

# LANCOM

Systems

## Reference Manual

### *LANCOM 1630 SDSL*

**LANCOM Systems GmbH**

Adenauerstrasse 20 / B2  
52146 Würselen  
Germany  
[www.lancom.de](http://www.lancom.de)

1	Technical summary.....	5
1.1	SW Features.....	5
1.1.1	Operating modes.....	5
1.1.2	ATM features.....	5
1.1.3	Protocol support.....	5
1.1.4	Supported SNMP MIBs.....	6
1.1.5	IPSec.....	7
1.1.6	Firewall and security functions.....	7
2	Parameters.....	8
2.1	Management.....	8
2.1.1	General.....	8
2.1.1.1	Device Name.....	8
2.1.1.2	Location.....	8
2.1.1.3	Administrator.....	8
2.1.1.4	Information.....	8
2.1.2	Security.....	8
2.1.2.1	Configuration access.....	8
2.1.2.1.1	Configuration interfaces.....	8
2.1.2.1.2	IP access list.....	9
2.1.2.2	Configuration password.....	9
2.1.2.2.1	Password.....	9
2.1.2.3	Configuration lock.....	9
2.1.2.3.1	Lock Configuration after.....	9
2.1.2.3.2	Lock Configuration for.....	9
2.1.2.3.3	Console inactivity timeout.....	9
2.2	Communication.....	10
2.2.1	Connections.....	10
2.2.1.1	WAN Connections.....	10
2.2.1.1.1	IPoA (IP over ATM).....	10
2.2.1.1.2	PPPoA (PPP over ATM).....	10
2.2.1.1.3	Plain Ethernet (Ethernet over ATM).....	11
2.2.1.1.4	PPP over Ethernet (PPPoE over ATM).....	11
2.2.1.2	Bridge.....	12
2.2.1.2.1	Bridge Interfaces.....	12
2.2.1.3	Router.....	12
2.2.1.3.1	Router Interfaces.....	12
2.3	Line Settings.....	13
2.3.1	General.....	13
2.3.1.1	Line Code.....	13
2.3.1.2	STU Mode.....	13
2.3.1.3	Additional SDSL BUN options.....	13
2.3.1.3.1	Device Options.....	13
2.3.1.3.2	Port Options.....	13
2.3.2	SHDSL.....	13
2.3.2.1	Auto Baud options.....	13
2.3.2.1.1	Minimum line rate.....	13
2.3.2.1.2	Maximum line rate.....	13
2.3.3	SDSL.....	13

2.3.3.1	General.....	13
2.3.3.1.1	Connection .....	13
2.3.3.1.2	Connect Mode.....	13
2.3.3.1.3	Framing.....	14
2.3.3.2	Fixed Rate Options.....	14
2.3.3.2.1	Fixed Rate.....	14
2.3.3.3	Auto Baud Options .....	14
2.3.3.3.1	Configuration rate.....	14
2.3.3.3.2	Minimum Line rate.....	14
2.3.3.3.3	Maximal Line rate.....	14
2.4	TCP/IP.....	15
2.4.1	DHCP .....	15
2.4.1.1	General.....	15
2.4.1.1.1	DHCP server enabled .....	15
2.4.1.1.2	Allow unknown clients .....	15
2.4.1.2	Lease time.....	15
2.4.1.2.1	Maximum lease time .....	15
2.4.1.2.2	Default lease time.....	15
2.4.1.3	Addresses for DHCP clients .....	15
2.4.1.3.1	IP address ranges .....	15
2.4.1.3.2	Fixed IP addresses.....	15
2.4.2	DNS.....	16
2.4.2.1	DNS relay .....	16
2.4.2.1.1	DNS relaying enabled .....	16
2.4.2.1.2	Relay address .....	16
2.4.2.1.3	Retries.....	16
2.5	IP router.....	17
2.5.1	General.....	17
2.5.1.1	Options.....	17
2.5.1.1.1	IP router active .....	17
2.5.1.1.2	Host routes.....	17
2.5.1.1.3	Poisoned reverse .....	17
2.5.1.2	RIP support .....	17
2.5.1.2.1	Accept.....	17
2.5.1.2.2	Send.....	17
2.5.1.3	Routing.....	18
2.5.1.3.1	Default route.....	18
2.5.1.3.2	Routing table .....	18
2.5.2	Masquerading.....	19
2.5.2.1	Options.....	19
2.5.2.1.1	IP masquerading (NAPT) active.....	19
2.5.2.2	Connections to be masked.....	19
2.5.2.2.1	Interfaces .....	19
2.5.2.3	Inverse masquerading.....	19
2.5.2.3.1	Services .....	19
2.5.3	VPN and Filtering .....	20
2.5.3.1	Information .....	20
2.5.3.1.1	Max. VPN connections.....	20
2.5.3.2	Options.....	20
2.5.3.2.1	Secure Interface.....	20

2.5.3.3	Filter rules.....	20
2.5.3.3.0	Filter .....	20
2.5.3.3.1	function.....	20
2.5.3.3.2	Rules .....	20
2.5.4	VPN .....	21
2.5.4.1	Connections .....	21
2.5.4.1.1	Allow only secure traffic.....	21
2.5.4.1.2	VPN Connections .....	21
2.5.4.1.3	Extranet Services .....	22
2.5.4.2	Proposal lists .....	23
2.5.4.2.1	IKE Proposals .....	23
2.5.4.2.2	IPSec Proposals.....	23
3	Command line reference.....	25
3.1	Help .....	25
3.2	Command rules .....	25
3.3	List of commands.....	25
3.3.1	cd <directory> .....	25
3.3.2	del <name>, rm <name> .....	25
3.3.3	dir [<directory>], ls [<directory>] .....	25
3.3.4	do <name> [<parameters>] .....	25
3.3.5	exit/quit/x .....	25
3.3.6	feature <code> .....	25
3.3.7	ping [IP address].....	25
3.3.8	readconfig.....	25
3.3.9	reboot [default], restart [default].....	25
3.3.10	set <name> <value(s)> .....	26
3.3.11	set [<name>] ? .....	26
3.3.12	sysinfo .....	26
3.3.13	trace [...].	26
3.3.14	up/down/top/bottom <name> .....	26
3.3.15	upload.....	26
3.3.16	writeconfig .....	26

# 1 Technical summary

## 1.1 SW Features

### 1.1.1 Operating modes

TCP/IP Router or Bridge

### 1.1.2 ATM features

- 8 PVCs
- OAM (I.610): F4 and F5 loop back
- VPI range 0...4095
- VCI range 1...65535
- ATM AAL-5
- UBR or CBR, with Peak Cell Rate limitation (PCR)

Encapsulation (RFC 2684, ex RFC 1483)

- LLC encapsulation
- VC based multiplexing

### 1.1.3 Protocol support

PPP (RFC 1661, RFC 1570,

- PPPoE (RFC 2516)
- PPPoA (RFC 2364)
- PAP (RFC 1334)
- CHAP (RFC 1994)
- IPCP (RFC 1332)

IPoA: ATM ARP (RFC 1577, RFC 1293, RFC 1483, RFC 1755)

UDP (RFC 768)

IP (RFC 791, RFC 894, RFC 950, RFC 1122, RFC 1191, RFC 1213, RFC 1812)

ICMP (RFC 792)

TCP (RFC 793)

ARP (RFC 826, RFC 1577)

RIP-1 (RFC 1058),

RIP-2 (RFC 1723),

TELNET (RFC 854, RFC 855, RFC 857, RFC 858)

TFTP (RFC 1350)

IGMP (RFC 2236)

SNMP V2 (RFC 1157)

DHCP server and DHCP client (RFC 2131, RFC 2132)

DNS relay (RFC 1035)

NAT/PAT (IP-Masquerading, RFC 2663)

Application support:

- FTP over NAT
- Quake I, II, III
- Real Audio and Real Video

#### **1.1.4 Supported SNMP MIBs**

MIB II (RFC 1213)

- System
- Interfaces
- Address translation group
- IP
- ICMP
- TCP
- UDP
- SNMP

Bridge MIB (RFC 1493)

- dot1dBase
- dot1dTp
- dot1dStp

PPP/LCP MIB (RFC 1471)

- PPP link

PPP/Security MIB (RFC 1472)

PPP/IP MIB (RFC 1473)

PPP/Bridge MIB (RFC 1474)

LANCOM MIB (on CD-ROM)

Notes: The SNMP read access can be password limited

### 1.1.5 IPSec

*Note: only with LANCOM VPN option kit*

#### Features

- IPSec Tunnel mode
- ESP and AH

#### Encryptions and bit depths:

- DES [56 bit]
- 3-DES [168 bit (eff. 112 bit)]
- CAST [128 bit]
- Blowfish [128, 192, 256, 384 or 448 bit]
- AES [128, 192, 256 bit]

#### Hashes

- MD-5
- SHA-1

#### IPSec throughput rates:

Algorithm	ESP (MD-5)	ESP (SHA-1)	ESP+AH (MD-5)	AH (MD-5)
DES	1,9 Mbps	1,6 Mbps	-	
3-DES	0,9 Mbps	1 Mbps	-	
CAST	-	-	-	
Blowfish (128 bit)	2,2 Mbps	1,9 Mbps	2,3 Mbps	2,3 Mbps
AES (128 bit)	1,9 Mbps	1,6 Mbps	-	

Tunnel setup time: ~ 800 ms/tunnel

### 1.1.6 Firewall and security functions

- Masquerading and inverse masquerading
- Packet filter firewall
- Filter rules based either on 'deny all' or 'allow all' strategy
- Filters for protocols, source and destination IP address and netmask, source and destination port range
- Password protection and access control List for configuration access, selectable per IP address range and protocol (TFTP, HTTP, Telnet, SNMP)
- Adjustable timeout after unsuccessful login attempts

# 2 Parameters

## 2.1 Management

### 2.1.1 General

#### 2.1.1.1 Device Name

String [16]

#### 2.1.1.2 Location

String [64]

#### 2.1.1.3 Administrator

String [64]

#### 2.1.1.4 Information

- Device type: LANCOM 1630 SDSL
- Hardware Release: B
- Firmware Version: 1.21.xxxx
- Format: A.BC.D
- A: Main version number
- B: Subversion number
- C: Sub-Sub-Version-Number
- D: Build-Number
- Serial number:
- Max. VPN connections: Maximum amount of VPN connections, depends on the installed VPN option
- Configuration status

## 2.1.2 Security

### 2.1.2.1 Configuration access

*You can limit access to the configuration to certain interfaces and to certain IP addresses.*

#### 2.1.2.1.1 Configuration interfaces

Table [16], default: empty, e.g.:

Name
USB
Ether
Bridge

*List of interfaces, over which configuration access is allowed.*



### 2.1.2.1.2 IP access list

Table [16], default: empty, e.g.:

First	Last	TFTP	HTTP	Telnet	SNMP
172.19.5.30	172.19.5.40	Yes	Yes	Yes	Yes

First, Last: IP address range

TFTP, HTTP, Telnet, SNMP: [yes, no], default = yes

*Table of configuration access filter*

*The source address table specifies, from which IP addresses the device may be configured and which access is allowed.*

*NOTE: An empty table permits ALL sources to configure the device!*

### 2.1.2.2 Configuration password

#### 2.1.2.2.1 Password

String [32]

### 2.1.2.3 Configuration lock

#### 2.1.2.3.1 Lock Configuration after

Integer [0...255], default = 5 in login failures

#### 2.1.2.3.2 Lock Configuration for

Integer [1...255], default = 5 in minutes

#### 2.1.2.3.3 Console inactivity timeout

Integer [30...999999], default = 60 in seconds

## 2.2 Communication

### 2.2.1 Connections

Configuration overview:

Field	Type	Range	Default	Description
Name	String	[0..16]	""	Arbitrary name of Interface
VPI	Integer	[0..255]	0	ATM Parameter: Virtual Path Identifier
VCI	Integer	[32..65535]	32	ATM Parameter: Virtual Channel Identifier
PCR	Integer	[0..6000]	6000	ATM Parameter: Peak cell rate
Type	List box	[UBR]	UBR	ATM Parameter: Traffic Type
Encapsulation	List box	[LLC, VCMUX] or [LLC] <sup>1)</sup>	LLC	RFC 1483: Method of Encapsulation: - LLC: Logical Link Control - VCMUX: ATM Virtual Circuits (VCs) Based Multiplexing
AC name	String	[0..64]	""	PPPoE: name of access concentrator - If no name is given, the client will attach to any ac
Service	String	[0..32]	""	PPPoE: Name of service - If no name is given, no service name tag will be sent to the ac
Control Protocol	List box	[IPCP, BCP]	IPCP	PPP: IP control protocol or Bridge control protocol
Short Hold	Integer	[0..999999]	0	PPP: Short hold time in seconds - 0: hold time is infinity
Username	String	[0..64]	""	PPP: Arbitrary username
Password	String / hidden	[0..32]	""	PPP: Arbitrary password

<sup>1)</sup> NOTE: For IPoA protocol only LLC is available

*If either username or password is empty no authentication is performed (client and server).*

#### 2.2.1.1 WAN Connections

*Use the following tables to define different types of WAN Connections. Each connection will be used as an interface.*

*The IPoA, PPPoA and PPPoE interface can be attached to the router module, whereas the EoA interface can be attached to the bridge module as well.*

##### 2.2.1.1.1 IPoA (IP over ATM)

Table [0...8], default: empty, e.g.:

Name	VPI	VCI	PCR	Type	Encapsulation
IPOA1	2	34	5000	UBR	LLC

*This interface can only be connected to the router.*

##### 2.2.1.1.2 PPPoA (PPP over ATM)

Table [0...8], default: empty, e.g.:

Name	VPI	VCI	PCR	Type	Encapsulation	Control Protocol	Short hold	Username	Password
PPPOA1	2	34	5000	UBR	LLC	IPCP	3000	Roger.Rabbit	*

*This interface can only be connected to the router.*



### 2.2.1.2 Bridge

Use the following table to specify which interfaces or Connections should be attached to the bridge.

#### 2.2.1.2.1 Bridge Interfaces

Table [0...8], default:

Name	Status
USB	Enabled
ETHER	Enabled

With Status [enabled, disabled]

### 2.2.1.3 Router

Use the following table to specify which interfaces or Connections should be attached to the router.

#### 2.2.1.3.1 Router Interfaces

Table [0...8], default:

Name	Status	IP address	Net mask	Gateway
BRIDGE	Enabled	172.19.5.33	255.255.255.0	0.0.0.0

e.g.:

Name	Status	IP address	Net mask	Gateway
BRIDGE	Enabled	172.19.5.33	255.255.255.0	0.0.0.0
IPOA1	Enabled	192.168.3.2	255.255.255.0	192.168.3.1

## **2.3 Line Settings**

### **2.3.1 General**

#### **2.3.1.1 Line Code**

List box

- SHDSL (G.991.2), default
- SDSL (2B1Q)

#### **2.3.1.2 STU Mode**

List box

- CPE: Customer premised equipment (default)
- CO: Central office

### **2.3.1.3 Additional SDSL BUN options**

#### **2.3.1.3.1 Device Options**

String [64], default ""

#### **2.3.1.3.2 Port Options**

String [64], default ""

### **2.3.2 SHDSL**

#### **2.3.2.1 Auto Baud options**

##### **2.3.2.1.1 Minimum line rate**

Integer [200...2312] in KBit/s, default 200

##### **2.3.2.1.2 Maximum line rate**

Integer [200...2312] in KBit/s, default 2312

### **2.3.3 SDSL**

#### **2.3.3.1 General**

##### **2.3.3.1.1 Connection**

List box

- Auto Baud, default
- Fixed Rate

##### **2.3.3.1.2 Connect Mode**

List box

- Basic
- FlowPoint, default

- GemV1
  - CopperMountain

### 2.3.3.1.3 Framing

List box

- Clear channel, default  
*No framing is performed. ATM-Cells are delivered one after the other without any spacing and encapsulation. If there are no information cells to deliver, empty cells are delivered. Cell borders are recognized via ATM-Header.*
- HDSL-Framing (ITU G.991.1)
- DLCC-Framing

### 2.3.3.2 Fixed Rate Options

#### 2.3.3.2.1 Fixed Rate

Integer [144...2320] in kBit, default 2320

These following 92 different line rates are supported:

[2320, 2288, 2256, 2224, 2192, 2160, 2128, 2096, 2064, 2032, 2000, 1968, 1936, 1904, 1872, 1840, 1808, 1776, 1744, 1712, 1680, 1648, 1616, 1584, 1568, 1552, 1536, 1520, 1488, 1456, 1424, 1392, 1360, 1328, 1296, 1264, 1232, 1200, 1168, 1152, 1136, 1104, 1072, 1040, 1008, 976, 944, 912, 880, 848, 816, 784, 768, 752, 720, 688, 656, 624, 592, 560, 528, 496, 464, 432, 416, 400, 384, 368, 352, 336, 320, 304, 288, 272, 256, 240, 224, 208, 192, 176, 160, 144]

### 2.3.3.3 Auto Baud Options

#### 2.3.3.3.1 Configuration rate

Integer [144...2320] in kBit, default 272

#### 2.3.3.3.2 Minimum Line rate

Integer [144...2320] in kBit, default 784

#### 2.3.3.3.3 Maximal Line rate

Integer [144...2320] in kBit, default 2320

## 2.4 TCP/IP

### 2.4.1 DHCP

#### 2.4.1.1 General

##### 2.4.1.1.1 DHCP server enabled

- On
- Off (default)

##### 2.4.1.1.2 Allow unknown clients

- On (default): Only allow clients configured in the fixed addresses table
- Off

#### 2.4.1.2 Lease time

##### 2.4.1.2.1 Maximum lease time

Integer [1...999999], default is 68.400 in minutes (1 day)

##### 2.4.1.2.2 Default lease time

Integer [1...999999], default is 34.200 in minutes (1/2 day)

#### 2.4.1.3 Addresses for DHCP clients

*You can use ranges of IP addresses to be assigned to the stations in your network, or you can explicitly assign specific IP addresses to specific stations.*

##### 2.4.1.3.1 IP address ranges

Table [0...32], default: empty, e.g.:

Network address	Status	First address	Last address	Net mask	Broadcast address	Name server address	Gateway
172.19.5.0	Enabled	172.19.5.1	172.19.5.10	255.255.255.0	172.19.5.255	172.19.5.33	172.19.5.33

##### 2.4.1.3.2 Fixed IP addresses

Table [0...128], default: empty, e.g.:

Host	Physical address	IP address
PC1	00:50:BF:06:C4:47	172.19.5.25
PC2	00:50:BF:06:C4:48	0.0.0.0

With Host: string [1...16]

*If IP address field is left empty in "Add" an IP address of 0.0.0.0 is generated.*

*If "Allow unknown clients" is switched on, only hosts which are defined in this table will get an IP address.*

*All hosts which are configured with the IP address 0.0.0.0 will get an arbitrary IP address from the DHCP server IP address pool otherwise it will get the specified IP address if it is in the of the DHCP server IP address pool range.*

## **2.4.2 DNS**

### **2.4.2.1 DNS relay**

#### **2.4.2.1.1 DNS relaying enabled**

- On (default)
- Off

#### **2.4.2.1.2 Relay address**

*IP address of DNS Server, default 0.0.0.0*

#### **2.4.2.1.3 Retries**

Integer [1...99], default 5



## 2.5 IP router

### 2.5.1 General

#### 2.5.1.1 Options

##### 2.5.1.1.1 IP router active

- On (default)
- Off

##### 2.5.1.1.2 Host routes

Broadcast also host routing entries

- On
- Off (default)

##### 2.5.1.1.3 Poisoned reverse

*Broadcast also local network routing entry into the same local network.*

- On
- Off (default)

#### 2.5.1.2 RIP support

##### 2.5.1.2.1 Accept

List box: *Configure passive mode*

- Nothing
- RIP-1
- RIP-2
- RIP-1 and RIP-2 (default)

##### 2.5.1.2.2 Send

List box: *Configure active mode*

- Nothing (default)
- RIP-1
- RIP-2

### 2.5.1.3 Routing

#### 2.5.1.3.1 Default route

Edit List box [0...number of Connections], default ""

*Use this table to specify the remote sites to be used to access different remote IP networks.*

#### 2.5.1.3.2 Routing table

Table [0...64], default: empty, e.g.:

Destination IP address	Destination net mask	Route	Distance
172.19.5.29	255.255.255.0	0.0.0.0	1
192.168.3.2	255.255.255.0	192.168.3.1	2

With Distance [0...16] default = 1

## 2.5.2 Masquerading

### 2.5.2.1 Options

#### 2.5.2.1.1 IP masquerading (NAPT) active

- On
- Off (default)

#### 2.5.2.2 Connections to be masked

Use the following table to specify all interfaces or connections for which masquerading of outgoing connections should be enabled.

##### 2.5.2.2.1 Interfaces

Table [0...8], default: empty, e.g.:

Name
IPOA1

#### 2.5.2.3 Inverse masquerading

You can make individual services (a Web Server, for instance) available to people outside your network, by specifying each service in this list.

##### 2.5.2.3.1 Services

Table [0...32], default: empty, e.g.:

Name	Protocol	Port	IP address
IPOA1	UDP	21	192.20.2.1

With

- Protocol [UDP, TCP]
- Port [1...65535]
- IP address: local IP address

## 2.5.3 VPN and Filtering

### 2.5.3.1 Information

#### 2.5.3.1.1 Max. VPN connections

Integer (read only)

*Maximum amount of VPN connections, depends on the installed LANCOM VPN option kit*

### 2.5.3.2 Options

#### 2.5.3.2.1 Secure Interface

Selection list, default: empty, e.g.:

Name
IPOA1

### 2.5.3.3 Filter rules

#### 2.5.3.3.1 Filter function

- Discard all packets with no matching rule ('deny all')
- Transfer all packets with no matching rule ('allow all') (default)

#### 2.5.3.3.2 Rules

"Rules ...": Table [0...128], default:

Prot.	Src. addr.	Src. mask	From	To	Dest. addr.	Dest. mask	From	To	Action	Connecti on <sup>1</sup>
TCP	0.0.0.0	0.0.0.0	137	139	0.0.0.0	0.0.0.0	0	0	Deny	
UDP	0.0.0.0	0.0.0.0	137	139	0.0.0.0	0.0.0.0	0	0	Deny	
UDP	0.0.0.0	0.0.0.0	0	0	0.0.0.0	0.0.0.0	520	520	Deny	
All	0.0.0.0	0.0.0.0	0	0	10.0.0.0	255.0.0.0	0	0	Deny	
All	0.0.0.0	0.0.0.0	0	0	172.16.0.0	255.240.0.0	0	0	Deny	
All	0.0.0.0	0.0.0.0	0	0	192.168.0.0	255.255.0.0	0	0	Deny	
All	0.0.0.0	0.0.0.0	0	0	224.0.0.0	240.0.0.0	0	0	Deny	

With

- Prot: Protocol [all, UDP, TCP, ICMP, ESP, AH, XTP, GRE]
- Src. address: IP network address from source
- Src. Mask: Network mask from source
- From [0...65535]: First port from source port range
- To [0...65535]: Last port from source port range
- Dest. address: IP network address from destination
- Dest. Mask: Network mask from destination

<sup>1</sup> This column is only available if VPN option is installed.

- From [0...65535]: First port from destination port range
- To [0...65535]: Last port from destination port range
- Action: [deny, allow] default: deny

Note:

The following parameters and actions are only available with an installed LANCOM VPN Option Kit:

- Action: [deny, allow, IPSec], default: deny
- VPN connection VPN connection name, default "" (empty)

Note:

An IP address „0.0.0.0“ with mask „0.0.0.0“ represents „any“ network address

### Default filter settings:

- All private networks (10.0.0.0, 172.16.0.0, 192.168.0.0)
- Multicast networks (224.0.0.0)
- NetBIOS (outbound, ports 137-139) [prevents unwanted WAN connections with Windows Networking]
- RIP (inbound, Port 520) [protect routing table from outside changes]

## 2.5.4 VPN

Note: only available if LANCOM VPN option kit installed

### 2.5.4.1 Connections

#### 2.5.4.1.1 Allow only secure traffic

- On
- Off (default)

#### 2.5.4.1.2 VPN Connections

Table [0...MAX\_TUNNELS], default: empty

Name	Extr. addr.	Gateway	IKE	IPSec	Secret	Dynamic
CONN_1	0.0.0.0	0.0.0.0	IKEPROP	IPSECPROP	*	Off

With

- Name: String [1...16], default: "" (empty)
- Extranet address: IP address, used for NAT, default: 0.0.0.0 (NAT inactive). NAT is active if this IP address is unequal 0.0.0.0.
- Gateway: IP address of remote Security Gateway, default: "" (empty)
- IKE: Proposal list taken from "IKE Proposals" table
- IPSec: Proposal list taken from "IPSec Proposals" table

- Secret: String [1...64], pre-shared key
- Dynamic: [off] *Parameter not used in this Version*

Note: MAX\_TUNNELS is depending on the purchased LANCOM VPN option kit

### 2.5.4.1.3 Extranet Services

Table [0...32], default: empty, e.g.:

Name	Protocol	Port	IP address
IPOA1	UDP	21	192.20.2.1

With

- Protocol [UDP, TCP]
- Port [1...65535]
- IP address: local IP address

You can make individual services (a Web Server, for instance) available to people outside your network, by specifying each service in this list.

This NAT is only active if Extranet IP address of the specified connection is unequal 0.0.0.0.

## 2.5.4.2 Proposal lists

### 2.5.4.2.1 IKE Proposals

Table [0...64], list of proposals

Name	Time Limit	PFS Group	Enable Proposal 1	Proposal 1 Cipher	Proposal 1 Hash	Proposal 1 Group
IKE_PROP1	2000	None	On	AES	MD5	5

Enable Proposal 2	Proposal 2 Cipher	Proposal 2 Hash	Proposal 2 Group
On	Blowfish	MD5	5

Enable Proposal 3	Proposal 3 Cipher	Proposal 3 Hash	Proposal 3 Group
On	3DES	MD5	5

With

- Name: string [1...16], default: "" (empty)
- Time Limit: Lifetime [30...30000], default: 2000 seconds
- PFS Group: Perfect-Forward-Security Group [none, 1 (MODP-768), 2 (MODP-1024), 5 (MODP-1536)], default: none
- Enable Proposal 1, 2, 3: [On, Off], default: On
- Proposal 1, 2, 3 Cipher: [AES, AES-128, AES-192, AES-256, BLOWFISH, BLOWFISH-128, BLOWFISH-192, BLOWFISH-256, BLOWFISH-320, BLOWFISH-384, BLOWFISH-448, CAST-128, 3DES, DES], default: Blowfish for proposal 1, AES for proposal 2 and 3DES for proposal 3
- Proposal 1, 2, 3 Hash: [MD5, SHA1], default: MD5
- ? Proposal 1, 2, 3 Group: [1 (MODP-768), 2 (MODP-1024), 5 (MODP-1536)], default: Group 5 for proposal 1 and 2 and group 1 for proposal 3

### 2.5.4.2.2 IPSec Proposals

Table [0...64], list of proposals

Name	Transfer Limit	Time Limit	Enable Proposal 1	Proposal 1 ESP Cipher	Proposal 1 ESP HMAC	Proposal 1 AH HMAC
IPSEC_PROP1	40000	800	On	BLOWFISH	MD5-96	No AH

Enable Proposal 2	Proposal 2 ESP Cipher	Proposal 2 ESP HMAC	Proposal 2 AH HMAC
On	AES	MD5-96	No AH

Enable Proposal 3	Proposal 3 ESP Cipher	Proposal 3 ESP HMAC	Proposal 3 AH HMAC
On	3DES	MD5-96	No AH

With

- Name: string [1...16] Name of proposal list, default: "" (empty)
- Transfer Limit: Lifetime [0...1000000000] Kbytes, default: 40,000 Kbytes
- Time Limit: Lifetime [30...30000] seconds, default: 800 seconds
- Enable Proposal 1, 2, 3: [On, Off], default: On
- Proposal 1, 2, 3 ESP Cipher: [none, AES, AES-128, AES-192, AES-256, BLOWFISH, BLOWFISH-128, BLOWFISH-192, BLOWFISH-256, BLOWFISH-320, BLOWFISH-384, BLOWFISH-448, CAST-128, 3DES, DES], default: Blowfish for Proposal 1, AES for proposal 2 and 3DES for proposal 3
- ? Proposal 1, 2, 3 ESP HMAC: [none, MD5-96, SHA1-96], default: MD5-96
- ? Proposal 1, 2, 3 AH HMAC: [no AH, MD5-96, SHA1-96], default: no AH



# 3 Command line reference

## 3.1 Help

- Syntax: `<command> help`

## 3.2 Command rules

Notes:

- All commands and directory/item names may be abbreviated as long as no ambiguity exists. For example, it is valid to shorten the "restart" command to "res" or a "cd Management" to "c ma". It is, however, not allowed to do a "c /s", since that might mean either "cd /Settings" or "cd /Status".
- Names with blanks in them must be enclosed in double quotes.

## 3.3 List of commands

### 3.3.1 `cd <directory>`

Change the current directory. Certain abbreviations exist, e.g. "cd .." can be abbreviated to "..", "cd /" can be abbreviated to "/" etc.

### 3.3.2 `del <name>, rm <name>`

Delete the table entry with the index <name>.

### 3.3.3 `dir [<directory>], ls [<directory>]`

Display the contents of a directory.

### 3.3.4 `do <name> [<parameters>]`

Execute the action <name> in the current directory. Parameters can be specified.

### 3.3.5 `exit/quit/x`

Close the console session.

### 3.3.6 `feature <code>`

Unlock the feature with the specified feature code.

### 3.3.7 `ping [IP address]`

Issues an ICMP echo request to the specified IP address

### 3.3.8 `readconfig`

Displays the complete configuration of the device in "readconfig" syntax.

### 3.3.9 `reboot [default], restart [default]`

Restart the device. If "default" is specified, the configuration is reset to the factory defaults for the device.

### **3.3.10 set <name> <value(s)>**

Set a configuration item to the specified value. If the item is a table entry, multiple values must be given (one for each table column). A "\*" as a value indicates that the column in question should be left at its previous value.

### **3.3.11 set [<name>] ?**

Show which values are allowed for a configuration item. If <name> is empty, this is displayed for each item in the current directory.

### **3.3.12 sysinfo**

Shows basic system information.

### **3.3.13 trace [...]**

Configures the trace output system for several modules, e.g.

- PPP
- ATM
- IP
- DNS
- DHCP
- all

To activate trace output for a module, type 'trace + [name]'.

Trace output can be deactivated by typing 'trace - [name]'.

Examples:

trace + PPP + DNS

trace - all

Do a "trace help" for further information on configuring the trace system (such as different trace levels).

### **3.3.14 up/down/top/bottom <name>**

Move the table entry with the index <name> to another position within the table.

### **3.3.15 upload**

Go into firmware upload (XModem) mode.

### **3.3.16 writeconfig**

Accept a new configuration in "readconfig" syntax. All subsequent lines are interpreted as configuration values until two blank lines in a row are encountered.