by IP Address and TCP-Port. E.g. ATD10,0,8,42,2023 will "dial" to port 2023 on IP Address 10.0.8.42
E	Echo on/off	Enable/Disable local echo of command
H0	Hang up	Terminate the TCP connection
I	Device Information	I0 through I9 report information
L	Speaker Volume	Ignored, always answered with OK
M	Speaker On/Off	Ignored, always answered with OK
N	Auto serial speed	N0 no Auto, N1 reports error
O	Return to data mode	
Q	Result Codes	Enable or disable result codes/strings
S=nn/S?	S-Register	Set/request configuration registers
V0/1	Responses	Numeric/text responses to commands
X	Busy/Dial detect	Ignored, always answered with OK
Z	Reset to User profile	Standard

Table 18: IP Modem Standard AT Commands

7.4.1.2 Extended AT-Commands

These commands are used in modern modems, and have slightly different syntax depending on the model.

AT	Standard-Extensions	IP Modem Function
&C	DCD control	When to turn on DCD (by IP Modems DTR)
&D	DTR meaning	Hang Up, Command Mode or Reset
&F	Load factory Default	
&K	Flow Control	
&S	DSR control	When to turn on DSR (by IP Modems DTR)
&V	View Profiles	
&W	Store Profile	&W0/&W1 is "Standard". ATZ1 loads profile 1
&Zn=dd	Save for short dial	Define possible targets by DNS name or IP Address
%C1	V.42bis enable	Ignored
\Q	Flow control	See &K

Table 19: IP Modem Extended AT-Commands

7.4.1.3 Non-AT commands All these commands apply in Command Mode. If a Dial command or an ATA succeeds with a CONNECT, the IP Modem is in data mode. Every data received on the serial port is sent to the other station/IP Modem. And there is a special character sequence in Data Mode, which changes back to Command Mode. This sequence is '+++’ by default, with an interval of 1 second before and after this command; the three characters must appear in one second.

7.4.2 S-Registers for Configuration

Traditional there is a set of registers to control certain operations. These registers are controlled via the AT S-command mentioned above. This is a list of those supported by IP Modem.

Reg.	Function	Range/units	Default
S0	Auto-Answer Ring	0-255	0 (no Auto-Answer)
S1	Ring Counter	0-255	0 (read only)
S2	Escape Code	0-127 (ASCII)	43 (= "+" for "+++")
S3	Carriage Return	0-127	13
S4	Line feed	0-127	10
S5	Backspace	0-32, 127	8
S8	Comma pause	0-255 (seconds)	Accept but ignore
S9	Carrier detect response time	1-255 (0.1 sec)	6
S12	Escape Guard time	20-255 (0.02 sec)	50 (= 1 second)
S25	DTR Ready Delay	0-255 (0.01 sec)	5 (= 50 msecs)
S26	RTS to CTS Delay	0-255 (0.01 sec)	1 (= 10 msecs)
S30	Disconnect Timer	0-90 (seconds)	0 (read only, AT\Tnn)

Table 20: IP Modem S-Registers for Configuration

S0 is frequently used to configure a modem to auto answer incoming calls. S1 may be checked by software if S0 is Zero, i.e. no Auto-Answer. S2 may be set to a different character, if the '+++’ may happen in typical data. Otherwise the software must insert a pause in the transmission.

7.4.3 Sample Commands used by Windows

The NetCom IP Modem is intended for manual installation as kind of a "Standard Modem" in Windows. The reference is the MDMGEN.INF file. The commands used in that file are:

```
"AT&F", "ATA", "ATH", "AT &F E0 V1 &C1 &D2 S95=47 S0=0<cr>", "ATS0=0<cr>", "ATX4",
"ATS7=<#>", "AT%C", "AT\N", "AT&K", "ATS30=<#>", "ATB", "ATDP", "ATDT", "ATL", "ATM"
```

7.5 Description of AT-Commands

The commands are listed more or less in a functional grouping. Configuration commands are listed also with their default settings in brackets.

7.5.1 AT D (dial)

This is the general Dial command. The target is defined as IP Address plus TCP-port number. The dots in the address are replaced by a comma, and the TCP port is also separated by a comma. On normal modems a comma generates a pause in the dialing sequence. This is commonly required, so all software will support it; even multiple comma.

The modifiers 'T' for Touch Tone and 'P' for Pulse dialing have no direct equivalent on the TCP connection. They are used to change between Modem and Host mode, if the ATB command enables this (ATB2 or ATB3). Otherwise the IP Modem will ignore them.

Basically dialing is done to a given IP Address plus a TCP port number. The IP Address is given in decimal Octet format, where comma replaces the dot as the separator. This is followed by another comma, separating the TCP Port from the IP Address. If the port is omitted, the target port is the same as the local TCP Data Port as defined in the configuration of IP Modem (see 6.2.2.2.7 above).

There are situations where the target is known by a DNS name. This name can not be used in a dial string, mostly because very few software will support it. So there is the option of dialing to a pre-defined entry by shortcut. This is given by an 'S' followed by one or two digits. The shortcuts S90 to S99 are reserved; so far only S1 to S4 are implemented. Shortcuts are defined and saved by 'AT&Znn=<FDN:Port>'.

All other non-numeric characters are understood as modifiers. The IP Modem will simply ignore them. This especially applies to space characters. Typically dial strings are:

ATDT192,168,254,254,2003<cr>	Dial another IP Modem as a Modem-to-Modem
AT&Z12=demokit.vscom.com.tw:23<cr>	Define a shortcut for configuration port
ATDPS12<cr>	Dial the other IP Modem as Modem-to-Host

Table 21: IP Modem Sample Dials

7.5.2 AT O (online / data mode)

If a connection is established, the IP Modem can still be in command mode. The ATO activates the transparent data mode.

7.5.3 AT A (answer call)

Have the IP Modem answer an incoming call, and establish a TCP connection. This command is required if Auto-Answer is disabled. Observe the operation mode defined by ATB.

7.5.4 AT B (modulation) [ATB1]

This command is used to define the modulation to use on the phone line. Since the only "modulation" available is IP, there is no choice. The command is used to change between Modem-to-Modem and Modem-to-Host mode.

ATB0	Modem-to-Host mode
ATB1	Modem-to-Modem mode, which is the default
ATB2	Modem-to-Modem when Touch Tone dialing, Modem-to-Host when Pulse dialing. Answer in Modem-to-Modem.
ATB3	Modem-to-Modem when Touch Tone dialing, Modem-to-Host when Pulse dialing. Answer in Modem-to-Host.

Table 22: IP Modem virtual Modulation

7.5.5 AT E (echo) [ATE1]

Disable and enable the echo of the commands received. ATE0 to disable and ATE1 to enable the echo.

7.5.6 AT Q (quiet) [ATQ0]

Configures the IP Modem to remain quiet. The Modem will not send any response messages to the serial port.

7.5.7 AT V (verbose) [ATV1]

Responses as numeric values (ATV0) or as text strings (ATV1).

OK	0	CONNECT	1
RING	2	NO CARRIER	3
ERROR	4	CONNECT 1200	5
NO DIALTONE	6	BUSY	7
NO ANSWER	8		

Table 23: IP Modem Responses

7.5.8 AT H (hangup) [ATH0]

Command to disconnect. Also used as ATH0. The related version ATH1 to just go off-hook is not supported, and reports an ERROR.

7.5.9 AT I(n) (information) [ATI0]

Report technical information about the IP Modem. It is frequently used to identify the device. The answer is always sent as

```
<cr><lf><#response#><cr><lf><cr><lf>OK<cr><lf>
```

Here are the defined #response#-strings.

ATI or ATI0	230	230.4kbps maximum
ATI1	100000000	100Mbps Ethernet
ATI2		
ATI3	Version 1.0 / <compile-date>	Version of Modem-Firmware
ATI4	Current Profile	
ATI5		
ATI6	NetCom 230k IP-Modem	Device Identification
ATI7		
ATI8		
ATI9	(<Name>\Serial#\IP-#:port\Com-X\NetCom)	Display serial port used
ATI10		
ATI11	<very extended information>	

Table 24: IP Modem Information Responses

7.5.10 AT S (setup)

Set and read the S-registers for configuration. `ATSrr?` is a request to read the current value of S-register number `rr`, `ATSrr=nnn` stores the value `nnn` in the register `rr`. Unknown registers report ERROR. See section 7.4.2 above for possible registers and parameters.

7.5.11 AT L (loudness)

and

7.5.12 AT M (speaker)

These commands are answered with OK, but completely ignored. There is no function like speaker.

7.5.13 AT N (auto baud) [ATN0]

Automatic detection of serial speed. For hardware reasons this detection is not implemented. The command `ATN0` to disable automatic detection is accepted and answered with OK. The `ATN1` to enable automatic detection is not available, and answered with the ERROR response.

7.5.14 AT Z (reset)

Reset the configuration to a stored profile. IP Modem only supports profile 0 for simplicity. Same as `ATZ0` or as `AT&F` or `AT&F0`.

7.5.15 AT &F (factory settings) [AT&F0]

This command has historically been designed as "Reset to Factory settings", while ATZ simply meant reset. At time of invention users could change the default behavior of their Modem, so ATZ activated the stored profile.

Nowadays the ATZ is ignored by many software. Instead AT&F is used, followed by complex initialization strings. User may save profiles, which are selected by AT&F0 or AT&F1. There is no longer a documented or commonplace way to revert to Factory Defaults.

The IP Modem has such an option (clear the InitString via Telnet/web), but this is not usable to reset the configuration when the device is used as a Modem. So IP Modem will support only user profile 0, and it uses AT&F9 to really reset the user profile to the Factory defaults.

7.5.16 AT &C (DCD configuration) [AT&C1]

Configure the DCD signal to the PC. As IP Modem this signal may be generated by the DTR output. A standard modem can have DCD always on, and it can have the DCD follow the external carrier signal. When set to always on by AT&C0 the DCD may have a separate source. The DTR is free to serve as a DSR to the PC. The operation of DSR is defined by AT&S, so these commands are related. AT&C1 is the default, the DTR operates as DCD to the PC (this will require a cable connecting NetCom-DTR to the DCD of the PC).

This command has priority over AT&S.

7.5.17 AT &S (DSR configuration) [AT&S0]

Configure the DSR signal to the PC. As IP Modem this signal may be generated by the DTR output. A standard modem can have DSR always on, as long as the Modem has power. Or it can have the DSR signaling whether the IP Modem is in command or in data mode. When set to always on by AT&S0 (this is the default) the DSR may have a separate source. The DTR is free to serve as a DCD to the PC. The operation of DCD is defined by AT&C, so these commands are related. An AT&S1 has DSR follow the data mode.

The AT&C has priority over this command. AT&S1 can only be effective, if AT&C0 is set.

7.5.18 AT &D (DTR configuration) [AT&D2]

Understand the DTR signal of the PC. The input on the IP Modem is the DSR, which requires a proper serial cable. Usually this signal is either ignored, or serves to disconnect from the phone line. There are four options:

AT&D0	Ignore DTR from PC	
AT&D1	Toggle DTR to enter command mode	
AT&D2	Toggle DTR to disconnect and enter command mode	default
AT&D3	Toggle DTR to reset the IP Modem	perform ATZ

Table 25: IP Modem DTR Configuration

7.5.19 AT &K (handshake) [AT&K3]

or as alternative command . . .

7.5.20 AT \Q [AT\Q3]

Configure serial Flow Control. AT&K0 and AT\Q0 disable all Flow Control. The default is AT&K3 and AT\Q3 to use RTS/CTS Hardware Flow Control between PC and IP Modem. AT&K4 and AT\Q1 configure for XON/XOFF Software Flow Control between PC and IP Modem. Other Options are not supported.

7.5.21 AT &V (view profile)

Show Profiles. This will display the current profile, the stored user profile, the short dial strings and the factory profile. Parameters are accepted but ignored. AT&V is AT&V0 and is AT&V1.

7.5.22 AT &W (save profile)

Save the current configuration as user profile. AT&W is the same as AT&W0, all other parameters report an ERROR.

7.5.23 AT &Z (save destination)

This command will save a destination in Internet syntax. It is given by <host>:<port>. The <host> is either an IP Address in dotted octet notation, or an FQN in correct syntax. The <port> is a string representing a decimal number. If :<port> is omitted, the target port is the local TCP Data Port as defined in the configuration of IP Modem (see [6.2.2.2.7](#) above).

8 Print Server Operation

Sometimes the Serial Device Servers are used together with serial printers. These printers are available via a network to several stations for printing. So far there have been two operation modes to achieve this. First the serial port can operate as a TCP Raw Server, and the station just sends the data to print via a TCP connection. As second option a computer running Windows could install the driver for virtual serial ports. The printer is then controlled via this Com port. In both these solutions the buffering of data occurred on the client station. Beginning with Firmware version 2.2 the NetCom Devices offer a true Print Server mode, using the Line Printer Daemon protocol as of RFC1197. Here a print server (lpd) is a station with one IP Address and a single defined port to accept commands and data for printing. Several printers may be attached to the print server. Each printer has a separate data queue for management of print jobs. The data of the jobs is saved in this queue, instead of the client as before.

8.1 Printer Queue

The basic function of an lpd is to accept the data for printing, store it in a spooler queue, and send it to the printer when this is ready for printing. This is done for several queues in parallel. Each printer is identified by the name of the queue, where it is attached to. The NetCom Device Servers allow to configure a custom name for each queue, while the default name is »lpd« plus the number of the serial port (lpd1, lpd2, ...). This name is set in the properties of the serial port. When the lpd is running on a separate computer, the hard disk is used to save the data of the queues. The NetCom Servers neither have a mass storage device, nor huge amounts of memory. Each queue accepts at least one job with a size of up to 250 KB print data. If the job has more data, memory is either assigned dynamically to save the job, or the data is spooled through a ring buffer. Data is printed while the client still sends data. The amount of available dynamic memory depends on the number of ports in a NetCom Device Server, and the operations active on these ports.

8.2 Printer Reset

Before a new job is sent to the printer, this printer should be in a well known state. On a parallel printer port this is easy to achieve. There is a defined signal to send a »reset« command to the printer.

Such a definition is not available for serial printers. Instead there is a reset command, which users may send via the serial line. Typically this command is specific to the manufacturer or even to the printer model. So the NetCom allows to specify this command by entering an 'InitString' for each queue.

8.2.1 Init String Definition

The Initialization of the printer typically involves ASCII control codes, ordinary ASCII characters and some binary data. On some models it may also be necessary to provide a certain state of the modem control signals RTS and DTR, applied with special timing. The 'InitString' in the NetCom Device Serves offer all these options.

8.2.1.1 ASCII Text Ordinary ASCII characters are entered as they are on the keyboard. The single exception is the 'Less Than' character '<', which is used for other special functions.

8.2.1.2 ASCII Control Codes ASCII control codes are entered by their standard name, enclosed in 'Angle Brackets', i.e. in '<' and '>' (Greater Than). Some examples of this are <ESC>, <CR> or <TAB>.

8.2.1.3 Numeric Codes Especially binary data must be sent by means of its numeric value. Since the '<' ASCII character has a special function, the only way to use this is the numeric method. This also applies to printable characters of some Extended ASCII character sets.

The NetCom accept the decimal value, also enclosed in angle brackets. Up to three decimal digits define the character to send to the printer. The '<' is used as <60>, while the <ESC> may also sent as <027>. The '>' may be used directly, however for clarity <62> should be preferred.

8.2.1.4 Modem Control Signals Via the 'InitString' control of RTS and DTR is available. This manual does not make statements about voltage levels on the signals, these are just set to an active or inactive state. <RTS+> and <RTS-> activate and deactivate the RTS signal, while <DTR+> and <DTR-> do the same for DTR.

8.2.1.5 Timing Options Especially when using Modem Control signals it will be required to hold them in a given state for a defined amount of time. This may be done by applying a »Pause«-command in the 'InitString'. The delay is given as numeric value in milliseconds (msec), preceded by a 'P'. So <P50> causes the NetCom to wait 50 msec before proceeding with the next command or start printing. Up to three digits are possible. If more than 999 msec are required, the Pause-command must be repeated.

Please note: The delay is not executed as an exact time. NetCom guarantees to wait at least the required amount of time. The smallest delay possible is 10 msec, due to internal handling of date and time.

8.2.2 Reset Example

For example here is a hypothetical serial printer. The serial port operates at 1200 bps, 7 bit and even parity and 1 stop bit. For Reset the printer requires the command "<ESC>@0" sent with DTR and RTS off. When the data is transmitted, DTR must be on, and 50 msec later RTS must also be on.

Each character sent is 10 bits long, including the start bit. At 1200 bps each character needs 8.3 msec for transmission. So the transmission lasts for 25 msec. To be sure the control signals are inactive, an extra delay is applied after change of signals. The resulting string would be <RTS-><DTR-><P10><ESC>@0<P35><DTR+><P50><RTS+> The delay of 35 msec after the command string "<ESC>@0" shall ensure, all data is completely transmitted to the printer.

8.3 Operation in Windows®

The Printer Server mode may be used to support serial printers in Windows® Operating System. This is a short instruction how to install and use it. Experience on installing printers in Windows is required for this instruction. First the installation of a new printer is given, the modification of an existing printer setup is described later.

8.3.1 Add a New Printer

From »Control Panel« open the »Printers and Faxes« windows. Select the »Add a printer« option. The usual »Add Printer« Wizard appears. Click the "Next" button to select the port, where the printer is attached to.

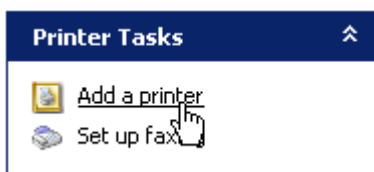


Figure 101: Add a printer

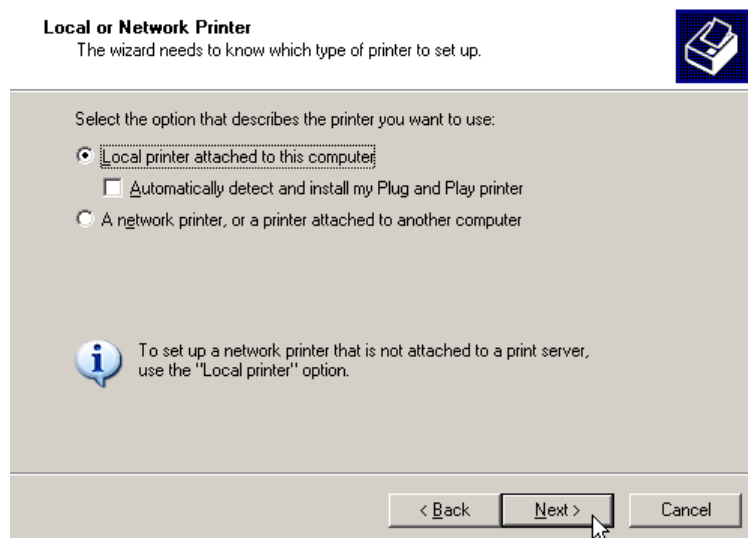


Figure 102: Select Printer Port

Select the option of »Local Printer ...«, but de-select the automatic detection of the printer type as shown below.

Click the "Next" button to continue.

8.3.1.1 Create new printer port You need to create a new port for the printer, the required type is a »Standard TCP/IP Port«.

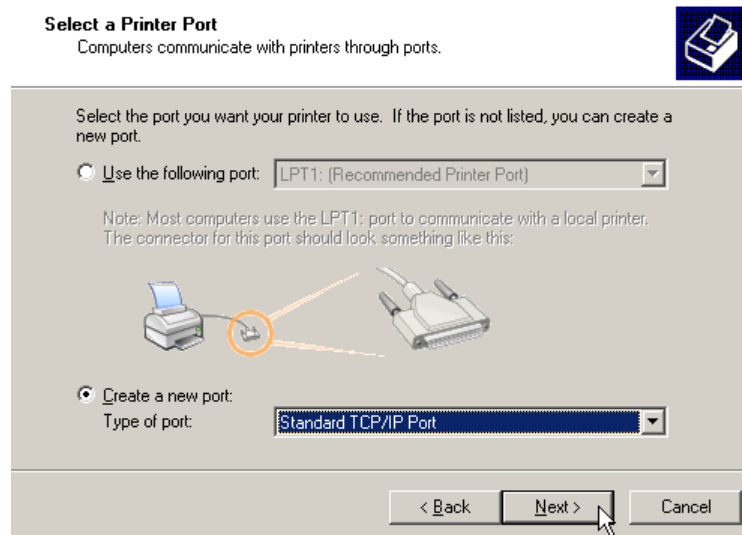


Figure 103: Create Printer Port

In the »Add Standard TCP/IP Port« Wizard just click the "Next" button, and have the NetCom Serial Device Server properly configured for LPD-operation.

8.3.1.2 Name the new Printer Port Then the properties of the new printer port must be entered.

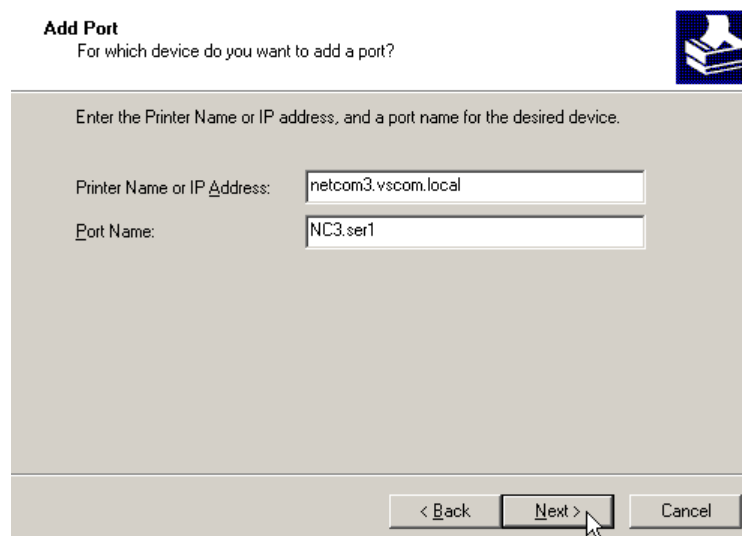


Figure 104: Name-Properties of Print Server Port

You need the network address of the NetCom, this may be the IP Address or a DNS name for the device. The port name is only for internal identification in Windows. It will be listed in the possible ports to connect printers to. The name is similar to »LPT1:« or »Com3:«, but it does not denote any real hardware in your computer. You are free to enter any name not used so far. The name is not related to the LPD Queue name on the NetCom. Again click the "Next" button.

8.3.1.3 Configure the Printer Port As the last step in creating the printer port for your printer you need to enter some additional information. As the »Device Type« select "Custom", and open the "Settings ...".

Figure 105: Mode-Properties of Print Server Port

Under »Port Settings« select the "LPR" protocol instead of the "Raw" method. The Port Number becomes unavailable, because the standard TCP Port 515 is used in this configuration. Enter the Queue name you configured in the NetCom. Each serial port on a NetCom has a separate Queue name to identify it. So it may be a good idea to name the queue after the printer attached to the serial port. Be sure to enable the "Byte Counting", because this is required by the Print Server function in the NetCom. Close these options with the "OK" button.

8.3.1.4 Install Printer Driver Now the printer port is installed, and the Printer installation Wizard continues. Select the printer from the list, or install a new type using an installation disk the usual way.

8.3.2 Modify an Existing Printer

In several situations it is necessary to modify the configuration of a printer, which is already installed in Windows. For example, the mode of use shall be changed to Printer Server Mode, the printer is moved from a local serial port to a NetCom Serial Device Server, or the installation program of the printer only accepts local serial ports to attach the printer to. In such situations it is required to create a new lpd port, and modify the configuration of the printer.

8.3.2.1 Open the properties Again open »Printers and Faxes« in the Control Panel.

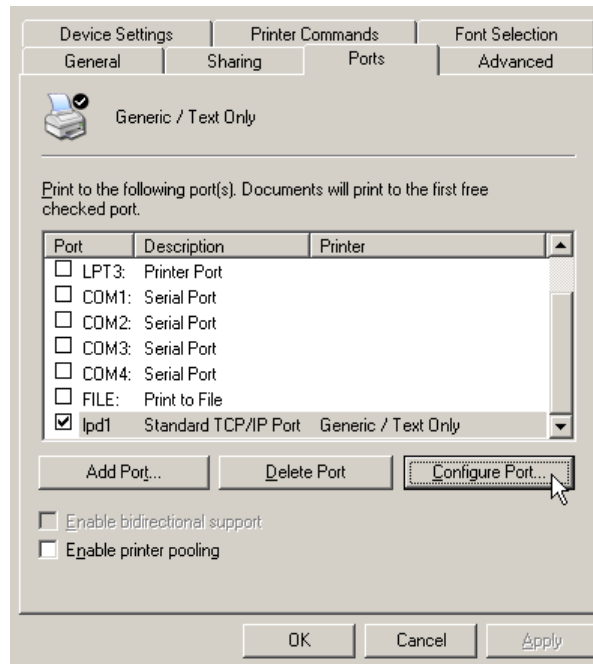


Figure 106: Select Port for Printer

Select the installed printer, and open the properties. In the properties select the tab for »Ports«.

8.3.2.2 Add the Print Server Port The button for "Add Port..." opens a dialog with the possible printer port types.

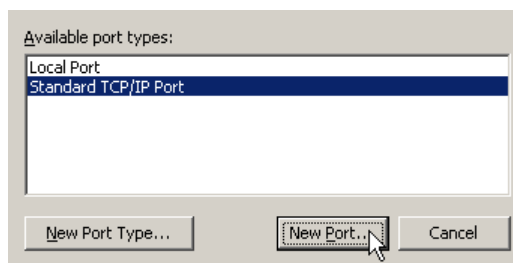


Figure 107: Add Printer Port

Select "Standard TCP/IP Port" and click on "New Port...". This will open the Add TCP Port wizard as of section 8.3.1.1 above. Proceed as described there.

9 OpenVPN™ Encryption

The NetCom PRO Serial Device Servers offer a special method of encrypted communication. Instead of modifying driver and application programs to support encryption (e.g. by using SSL), the NetCom PRO Servers provide a virtual direct network connection between the computer and the NetCom PRO. The function is similar to a cross-over Ethernet cable between the computer and the NetCom PRO. Such a technique is referred to as a "Virtual Private Network" or VPN for short. Encryption on this communication layer is totally different from WLAN Encryption like WEP or WPA, and it is independent of this option.

Applications installed on the computer just see an added network connection, if they really care about network configuration. They do not need to, the system sends and receives all data for and from the NetCom PRO on this new link. Since this link is encrypted, no application cares about it. Even a simple Telnet session becomes secure this way.

To establish the encrypted VPN link the NetCom PRO Servers use an Open Source product named OpenVPN™ (<http://openvpn.net>). OpenVPN™ is licensed under GPL, hence there is no added costs for using it. Currently OpenVPN™ is available for a wide range of systems, including Linux, Windows 2000 and above, as well as Mac OS X.

OpenVPN™ is a product full of features. In conjunction with the NetCom PRO Servers only a limited part is used. The connection is established via a TCP connection, the IP Addresses are assigned static. Further NetCom PRO Servers use the conventional encryption with static-keys based on strong AES cipher (pre-shared keys).

This section in the Manual will give information for the limited installation, and the use together with NetCom PRO Servers.

9.1 OpenVPN™ Installation

As the first step for encrypted communication the system needs the client software for OpenVPN™. This is a quite usual Application Wizard. You have to Accept a License Agreement, which is based on the GPL.

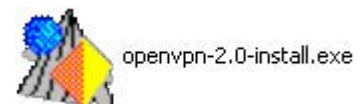


Figure 108: OpenVPN Installation Wizard

In the next step you have the option to select required components. All components are pre-selected. You may safely uncheck the »OpenVPN Source Code«.

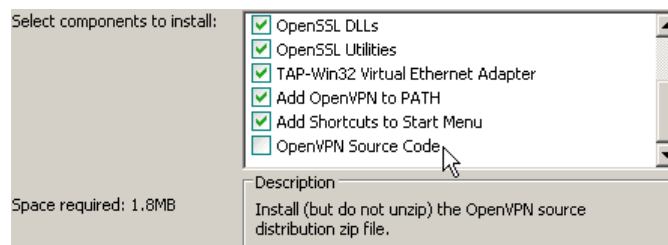


Figure 109: OpenVPN Installable Components

Proceed the installation by choosing a path for the program and related files. »OpenVPN« in your program files folder is suggested as with any other program, just accept it and continue. The Installation Wizard shows a protocol of its activities.

While installing all components, the Installation Wizard has to install a new driver for a virtual network card. Since Windows XP drivers are not only digitally signed, the system also requests either a valid signature or explicit confirmation of installation by the administrator. This time it is about the »TAP-Win32 Adapter« for OpenVPN™.



Figure 110: Installing TAP-Win32 Adapter

Just continue with the installation of OpenVPN. As the result of this installation there is a new entry in your Network Connections folder.

Installed is also a bunch of files and programs in your program files folder, and a new service for OpenVPN™. This service is configured to start "Manually", and is covered in a later section.



Figure 111: OpenVPN Network Adapter

9.2 NetCom OpenVPN Configuration

The next task is to configure the NetCom for encrypted communication. It is assumed the NetCom is already configured for the network. At this step it does not matter if the communication is via Ethernet (Cable) or via WLAN antenna (Wireless), as is mentioned above. Open your web browser, and go to the address of the NetCom Server. Select the 'Tools' page, and activate the option of 'DebugLog' (section 6.2.3.7 above). This is not required for operation, but will help to see what happens on the NetCom.

Next go to the 'Server Configuration' page, and scroll to the section of OpenVPN (section 6.2.1.4 above). Check all parameters to be the same as in the figure 65 above.

Open the 'Configuration-Settings of the Encryption-Key' (figure 67), and click the 'Show' button to display the current key. Save the key in OpenVPN config, in your program files folder. Use

the suggested name of »storedkey.cfg«. Select the Encryption by "AES-256-CBC", which is the default.

Warning: When the NetCom is configured for OpenVPN™ operation, there is no access or configuration without the valid key. Be sure to have all information saved to your system, before enabling the encryption. Otherwise the only way back to normal access is by setting the "Factory Defaults".

Then enable the Logging for NetComs OpenVPN function. Save all changes to the NetCom. Note: OpenVPN function is not enabled so far. This final step is done when everything else is ready, including the configuration of OpenVPN™.

9.3 OpenVPN™ Configuration

OpenVPN may be started in several ways. One option is the command line, which has the most flexibility. The next option is to use the Context-Menu of the configuration file, and finally the installed service for OpenVPN will also open the connection. All three methods are covered in short.

All details about that are given in the documentation on <http://openvpn.net>.

9.3.1 OpenVPN Configuration File

All installed connections by OpenVPN™ are defined and enabled by use of a configuration file. In principle they may also be configured by the command line directly, but a file is simpler to handle. So this manual only deals with such a configuration file.

```
remote 192.168.1.243 1194
dev tap
ifconfig 192.168.127.1 255.255.255.0
secret "..\config\storedkey.cfg"
cipher AES-256-CBC
proto tcp-client
verb 3
```

Figure 112: OpenVPN Configuration File

When installing OpenVPN™, the wizard already created a template named client.ovpn. Open this template in Notepad, typically this is done by just double-clicking on it. The content shall be like this:

Some parameters must be adjusted to the current installation. In the first line there is 192.168.1.243, which is the real IP Address of the NetCom in the (W)LAN. This IP Address may be replaced by a DNS name, which must be known to the client computer. This is the only parameter to adjust throughout this example, since all others are preset by the example configuration.

Also there is 1194 as the TCP port number defined for OpenVPN operation in the NetCom (figure 65).

The third line is the local configuration of the virtual network interface. The computer will use **192.168.127.1** as the own IP Address for the interface of OpenVPN, and **255.255.255.0** as the Netmask on it. This matches the 192.168.127.254, which is configured as the IP Address on the NetCom (figure 65). If several computers shall contact the same NetCom via OpenVPN, each must have a separate IP Address.

The other parameters should be left as they are.

To connect to more than one NetCom, each connection requires a separate configuration file. So it may be useful to name the file after the serial number of the NetCom. Any name is OK, as long as the extension (the Windows "file type") remains as ".ovpn".

9.3.2 Start OpenVPN™ by Context-Menu

This is the moment to open the web browser again, and access the Server Configuration of the NetCom. Go to the OpenVPN Parameter section (figure 65), and carefully double check all values. They must match the example used here. If you are sure, change the first parameter 'OpenVPN' from "Disabled" to "Server". Save the changes, and let the NetCom perform its Reboot. After some time your web browser will attempt to open the Server Configuration page again, but this will fail. This is desired, because now the communication must be done encrypted. The NetCom is still sending answers to PING on the Ethernet (or WLAN), and it will also accept a TCP connection for Debugging on Port 1200. Try it by opening a Telnet session to Port 1200. And finally the NetCom waits for a TCP connection on Port 1194, to establish a link via OpenVPN.

The Installation Wizard of OpenVPN™ associated the ".ovpn" file type with Notepad to open by double click. It also added an action available via the Context-Menu of the file.

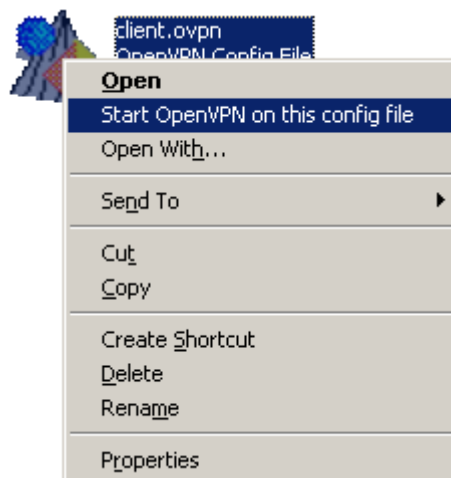


Figure 113: Context-Menu of OpenVPN™

The Context-Menu is available via right click on the file. Select the action "Start OpenVPN" to open the connection to the NetCom. This will start the `openvpn.exe` program in the "bin"-subfolder of OpenVPN. There will be a console window with a lot of text output, after some seconds it will end in the text:

```
Initialization Sequence Completed
```

At this stage the network connection becomes active and usable. Windows will show this with an icon in the System Tray: The speed of "10.0 Mbps" is a virtual speed. The achievable results depend on many parameters. These include the real network speed, the network load, and the number of connected clients.

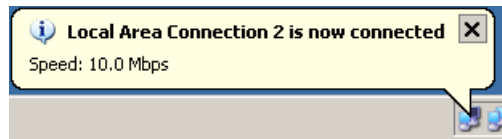


Figure 114: OpenVPN Connection is active

Open your web browser, and enter the IP Address 192.168.127.254 as the target address. The NetCom will answer, and sends the welcome page. Now you have encrypted communication with the NetCom.

Anyone else sniffing on the network (LAN, WLAN, Intra- or Internet) will just see data which appears like garbage. It is required to have the encryption key to get readable information.

The virtual network connection is active as long as the console window with the `openvpn.exe` program is open. Just close the windows, and the connection is closed also.

9.3.3 Start OpenVPN™ by Command line

The most simple way to activate the OpenVPN connection by command line is to use the already prepared configuration file. Open a console window, and change to the "config"-subfolder of OpenVPN. In this folder issue the command to start OpenVPN.

```
CD "Program files\OpenVPN\config"  
..\bin\openvpn --config "client.ovpn"
```

Figure 115: OpenVPN by Command line

There will be a lot of text output, after some seconds it will read as:

```
Initialization Sequence Completed
```

At this stage the network connection becomes active and usable. Use TELNET or PING to test the connection from a second console window. The encrypted link is closed by Ctrl-Break on the keyboard, or by closing the console window of the `openvpn.exe` program.

Instead of using the Context-Menu to start the connection, it may be preferred to create a link to do the job. The command of this must be

```
"C:\Program files\OpenVPN\bin\openvpn.exe" --config client.ovpn
```

and the working directory is "C:\Program files\OpenVPN\config". This link may be placed on the desktop or in the Start Menu.

9.3.4 Start OpenVPN™ as Windows Service

There are possible configurations, which require a functional connection to the NetCom Server without a user logged in. The driver for Virtual Ports is already loaded, however it does not immediately contact the NetCom Server. This is done when the serial port is opened. Without OpenVPN active there is no network link to the NetCom, so the serial port can not be opened.

Since Windows NT there is a method to start applications when the system is ready to have a user logon. Applications created for this task are called services. When such a Service application needs the serial ports of the NetCom, the network link to the NetCom must be functional. In the case of encrypted communication, this requires the `openvpn.exe` program already started.

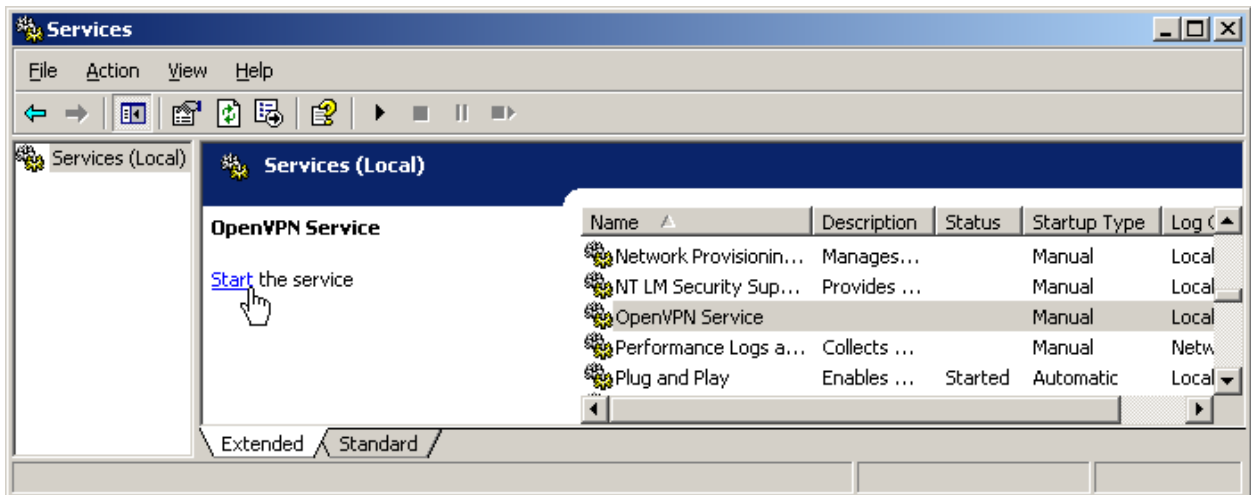


Figure 116: OpenVPN as Windows Service

The Installation Wizard also installed a Windows Service for OpenVPN in the Services applet of the Control Panel. The Startup Type is defined as "Manual", so it does not start without special user interaction or required by a dedicated application.

When the `openvpn.exe` program is started by means of this service, it scans the "config"-subfolder for configuration files of type ".ovpn". Each file causes OpenVPN to establish a connection, at least it attempts to do so. If the NetCom is not available at that moment, OpenVPN will try again and again. When the NetCom becomes available, the connection is established.

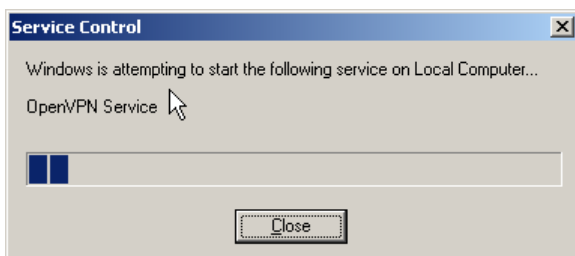


Figure 117: Start OpenVPN Service

For the first test start the Service manually by click on the "Start" link. Windows displays the progress. The connection of OpenVPN will be opened. Verify this by web browser or PING. When



Figure 118: Service Options

a service is started, Windows offers the option to "Stop" or to "Restart" it. Stopping the OpenVPN service will close all connections, Restarting will shortly drop and then re-establish them.

As each other service, also the OpenVPN service has three different types for Startup. When it is Disabled the service can't be started at all. Configured for Manual it requires explicit action to run the software. If the service is configured for Automatic start, the program is run when all drivers are finally loaded, and a user may log on to the system. But note, no user actually needs to log on to start the program. It is started independent from Startup options configured for any user.



Figure 119: Startup Types

When the configuration file "client.ovpn" is in its final state, it may be convenient to set the OpenVPN service to Automatic Startup Type. Even when the Virtual Serial Ports are only used by a dedicated user when he is logged on, nobody needs to care about enabling the network link. It will be simply available.

9.4 OpenVPN™ without Encryption

The implementation of OpenVPN™ in the NetCom Serial Device Servers also offers to use the VPN tunnel without encryption (figure 66, 'Encryption' as "None"). Why should one use a VPN tunnel for encryption, but actually transmit plaintext data? This option provides for a very simple setup to communicate through a complex network of Firewall implementations. As described in section Firewall Traversal Configuration, there are many parameters to provide for passing a Firewall Router, especially when this uses NAT for protection. If there is more than a single Router, this can be a lot of work. Now with OpenVPN™ only one single TCP connection must pass through the Router.

The configuration is much more simple, the Router does not need to have a lot of detailed data. All the different connections required between the Client computer and the NetCom to use the Serial Device Server are carried via this single OpenVPN™ connection in TCP mode. When OpenVPN™ is used this way, probably there is no need for an extra protection by encryption. An encryption of "None" obviously saves computation resources (i.e. performance) on the NetCom and on the Client computer.

9.5 Reconfigure Virtual Serial Ports for OpenVPN™

It may often happen the NetCom is already installed and tested. In this process typically the drivers for Virtual Com Ports are also installed, configured and tested. Now the situation may occur where encryption is a demand. The change of installation is a rather simple process.

First install and test the encrypted connection via OpenVPN™, as described above. Now the Virtual Com Ports are no longer accessible, because this function is blocked on the IP Address used on the standard network connection (Ethernet/WLAN). It is only available on the IP Address provided by OpenVPN™ protocol.

To the driver installation this is the same situation as if the normal IP Address has changed. The configuration requires a change as documented in section 4.4.5.1 about changed IP Address. Proceed as described there, and then use the Virtual Com Ports via the encrypted link.

10 PPP Network for Dial-In and -Out

The Point-to-Point Protocol (PPP) is the state-of-the-art method to establishing a network link over a serial connection. Users are familiar with this software, since a computer regularly uses PPP to establish the link to the Internet via an analogue Modem. PPP encapsulates many other protocols in PPP data frames. This allows to transport IP datagrams on the serial connection, established by the Modem.

The functionality of the NetCom Serial Device Servers is based on a functional network link, which transports IP protocols. The network link may be Ethernet or WLAN, if the second is available. But some serial devices are installed where no standard network is available, e.g. in remotely monitored buildings. It may be more easy to install an ordinary phone line at that place, instead of a complete Ethernet link based on fiber or wire. A Modem is cheap, and connected to this phone system the installation may be contacted by automated systems.

The Modem is connected to one serial port of the NetCom device server, and controlled by the PPP software. Then using the Modem a network link is established. On this link the NetCom device server accepts connections via TCP/IP or UDP, and performs the same tasks available via WLAN, Ethernet or Internet. Obviously this requires a NetCom device server with more than one port. The other ports are used as usual, i.e. in Driver Mode, as TCP server or client, or as any of the many other options.

10.1 PPP User Accounts

The PPP software in the NetCom accepts incoming calls, this is called the Server Mode. It also initiates outgoing calls via the Modem, which is the Client Mode. For special demands the serial port may be configured to perform both tasks at the same time.

The NetCom has two types of user accounts, one type for Dial-In and the other for Dial-Out operation.

10.1.1 PPP Accounts for Dial-In

The accounts for Dial-In simply consist of a username and a password, separated by a colon. They are saved in a global list, the accounts in the list are separated by comma. An example of such a list is "user1:passwd1,user2:passwd2". This list is valid for all serial ports, so the accounts are not restricted for use on certain serial ports. These accounts are used for the PPP-server function in the NetCom. If more than one port is configured for PPP Server Mode, all clients may share the same account. With separate accounts given to clients it is possible later to deny access of a client to the NetCom.

10.1.2 PPP Accounts for Dial-Out

When the NetCom initiates a dial-out call, there is a specified target, defined by the dial string. The NetCom has an extra account defined for this target, i.e. a username and a password for the PPP server. This account is fixed to the serial port. This account is also related to a phone number for the target to dial to.

10.2 PPP Hardware

PPP is available on several types of physical connections. In the strict meaning it is used as PPP over serial connections. The NetCom implement this version of the protocol.

Physical connections may be established in the classical way via a Modem using Dial-up functions. It is also possible to connect directly to the NetCom, using a Null-Modem cable.

10.2.1 PPP Modem Commands

PPP connections are established on serial ports on the NetCom. Typically an ISDN or analogue Modem is attached to the serial port.

A typical Modem requires initialization to configure for operation, and also a certain command to start the dialing process. This is done by two pre-defined strings. With most modern Modems the factory preset configuration is chosen for best performance with PPP appliances, so the Init-String may remain empty. Consult the manual of the Modem to check for required deviations. In most situations the Dial String is just the dial command, e.g. ATDT5558726 for phone 555-8726. However also a combined command ATX3DT5558726 may be used. The dial string is directly sent to the modem, without further interpretation. As is known with Modems, they may require some commands to adjust the operation. This may especially the situation with ISDN Modems, i.e. ISDN Adapters attached to a serial port. These devices will understand the Hayes command set, with some extensions. Please consult the manual of your Modem.

10.2.2 PPP Null Modem Configuration

A Null-Modem cable is another option to run the connection. Such a cable must cross RxD with TxD, RTS with CTS, and also DTR with DCD. Some systems also require to locally connect DCD and DSR, thus connecting both of them with the DTR of the opponent side.

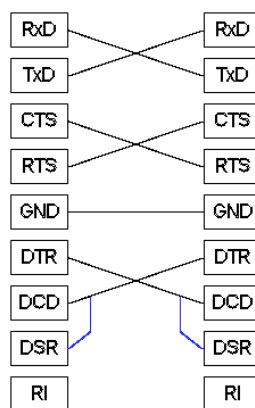


Figure 120: Null Modem Connections

Obviously such a cable does not require configuration. The Init or Dial Strings are not sent via this cable. Further the handling of DTR and RTS is somewhat different from operation with a real Modem.

The PPP function in the NetCom has been tested with Windows and Linux at the other end of the Null-Modem cable. Both functions in the Client and Server modes of PPP, i.e. the operate in both directions.

10.3 PPP Networks

When a PPP-Link is established with the NetCom, this is a new network interface on the NetCom. To transport the IP traffic this interface receives an IP Address. The NetCom suggests default values.

These are selected from the private IP range of 10.0.0.0/8, according to RFC1918. The first octet (number) must be a 10 then. The second octet is simply the number of the serial port. The third number is a 1 for the server mode of NetCom, or a 0 for the client mode. The last octet is a 1 for the local end (on NetCom) of the link, and a 2 for the remote end. The routing on the NetCom is managed automatically, there is no customer option to define specific routes. There is also no option to use IP forwarding. The NetCom can not be used to access it via PPP and this way get full access to the connected Ethernet.

10.3.1 PPP Client

The PPP connection is established when the NetCom has to transport data to the specified target IP Address. If a default gateway is defined in the Server Configuration, there is no need for the PPP connection, the data is transported along this way. If there is no such gateway (e.g. when there is no Ethernet connection at all), the NetCom may require the connection by use of the UDP or TCP Raw Client mode. Also a PING in the Tools menu may start the PPP dial-up.

The NetCom will either receive and use a dynamic IP Address from the connected PPP Server, or it will use the fixed address in the configuration. If configured this new connection may become the new default gateway for all network data transport.

10.3.2 PPP Server

When connecting to the NetCom as a PPP Client, it is recommended to accept the IP Address offered by the NetCom. Otherwise the customer is responsible for proper configuration on his side.

Also it is suggested to define this PPP interface as the default gateway. This is especially the case if the connected client is some kind of Router. Since such a Router and the NetCom do not exchange network routes, the NetCom has no special knowledge on how to send data to a connected TCP or UDP client. It will send all data to the Default Gateway.

11 TCP/IP Description

TCP/IP is the protocol used on the Internet. Nowadays it is also used in local networks. This opens access to any device connected somewhere to the Internet. But a simple contact like plugging in a cable is not enough. The network has to be configured. Your network administrator is responsible to do that. If any question during configuration, ask him. Configuration means to set certain parameters in any device and computer.

Since IP-configuration is a frequent source of problems, a little bit of theory is provided here.

11.1 Recommended Settings

Basically every device on the LAN has a so-called IP Address. In typical small networks the IP Address is similar to 192.168.X.Y, and there is a corresponding netmask of 255.255.255.0. The X ranges from 0 to 255, while Y is from 1 to 254. The combination of X.Y must be unique in your LAN, i.e. two stations must not have the same configuration.

11.1.1 Static Configuration

All stations on the network have a fixed IP Address. In small networks this is typically of the 192.168-type. To configure NetCom for your LAN, it must have the same 192.168.X as your computer, and the same netmask. So it needs a unique Y to establish communication.

11.1.2 DHCP Configuration

Another typical configuration is the automatic configuration. This requires a dedicated server in the LAN, which serves as a so-called DHCP server. Every device can send a request, the reply is a special configuration for this device on the network. The NetCom Devices support DHCP by default, so just use or activate it.

For best operation the DHCP server itself should be configured. It may identify the NetCom Device by its MAC- or Ethernet-Address. There should be an internal database, to always provide the same IP Address to stations with a given MAC. There are free DHCP server programs available⁹ for Windows Operating Systems.

If the DHCP server can not be configured to provide a reserved IP Address to the NetCom, it may happen the NetCom will receive a changed address after some time. This will make the driver for this NetCom inoperative. To solve such problems, driver version 1.5.6 invents the NetCom Helper Service (section [5.8 on page 57](#)) to assist.

⁹[DHCP Server for Windows, TFTP32](#)

11.1.3 Automatic Configuration (APIPA)

A different type of automatic configuration is used by Windows. If a station is prepared for automatic settings, it will search for a DHCP server (see above). But in SOHO networks this server might not exist.

Windows detects this failure, and the computer self-assigns an IP Address. This address is from the reserved LINKLOCAL block for such purposes. The IP Address is like 169.254.N.N, where N.N is from 1.0 to 254.255; the corresponding netmask 255.255.0.0 is mandatory.

The IP Address is selected by random, and checked if already used.

The NetCom Devices do not support this method. However it is possible to assign a static IP Address to the NetCom, which matches the network configuration. Try to find an unused address in your network, starting at 169.254.0.1. Check by PING and ARP, if the address is used. If not, assign it to the NetCom.

This is only a workaround. The better solution is to install or configure a simple DHCP server program. Typical SOHO Internet Routers of today already have such a server. Or you may change your network to static configuration.

11.1.4 Other Configuration

If the configuration of your computer differs from these examples, strong reasons are likely. Ask your network administrator for proper parameters in this situation.

12 Troubleshooting Guide

The most common problems when using NetCom are caused by a failure in the configuration of network parameters. This is a list of some symptoms, and tests to check them.

1. First examine the network configuration of your computer. Open a console window (MSDOS command prompt), and use the command `IPCONFIG /ALL` to retrieve the information. Among other information some data is displayed as this:

Ethernet adapter Local Area Connection:

```
Description.....: <Your LAN card>
Dhcp Enabled.....: Yes
Autoconfiguration Enabled....: Yes
IP Address.....: 192.168.1.154
Subnet Mask.....: 255.255.255.0
DHCP Server.....: 192.168.1.1
```

If DHCP is activated, and there is a DHCP server found, the configuration is OK. A common problem is an IP Address like 169.254.xxx.yyy, because this is an automated address of APIPA. If no DHCP server is present in the network, a static configuration is recommended. Here we prefer the range of 192.168.1.1 up to 192.168.1.254 for computer and NetCom. Change the computers configuration, and select a similar address for NetCom.

2. Start the NetCom Manager program. Search for the device, the Manager performs a discovery of available NetCom devices. Check the properties of each device for a matching serial number. Once the NetCom is identified, check the IP Address and the Netmask. If all this information is displayed as Zero, the IP settings do not match your computers settings. To correct this, you need administrative privileges for your computer. Start the NetCom Manager as Administrator, and configure correct parameters in the NetCom. Close the Manager program.
3. Important: The default configuration of NetCom may result in a fixed IP Address. It will be the same for all connected devices. As a side effect the Manager can not send a dedicated configuration to a certain device. Therefore it is best to connect several NetCom one by one, configure them, connect the next and search for that device.
4. Try to PING the NetCom. Open a console window and use `PING <IP-Address of NetCom>` to send some data. The replies should reach your computer in a few milliseconds. If they time out, check the IP parameters again.
5. Telnet to the NetCom. Open a console window, and use the `Telnet <IP-Address of NetCom>` command to connect. The configuration menu appears. If not, open NetCom Manager, and check the setting

- of **Telnet port** in the NetCom. The default is the name "telnet", or the number 23.
6. Telnet to the serial port of NetCom. Open a console window, and use the Telnet <IP-Address of NetCom> <data port> command to connect. Everything you type is sent out through the serial port. Every data received is displayed on the screen. To check the operation, place a standard loopback plug to the serial port. Then you see your own data as an Echo while typing.
 7. Check the Device Manager for error messages.
 8. Run Hyper Terminal, and open the serial port of NetCom device. Use the loopback plug to see the Echo of your typing. Use a Null Modem cable, and connect it from COM1 to the NetCom. Open a second Window of Hyper Terminal for COM1. Send some data between these two windows. Transfer a file using ZMODEM protocol.
 9. Often so-called Personal Firewall programs cause unspecific errors when other software starts communicating. Check the documentation of the program to see how to allow access.
 10. If some special function is not operative, check for the proper version of the Firmware. In case of doubt install the latest version available (<http://www.vsc.com.de/>).
 11. In rare cases or on special hardware the driver for Windows may have a problem. Please load and install the latest version (<http://www.vsc.com.de/>) and try again. It is necessary to uninstall the previous version.
 12. Transmissions on IP-networks impose some extra delay in transmit and receive times. These can add to between 5 and 10 milliseconds, depending on configurations. Such delays may cause applications to complain about non-functional hardware, in fact it is a protocol/delay problem.
 13. Wireless Connections may fail if the Access Point does not broadcast the SSID. The NetCom Servers need the broadcast to get the parameters from the Access Point. Hiding the SSID is not a security feature anyway.
 14. Many other problems occur because of a failed serial connection, caused by wrong cabling. Here are some frequent causes.
 - a) The serial cable in RS 232 mode may simply be too long. This mostly happens with higher transmission rates.
 - b) In RS 422 and RS 485 it is mandatory to also connect the GND signal of all devices. It is a very frequent error not to do this. The information is transferred (and defined) by the positive or negative difference of the Data+ and Data- lines. However the specification requires a common voltage range between the connected devices. To ensure this range the connection of GND is required.

- c) A network in RS 485 requires biasing resistors (polarization). The Data+ line requires a pull-up resistor to +5V, and the Data- line needs a pull-down resistor to GND. The value is about 750Ω to $1\text{ k}\Omega$. When no station is transmitting, the Data-lines float. This will cause noise and strange errors. The biasing resistors place a differential voltage to the lines, at least 200 mV. These resistors must not exist on the network more than once. Therefore they are not enabled in the NetCom serial ports. To enable them it is necessary to open the case, and set the Jumpers (see section [3.3](#)).

13 Glossary of Terms

AES: Advanced Encryption Standard

The successor of the now insecure DES. AES provides strong and modern encryption, with long keys up to 256 Bit (DES used 56 Bit).

APIPA: Automatic Private IP Addressing

A scheme to self-assign an Address to a network device. The device selects an address of the LINKLOCAL range 169.254.1.0 to 169.254.254.255 by random. If this address is unused, it assigns it to itself. Otherwise the next address is tested. It became widespread with Windows 98. The netmask is 255.255.0.0, these addresses are not routed on the Internet.

ART: Automatic Receive Transmit control

Special control for RS 485 modes. In RS 485 the line driver for transmitting must be disabled (tri-stated) when the device does not send data. In a 2-wire configuration this is known as data direction change, with 4-wire it is called line contention.

CSV: Comma Separated Values

A format to store tabular data in compact text form. Each line describes a new data set. Data fields are separated by a special character. Though the name CSV suggests a comma (','), in reality the delimiting character often is a semicolon or a <TAB> control character.

DHCP: Dynamic Host Configuration Protocol

A service used to retrieve an IP-configuration and optionally much more information from a database server.

FTP: File Transfer Protocol

A common protocol to access a file server.

HTTP: HyperText Transfer Protocol

The protocol used by web browsers to access a web server.

Internet: The net connecting networks

A set of protocols to exchange data between different networks. These information's are carried via a global network of fibers and satellite links.

IP: Internet Protocol

The basic definitions for data packages. These Internet frames are stored and transported embedded in data frames of the local network.

IP Address: Internet Address

The Internet address is noted as a group of 4 decimal numbers (IPv4). Each station on the Internet has a unique address. Some ranges are reserved for private networks, not connected to the Internet.

LINKLOCAL: Address range for private networks

This range 169.254.0.0-169.254.255.255 (Netmask of 255.255.0.0) is reserved for private networks, i.e. not connected to the Internet. Designed for small number of stations, using some automatic configuration scheme. Used with APIPA.

NAT: Network Address Translation

A technique to have a private LAN share one (few) public IP Address(es). With NAT the transport information in IP-frames is replaced by the public data of the NAT-Router.

Netmask: Groups stations to a Net

The AND-operation between the IP Address and the Mask is an important value. When to stations have the same result and the same mask, they are "in the same net". Which means they can communicate direct, without transmitting to a Router.

PAT: Port Address Translation

A technique to share a public IP Address by many internal servers on private addresses. The target address and port is replaced with values stored in an internal table. Mostly used together with NAT.

Router: Transmits data over the Internet

The backbone devices of the Internet. Routers connect two networks together. On one side they receive data frames containing IP-data. They extract these data, and send them on another side; there also stored in data frames of the second network. Typically they connect more than two networks. The basic task is to decide which route the IP-data must take now.

RS 232/V.24: common serial transmission

Characters are sent as separate bits, timing is well defined. The medium is copper cable, using typical +/- 12 Volt. Each signal is defined related to a common ground; one wire per signal plus GND. RS 232 is a point-to-point connection.

RS 422/V.11: Industrial serial transmission (multidrop)

A transmission method with balanced signals. Designed for higher speed, longer cables and is resistive against electrical noise. RS 422 allows for up to 16 receivers. The typical transmission is via twisted pair copper cable using balanced signals. Sender and receivers must share a common voltage range (max. +/-7Volt difference). Two lines per signal, plus common GND. RS 422 is a point-to-multipoint connection.

RS 485: Industrial serial transmission (multipoint)

The signals and cables are the same as RS 422. The transmitters can go tri-state. Several stations can send data on the same lines, at different times. RS 485 is a multipoint-to-multipoint connection.

SNMP: Simple Network Management Protocol

A general purpose configuration system. Devices understanding SNMP may be configured and monitored.

TCP/IP: Transmission Control Program/Internet Protocol

TCP establishes connections between two partners via the Internet. The data is sent in IP-frames, each frame is acknowledged by the recipient. Lost packages are repeated. Software using TCP has a secured transmission; the delivery of the data is guaranteed.

TKIP: Temporal Key Integrity Protocol

An encryption scheme for Wireless LAN. It was developed from the WEP. The key used for encryption is changed while data is transmitted. An attacker will not get enough data with the same key to break the code.

UDP: User datagram protocol

Similar to TCP the data is sent in IP-frames. But in opposite there is no connection or acknowledge by the recipient. The transmission is faster for small data, but data can get lost. Software using UDP must handle the related problems.

UPnP: Universal Plug and Play

Devices announce their presence on the network, and return their capabilities on the network. Depending on the type of device certain configuration is done, specific functions become available.

Specialized software can detect those devices, and offer their services without manual configuration.

VPN: Virtual Private Network

A public network is used to transport data for a limited set of stations. Drivers on these stations generate virtual network cables between the stations. In many installations the communication through the public network is encrypted, to avoid tampering of the lines.

WEP: Wired Equivalent Privacy

An encryption scheme used with early implementations of WLAN. The idea was to make it as difficult to read other persons data, as it was with cable communications. Due to weak definitions in WEP nowadays it may cost an attacker less than a minute to get the current encryption key.

WLAN: short for Wireless LAN

This is a general name, however today this phrase is used for the IEEE 802.11-protocol definitions.

WPA: Wireless Protected Access

This is the successor of WEP. WPA not only includes better/stronger encryption, there is also a set of functions to restrict access by means of user authorization, or different hardware parameters (MAC address, distance).

WPA2: Wireless Protected Access 2

This a modified version of WPA. Most important is the implementation of AES-256 as available cypher.

14 History

November 2008 First release of new manual

December 2008 Firmware version 2.6.0

June 2010 Firmware version 2.6.2
Add NetCom 411 PRO, 811 PRO and 1611RM PRO

July 2011 Added DHCP recommendations
Windows 7 Support included

November_2011 Re-ordered Common characteristics
Firmware 2.6.3

April 2012 Added filter-options to Ethernet
Firmware 2.6.4