

LANCOM Referenzhandbuch LCOS 5.00

© 2005 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows®, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM Systems, AirLancer und LCOS sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM Systems behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurden (<http://www.openssl.org/>).

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

LANCOM Referenzhandbuch LCOS 5.00, Revision 2

Würselen, 19. Juli 2005

Inhalt

1 Einleitung	13
2 System-Design	17
2.1 Einleitung	17
3 Konfiguration	19
3.1 Mittel und Wege für die Konfiguration	19
3.2 Software zur Konfiguration	19
3.3 Geräte suchen und konfigurieren	20
3.4 Die Konfiguration mit verschiedenen Tools	21
3.4.1 LANconfig	21
3.4.2 WEBconfig	23
3.4.3 Telnet	25
3.4.4 TFTP	29
3.4.5 SNMP	31
3.4.6 Verschlüsselte Konfiguration über SSH-Zugang	31
3.4.7 ISDN-Fernkonfiguration über das DFÜ-Netzwerk	32
3.5 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien	36
3.6 Neue Firmware mit LANCOM FirmSafe	37
3.6.1 So funktioniert LANCOM FirmSafe	37
3.6.2 So spielen Sie eine neue Software ein	38
3.7 Wie führt man einen Gerätereset durch?	40
3.8 Rechteverwaltung für verschiedene Administratoren	41
3.8.1 Die Rechte für die Administratoren	41
3.8.2 Administratorenzugänge über TFTP und SNMP	42
3.8.3 Konfiguration der Benutzerrechte	43
3.8.4 Einschränkungen der Konfigurationsbefehle	46
3.9 Mehrere Loopback-Adressen	47
4 Netzwerk-Management mit den LANtools	48
4.1 Projektmanagement mit LANconfig	48
4.1.1 Verzeichnisstruktur	49
4.1.2 Multithreading	50
4.1.3 Manuelle und automatische Suche nach Firmware-Updates	51
4.1.4 Passwortschutz für SNMP-Lesezugriff	53

4.2 Scripting	55
4.2.1 Anwendungen	55
4.2.2 Funktion des Scripting	56
4.2.3 Scriptdateien erstellen	57
4.2.4 Einspielen von Konfigurations-Befehlen und Script-Dateien	59
4.2.5 Mehrere Script-Sessions parallel	62
4.2.6 Die Befehle für das Scripting	62
4.3 Gruppen-Konfiguration mit LANconfig	66
4.3.1 Anlegen einer Gruppen-Konfiguration	67
4.3.2 Gerätekonfigurationen aktualisieren	68
4.3.3 Gruppen-Konfigurationen aktualisieren	69
4.3.4 Mehrere Gruppen-Konfigurationen verwenden	69
4.4 Anzeige-Funktionen im LANmonitor	70
4.5 LANmonitor – wissen, was läuft	73
4.5.1 Erweiterte Anzeige-Optionen	74
4.5.2 Abfrage der CPU- und Speicherauslastung über SNMP	75
4.5.3 Internet-Verbindung kontrollieren	75
4.6 Visualisierung großer WLANs mit dem WLANmonitor	77
4.6.1 Start des LANCOM WLANmonitors	78
4.6.2 Suche nach Access Points	78
4.6.3 Access Points hinzufügen	79
4.6.4 Access Points organisieren	79
5 Diagnose	81
5.1 Trace-Ausgaben – Infos für Profis	81
5.1.1 So starten Sie einen Trace	81
5.1.2 Übersicht der Schlüssel	82
5.1.3 Übersicht der Parameter	82
5.1.4 Kombinationsbefehle	84
5.1.5 Filter für Traces	84
5.1.6 Beispiele für die Traces	85
5.1.7 Traces aufzeichnen	85
5.2 SYSLOG-Speicher im Gerät	86
5.2.1 SYSLOG-Modul aktivieren	86
5.2.2 SYSLOG-Client konfigurieren	87
5.2.3 SYSLOG-Meldungen auslesen	87
5.3 Der Ping-Befehl	88
5.4 Monitor-Modus am Switch	89

5.5	Kabel-Tester	90
6	Sicherheit	92
6.1	Schutz für die Konfiguration	92
6.1.1	Passwortschutz	92
6.1.2	Die Login-Sperre	94
6.1.3	Einschränkung der Zugriffsrechte auf die Konfiguration	95
6.2	Den ISDN-Einwahlzugang absichern	98
6.2.1	Die Identifikationskontrolle	99
6.2.2	Der Rückruf	100
6.3	Diebstahlschutz mit der ISDN-Standort-Verifikation	101
6.3.1	Konfiguration der ISDN Standort-Verifikation	101
6.3.2	Statusabfrage der ISDN Standort-Verifikation	103
6.4	Die Sicherheits-Checkliste	104
7	Routing und WAN-Verbindungen	108
7.1	Allgemeines über WAN-Verbindungen	108
7.1.1	Brücken für Standard-Protokolle	108
7.1.2	Was passiert bei einer Anfrage aus dem LAN?	108
7.2	IP-Routing	109
7.2.1	Die IP-Routing-Tabelle	110
7.2.2	Policy-based Routing	112
7.2.3	Lokales Routing	114
7.2.4	Dynamisches Routing mit IP-RIP	114
7.2.5	SYN/ACK-Speedup	117
7.3	Die Konfiguration von Gegenstellen	118
7.3.1	Gegenstellenliste	118
7.3.2	Layer-Liste	120
7.4	IP-Masquerading	121
7.4.1	Einfaches Masquerading	122
7.4.2	Inverses Masquerading	124
7.4.3	Demilitarisierte Zone (DMZ)	126
7.4.4	Unmaskierter Internet-Zugang für Server in der DMZ	127
7.5	Multi-PPPoE	128
7.5.1	Anwendungsbeispiel: Home-Office mit privatem Internetzugang	128
7.5.2	Konfiguration	129

7.6	Load-Balancing	130
7.6.1	DSL-Port-Mapping	131
7.6.2	DSL-Kanalbündelung (MLPPPoE)	134
7.6.3	Dynamisches Load-Balancing	135
7.6.4	Statisches Load-Balancing	136
7.6.5	Konfiguration des Load Balancing	136
7.7	N:N-Mapping	139
7.7.1	Anwendungsbeispiele	140
7.7.2	Konfiguration	143
7.8	Verbindungsaufbau mit PPP	146
7.8.1	Das Protokoll	146
7.8.2	Alles o.k.? Leitungsüberprüfung mit LCP	148
7.8.3	Zuweisung von IP-Adressen über PPP	149
7.8.4	Einstellungen in der PPP-Liste	150
7.9	DSL-Verbindungsaufbau mit PPTP	151
7.10	Dauerverbindung für Flatrates – Keep-alive	151
7.11	Rückruf-Funktionen	152
7.11.1	Rückruf nach Microsoft CBCP	152
7.11.2	Schneller Rückruf mit dem LANCOM-Verfahren	154
7.11.3	Rückruf nach RFC 1570 (PPP LCP Extensions)	154
7.11.4	Konfiguration der Rückruf-Funktion im Überblick	155
7.12	ISDN-Kanalbündelung mit MLPPP	155
7.13	Betrieb eines Modems an der seriellen Schnittstelle	157
7.13.1	Einleitung	157
7.13.2	Systemvoraussetzungen	158
7.13.3	Installation	159
7.13.4	Einstellen der seriellen Schnittstelle auf Modem-Betrieb	159
7.13.5	Konfiguration der Modem-Parameter	160
7.13.6	Direkte Eingabe von AT-Befehlen	163
7.13.7	Statistik	163
7.13.8	Trace-Ausgaben	163
7.13.9	Konfiguration von Gegenstellen für V.24-WAN-Schnittstellen	164
7.13.10	Konfiguration einer Backup-Verbindung auf der seriellen Schnittstelle	165
7.13.11	Kontaktbelegung des LANCOM Modem Adapter Kits	166
7.14	Manuelle Definition der MTU	166
7.14.1	Konfiguration	167
7.14.2	Statistik	167

8 Firewall	168
8.1 Gefährdungsanalyse	168
8.1.1 Die Gefahren	168
8.1.2 Die Wege der Täter	169
8.1.3 Die Methoden	169
8.1.4 Die Opfer	170
8.2 Was ist eine Firewall?	170
8.2.1 Die Aufgaben einer Firewall	171
8.2.2 Unterschiedliche Typen von Firewalls	172
8.3 Die Firewall im LANCOM	176
8.3.1 So prüft die Firewall im LANCOM die Datenpakete	176
8.3.2 Besondere Protokolle	180
8.3.3 Allgemeine Einstellungen der Firewall	182
8.3.4 Die Parameter der Firewall-Regeln	185
8.3.5 Die Alarmierungsfunktionen der Firewall	191
8.3.6 Strategien für die Einstellung der Firewall	195
8.3.7 Tipps zur Einstellung der Firewall	197
8.3.8 Konfiguration der Firewall-Regeln	201
8.3.9 Firewall-Diagnose	211
8.3.10 Grenzen der Firewall	218
8.4 Abwehr von Einbruchsversuchen: Intrusion Detection	218
8.4.1 Beispiele für Einbruchsversuche	218
8.4.2 Konfiguration des IDS	219
8.5 Schutz vor "Denial-of-Service"-Angriffen	220
8.5.1 Beispiele für Denial-of-Service-Angriffe	220
8.5.2 Konfiguration der DoS-Abwehr	222
8.5.3 Konfiguration von ping-Blocking und Stealth-Modus	224
9 Quality-of-Service	226
9.1 Wozu QoS?	226
9.2 Welche Datenpakete bevorzugen?	226
9.2.1 Garantierte Mindestbandbreiten	229
9.2.2 Limitierte Maximalbandbreiten	229
9.3 Das Warteschlangenkonzept	230
9.3.1 Sendeseitige Warteschlangen	230
9.3.2 Empfangsseitige Warteschlangen	232
9.4 Reduzierung der Paketlänge	233
9.5 QoS-Parameter für Voice-over-IP-Anwendungen	235

9.6	QoS in Sende- oder Empfangsrichtung	238
9.7	QoS-Konfiguration	239
9.7.1	ToS- und DiffServ-Felder auswerten	239
9.7.2	Minimal- und Maximalbandbreiten definieren	241
9.7.3	Übertragungsraten für Interfaces festlegen	243
9.7.4	Sende- und Empfangsrichtung	244
9.7.5	Reduzierung der Paketlänge	245
10	Virtual Private Networks – VPN	247
10.1	Welchen Nutzen bietet VPN?	247
10.1.1	Private IP-Adressen im Internet?	249
10.1.2	Sicherheit des Datenverkehrs im Internet?	249
10.2	LANCOM VPN im Überblick	250
10.2.1	VPN Anwendungsbeispiel	250
10.2.2	Funktionen von LANCOM VPN	251
10.3	VPN-Verbindungen im Detail	252
10.3.1	LAN-LAN-Kopplung	252
10.3.2	Einwahlzugänge (Remote Access Service)	253
10.4	Was ist LANCOM Dynamic VPN?	254
10.4.1	Ein Blick auf die IP-Adressierung	254
10.4.2	So funktioniert LANCOM Dynamic VPN	255
10.4.3	Hinweise zur Dynamic VPN Lizenzierung	260
10.5	Konfiguration von VPN-Verbindungen	262
10.5.1	VPN-Tunnel: Verbindungen zwischen den VPN-Gateways	262
10.5.2	VPN-Verbindungen einrichten mit den Setup-Assistenten	263
10.5.3	VPN-Regeln einsehen	264
10.5.4	Manuelles Einrichten der VPN-Verbindungen	265
10.5.5	IKE Config Mode	266
10.5.6	VPN-Netzbeziehungen erstellen	267
10.5.7	Konfiguration mit LANconfig	270
10.5.8	Konfiguration mit WEBconfig	274
10.5.9	Diagnose der VPN-Verbindungen	277

10.6	Einsatz von digitalen Zertifikaten	278
10.6.1	Grundlagen	278
10.6.2	Vorteile von Zertifikaten	283
10.6.3	Aufbau von Zertifikaten	284
10.6.4	Sicherheit	286
10.6.5	Zertifikate beim VPN-Verbindungsaufbau	286
10.6.6	Zertifikate von Zertifikatsdiensteanbietern	288
10.6.7	Aufbau einer eigenen CA	288
10.6.8	Anfordern eines Zertifikates mit der Stand-alone Windows CA	289
10.6.9	Zertifikat in eine PKCS#12-Datei exportieren	291
10.6.10	Zertifikate mit OpenSSL erstellen	294
10.6.11	Zertifikate in das LANCOM laden	296
10.6.12	VPN-Verbindungen auf Zertifikatsunterstützung einstellen	297
10.6.13	Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen	302
10.6.14	LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen	306
10.6.15	Diagnose der VPN-Zertifikatsverbindungen	308
10.7	Konkrete Verbindungsbeispiele	308
10.7.1	Statisch/statisch	309
10.7.2	Dynamisch/statisch	310
10.7.3	Statisch/dynamisch (mit LANCOM Dynamic VPN)	310
10.7.4	Dynamisch/dynamisch (mit LANCOM Dynamic VPN)	312
10.7.5	VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“	313
10.8	Wie funktioniert VPN?	316
10.8.1	IPSec – Die Basis für LANCOM VPN	316
10.8.2	Alternativen zu IPSec	317
10.9	Die Standards hinter IPSec	318
10.9.1	Module von IPSec und ihre Aufgaben	318
10.9.2	Security Associations – nummerierte Tunnel	318
10.9.3	Verschlüsselung der Pakete – das ESP-Protokoll	319
10.9.4	Die Authentifizierung – das AH-Protokoll	321
10.9.5	Management der Schlüssel – IKE	323
11	Virtuelle LANs (VLANs)	325
11.1	Was ist ein Virtuelles LAN?	325
11.2	So funktioniert ein VLAN	325
11.2.1	Frame-Tagging	326
11.2.2	Umsetzung in den Schnittstellen des LANs	327
11.2.3	Anwendungsbeispiele	328

11.3	Konfiguration von VLANs	330
11.3.1	Die Netzwerktafel	330
11.3.2	Die Porttafel	330
11.3.3	Konfiguration mit LANconfig	331
11.3.4	Konfiguration mit WEBconfig oder Telnet	332
12	Wireless LAN – WLAN	334
12.1	Was ist ein WLAN?	334
12.1.1	Standardisierte Funkübertragung nach IEEE	334
12.1.2	Die Betriebsarten von Funk-LANs und Basis-Stationen	337
12.2	Entwicklung der WLAN-Sicherheit	344
12.2.1	Einige Grundbegriffe	344
12.2.2	WEP	345
12.2.3	WEPplus	347
12.2.4	EAP und 802.1x	347
12.2.5	TKIP und WPA	349
12.2.6	AES und 802.11i	351
12.2.7	Fazit	353
12.3	Absicherung des Funknetzwerks	353
12.3.1	LEPS – LANCOM Enhanced Passphrase Security	354
12.3.2	Standard-WEP-Verschlüsselung	356
12.4	Konfiguration der WLAN-Parameter	357
12.4.1	WLAN-Sicherheit	357
12.4.2	Allgemeine WLAN-Einstellungen	366
12.4.3	WLAN-Routing (Isolierter Modus)	367
12.4.4	Die physikalischen WLAN-Schnittstellen	368
12.4.5	Die logischen WLAN-Schnittstellen	376
12.4.6	Zusätzliche WLAN-Funktionen	380
12.5	IEEE 802.11i für Punkt-zu-Punkt-Verbindungen im WLAN	382
12.5.1	Mehr Sicherheit im P2P-Betrieb	382
12.5.2	Konfiguration	382
12.6	Aufbau von Outdoor-Funknetz-Strecken	385
12.6.1	Geometrische Auslegung der Funkstrecke	385
12.6.2	Antennen-Leistungen	387
12.6.3	Abstrahlleistung und maximale Distanz	390
12.6.4	Reduzieren der Sendeleistung	392

13 Backup-Lösungen	393
13.1 Hochverfügbarkeit von Netzwerken	393
13.1.1 Wie wird die Störung einer Netzwerkverbindung erkannt?	393
13.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung	398
13.1.3 Hochverfügbarkeit der Gateways – redundante Gateways mit VPN Load Balancing	400
13.1.4 Hochverfügbarkeit des Internetzugangs – Multi-PPPoE	401
13.1.5 Anwendungsbeispiele	401
14 Bürokommunikation mit LANCAPI	405
14.1 Welche Vorteile bietet die LANCAPI ?	405
14.2 Das Client-Server-Prinzip	405
14.2.1 Konfiguration des LANCAPI-Servers	406
14.2.2 Installation des LANCAPI-Clients	408
14.2.3 Konfiguration des LANCAPI-Clients	408
14.3 So setzen Sie die LANCAPI ein	409
14.4 Das LANCOM CAPI Faxmodem	409
14.5 LANCOM Faxmodem-Option	410
14.6 Unterstützte B-Kanal-Protokolle	411
15 Weitere Dienste	412
15.1 Automatische IP-Adressverwaltung mit DHCP	412
15.1.1 Der DHCP-Server	412
15.1.2 DHCP – 'Ein', 'Aus', 'Auto', 'Client' oder 'Weiterleiten'?	413
15.1.3 So werden die Adressen zugewiesen	414
15.2 DNS	417
15.2.1 Was macht ein DNS-Server?	417
15.2.2 DNS-Forwarding	418
15.2.3 So stellen Sie den DNS-Server ein	420
15.2.4 URL-Blocking	422
15.2.5 Dynamic DNS	423
15.3 Gebührenmanagement	425
15.3.1 Verbindungs-Begrenzung für DSL und Kabelmodem	425
15.3.2 Gebührenabhängige ISDN-Verbindungsbegrenzung	427
15.3.3 Zeitabhängige ISDN-Verbindungsbegrenzung	427
15.3.4 Einstellungen im Gebührenmodul	428
15.4 Das SYSLOG-Modul	428
15.4.1 Einrichten des SYSLOG-Moduls	429
15.4.2 Beispielkonfiguration mit LANconfig	429

15.5	Zeit-Server für das lokale Netz	431
15.5.1	Konfiguration des Zeit-Servers unter LANconfig	431
15.5.2	Konfiguration des Zeit-Servers mit WEBconfig oder Telnet	432
15.5.3	Konfiguration der NTP-Clients	432
15.6	Scheduled Events	433
15.6.1	Zeitautomatik für LCOS-Befehle	433
15.6.2	Die Cron-Tabelle	435
15.6.3	Konfiguration der Zeitautomatik	436
15.7	Port-Mapping	437
15.7.1	Freies Umsetzen von TCP/IP-Ports auf maskierten Verbindungen	437
15.7.2	Konfiguration	437
16	Anhang	439
16.1	Fehlermeldungen im LANmonitor	439
16.1.1	Allgemeine Fehlermeldungen	439
16.1.2	VPN-Fehlermeldungen	439
16.2	SNMP-Traps	443
16.3	Funkkanäle	444
16.3.1	Funkkanäle im 2,4 GHz Frequenzband	444
16.3.2	Funkkanäle im 5 GHz Frequenzband	445
16.3.3	Funkkanäle und Frequenzbänder für Indoor- und Outdoor-Verwendung	446
16.4	Unterstützte RFCs	448
16.5	Glossar	449
16.6	Übersicht über die Funktionen nach Modellen und LCOS*-Versionen	454
17	Index	460

1 Einleitung

Erweiterungen in LCOS 4.00

- ▶ 'Verschlüsselte Konfiguration über SSH-Zugang' →Seite 31
- ▶ 'VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“' →Seite 313
- ▶ 'Rechteverwaltung für verschiedene Administratoren' →Seite 41
- ▶ 'Manuelle Definition der MTU' →Seite 166
- ▶ 'LEPS – LANCOM Enhanced Passphrase Security' →Seite 354
- ▶ 'Standard-WEP-Verschlüsselung' →Seite 356
- ▶ 'Port-Mapping' →Seite 437
- ▶ 'Mehrere Loopback-Adressen' →Seite 47
- ▶ 'IEEE 802.11i für Punkt-zu-Punkt-Verbindungen im WLAN' →Seite 382
- ▶ 'Multi-PPPoE' →Seite 128
- ▶ 'IKE Config Mode' →Seite 266
- ▶ 'SYSLOG-Speicher im Gerät' →Seite 86

Erweiterungen in LCOS 4.10

- ▶ 'Hochverfügbarkeit von Netzwerken' →Seite 393
- ▶ 'Betrieb eines Modems an der seriellen Schnittstelle' →Seite 157
- ▶ 'Der Ping-Befehl' →Seite 88
- ▶ 'Firmware, Geräte-Konfiguration oder Script über TFTP laden' →Seite 29

Erweiterungen in LCOS 5.00

- ▶ 'Scripting' →Seite 55
- ▶ 'Einsatz von digitalen Zertifikaten' →Seite 278
- ▶ 'Adress-Anpassung' →Seite 374
- ▶ 'Client-Bridge-Unterstützung' →Seite 375
- ▶ 'DSL-Port-Mapping' →Seite 131
- ▶ 'Dynamisches Load-Balancing' →Seite 135
- ▶ 'Policy-based Routing' →Seite 112
- ▶ 'Monitor-Modus am Switch' →Seite 89
- ▶ 'Diebstahlschutz mit der ISDN-Standort-Verifikation' →Seite 101
- ▶ 'Gruppen-Konfiguration mit LANconfig' →Seite 66
- ▶ 'Visualisierung großer WLANs mit dem WLANmonitor' →Seite 77
- ▶ 'Automatische Auswahl der 5GHz-WLAN-Kanäle über DFS mit Black- und White-List' →Seite 369



Aufgrund der begrenzten Hardwaremöglichkeiten können nicht mehr alle der älteren Modelle mit der aktuellen LCOS-Version auf die hier vorgestellten Funktionen aufgerüstet werden. Bitte informieren Sie sich in der Übersichtstabelle ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' →Seite 454), welche Funktionen von Ihrem Gerät unterstützt werden.

Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus zwei Teilen: Dem Benutzerhandbuch und dem Referenzhandbuch.

- ▶ In den jeweiligen Benutzerhandbüchern der LANCOM-Geräte wird die Hardware dokumentiert. Neben der Beschreibung des speziellen Funktionsumfangs der verschiedenen Modelle finden Sie in den Benutzerhandbüchern Informationen über die Schnittstellen und Anzeigeelemente der Geräte sowie Anleitungen zur grundlegenden Konfiguration mit Hilfe der Assistenten.
- ▶ Sie lesen derzeit das Referenzhandbuch. Das Referenzhandbuch beschreibt alle Funktionen und Einstellungen der aktuellen Version von LCOS, dem Betriebssystem aller LANCOM-Router und LANCOM Wireless Access Points. Das Referenzhandbuch bezieht sich auf einen bestimmten Softwarestand, nicht aber auf eine spezielle Hardware.

Es ergänzt das Benutzerhandbuch und geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Dazu zählen beispielsweise:

- ▷ Systemdesign des Betriebssystems LCOS
- ▷ Konfiguration
- ▷ Management
- ▷ Diagnose
- ▷ Sicherheit
- ▷ Routing- und WAN-Funktionen
- ▷ Firewall
- ▷ Quality of Service (QoS)
- ▷ Virtuelle Private Netzwerke (VPN)
- ▷ Virtuelle lokale Netzwerke (VLAN)
- ▷ Drahtlose Netzwerke (WLAN)
- ▷ LANCAPI
- ▷ weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

LCOS, das Betriebssystem der LANCOM-Geräte

Alle LANCOM-Router und LANCOM Wireless Access Points setzen das gleiche Betriebssystem ein: das LCOS. Das von LANCOM Systems selbst entwickelte Betriebssystem ist von außen nicht angreifbar und bietet so eine hohe Sicherheit. Darüber hinaus steht die konsistente Verwendung von LCOS für eine komfortable und durchgängige Bedienung über alle LANCOM-Produkte. Das umfangreiche Featureset ist für alle LANCOM-Produkte (bei entsprechender

Unterstützung durch die Hardware) gleich verfügbar und wird durch kostenlose, regelmäßige Software-Updates ständig weiter entwickelt.

In diesem Referenzhandbuch gelten folgende Abgrenzungen von Software, Hardware und Hersteller:

- ▶ 'LCOS' bezeichnet das geräteunabhängige Betriebssystem
- ▶ 'LANCOM' steht als Oberbegriff für alle LANCOM-Router und LANCOM Wireless Access Points
- ▶ 'LANCOM Systems' steht als Kurzform für den Hersteller, die LANCOM Systems GmbH

Gültigkeit

Das vorliegende Referenzhandbuch gilt für alle LANCOM-Router und LANCOM Wireless Access Points mit einem Firmwarestand Version 5.00 oder neuer.

Die in diesem Referenzhandbuch beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt. Im Anhang befindet sich eine Tabelle, in der für die einzelnen Funktionen vermerkt ist, ab welcher Firmware-Version sie in den entsprechenden Geräte unterstützt werden ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' →Seite 450).

Die Abbildungen von Geräten sowie die Screenshots stellen immer nur Beispiele dar, die nicht unbedingt exakt dem aktuellen Firmwarestand entsprechen müssen.

Sicherheitseinstellungen

Für einen sorglosen Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z.B. Firewall, Verschlüsselung, Zugriffsschutz, Gebührensperre) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Der LANconfig-Assistent 'Sicherheitseinstellungen' unterstützt Sie bei dieser Aufgabe. Weitere Informationen zu diesem Thema finden Sie auch im Kapitel 'Sicherheit' auf Seite 92.

Zusätzlich bitten wir Sie, sich auf unserer Internet-Seite www.lancom.de über technische Weiterentwicklungen und aktuelle Hinweise zu Ihrem Produkt zu informieren und ggf. neue Software-Versionen herunterzuladen.

An der Erstellung dieser Dokumentation ...

... haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de



Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen (‘FAQs’)“. Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.

Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

Hinweis-Symbole



Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.



Wichtiger Hinweis, der beachtet werden sollte.



Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

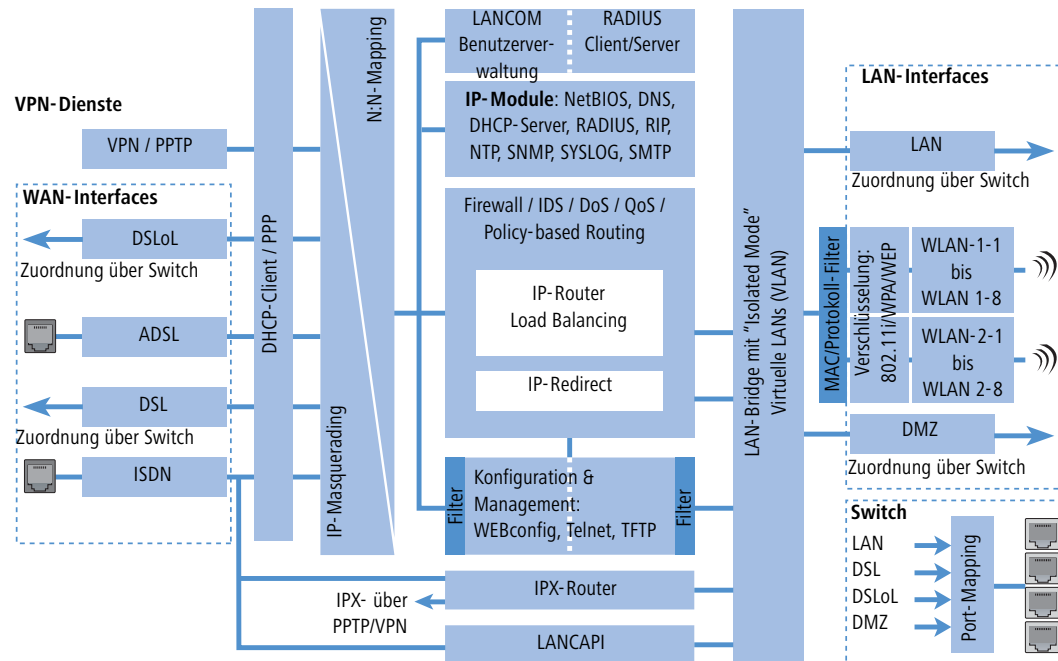
2 System- Design

2.1 Einleitung

Das LANCOM-Betriebssystem LCOS ist aus einer Vielzahl von verschiedenen Software-Modulen aufgebaut, die LANCOM-Geräte selbst verfügen über unterschiedliche Schnittstellen (Interfaces) zum WAN und zum LAN hin. Je nach Anwendung laufen die Daten auf dem Weg von einem Interface zum anderen über verschiedene Module.

Das folgende Blockschaltbild zeigt ganz abstrakt die generelle Anordnung der LANCOM-Interfaces und LCOS-Module. Die Beschreibungen der einzelnen Funktionen im weiteren Verlauf dieses Referenzhandbuchs greifen diese Darstellung jeweils auf, um die wichtigen Verbindungen der jeweiligen Anwendungen darzustellen und die daraus resultierenden Konsequenzen abzuleiten.

So kann dieses Schaubild z.B. verdeutlichen, bei welchen Datenströmen die Firewall zum Einsatz kommt oder an welcher Stelle bei einer Adressumsetzung (IP-Masquerading oder N:N-Mapping) welche Adressen gültig sind.



Hinweise zu den einzelnen Module und Interfaces:

- Der IP-Router sorgt für das Routing der Daten auf IP-Verbindungen zwischen den Interfaces aus LAN und WAN.
- Beim IP-Redirect werden Anfragen an ausgewählte Dienste im LAN gezielt auf bestimmte Rechner umgeleitet.

▷ Einleitung

- ▶ Die Firewall (mit den Diensten "Intrusion Detection", "Denial of Service" und "Quality of Service") umschließt den IP-Router wie eine Hülle. Alle Verbindungen über den IP-Router gehen also automatisch auch durch die Firewall.
- ▶ Als Schnittstellen ins LAN stellen die LANCOM-Geräte ein separates LAN-Interface oder einen integrierten Switch mit mehreren LAN-Interfaces bereit.
- ▶ LANCOM Wireless Access Points bzw. LANCOM-Router mit Wireless-Modul bieten daneben zusätzlich eine oder je nach Modell auch zwei Funkschnittstellen für die Anbindung von Wireless LANs. Jede Funkschnittstelle kann je nach Modell bis zu acht verschiedene WLAN-Netzwerke aufbauen („Multi-SSID“).
- ▶ Mit der DMZ-Schnittstelle kann bei einigen Modellen eine demilitarisierte Zone (DMZ) eingerichtet werden, die auch physikalisch in der LAN-Bridge von den anderen LAN-Interfaces getrennt ist.
- ▶ Die LAN-Bridge verfügt über einen Protokoll-Filter, der das Sperren von dedizierten Protokollen auf dem LAN ermöglicht. Darüber hinaus können durch den "Isolated Mode" einzelne LAN-Interfaces voneinander getrennt werden. Durch den Einsatz der VLAN-Funktionen können in der LAN-Bridge virtuelle LANs eingerichtet werden, die auf einer physikalischen Verkabelung den Betrieb von mehreren logischen Netzen erlaubt.
- ▶ Mit den verschiedenen IP-Modulen (NetBIOS, DNS, DHCP-Server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP) können die Anwendungen über den IP-Router oder direkt über die LAN-Bridge kommunizieren.
- ▶ Die Funktionen "IP-Masquerading" und "N:N-Mapping" sorgen für die geeignete Umsetzung von IP-Adressen zwischen den privaten und dem öffentlichen IP-Bereichen oder auch zwischen mehreren privaten Netzwerken.
- ▶ Auf die Dienste für Konfiguration und Management der Geräte (WEBconfig, Telnet, TFTP) kann von LAN- und auch von WAN-Seite aus (bei entsprechender Berechtigung) direkt zugegriffen werden. Diese Dienste sind durch Filter und Login-Sperre geschützt, es erfolgt hier jedoch **kein** Durchlauf durch die Firewall. Ein direktes "Durchgreifen" aus dem WAN in das LAN (oder umgekehrt) **über** die internen Dienste als Umweg um die Firewall ist jedoch **nicht** möglich.
- ▶ IPX-Router und LANCAPI greifen auf der WAN-Seite nur auf das ISDN-Interface zu. Beide Module sind unabhängig von der Firewall, die nur den Datenverkehr durch den IP-Router überwacht. Für IPX über VPN kann der IPX-Router zusätzlich direkt auf das PPTP/VPN-Modul zugreifen.
- ▶ Die VPN-Dienste (inklusive PPTP) erlauben das Verschlüsseln der Daten im Internet und damit den Aufbau von virtuellen privaten Netzwerken über öffentliche Datenverbindungen.
- ▶ Mit DSL, ADSL und ISDN stehen je nach Modell verschiedene WAN-Interfaces zur Verfügung.
- ▶ Das DSLoL-Interface (DSL over LAN) ist kein physikalisches WAN-Interface, sondern eher eine "virtuelle WAN-Schnittstelle". Mit der entsprechenden Einstellung im LCOS kann bei einigen Modellen ein LAN-Interface **zusätzlich** als DSL-Interface genutzt werden.

3 Konfiguration

In diesem Kapitel geben wir Ihnen einen Überblick, mit welchen Mitteln und über welche Wege Sie auf das Gerät zugreifen können, um Einstellungen vorzunehmen. Sie finden Beschreibungen zu folgenden Themen:

- ▶ Konfigurationstools
- ▶ Kontroll- und Diagnosefunktionen von Gerät und Software
- ▶ Sicherung und Wiederherstellung kompletter Konfigurationen
- ▶ Installation neuer Firmware im Gerät

3.1 Mittel und Wege für die Konfiguration

LANCOM sind flexible Geräte, die verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszügen) für die Konfiguration unterstützen. Zunächst der Blick auf die möglichen Wege.

LANCOM-Produkte können Sie über bis zu drei verschiedene Zugänge erreichen (je nach verfügbaren Anschlüssen):

- ▶ über das angeschlossene Netzwerk (sowohl LAN als auch WAN oder WLAN – Inband)
- ▶ über die Konfigurations-Schnittstelle (Config-Schnittstelle) des Routers (auch Outband genannt)
- ▶ Fernkonfiguration über den ISDN-Anschluss oder über ein Modem (analog oder GSM, in Verbindung mit dem LANCOM Modem Adapter Kit)

Nicht bei allen
Geräte verfüg-
bar

Nicht bei allen
Geräte verfüg-
bar

Was unterscheidet nun diese drei Wege?

Zum einen die Verfügbarkeit: Die Konfiguration über Outband ist immer verfügbar. Die Inband-Konfiguration ist jedoch z.B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist. Auch die ISDN-Fernkonfiguration ist abhängig von einer ISDN-Verbindung.

Zum anderen die Anforderungen an zusätzliche Hard- und Software: Die Inband-Konfiguration benötigt neben dem ohnehin vorhandenen Rechner im LAN, WAN oder WLAN nur noch eine geeignete Software, beispielsweise LANconfig oder WEBconfig (vgl. folgender Abschnitt). Die Outband-Konfiguration benötigt zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle. Für die ISDN-Fernkonfiguration sind die Voraussetzungen am umfangreichsten: Neben einem ISDN-Anschluss am LANCOM wird im Konfigurations-PC ein ISDN-Adapter oder Zugriff über LANCAPI auf einen weiteren LANCOM mit ISDN-Schnittstelle benötigt.

3.2 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich – aber auch die persönlichen Ansprüche und Vorlieben der Ausführenden. LANCOM-Router verfügen daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- ▶ **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines LANCOM einstellen. LANconfig benötigt einen Konfigurationsrechner mit Windows 98 oder höher.

▷ Geräte suchen und konfigurieren

- ▶ **WEBconfig** – diese Software ist fest eingebaut im Router. Auf dem Konfigurationsrechner wird nur ein Web-Browser vorausgesetzt. WEBconfig ist dadurch betriebssystemunabhängig.
- ▶ **SNMP** – geräteunabhängige Programme zum Management von IP-Netzwerken basieren üblicherweise auf dem Protokoll SNMP.
- ▶ **Terminalprogramm, Telnet** – ein LANCOM kann mit einem Terminalprogramm (z.B. HyperTerminal) oder innerhalb eines IP-Netzwerks (z. B. Telnet) konfiguriert werden.
- ▶ **TFTP** – innerhalb von IP-Netzwerken kann auch das Dateiübertragungs-Protokoll TFTP verwendet werden.

Die folgende Tabelle zeigt, über welchen Weg Sie mit den jeweiligen Mitteln auf die Konfiguration zugreifen können:

Konfigurationssoftware	LAN, WAN, WLAN (Inband)	Config-Schnittstelle (Outband)	ISDN-Fernkonfiguration	Analoge Einwahl (in Verbindung mit LANCOM Modem Adapter Kit)
LANconfig	Ja	Ja	Ja	Ja
WEBconfig	Ja	Nein	Ja	Ja
SNMP	Ja	Nein	Ja	Ja
Terminalprogramm	Nein	Ja	Nein	Nein
Telnet	Ja	Nein	Nein	Nein
TFTP	Ja	Nein	Ja	Ja



Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie beispielsweise in LANconfig Einstellungen ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.

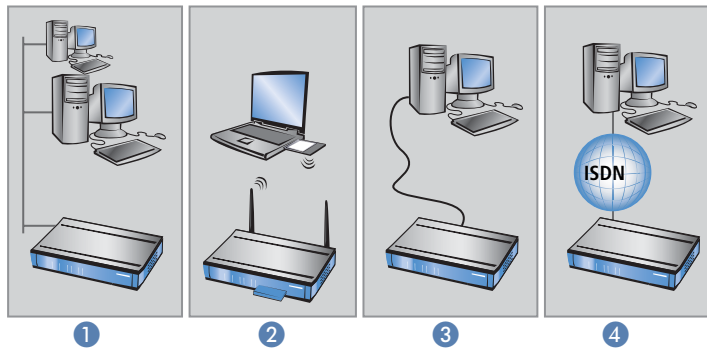
3.3 Geräte suchen und konfigurieren



Schalten Sie immer zuerst das Gerät ein, bevor Sie den Rechner zur Konfiguration starten.

Ein Router oder Access Point kann über die folgenden Wege konfiguriert werden (sofern das Modell über die entsprechende Schnittstelle verfügt):

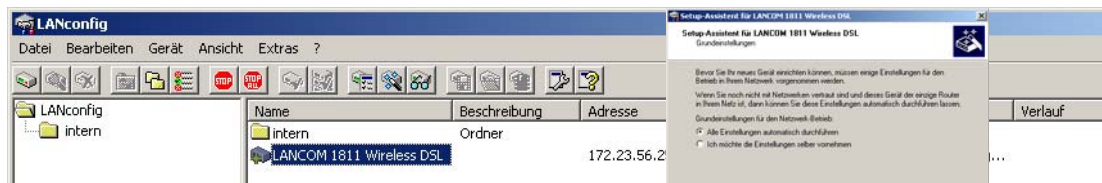
- ▶ Über das lokale Netzwerk (LAN) ①.
- ▶ Über das Funknetzwerk (WLAN) ②, wenn die WLAN-Verschlüsselung (z.B. 802.11i) in einem Gerät mit Wireless-Schnittstelle und im Konfigurationsrechner passend eingestellt bzw. deaktiviert ist.
- ▶ Über die serielle Konfigurationsschnittstelle ③.
- ▶ Über eine ISDN-Verbindung ④.



3.4 Die Konfiguration mit verschiedenen Tools

3.4.1 LANconfig

Rufen Sie LANconfig z.B. aus der Windows-Startleiste auf mit **Start ► Programme ► LANCOM ► LANconfig**. LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet LANconfig selbstständig den Setup-Assistenten.



Eine aktivierte „Internetverbindungsfirewall“ (Windows XP) oder eine andere „Personal Firewall“ auf dem Konfigurationsrechner kann dazu führen, dass LANconfig neue Geräte im LAN nicht findet. Deaktivieren Sie ggf. die Firewall für die Dauer der Konfiguration, wenn die unkonfigurierten Geräte nicht gefunden werden.

Ihr LANCOM-Gerät verfügt über eine umfangreiche eingebaute Firewall. Diese schützt Ihre Rechner auch dann, wenn keine weitere Firewall auf den Rechnern selbst – wie die „Internetverbindungsfirewall“ – eingeschaltet ist.

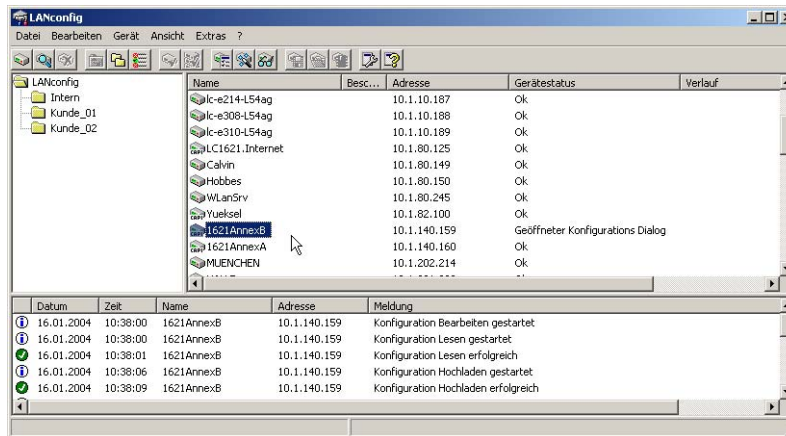
Neue Geräte suchen



Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche **Suchen** oder rufen den Befehl über **Datei ► Geräte suchen** auf. LANconfig erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

▷ Die Konfiguration mit verschiedenen Tools

Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.



Der erweiterte Funktionsumfang für Profis

Für die Konfiguration der Geräte mit LANconfig stehen zwei verschiedene Darstellungsmöglichkeiten zur Auswahl:

- ▶ In der 'einfachen Darstellung' werden nur die Einstellungen angezeigt, die für übliche Anwendungsfälle benötigt werden.
- ▶ In der 'vollständigen Darstellung' werden alle verfügbaren Einstellungen angezeigt. Einige davon sollten nur von erfahrenen Benutzern verändert werden.

Wählen Sie den Darstellungsmodus im Menü **Extras ▶ Optionen**.



Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Gerät ▶ Konfigurieren** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an.

Die eingebaute Hilfe-Funktion

Die weitere Bedienung des Programms erklärt sich selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie die kontextsensitive Hilfe aufrufen.

Verwaltung mehrerer Geräte gleichzeitig

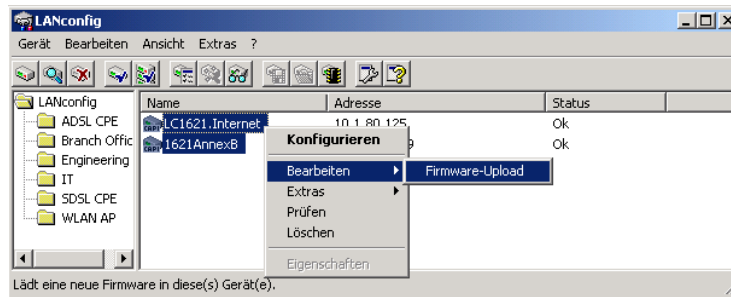
Mit LANconfig können mehrere Geräte gleichzeitig komfortabel (fern-) gewartet werden. Dazu einfach alle gewünschten Geräte selektieren, LANconfig führt dann alle Aktionen für alle ausgewählten Geräte nacheinander durch.

▷ Die Konfiguration mit verschiedenen Tools

Zur bequemen Verwaltung lassen sich Geräte zu Gruppen zusammenfassen. Dazu muss die Ansicht 'Verzeichnisbaum' aktiviert sein, dann können die Geräte durch einfaches Verschieben per 'drag und drop' in die gewünschten Ordner gruppiert werden.



In der Mehrgeräte-Konfiguration zeigt LANconfig nur die für die Mehrgeräte-Konfiguration geeigneten Eingabefelder an, z.B. bei LANCOM Wireless Access-Points die MAC Access-Control-Liste.



3.4.2 WEBconfig

Sie können die Einstellungen des Gerätes über einen beliebigen (auch textbasierten) Web-Browser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Web-Browser, um auf WEBconfig zuzugreifen.

Funktioniert mit beliebigem Web-Browser

WEBconfig bietet ähnliche Setup-Assistenten wie LANconfig an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des LANCOM – im Unterschied zu LANconfig, aber unter allen Betriebssystemen, für die es einen Web-Browser gibt.

Sicher mit HTTPS

WEBconfig bietet zur sicheren (Fern-) Konfiguration die Möglichkeit der verschlüsselten Übertragung der Konfigurationsdaten über HTTPS.

`https://<IP-Adresse oder Gerätenamen>`



Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Internet-Browsers verwenden. Unter Windows 2000 empfiehlt LANCOM Systems GmbH die Installation des sog. "High Encryption Pack" oder den Internet Explorer Version 5.5 mit Service Pack 2 oder besser.

▷ Die Konfiguration mit verschiedenen Tools

Zugang zum Gerät mit WEBconfig

Für die Verwendung von WEBconfig muss eine TCP/IP-Verbindung zum LAN- oder WAN-Anschluss aufgebaut sein. Der Zugriff auf WEBconfig erfolgt mit Hilfe eines Web-Browsers entweder über die IP-Adresse des LANCOM, über den Namen des Gerätes (sofern bereits zugewiesen) bzw. sogar über einen beliebigen Namen, falls das Gerät noch nicht konfiguriert wurde.

Die Erreichbarkeit zur Konfiguration über einen Webbrowser hängt davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen.

Nach dem Einschalten prüfen unkonfigurierte LANCOM-Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

WEBconfig-Zugang in einem Netz ohne DHCP-Server

In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechner im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP). In dieser Konstellation kann das Gerät von jedem Rechner mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter dem Namen **LANCOM** oder unter der IP-Adresse **172.23.56.254** erreicht werden.



Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000 oder Windows XP, mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **winipcfg** an der Eingabeaufforderung unter Windows Me oder Windows 9x bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das LANCOM unter der Adresse **x.x.x.254** (die "x" stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

WEBconfig-Zugang in einem Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes LANCOM-Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Diese IP-Adresse ist aber zunächst nicht bekannt, die Erreichbarkeit des Geräts hängt von der Namensauflösung ab:

▷ Die Konfiguration mit verschiedenen Tools

- ▶ Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem DHCP-Server aus, kann das Gerät unter dem Namen "LANCOM-<MAC-Adresse>" (z.B. "LANCOM-00a057xxxxx") erreicht werden.



Die MAC-Adresse finden Sie auf einem Aufkleber auf der Geräteunterseite.

- ▶ Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
 - ▷ Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
 - ▷ LANconfig verwenden.
 - ▷ Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschließen.

3.4.3 Telnet

Telnet-Sitzung starten

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

```
C:\>telnet 10.0.0.1
```

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.



Linux und Unix unterstützen auch Telnet-Sitzungen über SSL-verschlüsselte Verbindungen.

Je nach Distribution ist es dazu ggf. erforderlich, die Standard-Telnet-Anwendung durch eine SSL-fähige Version zu ersetzen. Die verschlüsselte Telnet-Verbindung wird dann mit dem folgenden Befehl gestartet:

```
C:\>telnet -z ssl 10.0.0.1 telnets
```

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. LANCOM werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle

▷ Die Konfiguration mit verschiedenen Tools

in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

Konfigurationstool	Aufruf (bei Englisch als eingestellter Konsolensprache)
WEBconfig	Expertenkonfiguration ► Config-Module ► Language
Telnet	set /Setup/Config-Module/Language Deutsch

Telnet-Sitzung beenden

Um die Telnet-Sitzung zu beenden, geben Sie an der Eingabeaufforderung den Befehl `exit` ein:

```
C:\>exit
```


Die Struktur im Kommandozeilen-Interface

Das LANCOM Kommandozeilen-Interface ist stets wie folgt strukturiert:

- **Status**
Enthält die Zustände und Statistiken aller internen Module des Gerätes
- **Setup**
Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes
- **Firmware**
Beinhaltet das Firmware-Management
- **Sonstiges**
Enthält Aktionen für Verbindungsauf- und abbau, Reset, Reboot und Upload

Befehle für die Kommandozeile

Das LANCOM Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden.

 Zum Ausführen einiger Befehle sind Supervisor-Rechte erforderlich.

Befehl	Beschreibung
beginscript	Versetzt eine Konsolensitzung in den Script-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes. 'Scripting' →Seite 55
cd [PFAD]	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc.
del [PFAD]*	Löscht eine komplette Tabelle in dem mit Path angegebenen Zweig des Menübaums.
default [-r] [PFAD]	Setzt einzelne Parameter, Tabellen oder ganze Menübaume in die Grundkonfiguration zurück. Zeigt PATH auf einen Zweig des Menübaums, muss zwingend die option -r (recursive) angegeben werden.

▷ Die Konfiguration mit verschiedenen Tools

Befehl	Beschreibung
dir [PFAD] list [PFAD] ls [PFAD] ll [PFAD]	Zeigt den Inhalt des aktuellen Verzeichnisses an. Der angehängte Parameter „-a“ gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte.
do [PFAD] [<Parameter>]	Führt die Aktion [PATH] im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden
echo <ARG>...	Argument auf Konsole ausgeben
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
flash Yes/No	Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (flash yes) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (flash no), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird ('flash Yes/No' →Seite 65).
history	Zeigt eine Liste der letzten ausgeführten Befehle. Mit dem Befehl „!#“ können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit „!3“ wird z.B. der dritte Befehl der Liste ausgeführt.
killscript	löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt. 'Scripting' →Seite 55
loadconfig	Konfiguration per TFTP-Client in das Gerät laden
loadfirmware	Firmware per TFTP-Client in das Gerät laden
loadscript	Script per TFTP-Client in das Gerät laden
passwd	Ändern des Passworts
passwd -n neues [altes]	Passwort ändern (Keine Eingabeaufforderung)
ping [IP-Adresse]	Sendet einen ICMP echo request an die angegebene IP-Adresse
readconfig	Anzeige der kompletten Konfiguration in der Geräte-Syntax
readmib	Anzeige der SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PFAD]	Erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden. 'Scripting' →Seite 55
repeat <INTERVAL> <Kommando>	Wiederholt das Kommando alle INTERVAL Sekunden, bis der Vorgang durch neue Eingaben beendet wird
sleep [-u] Wert[suffix]	Verzögert die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne oder terminiert sie auf einen bestimmten Zeitpunkt. Als Suffix sind s, m, oder h fuer Sekunden, Minuten, oder Stunden erlaubt, ohne Suffix arbeitet der Befehl in Millisekunden. Mit dem Optionsschalter -u nimmt das sleep-Kommando Zeitpunkte im Format MM/DD/YYYY hh:mm:ss (englisch) oder im Format TT.MM.JJJJ hh:mm:ss (deutsch) entgegen. Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist.
stop	Beendet den PING-Befehl
set [PFAD] <Wert(e)>	Setzt einen Konfigurationsparameter auf einen bestimmten Wert. Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte der ein Wert angegeben werden. Dabei übernimmt das Zeichen * als Eingabewert einen vorhandenen Tabelleneintrag unverändert.

▷ Die Konfiguration mit verschiedenen Tools

Befehl	Beschreibung
set [PFAD] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
setenv <NAME> <WERT>	Umgebungsvariable setzen
unsetenv <NAME>	Umgebungsvariable löschen
getenv <NAME>	Umgebungsvariable ausgeben (kein Zeilenvorschub)
printenv	Komplette Umgebung ausgeben
show <Optionen>	Anzeige spezieller interner Daten. show ? zeigt alle verfügbaren Informationen an, z.B. letzte Boot-Vorgänge ('bootlog'), Firewall Filterregeln ('filter'), VPN-Regeln ('VPN') und Speicherauslastung ('mem' und 'heap')
sysinfo	Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.)
testmail	Schickt eine E-Mail. Parameter siehe 'testmail ?'
time	Zeit setzen (TT.MM.JJJJ hh:mm:ss)
trace [...]	Konfiguration der Diagnose-Ausgaben. Siehe 'So starten Sie einen Trace' →Seite 81
who	aktive Sitzungen auflisten
writeconfig	Laden eines neuen Konfigurationsfiles in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten
writeflash	Laden einer neuen Firmware-Datei (nur via TFTP)
!!	letztes Kommando wiederholen
!<num>	Kommando <num> wiederholen
!<prefix>	letztes mit <prefix> beginnendes Kommando wiederholen
#<blank>	Kommentar

- PFAD:
 - ▷ Pfadname fuer ein Menue oder einen Parameter, getrennt durch / oder \
 - ▷ .. bedeutet eine Ebene hoeher
 - ▷ . bedeutet aktuelle Ebene
- WERT:
 - ▷ moeglicher Eingabewert
 - ▷ "" ist ein leerer Eingabewert
- NAME:
 - ▷ Sequenz von _ 0..9 A..Z
 - ▷ erstes Zeichen darf keine Ziffer sein
 - ▷ keine Unterscheidung Gross/Kleinschreibung

▷ Die Konfiguration mit verschiedenen Tools

- ▶ Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden - solange sie eindeutig sind. Zum Beispiel kann der Befehl "sysinfo" zu "sys" verkürzt werden, oder aber "cd Management" zu "c ma". Die Eingabe "cd /s" dagegen ist ungültig, da dieser Eingabe sowohl "cd /Setup" als auch "cd /Status" entspräche.
- ▶ Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.
- ▶ Für Aktionen und Befehle steht eine kommandospezifische Hilfsfunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Parameter aufgerufen wird. Zum Beispiel zeigt der Aufruf 'ping ?' die Optionen des eingebauten ping Kommandos an.
- ▶ Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von '?' auf der Kommandozeile.

3.4.4 TFTP

Bestimmte Funktionen lassen sich über Telnet nicht oder nicht befriedigend ausführen. Dazu gehören alle Funktionen, bei denen komplette Dateien übertragen werden, etwa der Upload von Firmware oder die Speicherung und Wiederherstellung von Konfigurationsdaten. In diesen Fällen wird TFTP eingesetzt.

TFTP steht standardmäßig unter den Betriebssystemen Windows XP, Windows 2000 und Windows NT zu Verfügung. Es ermöglicht den einfachen Dateitransfer von Dateien mit anderen Geräten über das Netzwerk.

Die Syntax des TFTP-Aufrufs ist abhängig vom Betriebssystem. Bei Windows 2000 und Windows NT lautet die Syntax:

```
tftp -i <IP-Adresse Host> [get|put] Quelle [Ziel]
```



Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z.B. Firmware) muss daher meist die binäre Übertragung explizit gewählt werden. In diesem Beispiel für Windows XP, Windows 2000 und Windows NT erreichen Sie das durch den Parameter '-i'.

Sofern das Gerät mit einem Passwort geschützt ist, müssen Username und Passwort in den TFTP-Befehl eingebaut werden. Der Filename baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando (für Supervisoren) oder aus der Kombination von Username und Passwort (für lokale Administratoren), die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

- ▶ <Master-Passwort><Kommando> bzw.
- ▶ <Username>:<Passwort>@<Kommando>

Weitere Informationen zu TFTP-Befehlen und den Rechten verschiedenener Administratoren finden Sie unter 'Rechtverwaltung für verschiedene Administratoren' →Seite 41 und 'Zugang über TFTP' →Seite 43.

Firmware, Geräte-Konfiguration oder Script über TFTP laden

Neben den Möglichkeiten, eine Firmware oder eine Konfigurationsdatei über LANconfig oder WEBconfig in ein Gerät einzuspielen, kann der Upload der entsprechenden Dateien über Telnet oder SSH auch direkt von einem TFTP-Server erfolgen. Dieses Vorgehen kann in größeren Installationen mit regelmäßigem Update von Firmware und/oder Kon-

▷ Die Konfiguration mit verschiedenen Tools

figuration die Administration der Geräte erleichtern. Über TFTP können auch Scripte – z.B. mit Teilkonfigurationen – in die Geräte geladen werden.

Dazu werden die Firmware- und Konfigurationsdateien oder Scripte auf einem TFTP-Server abgelegt. Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Von diesem TFTP-Server können die Dateien mit folgenden Befehlen abgerufen werden:

- ▶ LoadConfig
- ▶ LoadFirmware
- ▶ LoadScript

Zu diesen Befehlen können folgende Parameter angegeben werden:

- ▶ -s <Server-IP-Adresse oder Server-Name>
- ▶ -f <Dateipfad und Dateiname>

Im Dateinamen inclusive Pfad sind folgende Variablen erlaubt:

- ▷ %m - LAN MAC Adresse (Hexadezimal, kleine Buchstaben, ohne Trennzeichen)
- ▷ %s - Seriennummer
- ▷ %n - Gerätename
- ▷ %l - Ort ('Standort' - aus der Konfiguration)
- ▷ %d - Gerätetyp

Beispiele:

Mit dem folgenden Befehl wird eine Firmwaredatei mit dem Namen 'LC-1811-5.00.0019.upx' aus dem Verzeichnis 'LCOS/500' vom Server mit der IP-Adresse '192-168.2.200' in das Gerät geladen:

- ▶ LoadFirmware -s 192-168.2.200 -f LCOS/500/LC-1811-5.00.0019.upx

Mit dem folgenden Befehl wird ein zur MAC-Adresse passendes Script vom Server mit der IP-Adresse '192-168.2.200' in das Gerät geladen:

- ▶ LoadScript -s 192-168.2.200 -f %m.lcs

Werden die Parameter -s und/oder -f nicht angegeben, verwendet das Gerät die Standardwerte, die unter dem Pfad /setup/config/TFTP-Client gesetzt werden:

- ▶ Config-Adresse
- ▶ Config-Dateiname
- ▶ Firmware-Adresse
- ▶ Firmware-Dateiname

Die Nutzung dieser Standardwerte bietet sich an, wenn die aktuellen Konfigurationen und Firmware-Versionen immer unter dem gleichen Namen an der gleichen Stelle gespeichert werden. In diesem Fall können mit den einfachen Befehlen LoadConfig und LoadFirmware die jeweils gültige Dateien geladen werden.

3.4.5 SNMP

Das Simple Network Management Protocol (SNMP V.1 nach RFC 1157) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus.

Es gibt eine ganze Reihe von Konfigurations- und Management-Programmen, die über SNMP laufen. Kommerzielle Beispiele sind Tivoli, OpenView von Hewlett-Packard, SunNet Manager und CiscoWorks. Daneben existieren auch zahlreiche Programme auf Freeware- und Shareware-Basis.

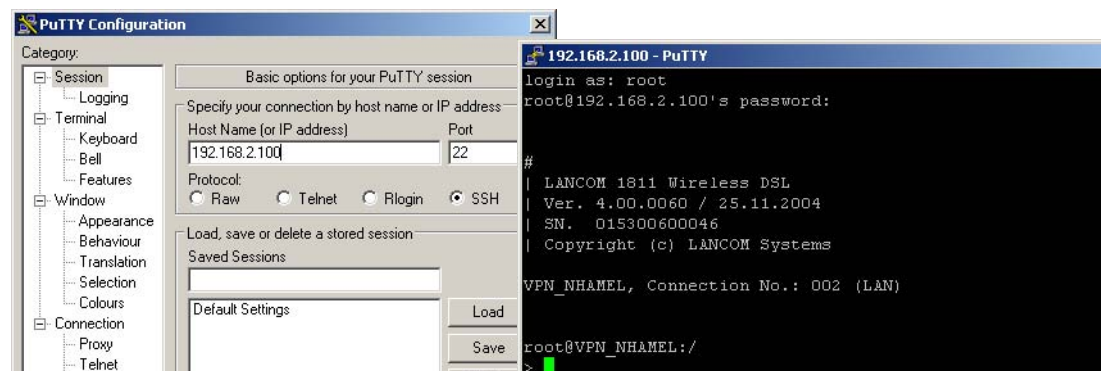
Ihr LANCOM kann die für die Verwendung in SNMP-Programmen benötigte Geräte-MIB-Datei (**M**anagement **I**nformation **B**ase) wie folgt exportieren.

Konfigurationstool	Aufruf
WEBconfig	SNMP-Geräte-MIB abrufen (im Hauptmenü)
TFTP	tftp 10.0.0.1 get readmib file1

3.4.6 Verschlüsselte Konfiguration über SSH-Zugang

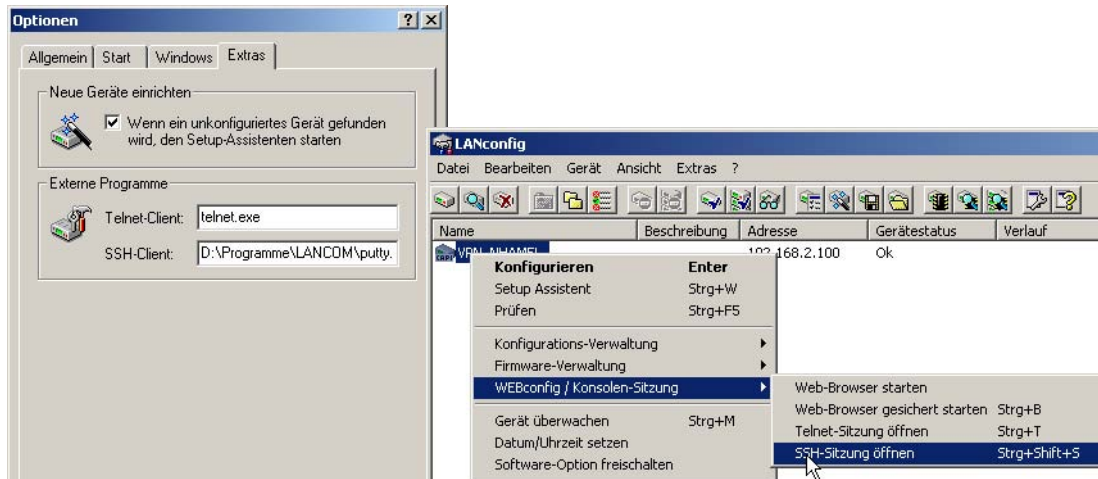
Neben den bisherigen Möglichkeiten, ein LANCOM über Telnet oder Terminalprogramm zu konfigurieren, gibt es ab der LCOS-Version 4.0 zusätzlich einen Zugang über SSH. Mit einem entsprechenden SSH-Client wie PuTTY können Sie so eine verschlüsselte Verbindung zum Gerät herstellen und die bei der Konfiguration übertragenen Daten so vor dem Abhören innerhalb des Netzwerks schützen.

Starten Sie z.B. PuTTY und geben Sie als Host Name die IP-Adresse des LANCOM ein. In der folgenden Eingabeaufforderung können Sie sich mit Ihren Benutzerdaten anmelden.



Alternativ können Sie im LANconfig unter **Extras** ► **Optionen** ► **Extras** Ihren SSH-Client als „externes Programm“ eintragen und den SSH-Zugang dann mit einem rechten Mausklick auf das Gerät und **WEBconfig/Konsolen-Sitzung** ► **SSH-Sitzung öffnen** starten.

▷ Die Konfiguration mit verschiedenen Tools



Zur Konfiguration verwenden Sie die gleichen Befehle wie über Telnet oder Terminalprogramm (Referenzhandbuch 'Befehle für die Kommandozeile' →Seite 22).

3.4.7 ISDN-Fernkonfiguration über das DFÜ-Netzwerk



Der komplette Abschnitt zur Fernkonfiguration gilt nur für Geräte mit ISDN-Schnittstelle oder mit Modem (analog oder GSM) an der seriellen Schnittstelle (mit LANCOM Modem Adapter Kit).

Besonders einfach wird die Konfiguration von Routern an entfernten Standorten mit der Fernkonfiguration über das DFÜ-Netzwerk von Windows. Das Gerät ist nach dem Einschalten und der Verbindung mit dem ISDN-Anschluss ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie bei der Konfiguration an entfernten Orten viel Zeit und Geld für die Reise oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der Router.

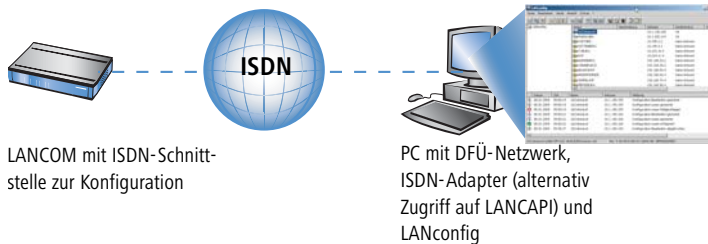
Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den Router zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

Das brauchen Sie für die ISDN-Fernkonfiguration

- ▶ Einen LANCOM mit ISDN-Anschluss, das von einem entfernten Standort aus konfiguriert werden soll
- ▶ Einen Konfigurations-PC mit PPP-Client (z.B. Windows DFÜ-Netzwerk) sowie ISDN-Adapter oder alternativ Zugriff über LANCAPi auf einen LANCOM mit ISDN-Anschluss
- ▶ Ein Programm für die Inband-Konfiguration, z.B. LANconfig oder Telnet

Die erste Fernverbindung mit DFÜ-Netzwerk

Für die Fernkonfiguration eines LANCOM mit LANconfig über das DFÜ-Netzwerk gehen Sie wie folgt vor:



- ① Wählen Sie im LANconfig **Datei ▶ Gerät hinzufügen**, aktivieren Sie die 'DFÜ-Verbindung' als Anschlusstyp und geben Sie die Rufnummer des ISDN-Anschlusses ein, an dem der LANCOM angeschlossen ist. Stellen Sie dazu ggf. die Zeit ein, nach der eine Verbindung ohne Datentransfer automatisch getrennt werden soll.
- ② LANconfig legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der LANCAP) für die Verbindung aus, und bestätigen Sie mit **OK**.
- ③ Anschließend zeigt LANconfig in der Geräteliste ein neues Gerät mit dem Namen 'Unbekannt' und der Rufnummer über DFÜ als Adresse an.

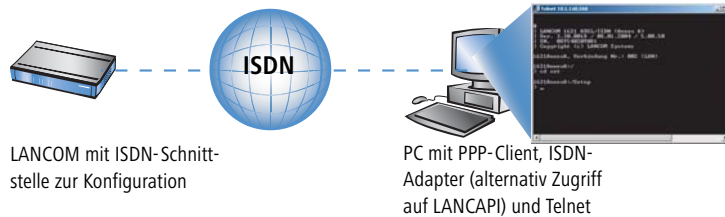
-
- ⓘ Mit dem Löschen eines Eintrags in der Geräteliste wird auch die zugehörige Verbindung im Windows-DFÜ-Netzwerk gelöscht.
 - ④ Sie können das Gerät über die Fernverbindung nun genauso konfigurieren wie alle anderen Geräte. Hierzu baut LANconfig eine Verbindung über das DFÜ-Netzwerk auf.

-
- ⚠ Schützen Sie die Einstellungen des Geräts immer durch die Vergabe eines Passworts! Geben Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bei der ersten Konfiguration ein Passwort ein!

Die erste Fernverbindung mit PPP-Client und Telnet

An Stelle der Fernkonfiguration mit LANconfig ist auch ein Zugriff über ISDN mit Telnet möglich. Für die Fernkonfiguration eines LANCOM mit Telnet über einen beliebigen PPP-Client gehen Sie wie folgt vor:

▷ Die Konfiguration mit verschiedenen Tools



- ① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum LANCOM her, verwenden Sie dabei folgende Angaben:
 - ▷ Benutzername 'ADMIN'
 - ▷ Passwort wie beim LANCOM eingestellt
 - ▷ eine IP-Adresse für die Verbindung, nur wenn erforderlich
- ② Starten Sie eine Telnet-Verbindung zum LANCOM. Verwenden Sie dazu die folgende IP-Adresse:
 - ▷ '172.17.17.18', wenn Sie keine IP-Adresse für den PPP-Client festgelegt haben. Diese Adresse verwendet der LANCOM automatisch, falls nichts anderes vereinbart ist. Der Konfigurations-PC reagiert dann auf die IP '172.17.17.17'.
 - ▷ Erhöhen Sie die IP-Adresse des PCs um eins, wenn Sie eine Adresse festgelegt haben. Beispiel: Sie haben für den PPP-Client die IP '10.0.200.123' festgelegt, dann hört der LANCOM auf die '10.0.200.124'. Ausnahme: Bei einer '254' am Ende der IP reagiert der Router auf die 'x.x.x.1'.
- ③ Sie können den LANCOM über die Fernverbindung nun genauso einstellen wie alle anderen Geräte.



Schützen Sie die Einstellungen des Geräts immer durch die Vergabe eines Passworts! Geben Sie bei einer Telnet- oder Terminalverbindung alternativ den folgenden Befehl ein:

```
passwd
```

Damit werden Sie zur Eingabe eines neuen Passworts mit Bestätigung aufgefordert.

Der Default-Layer für die Ferninbetriebnahme

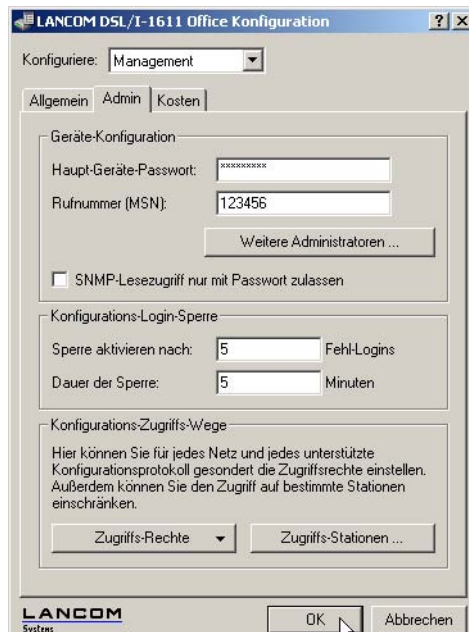
Die PPP-Verbindung von einer beliebigen ISDN-Gegenstelle zum Router gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

Aber vielleicht möchten Sie ja nach der ersten Konfiguration den Default-Layer z.B. für LAN-LAN-Verbindungen auf ein anderes Protokoll einstellen? Dann nimmt das Gerät die Rufe über die DFÜ-Verbindung nicht mehr mit den PPP-Einstellungen an. Abhilfe schafft hier die Vereinbarung einer speziellen Rufnummer des ISDN-Anschlusses für den Konfigurationszugriff:

Der ISDN-Administrationszugang für die Fernwartung

Empfängt das Gerät einen Ruf auf dieser Nummer, wird immer die Einstellung für PPP verwendet - unabhängig von der weiteren Konfiguration des Routers! Dabei wird nur ein spezieller Benutzername während der PPP-Verhandlung akzeptiert, der beim Verbindungsaufbau über LANconfig automatisch eingetragen wird ('ADMIN').

- ① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin'.



- ② Geben Sie als Rufnummer im Bereich 'Geräte-Konfiguration' eine Rufnummer (MSN) Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ über Telnet den folgenden Befehl ein:

```
set /setup/config-modul/Fernconfig 123456
```

- ! Solange keine MSN für den Konfigurations-Zugriff eingetragen ist, nimmt ein **unkonfiguriertes** LANCOM die Rufe auf alle MSNs an. Sobald die erste Änderung in der Konfiguration gespeichert ist, nimmt das Gerät nur noch die Anrufe auf der Konfigurations-MSN an!

Wenn bei der ersten Konfiguration keine Konfigurations-MSN eingetragen wird, ist die Fernkonfiguration damit ausgeschaltet und das Gerät gegen den Zugriff über die ISDN-Leitung geschützt.

▷ Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien

3.5 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien

Die aktuelle Konfiguration eines LANCOM kann als Datei abgespeichert und bei Bedarf wieder in das Gerät (oder in ein anderes Gerät desselben Typs) geladen werden.

Zusätzlich können mit LANconfig Konfigurationsdateien auch "offline" erzeugt und editiert werden - für alle unterstützten Gerätetypen, Firmware-Versionen und Software-Optionen.



Sicherheitskopien der Konfiguration

Mit dieser Funktion können Sie Sicherungskopien der Konfiguration Ihres LANCOM erstellen.

Komfortable Serienkonfiguration

Aber auch wenn Sie vor der Aufgabe stehen, mehrere gleichartige LANCOM konfigurieren zu müssen, werden Sie die Funktion des Abspeicherns und Wiederherstellens von Konfigurationen schätzen lernen. Sie können sich in diesem Fall einen großen Teil der Arbeit sparen, indem Sie in alle Geräte zunächst übereinstimmende Parameter als Grundkonfiguration einspielen und nur noch die individuellen Einstellungen an den einzelnen Geräten vornehmen.

Funktionsaufruf:

Konfigurationstool	Aufruf
LANconfig	Gerät ► Konfigurations-Verwaltung ► Als Datei sichern Gerät ► Konfigurations-Verwaltung ► Aus Datei wiederherstellen Bearbeiten ► Neue Konfigurations-Datei Bearbeiten ► Konfigurations-Datei bearbeiten Gerät ► Konfigurations-Verwaltung ► Drucken
WEBconfig	Konfiguration speichern ► Konfiguration laden (im Hauptmenü)
TFTP	tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig

3.6 Neue Firmware mit LANCOM FirmSafe

Die Software für die Geräte von LANCOM Systems wird ständig weiterentwickelt. Damit Sie auch in den Genuss von neuen Features und Funktionen kommen, haben wir die Geräte mit einem Flash-ROM-Speicher ausgerüstet, der das nachträgliche Ändern der Betriebssoftware zum Kinderspiel macht. Kein EPROM tauschen, kein Gehäuse öffnen: Einfach die neue Version einspielen und fertig!

3.6.1 So funktioniert LANCOM FirmSafe

LANCOM FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert. Damit ist Ihr Gerät insbesondere auch gegen die Folgen eines Stromausfalls oder einer Verbindungsunterbrechung während des Firmware-Uploads geschützt.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- ▶ 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
 - ▷ Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
 - ▷ Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.
- ▶ 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
 - ▷ Im Unterschied zur ersten Variante wartet das Gerät anschließend für den eingestellten Firmsafe-Timeout (unter WEBconfig im Menü **Expertenkonfiguration ▶ Firmware ▶ Timeout-Firmsafe**, unter Telnet einzustellen mit 'Firmware/Timeout-Firmsafe') auf einen erfolgreichen Login über Telnet, ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
 - ▷ Wenn das Gerät nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- ▶ 'Manuell': Bei der dritten Möglichkeit können Sie ebenfalls selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird. Unter LANconfig aktivieren Sie die neue Firmware mit **Gerät ▶ Firmware-Verwaltung ▶ Im Test laufende Firmware freischalten**, unter Telnet unter 'Firmware/Firmsafe-Tabelle' mit dem Befehl 'set # active' (dabei ist # die Position der Firmware in der Firmsafe-Tabelle). Unter WEBconfig finden Sie die Firmsafe-Tabelle unter **Expertenkonfiguration ▶ Firmware**.

Nicht unter
LANconfig

▷ *Neue Firmware mit LANCOM FirmSafe*

Den Modus für den Firmware-Upload stellen Sie unter WEBconfig im Menü **Expertenkonfiguration ▶ Firmware ▶ Modus- FirmSafe** ein, unter Telnet unter 'Firmware/Timeout-Firmsafe'. Unter LANconfig wählen Sie den Modus bei der Auswahl der neuen Firmware-Datei aus.



Das Laden einer zweiten Firmware ist nur dann möglich, wenn das Gerät über ausreichenden Speicherplatz für zwei vollständige Firmwareversionen verfügt. Aktuelle Firmwareversionen (ggf. mit zusätzlichen Software-Optionen) können bei älteren Hardwaremodellen manchmal mehr als die Hälfte des verfügbaren Speicherplatzes benötigen. In diesem Fall meldet die Konfigurationssoftware beim Upload-Versuch den Konflikt und empfiehlt die Verwendung des entsprechenden "Konverters".

Dieser Konverter kann kostenlos von der LANCOM Systems-Webseite geladen werden. Mit dem Konverter wird der Speicherplatz im LANCOM neu aufgeteilt in einen vergrößerten Bereich für die neue Firmwareversion und einen kleineren Bereich für die bestehende Version.

In den kleineren Speicherbereich wird beim anschließenden Upload einer neuen Firmware eine Minimalversion der bisherigen Firmware geladen. Diese Version ist als "Sicherungskopie" einsatzfähig mit folgenden Einschränkungen:

- ▷ Die Minimalversion der Firmware unterstützt nur einen Teil der LCOS-Funktionen zum Wiederherstellen des vorherigen Zustands oder zum Einspielen einer anderen Firmware. Insbesondere ist mit der Minimalversion der Firmware kein Internetzugang möglich.
- ▷ Ein LANCOM mit aktiver Minimalfirmware kann nur über das LAN, über das WLAN oder über die Outbandschnittstelle angesprochen werden. Es ist insbesondere keine Remote-Konfiguration möglich, auch nicht über ISDN.
- ▷ Die Minimalfirmware kann nicht konfiguriert werden. Änderungen in der Konfiguration über LANconfig, WEBconfig oder Telnet werden nicht in das Gerät gespeichert.

3.6.2 So spielen Sie eine neue Software ein

Beim Firmware-Upload (so heißt das Einspielen der Software) führen verschiedene Wege zum Ziel:

- ▶ LANconfig
- ▶ WEBconfig
- ▶ Terminalprogramm
- ▶ TFTP



Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei LANconfig z.B. mit **Gerät ▶ Konfigurations-Verwaltung ▶ Als Datei sichern**). Neben der Konfiguration sollten Sie auch eine Version der aktuellen Firmware vor dem Upload sichern. Wenn Ihnen diese nicht mehr als Datei zur Verfügung steht, laden Sie vor dem Firmware-Upload die aktuell verwendete Version von www.lancom.de.

Enthält die neu eingespielte Firmware Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

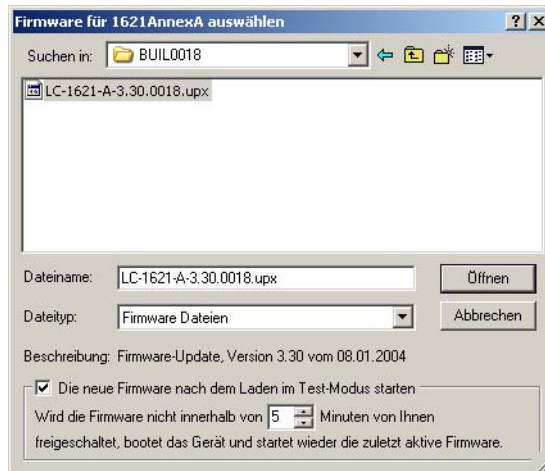
LANconfig



Beim LANconfig markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Gerät ▶ Konfigurations-Verwaltung ▶ Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

LANconfig informiert Sie dann in der Beschreibung über Versions-Nummer und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten ▶ Firmware-Verwaltung ▶ Im Test laufende Firmware freischalten**.



WEBconfig

Starten Sie WEBconfig in Ihrem Web-Browser. Auf der Startseite finden Sie den Link **Eine neue Firmware hochladen**. Im nächsten Fenster können Sie die Firmware-Datei im Verzeichnissystem suchen und anschließend auf die Schaltfläche **Upload** klicken.

Terminalprogramm (z.B. Hyperterminal von Windows)

Stellen Sie bei Terminalprogrammen im Menü 'Firmware' mit dem Befehl 'set Modus-Firmsafe' zunächst ein, in welchem Modus Sie die neue Firmware laden wollen (unmittelbar, login oder manuell). Stellen Sie ggf. zusätzlich mit 'set Timeout-Firmsafe' die Zeit für den Firmwaretest ein.

▷ *Wie führt man einen Geräteset durch?*

Mit dem Befehl 'do Firmware-Upload' wird der Router anschließend in Empfangsbereitschaft versetzt. Starten Sie anschließend den Upload-Vorgang von Ihrem Terminalprogramm aus:

- ▶ Bei Telix klicken Sie auf die Schaltfläche **Upload**, stellen 'XModem' für die Übertragung ein und wählen die gewünschte Datei zum Upload aus.
- ▶ Bei Hyperterminal klicken Sie auf **Übertragung** ▶ **Datei senden**, wählen die Datei aus, stellen 'XModem' als Protokoll ein und starten mit **OK**.



Der Firmware-Upload über ein Terminalprogramm kann nur über die serielle Konfigurationsschnittstelle erfolgen.

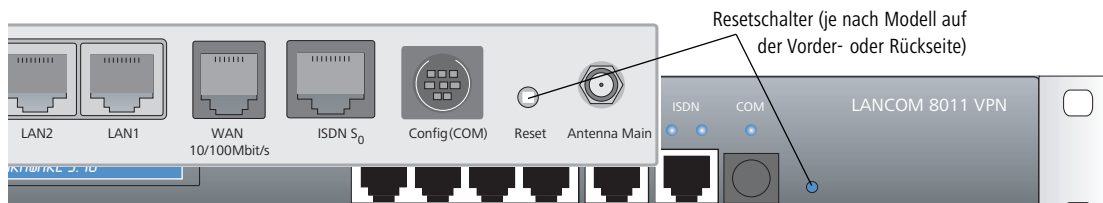
TFTP

Auf LANCOM kann auch mit TFTP eine neue Firmware aufgespielt werden. Dazu wird der Befehl (bzw. das Ziel) **writetflash** angegeben. Um eine neue Firmware in einen LANCOM mit der IP-Adresse 10.0.0.1 zu übertragen, geben Sie z.B. unter Windows XP, Windows 2000 oder Windows NT folgenden Befehl ein:

```
tftp -i 10.0.0.1 put Lc_16xxu.282 writetflash
```

3.7 Wie führt man einen Geräteset durch?

Wenn Sie unabhängig von den evtl. vorhandenen Einstellungen das Gerät neu konfigurieren müssen oder keine Verbindung zur Gerätekonfiguration zustande kommt, können Sie mit einem **Reset** das Gerät in den Auslieferungszustand zurücksetzen. Dazu müssen Sie den Resetschalter betätigen, bis die LEDs des Geräts aufleuchten (ca. 5 Sekunden).



Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, **alle** Einstellungen gehen dabei verloren. Sichern Sie daher **vor** dem Reset nach Möglichkeit die aktuelle Konfiguration des Geräts!



Beachten Sie, dass bei einem Reset auch die im Gerät definierten WLAN-Verschlüsselungseinstellungen verloren gehen und auf den **Standard-WEP-Schlüssel** zurückgesetzt werden.. Die drahtlose Konfiguration eines Geräts mit WLAN-Schnittstelle gelingt nach einem Reset nur, wenn der Standard-WEP-Schlüssel in der WLAN-Karte eingetragen ist!

3.8 Rechteverwaltung für verschiedene Administratoren

In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für ein LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden.



Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den „root“-Administrator mit dem Haupt-Geräte-Passwort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht gelöscht oder umbenannt werden. Um sich als root-Administrator anzumelden, geben Sie im Login-Fenster den Benutzernamen „root“ ein oder Sie lassen dieses Feld frei.

Sobald in der Konfiguration des Gerätes ein Passwort für den „root“-Administrator gesetzt ist, erscheint beim Aufruf von WEBconfig auf der Startseite die Schaltfläche **Login**, mit dem das Fenster zur Anmeldung eingeblendet wird. Nach Eingabe von korrektem Benutzernamen und Passwort erscheint das Hauptmenü der WEBconfig. In diesem Menü sind nur die Punkte vorhanden, für die der Administrator Zugriffs- bzw. Funktionsberechtigungen hat.

Ist mindestens ein weiterer Administrator in der Admin-Tabelle eingerichtet, so enthält das Hauptmenü zusätzlich eine Schaltfläche **Administrator wechseln**, der es erlaubt zu einer anderen Benutzerkennung (mit ggf. anderen Rechten) zu wechseln.

3.8.1 Die Rechte für die Administratoren

Bei den Rechten für die Administratoren werden zwei Bereiche unterschieden:

- ▶ Jeder Administrator gehört zu einer bestimmten Gruppe, der global definierte Rechte zugewiesen sind.
- ▶ Jeder Administrator verfügt außerdem über „Funktionsrechte“, die den persönlichen Zugriff auf bestimmte Funktionen wie z.B. die Setup-Assistenten regeln.

Administratorengruppen

Bezeichnung unter Telnet/Terminal	Bezeichnung unter LANconfig	Rechte
Supervisor	Alle	Supervisor - Mitglied in allen Gruppen
Admin-RW	Eingeschränkt	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RO	Nur lesen	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
kein	keine	kein Zugriff auf die Konfiguration

- ▶ Supervisor: Hat vollen Zugriff auf die Konfiguration
- ▶ lokaler Administrator mit Lese- und Schreibrechten: Ebenfalls voller Zugriff auf die Konfiguration, dabei sind jedoch die folgenden Möglichkeiten gesperrt:
 - ▷ Firmware in das Gerät hochladen
 - ▷ Konfiguration in das Gerät einspielen

▷ Rechteverwaltung für verschiedene Administratoren

▷ Konfiguration über LANconfig



Lokale Administratoren mit Schreibrechten können auch die Admintabelle bearbeiten. Dabei kann ein lokaler Administrator jedoch nur solche Einträge bearbeiten oder anlegen, die die gleichen oder weniger Rechte haben wie er selbst. Ein lokaler Administrator kann also keinen Supervisor anlegen und sich selbst auch nicht diese Rechte einräumen.

- ▶ lokaler Administrator mit Leserechten: Kann die Konfiguration über Telnet oder Terminalprogramm lesen, aber keine Werte verändern. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.
- ▶ keine: Kann die Konfiguration nicht lesen. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.

Funktionsrechte

Mit den Funktionsrechten werden dem Benutzer die folgenden Möglichkeiten eingeräumt:

- ▶ Grundkonfigurations-Assistent
- ▶ Sicherheits-Assistent
- ▶ Internet-Assistent
- ▶ Assistent zur Auswahl von Internet-Providern
- ▶ RAS-Assistent
- ▶ LAN-LAN-Kopplungs-Assistent
- ▶ Uhrzeit und Datum verändern
- ▶ Nach weiteren Geräten suchen
- ▶ WLAN-Linktest
- ▶ a/b-Assistent

3.8.2 Administratorenzugänge über TFTP und SNMP

Die zusätzlichen Administratorenzugänge werden in der Regel für die Konfiguration der Geräte über Telnet, Terminalprogramme oder SSH-Zugänge genutzt. Allerdings können die zusätzlichen Administratoren auch über TFTP oder SNMP auf die Geräte zugreifen.

Zugang über LANconfig

Ein Benutzer mit Supervisorrechten kann sich bei LANconfig anmelden, wenn er im Loginfenster im Feld für das Passwort seine Benutzerdaten in der Kombination <Username>:<Passwort> eingibt.

Zugang über TFTP

Im TFTP wird der Username und das Passwort im Quell- (TFTP-Read-Request) oder Ziel-Dateinamen (TFTP-Write-Request) kodiert. Der Dateiname baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando oder aus der Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

- ▶ <Master-Passwort><Kommando> bzw.
- ▶ <Username>:<Passwort>@<Kommando>

Beispiele (das LANCOM hat die Adresse mylancom.intern, das Master-Passwort lautet 'RootPwd' und es ist der User 'LocalAdmin' mit dem Passwort 'Admin' eingerichtet):

- ▶ Konfiguration aus dem Gerät auslesen (nur für den Supervisor)


```
tftp mylancom.intern GET RootPwdreadconfig mylancom.lcf
```
- ▶ Konfiguration in das Gerät schreiben (nur für den Supervisor)


```
tftp mylancom.intern PUT mylancom.lcf RootPwdwriteconfig
```
- ▶ Geräte-MIB aus dem Gerät auslesen (für lokalen Administrator)


```
tftp mylancom.intern GET localadmin:Adminreadmib
mylancom.lcf mylancom.mib
```

Für die Menüs und auszuführenden Befehle gelten die gleichen Rechte-Beschränkungen wie unter Telnet.

Zugang über SNMP-Management-Systeme

Auch bei der Verwaltung von Netzwerken mit Hilfe von SNMP-Tools wie HP OpenView können über die verschiedenen Administratoren-Zugänge die Rechte gezielt gesteuert werden.

Unter SNMP werden Username und Passwort in der „Community“ kodiert. Dort kann entweder die Community 'public' ausgewählt werden oder entweder das Master-Passwort oder eine Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, angegeben werden.



Die Community 'public' entspricht von den Rechten her einem lokalen Administrator mit Read-Only-Rechten, solange der SNMP-Lesezugriff ohne Passwort erlaubt wird ('Passwortschutz für SNMP-Lesezugriff' → Seite 53). Wird dieser Zugriff verboten, so darf die Community 'public' auf keinen Menüpunkt zugreifen.

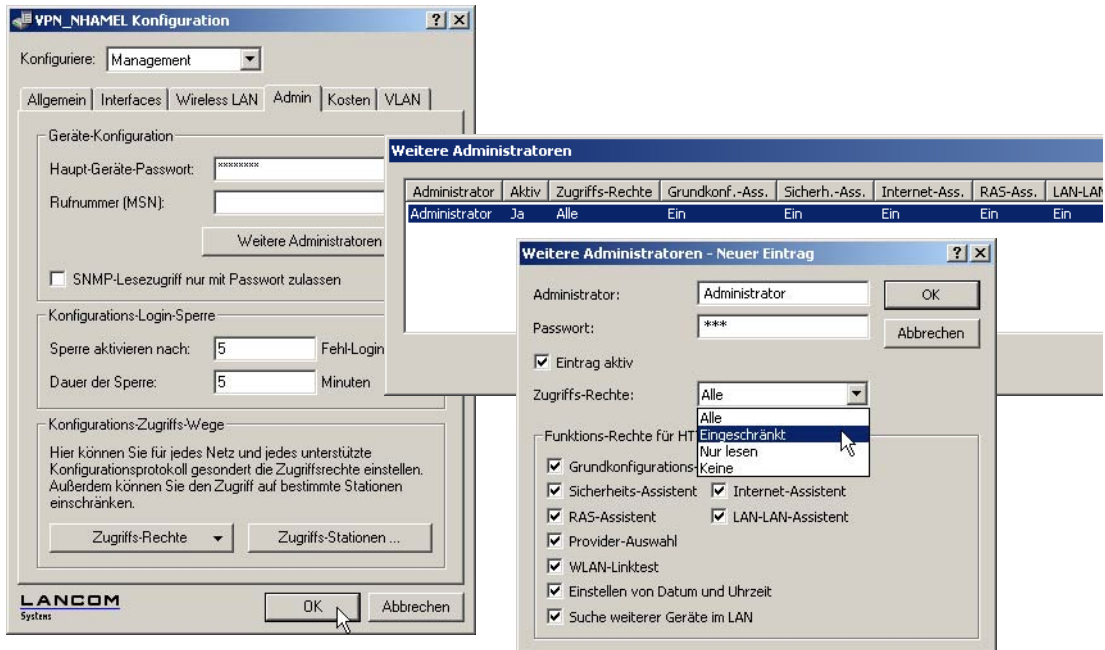
Ansonsten gelten für die Menüs die gleichen Rechte-Beschränkungen wie unter Telnet.

3.8.3 Konfiguration der Benutzerrechte

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Liste der Administratoren im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin' unter der Schaltfläche **Weitere Administratoren**.

► Rechteverwaltung für verschiedene Administratoren



Geben Sie hier folgende Werte ein:

- Name für den neuen Administrator mit Passwort.
- Zugriffsrechte
- Funktionsrechte



Sie können die Einträge über den Schalter 'Eintrag aktiv' vorübergehend deaktivieren, ohne sie ganz zu löschen.

WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Admin-Tabelle auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Config-Modul ► Admin.-Tabelle
Terminal/Telnet	Setup/Config-Modul/Admin.-Tabelle

▷ Rechteverwaltung für verschiedene Administratoren

Zur Darstellung der Benutzergruppen stehen die folgenden Werte zur Verfügung:

Bezeichnung	Rechte
Supervisor	Supervisor - Mitglied in allen Gruppen
Admin-RW	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RO	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
kein	kein Zugriff auf die Konfiguration

Zur Darstellung der Funktionsrechte stehen die folgenden Hexadezimalwerte zur Verfügung:

Wert	Rechte
0x00000001	Der Benutzer darf den Grundkonfigurations-Assistenten ausführen
0x00000002	Der Benutzer darf den Sicherheits-Assistenten ausführen
0x00000004	Der Benutzer darf den Internet-Assistenten ausführen
0x00000008	Der Benutzer darf den Assistenten zur Auswahl von Internet-Providern ausführen
0x00000010	Der Benutzer darf den RAS-Assistenten ausführen
0x00000020	Der Benutzer darf den LAN-LAN-Kopplungs-Assistenten ausführen
0x00000040	Der Benutzer darf die Uhrzeit und das Datum stellen (gilt auch für Telnet und TFTP)
0x00000080	Der Benutzer darf nach weiteren Geräten suchen
0x00000100	Der Benutzer darf den WLAN-Linktest ausführen (gilt auch für Telnet)
0x00000200	Der Benutzer darf den a/b-Assistenten ausführen

Der Eintrag ergibt sich aus der jeweiligen Summe in den ersten, zweiten und dritten Spalten von rechts. Soll der Benutzer z.B. die Funktionen „Sicherheits-Assistent“, „Auswahl der Internet-Provider“, „RAS-Assistent“, „Uhrzeit ändern“ und „WLAN-Linktest“ ausführen können, ergeben sich folgende Werte:

- ▶ erste Spalte von rechts: 2 (Sicherheits-Assistent) + 8 (Auswahl der Internet-Provider) = „a“ (Hexadezimal)
- ▶ zweite Spalte von rechts: 1 (RAS-Assistent) + 4 (Uhrzeit ändern) = „5“ (Hexadezimal)
- ▶ dritte Spalte von rechts: 1 (WLAN-Linktest) = „1“ (Hexadezimal)

Für dieses Beispiel tragen Sie in die Funktionsrechte also den Wert „0000015a“ ein.

▷ Rechteverwaltung für verschiedene Administratoren

Anders ausgedrückt handelt es sich hierbei um eine ODER-Verknüpfung der Hexadezimal-Werte:

Bezeichnung	Wert
Sicherheits-Assistent	0x00000002
Auswahl des Providers	0x00000008
RAS-Assistent	0x00000010
Uhrzeit ändern	0x00000040
WLAN-Linktest	0x00000100
ODER-verknüpft	0x0000015a

Beispiele:

Mit dem folgenden Befehl legen Sie einen neuen Benutzer in der Tabelle an, der als lokaler Administrator „Mueller“ mit dem Passwort „BW46zG29“ den Internetprovider auswählen darf. Der Benutzer wird dabei sofort aktiviert:

```
set Mueller BW46zG29 ja Admin-RW 00000008
```

Mit dem folgenden Befehl erweitern Sie die Funktionsrechte dahingehend, das Benutzer „Mueller“ auch den WLAN-Link-Test ausführen kann (die Sternchen stehen für die nicht zu verändernden Werte):

```
set Mueller * * * 00000108
```

3.8.4 Einschränkungen der Konfigurationsbefehle

Die Verfügbarkeit der Befehle bei der Konfiguration der Geräte über Telnet oder Terminalprogramm hängt von den Rechten der Benutzer ab:

Befehl	Supervisor	lokaler Administrator	Bemerkung
activateimage	✓		
cfgreset	✓		
linktest	✓		Der Befehl 'linktest' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, einen WLAN-Linktest durchzuführen
readconfig	✓		
writeconfig	✓		
writeflash	✓		
setenv	✓	✓	
testmail	✓	✓	

Befehl	Supervisor	lokaler Administrator	Bemerkung
time	✓	✓	Der Befehl 'time' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, die Systemzeit einzustellen
unsetenv	✓	✓	
delete/rm	✓	✓	
readmib	✓	✓	
WLA	✓	✓	
set	✓	✓	

Alle weiteren Befehle (wie 'cd', 'ls', 'trace', etc...) dürfen von allen Benutzern verwendet werden. Um Befehle ausführen zu können, die eine Konfigurationsänderung bewirken (z.B. 'do' oder 'time'), muss der jeweilige Benutzer mindestens Schreibrechte besitzen.



Die oben aufgeführten Befehle sind nicht in allen LCOS-Versionen und nicht für alle LANCOM-Modelle verfügbar.

3.9 Mehrere Loopback-Adressen

Ein LANCOM ist in einem lokalen Netz unter seiner Intranet IP-Adresse oder unter seiner DMZ-IP-Adresse ansprechbar. Bei der zentralen Verwaltung von großen Netzwerkstrukturen kann es jedoch sein, dass mehrere Geräte die gleiche Intranet IP-Adresse tragen. Damit die Geräte in einem solchen Szenario eindeutig ansprechbar sind, werden zusätzliche, frei definierbare IP-Adressen benötigt.

In einem LANCOM-Router können bis zu 16 dieser zusätzlichen „Loopback-Adressen“ eingerichtet werden. Die Loopback-Adressen dienen als weitere lokale IP-Adressen für das Gerät und können aus den privaten IP-Adresskreisen frei gewählt werden. Dabei müssen die Loopback-Adressen auch nicht im gleichen IP-Adress-Kreis liegen wie die Intranet- oder DMZ-Adressen. So können für das Management mehrerer oder stark strukturierter Netzwerke z.B. alle eingesetzten LANCOM-Router mit fortlaufenden IP-Adressen aus einem bestimmten IP-Adress-Kreis als Loopback-Adresse gekennzeichnet werden. Jedes Gerät ist dann eindeutig unter seiner Loopback-Adresse ansprechbar und SNMP-Traps können anhand dieser Loopback-Adresse der entsprechenden Quelle zugeordnet werden.

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Loopback-Liste auf folgenden Pfaden:

WEBconfig,
Telnet oder
Terminalprogramm

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► TCP-IP-Modul ► Loopback-Liste
Terminal/Telnet	Setup/TCP-IP-Modul/Loopback-Liste

▷ *Mehrere Loopback- Adressen*

▷ Projektmanagement mit LANconfig

4 Netzwerk-Management mit den LANtools

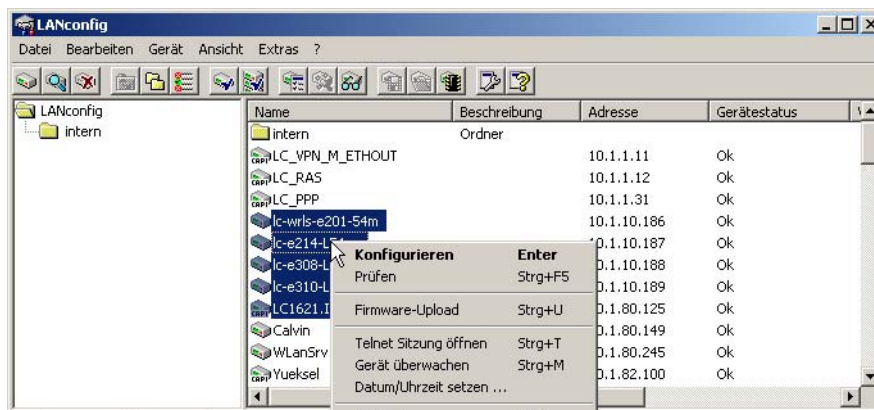
Die LANtools (bestehend aus LANconfig und LANmonitor) eignen sich hervorragend zum Konfigurieren und Überwachen von LANCOM-Geräten in komplexen Anwendungsszenarien. Mehrere Router und/oder Wireless Access Points können in einem Netzwerk können dabei genauso von einer zentralen Stelle aus administriert werden wie Geräte in verteilten Netzwerken, z.B. bei den Kunden eines Dienstleisters.

Beim Netzwerk- Management mit den LANtools stehen u.a. folgende Funktionen im Vordergrund:

- ▶ Konfiguration der Geräte
- ▶ Konfigurationsverwaltung, also sichern und wiederherstellen der Einstellungen
- ▶ Einspielen von neuen Firmware-Versionen
- ▶ Freischalten zusätzlicher Software-Optionen
- ▶ Überwachung des Gerätestatus
- ▶ Überwachung der Verbindungen (inklusive VPN)
- ▶ Überwachung der Firewallaktionen

4.1 Projektmanagement mit LANconfig

LANconfig erleichtert die Konfiguration von verschiedenen Geräten in einem Projekt mit einigen Funktionen, die gleichzeitig auf mehreren Geräten ausgeführt werden können. Sind in der Liste der Geräte im LANconfig mehrere Einträge markiert, können mit einem rechten Mausklick über das Kontextmenü folgende Aktionen aufgerufen werden:



- ▶ Konfigurieren: Öffnet für die ausgewählten Geräte den Konfigurationsdialog unter LANconfig.
- ▶ Prüfen: Prüft die ausgewählten Geräte auf Erreichbarkeit.
- ▶ Firmware-Upload: Lädt eine Firmware parallel in alle ausgewählten Geräte.
- ▶ Script anwenden: Führt ein Konfigurationsscript für alle ausgewählten Geräte aus.

The screenshot shows the LANconfig application window titled 'LANconfig - \Filialen'. The interface includes a menu bar (Datei, Bearbeiten, Gerät, Ansicht, Extras, ?), a toolbar, and a tree view on the left showing a folder structure: LANconfig, Filialen, Home Offices, and Zentrale. The main area displays a table of devices with columns for Name, Adresse, Gerätestatus, and Verlauf. Below the table is a log window showing the date, time, name, address, and message for each device's firmware update.

Name	Adresse	Gerätestatus	Verlauf
DRESDEN	10.1.202.192	Firmw. hochladen ...	53% (68968 Bytes/s)
GERA	10.1.202.193	Firmw. hochladen ...	58% (69240 Bytes/s)
GOETTINGEN	10.1.202.194	Firmw. hochladen ...	58% (55022 Bytes/s)
ERFURT	10.1.202.198	Firmw. hochladen ...	57% (43670 Bytes/s)
GOERLITZ	10.1.202.199	Firmw. hochladen ...	53% (68675 Bytes/s)
NUERNBERG	10.1.202.210	Firmw. hochladen ...	59% (70285 Bytes/s)
HOERSWERDA	10.1.202.211	Firmw. hochladen ...	53% (52147 Bytes/s)
MAGDEBURG	10.1.202.213	Firmw. hochladen ...	58% (53007 Bytes/s)
KOETHEN	10.1.202.217	Firmw. hochladen ...	56% (52525 Bytes/s)
LEIPZIG	10.1.202.218	Firmw. hochladen ...	32% (21644 Bytes/s)
TEMPELHOF	10.1.202.219	Firmw. hochladen ...	46% (53706 Bytes/s)
MERSEBURG	10.1.202.220	Firmw. hochladen ...	58% (50486 Bytes/s)
WITTENBERG	10.1.205.137	Firmw. hochladen ...	42% (66901 Bytes/s)
ANGERMUENDE	10.1.206.211	Firmw. hochladen ...	54% (62541 Bytes/s)
CHEMNITZ	10.1.206.212	Firmw. hochladen ...	53% (70732 Bytes/s)
ADLERSHOF	10.1.206.213	Firmw. hochladen ...	57% (55326 Bytes/s)
DESSAU	10.1.206.214	Firmw. hochladen ...	53% (65047 Bytes/s)

Datum	Zeit	Name	Adresse	Meldung
27.01.2004	10:38:00	LEIPZIG	10.1.202.218	Firmware hochladen gestartet
27.01.2004	10:38:00	TEMPELHOF	10.1.202.219	Firmware hochladen gestartet
27.01.2004	10:38:00	MERSEBURG	10.1.202.220	Firmware hochladen gestartet
27.01.2004	10:38:00	WITTENBERG	10.1.205.137	Firmware hochladen gestartet
27.01.2004	10:38:00	ANGERMUENDE	10.1.206.211	Firmware hochladen gestartet
27.01.2004	10:38:00	CHEMNITZ	10.1.206.212	Firmware hochladen gestartet
27.01.2004	10:38:00	ADLERSHOF	10.1.206.213	Firmware hochladen gestartet
27.01.2004	10:38:00	DESSAU	10.1.206.214	Firmware hochladen gestartet

- Telnet-Sitzung öffnen: Öffnet mehrere "DOS-Fenster" und startet zu jedem Gerät eine separate Telnet-Verbindung
- Gerät überwachen: Öffnet die ausgewählten Geräte im LANmonitor zur Überwachung
- Datum/Uhrzeit setzen: Stellt auf allen ausgewählten Geräten die Uhrzeit gleich ein.



Beachten Sie für die Einstellung der Uhrzeit auch die Funktionen des LANCOM als NTP-Client und NTP-Server ('Zeit-Server für das lokale Netz' →Seite 431).

- Löschen: Löscht die ausgewählten Geräte aus der Geräteliste im LANconfig.

4.1.1 Verzeichnisstruktur

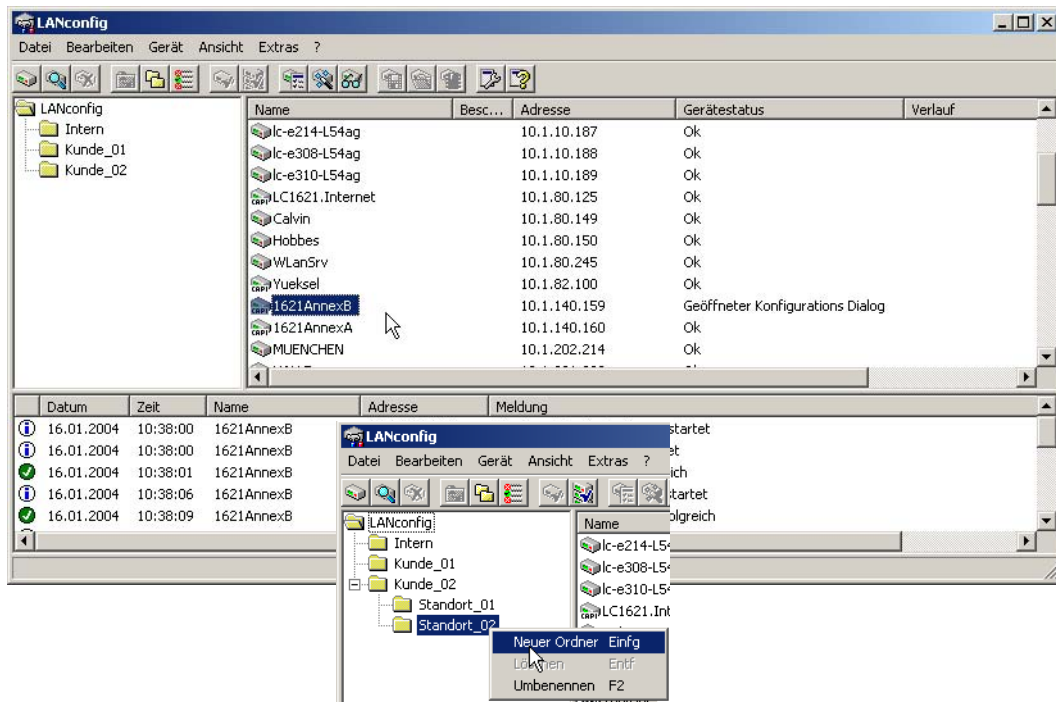
LANconfig erlaubt mit der Verzeichnisstruktur die übersichtliche Verwaltung einer Vielzahl von Geräten. Für jedes Projekt oder jeden Kunden kann ein eigener Ordner angelegt werden, in dem die entsprechenden Geräte organisiert werden:

▷ Projektmanagement mit LANconfig

- ▶ Ein neuer Ordner wird mit einem rechten Mausklick auf das übergeordnete Verzeichnis mit dem Eintrag 'Neuer Ordner' im Kontextmenü angelegt.
- ▶ Die einzelnen Geräte können dann aus der Liste der Geräte einfach mit der Maus in den entsprechenden Ordner gezogen werden. Auch das Verschieben der Geräte in einen anderen Ordner erfolgt auf diese Weise.



Die Zuordnung von einem Gerät zu einem bestimmten Ordner bezieht sich nur auf die Anzeige im LANconfig. Die Organisation der Ordner hat insbesondere keine Auswirkung auf die Konfiguration der Geräte.

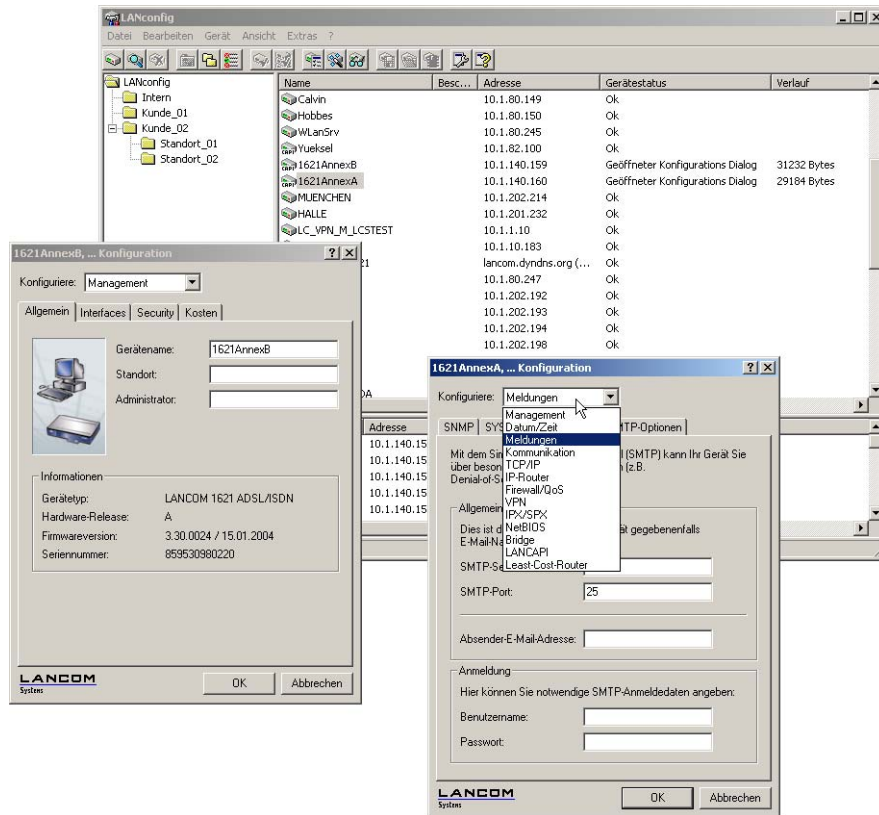


Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann mit der Funktionstaste **F6** oder über das Menü **Ansicht ▶ Verzeichnisbaum** ein- und ausgeschaltet werden.

4.1.2 Multithreading

Bei der Verwaltung von Projekten ist es oft hilfreich, die Konfigurationen von mehreren Geräte gleichzeitig zu öffnen, um darin Gemeinsamkeiten oder Unterschiede abzugleichen. LANconfig erlaubt das gleichzeitige Starten von mehreren Konfigurationsdialogen ("Multithreading"). Nach dem Öffnen einer Konfiguration können aus der Liste der

Geräte im LANconfig einfach weitere Konfigurationen geöffnet werden. Alle Konfigurationen können parallel bearbeitet werden.



Zwischen den geöffneten Konfigurationen können Inhalte mit "Cut and Paste" über die Zwischenablage übertragen werden.

Beim Multithreading können sowohl aus den erreichbaren Geräten ausgelesene Konfigurationen und Konfigurationsdateien bearbeitet werden. Jede Konfiguration wird separat beim schließen des entsprechenden Dialogs in die Datei bzw. das Gerät zurückgeschrieben.

4.1.3 Manuelle und automatische Suche nach Firmware-Updates

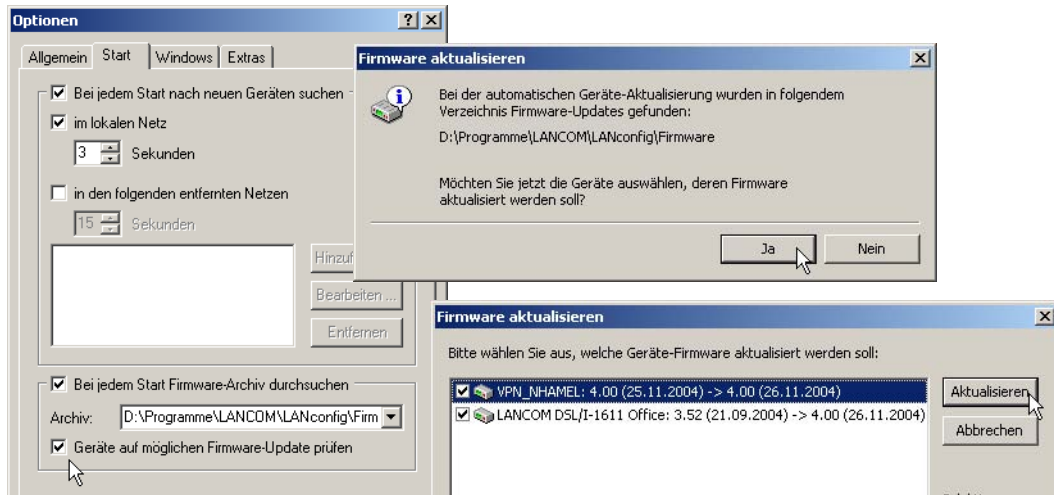
Um das Update auf neue Firmwareversionen in den LANCOM-Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen LANCOM-Modelle und LCOS-Versionen idealerweise in einem zentralen

▷ Projektmanagement mit LANconfig

Archiv-Verzeichnis abgelegt. Die Suche nach neuen Firmware-Versionen in diesem Verzeichnis kann entweder manuell angestoßen werden oder nach jedem Start von LANconfig automatisch durchgeführt werden.

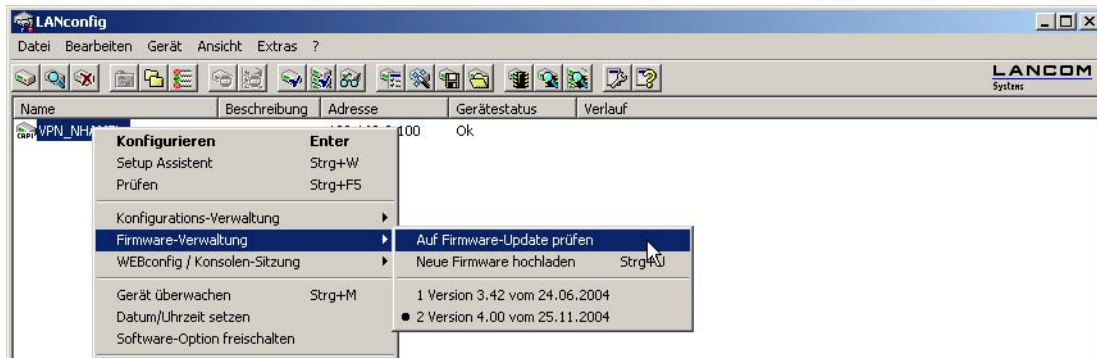
Automatische Suche nach Firmware-Updates

Das Verzeichnis, in dem LANconfig nach den Updates suchen soll, stellen Sie unter **Extras ▶ Optionen ▶ Extras** ein. Zusätzlich können Sie hier angeben, ob LANconfig nach jedem Start das Firmware-Archiv durchsuchen und die gefundenen Geräte auf mögliche Updates prüfen soll. Wenn Sie diese Optionen aktivieren, zeigt LANconfig nach dem Start automatisch die Geräte an, für die neue Updates zur Verfügung stehen.



Manuelle Suche nach Firmware-Updates

Für die manuelle Suche nach Firmware-Updates klicken Sie mit der rechten Maustaste auf einen markierten Eintrag in der Geräteliste und wählen im Kontextmenü den Punkt **Firmware-Verwaltung ▶ Auf Firmware-Updates prüfen**. Wenn Sie mehrere Geräte gleichzeitig updaten möchten, erscheint der Punkt **Auf Firmware-Updates prüfen** direkt im Kontextmenü.



Komplette Liste der Firmware-Versionen einsehen

Wenn bei der Suche im Archiv keine neueren Firmware-Versionen gefunden wurden, können Sie alternativ die komplette Liste alle gefundenen Firmware-Dateien ansehen. So können Sie u.a. auch auf ältere Versionen zurückschalten. LANconfig zeigt alle gefundenen Versionen für alle markierten Geräte an, dabei auch den aktuellen Versionsstand der Geräte. Für jedes Gerät können Sie genau eine Firmware-Version auswählen, die dann in das Gerät eingespielt wird.



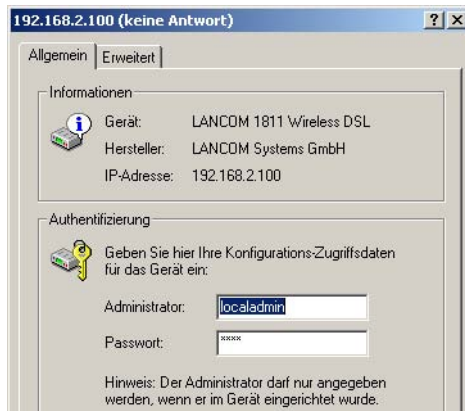
4.1.4 Passwortschutz für SNMP-Lesezugriff

Der Lesezugriff auf ein LANCOM-Gerät über SNMP – z.B. über LANmonitor – kann über ein Passwort geschützt werden. Dabei werden die gleichen Benutzerdaten verwendet wie beim Zugriff auf LANconfig. Wenn der SNMP-Zugriff passwortgeschützt ist, können nur bei der Eingabe der entsprechenden Benutzerdaten Informationen über den Gerätezustand etc. über SNMP ausgelesen werden.

LANmonitor

Die Benutzerinformationen können im LANmonitor für jedes Gerät getrennt eingetragen werden. Klicken Sie dazu mit der rechten Maustaste auf das gewünschte Gerät, wählen Sie im Kontextmenü den Eintrag **Optionen** und tragen Sie Ihre Benutzerdaten ein.

▷ Projektmanagement mit LANconfig

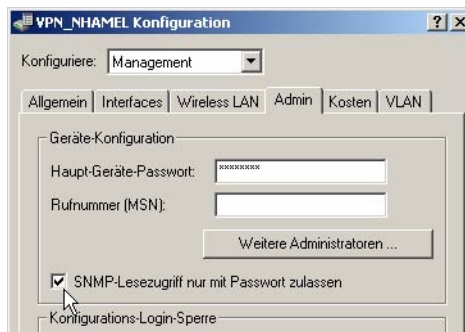


Die Zugriffsrechte im LANmonitor sind abhängig von den Rechten des Benutzers:

- ▶ Ein Supervisor hat vollen Zugriff auf die Informationen im LANmonitor und kann u.a. Aktionen ausführen wie das Trennen von Verbindungen.
- ▶ Ein lokaler Administrator hat ebenfalls vollen Zugriff auf die Informationen im LANmonitor und kann u.a. Aktionen ausführen wie das Trennen von Verbindungen.
- ▶ Ein Benutzer, der nur über Leserechte verfügt, kann die Informationen im LANmonitor ablesen, aber keine Aktionen wie das Trennen von Verbindungen ausführen.
- ▶ Ein Benutzer ohne Rechte hat keinen SNMP-Zugriff auf die Geräte-Informationen.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie den Schalter für den SNMP-Lesezugriff im Konfigurationsbereich 'Management' auf der Registerkarte 'Allgemein':



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Einstellungen für den SNMP-Lesezugriff auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Config-Modul ▶ Passw.Zwang-fuer-SNMP-lesezugriff
Terminal/Telnet	Setup/Config-Modul/Passw.Zwang-fuer-SNMP-lesezugriff

4.2 Scripting

In Installationen mit mehreren LANCOM-Geräte ist oft erwünscht, bestimmte Aufgaben der Konfiguration automatisiert auszuführen. Die Scripting-Funktionen im LANCOM erlauben es, ganze Sätze von Befehlen zur Konfiguration der Geräte in einer Datei – einem Script – zu speichern und in einem Vorgang in ein oder mehrere Geräte zu übertragen.

4.2.1 Anwendungen

Mit dem Scripting steht dem Anwender ein sehr mächtiges Werkzeug zur zentralen Konfiguration der LANCOM-Geräte mit vielfältigen Anwendungsmöglichkeiten zur Verfügung:

- ▶ Auslesen der Geräte-Konfiguration in einer gut lesbaren und speicherbaren Form
Die von LANconfig erzeugten Konfigurationsdateien sind nicht zur direkten Bearbeitung mit anderen Tools vorgesehen, einen direkten Überblick über die komplette Konfiguration erhält der Anwender nur mit einem Ausdruck der Konfigurationsdatei. Mit den Scripting-Funktionen lässt sich die Konfiguration als ASCII-Text ausgeben, der z.B. als einfache Textdatei gespeichert werden kann.
- ▶ Bearbeiten der Konfiguration mit einem einfachen Texteditor
Wenn die Offline-Konfiguration mit LANconfig nicht möglich ist oder nicht sinnvoll erscheint, kann eine mit Hilfe des Scripting erzeugte Konfigurationsdatei mit einem Texteditor bearbeitet und anschließend wieder in das Gerät zurückgespielt werden.
- ▶ Bearbeiten von Teilkonfigurationen
Anstelle einer kompletten Konfiguration können gezielt auch nur Teile davon aus einem Gerät ausgelesen werden (z.B. die Firewall-Einstellungen). Genau wie eine Komplettkonfiguration können auch Teilkonfigurationen bearbeitet und wieder in ein oder mehrere Geräte übertragen werden. Spezielle Einstellungen eines Gerätes können auf diese Weise auch in andere Modelle oder Geräte mit einem anderen Firmware-Stand eingespielt werden.
- ▶ Automatisieren von Konfigurationsupdates
Durch die zentrale Ablage von Konfigurationsscripten im Zusammenhang mit zeitgesteuerten LCOS-Befehlen (Cron-Jobs) können wichtige Konfigurationsteile wie z.B. die Verschlüsselungseinstellungen für ein WLAN automatisch in vielen Geräten auf dem gleichen Stand gehalten werden.

▷ Scripting

- ▶ Komfortabler Roll-Out in größeren Installationen

Bei der Installation von mehreren Geräten an unterschiedlichen Orten kann die Konfiguration sehr leicht zentral vorbereitet werden. Die Geräte können dann dezentral von Mitarbeitern ohne Administrator-Kenntnisse über einen einzigen Befehl eingestellt werden.

- ▶ Speichern der Konfiguration in einem nicht bootresistenten Modus

Mit den Scripting-Befehlen können die Änderungen der Konfiguration gezielt nur im RAM vorgenommen werden, die Übertragung in den bootresistenten Flash-Speicher wird verhindert. Auf diese Weise kann die Konfiguration gezielt nur bis zum nächsten Boot-Vorgang vorgehalten werden, um z.B. im Falle eines Diebstahls keine wichtigen Bestandteile der Konfiguration in fremde Hände gelangen zu lassen.

- ▶ Änderungen der Konfiguration im Testmodus

Über den gleichen Mechanismus lässt sich die Konfiguration sehr leicht im Testmodus ändern. Dabei wird mit Hilfe eines Scriptes ein zeitverzögerter Bootvorgang ausgelöst, bis zu dessen Aktivierung die Konfiguration des Gerätes gefahrlos verstellt werden kann. Falls die Änderungen der Konfiguration nicht erfolgreich sind, wird das Gerät nach dem Ablauf der Verzögerungszeit und dem folgenden Boot-Vorgang automatisch wieder in den vorherigen Konfigurationszustand zurückversetzt.

Mit dieser Variante lässt sich in Analogie zur FirmSafe-Funktion auch eine Art „ConfSafe“ realisieren. Wird nach einem Upgrade der Firmware die Konfiguration geändert, kann nach einem späteren Downgrade zur alten Firmware-Version die Konfiguration manchmal nicht mehr editiert werden. Wird hingegen die Konfiguration nach dem Firmware-Upgrade nur im Testmodus geändert, kann durch das Downgrade und den folgenden Bootvorgang sehr leicht der ursprüngliche Zustand der Geräte bzgl. Firmware **und** Konfiguration wieder hergestellt werden.

4.2.2 Funktion des Scripting

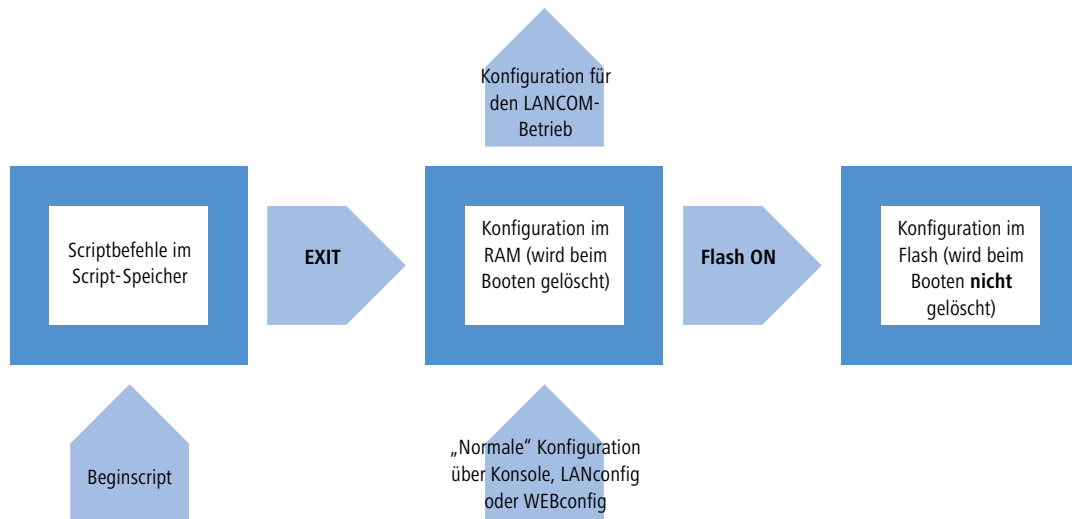
Beim Scripting wird eine Reihe von Konfigurationsbefehlen, so wie sie an der Konsole unter Telnet o.ä. eingegeben werden, gesammelt an ein LANCOM übertragen. Für diese Sammelübertragung von Konfigurationsbefehlen gibt es zwei Varianten:

- ▶ Das Gerät wird in einer Konsolensitzung mit dem Befehl `beginscript` in den Script-Modus versetzt. In diesem Zustand werden die übertragenen Befehle nicht einzeln ausgeführt, sondern zunächst in einen Zwischenspeicher (Script-Speicher) im LANCOM geschrieben. Erst durch ein weiteres Kommando (`exit`) wird die Ausführung der gespeicherten Befehle gestartet.
- ▶ Alternativ werden die Konfigurationsbefehle in einer Scriptdatei (Textdatei) offline gesammelt und editiert und dann als fertiges Script in das Gerät geladen.

Die über das Script ausgeführten Konfigurationsbefehle wirken sich zunächst nur auf die Konfiguration aus, die im RAM des Gerätes gespeichert ist. Der Flash-Modus entscheidet dann darüber, ob die Konfiguration auch im Flash geändert wird:

- ▶ Im Flash-Yes-Modus (Standard) werden die Konfigurationsbefehle auch gleichzeitig in den Flashspeicher des Gerätes geschrieben und werden damit bootresistent. Da bei der Konfiguration über die anderen Wege (Konsole

ohne Script, LANconfig LANconfig oder WEBconfig) der Flash-Modus immer auf ON steht, wird in diesen Varianten die Konfiguration nacheinander in den RAM-Speicher und dann direkt in den Flash geschrieben.



- ▶ Im Flash-No-Modus werden die Daten nur in den RAM geschrieben und sind damit nur bis zum nächsten Bootvorgang verfügbar.
 - ▷ Bei Booten holt sich das Gerät die aktuell im Flash gespeicherte Konfiguration.
 - ▷ Die Konfiguration aus dem RAM kann jederzeit mit dem Befehl „Flash Yes“ in den Flash-Speicher übertragen werden.

Die LANCOM-Geräte verwenden für den aktiven Betrieb die Informationen, die in der RAM-Konfiguration gespeichert sind. Die im Zwischenspeicher gelagerten Scriptbefehle sind ebenso wie die die Konfiguration im Flash für die aktuelle Funktionalität eines LANCOM nicht relevant.

4.2.3 Scriptdateien erstellen

Ein Script für eine LANCOM-Konfiguration liegt in Form einer normalen Textdatei vor. Sie enthält neben ggf. erforderlichen Kommentaren alle Befehle, so wie sie z.B. an der Telnet-Konsole zur Konfiguration angewendet würden. Zur Erstellung der Scriptdateien gibt es zwei verschiedene Wege:

- ▶ Das Script wird mit Hilfe eines Texteditors manuell komplett neu erstellt.
- ▶ Aus einem Gerät wird eine (Teil-)Konfiguration ausgelesen, als Scriptdatei gespeichert und dann mit dem Texteditor geeignet bearbeitet.



Beim Auslesen eines Scriptes aus einem Gerät werden standardmäßig nur die Parameter aufgeführt, die in der Konfiguration gegenüber dem Default-Zustand geändert wurden ('readscript' →Seite 62). Ein kom-

▷ Scripting

plettes Konfigurationsscript kann mit einem speziellen Befehlszusatz ausgelesen werden ('default' →Seite 64).

Konfiguration über die Konsole auslesen

- ① Melden Sie sich an der Konsole mit Supervisor-Rechten an.
- ② Wechseln Sie ggf. in den Zweig des Konfigurationsbaumes, dessen Teilkonfiguration Sie auslesen möchten.
- ③ Führen Sie an der Eingabeaufforderung den Befehl `readscript` aus. Beachten Sie dazu die möglichen Befehlsweiterungen ('Die Befehle für das Scripting' →Seite 62).
- ④ Kopieren Sie die gewünschten Textpassagen über die Zwischenablage in einen Texteditor und bearbeiten Sie dort das Script wie gewünscht.


Über TFTP vom Kommandozeilen-Interface (DOS-Box)

Die Befehle zur Konfiguration können vom Kommandozeilen-Interface direkt über TFTP ausgelesen werden.

- ① Öffnen Sie dazu z.B. eine DOS-Box.
- ② Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
C:\>tftp IP-Adresse get "PASSWORDreadscript Pfad" script.lcs
```

- ▷ IP-Adresse ist die Adresse des Gerätes, aus dem Sie die Konfigurationsbefehle auslesen möchten
- ▷ PASSWORD ist das entsprechende Geräte-Passwort
- ▷ Pfad gibt den Zweig im Menübaum der Konfiguration an, der ausgelesen werden soll. Fehlt die Pfad-Angabe, wird die gesamte Konfiguration ausgelesen.
- ▷ `script.lcs` ist der Name der Script-Datei, unter der die Befehle im aktuellen Verzeichnis gespeichert werden.

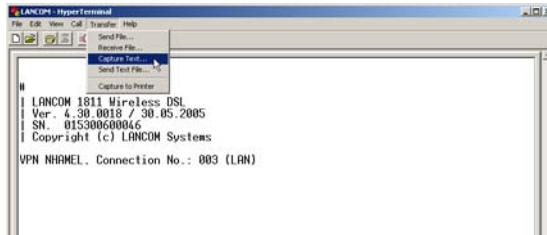
 Beachten Sie, dass die Passwörter der Geräte bei der Eingabe dieses Befehls im Klartext angezeigt werden!

Über Hyperterminal

Terminalprogramme wie Hyperterminal bieten die Möglichkeit, die an der Konsole ausgegebenen Texte direkt in eine Textdatei zu speichern. Mit diesem Verfahren kann man gerade bei umfangreichen Konfigurationsdateien die manchmal unübersichtliche Übertragung über die Zwischenablage umgehen.

- ① Stellen Sie mit Hyperterminal eine Verbindung zu Ihrem Gerät her.

- ② Wählen Sie den Menüpunkt **Übertragung ► Textdatei aufzeichnen** und wählen Sie den gewünschten Speicherort für das Script mit dem Dateinamen aus.



- ③ Führen Sie an der Eingabeaufforderung den Befehl `readscript` aus. Beachten Sie dazu die möglichen Befehlsweiterungen ('Die Befehle für das Scripting' →Seite 62).
- ④ Sobald alle Teilkonfigurationen wie gewünscht aufgerufen wurden, beenden Sie die Aufzeichnung über den Menüpunkt **Übertragung ► Textdatei aufzeichnen ► Beenden**.

Die Konfigurationsbefehle liegen nun als Scriptdatei vor und können entsprechend bearbeitet werden.

4.2.4 Einspielen von Konfigurations-Befehlen und Script-Dateien

Grundsätzlich können die Scriptbefehle auf zwei verschiedenen Wegen in den Zwischenspeicher des LANCOM gelangen:

- Die Befehle können an einer Konsole im Script-Modus (mit dem Befehl „beginscript“) manuell eingegeben werden. Dabei werden die Befehle direkt aus der Konsole in den Zwischenspeicher geschrieben. Nachdem alle Befehle wie gewünscht fertiggestellt sind, werden sie mit dem Befehl „exit“ abgearbeitet und in das RAM übertragen.
- Die gewünschten Befehlssequenzen können in einer Textdatei gespeichert werden. Diese Textdatei wird dann über geeignete Wege (LANconfig, Terminalprogramm, TFTP) an den Zwischenspeicher gesendet. Wenn die erforderlichen Befehle in der Datei enthalten sind, wird dann automatisch die Übertragung der Konfiguration in das RAM gestartet.

Zum Einspielen von Scriptdateien in die LANCOM-Geräte gibt es verschiedene Möglichkeiten, von denen Sie je nach verwendetem Konfigurationstool den für Sie passenden Weg auswählen können.

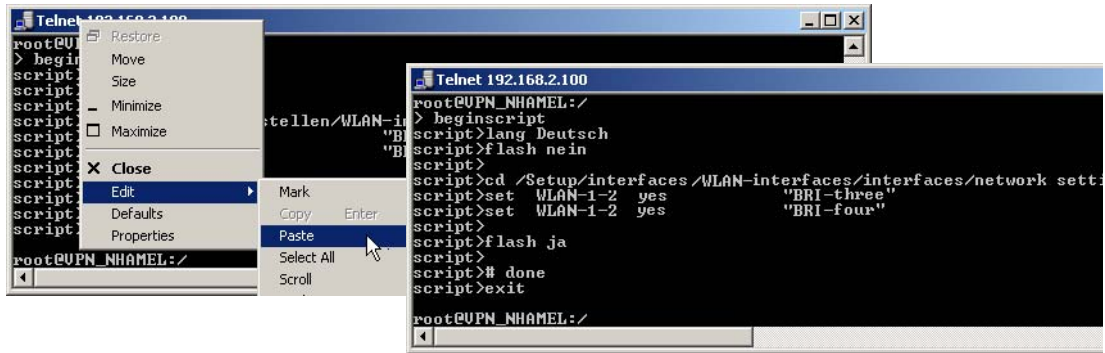
Befehlseingabe über Konsolen-Sitzung (Telnet, SSH)

In einer Konsolensitzung können Sie ein Script über die Zwischenablage in das Gerät einspielen:

- ① Öffnen Sie Ihr Script in einem beliebigen Texteditor und übertragen Sie die Konfigurationsbefehle in die Zwischenablage.
- ② Melden Sie sich an der Konsole mit Supervisor-Rechten an.

▷ Scripting

- ③ Starten Sie den Script-Modus mit dem Befehl `beginscript`.



- ④ Fügen nach dem Script-Prompt (`script>`) die Befehle aus der Zwischenablage ein. Unter Telnet z.B. mit einem rechten Mausklick auf den oberen Fensterrand.
- ⑤ Mit dem Befehl `exit` wird die Ausführung der Konfigurationsbefehle gestartet.



Falls der Befehl `exit` schon in den kopierten Befehlen enthalten ist, wird die Ausführung der Konfiguration gleich nach dem Einfügen automatisch gestartet!

Script hochladen mit TFTP-Client

Während einer Konsolensitzung (z.B. über Telnet oder SSH) können mit Hilfe des TFTP-Befehls auch Script-Dateien von einem TFTP-Server direkt in das Gerät geladen werden.

- ① Melden Sie sich an der Konsole mit Supervisor-Rechten an.
- ② Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
>loadscript -s IP-Adresse -f script.lcs
```

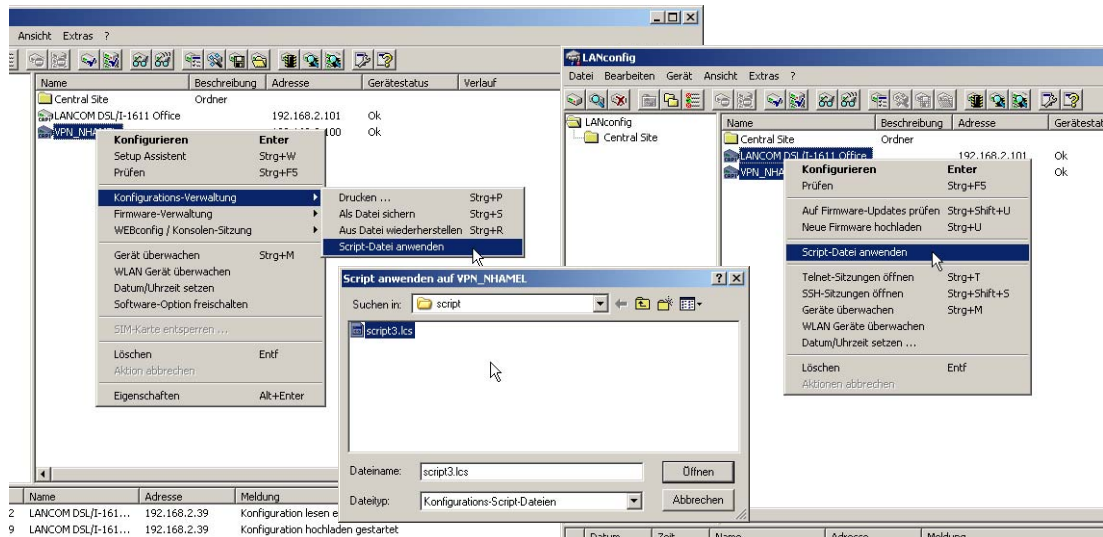
- ▷ IP-Adresse ist die Adresse des TFTP-Servers, auf dem die Script-Datei liegt
- ▷ `script.lcs` ist der Name der Script-Datei auf dem TFTP-Server

Script hochladen mit LANconfig

Unter LANconfig haben Sie die Möglichkeit, ein Script entweder nur auf ein Gerät oder parallel auf viele Geräte gleichzeitig anzuwenden.

- ① Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie im Kontextmenü den Eintrag **Konfigurationsverwaltung ▶ Script-Datei anwenden**. Bei mehreren markierten Geräten erscheint der Eintrag **Script-Datei anwenden** direkt im Kontextmenü.

- ② Wählen Sie im folgenden Dialog die gewünschte Script-Datei (*.lcs) für den Upload aus.



- i** Der Upload des Scriptes wird automatisch gestartet. Status- und Fehlermeldungen werden entweder über LANconfig direkt ausgegeben oder können in einer Konsolensitzung mit dem Befehl `show script` eingesehen werden.

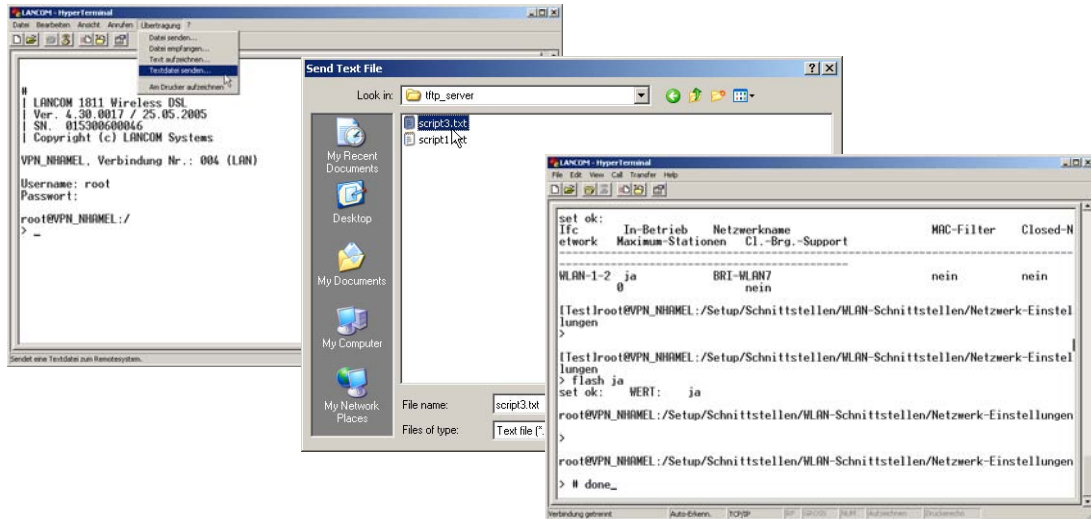
Script hochladen mit Hyperterminal

Auch über Terminalprogramme wie das mit Windows gelieferte Hyperterminal können Scripte in ein LANCOM geladen werden.

- ① Stellen Sie mit Hyperterminal eine Verbindung zu Ihrem Gerät her.
- ② Wählen Sie den Menüpunkt **Übertragung ► Textdatei senden**.

▷ Scripting

③ Wählen Sie die gewünschte Scriptdatei und starten Sie die Übertragung.



Nach dem erfolgreichen Beenden der Übertragung wird das Script automatisch gestartet.

4.2.5 Mehrere Script-Sessions parallel

Das LANCOM kann mehrere Script-Sessions parallel verwalten. So wie mehrere Konsolensitzungen gleichzeitig auf einem Gerät ablaufen können, können auch verschiedene Scripte gleichzeitig auf das LANCOM zugreifen. Parallele Script-Sessions machen z.B. in folgenden Szenarien Sinn:

- ▶ Mit einem Script ① wird ein zeitverzögerter Reboot des Gerätes gestartet, z.B. nach Ablauf von 30 Minuten. Mit einem zweiten Script ② wird während der Laufzeit des Gerätes die Konfiguration zu Testwecken verändert, der Flash-Modus wird dabei ausgeschaltet. Sollte das Gerät durch die Konfigurationsänderungen von Script ② nicht mehr erreichbar sein, startet Script ① das Gerät nach 30 Minuten neu und verwirft so die Änderungen in der Konfiguration.
- ▶ Bei der Anwendung von verschiedenen Scripten für Teilkonfigurationen können mehrere Scripte z.B. über Cron-Jobs automatisch gleichzeitig gestartet werden. Die einzelnen Konfigurationsaufgaben müssen dabei nicht abwarten, bis das vorhergehende Script abgearbeitet ist.

4.2.6 Die Befehle für das Scripting

- ▶ readscript

Der Befehl readscript erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden. Im einfachsten Fall gibt das LANCOM nur die Befehle aus, mit denen von der Grundeinstellung abweichende Parameter modifiziert werden.

Syntax: readscript [-n] [-d] [-c] [-m] [PATH]

i Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

Beispiel: Der Befehl `readscript` führt ohne weitere Einschränkungen bei einem LANCOM, für das nur ein Internet-by-Call-Zugang über ISDN eingerichtet wurde, zu folgender Ausgabe an der Konsole:

```
Telnet 192.168.2.101
#
! LANCOM DSL/I-1611 Office
! Ver. 4.30.0018 / 30.05.2005
! SN. 000590300000
! Copyright (c) LANCOM Systems
Connection No.: 002 (LAN)

root@:/
> readscript
# Head
lang English
flash No

cd /Setup/VAN/Dialup-Remote-Peers
del *
add "DEFAULT" "" "" 20 20 ""
add "ARCOR" "" "0192070" 90 90 "ARCOR"
cd /Setup/VAN/Layer
del *
add "DEFAULT" TRANS PPP TRANS bnd+cmpr HDLC64K
add "I-ISDN" TRANS PPP TRANS none HDLC64K
add "PPP" TRANS PPP TRANS bnd+cmpr HDLC64K
add "PPPHDLC" TRANS PPP TRANS none HDLC64K
add "RAVHDLC" TRANS TRANS TRANS none HDLC64K
add "I-ISL" TRANS PPP PPPOE none ETH
add "PPPOE" TRANS PPP PPPOE none ETH
add "IPOE" ETHER TRANS TRANS none ETH
add "DHCP" ETHER DHCP TRANS none ETH
add "V.24_DEF" TRANS GPPP TRANS none SERIAL
add "ARCOR" TRANS PPP TRANS none HDLC64K
cd /Setup/VAN/PPP
del *
add "DEFAULT" PAP "" 0 5 ""
add "ARCOR" none "arcor" 0 5 "arcor"
set /Setup/LAN/Connector 32
set /Setup/TCP-IP/Intranet-Address 192.168.2.101
cd /Setup/IP-Router/IP-Routing-Table
del *
add 192.168.0.0 255.255.0.0 0 "0.0.0.0" 0 No
add 172.16.0.0 255.240.0.0 0 "0.0.0.0" 0 No
add 10.0.0.0 255.0.0.0 0 "0.0.0.0" 0 No
add 224.0.0.0 224.0.0.0 0 "0.0.0.0" 0 No
add 255.255.255.255 0.0.0.0 0 "ARCOR" 0 on
set /Setup/MIC/Operating No
cd /Setup/Config/Access-Table
set LAN Yes Yes Yes Yes No Yes Yes No
set /Setup/Mail/SMTP-Port 0
set /Setup/Mail/POP3-Port 0
set /Setup/Mail/Send-Again-(min.) 0
set /Setup/Mail/Hold-Time-(hrs.) 0
set /Setup/Mail/Buffer 0
Flash Yes

# done
exit

root@:/
>
```

An diesem Beispiel ist das Verhalten des Scripts zu erkennen, das mit dem Befehl `readscript` erzeugt wird.

- ▷ Zunächst werden nur die Parameter aufgeführt, die in der Konfiguration gegenüber dem Default-Zustand geändert wurden.
- ▷ Die Werte in den Tabellen und für einzelne Werte werden jeweils gelöscht (`del *`) und mit den aktuellen Werten der Konfiguration neu gesetzt (`add *`).
- ▷ Nur Tabelleneinträge oder Werte, die nicht leer sein dürfen, werden mit dem `Set`-Befehl direkt geändert.

i Bei Tabellenzeilen oder Strings, die Passwörter enthalten, werden die Passwörter im Klartext ausgegeben, da diese Form auch von der Telnetoberfläche verlangt wird.

▷ Scripting

Mit dem erzeugten Script ist der Anwender in der Lage, ein LANCOM genau so zu konfigurieren wie das Ursprungsgerät.

Da die Scripte zur Anpassung der Konfiguration in manchen Fällen sehr umfangreich sind, können auch gezielt Scripte von Teilen der Konfiguration erzeugt werden. Dazu wechseln Sie z.B. zunächst in das Verzeichnis, dessen Konfiguration Sie in einem Script festhalten wollen (z.B. `cd set/ip-router/firewall` für die Firewall-einstellungen) und führen dann den `readscript`-Befehl aus. Alternativ übergeben Sie den Pfad zum gewünschten Menü direkt mit dem `readscript`-Befehl als Path-Parameter (z.B. `readscript set/ip-router/firewall`). In beiden Fällen werden nur die – im Vergleich zur Default-Konfiguration – geänderten Einstellungen der Firewall in das Script übernommen.

Mit folgenden Optionen kann der `readscript`-Befehl zusätzlich erweitert werden:

- ▷ `-d` (default): Dabei werden auch die Befehle zur Modifikation derjenigen Parameter erzeugt, die den gleichen Wert wie in der Grundkonfiguration haben. Solche umfangreichen Scripte eignen sich z.B. bei der Übertragung von Konfigurationen auf Geräte eines anderen Typs oder mit einem anderen Firmwarestand, da die Grundkonfiguration in diesen Fällen abweichen kann.
- ▷ `-n` (numeric): Mit diesem Zusatz werden die Pfade im Script nicht im Klartext, sondern numerisch anhand der SNMP-Bezeichnung ausgegeben. Auch diese Variante trägt zur Übertragbarkeit von Scripten auf andere Firmwarestände bei, da sich die Bezeichnungen der Pfade durchaus ändern können, die Positionen im SNMP-Baum jedoch üblicherweise nicht.
- ▷ `-c` (comment): Dieser Parameter erzeugt im Zusammenspiel mit `-d` und `-n` zusätzliche Kommentare, die das Lesen der Scripte erleichtern. Für den Parameter `-d` wird jede Befehlskombination die einen Defaultwert setzt mit `# default value` gekennzeichnet. Bei `-n` wird jeder numerische Pfad mit seinem textuellen Äquivalent kommentiert.
- ▷ `-m` (minimize): Mit diesem Parameter werden vorhandene Lücken aus dem Script entfernt, die Datei wird kleiner und kompakter.

▶

Das Zeichen `#` am Zeilenbeginn – gefolgt von einem Leerzeichen – leitet einen Kommentar ein. Bis zum Zeilenende werden alle Zeichen ignoriert.



Das Leerzeichen nach dem `#` ist zwingend erforderlich.

▶ `del *`

Dieser Befehl löscht eine komplette Tabelle in dem mit `Path` angegebenen Zweig des Menübaums.

Syntax: `del [PATH] *`

▶ `default`

Mit diesem Befehl ist es möglich, einzelne Parameter, Tabellen oder ganze Menübaume in die Grundkonfiguration zurückzusetzen.

Syntax: `default [-r] [PATH]`

Dieser Befehl setzt den mit `PATH` adressierten Parameter auf den Grundzustand. Zeigt `PATH` auf einen Zweig des Menübaums, muss zwingend die option `-r` (recursive) angegeben werden.

i Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

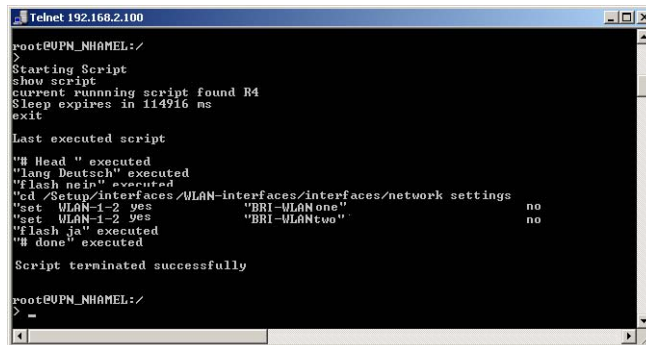
► `beginscript`

Mit dem Befehl `beginscript` wird eine Konsolensitzung in den Script-Modus versetzt. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes. Erst bei Aufruf des Befehls `exit` wird die sequenzielle Übertragung der Befehle über eine Script-Session in den Konfigurations-RAM gestartet.

i Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

► `show script`

Der Befehl `show script` zeigt den Inhalt des zuletzt ausgeführten Scripts und eine Übersicht über die Scripte, die aktuell noch ausgeführt werden. Die bei der Ausgabe der aktuellen Scripte angezeigten Namen können zum vorzeitigen Abbrechen der Scripte verwendet werden ('`killscript`' →Seite 65).



```

Telnet 192.168.2.100
root@UPN_NHAMEL:/
>
Starting Script
show script
current running script found R4
Sleep expires in 114916 ms
exit

Last executed script
"# Head " executed
"lang Deutsch" executed
"flash nein" executed
"cd /Setup/interfaces/WLAN-interfaces/interfaces/network settings
"set WLAN-1-2 yes          "BRI-VLANtwo"
"set WLAN-1-2 yes          "BRI-VLANtwo"
"flash ja" executed
"# done" executed

Script terminated successfully

root@UPN_NHAMEL:/
>

```

i Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

► `killscript`


Der Befehl `killscript` löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt ('`show script`' →Seite 65).

i Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.

► `flash Yes/No`

▷ Gruppen- Konfiguration mit LANconfig

Da beim Konfigurieren eines Gerätes mittels Script jeder `add-`, `set-` oder `del-` Befehl dazu führen kann, dass ein – unerwünschtes – Aktualisieren der Konfiguration im Flash erfolgt, kann das Aktualisieren im Flash abgeschaltet werden. Nach Abschluss der Konfiguration wird das Aktualisieren mit `flash Yes` wieder eingeschaltet. Änderungen in der RAM-Konfiguration werden dann ins Flash geschrieben. Der Status `flash Yes/No` wird global gespeichert.

 Um diesen Befehl auszuführen sind Supervisor-Rechte erforderlich.


▶ `sleep`

Mit dem Befehl `sleep` lässt sich die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne verzögern oder auf einen bestimmten Zeitpunkt terminieren.

Syntax: `sleep [-u] Wert[suffix]`

Als Suffix sind `s`, `m`, oder `h` fuer Sekunden, Minuten, oder Stunden erlaubt, ohne Suffix arbeitet der Befehl in Millisekunden.

Mit dem Optionsschalter `-u` nimmt das `sleep`-Kommando Zeitpunkte im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch) entgegen.

 Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist.

Die `Sleep`-Funktion ist hilfreich z.B. für einen zeitversetzten Reboot beim Testen einer geänderten Konfiguration oder für ein zeitgesteuertes Update der Firmware bei einem größeren Roll-Out von mehreren Geräten.

4.3 Gruppen-Konfiguration mit LANconfig

Bei der Verwaltung vieler Geräte ist es hilfreich, eine Auswahl an Konfigurations-Parametern gleichzeitig in eine Gruppe von Geräten einzuspielen, statt die Parameter einzeln in jedem Gerät manuell zu setzen, z.B. bei identischen Clientberechtigungen in WLAN-Access-Points. Das Importieren einer kompletten Konfigurationsdatei eines Gerätes ist insofern nicht sinnvoll, da hierbei gerätespezifische Parameter wie die IP-Adresse ebenfalls übernommen werden. Die Gruppen-Konfiguration von LANconfig ermöglicht das einfache Importieren von Teil-Konfigurationsdateien und damit das gleichzeitige Verwalten mehrerer Geräte.

Die Teil-Konfigurationsdateien mit den gemeinsamen Parametern für eine Gruppe von LANCOM-Geräten werden wie komplette Konfigurationsdateien auf der Festplatte oder einem Server gespeichert. Für die Konfiguration von ganzen Geräte-Gruppen werden unter LANconfig Verweise auf diese Teil-Konfigurationsdateien angelegt, die eine komfortable Verbindung zwischen den Geräteeinträgen in LANconfig und den Teil-Konfigurationsdateien herstellen.

 Die Gruppenkonfiguration wird für LANCOM-Geräte mit einer Firmware LCOS 5.00 oder höher unterstützt.

▷ Gruppen- Konfiguration mit LANconfig

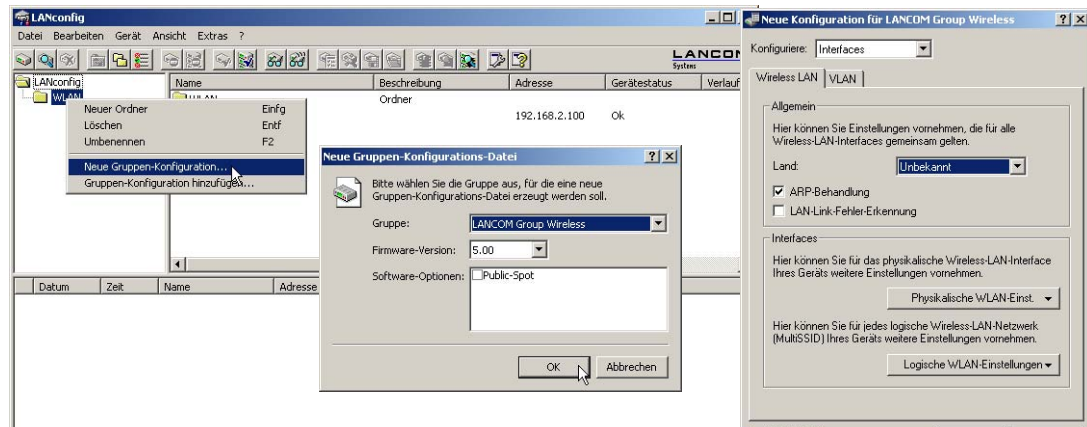
In der LCOS-Version 5.00 werden zunächst Gruppen-Konfigurationen für WLAN-Geräte unterstützt. In späteren Firmware-Versionen werden auch andere Gruppen-Konfigurationen (z.B. für die VPN-Parameter) unterstützt. Informieren Sie sich auf der LANCOM-Webseite www.lancom.de über aktuelle Firmware-Versionen mit erweiterten Möglichkeiten der Gruppen-Konfiguration.

4.3.1 Anlegen einer Gruppen-Konfiguration

Voraussetzung für die Verwendung der Gruppenkonfiguration ist die Gruppierung der Geräte in Ordnern. Diese LANconfig-Ordner enthalten die Geräteeinträge, für die eine gemeinsame Teilkonfiguration sinnvoll ist sowie die Gruppen-Konfigurationen als Verweise zu den Teil-Konfigurationsdateien.

Gruppen-Konfiguration mit neuer Teil-Konfigurationsdatei

- ① Legen Sie einen neuen Ordner an und verschieben Sie die zu gruppierenden Geräte mit der Maus in diesen neuen Ordner.
- ② Klicken Sie anschließend mit der rechten Maustaste auf den neuen Ordner und wählen Sie im Kontextmenü den Eintrag **Neue Gruppen-Konfiguration...**. Nach der Auswahl des Gruppen-Typs und der Firmwareversion öffnet sich der Konfigurationsdialog von LANconfig mit reduzierten Konfigurationsmöglichkeiten.

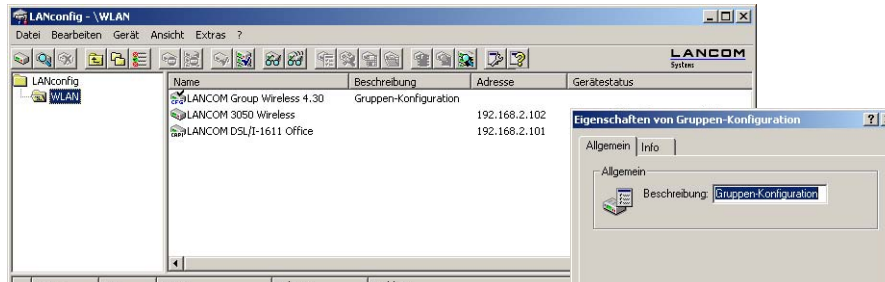


- ③ Stellen Sie in der Konfiguration die Parameter so ein, wie sie für die gesamte Gruppe gelten sollen. Beim Schließen des Konfigurationsdialogs fordert LANconfig Sie auf, die entsprechende Teil-Konfigurationsdatei an einem beliebigen Ort zu speichern.

! Die Gruppen-Konfiguration speichert alle Parameter in eine Teil-Konfigurationsdatei. Dabei werden auch die Parameter mit den Standardwerten gespeichert, die nicht geändert wurden. Verwenden Sie die Scripting-Funktionen ('Scripting' → Seite 55), um nur die von der Standardeinstellung abweichenden Parameter aus dem Gerät auszulesen und ggf. auf andere Geräte zu übertragen.

▷ Gruppen- Konfiguration mit LANconfig

- ④ Der Verweis zur Teil-Konfigurationsdatei erscheint in der Liste der Einträge mit der Beschreibung 'Gruppen-Konfiguration'. Der Name der Gruppen-Konfiguration kann über die Eigenschaften geändert werden. Klicken Sie dazu den Eintrag mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**.



- ! Die Gruppen-Konfiguration ist ein Verweis auf die Teil-Konfigurationsdatei. Beachten Sie, dass Änderungen der Teil-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfiguration zur Folge haben.

Bestehende Teil-Konfigurationsdatei verwenden

In manchen Fällen ist es sinnvoll, die mit LANconfig verwalteten Geräte anders in Ordnern zu strukturieren, als es die Gruppen-Konfiguration erfordern würde. Die Geräte in standortspezifischen Ordnern können z.B. durchaus mit den gleichen Gruppen-Konfigurationen eingestellt werden. Um nicht für jeden Ordner redundant die gleichen Teil-Konfigurationsdateien zu erstellen, können in mehreren Ordnern Verweise auf eine gemeinsame Teil-Konfigurationsdatei erstellt werden.

- ① Um eine vorhandene Teil-Konfigurationsdatei für eine Gruppen-Konfiguration zu verwenden, klicken Sie mit der rechten Maustaste auf den gewünschten Ordner und wählen im Kontextmenü den Eintrag **Gruppen-Konfiguration hinzufügen...**
- ② Wählen Sie im folgenden Dialog die bereits bestehende Teil-Konfigurationsdatei aus und erstellen Sie so in dem Ordner einen Verweis auf diese Datei.

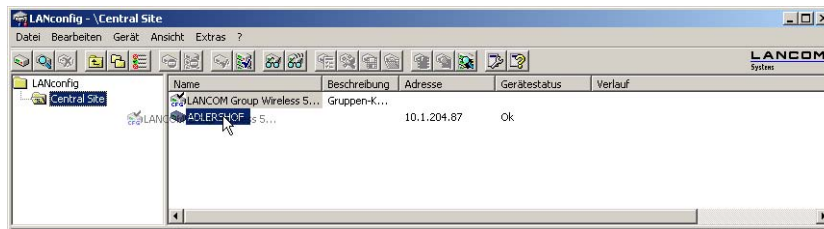
- ! Beachten Sie, dass Änderungen der Teil-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfigurationen in verschiedenen Ordnern zur Folge haben.

4.3.2 Gerätekonfigurationen aktualisieren

Beim Aufrufen oder Aktualisieren eines Ordners prüft LANconfig, ob die Konfiguration der Geräte in diesem Ordner mit den Einstellungen in der aktiven Gruppen-Konfiguration übereinstimmt. Über Abweichungen von der Gruppen-Konfiguration informiert der Gerätestatus 'Gruppen-Aktualisierung empfohlen'.

Um die Gruppen-Konfiguration in das WLAN-Gerät zu laden, ziehen Sie den Gruppen-Konfigurationseintrag auf den entsprechenden Geräteeintrag. Nach erfolgreicher Übertragung der Parameter ändert sich der Gerätestatus auf 'OK'.

▷ Gruppen- Konfiguration mit LANconfig



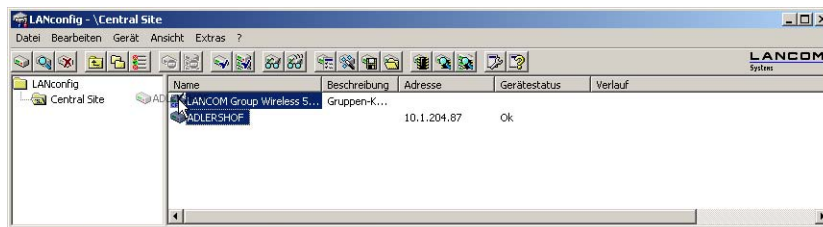
Es ist auch möglich, die Teil-Konfiguration eines Gerätes als Gruppen-Konfiguration zu verwenden. Ziehen Sie hierzu den Geräteeintrag auf den Gruppen-Konfigurationseintrag.

4.3.3 Gruppen-Konfigurationen aktualisieren

Neben dem manuellen Verändern der Parameter einer Gruppen-Konfiguration kann auch die aktuelle Konfiguration eines Gerätes als Basis für eine Gruppen-Konfiguration verwendet werden. Ein Gerät wird damit zum „Master“ für alle anderen Geräte im gleichen Ordner.

Um die Parameter einer Gruppen-Konfiguration von einer aktuellen Geräte-Konfiguration zu übernehmen, ziehen Sie einfach den Eintrag des Gerätes auf die gewünschte Gruppen-Konfiguration. Alle in der Gruppen-Konfiguration definierten Parameter werden dabei mit den Werten der Geräte-Konfiguration überschrieben.

Beim folgenden Prüfen der Geräte wird LANconfig feststellen, dass die Konfigurationen der anderen Geräte im Ordner nicht mehr mit der neuen Gruppen-Konfiguration übereinstimmen und dies über den Gerätestatus entsprechend anzeigen.



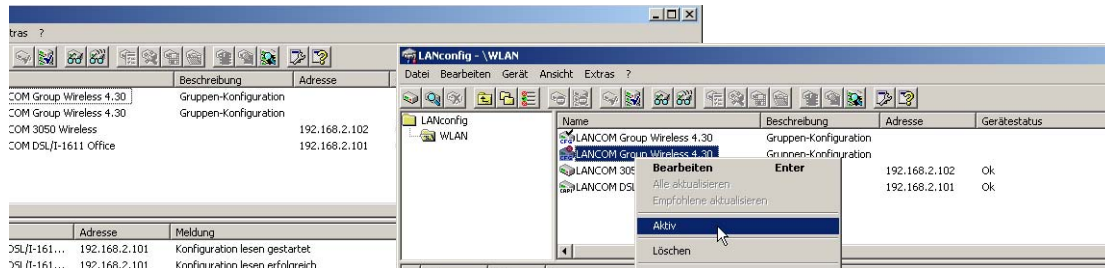
4.3.4 Mehrere Gruppen-Konfigurationen verwenden

Innerhalb eines Ordners können mehrere Gruppen-Konfigurationen angelegt werden. Von diesen Gruppen-Konfigurationen darf jeweils nur eine aktiv sein, da sich der Gerätestatus nur auf **eine** Gruppen-Konfiguration beziehen kann. Aktive Gruppen-Konfigurationen sind mit einem blauen Häkchen, inaktive Gruppen-Konfigurationen mit einem roten Kreuz gekennzeichnet. Um eine Gruppen-Konfiguration zu aktivieren, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen im Kontextmenü den Eintrag **Aktiv**. Alle anderen Gruppen-Konfigurationen werden dabei automatisch deaktiviert.

▷ Anzeige- Funktionen im LANmonitor

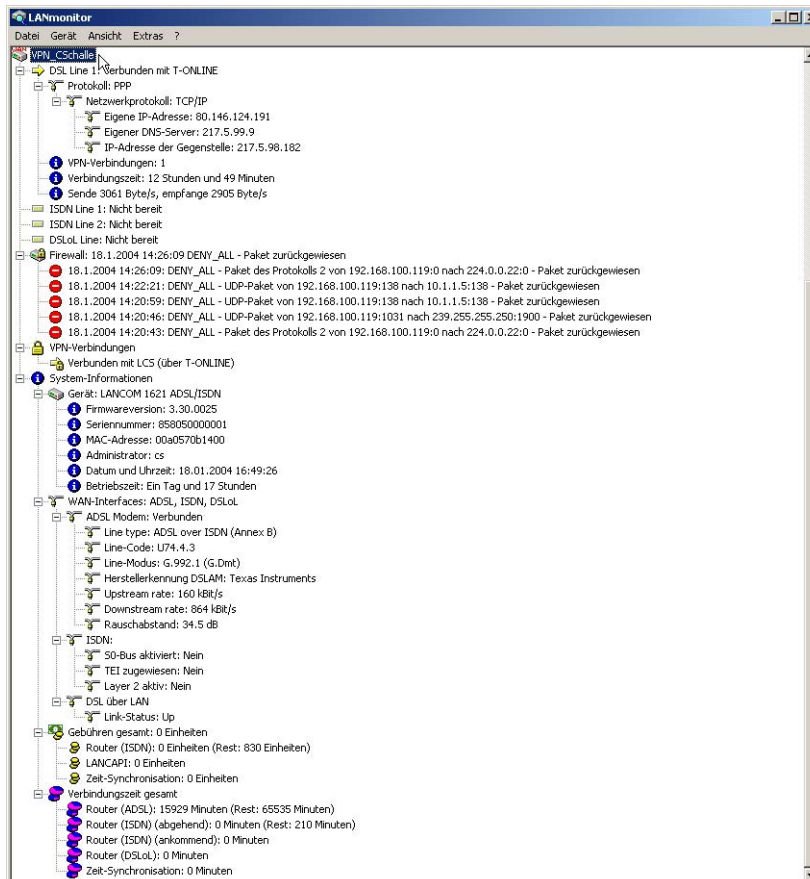


Unterschiedliche Gruppenkonfigurationen in einem Ordner dürfen nicht auf die gleiche Teil- Konfigurations- datei verweisen!



4.4 Anzeige-Funktionen im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen LANCOM-Anwendungen mit einer Reihe von Funktionen, die das Überwachen von Geräten an verteilten Standorten erleichtern. Schon in der Übersicht der überwachten Geräte zeigt LANmonitor die wichtigsten Informationen über den Status der Geräte an:



Zu den Informationen, die in der Übersicht abgelesen werden können, gehören u.a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

Mit einem rechten Mausklick auf die Geräte im LANmonitor können im Kontextmenü Listen mit weiteren Informationen aufgerufen werden:

► VPN-Verbindungen

In der Liste der VPN-Verbindungen werden die letzten 100 VPN-Verbindungen protokolliert. Dabei werden u.a. folgenden Detailinformationen erfasst

▷ Anzeige- Funktionen im LANmonitor

Netzwerk-Management mit den LANtools

Name	Status	Letzter Fehler	Haltezeit	Verbindung	Gateway	Verschlüsselungs-Algo...	Hmac-Algorithmus	Hash-Algorithmus
VPN_AMAY	Nicht Verbunden	Leitungsüberwa...	0 Sekunden	INTERNET	217.228.41.56	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_CBUERSCH	Verbunden		0 Sekunden	INTERNET	80.142.186.239	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_CSCHALLE	Verbunden		0 Sekunden	INTERNET	80.146.98.22	AES (128 Bit)	(none) (0 Bit)	HMAC_MDS (128 Bit)
VPN_DEICH	Verbunden		0 Sekunden	INTERNET	80.142.139.67	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_ETRABER	Verbunden		0 Sekunden	INTERNET	212.202.73.28	BLOWFISH (128 Bit)	SHA (160 Bit)	HMAC_SHA (160 Bit)
VPN_FJANSSEN	Verbunden		0 Sekunden	INTERNET	82.82.232.129	BLOWFISH (128 Bit)	SHA (160 Bit)	HMAC_SHA (160 Bit)
VPN_FTHEINEN	Verbunden		0 Sekunden	INTERNET	80.146.66.20	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_HBATTI	Verbunden		0 Sekunden	INTERNET	80.146.114.101	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_MBAGSIK	Verbunden		0 Sekunden	INTERNET	213.23.254.236	AES (128 Bit)	(none) (0 Bit)	HMAC_MDS (128 Bit)
VPN_MBRIX	Verbunden		0 Sekunden	INTERNET	213.54.77.150	AES (128 Bit)	(none) (0 Bit)	HMAC_MDS (128 Bit)
VPN_MPLUM	Verbunden		0 Sekunden	INTERNET	80.146.89.25	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_OSCHILPE	Verbunden		0 Sekunden	INTERNET	82.72.51.100	AES (128 Bit)	(none) (0 Bit)	HMAC_MDS (128 Bit)
VPN_TINDO	Verbunden		0 Sekunden	INTERNET	217.82.205.102	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_WOHN	Verbunden		0 Sekunden	INTERNET	217.136.170.119	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)
VPN_WTIW	Verbunden		0 Sekunden	INTERNET	217.80.153.52	BLOWFISH (128 Bit)	(none) (0 Bit)	HMAC_SHA (160 Bit)

- ▷ Name der Gegenstelle
- ▷ aktueller Status
- ▷ letzte Fehlermeldung
- ▷ IP-Adresse des Gateways
- ▷ Verschlüsselungsinformationen
- ▶ Accounting-Informationen

Mit den Accounting-Informationen werden die Verbindungen der einzelnen Stationen im LAN zu den erreichbaren Gegenstellen im WAN protokolliert. Dabei werden u.a. folgenden Detailinformationen erfasst:

Benutzer	Gegenstelle	Typ	Verbindungen	Empfangen	Gesendet	Verbindungszeit gesamt
dual-p3	VPN_MPLUM	VPN-Verbindung	2	2.411 MB	32.090 MB	69 Tage und 8 Stundt
w2k-prodtest-sv	VPN_HBATTI	VPN-Verbindung	0	3.989 MB	1.977 MB	88 Tage und 21 Stundt
lc_vpn_m_ethout	VPN_WOHN	VPN-Verbindung	0	739.406 KB	2.541 MB	88 Tage und 18 Stundt
ics-mail	VPN_WTIW	VPN-Verbindung	0	917.816 KB	799.849 KB	76 Tage und 21 Stundt
fthein2	VPN_FTHEINEN	VPN-Verbindung	0	108.579 KB	159.375 KB	72 Tage und 23 Stundt
lc_vpn_m_ethout	VPN_CSCHALLE	VPN-Verbindung	0	187.790 KB	448.049 KB	53 Tage und 18 Stundt
10.1.1.1	VPN_WTIW	VPN-Verbindung	0	1.783 KB	1.553 KB	36 Tage und 5 Stundt
ics-mail	VPN_FJANSSEN	VPN-Verbindung	0	464.767 KB	1.968 MB	36 Tage und 0 Stundt
lc_vpn_m_ethout	VPN_WOHN	VPN-Verbindung	0	7.015 KB	231.069 KB	35 Tage und 19 Stundt
10.1.80.172	VPN_FTHEINEN	VPN-Verbindung	0	11.010 KB	21.643 KB	34 Tage und 15 Stundt
ics-data	VPN_MPLUM	VPN-Verbindung	0	7.768 KB	50.828 KB	33 Tage und 19 Stundt
10.1.1.1	VPN_CSCHALLE	VPN-Verbindung	0	25.226 KB	21.042 KB	33 Tage und 14 Stundt
cbuersch-gs	VPN_CBUERSCH	VPN-Verbindung	0	519.200 KB	49.536 KB	32 Tage und 21 Stundt
10.1.80.173	VPN_HBATTI	VPN-Verbindung	0	959.701 KB	177.880 KB	32 Tage und 18 Stundt
lc_vpn_m_ethout	VPN_WTIW	VPN-Verbindung	0	1.092 KB	45.518 KB	30 Tage und 20 Stundt
deichel3	VPN_DEICH	VPN-Verbindung	0	771.258 KB	826.401 KB	30 Tage und 14 Stundt
lc_vpn_m_ethout	VPN_CBUERSCH	VPN-Verbindung	2	4.946 KB	363.813 KB	27 Tage und 11 Stundt
10.1.80.172	VPN_FTHEINEN	VPN-Verbindung	0	188 KB	30.061 KB	26 Tage und 9 Stundt
lc_vpn_m_ethout	VPN_HBATTI	VPN-Verbindung	0	14.907 KB	546.058 KB	25 Tage und 4 Stundt
dual-n3	VPN_MPLUM	VPN-Verbindung	0	294.443 KB	295.600 KB	19 Tage und 7 Stundt

- ▷ Name bzw. IP-Adresse der Station
- ▷ Gegenstelle, über die eine Verbindung aufgebaut wurde
- ▷ Typ der Verbindung, also z.B. DSL- oder VPN-Verbindung
- ▷ Anzahl der Verbindungen
- ▷ gesendetes bzw. empfangenes Datenvolumen
- ▷ Verbindungszeit
- ▶ Aktivitätsprotokoll

▷ LANmonitor – wissen, was läuft

Mit dem Aktivitätsprotokoll werden die Aktivitäten auf WAN-, WLAN-, VPN-, LANCAPI- und a/b-Port-Verbindungen sowie der Firewall protokolliert. Dabei werden u.a. folgenden Detailinformationen erfasst

Datum und Uhrzeit	Quelle	Meldung
16.01.2004 10:44:16		Start des Aktivitätsprotokolls
16.01.2004 10:44:16	WAN	DSL Line -> INTERNET , Verbunden
16.01.2004 10:44:16	VPN	Nicht verbunden mit VPN_AMAY - Letzter Fehler: Leitungsüberwachung (Line polling) zum ...
16.01.2004 10:44:16	VPN	Verbunden mit VPN_CBUERSCH (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_CSCHALLE (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_DEICH (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_ETRABER (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_FJANSENEN (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_FTHEINEN (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_HBATTI (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_MBAGSIK (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_MBRDX (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_MPLUM (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_OSCHILPE (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_TNIO (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_WOHN (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_WTIW (über INTERNET)
16.01.2004 10:44:27	VPN	Abgehender Ruf zu VPN_CBUERSCH (über INTERNET) - Letzter Fehler: Leitungsüberwachu...

- ▷ Datum und Uhrzeit
- ▷ Quelle
- ▷ Meldung
- ▶ Firewall-Ereignisanzeige

Mit der Firewall-Ereignisanzeige werden die letzten 100 Aktionen der Firewall protokolliert. Dabei werden u.a. folgenden Detailinformationen erfasst

Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Protokoll	Quell-Port	Ziel-Port	Firewall-Regel	Limit	Aktion
1	1/16/2004 10:44:02	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
2	1/16/2004 10:41:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
3	1/16/2004 10:39:53	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
4	1/16/2004 10:38:49	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
5	1/16/2004 10:37:38	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
6	1/16/2004 10:33:52	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
7	1/16/2004 10:32:43	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
8	1/16/2004 10:28:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
9	1/16/2004 10:27:23	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
10	1/16/2004 10:25:11	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
11	1/16/2004 10:23:48	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
12	1/16/2004 10:16:25	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
13	1/16/2004 10:14:58	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
14	1/16/2004 10:11:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet
15	1/16/2004 10:10:02	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Sofort	Paket verworfen; SYSLOG gesendet

- ▷ Zeitpunkt
- ▷ Quell- und Zieladresse
- ▷ Protokoll mit Quell- und Ziel-Port
- ▷ auslösende Firewall-Regel und überschrittenes Limit
- ▷ ausgeführte Aktion

4.5 LANmonitor – wissen, was läuft

Mit dem Überwachungstool LANmonitor können Sie sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status Ihrer Router auf dem Bildschirm anzeigen lassen. Und zwar den Status aller LANCOM im Netz.

▷ LANmonitor – wissen, was läuft

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.



Erläuterungen zu den einzelnen Meldungen im LANmonitor und Hinweise zur Abhilfe finden Sie im Anhang unter 'Fehlermeldungen im LANmonitor' →Seite 307.

Sie können mit LANmonitor auch den Datenverkehr auf den verschiedenen Schnittstellen der Router beobachten und erhalten so wichtige Hinweise darüber, mit welchen Einstellungen Sie den Datenverkehr optimieren können.

Neben den Statistiken des Geräts, die Sie zum Beispiel auch in einer Telnet- oder Terminalsitzung oder mit WEBconfig auslesen können, stehen Ihnen im LANmonitor noch weitere nützliche Funktionen zur Verfügung, wie beispielsweise die Freischaltung eines zusätzlichen Gebührenlimits.



Sie können mit LANmonitor nur solche Geräte überwachen, die Sie über IP erreichen (lokal oder remote). Über die serielle Schnittstelle können Sie einen Router mit diesem Programm nicht ansprechen.

4.5.1 Erweiterte Anzeige-Optionen

Unter **Ansicht ▶ Anzeigen** können Sie folgende Anzeige-Optionen ein- und ausschalten:

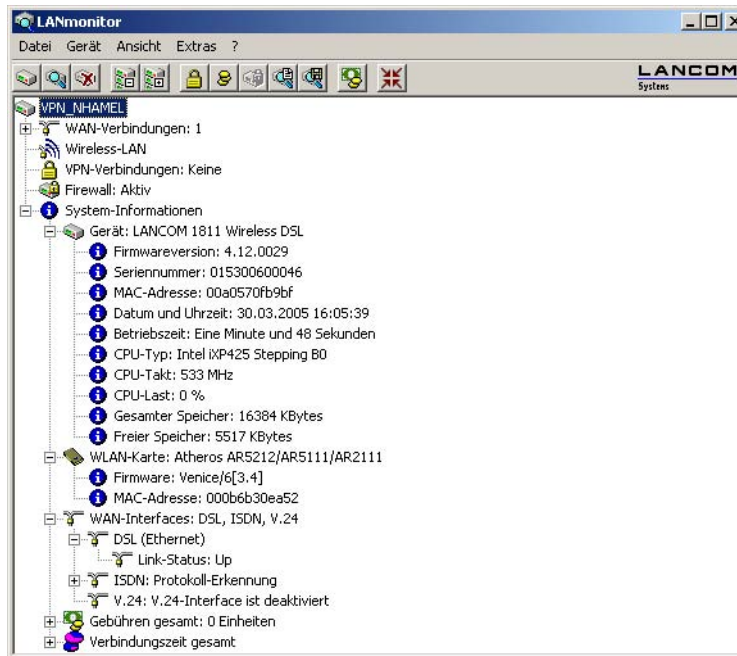
- ▶ Fehlermeldungen
- ▶ Diagnosemeldungen
- ▶ System-Informationen



Viele wichtige Details zum Status des LANCOM werden erst angezeigt, wenn die Anzeige der System-Informationen aktiviert ist. Dazu gehören beispielsweise die Schnittstellen und das Gebührenmanagement. Wir empfehlen daher interessierten Benutzern, die Anzeige der System-Informationen einzuschalten.

4.5.2 Abfrage der CPU- und Speicherauslastung über SNMP

Die CPU- und Speicherauslastung des LANCOM kann über SNMP abgefragt oder im LANmonitor angezeigt werden.



4.5.3 Internet-Verbindung kontrollieren

Als Beispiel für die Funktionen von LANmonitor zeigen wir Ihnen zuerst einmal, welche Informationen LANmonitor über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt.

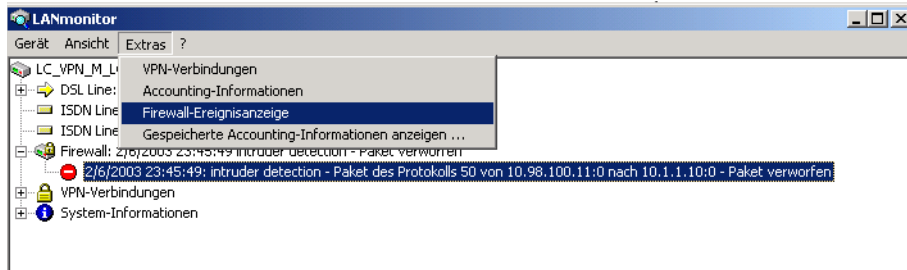
- ① Starten Sie LANmonitor mit **Start ► Programme ► LANCOM ► LANmonitor**. Legen Sie mit **Datei ► Gerät hinzufügen** ein neues Gerät an und geben im folgenden Fenster die IP-Adresse für den Router an, den Sie überwachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein.

Alternativ können Sie über LANconfig das Gerät auswählen und mit **Gerät ► Gerät überwachen** die Überwachung für ein Gerät starten.

- ② LANmonitor legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle. Starten Sie Ihren Web-Browser, und geben Sie eine beliebige Webseite ein. LANmonitor zeigt nun an, wie auf einem Kanal eine Verbindung aufgebaut wird und welche Gegenstelle dabei gerufen wird. Sobald die Verbindung hergestellt ist, zeigt der Kommunikationskanal durch das Pluszeichen vor dem Eintrag an, dass zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen oder Doppelklick auf

▷ LANmonitor – wissen, was läuft

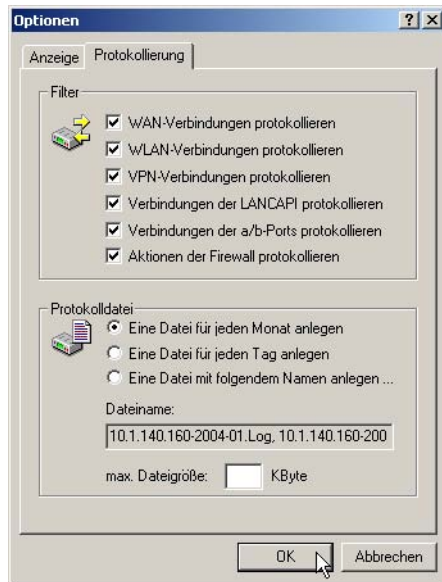
einen entsprechenden Eintrag öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen able- sen können.



In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.

Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.

- ③ Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspassword.
- ④ Wenn Sie ein Protokoll der LANmonitor-Ausgaben in Form einer Datei wünschen, starten Sie das Aktivitätsprotokoll mit **Gerät ▶ Aktivitätsprotokoll**. Öffnen Sie mit **Extras ▶ Optionen** den Dialog für die Einstellungen des Aktivitätsprotokolls.



Auf der Registerkarte 'Protokollierung'. können Sie die folgenden Aktivitäten für die Protokollierung auswählen:

- ▷ WAN-Verbindungen
- ▷ WLAN-Verbindungen
- ▷ VPN-Verbindungen
- ▷ LANCAPAPI-Verbindungen
- ▷ a/b-Port-Verbindungen
- ▷ Firewall-Aktionen

Zusätzlich stellen Sie hier ein, ob LANmonitor täglich, monatlich oder fortlaufend eine Protokolldatei erstellt und wo diese gespeichert wird.

4.6 Visualisierung großer WLANs mit dem WLANmonitor

Mit dem LANCOM WLANmonitor können Sie zentral den Status eines drahtlosen Netzwerkes (WLAN) überwachen. Es stehen sowohl Informationen über das gesamte Netzwerk als auch Detailinformationen zu einzelnen Access-Points und zu eingeloggtten Clients zur Verfügung. Zudem bietet der LANCOM WLANmonitor die Möglichkeit, Access Points zu Gruppen zusammenzufassen. Solche Gruppen können z.B. Etagen, Abteilungen oder Standorte umfassen. Dies erleichtert gerade bei großen WLAN-Infrastrukturen den Überblick über das gesamte Netzwerk.

▷ Visualisierung großer WLANs mit dem WLANmonitor

4.6.1 Start des LANCOM WLANmonitors

Der WLANmonitor ist Bestandteil des LANmonitor. Starten Sie den WLANmonitor aus dem LANmonitor über den Menüpunkt **Extras ▶ WLANmonitor**, über den entsprechenden Button in der LANmonitor-Buttonleiste oder direkt über **Start ▶ Programme ▶ LANCOM ▶ WLANmonitor**.



Alternativ kann der WLANmonitor von der Konsole aus mit dem Befehl

```
[Installationspfad]lanmon -wlan
```

gestartet werden.

4.6.2 Suche nach Access Points

Starten Sie nach dem Start des WLANmonitors die Suche nach verfügbaren Access Points über den Menüpunkt **Datei ▶ Access-Points suchen**. In der mittleren Spalte (Access-Point-Liste) werden dann die gefundenen Access Points aufgelistet. Zusätzlich erscheinen hier die wichtigsten Basisinformationen über den Access Point:

- ▶ Name des Access Points
- ▶ Anzahl der auf ihm angemeldeten Clients
- ▶ das verwendete Frequenzband
- ▶ der verwendete Kanal
- ▶ IP-Adresse des Access Point

In der rechten Spalte (Client-Liste) werden die auf dem ausgewählten Access Point eingeloggten Clients aufgelistet. Zu jedem Client werden folgende Informationen angezeigt:

- ▶ Verbindungsqualität in Form eines Balkendiagramms
- ▶ Identifikation: Name des eingeloggten Clients, sofern dieser in der Access-Liste oder in einem RADIUS-Server eingetragen ist.

LANconfig: **WLAN-Sicherheit ▶ Stationen ▶ Stationen**.

Telnet: /Setup/WLAN/Zugangsliste

WEBconfig: **Expertenkonfiguration ▶ Setup ▶ WLAN ▶ Zugangsliste**

- ▶ Signal: Signalstärke der Verbindung
- ▶ Access Point: Name des Access Points, auf dem der Client eingeloggt ist
- ▶ SSID: Identifikationsnummer des WLAN-Netzwerkes
- ▶ Verschlüsselung: Typ des Verschlüsselungsverfahrens der Funkverbindung
- ▶ WPA-Version (WPA-1 oder WPA-2)

▷ Visualisierung großer WLANs mit dem WLANmonitor

- ▶ MAC-Adresse: Hardwareadresse des WLAN-Clients
- ▶ TX-Rate: Übertragungsrate beim Senden
- ▶ RX-Rate: Übertragungsrate beim Empfangen
- ▶ Letztes Ereignis, z.B. 'Authentifikation erfolgreich', 'RADIUS erfolgreich', 'Schlüsselaustausch erfolgreich'
- ▶ IP-Adresse des WLAN-Clients

Access Points					Clients										
Name	Clients	Band	Kanal	IP-Adresse	Identifikation	Signal	Access Point	SSID n	Verschlüsselung	WPA	MAC-Adresse	TX-Rate	RX-Rate	Letztes Ereignis	IP-Adresse
WLAN_AP2	0	2,4 GHz	10	192.168.2.102	Nfamel Mobil	63 %	WLAN_NFAMEL	1	AES-CCM	1	0010c6252a2f	9 MBit/s	54 MBit/s	Schlüsselaustausch erfolgreich	192.168.2.99

4.6.3 Access Points hinzufügen

Möchten Sie einen Access Point zur Liste hinzufügen, der nicht automatisch erkannt wurde, wählen Sie den Menüpunkt **Datei ► Access Point hinzufügen**. Im folgenden Fenster geben Sie die IP-Adresse bzw. den Namen des Access Points und den Administratortypen sowie das zugehörige Passwort an.

Neues Gerät

Adresse

Bitte geben Sie hier die IP-Adresse oder den Namen des Geräts ein, das Sie überwachen

IP-Adr./Name:

Authentifizierung

Geben Sie hier Ihre Konfigurations-Zugriffsdaten für das Gerät ein:

Administrator:

Passwort:

Hinweis: Der Administrator darf nur angegeben werden, wenn er im Gerät eingerichtet wurde.

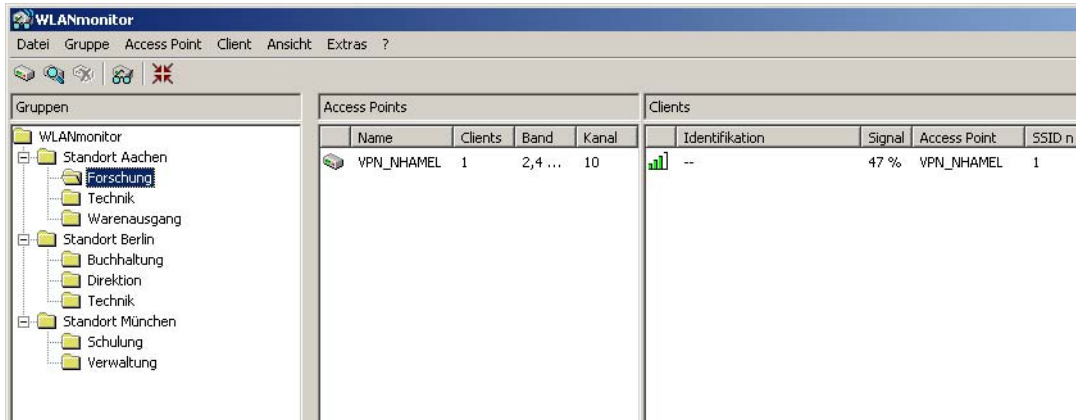
4.6.4 Access Points organisieren

Der LANCOM WLANmonitor bietet Ihnen die Möglichkeit, alle verfügbaren Access Points unabhängig von ihren physikalischen Standorten anzuordnen. Das erleichtert den Überblick im Netzwerk und hilft bei der Lokalisierung von evtl. auftretenden Problemen. Zudem lassen sich WLAN-Informationen gruppenweise abrufen. Sie können Ihre Access Points z.B. nach Abteilungen, Standorten oder Ihrem Verwendungszweck (z.B. öffentlicher Hotspot) gruppieren.

In der linken Spalte des WLANmonitors (Gruppen-Baum) werden die Gruppen angezeigt. Von der obersten Gruppe 'WLANmonitor' ausgehend können Sie über den Menüpunkt **Datei ► Gruppe hinzufügen** neue Untergruppen anlegen und so eine Struktur aufbauen. Die bei der Suche gefundenen Access-Points befinden sich jeweils in der

▷ Visualisierung großer WLANs mit dem WLANmonitor

aktuell ausgewählten Gruppe im Gruppen-Baum. Die bereits erkannten Access Points können Sie per Drag and Drop in die gewünschte Gruppe ziehen.



Um die Zuordnung von Access-Points und Clients zu erleichtern, können Sie ein Gerät mit der Maus markieren. Das jeweilige Pendant wird dann in der entsprechenden Liste ebenfalls markiert:

- ▶ Wenn in der Access-Point-Liste ein Access-Point markiert wird, werden alle auf diesem Gerät eingeloggten Client in der Client-Liste ebenfalls markiert.
- ▶ Wenn in der Client-Liste ein Client markiert wird, wird in der Access-Point-Liste der Access-Point markiert, auf dem der gewählte Client eingeloggt ist.

5 Diagnose

5.1 Trace-Ausgaben – Infos für Profis

Zur Kontrolle der internen Abläufe im Router während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Durch einen solchen Trace werden z.B. die einzelnen Schritte bei der Verhandlung des PPPs angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Router als auch bei der Gegenseite zu finden sein.



Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

5.1.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie in einer Telnet-Sitzung. Stellen Sie zunächst eine Telnet-Verbindung zu Ihrem Gerät her. Der Trace-Aufruf erfolgt dann mit dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt.

▷ Trace-Ausgaben – Infos für Profis

5.1.2 Übersicht der Schlüssel

Dieser Schlüssel ruft in Verbindung mit Trace die folgende Reaktion hervor:
?	zeigt einen Hilfetext an
+	schaltet eine Trace-Ausgabe ein
-	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen den verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

5.1.3 Übersicht der Parameter



Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Kommandozeile angezeigt werden.

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
Status	Status-Meldungen der Verbindungen
Fehler	Fehler-Meldungen der Verbindungen
IPX-Router	IPX-Routing
PPP	Verhandlung des PPP-Protokolls
Script	Erweiterte Protokoll-Verhandlung
SAP	IPX Service Advertising Protocol
IPX-Watchdog	IPX-Watchdog-Spoofing
SPX-Watchdog	SPX-Watchdog-Spoofing
LCR	Least-Cost-Router
Script	Script-Verhandlung
RIP	IPX Routing Information Protocol
IP-Router	IP-Routing
IP-RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS-Verwaltung

▷ Trace- Ausgaben – Infos für Profis

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
DNS	Domain Name Service Protocol
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
ATM	ATM-Paketebene
ADSL	ADSL-Verbindungsstatus
VPN-Status	IPSec und IKE Verhandlungen
VPN-Packet	IPSec und IKE Pakete
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll
Cron	Aktivitäten der Zeitautomatik (Cron-Tabelle)
WLAN	Informationen über die Aktivitäten in den Funknetzwerken
IAPP	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
DFS	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
Bridge	Informationen über die WLAN-Bridge
EAP	Trace zum EAP, dem bei WPA/802.11i und 802.1x verwendeten Protokoll zur Schlüsselaushandlung
NTP	Timeserver Trace
Firewall	Zeigt die Aktionen der Firewall
LANAUTH	LAN-Authentifizierung (z.B. Public Spot)
RADIUS	RADIUS-Trace
Connect	Meldungen aus dem Aktivitätsprotokoll ('Aktivitätsprotokoll' →Seite 72)

▷ Trace-Ausgaben – Infos für Profis

5.1.4 Kombinationsbefehle

Dieser Kombinations-Befehl ruft beim Trace die folgende Anzeige hervor:
All	alle Trace-Ausgaben
Display	Status- und Error-Ausgaben
Protocol	PPP- und Script-Ausgaben
TCP-IP	IP-Routing-, IP-RIP-, ICMP- und ARP-Ausgaben
IPX-SPX	IPX-Routing-, RIP-, SAP-, IPX-Wd.-, SPX-Wd.-, und NetBIOS-Ausgaben
Time	zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an
Source	zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlasst hat

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

5.1.5 Filter für Traces

Manche Traces wie der IP-Router-Trace oder die VPN-Traces erzeugen eine große Anzahl von Ausgaben. Damit wird die Ausgabe schnell unübersichtlich. Mit den Trace-Filtern haben Sie die Möglichkeit, nur die für Sie wichtigen Informationen aus den gesamten Traces herauszufiltern.

Zum Einschalten eines Trace-Filters wird das Trace-Kommando um den Parameter „@“ erweitert, der die folgende Filterbeschreibung einleitet. In der Filterbeschreibung gelten folgende Operatoren:

Operator	Beschreibung
(Leerzeichen)	ODER-Verknüpfung: Der Filter passt dann, wenn einer Operanden in der Trace-Ausgabe vorkommen
+	UND-Verknüpfung: Der Filter passt dann, wenn der Operand in der Trace-Ausgabe vorkommt
-	Nicht-Verknüpfung: Der Filter passt dann, wenn der Operand nicht in der Trace-Ausgabe vorkommt
"	die Ausgabe muss exakt dem Suchmuster entsprechen

Als Operanden können beliebige Zeichenketten eingetragen werden, z.B. die Namen von Gegenstellen, Protokollen oder Ports. Der Trace-Filter verarbeitet diese Angaben dann nach den Regeln der verwendeten Operatoren so wie z.B. die Suchmaschinen im Internet. Beispiel für die Verwendung der Filter finden Sie unter 'Beispiele für die Traces' →Seite 85.

5.1.6 Beispiele für die Traces

Dieser Schlüssel ruft in Verbindung mit Trace die folgende Reaktion hervor:
trace	zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF)
trace + all	schaltet alle Trace-Ausgaben ein
trace - all	schaltet alle Trace-Ausgaben aus
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein
trace + all - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein
trace ppp	zeigt den Zustand des PPPs an
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B -ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen, die nicht ICMP verwenden
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B +ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen und die ICMP verwenden
trace + ip-router @+TCP +"port: 80"	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die TCP/IP und den Port 80 verwenden. "port: 80" steht in Anführungszeichen, um auch das Leerzeichen als Teil der Zeichenkette einzubeziehen.

5.1.7 Traces aufzeichnen

Um einen Trace komfortabel mit einem Windows-System aufzuzeichnen (z.B. als Unterstützung für den Support), empfehlen wir Ihnen folgende Vorgehensweise:

Öffnen Sie bitte HyperTerminal unter **Start ▶ Programme ▶ Zubehör ▶ Kommunikation ▶ Hyper Terminal**. Als Name geben Sie einen beliebigen Namen ein.



▷ SYSLOG-Speicher im Gerät

Wählen Sie im Fenster 'Verbinden mit' im Pulldown-Menü 'Verbindung herstellen über' den Eintrag 'TCP/IP'. Geben Sie anschließend als 'Hostadresse' die lokale/öffentliche IP-Adresse oder den FQDN des Gerätes ein. Nach der Bestätigung erscheint im HyperTerminal eine Login Aufforderung. Geben Sie nun das Konfigurationspasswort ein.

Zum Aufzeichnen des Traces klicken Sie in der Menüleiste auf **Übertragen ► Text aufzeichnen**. Geben Sie den Pfad an, in dem die Textdatei gespeichert werden soll. Wechseln Sie nun wieder in das Dialogfenster und geben den Befehl entsprechenden Trace-Befehl ein.

Um den Trace wieder zu stoppen, klicken Sie im HyperTerminal in der oberen Menüleiste auf **Übertragen ► Text aufzeichnen beenden**.

5.2 SYSLOG-Speicher im Gerät

Über SYSLOG werden die Aktivitäten eines LANCOM-Geräts protokolliert. Als Erweiterung zur Ausgabe der SYSLOG-Informationen über einen entsprechenden SYSLOG-Client werden die letzten 100 SYSLOG-Meldungen im RAM der Geräte gespeichert. Damit können die SYSLOG-Meldungen direkt am Gerät zu Diagnose-Zwecken eingesehen werden.

5.2.1 SYSLOG-Modul aktivieren

Damit das SYSLOG-Modul die Aktivitäten protokolliert, muss es zunächst eingeschaltet werden. Zusätzlich muss ein passender SYSLOG-Client eingerichtet werden ('SYSLOG-Client konfigurieren' →Seite 87).

LANconfig

Bei der Konfiguration mit LANconfig finden Sie das SYSLOG-Modul im Konfigurationsbereich 'Meldungen' auf der Registerkarte 'SYSLOG'.



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie das SYSLOG-Modul auf folgenden Pfaden:

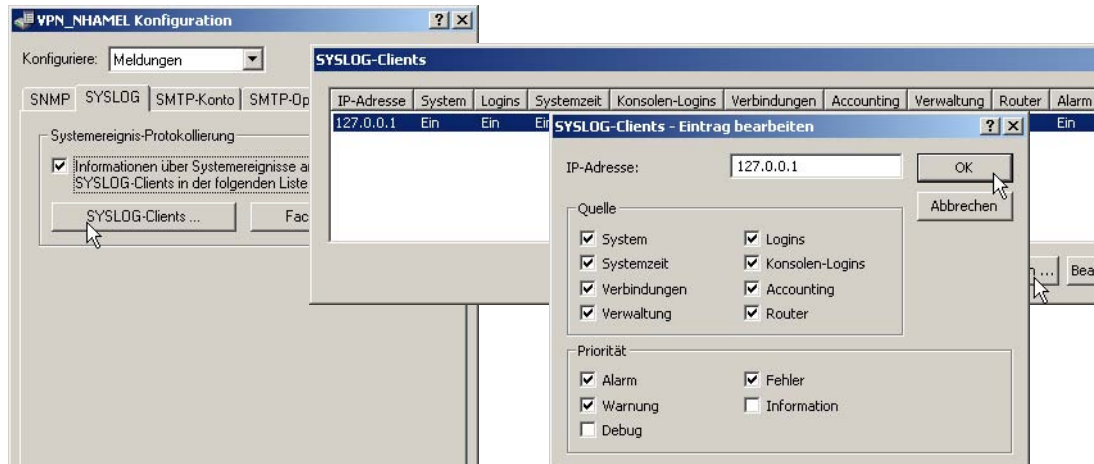
Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► SYSLOG-Modul
Terminal/Telnet	/Setup/SYSLOG-Modul

5.2.2 SYSLOG-Client konfigurieren

Das SYSLOG-Modul kann viele verschiedene Meldungen in den Gerätespeicher schreiben. Wenn Sie z.B. die Debug- und Informationsmeldungen nicht benötigen, können Sie den Umfang der Meldungen entsprechend reduzieren, indem Sie eine lokale Loopback-Adresse Ihres LANCOM-Geräts aus dem 127.x.x.x-Adresskreis (z.B. 127.0.0.1) als SYSLOG-Client eintragen und für diesen Client nur bestimmte Quellen und/oder Prioritäten aktivieren.

LANconfig

Bei der Konfiguration mit LANconfig öffnen Sie die Liste der SYSLOG-Clients im Konfigurationsbereich 'Meldungen' auf der Registerkarte 'SYSLOG' mit der Schaltfläche **SYSLOG-Clients**.



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie Liste der SYSLOG-Clients auf folgenden Pfaden:




Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► SYSLOG-Modul ► Tabelle-SYSLOG
Terminal/Telnet	/Setup/SYSLOG-Modul/Tabelle-SYSLOG

5.2.3 SYSLOG-Meldungen auslesen

Zum Auslesen der SYSLOG-Meldungen öffnen Sie die Statistiken unter WEBconfig oder Telnet. Sie finden die SYSLOG-Ausgabe unter **Status ► TCP-IP-Statistik ► Syslog-Statistiken**:

► Der Ping-Befehl

[Experten-Konfiguration](#)

-  [Status](#)
-  [TCP-IP-Statistik](#)
-  [Syslog-Statistiken](#)

Letzte-Meldungen

Idx.	Zeit	Quelle	Level	Meldung
197	30.11.2004 12:31:06	LOCAL3	Hinweis	HTTP 236133 packets (= 26.55%), 144530 kbytes (= 40.58%)
198	30.11.2004 12:31:06	LOCAL3	Hinweis	SMTP 10178 packets (= 1.14%), 8764 kbytes (= 2.46%)
199	30.11.2004 12:31:06	LOCAL3	Hinweis	DNS 4349 packets (= 0.49%), 326 kbytes (= 0.09%)
200	30.11.2004 12:31:06	LOCAL3	Hinweis	Telnet 3 packets (= 0.00%), 0 kbytes (= 0.00%)
201	30.11.2004 12:31:06	LOCAL3	Hinweis	TFTP 1228 packets (= 0.14%), 125 kbytes (= 0.04%)
202	30.11.2004 12:31:06	LOCAL3	Hinweis	DHCP 0 packets (= 0.00%), 0 kbytes (= 0.00%)

5.3 Der Ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Telnet- oder Terminal-Verbindung sendet ein „ICMP Echo-Request“-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem „ICMP Echo-Reply“. Ist der Zielrechner nicht erreichbar, antworten der letzte Router vor dem Host mit „Network unreachable“ (Netzwerk nicht erreichbar) oder „Host unreachable“ (Gegenstelle nicht erreichbar).

Die Syntax des Ping-Kommandos lautet wie folgt:

```
► ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] Ziel-Host
```

Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Parameter	Bedeutung
-a a.b.c.d	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Routers)
-a INT	Setzt die Intranet-Adresse des Routers als Absenderadresse
-a DMZ	Setzt die DMZ-Adresse des Routers als Absenderadresse
- a LBx	Setzt eine der 16 im Lancom Loopback-Adressen als Absenderadresse. Gültige Werte für x sind die Hexadezimalen Werte 0-f
-f	flood ping: Sendet große Anzahl von Ping-Signalen in kurzer Zeit. Kann z.B. zum Testen der Netzwerkbandbreite genutzt werden. ACHTUNG: flood ping kann leicht als DoS Angriff fehlinterpretiert werden.
-n	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück
-q	Ping-Kommando liefert keine Ausgaben auf der Konsole
-r	Wechselt in Traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt
-s n	Setze Größe der Pakete auf n Byte (max. 1472)

Parameter	Bedeutung
-i n	Zeit zwischen den einzelnen Paketen in Sekunden
-c n	Sende n Ping-Signale
Zielcomputer	Adresse oder Hostnamen des Zielcomputers
stop /<RETURN>	Die Eingabe von "stop" oder das Drücken der RETURN-Taste beenden das Ping-Kommando

```

192.168.2.100 - PuTTY
root@VPN_NHAMEL:/
> ping -a 192.168.2.50 -c 217.160.175.241
': Syntax error

root@VPN_NHAMEL:/
> ping -a 192.168.2.50 -c 2 217.160.175.241

56 Byte Packet from 217.160.175.241 seq.no=0 time=53.556 ms

---217.160.175.241 ping statistic---
56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@VPN_NHAMEL:/
> ping -n -c 1 217.160.175.241
p15125178.pureserver.info
56 Byte Packet from 217.160.175.241 seq.no=0 time=53.279 ms

---217.160.175.241 ping statistic---
56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@VPN_NHAMEL:/
> ping -R www.lancom.de

1 Traceroute 217.5.98.182      seq.no=0 time=47.961 ms
2 Traceroute 217.237.154.146  seq.no=1 time=44.962 ms
3 Traceroute 62.154.46.182   seq.no=2 time=55.810 ms
4 Traceroute 194.140.114.121 seq.no=3 time=56.797 ms
5 Traceroute 194.140.115.244 seq.no=4 time=71.948 ms
6 Traceroute 212.99.215.81   seq.no=5 time=78.293 ms
7 Traceroute 213.217.69.77   seq.no=6 time=82.287 ms
  Traceroute 213.217.69.69   seq.no=7 time=79.340 ms

---213.217.69.69 ping statistic---
56 Bytes Data, 8 packets transmitted, 8 packets received, 0% loss

root@VPN_NHAMEL:/
>

```

5.4 Monitor-Modus am Switch

Die über den Switch der LANCOM-Geräte übertragenen Daten werden zielgerichtet nur auf den Port aufgelegt, an dem der entsprechende Zielrechner angeschlossen ist. An den anderen Ports sind diese Verbindungen daher nicht sichtbar.

▷ Kabel-Tester

Um den Datenverkehr zwischen den einzelnen Ports mithören zu können, können die Ports in den Monitor-Modus geschaltet werden. In diesem Zustand werden auf diesem Ports alle Daten ausgegeben, die zwischen Stationen im LAN und WAN über den Switch des Gerätes ausgetauscht werden.

LANconfig

Bei der Konfiguration mit LANconfig öffnen Sie die Ethernet-Switch-Einstellungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'LAN' mit der Schaltfläche **Ethernet-Ports**.



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Ethernet-Switch-Einstellungen auf folgenden Pfaden:

Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► Ethernet-Ports
Terminal/Telnet	/Setup/Schnittstellen/Ethernet-Ports

5.5 Kabel-Tester

Werden auf Ihren LAN- oder WAN-Verbindungen gar keine Daten übertragen, obwohl die Konfiguration der Geräte keine erkennbaren Fehler aufweist, liegt möglicherweise ein Defekt in der Verkabelung vor.

Mit dem Kabel-Test können Sie aus dem LANCOM heraus die Verkabelung testen. Wechseln Sie dazu unter WEBconfig in den Menüpunkt **Expertenkonfiguration ► Status ► Ethernet-Ports ► Kabel-Test**. Geben Sie dort die Bezeichnung des Interfaces ein, das Sie testen wollen (z.B. "DSL1" oder "LAN-1"). Achten Sie dabei auf die genaue Schreibweise der Interfaces. Mit einem Klick auf die Schaltfläche **Ausführen** starten Sie den Test für das eingetragene Interface.

- [Experten-Konfiguration](#)
- [Status](#)
- [Ethernet-Ports](#)

Kabel-Test

Hier haben Sie die Möglichkeit, Parameter für das auszuführende Kommando einzugeben:

Parameter



Wechseln Sie anschließend in den Menüpunkt **Expertenkonfiguration ▶ Status ▶ Ethernet-Ports ▶ Kabel-Test-Ergebnisse**. In der Liste sehen Sie die Ergebnisse, die der Kabel-Test für die einzelnen Interfaces ergeben hat.

[Experten-Konfiguration](#)

[Status](#)

[Ethernet-Ports](#)

Kabel-Test-Ergebnisse

Port	Rx-Status	Rx-Distanz	Tx-Status	Tx-Distanz
DSL1	offen	0m	offen	0m
LAN-1	Impedanzfehler		OK	
LAN-2	OK		OK	
LAN-3	offen	0m	offen	0m
LAN-4	OK		OK	

Als Ergebnisse können folgende Werte erscheinen:

- ▶ **OK**: Kabel richtig eingesteckt, Leitung in Ordnung.
- ▶ **offen** mit Distanz **"0m"**: kein Kabel eingesteckt oder eine Unterbrechung in weniger als ca. 10 Metern.
- ▶ **offen** mit Angabe einer konkreten Distanz: Kabel ist eingesteckt, hat jedoch in der angegebenen Entfernung einen Defekt.
- ▶ **Impedanzfehler**: Das Kabelpaar am anderen Ende ist nicht mit der korrekten Impedanz abgeschlossen.

6 Sicherheit

Sie mögen es sicher nicht, wenn Außenstehende die Daten auf Ihren Rechnern einsehen oder verändern können. Darüber hinaus sollten Sie die Konfigurationseinstellungen Ihrer Geräte vor ungefügten Änderungen schützen. Dieses Kapitel widmet sich daher einem sehr wichtigen Thema: der Sicherheit. Die Beschreibung der Sicherheitseinstellungen ist in folgende Abschnitte unterteilt:

- ▶ Schutz für die Konfiguration
 - ▷ Passwortschutz
 - ▷ Login-Sperre
 - ▷ Zugangskontrolle
- ▶ Absichern des ISDN-Einwahlzugangs

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr LANCOM bestens abgesichert ist.



Zur Sicherheit der Daten tragen auch noch einige weitere Funktionen des LCOS bei, die in separaten Kapiteln beschrieben sind:

- ▷ 'Firewall' →Seite 168
- ▷ 'IP-Masquerading' →Seite 121
- ▷ 'Virtuelle LANs (VLANs)' →Seite 325

6.1 Schutz für die Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z.B. dazu.


Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein LANCOM die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

6.1.1 Passwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts.



Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Beispielsweise könnten Ihre Internetzugangsdaten eingesehen werden, oder der Router so umkonfiguriert werden, dass alle Schutzmechanismen außer Kraft gesetzt werden.

 Hinweis: Ein nicht gesetztes Passwort wird auf allen LANCOM durch eine blinkende Power-LED signalisiert, sofern die Geräte in Betrieb genommen worden sind (lokale Intranet-Adresse vorhanden).

Tipps für den richtigen Umgang mit Passwörtern

Für den Umgang mit Passwörtern möchten wir Ihnen an dieser Stelle einige Tipps ans Herz legen:

▶ **Halten Sie ein Passwort so geheim wie möglich.**


Notieren Sie niemals ein Passwort. Beliebte aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verraten Sie Ihr Passwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.

▶ **Passwörter nur sicher übertragen.**

Ein gewähltes Passwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschütztes E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Passwort auf beiden Seiten persönlich eingeben.

▶ **Wählen Sie ein sicheres Passwort.**

Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Passwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&"?#-*+_:;!,°' erschweren es Angreifern, Ihr Passwort zu erraten und erhöhen so die Sicherheit des Passworts.

 Groß- und Kleinschreibung werden beim Passwort für die Konfiguration unterschieden.

▶ **Verwenden Sie ein Passwort niemals doppelt.**

Wenn Sie dasselbe Passwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheitswirkung. Wenn eine Gegenseite unsicher wird, gefährden Sie mit einem Schlag auch alle anderen Verbindungen, für die Sie dieses Passwort verwenden.

▶ **Wechseln Sie das Passwort regelmäßig.**

Passwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Passwortes beträchtlich.

▶ **Wechseln Sie das Passwort sofort bei Verdacht.**

Wenn ein Mitarbeiter mit Zugriff auf ein Passwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Passwort zu wechseln. Ein Passwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie ein hohes Maß an Sicherheit.

▷ Schutz für die Konfiguration

Eingabe des Passwortes

Das Feld zur Eingabe des Passwortes finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. Unter WEBconfig rufen Sie den Assistenten **Sicherheitseinstellungen** auf. In einer Terminal- bzw. einer Telnet-Sitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`.

Konfigurationstool	Aufruf
LANconfig	Management ▶ Admin ▶ Passwort
WEBconfig	Sicherheitseinstellungen
Terminal/Telnet	<code>passwd</code>

Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet.

Konfigurationstool	Aufruf
LANconfig	Management ▶ Admin ▶ SNMP-Lesezugriff nur mit Passwort zulassen
WEBconfig	Experten-Konfiguration ▶ Setup ▶ SNMP ▶ Passw.Zwang-fuer-SNMP-Lesezugriff
Terminal/Telnet	<code>Setup/SNMP/Passw.Zwang</code>

6.1.2 Die Login-Sperre

Die Konfiguration im LANCOM ist durch eine Login-Sperre gegen „Brute-Force-Angriffe“ geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

Zur Konfiguration der Login-Sperre stehen in den Konfigurationstools folgende Einträge zur Verfügung:

- ▶ Sperre aktivieren nach (Anzahl Login-Fehler)
- ▶ Dauer der Sperre (Sperr-Minuten)

Konfigurationstool	Aufruf
LANconfig	Management ▶ Admin
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Config
Terminal/Telnet	<code>Setup/Config</code>

6.1.3 Einschränkung der Zugriffsrechte auf die Konfiguration

Der Zugriff auf die internen Funktionen kann wie folgt getrennt nach Interfaces getrennt konfiguriert werden:

- ▶ ISDN-Administrationszugang
- ▶ LAN
- ▶ Wireless LAN (WLAN)
- ▶ WAN (z.B. ISDN, DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z.B. dass nur die Konfiguration von bestimmten IP-Adressen oder LANCAPI-Clients vorgenommen werden darf. Ferner sind die folgenden internen Funktionen getrennt schaltbar:

- ▶ LANconfig (TFTP)
- ▶ WEBconfig (HTTP, HTTPS)
- ▶ SNMP
- ▶ Terminal/Telnet



Bei Geräten mit VPN-Unterstützung kann die Nutzung der einzelnen internen Funktionen über WAN-Interfaces auch nur auf VPN-Verbindungen beschränkt werden.

Den ISDN-Administrationszugang einschränken

Solange keine MSN für den Konfigurations-Zugriff eingetragen ist, nimmt ein **unkonfiguriertes** LANCOM die Rufe auf alle MSNs an. Sobald die erste Änderung in der Konfiguration gespeichert ist, nimmt das Gerät nur noch die Anrufe auf der Konfigurations-MSN an!

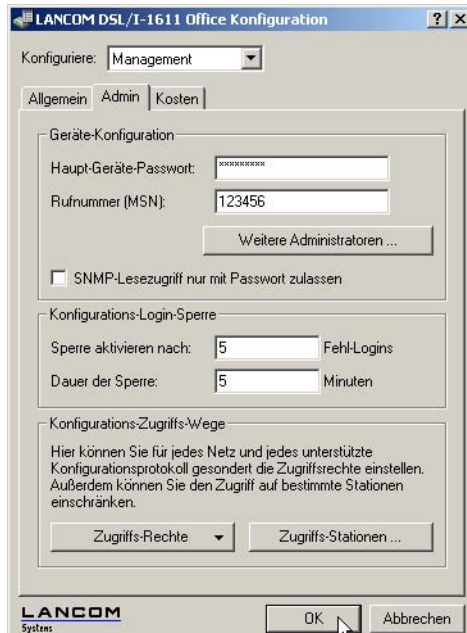


Wenn bei der ersten Konfiguration keine Konfigurations-MSN eingetragen wird, ist die Fernkonfiguration damit ausgeschaltet und das Gerät gegen den Zugriff über die ISDN-Leitung geschützt.

- ① Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin'.

Nur für
Modelle mit
ISDN-Schnitt-
stelle.

▷ Schutz für die Konfiguration



- ② Geben Sie als Rufnummer im Bereich 'Geräte-Konfiguration' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

Geben Sie alternativ unter Telnet den folgenden Befehl ein:

```
set /setup/config/Fernconfig 123456
```

- ! Der ISDN-Administrationszugang ist als einzige Konfigurationsmethode von den im folgenden beschriebene Netzwerk-Zugangsbeschränkungen ausgenommen. D.h. alle auf der ADMIN-MSN eingehenden Verbindungen werden nicht über die Zugriffssteuerung von entfernten Netzen eingeschränkt.

- i Wenn Sie die ISDN-Fernwartung ganz abschalten wollen, lassen Sie das Feld mit der ADMIN-MSN leer.

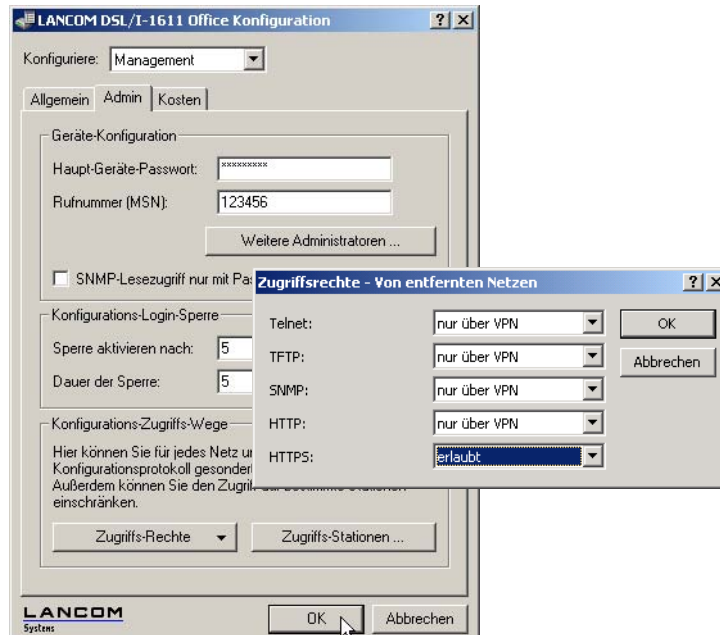
Den Netzwerk-Konfigurationszugriff einschränken


Der Zugriff auf die internen Funktionen kann - getrennt für Zugriffe aus dem lokalen Netz, aus entfernten Netzen oder aus Wireless LANs - für alle Konfigurationsdienste getrennt gesteuert werden.

Dabei kann der Konfigurationszugriff generell erlaubt oder verboten werden, als reiner Lesezugriff oder - falls Ihr Modell mit VPN ausgerüstet ist - auch nur über VPN erlaubt werden.

Konfiguration
mit LANconfig

Die Konfigurationsdialoge mit den Zugriffsrechten vom lokalen oder aus entfernten Netzen werden über die Schaltfläche **Zugriffsrechte** geöffnet:



 Wenn Sie den Netzwerkzugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von entfernten Netzen für alle Methoden auf 'nicht erlaubt'.

Konfiguration
mit WEBconfig
oder Telnet

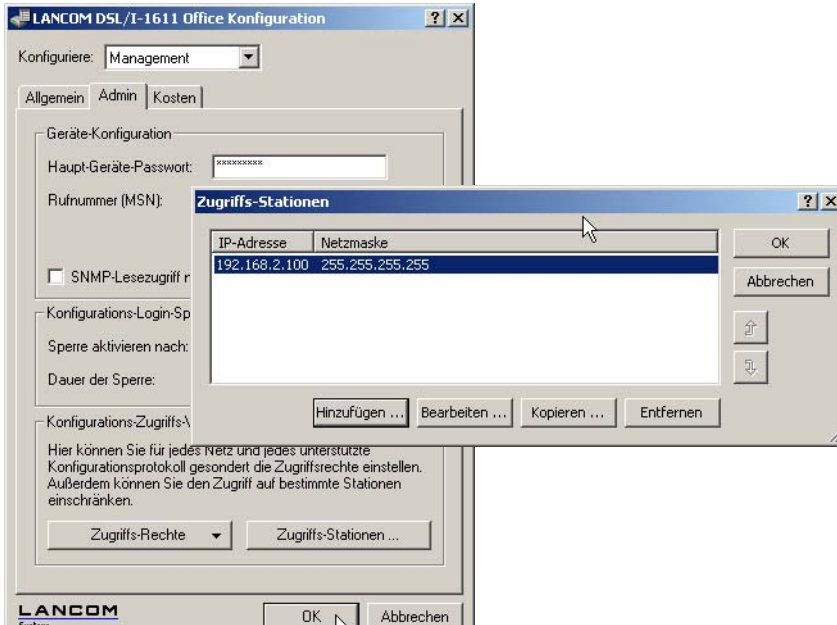
Unter WEBconfig oder Telnet erreichen Sie die Konfiguration der Zugangsliste über folgende Menü:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► Config ► Zugriffstabelle
Terminal/Telnet	/Setup/Config/Zugangsliste

Einschränkung des Netzwerk-Konfigurationszugriffs auf bestimmte IP-Adressen

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte auf bestimmte IP-Adressen eingeschränkt werden. Der Konfigurationsdialog mit den Zugriffsrechten vom lokalen oder aus entfernten Netzen werden über die Schaltfläche **Zugriffs-Stationen** geöffnet:

▷ Den ISDN- Einwahlzugang absichern



Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Unter WEBconfig oder Telnnet erreichen Sie die Konfiguration der Zugangsliste über folgende Menüs:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► TCP-IP ► Zugangs-Liste
Terminal/Telnnet	/Setup/TCP-IP/Zugangsliste

6.2 Den ISDN-Einwahlzugang absichern

Bei einem Gerät mit ISDN-Anschluss kann sich prinzipiell jeder Teilnehmer in Ihren LANCOM einwählen. Um unerwünschte Eindringlinge zu vermeiden, müssen Sie deshalb einen besonderen Augenmerk auf die Absicherung des ISDN-Zugangs legen.

Die Absicherungsfunktionen des ISDN-Zugangs können in zwei Gruppen eingeteilt werden:

- Identifikationskontrolle
 - ▷ Zugangsschutz mit Name und Passwort

▷ Den ISDN-Einwahlzugang absichern

- ▷ Zugangsschutz über die Anruferkennung
- ▶ Rückruf an festgelegte Rufnummern

6.2.1 Die Identifikationskontrolle

Zur Identifikationskontrolle kann entweder der Name der Gegenstelle oder die sogenannte Anruferkennung herangezogen werden. Die Anruferkennung ist die Telefonnummer des Anrufers, die bei ISDN normalerweise mit dem Anruf an die Gegenstelle übermittelt wird.

Welcher "Identifizier" zur Erkennung des Anrufers verwendet werden soll, wird im folgender Liste eingestellt:

Konfigurationstool	Aufruf
LANconfig	Kommunikation ▶ Ruf-Verwaltung
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WAN ▶ Schutz
Terminal/Telnet	/Setup/WAN/Schutz

Zur Auswahl stehen die folgenden Möglichkeiten:

- ▶ kein Schutz: Anrufe aller Gegenstellen werden angenommen.
- ▶ nach Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) in der Nummernliste eingetragen sind.
- ▶ nach geprüfter Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) einerseits in der Nummernliste eingetragen sind, sowie andererseits von der Vermittlungsstelle für korrekt befunden wurden.

Die Identifizierung setzt natürlich voraus, dass die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Benutzernamens und des Kennwortes

Bei einer PPP-Einwahl wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in den LANCOM ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

Baut der Router selber eine Verbindung auf, etwa zu einem Internet Service Provider, so verwendet er seinerseits Benutzername und Passwort aus der PPP-Liste. Ist dort kein Benutzername eingetragen, wird stattdessen der Gerätenamen verwendet.

Die PPP-Liste finden Sie wie folgt:

Konfigurationstool	Aufruf
LANconfig	Kommunikation ▶ Protokolle ▶ PPP-Liste
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WAN ▶ PPP
Terminal/Telnet	/Setup/WAN/PPP

▷ Den ISDN- Einwahlzugang absichern

Außerdem kann beim PPP-Protokoll auch der Anrufer von der Gegenstelle eine Authentifizierung verlangen. Er fordert dann die Gegenstelle zur Übermittlung eines Benutzer- bzw. Gerätenamens und eines Passwortes auf.



Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem LANCOM z.B. einen Internet Service Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Passwort zu beantworten ...

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – **C**alling **L**ine **I**dentifier).

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im LANCOM über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekanntem Rufnummern abgelehnt.

Der Schutz mit Hilfe der Rufnummer kann mit allen B-Kanal-Protokollen (Layern) verwendet werden.

6.2.2 Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Gegenstellenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

Konfigurationstool	Aufruf
LANconfig	Kommunikation ► Gegenstellen ► Gegenstellen (ISDN/seriell)
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Einwahl-Gegenstellen
Terminal/Telnet	/Setup/WAN/Einwahl-Gegenstellen

Mit den Einstellungen in Namen- und Nummernliste können Sie das Rückrufverhalten Ihres Routers steuern:

- Der Router kann den Rückruf ablehnen.
- Er kann eine voreingestellte Rufnummer zurückrufen.
- Er kann zunächst den Namen überprüfen und dann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Gegenstellenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühreneinheiten bis auf die, die für die Namensübermittlung benötigt wird. Ebenfalls fallen Einheiten für den Anrufer an, wenn der Anrufer nicht über CLIP (**C**alling **L**ine **I**dentifier **P**rotocol) identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg (Rückruf über den D-Kanal).

▷ Diebstahlschutz mit der ISDN- Standort-Verifikation

Eine besonders effektive Methode des Rückrufs ist das Fast-Call-Back-Verfahren (zum Patent angemeldet). Dieses Verfahren beschleunigt die Rückrufprozedur beträchtlich. Das Verfahren funktioniert nur dann, wenn es von beiden Gegenstellen unterstützt wird. Alle aktuellen LANCOM-Router beherrschen das Fast-Call-Back-Verfahren.



Weitere Informationen zum Rückruf finden Sie im Abschnitt 'Rückruf-Funktionen' →Seite 152.

6.3 Diebstahlschutz mit der ISDN- Standort-Verifikation

In größeren Installationen mit zum Teil unbeaufsichtigt aufgestellten Routern oder Access Points besteht die Gefahr, dass Geräte entwendet werden und an einer anderen Stelle wieder eingesetzt werden. Wenn in den Geräten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen konfiguriert sind, kann sich ein Dieb mit dem gestohlenen Gerät von einem anderen Ort aus Zugang zu geschützten Netzwerken verschaffen.

Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wird, kann das Gerät Nutzdaten über die WAN-Interfaces übertragen.

Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation:

- ▶ Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein.
- ▶ Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z.B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

6.3.1 Konfiguration der ISDN Standort-Verifikation

LANconfig

Die Parameter für die ISDN Standort-Verifikation finden Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Standort'.

Mit der Option 'ISDN-Standort-Überprüfung einschalten' aktivieren Sie die ISDN-Standort-Verifikation.

Für die weitere Konfiguration müssen folgende Angaben eingetragen werden:

- ▶ Die 'Ziel-Rufnummer' gibt an, welche Telefonnummer beim ISDN-Testanruf vom Router gewählt werden soll. Die Ziel-Rufnummer muss auf jeden Fall eingetragen werden, damit der Router einen Testanruf starten kann.
- ▶ Die 'Abgehende Nr. (MSN)' bestimmt, welche Telefonnummer der Gegenstelle als eingehender Anruf angezeigt werden soll.

Dieser Eintrag ist optional. Wenn die abgehende Rufnummer nicht definiert ist, verwendet das Gerät hier die als Ziel-Rufnummer eingetragene Rufnummer. Die Definition einer abgehenden Rufnummer ist meistens nur erforderlich, wenn der Router an einer Telefonanlage betrieben wird. In diesen Fällen kann durch die Definition einer abgehenden Rufnummer das Verhalten der Telefonanlage berücksichtigt werden.

▷ Diebstahlschutz mit der ISDN- Standort-Verifikation

- ▶ Die 'Anrufende Nummer' wird vom Router zur Verifizierung des ISDN-Selbstanrufs erwartet. Diese Nummer vergleicht das Gerät mit der Rufnummer des Anrufers. Erst wenn beide Nummern identisch sind, ist die ISDN-Standort-Verifikation erfolgreich.

Dieser Eintrag ist optional. Wenn die eingehende Rufnummer nicht definiert ist, erwartet das Gerät hier die als Ziel-Rufnummer eingetragene Rufnummer. Die Definition einer anrufenden Nummer ist notwendig, um die Rufnummernveränderungen durch die Telefonanlage oder die Vermittlungsstelle beim abgehenden Ruf berücksichtigen zu können. Hier wird also immer die Rufnummer eingetragen, die die Telefonanlage oder die Vermittlungsstelle anstelle der abgehenden Nummer einträgt.

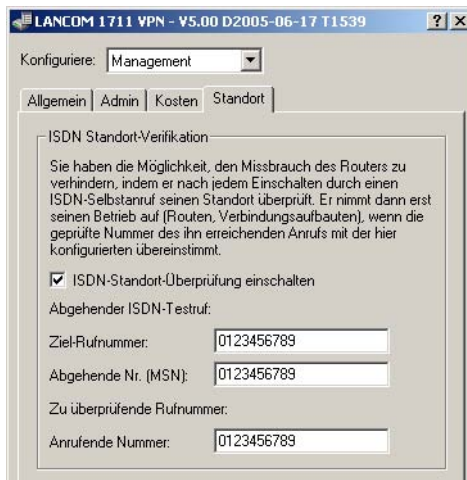
Wenn Sie nicht sicher sind, welche Rufnummern von Ihrer Telefonanlage übermittelt werden, können Sie die richtige Rufnummer auf folgende Weise ermitteln:

- ① Tragen Sie zunächst nur die Ziel-Rufnummer ein und aktivieren Sie die ISDN-Standort-Verifikation. Der Vergleich der eingehenden und der erwarteten Rufnummer wird voraussichtlich scheitern, das Gerät wird zunächst gesperrt.
- ② Prüfen Sie anschließend über den Status in WEBconfig oder Telnet, welche Rufnummer der Router als eingehenden Ruf erkannt hat.
- ③ Schalten Sie die ISDN-Standort-Verifikation aus und tragen Sie unter 'Zuletzt-gesehener-Ruf-von' gemeldete Rufnummer als neue 'Anrufende Nummer' ein.
- ④ Schalten Sie die ISDN-Standort-Verifikation wieder ein. Das Gerät wird erneut einen ISDN-Selbstanruf durchführen und nun mit dem Vergleich der eingehenden und der erwarteten Rufnummer erfolgreich sein, das Gerät wird wieder freigeschaltet.



Geben Sie immer vollständige Rufnummern an. Diese beinhaltet die Amtseinholung (falls vorhanden), die Landesvorwahl, die Ortsvorwahl und die Rufnummer der Gegenstelle. Viele Vermittlungsstellen im öffentlichen Telefonnetz ergänzen die Vorwahlen bei der Rufnummernübermittlung. Das Eintragen von Rufnummern ohne Vorwahlen führt in diesen Fällen zu einer Abweichung von erwarteten und übermittelten Rufnummern und damit zum Scheitern der ISDN-Standort-Verifikation. Die führenden Nullen werden beim Rufnummernvergleich nicht berücksichtigt, können jedoch eingetragen werden.

▷ Diebstahlschutz mit der ISDN- Standort-Verifikation



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig, Telnet bzw. Terminalprogramm finden Sie die Einstellungen für die ISDN Standort-Verifikation auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Expertenkonfiguration ► Setup ► Config ► Standortverifikation
Terminal/Telnet	Setup/Config/Standortverifikation

6.3.2 Statusabfrage der ISDN Standort-Verifikation

Der Status der ISDN-Standortverifikation kann über den LANmonitor eingesehen werden:



Mit WEBconfig (**Expertenkonfiguration ► Status ► Config ► Standortverifikation**) oder Telnet (**Status/Con-fig/Standortverifikation**) können Sie den Status der ISDN-Standort-Verifikation ebenfalls einsehen:

▷ Die Sicherheits- Checkliste

[Experten-Konfiguration](#) [Status](#) [Config](#)**Standortverifikation**

👁 Zustand	Erfolgreich
👁 Abgehender-Ruf-zu	241520319
👁 Erwarte-Ruf-von	241520319
👁 Zuletzt-gesehener-Ruf-von	241520319
👁 Ruf-wurde-angenommen	nein
👁 Ankommender-Ruf	ja
👁 Letzter-Fehler	Keine_Reaktion

Erst wenn die Standort-Verifikation im Zustand 'Erfolgreich' ist, kann der Router Daten über die WAN-Interfaces übertragen. Eine Standort-Verifikation ist dann erfolgreich, wenn die Nummer 'Erwarte-Ruf-von' mit der Nummer der 'Zuletzt-gesehener-Ruf-von' übereinstimmt. Der Anruf wird dabei nicht vom Router angenommen. Der Status zeigt außerdem an, ob der Router überhaupt einen Ruf erkannt hat.

6.4 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Sie die wichtigsten Sicherheitsfunktionen im Überblick. Damit Sie ganz sicher sein können, nichts Wesentliches bei der Sicherheitskonfiguration Ihres LANCOM übersehen zu haben.

▶ **Haben Sie ein Kennwort für die Konfiguration vergeben?**

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Saucieret'. Es ist insbesondere dann unerlässlich, ein Kennwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

▶ **Haben Sie die Fernkonfiguration zugelassen?**

Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - von entfernten Netzen' für alle Konfigurationsarten die Option 'nicht erlaubt'

▶ **Haben Sie die Konfiguration vom Funk-Netzwerk aus zugelassen?**

Wenn Sie die Konfiguration vom Funk-Netzwerk aus nicht benötigen, so schalten Sie sie ab. Das Feld zur Abschaltung der Konfiguration vom Funk-Netzwerk aus finden Sie ebenfalls in LANconfig im Konfigurationsbe-

reich 'Management' auf der Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - Vom Wireless LAN' für alle Konfigurationsarten die Option 'nicht erlaubt'.

▶ **Haben Sie die SNMP-Konfiguration mit einem Kennwort versehen?**

Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

▶ **Haben Sie den Remote Access erlaubt?**

Wenn Sie keinen Remote Access benötigen, schalten Sie die Rufannahme aus, indem Sie in LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Rufannahme' eine Rufannahme nach Nummer wählen und die Nummernliste leer lassen.

▶ **Haben Sie die Rückrufoptionen für den Remote Access aktiviert, und ist CLI eingeschaltet?**

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zu Stande kommt (CLI – Calling Line Identifier). Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen (dieser Rückruf über den D-Kanal wird vom Windows-DFÜ-Netzwerk nicht unterstützt). Ist ein Schutz im LANCOM über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekanntem Rufnummern abgelehnt.

▶ **Haben Sie die Firewall aktiviert?**

Die Stateful-Inspection Firewall der LANCOM Router sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann. Die Firewall können Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Allgemein' einschalten.

▶ **Verwenden Sie eine 'Deny-All' Firewall-Strategie?**

Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich unter 'Aufbau einer expliziten "Deny-All"-Strategie' →Seite 198.

▶ **Haben Sie IP-Masquerading aktiviert?**

IP-Masquerading heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router'.

▶ **Haben Sie kritische Ports über Filter geschlossen?**

Die Firewall-Filter des LANCOM Wireless bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne

▷ Die Sicherheits- Checkliste

Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter 'Firewall/QoS' finden Sie die Karteikarte 'Regeln', mit deren Hilfe Filterregeln definiert und verändert werden können.

▶ **Haben Sie bestimmte Stationen von dem Zugriff auf den Router ausgeschlossen?**

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

▶ **Lagern Sie Ihre abgespeicherte LANCOM-Konfiguration an einem sicheren Ort?**

Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

▶ **Haben Sie das Funknetzwerk durch eine Verschlüsselung und eine ACL abgesichert?**

Mit Hilfe von 802.11i, WPA oder WEP verschlüsseln Sie die Daten im Funknetzwerk mit verschiedenen Verschlüsselungsmethoden wie AES, TKIP oder WEP. LANCOM Systems empfiehlt die stärkste mögliche Verschlüsselung mit 802.11i und AES. Wenn der eingesetzte WLAN Client Adapter diese nicht unterstützt, nutzen Sie TKIP oder zumindest WEP. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter Verschlüsselungs-Funktion mindestens eine Passphrase oder ein WEP-Schlüssel eingetragen und zur Verwendung ausgewählt ist. Zur Kontrolle der WEP-Einstellungen wählen Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces' im Abschnitt 'Wireless-LAN' das jeweils zu konfigurierende Wireless-LAN Interface aus.

Mit der Access Control List (ACL) gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-Netzwerkarten. Zur Kontrolle der Access Control List wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Zugriff' auf der Registerkarte 'Stationen'.

▶ **Haben Sie für besonders sensiblen Datenaustausch auf dem Funknetzwerk die Funktionen 802.1x oder IPsec over WLAN eingerichtet?**

Wenn Sie auf Ihrem Funk-LAN besonders sensible Daten austauschen, können Sie zur weiteren Absicherung die IEEE-802.1x-Technologie verwenden. Um die IEEE-802.1x-Einstellungen zu kontrollieren oder zu aktivieren, wählen Sie in LANconfig den Konfigurationsbereich 'Benutzer-Anmeldung'.

Sofern Ihre Basis-Station VPN-fähig ist, können Sie alternativ zu IEEE-802.1x in der Betriebsart IPsec over WLAN die Daten zwischen Funknetzwerk und lokalem Netzwerk in einem 'VPN-Tunnel' schützen.

▶ **Haben Sie die Möglichkeiten zum Schutz der Konfiguration bei einem Diebstahl des Gerätes aktiviert?**

Die geheimen Zugangsdaten aus RAS-Zugängen, LAN-Kopplungen oder VPN-Verbindungen können bei einem Diebstahl des Gerätes in fremde Hände gelangen. Die Konfiguration des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass sie nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

- ▷ Durch die Funktion der ISDN-Standort-Verifikation kann das Gerät nur einem bestimmten ISDN-Anschluß betrieben werden. Nach dem Einschalten prüft das Gerät über einen Selbstanruf zu einer festgelegten Rufnummer, ob es sich noch am „richtigen“ ISDN-Anschluß befindet ('Diebstahlschutz mit der ISDN-Standort-Verifikation' →Seite 101).
- ▷ Mit den Funktionen des Scripting kann die gesamte Konfiguration des Gerätes nur im RAM gespeichert werden, der beim Booten des Gerätes gelöscht wird. Die Konfiguration wird dabei gezielt nicht in den bootresistenten Flash-Speicher geschrieben. Mit dem Trennen von der Stromversorgung und dem Aufstellen an einem anderen Ort wird damit die gesamte Konfiguration des Gerätes gelöscht ('Scripting' →Seite 55).

▷ *Allgemeines über WAN-Verbindungen*

7 Routing und WAN-Verbindungen

Dieses Kapitel beschreibt die wichtigsten Protokolle und Konfigurationseinträge, die bei WAN-Verbindungen eine Rolle spielen. Es zeigt auch Wege auf, WAN-Verbindungen zu optimieren.

7.1 Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- ▶ Internet-Zugang
- ▶ LAN-LAN-Kopplung
- ▶ Remote Access

7.1.1 Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen (beispielsweise über die LANCAPI) dadurch, dass die Daten im WAN über standardisierte Netzwerk-Protokolle übertragen werden, die auch im LAN Anwendung finden. Direkte Verbindungen arbeiten hingegen mit proprietären Verfahren, die speziell für Punkt-zu-Punkt-Verbindungen entwickelt worden sind.

Über WAN-Verbindungen wird ein LAN erweitert, bei direkten Verbindungen erhält nur ein einzelner PC eine Verbindung zu einem anderen PC. WAN-Verbindungen bilden gewissermaßen Brücken für die Kommunikation zwischen Netzwerken (bzw. für die Anbindung einzelner Rechner an ein LAN).

Welche Protokolle werden auf WAN-Verbindungen eingesetzt?

Auf WAN-Verbindungen über den Highspeed-Anschluss (z.B. DSL-Verbindungen) werden Pakete nach dem IP-Standard übertragen. Geräte mit ISDN-Schnittstelle unterstützen auf der ISDN-Schnittstelle neben IP auch IPX.

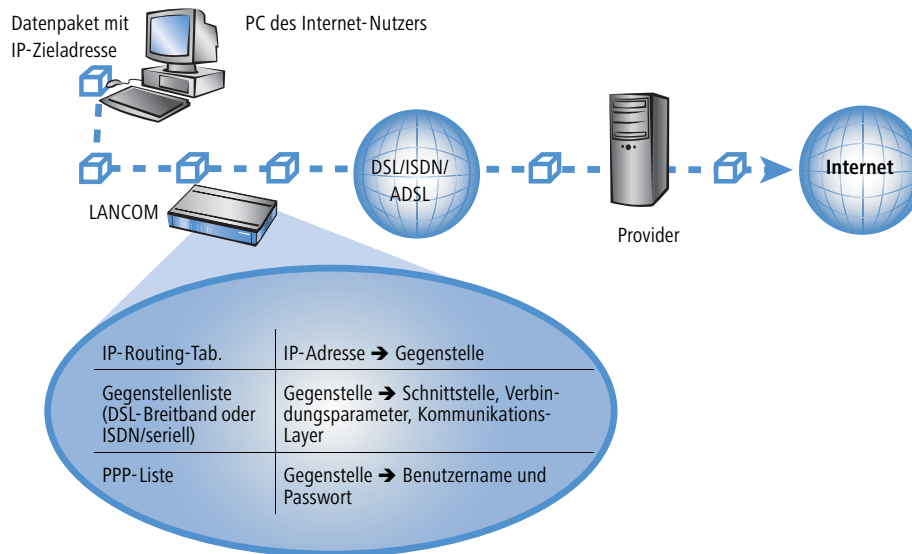
Die enge Zusammenarbeit mit den Router-Modulen

Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im LANCOM. Die Router-Module (IP und IPX) sorgen für die Verbindung von LAN und WAN. Sie bedienen sich der WAN-Module, um Anfragen von PCs aus dem LAN nach externen Ressourcen zu erfüllen.

7.1.2 Was passiert bei einer Anfrage aus dem LAN?

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendigen Verbindungen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen. Dabei gehen wir davon aus, dass die IP-Adresse des gesuchten Rechners im Internet bekannt ist.



① Auswahl der richtigen Route

Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router ermittelt in seiner IP-Routing-Tabelle die Gegenstelle, über die die Ziel-IP-Adresse erreichbar ist, z. B. 'Provider'.

② Verbindungsdaten für die Gegenstelle

Mit diesem Namen prüft der Router dann die Gegenstellenliste und findet die notwendigen Verbindungsdaten für den Provider. Zu diesen Verbindungsdaten gehören z. B. die WAN-Schnittstelle (DSL, ISDN) über die der Provider angewählt wird, Protokollinformationen oder die für eine ISDN-Wählverbindung notwendige Rufnummer. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung notwendig sind.

③ Aufbau der WAN-Verbindung

Der Router kann dann eine Verbindung über eine WAN-Schnittstelle zum Provider aufbauen. Er authentifiziert sich mit Benutzernamen und Passwort.

④ Weitergabe des Datenpaketes

Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket ins Internet weitergeben.

7.2 IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Abschnitt erfahren Sie, wie die

▷ IP-Routing

IP-Routing-Tabelle in einem Router von LANCOM Systems aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

7.2.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbstständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 256 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

Außerdem sagen Sie dem Router in der IP-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit IP-RIP bei mehreren Routen zum gleichen Ziel der günstigste ausgewählt werden kann. Die Grundeinstellung für die Distanz zu einem anderen Router ist 2, d.h., der Router ist direkt erreichbar. Alle lokal erreichbaren Geräte, also weitere Router im eigenen LAN oder Arbeitsplatzrechner, die über Proxy-ARP angeschlossen sind, werden mit der Distanz 0 eingetragen. Mit dem gezielten Eintrag einer höheren Distanz (bis 14) wird die „Qualität“ dieser Route herabgesetzt. Solche „schlechteren“ Routen sollen nur dann verwendet werden, wenn keine andere Route zu der entsprechenden Gegenstelle gefunden werden kann.

Konfiguration der Routing-Tabelle

Konfigurationstool	Aufruf
LANconfig	IP-Router ► Routing ► Routing-Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► IP-Routing-Tabelle
Terminal/Telnet	cd /Setup/IP-Router/IP-Routing-Tab.

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	Netzmaske	Routing-Tag	Router	Distanz	Maskierung	Aktiv
192.168.120.0	255.255.255.0	0	MAIN	2	Aus	Ja
192.168.125.0	255.255.255.0	0	NODE1	3	Aus	Ja
192.168.130.0	255.255.255.0	0	191.168.140.123	0	Aus	Ja

Was bedeuten die einzelnen Einträge in der Liste?

▶ IP-Adresse und Netzmaske

Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

Die Route mit der IP-Adresse '255.255.255.255' und der Netzmaske '0.0.0.0' ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

▶ Routing-Tag

Mit dem Routing-Tag kann die Auswahl der Zielroute genauer gesteuert werden. Dabei wird für die Auswahl der Route nicht nur die Ziel-IP-Adresse, sondern auch weitere Informationen ausgewertet, die den Datenpaketen über die Firewall zugefügt werden ('Policy-based Routing' →Seite 112). Mit dem Routing-Tag „0“ gilt der Routing-Eintrag für alle Pakete.

▶ Router

An diese Gegenstelle überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete.

- ▷ Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier der Name der Gegenstelle.
- ▷ Kann der eigene Router die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers im LAN, der den Weg ins Zielnetz kennt.

Der Name der Gegenstellen gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

- ▷ Routen mit dem Eintrag '0.0.0.0' bezeichnen Ausschluss-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (private Adressräume, z.B. '10.0.0.0') von der Übertragung ausgeschlossen.
- ▷ Wird als Gegenstelle eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

▶ Distanz

Anzahl der zwischen dem eigenen und dem Ziel liegenden Router. Dieser Wert wird bei Weitverkehrsverbindungen oft auch mit den Kosten der Übertragung gleichgesetzt und zur Unterscheidung zwischen preiswerten und teuren Übertragungswegen genutzt. Die eingetragenen Distanzwerte werden wie folgt propagiert:

- ▷ Während eine Verbindung zu einem Zielnetz existiert, werden alle über diese Verbindung erreichbaren Netze mit einer Distanz von 1 propagiert.
- ▷ Alle nicht verbundenen Netze werden mit der Distanz propagiert, die in der Routing-Tabelle eingetragen ist (mindestens jedoch mit einer Distanz von 2), solange noch ein freier Übertragungskanal verfügbar ist.
- ▷ Ist kein Kanal mehr frei, so werden die verbleibenden Netze mit einer Distanz 16 (= unreachable) propagiert.
- ▷ Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts“ werden gar nicht propagiert.

▷ IP-Routing

► Maskierung

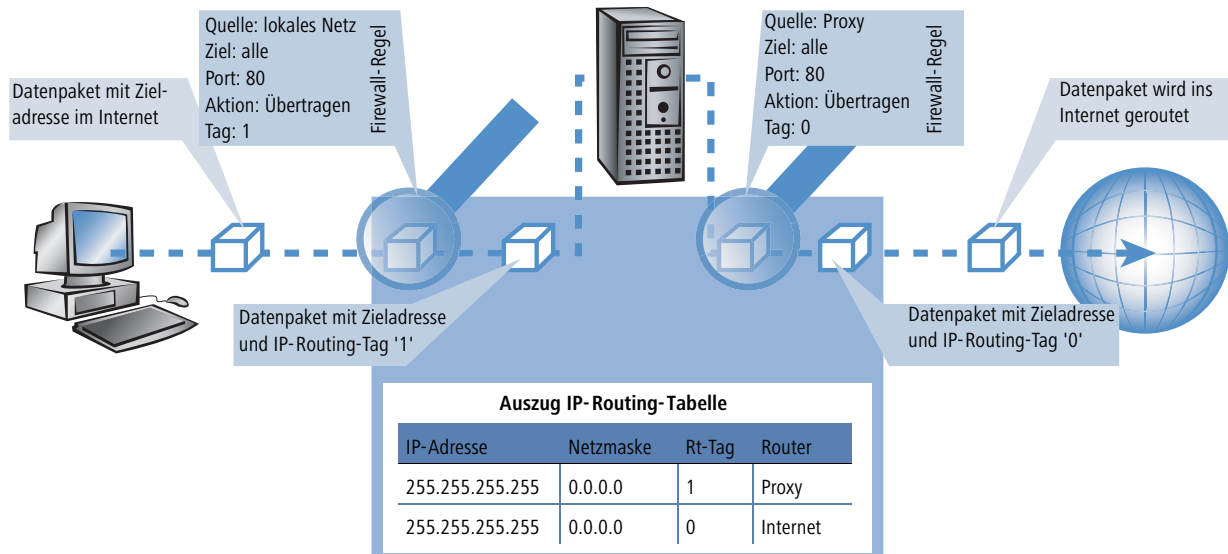
Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

Weitere Informationen finden Sie im Abschnitt 'IP-Masquerading' →Seite 121.

7.2.2 Policy-based Routing

Beim Policy-based Routing wird die Zielroute (also die Gegenstelle, über die die Daten übertragen werden), nicht ausschließlich anhand der Ziel-IP-Adressen ausgewählt. Weitere Informationen wie z.B. der verwendete Dienst oder das verwendete Protokoll sowie Adressen von Absender oder Ziel der Datenpakete können für die Auswahl der Zielroute genutzt werden. Mit Hilfe von Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich, z.B. in folgenden Anwendungsszenarien:

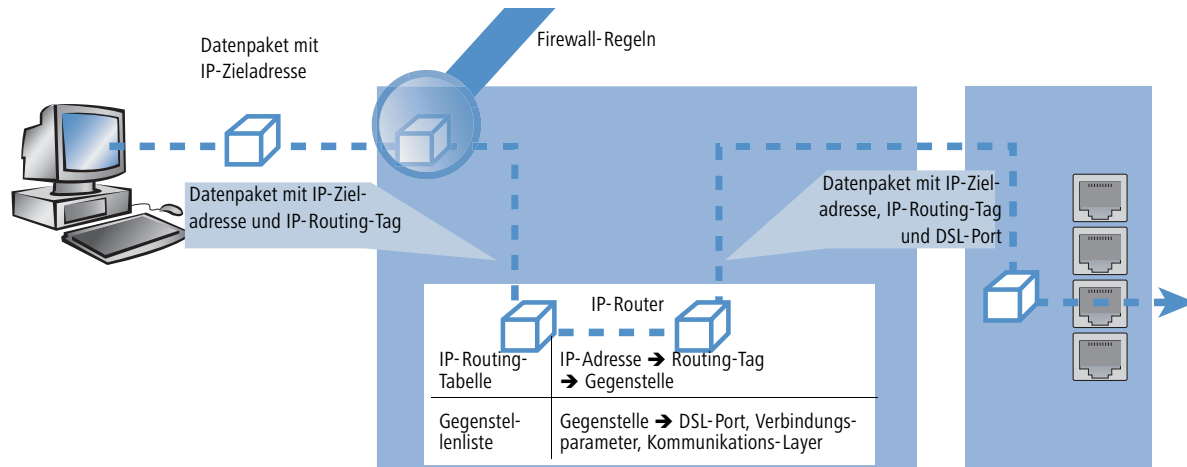
- Der gesamte Internetverkehr eines LANs wird über einen Proxy umgeleitet, ohne das Eintragen der Proxy-Adresse in den Browsern. Das Routing über den Proxy läuft unbemerkt für die Anwender ab, man spricht daher hier auch von einem „transparenten“ Proxy.



- Beim Load-Balancing wird der Datenverkehr für bestimmte Protokolle über einen bestimmten DSL-Port mit einem zusätzlichen externen ADSL-Modem geleitet.
- Ein Server im lokalen Netz, der über eine feste IP-Adresse aus dem WAN erreichbar sein sollte, wird über ein bestimmtes WAN-Interface geroutet.
- Der VPN-Verkehr wird mit dem Routing-Tag '0' durch einen VPN-Tunnel mit dynamischen Endpunkten geleitet, der restliche Internetverkehr der Firma wird mit einem entsprechenden Routing-Tag auf eine andere Firewall umgeleitet.

Um die Kanalauswahl aufgrund anderer Informationen als nur der Ziel-IP-Adresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag“ zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. So wird z.B. über eine Regel dem gesamten Datenverkehr einer lokalen Rechnergruppe (entsprechend dem IP-Adress-Bereich) das Routing-Tag '2' angehängt. Alternativ definieren gezielt einige Protokolle ein anderes Routing-Tag.

Die Zeichnung zeigt die Anwendung des Policy-based Routing beim Load-Balancing:



- Beim Aufbau der Verbindungen prüft zunächst die Firewall, ob die anstehenden Pakete zu einer Regel passen, in der ein Routing-Tag enthalten ist. Das Routing-Tag wird in das Datenpaket eingetragen.
- Mit dem gefundenen Routing-Tag und der Ziel-IP-Adresse kann in der IP-Routing-Tabelle die passende Gegenstelle gefunden werden. Dazu wird die IP-Routing-Tabelle wie üblich von oben nach unten durchgearbeitet.
- Wird ein übereinstimmender Eintrag für das Netzwerk gefunden, wird im zweiten Schritt das Routing-Tag geprüft. Mit dem passenden Routing-Tag kann so die gewünschte Gegenstelle gefunden werden. Über die Gegenstelle kann das LANCOM beim Load-Balancing aus der Gegenstellenliste den richtigen DSL-Port ermitteln.

i Wenn das Routing-Tag den Wert „0“ hat (Default), dann gilt der Routing-Eintrag für alle Pakete.

- Interne Dienste verwenden implizit immer das Default-Tag. Wenn der Anwender z.B. die Default-Route durch einen VPN-Tunnel leiten will, der einen dynamischen Tunnelendpunkt hat, so nutzt das VPN-Modul standardmäßig die Default-Route mit dem Routing-Tag „0“.

Um die Default-Route dennoch durch den VPN-Tunnel zu führen, legen Sie eine zweite Default-Route mit dem Routing-Tag „1“ und der VPN-Gegenstelle als Router-Namen an. Mit einer passenden Firewall-Regel übertragen Sie alle Dienste von allen Quell-Stationen zu allen Ziel-Stationen mit dem Routing-Tag „1“.

- Routing-Tags und RIP: Das Routing-Tag wird auch in RIP-Paketen versendet und beim Empfang ausgewertet, damit z.B. die geänderten Distanzen in den richtigen Routen geändert werden können.

▷ IP-Routing

7.2.3 Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Standard-Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannt IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Zielnetz kennt (diese Antwort nennt man ICMP-Redirect). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keine ICMP-Redirects mehr geschickt. Die Einstellung erfolgt unter:

Konfigurationstool	Aufruf
LANconfig	IP-Router ▶ Allgemein ▶ Pakete im lokalen Netz weiterleiten
WEBconfig	Experten-Konfiguration ▶ Setup ▶ IP-Router ▶ Lok.-Routing
Terminal/Telnet	<code>set /Setup/IP-Router/Lok.-Routing Ein</code>

Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

7.2.4 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von LANCOM Systems auch über eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die er in seiner eigenen statischen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- ▶ Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- ▶ Routen, die auf andere Router im lokalen Netz lauten.

- ▶ Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

Die Einträge in der statischen Routing-Tabelle werden zwar von Hand gesetzt, trotzdem ändern sich diese Informationen je nach Verbindungssituation der Router und damit auch die versendeten RIP-Pakete.

- ▶ Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt er alle über diese Route erreichbaren Netze in den RIPs mit der Distanz '1' weiter. Damit werden andere Router im LAN darüber informiert, dass hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.
- ▶ Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar“. Dass ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
 - ▷ Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt (auch über LANCAP1).
 - ▷ Die Y-Verbindungen für den S₀-Anschluss sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
 - ▷ Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).
 - ▷ Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Nur wenige ISDN-Anbieter ermöglichen es, neben einer Festverbindung auf dem ersten B-Kanal eine Wählverbindung auf dem zweiten B-Kanal aufzubauen.

Welche Informationen entnimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	IP-Netzmaske	Zeit	Distanz	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekannt gemacht hat. Bleibt die 'Zeit'. Damit zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

▷ IP-Routing

Wenn der Router nun ein IP-RIP-Paket empfängt, muss er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- ▶ Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- ▶ Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- ▶ Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- ▶ Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekannt gegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekannt macht (z.B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.



RIP-Pakete aus dem WAN werden nicht beachtet und sofort verworfen! RIP-Pakete aus dem LAN werden ausgewertet und nicht im LAN weitergeleitet!

Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

Skalierung durch IP-RIP

Verwenden Sie mehrere Router in einem lokalen Netz mit IP-RIP, können Sie die Router im lokalen Netz nach außen hin als einen einzigen großen Router darstellen. Dieses Vorgehen nennt man auch „Skalierung“. Durch den regen Informationsaustausch der Router untereinander steht so ein Router mit prinzipiell beliebig vielen Übertragungswegen zur Verfügung.

Konfiguration der IP-RIP-Funktion

Konfigurationstool	Menü/Tabelle
LANconfig	IP-Router ► Allgemein ► RIP-Optionen
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► RIP-Einstellung
Terminal/Telnet	cd /Setup/IP-Router/RIP-Einstellung

- ▶ Im Feld 'RIP-Unterstützung' (bzw. 'RIP-Typ') gibt es folgende Auswahl:
 - ▷ 'Aus': IP-RIP wird nicht verwendet (Standard).

- ▷ 'RIP-1': RIP-1- und RIP-2-Pakete werden empfangen, aber nur RIP-1-Pakete gesendet.
- ▷ 'RIP-1 kompatibel': es werden ebenfalls RIP-1- und RIP-2-Pakete empfangen. Gesendet werden RIP-2-Pakete als IP-Broadcast.
- ▷ 'RIP-2': Wie 'RIP-1 kompatibel', nur werden alle RIP-Pakete an die IP-Multicast-Adresse 224.0.0.9 gesendet.
- ▶ Der Eintrag unter 'RIP-1-Maske' (bzw. 'R1-Maske') kann auf folgende Werte gesetzt werden:
 - ▷ 'Klasse' (Standard): Die im RIP-Paket verwendete Netzwerkmaske ergibt sich direkt aus der IP-Adress-Klasse, d. h., für die Netzwerkklassen werden folgende Netzwerkmasken verwendet:

Klasse A	255.0.0.0
Klasse B	255.255.0.0
Klasse C	255.255.255.0

- ▷ 'Adresse': Die Netzwerkmaske ergibt sich aus dem 1. gesetzten Bit der eingetragenen IP-Adresse. Dieses und alle höherwertigen Bits innerhalb der Netzwerkmaske werden gesetzt. Aus der IP-Adresse 127.128.128.64 ergibt sich so z.B. die IP-Netzmaske 255.255.255.192.
- ▷ 'Klasse + Adresse': Die Netzwerkmaske wird aus der IP-Adressen-Klasse und einem angefügten Teil nach dem Adressverfahren gebildet. Aus obiger Adresse und der Netzmaske 255.255.0.0 ergibt sich somit die IP-Netzmaske 255.128.0.0.



RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Der Router ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn er eine eindeutige IP-Adresse hat. In der Grundeinstellung mit der IP-Adresse xxx.xxx.xxx.254 ist das IP-RIP-Modul ausgeschaltet.

7.2.5 SYN/ACK-Speedup

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (SYN für Synchronisation und ACK für Acknowledge) innerhalb des Sendebuffers gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sendeschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Anschlüssen (z.B. ADSL) ein, wenn gleichzeitig in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

Ausschalten in Problemfällen

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das

▷ Die Konfiguration von Gegenstellen


betrifft nur Anwendungen, die abweichend vom Protokollstandard eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall kann der SYN/ACK-Speedup ausgeschaltet werden:

Konfigurationstool	Menü/Tabelle
LANconfig	IP-Router ► Allgemein ► TCP SYN- und ACK-Pakete bevorzugt weiterleiten
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► Routing-Methode ► SYN/ACK-Speedup
Terminal/Telnet	<code>cd /Setup/IP-Router/Routing-Methode</code> <code>set SYN/ACK-Speedup AUS</code>

7.3 Die Konfiguration von Gegenstellen

Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Gegenstellenliste (bzw. den Gegenstellenlisten) werden alle Informationen eingestellt, die individuell für nur eine Gegenstelle gelten.
- Parameter für die unteren Protokollebenen (unterhalb von IP bzw. IPX) werden in der Kommunikations-Layer-Tabelle definiert.

 In diesem Abschnitt wird die Konfiguration der Authentifizierung (Protokoll, Benutzername, Passwort) nicht behandelt. Informationen zur Authentifizierung finden Sie im Abschnitt 'Verbindungsaufbau mit PPP' →Seite 146.

7.3.1 Gegenstellenliste

Die verfügbaren Gegenstellen werden in der Gegenstellenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt. Für jedes WAN-Interface gibt es eine separate Gegenstellenliste. Die Gegenstellenlisten können auf folgenden Wegen aufgerufen werden:

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation ► Gegenstellen ► Gegenstellen (DSL)
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► DSL-Breitband-Gegenstellen bzw. Einwahl-Gegenstellen
Terminal/Telnet	<code>cd /Setup/WAN</code> <code>set DSL-Breitband-Gegenstellen [...]</code> <code>set Einwahl-Gegenstellen [...]</code>

▷ Die Konfiguration von Gegenstellen

Für eine Gegenstelle sind folgende Parameter erforderlich:

Gegenstellen-liste	Parameter	Bedeutung
DSL-Breitband-Gegenstellen	Name	Mit diesem Namen wird die Gegenstelle in den Routermodulen identifiziert. Sobald das Routermodul anhand der IP-Adresse ermittelt hat, bei welcher Gegenstelle das gewünschte Ziel erreicht werden kann, können aus der Gegenstellenliste die zugehörigen Verbindungsparameter ermittelt werden.
	Haltezeit	Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch beendet. Bei einer Haltezeit von 9999 Sekunden werden abgebrochen Verbindungen selbstständig wiederhergestellt (siehe 'Dauerverbindung für Flatrates – Keep-alive' →Seite 151).
	Access Concentrator	Der Access Concentrator (AC) steht für den Server, der über diese Gegenstelle erreicht werden kann. Stehen mehrere Provider zur Auswahl, die über Ihren ADSL-Anschluss genutzt werden können, wählen Sie mit dem Namen des AC den Provider aus, der für den IP-Adresskreis dieser Gegenstelle zuständig ist. Der Wert für den AC wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den AC eingetragen, wird jeder AC angenommen, der den geforderten Service anbietet.
	Service	Tragen Sie hier den Dienst ein, den Sie bei Ihrem Provider nutzen möchten. Das kann z. B. einfaches Internet-Surfen sein oder aber auch Video-Downstream. Der Wert für den Service wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den Service eingetragen, wird jeder Service angenommen, den der geforderte AC anbietet.
	Layername	Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.
	VPI	Virtual Path Identifier.
	VCI	Virtual Channel Identifier. Die Werte für VCI und VPI werden vom ADSL-Netzbetreiber mitgeteilt. Übliche Werte für die Kombination von VPI und VCI sind: 0/35, 0/38, 1/32, 8/35, 8/48.
Einwahl-Gegenstellen	Name	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Rufnummer	Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der RoundRobin-Liste eingetragen werden.
	Haltezeit	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Haltezeit für Bündelung	Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.
	Layername	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Automatischer Rückruf	Der automatische Rückruf ermöglicht eine sichere Verbindung und senkt die Kosten für den Anrufer. Nähere Informationen finden Sie im Abschnitt 'Rückruf-Funktionen' →Seite 152.



Bitte beachten Sie bei der Bearbeitung der Gegenstellenlisten folgende Hinweise:

▷ Die Konfiguration von Gegenstellen

- ▷ Werden in zwei Gegenstellenlisten (z.B. DSL-Breitband-Gegenstellen und Einwahl-Gegenstellen) Einträge mit identischen Namen für die Gegenstelle vorgenommen, verwendet das LANCOM beim Verbindungsaufbau zu der entsprechenden Gegenstelle automatisch das "schnellere" Interface. Das andere Interface wird in diesem Fall als Backup verwendet.
- ▷ Werden in der Liste der DSL-Breitband-Gegenstellen weder Access Concentrator noch Service angegeben, stellt der Router eine Verbindung zum ersten AC her, der sich auf die Anfrage über die Vermittlungsstelle meldet.
- ▷ Für ein ggf. vorhandenes DSLoL-Interface gelten die gleichen Einträge wie für ein DSL-Interface. Die Einträge dazu werden in der Liste der DSL-Breitband-Gegenstellen vorgenommen.

7.3.2 Layer-Liste

Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll. Die Liste der Kommunikations-Layer finden Sie unter:

Konfigurationstool	Liste
LANconfig	Kommunikation ► Allgemein ► Kommunikations-Layer
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Layer-Liste
Terminal/Telnet	cd /Setup/WAN set Layer-Liste [...]

In der Kommunikations-Layer-Liste sind die gängigen Protokollkombinationen bereits vordefiniert. Änderungen oder Ergänzungen sollten Sie nur vornehmen, wenn Gegenstellen inkompatibel zu den vorhandenen Layern sind. Die möglichen Optionen finden Sie in der folgenden Übersicht.



Beachten Sie, dass die im LANCOM vorhandenen Parameter vom Funktionsumfang des Gerätes abhängen. Es kann daher sein, dass Ihr Gerät nicht alle hier beschriebenen Optionen anbietet.

Parameter	Bedeutung	
Layername	Unter diesem Namen wird der Layer in den Gegenstellenlisten ausgewählt.	
Encapsulation	Für die Datenpakete können zusätzliche Kapselungen eingestellt werden.	
	'Transparent'	Keine zusätzliche Kapselung.
	'Ethernet'	Kapselung als Ethernet-Frames.
	'LLC-MUX'	Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.
'VC-MUX'	Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.	

Parameter	Bedeutung	
Layer-3	Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'PPP'	Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d.h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.
	'AsyncPPP'	Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
	'... mit Script'	Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
	'DHCP'	Zuordnung der Netzwerkparameter über DHCP.
Layer-2	In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'X.75LAPB'	Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
	'PPPoE'	Kapselung der PPP-Protokollinformationen in Ethernet-Frames.
Optionen	Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'ISDN-Kanalbündelung mit MLPPP' →Seite 155.	
Layer-1	In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'AAL-5'	ATM-Anpassungsschicht
	'ETH-10'	Transparentes Ethernet nach IEEE 802.3.
	'HDLC'	Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus).
	'V.110'	Übertragung nach V.110 mit maximal 38.400 bit/Sekunde, z.B. für Einwahl per HSCSD-Mobiltelefon
	Modem	Modem-Übertragung (benötigt Fax-Modem-Option)

7.4 IP-Masquerading

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus z. B. auf das Internet zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Damit nicht jeder Arbeitsplatzrechner mit seiner IP-Adresse im gesamten Internet bekannt sein muss, wird das „IP-Masquerading“ als Versteck für alle Rechner im Intranet eingesetzt. Beim IP-Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige Intranet-IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige, öffentliche IP-Adresse haben (fest vergeben sein oder vom Provider dynamisch zugewiesen).

▷ IP-Masquerading

Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, muss der Router über zwei IP-Adressen verfügen:

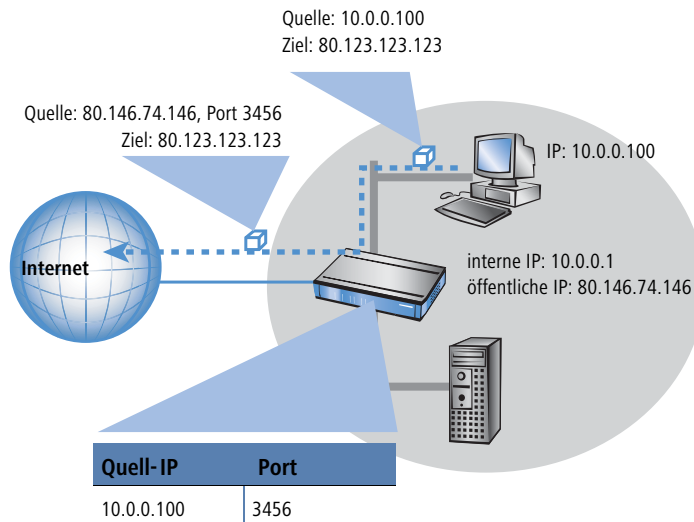
- ▶ die Intranet IP-Adresse zur Kommunikation mit den Rechnern im LAN
- ▶ die öffentliche IP-Adresse zur Kommunikation mit den Gegenstellen im Internet

Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet.

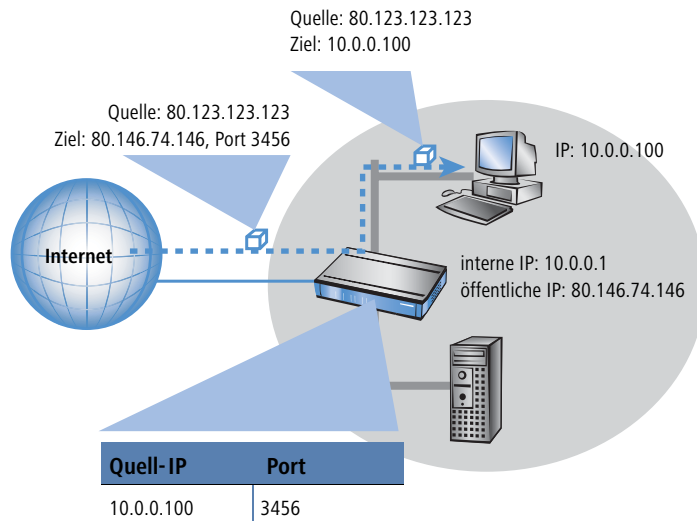
7.4.1 Einfaches Masquerading

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.



Die Antwort auf dieses Paket geht nun an die IP-Adresse des Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.



Welche Protokolle können mit IP-Masquerading übertragen werden?

Das IP-Masquerading funktioniert problemlos für all jene IP-Protokolle, die auf TCP, UDP oder ICMP basieren und dabei ausschließlich über Ports kommunizieren. Zu diesen unproblematischen Protokollen zählt beispielsweise das Basis-Protokoll des World Wide Web: HTTP.

Einzelne IP-Protokolle verwenden zwar TCP oder UDP, kommunizieren allerdings nicht ausschließlich über Ports. Derartige Protokolle verlangen beim IP-Masquerading eine entsprechende Sonderbehandlung. Zu den vom IP-Masquerading im LANCOM unterstützten Protokollen mit Sonderbehandlung gehören:

- ▶ FTP (über die Standardports)
- ▶ H.323 (im Umfang, wie ihn Microsoft Netmeeting verwendet)
- ▶ PPTP
- ▶ IPSec
- ▶ IRC

▷ IP-Masquerading

Konfiguration des IP-Masquerading

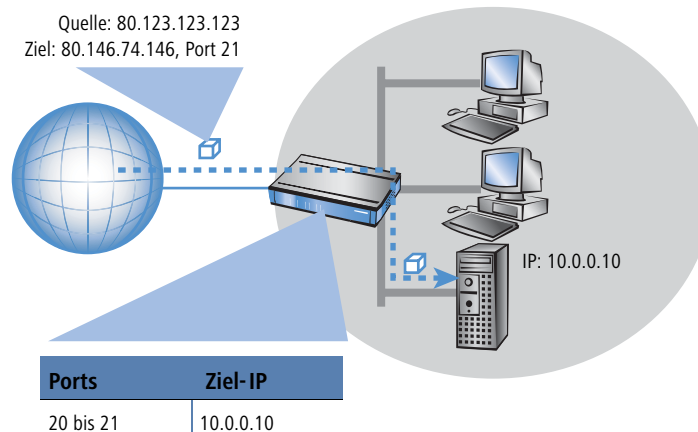
Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle erreichen Sie wie folgt:

Konfigurationstool	Aufruf
LANconfig	IP-Router ► Routing ► Routing-Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► IP-Routing-Tab
Terminal/Telnet	/Setup/IP-Router/IP-Routing-Tab

7.4.2 Inverses Masquerading

Beim einfachen Masquerading werden alle IP-Adressen im lokalen Netz hinter der IP-Adresse des Routers maskiert (versteckt). Soll nun ein bestimmter Rechner im LAN für Stationen aus dem Internet erreichbar sein (z.B. ein FTP-Server), dann ist bei Einsatz des einfachen Masquerading auch die IP-Adresse des FTP-Servers im Internet nicht bekannt. Ein Verbindungsaufbau zu diesem FTP-Server aus dem Internet ist also so nicht mehr möglich.

Um den Zugriff auf einen solchen Server ("exposed host") im LAN zu ermöglichen, wird in einer Tabelle (Service-Tabelle) die IP-Adresse des FTP-Servers eingetragen mit allen Diensten (Ports), die er auch außerhalb des LANs anbieten soll. Schickt nun ein Rechner aus dem Internet ein Paket an den FTP-Server im LAN, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest anhand des verwendeten Protokolls aus dem Eintrag in der Service-Tabelle die IP-Adresse des FTP-Servers im LAN und leitet das Paket an die dort eingetragene lokale IP-Adresse weiter. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden wieder hinter der IP-Adresse des Routers versteckt.



Der generelle Unterschied zwischen einfachem und inversem Masquerading:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muss beim inversen Masquerading manuell durch Angabe einer Port-Nummer definiert werden. In der Service-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z.B. des FTP-Servers angegeben.
- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adress-Informationen automatisch durch den Router selbst vorgenommen.



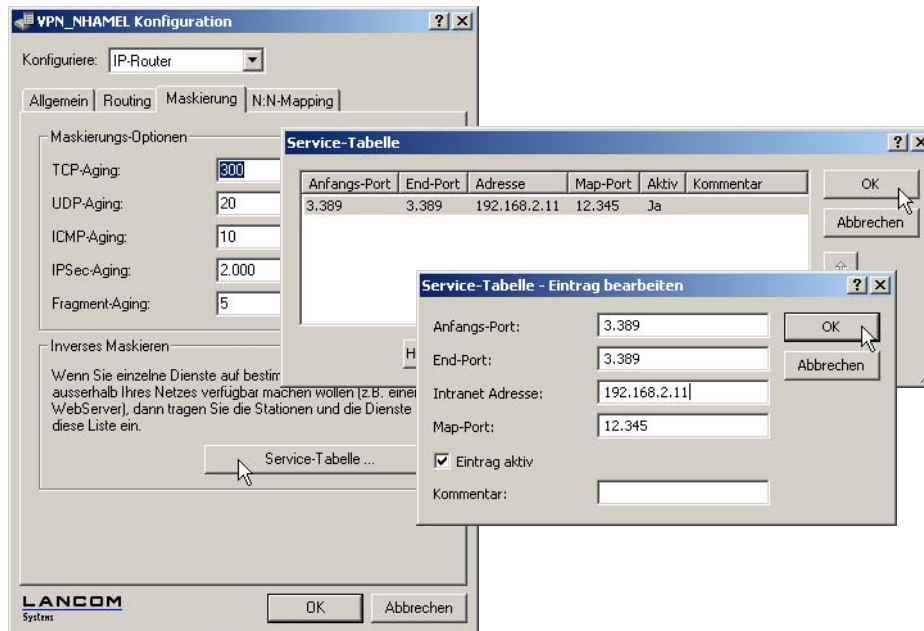
Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

Nach einer einstellbaren Zeit geht der Router jedoch davon aus, dass der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Konfiguration des inversen Masqueradings

Konfiguration
mit LANconfig

Die Service-Tabelle zur Einstellung des inversen Masqueradings finden Sie unter LANconfig im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Maskierung':




▷ IP-Masquerading

Konfiguration mit WEBconfig oder Telnet

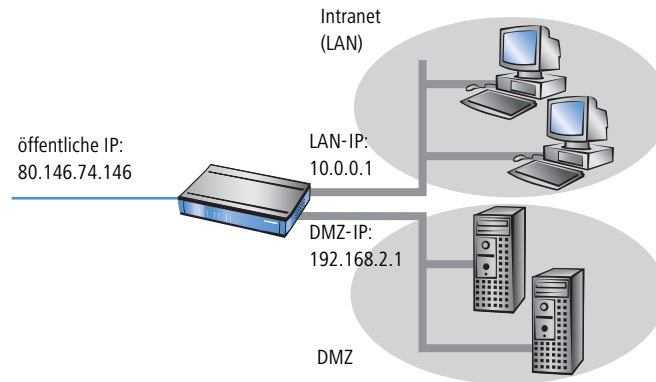
Unter WEBconfig oder Telnet finden Sie die Parameter zur Einstellung des inversen Masqueradings an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► Masquerading ► Service-Tabelle
Terminal/Telnet	/Setup/IP-Router/Masquerading/Service-Tabelle

 **Stateful-Inspection und inverses Masquerading:** Wenn im Masquerading-Modul ein Port freigeschaltet wird (d.h. alle auf diesem Port empfangenen Pakete sollen an einen Rechner im lokalen Netz weitergeleitet werden), so erfordert dies bei einer Deny-All Firewall-Strategie einen **zusätzlichen** Eintrag in der Stateful-Inspection Firewall, der den Zugriff aller Rechner auf den jeweiligen Server ermöglicht.

7.4.3 Demilitarisierte Zone (DMZ)

Auf der lokalen Seite kann der Router zwei unterschiedliche IP-Adresskreise verwalten: Das Intranet (LAN) und die DMZ ('De-Militarized Zone'). Die DMZ bezeichnen einen eigenen Bereich, welcher in der Regel für aus dem Internet erreichbare Server verwendet wird:



Mit der Option **Maskierung** in der Routing-Tabelle informieren Sie den Router darüber, ob die lokalen Intranet- oder DMZ-Adressen hinter der Internet-IP-Adresse des Routers versteckt werden sollen:

- **IP-Masquerading abgeschaltet:** Es wird keine Maskierung durchgeführt. Diese Variante ist für Internetzugänge mit mehreren statischen IP-Adressen (einzutragen unter DMZ-Adresse und DMZ-Netzmaske) vorgesehen, mit denen ausschließlich Server an das Internet gekoppelt werden, oder aber um z.B. zwei Intranet-Subnetze via VPN zu koppeln.
- **Intranet und DMZ maskieren (Standard):** In dieser Einstellung werden alle lokalen Adressen maskiert. Neben dem Intranet (LAN) kann zusätzlich noch ein zweites lokales Netz mit privaten Adressen an das Internet angebunden werden.

- ▶ **Nur Intranet maskieren:** Diese Einstellung ist insbesondere für Internetzugänge mit mehreren statischen IP-Adressen geeignet. Anders als beim Fall 'IP-Masquerading abgeschaltet' steht jedoch neben der DMZ noch der Intranet-Adresskreis mit maskierten, privaten IP-Adressen für ein LAN zur Verfügung.

Die Zuweisung der DMZ und der Intranet Adressen des LANCOM kann wie folgt vorgenommen werden:

Konfigurationstool	Aufruf
LANconfig	TCP/IP ▶ Allgemein
WEBconfig	Experten-Konfiguration ▶ Setup ▶ TCP-IP
Terminal/Telnet	/Setup/TCP-IP

7.4.4 Unmaskierter Internet-Zugang für Server in der DMZ

Das im vorangegangenen Abschnitt beschriebene inverse Maskieren erlaubt zwar, jeweils einen bestimmten Dienst zu exponieren (z.B. je ein Web-, Mail- und FTP-Server), hat aber z.T. weitere Einschränkungen:

- ▶ Der betreffende Dienst des 'exposed host' muss vom Maskierungsmodul unterstützt und verstanden werden. Zum Beispiel benutzen einige VoIP-Server nicht-standarisierte, proprietäre Ports für eine erweiterte Signalisierung. Dadurch können solche Server-Dienste nur an Verbindungen ohne Maskierung betrieben werden.
- ▶ Vom Sicherheitsstandpunkt muss beachtet werden, dass sich der 'exposed host' im lokalen Netz befindet. Falls der Rechner unter die Kontrolle eines Angreifers gebracht wird, so kann dieser Rechner als Ausgangsbasis für Angriffe gegen weitere Maschinen im lokalen Netz missbraucht werden.



Um Angriffe von 'geknackten' Servern auf das lokale Netz zu verhindern, verfügen einige LANCOM über ein dediziertes DMZ-Interface (LANCOM 7011 VPN). Alle anderen Modelle mit 4-Port-Switch (LANCOM 821 ADSL/ISDN, LANCOM 1511 DSL, LANCOM 1521 ADSL, LANCOM 1621 ADSL/ISDN, LANCOM 1711 VPN, LANCOM 1811 DSL und LANCOM 1821 ADSL) oder können die LAN-Ports per Hardware auf Ethernet-Ebene einzeln oder „en bloc“ voneinander trennen.

Zwei lokale Netze - Betrieb von Servern in der DMZ

Hierfür ist ein Internetzugang mit mehreren statischen IP-Adressen notwendig. Bitte kontaktieren Sie Ihren ISP ggf. für ein entsprechendes Angebot.

▷ Multi-PPPoE

Ein Beispiel: Sie erhalten die Internet IP-Netzadresse 123.45.67.0 mit der Netzmaske 255.255.255.248 vom Provider zugewiesen. Dann könnten Sie die IP-Adressen wie folgt verteilen:

öffentliche DMZ IP-Adresse	Bedeutung/Verwendung
123.45.67.0	Netzadresse
123.45.67.1	LANCOM als Gateway für das Intranet
123.45.67.2	Gerät im lokalen Netzwerk, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise ein Web-Server am DMZ-Port
123.45.67.3	Broadcast-Adresse

Alle Rechner und Geräte im Intranet haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des LANCOM (123.45.67.1) im Internet auf.

Trennung von Intranet und DMZ



Obwohl Intranet und DMZ vielleicht bereits schon auf Ethernet-Ebene durch dedizierte Interfaces voneinander getrennt sind, so muss in jedem Fall noch eine Firewall-Regel zur Trennung auf IP-Ebene eingerichtet werden!

Dabei soll der Server-Dienst vom Internet und aus dem Intranet heraus erreichbar sein, aber jeglicher IP-Traffic aus der DMZ Richtung Intranet soll unterbunden werden. Für das obige Beispiel ergäbe sich folgendes:

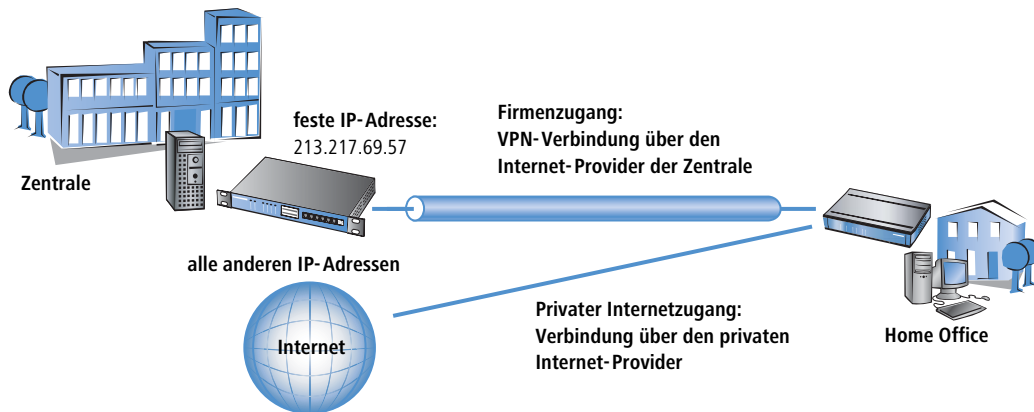
- Bei einer "Allow-All"-Strategie (default): Zugriff von "123.45.67.2" auf "Alle Stationen im lokalen Netz" verbieten
- Bei einer "Deny-All"-Strategie ('Aufbau einer expliziten "Deny-All"-Strategie' →Seite 198): Zugriff von "Alle Stationen im lokalen Netz" auf "123.45.67.2" erlauben

7.5 Multi-PPPoE

In den meisten Fällen wird auf einem DSL- oder ADSL-WAN-Interface immer nur eine Verbindung zu einer Zeit aufgebaut sein. Es gibt aber durchaus sinnvolle Anwendungen, in denen mehrere parallele Verbindungen auf dem WAN-Interface benötigt werden. LANCOM-Geräte mit DSL- oder ADSL-Interface können bis zu acht verschiedene Kanäle ins WAN parallel auf dem gleichen physikalischen Interface aufbauen.

7.5.1 Anwendungsbeispiel: Home-Office mit privatem Internetzugang

Eine mögliche Anwendung ist z.B. das Home-Office eines Außendienst-Mitarbeiters, der über eine VPN-Verbindung einen Zugang zum Netzwerk der Zentrale erhalten soll. Das Unternehmen zahlt dabei die Kosten für die VPN-Verbindung, der Mitarbeiter im Home-Office zahlt seinen privaten Internet-Datenverkehr selbst.



Um die beiden Datenverbindungen exakt trennen zu können, werden zwei Internetverbindungen für die jeweiligen Provider eingerichtet. Die Default-Route wird in der IP-Routing-Tabelle dann dem privaten Provider zugeordnet, das Netzwerk der Zentrale über die VPN-Verbindung wird über den Provider der Zentrale geroutet.

7.5.2 Konfiguration

Zur Konfiguration eines solchen Szenarios sind im Home-Office-Router die folgenden Schritte notwendig:

- ▶ Konfiguration des privaten Internetzugangs, z.B. über den Assistenten von LANconfig oder WEBconfig
- ▶ Konfiguration des Internetzugangs, der über die Zentrale abgerechnet wird
- ▶ Auswahl des privaten Providers für die Default-Route in der IP-Routing-Tabelle (z.B. manuell in LANconfig oder mit dem Assistenten zur Auswahl des Internetproviders unter WEBconfig)
- ▶ Konfiguration der VPN-Verbindung zum Netzwerk der Zentrale
- ▶ Zuweisung der VPN-Verbindung zum Provider der Zentrale:

Damit der Datenverkehr zur Zentrale über den richtigen Internetprovider geroutet wird, muss in der IP-Routing-Tabelle noch ein neuer Eintrag angelegt werden. Darin wird das VPN-Gateway der Zentrale mit seiner festen IP-Adresse und der passenden Netzmaske eingetragen und auf die Gegenstelle für den Internetprovider der Zentrale geleitet.



Wichtig ist, dass die Route zum Internetprovider der Zentrale maskiert wird, denn sonst würde das LANCOM nicht die WAN-Adresse, sondern seine LAN-Adresse in die VPN-Pakete einsetzen und die Verbindung käme niemals zustande.

Weitere Informationen zu diesen Konfigurationsschritten finden Sie an den entsprechenden Stellen in der Dokumentation zum Ihrem LANCOM-Gerät.

▷ Load-Balancing

! **Administrator-Rechte des Mitarbeiters im Home-Office:** Damit der Mitarbeiter im Home-Office nicht versehentlich die Einstellungen für die Internet-Provider oder den VPN-Zugang verändert, sollten Sie ihm je nach Vereinbarung nur die WEBconfig-Funktionsrechte für die Assistenten „Internet-Zugang“ und „Auswahl von Internet-Providern“ zuweisen. Informationen über die Konfiguration von speziellen Benutzerrechten finden Sie in diesem Addendum unter 'Rechteverwaltung für verschiedene Administratoren' →Seite 41.

i Sorgen Sie mit den entsprechenden Filterregeln im Bereich 'Firewall/QoS' dafür, dass der Internetverkehr nicht versehentlich über das Netzwerk der Zentrale läuft.

7.6 Load-Balancing

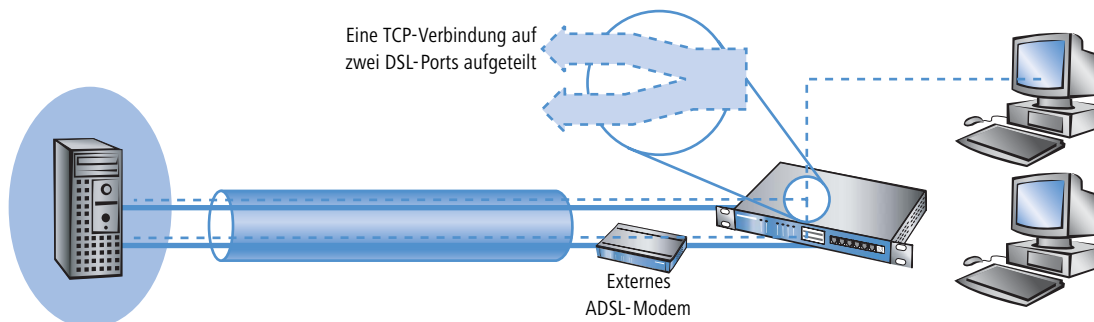
Trotz immer weiter steigender Bandbreite auf DSL-Zugängen stellen diese immer noch das Nadelöhr in der Kommunikation dar. In manchen Fällen ist es durchaus sinnvoll, mehrere DSL-Zugänge zu bündeln. Hierzu gibt es mehrere Möglichkeiten, die zum Teil vom Internet-Provider aktiv unterstützt werden müssen:

► **DSL-Kanalbündelung (Multilink-PPPoE – MLPPPoE)**

Bei der direkten Bündelung ist der Anwender auf das Angebot des Carriers angewiesen, der dieses Verfahren unterstützen muss. Dem Anwender steht dabei die Summe der Bandbreiten aller gebündelter Kanäle zur Verfügung. Multilink-PPPoE kann nur zum Bündeln von PPP-Verbindungen eingesetzt werden.

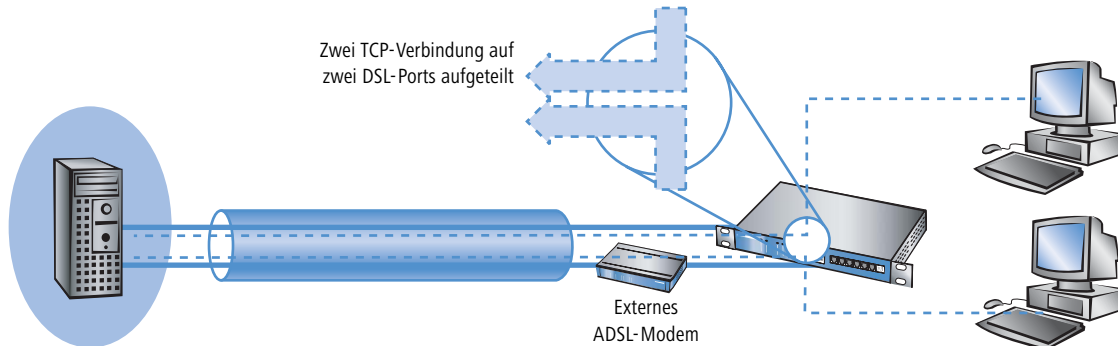
i Diese Variante der Kanalbündelung stellt als Summe ein Vielfaches der kleinsten der gebündelten Kanäle zur Verfügung. Sie ist daher besonders effizient, wenn Kanäle mit gleichen Bandbreiten verbunden werden. Bei der direkten Bündelung unterschiedlicher Bandbreiten geht für die Kanäle mit hohen Datenraten effektive Bandbreite verloren.

MLPPPoE verhält sich beim Bündeln von DSL-Kanälen wie das bekannte MLPPP bei ISDN-Kanalbündelung 'ISDN-Kanalbündelung mit MLPPP' →Seite 155.



► Load-Balancing

Beim Load-Balancing werden TCP-Verbindungen dynamisch auf voneinander unabhängigen DSL-Verbindungen verteilt. Dem Anwender steht damit zwar auch die Summen-Bandbreite der gebündelten Kanäle zur Verfügung, dennoch ist jede einzelne TCP-Verbindung auf die Bandbreite des zugewiesenen DSL-Anschlusses beschränkt.



i Im Gegensatz zur direkten Kanalbündelung steht beim Load-Balancing tatsächlich die Summe aller gebündelten Bandbreiten zur Verfügung. Diese Variante eignet sich daher besonders gut zum Verbinden unterschiedlicher Bandbreiten.

7.6.1 DSL-Port-Mapping

Grundvoraussetzung für eine DSL-Kanalbündelung ist die Unterstützung von mehr als einem DSL-Interface pro Gerät. Dazu werden an den Switch eines LANCOM-Routers ein oder mehrere externe DSL-Modems angeschlossen.

i Bitte informieren Sie sich in der Featurotable im Anhang (Kapitel 16 ab Seite 454), ob Ihr Gerät den Anschluss externer DSL-Modems unterstützt.

Zuordnung der Switch-Ports zu den DSL-Ports

Bei Geräten mit integriertem Switch können je nach Modell ('Übersicht über die Funktionen nach Modellen und LCOS*-Versionen' → Seite 454) einige der LAN-Ports als zusätzlicher WAN-Port zum Anschluss externer DSL-Modems dienen. Diese Ports werden in der Interface-Tabelle als getrennte DSL-Interfaces aufgeführt (DSL-1, DSL-2 usw.). Die DSL-Ports werden in der Liste der WAN-Interfaces als DSL-Interface aktiviert, mit den korrekten Up- und

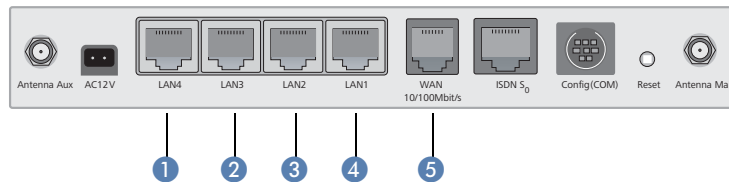
▷ Load-Balancing

Downstreamraten konfiguriert und in der Liste der LAN-Interfaces den Switch-Ports zugeordnet (Beispiel: LANCOM Wireless 1811 DSL):

Port	Zuordnung	Anschluss	MDI-Modus	Privat-Modus
LAN-1	LAN-1	Auto	Auto	Nein
LAN-2	LAN-1	Auto	Auto	Nein
LAN-3	LAN-1	Auto	Auto	Nein
LAN-4	LAN-1	Auto	Auto	Nein
WAN	DSL-1	Auto	Auto	Nein

- In der Spalte 'Port' steht die Bezeichnung, die die jeweiligen Ports auf der Rückblende des Geräts haben.
- In der Spalte 'Zuordnung' wird die Verwendung des Ports angegeben:
 - ▷ keine: Der Port ist deaktiviert
 - ▷ LAN-1: Der Port ist dem LAN zugeordnet
 - ▷ DSL-1, DSL-2, ... : Der Port ist einem der DSL-Interfaces zugeordnet
 - ▷ Monitor: Der Port ist ein Monitor-Port, d.h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z.B. ein Paket-Sniffer (wie Ethereal) angeschlossen werden.

Die Zuordnung der DSL-Ports zu den Ethernetports ist dabei beliebig wählbar. Eine sinnvolle und übersichtliche Zuordnung ergibt sich, wenn Sie die DSL-Ports in umgekehrter Reihenfolge den Ports am Switch zuordnen (Beispiel: LANCOM Wireless 1811 DSL):



- 1 LAN4 ▷ DSL-2
- 2 LAN3 ▷ DSL-3
- 3 LAN2 ▷ DSL-4
- 4 LAN1 ▷ LAN-1: Dieser Port bleibt für das LAN reserviert
- 5 WAN ▷ DSL-1: (dedizierter WAN-Port des Geräts)

In der Liste der DSL-Breitband-Gegenstellen wird der zu verwendende DSL-Port angegeben, wenn das Gerät über mehr als einen DSL-Port verfügt:

- ▶ Wird kein Port (oder der Port „0“) angegeben, so wählt das LANCOM den Port nach dem für die Verbindung gewählten Kommunikations-Layer aus.
 - ▷ Wenn auf Layer-1 'AAL-5' eingestellt ist, wird das ADSL-Interface ausgewählt.
 - ▷ Wenn auf Layer-1 'ETH' eingestellt ist, wird der erste DSL-Port (also DSL-1) ausgewählt.
- ▶ Wird ein bestimmter Port (ungleich „0“) angegeben, so wird dieser für die Verbindung verwendet.



Beachten Sie, dass der für die Verbindung über diesen Port eingestellte Kommunikations-Layer im Layer 1 auf 'ETH' eingestellt ist.

- ▶ Um eine Kanalbündelung über mehrere DSL-Interfaces zu ermöglichen, werden für die Gegenstelle in der Gegenstellenliste die entsprechenden Ports eingetragen (als kommaseparierte Port-Liste '1,2,3' oder als Port-Bereich '1-3'). Bei einer Port-Liste werden die Bündelkanäle genau in der angegebenen Reihenfolge aufgebaut, nur im Fehlerfall werden die Kanäle nach aufsteigender Reihenfolge versucht. Bei einem Port-Bereich werden die Kanäle immer in aufsteigender Reihenfolge aufgebaut.
 - ▷ Die Ports müssen in der Liste der Ethernet-Ports als DSL-Port geschaltet sein.
 - ▷ Die DSL-Ports müssen in der Liste der WAN-Interfaces als DSL-Interface aktiviert und mit den korrekten Up- sowie Downstreamraten konfiguriert sein.
 - ▷ In dem für die Verbindung verwendeten Layer muss die Bündelung aktiviert sein, die auch von der Gegenstelle unterstützt werden muss.
 - ▷ Um eine Kanalbündelung mit einem internen ADSL-Interface zu konfigurieren, wird der ADSL-Port '0' **an erster Stelle** in die Liste der Ports aufgenommen (z.B. '0,1,3' als Port-Liste oder '0-3' als Port-Bereich). Für die Gegenstelle muss im verwendeten Kommunikations-Layer auf Layer 1 'AAL-5' eingestellt werden.



Ein Eintrag in der Gegenstellenliste kann verschiedene Ports (z.B. ADSL und Ethernet) enthalten, kann aber nur **einen** Kommunikations-Layer referenzieren, in dem nur **ein** Layer-1-Protokoll angegeben werden kann. Für die gebündelte Kommunikation über ADSL- und Ethernet-Ports sind jedoch **zwei** verschiedene Layer-1-Protokolle notwendig. Aus diesem Grund wird der Layer 1 in diesen Fällen auf 'AAL-5' für ADSL eingestellt. Da nur ein ADSL-Interface in den Geräten vorhanden sein kann, wird für alle zugebündelten Interfaces automatisch auf den Layer 1 mit 'ETH' für Ethernet-DSL-Ports umgestellt. Diese automatische Layerumstellung gelingt jedoch nur, wenn das ADSL-Interface als erstes für die Bündel-Verbindungen gewählt wird.

- ▷ Bei Geräten mit einem eingebauten ADSL-Modem und einem zusätzlichen Ethernet-Interface (DSL oder DSLoL) ist klar, welche Ports bei einer Bündelung verwendet werden. In diesem Fall ist daher die Angabe der

▷ Load-Balancing

Ports in der Gegenstellenliste nicht erforderlich. Bei diesen Geräten wird immer intern eine Port-Liste '0,1' angenommen, damit das interne ADSL-Interface als erstes für die Bündelung verwendet wird.



Bei Multi-PPPoE ('Multi-PPPoE' →Seite 128) teilen sich mehrere PPPoE-Verbindungen eine physikalische DSL-Leitung. Bei Multi-DSL werden mehrere PPPoE-Verbindungen auf die vorhandenen DSL-Interfaces verteilt. Die Anzahl der parallel möglichen Verbindungen ist auf maximal 8 Kanäle begrenzt.

Zuordnung der MAC-Adresse zu den DSL-Ports

Wenn ein LANCOM durch die Verwendung der Switch-Ports über mehrere DSL(WAN)-Interfaces verfügt, müssen auch entsprechend viele MAC-Adressen zur Unterscheidung der DSL-Ports genutzt werden. Da die zu verwendende MAC-Adresse in manchen Fällen von der Gegenstelle abhängt, die aufgrund der MAC-Adresse die z.B. die Abrechnung eines DSL-Zugangs durchführt, werden die MAC-Adressen für die logischen DSL-Gegenstellen und nicht für die physikalischen DSL-Ports definiert.

Für die Einstellung der MAC-Adresse stehen folgende Optionen zur Verfügung:

- ▶ Global: Globale System-MAC-Adresse
- ▶ Lokal: aus der globalen Adresse wird eine eindeutige, lokal administrierte MAC-Adresse berechnet
- ▶ Benutzerdefiniert: Eine vom Benutzer frei wählbare MAC-Adresse



Jede aufgebaute DSL-Verbindung erhält eine eigene MAC-Adresse. Sollten für zwei Gegenstellen die gleichen MAC-Adressen konfiguriert sein, so wird für die erste aufzubauende Verbindung die konfigurierte MAC-Adresse verwendet. Für die zweite Verbindung wird hingegen aus der konfigurierten MAC-Adresse eine „lokal administrierte MAC-Adresse“ errechnet, die somit wieder eindeutig ist.

Ebenso wird bei einer Kanalbündelung für die erste Verbindung die konfigurierte MAC-Adresse verwendet für die weiteren Bündelverbindungen eine „lokal administrierte“ MAC-Adresse auf Grundlage der konfigurierten MAC-Adresse berechnet.

Sollte eine Ihrer Verbindungen über die MAC-Adresse abgerechnet werden, konfigurieren Sie diese MAC-Adresse nur auf der separat abgerechneten Verbindung. Verwenden Sie für alle übrigen Verbindungen eine andere Adresse.

7.6.2 DSL-Kanalbündelung (MLPPPoE)

Um DSL-Anschlüsse zu bündeln, werden die zu verwendenden DSL-Ports in der Liste der DSL-Breitband-Gegenstellen eingetragen. Dabei wird nur die Nummer des DSL-Ports angegeben, bei mehreren Ports durch Kommata separiert (1,2,4) oder als Bereich (1-4).

Um PPPoE-Verbindungen zu bündeln reicht es aus, die Bündelung im verwendeten Layer zu aktivieren und in der Portliste die zu verwendenden Ports zuzuweisen.

7.6.3 Dynamisches Load-Balancing

Wenn der Internet-Provider eine direkte Bündelung nicht unterstützt, werden mehrere normale DSL-Zugänge über einen Load-Balancer gekoppelt. Hierzu werden zuerst die DSL-Zugänge für die benötigten DSL-Ports eingerichtet. Danach werden diese über eine Load-Balancing-Tabelle miteinander gekoppelt. Diese Liste ordnet einer virtuellen Balancing-Verbindung (das ist die Verbindung, die in der Routing-Tabelle eingetragen wird) die weiteren realen DSL-Verbindungen (Bündel-Verbindungen) zu. Einer Balancing-Verbindung können dabei je nach Anzahl der verfügbaren DSL-Ports mehrere Bündel-Verbindungen zugeordnet werden.



Die Balancing-Verbindung wird als „virtuelle“ Verbindung angelegt. Für diese Verbindung werden also keine Zugangsdaten etc. eingetragen. Dieser Eintrag dient nur als „Verteiler“, um einem Eintrag in der Routing-Tabelle mit Hilfe der Load-Balancing-Tabelle mehrere „reale“ Bündel-Verbindungen zuweisen zu können.



Bei der DSL-Bündelung handelt es sich um eine statische Bündelung. Die evtl. zusätzlichen Kanäle werden also **nicht** nur nach Bedarf des übertragenen Datenvolumens auf- und wieder abgebaut.

Die Entscheidung über das Routing der Datenpakete kann beim Load-Balancing nicht mehr allein anhand der IP-Adressen getroffen werden, da die einzelnen gebündelten DSL-Verbindungen unterschiedliche IP-Adressen haben. Beim Load-Balancing werden daher zusätzlich die Informationen aus der Verbindungsliste der Firewall berücksichtigt. In dieser Liste wird für jede TCP-Verbindung ein Eintrag angelegt, der für das Load-Balancing zusätzlich die Information über den verwendeten DSL-Port bereitstellt.

Verbindungsaufbau

Bei der Anforderung für eine Datenübertragung zu einer Balancing-Gegenstelle wird zunächst die **erste** Bündel-Verbindung aus der Load-Balancing-Tabelle aufgebaut. Der weitere Verlauf hängt vom Erfolg der Verbindungsaufbaus ab:

- Wird die Verbindung erfolgreich aufgebaut, werden zunächst alle anstehenden TCP-Verbindungen diesem Kanal zugewiesen. Anschließend werden sukzessive alle konfigurierten Bündel-Verbindungen aufgebaut. Sobald mindestens zwei Bündel-Verbindungen aktiv sind, werden neue TCP-Verbindungen unter den aktiven Bündel-Verbindungen verteilt.
- Scheitert jedoch der Aufbau der ersten Bündel-Verbindung, so wird nacheinander der Aufbau der weiteren Bündel-Verbindungen versucht. Sobald eine der Bündel-Verbindungen aufgebaut werden konnte, werden alle zu diesem Zeitpunkt anstehenden TCP-Verbindungen auf diesen Kanal umgeleitet.

Verteilung der Datenlast

Für die Verteilung der Datenlast auf die verfügbaren Kanäle stehen prinzipiell zwei Varianten zur Auswahl:

- Wenn die Bandbreite des jeweiligen Kanals bekannt ist, dann werden die Verbindungen dem Kanal zugewiesen, der die geringste (prozentuale) Auslastung hat.

▷ Load-Balancing

- ▶ Wenn die Bandbreite unbekannt ist, dann wird unterschieden, ob es sich bei der Verbindung um eine TCP-Verbindung handelt oder ob das LANCOM eine VPN- oder PPTP-Verbindung aufbauen will.
 - ▷ Wenn eine TCP-Verbindung einen Kanal anfordert, dann wird derjenige mit der geringsten absoluten Last ausgewählt.
 - ▷ Wenn eine VPN- oder PPTP-Verbindung einen Kanal anfordert, dann werden die PPTP- und VPN-Verbindung gleichmäßig auf die verfügbaren Kanäle verteilt.



Für die sinnvolle Nutzung des Load-Balancing ist daher die Angabe der Bandbreite in der Liste der WAN-Interfaces unter LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' unter der Schaltfläche **Interface-Einstellungen** erforderlich (Telnet: /Setup/Schnittstellen/DSL, WEBconfig: **Expertenkonfiguration ▶ Setup ▶ Schnittstellen ▶ DSL**).

7.6.4 Statisches Load-Balancing

Neben der im vorhergehenden Abschnitt beschriebenen dynamischen Verbindungsauswahl sind Szenarien vorstellbar, in denen für eine bestimmte TCP-Verbindung immer die gleiche DSL-Verbindung benutzt werden soll. Hierbei sind zwei Fälle zu unterscheiden:

- ▶ Ein Server mit einer festen IP-Adresse ist nur über eine dedizierte Verbindung erreichbar. Hierfür reicht die Auswahl anhand der Ziel-IP-Adresse.
- ▶ Ein Server verwendet ein Protokoll, das neben einem Kontrollkanal weitere Kanäle zur Datenübertragung benötigt (z.B. FTP, H.323, PPTP). Dabei akzeptiert der Server den Aufbau der Datenkanäle nur von der gleichen IP-Adresse, von der auch der Kontrollkanal aufgebaut wurde.

Zielbasierte Kanalvorgabe

Für die Zielbasierte Kanalvorgabe genügt es, für den jeweiligen Server einen Eintrag in der Routing-Tabelle aufzunehmen, der als Ziel nicht die „virtuelle“ Balancing-Verbindung, sondern eine der Bündel-Verbindungen direkt verwendet.

Regelbasierte Kanalvorgabe (Policy-based Routing)

Um die Kanalauswahl aufgrund des Zielports oder der Quelladresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag“ zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. Weitere Informationen finden Sie unter 'Policy-based Routing' →Seite 112.

7.6.5 Konfiguration des Load Balancing

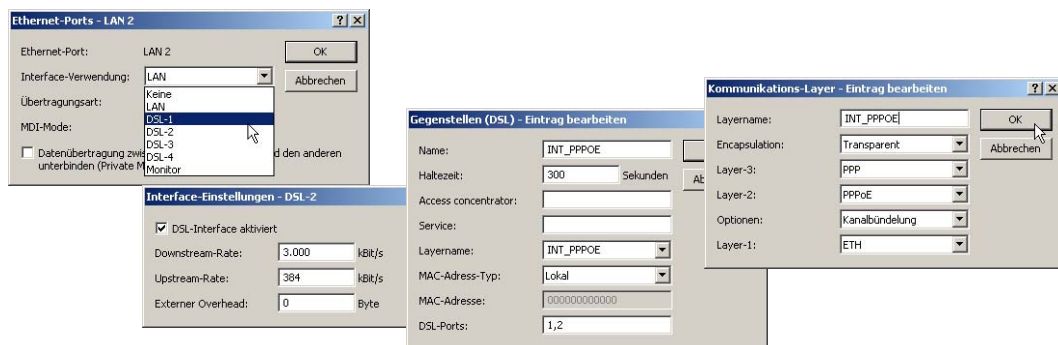


Für die folgenden Konfigurationen gehen wir davon aus, dass die entsprechenden Gegenstellen mit allen Zugangsdaten bereits eingerichtet sind.

Direkte Kanalbündelung über PPPoE

Zur Konfiguration der direkten Kanalbündelung über PPPoE gehen Sie folgendermaßen vor:

- ① Ordnen Sie den Ethernet-Ports die gewünschten DSL-Ports zu, in LANconfig über **Interfaces ► LAN ► Ethernet-Ports**.
Telnet: /Setup/Schnittstellen/Ethernet-Ports
WEBconfig: **Expertenkonfiguration ► Setup ► Schnittstellen ► Ethernet-Ports**
- ② Aktivieren Sie die zusätzlichen DSL-Interfaces in LANconfig über **Interfaces ► WAN ► Interface-Einstellungen**. Geben Sie dabei die Datenraten für Up- und Downstream an.
Telnet: /Setup/Schnittstellen/DSL
WEBconfig: **Expertenkonfiguration ► Setup ► Schnittstellen ► DSL**
- ③ Tragen Sie für die gewünschte Gegenstelle die zu verwendenden DSL-Ports in LANconfig über **Kommunikation ► Gegenstellen ► Gegenstellen (DSL)** ein.
Telnet: /Setup/WAN/DSL-Breitband-Gegenstellen
WEBconfig: **Expertenkonfiguration ► Setup ► WAN ► DSL-Breitband-Gegenstellen**
- ④ Aktivieren Sie für den verwendeten Layer die Kanalbündelung in LANconfig über **Kommunikation ► Allgemein ► Kommunikations-Layer**.
Telnet: /Setup/WAN/Layer
WEBconfig: **Expertenkonfiguration ► Setup ► WAN ► Layer**



Dynamisches Load-Balancing mit mehreren DSL-Zugängen

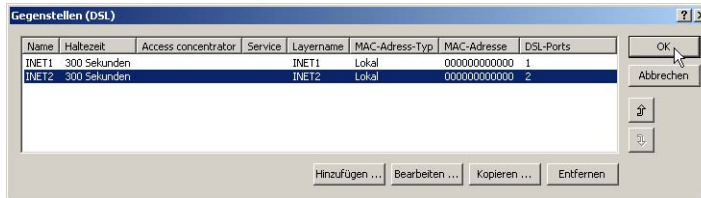
Für das dynamische Load-Balancing werden zunächst die Internetzugänge z.B. mit den Assistenten von LANconfig eingerichtet, z.B. 'INET1' und 'INET2'.

- ① Um den Internet-Traffic auf verschiedene DSL-Interfaces zu verteilen, werden den einzelnen Gegenstellen in LANconfig unter **Kommunikation ► Gegenstellen ► Gegenstellen (DSL)** unterschiedliche DSL-Ports zugewiesen.

▷ Load-Balancing

Telnet: /Setup/WAN/DSL-Breitband-Gegenstellen

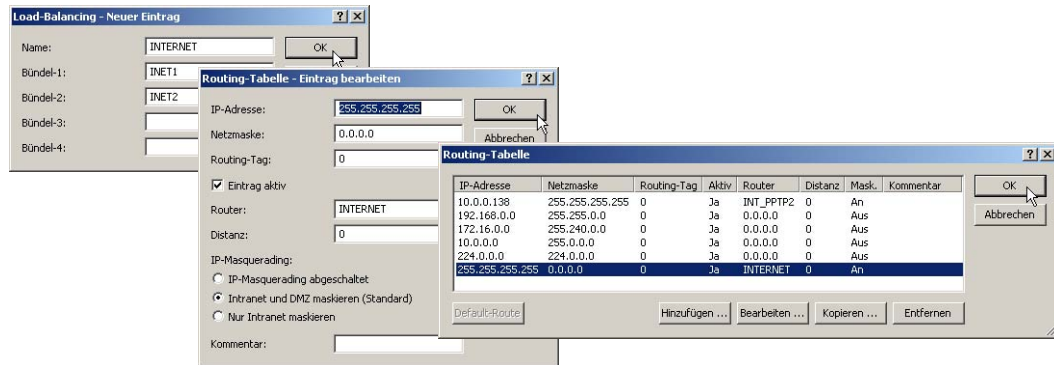
WEBconfig: **Expertenkonfiguration** ► **Setup** ► **WAN** ► **DSL-Breitband-Gegenstellen**



- ② Die beiden DSL-Gegenstellen werden dann in der Load-Balancing-Liste in LANconfig über **IP-Router** ► **Routing** ► **Load-Balancing** einer neuen, virtuellen Gegenstelle 'INTERNET' zugeordnet.

Telnet: /Setup/IP-Router/Load-Balancer

WEBconfig: **Expertenkonfiguration** ► **Setup** ► **IP-Router** ► **Load-Balancer**



- ③ Die virtuelle Gegenstelle wird in der Routing-Tabelle in LANconfig über **IP-Router** ► **Routing** ► **IP-Routing-Tabelle** als Router für die Default-Route eingetragen.

Telnet: /Setup/IP-Router/IP-Routing-Tabelle

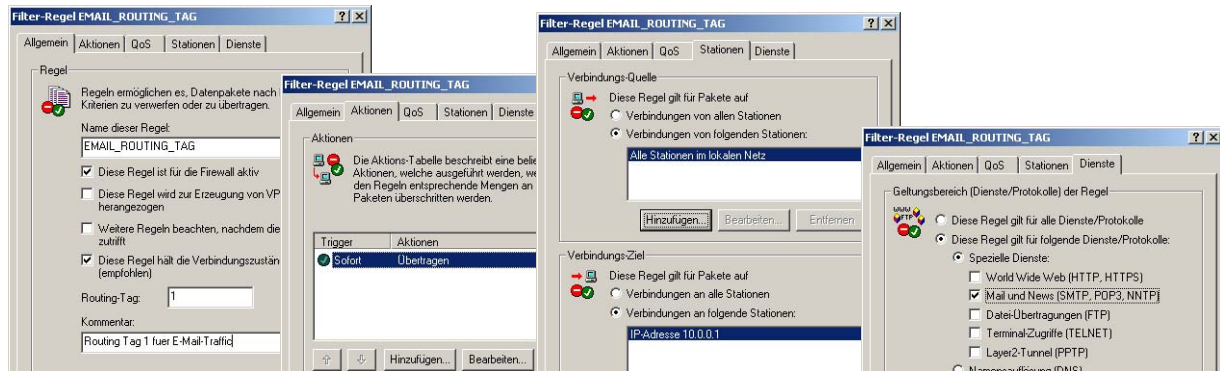
WEBconfig: **Expertenkonfiguration** ► **Setup** ► **IP-Router** ► **IP-Routing-Tabelle**

i Für den Zugang zum Internet wird nun die virtuelle Gegenstelle 'INTERNET' verwendet. Wenn Daten über diese Verbindung geroutet werden, werden anhand der Load-Balancing-Tabelle die „echten“ DSL-Verbindungen aufgebaut und die Daten entsprechend über die gewählten DSL-Ports übertragen.

- ④ Um den Datenverkehr je nach Anwendung gezielter auf die DSL-Ports zu verteilen, können die Routing-Tags genutzt werden. Soll z.B. der ausgehende E-Mail-Traffic über die bestimmtes DSL-Interface mit einer bestimmten IP-Adresse geroutet werden, wird in der Firewall unter LANconfig über **Firewall/QoS** ► **Regeln** eine entsprechende Regel angelegt, die den Datenverkehr über E-Mail-Dienste von allen lokalen Stationen zum Mail-Server überträgt und dabei das Routing-Tag '1' setzt.

Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

WEBconfig: **Expertenkonfiguration** ► **Setup** ► **IP-Router** ► **Firewall** ► **Regel-Tabelle**



7.7 N:N-Mapping

Das Verfahren der Network Address Translation (NAT) kann für mehrere Dinge benutzt werden:

- um die immer knapper werdenden IPv4-Adressen besser zu nutzen
- um Netze mit gleichen (privaten) Adressbereichen miteinander zu koppeln
- um eindeutige Adressen zum Netzwerkmanagement zu erzeugen

Für die erste Anwendung kommt das sogenannte N:1-NAT, auch als IP-Masquerading ('IP-Masquerading' →Seite 121) bekannt, zum Einsatz. Hierbei werden alle Adressen ("N") des lokalen Netzes auf eine einzige ("1") öffentliche Adresse gemappt. Die eindeutige Zuordnung der Datenströme zu den jeweiligen internen Rechnern erfolgt in der Regel über die Ports der Protokolle TCP und UDP, weshalb man hier auch von NAT/PAT (Network Address Translation/Port Address Translation) spricht.

Durch die dynamische Umsetzung der Ports sind beim N:1-Masquerading nur Verbindungen möglich, die vom internen Netz aus aufgebaut werden. Ausnahme: eine interne IP-Adresse wird statisch einem bestimmten Port zugeordnet, z.B. um einen Server im LAN von außen zugänglich zu machen. Dieses Verfahren nennt man "Inverses Masquerading" ('Inverses Masquerading' →Seite 124).

Zur Kopplung von Netzwerken mit gleichen Adressräumen wird ein N:N-Mapping verwendet. Dieses setzt mehrere Adressen ("N") des lokalen Netzes eineindeutig auf mehrere ("N") Adressen eines beliebigen anderen Netzes um. Durch diese Umsetzung wird der Adresskonflikt verhindert.

Die Regeln für diese Adressumsetzung werden in einer statischen Tabelle im LANCOM definiert. Dabei werden für einzelne Stationen im LAN, Teilnetze oder das gesamte LAN neue IP-Adressen festgelegt, unter denen die Stationen dann mit dem anderen Netzen in Kontakt treten können.

Bei einigen Protokollen (FTP, H.323) werden während der Protokollverhandlung Parameter ausgetauscht, die Einfluss auf die Adressumsetzung beim N:N-Mapping haben können. Die entsprechenden Verbindungsinformationen wer-

▷ N:N- Mapping

den bei diesen Protokollen daher mit den Funktionen der Firewall in einer dynamischen Tabelle festgehalten und zusätzlich zu den Einträgen aus der statischen Tabelle für die korrekte Funktion der Adressumsetzung verwendet.



Die Adressumsetzung erfolgt "Outbound", d.h. bei abgehenden Datenpaketen wird die Quelladresse umgesetzt, und bei eingehenden Datenpaketen wird die Zieladresse umgesetzt, sofern die Adressen im definierten Umsetzungsbereich liegen. Ein "Inbound"-Adressmapping, bei dem bei eingehenden Datenpaketen die Quelladresse (anstelle der Zieladresse) umgesetzt wird, muss stattdessen durch eine entsprechende "Outbound"-Adressumsetzung auf der Gegenseite eingerichtet werden.

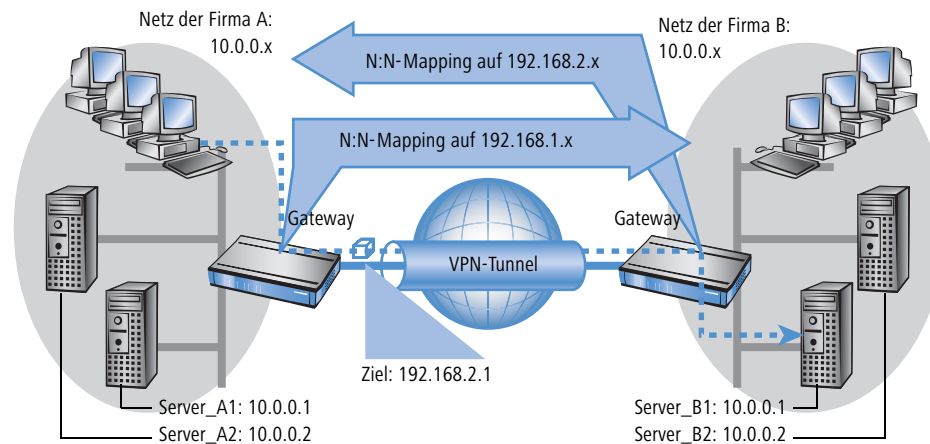
7.7.1 Anwendungsbeispiele

Im folgenden werden die folgenden typischen Anwendungen vorgestellt:

- Kopplung von privaten Netzen, die den gleichen Adressraum belegen
- Zentrale Fernüberwachung durch Dienstleister

Netzwerkkopplung

Ein häufig anzutreffendes Szenario stellt die Kopplung zweier Firmennetze dar, die intern den gleichen Adressraum (z.B. 10.0.0.x) belegen. Dies erfolgt meist dann, wenn eine Firma Zugriff auf einen (oder mehrere) Server der anderen erhalten soll:

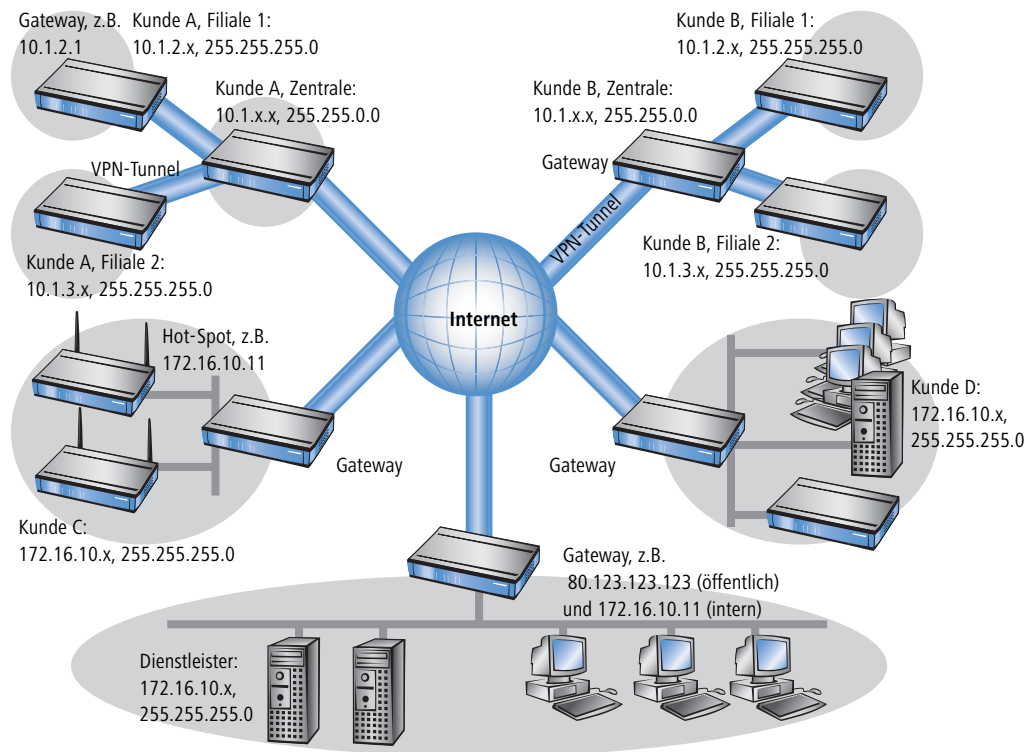


In diesem Beispiel stehen in den Netzen der Firmen A und B Server, die über einen VPN-Tunnel auf das jeweils andere Netz zugreifen wollen. Allen Stationen im LAN soll dabei der Zugang zu den Servern im remoten Netz erlaubt werden. Da beide Netze den gleichen Adresskreis nutzen, ist in dieser Konfiguration zunächst kein Zugriff in das andere Netz möglich. Wenn eine Station aus dem Netz der Firma A auf den Server 1 der Firma B zugreifen will, wird der Adressat (mit einer Adresse aus dem 10.0.0.x-Netz) im eigenen lokalen Netz gesucht, die Anfrage gelangt gar nicht bis zum Gateway.

Mit dem N:N-Mapping werden alle Adressen des LANs für die Kopplung mit dem anderen Netz in einen neuen Adresskreis übersetzt. Das Netz der Firma A wird z.B. auf die 192.168.1.x umgesetzt, das Netz der Firma B auf 192.168.2.x. Unter diesen neuen Adressen sind die beiden LANs nun für das jeweils andere Netz erreichbar. Die Station aus dem Netz der Firma A spricht den Server 1 der Firma B nun unter der Adresse 192.168.2.1 an. Der Adressat liegt nun nicht mehr im eigenen Netz, die Anfrage wird an das Gateway weitergeleitet und das Routing in das andere Netz funktioniert wie gewünscht.

Fernwartung und -überwachung von Netzwerken

Der Fernwartung und -überwachung von Netzwerken kommt durch die Möglichkeiten von VPN immer größere Bedeutung zu. Mit der Nutzung der fast flächendeckend vorhandenen Breitband-Internetanschlüsse kann sich der Administrator von solchen Management-Szenarien unabhängig machen von den unterschiedlichen Datenübertragungstechnologien oder teuren Standleitungen.



In diesem Beispiel überwacht ein Dienstleister von einer Zentrale aus die Netzwerke verschiedener Kunden. Zu diesem Zweck sollen die SNMP-fähigen Geräte die entsprechenden Traps über wichtige Ereignisse automatisch an den

▷ N:N- Mapping

SNMP-Trap-Empfänger (z.B. LANmonitor) im Netz des Dienstleisters senden. Der Administrator im LAN des Dienstleisters hat damit jederzeit einen aktuellen Überblick über der Zustand der Geräte.

Die einzelnen Netze können dabei sehr unterschiedlich aufgebaut sein: Die Kunden A und B binden ihre Filialen mit eigenen Netzwerken über VPN-Verbindungen in ihr LAN ein, Kunde C betreibt ein Netz mit mehreren öffentlichen WLAN-Basisstationen als Hot-Spots und Kunde D hat in seinem LAN u.a. einen weiteren Router für ISDN-Einwahlzugänge.



Die Netze der Kunden A und B in der jeweiligen Zentrale und den angeschlossenen Filialen nutzen verschiedene Adresskreise. Zwischen diesen Netzen ist also eine normale Netzwerkkopplung über VPN möglich.

Um den Aufwand zu vermeiden, zu jedem einzelnen Subnetz der Kunden A und B einen eigenen VPN-Tunnel aufzubauen, stellt der Dienstleister nur eine VPN-Verbindung zur Zentrale her und nutzt für die Kommunikation mit den Filialen die ohnehin vorhandenen VPN-Leitungen zwischen der Zentrale und den Filialen.

Die Traps aus den Netzen melden dem Dienstleister, ob z.B. ein VPN-Tunnel auf- oder abgebaut wurde, ob ein User sich dreimal mit dem falschen Passwort einloggen wollte, ob sich ein User an einem Hot-Spot angemeldet hat oder ob irgendwo ein LAN-Kabel aus einem Switch gezogen wurde.



Eine komplette Liste aller SNMP-Traps, die vom LANCOM unterstützt werden, finden Sie im Anhang dieses Referenz-Handbuchs ('SNMP-Traps' →Seite 311).

Das Routing dieser unterschiedlichen Netzwerke stößt dabei sehr schnell an seine Grenzen, wenn zwei oder mehrere Kunden gleiche Adresskreise verwenden. Wenn zusätzlich noch einige Kunden den gleichen Adressbereich nutzen wie der Dienstleister selbst, kommen weitere Adresskonflikte hinzu. In diesem Beispiel hat z.B. einer der Hot-Spots von Kunde C die gleiche Adresse wie das Gateway des Dienstleisters.

Für die Lösung dieser Adresskonflikte gibt es zwei verschiedene Varianten:

Loopback:
dezentrales
1:1-Mapping

- ▶ Bei der dezentralen Variante werden den zu überwachenden Geräten per 1:1-Mapping jeweils alternative IP-Adressen für die Kommunikation mit dem SNMP-Empfänger zugewiesen. Diese Adresse ist in der Fachsprache auch als "Loopback-Adresse" bekannt, die Methode wird entsprechend als "Loopback-Verfahren" bezeichnet.



Die Loopback-Adressen gelten jeweils nur für die Kommunikation mit bestimmten Gegenstellen auf den zugehörigen Verbindungen. Ein LANCOM ist damit nicht generell unter dieser IP-Adresse erreichbar.

Alternativ:
zentrales
N:N-Mapping

- ▶ Eleganter ist die Lösung des zentralen Mappings: statt jedes einzelne Gateway in den Filialnetzen zu konfigurieren, stellt der Administrator hier die Adressumsetzung im Gateway der Zentrale ein. Dabei werden automatisch auch alle "hinter" der Zentrale liegenden Subnetze mit den erforderlichen neuen IP-Adressen versorgt.

In diesem Beispiel wählt der Administrator des Dienstleisters für das Netz des Kunden B die zentrale Adressumsetzung auf 10.2.x.x, damit die beiden Netze mit eigentlich gleichen Adresskreisen für das Gateway des Dienstleisters wie zwei verschiedene Netz erscheinen.

Für die Kunden C und D wählt er die Adresskreise 192.168.2.x und 192.168.3.x, damit diese Netze sich in ihren Adressen von dem eigenen Netz des Dienstleisters unterscheiden.

Damit das Gateway des Dienstleisters die Netze der Kunden C und D ansprechen kann, richtet er auch für das eigene Netz eine Adressumsetzung auf 192.168.1.x ein.

7.7.2 Konfiguration

Einrichten der Adressumsetzung

Die Konfiguration des N:N-Mappings gelingt mit recht wenigen Informationen. Da ein LAN durchaus mit mehreren anderen Netzen per N:N gekoppelt werden kann, können für einen Quell-IP-Bereich bei verschiedenen Zielen auch unterschiedliche Adressumsetzungen gelten. In der NAT-Tabelle können maximal 64 Einträge vorgenommen werden, die folgende Informationen beinhalten:

- ▶ **Index:** Eindeutiger Index des Eintrags.
- ▶ **Quell-Adresse:** IP-Adresse des Rechners oder Netzes, das eine alternative IP-Adresse erhalten soll.
- ▶ **Quell-Maske:** Netzmaske des Quell-Bereiches.
- ▶ **Gegenstelle:** Name der Gegenstelle, über die das entfernte Netzwerk erreicht werden kann.
- ▶ **Neue Netz-Adresse:** IP-Adresse oder -Adressebereich, der für die Umsetzung verwendet werden soll.

Für die neue Netzadresse wird jeweils die gleiche Netzmaske verwendet, die auch schon die Quell-Adresse verwendet. Für die Zuordnung von Quell- und Mapping-Adresse gelten folgende Hinweise:

- ▶ Bei der Umsetzung von einzelnen Adressen können Quelle und Mapping beliebig zugeordnet werden. So kann z.B. dem Server im LAN mit der IP-Adresse 10.1.1.99 die Mapping-Adresse 192.168.1.88 zugewiesen werden.
- ▶ Bei der Umsetzung von ganzen Adressbereichen wird der rechnerbezogene Teil der IP-Adresse direkt übernommen und nur an den netzbezogenen Teil der Mapping-Adresse angehängt. Bei einer Zuweisung von 10.0.0.0/255.255.255.0 nach 192.168.1.0 wird also dem Server im LAN mit der IP-Adresse 10.1.1.99 zwangsweise die Mapping-Adresse 192.168.1.99 zugewiesen.



Der Adressbereich für die Umsetzung muss mindestens so groß sein wie der Quell-Adressbereich.



Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist ('Firewall/QoS-Aktivierung' →Seite 182)!

Zusätzliche Konfigurationshinweise

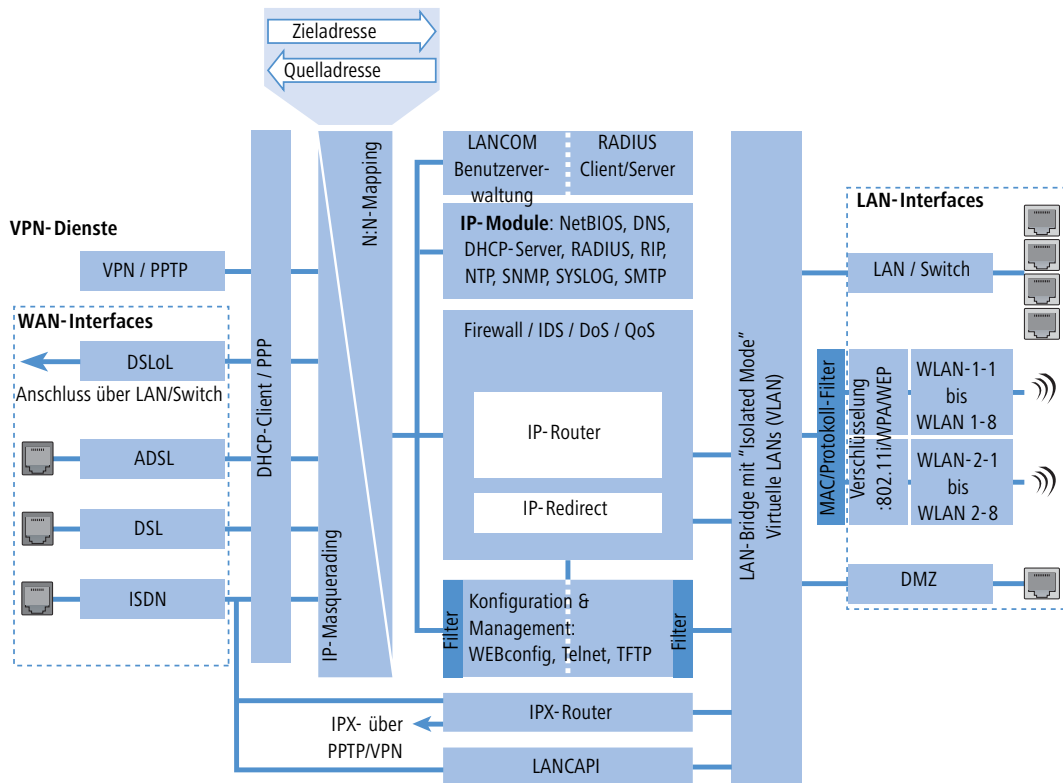
Mit dem Einrichten der Adressumleitung in der NAT-Tabelle werden die Netze und Rechner zunächst nur unter einer anderen Adresse im übergeordneten Netzverbund sichtbar. Für das einwandfreie Routing der Daten zwischen den Netzen sind aber noch einige weitere Einstellungen notwendig:

- ▶ Einträge in den Routing-Tabellen, damit die Pakete mit den neuen Adressen auch den Weg zum Ziel finden.

▷ N:N- Mapping

- ▶ DNS-Forwarding-Einträge, damit die Anfragen nach bestimmten Geräten in den jeweils anderen Netzen in die gemappten IP-Adressen aufgelöst werden können ('DNS-Forwarding' →Seite 418).
- ▶ Die Regeln der Firewalls in den Gateways müssen so angepasst werden, dass ggf. auch der Verbindungsaufbau von außen von den zulässigen Stationen bzw. Netzwerken her erlaubt ist.
- ▶ VPN-Regeln für Loopback-Adressen, damit die neu zugewiesenen IP-Adressen auch durch die entsprechenden VPN-Tunnel übertragen werden können.

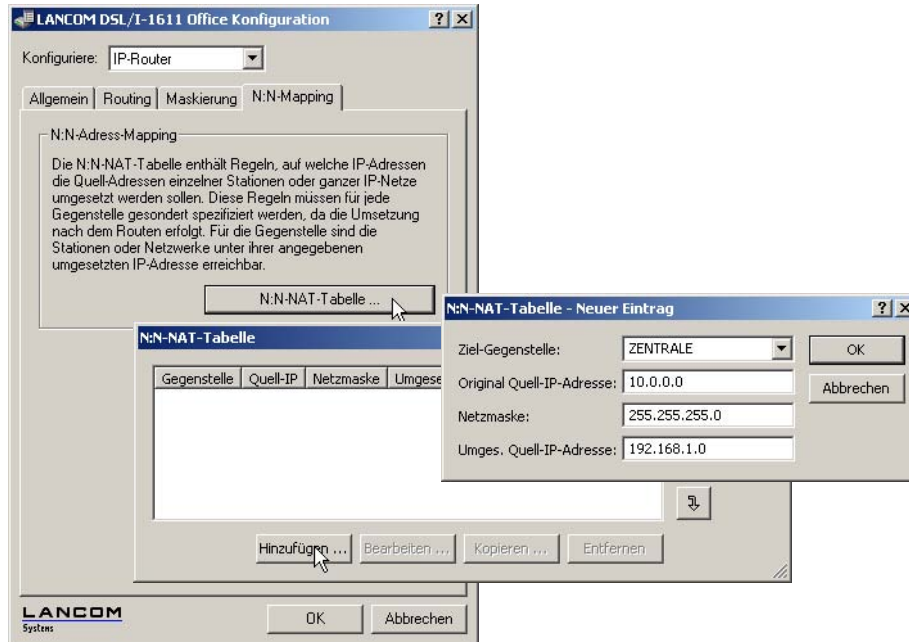
! Die Umsetzung der IP-Adressen findet im LANCOM zwischen Firewall und IP-Router auf der einen Seite und dem VPN-Modul auf der anderen Seite statt. Alle Regeln, die sich auf das eigene lokale Netz beziehen, verwenden daher die "ungemappten", originalen Adressen. Die Einträge für das entfernte Netz nutzen also die "gemappten" Adressen der Gegenseite, die auf der VPN-Strecke gültig sind.



Konfiguration mit den verschiedenen Tools

LANconfig

Unter LANconfig stellen Sie die Adressumsetzung im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'N:N-Mapping' ein:



WEBconfig,
Telnet

Unter WEBconfig und Telnet finden Sie die NAT-Tabelle zur Konfiguration des N:N-Mappings an folgenden Stellen des Menübaums:

Konfigurationstool	Aufruf
WEBconfig	Expertenkonfiguration ► Setup ► IP-Router ► NAT-Tabelle
Terminal/Telnet	Setup / IP-Router / NAT-Tabelle

Die NAT-Tabelle präsentiert sich unter WEBconfig beim Anlegen eines neuen Eintrags folgendermaßen:

▷ Verbindungsaufbau mit PPP

The screenshot shows the 'Experten-Konfiguration' (Expert Configuration) window. Under 'Setup' > 'IP-Router-Modul', the 'NAT-Tabelle' (NAT Table) is displayed. It contains the following fields:

Idx.	<input type="text" value="1"/>
Quell-Adresse	<input type="text" value="10.0.0.0"/>
Quell-Maske	<input type="text" value="255.255.255.0"/>
Ziel-Gegenstelle	<input type="text" value="FIRMA_B"/>
Neue-Netz-Adr.	<input type="text" value="192.168.1.0"/>

At the bottom, there are two buttons: 'Setzen' (Set) and 'Zurücksetzen' (Reset).

7.8 Verbindungsaufbau mit PPP

Router von LANCOM Systems unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

7.8.1 Das Protokoll

Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle (auch ISDN, DSL u.ä.) entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- ▶ Passwortschutz nach PAP, CHAP oder MS-CHAP
- ▶ Rückruf-Funktionen
- ▶ Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z.B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z.B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- ▶ Aushandeln von Verbindungsparametern wie z.B. der MTU (Maximum Transmission Unit, 'Manuelle Definition der MTU' →Seite 166).
- ▶ Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- ▶ Bündelung von mehreren ISDN- oder DSL-Kanälen (Multilink-PPP bzw. Multilink-PPPoE)

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungssoftware unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzustellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (z.B. LCP, IPCP, CCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- ▶ aus Kompatibilitätsgründen z.B. bei Kommunikation mit Fremdroutern
- ▶ Remote Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern
- ▶ Internet-Access (mit der Übermittlung von Adressen)

Das im LANCOM implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

▶ Establish-Phase

Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.

Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.

▶ Authenticate-Phase

Falls notwendig, werden danach die Passwörter ausgetauscht. Bei Authentifizierung nach PAP wird das Passwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Passwort periodisch in einstellbaren Abständen gesendet.

Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.

▶ Network-Phase

Im LANCOM sind die Protokolle IPCP und IPXCP implementiert.

Nach erfolgreicher Übertragung des Passwortes können die Netzwerk-Layer IPCP und/oder IPXCP aufgebaut werden.

Ist die Verhandlung der Parameter für mindestens eines der Netzwerk-Layer erfolgreich verlaufen, können von den Router-Modulen IP- und/oder IPX-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

▶ Terminate-Phase

▷ Verbindungsaufbau mit PPP

In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

Die PPP-Verhandlung im LANCOM

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

7.8.2 Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z.B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Passwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Streikt beispielsweise die Highspeed-Verbindung, kann als Backup eine vorhandene ISDN-Schnittstelle den Weg ins Internet bahnen.



Beim Remote Access von einzelnen Arbeitsplatzrechnern mit Windows-Betriebssystem empfehlen wir, die regelmäßigen LCP-Anfragen des LANCOM auszuschalten, weil diese Betriebssysteme die LCP-Echo-Requests nicht beantworten und die Verbindung dadurch abgebaut würde.



Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

7.8.3 Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z.B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann der LANCOM ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

Diese Art der Adresszuweisung wird während der PPP-Verhandlung durchgeführt und nur für Verbindungen über das WAN eingesetzt. Die Zuweisung von Adressen mittels DHCP wird dagegen (normalerweise) innerhalb eines lokalen Netzwerks verwendet.



Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn der LANCOM die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

Beispiele

▶ Remote Access

Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim LANCOM anmelden muss.

Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (Domain Name Server und NetBIOS Name Server) inkl. des Backup-Servers aus den Einträgen im TCP/IP-Modul übermittelt.

Damit das Ganze funktioniert, muss die Gegenstelle natürlich auch so eingestellt sein, dass sie die IP-Adresse und die Namensserver vom LANCOM bezieht. Das geschieht z.B. im DFÜ-Netzwerk von Windows durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

▶ Internet-Zugang

Wird über den LANCOM der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen der LANCOM selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen lässt. Neben der IP-Adresse erhält der LANCOM während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

Im lokalen Netz ist der LANCOM nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z.B. den DNS-Server erreichen.

▷ Verbindungsaufbau mit PPP

Die zugewiesenen Adressen schauen sich Windows-Anwender per LANmonitor an. Neben dem Namen der verbundenen Gegenstelle finden Sie hier die aktuelle IP-Adresse sowie die Adressen von DNS- und NBNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.

7.8.4 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Konfigurationstool	Liste
LANconfig	Kommunikation ► Protokolle ► PPP-Liste
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► PPP
Terminal/Telnet	<code>cd /Setup/WAN</code> <code>set PPP [...]</code>

Die PPP-Liste kann bis zu 64 Einträge aufnehmen und die folgende Werte enthalten:

In dieser Spalte der PPP-Liste tragen Sie folgende Werte ein:
Gegenstelle (Gerätename)	Name der Gegenstelle, mit dem sich diese bei Ihrem Router anmeldet
Benutzername (Username)	Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Geräte-name Ihres Routers verwendet.
Passwort	Passwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert). * in der Liste zeigt an, dass ein Eintrag vorhanden ist.
Überprüfung der Gegenstelle (Authentifizierung)	Verfahren zur Sicherung der PPP-Verbindung ('PAP', 'CHAP' oder 'keine'). Ihr eigener Router verlangt von der Gegenstelle die Einhaltung dieses Verfahrens! Nicht etwa umgekehrt. Daher bietet sich die Sicherung nach 'PAP', 'CHAP' nicht an bei Verbindungen zu Internet Service Providern, die uns vielleicht kein Passwort übermitteln wollen. Für solche Verbindungen wählen Sie 'keine' Sicherung.
Zeit	Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe folgender Abschnitt). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z.B. 2 für 20 Sekunden). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!
Wiederholungen (Wdh)	Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die Anzahl der „Configure Requests“, die der Router maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.
Conf, Fail, Term	Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über LANconfig, SNMP oder TFTP verändert werden!

7.9 DSL-Verbindungsaufbau mit PPTP

Einige DSL-Anbieter ermöglichen die Einwahl nicht über PPPoE, sondern über PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). Bei PPTP handelt es sich um eine Protokoll-Erweiterung von PPP, die vorrangig von Microsoft entwickelt wurde.

PPTP ermöglicht es, „Tunnel“ über IP-Netze zu einer Gegenstelle aufzubauen. Unter einem Tunnel versteht man eine logisch abgeschirmte Verbindung, die die übertragenen Daten vor dem unbefugten Zugriff Dritter schützen soll. Dazu wird der Verschlüsselungsalgorithmus RC4 eingesetzt.

Konfiguration von PPTP

Im LANCOM werden alle notwendigen PPTP-Parameter vom Internet-Zugangs-Assistenten abgefragt, sobald der Internet-Zugang über PPTP ausgewählt wird. Zusätzlich zu den Eingaben, die auch beim normalen PPPoE-Zugang abgefragt werden, ist dabei nur die IP-Adresse des PPTP-Gateways anzugeben. Beim PPTP-Gateway handelt es sich zumeist um das DSL-Modem. Genauere Informationen stellt Ihnen Ihr DSL-Anbieter zur Verfügung.

Änderungen an der Konfiguration werden in der PPTP-Liste vorgenommen:

Konfigurationstool	Liste
LANconfig	Kommunikation ► Protokolle ► PPTP-Liste
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► PPTP-Liste
Terminal/Telnet	<code>cd /Setup/WAN</code> <code>set PPTP-Liste [...]</code>

Die PPTP-Konfiguration besteht aus drei Parametern:

- 'Gegenstelle' – Die Bezeichnung aus der Liste der DSL-Breitband-Gegenstellen.
- 'IP-Adresse' – IP-Adresse des PPTP-Gateways, zumeist die Adresse des DSL-Modems
- 'Port' – IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

7.10 Dauerverbindung für Flatrates – Keep-alive

Als Flatrates bezeichnet man pauschale Verbindungsstarife, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue Mails sollen direkt am PC gemeldet werden, der Heimarbeitsplatz soll kontinuierlich mit dem Firmennetzwerk verbunden sein und man möchte für Freunde und Kollegen über Internet Messenger Dienste (ICQ und ähnliche) pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrechterhalten werden.

Beim LANCOM sorgt das Keep-alive-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

▷ Rückruf-Funktionen

Konfiguration des Keep-alive-Verfahrens

Das Keep-alive-Verfahren wird in der Gegenstellenliste konfiguriert.

Wird die Haltezeit auf 0 Sekunden gesetzt, so wird die Verbindung nicht aktiv vom LANCOM beendet. Der automatische Abbau von Verbindungen, über die längere Zeit keine Daten mehr übertragen wurden, wird mit einer Haltezeit von 0 Sekunden also deaktiviert. Durch die Gegenseite unterbrochene Verbindungen werden in dieser Einstellung allerdings nicht automatisch wiederhergestellt.

Bei einer Haltezeit von 9999 Sekunden wird die Verbindung nach jeder Trennung immer automatisch wieder neu aufgebaut. Ebenso wird die Verbindung nach dem Booten des Gerätes automatisch wieder aufgebaut ('auto reconnect').

7.11 Rückruf-Funktionen

LANCOM mit ISDN-Schnittstelle unterstützen einen automatischen Rückruf.

Neben dem Rückruf über den D-Kanal wird auch das von Microsoft spezifizierte CBCP (**C**allback **C**ontrol **P**rotocol) sowie der Rückruf über PPP nach RFC 1570 (PPP LCP Extensions) angeboten. Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von LANCOM Systems entwickeltes Verfahren. PCs mit Windows-Betriebssystem können nur über das CBCP zurückgerufen werden.

7.11.1 Rückruf nach Microsoft CBCP

Das Microsoft CBCP erlaubt verschiedene Arten, die Rückrufnummer zu bestimmen:

- ▶ Der Angerufene ruft nicht zurück.
- ▶ Der Angerufene erlaubt es dem Anrufer, die Rückrufnummer selbst anzugeben.
- ▶ Der Angerufene kennt die Rückrufnummer und ruft auch **nur** diese zurück.

Über das CBCP ist es möglich, von einem Rechner mit einem Windows-Betriebssystem eine Verbindung zum LANCOM aufzunehmen und sich von diesem zurückrufen zu lassen. Die drei möglichen Einstellungen werden über den Rückruf-Eintrag sowie den Rufnummern-Eintrag in der Gegenstellenliste ausgewählt.

The screenshot shows a dialog box titled "Gegenstellen (ISDN/seriell) - Neuer Eintrag". It contains the following fields and options:

- Name: MAIN
- Rufnummer: 123456
- Haltezeit: 20 Sekunden
- Haltezeit für Bündelung: 20 Sekunden
- Layername: PPPHDLC
- Automatischer Rückruf:
 - Keinen Rückruf durchführen
 - Die Gegenstelle zurückrufen
 - Die Gegenstelle zurückrufen (schnelles Verfahren)
 - Die Gegenstelle nach Überprüfung des Namens zurückrufen
 - Den Rückruf der Gegenstelle erwarten

Buttons: OK, Abbrechen

Keinen Rückruf durchführen

Für diese Einstellung muss der Rückruf-Eintrag bei der Konfiguration über WEBconfig oder in der Konsole den Wert 'Aus' haben.

Rückrufnummer vom Anrufer bestimmt

Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in WEBconfig oder in der Konsole den Wert 'Name' haben). In der Gegenstellenliste darf **keine** Rufnummer angegeben sein.

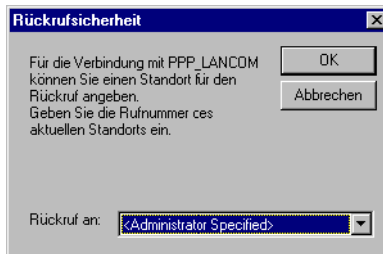
Nach der Authentifizierung erscheint beim Anrufer in Windows ein Eingabefenster, das ihn nach der ISDN-Rufnummer des PC fragt.

Rückrufnummer im LANCOM bestimmt

Für diese Einstellung muss der Rückruf-Eintrag auf 'Die Gegenstelle nach Überprüfung des Namens zurückrufen' stehen (bzw. in WEBconfig oder in der Konsole auf den Wert 'Name' gesetzt sein). In der Gegenstellenliste muss **eine** Rufnummer angegeben sein.

Einige Windows-Versionen (insbesondere Windows 98) fordern den Benutzer mit einem Eingabefenster auf, den Rückruf an die im LANCOM hinterlegte Rufnummer ('Administrator Specified') zu bestätigen. Andere Windows-Versionen informieren den Benutzer nur darüber, dass der PC auf den Rückruf vom LANCOM wartet.

▷ Rückruf- Funktionen



Der Rückruf an einen Windows-Rechner erfolgt ca. 15 Sekunden, nachdem die erste Verbindung abgebaut wurde. Diese Zeit kann nicht verkürzt werden, da sie von Windows vorgegeben wird.

7.11.2 Schneller Rückruf mit dem LANCOM-Verfahren

Sollen zwei LANCOM miteinander kommunizieren, wobei der eine zurückgerufen wird, bietet sich der schnelle Rückruf über das LANCOM-spezifische Verfahren an.

- ▶ Der Anrufer, der gerne zurückgerufen werden möchte, stellt in der Gegenstellenliste 'Den Rückruf der Gegenstelle erwarten' ein ('Looser' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet).
- ▶ Der Rückrufer wählt 'Die Gegenstelle zurückrufen (schnelles Verfahren)' in der Gegenstellenliste und stellt die Rufnummer ein ('fast' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet).



Für den schnellen Rückruf nach LANCOM-Verfahren muss die Nummernliste für die Rufannahme auf beiden Seiten gepflegt sein.

7.11.3 Rückruf nach RFC 1570 (PPP LCP Extensions)

Der Rückruf nach 1570 ist das Standardverfahren für den Rückruf von Routern anderer Hersteller. Diese Protokollerweiterung beschreibt fünf Möglichkeiten, einen Rückruf anzufordern. Alle Versionen werden vom LANCOM akzeptiert. Es wird jedoch bei allen Varianten gleich verfahren:

Der LANCOM baut nach der Authentifizierung der Gegenstelle die Verbindung ab und ruft diese dann einige Sekunden später zurück.

Konfiguration

Für den Rückruf nach PPP wählen Sie in LANconfig die Option 'Die Gegenstelle zurückrufen' bzw. 'Auto' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet.



Für den Rückruf nach PPP muss die Nummernliste für die Rufannahme im LANCOM gepflegt sein.

7.11.4 Konfiguration der Rückruf-Funktion im Überblick

In der Gegenstellenliste stehen unter WEBconfig und Terminalprogramm/Telnet für den Rückruf-Eintrag folgende Optionen zur Verfügung:

Mit diesem Eintrag stellen Sie den Rückruf so ein:
'Aus'	Es wird nicht zurückgerufen.
'Auto' (nicht bei Windows-Betriebssystemen, s. u.)	Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.
'Name'	Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z.B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen geringe Gebühren an.
'fast'	Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d.h., der LANCOM sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.
'Looser'	Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D.h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'LANCOM Systems' eingestellt sein muss.



Die Einstellung 'Name' bietet die höchste Sicherheit, wenn sowohl ein Eintrag in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'LANCOM' ermöglicht die schnellste Rückrufmethode zwischen zwei LANCOM Systems-Routern.



Bei Windows-Gegenstellen **muss** die Einstellung 'Name' gewählt werden.

7.12 ISDN-Kanalbündelung mit MLPPP

Wenn Sie eine ISDN-Verbindung zu einer PPP-fähigen Gegenstelle aufbauen, können Sie Ihren Daten Beine machen: Sie können die Daten komprimieren und/oder mehrere B-Kanäle zur Übertragung verwenden (Kanalbündelung).

Die Verbindung mit Kanalbündelung unterscheidet sich von „normalen“ Verbindungen dadurch, dass nicht nur ein, sondern mehrere B-Kanäle parallel für die Übertragung der Daten verwendet werden.

▷ ISDN- Kanalbündelung mit MLPPP

Für die Kanalbündelung wird dabei MLPPP (**M**ultilink **PPP**) verwendet. Dieses Verfahren steht natürlich nur zur Verfügung, wenn PPP als B-Kanal-Protokoll verwendet wird. MLPPP bietet sich z.B. an für den Internet-Zugang über Provider, die bei Ihren Einwahlknoten ebenfalls MLPPP-fähige Gegenstellen betreiben.



Auch für DSL-Kanäle kann eine Bündelung über MLPPPoE eingerichtet werden ('DSL-Kanalbündelung (Multilink-PPPoE – MLPPPoE)' →Seite 130).

Zwei Methoden der Kanalbündelung

▶ Statische Kanalbündelung

Wenn eine Verbindung mit statischer Kanalbündelung aufgebaut wird, versucht der LANCOM nach dem ersten B-Kanal sofort, auch den zweiten B-Kanal aufzubauen. Gelingt dies nicht, weil z.B. dieser Kanal schon durch ein anderes Gerät oder durch eine andere Verbindung im LANCOM besetzt ist, wird dieser Aufbauversuch automatisch und regelmäßig solange wiederholt, bis auch der zweite Kanal für diese Verbindung zur Verfügung steht.

▶ Dynamische Kanalbündelung

Bei einer Verbindung mit dynamischer Kanalbündelung baut der LANCOM zunächst nur einen B-Kanal auf und beginnt mit der Datenübertragung. Wenn er dann während der Verbindung feststellt, dass der Durchsatz eine Weile über einem bestimmten Schwellwert liegt, versucht er den zweiten Kanal dazuzunehmen.

Wenn der zweite Kanal aufgebaut ist und der Datendurchsatz wieder unter den Grenzwert zurückgeht, wartet der LANCOM noch die eingestellte B2-Haltezeit ab und schließt den Kanal dann automatisch wieder. Dabei werden die begonnenen Gebühreneinheiten ausgenutzt, sofern die Gebühreninformationen während der Verbindung übermittelt werden. Der LANCOM benutzt den zweiten B-Kanal also nur, wenn und solange er ihn auch wirklich braucht!

So stellen Sie die Kanalbündelung ein

Die Konfiguration der Kanalbündelung für eine Verbindung setzt sich aus drei Einstellungen zusammen:

- ① Wählen für die Gegenstelle einen Kommunikations-Layer aus der Layer-Liste aus, der in den Layer-2-Optionen die Bündelung aktiviert hat. Wählen Sie unter folgenden Layer-2-Optionen:
 - ▷ **compr.** nach dem LZS-Datenkompressionsverfahren (Stac) reduziert das Datenvolumen, wenn die Daten nicht schon vorher komprimiert waren. Dieses Verfahren wird auch von Routern anderer Hersteller und von ISDN-Adaptern unter Windows-Betriebssystemen unterstützt.
 - ▷ **buendeln** verwendet zwei B-Kanäle für eine Verbindung.
 - ▷ **bnd+compr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.
- ② Erstellen Sie nun einen neuen Eintrag in der Gegenstellenliste. Achten Sie dabei auf die Haltezeiten für die Verbindung. Beachten Sie folgende Regeln:

▷ *Betrieb eines Modems an der seriellen Schnittstelle*

- ▷ Die B1-Haltezeit sollte je nach Anwendungsfall so groß gewählt werden, dass die Verbindung nicht durch das kurzzeitige Ausbleiben von Paketen zu früh abgebaut wird. Erfahrungsgemäß sind Werte zwischen 60 und 180 Sekunden für den Beginn eine gute Basis, die man im Betrieb dann weiter anpassen kann.
 - ▷ Die B2-Haltezeit entscheidet darüber, ob es sich um eine statische oder dynamische Kanalbündelung handelt (siehe oben). Mit einer B2-Haltezeit von '0' oder '9999' wird die Bündelung statisch, mit Werten dazwischen schaffen Sie die Möglichkeit der dynamischen Kanalbündelung. Die B2-Haltezeit definiert, wie lange der Datendurchsatz unter der Schwelle für die dynamische Kanalbündelung liegen darf, ohne dass der zweite B-Kanal automatisch abgebaut wird.
- ③ Legen Sie in der Router-Interface-Liste mit dem Eintrag für die Y-Verbindung fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

WEBconfig	Experten-Konfiguration ▶ Setup ▶ WAN ▶ Router-Interface-Liste
Terminal/Telnet	cd /Setup/WAN set Router-Interface-Liste [...]

- ▷ Y-Verbindung **Ein**: Der Router unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).
- ▷ Y-Verbindung **Aus**: Der Router hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.



Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

7.13 Betrieb eines Modems an der seriellen Schnittstelle



Die Ausführungen dieses Abschnitts beziehen sich nur auf Geräte mit serieller Konfigurationsschnittstelle.

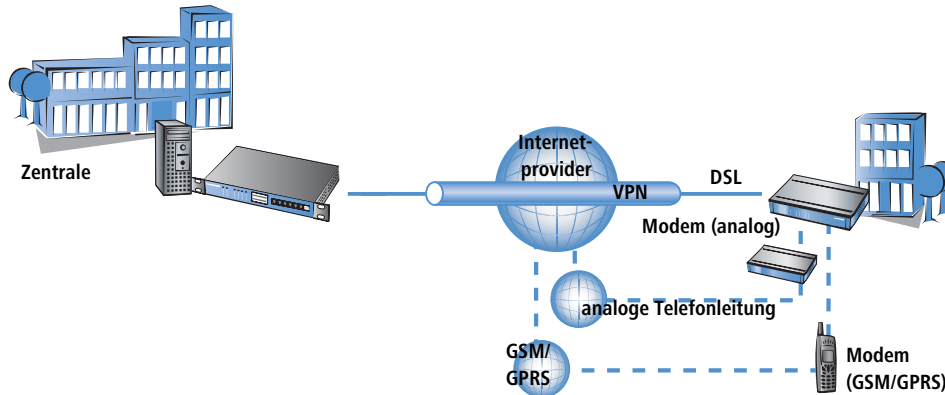
7.13.1 Einleitung

International sind analoge Leitungen auch im Geschäftskundenbereich ähnlich häufig anzutreffen wie das in Deutschland dominierende ISDN. Der Betrieb von internationalen Netzwerken stellt daher besondere Anforderungen an Fernwartungsmöglichkeiten und Hochverfügbarkeit der eingesetzten Gateways und erfordert somit andere Schnittstellen als die in Deutschland in vielen Routern integrierte ISDN-Schnittstelle. Neben den normalen analogen Telefonleitungen stellt in machen Fällen das Mobilfunknetz über GSM oder GPRS die einzige Möglichkeit dar, eine Fernwartung auch ohne die Breitbandzugänge oder andere kabelgebundene Verbindungen sicherzustellen.

▷ *Betrieb eines Modems an der seriellen Schnittstelle*

Um diesen Anforderungen gerecht zu werden, können die meisten LANCOM-Modelle mit serieller Schnittstelle um ein zusätzliches WAN-Interface über analoge Modems oder GSM bzw. GPRS erweitert werden. Mit einem geeignetem Modem und dem LANCOM Modem Adapter Kit stehen die folgenden Funktionen zur Verfügung:

- ▶ Internet-Zugang über Modem-Verbindung mit Nutzung aller Routerfunktionen wie Firewall, automatischer Verbindungsauf- und -Abbau etc.
- ▶ Fernwartung (z.B. Einwahl auf internationale Standorte)
- ▶ Backup-Verbindung (z.B. Hochverfügbarkeit durch GSM/GPRS Modem-Verbindung)



7.13.2 Systemvoraussetzungen

Für die Einrichtung einer zusätzlichen WAN-Schnittstelle über den seriellen Anschluss benötigen Sie:

- ▶ LANCOM mit serieller Konfigurationsschnittstelle aus der folgenden Liste:
 - ▷ LANCOM L-54g Wireless, LANCOM L-54ag Wireless und LANCOM IAP-54 Wireless
 - ▷ LANCOM 1511 Wireless DSL, LANCOM 1521 Wireless ADSL, LANCOM 1811 Wireless DSL und LANCOM 1821 Wireless ADSL
 - ▷ LANCOM 1711 VPN
 - ▷ LANCOM 8011 VPN
 - ▷ LANCOM 7111 VPN
 - ▷ LANCOM DSL/I-1611 Office
 - ▷ LANCOM DSL/I-10+
 - ▷ LANCOM 800+
 - ▷ LANCOM 821 ADSL/ISDN
 - ▷ LANCOM 1621 ADSL/ISDN
- ▶ LANconfig, alternativ Webbrowser oder Telnet zur Konfiguration
- ▶ serielles Konfigurationskabel (im Lieferumfang des Gerätes enthalten)

▷ *Betrieb eines Modems an der seriellen Schnittstelle*

- ▶ Externes Modem mit Standard AT-Kommandosatz (Hayes-kompatibel) und D-Sub9 oder D-Sub25 Anschluss
- ▶ LANCOM Modem Adapter Kit zur Anschluss des Modems über das serielle Konfigurationskabel

7.13.3 Installation

Zur Installation wird das Modem einfach über den LANCOM Modem Adapter Kit mit der seriellen Konfigurations-schnittstelle des LANCOM verbunden.



Bitte verwenden Sie ausschließlich das originale LANCOM Modem Adapter Kit! Die Kontaktbelegung beim LANCOM Modem Adapter Kit unterscheidet sich von anderen handelsüblichen Adapters wie z.B. dem „Null-modem-Kabel“. Der Einsatz von nicht geeignetem Zubehör kann zu ernsthaften Schäden an Ihrem LANCOM oder Ihrem Modem führen. Weitere Details entnehmen Sie bitte der 'Kontaktbelegung des LANCOM Modem Adapter Kits' →Seite 166.

7.13.4 Einstellen der seriellen Schnittstelle auf Modem-Betrieb

Für den Betrieb der seriellen Schnittstelle können Sie die Betriebsart und die Bitrate einstellen.

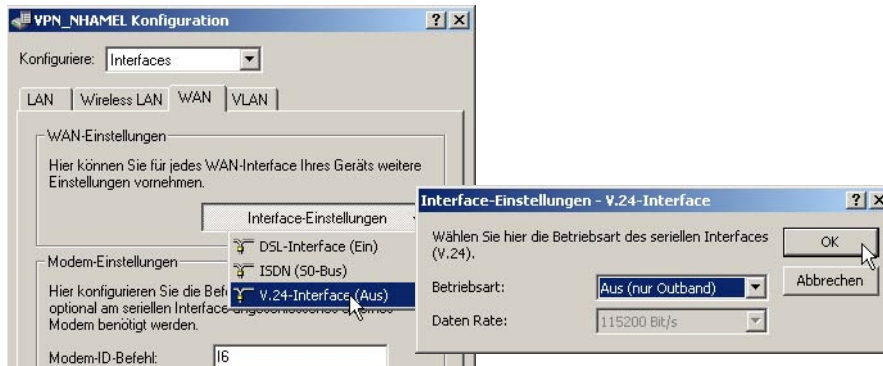
- ▶ Betriebsart [Default: Outband]
 - ▷ Outband: In dieser Betriebsart wird die serielle Schnittstelle nur zur Konfiguration über ein Terminalprogramm verwendet.
 - ▷ Modem: In der Einstellung als 'Modem' versucht das Gerät, an der seriellen Schnittstelle ein Modem zu erkennen. Bei Erfolg kann das Modem als zusätzliche WAN-Schnittstelle verwendet werden. Wird jedoch ein angeschlossener Rechner mit Terminalprogramm an der seriellen Schnittstelle festgestellt, schaltet das Gerät die Schnittstelle automatisch in den Modus zur Outband-Konfiguration um.
 - ▷ Interlink: Direktverbindung zwischen zwei LANCOM-Geräten
- ▶ Bitrate [Default: 115.200 Bit/s.]

Stellen Sie hier die Bitrate ein, die Ihr Modem maximal unterstützt. LANCOM-Geräte unterstützen an der seriellen Schnittstelle von 19.200 Bit/s, 38.400 Bit/s, 57.600 Bit/s bis maximal 115.200 Bit/s.

Konfiguration
mit LANconfig

Die Einstellungen für die serielle Schnittstelle als WAN-Schnittstelle finden Sie in LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN'. Wählen Sie hier die V.24-Schnittstelle aus.

▷ *Betrieb eines Modems an der seriellen Schnittstelle*



Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Einstellungen für die serielle Schnittstelle auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► V.24-Schnittstelle
Terminal/Telnet	Setup/Schnittstellen/V.24-Schnittstelle



Solange das LANCOM auf Modem-Betrieb eingestellt ist, werden bei einer Verbindung mit einem Terminalprogramm über die serielle Schnittstelle die AT-Kommandos angezeigt, mit denen das LANCOM ein angeschlossenes Modem erkennen will. Drücken Sie im Terminal einige Male die Return-Taste, um die Modemerkenkung zu unterbrechen und die Konfigurationssitzung zu starten.

7.13.5 Konfiguration der Modem-Parameter

Für den Betrieb eines Modems an der seriellen Schnittstelle müssen folgende Parameter eingestellt werden:

- Modem-ID-Befehl [Default: AT16]
- Reset-String [Default: AT&F]
- Initialisierungs-String [Default: ATL0M1X1S0=0]
 - ▷ L0: Lautsprecher leise
 - ▷ M1: Lautsprecher an während der Aufbauphase
 - ▷ X1: Betrieb an einer Nebenstelle
 - ▷ S0=0: Rufannahme ausschalten
- Modem-Echo ausschalten [Default: ATE0]
- AT-Prüfzyklus-Zeit [Default: 1 in Sekunden]
- AT-Prüfzyklus-Anzahl [Default: 5]
- Rufzahl zur Rufannahme [Default: 1]

▷ *Betrieb eines Modems an der seriellen Schnittstelle*

- ▶ Rufannahme-Initialisierungs-Befehl
- ▶ Rufannahme -Befehl [Default: ATA]
- ▶ Wähl-Initialisierungs-Befehl
- ▶ Wähl-Befehl [Default: ATDT]
- ▶ Escapesequence zum Beenden der Datenphase bzw. zur Rückkehr in die Kommandophase [Default: +++]
- ▶ Wartezeit nach Escapesequence [Default: 1000 in Millisekunden]
- ▶ Verbindung trennen: Zeichenfolge, die das Modem in der Datenphase als Anweisung zum Auflegen interpretiert. [Default: ATH]



Die Modem-Parameter sind mit Werten vorbelegt, die für die meisten Modem-Typen passen – Änderungen sind daher in der Regel nicht erforderlich. Informieren Sie sich in der Dokumentation zu Ihrem Modem über evtl. abweichende Einstellungen.

GRPS-Backup-Verbindung einrichten

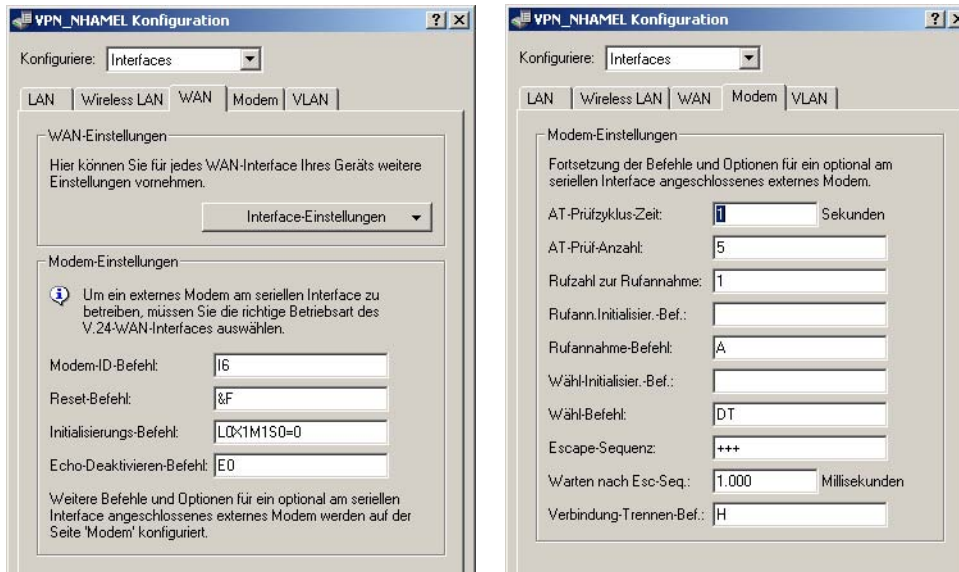
Wenn Sie für die Verbindung über die serielle Schnittstelle ein GRPS-fähiges Modem einsetzen, benötigen Sie den APN-Namen und die Einwahlnummer. Für T-Mobile und Vodafone ergeben sich dabei folgende Initstrings in der Konfiguration:

- ▶ T-Mobile
 - ▷ Initstring: L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"
 - ▷ Anwahlnummer : *99#
- ▶ Vodafone
 - ▷ Initstring: L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"
 - ▷ Anwahlnummer : *99# oder *99***1#

Konfiguration
mit LANconfig

Die Modem-Parameter finden Sie in LANconfig im Konfigurationsbereich 'Interfaces' auf den Registerkarten 'WAN' und 'Modem'.

▷ *Betrieb eines Modems an der seriellen Schnittstelle*



Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Modem-Parameter auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► Modem-Parameter
Terminal/Telnet	Setup/Schnittstellen/Modem-Parameter

Eingabe von Sonderzeichen an der Konsole

Die GPRS-Einwahl erfordert es, Initialisierungsstrings mit Anführungszeichen und Gleichheitszeichen eingeben zu können. Bestimmte Sonderzeichen können durch voranstellen eines Backslash entsprechend markiert werden:

- ▶ *
- ▶ "
- ▶ =
- ▶ Leerzeichen
- ▶ **Beispiel:** +cgdcont=1,\"IP\", \"internet.t-d1.de\"

Alternativ kann die gesamte Befehlssequenz in Anführungszeichen eingeschlossen werden. Dabei müssen den inneren Anführungszeichen innerhalb der umgebenden Anführungszeichen auch Backslashes vorangestellt werden.

- ▶ **Beispiel:** "+cgdcont=1,\"IP\", \"internet.t-d1.de\""

7.13.6 Direkte Eingabe von AT-Befehlen

Mit dem Befehl

- ▶ `sendserial „AT...“`

können Sie bei einer aktiven Telnet-Verbindung zu einem LANCOM mit angeschlossenem Modem eine Zeichenkette direkt an das Modem übertragen. Mit dieser Funktion können Sie z.B. beliebige AT-Befehle auf dem Modem ausführen.



Das Senden von AT-Befehlen ist nur möglich, wenn sich das Modem im internen Zustand 'idle' oder 'Modem bereit' befindet. Die Rückmeldungen sind im seriellen Trace ('Trace-Ausgaben' →Seite 163) zu finden.

7.13.7 Statistik

Die Statistiken über die Aktivitäten auf der seriellen Schnittstelle finden Sie beim Zugang über Terminalprogramm oder Telnet unter:

Status/Modem-Status

Die Statistik zeigt den erkannten Modemtyp an und den letzten Verbindungszustand des angeschlossenen Modems, z.B. die Übertragungsrate, den verwendeten Übertragungsstandard oder die eingesetzte Fehlererkennung.

Die Statistik zeigt die folgenden Zustände:

- ▶ den Typ des angeschlossenen Modems
- ▶ den Status der letzten Verbindung, z.B. die Datenübertragungsrate, das verwendete Protokoll oder die verwendete Fehlererkennungsmethode
- ▶ den internen Zustand des Modems, z.B.:
 - ▷ Geräteerkennung
 - ▷ Schnittstelle ausgeschaltet
 - ▷ Modeminitialisierung
 - ▷ Modem bereit
 - ▷ Verbindungsaufbau
 - ▷ Modem im Übertragungsmodus

Diese Meldung sind hilfreich für die Fehlersuche.

7.13.8 Trace-Ausgaben

Mit dem Befehl

- ▶ `trace + serial`

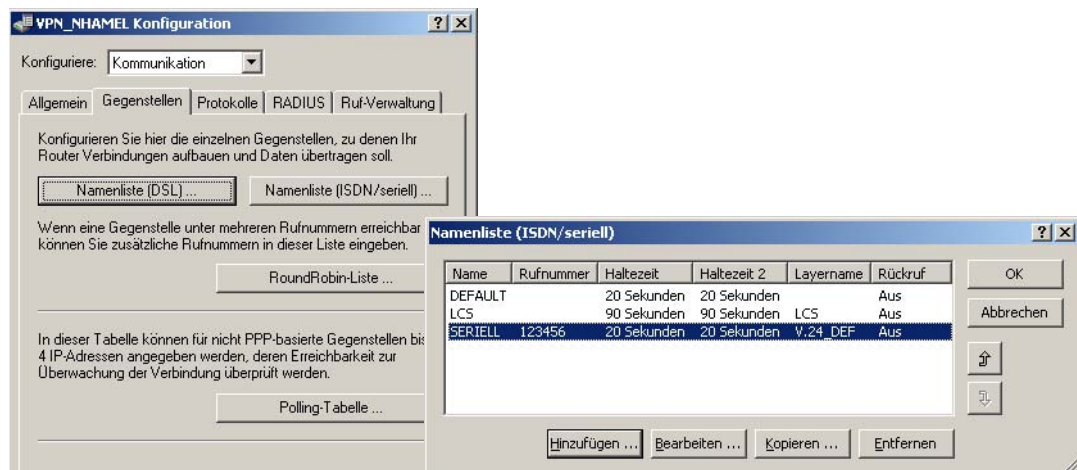
können Sie bei einer aktiven Telnet-Verbindung zu einem LANCOM mit angeschlossenem Modem die Traceausgabe für die serielle Schnittstelle starten. Die Ausgabe zeigt alle Meldungen an, die bis zum Aufbau der Datenübertragung zwischen dem Modem und dem LANCOM ausgetauscht werden.

▷ *Betrieb eines Modems an der seriellen Schnittstelle*

7.13.9 Konfiguration von Gegenstellen für V.24-WAN-Schnittstellen

Um eine Verbindung zu einer Gegenstelle über das an der seriellen Schnittstelle angeschlossene Modem aufzubauen, muss ein entsprechender Eintrag in der Gegenstellenliste (ISDN/seriell) erstellt werden. Die Gegenstellenliste (ISDN/seriell) enthält die folgenden Informationen:

- ▶ Name: Name der Gegenstelle
- ▶ Rufnummer: Rufnummer, über die die Gegenstelle erreicht werden kann. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen.
- ▶ Haltezeit: Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch getrennt. Eine Haltezeit mit dem Wert „9999“ bedeutet, dass die Verbindung permanent offen gehalten wird. Bei einer Trennung wird sie sofort wieder aktiv aufgebaut. Dieses Verhalten wird auch als **Keep-Alive** bezeichnet.
- ▶ 2. Haltezeit: Wird ignoriert.
- ▶ Layername: Für die Verbindung über die serielle WAN-Schnittstelle wird der Layer 'V.24_DEF' ausgewählt. Der Layer ist voreingestellt und muss nicht weiter konfiguriert werden. Der Layer 'V.24_DEF' verwendet folgende Einstellungen:
 - ▷ Encapsulation: Transparent
 - ▷ Layer-3: APPP (asynchrones PPP)
 - ▷ Layer-2: Transparent
 - ▷ Optionen: keine
 - ▷ Layer-1: SERIAL (zeigt die Verwendung der seriellen Schnittstelle für Verbindungen über den Layer 'V.24_DEF' an)



▷ *Betrieb eines Modems an der seriellen Schnittstelle*

Die Gegenstellenliste mit den Gegenstellen für das Modem an der seriellen Schnittstelle finden Sie auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation ► Gegenstellen ► Gegenstellen (ISDN/seriell)
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Einwahl-Gegenstellen
Terminal/Telnet	Setup/WAN/Einwahl-Gegenstellen

Wenn Sie für die serielle WAN-Schnittstelle einen Eintrag in der Gegenstellenliste erzeugt haben, kann diese Gegenstelle wie alle anderen auch für Routing und WAN-Verbindungen

7.13.10 Konfiguration einer Backup-Verbindung auf der seriellen Schnittstelle

Für die Konfiguration einer Backupverbindung über ein Modem an der seriellen Schnittstelle muss zunächst ein Eintrag in der Liste der Einwahl-Gegenstellen angelegt werden, über den die gewünschte Gegenstelle erreicht werden kann. Zusätzlich werden noch folgende Einträge in der Konfiguration des LANCOM benötigt:

► Eintrag in der Backup-Tabelle

Legen Sie in der Backup-Tabelle einen Eintrag an für die Gegenstelle, die über die Backup-Verbindung abgesichert werden soll. Dieser Gegenstelle ordnen Sie die Gegenstelle zu, die über das Modem an der seriellen Schnittstelle erreicht werden kann.

Die Backup-Tabelle finden Sie auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation ► Ruf-Verwaltung ► Backup-Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Backup-Tabelle
Terminal/Telnet	Setup/WAN/Backup-Tabelle

► Eintrag in der Polling-Tabelle

Wenn die Erreichbarkeit für die zu sichernde Gegenstelle nicht über LCP-Polling (nur bei PPP) geprüft werden kann, legen Sie zusätzlich noch einen Eintrag in der Polling-Tabelle an. Darin ordnen Sie der Gegenstelle eine IP-Adresse zu, deren Erreichbarkeit regelmäßig mit einem Ping-Befehl geprüft wird. Als IP-Adresse wählen Sie dabei üblicherweise einen Rechner direkt am Ende der zu prüfenden Verbindung, z.B. einen DNS-Server im Netz Ihres Providers.

▷ Manuelle Definition der MTU

Die Polling-Tabelle finden Sie auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation ► Gegenstellen ► Polling-Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Polling-Tabelle
Terminal/Telnet	Setup/WAN/Polling-Tabelle

7.13.11 Kontaktbelegung des LANCOM Modem Adapter Kits

LANCOM-Signal	D-Sub9-Stecker	LANCOM- oder Modemsignal	D-Sub9-Stecker
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

7.14 Manuelle Definition der MTU

Verschiedene Internet-Provider betreiben zwar einen eigenen Backbone, bedienen sich aber für die Einwahl ihrer Kunden der Zugangsknoten der Telekom. Dieses „zweistufige“ Einwahlverfahren kann zu Problemen mit dem realisierten Datendurchsatz führen:

- Bei der Einwahl in den Knoten der Telekom handelt ein LANCOM in der PPP-Verhandlung eine zulässige MTU aus, also die maximale Größe eines unfragmentierten Datenpakets. Diese MTU wird dann von Seiten des LANCOM auch verwendet.
- Bei der Weitergabe der Datenpakete an den Backbone des eigentlichen Providers wird ein zusätzlicher Header aufgeschlagen, die Datenpakete werden also noch einmal größer. Um nun trotzdem wieder in die erlaubte Größe zu passen, werden die Datenpakete fragmentiert, also in kleinere Teile aufgeteilt. Diese zusätzliche Fragmentierung kann zu Geschwindigkeitseinbußen in der Datenübertragung führen.

Um diese Problematik zu umgehen, kann für jede Gegenstelle eine feste MTU eingetragen werden.

WEBconfig,
Telnet oder
Terminalpro-
gramm

7.14.1 Konfiguration

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die MTU-Liste mit maximale 16 Einträgen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► MTU-Liste
Terminal/Telnet	Setup/WAN/MTU-Liste

Die Tabelle enthält folgende Einträge:

- **Gerätename:** Name der Gegenstelle. Es kann eine physikalische oder eine virtuelle (PPTP/VPN) Gegenstelle sein
- **MTU:** Auf der Verbindung zu verwendende MTU

7.14.2 Statistik

Unter **Status ► WAN-Statistik** finden Sie die MTU-Statistik, in der für alle aktiven Verbindungen die verwendeten MTUs festgehalten werden. Diese Tabelle ist halbdynamisch und beginnt mit 16 Einträgen. Sie enthält wie die MTU-Liste unter **Setup ► WAN** zwei Spalten in denen der Gegenstellen-Name und die MTU abgelegt werden.

Gegenstelle	MTU	Bemerkung
INET	1200	Die Gegenstelle INET ist die Internet-Verbindung und hat eine erzwungene MTU von 1200 Bytes.
MULTI	1492	MULTI ist eine PPPoE-Verbindung, auf der die MTU ausgehandelt wurde (daher beträgt sie 1492 Bytes).
TESTVPN	1100	TESTVPN ist eine VPN-Verbindung, die über die Internet-Verbindung aufgebaut wurde. Für VPN-Verbindungen wird ein fester Overhead von 100 Bytes angenommen, weshalb die MTU hier 1100 Bytes beträgt.
TESTVPN-PPTP	1060	TESTVPN-PPTP ist eine PPTP-Verbindung, die über die VPN-Verbindung TESTVPN aufgebaut wurde. Der Overhead von PPTP-Verbindungen beträgt 40 Bytes, weshalb die MTU hier 1060 Bytes beträgt.



MTU-Liste und MTU-Statistik existieren nur auf Geräten mit DSL oder ADSL-Interface

8 Firewall

Für die meisten Firmen und viele Privatanwender ist eine Arbeit ohne das Internet nicht mehr denkbar. E-Mail und Web sind für die Kommunikation und Informationsrecherche unverzichtbar. Jede Verbindung der Rechner aus dem eigenen, lokalen Netzwerk mit dem Internet stellt aber eine potentielle Gefahr dar: Unbefugte können über diese Internet-Verbindung versuchen, Ihre Daten einzusehen, zu verändern oder Ihre Rechner zu manipulieren.

In diesem Kapitel widmen wir uns daher einem sehr wichtigen Thema: der Firewall als Abwehrmaßnahme vor diesen Zugriffen. Neben einer kurzen Einführung in das Thema Internetsicherheit zeigen wir Ihnen, welchen Schutz Ihnen ein LANCOM bei richtiger Konfiguration bieten kann und wie Sie die entsprechenden Einstellungen konkret vornehmen.

8.1 Gefährdungsanalyse

Um die geeigneten Maßnahmen zur Gewährleistung der Sicherheit planen und umsetzen zu können, muss man sich zunächst einmal über die möglichen Gefahrenquellen im Klaren sein:

- ▶ Welche Gefahren bedrohen das eigene LAN bzw. die eigenen Daten?
- ▶ Über welche Wege verschaffen sich Eindringlinge den Zugang zu Ihrem Netzwerk?



Das Eindringen in geschützte Netzwerke bezeichnen wir im Weiteren dem allgemeinen Sprachgebrauch folgend als "Angriff", den Eindringling daher auch als "Angreifer".

8.1.1 Die Gefahren

Die Gefahren im Internet entspringen grundsätzlich ganz verschiedenen Motiven. Zum einen versuchen die Täter, sich persönlich zu bereichern oder die Opfer gezielt zu schädigen. Durch das immer stärker verbreitete Know-How der Täter ist das "Hacken" aber auch schon zu einer Art Sport geworden, bei dem sich oft Jugendliche darin messen, wer die Hürden der Internetsicherheit am schnellsten überwindet.

Was auch immer im einzelnen Fall das Motiv ist, die Absichten der Täter laufen meistens auf die folgenden Muster hinaus:

- ▶ Einblick in vertrauliche Informationen wie Betriebsgeheimnisse, Zugangsinformationen, Passwörter für Bankkonten etc.
- ▶ Nutzung der Rechner im LAN für die Zwecke der Eindringlinge, z.B. für die Verbreitung von eigenen Inhalten, Angriffe auf dritte Rechner etc.
- ▶ Verändern der Daten auf den Rechnern im LAN, z.B. um sich auf diese Weise weitere Zugangsmöglichkeiten zu schaffen
- ▶ Zerstören von Daten auf den Rechnern im LAN
- ▶ Lahmlegen von Rechnern im LAN oder der Verbindung mit dem Internet



Wir beschränken uns hier auf die Angriffe auf lokale Netzwerke (LAN) bzw. auf Arbeitsplatzrechner und Server in solchen LANs.

8.1.2 Die Wege der Täter

Um ihrem Unwesen nachgehen zu können, brauchen die Täter natürlich zunächst einen Weg für den Zugriff auf Ihre Rechner und Daten. Im Prinzip stehen dazu folgende Wege offen, solange sie nicht gesperrt bzw. geschützt sind:

- ▶ Über die zentrale Internetverbindung, z.B. über einen Router
- ▶ Über dezentrale Verbindungen ins Internet, z.B. Modems an einzelnen PCs oder Mobiltelefone an Notebooks
- ▶ Über Funknetzwerke, die als Ergänzung zum drahtgebundenen Netzwerk eingesetzt werden



In diesem Kapitel betrachten wir ausschließlich die Wege über die zentrale Internetverbindung, über den Router.



Hinweise zum Schutz der Funknetzwerke entnehmen Sie bitte den entsprechenden Kapiteln dieses Referenzhandbuchs bzw. der jeweiligen Gerätedokumentation.

8.1.3 Die Methoden

Normalerweise haben fremde Personen natürlich keinen Zugang zu Ihrem lokalen Netz oder den Rechnern darin. Ohne die entsprechenden Zugangsdaten oder Passwörter kann also niemand auf den geschützten Bereich zugreifen. Wenn das Ausspionieren dieser Zugangsdaten nicht möglich ist, versuchen die Angreifer auf einem anderen Weg zum Ziel zu kommen.

Ein grundlegender Ansatz dabei ist es, auf einem der zugelassenen Wege für den Datenaustausch Daten in das Netzwerk einzuschmuggeln, die dann von innen her den Zugang für den Angreifer öffnen. Durch Anhänge in E-Mails oder aktive Inhalte auf Webseiten kann so z.B. ein kleines Programm auf einen Rechner aufgespielt werden, der diesen anschließend zum Absturz bringt. Den Absturz nutzt das Programm dann, um einen neuen Administrator auf dem Rechner anzulegen, der anschließend aus der Ferne für weitere Aktionen im LAN genutzt werden kann.

Wenn der Zugang über E-Mail oder WWW nicht möglich ist, kann der Angreifer auch ausspähen, ob ein Server im LAN bestimmte Dienste anbietet, die er für seine Zwecke nutzen kann. Da die Dienste auf den Servern über bestimmte Ports im TCP/IP-Protokoll identifiziert werden, wird das Suchen nach offenen Ports auch als "Port-Scanning" bezeichnet. Der Angreifer startet dabei mit einem bestimmten Programm entweder allgemein im Internet oder nur auf bestimmten Netzwerken eine Anfrage nach den gewünschten Diensten und bekommt von ungeschützten Rechnern auch die entsprechende Antwort.

Eine dritte Möglichkeit besteht darin, sich in eine bestehende Datenverbindung einzuklinken und als Trittbrettfahrer zu nutzen. Dabei hört der Angreifer die Internetverbindung des Opfers ab und analysiert die Verbindungen. Eine aktive FTP-Verbindung nutzt er dann z.B., um auf dieser Verbindung seine eigenen Datenpakete mit in das zu schützende LAN zu schleusen.

▷ Was ist eine Firewall?

Eine Variante dieser Methode ist der "man-in-the-middle". Dabei hört der Angreifer zunächst die Kommunikation zwischen zwei Rechnern ab und klinkt sich dann dazwischen.

8.1.4 Die Opfer

Die Frage nach dem Gefährdungsgrad für einen Angriff beeinflusst in hohem Maße den Aufwand, den man für die Abwehr treffen will oder muss. Um einzuschätzen, ob Ihr Netzwerk als Opfer für einen Angreifer besonders interessant ist, können Sie folgende Kriterien heranziehen:

- ▶ Besonders gefährdet sind Netzwerke von allgemein bekannten Firmen oder Institutionen, in denen wertvolle Informationen vermutet werden. Dazu gehören z.B. die Ergebnisse einer Forschungsabteilung, die von Industriespionen gerne eingesehen werden, oder Bankserver, auf denen das große Geld verteilt wird.
- ▶ In zweiter Linie sind aber auch die Netzwerke von kleineren Organisationen gefährdet, die vielleicht nur für ganz bestimmte Gruppen interessant sind. Auf den Rechnern von Steuerberatern, Rechtsanwälten oder Ärzten schlummern sicherlich auch einige Informationen, die für Dritte durchaus interessant sein können.
- ▶ Nicht zuletzt sind aber auch die Rechner und Netzwerke Opfer von Angriffen, die augenscheinlich überhaupt keinen Nutzen für die Angreifer bieten. Gerade die "Script-Kiddies", die aus jugendlichem Ehrgeiz ihre Möglichkeiten austesten, suchen manchmal einfach nur nach einem wehrlosen Opfer, um sich für höhere Aufgaben zu üben.

Der Angriff auf einen eigentlich gar nicht interessanten, ungeschützten Rechner einer Privatperson kann auch dem Zweck dienen, eine Ausgangsbasis für Attacken auf die eigentlichen Ziele im zweiten Schritt vorzubereiten. Der "uninteressante" Rechner wird damit zur Quelle des Angriffs im zweiten Schritt, der Angreifer kann seine Identität verschleiern.

Unter dem Strich kann man also festhalten, dass die statistische Wahrscheinlichkeit für einen Angriff auf das Netzwerk der Global Player in der Industrie zwar größer ist als auf das Kleinst-Netzwerk im Home-Office. Aber auf der anderen Seite ist es bei einem schutzlos im Internet aufgestellten Rechner wahrscheinlich nur eine Frage der Zeit, bis er evtl. sogar zufällig einmal das Opfer von Angriffen wird.

8.2 Was ist eine Firewall?

Der Begriff der "Firewall" wird sehr unterschiedlich interpretiert. Wir möchten an dieser Stelle erläutern, was im Rahmen dieses Referenz-Handbuchs mit der "Firewall" gemeint ist:

Eine Firewall ist eine Zusammenstellung von Komponenten, die an einer zentralen Stelle den Datenaustausch zwischen zwei Netzwerken überwacht. Meistens überwacht die Firewall dabei den Datenaustausch zwischen einem internen, lokalen Netzwerk (LAN) und einem externen Netzwerk wie dem Internet.

Die Firewall kann dabei aus Hard- und/oder Softwarekomponenten bestehen:

- ▶ In reinen Hardware-Systemen läuft oft die Firewall-Software auf einem proprietären Betriebssystem.

▷ Was ist eine Firewall?

- ▶ Die Firewall-Software kann aber auch auf einem normalen Rechner mit Linux, Unix oder Windows laufen, der für diese Aufgabe abgestellt wurde.
- ▶ Als dritte und häufig anzutreffende Alternative läuft die Firewall-Software direkt in dem Router, der das LAN mit dem Internet verbindet.

Wir betrachten in den folgenden Abschnitten nur die Firewall in einem Router.



Die Funktionen "Intrusion Detection" und "DoS-Abwehr" gehören in manchen Anwendungen mit zum Umfang einer Firewall. Im LANCOM sind diese Funktionen natürlich auch enthalten, aber als separate Module neben der Firewall realisiert.

Weitere Informationen dazu finden Sie in den Abschnitten 'Abwehr von Einbruchversuchen: Intrusion Detection' →Seite 218 und 'Schutz vor "Denial-of-Service"-Angriffen' →Seite 220.

8.2.1 Die Aufgaben einer Firewall

Prüfung der Datenpakete

Wie überwacht die Firewall den Datenverkehr? Im Prinzip arbeitet die Firewall wie ein Türwächter für Datenpakete: Jedes Paket wird daraufhin geprüft, ob es die Türe des Netzwerks (die Firewall) in der gewünschten Richtung passieren darf oder nicht. Für diese Prüfung werden verschiedene Kriterien verwendet, die im Sprachgebrauch der Firewalls "Regeln" oder "Richtlinien" bezeichnet werden. Nach der Art der Informationen, die für die Erstellung der Regeln verwendet und im Betrieb der Firewall geprüft werden, unterscheidet man verschiedene Typen von Firewalls.

Wichtig ist vor allem der Aspekt der "zentralen" Positionierung: nur wenn wirklich der gesamte Datenverkehr zwischen "innen" und "außen" über die Firewall läuft, kann sie ihre Aufgabe sicher erfüllen. Jeder alternative Weg kann die Sicherheit der Firewall herabsetzen oder gar ausschalten. Diese zentrale Stellung der Firewall vereinfacht nebenbei auch die Wartung: eine Firewall als gemeinsamer Übergang zwischen zwei Netzwerken ist sicherlich einfacher zu pflegen als eine "Personal Firewall" auf jedem der im LAN angeschlossenen Rechner.



Prinzipiell arbeiten Firewalls an der Schnittstelle zwischen zwei oder mehreren Netzwerken. Für die folgenden Ausführungen werden wir als Beispiel nur den Übergang zwischen einem lokalen Netzwerk in einem Unternehmen und dem Internet betrachten. Diese Erklärungen lassen sich aber sinngemäß auch auf anderen Netzwerk-Konstellationen übertragen, z.B. für den Schutz eines Subnetzes der Personalabteilung in einem Unternehmen gegen die restlichen Netzwerkbenutzer.

Protokollierung und Alarmierung

Eine wichtige Funktion einer Firewall ist neben dem Prüfen der Datenpakete und der richtigen Reaktion auf die Ergebnisse dieser Prüfung auch die Protokollierung aller Aktionen, die bei der Firewall ausgelöst wurden. Durch die Auswertung dieser Protokolle kann der Admin Rückschlüsse auf die erfolgten Angriffe ziehen und auf Grund dieser Informationen ggf. die Konfiguration der Firewall weiter verbessern.

▷ Was ist eine Firewall?

Die Protokollierung alleine kommt aber manchmal zu spät. Oft kann durch ein sofortiges Eingreifen des Admins ein größerer Schaden verhindert werden. Aus diesem Grund verfügen Firewalls meistens über eine Alarmierungsfunktion, bei der die Meldungen der Firewall z.B. per E-Mail an den Administrator gemeldet werden.

8.2.2 Unterschiedliche Typen von Firewalls

Im Laufe der letzten Jahre hat sich die Arbeitsweise von Firewalls immer weiter entwickelt. Unter dem Oberbegriff "Firewall" werden eine ganze Reihe unterschiedlicher technischer Konzepte angeboten, mit denen das LAN geschützt werden soll. Hier stellen wir die wichtigsten Typen vor.

Paketfilter

Von einer paketfilterbasierten Firewall spricht man, wenn der Router nur die Angaben im Header der Datenpakete prüft und anhand dieser Informationen entscheidet, ob das Paket durchgelassen werden soll oder nicht. Zu den geprüften Informationen der Datenpakete gehören:

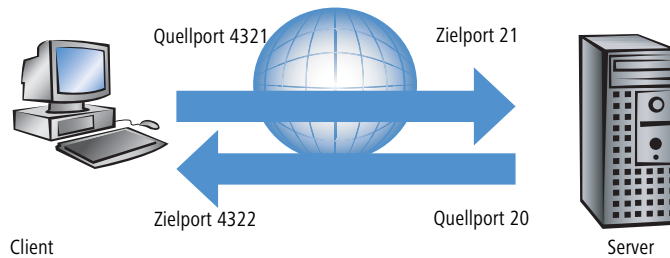
- ▶ IP-Adresse von Quelle und Ziel
- ▶ Übertragungsprotokoll (TCP, UDP oder ICMP)
- ▶ Portnummern von Quelle und Ziel
- ▶ MAC-Adresse

Die in einer paketfilterorientierten Firewall definierten Regeln legen z.B. fest, ob die Pakete von einem bestimmten IP-Adresskreis in das lokale Netzwerk weitergeleitet werden dürfen oder ob Pakete für bestimmte Dienste (d.h. mit speziellen Portnummern) gefiltert werden sollen. Durch diese Maßnahmen kann die Kommunikation mit bestimmten Rechnern, ganzen Netzwerken oder über bestimmte Dienste eingeschränkt oder verhindert werden. Die Regeln können dabei auch kombiniert werden, so kann z.B. der Zugang zum Internet über den TCP-Port 80 nur Rechnern mit bestimmten IP-Adressen erlaubt werden, während dieser Dienst für alle anderen Rechner gesperrt ist.

Die Konfiguration von paketfilternden Firewalls ist recht einfach, die Liste mit den zugelassenen oder verbotenen Paketen kann sehr schnell erweitert werden. Da auch die Anforderungen an die Performance eines Paketfilters mit recht geringen Mitteln erreicht werden kann, sind Paketfilter in der Regel direkt in Routern implementiert, die ohnehin als Schnittstelle zwischen den Netzwerken eingesetzt werden.

Nachteilig für die Paketfilter wirkt sich aus, dass die Liste der Regeln nach einiger Zeit nicht mehr so einfach zu überschauen ist. Außerdem werden bei einigen Diensten die Ports für die Verbindung dynamisch ausgehandelt. Um diese Kommunikation zu ermöglichen, muss der Administrator also alle dazu möglicherweise verwendeten Ports offen lassen, was der Grundausrichtung in den meisten Sicherheitskonzepten entgegensteht.

Ein Beispiel für einen Vorgang, der für einfache Paketfilter recht problematisch ist, ist der Aufbau einer FTP-Verbindung von einem Rechner im eigenen LAN zu einem FTP-Server im Internet. Beim üblicherweise verwendeten aktiven FTP sendet der Client (aus dem geschützten LAN) eine Anfrage von einem Port im oberen Bereich (>1023) an den Port 21 des Servers. Dabei teilt der Client dem Server mit, auf welchem Port er die Verbindung erwartet. Der Server baut daraufhin von seinem Port 20 eine Verbindung zum gewünschten Port des Clients auf.



Um diesen Vorgang zu ermöglichen, muss der Administrator des Paketfilters alle Ports für eingehende Verbindungen öffnen, da er nicht vorher weiß, zu welchen Ports der Client die FTP-Verbindung anfordert. Eine Alternative ist über das passive FTP gegeben. Dabei baut der Client selbst die Verbindung zum Server auf über einen Port, den er vorher dem Server mitgeteilt hat. Dieses Verfahren wird jedoch nicht von allen Clients/Servern unterstützt.

Wenn man die Firewall weiterhin mit einem Pförtner vergleicht, prüft dieser Türsteher nur, ob er den Boten mit dem Paket an der Tür kennt oder nicht. Wenn der Kurier bekannt ist und schon einmal in das Gebäude hinein durfte, darf er auch bei allen folgenden Aufträgen ungehindert und unkontrolliert in das Gebäude bis zum Arbeitsplatz des Empfängers.

Stateful-Packet-Inspection

Die Stateful-Packet-Inspection (SPI) oder kurz Stateful Inspection erweitert den Ansatz der Paketfilter um eine Prüfung weiterer Verbindungsinformationen. Neben der eher statischen Tabelle mit den zugelassenen Ports und Adressbereichen wird bei dieser Variante eine dynamische Tabelle gepflegt, in die Informationen über den Zustand der einzelnen Verbindungen eingetragen werden. Diese dynamische Tabelle ermöglicht es, alle gefährdeten Ports zunächst zu sperren und nur bei Bedarf für eine zulässige Verbindung (festgelegt durch Quell- und Zieladresse) einen Port zu öffnen. Das Öffnen der Ports geschieht dabei immer nur vom geschützten Netzwerk zum ungeschützten hin, also meistens vom LAN zum WAN (Internet). Datenpakete, die nicht zu einer in der Zustandstabelle gespeicherten Verbindung gehören, werden automatisch verworfen.

Stateful Inspection: richtungsabhängige Prüfung

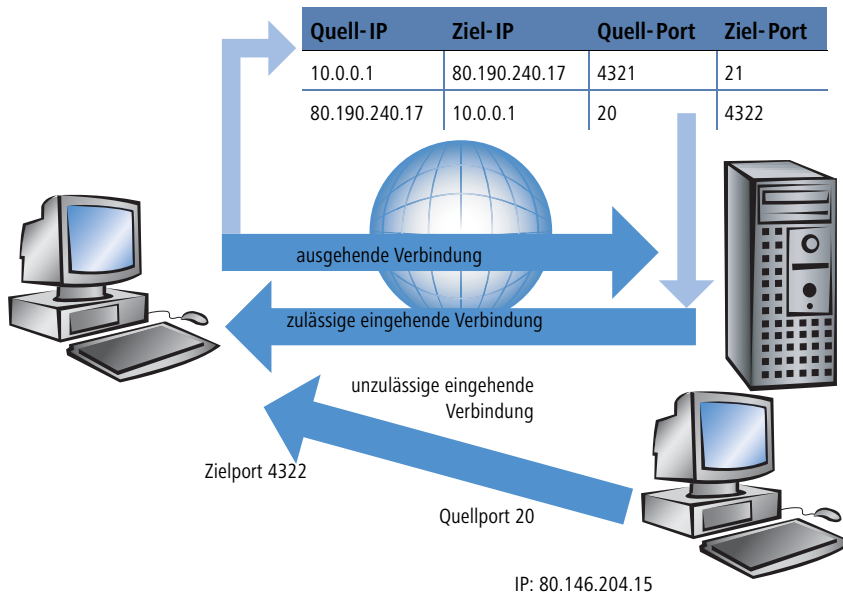
Die Filter-Regeln einer Stateful-Inspection Firewall sind - anders als bei klassische Portfilter-Firewalls - richtungsabhängig: Ein Verbindung kann immer von nur der Quelle zum Ziel aufgebaut werden; es sei denn, für die Rückrichtung ist ein expliziter Eintrag vorhanden. Ist eine Verbindung aufgebaut, so werden nur die zu dieser Verbindung gehörenden Datenpakete - in beide Richtungen natürlich - übertragen. Damit lassen sich z.B. alle Zugriffe, die unaufgefordert und nicht aus dem lokalen Netz heraus erfolgen, zuverlässig abblocken.

Zusätzlich kann die Stateful Inspection aus dem Verbindungsaufbau ableiten, ob dabei zusätzliche Kanäle für den Datenaustausch ausgehandelt werden. Einige Protokolle wie z.B. FTP (für den Datentransfer), T.120, H.225, H.245 und H.323 (für Netmeeting oder IP-Telefonie), PPTP (für VPN-Tunnel) oder IRC (für den Chat) signalisieren beim Aufbau der Verbindung vom LAN zum Internet durch den verwendeten Quell-Port, dass sie weitere Ports mit der Gegen-

▷ Was ist eine Firewall?

stelle vereinbaren. Die Stateful Inspection trägt dann auch diese zusätzlichen Ports in der Verbindungsliste mit ein, natürlich auch hier wieder beschränkt auf die jeweiligen Quell- und Ziel-Adressen.

Sehen wir uns dazu noch einmal das Beispiel FTP-Download an. Bei Starten der FTP-Sitzung baut der Client vom Quell-Port '4321' eine Verbindung zum Ziel-Port '21' beim Server auf. Die Stateful Inspection erlaubt diesen ersten Aufbau, sofern das FTP-Protokoll von den lokalen Rechnern nach außen freigegeben ist. In die dynamische Tabelle trägt die Firewall Quell- und Ziel adresse sowie die jeweiligen Ports ein. Gleichzeitig kann die Stateful Inspection die Steuerinformationen einsehen, die an den Port 21 des Servers gesendet werden. Aus diesen Steuersignalen geht hervor, dass der Client damit eine Verbindung des Servers von dessen Port 20 auf den Port 4322 des Clients anfordert. Die Firewall trägt auch diese Werte in die dynamische Tabelle ein, weil die Verbindung in das LAN hinein vom Client angefordert wird. Der Server kann also anschließend wie gewünscht die Daten an den Client senden.



Versucht hingegen ein anderer Rechner im Internet, den gerade offenen Port 4322 im LAN zu nutzen, um selbst Daten von seinem Port 20 auf dem geschützten Client abzulegen, wird dieser Versuch von der Firewall unterbunden, denn die IP-Adresse des Angreifers passt nicht zur erlaubten Verbindung!



Nach der erfolgreichen Datenübertragung verschwinden die Einträge automatisch wieder aus der dynamischen Tabelle, die Ports werden also wieder geschlossen.

Eine Firewall mit Stateful-Inspection ist zudem meistens in der Lage, die empfangenen Datenpakete zu re-assemblieren, also einzelne Bestandteile zwischenspeichern und wieder zu einem gesamten Paket zusammenzubauen.

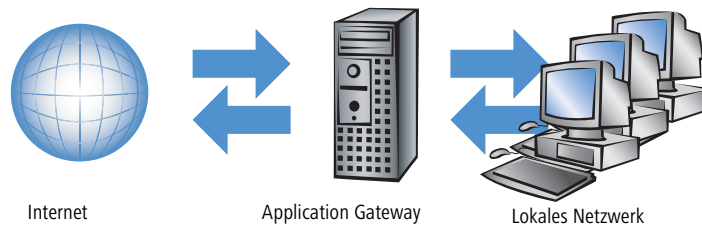
▷ Was ist eine Firewall?

Dadurch können bei fragmentierten Paketen nicht nur die einzelnen Teile von der Firewall geprüft werden, sondern auch das vollständige IP-Paket.

Dieser Pförtner macht seine Aufgabe also schon deutlich besser. Wenn in dieser Firma jemand einen Kurier bestellt, muss er parallel dazu auch den Pförtner anrufen und mitteilen, das er einen Kurier erwartet, um welche Uhrzeit der da sein wird und was auf dem Lieferschein des Paketes steht. Nur wenn diese Angaben beim Eintreffen des Kuriers mit dem Eintrag im Logbuch des Pförtners übereinstimmen, wird er den Kurier durchlassen. Bringt der Kurier nicht nur ein Paket, sondern gleich zwei, wird nur das mit dem richtigen Lieferschein durchgelassen. Ebenso wird auch ein zweiter Kurier, der Durchlass zu dem Mitarbeiter verlangt, an der Pforte abgewiesen.

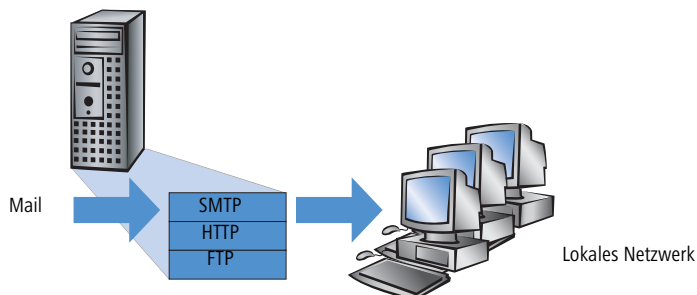
Application Gateway

Die Application Gateways erweitern die Adressprüfung der Paketfilter und die Verbindungsüberwachung der Stateful-Packet-Inspection um die Prüfung der Inhalte auf Anwendungsebene. Das Application Gateway läuft aufgrund der hohen Anforderungen an die Hardware-Performance in der Regel auf einem separaten Rechner. Dieser Rechner steht zwischen dem lokalen Netzwerk und dem Internet. Aus beiden Richtungen gesehen ist dieser Rechner die einzige Möglichkeit, mit dem jeweils anderen Netzwerk Daten auszutauschen. Es gibt keine direkte Verbindung zwischen den beiden Netzwerken, sondern immer nur bis zum Application Gateway.



Das Application Gateway steht damit als eine Art Vertreter (Proxy) für jedes der beiden Netzwerke da. Eine andere Bezeichnung für diese Konstellationen ist die des "dualhomed Gateway", weil dieser Rechner sozusagen in zwei Netzwerken zu Hause ist.

Für jede Anwendung, die über dieses Gateway erlaubt werden soll, wird auf dem Gateway ein eigener Dienst eingerichtet, z.B. SMTP für Mail, HTTP zum Surfen im Internet oder FTP für den Datendownload.



▷ Die Firewall im LANCOM

Dieser Dienst nimmt die Daten an, die von einer der beiden Seiten empfangen werden, und bildet sie für die jeweils andere Seite wieder ab. Was auf den ersten Blick wie ein ziemlich unnötiges Spiegeln vorhandener Daten aussieht, stellt bei näherem Hinsehen aber das tiefgreifende Konzept der Application Gateways dar: Es gibt in dieser Konstellation niemals eine direkte Verbindung z.B. zwischen einem Client im lokalen Netzwerk und einem Server im Internet. Die Rechner im LAN "sehen" immer nur den Proxy, die Rechner aus dem Internet ebenfalls. Diese physikalische Trennung von LAN und WAN macht es einem Angreifer schon sehr viel schwerer, in das geschützte Netzwerk einzudringen.

In der Übersetzung in das Pförtner-Beispiel wird das Paket hier am Tor abgegeben, der Kurier darf gar nicht selbst auf das Firmengelände. Der Pförtner nimmt das Paket an, öffnet es nach Prüfung von Anschrift und Lieferschein und kontrolliert den Inhalt. Wenn das Paket alle diese Hürden erfolgreich genommen hat, bringt ein firmeninterner Bote das Paket selbst weiter zum Empfänger in der Firma. Es wird damit zum Vertreter des Kuriers auf dem Firmengelände. Umgekehrt müssen alle Mitarbeiter, die ein Paket verschicken wollen, den Pförtner anrufen, der das Paket am Arbeitsplatz abholen lässt und am Tor an einen bestellten Kurier übergibt.



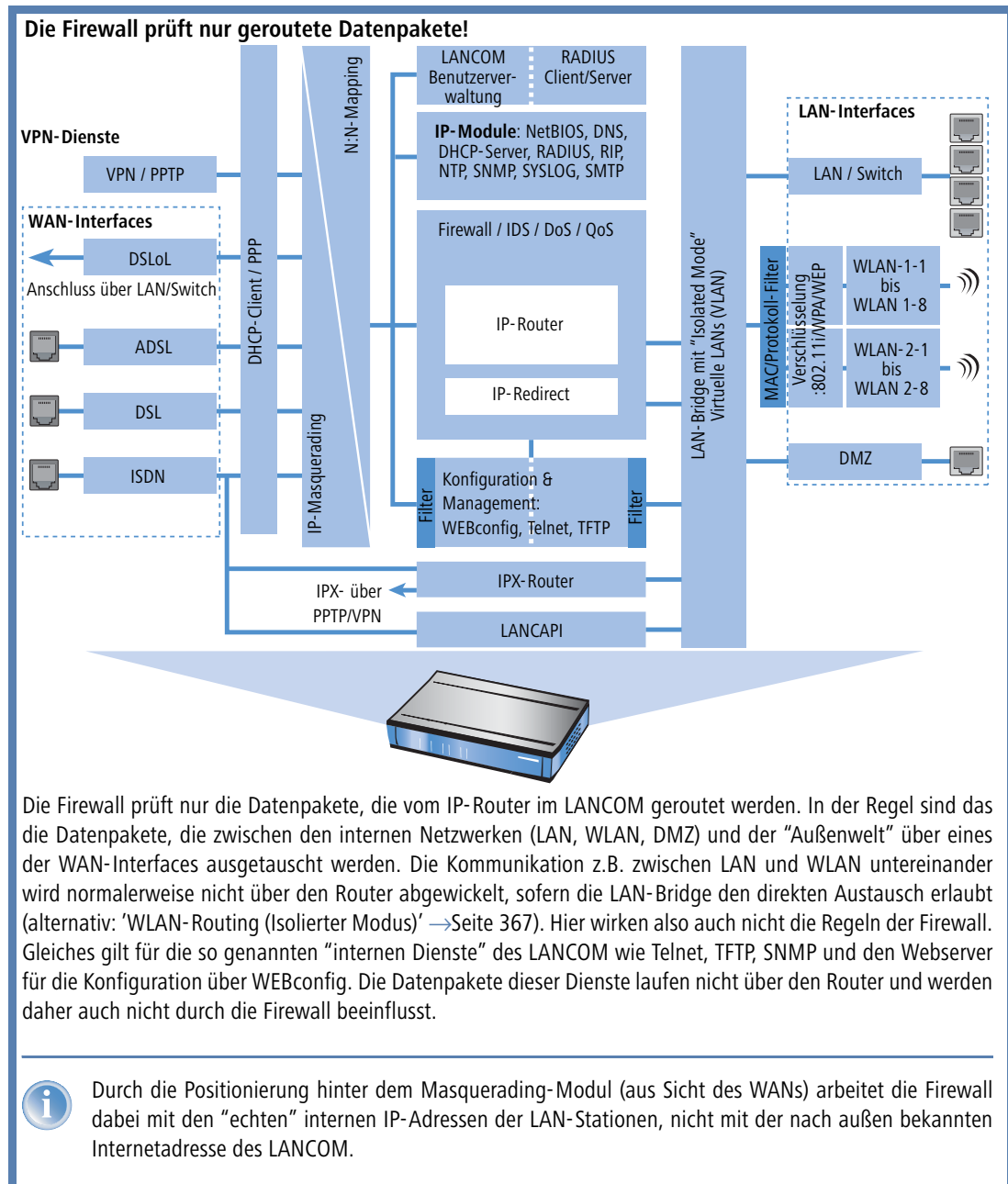
Die Funktion eines Application Gateways wird vom LANCOM aufgrund der hohen Anforderungen an die Hardware nicht unterstützt.

8.3 Die Firewall im LANCOM

Nach den allgemeinen Erläuterungen zu den Gefahren aus dem Internet sowie den Aufgaben und Typen von Firewalls finden sich in diesem Kapitel Beschreibungen zu den speziellen Funktionen der Firewall im LANCOM und Hinweise auf die konkrete Konfiguration.

8.3.1 So prüft die Firewall im LANCOM die Datenpakete

Die Firewall filtert aus dem gesamten Datenstrom, der über den IP-Router des LANCOM läuft, diejenigen Datenpakete heraus, für die eine bestimmte Behandlung vorgesehen ist.



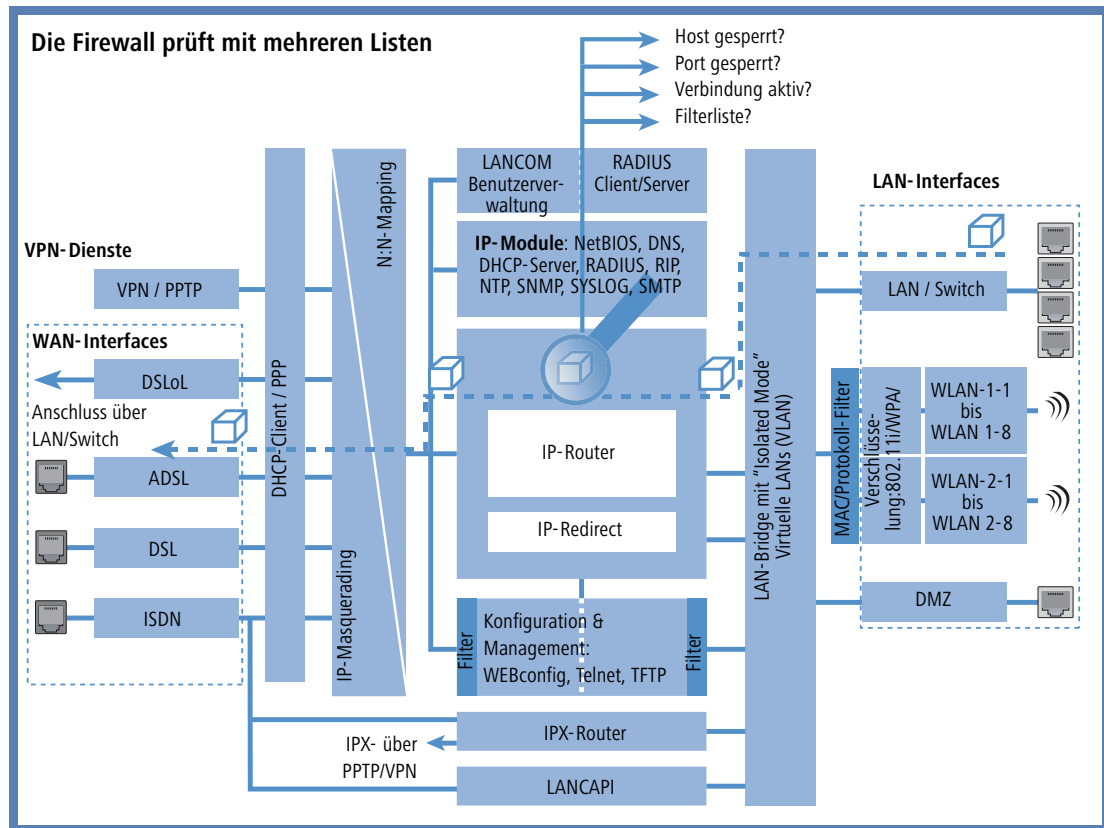
▷ Die Firewall im LANCOM

Die Firewall im LANCOM verwendet für die Prüfung der Datenpakete mehrere Listen, die aus den Firewall-Regeln, den daraus ausgelösten Firewall-Aktionen oder den aktiven Datenverbindungen automatisch erzeugt werden:

- ▶ Hostsperrliste
- ▶ Portsperrliste
- ▶ Verbindungsliste
- ▶ Filterliste

Und so setzt die Firewall die Listen ein, wenn ein Datenpaket über den IP-Router geleitet werden soll:

- ① Zuerst wird nachgeschaut, ob das Paket von einem Rechner kommt, der in der **Hostsperrliste** vermerkt ist. Ist der Absender gesperrt, wird das Paket verworfen.
- ② Ist der Absender dort nicht gesperrt, wird in der **Portsperrliste** geprüft, ob die verwendete Port/Protokoll-Kombination auf dem Zielrechner geschlossen ist. In diesem Fall wird das Paket verworfen.
- ③ Sind Absender und Ziel in den beiden ersten Listen nicht gesperrt, wird geprüft, ob für dieses Paket ein Verbindungseintrag in der **Verbindungsliste** existiert. Existiert ein solcher Eintrag, dann wird mit dem Paket so verfahren, wie in der Liste vermerkt ist.
- ④ Wird für das Paket kein Eintrag gefunden, dann wird die **Filterliste** durchsucht, ob ein passender Eintrag vorhanden ist und die dort angegebene Aktion ausgeführt. Wenn die Aktion besagt, dass das Paket akzeptiert werden soll, so wird ein Eintrag in der Verbindungsliste vorgenommen und etwaige weitere Aktionen dort vermerkt.



Existiert für ein Datenpaket keine explizite Firewall-Regel, so wird das Paket akzeptiert ('Allow-All'). Damit ist eine Abwärtskompatibilität zu bestehenden Installationen gegeben. Für einen maximalen Schutz durch die Stateful-Inspection beachten Sie bitte den Abschnitt 'Aufbau einer expliziten "Deny-All"-Strategie' →Seite 198.

Bleibt die Frage, woher die vier Listen ihre Informationen beziehen:

- In der **Hostsperrliste** werden die Stationen aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Die Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.
- In der **Portsperrliste** werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Auch diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

▷ Die Firewall im LANCOM

- In der **Verbindungsliste** wird für jede aufgebaute Verbindung ein Eintrag vorgenommen, wenn das geprüfte Paket von der Filterliste akzeptiert wird. In der Verbindungsliste wird festgehalten, von welcher Quelle zu welchem Ziel, über welches Protokoll und welchen Port eine Verbindung aktuell erlaubt ist. Darüber hinaus wird in dieser Liste festgehalten, wie lange der Eintrag noch in der Liste stehen bleibt und welche Firewall-Regel den Eintrag erzeugt hat. Diese Liste ist sehr dynamisch und permanent "in Bewegung".
- Die **Filterliste** wird aus den Regeln der Firewall erzeugt. Die darin enthaltenen Filter sind statisch und ändern sich nur beim Hinzufügen, Bearbeiten oder Löschen von Firewall-Regeln.

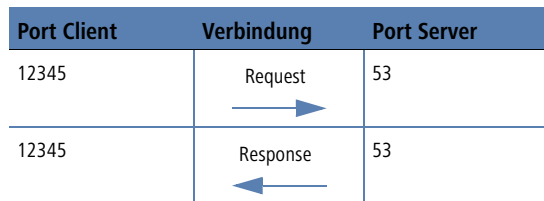
Alle Listen, die von der Firewall zur Prüfung der Datenpakete herangezogen werden, basieren also letztendlich auf den Firewall-Regeln ("Die Parameter der Firewall-Regeln" →Seite 185).

8.3.2 Besondere Protokolle

Ein wichtiger Punkt bei der Verbindungsüberwachung ist die Behandlung von Protokollen, die dynamisch Ports und / oder Adressen aushandeln, über die die weitere Kommunikation passiert. Beispiele für diese Protokolle sind FTP, H.323 oder auch viele UDP-basierte Protokolle. Hier ist es nötig, dass zusätzlich zu der ersten Verbindung ggf. weitere Verbindungen geöffnet werden. (siehe dazu auch 'Unterschiedliche Typen von Firewalls' →Seite 172).

UDP-Verbindungen

UDP ist eigentlich ein zustandsloses Protokoll, trotzdem kann man auch bei UDP-basierten Protokollen von einer nur kurzfristigen Verbindung sprechen, da es sich meistens um Request/Response-basierte Protokolle handelt, bei denen ein Client seinen Request an den Well-Known Port des Servers (z.B. 53 für DNS) richtet, und dieser darauf den Response wieder an den vom Client gewählten Quellport sendet:



Wenn der Server hingegen größere Datenmengen senden (z.B. TFTP) will und auf dem Well-Known Port nicht zwischen Requests und Acknowledges unterscheiden möchte oder kann, so schickt er zunächst das Response-Paket an

den Quellport des Absenders. Dabei setzt er aber als eigenen Quellport einen freien Port ein, auf dem er nun mit dem Client Daten austauschen möchte:

Port Client	Verbindung	Port Server
12345	Request →	69
12345	Response ←	54321
12345	Ack/Data →	54321
12345	Data/Ack ←	54321

Während sich die Datenübertragung nun über die Ports 12345 und 54321 abspielt, kann der Server auf dem Well-Known Port (69) weitere Requests annehmen. Wenn das LANCOM eine "Deny-All-Strategie" verfolgt, wird durch die erste Anfrage des Clients ein Eintrag in der Verbindungsliste erzeugt, der nur die Datenpakete des Servers auf Port 69 zulässt. Die Antwort des Servers würde dabei also einfach verworfen. Um dies zu verhindern, wird beim Anlegen des Eintrags in der Verbindungsliste der Zielport der Verbindung zunächst freigehalten, und erst beim Eintreffen des ersten Antwortpakets gesetzt, wodurch beide möglichen Fälle einer UDP Verbindung abgedeckt werden.

TCP-Verbindungen

TCP-Verbindungen können nicht einfach nur durch die Prüfung der Ports nachgehalten werden. Bei einigen Protokollen wie z.B. FTP, PPTP oder H.323 sind Prüfungen der Nutzdaten nötig, um alle später ausgehandelten Verbindungen zu öffnen, und nur die wirklich zu den Verbindungen gehörenden Pakete zu akzeptieren. Dies entspricht einer vereinfachten Version dessen, was auch beim IP-Masquerading gemacht wird, nur ohne Adress- und Port-Mapping. Es reicht aus, die Verhandlung nachzuverfolgen, die entsprechenden Ports zu öffnen und mit der Hauptverbindung zu verknüpfen. Damit werden diese Ports einerseits mit dem Schließen der Hauptverbindung ebenfalls geschlossen, und andererseits hält der Datenverkehr auf den Nebenverbindungen auch die Hauptverbindung weiter offen.

ICMP-Verbindungen

Für ICMP werden zwei Fälle unterschieden: Das sind zum einen die ICMP-Request/Reply-Verbindungen, wie sie z.B. beim "ping" verwendet werden, zum anderen die ICMP-Fehlermeldungen, die als Antwort auf ein beliebiges IP-Paket empfangen werden können.

ICMP Request/Reply-Verbindungen können eindeutig durch den vom Initiator verwendeten Identifier zugeordnet werden, d.h. in der Zustandsdatenbank wird beim Senden eines ICMP-Requests ein Eintrag erstellt, der nur ICMP-Replies mit dem korrekten Identifier durchlässt. Alle anderen ICMP-Replies werden stillschweigend verworfen.

▷ Die Firewall im LANCOM

Bei ICMP-Fehlermeldungen steht der IP-Header und die ersten 8 Bytes des IP-Pakets (i.A. UDP- oder TCP-Header) innerhalb des ICMP-Pakets. Anhand dieser Information wird beim Empfang einer ICMP-Fehlermeldung der zugehörige Eintrag in der Zustandsdatenbank gesucht. Das Paket wird nur weitergeleitet, wenn ein solcher Eintrag existiert, ansonsten wird es stillschweigend verworfen. Zusätzlich dazu werden potentiell gefährliche ICMP-Fehlermeldungen (Redirect-Route) herausgefiltert.

Verbindungen sonstiger Protokolle

Bei allen anderen Protokollen können keine verwandten Verbindungen nachgehalten werden, d.h. bei ihnen kann nur eine Verbindung zwischen den beteiligten Hosts in der Zustandsdatenbank aufgenommen werden. Diese können auch nur von einer Seite aus initiiert werden, es sei denn, in der Firewall ist ein dedizierter Eintrag für die "Gegenrichtung" vorhanden.

8.3.3 Allgemeine Einstellungen der Firewall

Neben den einzelnen Firewall-Regeln, die für die Einträge in den Filter- Verbindungs- und Sperrlisten sorgen, gelten einige Einstellungen für die Firewall allgemein:

- ▶ Firewall/QoS-Aktivierung
- ▶ Administrator-E-Mail (→Seite 182)
- ▶ Fragmente (→Seite 182)
- ▶ Sitzungswiederherstellung (→Seite 183)
- ▶ Ping-Block (→Seite 183)
- ▶ Stealth-Modus (→Seite 184)
- ▶ Authentifizierungs-Port tarnen (→Seite 184)

Firewall/QoS-Aktivierung

Mit dieser Option wird die gesamte Firewall inklusive der Quality-of-Service-Funktionen ein- bzw. ausgeschaltet.



Bitte beachten Sie, dass die Funktionen des N:N-Mapping ('N:N-Mapping' →Seite 139) nur wirksam sind, wenn die Firewall eingeschaltet ist!

Administrator-E-Mail

Zu den Aktionen, die die Firewall auslösen können, gehört auch die Alarmierung des Administrators per E-Mail. Die "Administrator-E-Mail" ist die Mail-Adresse ein, an die die entsprechenden Alarmierungs-Mails verschickt werden.

Fragmente

Manche Angriffe aus dem Internet versuchen, die Firewall durch fragmentierte Pakete (also in mehrere kleine Einheiten aufgeteilte Pakete) zu überlisten. Zu den Haupteigenschaften einer Stateful Inspection wie im LANCOM gehört auch die Fähigkeit, fragmentierte Pakete zu Re-assemblieren (wieder zusammensetzen), um anschließend das gesamte IP-Paket prüfen zu können.

Das gewünschte Verhalten der Firewall kann zentral eingestellt werden. Dabei stehen folgende Möglichkeiten zur Auswahl:

- ▶ **Filtern:** Die fragmentierten Pakete werden von der Firewall direkt verworfen.
- ▶ **Weiterleiten:** Die fragmentierten Pakete werden ohne weitere Prüfung von der Firewall weitergeleitet, sofern die gültigen Filtereinstellungen das zulassen.
- ▶ **Re-assemblieren:** Die fragmentierten Pakete werden zwischengespeichert und wieder zu einem kompletten IP-Paket zusammengesetzt. Das re-assemblierte Paket wird dann nach den gültigen Filtereinstellung geprüft und entsprechend behandelt.

Sitzungswiederherstellung

Die Firewall trägt in der Verbindungsliste alle aktuell erlaubten Verbindungen ein. Die Einträge verschwinden nach einer bestimmten Zeit (Timeout) automatisch wieder aus der Verbindungsliste, wenn keine Daten über die Verbindung übertragen werden und den Timeout erneuern.

Manchmal werden die Verbindungen gemäß den allgemeinen Aging-Einstellungen beendet, bevor die mit einer Anfrage angeforderten Datenpakete von der Gegenstelle empfangen wurden. In diesem Fall steht möglicherweise in der Verbindungsliste noch ein Eintrag für eine zulässige Verbindung, die Verbindung selbst ist aber nicht mehr vorhanden.

Der Parameter "Sitzungswiederherstellung" bestimmt das Verhalten der Firewall für Pakete, die auf eine ehemalige Verbindung schließen lassen:

- ▶ **Verbieten:** Die Firewall stellt die Sitzung auf keinen Fall wieder her und verwirft das Paket.
- ▶ **Verbieten für Default-Route:** Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über die Default-Route empfangen wurde.
- ▶ **Verbieten für WAN-Interfaces:** Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über eines der WAN-Interfaces empfangen wurde.
- ▶ **Erlauben:** Die Firewall stellt die Verbindung grundsätzlich wieder her, wenn das Paket zu einer "ehemaligen" Verbindung aus der Verbindungsliste gehört.

Ping-Blocking

Eine - nicht unumstrittene - Methode die Sicherheit zu erhöhen, ist das Verstecken des Routers; frei nach der Methode: "Wer mich nicht sieht, wird auch nicht versuchen mich anzugreifen...". Viele Angriffe beginnen mit der Suche nach Rechnern und/oder offenen Ports über eigentlich recht harmlose Anfragen, z.B. mit Hilfe des "ping"-Befehls oder mit einem Portscan. Jede Antwort auf diese Anfragen, auch die "Ich bin nicht hier"-Antwort, zeigt dem Angreifer, dass er ein potenzielles Ziel gefunden hat. Denn wer antwortet, der ist auch da. Um diese Rückschlüsse zu verhindern, kann das LANCOM die Antworten auf diese Anfragen unterdrücken.

Um dies zu erreichen, kann das LANCOM angewiesen werden, ICMP-Echo-Requests nicht mehr zu beantworten. Gleichzeitig werden auch die bei einem "traceroute" benutzten TTL-Exceeded Meldungen unterdrückt, so dass das LANCOM weder durch ein "ping" noch ein "traceroute" gefunden werden kann.

Mögliche Einstellungen sind:

▷ Die Firewall im LANCOM

- ▶ **Aus:** ICMP-Antworten werden nicht blockiert
- ▶ **Immer:** ICMP-Antworten werden immer blockiert
- ▶ **WAN:** ICMP-Antworten werden auf allen WAN-Verbindungen blockiert
- ▶ **Default Route:** ICMP-Antworten werden auf der Default-Route (i.d.R. Internet) blockiert

TCP-Stealth-Modus

Neben ICMP-Meldungen verrät auch das Verhalten bei TCP- und UDP-Verbindungen, ob sich an der angesprochenen Adresse ein Rechner befindet. Je nach umgebendem Netzwerk kann es sinnvoll sein, wenn TCP- und UDP-Pakete einfach verworfen werden, anstatt mit einem TCP-Reset bzw. einer ICMP-Meldung (port unreachable) zu antworten, wenn kein Listener für dem jeweiligen Port existiert. Das jeweils gewünschte Verhalten kann im LANCOM eingestellt werden.



Werden Ports ohne Listener versteckt, so ergibt sich auf maskierten Verbindungen das Problem, dass der "authenticate"- bzw. "ident"-Dienst nicht mehr funktioniert (bzw. nicht mehr korrekt abgelehnt wird). Der entsprechende Port kann daher gesondert behandelt werden ('Authentifizierungs-Port tarnen' → Seite 184).

Mögliche Einstellungen sind:

- ▶ **aus:** Alle Ports sind geschlossen und TCP-Pakete werden mit einem TCP-Reset beantwortet
- ▶ **immer:** Alle Ports sind versteckt und TCP-Pakete werden stillschweigend verworfen.
- ▶ **WAN:** Auf der WAN-Seite sind alle Ports versteckt und auf der LAN-Seite geschlossen
- ▶ **Default-Route:** Die Ports sind auf der Default-Route (i.d.R. Internet) versteckt und auf allen anderen Routen geschlossen

Authentifizierungs-Port tarnen

Wenn TCP- oder UDP-Ports versteckt werden, können z.B. die Anfragen von Mailservern zur Authentifizierung der Benutzer nicht mehr richtig beantwortet werden. Die Anfragen der Server laufen dann in einen Timeout, die Zustellung der Mails verzögern sich erheblich.

Auch bei aktiviertem TCP-Stealth-Modus erkennt die Firewall die Absicht einer Station im LAN, eine Verbindung zu einem Mailserver aufzubauen. Daraufhin wird der benötigte Port für die Authentifizierungsanfrage kurzzeitig (für 20 Sekunden) geöffnet.

Dieses Verhalten der Firewall im TCP-Stealth-Modus kann mit dem Parameter "Authentifizierungs-Port tarnen" gezielt unterdrückt werden.



Das Aktivieren der Option "Authentifizierungs-Port tarnen" kann zu erheblichen Verzögerungen beim Versand und Empfang z.B. von E-Mails oder News führen!

Ein Mail- oder News-Server, der mit Hilfe dieses Dienstes etwaige zusätzliche Informationen vom User anfordert, läuft dann zunächst in einen störenden Timeout, bevor er beginnt, die Mails auszuliefern. Dieser Dienst benötigt also einen eigenen Schalter um ihn zu verstecken bzw. "konform" zu halten.

Die Problematik dabei ist nun allerdings, dass eine Einstellung, die alle Ports versteckt, den ident-Port aber zurückweist, unsinnig ist - denn allein dadurch, dass der Ident-Port zurückgewiesen wird, wäre das LANCOM zu sehen.

Das LANCOM bietet zur Lösung dieses Problems an, Ident-Anfragen nur von den Mail und News-Servern abzulehnen, und bei Anfragen von allen anderen Rechnern diese einfach zu verwerfen. Hierzu werden bei der Abfrage eines Mail- (SMTP, POP3 IMAP2) oder Newsservers (NNTP) für eine Kurze Zeit (20 Sekunden) ident-Anfragen von den jeweiligen Servern abgelehnt.

Ist die Zeit abgelaufen, so wird der Port wieder versteckt.

8.3.4 Die Parameter der Firewall-Regeln

In diesem Abschnitt stellen wir vor, aus welchen Komponenten eine Firewall-Regel besteht und welche Optionen zur Einstellung der verschiedenen Parameter zur Verfügung stehen.



Informationen zur konkreten Definition der Firewall-Regeln mit den verschiedenen Konfigurationstools (LANconfig, WEBconfig oder Telnet) finden Sie im Kapitel 'Konfiguration der Firewall-Regeln' →Seite 201.

Die Komponenten einer Firewall-Regel

Eine Firewall-Regel wird zunächst bestimmt durch ihren Namen und einige weitere Optionen:

- ▶ **Ein-/Ausschalter:** Ist die Regel aktiv?
- ▶ **Priorität:** Mit welcher Priorität wird die Regel bearbeitet? (→Seite 185)
- ▶ **Verknüpfung:** Sollen weitere Firewall-Regeln beachtet werden, wenn diese Regel für ein Datenpaket zutrifft? (→Seite 186)
- ▶ **VPN-Regel:** Wird die Firewall-Regel auch zur Erzeugung von VPN-Regeln verwendet? (→Seite 186)
- ▶ **Routing-Tag:** Mit dem Einsatz des Routing-Tags können über die Ziel-IP-Adressen weitere Informationen wie z.B. der verwendete Dienst oder das verwendete Protokoll für die Auswahl der Zielroute genutzt werden. Durch das so realisierte Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich ('Policy-based Routing' →Seite 112).

Priorität

Das LANCOM nimmt beim Aufbau der Filterliste aus den Firewall-Regeln eine automatische Sortierung der Einträge vor. Dabei wird der "Detailierungsgrad" berücksichtigt: Zunächst werden alle speziellen Regeln beachtet, danach die allgemeinen (z.B. Deny-All).

Wenn sich durch die automatische Sortierung nicht das gewünschte Verhalten der Firewall einstellt, kann die Priorität von Hand verändert werden. Je höher die Priorität der Firewall-Regel, desto eher wird der zugehörige Filter in der Filterliste platziert.



Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im Abschnitt 'Firewall-Diagnose' →Seite 211 beschrieben.

Verknüpfung

Es gibt Anforderungen an die Firewall, die mit einer einzelnen Regel nicht abgedeckt werden können. Wenn die Firewall dazu eingesetzt wird, den Internet-Traffic verschiedener Abteilungen (in eigenen IP-Subnetzen) zu begrenzen, können einzelne Regeln z.B. nicht gleichzeitig die gemeinsame Obergrenze abbilden. Soll jeder von z.B. drei Abteilungen eine Bandbreite von maximal 512 kBit/s zugestanden werden, die gesamte Datenrate der drei Abteilungen aber ein Limit von 1024 kBit/s nicht überschreiten, so muss eine mehrstufige Prüfung der Datenpakete eingerichtet werden:

- ▶ In der ersten Stufe wird geprüft, ob die aktuelle Datenrate der einzelnen Abteilung die Grenze von 512 kBit/s nicht übersteigt.
- ▶ In der zweiten Stufe wird geprüft, ob die Datenrate aller Abteilungen zusammen die Grenze von 1024 kBit/s nicht übersteigt.

Normalerweise wird die Liste der Firewall-Regeln der Reihe nach auf ein empfangenes Datenpaket angewendet. Trifft eine Regel zu, wird die entsprechende Aktion ausgeführt. Die Prüfung durch die Firewall ist damit beendet, es werden keine weiteren Regeln auf das Paket angewendet.

Um eine zwei- oder mehrstufige Prüfung eines Datenpaketes zu erreichen, wird die "Verknüpfungsoption" für die Regeln aktiviert. Wenn eine Firewall-Regel mit aktivierter Verknüpfungsoption auf ein Datenpaket zutrifft, wird zunächst die entsprechende Aktion ausgeführt, anschließend wird die Prüfung in der Firewall jedoch fortgesetzt. Trifft eine der weiteren Regeln auch auf dieses Paket zu, wird auch die in dieser Regel definierte Aktion ausgeführt. Ist auch bei dieser folgenden Regel die Verknüpfungsoption aktiviert, wird die Prüfung solange fortgesetzt, bis

- ▶ entweder eine Regel auf das Paket zutrifft, bei der die Verknüpfung nicht aktiviert ist
- ▶ oder die Liste der Firewall-Regeln ganz durchgearbeitet ist, ohne dass eine weitere Regel auf das Paket zutrifft.

Zur Realisierung dieses Szenarios wird also für jedes Subnetz eine Firewall-Regel eingerichtet, die ab einer Datenrate von 512 kBit/s zusätzliche Pakete der Protokolle FTP und HTTP verwirft. Für diese Regeln wird die Verknüpfungsoption aktiviert. In einer weiteren Regel für alle Stationen im LAN werden alle Pakete verworfen, die über 1024 kBit/s hinausgehen.

VPN-Regeln

Wie im Abschnitt 'Default-VPN-Regeln' →Seite 182 beschrieben, bezieht eine VPN-Regel die Informationen über Quell- und Ziel-Netz u.a. aus den Firewall-Regeln.

Mit dem Aktivieren der Option "VPN-Regel" für eine Firewall-Regel wird festgelegt, dass aus dieser Firewall-Regel eine VPN-Regel abgeleitet wird.

Neben diesen Basisinformationen beantwortet eine Firewall-Regel die Fragen, wann bzw. worauf sie angewendet werden soll und welche Aktionen ggf. ausgeführt werden:

- ▶ **Verbindung:** Auf welche Stationen/Netzwerke und Dienste/Protokolle bezieht sich die Regel? (→Seite 188)

▷ Die Firewall im LANCOM

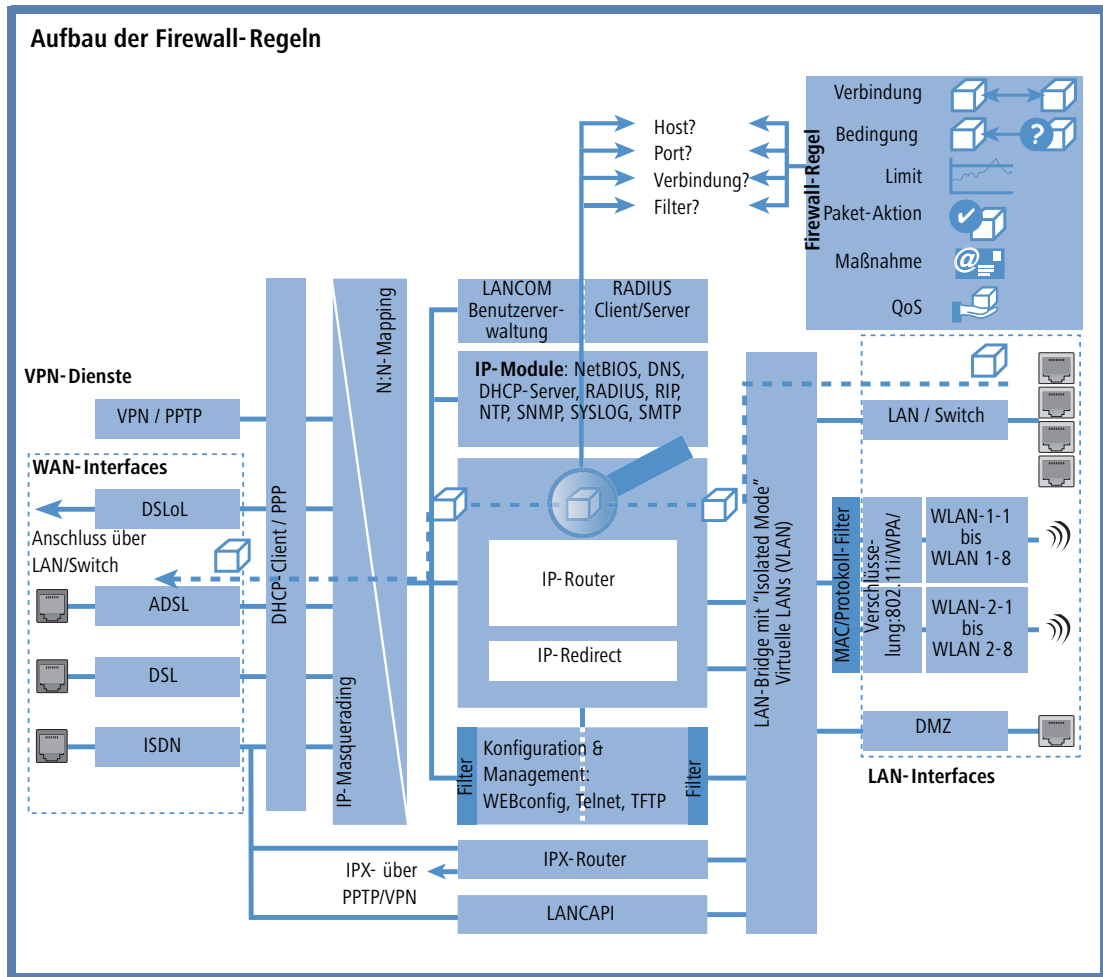
- ▶ **Bedingung:** Ist die Wirksamkeit der Regel durch Bedingungen eingeschränkt? (→Seite 189)
- ▶ **Limit (Trigger):** Beim Erreichen welcher Schwellwerte soll die Regel anspringen? (→Seite 189)
- ▶ **Paket-Aktion:** Was soll mit den Datenpaketen passieren, wenn die Bedingung erfüllt und das Limit erreicht sind? (→Seite 190)
- ▶ **Sonstige Maßnahmen:** Sollen neben der Paket-Aktion noch weitere Maßnahmen eingeleitet werden? (→Seite 190)
- ▶ **Quality of Service (QoS):** Werden Datenpakete bestimmter Anwendungen oder mit entsprechenden Markierungen durch die Zusicherung von speziellen Dienstgütern besonders bevorzugt? (→Seite 191)



Bedingung, Limit, Paket-Aktion und sonstige Maßnahmen bilden zusammen ein so genanntes "Aktionen-Set". Jede Firewall-Regel kann mehrere Aktionen-Sets beinhalten. Wenn für mehrere Aktionen-Sets das gleiche Limit verwendet wird, kann die Reihenfolge der Aktionen-Sets eingestellt werden.

Im Abschnitt 'So prüft die Firewall im LANCOM die Datenpakete' →Seite 176 wurde bereits dargestellt, dass die Listen zur Prüfung der Datenpakete letztlich aus den Firewall-Regeln gebildet werden. Die Erweiterung der Grafik stellt sich damit wie folgt dar:

▷ Die Firewall im LANCOM



Verbindung



Mit der Verbindung in der Firewall-Regel legen Sie fest, auf welche Datenpakete sich die Vorschrift bezieht. Eine Verbindung wird definiert durch die Quelle, das Ziel und den verwendeten Dienst. Zur Bezeichnung von Quelle oder Ziel können die folgenden Angaben verwendet werden:

- ▶ Alle Stationen
- ▶ Das gesamte lokale Netz (LAN)
- ▶ Bestimmte Gegenstellen (bezeichnet durch den Namen aus der Gegenstellenliste)
- ▶ Bestimmte Stationen im LAN (bezeichnet durch den Hostnamen)

- ▶ Bestimmte MAC¹-Adressen
- ▶ Bereiche von IP-Adressen
- ▶ Komplette IP-Netzwerke

Hostnamen können nur dann verwendet werden, wenn das LANCOM die Namen in IP-Adressen auflösen kann. Dafür muss das LANCOM die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.



Werden die Quelle oder Ziel für eine Firewall-Regel nicht näher bestimmt, gilt die Regel generell für Datenpakete "von allen Stationen" bzw. "an alle Stationen".

Der Dienst wird bestimmt durch die Kombination eines IP-Protokolls mit entsprechenden Quell- und/oder Zielports. Für häufig verwendete Dienste (WWW, Mail etc.) sind die entsprechenden Verknüpfungen im LANCOM schon vordefiniert, andere können je nach Bedarf zusätzlich angelegt werden.



Bedingung

Mit den zusätzlichen Bedingungen schränkt man die Wirksamkeit einer Firewall-Regel weiter ein. Folgende Bedingungen stehen zur Auswahl:

- ▶ Nur für Pakete mit bestimmten ToS- bzw. DiffServ-Markierungen
- ▶ Nur wenn Verbindung noch nicht besteht
- ▶ Nur für Defaultroute (Internet)
- ▶ Nur für VPN-Routen



Limit (Trigger)

Das Limit (oder auch Trigger) bezeichnet einen quantifizierten Schwellwert, der auf der definierten Verbindung überschritten werden muss, bevor der Filter ein Datenpaket erfasst. Ein Limit setzt sich zusammen aus folgenden Eckwerten:

- ▶ Einheit (kBit, kByte oder Pakete)
- ▶ Betrag, also Datenrate oder Anzahl
- ▶ Bezugsgröße (pro Sekunde, pro Minute, pro Stunde oder absolut)

Zusätzlich kann für das Limit vereinbart werden, ob es sich auf eine logische Verbindung bezieht oder auf alle Verbindungen gemeinsam, die zwischen den festgelegten Ziel- und Quell-Stationen über die zugehörigen Dienste

1. MAC steht für Media Access Control und ist Dreh- und Angelpunkt für die Kommunikation innerhalb eines LAN. Jedem Netzwerkadapter ist eine MAC-Adresse fest gespeichert. MAC-Adressen sind weltweit eindeutig und unverwechselbar, ähnlich zu Seriennummern von Geräten. Über die MAC-Adressen lassen sich die PCs im LAN zuverlässig auswählen, um ihnen gezielt Rechte auf IP-Paketebene zu gewähren oder zu versagen. MAC-Adressen werden häufig außen auf den Netzwerkgeräten in hexadezimaler Darstellung (z. B. 00:A0:57:01:02:03) angebracht.

▷ Die Firewall im LANCOM

bestehen. So wird gesteuert, ob der Filter greift, wenn z.B. alle HTTP-Verbindungen der User im LAN in Summe das Limit überschreiten oder ob es ausreicht, wenn eine einzige der parallel aufgebauten HTTP-Verbindungen den Schwellwert durchbricht.

Bei absoluten Werten kann außerdem definiert werden, dass der zugehörige Zähler beim Überschreiten des Limits zurückgesetzt wird.



Die Daten werden bis zum Erreichen des Limits auf jeden Fall übertragen! Mit einem Betrag von "0" wird die Regel sofort aktiv, wenn auf der definierten Verbindung Datenpakete zur Übertragung anstehen.



Paket-Aktion

Die Firewall hat drei Möglichkeiten, ein gefiltertes Paket zu behandeln:

- ▶ **Übertragen:** Das Paket wird normal übertragen.
- ▶ **Verwerfen:** Das Paket wird stillschweigend verworfen.
- ▶ **Zurückweisen:** Das Paket wird zurückgewiesen, der Empfänger erhält eine entsprechenden Nachricht über ICMP.



Sonstige Maßnahmen

Die Firewall dient nicht nur dazu, die gefilterten Datenpakete zu verwerfen oder durchzulassen, sie kann auch zusätzliche Maßnahmen ergreifen, wenn ein Datenpaket durch den Filter erfasst wurde. Die Maßnahmen gliedern sich dabei in die beiden Bereiche "Protokollierung/Benachrichtigung" und "Verhindern weiterer Angriffe":

- ▶ **Syslog-Nachricht senden:** Sendet eine Nachricht über das SYSLOG-Modul an einen SYSLOG-Client, wie im Konfigurationsbereich "Meldungen" festgelegt.
- ▶ **E-Mail-Nachricht senden:** Sendet eine E-Mail-Nachricht an den Administrator, der im Konfigurationsbereich "Meldungen" festgelegt ist.
- ▶ **SNMP senden:** Sendet einen SNMP-Trap, der z.B. vom LANmonitor ausgewertet wird.



Jede dieser drei Benachrichtigungsmaßnahmen führt automatisch zu einem Eintrag in der Firewall-Ereignis-tabelle.

- ▶ **Verbindung trennen:** Trennt die Verbindung, über die das gefilterte Paket empfangen wurden.



Dabei wird physikalische Verbindung getrennt (also z.B. die Internetverbindung), nicht nur die logische Verbindung zwischen den beiden beteiligten Rechnern!

- ▶ **Absender-Adresse sperren:** Sperrt die IP-Adresse, von der das gefilterte Paket empfangen wurde, für eine einstellbare Zeit.
- ▶ **Ziel-Port sperren:** Sperrt den Ziel-Port, an den das gefilterte Paket gesendet wurde, für eine einstellbare Zeit.



Quality of Service (QoS)

Neben den Beschränkungen für die Übertragung von Datenpaketen kann die Firewall auch für bestimmte Anwendungen eine "Sonderbehandlung" einräumen. Die QoS-Einstellungen nutzen dabei die Möglichkeiten der Firewall, Datenpakete gezielt Verbindungen oder Diensten zuordnen zu können.



Weitere Informationen zu den QoS und der entsprechenden Konfiguration finden Sie im Kapitel 'Quality-of-Service' →Seite 226.

8.3.5 Die Alarmierungsfunktionen der Firewall

In diesem Abschnitt werden die Meldungen, die von der Firewall bei sicherheitsrelevanten Ereignissen verschickt werden, im Detail beschrieben. Es stehen die folgenden Meldungstypen zur Verfügung:

- ▶ E-Mail-Benachrichtigung
- ▶ SYSLOG-Meldung
- ▶ SNMP-Trap

Benachrichtigungen können dabei jeweils getrennt entweder durch die Intrusion Detection, die Denial-of-Service Protection oder durch frei einstellbare Maßnahmen in der Firewall ausgelöst werden. Die spezifischen Parameter für die verschiedenen Benachrichtigungsarten (wie z.B. das zu benutzende E-Mail-Konto) können Sie an folgenden Stellen angeben:

Konfigurationstool	Aufruf
LANconfig	Meldungen ▶ SMTP-Konto bzw. Meldungen ▶ SYSLOG
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Mail bzw. Experten-Konfiguration ▶ Setup ▶ SYSLOG
Terminal/Telnet	/Setup/Mail bzw. /Setup/SYSLOG

Ein Beispiel:

Es sei ein Filter namens 'BLOCKHTTP' definiert, der den Zugriff auf einen HTTP-Server (192.168.200.10) abblockt, und für den Fall, dass doch jemand auf den Server zugreifen wollte, jeden Traffic von und zu diesem Rechner unterbindet und den Administrator über SYSLOG informiert.

Benachrichtigung per SYSLOG

Wenn die Portfilter-Firewall ein entsprechendes Paket verwirft, wird über Syslog (siehe auch 'Einrichten des SYSLOG-Moduls' →Seite 429) eine Meldung ausgegeben, z.B.:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
```

Die Ports werden dabei nur bei portbehafteten Protokollen ausgegeben. Zusätzlich werden Rechnernamen dann ausgegeben, wenn das LANCOM diese direkt (d.h. ohne weitere DNS-Anfrage) auflösen kann.

▷ Die Firewall im LANCOM

Werden für einen Filter die Syslog-Meldungen aktiviert (%s-Aktion), so wird diese Meldung ausführlicher. Dann werden Name des Filters, überschrittenes Limit, sowie ausgeführte Aktionen zusätzlich mit ausgegeben. Für das obige Beispiel könnte die Meldung dann so aussehen:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

Benachrichtigung per E-Mail

Ist das E-Mail-System des LANCOM aktiviert, so können Sie die bequeme Benachrichtigung per E-Mail nutzen. Das Gerät sendet dann eine E-Mail in der folgenden Form an den Administrator, sobald die entsprechende Aktion der Firewall ausgeführt wurde:

```
FROM: LANCOM_Firewall@MyCompany.com
TO: Administrator@MyCompany.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46
```

The packet below

```
Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)
45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E...P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .....P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | ` .t... ....
```

```
matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a connection
because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

Damit der Mailversand aus dem LANCOM an den Administrator funktioniert, muss die E-Mailadresse des Empfängers richtig eingetragen sein. Unter LANconfig tragen Sie die Administrator-E-Mailadresse im Konfigurationsbereich 'Firewall/QoS' auf der Registerkarte 'Allgemein' ein.



Unter WEBconfig oder Telnet finden Sie die Administrator- E- Mailadresse unter:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ▶ Setup ▶ IP-Router ▶ Firewall
Terminal/Telnet	/Setup/IP-Router/Firewall

Außerdem muss ein Mail-Postfach eingerichtet sein, über das die E-Mail verschickt werden kann. Die erforderlichen Einstellungen finden Sie unter LANconfig im Konfigurationsbereich 'Meldungen' auf der Registerkarte 'SMTP'.



▷ Die Firewall im LANCOM

Unter WEBconfig oder Telnet finden Sie die SMTP-Einstellungen unter:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► SMTP
Terminal/Telnet	/Setup/SMTP

Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde (siehe auch 'SNMP' →Seite 31), so wird die erste Zeile der Logging-Tabelle als Enterprise-Specific Trap 26 verschickt. Dieser Trap enthält zusätzlich noch den System-Descriptor und den System-Namen aus der MIB-2.

Für das Beispiel wird ein SNMP-Trap erzeugt, aus dem man u.a. folgende Informationen ablesen kann:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
System-Descriptor SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
Device-String SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
Time-Stamp SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
Quell-Adresse SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
Ziel-Adresse SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
Protokoll (6 = TCP) SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

Quell-Port	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6. SNMP: Integer Value = 4353 (0x1101)
Ziel-Port (80 = HTTP)	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7. SNMP: Integer Value = 80 (0x50)
Name der Filterregel	SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8. SNMP: String Value = BLOCKHTTP



Dieser Trap und alle anderen im LANCOM generierten Traps werden sowohl an alle manuell konfigurierten Trap-Empfänger gesendet, ebenso wie auch an jeden angemeldeten LANmonitor, welcher diesen und u.U. auch alle anderen Traps auswerten kann

8.3.6 Strategien für die Einstellung der Firewall

Firewalls bilden die Schnittstelle zwischen Netzwerken und schränken dort den ungehinderten Datenaustausch mehr oder weniger deutlich ein. Damit stehen die Firewalls den Zielsetzungen der Netzwerke, zu denen sie selbst gehören, entschieden entgegen: Netzwerke sollen Rechner verbinden, Firewalls sollen die Verbindung verhindern.

Aus diesem Widerspruch lässt sich das Dilemma der verantwortlichen Administratoren erkennen, die in der Folge verschiedene Strategien zur Lösung entwickelt haben.

Allow-All

Die Allow-All-Strategie stellt die ungehinderte Kommunikation der Mitarbeiter in den Netzwerken über die Sicherheit. Dabei wird zunächst jede Kommunikation erlaubt, das LAN steht für Angreifer weiter offen. Erst durch die Konfiguration des Admins wird das LAN sukzessive sicherer, in dem nach und nach neue Regeln aufgebaut werden, die Teile der Kommunikation einschränken oder verhindern.

Deny-All

Bei der Deny-All-Strategie wird zunächst nach der Methode "Alles sperren!" verfahren, die Firewall blockt die Kommunikation zwischen dem zu schützenden Netzwerk und dem Rest der Welt vollständig ab. Im zweiten Schritt öffnet der Administrator dann die Adressbereiche oder Ports, die für die tägliche Kommunikation mit dem Internet etc. erforderlich sind.

Dieser Ansatz ist für die Sicherheit des LANs besser als die Allow-All-Strategie, führt aber in der Anfangsphase oft zu Schwierigkeiten mit den Benutzern. Einige Dinge laufen eben nach Einschalten der Deny-All-Firewall vielleicht nicht mehr so wie vorher, bestimmte Rechner können ggf. nicht mehr erreicht werden etc.

Firewall mit DMZ

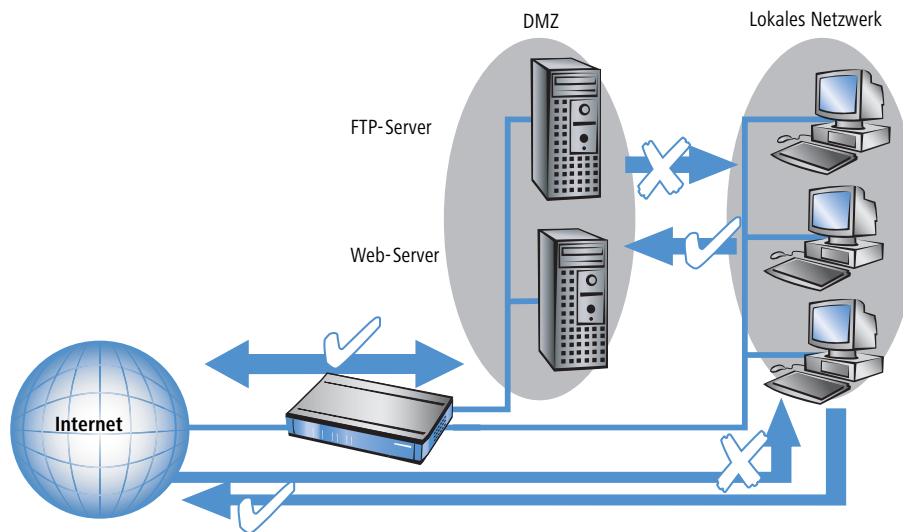
Die demilitarisierte Zone (DMZ) stellt einen speziellen Bereich des lokalen Netzes dar, der durch eine Firewall sowohl gegen das Internet als auch gegen das eigentliche LAN abgeschirmt ist. In diesem Netzabschnitt werden alle Rech-

Die Firewall im LANCOM

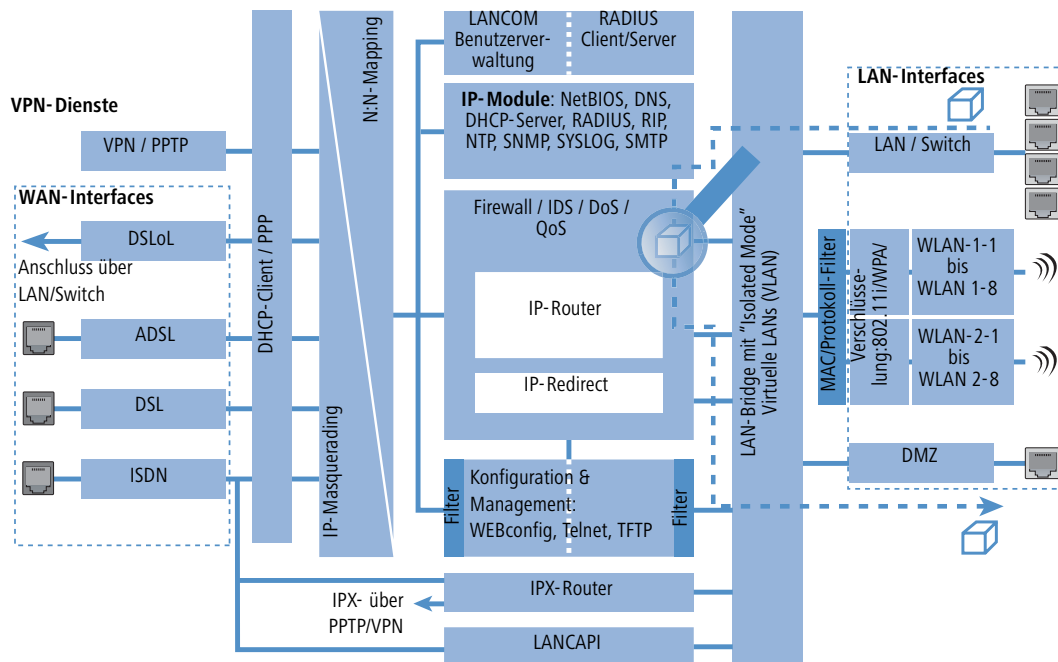
ner positioniert, auf die aus dem unsicheren Netz (Internet) direkt zugegriffen werden soll. Dazu gehören z.B. die eigenen FTP- und Web-Server.

Die Firewall schützt dabei zunächst die DMZ gegen Angriffe aus dem Internet. Zusätzlich schützt die Firewall aber auch das LAN gegen die DMZ. Die Firewall wird dazu so konfiguriert, dass nur folgende Zugriffe möglich sind:

- ▶ Stationen aus dem Internet können auf die Server in der DMZ zugreifen, der Zugriff aus dem Internet auf das LAN ist jedoch nicht möglich.
- ▶ Die Stationen aus dem LAN können auf das Internet und auf die Server in der DMZ zugreifen.
- ▶ Die Server aus der DMZ können nicht auf die Stationen im LAN zugreifen. damit ist sichergestellt, dass auch ein "gehackerter" Server aus der DMZ nicht zu einem Sicherheitsrisiko für das LAN wird.



Einige LANCOM-Modelle unterstützen diesen Aufbau durch eine separate LAN-Schnittstelle, die nur für die DMZ verwendet wird. Betrachtet man den Weg der Daten durch das LANCOM, dann wird die Funktion der Firewall für die Abschirmung des LANs gegenüber der DMZ deutlich.



Der direkte Datenaustausch zwischen LAN und DMZ ist über die LAN-Bridge nicht möglich, wenn ein DMZ-Port verwendet wird. Der Weg vom LAN in die DMZ und umgekehrt geht also nur über den Router, und damit auch über die Firewall! Die wiederum schirmt das LAN gegen Anfragen aus der DMZ genau so ab wie gegenüber dem Internet.



Das Abschirmen der DMZ gegenüber dem Internet auf der einen und dem LAN auf der anderen Seite wird in vielen Netzstrukturen mit zwei separaten Firewalls gelöst. Beim Einsatz eines LANCOM mit DMZ-Port benötigt man für diesen Aufbau nur ein Gerät, was u.a. den Vorteil einer deutlich vereinfachten Konfiguration mit sich bringt.

8.3.7 Tipps zur Einstellung der Firewall

Mit der LANCOM Firewall steht ein extrem flexibles und leistungsfähiges Werkzeug zur Verfügung. Um Ihnen bei der Erstellung individuell angepasster Firewall-Regeln behilflich zu sein, finden Sie im folgenden Hinweise zur optimalen Einstellung für Ihre spezifische Anwendung.

Die Default-Einstellung der Firewall

Im Auslieferungszustand befindet sich mit der "WINS-Regel" genau ein Eintrag in der Firewall-Regeltabelle. Diese Regel verhindert unerwünschte Verbindungsaufbauten auf der Default-Route (i.d.R. zum Internet) durch das NetBIOS-Protokoll. Windows Netzwerke senden in regelmäßigen Intervallen Anfragen in das Netzwerk um herauszufin-

▷ Die Firewall im LANCOM

den, ob die bekannten Stationen noch verfügbar sind. Dies führt bei zeitbasierter Abrechnung einer Netzwerkkopplung zu unerwünschten Verbindungsaufbauten.



Das LANCOM kann durch den integrierten NetBIOS-Proxy auch für Netzwerkkopplungen diese unerwünschten Verbindungsaufbauten verhindern, indem es selbst solange eine Antwort für die betreffende Ressource vortäuscht, bis ein tatsächlicher Zugriff erfolgt.

Sicherheit durch NAT und Stateful-Inspection

Sofern keine weitere Firewall-Regel eingetragen wird, wird das lokale Netz durch das Zusammenspiel von Network Address Translation und Stateful-Inspection geschützt: Nur Verbindungen aus dem lokalen Netz heraus erzeugen einen Eintrag in der NAT-Tabelle, woraufhin das LANCOM einen Kommunikationsport öffnet. Die Kommunikation über diesen Port wird durch die Stateful-Inspection überwacht: Nur Pakete, die genau zu dieser Verbindung gehören, dürfen über diesen Port kommunizieren. Für Zugriff von außen auf das lokale Netzwerk ergibt sich somit eine implizite "Deny-All"-Strategie.

Firewall-Regeln mit Scripten übertragen

Firewall-Regeln können einfach und komfortabel mittels Scripten über Geräte- und Softwareversionen hinweg übertragen werden ('Scripting' →Seite 55). Explizite Beispielscripte finden sich in der LANCOM KnowledgeBase unter www.lancom.de/support.



Sofern Sie in Ihrem LAN einen Server betreiben, der über Einträge in der Servicetabelle für Zugriffe aus dem Internet freigegeben ist (siehe 'IP-Masquerading' →Seite 121), können Stationen aus dem Internet von außen Verbindungen zu diesem Server aufbauen. Das inverse Masquerading hat in diesem Fall Vorrang vor der Firewall, solange keine explizite "Deny-All"-Regel eingerichtet wurde.

Aufbau einer expliziten "Deny-All"-Strategie

Für einen maximalen Schutz und bestmögliche Kontrolle über den Datenverkehr wird empfohlen, zunächst einmal jeglichen Datentransfer durch die Firewall zu unterbinden. Danach werden dann selektiv nur genau die benötigten Funktionen und Kommunikationspfade freigeschaltet. Dies bietet z.B. Schutz vor sog. 'Trojanern' bzw. E-Mail-Viren, die aktiv eine abgehende Verbindung auf bestimmten Ports aufbauen.

Deny-All: Die wichtigste Regel der Firewall!

Die Deny-All-Regel ist mit Abstand die wichtigste Regel zum Schutz des lokalen Netzwerks. Mit dieser Regel verfährt die Firewall nach dem Prinzip: "Alles, was nicht ausdrücklich erlaubt ist, bleibt verboten!" Nur mit dieser Strategie kann der Administrator sicher sein, dass er nicht irgendwo eine Zugangsmöglichkeit "vergessen" hat, denn es gibt nur die Zugänge, die er selbst geöffnet hat.

Wir empfehlen die Einrichtung der Deny-All-Regel, bevor das LAN über ein LANCOM mit dem Internet verbunden wird. Anschließend kann man in der Logging-Tabelle (z.B. über LANmonitor zu starten) sehr komfortabel nachvollziehen, welche Verbindungsaufbauten von der Firewall verhindert werden. Mit diesen Informationen wird dann sukzessive die Firewall und "Allow-Regeln" erweitert.

Einige typische Anwendungsfälle sind im Folgenden aufgezeigt.



Alle hier beschriebenen Filter können sehr komfortabel mit dem Firewall-Assistenten eingerichtet werden, um danach bei Bedarf mit z.B. LANconfig weiter verfeinert zu werden.

► Beispielkonfiguration "Basic Internet"

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_HTTP	Lokales Netzwerk	Alle Stationen	Übertragen	HTTP, HTTPS
ALLOW_FTP	Lokales Netzwerk	Alle Stationen	Übertragen	FTP
ALLOW_EMAIL	Lokales Netzwerk	Alle Stationen	Übertragen	MAIL, NEWS
ALLOW_DNS_FORWARDING	Lokales Netzwerk	IP-Adresse des LANOM (alternativ: Lokales Netzwerk)	Übertragen	DNS
DENY_ALL	Alle Stationen	Alle Stationen	Zurückweisen	ANY

► Sofern Sie VPN-Einwahl auf ein LANCOM als VPN-Gateway gestatten wollen, benötigen Sie eine Firewall-Regel, die die Kommunikation des Clients mit dem lokalen Netz erlaubt:

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_VPN_DIAL_IN	Gegenstellename	Lokales Netzwerk	Übertragen	ANY

▷ Die Firewall im LANCOM

- Für den Fall, dass ein VPN nicht vom LANCOM selbst terminiert wird (z.B. VPN-Client im lokalen Netz, oder LANCOM als Firewall vor einem zusätzlichem VPN-Gateway), so müssen Sie zusätzlich IPsec bzw. PPTP (für das 'IPsec over PPTP' des LANCOM VPN Clients) freischalten:

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_VPN	VPN-Client	VPN-Server	Übertragen	IPSEC, PPTP

- Sofern Sie ISDN-Einwahl oder V.110-Einwahl (z.B. per HSCSD-Handy) gestatten, müssen Sie die betreffende Gegenstelle freischalten (siehe auch 'Die Konfiguration von Gegenstellen' →Seite 118):

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_DIAL_IN	Gegenstellename	Lokales Netzwerk	Übertragen	ANY

- Für eine Netzwerkkopplung gestatten Sie zusätzlich die Kommunikation zwischen den beteiligten Netzwerken:

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	Übertragen	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	Übertragen	ANY

- Wenn Sie einen z.B. einen eigenen Webserver betreiben, so schalten Sie selektiv den Server frei:

Regel	Quelle	Ziel	Aktion	Dienst (Zielport)
ALLOW_WEBSERVER	ANY	Webserver	Übertragen	HTTP, HTTPS

- Für Diagnosezwecke empfiehlt sich ferner die Freischaltung des ICMP-Protokolls (z.B. ping):

Regel	Quelle	Ziel	Aktion	Dienst
ALLOW_PING	Lokales Netzwerk	Alle Stationen	Übertragen	ICMP

Diese Regeln können jetzt beliebig verfeinert werden - z.B. durch die Angabe von Mindest- und Maximalbandbreiten für den Serverzugriff, oder aber durch die feinere Einschränkung auf bestimmte Dienste, Stationen oder Gegenstellen.



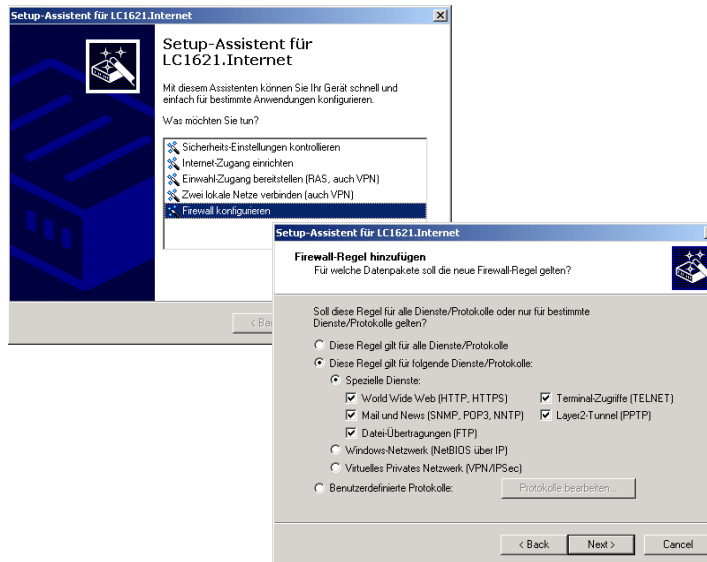
Das LANCOM nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen

werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemein (z.B. Deny-All). Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im nachfolgenden Abschnitt beschrieben.

8.3.8 Konfiguration der Firewall-Regeln

Firewall-Assistent

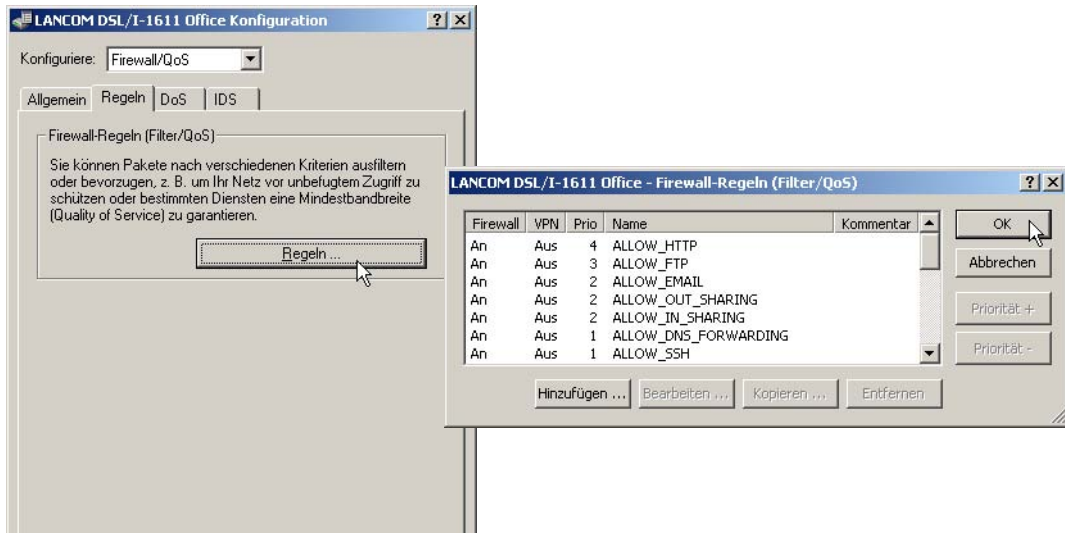
Die schnellste Methode zur Konfiguration der Firewall steht mit dem Firewall-Assistenten in LANconfig zur Verfügung:



LANconfig

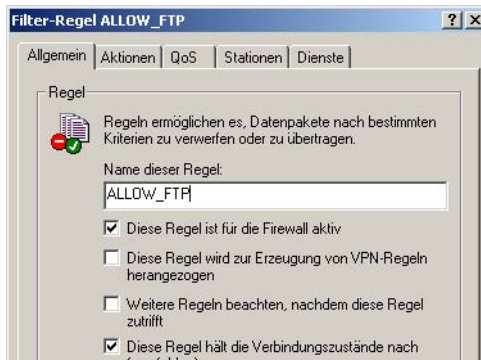
Die Einrichtung der Filter mit Hilfe von LANconfig ist besonders komfortabel. Im Konfigurationsbereich 'Firewall/QoS' befinden sich auf der Registerkarte 'Regeln' die Möglichkeiten zum Bearbeiten und Hinzufügen der Firewall-Regeln.

► Die Firewall im LANCOM

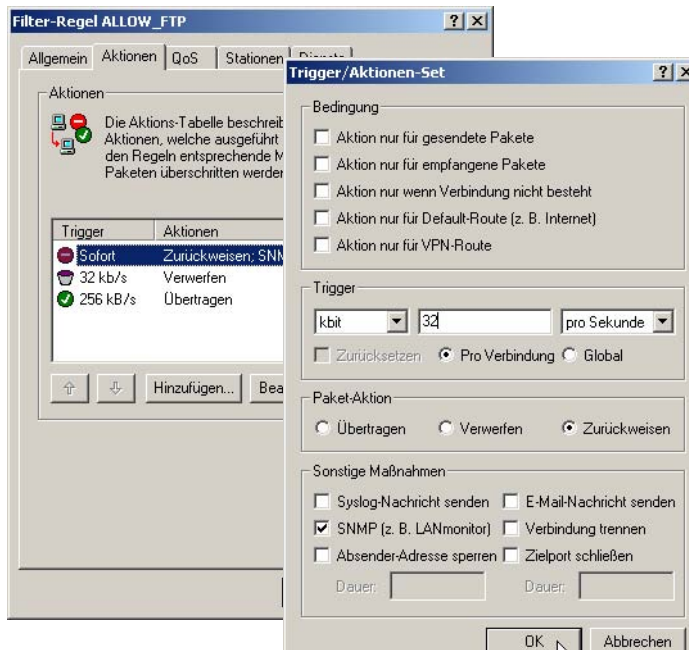


Im Dialog zur Definition der Filterregeln findet man auf den verschiedenen Registerkarten folgende Optionen:

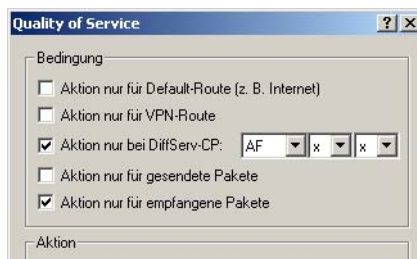
- **Allgemein:** Hier wird der Name der Firewall-Regel festgelegt. Außerdem wird hier definiert, ob weitere Regeln beachtet werden sollen, wenn diese Regel erfüllt wurde, und ob aus dieser Regel eine VPN-Regel abgeleitet werden soll.



- ▷ Mit der Option 'Weitere Regeln beachten...' können z.B. komplexe Funktionen für die Sicherung der Bandbreiten mit QoS realisiert werden ('Verknüpfung' →Seite 186).
 - ▷ Mit der Option 'Diese Regel für die Erzeugung von VPN-Regeln heranziehen' können die Informationen über Quell- und Zielnetzwerke dieser Regel auch für die Bildung von VPN-Netzwerken verwendet werden ('Default-VPN-Regeln' →Seite 182).
- **Aktionen:** Hier legen Sie die Firewall-Aktion fest, bestehend aus Bedingung, Limit, Paket-Aktion und sonstigen Maßnahmen.

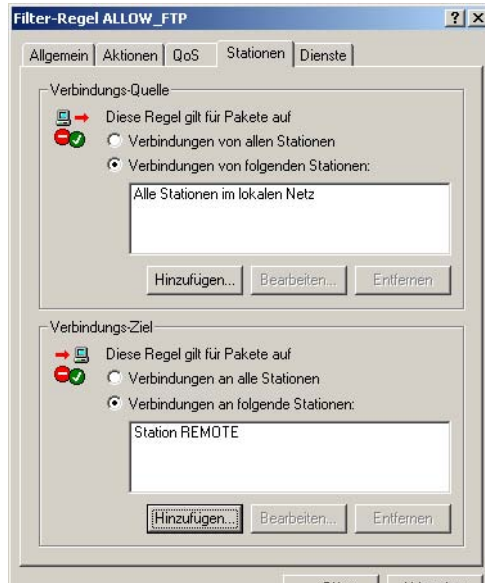


- **QoS:** Hier können Sie Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die betreffende Firewall-Regel spezifiziert sind (siehe auch 'Minimal- und Maximalbandbreiten definieren' →Seite 241).

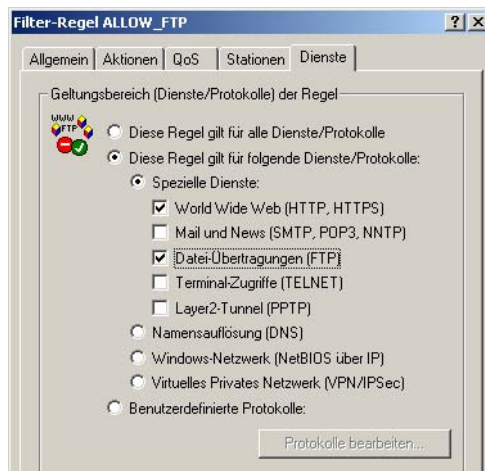


- **Stationen:** Hier werden die Stationen – als Absender oder Adressat der Pakete – festgelegt, für die die Filterregel gelten soll.

► Die Firewall im LANCOM



- **Dienste:** Hier wird festgelegt, für welche IP-Protokolle, Quell- und Zielports die Filterregel gelten soll. Beispielsweise können Sie hier angeben, dass nur der Zugriff auf Internetseiten und E-Mail gestattet sein soll.



WEBconfig, Telnet

Unter WEBconfig oder Telnet werden die Firewall-Regeln in folgenden Menüs und Listen konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration / Setup / IP-Router / Firewall: Regel-Tabelle, Objekt-Tabelle, Aktions-Tabelle
Terminal/Telnet	/Setup/IP-Router/Firewall/Regel-Tabelle, Objekt-Tabelle, Aktions-Tabelle

Zur Beschreibung der Firewall-Regeln gibt es im LCOS eine spezielle Syntax. Diese Syntax erlaubt es, auch komplexe Zusammenhänge für die Prüfung und Behandlung von Datenpakete in der Firewall mit wenigen Zeichen darzustellen.

Die Regeln werden in der Regel-Tabelle definiert. Damit häufig verwendete Objekte nicht jedesmal wieder neu in der LCOS-Syntax eingetragen werden müssen, können in zwei weiteren Tabellen vordefinierte Objekte gespeichert werden:

- ▶ In der Aktionstabelle sind die Firewall-Aktionen enthalten
- ▶ In der Objekttabelle sind die Stationen und Dienste enthalten



Die Objekte aus diesen Tabellen können bei der Regeldefinition verwendet werden, müssen es aber nicht! Sie erleichtern lediglich die Verwendung von häufiger verwendeten Objekten.

Regel-Tabelle

In der Regel-Tabelle werden verschiedene Informationen zu einer Firewall-Regel verknüpft. Die Regel enthält das zu filternde Protokoll, die Quelle, das Ziel sowie die auszuführende Firewall-Aktion. Zusätzlich gibt es für jede Firewall-Regel einen Ein-/Ausschalter, eine Priorität, die Option für eine Verknüpfung mit anderen Regeln und eine Aktivierung der Regel für VPN-Verbindungen. Allgemeine Informationen zu diesen Parametern finden Sie im Abschnitt 'Die Parameter der Firewall-Regeln' →Seite 185.

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekt-Tabelle für Protokolle, Dienste, Stationen (→Seite 206) und der Aktions-Tabelle für die Firewall-Aktionen (→Seite 207) bestehen als auch direkte Beschreibungen in der entsprechenden LCOS-Syntax enthalten (z.B. %P6 für TCP).

▷ Die Firewall im LANCOM

Experten-Konfiguration

- Setup
- IP-Router-Modul
- Firewall

Regel-Tabelle

Name: ALLOW_HTTP

Prot.:

Quelle:

Ziel:

Aktion:

verknuepft:

Prio:

Activ:

VPN-Regel:



Bei der direkten Eingabe der Pegel-Parameter in der LCOS-Syntax gelten die gleichen Regeln, wie sie in den folgenden Abschnitten für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

Objekttabelle

In der Objekt-Tabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regel-Tabelle der Firewall verwendet werden sollen. Objekte können sein:

- ▶ einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- ▶ ganze Netze
- ▶ Protokolle
- ▶ Dienste (Ports oder Port-Bereiche, z.B. HTTP, Mail&News, FTP, ...)

Diese Elemente lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z.B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man drauf aufbauend Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

In der Objekttablette können die Stationen und Dienste nach folgenden Regeln beschrieben werden:

Beschreibung	Objekt-ID	Beispiele und Bemerkungen
lokales Netz	%L	
Gegenstellen	%H	Name muss in DSL-/ISDN-/PPTP- oder VPN-Gegenstellenliste stehen
Hostname	%D	Hinweis zu Hostnamen beachten (→Seite 189)
MAC-Adresse	%E	00:A0:57:01:02:03
IP-Adresse	%A	%A10.0.0.1, 10.0.0.2; %A0 (alle Adressen)
Netzmaske	%M	%M255.255.255.0
Protokoll (TCP/UDP/ICMP etc.)	%P	%P6 (für TCP)
Dienst (Port)	%S	%S20-25 (für Ports 20 bis 25)

Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen. Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt.

The screenshot shows the 'Experten-Konfiguration' window with a tree view containing 'Setup', 'IP-Router-Modul', and 'Firewall'. Below this is the 'Objekt-Tabelle' section with two input fields: 'Name' containing 'FTP' and 'Beschreibung' containing '%P6 %S21'. At the bottom are 'Setzen' and 'Zurücksetzen' buttons.



Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Ziel, Quelle) jeweils in Anführungszeichen (Zollzeichen: ") eingeschlossen werden.

Aktionstabelle

Wie schon dargestellt, besteht eine Firewall-Aktion aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen. In der Aktionstabelle werden die Firewall-Aktionen als beliebige Kombinationen aus den folgenden Elementen zusammengestellt:

▷ Die Firewall im LANCOM

► Bedingungen

Bedingung	Beschreibung	Objekt-ID
Connect-Filter	Der Filter ist aktiv, wenn keine physikalische Verbindung zum Ziel des Pakets besteht	@c
DiffServ-Filter	Der Filter ist aktiv, wenn das Paket den angegebenen Differentiated Services Code Point (DSCP) enthält (siehe 'ToS- und DiffServ-Felder auswerten' →Seite 239)	@d (plus DSCP)
Internet-Filter	Der Filter ist aktiv, wenn das Paket über die Defaultroute empfangen wurde oder gesendet werden soll	@i
VPN-Filter	Der Filter ist aktiv, wenn das Paket über eine VPN-Verbindung empfangen wurde oder gesendet werden soll	@v

Wenn zum "Connect-" oder "Internet-" Filter keine weitere Aktion angegeben wird, dann wird implizit eine Kombination dieser Filter mit der "Reject" Aktion angenommen.

► Limits

Jede Firewall-Aktion kann mit einem Limit verknüpft werden, dessen Überschreitung zur Auslösung der Aktion führt. Über mehrere Limits für einen Filter sind dadurch auch Aktionsketten möglich.

Limit-Objekte werden dabei allgemein mit %L eingeleitet, gefolgt von

- ▷ Bezug: verbindungsbezogen (c) oder global (g)
- ▷ Art: Datenrate (d), Anzahl der Pakete (p) oder Paketrate (b)
- ▷ Wert des Limits
- ▷ Weitere Parameter (z.B. Zeitraum und Größe)

Es stehen folgende Limitierungen zur Verfügung:

Limit	Beschreibung	Objekt-ID
Data (abs)	Absolute Anzahl von Kilobytes auf der Verbindung nach denen die Aktion ausgeführt wird	%lcd
Data (rel)	Anzahl von Kilobytes/Sekunde, Minute, Stunde auf der Verbindung nach denen die Aktion ausgeführt wird	%lcds %lcdm %lcdh
Packet (abs)	Absolute Anzahl von Paketen auf der Verbindung nach denen die Aktion ausgeführt wird	%lcp
Packet (rel)	Anzahl von Paketen/Sekunde Minute, Stunde oder absolut auf der Verbindung nach denen die Aktion ausgeführt wird	%lcps %lcpm %lcpH
global Data (abs)	Absolute Anzahl von Kilobytes, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgd
global Data (rel)	Anzahl von Kilobytes/Sekunde, Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgds %lgdm %lgdh
global Packet (abs)	Absolute Anzahl von Paketen, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	%lgp

Limit	Beschreibung	Objekt-ID
global Packet (rel)	Anzahl von Paketen/Sekunde Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurden, nach denen die Aktion ausgeführt wird	%lgps %lgpm %lgph
receive Option	Beschränkung des Limits auf die Empfangsrichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdsr %lcdsr
transmit Option	Beschränkung des Limits auf die Senderichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdst %lcdst



Wird eine Aktion ohne Limit angegeben, so wird implizit ein Paket-Limit angenommen, welches sofort beim ersten Paket überschritten wird.

► Paket-Aktionen

Paket-Aktion	Beschreibung	Objekt-ID
Accept	Das Paket wird angenommen	%a
Reject	Das Paket wird mit einer passenden Fehlermeldung zurückgewiesen	%r
Drop	Das Paket wird stillschweigend verworfen	%d

Diese Pakete-Aktionen sind beliebig miteinander kombinierbar, wobei bei widersinnigen oder nicht eindeutigen Aktionen (z.B.: Accept + Drop) die sicherere, d.h. im Beispiel "Drop" genommen wird.

► Sonstige Maßnahmen

Maßnahmen	Beschreibung	Objekt-ID
Syslog	Gibt eine detaillierte Meldung über Syslog aus	%s
Mail	Schickt eine E-Mail an den Administrator	%m
SNMP	Sendet einen SNMP-Trap	%n
Close-Port	Schließt den Zielport des Pakets für eine einstellbare Zeit	%p
Deny-Host	Sperrt die Absender-Adresse des Pakets für eine einstellbare Zeit	%h
Disconnect	Trennt die physikalische Verbindung zur Gegenstelle, über die das Paket empfangen wurde oder gesendet werden sollte	%t
Zero-Limit	Setzt den Limit-Counter (s.u.) bei überschreiten der Trigger-Schwelle wieder auf 0	%z
Fragmentierung	erzwingt die Fragmentierung aller nicht auf die Regel passenden Pakete	%f

Die Firewall im LANCOM

Wenn die "Close-Port" Aktion ausgeführt wird, wird ein Eintrag in einer Sperrliste vorgenommen, durch den alle Pakete, die an den jeweiligen Rechner und Port gesendet werden, verworfen werden. Für das "Close-Port"-Objekt kann eine Sperrzeit in Sekunden, Minuten oder Stunden angegeben werden, die direkt hinter der Objekt-ID vermerkt wird. Diese Zeitangabe baut sich zusammen aus dem Bezeichner für die Zeiteinheit (h, m, s für Stunde, Minute und Sekunde) sowie der eigentlichen Zeitangabe. So sperrt z.B. %pm10 den Port für 10 Minuten. Wird keine Zeiteinheit angegeben, so wird "Minuten" als Einheit angenommen. (damit ist %p10 gleichbedeutend mit %pm10)

Wird die "Deny-Host" Aktion ausgeführt, so wird der Absender des Pakets in eine Sperrliste eingetragen. Ab diesem Moment werden alle Pakete, die von dem gesperrten Rechner empfangen werden verworfen. Auch das "Deny-Host"-Objekt kann mit einer Sperrzeit versehen werden, die wie bei der "Close-Port" Option beschrieben gebildet wird.

Will man z.B. die Datenrate, die für eine Verbindung zulässig ist, auf 8 KBit/s limitieren, und bei einem Flooding-Versuch den Angreifer aussperren sowie eine Email an den Administrator senden, dann lautet die Objektbeschreibung für die Aktion wie folgt:

The screenshot shows the configuration interface for a firewall rule. The breadcrumb path is: Experten-Konfiguration > Setup > IP-Router-Modul > Firewall. The title of the configuration page is 'Objekt-Tabelle'. There are two input fields: 'Name' with the value 'CLOSE_ON_FLOODING' and 'Beschreibung' with the value '%a.%lcds8%d %lgbs100%h10%m'. At the bottom of the form are two buttons: 'Setzen' and 'Zurücksetzen'.

- ▶ Diese Beschreibung erlaubt zunächst den Datenverkehr (%a). Ein einfaches %a am Anfang der Beschreibung ist im übrigen gleichbedeutend mit einem %lp0%a (= Akzeptiere, wenn das Limit von Null Paketen überschritten wurde, d.h. beim ersten Paket).
- ▶ Wenn über die aktuelle Verbindung in einer Sekunde nun 8 kBit (%lcds8) übertragen wurden, dann werden alle weiteren Pakete bis zum Ablauf der Sekunde stillschweigend verworfen (%d), wodurch sich automatisch ein Traffic-Shaping ergibt.
- ▶ Treffen aber in einer Sekunde 100 Pakete für den Server (Ziel-Adresse der Verbindung) ein (%lgbs100), so wird der entfernte Host (Quell-Adresse) für 10 Minuten gesperrt (%h10) und eine E-Mail an den Administrator geschickt (%m)

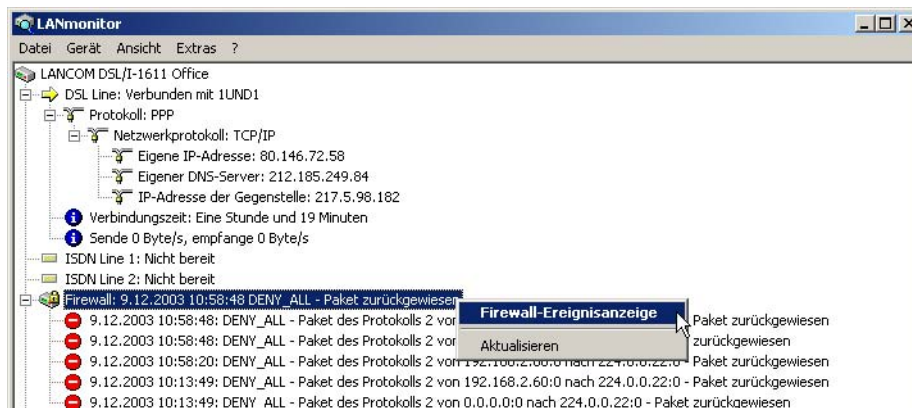
Die Aktionsobjekte können wie bereits die Protokoll-, Adress- und Dienstobjekte in der Objekt-Tabelle mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden.

Beim Aufbau der eigentlichen Filter-Tabelle werden die Aktionsobjekte dann genau so wie Protokoll-, Adress- und Dienstobjekte auf die kleinste notwendige Anzahl reduziert, d.h. Mehrfachdefinitionen einer Aktion werden eliminiert und bei widersprüchlichen Aktionen wird die "sicherste" ausgewählt. So wird z.B. aus %a (Accept) und %d (Drop) nur %d und aus %r (Reject) und %d wird %r.

8.3.9 Firewall-Diagnose

Alle Ereignisse, Zustände und Verbindungen der Firewall können detailliert protokolliert und überwacht werden.

Die komfortabelste Überwachung ergibt sich mit der Anzeige der Logging-Tabelle (s. u.) durch den LANmonitor. Im LANmonitor werden im Bereich 'Firewall' die letzten fünf Ereignisse angezeigt, die durch eine Firewall-Regel, das DoS- oder IDS-System mit aktivierter 'SNMP'-Option ausgelöst wurden.



Mit einem Klick der rechten Maustaste auf diese Rubrik öffnet sich im Kontextmenü unter dem Eintrag **Firewall-Ereignisanzeige** ein neues Fenster mit der vollständigen Logging-Tabelle (→Seite 211).

Alle in diesem Abschnitt beschriebenen Listen und Tabellen finden Sie unter folgenden Menüpunkten:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration / Status / IP-Router-Statistik
Terminal/Telnet	/Status/IP-Router-Statistik

Die Firewall-Tabelle

Wenn ein zu loggendes Ereignis eingetreten ist, d.h. als auszuführende Aktion beim Empfang eines Paketes ist eine Mitteilung per E-Mail, Syslog oder SNMP gefordert, so wird dieses Ereignis in einer Logging-Tabelle festgehalten.

Wird die Logging-Tabelle über den LANmonitor aufgerufen, präsentiert sie sich in folgender Darstellung:

► Die Firewall im LANCOM

Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Protokoll	Quell-Port	Ziel-Port	Firewall-Regel	Limit	Aktion
1	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
2	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
3	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
4	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
5	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
6	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
7	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
8	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
9	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
10	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet
11	8.12.2003 20:16:55	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewiesen; SNMP gesendet

Wird die Logging-Tabelle über WEBconfig aufgerufen, präsentiert sie sich in folgender Darstellung:

[Experten-Konfiguration](#)
[Status](#)
[IP-Router-Statistik](#)

Log-Tabelle

Idx.	System-Zeit	Quell-Adresse	Ziel-Adresse	Prot.	Quell-Port	Ziel-Port	Filterregel	Limit	Schwelle	Aktion
0001	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0002	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0003	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0004	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0005	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0006	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0007	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0008	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0009	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
000a	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108

Diese Tabelle enthält die folgenden Werte:

Element	Bedeutung
Idx.	laufender Index (damit die Tabelle auch über SNMP abgefragt werden kann)
System-Zeit	System-Zeit in UTC Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt)
Quell-address	Quell-Adresse des gefilterten Pakets
Ziel-address	Zieladresse des gefilterten Pakets
Prot.	Protokoll (TCP, UDP etc.) des gefilterten Pakets
Quell-Port	Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)
Ziel-Port	Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)

Element	Bedeutung
Filterregel	Name der Regel, die den Eintrag erzeugt hat.
Limit	Bitfeld, das das überschrittene Limit beschreibt, durch welches das Paket gefiltert wurde. Es sind zur Zeit folgende Werte definiert: 0x01 Absolute Anzahl, 0x02 Anzahl pro Sekunde, 0x04 Anzahl pro Minute, 0x08 Anzahl pro Stunde, 0x10 globales Limit, 0x20 Bytelimit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit), 0x40 limit gilt nur in Empfangsrichtung, 0x80 limit gilt nur in Senderichtung
Schwelle	überschrittener Grenzwert des auslösenden Limits
Action	Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind zur Zeit folgende Werte definiert: 0x00000001 Accept 0x00000100 Reject 0x00000200 Aufbaufilter 0x00000400 Internet- (Defaultrouten-) Filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Quell-Adresse sperren 0x00020000 Zieladresse und -port sperren 0x20000000 Sende Syslog-Benachrichtigung 0x40000000 Sende SNMP-Trap 0x80000000 Sende E-Mail



Alle Firewall-Aktionen werden ebenfalls im IP-Router-Trace angezeigt ('So starten Sie einen Trace' →Seite 81). Einige LANCOM-Modelle verfügen ferner über eine Firewall-LED, welche jedes gefilterte Paket signalisiert.

Die Filterliste

Über die Filterliste können die aus den in der Aktions-, Objekt- und Regeltabelle definierten Regeln erzeugten Filter ermittelt werden.



Bei einer manuellen Filter-Definition über Telnet oder WEBconfig wird kein Eintrag in der Filterliste angelegt, wenn die Definition Fehler in der Syntax enthält. In diesem Fall wird auch keine Fehlermeldung ausgegeben! Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall anhand der Filterliste überprüfen, ob die gewünschten Filter erzeugt wurden.

Auf Telnet-Ebene kann der Inhalt der Filterliste auch mit dem Kommando `show filter` angezeigt werden:

▷ Die Firewall im LANCOM

```

Telnet 192.168.2.100

#
: LANCOM DSL/I-1611 Office
: Ver. 3.30.0003 / 12.11.2003
: SN. 000590300000
: Copyright (c)

Verbindung Nr.: 002 <LAN>
Passwort:
: /
> show filter

Filter 0001 from Rule ALLOW_PPTP:
Protocol: 187
Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
Limit per conn.: after transmitting or receiving of 0 kilobits per second
actions after exceeding the limit:
accept

Filter 0002 from Rule ALLOW_UPN:
Protocol: 108
Src: 00:00:00:00:00:00 192.168.2.0 255.255.255.0 0-0
Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 500-500
Limit per conn.: after transmitting or receiving of 0 kilobits per second
actions after exceeding the limit:
accept
    
```

Unter WEBconfig hat die Filterliste den folgenden Aufbau:

Experten-Konfiguration

- Status
- IP-Router-Statistik

Filter-Liste

Idx.	Prot.	Quell-MAC	Quell-Adresse	Quell-Netz-Maske	Q-von	Q-bis	Ziel-MAC	Ziel-Adresse	Ziel-Netz-Maske	Z-von	Z-bis	Aktion
0001	187	000000000000	0.0.0.0	0.0.0.0	0	0	000000000000	0.0.0.0	0.0.0.0	0	0	limit: accept
0002	108	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept
0003	51	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept
0004	50	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept
0005	17	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0	0	0	limit: inet: reject
0006	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept
0007	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	192.168.2.100	255.255.255.255	53	53	limit: accept

Die einzelnen Felder in der Filterliste haben folgende Bedeutung:

Eintrag	Beschreibung
Idx.	laufender Index
Prot	zu filterndes Protokoll, also z.B. 6 für TCP oder 17 für UDP
Quell-MAC	Ethernet-Quell-Adresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Quell-Adresse	Quell-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Quell-Netzmaske	Quell-Netzmaske, die zusammen mit der Quell-IP-Adresse das Quell-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete aus allen Netzen gelten soll


Eintrag	Beschreibung
Q-von	Start-Quell-Port der zu filternden Pakete.
Q-bis	End-Quell-Port der zu filternden Pakete. Spannt zusammen mit dem Start-Quell-Port einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Quell-Ports
Ziel-MAC	Ethernet-Zieladresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Ziel-Adresse	Ziel-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Ziel-Netzmaske	Ziel-Netzmaske, die zusammen mit der Ziel-IP-Adresse das Ziel-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete zu allen Netzen gelten soll
Z-von	Start-Zielport der zu filternden Pakete.
Z-bis	End-Zielport der zu filternden Pakete. Spannt zusammen mit dem Start-Zielport einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Zielports
Aktion	In dieser Spalte wird die "Hauptaktion", also die Aktion textuell ausgegeben, die bei überschreiten des ersten Limits ausgeführt wird. Das erste Limit kann auch ein implizites Limit sein, so z.B. wenn nur ein Limit zur Beschränkung des Durchsatzes konfiguriert wurde, so wird ein implizites Limit, das mit einer "accept" Aktion verknüpft ist eingefügt. Als Hauptaktion wird in diesem Fall "accept" ausgegeben. Die vollständigen Aktionen lassen sich über das Kommando <code>show filter anzeigen</code>
verknüpft	Gibt an, ob es sich bei dieser Regel um eine "First Match"-Regel handelt (verknüpft = Nein). Nur bei verknüpften Regeln werden im Falle des Zutreffens dieser Regel auch weitere Regeln ausgewertet.
Prio	Priorität der Regel, durch die der Eintrag erzeugt wurde.


Die Verbindungsliste

In der Verbindungstabelle werden Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port, Ziel-Port, etc. einer Verbindung nachgehalten sowie mögliche Aktionen gespeichert. Diese Tabelle ist sortiert nach Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port und Ziel-Port des Pakets, das den Eintrag in der Tabelle hervorgerufen hat.





Unter WEBconfig hat die Filterliste den folgenden Aufbau:

[Experten-Konfiguration](#)

 [Status](#)

 [IP-Router-Statistik](#)

Verbindungsliste

	Quell-Adresse	Ziel-Adresse	Prot.	Quell-Port	Ziel-Port	Timeout	Flags	Filterregel	Quell-Route	Ziel-Route
	192.168.2.60	212.227.15.133	6	3584	110	8	00020038	ALLOW_MAIL	1UND1	
	192.168.2.60	212.227.15.133	6	3586	110	9	00020038	ALLOW_MAIL	1UND1	
	192.168.2.60	212.227.15.133	6	3588	110	300	00020008	ALLOW_MAIL	1UND1	
	192.168.2.60	217.72.195.42	6	3577	80	25	00020001	ALLOW_HTTP	1UND1	

▷ Die Firewall im LANCOM

Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Quell-Adresse	Quell-Adresse der Verbindung
Ziel-Adresse	Ziel-Adresse der Verbindung
Protocol	verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben
Quell-Port	Quell-Port der Verbindung. Der Port wird nur bei portbehafteten Protokollen (TCP/UDP) oder Protokollen, die ein vergleichbares Feld besitzen (ICMP/GRE) angegeben
Ziel-Port	Ziel-Port der Verbindung (bei UDP-Verbindungen wird dieser erst mit der ersten Antwort besetzt)
Timeout	Jeder Eintrag altert mit der Zeit aus dieser Tabelle heraus, damit die Tabelle bei "gestorbenen" Verbindungen nicht überläuft
Flags	In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert (→Seite 216). Als Zustände sind folgende Werte möglich: new, establish, open, closing, closed, rejected (entsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST) UDP-Verbindungen kennen nun die Zustände new, open und closing (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z.B. beim Protokoll H.323 der Fall)
Quell-Route	Name der Gegenstelle, über die das erste Paket empfangen wurde.
Ziel-Route	Name der Gegenstelle, auf die das erste Paket gesendet wird.
Filterregel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Bedeutung der Flags in der Verbindungsliste

Flag	Bedeutung
00000001	TCP: SYN gesendet
00000002	TCP: SYN/ACK empfangen
00000004	TCP: warte auf ACK des Servers
00000008	alle: Verbindung offen
00000010	TCP: FIN empfangen
00000020	TCP: FIN gesendet
00000040	TCP: RST gesendet oder empfangen
00000080	TCP: Sitzung wird wiederhergestellt
00000100	FTP: passive FTP-Verbindung wird aufgebaut
00000400	H.323: zugehörige T.120-Verbindung
00000800	Verbindung über Loopback-Interface
00001000	prüfe verkettete Regeln

Flag	Bedeutung
00002000	Regel ist verkettet
00010000	Ziel ist auf "lokaler Route"
00020000	Ziel ist auf Default-Route
00040000	Ziel ist auf VPN-Route
00080000	physikalische Verbindung ist nicht aufgebaut
00100000	Quelle ist auf Default-Route
00200000	Quelle ist auf VPN-Route
00800000	keine Route zum Ziel
01000000	enthält globale Aktion mit Bedingung

Portsperrliste

Wenn als Aktion die Sperrung des Zielports auf dem Zielrechner ausgewählt wurde, so werden Adresse, Protokoll und Port des Zielrechners in der Portsperrtabelle abgelegt. Diese Tabelle ist ebenfalls eine sortierte halbdynamische Tabelle. Die Sortierung erfolgt nach Adresse, Protokoll und Port. Die Tabelle enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, für den die Sperre gelten soll.
Protocol	Verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben.
Port	Zu sperrender Port auf dem Rechner. Wenn das jeweilige Protokoll nicht portbehaftet ist, dann wird das gesamte Protokoll für diesen Rechner gesperrt.
Timeout	Dauer der Sperre in Minuten.
Filterregel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Hostsperrliste

Wenn als Aktion eines Filters die Sperrung des Absenders ausgewählt wurde, so werden Adresse des Rechners in der Hostsperrtabelle abgelegt. Diese Tabelle ist eine nach der Absenderadresse sortierte halbdynamische Tabelle und enthält die folgenden Elemente:

Element	Bedeutung
Address	Adresse des Rechners, der gesperrt werden soll
Timeout	Dauer der Sperre in Minuten
Filter-Regel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

▷ Abwehr von Einbruchsversuchen: Intrusion Detection

8.3.10 Grenzen der Firewall

Neben dem Verständnis der Funktionsweise der Firewall ist es auch sehr wichtig, ihre Grenzen zu erkennen und sie ggf. weiter zu ergänzen. So schützt die Firewall grundsätzlich nicht vor bösartigen Inhalten, die auf den zugelassenen Wegen in das lokale Netzwerk gelangen. Die Auswirkungen einiger Viren und Würmer werden zwar unterbunden, weil die Kommunikation über die benötigten Ports gesperrt ist, aber einen echten Schutz vor Viren bietet die Firewall allein nicht.

Auch das Abhören von sensiblen Daten im Internet wird durch die Firewall nicht verhindert. Sind die Daten erst einmal über die Firewall hinaus in das unsichere Netz gelangt, stehen sie dort weiterhin den bekannten Gefahren gegenüber. Vertrauliche Informationen wie Verträge, Passwörter, Entwicklungsinformationen etc. sollten daher auch bei Einsatz einer Firewall nur geschützt übertragen werden, z.B. durch den Einsatz geeigneter Verschlüsselungsverfahren oder über VPN-Verbindungen.

8.4 Abwehr von Einbruchsversuchen: Intrusion Detection

Die Firewall hat die Aufgabe, den Datenverkehr über die Grenzen zwischen den Netzwerken hinweg zu prüfen und diejenigen Datenpakete, die keine Erlaubnis für die Übertragung mitbringen, zurückzuweisen bzw. zu verwerfen. Neben dem Ansatz, direkt auf einen Rechner im geschützten Netzwerk zuzugreifen, gibt es aber auch Angriffe auf die Firewall selbst oder Versuche, die Firewall mit gefälschten Datenpaketen zu überlisten.

Solche Versuche werden über ein Intrusion-Detection-System (IDS) erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYSLOG-Alarmen gewählt werden. Das IDS prüft den Datenverkehr auf bestimmte Eigenschaften hin und erkennt so auch neue Angriffe, die nach auffälligen Mustern ablaufen.

8.4.1 Beispiele für Einbruchsversuche

Als typische Einbruchsversuche kann man gefälschte Absender-Adressen ("IP-Spoofing") und Portscans ansehen, sowie den Missbrauch spezieller Protokolle wie z.B. FTP, um einen Port im angegriffenen Rechner und der davor hängenden Firewall zu öffnen.

IP-Spoofing

Beim IP-Spoofing gibt sich der Absender eines Pakets als ein anderer Rechner aus. Dies geschieht entweder, um Firewalls überlisten, die Paketen aus dem eigenen Netz mehr Vertrauen schenken als Paketen aus fremden Netzen, oder um den Urheber eines Angriffs (z.B. Smurf) zu verschleiern.

Die LANCOM Firewall schützt sich davor durch Routenprüfung, d.h. sie überprüft, ob das Paket überhaupt über das Interface empfangen werden durfte, von dem es empfangen wurde.

Portscan-Erkennung

Das Intrusion-Detection System versucht Portscans zu erkennen, zu melden und geeignet auf den Angriff zu reagieren. Dies geschieht ähnlich der Erkennung eines 'SYN Flooding'-Angriffs (siehe 'SYN Flooding' →Seite 220): Es wer-

▶ *Abwehr von Einbruchsversuchen: Intrusion Detection*

den auch hier die "halboffenen" Verbindungen gezählt, wobei ein TCP-Reset, das vom gescannten Rechner gesendet wird, die "halboffene" Verbindung weiterhin offen lässt.

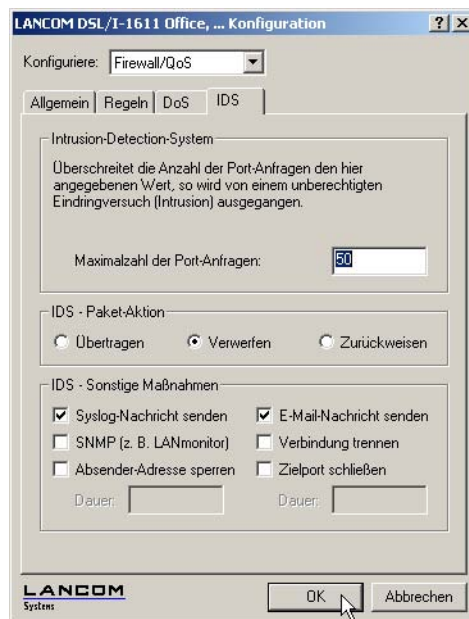
Wenn eine bestimmte Anzahl von halboffenen Verbindungen zwischen dem gescannten und dem scannenden Rechner existiert, so wird dies als Portscan gemeldet.

Ebenso wird der Empfang von leeren UDP-Paketen als versuchter Portscan interpretiert

8.4.2 Konfiguration des IDS

LANconfig

Die Parameter des Intrusion Detection Systems werden im LANconfig im Konfigurationsbereich 'Firewall/QoS' auf der Registerkarte 'IDS' festgelegt:



Neben der Maximalzahl der Portanfragen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- ▶ Die Verbindung wird getrennt
- ▶ Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- ▶ Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

▷ Schutz vor "Denial-of-Service"-Angriffen

WEBconfig,
Telnet

Die Verhaltensweise des Intrusion Detection Systems wird unter WEBconfig oder Telnet hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router/Firewall
Terminal/Telnet	Setup/IP-Router/Firewall

8.5 Schutz vor "Denial-of-Service"-Angriffen

Angriffe aus dem Internet können neben Einbruchversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Diese Angriffe nennt man auch "Denial-Of-Service". LANCOM-Geräte sind mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit erhalten.

8.5.1 Beispiele für Denial-of-Service-Angriffe

Denial-Of-Service-Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementierungen von TCP/IP-Protokollstacks aus. Zu den Angriffen, die prinzipiellen Schwächen ausnutzen, gehören z.B. SYN-Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementierungen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z.B. Teardrop), oder die mit gefälschten Absenderadressen arbeiten (z.B. Land). Im folgenden werden einige dieser Attacken, deren Auswirkungen und mögliche Gegenmaßnahmen beschrieben.

SYN Flooding

Beim SYN-Flooding schickt der Angreifer in kurzen zeitlichen Abständen TCP-Pakete, mit gesetztem SYN-Flag und sich ständig ändernden Quell-Ports auf offene Ports seines Opfers. Der angegriffene Rechner richtet darauf hin eine TCP-Verbindung ein, sendet dem Angreifer ein Paket mit gesetztem SYN- und ACK-Flags und wartet nun vergeblich auf die Bestätigung des Verbindungsaufbaus. Dadurch bleiben dann hunderte "halboffener" TCP-Verbindungen zurück, und verbrauchen Ressourcen (z.B. Speicher) des angegriffenen Rechners. Das ganze kann letztendlich so weit gehen, dass das Opfer keine TCP-Verbindung mehr annehmen kann oder gar aufgrund von Speichermangel abstürzt. Als Gegenmaßnahme in einer Firewall hilft nur, die Anzahl "halboffener" TCP-Verbindungen, die zwischen zwei Rechnern bestehen zu überwachen und zu beschränken, d.h. falls weitere TCP-Verbindungen zwischen diesen Rechnern aufgebaut werden, dann müssen diese von der Firewall abgeblockt werden.

Smurf

Der Smurf-Angriff arbeitet zweistufig und legt gleich zwei Netze lahm. Im ersten Schritt wird mit gefälschter Absenderadresse ein Ping (ICMP Echo-Request) an die Broadcastadresse des erste Netzes gesendet, worauf alle Rechner in diesem Netz mit einem ICMP-Echo-Reply und die gefälschte Absenderadresse (die im zweiten Netz liegt) antworten. Wenn die Rate der einkommenden Echo-Requests sowie die Anzahl der antwortenden Rechner hoch genug ist, dann wird zum einen der gesamte einkommende Traffic des zweiten Netzes für die Dauer der Attacke blockiert, zum anderen kann der Besitzer der gefälschten Adresse für die Dauer der Attacke keine normalen Daten mehr annehmen.

▷ Schutz vor "Denial-of-Service"-Angriffen

Ist die gefälschte Absenderadresse die Broadcastadresse des zweiten Netzes, so sind sogar alle Rechner in diesem Netz blockiert.

In diesem Fall blockiert die DoS-Erkennung des LANCOM das Weiterleiten von Paketen, die an die lokale Broadcastadresse gerichtet sind.

LAND

Beim LAND-Angriff handelt es sich um ein TCP-Paket, das mit gesetztem SYN-Flag und gefälschter Absenderadresse an den Opferrechner geschickt wird. Das Pikante dabei ist, dass die gefälschte Absenderadresse gleich der Adresse des Opfers ist. Bei einer unglücklichen Implementierung des TCP wird das auf dieses Paket gesendete SYN-ACK vom Opfer wieder als "SYN" interpretiert und ein neues SYN-ACK gesendet. Dies führt zu einer Endlosschleife, die den Rechner einfrieren lässt.

Bei einer neueren Variante wird als Absenderadresse des Pakets nicht die Adresse des angegriffenen Rechners eingesetzt, sondern die Loopback-Adresse "127.0.0.1". Sinn dieser Täuschung ist es, Personal Firewalls zu überlisten, die zwar auf die klassische Variante (Absenderadresse = Zieladresse) reagieren, die neue Form aber ungehindert durchlassen. Diese Form wird vom LANCOM ebenfalls erkannt und geblockt.

Ping of Death

Der Ping of Death gehört zu den Angriffen, die Fehler bei der Reassemblierung von fragmentierten Paketen ausnutzen. Dies funktioniert wie folgt:

Im IP-Header befindet sich das Feld "Fragment-Offset" das angibt, an welcher Stelle das empfangene Fragment in das IP-Paket eingebaut werden soll. Dieses Feld hat eine Länge 13 Bit und gibt die Einfügeposition in jeweils 8 Byte grossen Schritten an. Die Einfügeposition kann daher zwischen 0 und 65528 Bytes liegen. Bei einer MTU auf dem Ethernet von 1500 Bytes kann somit ein bis zu $65528 + 1500 - 20 = 67008$ Byte großes IP-Paket erzeugt werden, was zu Überläufen von internen Zählern führen oder gar Pufferüberläufe provozieren kann und es somit dem Angreifer gar die Möglichkeit eröffnet, eigenen Code auf dem Opferrechner auszuführen.

Hier bieten sich der Firewall zwei Möglichkeiten: Entweder, die Firewall re-assembliert das gesamte einkommende Paket und prüft dessen Integrität, oder aber es wird nur das Fragment, das über die maximale Paketgröße hinaus geht, verworfen. Im ersten Fall kann die Firewall bei einer fehlerhaften Implementation selbst zum Opfer werden, im zweiten Fall sammeln sich beim Opfer "halb" reassemblierte Pakete an, die erst nach einer gewissen Zeit verworfen werden, wodurch sich ein neuer Denial-Of-Service Angriff ergeben kann, wenn dem Opfer dadurch der Speicher ausgeht.

Teardrop

Der Teardrop-Angriff arbeitet mit überlappenden Fragmenten. Dabei wird nach dem ersten Fragment ein weiteres geschickt, das komplett innerhalb des ersten liegt, d.h. das Ende des zweiten Fragments liegt vor dem Ende des ersten. Wird nun aus Bequemlichkeit des Programmierers des IP-Stack bei der Ermittlung der Länge der zur Reassemblierung zu kopierenden Bytes einfach "neues Ende" - "altes Ende" gerechnet, so ergibt sich ein negativer Wert, bzw. ein sehr großer positiver wert, durch den bei der Kopieroperation Teile des Speichers des Opfers überschrieben werden und der Rechner daraufhin abstürzt.

▷ Schutz vor "Denial-of-Service"-Angriffen

Auch hier hat die Firewall wieder zwei Möglichkeiten: Entweder sie reassembliert selbst und verwirft ggf. das gesamte Paket, oder sie hält nur minimalen Offset und maximales Ende des Pakets nach und verwirft alle Fragmente, deren Offset oder Ende in diesen Bereich fallen. Im ersten Fall muss die Implementation innerhalb der Firewall korrekt sein, damit diese nicht selbst Opfer wird, im anderen Fall sammeln sich wieder "halb" reassemblierte Pakete beim Opfer.

Bonk/Fragrouter

Bonk ist eine Variante des Teardrop-Angriffs, die jedoch nicht zum Ziel hat den angegriffenen Rechner zum Absturz zu bringen, sondern einfache Portfilter Firewalls, die auch fragmentierte Pakete akzeptieren auszutricksen und somit in das zu schützende Netz einzudringen. Bei diesem Angriff wird nämlich durch geschickte Wahl des Fragment-Offsets der UDP- oder TCP-Header des ersten Fragments überschrieben. Hierdurch akzeptieren einfache Portfilter-Firewalls das erste Paket und die dazugehörigen Fragmente. Durch das Überschreiben des Headers im zweiten Fragment, wird so ganz plötzlich aus einem erlaubten Paket ein Paket, das eigentlich in der Firewall geblockt werden sollte.

Auch hier gilt, die Firewall kann entweder selbst Re-assemblieren, oder nur das falsche Fragment (und alle nachfolgenden) filtern, mit den bereits oben angedeuteten Problemen der einen oder anderen Lösung.



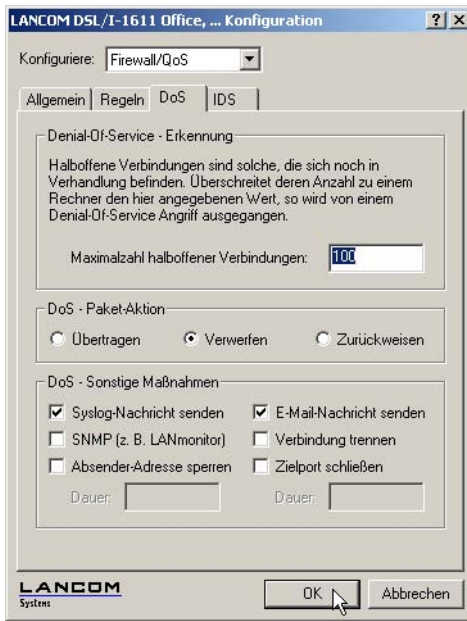
In der Default-Einstellung sind alle Einstellungen auf "sicher" konfiguriert, d.h. maximal 100 zulässige halb-offene Verbindungen von verschiedenen Rechnern (vgl. SYN-Flooding), maximal 50 halboffene Verbindungen von einem Rechner (vgl. Portscan) fragmentierte Pakete werden re-assembliert.

8.5.2 Konfiguration der DoS-Abwehr

LANconfig

Die Parameter gegen die DoS-Attacken werden im LANconfig im Konfigurationsbereich 'Firewall/QoS' auf der Registerkarte 'DoS' festgelegt:

► Schutz vor "Denial-of-Service"-Angriffen



Um die Anfälligkeit des Netzes vor DoS-Attacken schon im Vorfeld drastisch zu reduzieren, dürfen Pakete aus entfernten Netzen nur dann angenommen werden, wenn entweder eine Verbindung vom internen Netz aus initiiert wurde, oder die einkommenden Pakete durch einen expliziten Filtereintrag (Quelle: entferntes Netz, Ziel: lokales Netz) zugelassen werden. Diese Maßnahme blockiert bereits eine Vielzahl von Angriffen.

Für alle erlaubten Zugriffe werden im LANCOM explizit Verbindungszustand, Quell-Adressen und Korrektheit von Fragmenten überprüft. Dies geschieht sowohl für einkommende als auch für ausgehende Pakete, da ein Angriff auch aus dem lokalen Netz heraus gestartet werden kann.

Um nicht durch fehlerhafte Konfiguration der Firewall ein Tor für DoS-Angriffe zu öffnen, wird dieser Teil zentral konfiguriert. Neben der Maximalzahl der halboffenen Verbindungen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- Die Verbindung wird getrennt
- Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

▷ Schutz vor "Denial-of-Service"-Angriffen

WEBconfig,
Telnet

Die Verhaltensweise der DoS-Erkennung und -Abwehr wird unter WEBconfig oder Telnet hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router/Firewall
Terminal/Telnet	Setup/IP-Router/Firewall

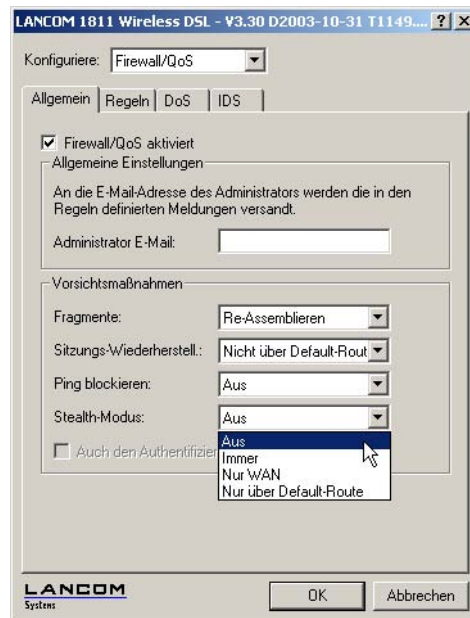
Immer aktiv hingegen sind folgende Schutzmechanismen:

- ▶ Adressüberprüfung (gegen IP-Spoofing)
- ▶ Abblocken von Broadcasts in lokale Netz (gegen Smurf und Co).

8.5.3 Konfiguration von ping-Blocking und Stealth-Modus

LANconfig

Die Parameter für das ping-Blocking und den Stealth-Modus werden im LANconfig im Konfigurationsbereich 'Fire-wall/QoS' auf der Registerkarte 'Allgemein' festgelegt:



▷ Schutz vor "Denial- of- Service"- Angriffen

WEBconfig,
Telnet

Unter WEBconfig oder Telnet wird das Unterdrücken der Antworten hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router/Firewall
Terminal/Telnet	Setup/IP-Router/Firewall

▷ Wozu QoS?

9 Quality-of-Service

Dieses Kapitel widmet sich dem Thema Quality-of-Service (kurz: QoS). Unter diesem Oberbegriff sind die Funktionen des LCOS zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstgütern befassen.

9.1 Wozu QoS?

Generell möchte man mit dem Quality-of-Service erreichen, dass bestimmte Datenpakete entweder besonders sicher oder möglichst sofort übertragen werden:

- ▶ Bei der Datenübertragung kann es durchaus vorkommen, dass Datenpakete gar nicht beim Empfänger ankommen. Für manche Anwendungen ist es aber sehr wichtig, dass alle abgeschickten Pakete auch wirklich ankommen. Eine in mehrere kleine Datenpakete aufgeteilte E-Mail kann z.B. beim Empfänger nur dann wieder zusammengebaut werden, wenn alle Teile vollständig angekommen sind. Ob das eine oder andere Paket dabei mit kleinen Zeitverzögerungen eintrifft, ist jedoch weniger wichtig. Diese Anwendungen setzen meistens auf das verbindungsorientierte Transmission Control Protocol (TCP). Dieses Protokoll stellt sicher, dass die Daten korrekt und in der richtigen Reihenfolge über das Netz transportiert werden. Es regelt dabei die Sende- und Empfangsraten selbst herunter, wenn die Bestätigungen der verschickten Datenpakete länger auf sich warten lassen, und sorgt im Falle eines Paketverlustes automatisch für ein erneutes Übertragen.
- ▶ Bei anderen Anwendungen wie z.B. der Telefonie über das Internet (Voice-over-IP, VoIP) ist es im Gegenteil dazu sehr wichtig, dass die Datenpakete nur mit geringer zeitlicher Verzögerung beim Empfänger eintreffen. Ob dabei einmal ein Datenpaket verloren geht, ist hier weniger wichtig. Der Teilnehmer am anderen Ende der Verbindung versteht den Anrufer auch dann, wenn kleine Teile der Sprache verloren gehen. Bei dieser Anwendung steht also der Wunsch im Vordergrund, dass die zu versendenden Datenpakete möglichst sofort verschickt werden. Für diese Anwendungen wird oft das verbindungslose User Datagram Protocol (UDP) eingesetzt. Bei diesem Protokoll ist der Overhead für die Verwaltung sehr gering. Allerdings ist die Zustellung der Pakete in der richtigen Reihenfolge nicht garantiert, die Datenpakete werden einfach losgeschickt. Da es keine Empfangsbestätigung gibt, werden verlorene Pakete auch nicht erneut zugestellt.

9.2 Welche Datenpakete bevorzugen?

Die Notwendigkeit für das QoS-Konzept entsteht erst durch die Tatsache, dass die verfügbare Bandbreite nicht immer ausreicht, um alle anstehenden Datenpakete zuverlässig und rechtzeitig zu übertragen. Werden über die Datenleitung gleichzeitig große FTP-Downloads gefahren, E-Mails ausgetauscht und IP-Telefone verwendet, kommt es sehr schnell zu Belastungsspitzen. Um auch in diesen Situationen die Anforderungen an die gewünschte Datenübertragung sicher zu stellen, müssen bestimmte Datenpakete bevorzugt behandelt werden. Dazu muss ein LANCOM zunächst einmal erkennen, welche Datenpakete denn überhaupt bevorzugt werden sollen.

Es gibt zwei Möglichkeiten, den Bedarf für eine bevorzugte Behandlung von Datenpaketen im LANCOM zu signalisieren:

- ▶ Die Applikation, wie z.B. die Software von einigen IP-Telefonen, kann die Datenpakete selbst entsprechend kennzeichnen. Diese Kennzeichnung, das "Tag", wird in den Header der IP-Pakete eingefügt. Die beiden ver-

▷ Welche Datenpakete bevorzugen?

schiedenen Varianten dieser Kennzeichnung "ToS" und "DiffServ" können vereinfacht dargestellt folgende Zustände annehmen:

- ▷ ToS "Low Delay"
- ▷ ToS "High Reliability"
- ▷ DiffServ "Expedited Forwarding"
- ▷ DiffServ "Assured Forwarding"



Die IP-Header-Bits des ToS- bzw. DiffServ-Feldes werden im Falle einer VPN-Strecke auch in den umgebenden IP-Header des IPSec-VPN-Paketes kopiert. Somit steht QoS auch für VPN-Strecken über das Internet zur Verfügung, sofern der Provider entsprechende Pakete auch im WAN bevorzugt behandelt.

- ▶ Wenn die Applikation selbst nicht die Möglichkeit hat, die Datenpakete entsprechend zu kennzeichnen, kann das LANCOM für die richtige Behandlung sorgen. Dazu werden die vorhandenen Funktionen der Firewall genutzt, die Datenpakete z.B. nach Subnetzen oder Diensten (Anwendungen) klassifizieren kann. Mit diesen Funktionen ist es z.B. möglich, die Datenpakete einer FTP-Verbindung oder die einer bestimmten Abteilung (in einem separaten Subnetz) gesondert zu behandeln.

Für die Behandlung von Datenpaketen, die über die Firewall klassifiziert werden, stehen die beiden folgenden Möglichkeiten zur Auswahl:

- ▷ Garantierte Mindestbandbreite
- ▷ Limitierte Maximalbandbreite

▷ Welche Datenpakete bevorzugen?

Was ist DiffServ?

DiffServ steht für "Differentiated Services" und stellt ein relativ neues Modell dar, die Priorität der Datenpakete zu signalisieren. DiffServ basiert auf dem bekannten Type-of-Service(ToS)-Feld und nutzt das gleiche Byte im IP-Header.

ToS verwendet die ersten drei Bits zur Kennzeichnung der Prioritäten (Precedence) 0 bis 7 und vier weitere Bits (die ToS-Bits) zur Optimierung des Datenflusses (u.a. "Low Delay" und "High Reliability"). Dieses Modell ist recht unflexibel und wurde daher in der Vergangenheit eher selten verwendet.

Das DiffServ-Modell nutzt die ersten 6 Bits zur Unterscheidung verschiedener Klassen. Damit sind bis zu 64 Abstufungen (Differentiated Services Code Point, DSCP) möglich, die eine feinere Priorisierung des Datenflusses ermöglichen:

- ▶ Um die Abwärtskompatibilität zur ToS-Implementation sicherzustellen, können mit den "Class Selectors" (CS0 bis CS7) die bisherigen Precedence-Stufen abgebildet werden. Die Stufe "CS0" wird dabei auch als "Best Effort" (BE) bezeichnet und steht für die normale Übertragung der Datenpakete ohne besondere Behandlung.
- ▶ Die "Assured Forwarding"-Klassen werden für die gesicherte Übertragung von Datenpaketen eingesetzt. Die erste Ziffer des AF-Klasse steht jeweils für die Priorität der Übertragung (1 bis 4), die zweite Ziffer für "Drop-Wahrscheinlichkeit" (1 bis 3). Pakete mit AFxx-Kennzeichnung werden "gesichert" übertragen, also nicht verworfen.
- ▶ Mit der Klasse "Expedited Forwarding" schließlich werden die Pakete markiert, die vor allen anderen Paketen (bevorzugt) übertragen werden sollen.

Code-point	DSCP Bits	Dez.	Code-point	DSCP Bits	Dez.	Code-point	DSCP Bits	Dez.
CS0 (BE)	000000	0	AF11	001010	10	AF33	011110	30
CS1	001000	8	AF12	001100	12	AF41	100010	34
CS2	010000	16	AF13	001110	14	AF42	100100	36
CS3	011000	24	AF21	010010	18	AF43	100110	38
CS4	100000	32	AF22	010100	20	EF	101110	46
CS5	101000	40	AF23	010110	22			
CS6	110000	48	AF31	011010	26			
CS7	111000	56	AF32	011100	28			

▷ Welche Datenpakete bevorzugen?

9.2.1 Garantierte Mindestbandbreiten

Hiermit geben Sie Vorfahrt für sehr wichtige Applikationen, Voice-over-IP (VoIP)-TK-Anlagen oder bestimmte Benutzergruppen.

Volldynamisches Bandbreitenmanagement beim Senden

Das Bandbreitenmanagement erfolgt in Senderichtung dynamisch. Dies bedeutet, dass z.B. eine garantierte Mindestbandbreite nur solange zur Verfügung stellt wird, wie auch tatsächlich entsprechender Datentransfer anliegt.

Ein Beispiel:

Zur Übertragung von VoIP-Daten eines entsprechenden VoIP-Gateways immer soll eine Bandbreite von 256 kBit/s garantiert werden. Ein einzelne VoIP-Verbindung benötige 32 kBit/s.

Solange niemand telefoniert, steht die gesamte Bandbreite anderen Diensten zur Verfügung. Mit jeder neu aufgebauten VoIP-Verbindung stehen den anderen Anwendungen jeweils 32 kBit/s weniger zur Verfügung, bis 8 VoIP-Verbindungen aktiv sind. Sobald eine VoIP-Verbindung beendet ist, steht die entsprechende Bandbreite wieder allen anderen Anwendungen zur Verfügung.



Für das korrekte Funktionieren dieses Mechanismus darf die Summe der konfigurierten Mindestbandbreiten die effektiv zur Verfügung stehende Sendebandbreite nicht übersteigen.

Dynamisches Bandbreitenmanagement auch beim Empfang

Zur empfangsseitigen Bandbreitensteuerung können Pakete zwischengespeichert und erst verzögert bestätigt werden. Dadurch regeln sich TCP/IP-Verbindungen selbständig auf eine geringere Bandbreite ein.

Jedem WAN-Interface ist eine maximale Empfangsbandbreite zugeordnet. Diese Bandbreite wird durch jede QoS-Regel, die eine minimale Empfangsbandbreite auf diesem Interface garantiert, entsprechend erniedrigt.

- ▶ Ist die QoS-Regel verbindungsbezogen definiert, wird die reservierte Bandbreite direkt nach dem Beenden der Verbindung wieder freigegeben, und die maximal auf dem WAN-Interface verfügbare Bandbreite steigt entsprechend an.
- ▶ Ist die QoS-Regel global definiert, wird die reservierte Bandbreite erst nach dem Beenden der letzten Verbindung wieder freigegeben.

9.2.2 Limitierte Maximalbandbreiten

Hiermit schränken Sie z.B. die gesamte oder verbindungsbezogene Maximalbandbreite für Serverzugriffe ein.

Ein Beispiel:

Sie betreiben einen Webserver und ein lokales Netzwerk an einem gemeinsamen Internetzugang.

Um zu verhindern, dass Ihr Produktivnetz (LAN) von vielen Internetzugriffen auf Ihren Webserver lahmgelegt wird, limitieren Sie alle Serverzugriffe auf die Hälfte der Ihnen zur Verfügung stehenden Bandbreite. Um ferner sicherzu-

▷ *Das Warteschlangenkonzept*

stellen, dass Ihre Serverdienste vielen Usern gleichzeitig und gleichberechtigt zugute kommen, setzen Sie pro Verbindung zum Server eine bestimmte Maximalbandbreite.

Kombination möglich

Minimal- und Maximalbandbreiten können kombiniert zusammen verwendet werden. Somit kann die zur Verfügung stehende Bandbreite speziell nach Ihren Erfordernissen z.B. auf bestimmte Benutzergruppen oder Anwendungen verteilen werden.

9.3 Das Warteschlangenkonzept

9.3.1 Sendeseitige Warteschlangen

Die Anforderungen an die Dienstgüte werden im LCOS durch den Einsatz mehrerer Warteschlangen (Queues) für die Datenpakete realisiert. Auf der Sendeseite kommen folgende Queues zum Einsatz:

▶ Urgent-Queue I

Diese Queue wird immer vor allen anderen abgearbeitet. Hier landen folgende Datenpakete:

- ▷ Pakete mit ToS "Low Delay"
- ▷ Pakete mit DiffServ "Expedited Forwarding"
- ▷ Alle Pakete, denen eine bestimmte Mindestbandbreite zugewiesen wurde, solange die garantierte Minimalbandbreite nicht überschritten wird
- ▷ TCP-Steuerungspakete können ebenfalls durch diese Queue bevorzugt versendet werden (siehe 'SYN/ACK-Speedup' →Seite 117)

▶ Urgent Queue II

Hier landen alle Pakete, die eine garantierte Mindestbandbreite zugewiesen bekommen haben, deren Verbindung diese aber überschritten hat.

Solange das Intervall für die Mindestbandbreite läuft (z.B. bis zum Ende der laufenden Sekunde) werden alle Pakete in dieser Queue ohne weitere besondere Priorität behandelt. Alle Pakete in dieser Queue, der "gesicherten Queue" und der "Standard-Queue" teilen sich von nun an die vorhandene Bandbreite. Die Pakete werden beim Senden in der Reihenfolge aus den Queues geholt, in der sie auch in die Queues gestellt wurden. Läuft das Intervall ab, werden alle Blöcke, die sich zu diesem Zeitpunkt noch in der "Urgent-Queue II" befinden, bis zum Überschreiten der jeweils zugeteilten Mindestbandbreite wieder in die "Urgent-Queue I" gestellt, der Rest verbleibt in der "Urgent-Queue II".

Mit diesem Verfahren wird sichergestellt, dass priorisierte Verbindungen den restlichen Datenverkehr nicht erdrücken.

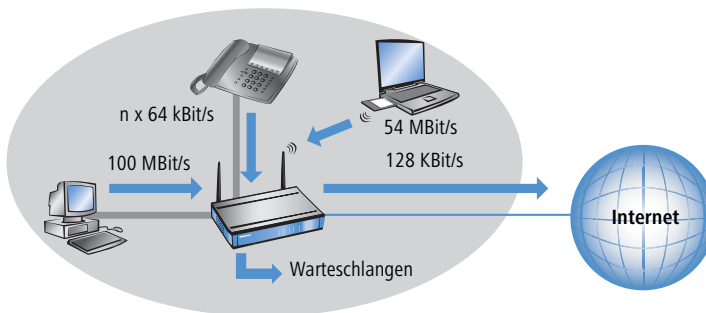
▶ gesicherte Queue

Diese Warteschlange hat keine gesonderte Priorität. Jedoch werden Pakete in dieser Queue niemals verworfen (garantierte Übertragung). Hier landen folgende Datenpakete:

- ▷ Pakete mit ToS "High Reliability"
- ▷ Pakete mit DiffServ "Assured Forwarding"
- ▶ Standard-Queue

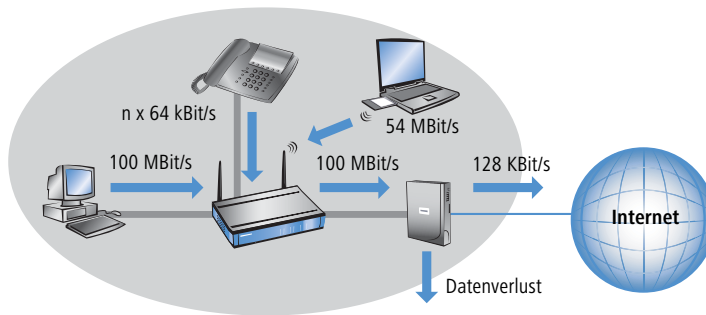
Die Standard-Warteschlange enthält alle nicht klassifizierten Datenpakete. Pakete in dieser Queue werden zuerst verworfen, sofern die Datenpakete nicht schnell genug abgeliefert werden können.

Das Konzept der Warteschlangen funktioniert natürlich nur, wenn sich an der Schnittstelle vom LAN zum WAN ein "Stau" von Datenpaketen bildet. Dieser Stau bildet sich dann, wenn das Interface im LANCOM weniger Daten an das WAN abgeben kann, als aus dem LAN in den Spitzenzeiten angeliefert werden. Das ist z.B. dann der Fall, wenn die Schnittstelle zum WAN ein integriertes ADSL Interface mit vergleichsweise geringer Sendegeschwindigkeit ("Upstream") ist. Das integrierte ADSL-Modem meldet selbständig an das LANCOM zurück, wie viele Datenpakete es noch aufnehmen kann und bremst so den Datenfluss schon im Router. Dabei werden dann automatisch die Warteschlangen gefüllt.



Anders sieht das aus, wenn ein Ethernet-Interface die Verbindung ins WAN darstellt. Aus Sicht des LANCOM sieht die Verbindung ins Internet über das ein externes DSL-Modem wie ein Ethernet-Abschnitt aus. Auf der Strecke vom LANCOM zum DSL-Modem werden die Daten auch mit der vollen LAN-Geschwindigkeit von 10 oder 100 MBit/s übertragen. Hier bildet sich also kein natürlicher Stau, da die Ein- und Ausgangsgeschwindigkeiten gleich sind. Außerdem meldet das Ethernet zwischen LANCOM und DSL-Modem nichts über die Kapazität der Verbindung zurück. Die Folge: erst im DSL-Modem kommt es zum Stau. Da hier keine Warteschlangen mehr vorhanden sind, gehen die überschüssigen Daten verloren. Eine Priorisierung der "bevorzugten" Daten ist also nicht möglich

▷ Das Warteschlangenkonzept



Um dieses Problem zu lösen, wird die Übertragungsrate des WAN-Interfaces im LANCOM künstlich gedrosselt. Die Schnittstelle wird dabei auf die Übertragungsrate eingestellt, die für den Transport der Daten ins WAN zur Verfügung stehen. Bei einem Standard-DSL-Anschluss wird also das DSL-Interface im LANCOM auf die entsprechende Upstreamrate (128 KBit/s) eingestellt.

Bei der von den Providern angegebenen Datenraten handelt es sich meistens um die Nettodatenrate. Die für das Interface nutzbare Bruttodatenrate liegt etwas höher als die vom Provider garantierte Nettodatenrate. Wenn Sie die Bruttodatenrate Ihres Providers kennen, können Sie diesen Wert für das Interface eintragen und damit den Datendurchsatz leicht steigern. Mit der Angabe der Nettodatenrate sind Sie aber auf jeden Fall auf der sicheren Seite!

9.3.2 Empfangsseitige Warteschlangen

Neben der Übertragungsrate in Senderichtung gilt die gleiche Überlegung auch für die Empfangsrichtung. Hier bekommt das WAN-Interface des LANCOM vom DSL-Modem deutlich weniger Daten angeliefert, als eigentlich aufgrund des 10 oder 100 MBit Ethernet-Interfaces möglich wäre. Alle auf dem WAN-Interface empfangenen Datenpakete werden gleichberechtigt in das LAN übertragen.

Um die eingehenden Daten priorisieren zu können, muss also auch in dieser Richtung eine künstliche "Bremse" eingeschaltet werden. Wie schon bei der Senderichtung wird daher die Übertragungsrate der Schnittstelle in Empfangsrichtung an das Angebot des Providers angepasst, für einen Standard-DSL-Anschluss also z.B. auf eine Downstreamrate von 768 KBit/s. Auch hier kann wie bei der Upstreamrate die Bruttodatenrate eingetragen werden, wenn bekannt.

Das Reduzieren der Empfangsbandbreite macht es nun möglich, die empfangenen Datenpakete angemessen zu behandeln. Die bevorzugten Datenpakete werden bis zur garantierten Mindestbandbreite direkt in das LAN weitergegeben, die restlichen Datenpakete laufen in einen Stau. Dieser Stau führt in der Regel zu einer verzögerten Bestätigung der Pakete. Bei einer TCP-Verbindung wird der sendende Server auf diese Verzögerungen reagieren, seine Sendefrequenz herabsetzen und sich so der verfügbaren Bandbreite anpassen.

Auf der Empfangsseite kommen folgende Queues zum Einsatz:

- ▶ Deferred Acknowledge Queue

▷ Reduzierung der Paketlänge

Jedes WAN-Interface erhält zusätzlich eine QoS-Empfangsqueue, welche die Pakete aufnimmt, die "ausgebremst" werden sollen. Die Verweildauer jedes einzelnen Pakets richtet sich nach der Länge des Pakets und der aktuell zulässigen Empfangsbandbreite. Pakete, für die über eine QoS-Regel eine empfangsseitige Mindestbandbreite definiert ist, werden ungebremst durchgelassen, solange die Mindestbandbreite nicht überschritten wurde.

▶ normale Empfangsqueue

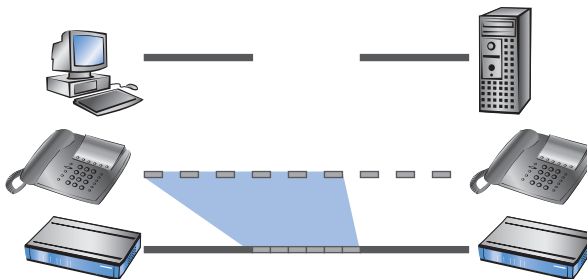
Hier landen alle Pakete, die nicht aufgrund einer empfangsseitig aktiven QoS-Regel gesondert behandelt werden müssen. Pakete in dieser Queue werden direkt weitergeleitet bzw. bestätigt, ohne Maximalbandbreiten zu berücksichtigen.

9.4 Reduzierung der Paketlänge

Die bevorzugte Behandlung von Datenpaketen einer wichtigen Applikation kann je nach Situation durch extrem lange Datenpakete anderer Anwendungen gefährdet werden. Das ist z.B. dann der Fall, wenn IP-Telefonie und ein FTP-Datentransfer gleichzeitig auf der WAN-Verbindung aktiv sind.



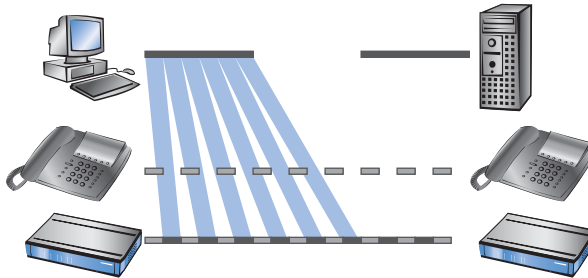
Der FTP-Transfer setzt recht große Datenpakete von 1500 Byte ein, während die Voice-over-IP-Verbindung Pakete von z.B. netto 24 Byte in relativ kurzen Takten verschickt. Wenn sich in dem Moment, in dem ein VoIP-Paket übertragen werden soll, z.B. schon FTP-Pakete in der Sendequete des LANCOM befinden, kann das VoIP-Paket erst dann verschickt werden, wenn die Leitung wieder frei ist. Je nach Übertragungsrates der Verbindung kann das zu einer merklichen Verzögerung der Sprachübertragung führen.



Dieses störende Verhalten kann ausgeglichen werden, wenn alle Datenpakete, die nicht zu der über QoS bevorzugten Verbindung gehören, eine bestimmte Länge nicht überschreiten. Auf der FTP-Verbindung werden dann z.B. nur so kleine Pakete verschickt, dass die zeitkritische VoIP-Verbindung die Pakete in der benötigten Taktung ohne zeit-

▷ Reduzierung der Paketlänge

liche Verzögerung zustellen kann. Für die TCP-gesicherte FTP-Übertragung wirkt sich die möglicherweise einstellende Verzögerung nicht nachteilig aus.



Zur Beeinflussung der Paketlänge gibt es zwei verschiedene Verfahren:

- ▶ Das LANCOM kann die Teilnehmer der Datenverbindung informieren, dass sie nur Datenpakete bis zu einer bestimmten Länge verschicken sollen. Dabei wird eine passende PMTU (Path Maximum Transmission Unit) auf der Sendeseite erzwungen, das Verfahren bezeichnet man als "PMTU-Reduzierung".

Die PMTU-Reduzierung kann dabei sowohl in Sende- als auch in Empfangsrichtung eingesetzt werden. Für die Senderichtung werden die Absender im eigenen LAN mit der PMTU-Reduzierung auf eine geringere Paketgröße eingestellt, für die Empfangsrichtung die Absender im WAN, z.B. Web- oder FTP-Server im Internet.

Sofern die Datenverbindung schon besteht, wenn die VoIP-Verbindung gestartet wird, regeln die Absender die Paketlänge sehr schnell auf den zulässigen Wert zurück. Beim Aufbau von neuen Datenverbindungen, während die VoIP-Verbindung schon steht, wird während der Verbindungsverhandlung direkt die maximal zulässige Paketlänge vereinbart.



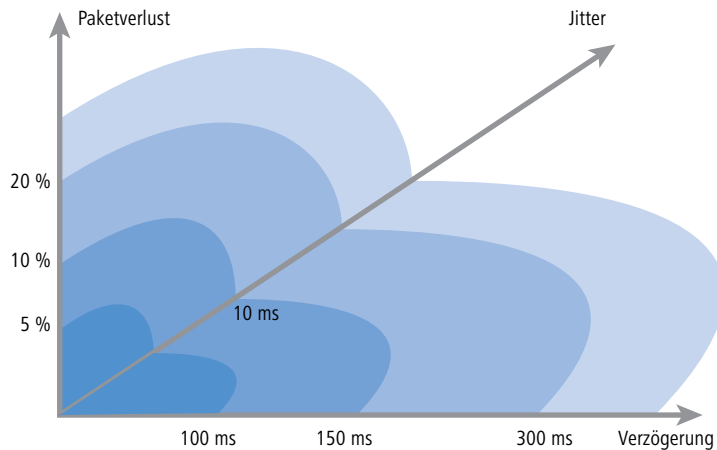
Die reduzierte Paketlänge auf der Datenverbindung bleibt auch nach dem Beenden der VoIP-Verbindung bestehen, bis der Absender den PMTU-Wert erneut überprüft.

- ▶ Das LANCOM kann die zu sendenden Pakete oberhalb einer einstellbaren Maximalgröße (z.B. 256 Byte) selbst in kleinere Einheiten aufteilen. Dieses als "Fragmentieren" bezeichnete Verfahren wird jedoch nicht von allen Servern im Internet unterstützt, da die Verarbeitung von fragmentierten Pakete als Sicherheitsrisiko betrachtet wird und in vielen Servern ausgeschaltet ist. Dadurch kann es zu Störungen z.B. beim Datendownload oder bei der Übertragung von Webseiten kommen.

Dieses Verfahren ist daher nur für solche Verbindungen zu empfehlen, bei denen keine unbekanntenen Server im Internet beteiligt sind, z.B. bei der direkten Anbindung von Filialen an eine Zentrale über eine VPN-Verbindung, über die nicht gleichzeitig der Internet-Traffic läuft.

9.5 QoS- Parameter für Voice- over- IP- Anwendungen

Eine wichtige Aufgabe bei der Konfiguration von VoIP-Systemen ist die Sicherstellung einer ausreichenden Sprachqualität. Zwei Faktoren beeinflussen die Sprachqualität einer VoIP-Verbindung wesentlich: Die Verzögerung der Sprache auf dem Weg vom Sender zum Empfänger sowie der Verlust von Datenpaketen, die nicht oder nicht rechtzeitig beim Empfänger eintreffen. Die "International Telecommunication Union" (ITU) hat in umfangreichen Tests untersucht, was der Mensch als ausreichende Sprachqualität empfindet, und als Resultat die Empfehlung der ITU G.114 veröffentlicht.



Bei einer Verzögerung von nicht mehr als 100 ms und einem Paketverlust von weniger als 5% wird die Qualität wie bei einer "normalen" Telefonverbindung empfunden, bei nicht mehr als 150 ms Verzögerung und weniger als 10% Paketverlust empfindet der Telefonteilnehmer immer noch eine sehr gute Qualität. Bis zu 300 ms bei 20% schließlich empfinden manche Hörer die Qualität noch als brauchbar, darüber hinaus gilt die Verbindung als nicht mehr brauchbar für die Sprachübertragung.

Neben der mittleren Verzögerungszeit wird auch die Schwankung in dieser Verzögerung vom menschlichen Ohr wahrgenommen. Die Unterschiede in der Laufzeit der Sprachinformationen vom Sender zum Empfänger (Jitter) werden bis zu 10 ms noch toleriert, darüber hinaus als störend empfunden.

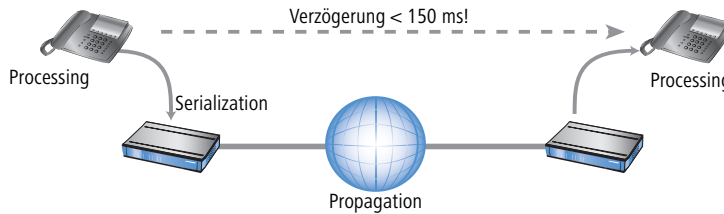
Die Konfiguration einer VoIP-Verbindung soll dementsprechend so erfolgen, dass die Randwerte für eine gute Sprachqualität eingehalten werden: Paketverlust bis 10%, Verzögerung bis 150 ms, Jitter bis 10ms.

- ▶ Der Jitter kann beim Empfänger durch einen entsprechenden Puffer ausgeglichen werden. In diesem Puffer (Jitter-Buffer) werden einige Pakete zwischengespeichert und mit konstantem Abstand an den Empfänger weitergegeben. Durch diese Zwischenspeicherung können die Schwankungen in der Übertragungszeit zwischen den einzelnen Paketen ausgeglichen werden.
- ▶ Die Verzögerung wird von mehreren Komponenten beeinflusst:

▷ QoS- Parameter für Voice- over- IP- Anwendungen

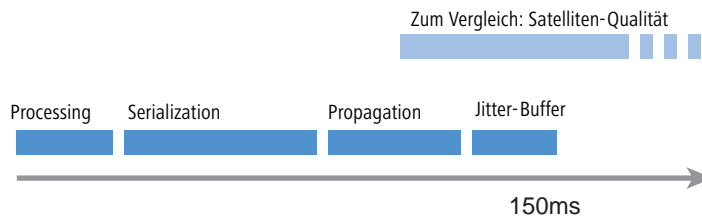
- ▷ Zum fixen Anteil der Verzögerung tragen die Zeit der Verarbeitung (Processing: Paketierung, Kodierung und Kompression beim Absender sowie beim Empfänger), die Dauer für Übergabe des Pakets von der Anwendung an das Interface (Serialization) und die Zeit für die Übertragung über die WAN-Strecke (Propagation).
- ▷ Der variable Anteil wird vom Jitter bzw. dem eingestellten Jitter-Buffer bestimmt.

Diese beiden Anteile ergeben zusammen die Verzögerung, die idealerweise nicht mehr als 150 ms betragen sollte.



- ▶ Der Paketverlust schließlich wird neben dem allgemeinen Verlust durch die Netzübertragung maßgeblich durch den Jitter-Buffer beeinflusst. Wenn Pakete mit einer größeren Verzögerung ankommen als durch den Jitter-Buffer ausgeglichen werden kann, werden die Pakete verworfen und erhöhen den Paketverlust. Je größer also der Jitter-Buffer, desto kleiner der Verlust. Umgekehrt steigt mit dem Jitter-Buffer auch die gesamte Verzögerung, so dass bei der Konfiguration der Jitter-Buffer so klein gewählt werden sollte, dass die Qualität noch als ausreichend betrachtet werden kann.

Die Verzögerung wird im Detail vor allem durch den verwendeten Codec, die daraus resultierende Paketgröße und die verfügbare Bandbreite bestimmt:



- ▶ Die Zeit für die Verarbeitung wird durch den verwendeten Codec festgelegt. Bei einer Samplingzeit von 20 ms wird genau alle 20 ms ein neues Paket gebildet. Die Zeiten für die Komprimierung etc. können meistens vernachlässigt werden.

▷ QoS- Parameter für Voice- over- IP- Anwendungen

- Die Zeit für die Übergabe der Pakete an das Interface wird durch den Quotient aus Paketgröße und verfügbarer Bandbreite definiert:

Paketgröße in Byte							
	1	64	128	256	512	1024	1500
56 Kbit/s	0,14	9	18	36	73	146	215
64 Kbit/s	0,13	8	16	32	64	128	187
128 Kbit/s	0,06	4	8	16	32	64	93
256 Kbit/s	0,03	2	4	8	16	32	47
512 Kbit/s	0,016	1	2	4	8	16	23
768 Kbit/s	0,010	0,6	1,3	2,6	5	11	16
1536 Kbit/s	0,005	0,3	0,6	1,3	3	5	8

Ein 512 Byte großes Paket einer FTP-Verbindung belegt auf einer 128 Kbit/s-Upstream also für mindestens 32 ms die Leitung.

Die Pakete der VoIP-Verbindung selbst sind außerdem oft deutlich größer als die reine Nutzlast. Zu den Nutzdaten müssen die zusätzlichen IP-Header sowie ggf. die IPsec-Header addiert werden. Die Nutzlast ergibt sich aus dem Produkt von Nutzdatenrate und Samplingzeit des verwendeten Codecs. Dazu kommen für alle Codecs jeweils 40 Byte für IP-, RTP- und UDP-Header und mindestens 20 Byte für den IPsec-Header (RTP- und IPsec-Header können allerdings je nach Konfiguration auch größer sein).

Codec	Nutzdatenrate	Sampling	Pakete/s	Nutzlast	IPsec-Paket	Bandbreite
G.723.1	6,3 Kbit/s	30 ms	33,3	24 Byte	64 Byte	22,3 Kbit/s
G.711	64 Kbit/s	20 ms	50	160 Byte	276 Byte	110,4 Kbit/s

Da die mit DES, 3DES oder AES verschlüsselten Pakete nur in Blockgrößen von 64 Bytes wachsen können, ergibt sich beim G.711-Codec das IPsec-Paket zu 160 Bytes Nutzlast + 96 Bytes auffüllen bis zu nächsten Blockgrenze + 20 Bytes IPsec-Header zu 276 Bytes.

Eine ähnliche "Verlustquote" kann sich auch beim G.723-Codec ergeben, wenn z.B. der RTP-Header länger als 12 Bytes ist. Dann wächst das IP-Paket auf die nächste Blockgrenze von 128 Bytes; zzgl. 20 Bytes für den IPsec-Header ergeben sich Pakete mit einer Gesamtlänge von 128 Bytes, also mehr als das 6-fache der Nutzlast!

Die benötigte Bandbreite für die Übertragung ergibt sich letztlich als Quotient aus der Paketgröße und der Samplingzeit.

- Die Zeit für die Übertragung über das Internet ist abhängig von der Entfernung (ca. 1 ms pro 200 km) und von den dabei passiert Routern (ca. 1 ms pro Hop). Diese Zeit kann als Hälfte des Mittelwertes einer Reihe von Ping-Zeiten auf die Gegenstelle angenähert werden.

▷ QoS in Sende- oder Empfangsrichtung

- ▶ Der Jitter-Buffer kann an vielen IP-Telefonen direkt eingestellt werden, z.B. als feste Anzahl von Paketen, die für die Zwischenspeicherung verwendet werden sollen. Die Telefone laden dann bis zu 50% der eingestellten Pakete und beginnen dann mit der Wiedergabe. Der Jitter-Buffer entspricht damit der Hälfte der eingestellten Paketanzahl multipliziert mit der Samplingzeit des Codecs.
- ▶ Fazit: Die gesamte Verzögerung ergibt sich bei der entsprechenden Bandbreite, einer Ping-Zeit von 100 ms zur Gegenstelle und einem Jitter-Buffer von 4 Paketen für die beiden Codecs im Beispiel zu:

Codec	Processing	Serialization	Propagation	Jitter-Buffer	Summe
G.723.1	30 ms	32 ms	50 ms	60 ms	172 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

Die Übertragungszeit der Pakete auf das Interface (Serialization) geht dabei von einer PMTU von 512 Byte für eine 128 Kbit-Verbindung aus. Für langsamere Interfaces oder andere Codecs müssen ggf. andere Jitter-Buffer und/oder PMTU-Werte eingestellt werden.



Bitte beachten Sie, dass die benötigten Bandbreiten jeweils in Sende- und Empfangsrichtung sowie für ein einzelne Verbindung gelten.

9.6 QoS in Sende- oder Empfangsrichtung

Bei der Steuerung der Datenübertragung mit Hilfe der QoS kann man auswählen, ob die entsprechende Regel für die Sende- oder Empfangsrichtung gilt. Welche Richtung bei einer konkreten Datenübertragung jetzt aber Sende- und welche Empfangsrichtung ist, hängt vom Blickwinkel der Betrachtung ab. Es gibt dabei die beiden folgenden Varianten:

- ▶ Die Richtung entspricht dem logischen Verbindungsaufbau
- ▶ Die Richtung entspricht der physikalischen Datenübertragung über das jeweilige Interface

Die Betrachtung eines FTP-Transfers macht die Unterschiede deutlich. Ein Client im LAN und ist über ein LANCOM mit dem Internet verbunden.

- ▶ Bei einer aktiven FTP-Session sendet der Client dem Server über den PORT-Befehl die Informationen, auf welchem Port er die DATA-Verbindung erwartet. Der Server baut daraufhin die Verbindung zum Client auf und sendet in der gleichen Richtung die Daten. Hier gehen also sowohl die logische Verbindung als auch der tatsächliche Datenstrom über das Interface vom Server zum Client, das LANCOM wertet beides als Empfangsrichtung.
- ▶ Anders sieht es aus bei einer passiven FTP-Session. Dabei baut der Client selbst die Verbindung zum Server auf. Der logische Verbindungsaufbau geht hierbei also vom Client in Richtung Server, die Datenübertragung über das physikalische Interface jedoch in umgekehrter Richtung vom Server zum Client.

In der Standardeinstellung bewertet ein LANCOM die Sende- oder Empfangsrichtung anhand des logischen Verbindungsaufbaus. Weil diese Sichtweise in manchen Anwendungsszenarien nicht einfach zu durchschauen ist, kann der Blickwinkel alternativ auf die Betrachtung des physikalischen Datenstroms umgestellt werden.



Die Unterscheidung von Sende- und Empfangsrichtung gilt nur für die Einrichtung von Maximalbandbreiten. Bei einer garantierten Mindestbandbreite sowie bei Fragmentierung und PMTU-Reduzierung gilt immer physikalische Datenübertragung über das jeweilige Interface als Richtung!

9.7 QoS- Konfiguration

9.7.1 ToS- und DiffServ-Felder auswerten

ToS- oder DiffServ?

LANconfig

Wählen Sie bei der Konfiguration mit LANconfig den Konfigurationsbereich 'IP-Router'. Auf der Registerkarte 'Allgemein' wird eingestellt, ob das 'Type-of-Service-Feld' oder alternativ das 'DiffServ-Feld' bei der Priorisierung der Datenpakete berücksichtigt wird. Werden beide Optionen ausgeschaltet, wird das ToS/DiffServ-Feld ignoriert.

WEBconfig,
Telnet

Bei der Konfiguration mit WEBconfig oder Telnet wird die Entscheidung für die Auswertung der ToS- oder DiffServ-Felder an folgenden Stellen eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP- Routermodul/Routing- Methode
Telnet	Setup/IP- Routermodul/Routing- Methode

Die Einstellmöglichkeiten des Wertes Routing- Methode sind folgende:

- ▶ **Normal:** Das ToS/DiffServ-Feld wird ignoriert.
- ▶ **TOS:** Das ToS/DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits "Low-Delay" und "High-Reliability" ausgewertet.

► QoS- Konfiguration

- **DiffServ:** Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

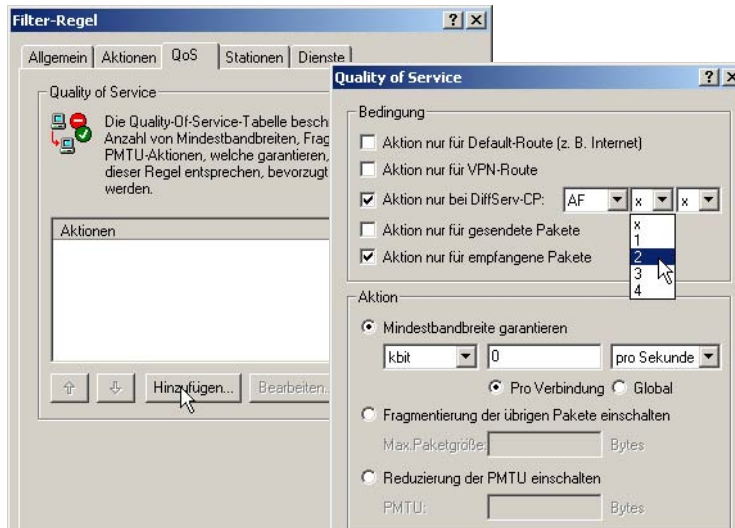
DSCP Codepoints	Übertragungsweise
CSx (inklusive CS0 = BE)	normal übertragen
AFxx	gesichert übertragen
EF	bevorzugt übertragen

DiffServ in den Firewall-Regeln

In den Firewallregeln können die Code Points aus dem DiffServ-Feld ausgewertet werden, um weitere QoS-Parameter wie Mindestbandbreiten oder PMTU-Reduzierung zu steuern.

LANconfig

Die Parameter für die Auswertung der DiffServ-Felder werden im LANconfig beim Definieren der QoS-Regel festgelegt:



Je nach Auswahl des DSCP-Typs (BE, CS, AF, EF) können in zusätzlichen Drop-Down-Listen die gültigen Werte eingestellt werden. Alternativ kann auch der DSCP-Dezimalwert direkt eingetragen werden. Eine Tabelle mit den gültigen Werten findet sich unter 'Was ist DiffServ?' →Seite 228.

WEBconfig,
Telnet

Bei der Konfiguration mit WEBconfig oder Telnet werden diese Parameter an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP- Router/Firewall/Regelliste
Telnet	Setup/IP- Router/Firewall/Regel-Liste

Die Regel in der Firewall wird dabei um die Bedingung "@d" und den DSCP (Differentiated Services Code Point) erweitert. Der Code Point kann entweder über seinen Namen (CS0 - CS7, AF11 bis AF 43, EF oder BE) oder seine dezimale bzw. hexadezimale Darstellung angegeben werden. "Expedited Forwarding" kann somit als "@dEF", "@d46" oder "@d0x2e" angegeben werden. Desweiteren sind Sammelnamen (CSx bzw. AFxx) möglich.

Beispiele:

- ▶ **%Lcds0 @dAFxx %A**: Akzeptieren (gesichert Übertragen) bei DiffServ "AF", Limit "0"
- ▶ **%Qcds32 @dEF**: Mindestbandbreite für DiffServ "EF" von 32 kBit/s
- ▶ **%Fprw256 @dEF**: PMTU-Reduzierung beim Empfang für DiffServ "EF" auf 256 Bytes)

Mit den hier aufgeführten Beispielen kann man für Voice-over-IP-Telefonate die gewünschte Bandbreite freihalten. Der erste Baustein "%Lcds0 @dAFxx %A" akzeptiert die mit dem DSCP "AFxx" markierten Pakete zur Signalisierung eines Anrufs. Die mit "EF" gekennzeichneten Sprachdaten werden durch den Eintrag "%Qcds32 @dEF" priorisiert übertragen, dabei wird eine Bandbreite von 32 KBit/s garantiert. Parallel dazu wird mit "%Fprw256 @dEF" die PMTU auf 256 Byte festgelegt, was eine Sicherung der erforderlichen Bandbreite in Empfangsrichtung erst möglich macht.



Weitere Informationen zum Definieren der Firewallregeln finden Sie im Kapitel 'Firewall' →Seite 168.

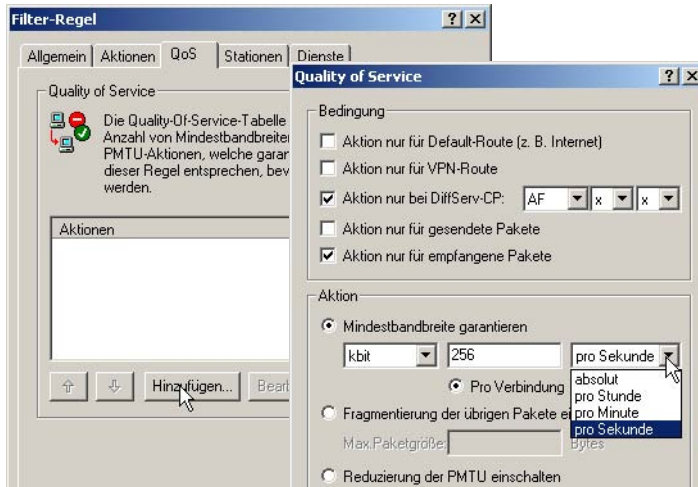
9.7.2 Minimal- und Maximalbandbreiten definieren

LANconfig

Eine Mindestbandbreite für eine bestimmte Anwendung wird im LANconfig über eine Firewallregel nach den folgenden Randbedingungen definiert:

- ▶ Die Regel benötigt keine Aktion, da für die QoS-Regeln immer implizit das "Übertragen" als Aktion vorausgesetzt wird.
- ▶ Auf der Registerkarte 'QoS' wird die garantierte Bandbreite festgelegt.

► QoS- Konfiguration



Quality-of-Service

- ▶ Mit der Option 'Aktion nur für Default-Route' beschränkt man die Regel auf Pakete, die über die Defaultroute gesendet oder empfangen werden.
- ▶ Mit der Option 'Aktion nur für VPN-Route' beschränkt man die Regel auf Pakete, die über einen VPN-Tunnel gesendet oder empfangen werden.
- ▶ Mit der Option 'Pro Verbindung' bzw. 'Global' wird festgelegt, ob die hier eingestellte Mindestbandbreite für jede einzelne Verbindung gilt, die dieser Regel entspricht (Pro Verbindung), oder ob es sich dabei um die Obergrenze für die Summe aller Verbindungen gemeinsam handelt (Global).

- ▶ Auf den Registerkarten 'Stationen' und 'Dienste' wird wie bei anderen Firewallregeln vereinbart, für welche Stationen im LAN / WAN und für welche Protokolle diese Regel gilt.

WEBconfig,
Telnet

Bei der Konfiguration mit WEBconfig oder Telnet werden die Minimal- bzw. Maximalbandbreiten an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Eine geforderte Mindestbandbreite wird in den Regeln mit dem Bezeichner "%Q" eingeleitet. Dabei wird implizit angenommen, dass es sich bei der entsprechenden Regel um eine "Accept"-Aktion handelt, die Pakete also übertragen werden.

Für eine Maximalbandbreite wird eine einfache Limit-Regel definiert, die mit einer "Drop"-Aktion alle Pakete verwirft, die über die eingestellte Bandbreite hinausgehen.

Beispiele:

- ▶ **%Qcds32:** Mindestbandbreite von 32 kBit/s für jede Verbindung

- ▶ **%Lgds256 %d**: Maximalbandbreite von 256 kBit/s für alle Verbindungen (global)



Weitere Informationen zum Definieren der Firewall-Regeln finden Sie im Kapitel 'Firewall' →Seite 168.

9.7.3 Übertragungsraten für Interfaces festlegen



Geräte mit eingebautem ADSL/SDSL-Modem bzw. mit ISDN-Adapter nehmen diese Einstellungen für das jeweilige Interface selbständig vor. Bei einem LANCOM-Modell mit DSL- **und** ISDN-Interface wird diese Einstellung also nur für das Ethernet-Interface vorgenommen.

LANconfig

Die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL-Interfaces werden im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' bei den Einstellungen für die verschiedenen WAN-Interfaces festgelegt:



- ▶ Ein DSL-Interface kann in diesem Dialog vollständig ausgeschaltet werden.
- ▶ Als Upstream- und Downstream-Rate werden hier die Bruttodatenraten angegeben, die üblicherweise etwas über den Nettodatenraten liegen, die der Provider als garantierte Datenrate angibt (siehe auch 'Das Warteschlangenkonzept' auf Seite 230).
- ▶ Der "externe Overhead" berücksichtigt Informationen, die bei der Datenübertragung den Paketen zusätzlich angehängt werden. Bei Anwendungen mit eher kleinen Datenpaketen (z.B. Voice-over-IP) macht sich diese Extra-Overhead durchaus bemerkbar. Beispiele für den externen Overhead:

Übertragung	externer Overhead	Bemerkung
T-DSL	36 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
PPTP	24 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (LLC)	22 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (VC-MUX)	18 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
Kabelmodem	0	direkte Übertragung von Ethernet-Paketen

▷ QoS- Konfiguration

WEBconfig,
Telnet

Unter WEBconfig oder Telnet können die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL- Interfaces an folgender Stelle eingetragen werden:

Konfigurationstool	Aufruf
WEBconfig	Setup/Schnittstellen/DSL-Schnittstellen
Telnet	Setup/Schnittstellen/DSL-Schnittstellen

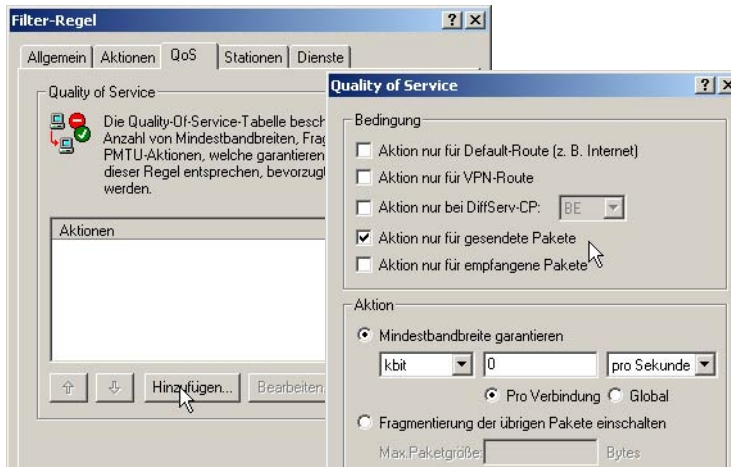


Die Werte für die Upstream-Rate und die Downstream-Rate werden in KBit/s angegeben, die Werte für den externen Overhead in Bytes/Paket.

9.7.4 Sende- und Empfangsrichtung

LANconfig

Die Bedeutung der Datenübertragungsrichtung wird im LANconfig beim Definieren der QoS-Regel festgelegt:



WEBconfig,
Telnet

Bei der Konfiguration mit WEBconfig oder Telnet wird die Bedeutung der Datenübertragungsrichtung über die Parameter "R" für receive (Empfangen), "T" für transmit (Senden) und "W" für den Bezug zum WAN-Interface an folgenden Stellen in eine neue Regel der Firewall eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Die Beschränkung der Datenübertragung auf 16 KBit/s in Senderichtung bezogen auf das physikalische WAN-Interface wird also z.B. durch die folgende Regel in der Firewall erreicht:

- ▶ %Lcdstw16%d

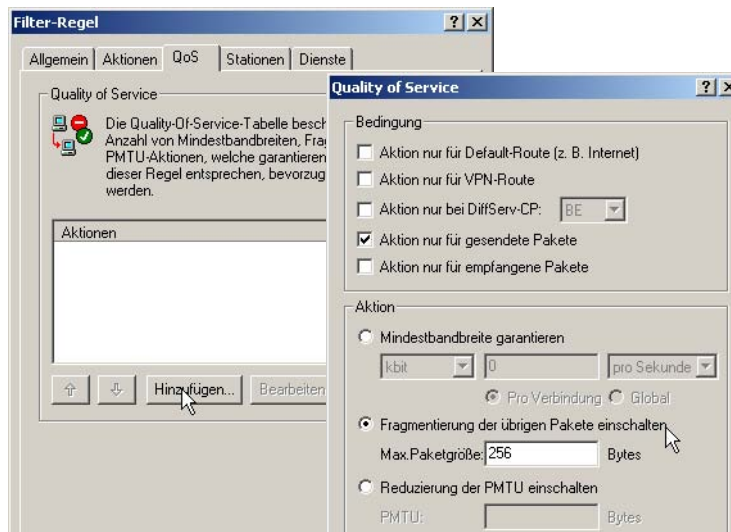
9.7.5 Reduzierung der Paketlänge

Die Längenreduzierung der Datenpakete wird definiert über eine Regel in der Firewall nach den folgenden Randbedingungen:

- ▶ Die Reduzierung bezieht sich auf **alle** Pakete, die auf das Interface gesendet werden und **nicht** der Regel entsprechen.
- ▶ Es werden nicht bestimmte Protokolle reduziert, sondern global alle Pakete auf dem Interface.

LANconfig

Die Längenreduzierung der Datenpakete wird im LANconfig beim Definieren der QoS-Regel festgelegt:



WEBconfig,
Telnet

Bei der Konfiguration mit WEBconfig oder Telnet wird die Reduzierung über die Parameter "P" für die Reduzierung der PMTU (Path MTU, MTU = Maximum Transmission Unit) und "F" für die Größe der Fragmente an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste



PMTU-Reduzierung und Fragmentierung beziehen sich immer auf die physikalische Verbindung. Die Angabe des Parameters "W" für die WAN-Senderichtung ist also hier nicht erforderlich und wird ggf. ignoriert, falls vorhanden.

▷ QoS- Konfiguration

Das folgende Beispiel zeigt eine Einstellung für Voice-over-IP-Telefonie:

Regel	Quelle	Ziel	Aktion	Protokoll
VOIP	IP-Adressen der IP-Telefone im LAN, alle Ports	IP-Adressen der IP-Telefone im LAN, alle Ports	%Qcds32 %Prt256	UDP

Diese Regel setzt die Mindestbandbreite für Senden und Empfang auf 32 KBit/s, erzwingt und verringert die PMTU beim Senden und Empfang auf 256 Byte große Pakete. Für die TCP-Verbindungen wird die Maximum Segment Size des lokalen Rechners auf 216 gesetzt, damit der Server maximal 256 Bytes große Pakete sendet (Verringerung der PMTU in Sende- und Empfangsrichtung).

10 Virtual Private Networks – VPN

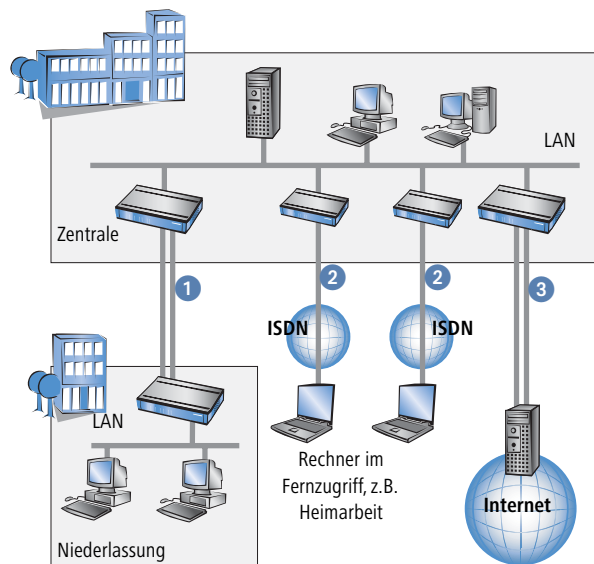
10.1 Welchen Nutzen bietet VPN?

Mit einem VPN (**V**irtual **P**riate **N**etwork) können sichere Datenverkehrsverbindungen über kostengünstige, öffentliche IP-Netze aufgebaut werden, beispielsweise über das Internet.

Was sich zunächst unspektakulär anhört, hat in der Praxis enorme Auswirkungen. Zur Verdeutlichung schauen wir uns zunächst ein typisches Unternehmensnetzwerk ohne VPN-Technik an. Im zweiten Schritt werden wir dann sehen, wie sich dieses Netzwerk durch den Einsatz von VPN optimieren lässt.

Herkömmliche Netzwerkstruktur

Blicken wir zunächst auf eine typische Netzwerkstruktur, die in dieser oder ähnlicher Form in vielen Unternehmen anzutreffen ist:



Das Unternehmensnetzwerk basiert auf einem internen Netzwerk (LAN) in der Zentrale. Dieses LAN ist über folgende Wege mit der Außenwelt verbunden:

- 1 Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
- 2 Rechner wählen sich über ISDN oder Modem ins zentrale Netzwerk ein (Remote Access Service – RAS).
- 3 Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit zum Versand und Empfang von E-Mails zu geben.

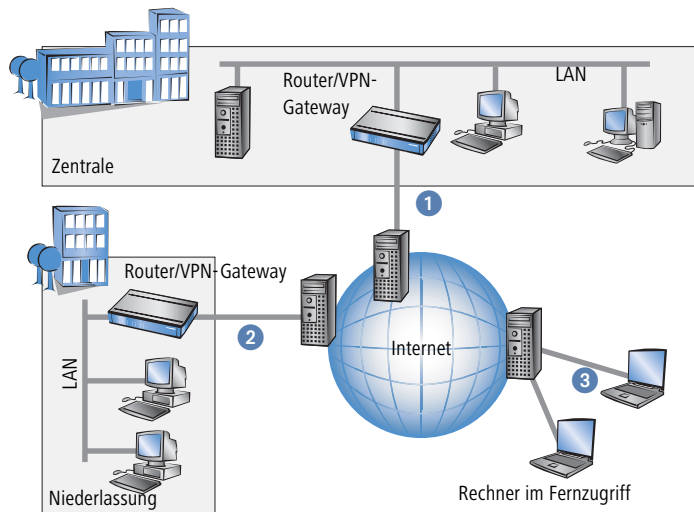
▷ Welchen Nutzen bietet VPN?

Alle Verbindungen zur Außenwelt basieren auf dedizierten Leitungen, d.h. Wähl- oder Standleitungen. Dedizierte Leitungen gelten einerseits als zuverlässig und sicher, andererseits aber auch als teuer. Ihre Kosten sind in aller Regel von der Verbindungsstrecke abhängig. So hat es gerade bei Verbindungen über weite Strecken Sinn, nach preisgünstigeren Alternativen Ausschau zu halten.

In der Zentrale muss für jeden verwendeten Zugangs- und Verbindungsweg (analoge Wählverbindung, ISDN, Standleitungen) entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

Vernetzung über Internet

Bei Nutzung des Internets anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teuren dedizierten Leitungen zwischen den Teilnehmern mehr.

- 1 Nur noch die Internet-Verbindung des LANs der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.
- 2 Die Niederlassung ist ebenfalls mit einer eigenen Verbindung ans Internet angeschlossen.
- 3 Die RAS-Rechner wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber herkömmlichen Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selber nur einen Zugang ins Internet. Die Zugangstechnologie spielt dabei keine Rolle: Idealerweise kommen

▷ *Welchen Nutzen bietet VPN?*

Breitbandtechnologien wie DSL (Digital Subscriber Line) in Verbindung mit Flatrates zum Einsatz. Aber auch herkömmliche ISDN-Verbindungen können verwendet werden.

Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

Niedrige Verbindungskosten und hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Übertragungsmedium für ein Unternehmensnetzwerk.

Zwei technische Eigenschaften des IP-Standards stehen allerdings der Nutzung des Internets als Teil von Unternehmensnetzwerken entgegen:

- ▶ Die Notwendigkeit öffentlicher IP-Adressen für alle Teilnehmer
- ▶ Fehlende Datensicherheit durch ungeschützte Datenübertragung

10.1.1 Private IP-Adressen im Internet?

Der IP-Standard definiert zwei Arten von IP-Adressen: öffentliche und private. Eine öffentliche IP-Adresse hat weltweite Gültigkeit, während eine private IP-Adresse nur in einem abgeschotteten LAN gilt.

Öffentliche IP-Adressen müssen weltweit eindeutig und daher einmalig sein. Private IP-Adressen dürfen weltweit beliebig häufig vorkommen, innerhalb eines abgeschotteten Netzwerkes jedoch nur einmal.

Normalerweise haben Rechner im LAN nur private IP-Adressen, lediglich der Router mit Anschluss ans Internet verfügt auch über eine öffentliche IP-Adresse. Die Rechner hinter diesem Router greifen über dessen öffentliche IP-Adresse auf das Internet zu (IP-Masquerading). In einem solchen Fall ist nur der Router selber über das Internet ansprechbar. Rechner hinter dem Router sind aus dem Internet heraus ohne Vermittlung durch den Router nicht ansprechbar.

Routing auf IP-Ebene mit VPN

Soll das Internet zur Kopplung von Netzwerken eingesetzt werden, müssen deshalb IP-Strecken zwischen Routern mit jeweils öffentlicher IP-Adresse eingerichtet werden. Diese Router stellen die Verbindung zwischen mehreren Teilnetzen her. Schickt ein Rechner ein Paket an eine private IP-Adresse in einem entfernten Netzwerksegment, dann setzt der eigene Router dieses Paket über das Internet an den Router des entfernten Netzwerksegments ab.

Das „Einpacken“ der Datenpakete mit privaten IP-Adressen in Pakete mit öffentlichen IP-Adressen übernimmt das VPN-Gateway. Ohne VPN können Rechner ohne eigene öffentliche IP-Adresse nicht über das Internet miteinander kommunizieren.

10.1.2 Sicherheit des Datenverkehrs im Internet?

Es existiert Skepsis gegenüber der Idee, Teile der Unternehmenskommunikation über das Internet abzuwickeln. Der Grund für die Skepsis ist die Tatsache, dass sich das Internet dem direkten Einflussbereich des Unternehmens entzieht. Anders als bei dedizierten Verbindungen laufen die Daten durch fremde Netzstrukturen, deren Eigentümer dem Unternehmen häufig unbekannt sind.

▷ LANCOM VPN im Überblick

Das Internet basiert außerdem nur auf einer simplen Form der Datenübertragung in Form unverschlüsselter Datenpakete. Dritte, durch deren Netze diese Pakete laufen, können sie mitlesen und möglicherweise sogar manipulieren. Der Zugang zum Internet ist für jedermann möglich. Dadurch ergibt sich die Gefahr, dass sich auch Dritte unbefugt Zugang zu den übertragenen Daten verschaffen.

VPN – Sicherheit durch Verschlüsselung

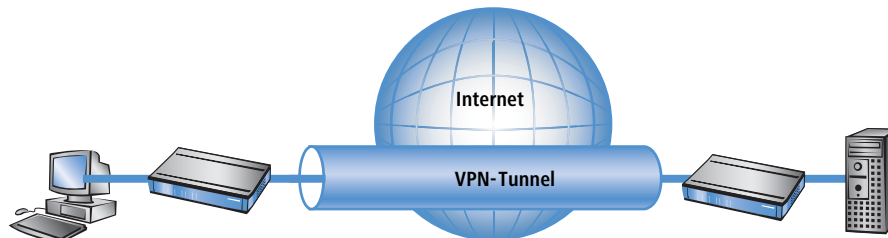
Zur Lösung dieses Sicherheitsproblems wird der Datenverkehr zwischen zwei Teilnehmern im VPN verschlüsselt. Während der Übermittlung sind die Daten für Dritte unlesbar.

Für die Verschlüsselung kommen die modernsten und sichersten Kryptografieverfahren zum Einsatz. Aus diesem Grund übertrifft die Übertragungssicherheit im VPN das Sicherheitsniveau dedizierter Leitungen bei weitem.

Für die Datenverschlüsselung werden Codes zwischen den Teilnehmern vereinbart, die man üblicherweise als „Schlüssel“ bezeichnet. Diese Schlüssel kennen nur die Beteiligten im VPN. Ohne gültigen Schlüssel können Datenpakete nicht entschlüsselt werden. Die Daten bleiben Dritten unzugänglich, sie bleiben „privat“.

Schicken Sie Ihre Daten in den Tunnel – zur Sicherheit

Jetzt wird auch klar, warum VPN ein virtuelles privates Netz aufbaut: Es wird zu keinem Zeitpunkt eine feste, physikalische Verbindung zwischen den Geräten aufgebaut. Die Daten fließen vielmehr über geeignete Routen durchs Internet. Dennoch ist es unbedenklich, wenn Dritte die übertragenen Daten während der Übertragung abfangen und aufzeichnen. Da die Daten durch VPN verschlüsselt sind, bleibt ihr eigentlicher Inhalt unzugänglich. Experten vergleichen diesen Zustand mit einem Tunnel: Offen nur am Anfang und am Ende, dazwischen perfekt abgeschirmt. Die sicheren Verbindungen innerhalb eines öffentlichen IP-Netzes werden deshalb auch „Tunnel“ genannt..



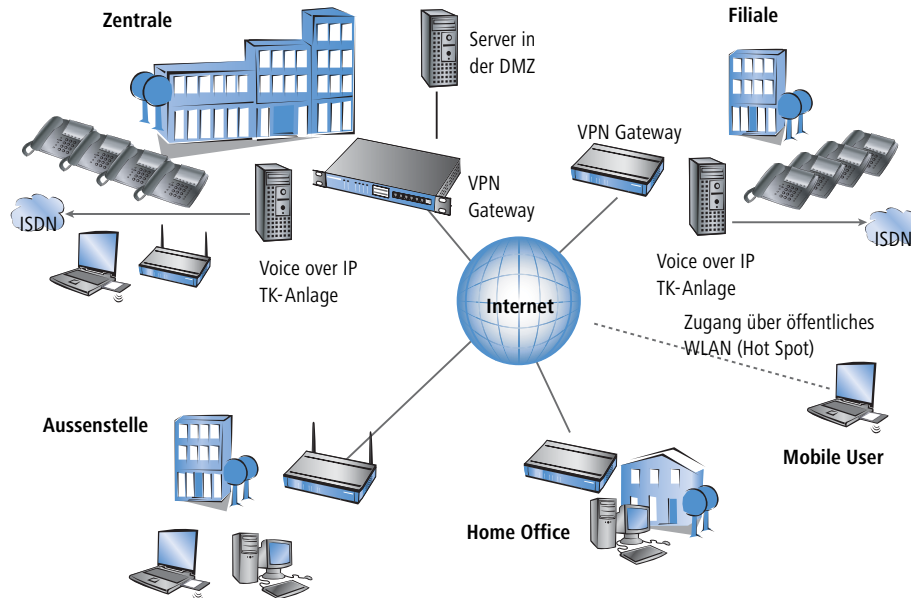
Damit ist das Ziel moderner Netzwerkstrukturen erreicht: Sichere Verbindungen über das größte und kostengünstigste aller öffentlichen IP-Netze: das Internet.

10.2 LANCOM VPN im Überblick

10.2.1 VPN Anwendungsbeispiel

VPN-Verbindungen werden in sehr unterschiedlichen Anwendungsgebieten eingesetzt. Meistens kommen dabei verschiedene Übertragungstechniken für Daten und auch Sprache zum Einsatz, die über VPN zu einem integrierten

Netzwerk zusammenwachsen. Das folgende Beispiel zeigt eine typische Anwendung, die so oder ähnlich in der Praxis oft anzutreffen ist.



Die wesentlichen Komponenten und Merkmale dieser Anwendungen:

- ▶ Kopplung von Netzwerken z.B. zwischen Zentrale und Filiale
- ▶ Anbindung von Aussenstellen ohne feste IP-Adressen über VPN-Router
- ▶ Anbindung von Home Offices ohne feste IP, ggf. über ISDN oder analoge Modems
- ▶ Anbindung an Voice-over-IP-Telefonanlagen
- ▶ Anbindung von mobilen Usern, z.B. über öffentliche WLAN-Zugänge

10.2.2 Funktionen von LANCOM VPN

In diesem Abschnitt sind alle Funktionen und Eigenschaften von LANCOM VPN aufgelistet. VPN-Experten wird dieser Überblick viel sagen. Er ist sehr kompakt, verwendet allerdings eine Vielzahl komplexer Fachbegriffe. Für das Verständnis ist die Kenntnis der technischen Grundlagen von VPN notwendig. Seien Sie beruhigt: Sie können diesen Abschnitt auch bedenkenlos überspringen. Für Inbetriebnahme und Betrieb von LANCOM VPN sind die Informationen nicht erforderlich.

- ▶ VPN nach dem IPSec-Standard
- ▶ VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- ▶ IKE Main- und Aggressive Modus

▷ VPN-Verbindungen im Detail

- ▶ LANCOM Dynamic VPN: Öffentliche IP-Adresse können statisch oder dynamisch sein (für den Aufbau zu Gegenstellen mit dynamischer IP-Adresse ist ISDN-Verbindung erforderlich)
- ▶ IPSec-Protokolle ESP, AH und IPCOMP im Transport- und Tunnelmodus
- ▶ Hash-Algorithmen:
 - ▷ HMAC-MD5-96, Hashlänge 128 Bits
 - ▷ HMAC-SHA-1-96, Hashlänge 160 Bits
- ▶ Symmetrische Verschlüsselungsverfahren
 - ▷ AES, Schlüssellänge 128, 192 und 256 Bits
 - ▷ Triple-DES, Schlüssellänge 168 Bits
 - ▷ Blowfish, Schlüssellänge 128-448 Bits
 - ▷ CAST, Schlüssellänge 128 Bits
 - ▷ DES, Schlüssellänge 56 Bits
- ▶ Kompression mit „Deflate“ (ZLIB) und LZS
- ▶ IKE Config Mode
- ▶ IKE mit Preshared Keys
- ▶ IKE mit RSA-Signature und digitalen Zertifikaten (X.509)
- ▶ Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit Schlüssellänge 768 Bits, 1024 Bits oder 1536 Bits (well known groups 1, 2 und 5)
- ▶ Schlüsselmanagement nach ISAKMP

10.3 VPN-Verbindungen im Detail

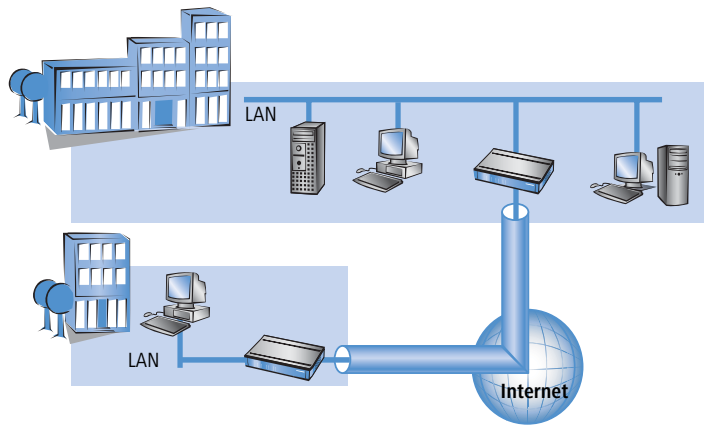
Es existieren zwei Arten von VPN-Verbindungen:

- ▶ VPN-Verbindungen zur Kopplung zweier lokaler Netzwerke. Diese Verbindungsart wird auch „LAN-LAN-Kopplung“ genannt.
- ▶ Den Anschluss eines einzelnen Rechners mit einem Netzwerk, in der Regel über Einwahlzugänge (Remote Access Service – RAS).

10.3.1 LAN-LAN-Kopplung

Als „LAN-LAN-Kopplung“ wird die Verbindung von zwei entfernten Netzen bezeichnet. Besteht eine solche Verbindung, dann können die Geräte in dem einen LAN auf Geräte des entfernten LANs zugreifen (sofern sie die notwendigen Rechte besitzen).

LAN-LAN-Kopplungen werden in der Praxis häufig zwischen Firmenzentrale und -niederlassungen oder zu Partnerunternehmen aufgebaut.



Auf jeder Seite des Tunnels befindet sich ein VPN-fähiger Router (VPN-Gateway). Die Konfiguration beider VPN-Gateways muss aufeinander abgestimmt sein.

Für die Rechner und sonstigen Geräte in den lokalen Netzwerken ist die Verbindung transparent, d. h., sie erscheint ihnen wie eine gewöhnliche direkte Verbindung. Nur die beiden Gateways müssen für die Benutzung der VPN-Verbindung konfiguriert werden.

Parallele Internet-Nutzung

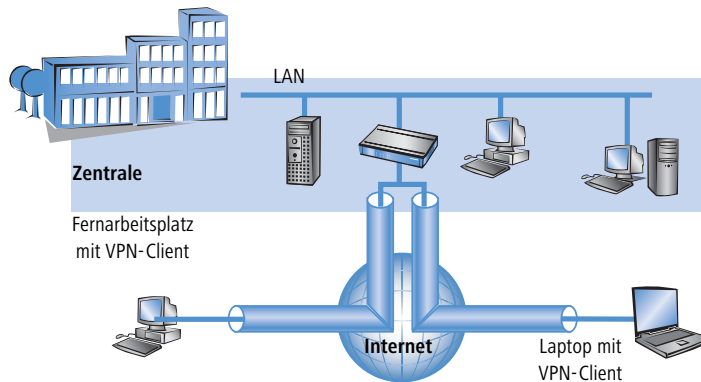
Die Internet-Verbindung, über die eine VPN-Verbindung aufgebaut wurde, kann weiterhin parallel für herkömmliche Internet-Anwendungen (Web, Mail etc.) verwendet werden. Aus Sicherheitsgründen kann die parallele Internet-Nutzung allerdings auch unerwünscht sein. So beispielsweise, wenn auch die Filiale nur über die zentrale Firewall auf das Internet zugreifen können soll. Für solche Fälle kann die parallele Internet-Nutzung auch gesperrt werden.

10.3.2 Einwahlzugänge (Remote Access Service)

Über Einwahlzugänge erhalten einzelne entfernte Rechner (Clients) Zugriff auf die Ressourcen eines LANs. Beispiele in der Praxis sind Heimarbeitsplätze oder Außendienstmitarbeiter, die sich in das Firmennetzwerk einwählen.

Soll die Einwahl eines einzelnen Rechners in ein LAN über VPN erfolgen, dann wählt sich der einzelne Rechner ins Internet ein. Eine spezielle VPN-Client-Software baut dann auf Basis dieser Internetverbindung einen Tunnel zum VPN-Gateway in der Zentrale auf.

▷ Was ist LANCOM Dynamic VPN?



Das VPN-Gateway in der Zentrale muss den Aufbau von VPN-Tunneln mit der VPN-Client-Software des entfernten Rechners unterstützen.

10.4 Was ist LANCOM Dynamic VPN?

LANCOM Dynamic VPN ist eine Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen.

Wer benötigt LANCOM Dynamic VPN und wie funktioniert es? Die Antwort erfolgt in zwei Schritten: Zunächst zeigt ein Blick auf die Grundlagen der IP-Adressierung das Problem statischer IP-Adressen. Der zweite Schritt zeigt die Lösung durch LANCOM Dynamic VPN.

10.4.1 Ein Blick auf die IP-Adressierung

Im Internet benötigt jeder Teilnehmer eine eigene IP-Adresse. Er benötigt sogar eine besondere Art von IP-Adresse, nämlich eine öffentliche IP-Adresse. Die öffentlichen IP-Adressen werden von zentralen Stellen im Internet verwaltet. Jede öffentliche IP-Adresse darf im gesamten Internet nur ein einziges Mal existieren.

Innerhalb lokaler Netzwerke auf IP-Basis werden keine öffentlichen, sondern private IP-Adressen verwendet. Für diesen Zweck wurden einige Nummernbereiche des gesamten IP-Adressraums als private IP-Adressen reserviert.

Einem Rechner, der sowohl an ein lokales Netzwerk als auch direkt an das Internet angeschlossen ist, sind deshalb zwei IP-Adressen zugeordnet: Eine öffentliche für die Kommunikation mit dem Rest des Internets und eine private, unter der er in seinem lokalen Netzwerk erreichbar ist.

Statische und dynamische IP-Adressen

Öffentliche IP-Adressen müssen beantragt und verwaltet werden, was mit Kosten verbunden ist. Es gibt auch nur einen begrenzten Vorrat an öffentlichen IP-Adressen. Aus diesem Grund verfügt auch nicht jeder Internet-Benutzer über eine eigene feste (statische) IP-Adresse.

▷ Was ist LANCOM Dynamic VPN?

Die Alternative zu statischen IP-Adressen sind die sogenannten dynamischen IP-Adressen. Eine dynamische IP-Adresse wird dem Internet-Benutzer von seinem Internet Service Provider (ISP) bei der Einwahl für die Dauer der Verbindung zugewiesen. Der ISP verwendet dabei eine beliebige unbenutzte Adresse aus seinem IP-Adress-Pool. Die zugewiesene IP-Adresse ist dem Benutzer nur temporär zugewiesen, nämlich für die Dauer der aktuellen Verbindung. Wird die Verbindung gelöst, so wird die zugewiesene IP-Adresse wieder freigegeben, und der ISP kann sie für den nächsten Benutzer verwenden.

Auch bei vielen Flatrate-Verbindungen handelt es sich oftmals um dynamische IP-Adressen. Dabei findet z.B. alle 24h eine Zwangstrennung der Verbindung statt. Nach dieser Zwangstrennung bekommt der Anschluss i.d.R. eine neue, andere IP-Adresse zugewiesen.

Vor- und Nachteile dynamischer IP-Adressen

Dieses Verfahren hat für den ISP einen wichtigen Vorteil: Er benötigt nur einen relativ kleinen IP-Adress-Pool. Auch für den Benutzer sind dynamische IP-Adressen günstig: Er muss nicht zuerst eine statische IP-Adresse beantragen, sondern kann sich sofort ins Internet einwählen. Auch die Verwaltung der IP-Adresse entfällt. Dadurch erspart er sich Aufwand und Gebühren. Die Kehrseite der Medaille: Ein Benutzer ohne statische IP-Adresse lässt sich aus dem Internet heraus nicht direkt adressieren.

Für den Aufbau von VPNs ergibt sich daraus ein erhebliches Problem. Möchte beispielsweise Rechner A einen VPN-Tunnel zu Rechner B über das Internet aufbauen, so benötigt er dessen IP-Adresse. Besitzt B nur eine dynamische IP-Adresse, so kennt A sie nicht, er kann B deshalb nicht ansprechen.

Hier bietet die Technik von LANCOM Dynamic VPN die Patentlösung.

10.4.2 So funktioniert LANCOM Dynamic VPN

Verdeutlichen wir die Funktionsweise von LANCOM Dynamic VPN an Hand dreier Beispiele (Bezeichnungen beziehen sich auf die IP-Adressart der beiden VPN-Gateways):

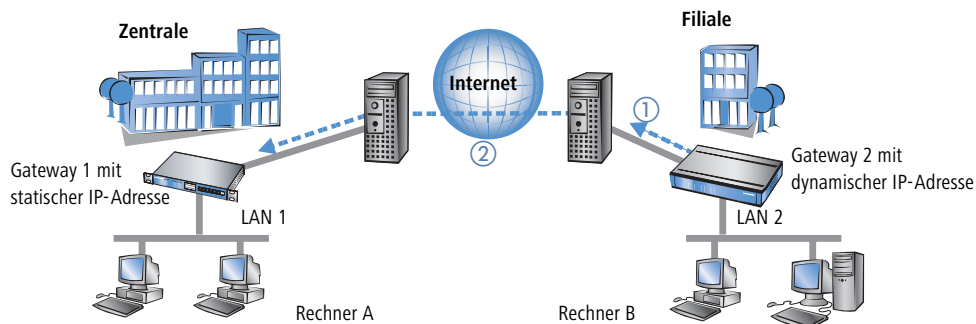
- ▶ dynamisch – statisch
- ▶ statisch – dynamisch
- ▶ dynamisch – dynamisch

Dynamisch – statisch

Möchte ein Benutzer an Rechner B im LAN 2 eine Verbindung zu Rechner A im LAN 1 aufbauen, dann erhält Gateway 2 die Anfrage und versucht, einen VPN-Tunnel zu Gateway 1 aufzubauen. Gateway 1 verfügt über eine statische IP-Adresse und kann daher direkt über das Internet angesprochen werden.


Problematisch ist, dass die IP-Adresse von Gateway 2 dynamisch zugeteilt wird, und Gateway 2 seine aktuelle IP-Adresse beim Verbindungsaufbau an Gateway 1 übermitteln muss. In diesem Fall sorgt LANCOM Dynamic VPN für die Übertragung der IP-Adresse beim Verbindungsaufbau.

▷ Was ist LANCOM Dynamic VPN?



- ① Gateway 2 baut eine Verbindung zu seinem Internet-Anbieter auf und erhält eine dynamische IP-Adresse zugewiesen.
- ② Gateway 2 spricht Gateway 1 über dessen öffentliche IP-Adresse an. Über Funktionen von LANCOM Dynamic VPN erfolgen Identifikation und Übermittlung der IP-Adresse an Gateway 2. Schließlich baut Gateway 1 den VPN-Tunnel auf.

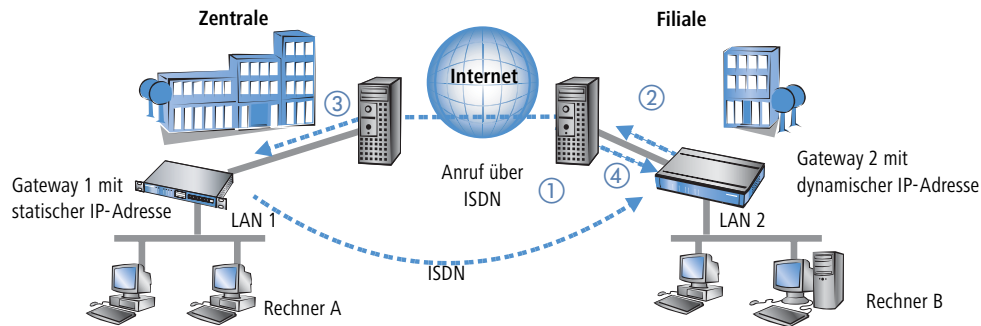
Der große Vorteil der LANCOM-Geräte bei dieser Anwendung: an Stelle des „Aggressive Mode“, der normalerweise für die Einwahl von VPN-Clients in eine Zentrale verwendet wird, kommt hier der wesentlich sicherere „Main Mode“ zum Einsatz. Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode.

 Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

Statisch – dynamisch

Möchte umgekehrt Rechner A im LAN 1 eine Verbindung zu Rechner B im LAN 2 aufbauen, z.B. um alle Außenstellen aus der Zentrale heraus fernzuwarten, dann erhält Gateway 1 die Anfrage und versucht einen VPN-Tunnel zu Gateway 2 aufzubauen. Gateway 2 verfügt nur über eine dynamische IP-Adresse und kann daher nicht direkt über das Internet angesprochen werden.

Mit Hilfe von LANCOM Dynamic VPN kann der VPN-Tunnel trotzdem aufgebaut werden. Dieser Aufbau geschieht in drei Schritten:



- ① Gateway 1 wählt Gateway 2 über ISDN an. Es nutzt dabei die ISDN-Möglichkeit, kostenlos seine eigene Rufnummer über den D-Kanal zu übermitteln. Gateway 2 ermittelt anhand der empfangenen Rufnummer aus den konfigurierten VPN-Gegenstellen die IP-Adresse von Gateway 1.

Für den Fall, dass Gateway 2 keine Rufnummer über den D-Kanal erhält (etwa weil das erforderliche ISDN-Leistungsmerkmal nicht zur Verfügung steht) oder eine unbekanntes Rufnummer übertragen wird, nimmt Gateway 2 den Anruf entgegen, und die Geräte authentifizieren sich über den B-Kanal. Nach erfolgreicher Aushandlung übermittelt Gateway 1 seine IP-Adresse und baut den B-Kanal sofort wieder ab.

- ② Nun ist Gateway 2 an der Reihe: Zunächst baut es eine Verbindung zu seinem ISP auf, von dem es eine dynamische IP-Adresse zugewiesen bekommt.
- ③ Gateway 2 authentifiziert sich bei Gateway 1, dessen statische Adresse ihm bekannt ist.
- ④ Gateway 1 kennt nun die Adresse von Gateway 2 und kann den VPN-Tunnel zu Gateway 2 jetzt aufbauen.

Der Vorteil der LANCOM-Geräte z.B. beim Aufbau der Verbindung aus der Zentrale zu den Filialen: Mit den Funktionen von LANCOM Dynamic VPN können auch Netzwerk ohne Flatrate erreicht werden, die also nicht „always online“ sind. Der ISDN-Anschluss ersetzt mit der bekannten MSN eine andere Adresse, z.B. eine statische IP-Adresse oder eine dynamische Adressauflösung über Dynamic-DNS-Dienste, die i.d.R. nur bei Flatrate-Anschlüssen zum Einsatz kommen.

i Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

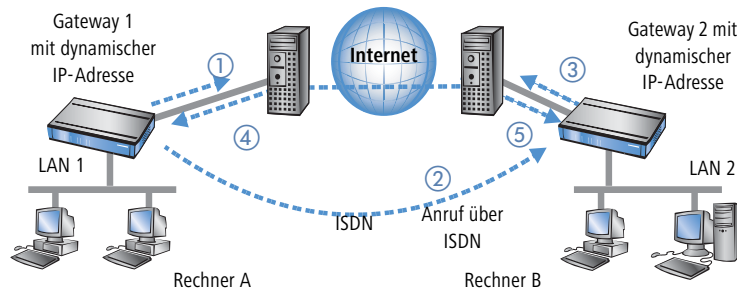
i Beachten Sie auch die 'Hinweise zur Dynamic VPN Lizenzierung' →Seite 260.

Dynamisch – dynamisch

Der Aufbau von VPN-Tunneln gelingt mit LANCOM Dynamic VPN auch zwischen zwei Gateways, die beide nur über dynamische IP-Adressen verfügen. Passen wir das besprochene Beispiel an, so dass diesmal auch Gateway 1 nur

▷ Was ist LANCOM Dynamic VPN?

über eine dynamische IP-Adresse verfügt. Auch in diesem Beispiel möchte Rechner A eine Verbindung zu Rechner B aufbauen:



- ① Gateway 1 baut eine Verbindung zu seinem ISP auf, um eine öffentliche dynamische Adresse zu erhalten.
- ② Es folgt der Anruf über ISDN bei Gateway 2 zur Übermittlung dieser dynamischen Adresse. Zur Übermittlung werden drei Verfahren verwendet:
 - ▷ **Als Information im LLC-Element des D-Kanals.** Über das D-Kanal-Protokoll von Euro-ISDN (DSS-1) können im sogenannten LLC-Element (**L**ower **L**ayer **C**ompatibility) beim Anruf zusätzliche Informationen an die Gegenstelle übermittelt werden. Diese Übermittlung findet vor dem Aufbau des B-Kanals statt. Die Gegenstelle lehnt nach erfolgreicher Übertragung der Adresse den Anruf ab. Eine gebührenpflichtige Verbindung über den B-Kanal kommt auf diese Weise nicht zustande. Die IP-Adresse wird aber trotzdem übertragen.





Das LLC-Element steht normalerweise im Euro-ISDN ohne besondere Anmeldung oder Freischaltung zur Verfügung. Es kann allerdings von Telefongesellschaften, einzelnen Vermittlungsstellen oder Telefonanlagen gesperrt werden. Im nationalen ISDN nach 1TR6 gibt es kein LLC-Element. Das beschriebene Verfahren funktioniert daher nicht.

- ▷ **Als Subadresse über den D-Kanal.** Funktioniert die Adressübermittlung über das LLC-Element nicht, dann versucht Gateway 1 die Adresse als sogenannte Subadresse zu übermitteln. Die Subadresse ist wie das LLC-Element ein Informationselement des D-Kanal-Protokolls und ermöglicht wie dieses die kostenlose Übermittlung kurzer Informationen. Allerdings muss hier die Telefongesellschaft das ISDN-Merkmal 'Subadressierung' (normalerweise gegen Berechnung) freischalten. Wie beim LLC-Element wird der Anruf nach erfolgreicher Übertragung der IP-Adresse von der Gegenstelle abgelehnt und die Verbindung bleibt gebührenfrei.
- ▷ **Über den B-Kanal.** Scheitern beide Versuche, die IP-Adresse über den D-Kanal zu übertragen, dann muss für die Übertragung der IP-Adresse eine konventionelle Verbindung über den B-Kanal aufgebaut werden. Nach der Übertragung der IP-Adresse wird die Verbindung sofort abgebaut. Es fallen die üblichen Gebühren an.

▷ Was ist LANCOM Dynamic VPN?

- ③ Gateway 2 baut eine Verbindung zum ISP auf, der ihm eine dynamische IP-Adresse zuweist.
- ④ Gateway 2 authentifiziert sich bei Gateway 1 (dessen Adresse durch Schritt ② bekannt ist).
- ⑤ Gateway 1 kennt nun die Adresse von Gateway 2 und kann so den VPN-Tunnel zu Gateway 2 aufbauen.

 Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

 Beachten Sie auch die 'Hinweise zur Dynamic VPN Lizenzierung' →Seite 260.

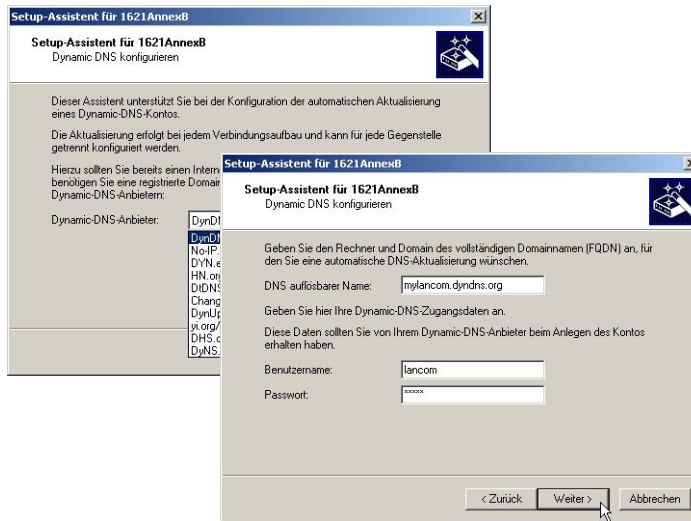
Dynamische IP-Adressen und DynDNS

Der Verbindungsaufbau zwischen zwei Stationen mit dynamischen IP-Adressen ist ebenfalls unter Verwendung eines so genannten Dynamic-DNS-Dienstes (DynDNS) möglich. Dazu wird die Tunnel-Endpunktadresse nicht in Form einer IP-Adresse angegeben (die ja dynamisch ist und häufig wechselt), sondern in Form eines statischen Namens (z.B. MyLANCOM@DynDNS.org).

Für die Namensauflösung zu einer jeweils aktuellen IP-Adresse werden zwei Dinge benötigt: Ein Dynamic-DNS-Server und ein Dynamic-DNS-Client:

- ▶ Ersterer ist ein Server, wie er von vielen Dienstleistern im Internet angeboten wird und der mit Internet-DNS-Servern in Verbindung steht.
- ▶ Der Dynamic-DNS-Client ist im Gerät integriert. Er kann zu einer Vielzahl von Dynamic-DNS-Serviceanbietern Kontakt aufnehmen und bei jeder Änderung seiner IP-Adresse automatisch ein vorher angelegtes Benutzerkonto zur DNS-Namensauflösung beim Dynamic-DNS-Anbieter aktualisieren. Die Einrichtung geschieht komfortabel mit einem Assistenten unter LANconfig (siehe auch 'Dynamic DNS' auf Seite 423):

▷ Was ist LANCOM Dynamic VPN?



Aus Sicherheits- und Verfügbarkeitsgründen empfiehlt LANCOM Systems den Einsatz des Dynamic VPN Verfahrens gegenüber Dynamic DNS basierten VPN-Lösungen. Dynamic VPN basiert auf Verbindungen über das ISDN-Netz, das eine deutlich höhere Verfügbarkeit garantiert als die Erreichbarkeit eines Dynamic-DNS-Diensts im Internet.

10.4.3 Hinweise zur Dynamic VPN Lizenzierung

Aus patentrechtlichen Gründen muss die Verwendung der Funktion „Dynamic VPN“ mit Übertragung der IP-Adressen über den ISDN-Anschluss lizenziert werden. Diese Betriebsart kommt in der Regel dann zum Einsatz, wenn Sie VPN-Kopplungen mit beidseitig dynamischen IP-Adressen nutzen und dabei keine Dynamic-DNS-Dienste verwenden. Alle anderen Betriebsarten von Dynamic VPN (also die Übermittlung der IP Adresse per ICMP, das Anklopfen bei der Gegenstelle per ISDN, um einen Rückruf herbeizuführen etc.) sind davon **nicht** betroffen.

Die Registrierung erfolgt anonym über das Internet, es werden keine Personen- oder Unternehmensspezifischen Daten übertragen.

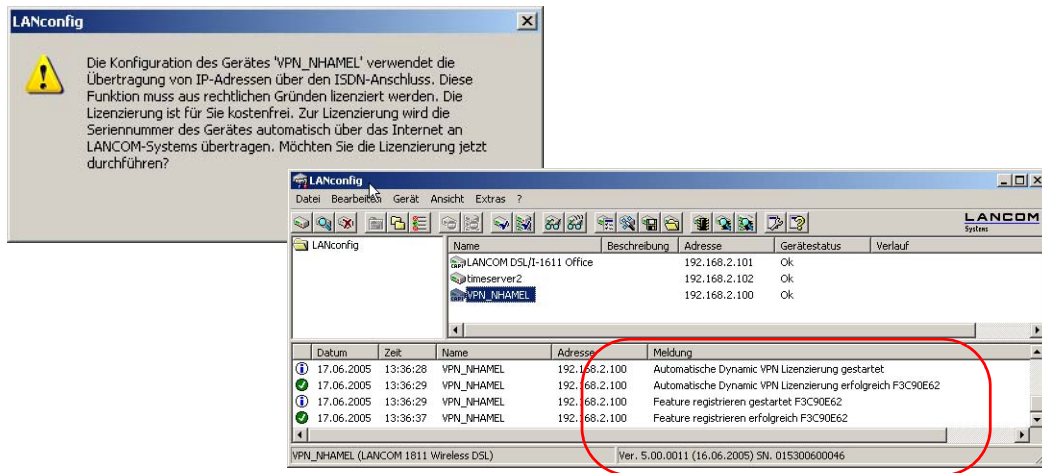


Für die Registrierung der Dynamic-VPN-Option sind Administratorrechte auf dem Gerät erforderlich.

Registrieren
über
LANconfig

LANconfig erkennt beim Prüfen der Geräte z.B. direkt nach dem Programmstart automatisch, wenn ein Gerät aufgrund seiner Konfiguration registriert werden muss. Nach der Bestätigung der entsprechenden Meldung überträgt LANconfig automatisch die erforderlichen Daten des Gerätes an den Registrierungsserver von LANCOM Systems. Der Freischaltcode wird dann ebenfalls automatisch an das Gerät zurückübertragen und aktiviert. Der Vorgang kann in der Statuszeile von LANconfig beobachtet werden.

▷ Was ist LANCOM Dynamic VPN?



Registrieren über WEBconfig

Zur Registrierung über WEBconfig wird die Chargen- bzw. Seriennummer des zu registrierenden Produkts benötigt. Sie finden diese Informationen auf der Unterseite des Gerätes.

(LANCOM 1811 Wireless DSL 5.00.0011 / 16.06.2005)

Dynamic-VPN Registrierung

Die Konfiguration des Gerätes verwendet die Übertragung von IP-Adressen über den ISDN-Anschluss. Diese Funktion muss aus rechtlichen Gründen lizenziert werden. Die Lizenzierung ist für Sie kostenfrei. Zur Lizenzierung wird die Seriennummer des Gerätes automatisch über das Internet an LANCOM-Systems übertragen. Möchten Sie die Lizenzierung jetzt durchführen?

[Dynamic VPN-Option registrieren](#)

Setup-Assistenten

Assistenten erlauben es Ihnen, häufig auftretende Aufgaben zu vereinfachen.

- [Grundeinstellungen](#)
- [Sicherheitseinstellungen](#)
- [Internet-Verbindung einrichten](#)
- [Auswahl des Internet-Anbieters](#)
- [Einwahl-Zugang bereitstellen \(RAS\)](#)
- [Zwei lokale Netze verbinden](#)

Registrierung Dynamic VPN

Sehr geehrte Kundin, sehr geehrter Kunde,

aus patentrechtlichen Gründen müssen wir Sie bitten, die Verwendung (Übertragung der IP-Adressen über den ISDN-Anschluss) ab sofort zu der Regel dann zum Einsatz, wenn Sie VPN Kopplungen mit **beide** und dabei **keine Dynamic DNS Dienste verwenden**. Alle andere die Übermittlung der IP Adresse per ICMP, das Anknüpfen bei der Geräteherbeizuführen, etc., sind davon nicht betroffen. Die Registrierung erfolgt bzw. Seriennummer Ihres zu registrierenden Produkts benötigt.

Nach dem Absenden der Registrierung erhalten Sie den Freischaltcode Sie zur Registrierung angegeben haben.

Unter dem Gerät finden Sie, je nach Gerätetyp, die 16-stellige Seriennummer. Bitte geben Sie die entsprechende Nummer (1 / Chargennummer ein. Die 12-stellige Seriennummer wird fern bei ausgewähltem Gerät angezeigt.

Registrierung Dynamic VPN

Ihr Schlüssel wurde erfolgreich generiert.

Nachfolgend finden Sie eine Übersicht der Registrierungsinfos Ihrer Router. Bitte speichern Sie diese Seite oder drucken Sie die Seite aus.

Freischaltcode: f50a3477

Um diesen Freischaltcode in Ihren Router zu laden, gehen Sie bitte wie folgt vor:

Mit LANconfig:
Markieren Sie den entsprechenden Router in der Übersicht. Wählen Sie 'Gerät' und 'Software-Option freischalten' aus. In der darauf erscheinenden Dialogbox geben Sie den Freischaltcode ein und bestätigen den Dialog mit 'ok'.

Mit WEBconfig:
Loggen Sie sich in WEBconfig mit Administratorrechten auf dem Router ein. Gehen Sie auf 'Einstellungen' > 'VPN' > 'Dynamic VPN' > 'Freischaltcode'. Geben Sie den Freischaltcode ein und bestätigen den Dialog mit 'ok'.

Beim Anmelden auf dem Gerät mit WEBconfig finden Sie auf der Startseite einen Link, der Sie zum Formular auf dem Registrierungsserver von LANCOM Systems führt. Geben Sie dort die Chargen/Seriennummer des Gerätes und Ihre E-Mailadresse an. Nach dem Absenden der Registrierungsanforderung erhalten Sie den Freischaltcode für das Gerät. Um diesen Freischaltcode in Ihren Router zu laden, gehen Sie bitte wie folgt vor:

▷ Konfiguration von VPN-Verbindungen

Melden Sie sich mit Administratorrechten unter WEBconfig auf dem entsprechenden Gerät an. Wählen Sie auf der Startseite den Eintrag **Software-Option freischalten** aus. Geben Sie auf der folgenden Seite den Freischaltcode ein und bestätigen Sie mit **Setzen**.

10.5 Konfiguration von VPN-Verbindungen

Bei der Konfiguration von VPN-Verbindungen werden drei Fragen beantwortet:

- ▶ Zwischen welchen VPN-Gateways (Gegenstellen) wird die Verbindung aufgebaut?
- ▶ Mit welchen Sicherheitsparametern wird der VPN-Tunnel zwischen den beiden Gateways gesichert?
- ▶ Welche Netzwerke bzw. Rechner können über diesen Tunnel miteinander kommunizieren?



In diesem Abschnitt werden die grundsätzlichen Überlegungen zur Konfiguration von VPN-Verbindungen vorgestellt. Dabei bezieht sich die Beschreibung zunächst auf die einfache Verbindung von zwei lokalen Netzwerken. Sonderfälle wie die Einwahl in LANs mit einzelnen Rechnern (RAS) oder die Verbindung von strukturierten Netzwerken werden im weiteren Verlauf dargestellt.

10.5.1 VPN-Tunnel: Verbindungen zwischen den VPN-Gateways

In virtuellen privaten Netzwerken (VPNs) werden lokale Netzwerke über das Internet miteinander verbunden. Dabei werden die privaten IP-Adressen aus den LANs über eine Internet-Verbindung zwischen zwei Gateways mit öffentlichen IP-Adressen geroutet.

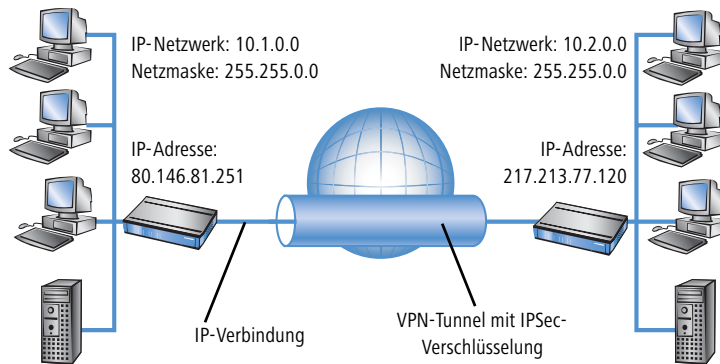
Um das gesicherte Routing der privaten IP-Adressbereiche über die Internet-Verbindung zu ermöglichen, wird zwischen den beiden LANs eine VPN-Verbindung etabliert, die auch als VPN-Tunnel bezeichnet wird.

Der VPN-Tunnel hat zwei wichtige Aufgaben:

- ▶ Abschirmen der transportierten Daten gegen den unerwünschten Zugriff von Unbefugten
- ▶ Weiterleiten der privaten IP-Adressen über eine Internet-Verbindung, auf der eigentlich nur öffentliche IP-Adressen geroutet werden können.

Die VPN-Verbindung zwischen den beiden Gateways wird durch die folgenden Parameter definiert:

- ▶ Die Endpunkte des Tunnels, also die VPN-Gateways, die jeweils über eine öffentliche IP-Adresse (statisch oder dynamisch) erreichbar sind
- ▶ Die IP-Verbindung zwischen den beiden Gateways
- ▶ Die privaten IP-Adressbereiche, die zwischen den VPN-Gateways geroutet werden sollen
- ▶ Sicherheitsrelevante Einstellungen wie Passwörter, IPSec-Schlüssel etc. für die Abschirmung des VPN-Tunnels

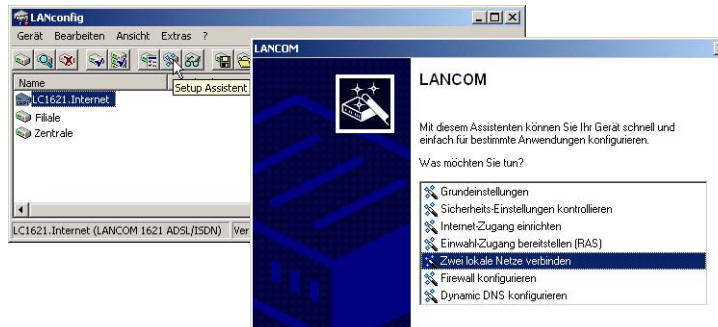


Diese Informationen sind in den so genannten VPN-Regeln enthalten.

10.5.2 VPN-Verbindungen einrichten mit den Setup-Assistenten

Verwenden Sie für die Einrichtung der VPN-Verbindungen zwischen den lokalen Netzen nach Möglichkeit die Setup-Assistenten von LANconfig. Die Assistenten leiten Sie durch die Konfiguration und nehmen alle benötigten Einstellungen vor. Führen Sie die Konfiguration nacheinander an beiden Routern durch.

- 1 Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras ► Setup Assistent**.



- 2 Folgen Sie den Anweisungen des Assistenten und geben Sie notwendigen Daten ein. Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
- 3 Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit ping) anzusprechen. Das Gerät sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

Mit diesem Assistenten werden für eine normale LAN-LAN-Kopplung allnotwendigen VPN-Verbindungen automatisch angelegt. Die manuelle Konfiguration der VPN-Verbindungen ist in den folgenden Fällen erforderlich:

▷ Konfiguration von VPN-Verbindungen

- ▶ Wenn kein Windows-Rechner mit LANconfig zur Konfiguration verwendet werden kann. In diesem Fall nehmen Sie die Einstellung der erforderliche Parameter über WEBconfig oder die Telnet-Konsole vor.
- ▶ Wenn nicht das komplette lokale LAN (Intranet) über die VPN-Verbindung mit anderen Rechnern kommunizieren soll. Das ist z.B. dann der Fall, wenn an das Intranet weitere Subnetze mit Routern angeschlossen sind, oder wenn nur Teile des Intranets auf die VPN-Verbindung zugreifen können sollen. In diesen Fällen werden die Parameter der Setup-Assistenten nachträglich um weitere Einstellungen ergänzt.
- ▶ Wenn VPN-Verbindungen zu Fremdgeräten konfiguriert werden sollen.

10.5.3 VPN-Regeln einsehen

Da die VPN-Regeln stets eine Kombination von verschiedenen Informationen repräsentieren, werden diese Regeln in einem LANCOM-Gerät nicht direkt definiert, sondern aus verschiedenen Quellen zusammengestellt. Aus diesem Grund können die VPN-Regeln nicht über LANconfig oder ein anderes Konfigurations-Tool eingesehen werden.

Die Informationen über die aktuellen VPN-Regeln im Gerät können Sie über die Telnet-Konsole abrufen. Stellen Sie dazu eine Telnet-Verbindung zu dem VPN-Gateway her und geben Sie an der Konsole den Befehl **show vpn** ein:

```

Telnet 192.168.2.100
#
! LANCOM 1811 Wireless DSL
! Ver. 3.32.0015 / 02.03.2004
! SN. 015300600046
! Copyright (c) LANCOM Systems
VPN_NHAMEL, Connection No.: 002 <LAN>
Password:
VPN_NHAMEL:/
> show vpn
VPN PM SPD and Ike configuration:
# of connections = 1
Connection #1          ipsec 192.168.2.0/255.255.255.0<->10.0.0.0/255.0.0.0 any
  Name:                 VPN-GW-2
  Unique Id:            ipsec-1-VPN-GW-2-pr0-10-r0
  Flags:                PE main mode
  Local Network [0]:    IPv4_ADDR_SUBNET<any:0, 192.168.2.0/255.255.255.0>
  Local Gateway:        IPv4_ADDR<any:0, 80.146.81.251>
  Remote Gateway:       IPv4_ADDR<any:0, 217.213.77.120>
  Remote Network [0]:   IPv4_ADDR_SUBNET<any:0, 10.0.0.0/255.0.0.0>

```

In der Ausgabe finden Sie die Informationen über die Netzbeziehungen, die für den Aufbau von VPN-Verbindungen zu anderen Netzwerken in Frage kommen.

In diesem Fall wird das lokale Netzwerk einer Filiale (Netzwerk 192.168.2.0 mit der Netzmaske 255.255.255.0) und das Netz der Zentrale (Netzwerk 10.0.0.0 mit der Netzmaske 255.0.0.0) angebunden. Die öffentliche IP-Adresse des eigenen Gateways lautet 80.146.81.251, die des entfernten VPN-Gateways ist die 217.213.77.120.



Die Angabe "any:0" zeigt die über die Verbindung erlaubten Protokolle und Ports an.

Eine erweiterte Ausgabe wird über den Befehl "show vpn long" aufgerufen. Hier finden Sie neben den Netzbeziehungen auch die Informationen über die sicherheitsrelevanten Parameter wie IKE- und IPSec-Proposals.

10.5.4 Manuelles Einrichten der VPN-Verbindungen

Beim manuellen Einrichten der VPN-Verbindungen fallen die schon beschriebenen Aufgaben an:

- ▶ Definition der Tunnelendpunkte
- ▶ Definition der sicherheitsrelevanten Parameter (IKE und IPSec)
- ▶ Definition der VPN-Netzbeziehungen, also der zu verbindenden IP-Adressbereiche. Bei überschneidenden IP-Netzbereichen auf den beiden Seiten der Verbindung bitte auch den Abschnitt 'N:N-Mapping' auf Seite 139 beachten.
- ▶ Bei Kopplung von Windows Netzwerken (NetBIOS/IP): Ohne WINS-Server auf beiden Seiten der VPN-Verbindung (z.B. bei der Anbindung von Home-Offices) kann das LANCOM entsprechende NetBIOS-Proxy-Funktionen übernehmen. Dazu muss das NetBIOS-Modul des LANCOM aktiviert sein, und die entsprechende VPN-Gegenstelle muss im NetBIOS-Modul als Gegenstelle eingetragen sein. Sind jedoch bei einer Standortkopplung in beiden Netzwerken eigene WINS-Server vorhanden, dann sollte das NetBIOS-Modul deaktiviert werden, so dass das LANCOM keine NetBIOS-Proxy-Funktionen mehr ausführt.



Um den NetBIOS-Proxy des LANCOM nutzen zu können muss entweder LANCOM Dynamic VPN verwendet werden, da dieses alle nötigen Adressen übermittelt, oder die IP-Adresse der Gegenstelle (hinter dem Tunnel, d.h. die dessen Intranet-Adresse) als primärer NBNS in der IP-Parameterliste (LANconfig: Kommunikation / Protokolle) eingetragen werden.

- ▶ Bei Nutzung von LANCOM Dynamic VPN: Eintrag für die entsprechende Gegenstelle in der PPP-Liste mit einem geeigneten Passwort für die Dynamic VPN Verhandlung. Als Benutzername ist derjenige VPN-Verbindungsname einzutragen, unter dem das Gerät in der VPN-Verbindungsliste der entfernten Gegenstelle angesprochen wird. Aktivieren Sie das „IP Routing“. Sollen auch Windows Netzwerke gekoppelt werden, so ist in diesem Eintrag zusätzlich NetBIOS zu aktivieren.

Als Tunnelendpunkt wird neben dem eigenen, lokalen VPN-Gateway jeweils eine VPN-Gegenstelle in der VPN-Verbindungsliste eingetragen.

Die manuelle Konfiguration der VPN-Verbindungen umfasst die folgenden Schritte:

- ① Legen Sie das entfernte VPN-Gateway in der Verbindungsliste an und tragen Sie dabei die öffentlich erreichbare Adresse ein.
- ② Die Sicherheitsparameter für die VPN-Verbindung werden in der Regel aus den vorbereiteten Listen entnommen, hier besteht neben der Definition eines IKE-Schlüssels kein weiterer Handlungsbedarf.
- ③ Bei einer Dynamic VPN-Verbindung erzeugen Sie einen neuen Eintrag in der PPP-Liste mit dem Namen des entfernten VPN-Gateways als Gegenstelle, mit dem Namen des lokalen VPN-Gateways als Benutzername und einem geeigneten Passwort. Für diese PPP-Verbindung aktivieren Sie auf jeden Fall das IP-Routing sowie je nach Bedarf auch das Routing von "NetBIOS über IP". Die restlichen PPP-Parameter wie das Verfahren für die Überprüfung der Gegenstelle können analog zu anderen PPP-Verbindungen definiert werden.


▷ Konfiguration von VPN-Verbindungen

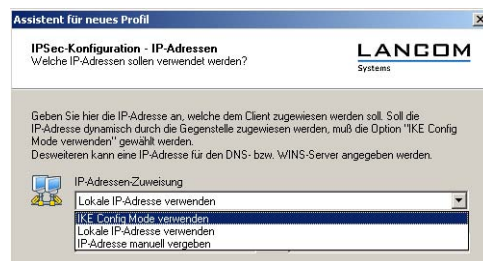
- ④ Die Hauptaufgabe bei der Einrichtung von VPN-Verbindungen liegt schließlich in der Definition der Netzbeziehungen: Welche IP-Adressbereiche sollen auf den beiden Seiten des VPN-Tunnels in die gesicherte Verbindung einbezogen werden?

10.5.5 IKE Config Mode

Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der „IKE-CFG“-Modus angegeben. Dieser kann die folgenden Werte annehmen:

- ▶ **Server:** In dieser Einstellung fungiert das Gerät als Server für diese VPN-Verbindung. Für die Zuweisung der IP-Adresse an den Client gibt es zwei Möglichkeiten:
 - ▷ Wenn die Gegenstelle in der Routing-Tabelle eingetragen ist, wird ihr die dort konfigurierte IP-Adresse zugewiesen.
 - ▷ Wenn die Gegenstelle nicht in der Routing-Tabelle eingetragen ist, wird eine freie IP-Adresse aus dem IP-Pool für die Einwahlzugänge entnommen.

 Die Gegenstelle muss dabei als IKE-CFG-Client konfiguriert sein und so vom Server eine IP-Adresse für die Verbindung anfordern. Für die Einwahl mit einem LANCOM Advanced VPN Client aktivieren Sie im Verbindungsprofil die Option **IKE Config Mode verwenden**.



- ▶ **Client:** In dieser Einstellung fungiert das Gerät als Client für diese VPN-Verbindung und fordert eine IP-Adresse für die Verbindung von der Gegenstelle (Server) an. Das Gerät verhält sich also so ähnlich wie ein VPN-Client.
- ▶ **Aus:** Ist der IKE-CFG-Modus ausgeschaltet, werden keine IP-Adressen für die Verbindung zugewiesen. Auf beiden Seiten der VPN-Strecke muss fest konfiguriert sein, welche IP-Adressen für diese Verbindung zu verwenden sind.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die VPN-Verbindungsliste im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' unter der Schaltfläche **Verbindungs-Liste**.

WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Einstellungen für den IKE-CFG-Modus auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► VPN ► Name-Liste
Terminal/Telnet	Setup/VPN/Namen-Liste

10.5.6 VPN-Netzbeziehungen erstellen

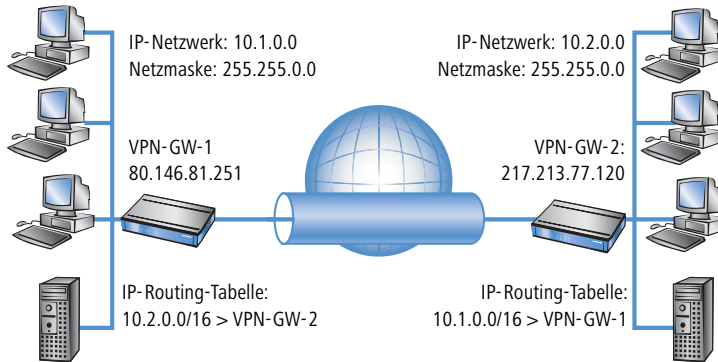
Mit der integrierten Firewall verfügen die LANCOM-Router über eine leistungsfähiges Instrument zur Definition von Quell- und Ziel-Adressbereichen, für die eine Datenübertragung (ggf. mit weiteren Einschränkungen) erlaubt bzw. verboten werden soll. Diese Funktionen werden auch für die Einrichtung der Netzbeziehungen für die VPN-Regeln verwendet.

Im einfachsten Fall kann die Firewall die VPN-Regeln automatisch erzeugen:

- Als Quellnetz wird dabei das lokale Intranet eingesetzt, also derjenige private IP-Adressbereich, zu dem das lokale VPN-Gateway selbst gehört.
- Als Zielnetze dienen für die automatisch erstellten VPN-Regeln die Netzbereiche aus der IP-Routing-Tabelle, für die als Router ein entferntes VPN-Gateway eingetragen ist.

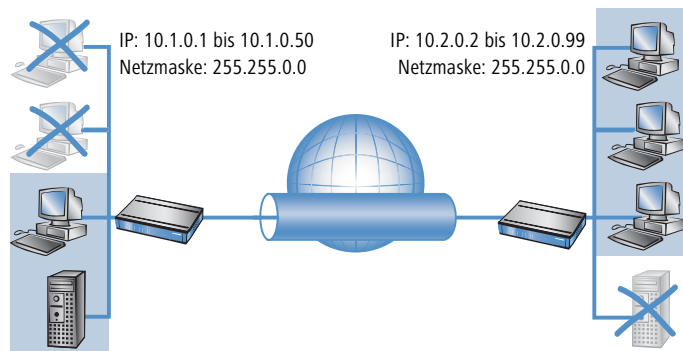
▷ Konfiguration von VPN-Verbindungen

Zum Aktivieren dieser automatischen Regelerzeugung reicht es aus, die entsprechende Option in der Firewall einzuschalten¹. Bei der Kopplung von zwei einfachen lokalen Netzwerken kann die VPN-Automatik aus dem IP-Adressbereich des eigenen LANs und dem Eintrag für das entfernte LAN in der IP-Routing-Tabelle die erforderliche Netzbeziehung ableiten.



Etwas aufwändiger wird die Beschreibung der Netzbeziehungen dann, wenn die Quell- und Zielnetze nicht nur durch den jeweiligen Intranet-Adressbereich der verbundenen LANs abgebildet werden:

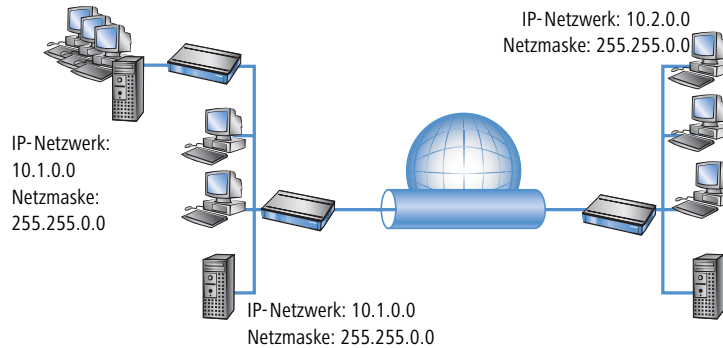
- Wenn nicht das gesamte lokale Intranet in die Verbindung mit dem entfernten Netz einbezogen werden soll, würde die Automatik einen zu großen IP-Adressbereich für die VPN-Verbindung freigeben.



- In vielen Netzstrukturen sind an das lokale Intranet über weitere Router noch andere Netzabschnitte mit eigenen IP-Adressbereichen angebunden. Diese Adressbereiche müssen über zusätzliche Einträge in die Netzbeziehung einbezogen werden.

1. automatisch bei Verwendung des VPN-Installationsassistenten unter LANconfig

▷ Konfiguration von VPN-Verbindungen



In diesen Fällen müssen die Netzbeziehungen zur Beschreibung der Quell- und Zielnetze manuell eingetragen werden. Je nach Situation werden dabei die automatisch erzeugten VPN-Regeln erweitert, manchmal muss die VPN-Automatik ganz abgeschaltet werden, um unerwünschte Netzbeziehungen zu vermeiden.

Die erforderlichen Netzbeziehungen werden durch entsprechende Firewall-Regeln unter den folgenden Randbedingungen definiert:

- ▶ Für die Firewall-Regel muss die Option "Diese Regel wird zur Erzeugung von VPN-Regeln herangezogen" aktiviert sein.



Die Firewall-Regeln zur Erzeugung von VPN-Regeln sind auch dann aktiv, wenn die eigentliche Firewall-Funktion im LANCOM-Gerät nicht benötigt wird und ausgeschaltet ist!

- ▶ Als Firewall-Aktion muss auf jeden Fall "Übertragen" gewählt werden.
- ▶ Als Quelle und Ziel für die Verbindung können einzelne Stationen, bestimmte IP-Adressbereiche oder ganze IP-Netzwerke eingetragen werden.



Die Zielnetze müssen auf jeden Fall in der IP-Routing-Tabelle definiert sein, damit der Router in den LANCOM-Geräten die entsprechenden Datenpakete in das andere Netz weiterleiten kann. Die dort schon vorhandenen Einträge können Sie nutzen und nur ein übergeordnetes Netzwerk als Ziel eintragen. Die Schnittmenge aus dem Eintrag des Zielnetzes in der Firewall und den untergeordneten Einträgen in der IP-Routing-Tabelle fließt in die Netzbeziehungen für die VPN-Regeln ein.

Beispiel: In der IP-Routing-Tabelle sind die Zielnetze 10.2.1.0/24, 10.2.2.0/24 und 10.2.3.0/24 eingetragen, die alle über den Router VPN-GW-2 erreichbar sind. In der Firewall reicht ein Eintrag mit dem Zielnetz 10.2.0.0/16, um die drei gewünschten Subnetze in die VPN-Regeln einzubeziehen.

▷ Konfiguration von VPN-Verbindungen

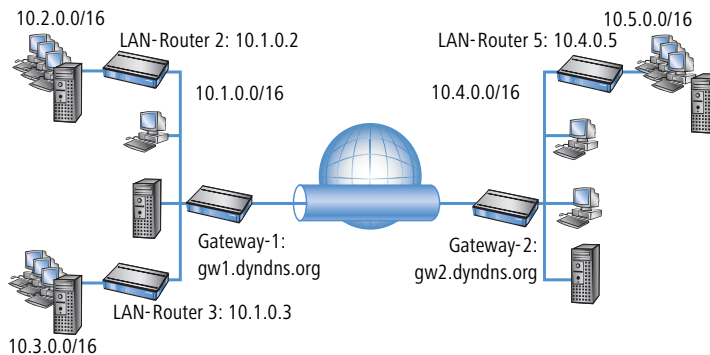
i Die Quell- und Zielnetze müssen auf beiden Seiten der VPN-Verbindung übereinstimmend definiert werden. Es ist z.B. nicht möglich, einen größeren Ziel-Adressbereich auf einen kleineren Quell-Adressbereich auf der Gegenseite abzubilden. Maßgebend sind dabei die in den VPN-Regeln gültigen IP-Adressbereiche, nicht die in den Firewall-Regeln eingetragenen Netze. Diese können aufgrund der Schnittmengenbildung durchaus von den Netzbeziehungen in den VPN-Regeln abweichen.

▶ Je nach Bedarf kann die VPN-Verbindung zusätzlich auf bestimmte Dienste oder Protokolle eingeschränkt werden. So kann die VPN-Verbindung z.B. nur auf die Nutzung für ein Windows-Netzwerk reduziert werden.

i Verwenden Sie für diese Einschränkungen eigene Regeln, die nur für die Firewall gelten und nicht zur Erzeugung von VPN-Regeln herangezogen werden. Kombinierte Firewall/VPN-Regeln können sehr leicht komplex und schwer überschaubar werden.

10.5.7 Konfiguration mit LANconfig

Dieser Abschnitt zeigt die Konfiguration einer LAN-LAN-Kopplung mit zusätzlichen Subnetzen mit Hilfe von LANconfig. In diesem Abschnitt wird das VPN-Gateway 1 konfiguriert, die Einstellung von Gateway 2 wird anschließend mit Hilfe von WEBconfig demonstriert.



① Legen Sie im Konfigurationsbereich VPN auf der Registerkarte „IKE-Param.“ einen neuen IKE-Schlüssel für die Verbindung an:



▷ Konfiguration von VPN-Verbindungen

- ② Erstellen Sie auf der Registerkarte „Allgemein“ einen neuen Eintrag in der Liste der Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus. PFS- und IKE-Gruppe können Sie ebenso wie IKE- und IPSec-Proposals aus den vorbereiteten Möglichkeiten wählen.

- ③ Erstellen Sie dann einen neuen Eintrag in der Verbindungs-Liste mit dem Namen des entfernten Gateways als „Name der Verbindung“. Für LANCOM Dynamic VPN Verbindungen muss der Eintrag „Entferntes Gateway“ leer bleiben. Andernfalls tragen Sie hier die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.

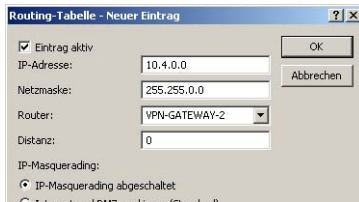
Name	Haltezeit	DPD	Extranet	Gateway	Parameter	Regel	Dynamisch	IKE-Exchange	IKE-CFG
LCS	30 Sekunden	0 Sekunden	10.99.100.52	213.217.69.77	LCS	Automatisch	Ja (ICMP)	Main Mode	Aus
CHOFMJJSTER	0 Sekunden	0 Sekunden	0.0.0.0	0.0.0.0	P-CHOFMJJSTER	Automatisch	Nein	Main Mode	Aus
JWRIGHT	0 Sekunden	60 Sekunden	0.0.0.0	0.0.0.0	P-JWRIGHT	Manuell	Nein	Aggr. Mode	Aus
CHOFMJJSTER2	0 Sekunden	60 Sekunden	0.0.0.0	0.0.0.0	P-CHOFMJJSTER2	Manuell	Nein	Aggr. Mode	Aus
KMJJSTERMANN	0 Sekunden	60 Sekunden	0.0.0.0	0.0.0.0	P-KMJJSTERMANN	Manuell	Nein	Aggr. Mode	Aus
NHAMEL_MOEBIL	0 Sekunden	60 Sekunden	0.0.0.0	0.0.0.0	P-NHAMEL_MOEBIL	Manuell	Nein	Aggr. Mode	Aus
TEST	0 Sekunden	3.000 Sekunden	0.0.0.0	0.0.0.0	P-TEST	Manuell	Nein	Aggr. Mode	Aus

- ④ Bei Nutzung von LANCOM Dynamic VPN: Wechseln Sie in den Konfigurationsbereich „Kommunikation“. Erstellen Sie auf der Registerkarte „Protokolle“ in der PPP-Liste einen neuen Eintrag. Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie ein geeignetes, auf beiden Seiten identisches Passwort ein, welches aus Sicherheitsgründen nicht identisch mit dem verwendeten Pre-Shared Key sein sollte.

Aktivieren Sie auf jeden Fall das „IP-Routing“ und je nach Bedarf „NetBIOS über IP“ (→Seite 265).

▷ Konfiguration von VPN-Verbindungen

- ⑤ Wechseln Sie in den Konfigurationsbereich „IP-Router“. Erstellen Sie auf der Registerkarte „Routing“ einen neuen Eintrag in der Routingtabelle für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.



Für das „VPN-Gateway-1“ sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

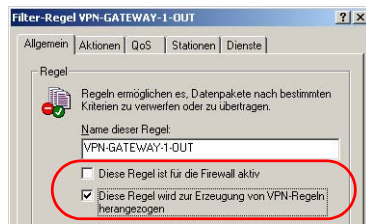
IP-Adresse	Netzmaske	Router	IP-Masquerading
10.4.0.0	255.255.0.0	VPN-Gateway-2	Nein
10.5.0.0	255.255.0.0	VPN-Gateway-2	Nein

Für die an das eigene LAN angebandenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	Netzmaske	Router	IP-Masquerading
10.2.0.0	255.255.0.0	10.1.0.2	Nein
10.3.0.0	255.255.0.0	10.1.0.3	Nein

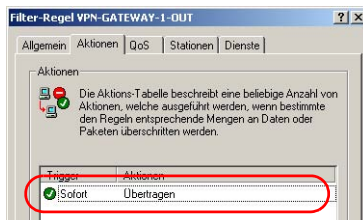
Mit diesen Einträgen ist das VPN-Gateway 1 in der Lage, auch die aus dem entfernten Netz eintreffende Pakete für die angebandenen Netzabschnitte richtig weiterzuleiten.

- ⑥ Wechseln Sie in den Konfigurationsbereich „Firewall/QoS“. Erstellen Sie auf der Registerkarte „Regeln“ eine neue Firewall-Regel mit dem Namen „VPN-GATEWAY-1-OUT“ und aktivieren Sie für diese Regel die Option „Diese Regel wird für die Erzeugung von VPN-Regeln herangezogen“. Damit legen Sie fest, dass die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.

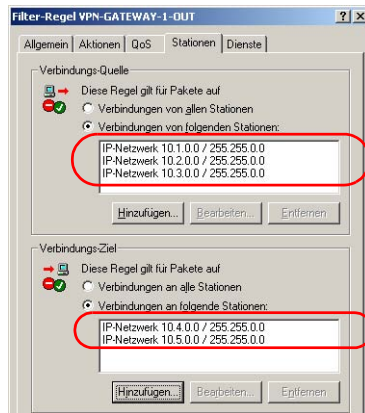


Die Firewall-Regeln zum Erzeugen von VPN-Netzbeziehungen mit Angabe der Tunnelendpunkte (IP-Quell- und Ziel-Adressen) sollten auf jeden Fall von Firewall-Regeln zum Filtern (z.B. der zu übertragenden bzw. der zu sperrenden Protokolle) getrennt werden. Die Verknüpfung dieser beiden Aspekte kann zu einer hohen Anzahl der intern verwalteten VPN-Beziehungen und damit zu Performanceverlusten in den VPN-Tunneln führen.

- ⑦ Auf der Registerkarte „Aktionen“ dieser Firewall-Regel stellen Sie als Paketaktion „Übertragen“ ein.

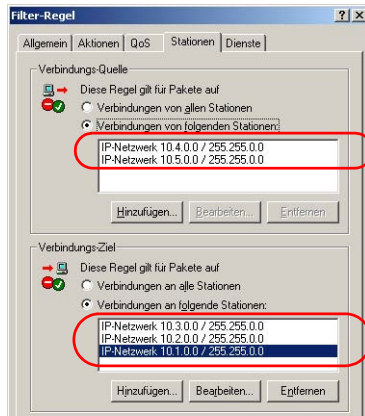


- ⑧ Auf der Registerkarte „Stationen“ dieser Firewall-Regel stellen Sie für die ausgehende Datenübertragung als Quelle als Teilnetze auf der lokalen Seite ein, als Ziel alle Teilnetze auf der entfernten Seite.



► Konfiguration von VPN-Verbindungen

- ⑨ Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GATEWAY-1-IN“ mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:



10.5.8 Konfiguration mit WEBconfig

- ① Legen Sie unter **Konfiguration ► VPN ► IKE-Param. ► IKE-Schlüssel** einen neuen IKE-Schlüssel für die Verbindung an:



- ② Erstellen Sie unter **Konfiguration ► VPN ► Allgemein ► Verbindungsparameter** einen neuen „VPN-Layer“ für die Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus.



▷ Konfiguration von VPN-Verbindungen

- ③ Erstellen Sie unter **Konfiguration ► VPN ► Verbindungsliste** einen neuen Eintrag mit dem Namen des entfernten Gateways als „Name“. Als „Entferntes Gateway“ tragen Sie die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.

- ④ Bei Nutzung von LANCOM Dynamic VPN: Erstellen Sie unter **Konfiguration ► Setup ► WAN ► PPP** einen neuen Eintrag. Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie geeignetes, auf beiden Seiten identisches Passwort ein.

Aktivieren Sie auf jeden Fall das „IP-Routing“ und je nach Bedarf „NetBIOS über IP“ (→Seite 265).

- ⑤ Erstellen Sie unter **Konfiguration ► Setup ► IP-Router ► IP-Routing-Tabelle** einen neuen Eintrag für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.

▷ Konfiguration von VPN-Verbindungen

Für das „VPN-Gateway-2“ sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

IP-Adresse	Netzmaske	Router	IP-Masquerading
10.1.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.2.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.3.0.0	255.255.0.0	VPN-Gateway-1	Nein

Für die an das eigene LAN angebandenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	Netzmaske	Router	IP-Masquerading
10.5.0.0	255.255.0.0	10.4.0.5	Nein

Mit diesen Einträgen ist das VPN-Gateway 2 in der Lage, auch die aus dem entfernten Netz eintreffen Pakete für die angebandenen Netzabschnitte richtig weiterzuleiten.

- ⑥ Erstellen Sie unter **Konfiguration ► Firewall/QoS ► Objekt-Tabelle** jeweils einen Eintrag für die Netzbereiche, die bei der VPN-Verbindung mit „VPN-GATEWAY-1“ als Quelle oder Ziel verwendet werden sollen („VPN-GW1-LOCAL“ und „VPN-GW1-REMOTE“). Geben Sie dabei die Netzbereiche z.B. in der Form „%A10.1.0.0%M255.255.0.0“ ein.



- ⑦ Erstellen Sie unter **Konfiguration ► Firewall/QoS ► Regel-Tabelle** eine neue Firewall-Regel mit dem Namen „VPN-GW1-OUT“. Verwenden Sie dabei die Objekte „VPN-GW1-LOCAL“ und „VPN-GW1-REMOTE“, die Protokolle „ANY“ und die Aktion „ACCEPT“. Aktivieren Sie die Option „VPN-Regel“, damit die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.

Experten-Konfiguration
 Setup
 IP-Router-Modul
 Firewall

Regel-Tabelle

Name: VPN-GW1-OUT
 Prot.: ANY
 Quelle: VPN-GW1-LOCAL
 Ziel: VPN-GW1-REMOTE
 Aktion: ACCEPT
 verknuepft: nein
 Prio: 0
 Aktiv: ja
 VPN-Regel: ja
 Stateful: nein
 Kommentar:



In der Regel empfiehlt sich die Trennung von Regeln, mit denen die VPN-Netzbeziehungen gebildet werden, und den Firewall-Regeln, die Auswirkungen z.B. auf die bei der Kommunikation zugelassenen Dienste haben.

- ⑧ Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GW1-IN“ mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:

Experten-Konfiguration
 Setup
 IP-Router-Modul
 Firewall

Regel-Tabelle

Name: VPN-GW1-IN
 Prot.: ANY
 Quelle: VPN-GW1-REMOTE
 Ziel: VPN-GW1-LOCAL
 Aktion: ACCEPT

10.5.9 Diagnose der VPN-Verbindungen

Wenn die VPN-Verbindungen nach der Konfiguration der entsprechenden Parameter nicht wie gewünscht zustande kommen, stehen folgende Möglichkeiten zur Diagnose zur Verfügung:

- ▶ Mit dem Befehl **show vpn spd** an der Telnet-Konsole rufen Sie die „Security Policy Definitions“ auf.
- ▶ Mit dem Befehl **show vpn sadb** rufen Sie die Informationen über die ausgehandelten „Security Associations“ (SAs) auf.
- ▶ Mit dem Befehl **trace + vpn** [status, packet] können Sie die Status- und Fehlermeldungen der aktuellen VPN-Verhandlung aufrufen.
 - ▷ Die Fehlermeldung „No proposal chosen“ deutet auf einen Fehler in der Konfiguration der Gegenstelle hin.
 - ▷ Die Fehlermeldung „No rule matched“ deutet hingegen auf einen Fehler in der Konfiguration des lokalen Gateways hin.

▷ Einsatz von digitalen Zertifikaten

10.6 Einsatz von digitalen Zertifikaten

Die Sicherheit der Kommunikation über VPN erfüllt im Kern drei Anforderungen:

- **Vertraulichkeit:** Die übertragenen Daten können von keinem Unbefugten gelesen werden (über Verschlüsselung).
- **Integrität:** Die Daten können während der Übertragung nicht unbemerkt verändert werden (über Authentifizierung).
- **Authentizität:** Der Empfänger kann sicher sein, dass die empfangenen Daten auch tatsächlich vom vermuteten Absender stammen (über Authentifizierung).

Für die Verschlüsselung und Authentifizierung von Daten stehen zahlreiche Verfahren zur Verfügung, mit denen die beiden ersten Aspekte – Vertraulichkeit und Integrität – ausreichend abgedeckt werden können. Der Einsatz von digitalen Zertifikaten verfolgt das Ziel, auch die Authentizität der Kommunikationspartner zu sichern.

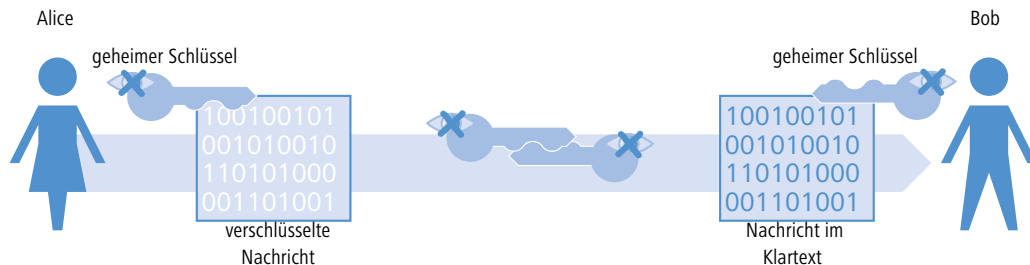
10.6.1 Grundlagen

Verschlüsselungsverfahren kann man in zwei Kategorien einteilen: Die symmetrische und die asymmetrische Verschlüsselung.

Die symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist seit Jahrtausenden bekannt und basiert darauf, dass sowohl der Sender als auch der Empfänger einer Nachricht über einen gemeinsamen, geheimen Schlüssel verfügen. Dieser Schlüssel kann sehr unterschiedliche Gestalt haben: Die Römer verwendeten zum Ver- und Entschlüsseln z.B. einen Stab mit einem ganz bestimmten Durchmesser.

In der heutigen digitalen Kommunikation handelt es sich bei dem Schlüssel meist um ein besonderes Passwort. Mit Hilfe dieses Passwortes und eines Verschlüsselungsalgorithmus werden die Daten vom Sender verändert. Der Empfänger verwendet den gleichen Schlüssel und einen passenden Entschlüsselungsalgorithmus, um die Daten wieder lesbar zu machen. Jede andere Person, die den Schlüssel nicht kennt, kann die Daten nicht lesen. Ein übliches symmetrisches Verschlüsselungsverfahren ist z.B. 3DES.



Beispiel:

▷ Einsatz von digitalen Zertifikaten

- ▶ Alice möchte Bob eine vertrauliche Nachricht zukommen lassen. Dazu verschlüsselt sie die Nachricht mit einem geheimen Schlüssel und einem geeigneten Verfahren, z.B. 3DES. Die verschlüsselte Nachricht schickt sie an Bob und teilt ihm dabei mit, welches Verschlüsselungsverfahren sie verwendet hat.
- ▶ Bob verfügt über den gleichen Schlüssel wie Alice. Da er von Alice nun auch das Verschlüsselungsverfahren kennt, kann er die Nachricht entschlüsseln und in den Klartext zurückverwandeln.

Die symmetrische Verschlüsselung ist sehr einfach und effizient in der Handhabung, hat aber zwei gravierende Nachteile:

- ▶ Für jede geheime Kommunikationsbeziehung wird ein eigener Schlüssel benötigt. Wenn neben Alice und Bob noch Carol dazukommt, werden schon drei Schlüssel benötigt, um die jeweiligen Datenübertragungen untereinander abzusichern, bei vier Teilnehmern sechs Schlüssel, bei 12 Teilnehmern 66 und bei 1000 Teilnehmern schon fast 500.000! In einem weltweiten Netz mit immer höheren Anforderungen an die gesicherte Kommunikation zahlreicher Teilnehmer wird das schon zu einem ernsthaften Problem.
- ▶ Während der erste Nachteil mit Hilfe der Technik evtl. zu lösen wäre, ist der Zweite ein Kernproblem der symmetrischen Verschlüsselung: Der geheime Schlüssel muss auf beiden Seiten der Datenübertragung bekannt sein und darf nicht in unbefugte Hände geraten. Alice kann den Schlüssel also nicht einfach per E-Mail an Bob schicken, bevor die Datenverbindung ausreichend gesichert ist, wozu genau dieser Schlüssel beitragen soll. Sie müsste den Schlüssel schon persönlich an Bob übergeben oder ihn zumindest über ein „abhörsicheres“ Verfahren übermitteln. Diese Aufgabe ist in Zeiten weltweiter dynamischer Datenkommunikation kaum zu bewältigen.

Das Verfahren der asymmetrischen Verschlüsselung

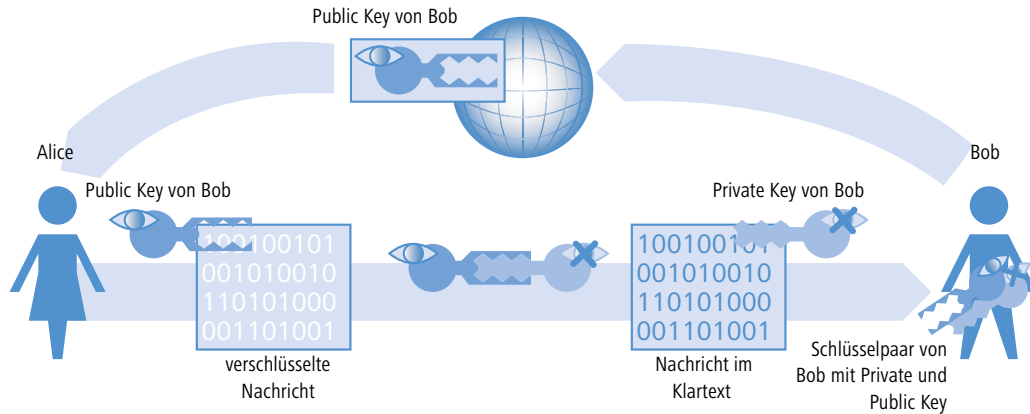
Als grundlegend neuer Ansatz wurde in den 1970er Jahren die asymmetrische Verschlüsselung entwickelt. Diese Variante setzt nicht mehr auf einen Schlüssel, der auf beiden Seiten bekannt und dabei geheim ist, sondern auf ein Schlüsselpaar:

- ▶ Der erste Teil des Schlüsselpaares wird zum **Verschlüsseln** der Daten verwendet, die zum Eigentümer des Schlüssels gesendet werden. Dieser öffentliche Schlüssel (oder im Folgenden Public Key genannt) darf weltweit allen Interessenten öffentlich zur Verfügung gestellt werden.
- ▶ Der zweite Teil des Schlüsselpaares ist der private Schlüssel (Private Key), der nur zum **Entschlüsseln** der empfangenen Botschaften verwendet wird. Dieser Schlüssel ist geheim und darf nicht in die Hände Unbefugter geraten.

Der große Unterschied gegenüber den symmetrischen Verschlüsselungen: Es wird ein öffentlich bekannter Schlüssel verwendet, daher spricht man hier auch vom „Public-Key-Verfahren“. Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist z.B. RSA.

▷ Einsatz von digitalen Zertifikaten

Sehen wir uns wieder das Beispiel von Alice und Bob an:



- ▶ Bob erzeugt für die gesicherte Kommunikation zunächst ein Schlüsselpaar mit einem Private Key und einem Public Key, die genau zueinander passen. Beim Erstellen dieser Schlüssel wird ein Verfahren verwendet, mit dem der Private Key nicht aus dem Public Key zurückgerechnet werden kann. Den Public Key kann Bob jetzt bedenkenlos öffentlich bekannt machen. Er kann ihn per Mail an Alice schicken oder einfach auf seinem Webserver ablegen.
- ▶ Alice verschlüsselt nun die Nachricht an Bob mit dessen Public Key. Die so unkenntlich gemachte Botschaft kann nur noch mit dem Private Key von Bob entschlüsselt werden. Selbst wenn die Daten auf dem Weg von Alice zu Bob mitgehört werden, kann niemand außer Bob den Klartext entziffern!

Die asymmetrische Verschlüsselung bietet gegenüber der symmetrischen Variante folgende Vorteile:

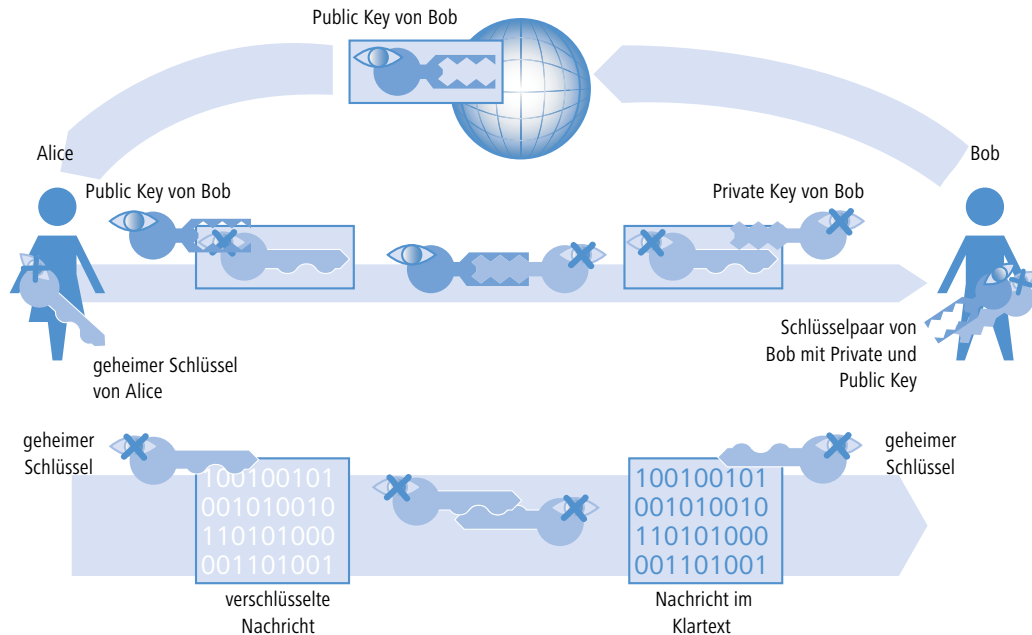
- ▶ Es wird nicht für jede Kommunikationsbeziehung ein Schlüsselpaar benötigt, sondern nur für jeden Teilnehmer. Bei 1000 Teilnehmern benötigt jeder nur sein eigenes Schlüsselpaar, von dem er den Public Key öffentlich zur Verfügung stellt. Anstelle der 500.000 geheimen Schlüssel werden beim Public Key-Verfahren also nur 1000 Schlüsselpaare verwendet.
- ▶ Die unsichere Übertragung des geheimen Schlüssels an die Kommunikationspartner entfällt, da nur der Public Key auf der jeweils anderen Seite der Kommunikationsbeziehung bekannt sein muss. Damit wird ein wesentliches Problem bei der dynamischen Verschlüsselung von Daten zwischen vielen Teilnehmern gelöst.

Kombination von symmetrischer und asymmetrischer Verschlüsselung

Aufgrund Ihrer Sicherheit konnten sich asymmetrische Verschlüsselungsverfahren schnell etablieren. Doch hat die Sicherheit auch Ihren Preis: Asymmetrische Verschlüsselungsverfahren sind langsam. Die mathematischen Verfahren zum Ver- und Entschlüsseln von Nachrichten sind sehr viel aufwändiger als bei symmetrischen Verschlüsselungsverfahren und brauchen daher auch mehr Rechenzeit, was bei der Übertragung von großen Datenmengen zum Ausschlusskriterium wird.

Die Vorteile von symmetrischer und asymmetrischer Verschlüsselung können in einer geeigneten Kombination ausgenutzt werden. Dabei wird die sichere asymmetrische Verschlüsselung dazu verwendet, die Übertragung des gehei-

men Schlüssels zu schützen. Die eigentlichen Nutzdaten der Verbindung werden anschließend mit den schnelleren symmetrischen Verfahren verschlüsselt.



- Bob erstellt im ersten Schritt sein Schlüsselpaar und stellt den Public Key öffentlich bereit.
- Alice verwendet den Public Key, um damit einen geheimen, symmetrischen Schlüssel zu **verschlüsseln** und schickt ihn an Bob. Dieser geheime Schlüssel wird bei jeder Übertragung durch ein Zufallsverfahren neu bestimmt.
- Nur Bob kann den geheimen Schlüssel nun wieder mit Hilfe seines Private Keys **entschlüsseln**.
- Alice und Bob verwenden dann den geheimen Schlüssel zum **Ver-** und **Entschlüsseln** der deutlich größeren Nutzdaten-Volumina.

Public-Key-Infrastructure

Die Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren erlaubt es, auch über zunächst ungesicherte Verbindungen eine sichere Datenkommunikation aufzubauen. Dabei wurde bisher der Aspekt der Authentizität nicht beleuchtet: Woher weiß Alice, dass der verwendete Public Key auch tatsächlich von Bob stammt? Die Verwendung von Public-Keys hängt also vom Vertrauen an die Authentizität der Kommunikationspartner ab.

Um dieses Vertrauen zu sichern, können die verwendeten Schlüsselpaare der asymmetrischen Verschlüsselung von öffentlich anerkannten, vertrauenswürdigen Stellen bestätigt werden. So ist z.B. in Deutschland die Regulierungsbehörde für Telekommunikation und Post (RegTP) die oberste vertrauenswürdige Instanz bei der Bestätigung von

▷ Einsatz von digitalen Zertifikaten

digitalen Schlüsseln. Diese wiederum vergibt Akkreditierungen an geeignete Dienstleister, die ebenfalls als vertrauenswürdig angesehen werden.

i Auf der Webseite der RegTP (www.regtp.de) finden Sie ständig aktuelle Listen mit akkreditierten Zertifizierungsdiensteanbietern sowie Hinweise auf widerrufenen Akkreditierungen. Unter den akkreditierten Dienstleistern befinden sich z.B. zahlreiche Steuerberater und Anwaltskammern.

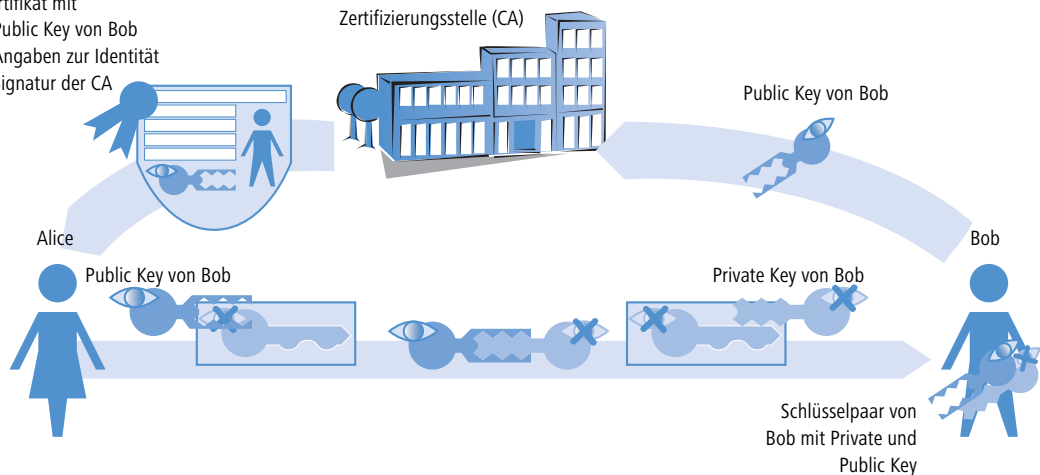
Die Aufgabe dieser Stellen ist es, einen Public Key genau einer Person oder Organisation zuzuordnen. Diese Zuordnung wird in einem bestimmten Dokument – einem Zertifikat – festgehalten und öffentlich bekannt gemacht. Diese Anbieter werden daher auch als Zertifizierungsstellen bezeichnet, im Englischen als „Certification Authority“ oder kurz CA bezeichnet. Die oberste Zertifizierungsstelle gilt als die Stamm oder Wurzel-CA bzw. Root-CA.

An eine solche CA kann sich Bob nun wenden, wenn er seinen Public Key für seine eigene Person zertifizieren lassen möchte. Dazu reicht er seinen Public Key bei der CA ein, die die Zugehörigkeit des Schlüssels zu Bob bestätigt.

Die CA stellt über diese Bestätigung ein Zertifikat aus, das neben dem Public Key von Bob auch weitere Angaben u.a. über seine Identität enthält.

Zertifikat mit

- Public Key von Bob
- Angaben zur Identität
- Signatur der CA



Das Zertifikat selbst wird von der CA wiederum signiert, damit auch die Bestätigung nicht angezweifelt werden kann. Da das Zertifikat nur aus einer kleinen Datenmenge besteht, kann dazu ein asymmetrisches Verfahren verwendet werden. Bei der Signatur wird das asymmetrische Verfahren jedoch in umgekehrter Richtung eingesetzt:

- Auch die CA verfügt über ein Schlüsselpaar aus Private und Public Key. Als vertrauenswürdige Stelle kann ihr eigenes Schlüsselpaar als zuverlässig angesehen werden.
- Die CA berechnet einen Hash-Wert über das Zertifikat, verschlüsselt diesen und signiert damit das Zertifikat von Bob. Dadurch wird die Zuordnung von Bobs Public Key zu seiner Identität bestätigt.

▷ Einsatz von digitalen Zertifikaten

Dieser Vorgang verhält sich genau umgekehrt wie bei der normalen asymmetrischen Verschlüsselung. Hier hat die Verschlüsselung aber nicht die Aufgabe, die Daten vor Unbefugten zu sichern, sondern die Signatur der CA zu bestätigen.

- ▶ Jeder Teilnehmer einer Datenkommunikation weltweit ist nun mit dem Public Key der CA in der Lage, das so signierte Zertifikat zu überprüfen.

Nur die CA kann mit ihrem eigenen Private Key Signaturen erzeugen, die mit dem Public Key der CA wieder entschlüsselt werden können. Durch diese Signatur ist sichergestellt, dass das Zertifikat tatsächlich von der ausstellenden CA stammt.

10.6.2 Vorteile von Zertifikaten

Die Verwendung von Zertifikaten zur Absicherung von VPN-Verbindungen bietet sich in manchen Fällen als Alternative zum sonst eingesetzten Preshared-Key-Verfahren (PSK-Verfahren) an:

- ▶ Sicherere VPN-Client-Verbindungen (mit IKE Main Mode)

Beim PSK-Verbindungsaufbau von Peers mit dynamischen IP-Adressen kann der Main Mode nicht eingesetzt werden. Hier muss der Aggressive Mode mit geringerer Sicherheit verwendet werden. Der Einsatz von Zertifikaten erlaubt auch bei Peers mit dynamischen IP-Adressen wie z.B. Einwahlrechnern mit LANCOM Advanced VPN Client die Verwendung des Main Mode und damit eine Steigerung der Sicherheit.

- ▶ Höhere Sicherheit der verwendeten Schlüssel bzw. Kennwörter

Preshared Keys sind genau so anfällig wie alle anderen Kennwörter auch. Der Umgang der Anwender mit diesen Kennwörtern („menschlicher Faktor“) hat also erheblichen Einfluss auf die Sicherheit der Verbindungen. Bei einem zertifikatsbasierten VPN-Aufbau werden die in den Zertifikaten verwendeten Schlüssel automatisch mit der gewünschten Schlüssellänge erstellt. Darüber hinaus sind die von Rechnern erstellten, zufälligen Schlüssel auch bei gleicher Schlüssellänge sicherer gegen Angriffe (z.B. Wörterbuchangriffe) als die von Menschen erdachten Preshared Keys.

- ▶ Prüfung der Authentizität der Gegenseite möglich

Beim VPN-Verbindungsaufbau über Zertifikate müssen sich die beiden Gegenstellen authentifizieren. In den Zertifikaten können dabei weitere Info-Elemente enthalten sein, die zur Prüfung der Gegenstellen herangezogen werden. Die zeitliche Befristung der Zertifikate gibt zusätzlichen Schutz z.B. bei der Vergabe an Anwender, die nur vorübergehend Zugang zu einem Netzwerk erhalten sollen.

- ▶ Unterstützung von Tokens und Smartcards

Mit der Auslagerung der Zertifikate auf externe Datenträger gelingt auch die Integration in „Strong Security“-Umgebungen, das Auslesen von Kennwörtern aus Computern oder Notebooks wird verhindert.

Den Vorteilen von Zertifikaten steht allerdings der höhere Aufwand für die Einführung und Pflege einer Public Key Infrastructure (PKI) gegenüber.

▷ Einsatz von digitalen Zertifikaten

10.6.3 Aufbau von Zertifikaten

Inhalte

Um seinen Aufgaben gerecht werden zu können, enthält ein Zertifikat diverse Informationen. Einige davon sind verpflichtend, andere sind optional. Es gibt verschiedene Formate, in denen ein Zertifikat gespeichert werden kann. Ein Zertifikat nach dem X.509-Standard beinhaltet z.B. folgende Informationen:

- ▶ Version: Dieser Eintrag enthält die Version des X.509-Standards. Die derzeit (06/2005) aktuelle Version ist 'v3'.
- ▶ Serial Number: Eine eindeutige Seriennummer, über die ein Zertifikat identifiziert werden kann.
- ▶ Signature Algorithm: Identifiziert den Algorithmus, mit dem der Aussteller das Zertifikat unterschreibt. Außerdem findet sich hier die digitale Unterschrift des Ausstellers.
- ▶ Validity: Zertifikate sind zeitlich begrenzt gültig. Validity enthält Informationen über die Dauer.
- ▶ Issuer: Daten zur Identifizierung des Ausstellers, z.B. Name, Email-Adresse, Nationalität etc.
- ▶ Subject: Daten zur Identifizierung des Eigentümers des Zertifikates, z.B. Name, Institution, Email-Adresse, Nationalität, Stadt etc.
- ▶ Subject Public Key: Informationen, welches Verfahren zum Generieren des öffentlichen Schlüssels des Zertifikatsinhabers verwendet wurde. Außerdem findet sich unter diesem Punkt der Public Key des Eigentümers.

Zielanwendung

Bei der Erstellung der Zertifikate wird üblicherweise ausgewählt, für welchen Zweck die Zertifikate eingesetzt werden können. Manche Zertifikate sind gezielt nur für Webbrowser oder E-Mail-Übertragung gedacht, andere sind allgemein für beliebige Zwecke einsetzbar.



Achten Sie bei der Erstellung der Zertifikate darauf, dass sie für den gewünschten Zweck ausgestellt werden.

Formate

Für die Form der Zertifikate ist der ITU-Standard X.509 weit verbreitet. In Textdarstellung sieht ein solches Zertifikat z.B. wie folgt aus:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/
Email=ca@trustme.dom

Validity

▷ Einsatz von digitalen Zertifikaten

```
Not Before: Oct 29 17:39:10 2000 GMT
Not After : Oct 29 17:39:10 2001 GMT
Subject: C=DE, ST=Austria, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/
Email=xyz@anywhere.com
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
      d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
      9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
      90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
      1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
      7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
      50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
      8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
      f0:b4:95:f5:f9:34:9f:f8:43
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Alternative Name:
    email:xyz@anywhere.com
  Netscape Comment:
    mod_ssl generated test server certificate
  Netscape Cert Type:
    SSL Server
Signature Algorithm: md5WithRSAEncryption
12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
```

▷ Einsatz von digitalen Zertifikaten

ff:8e

Dateitypen

Digitale Zertifikate und Private Keys liegen je nach Aussteller mit verschiedenen Dateierendungen vor. Üblich sind z.B. die Endungen:

- ▶ *.pfx und *.p12: PKCS#12-Dateien
- ▶ *.pem, *.cer und *.crt: BASE-64-codierte Zertifikate
- ▶ *.cer, *.crt und *.der: DER-codierte Zertifikate
- ▶ *.key: BASE64- oder DER-codierte Schlüssel
- ▶ *.pvk: Microsoft-spezifisches Schlüsselformat

Im Umfeld der zertifikatsgesicherten VPN-Verbindungen ist neben den reinen Zertifikaten noch ein weiterer Dateityp von großer Bedeutung: die PCKS#12-Dateien, in denen mehrere Komponenten enthalten sein können, u.a. ein Zertifikat und ein Private Key. Zur Verarbeitung der PKCS#12-Dateien ist ein Kennwort erforderlich, das beim Exportieren der Zertifikate festgelegt wird.



BASE64-codierte Zertifikate tragen im Header üblicherweise die Zeile:

```
----- BEGIN CERTIFICATE -----
```

Gültigkeit

Darüber hinaus kann optional ein Verweis auf eine so genannte Certificate Revocation List (CRL) eingefügt werden. In CRL's sind Zertifikate aufgelistet, die ungültig geworden sind, z.B. weil ein Mitarbeiter eine Firma verlassen hat und sein Zertifikat deshalb zurückgezogen wurde. Mit dieser Angabe kann bei der Prüfung der Zertifikate die richtige CRL verwendet werden.

10.6.4 Sicherheit

Auch beim Umgang mit Zertifikaten sind bestimmte Sicherheitsaspekte zu beachten:

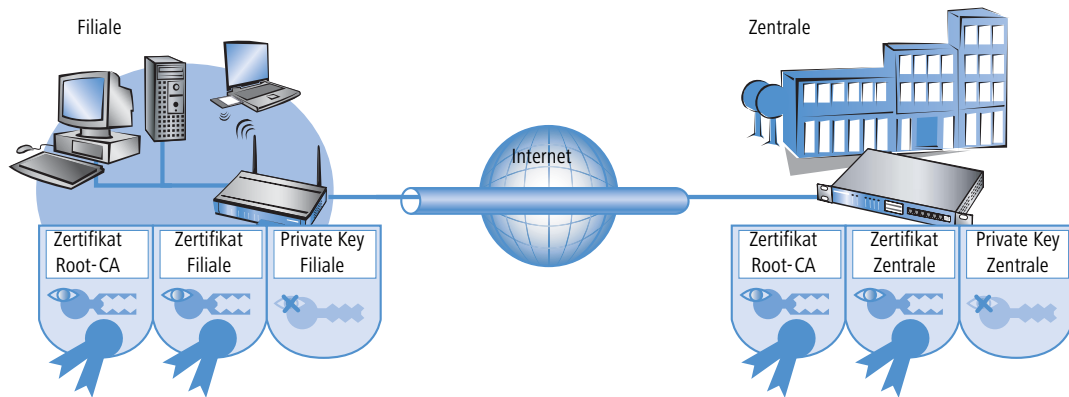
- ▶ Übertragen Sie die Private Keys nur über sichere Verbindungen, z.B. mit HTTPS.
- ▶ Verwenden Sie als Kennwörter für Schlüssel oder PKCS#12-Dateien nur ausreichend lange und sichere Passphrasen.

10.6.5 Zertifikate beim VPN-Verbindungsaufbau

Neben den grundlegenden Informationen zum Thema Zertifikate betrachten wir in diesem Abschnitt die konkrete Anwendung beim VPN-Verbindungsaufbau. Für einen solchen Verbindungsaufbau mit Zertifikatsunterstützung müs-

▷ Einsatz von digitalen Zertifikaten

sen auf beiden Seiten der Verbindung (z.B. Anbindung einer Filiale an das Netzwerk der Zentrale über LANCOM-Router) bestimmte Informationen vorhanden sein:



- Die Filiale verfügt über folgende Komponenten:
 - ▷ Zertifikat der Root-CA mit dem Public Key der CA
 - ▷ Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
 - ▷ Eigener Private Key
- Die Zentrale verfügt über folgende Komponenten:
 - ▷ Zertifikat der Root-CA mit dem Public Key der CA
 - ▷ Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
 - ▷ Eigener Private Key

Beim VPN-Verbindungsaustausch laufen vereinfacht dargestellt im Main Mode folgende Vorgänge ab (in beide Richtungen symmetrisch):

- ① In einem ersten Paketaustausch handeln die Peers z.B. die verwendeten Verschlüsselungsmethoden und die Verfahren zur Authentifizierung aus. In dieser Phase haben beide Seiten noch keine gesicherte Kenntnis darüber, mit wem sie gerade verhandeln, das ist jedoch bis zu diesem Zeitpunkt nicht notwendig.
- ② Im nächsten Schritt wird ein gemeinsames Schlüsselmaterial für die weitere Verwendung ausgehandelt, darin u.a. symmetrische Schlüssel und asymmetrische Schlüsselpaare. Auch in diesem Zustand können beide Seiten noch nicht sicher sein, mit wem sie die Schlüssel ausgehandelt haben.
- ③ Im nächsten Schritt wird mit Hilfe der Zertifikate geprüft, ob der Peer aus der Verhandlung des Schlüsselmaterials auch tatsächlich der beabsichtigte Kommunikationspartner ist:

▷ Einsatz von digitalen Zertifikaten

- ▷ Die Filiale errechnet aus dem Schlüsselmaterial der aktuellen Verhandlung eine Prüfsumme (Hash), die lediglich die beiden beteiligten Peers (Filiale und Zentrale) und nur während dieser Verbindung berechnen können.
- ▷ Diesen Hash verschlüsselt die Filiale mit dem eigenen Private Key und erzeugt damit eine Signatur.
- ▷ Diese Signatur übermittelt die Filiale zusammen mit dem eigenen Zertifikat dem Peer in der Zentrale.
- ▷ Die Zentrale prüft dann die Signatur für das empfangene Zertifikat der Filiale. Das kann sie mit Hilfe des Public Keys im Root-CA, welcher in beiden Peers identisch vorhanden ist. Kann die Signatur aus dem Filialen-Zertifikat (erstellt mit dem Private Key der CA) mit dem Public Key der CA entschlüsselt werden, dann ist die Signatur gültig und dem Zertifikat kann vertraut werden.
- ▷ Im nächsten Schritt prüft die Zentrale dann die Signatur der verschlüsselten Prüfsumme. Der Public Key der Filiale aus dem entsprechenden Zertifikat wurde im vorigen Schritt für gültig befunden. Daher kann die Zentrale prüfen, ob die signierte Prüfsumme mit dem Public Key der Filiale entschlüsselt werden kann. Die Zentrale kann die gleiche Prüfsumme aus dem Schlüsselmaterial der aktuellen Verbindung berechnen wie die Filiale. Wenn diese Prüfung erfolgreich ist, kann der Peer „Filiale“ als authentifiziert angesehen werden.

10.6.6 Zertifikate von Zertifikatsdiensteanbietern

Die von öffentlichen Zertifikatsstellen angebotenen Zertifikate können in der Regel in verschiedenen Sicherheitsklassen beantragt werden. Mit höherer Sicherheit steigt dabei jeweils der Aufwand des Antragstellers, sich gegenüber der CA mit seiner Identität zu authentifizieren. Die Trustcenter AG in Hamburg verwendet z.B. die folgenden Klassen:

- ▶ Class 0: Diese Zertifikate werden ohne Prüfung der Identität ausgestellt und dienen nur zu Testzwecken für Geschäftskunden.
- ▶ Class 1: Hier wird nur die Existenz einer E-Mail-Adresse geprüft. Diese Stufe eignet sich für private Anwender, die z.B. Ihre E-Mails signieren möchten.
- ▶ Class 2: Auch in dieser Stufe findet keine persönliche Identitätsprüfung statt. Die Übersendung eines Antrags mit einer Kopie z.B. eines Handelsregisterauszugs ist ausreichend. Diese Stufe eignet sich daher für die Kommunikation zwischen Unternehmen, die vorher untereinander bekannt sind.
- ▶ Class 3: In dieser Stufe wird die Person oder das Unternehmen persönlich überprüft. Dabei werden die Angaben in dem ausgestellten Zertifikat mit denen im Pass bzw. einer beglaubigten Kopie des Handelsregisterauszugs verglichen. Diese Stufe eignet sich für fortgeschrittene Anwendungen z.B. im e-Business oder Online-Banking.

Wenn Sie mit einem öffentlichen Zertifikatsdiensteanbieter zusammenarbeiten, prüfen Sie genau die angebotenen Sicherheitsstufen bzgl. der Prüfung der Identität. Nur so können Sie feststellen, ob die verwendeten Zertifikate auch tatsächliche Ihrer Sicherheitsanforderung entsprechen.

10.6.7 Aufbau einer eigenen CA

Die Nutzung von öffentlichen CAs ist für die sichere Unternehmenskommunikation nur bedingt empfehlenswert:

- ▶ Die Ausstellung von neuen Zertifikaten ist aufwändig und manchmal nicht schnell genug.
- ▶ Die verwendeten Schlüssel werden über unzureichend gesicherte Verbindungen übertragen.

▷ Einsatz von digitalen Zertifikaten

- ▶ Die Kommunikation basiert auf dem Vertrauen gegenüber der CA.


Als Alternative eignet sich daher für die Unternehmenskommunikation der Aufbau einer eigenen CA. Hierfür bieten sich z.B. die Microsoft CA auf einem Microsoft Windows 2003 Server oder OpenSSL als OpenSource-Variante an. Mit einer eigenen CA können Sie ohne Abhängigkeit von fremden Stellen alle benötigten Zertifikate zur Sicherung des Datenaustauschs selbst erstellen und verwalten.

Der Einsatz einer eigenen CA ist für Unternehmen sicherlich eher zu empfehlen als die Nutzung öffentlicher Anbieter für Zertifizierungsdienste. Allerdings sind schon bei der Planung einer CA einige wichtige Punkte zu beachten. So werden z.B. schon bei der Installation einer Windows-CA die Gültigkeitszeiträume für die Root-CAs festgelegt, die nachträglich nicht mehr geändert werden können. Weitere Aspekte der Planung sind u.a.:

- ▶ Die Zertifikats-Policy, also die Sicherheitsstufe, die mit Hilfe der Zertifikate erreicht werden soll
- ▶ Der verwendete Namensraum
- ▶ Die Schlüssellängen
- ▶ Die Lebensdauer der Zertifikate
- ▶ Die Verwaltung von Sperrlisten

Eine genaue Planung zahlt sich auf jedem Fall aus, da spätere Korrekturen teilweise nur mit hohem Aufwand zu realisieren sind.

10.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA

 Für die Verwendung in einem LANCOM leistet eine Kombination aus PKCS#12-Datei mit Root-Zertifikat, eigenem Geräte Zertifikat und Public Key des Gerätes die besten Dienste.

- ① Rufen Sie in Ihrem Browser die Startseite des Microsoft Zertifikatsdienstes auf.
- ② Wählen Sie als Zertifikattyp die 'erweiterte Zertifikatanforderung'.
- ③ Wählen Sie im nächsten Schritt die Option 'Eine Anforderung an diese Zertifikatsstelle erstellen und einreichen'.

 Nur wenn das Root-Zertifikat schon in einer separaten Datei vorliegt, wählen Sie hier die Option 'BASE64'.

▷ Einsatz von digitalen Zertifikaten

- ④ Im nächsten Schritt werden die Daten zur Identifikation eingetragen.

Microsoft Zertifikatsdienste - Microsoft Internet Explorer

Adresse http://10.1.207.135/certsrv/certreqna.asp

Microsoft Zertifikatsdienste -- Test CA Startseite

Erweiterte Zertifikatanforderung

Identifikationsinformationen:

Name: Max Muster

E-Mail-Adresse: max.muster@firma.de

Firma: FIRMA

Abteilung: IT-Solutions

Stadt: Aachen

Bundesland/Kanton: NRW

Land/Region: DE

- ⑤ Wählen Sie im gleichen Dialog als Typ des Zertifikats die Option 'Anderer...' und löschen Sie den daraufhin erscheinenden Wert für die 'Objektkennung'.

Typ des erforderlichen Zertifikats:

Objektkennung:

- ⑥ Markieren Sie die 'Automatische Schlüsselerstellung'. Damit werden Public und Private Key für den aktuellen Benutzer automatisch von der CA erstellt.

Schlüsseloptionen:

Neuen Schlüsselsatz erstellen Bestehenden Schlüsselsatz verwenden

Kryptografiedienstanbieter: Microsoft Enhanced Cryptographic Provider v1.0

Schlüsselverwendung: Exchange Signatur Beide

Schlüsselgröße: 2048 Min.: 294 Max.: 16384 (Allgemeine Schlüsselgrößen: 512 1024 2048 4096 8192 16384)

Automatischer Schlüsselcontainername Vom Benutzer angegebener Containername

Schlüssel als "Exportierbar" markieren

Schlüssel in Datei exportieren

Verstärkte Sicherheit für den privaten Schlüssel aktivieren.

- ⑦ Wählen Sie eine geeignete Schlüssellänge (passend zur Zertifikats-Policy), aktivieren Sie die Option für exportierbare Schlüssel.



Der Schlüssel wird an dieser Stelle nicht exportiert, daher muss auch kein Dateiname angegeben werden. Beim Exportieren würde eine Datei im Microsoft-spezifischen *.pvk-Format angelegt, die für die Weiterverarbeitung in einem LANCOM ungeeignet ist.

- ⑧ Wählen Sie zuletzt als Hash-Algorithmus 'SHA-1' und reichen Sie die Zertifikatanforderung mit **Einsenden** ein.

Anforderungsformat: CMC PKCS10
Hashalgorithmus: SHA-1
Wird nur zum Signieren der Anforderung verwendet.
 Anforderung in Datei speichern
Attribute:
Anzeigename:
Einsenden

- ⑨ Den Status der eingereichten Zertifikatanforderungen können Sie jederzeit über die Startseite der Windows-CA einsehen. Sie können die Zertifikatanforderungen nur vom gleichen Rechner aus einsehen, mit dem Sie die Anforderung eingereicht haben.
- ⑩ Sobald der Administrator der CA die Zertifikatanforderung geprüft und das Zertifikat erstellt hat, können Sie dieses auf Ihrem Rechner installieren.

- ⑪ Sie können die Zertifikate nur auf dem gleichen Rechner installieren, mit dem Sie die Anforderung eingereicht haben.

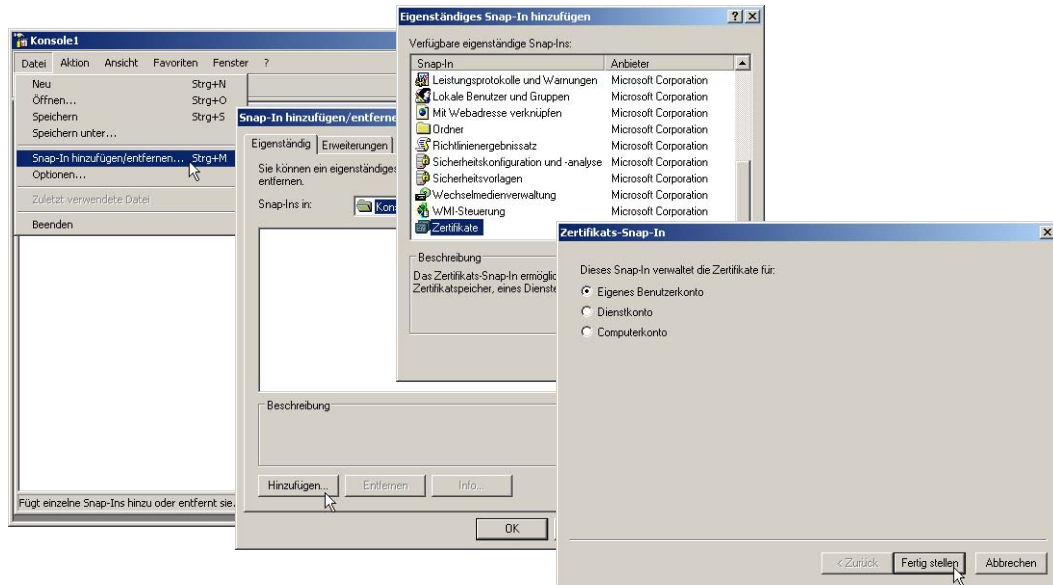
10.6.9 Zertifikat in eine PKCS#12-Datei exportieren

Mit der Installation wird das Zertifikat in Ihrem Betriebssystem gespeichert, es liegt noch nicht als separate Datei vor. Diese benötigen Sie jedoch für die Installation im LANCOM. Um zu einem Zertifikat in Dateiform zu gelangen, müssen Sie es zunächst exportieren.

▷ Einsatz von digitalen Zertifikaten

Export über den Windows- Konsolenstamm

- 1 Öffnen Sie dazu die Management-Konsole über den Befehl `mimc` an der Eingabeaufforderung und wählen Sie den Menüpunkt **Datei ▶ Snap-In hinzufügen/entfernen**.

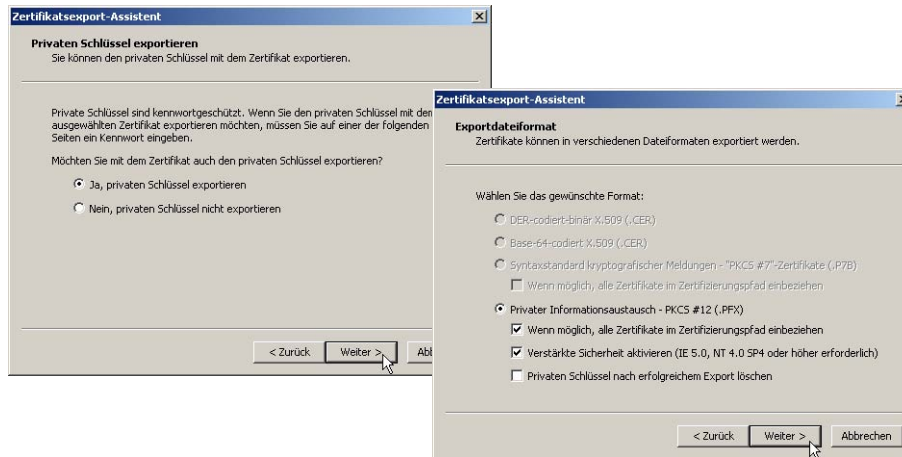


- 2 Klicken Sie auf **Hinzufügen...** und wählen Sie den Eintrag 'Zertifikate'. Bestätigen Sie mit **Hinzufügen**, markieren Sie anschließend 'Eigenes Benutzerkonto' und klicken Sie auf **Fertig stellen**.
- 3 Um das gewünschte Zertifikat in eine Datei zu exportieren, klicken Sie anschließend in der Managementkonsole in der Gruppe **Zertifikate - Aktueller Benutzer ▶ Eigene Zertifikate ▶ Zertifikate** mit der rechten Maustaste und wählen im Kontextmenü den Eintrag **Alle Tasks ▶ Exportieren**,



▷ Einsatz von digitalen Zertifikaten

- ④ Aktivieren Sie im Verlaufe des Zertifikatsexportassistenten die Option zum Exportieren des privaten Schlüssels. Optional können Sie den privaten Schlüssel nach dem Export aus dem System löschen.



- i** Die Option 'alle Zertifikate in den Zertifizierungspfad mit einbeziehen' muss aktiviert sein, damit das Root-Zertifikat mit in die PKCS#12-Datei exportiert wird.
- ⑤ Beim Export werden Sie aufgefordert, ein Kennwort zum Schutz des privaten Schlüssels einzugeben. Wählen Sie hier ein sicheres Kennwort ausreichender Länge (Passphrase). Dieses Kennwort werden Sie bei der Installation der Zertifikate im LANCOM wieder benötigen.

- i** Für das Kennwort werden je nach Umgebung auch die synonymen Begriffe „Passwort“ oder „PIN“ verwendet.

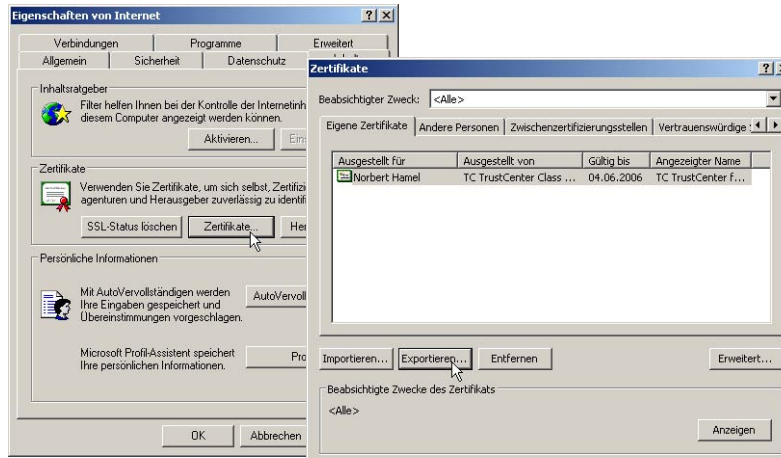
Export über die Systemsteuerung

Alternativ können Sie die auf dem System installierten Zertifikate über die Systemsteuerung öffnen.

- ① Wählen Sie dazu **Start ► Systemsteuerung ► Internetoptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.

▷ Einsatz von digitalen Zertifikaten

- ② Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf **Exportieren**.



- i** Der folgende Zertifikatsexportassistenten verhält sich genau so wie unter 'Export über den Windows-Konsolenstamm' →Seite 292 beschrieben.

10.6.10 Zertifikate mit OpenSSL erstellen

Mit OpenSSL steht eine weitere Möglichkeit zur Verfügung, eigene Zertifikate zu erstellen und Zertifikats-Verbindungen zu testen. OpenSSL ist als OpenSource-Projekt kostenlos für Linux und Windows erhältlich, als Kommandozeilen-Tool jedoch auch weniger anwenderfreundlich als andere CA-Varianten.

- i** Die Konfigurations-Datei openssl.cnf muss dabei an Ihre spezifischen Bedürfnisse angepasst werden. Nähere Informationen dazu finden Sie in der Dokumentation zu OpenSSL.


OpenSSL installieren

- ① Laden Sie eine aktuelle OpenSSL-Version von <http://www.slproweb.com/products/Win32OpenSSL.html>.
- ② Installieren Sie das Paket und erstellen Sie im Verzeichnis `./bin/PEM/demoCA` zusätzlich die Unterverzeichnisse:
 - ▷ `/certs`
 - ▷ `/newcerts`
 - ▷ `/crl`.
- ③ Ändern Sie in der Datei `openssl.cnf` den Pfad in der Gruppe `[CA_default]` auf: `dir= ./PEM/demoCA`
- ④ Starten Sie OpenSSL durch einen Doppelklick auf die `openssl.exe` im Verzeichnis `./bin`.

Zertifikat für Root-CA ausstellen

- 1 Erstellen Sie einen Schlüssel für die CA mit dem Befehl:

▷ `genrsa -des3 -out ca.key 2048`

-
-  Merken Sie sich das Kennwort, das Sie nach der Aufforderung für den CA-Schlüssel eingeben, es wird später wieder benötigt!

Dieser Befehl erstellt die Datei 'ca.key' im aktuellen Verzeichnis.

- 2 Erstellen Sie eine Zertifikatsanforderung (Request) für die CA mit dem Befehl:


▷ `req -key ca.key -new -subj /CN="Test_CA" -out ca.req`

-
-  Hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

Dieser Befehl erstellt die Datei 'ca.req' im aktuellen Verzeichnis.

- 3 Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

▷ `x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt`

-
-  Auch hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

Dieser Befehl signiert die Zertifikatsanforderung 'ca.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'ca.crt' aus.

Zertifikat für Benutzer oder Geräte ausstellen

- 1 Erstellen Sie einen Schlüssel für das Gerät oder den Benutzer mit dem Befehl:

▷ `genrsa -out device.key 2048`

Dieser Befehl erstellt die Datei 'device.key' im aktuellen Verzeichnis.

- 2 Erstellen Sie eine Zertifikatsanforderung (Request) für das Gerät oder den Benutzer mit dem Befehl:

▷ `req -key device.key -new -subj /CN=DEVICE -out device.req`

Dieser Befehl erstellt die Datei 'device.req' im aktuellen Verzeichnis.

- 3 Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

▷ `x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt`

▷ Einsatz von digitalen Zertifikaten

Dieser Befehl signiert die Zertifikatsanforderung 'device.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'device.cert' aus. Zusätzlich wird dabei die Konfigurationsdatei openssl.cnf verwendet.

- ④ Exportieren Sie das Zertifikat für das Gerät oder den Benutzer mit dem Befehl:

```
▷ pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12
```


Dieser Befehl fasst den Schlüssel 'device.key', das Geräte-Zertifikat 'device.crt' und das Root-Zertifikat 'ca.crt' zusammen und speichert sie gemeinsam in der Datei 'device.p12'. Diese PKCS#12-Datei können Sie direkt in das gewünschte Gerät laden ('Zertifikate in das LANCOM laden' →Seite 296).

10.6.11 Zertifikate in das LANCOM laden

Für den zertifikatgesicherten VPN-Verbindungsaufbau müssen in einem LANCOM die folgenden Komponenten vorhanden sein:

- ▶ Zertifikat der Root-CA mit dem Public Key der CA
- ▶ Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
- ▶ Eigener Private Key

Sofern Sie die Anleitungen zur Ausstellung der Zertifikate über eine Windows-CA und den Export befolgt haben, liegen diese Informationen nun in Form einer gemeinsamen PKCS#12-Datei vor. Alternativ haben Sie ein anderes Verfahren verwendet und die einzelnen Komponenten liegen in separaten Dateien vor.

 Die Zertifikatsdateien können derzeit nur mit WEBconfig in die Geräte geladen werden. Verwenden Sie unbedingt eine HTTPS-Verbindung, da die Passphrase für die PKCS#12-Datei unverschlüsselt übertragen wird.

- ① Melden Sie sich mit Administratorrechten über WEBconfig an dem gewünschten Gerät an.
- ② Wählen Sie den Eintrag **Zertifikat oder Datei hochladen**.

Zertifikate oder Datei hochladen


Wählen Sie aus, welche Datei Sie hochladen wollen sowie deren Namen, dann klicken Sie auf 'Upload starten'.

Dateityp:	VPN - Root-CA-Zertifikat
Dateiname:	VPN - Root-CA-Zertifikat
Passwort (falls benötigt):	VPN - Geräte-Zertifikat
	VPN - Private-Geräte-Schlüssel
	VPN - Container als PKCS#12-Datei (Passwort erforderlich)
	Meldung von Login

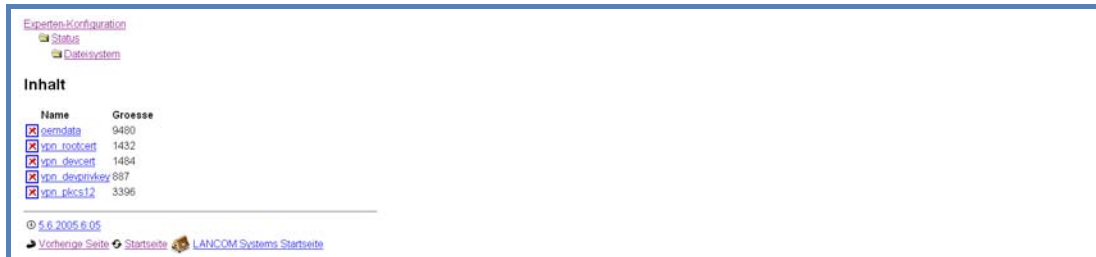
© 5.6.2005 5:54

[Vorherige Seite](#) [Startseite](#) [LANCOM Systems Startseite](#)

- ③ Wählen Sie aus, welche Komponenten Sie in das Gerät laden wollen:
 - ▷ Root-Zertifikat
 - ▷ Geräte-Zertifikat
 - ▷ Private Key des Gerätes
 - ▷ PKCS#12-Datei mit einer Kombination aus Root-Zertifikat, Geräte-Zertifikat und Private Key


 Je nach Typ der hochgeladenen Datei muss ggf. das entsprechende Kennwort eingegeben werden.

Die hochgeladenen Dateien können anschließend in einer Liste unter **Expertenkonfiguration ▶ Status ▶ Dateisystem ▶ Inhalt** eingesehen werden.




 Eine kombinierte PKCS#12-Datei wird beim Upload automatisch in die benötigten Teile zerlegt.


10.6.12 VPN-Verbindungen auf Zertifikatsunterstützung einstellen

 VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das LANCOM über die korrekte Uhrzeit verfügt. Wenn das Gerät keine aktuelle Uhrzeit hat, kann die Gültigkeit der Zertifikate nicht richtig beurteilt werden, die Zertifikate werden dann abgelehnt und es kommt keine Verbindung zustande.

Um VPN-Verbindungen auf die Unterstützung von Zertifikaten einzustellen, müssen verschiedene Teile der Konfiguration entsprechend vorbereitet werden:

- ▶ IKE-Proposals
- ▶ IKE-Proposal-Listen
- ▶ IKE-Schlüssel
- ▶ VPN-Parameter
- ▶ Verbindungs-Parameter

 Je nach Firmwarestand sind die benötigten Werte teilweise schon in Ihrem Gerät vorhanden. Prüfen Sie in diesem Fall nur die Werte auf richtige Einstellung.

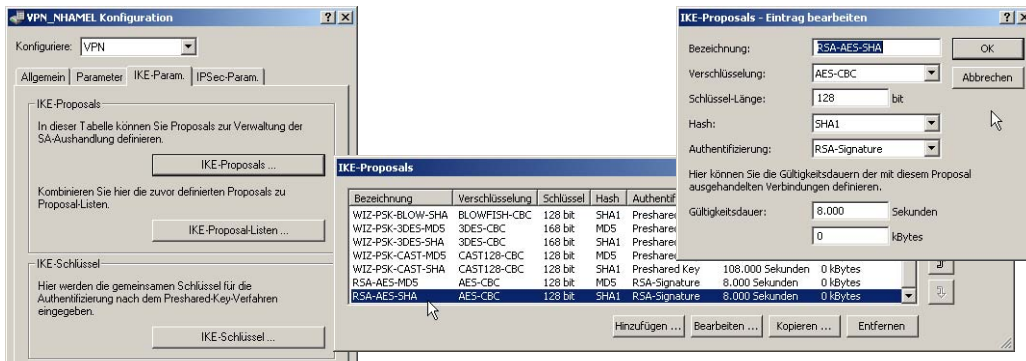
 Wenn Sie ein entferntes Gerät auf die nachfolgende beschriebene Weise auf Zertifikatsunterstützung umstellen wollen, das nur über einen VPN-Tunnel erreichbar ist, müssen Sie auf jeden Fall zuerst das entfernte Gerät umstellen, bevor Sie die Verbindung des lokalen Geräts ändern. Durch die Änderung der lokalen Konfiguration ist das entfernte Gerät ansonsten nicht mehr erreichbar!

▷ Einsatz von digitalen Zertifikaten

- ① In den Listen der Proposals werden zwei neue Proposals mit den exakten Bezeichnung 'RSA-AES-MD5' und 'RSA-AES-SHA' benötigt, die beide als Verschlüsselung 'AES-CBC' und als Authentifizierungsmodus 'RSA-Signature' verwenden und sich nur im Hash-Verfahren (MD5 bzw. SHA1) unterscheiden.

Konfiguration mit LANconfig

Die IKE-Proposals finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'IKE-Param.' mit einem Klick auf die Schaltfläche **IKE-Proposals**:



Konfiguration mit WEBconfig oder Telnet

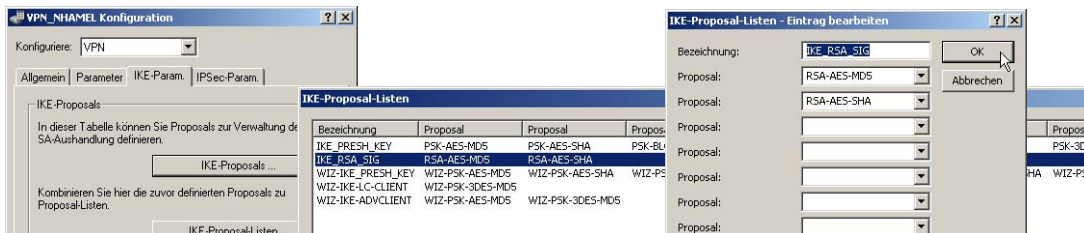
Unter WEBconfig oder Telnet finden Sie die IKE-Proposals an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ▶ Setup ▶ VPN ▶ Proposals ▶ IKE
Terminal/Telnet	/Setup/VPN/Proposals/IKE

- ② In den Proposal-Listen wird eine neue Liste benötigt mit den exakten Bezeichnung 'IKE_RSA_SIG', in der die beiden neuen Proposals 'RSA-AES-MD5' und 'RSA-AES-SHA' aufgeführt sind.

Konfiguration mit LANconfig

Die VPN-Proposal-Listen finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'IKE-Param.' mit einem Klick auf die Schaltfläche **IKE-Proposallisten**:



Konfiguration
mit WEBconfig
oder Telnet

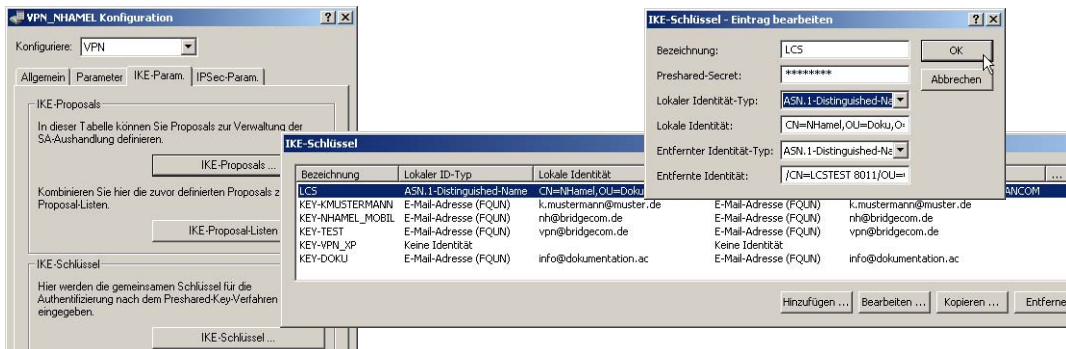
Unter WEBconfig oder Telnet finden Sie die IKE-Proposal-Listen an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► VPN ► Proposals ► IKE-Proposal-Listen
Terminal/Telnet	/Setup/VPN/Proposals/IKE-Proposal-Listen

- ③ In der Liste der IKE-Schlüssel müssen für alle Zertifikats-Verbindungen die entsprechenden Identitäten eingestellt werden.

Konfiguration
mit LANconfig

Die IKE-Schlüssel finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'IKE-Param.' mit einem Klick auf die Schaltfläche **IKE-Schlüssel**:



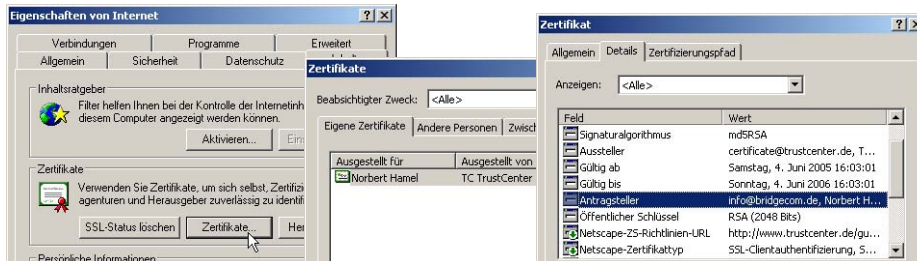
- ▷ Der Preshared Key kann ggf. gelöscht werden, wenn er endgültig nicht mehr benötigt wird.
- ▷ Der Typ der Identitäten wird auf ASN.1 Distinguished Names umgestellt (lokal und remote).
- ▷ Die Identitäten werden exakt so eingetragen wie in den Zertifikaten. Die einzelnen Werte z.B. für 'CN', 'O' oder 'OU' können durch Kommata oder Slashes getrennt werden.

Es müssen alle in den Zertifikaten eingetragenen Werte aufgeführt werden, in der gleichen Reihenfolge. Prüfen Sie ggf. über die Systemsteuerung den Inhalt der Zertifikate. Wählen Sie dazu **Start ► Systemsteuerung ► Internetooptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.

Öffnen Sie das gewünschte Zertifikat und wählen Sie auf der Registerkarte 'Details' den entsprechenden Wert aus. Für den Antragsteller finden Sie hier z.B. die benötigten ASN.1 Distinguished Names mit den zuge-

▷ Einsatz von digitalen Zertifikaten

hörigen Kurzzeichen. Die in den Zertifikaten von oben nach unten aufgeführten Werte müssen in den IKE-Schlüssel von links nach rechts eingetragen werden. Beachten Sie auch die Groß- und Kleinschreibung!



i Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Familienname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

i Sonderzeichen in den ASN.1 Distinguished Names können durch die Angabe der ASCII-Codes in Hexadezimaldarstellung mit einem vorangestellten Backslash eingetragen werden. „\61“ entspricht z.B. einem kleinen „a“.

Konfiguration mit WEBconfig oder Telnet

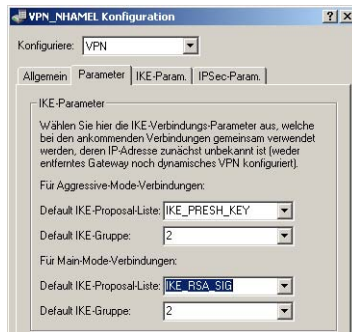
Unter WEBconfig oder Telnet finden Sie die IKE-Schlüssel an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► VPN ► Zertifikate-Schlüssel ► IKE-Keys
Terminal/Telnet	/Setup/VPN/Zertifikate-Schlüssel/IKE-Keys

4 In den IKE-Verbindungs-Parametern müssen die Default-IKE-Proposal-Listen für eingehende Aggressive-Mode- und Main-Mode-Verbindungen auf die Proposal-Liste 'IKE_RSA_SIG' eingestellt sein. Beachten Sie außerdem die Einstellung der Default-IKE-Gruppe, die im nächsten Schritt ggf. angepasst werden muss.

Konfiguration mit LANconfig

Die Default-IKE-Proposal-Listen und Default-IKE-Gruppen finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Parameter':



Konfiguration
mit WEBconfig
oder Telnnet

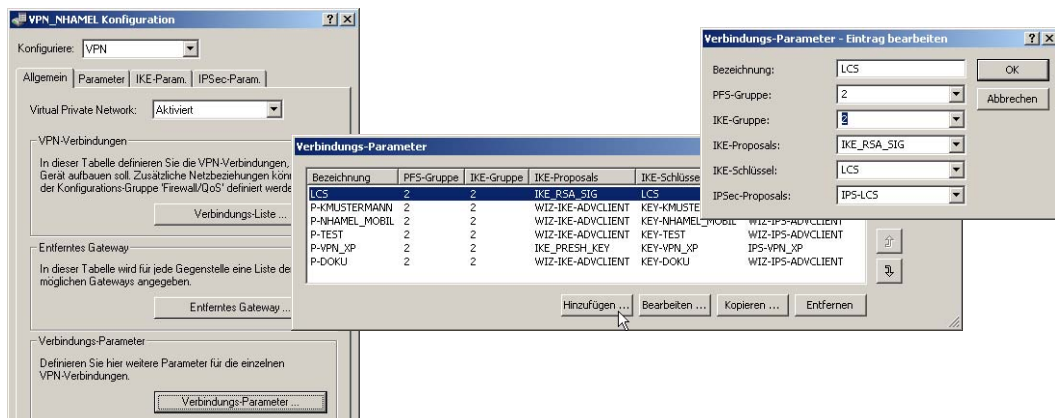
Unter WEBconfig oder Telnnet finden Sie die Default-IKE-Proposal-Listen und Default-IKE-Gruppen an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► VPN
Terminal/Telnnet	/Setup/VPN

- ⑤ In den VPN-Verbindungs-Parametern müssen zum Schluss die VPN-Verbindungen auf die Verwendung der richtigen IKE-Proposals eingestellt werden ('IKE_RSA_SIG'). Dabei müssen die Werte für 'PFS-Gruppe' und 'IKE-Gruppe' mit den in den IKE-Verbindungs-Parametern eingestellten Werten übereinstimmen.

Konfiguration
mit LANconfig

Die VPN-Verbindungs-Parameter finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' mit einem Klick auf die Schaltfläche **Verbindungs-Parameter**:



▷ Einsatz von digitalen Zertifikaten


Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die VPN-Verbindungs-Parameter an folgenden Stellen:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► VPN ► VPN-Layer
Terminal/Telnet	/Setup/VPN/VPN-Layer

10.6.13 Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen


Mit dem Setup-Assistenten von LANconfig können Sie schnell und bequem zertifikatsbasierte LAN-Kopplungen oder RAS-Zugänge über VPN einrichten.

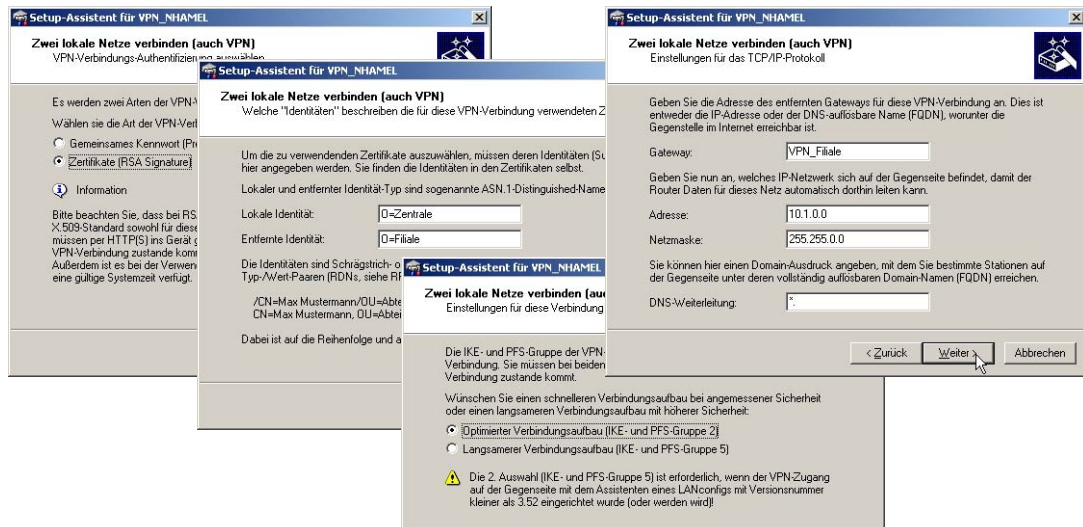
 VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das LANCOM über die korrekte Uhrzeit verfügt und die entsprechenden Zertifikate in das Gerät geladen wurden ('Zertifikate in das LANCOM laden' →Seite 296).

LAN-Kopplungen

- ① Wählen Sie den Assistenten zum Verbinden von Netzwerken über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature).
- ② Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.

 Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielsweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Familienname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

 Der Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem LANCOM, u.a. dabei die eingetragenen Distinguished Names (DN) unter „Subject“. Die Distinguished Names werden in dieser Darstellung in umgekehrter Reihenfolge angezeigt!



- ③ Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit IKE- und PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 für IKE und PFS, wenn dies von der Gegenstelle verlangt wird. Dies ist z.B. dann der Fall, wenn die VPN-Gegenstelle mit LANconfig 3.52 oder kleiner konfiguriert wird.
- ④ Tragen Sie den Namen der VPN-Gegenstelle, die IP-Adresse und die Netzmaske des entfernten Netzes sowie die ggf. verwendeten Domain für die DNS-Weiterleitung ein. Aktivieren Sie je nach Bedarf die „Extranet“-Funktion und das „NetBIOS-Routing“.

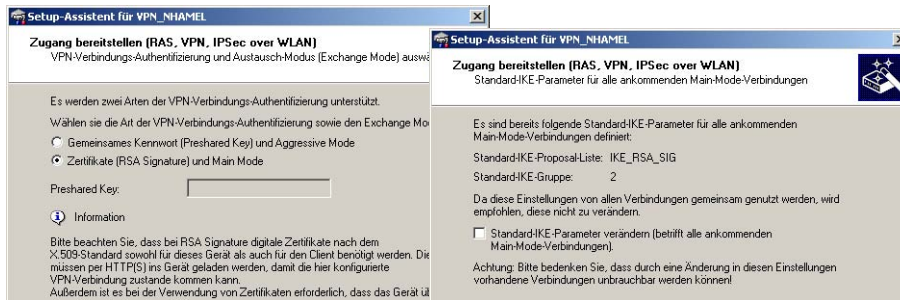
RAS-Zugänge

RAS-Zugänge mit Zertifikatsunterstützung können für den LANCOM Advanced VPN Client oder für einen anderen VPN-Client mit benutzerdefinierten Parametern eingerichtet werden. Der LANCOM Standard VPN Client bietet keine Unterstützung für Zertifikate an.

i Die abgefragten Parameter unterscheiden sich je nach Auswahl des Clients bzw. der Optionen während der Dialoge. Diese Beschreibung zeigt vollständig alle evtl. auftretenden Dialoge des Assistenten, von denen nicht alle für Ihre Anwendung relevant sein müssen.

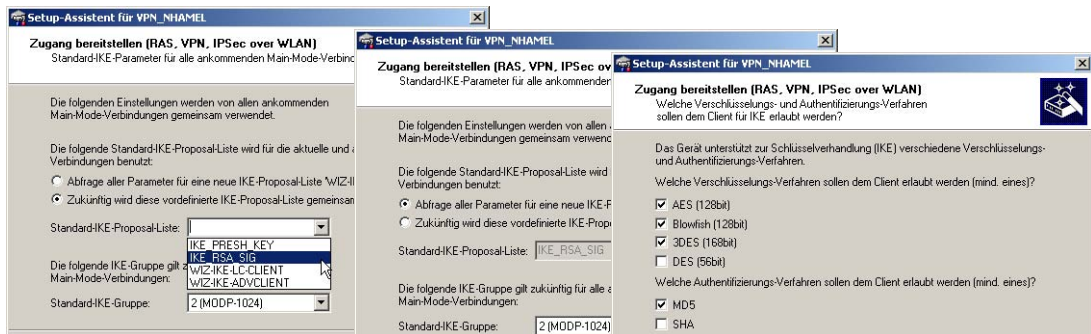
- ① Wählen Sie den Assistenten zum Bereitstellen von Zugängen über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature). Als „Exchange Mode“ wird dabei automatisch der Main Mode verwendet.

► Einsatz von digitalen Zertifikaten

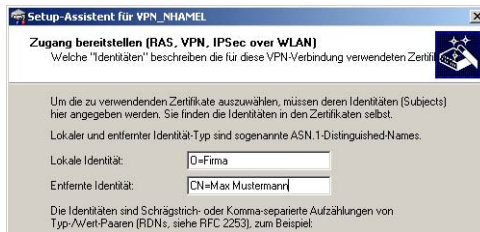


Nur bei benutzerdefiniertem VPN-Client

- ② In der Konfiguration sind üblicherweise bereits Standard-IKE-Parameter für ankommende Main-Mode-Verbindungen in der Standard-IKE-Proposal-Liste 'IKE_RSA_SIG' definiert. Verwenden Sie nach Möglichkeit diese Liste mit den vorbereiteten IKE-Parametern.
- ③ Wenn Sie gezielt andere Parameter für die ankommenden Main-Mode-Verbindungen nutzen möchten, können Sie die Standard-IKE-Parameter an Ihre Bedürfnisse anpassen. Sie können entweder über die Abfrage der benötigten Parameter eine neue Liste 'WIZ-IKE-MAIN-MODE' erstellen oder eine der vorhandenen IKE-Proposal-Listen als neue „Standard-IKE-Proposal-Liste“ auswählen. Die hier definierte Liste wird in Zukunft von allen ankommenden Main-Mode-Verbindungen verwendet. Für eine neue IKE-Proposal-Liste können Sie auswählen, welche Verschlüsselungsverfahren und Authentifizierungsverfahren der Client während der IKE-Verhandlung verwenden kann.



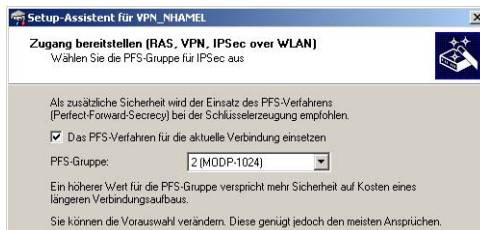
- ④ Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.



i Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielsweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Familienname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

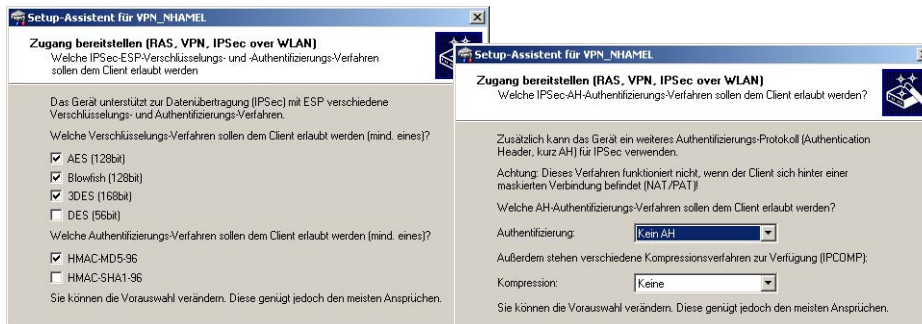
i Der Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem LANCOM, u.a. dabei die eingetragenen Distinguished Names (DN) unter „Subject“. Die Distinguished Names werden in dieser Darstellung in umgekehrter Reihenfolge angezeigt!

5 Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 als PFS-Gruppe, wenn dies vom Client verlangt wird.



6 Für die Übertragung der Nutzdaten mit IPsec können in den folgenden Dialogen die Verschlüsselungs- und Authentifizierungsverfahren sowie die „Authentication Header“ und die Datenkompression festgelegt werden, die der Client verwenden kann. Verwenden Sie nach Möglichkeit die voreingestellten Werte, sofern der Client keine anderen Einstellungen erwartet.

▷ Einsatz von digitalen Zertifikaten



- ⑦ Tragen Sie die IP-Adresse für den Client und den für den Zugriff erlaubten Adress-Bereich im lokalen Netzwerk ein. Aktivieren Sie je nach Bedarf das „NetBIOS-Routing“.

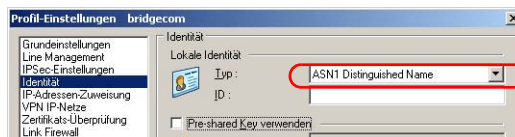
10.6.14 LANCOM Advanced VPN Client auf Zertifikatsverbindungen einstellen

Bei der Einwahl mit dem LANCOM Advanced VPN Client in einen LANCOM-Router müssen die entsprechenden Profil-Einstellungen an die Verwendung von Zertifikaten angepasst werden.

- ① Stellen Sie in den IPSec-Einstellungen des Profils die IKE-Richtlinie auf 'RSA-Signatur' um.

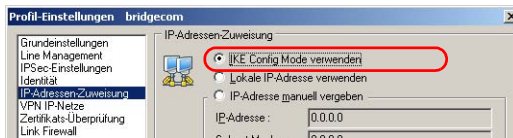


- ② Stellen Sie die Identität auf 'ASN1 Distinguished Names' um. Die 'Identität' kann frei bleiben, da diese Information aus dem Zertifikat ausgelesen wird.



- ③ Verwenden Sie bei der IP-Adress-Zuweisung den 'IKE Config Mode'.

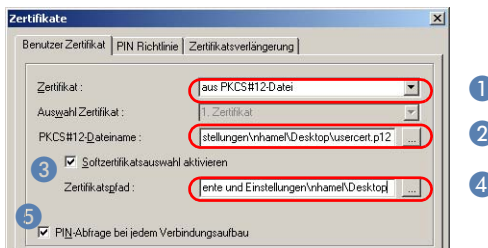
▷ Einsatz von digitalen Zertifikaten



- ④ Bei der Zertifikatsüberprüfung können Sie optional die Zertifikate einschränken, die der LANCOM Advanced VPN Client akzeptiert. Dazu geben Sie den Benutzer und/oder den Aussteller des eingehenden Zertifikats und ggf. den zugehörigen „Fingerprint“ an.



- ⑤ Nachdem Sie das geänderte Verbindungsprofil gespeichert haben, öffnen Sie über den Menüpunkt **Konfiguration** ► **Zertifikate** die Einstellungen für die Benutzerzertifikate.

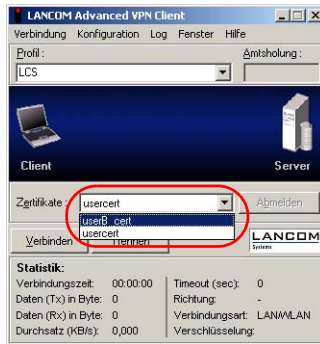


- ▷ Wählen Sie als Zertifikatetyp die 'PKCS#12-Datei' aus ① und geben Sie die gewünschte Zertifikatsdatei an ②.
- ▷ Wenn Sie mit verschiedenen Zertifikaten arbeiten möchten, aktivieren Sie die Option 'Softzertifikatsauswahl' ③ und geben den Pfad zum Ordner an, in dem die Zertifikatsdateien abgelegt sind ④.
- ▷ Wählen Sie aus, ob die PIN (das Kennwort) für das Zertifikat bei jedem Verbindungsaufbau abgefragt werden soll ⑤. Alternativ können Sie die PIN über den Menüpunkt **Verbindung** ► **PIN eingeben** fest im LANCOM Advanced VPN Client speichern.



▷ Konkrete Verbindungsbeispiele

- ▶ Bei aktivierter Softzertifikatsauswahl können Sie beim Verbindungsaufbau im Hauptfenster des LANCOM Advanced VPN Client jeweils das gewünschte Zertifikat aus der Liste auswählen, passend zum gewählten Profil.



10.6.15 Diagnose der VPN-Zertifikatsverbindungen

Die folgenden Befehle an der LANCOM-Konsole können hilfreiche Aufschlüsse geben, sollte der VPN-Verbindungsaufbau nicht wie gewünscht funktionieren:

- ▶ `trace + vpn-status`
Zeigt einen Trace der aktuellen VPN-Verbindungen.
- ▶ `show vpn long`
Zeigt die Inhalte der VPN-Konfiguration, u.a. dabei die eingetragenen Distinguished Names (DN).
- ▶ `show vpn ca`
Zeigt den Inhalt des Root-Zertifikats.
- ▶ `show vpn cert`
Zeigt den Inhalt des eigenen Geräte-Zertifikats.



Die Distinguished Names werden in dieser Darstellung in umgekehrter Reihenfolge angezeigt!

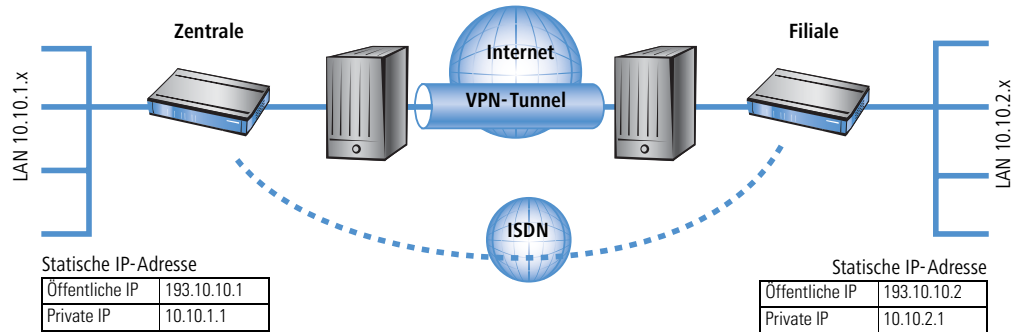
10.7 Konkrete Verbindungsbeispiele

In diesem Kapitel werden die vier möglichen VPN-Verbindungstypen an Hand konkreter Beispiele veranschaulicht. Die vier Verbindungsarten werden nach der IP-Adressart der beiden VPN-Gateways kategorisiert:

- ▶ statisch/statisch
- ▶ dynamisch/statisch (die dynamische Seite initiiert die Verbindung)
- ▶ statisch/dynamisch (die statische Seite initiiert die Verbindung)

► dynamisch/dynamisch

Zu jeder dieser vier VPN-Verbindungsarten gibt es einen eigenen Abschnitt mit einer Aufführung aller notwendigen Konfigurationsangaben in Form der bereits bekannten Tabelle.

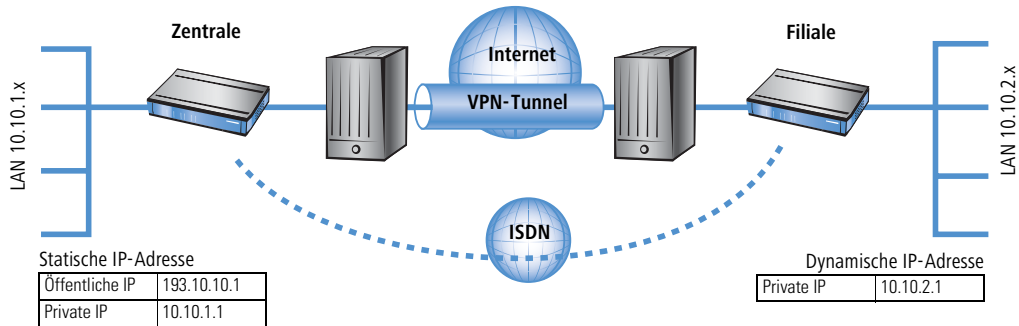
10.7.1 Statisch/statisch

Zwischen den beiden LANCOM **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Gateways verfügen über statische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

Angabe	Zentrale	Filiale
Typ der eigenen IP-Adresse	statisch	statisch
Typ IP-Adresse der Gegenstelle	statisch	statisch
Name des eigenen Gerätes	Zentrale	Filiale
Name der Gegenstelle	Filiale	Zentrale
Shared Secret für Verschlüsselung	geheim	geheim
IP-Adresse der Gegenseite	193.10.10.2	193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0	10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0	255.255.255.0


▷ Konkrete Verbindungsbeispiele

10.7.2 Dynamisch/statisch



Das VPN-Gateway **Filiale** baut eine VPN-Verbindung zum Gateway **Zentrale** auf. **Filiale** verfügt über eine dynamische IP-Adresse (die ihm bei der Internet-Einwahl von seinem Internet-Anbieter zugewiesen wurde), **Zentrale** hingegen über eine statische. Während des Verbindungsaufbaus überträgt **Filiale** seine aktuelle IP-Adresse an **Zentrale** (standardmäßig über ICMP, alternativ auch über UDP Port 87).

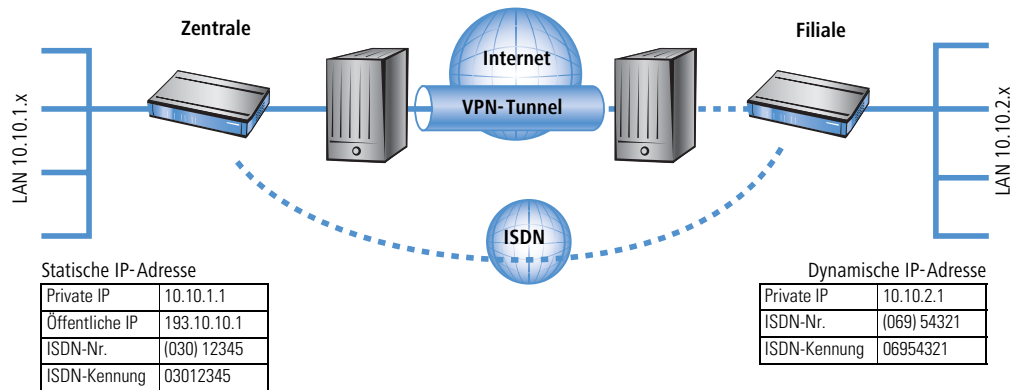
Angabe	Zentrale	Filiale
Typ der eigenen IP-Adresse	statisch	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch	statisch
Name des eigenen Gerätes	Zentrale	Filiale
Name der Gegenstelle	Filiale	Zentrale
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	vertraulich
Shared Secret für Verschlüsselung	geheim	geheim
IP-Adresse der Gegenseite	–	193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0	10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0	255.255.255.0

 Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

10.7.3 Statisch/dynamisch (mit LANCOM Dynamic VPN)

In diesem Fall initiiert (im Gegensatz zur dynamisch/statischen Verbindung) die statische Seite den Aufbau der VPN-Verbindung.

▷ Konkrete Verbindungsbeispiele



Das VPN-Gateway **Zentrale** baut eine VPN-Verbindung zu **Filiale** auf. **Zentrale** verfügt über eine statische IP-Adresse, **Filiale** über eine dynamische.



Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.




Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird als Pendant zur statischen IP-Adresse in der Zentrale auf der Seite der Filiale ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dynamischen IP-Adresse erlaubt. Weitere Informationen dazu finden Sie unter 'Dynamische IP-Adressen und DynDNS' → Seite 259.

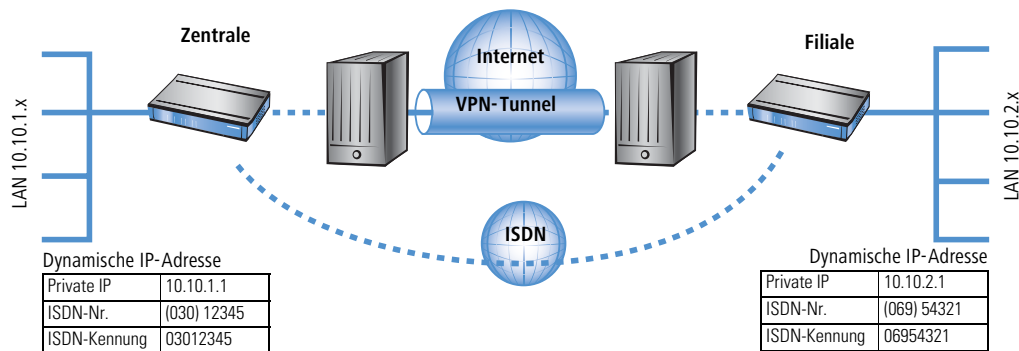
Angabe	Zentrale	Filiale
Typ der eigenen IP-Adresse	statisch	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch	statisch
Name des eigenen Gerätes	Zentrale	Filiale
Name der Gegenstelle	Filiale	Zentrale
ISDN-Rufnummer Gegenstelle	06954321	03012345
ISDN-Anruferkennung Gegenstelle	06954321	03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	vertraulich
Shared Secret für Verschlüsselung	geheim	geheim

▷ Konkrete Verbindungsbeispiele


Angabe	Zentrale	Filiale
IP-Adresse der Gegenseite		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0	10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0	255.255.255.0

 Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

10.7.4 Dynamisch/dynamisch (mit LANCOM Dynamic VPN)







Zwischen den beiden LANCOM **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Seiten haben dynamische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

 Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

 Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird an Stelle einer statischen IP-Adresse ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dyna-

▷ Konkrete Verbindungsbeispiele

mischen IP-Adresse erlaubt. Weitere Informationen dazu finden Sie unter 'Dynamische IP-Adressen und DynDNS' →Seite 259.

Angabe	Zentrale		Filiale
Typ der eigenen IP-Adresse	dynamisch		dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		dynamisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich		vertraulich
Shared Secret für Verschlüsselung	geheim		geheim
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0



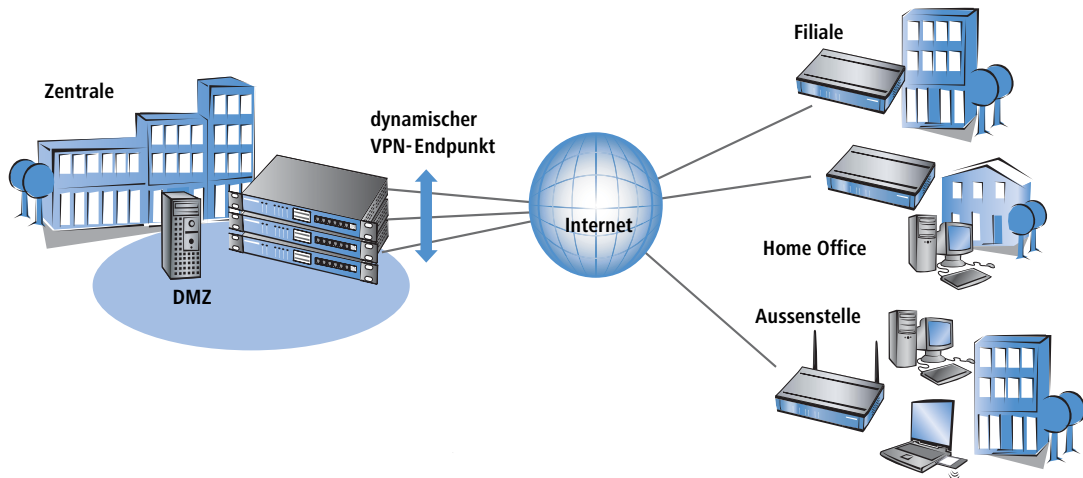
Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

10.7.5 VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“

Mehrere VPN-Gateway-Adressen

In verteilten Unternehmensstrukturen, die auf Vernetzung der Standorte über VPN setzen, kommt der Verfügbarkeit der zentralen VPN-Gateways eine besondere Bedeutung zu. Nur wenn diese zentralen Einwahlknoten einwandfrei funktionieren, kann die betriebliche Kommunikation reibungslos ablaufen.

▷ Konkrete Verbindungsbeispiele



Mit der Möglichkeit, mehrere „Remote-Gateway“-Adressen als „dynamischer VPN-Endpunkt“ für eine VPN-Verbindung zu konfigurieren, bieten LANCOM VPN-Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN-Konfiguration eingesetzt. In den Außenstellen werden alle vorhandenen Gateways als mögliche Gegenstellen für die gewünschte VPN-Verbindung eingetragen. Falls eines der Gateways nicht erreichbar ist, weicht der entfernte Router automatisch auf eine der anderen Gegenstellen aus.

Damit die Rechner im LAN der Zentrale auch wissen, welche Aussenstelle gerade über welches VPN-Gateway erreicht werden kann, werden die jeweils aktuellen Outband-Routen zu den verbundenen Gegenstellen über RIPv2 im Netzwerk der Zentrale propagiert.




Wenn die Außenstellen so konfiguriert werden, dass sie beim Aufbau der VPN-Verbindung die Gegenstelle zufällig auswählen, wird mit diesem Mechanismus die Hochverfügbarkeit mit gleichmäßiger Lastverteilung zwischen den VPN-Gateways in der Zentrale realisiert („Load Balancing“).

Konfiguration

Bei der Konfiguration tragen Sie in der Liste der „Remote Gateways“ zusätzliche Ziele für eine VPN-Verbindung ein. Die Liste besteht aus den folgenden Einträgen:

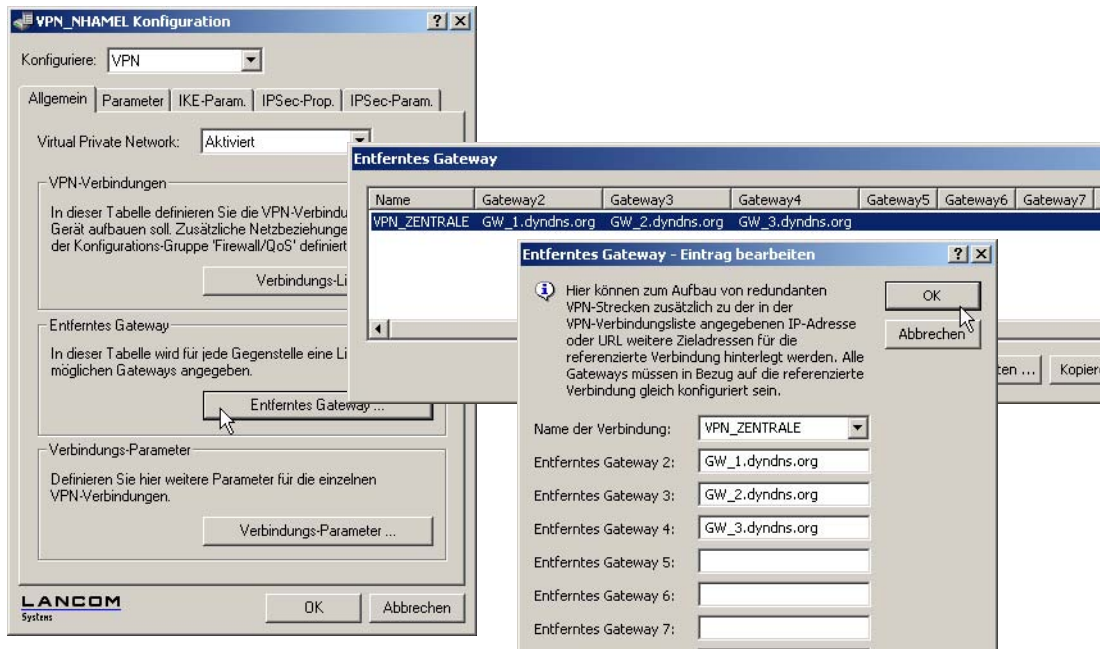
- ▶ Name: Name der Gegenstelle aus der VPN-Verbindungsliste, das „Ziel“ der VPN-Verbindung.
- ▶ Gateway 2 bis Gateway 9: Adresse der alternativen Gateways, als IP-Adresse oder auflösbarer DNS-Name.
- ▶ Anfang: In welcher Reihenfolge sollen die Einträge versucht werden. Zur Auswahl stehen:
 - ▷ Zuletzt benutzer: Wählt den Eintrag, zu dem zuletzt erfolgreich eine VPN-Verbindung hergestellt werden konnte.
 - ▷ Erster: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.

- ▷ Zufall: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

 Der Eintrag für das Gateway in der VPN-Verbindungsliste kann frei bleiben, wenn alle möglichen Gateways in der Liste der „Remote Gateways“ eingetragen sind.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Liste der Gateway-Adressen im Konfigurationsbereich 'VPN' auf die Registerkarte 'Allgemein' unter der Schaltfläche **Entferntes Gateway**.



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Einstellungen für die Remote-Gateway-Adressen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Config ► Remote-Gateway-Liste
Terminal/Telnet	Setup/VPN/Remote-Gateway-Liste

Zur Definition der Strategie, nach der die konfigurierten Remote-Gateway-Adressen verwendet werden, stehen folgende Möglichkeiten zur Verfügung:

- zuletzt-verwendetem

▷ *Wie funktioniert VPN?*

- ▶ erstem
- ▶ zufaellichem

Beispiel:

Mit dem folgenden Befehl legen Sie drei Gateways als Ziel in der Zentrale fest, die zufällig ausgewählt werden:
 set VPN_ZENTRALE 213.217.69.75 213.217.69.76 213.217.69.77 * * * * * zufaellichem

10.8 Wie funktioniert VPN?

Ein VPN muss in der Praxis einer Reihe von Ansprüchen gerecht werden:

- ▶ Unbefugte Dritte dürfen die Daten nicht lesen können (Verschlüsselung)
- ▶ Ausschluss von Datenmanipulationen (Datenintegrität)
- ▶ Zweifelsfreie Feststellung des Absenders der Daten (Authentizität)
- ▶ Einfache Handhabung der Schlüssel
- ▶ Kompatibilität mit VPN-Geräten verschiedener Hersteller

Diese fünf wichtigen Ziele erreicht LANCOM VPN durch die Verwendung des weitverbreiteten IPSec-Standards.

10.8.1 IPSec – Die Basis für LANCOM VPN

Das ursprüngliche IP-Protokoll enthält keinerlei Sicherheitsvorkehrungen. Erschwerend kommt hinzu, dass Pakete unter IP nicht gezielt an den Empfänger gesendet werden, sondern über das gesamte Netzwerksegment an alle angeschlossenen Rechner gestreut werden. Wer auch immer möchte, bedient sich und liest die Pakete mit. Datenmissbrauch ist so möglich.

Deshalb wurde IP weiterentwickelt und es gibt IP inzwischen auch in einer sicheren Variante: IPSec. LANCOM VPN basiert auf IPSec.

IPSec steht für „**IP Security Protocol**“ und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der **Internet Engineering Task Force**. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

Wichtig ist, dass IPSec selber kein Protokoll ist, sondern nur der Standard für ein Protokoll-Rahmenwerk. IPSec besteht in der Tat aus verschiedensten Protokollen und Algorithmen für die Verschlüsselung, die Authentifizierung und das Schlüssel-Management. Diese Standards werden in den folgenden Abschnitten vorgestellt.

Sicherheit im IP-Gewand

IPSec ist (nahezu) vollständig innerhalb in Ebene 3 des OSI-Modells implementiert, also in der Vermittlungsebene (dem Network Layer). Auf Ebene 3 wird in IP-Netzwerken der Verkehr der Datenpakete auf Basis des IP-Protokolls abgewickelt.

Damit ersetzt IPSec das IP-Protokoll. Die Pakete werden unter IPSec intern anders aufgebaut als IP-Pakete. Ihr äußerer Aufbau bleibt dabei aber vollständig kompatibel zu IP. IPSec-Pakete werden deshalb weitgehend problemlos

▷ *Wie funktioniert VPN?*

innerhalb bestehender IP-Netze transportiert. Die für den Transport der Pakete zuständigen Geräte im Netzwerk können IPSec-Pakete bei Blick aufs Äußere nicht von IP-Paketen unterscheiden.

Ausnahmen sind bestimmte Firewalls und Proxy-Server, die auch auf den Inhalt der Pakete zugreifen. Die Probleme resultieren dabei aus (teilweise funktionsbedingten) Inkompatibilitäten dieser Geräte mit dem geltenden IP-Standard. Diese Geräte müssen entsprechend an IPSec angepasst werden.

In der nächsten Generation des IP-Standards (IPv6) wird IPSec fest implementiert werden. Man kann deshalb davon ausgehen, dass IPSec auch in Zukunft der wichtigste Standard für virtuelle private Netzwerke sein wird.

10.8.2 Alternativen zu IPSec

IPSec ist ein offener Standard. Er ist unabhängig von einzelnen Herstellern und wird innerhalb der IETF unter Einbezug der interessierten Öffentlichkeit entwickelt. Die IETF steht jedermann offen und verfolgt keine wirtschaftliche Interessen. Aus dieser offenen Gestaltung zur Zusammenführung verschiedener technischer Ansätze resultiert die breite Anerkennung von IPSec.

Dennoch gab und gibt es andere Ansätze zur Verwirklichung von VPNs. Nur die beiden wichtigsten seien hier erwähnt. Sie setzen nicht auf der Netzwerkebene wie IPSec an, sondern auf Verbindungsebene und auf Anwendungsebene.

Sicherheit auf Verbindungsebene – PPTP, L2F, L2TP

Bereits auf der Verbindungsebene (Level 2 des OSI-Modells) können Tunnel gebildet werden. Microsoft und Ascend entwickelten frühzeitig das **Point-to-Point Tunneling Protocol (PPTP)**. Cisco stellte ein ähnliches Protokoll mit **Layer 2 Forwarding (L2F)** vor. Beide Hersteller einigten sich auf ein gemeinsames Vorgehen und in der IETF wurde daraus das **Layer 2 Tunnel Protocol (L2TP)**.

Der Vorteil dieser Protokolle gegenüber IPSec liegt vor allem darin, dass beliebige Netzwerk-Protokolle auf eine solche sichere Netzwerkverbindung aufgesetzt werden können, insbesondere NetBEUI und IPX.

Ein wesentlicher Nachteil der beschriebenen Protokolle ist die fehlende Sicherheit auf Paketebene. Außerdem wurden die Protokolle speziell für Einwahlverbindungen entwickelt.

Sicherheit auf höherer Ebene – SSL, S/MIME, PGP

Auch auf höheren Ebenen des OSI-Modells lässt sich die Kommunikation durch Verschlüsselung absichern. Bekannte Beispiele für Protokolle dieser Art sind **SSL (Secure Socket Layer)** vornehmlich für Webbrowser-Verbindungen, **S/MIME (Secure Multipurpose Internet Mail Extensions)** für E-Mails und **PGP (Pretty Good Privacy)** für E-Mails und Dateien.

Bei allen obengenannten Protokollen übernimmt eine Anwendung die Verschlüsselung der übertragenen Daten, beispielsweise der Webbrowser auf der einen Seite und der HTTP-Server auf der anderen Seite.

Ein Nachteil dieser Protokolle ist die Beschränkung auf bestimmte Anwendungen. Für verschiedene Anwendungen werden zudem in aller Regel verschiedene Schlüssel benötigt. Die Verwaltung der Konfiguration wird auf jedem einzelnen Rechner vorgenommen und kann nicht komfortabel nur auf den Gateways erfolgen, wie das bei IPSec möglich

▷ *Die Standards hinter IPSec*

ist. Zwar sind Sicherungsprotokolle auf Anwendungsebene intelligenter, schließlich kennen sie die Bedeutung der übertragenen Daten. Zumeist sind sie aber auch deutlich komplexer.

Alle diese Layer-2-Protokolle erlauben nur Ende-Ende-Verbindungen, sind also (ohne Ergänzungen) ungeeignet für die Kopplung ganzer Netzwerke.

Andererseits benötigen diese Mechanismen nicht die geringsten Änderungen der Netzwerkgeräte oder der Zugangssoftware. Zudem können sie im Unterschied zu Protokollen in unteren Netzwerkebenen auch dann noch wirken, wenn die Dateninhalte schon in den Rechner gelangt sind.

Die Kombination ist möglich

Alle genannten Alternativen sind verträglich zu IPSec und daher auch parallel anzuwenden. Auf diese Weise kann das Sicherheitsniveau erhöht werden. Es ist beispielsweise möglich, sich mit einer L2TP-Verbindung ins Internet einzuwählen, einen IPSec-Tunnel zu einem Web-Server aufzubauen und dabei die HTTP-Daten zwischen Webserver und Browser im gesicherten SSL-Modus auszutauschen.

Allerdings beeinträchtigt jede zusätzlich eingesetzte Verschlüsselung den Datendurchsatz. Der Anwender wird im Einzelfall entscheiden, ob ihm die Sicherheit alleine über IPSec ausreicht oder nicht. Nur in seltenen Fällen wird eine höhere Sicherheit tatsächlich notwendig sein. Zumal sich der verwendete Grad an Sicherheit auch innerhalb von IPSec noch einstellen lässt.

10.9 Die Standards hinter IPSec

IPSec basiert auf verschiedenen Protokollen für die verschiedenen Teilfunktionen. Die Protokolle bauen aufeinander auf und ergänzen sich. Die durch dieses Konzept erreichte Modularität ist ein wichtiger Vorteil von IPSec gegenüber anderen Standards. IPSec ist nicht auf bestimmte Protokolle beschränkt, sondern kann jederzeit um zukünftige Entwicklungen ergänzt werden. Die bisher integrierten Protokolle bieten außerdem schon jetzt ein so hohes Maß an Flexibilität, dass IPSec perfekt an nahezu jedes Bedürfnis angepasst werden kann.

10.9.1 Module von IPSec und ihre Aufgaben

IPSec hat eine Reihe von Aufgaben zu erfüllen. Für jede dieser Aufgaben wurde eines oder mehrere Protokolle definiert.

- ▶ Sicherung der Authentizität der Pakete
- ▶ Verschlüsselung der Pakete
- ▶ Übermittlung und Management der Schlüssel

10.9.2 Security Associations – nummerierte Tunnel

Eine logische Verbindung (Tunnel) zwischen zwei IPSec-Geräten wird als SA (**S**ecurity **A**ssociation) bezeichnet. SAs werden selbstständig vom IPSec-Gerät verwaltet. Eine SA besteht aus drei Werten:

- ▶ **Security Parameter Index (SPI)**

Kennziffer zur Unterscheidung mehrerer logischer Verbindungen zum selben Zielgerät mit denselben Protokollen

- ▶ **IP-Ziel-Adresse**
- ▶ **Verwendetes Sicherheitsprotokoll**

Kennzeichnet das bei der Verbindung eingesetzte Sicherheitsprotokoll: AH oder ESP (zu diesen Protokollen in den folgenden Abschnitten mehr).

Eine SA gilt dabei nur für eine Kommunikationsrichtung der Verbindung (simplex). Für eine vollwertige Send- und Empfangsverbinding werden zwei SAs benötigt. Außerdem gilt eine SA nur für ein eingesetztes Protokoll. Werden AH und ESP verwendet, so sind ebenfalls zwei separate SAs notwendig, also jeweils zwei für jede Kommunikationsrichtung.

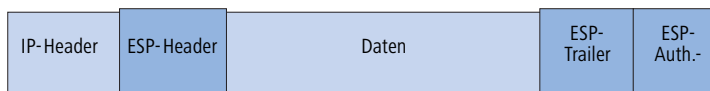
Die SAs werden im IPsec-Gerät in einer internen Datenbank verwaltet, in der auch die erweiterten Verbindungsparameter abgelegt werden. Zu diesen Parametern gehören beispielsweise die verwendeten Algorithmen und Schlüssel.

10.9.3 Verschlüsselung der Pakete – das ESP-Protokoll

Das ESP-Protokoll (**Encapsulating Security Payload**) verschlüsselt die Pakete zum Schutz vor unbefugtem Zugriff. Diese ehemals einzige Funktion von ESP wurde in der weiteren Entwicklung des Protokolls um Möglichkeiten zum Schutz der Integrität und zur Feststellung der Authentizität erweitert. Zudem verfügt auch ESP inzwischen über einen wirksamen Schutz gegen Wiedereinspielung von Paketen. ESP bietet damit alle Funktionen von AH an.

Arbeitsweise von ESP

Der Aufbau von ESP ist komplizierter als der von AH. Auch ESP fügt einen Header hinter den IP-Header ein, zusätzlich allerdings auch noch einen eigenen Trailer und einen Block mit ESP-Authentifizierungsdaten.



Transport- und Tunnel-Modus

ESP kann (wie AH auch) in zwei Modi verwendet werden: Im Transport-Modus und im Tunnel-Modus.

Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt.

Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.

Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

▷ Die Standards hinter IPsec

Verschlüsselungs-Algorithmen

IPsec setzt als übergeordnetes Protokoll keine bestimmte Verschlüsselungs-Algorithmen voraus. In der Wahl der angewandten Verfahren sind die Hersteller von IPsec-Produkten daher frei. Üblich sind folgende Standards:

▶ AES – Advanced Encryption Standard

AES ist der offizielle Verschlüsselungsstandard für die Verwendung in US-amerikanischer Regierungsbehörden und damit die wichtigste Verschlüsselungstechnik weltweit. Im Jahr 2000 entschied sich das **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) nach einem weltweiten Wettbewerb zwischen zahlreichen Verschlüsselungsalgorithmen für den Rijndael-Algorithmus (gesprochen: „Reindoll“) und erklärte ihn 2001 zum AES.

Beim Rijndael-Algorithmus handelt es sich um ein symmetrisches Verschlüsselungsverfahren, das mit variablen Block- und Schlüssellängen arbeitet. Es wurde von den beiden belgischen Kryptografen Joan Daemen und Vincent Rijmen entwickelt und zeichnet sich durch hohe Sicherheit, hohe Flexibilität und hervorragende Effizienz aus.

▶ DES – Data Encryption Standard

DES wurde Anfang der 70er Jahre von IBM für die NSA (National Security Agency) entwickelt und war jahrelang weltweiter Verschlüsselungsstandard. Die Schlüssellänge dieses symmetrischen Verfahrens beträgt 56 Bits. Es gilt heute aufgrund der geringen Schlüssellänge als unsicher und wurde vom NIST im Jahr 2000 durch den AES (Rijndael-Algorithmus) ersetzt. Er sollte nicht mehr verwendet werden.

▶ Triple-DES (auch 3-DES)

Ist eine Weiterentwicklung des DES. Der herkömmliche DES-Algorithmus wird dreimal hintereinander angewendet. Dabei werden zwei verschiedene Schlüssel mit jeweils 56 Bits Länge eingesetzt, wobei der Schlüssel des ersten Durchlaufs beim dritten Durchlauf wiederverwendet wird. Es ergibt sich eine nominale Schlüssellänge von 168 Bit bzw. eine effektive Schlüssellänge von 112 Bit.

Triple-DES kombiniert die ausgeklügelte Technik des DES mit einem ausreichend langen Schlüssel und gilt daher als sehr sicher. Triple-DES arbeitet allerdings langsamer als andere Verfahren.

▶ Blowfish

Die Entwicklung des prominenten Kryptografen Bruce Schneier verschlüsselt symmetrisch. Blowfish erreicht einen hervorragenden Datendurchsatz und gilt als sehr sicher.

▶ CAST (nach den Autoren Carlisle Adams und Stafford Tavares)

Ist ein symmetrisches Verfahren mit einer Schlüssellänge von 128 Bits. CAST ermöglicht eine variable Änderung von Teilen des Algorithmus' zur Laufzeit.

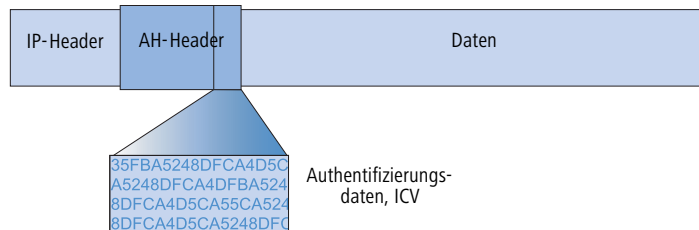


Die Verschlüsselung kann unter LANconfig in der Expertenkonfiguration angepasst werden. Eingriffe dieser Art sind in der Regel nur dann erforderlich, wenn VPN-Verbindungen zwischen Geräten unterschiedlicher Hersteller aufgebaut werden sollen. Standardmäßig bieten LANCOM-Gateways die Verschlüsselung entweder nach AES (128-bit), Blowfish (128-bit) oder Triple-DES (168-bit) an.

10.9.4 Die Authentifizierung – das AH-Protokoll

Das AH-Protokoll (**A**uthentication **H**eder) gewährleistet die Integrität und Authentizität der Daten. Häufig wird die Integrität als Bestandteil der Authentizität betrachtet. Wir betrachten im Folgenden die Integrität als separates Problem, das von AH gelöst wird. Neben Integrität und Authentizität bietet AH auch einen wirksamen Schutz gegen Wiedereinspielen empfangener Pakete (Replay Protection).

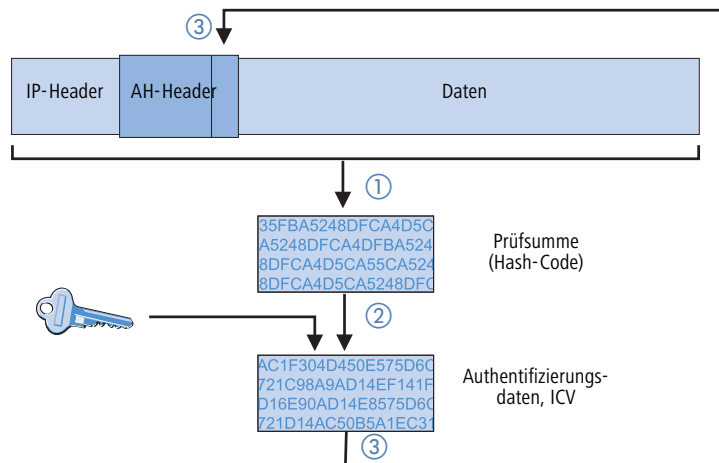
IP-Paketen fügt AH einen eigenen Header direkt hinter dem ursprünglichen IP-Header hinzu. Wichtigster Bestandteil dieses AH-Headers ist ein Feld mit Authentifizierungsdaten (Authentication Data), häufig auch als Integrity Check Value (ICV) bezeichnet.



Der Ablauf von AH im Sender

Im Sender der Pakete läuft die Erstellung der Authentication Data in 3 Schritten ab.

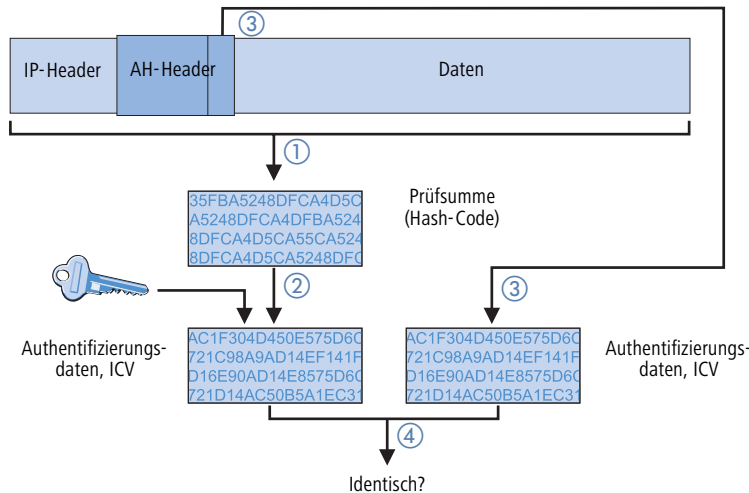
- ① Aus dem Gesamtpaket wird eine Prüfsumme mittels Hash-Algorithmen errechnet.
- ② Diese Prüfsumme wird zusammen mit einem dem Sender und Empfänger bekannten Schlüssel erneut durch einen Hash-Algorithmus geschickt.
- ③ Es ergeben sich die gesuchten Authentifizierungsdaten, die im AH-Header abgelegt werden.



▷ Die Standards hinter IPsec

Prüfung von Integrität und Authentizität im Empfänger

Beim Empfänger läuft das AH-Protokoll sehr ähnlich ab. Auch der Empfänger berechnet zunächst mit seinem Schlüssel die Authentifizierungsdaten für das empfangene Paket. Beim Vergleich mit dem übermittelten ICV des Paketes stellt sich heraus, ob Integrität und Authentizität des Paketes gegeben sind oder nicht.



Bildung der Prüfsumme für den Integritäts-Check

Um die Integrität, also die Korrektheit der transferierten Pakete zu gewährleisten, versieht AH beim Versand jedes Paket mit einer Prüfsumme. Beim Empfänger prüft AH, ob die Prüfsumme zum Inhalt des Paketes passt. Ist das nicht der Fall, dann wurde es entweder falsch übertragen oder bewusst verändert. Solche Pakete werden sofort verworfen und gelangen nicht mehr auf höhere Protokollebenen.

Zur Errechnung der Prüfsumme stehen verschiedene sogenannte Hash-Algorithmen zur Verfügung. Hash-Algorithmen zeichnen sich dadurch aus, dass das Ergebnis (der Hash-Code) charakteristisch für die Eingangsdaten ist („Fingerabdruck“), ohne dass umgekehrt vom Hash-Code auf die Eingangsdaten geschlossen werden könnte. Außerdem haben bei einem hochwertigen Hash-Algorithmus kleinste Änderungen des Eingangswertes einen völlig unterschiedlichen Hash-Code zur Folge. So werden systematische Analysen mehrerer Hash-Codes erschwert.

LANCOM VPN unterstützt die beiden gängigsten Hash-Algorithmen: MD5 und SHA-1. Beide Methoden arbeiten übrigens ohne Schlüssel, d.h. alleine auf der Basis fester Algorithmen. Schlüssel kommen erst in einem späteren Schritt von AH ins Spiel: bei der endgültigen Berechnung der Authentication Data. Die Integritäts-Prüfsumme ist nur ein notwendiges Zwischenergebnis auf dem Weg dorthin.

Berechnung der Authentifizierungsdaten

Im zweiten Schritt bildet AH einen neuen Hash-Code aus der Prüfsumme und einem Schlüssel, die endgültigen Authentifizierungsdaten. Auch für diesen Prozess gibt es unter IPsec verschiedene Standards zur Auswahl. LANCOM VPN unterstützt HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). Als Hash-Algorithmen stehen die Hash-Funktionen MD5 und SHA-1 zur Verfügung. Die HMAC-Versionen heißen entsprechend HMAC-MD5-96 und HMAC-SHA-1-96.

Jetzt wird deutlich, dass AH das Paket selber unverschlüsselt lässt. Lediglich die Prüfsumme des Paketes und der eigene Schlüssel werden gemeinsam zum ICV, den Authentifizierungsdaten, chiffriert und dem Paket als Prüfkriterium beigelegt.

Replay Protection – Schutz vor wiederholten Paketen

AH kennzeichnet zusätzlich zur Beschriftung mit dem ICV jedes Paket auch mit einer eindeutigen, fortlaufenden Nummer (Sequence Number). Dadurch kann der Empfänger solche Pakete erkennen, die von einem Dritten aufgenommen wurden und nun wiederholt gesendet werden. Diese Art von Angriffen wird als „Packet Replay“ bezeichnet.



Mit AH ist keine Maskierung von IPsec-Tunneln möglich, sofern nicht zusätzliche Maßnahmen wie NAT-Traversal oder ein äußeres Layer-2-Tunneling (z.B. PPPT/L2TP) nochmals einen „veränderbaren“ äußeren IP-Header bereitstellen.

10.9.5 Management der Schlüssel – IKE

Das Internet **K**ey **E**xchange Protocol (IKE) ist ein Protokoll, in dem Unterprotokolle zum Aufbau der SAs und für das Schlüsselmanagement eingebunden werden können.

Innerhalb von IKE werden in LANCOM VPN zwei Unterprotokolle verwendet: Oakley für die Authentifizierung der Partner und den Schlüsselaustausch sowie ISAKMP für die Verwaltung der SAs.

Aufbau der SA mit ISAKMP/Oakley

Jeder Aufbau einer SA erfolgt in mehreren Schritten (bei dynamischen Internet-Verbindungen erfolgen diese Schritte, nachdem die öffentliche IP-Adresse übertragen wurde):

- ① Per ISAKMP sendet der Initiator an die Gegenstelle eine Meldung im Klartext mit der Aufforderung zum Aufbau einer SA und Vorschlägen (Proposals) für die Sicherheitsparameter dieser SA.
- ② Die Gegenstelle antwortet mit der Annahme eines Vorschlags.
- ③ Beide Geräte erzeugen nun Zahlenpaare (bestehend aus öffentlichem und privatem Zahlenwert) für das Diffie-Hellman-Verfahren.
- ④ In zwei weiteren Mitteilungen tauschen beide Geräte ihre öffentlichen Zahlenwerte für Diffie-Hellman aus.
- ⑤ Beide Seiten erzeugen aus übertragenem Zahlenmaterial (nach dem Diffie-Hellman-Verfahren) und Shared Secret einen gemeinsamen geheimen Schlüssel, mit dem die weitere Kommunikation verschlüsselt wird. Außerdem

▷ *Die Standards hinter IPSec*

authentifizieren sich beide Seiten gegenseitig anhand von Hash-Codes ihres gemeinsamen Shared Secrets. Die sogenannte Phase 1 des SA-Aufbaus ist damit beendet.

- ⑥ Phase 2 basiert auf der verschlüsselten und authentifizierten Verbindung, die in Phase 1 aufgebaut wurde. In Phase 2 werden die Sitzungsschlüssel für die Authentifizierung und die symmetrische Verschlüsselung des eigentlichen Datentransfers erzeugt und übertragen.



Für die Verschlüsselung des eigentlichen Datentransfers werden symmetrische Verfahren eingesetzt. Asymmetrische Verfahren (auch bekannt als Public-Key-Verschlüsselung) sind zwar sicherer, da keine geheimen Schlüssel übertragen werden müssen. Zugleich erfordern sie aber aufwändige Berechnungen und sind daher deutlich langsamer als symmetrische Verfahren. In der Praxis wird Public-Key-Verschlüsselung meist nur für den Austausch von Schlüsselmaterial eingesetzt. Die eigentliche Datenverschlüsselung erfolgt anschließend mit schnellen symmetrischen Verfahren.

Der regelmäßige Austausch neuer Schlüssel

ISAKMP sorgt während des Bestehens der SA dafür, dass regelmäßig neues Schlüsselmaterial zwischen den beiden Geräten ausgetauscht wird. Dieser Vorgang geschieht automatisch und kann über die Einstellung der 'Lifetime' in der erweiterten Konfiguration von LANconfig kontrolliert werden.

11 Virtuelle LANs (VLANs)

11.1 Was ist ein Virtuelles LAN?

Die steigende Verfügbarkeit von preiswerten Layer-2-Switches erlaubt den Aufbau sehr viel größerer LANs als in der Vergangenheit. Bisher wurden oft kleinere Abschnitte eines Netzwerks mit Hubs zusammengeschlossen. Diese einzelnen Segmente (Collision Domains) wurden dann über Router zu größeren Einheiten zusammengeschlossen. Da ein Router jedoch immer die Grenze zwischen zwei LANs bildet, entstehen in dieser Struktur mehrere LANs mit eigenen IP-Adresskreisen.

Mit dem Einsatz von Switches können dagegen sehr viel mehr Stationen zu einem großen LAN zusammen geschlossen werden. Durch die gezielte Steuerung des Datenflusses auf die einzelnen Ports wird die verfügbare Bandbreite besser genutzt als beim Einsatz von Hubs, die Konfiguration und Wartung von Routern im Netzverbund entfällt.

Aber auch eine auf Switches basierende Netzwerkstruktur hat ihrer Nachteile:

- ▶ Broadcasts werden wie auch bei den Hubs über das gesamte LAN gesendet, selbst wenn die entsprechenden Datenpakete nur für ein bestimmtes Segment des LANs von Bedeutung sind. Bei einer ausreichenden Anzahl von Stationen im Netz kann das schon zu einer deutlichen Einschränkung der verfügbaren Bandbreite im LAN führen.
- ▶ Der gesamte Datenverkehr auf dem physikalischen LAN ist "öffentlich". Selbst wenn einzelne Segmente unterschiedliche IP-Adresskreise nutzen, kann jede Station im LAN theoretisch den Datenverkehr aus allen logischen Netzen auf dem Ethernetstrang abhören. Der Schutz einzelner LAN-Segmente mit Firewalls oder Router erhöht wieder die Anforderungen an die Administration des Netzwerks.

Eine Möglichkeit, diese Probleme zu überwinden, stellen die virtuellen LANs (VLAN) dar, wie sie in IEEE 802.1p/q beschrieben sind. Bei diesem Konzept werden auf einem physikalischen LAN mehrere virtuelle LANs definiert, die sich gegenseitig nicht behindern und die auch den Datenverkehr der jeweils anderen VLANs auf dem physikalischen Ethernetstrang nicht empfangen oder abhören können.

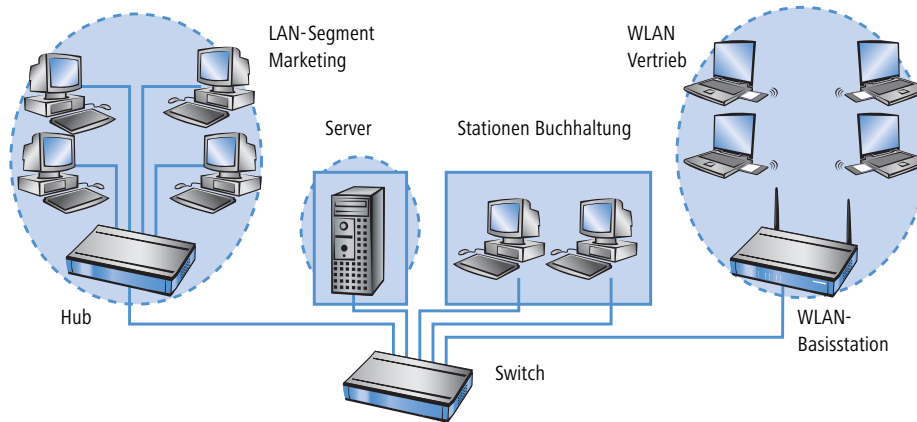
11.2 So funktioniert ein VLAN

Mit der Definition von VLANs auf einem LAN sollen folgende Ziele erreicht werden:

- ▶ Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern abgeschirmt werden.
- ▶ Der Broadcast-Datenverkehr soll ebenfalls auf die logischen Einheiten reduziert werden und nicht das gesamte LAN belasten.
- ▶ Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern mit einer besonderen Priorität übertragen werden.

Zur Verdeutlichung ein Beispiel: In einen LAN ist an einen Switch ein Hub angeschlossen, der vier Stationen aus dem Marketing an das Netz anbindet. Ein Server und zwei Stationen der Buchhaltung sind direkt an den Switch angeschlossen. Den letzten Abschnitt bildet die Basisstation eine Funknetzwerks, in dem sich vier WLAN-Clients aus dem Vertrieb befinden.

▷ So funktioniert ein VLAN



Die Stationen aus Marketing und Vertrieb sollen miteinander kommunizieren können. Außerdem sollen Sie auf den Server zugreifen. Die Buchhaltung benötigt ebenfalls Zugriff auf den Server, soll aber ansonsten von den anderen Stationen abgeschirmt werden.

11.2.1 Frame-Tagging

Um den Datenverkehr eines virtuellen LANs gegen die anderen Netzteilnehmer abschirmen und ggf. priorisieren zu können, müssen die Datenpakete eine entsprechende Kennzeichnung aufweisen. Dazu werden die MAC-Frames um ein zusätzliches Merkmal (ein "Tag") erweitert. Das entsprechende Verfahren wird daher auch als "Frame-Tagging" bezeichnet.

Das Frame-Tagging muss dabei so realisiert sein, dass folgende Anforderungen erfüllt werden:

- ▶ Datenpakete mit und ohne Frame-Tagging müssen auf einem physikalischen LAN parallel nebeneinander her existieren können.
- ▶ Stationen und Switches im LAN, welche die VLAN-Technik nicht unterstützen, müssen die Datenpakete mit Frame-Tagging ignorieren bzw. wie "normale" Datenpakete behandeln.

Das Tagging wird durch ein zusätzliches Feld im MAC-Frame realisiert. In diesem Feld sind zwei für das virtuelle LAN wesentliche Informationen enthalten:

- ▶ **VLAN-ID:** Mit einer eindeutigen Nummer wird das virtuelle LAN gekennzeichnet. Diese ID bestimmt die Zugehörigkeit eines Datenpakets zu einem logischen (virtuellen) LAN. Mit diesem 12-Bit-Wert können bis zu 4094 unterschiedliche VLANs definiert werden (die VLAN-IDs "0" und "4095" sind reserviert bzw. nicht zulässig).



Die VLAN-ID "1" wird von vielen Geräten als Default-VLAN-ID verwendet. Bei einem unkonfigurierten Gerät gehören alle Ports zu diesem Default-VLAN. Diese Zuweisung kann bei der Konfiguration allerdings auch wieder verändert werden ('Die Porttabelle' → Seite 330).

▷ So funktioniert ein VLAN

- ▶ **Priorität:** Die Priorität eines VLAN-gekennzeichneten Datenpakets wird mit einem 3-Bit-Wert markiert. Dabei steht die "0" für die geringste, die "7" für die höchste Priorität. Datenpakete ohne VLAN-Tag werden mit der Priorität "0" behandelt.

Durch dieses zusätzliche Feld werden die MAC-Frames länger als eigentlich erlaubt. Diese "überlangen" Pakete können nur von VLAN-fähigen Stationen und Switches richtig erkannt und ausgewertet werden. Bei Netzteilnehmern ohne VLAN-Unterstützung führt das Frame-Tagging quasi nebenbei zum gewünschten Verhalten:

- ▶ Switches ohne VLAN-Unterstützung leiten diese Datenpakete einfach weiter und ignorieren die zusätzlichen Felder im MAC-Frame.
- ▶ Stationen ohne VLAN-Unterstützung können in den Paketen aufgrund des eingefügten VLAN-Tags den Protokolltyp nicht erkennen und verwerfen sie stillschweigend.



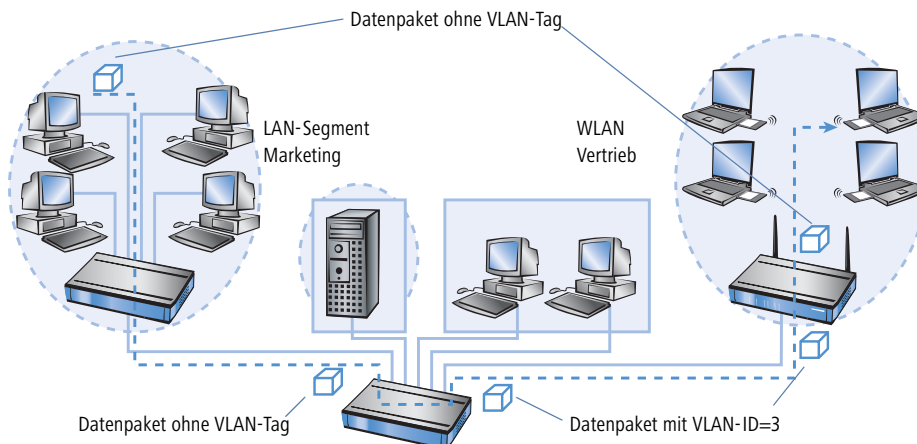
Ältere Switches in LAN können überlange Frames möglicherweise nicht richtig zwischen den einzelnen Ports weiterleiten und verwerfen die getaggten Pakete.

11.2.2 Umsetzung in den Schnittstellen des LANs

Mit den virtuellen LANs sollen bestimmte Stationen zu logischen Einheiten zusammengefasst werden. Die Stationen selbst können aber die notwendigen VLAN-Tags in der Regel weder erzeugen noch verarbeiten.

Der Datenverkehr zwischen den Netzteilnehmern läuft immer über die verschiedenen Schnittstellen (Interfaces) der Verteiler im LAN. Diesen Verteilern (Switches, Basisstationen) fällt damit also die Aufgabe zu, die VLAN-Tags der gewünschten Anwendung entsprechend in die Datenpakete einzubauen, sie auszuwerten und ggf. wieder zu entfernen. Da die logischen Einheiten jeweils mit den verschiedenen Interfaces der Verteiler verbunden sind, werden die Regeln über die Generierung und Verarbeitung der VLAN-Tags den einzelnen Schnittstellen zugewiesen.

Greifen wir dazu das erste Beispiel wieder auf:



▷ So funktioniert ein VLAN

Ein Rechner aus dem Marketing schickt ein Datenpaket an einen Rechner im Vertrieb. Der Hub im Marketing leitet das Paket einfach weiter an den Switch. Der Switch empfängt das Paket auf seinem Port Nr. 1 und weiß, dass dieser Port zum VLAN mit der VLAN-ID "3" gehört. Er setzt in den MAC-Frame das zusätzliche Feld mit dem richtigen VLAN-Tag ein und gibt das Paket auch nur auf den Ports (2 und 5) wieder aus, die ebenfalls zum VLAN 3 gehören. Die Basisstation im Vertrieb empfängt das Paket auf dem LAN-Interface. Anhand der Einstellungen kann die Basisstation erkennen, dass die WLAN-Schnittstelle ebenfalls zum VLAN 3 gehört. Sie entfernt das VLAN-Tag aus dem MAC-Frame und gibt das Paket auf der drahtlosen Schnittstelle wieder aus. Der Client im WLAN kann das Paket, das nun wieder die "normale" Länge hat, wie jedes andere Datenpaket ohne VLAN-Tagging verarbeiten.

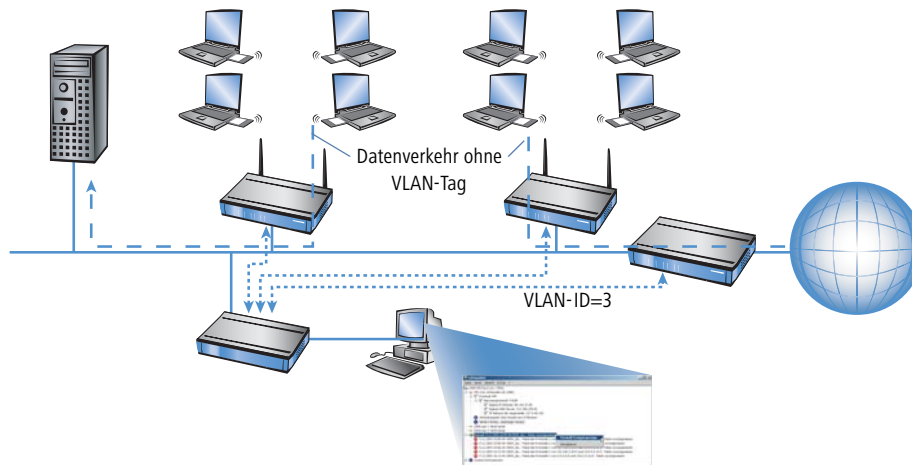
11.2.3 Anwendungsbeispiele

Die Hauptanwendung von virtuellen LANs ist die Aufgabe, auf einem physikalischen Ethernetstrang unterschiedliche logische Netzwerke einzurichten, deren Datenverkehr vor den anderen logischen Netzen geschützt ist.

Die folgenden Abschnitte zeigen Beispiele für den Einsatz von virtuellen LANs vor diesem Hintergrund.

Management- und User-Traffic auf einem LAN

Auf dem Campus einer Universität werden mehrere Hot-Spots aufgestellt. Damit ist den Studenten über Notebooks mit WLAN-Karten der Zugang zum Server der Bibliothek und zum Internet möglich. Die Hot-Spots sind an das LAN der Universität angeschlossen. Über dieses LAN greifen die Administratoren auch auf die Basisstationen zu, um über SNMP verschiedene Management-Aufgaben zu erledigen.

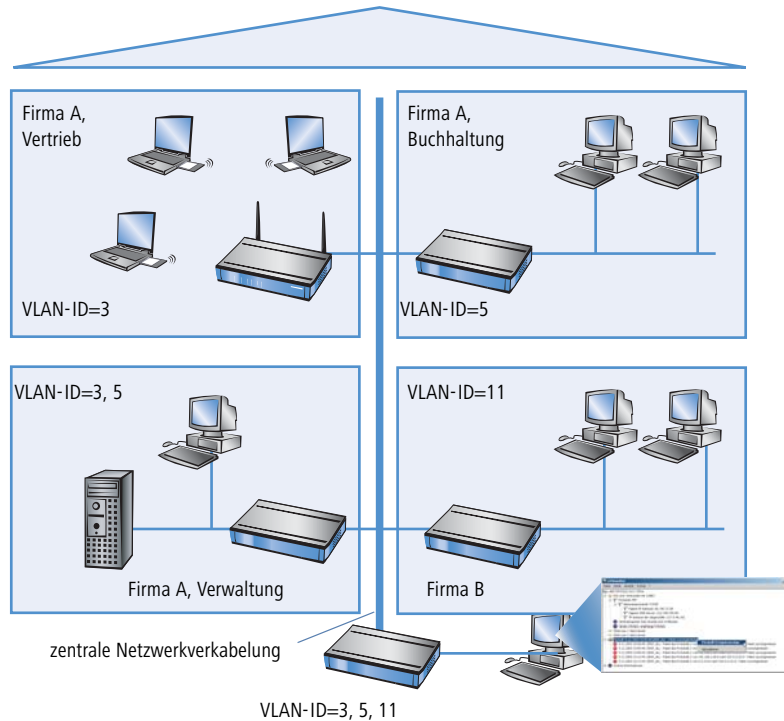


Mit dem Einrichten eines virtuellen LANs zwischen den Basisstationen und dem Switch des Administrators wird der Management-Datenverkehr von dem "öffentlichen" Verkehr auf dem LAN abgeschirmt.

▷ So funktioniert ein VLAN

Verschiedene Organisationen auf einem LAN

Die Flexibilität der modernen Arbeitswelt bringt für die Administratoren neue Herausforderungen an die Planung und Wartung der Netzwerkstrukturen. In öffentlichen Bürogebäuden ändert sich permanent die Belegung der Räume durch die Mieter, und auch innerhalb einer Firma werden die Teams häufig neu zusammengestellt. In beiden Fällen müssen die einzelnen Einheiten jedoch über ein unabhängiges, abgeschirmtes LAN verfügen. Diese Aufgabe lässt sich mit Änderungen an der Hardware nur sehr aufwändig oder gar nicht realisieren, weil z.B. in einem Bürogebäude nur eine zentrale Verkabelung vorhanden ist.



Mit virtuellen LANs lässt sich diese Aufgabe sehr elegant lösen. Auch bei einem späteren Wechsel von Abteilungen oder Firmen im Gebäude kann die Netzstruktur sehr einfach angepasst werden.

Alle Netzteilnehmer nutzen in diesem Beispiel das zentrale Ethernet, das mit den angeschlossenen Geräten von einem Dienstleister überwacht wird. Die Firma A hat drei Abteilungen in zwei Etagen. Der Vertrieb kann über die VLAN-ID 3 mit der Verwaltung kommunizieren, die Buchhaltung mit der Verwaltung über die VLAN-ID 5. Untereinander sehen sich die Netze von Buchhaltung und Vertrieb nicht. Die Firma B ist über die VLAN-ID 11 ebenfalls von den anderen Netzen abgeschirmt, nur der Dienstleister kann zu Wartungszwecken auf alle Geräte zugreifen.

11.3 Konfiguration von VLANs



Die Funktionen der VLAN-Technik werden derzeit nur von LANCOM Wireless-Geräten unterstützt.

Die Konfiguration im VLAN-Bereich der LANCOM Wireless-Geräte hat zwei wichtige Aufgaben:

- ▶ Virtuelle LANs definieren und ihnen dabei einen Namen, eine VLAN-ID und die zugehörigen Interfaces zuordnen
- ▶ Für die Interfaces definieren, wie mit Datenpaketen mit bzw. ohne VLAN-Tags verfahren werden soll

11.3.1 Die Netzwerktabelle

In der Netzwerktabelle werden die virtuellen LANs definiert, an denen das LANCOM teilnehmen soll. Die Tabelle enthält maximal 32 Einträge mit folgenden Informationen:

- ▶ **Name:** Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.
- ▶ **VLAN-ID:** Diese Nummer kennzeichnet das VLAN eindeutig. Werte von 1 bis 4094 sind hier möglich.
- ▶ **Portliste:** In dieser Liste werden die Interfaces des LANCOM eingetragen, die zu dem VLAN gehören. Als Ports können eingetragen werden:
 - ▷ "LAN-n" für die Ethernet-Ports des Gerätes
 - ▷ "WLAN-n" für Point-to-Station WLAN-Ports
 - ▷ "P2P-n" für Point-to-Point WLAN-Ports

Für ein Gerät mit einem LAN-Interface und einem WLAN-Port können z.B. die Ports "LAN-1" und "WLAN-1" eingetragen werden. Bei Portbereichen werden die einzelnen Ports durch eine Tilde getrennt: "P2P-1~P2P-4".



Die verfügbaren Ports können in der Porttabelle (→Seite 330) nachgesehen werden.

Beispiel für eine Netzwerktabelle:

Name	VLAN-ID	Portliste
Default	1	LAN-1, WLAN-1, WLAN-2
Vertrieb	2	LAN-1, WLAN-1
Marketing	3	LAN-1, WLAN-2

11.3.2 Die Porttabelle

In der Porttabelle werden die einzelnen Ports des Gerätes für die Verwendung im VLAN konfiguriert. Die Tabelle hat einen Eintrag für jeden Port des Gerätes mit folgenden Werten:

- ▶ **Port:** Der Name des Ports, nicht editierbar

▷ Konfiguration von VLANs

- ▶ **Tagging verwenden:** Diese Option gibt an, ob Datenpakete auf diesem Port getaggt werden sollen. Das Tagging bezieht sich nur auf solche Datenpakete, die über diesen Port **versendet** werden.
- ▶ **Ungetaggte Frames zulassen:** Diese Option gibt an, ob ungetaggte Datenpakete weitergeleitet werden, die auf diesem Port **empfangen** wurden.
- ▶ **Alle VLANs zulassen:** Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port selbst nicht zur gleichen VLAN-ID gehört.
- ▶ **Default-ID:** Diese VLAN-ID hat zwei Funktionen:
 - ▷ Ungetaggte Pakete, die auf diesem Port empfangen wurden, werden mit dieser VLAN-ID versehen.
 - ▷ Wenn das Tagging für gesendete Pakete eingeschaltet ist, wird diese VLAN-ID den Paketen **nicht** zugewiesen. Wird ein Paket mit dieser VLAN-ID empfangen, wird es beim weiterleiten **ohne** diese ID versendet, obwohl das Tagging eingeschaltet ist.

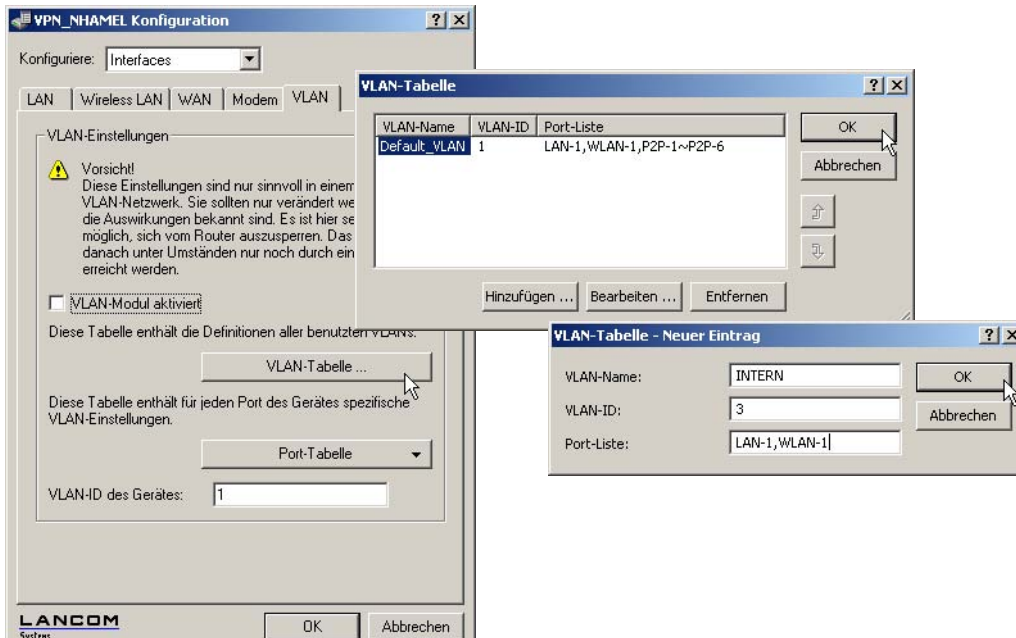
Beispiel für eine Porttabelle:

Port	Tagging verwenden	Ungetaggte Frames zulassen	Alle VLANs zulassen	Default-ID
LAN-1	Ein	Ein	Ein	1
WLAN-1	Aus	Ein	Aus	1
WLAN-2	Aus	Ein	Aus	1
P2P-1	Aus	Ein	Aus	1
P2P-2	Aus	Ein	Aus	1
P2P-3	Aus	Ein	Aus	1
P2P-4	Aus	Ein	Aus	1
P2P-5	Aus	Ein	Aus	1
P2P-6	Aus	Ein	Aus	1

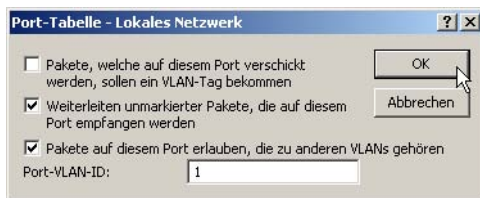
11.3.3 Konfiguration mit LANconfig

Unter LANconfig stellen Sie die Parameter für die virtuellen Netze im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'VLAN' ein. Über die Schaltfläche **VLAN-Tabelle** erreichen Sie die Definition der verwendeten virtuellen Netze:

▷ Konfiguration von VLANs



Über die Schaltfläche **Port-Tabelle** öffnen Sie eine Drop-Down-Liste, in der Sie jeweils einen VLAN-Port zur Bearbeitung auswählen können:



11.3.4 Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Tabellen zur Konfiguration der VLANs auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► LAN-Bridge ► VLAN-Konfiguration
Terminal/Telnet	cd /Setup/LAN-Bridge/VLAN-Konfiguration

Unter WEBconfig präsentiert sich die VLAN-Konfiguration folgendermaßen:

[Experten-Konfiguration](#)

-  [Setup](#)
-  [LAN-Management-Modul](#)

VLAN-Konfiguration

-  [Netzwerk-Tabelle](#) 32 x [Name,VLAN-ID,Port-Liste]
-  [Port-Tabelle](#) 8 x [Port,Tagging-Benutzen,Ungetaggte-Frames-zulassen...]
-  [Geraete-VLAN-ID](#) 1

 [Hilfe \(Referenzhandbuch\)](#)  11.12.2003 14:06

 [Vorherige Seite](#)  [Startseite](#)  [LANCOM Systems Startseite](#)

▷ Was ist ein WLAN?

12 Wireless LAN – WLAN

12.1 Was ist ein WLAN?



Die folgenden Abschnitte beschreiben allgemein die Funktionalität des LCOS-Betriebssystems im Zusammenhang mit Funknetzwerken. Welche Funktionen von Ihrem Gerät unterstützt werden, entnehmen Sie bitte dem Handbuch zum jeweiligen Gerät.

In diesem Kapitel stellen wir Ihnen kurz die Technologie von Funk-Netzwerken vor. Außerdem geben wir Ihnen einen Überblick über die vielfältigen Einsatzmöglichkeiten, Funktionen und Fähigkeiten Ihrer LANCOM Access Points und WLAN-Router.

Ein Funk-LAN verbindet einzelne Endgeräte (PCs und mobile Rechner) zu einem lokalen Netzwerk (auch LAN – **Local Area Network**). Im Unterschied zu einem herkömmlichen LAN findet die Kommunikation nicht über Netzkabel, sondern über Funkverbindungen statt. Aus diesem Grund nennt man ein Funk-LAN auch **Wireless Local Area Network (WLAN)**.

In einem Funk-LAN stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der einzelnen Stationen in ein firmeninternes Mailsystem oder der Zugang zum Internet.

Die Vorteile von Funk-LANs liegen auf der Hand: Notebooks und PCs können dort aufgestellt werden, wo es sinnvoll ist – Probleme mit fehlenden Anschlüssen oder baulichen Veränderungen gehören bei der drahtlosen Vernetzung der Vergangenheit an.

12.1.1 Standardisierte Funkübertragung nach IEEE

IEEE 802.11

LANCOM Funknetzwerkprodukte arbeiten nach dem IEEE-Standard 802.11. Diese Standard-Familie stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet die bekannteste ist. Innerhalb der IEEE 802.11 Familie gibt es verschiedene Standards für die Funkübertragung in unterschiedlichen Frequenzbereichen und mit unterschiedlichen Geschwindigkeiten. LANCOM Basis-Stationen und AirLancer Client Adapter unterstützen je nach Ausführung unterschiedliche Standards:

- ▶ IEEE 802.11a mit bis zu 54 MBit/s Übertragungsrate im 5 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).
- ▶ IEEE 802.11b mit bis zu 11 MBit/s Übertragungsrate im 2,4 GHz Frequenzband.
- ▶ IEEE 802.11g mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).

IEEE 802.11a: 54 MBit/s

IEEE 802.11a sieht den Betrieb von Funk-LANs im 5 GHz Frequenzband (5,15 GHz bis 5,75 GHz) mit bis zu 54 MBit/s maximaler Übertragungsrate vor. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung,

beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 48 MBit/s, danach auf 36 MBit/s usw. bis auf minimal 6 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 125 m, in Gebäuden typischerweise bis zu 25 m. Der IEEE 802.11a Standard verwendet OFDM (**O**rt**H**ogonal **F**requen**y** **D**ivision **M**ultiplexing) als Modulationsverfahren.

OFDM

Bei OFDM handelt es sich um ein Modulationsverfahren, das mehrere unabhängige Trägerfrequenzen für die Übertragung des Datensignals verwendet und diese Trägerfrequenzen mit einer verringerten Übertragungsrate moduliert. Das OFDM Modulationsverfahren ist dabei insbesondere sehr unempfindlich gegen Echos und andere Beeinträchtigungen und ermöglicht hohe Übertragungsraten.

Turbo-Modus

Im 'Turbo-Modus' können LANCOM Wireless Basis-Stationen zwei Funkkanäle gleichzeitig nutzen und damit die Übertragungsrate auf maximal 108 MBit/s steigern. Der Turbo-Modus kann in Verbindung mit dem IEEE 802.11a-Standard genutzt werden zwischen LANCOM Basis-Stationen und AirLancer Funknetzwerkarten. Diese Steigerung der Übertragungsrate muss in der Basisstation entsprechend eingeschaltet werden und kann zu einer Reduzierung der Sendeleistung und damit der Reichweite der Funkverbindung führen.

IEEE 802.11b: 11 MBit/s

IEEE 802.11b sieht den Betrieb von lokalen Funk-LANs im ISM-Frequenzband vor (**I**ndustrial, **S**cientific, **M**edical: 2.4 bis 2.483 GHz). Die maximale Bandbreite der Datenübertragung beträgt bis zu 11 MBit/s. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung, beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 5,5 MBit/s, danach auf 2 und schließlich auf 1 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 150 m, in Gebäuden typischerweise bis zu 30 m. IEEE 802.11b ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a.

DSSS

Zur Abschirmung gegen Störungen durch andere Sender, die gegebenenfalls das gleiche Frequenzband verwenden, wird im 2,4 GHz Frequenzband für IEEE 802.11b das DSSS-Verfahren verwendet (**D**irect **S**equence **S**pread **S**pectrum). Normalerweise benutzt ein Sender nur einen sehr schmalen Bereich des verfügbaren Frequenzbandes zur Übertragung. Wird genau dieser Bereich auch von einem weiteren Sender verwendet, kommt es zu Störungen in der Übertragung. Beim DSSS-Verfahren nutzt der Sender einen breiteren Teil des möglichen Frequenzbandes und wird so unempfindlicher gegen schmalbandige Störungen. Dieses Verfahren wird auch im militärischen Bereich zur Steigerung der Abhörsicherheit eingesetzt.

IEEE 802.11g: 54 MBit/s

Der IEEE 802.11g Standard arbeitet ebenfalls mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz ISM-Frequenzband. Im Gegensatz zu IEEE 802.11b wird jedoch bei IEEE 802.11g die OFDM Modulation verwendet wie schon bei IEEE 802.11a. IEEE 802.11g enthält einen besonderen Kompatibilitätsmodus der eine Abwärtskompatibilität zu dem weit verbreiteten IEEE 802.11b Standard gewährleistet. Wird dieser Kompatibilitätsmodus verwendet, so ist jedoch mit Geschwindigkeitseinbußen bei der Datenübertragung zu rechnen. IEEE 802.11g ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a. Die Reichweiten von IEEE 802.11g Produkten sind vergleichbar mit denen von IEEE 802.11b Produkten.

▷ Was ist ein WLAN?

Turbo-Modus

Auch im 802.11g-Standard kann mit dem 'Turbo-Modus' durch die parallele Nutzung von zwei Funkkanälen die Übertragungsrate auf maximal 108 MBit/s gesteigert werden. Da im 2,4 GHz-Band jedoch weniger Kanäle als im 5 GHz-Band genutzt werden können, schränkt die Verwendung des Turbo-Modus hier die Kanalwahl deutlich ein.

Übertragungsraten

Die angegebenen Übertragungsraten sind stets als Bruttodatenraten zu verstehen, das heißt, das der gesamte Protokoll-Overhead wie zum Beispiel die aufwendigen Protokolle zur Sicherung der Funkübertragung in den angegebenen Übertragungsraten enthalten sind. Die Nettoübertragungsrate kann bei allen oben erwähnten IEEE 802.11 Standards somit nur etwa die Hälfte der angegebenen Bruttodatenraten betragen.

Reichweite

Die tatsächlich erzielten Reichweiten bei Funkübertragungen hängen bei allen Übertragungsstandards stark von der räumlichen Umgebung ab. Insbesondere elektromagnetische Störungen und Hindernisse haben Einfluss auf die Reichweite. Entscheidend ist häufig eine optimale Positionierung der Funkstationen (Netzwerkadapter und Basis-Stationen).

Verbesserungen können durch die optimale Positionierung der Funkstationen (Netzwerkadapter und Basis-Stationen) erreicht werden. Für weitere Reichweitengewinne empfiehlt sich der Einsatz zusätzlicher Antennen (z. B. AirLancer Extender).

IEEE-Standards

Um ein Höchstmaß an Kompatibilität zu garantieren, hält sich LANCOM Systems an die Industriestandards der IEEE¹, die im vorhergehenden Absatz beschrieben wurden. Ihre LANCOM Basis-Station arbeitet daher problemlos und zuverlässig auch mit Geräten anderer Hersteller zusammen.

Ihre LANCOM Basis-Station unterstützt je nach Modell die Standards IEEE 802.11g (abwärtskompatibel zu IEEE 802.11b) und/oder IEEE 802.11a.

Der Betrieb der integrierten Funkkarte Ihrer Basis-Station ist jeweils nur in einem Frequenzband, also entweder 2,4 GHz oder 5 GHz möglich. Der gleichzeitige Betrieb von IEEE 802.11g und IEEE 802.11a ist nicht möglich. Da IEEE 802.11g abwärtskompatibel zu IEEE 802.11b ist, ist der gleichzeitige Betrieb dieser beiden Standards mit Geschwindigkeitseinbußen möglich.

1. Institute of Electrical and Electronic Engineers – internationale Vereinigung, die unter anderem zahlreiche Technologiestandards etabliert hat („IEEE“ wird üblicherweise „ei-trippel-i“ ausgesprochen).

Übertragungsraten im Kompatibilitätsmodus

Bitte beachten Sie, dass die erreichten Datenübertragungsraten vom verwendeten 2,4-GHz-Modus abhängen. Wird die Basis-Station im 802.11g-Modus betrieben, erzielen Sie die höchsten Übertragungsraten. Werden die 802.11b-Stationen in einem Funknetzwerk mit eingeschaltetem Kompatibilitätsmodus aktiv, sinkt die tatsächliche Übertragungsraten ab.



Bitte beachten Sie, dass nicht alle Frequenzen in jedem Land erlaubt sind! Eine Tabelle mit den Frequenzen und die Zulassungsvorschriften finden Sie im Anhang des Handbuchs zum jeweiligen Gerät.

12.1.2 Die Betriebsarten von Funk-LANs und Basis-Stationen

Die Funk-LAN-Technologie und die Basis-Stationen in Funk-LANs werden in folgenden Betriebsarten eingesetzt:

- ▶ Einfache, direkte Verbindung zwischen Endgeräten ohne Basis-Station (Ad-hoc-Modus, nur im 2,4 GHz-Band)
- ▶ Strukturierte Funk-LANs, evtl. Anschluss an LAN mit einer oder mehreren Basis-Stationen (Infrastruktur-Modus)
- ▶ Verbinden zweier LANs über eine Funkstrecke (Point-to-Point-Modus – Point-to-Multipoint), auch mehrere Brücken gleichzeitig
- ▶ Anbindung von Geräten mit Ethernet-Schnittstelle über eine Basis-Station (Client-Modus)
- ▶ Erweitern eines bestehenden Ethernet-Netzwerks um WLAN (Bridge-Modus)
- ▶ Mehrere Funkzellen mit nur einer Basisstation (Multi-SSID)

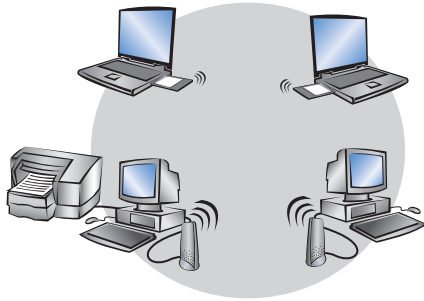
Der Ad-hoc-Modus

Wenn zwei oder mehr Endgeräte mit kompatiblen Funk-Schnittstellen ausgerüstet sind, so können beide direkt miteinander über Funk kommunizieren. Diese einfachste Anwendung nennt sich Ad-hoc-Modus.

Im Ad-hoc-Netzwerk (spontanes Netzwerk) verbinden Sie zwei oder mehrere Rechner mit eigenen Schnittstellen zum Funk-LAN direkt miteinander.

Nur im IEEE
802.11b- oder
IEEE 802.11g-
Standard

▷ Was ist ein WLAN?



Diese Betriebsart wird allgemein auch als Peer-to-Peer-Netzwerk bezeichnet. Die einzelnen PCs können sofort Verbindung miteinander aufnehmen und Daten untereinander austauschen.

Das Infrastruktur-Netzwerk

Komfortabler und leistungsfähiger wird ein Funk-LAN durch den Einsatz einer oder mehrerer Basis-Stationen (auch Access-Point genannt). Ein Funk-LAN mit einer oder mehreren Basis-Stationen nennt man in der Funk-LAN-Terminologie Infrastruktur-Netzwerk.



In manchen Geräten ist der Access Point in einen Router eingebaut, in diesen Fällen spricht man vom „WLAN-Router“.

Durch die LAN-Anbindung von Basis-Stationen ergeben sich für das Funk-LAN interessante Anwendungen:

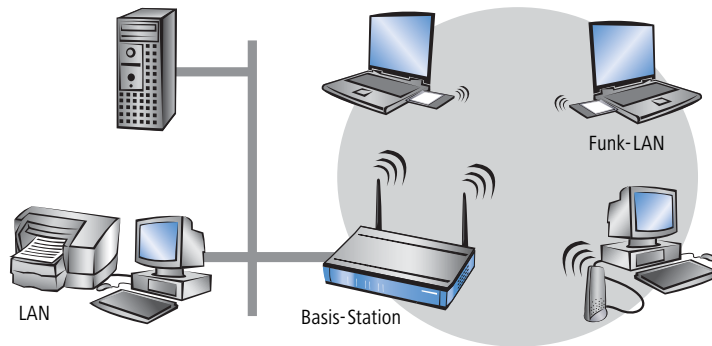
- ▶ Anbindung des Funk-LANs an ein bestehendes LAN
- ▶ Erweitern der Ausdehnung eines Funk-LANs

Zusätzlich ermöglicht der Einsatz einer Basis-Station die zentrale Administration des Funk-LANs.

Ein Infrastruktur-Netzwerk eignet sich hervorragend als Ergänzung zu bestehenden LANs. Bei der Erweiterung eines LANs in Bereichen, in denen eine Verkabelung nicht möglich oder unwirtschaftlich ist, stellt das Infrastruktur-Netzwerk die ideale Lösung dar.

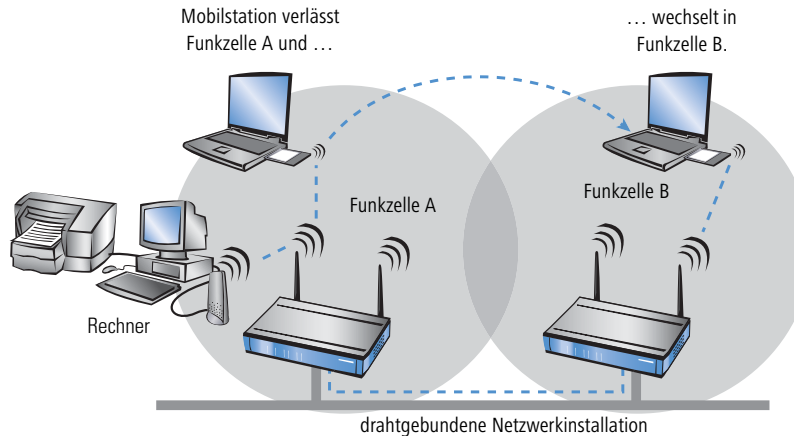
Anschluss an ein bestehendes LAN

▷ Was ist ein WLAN?



Größere Ausdehnung durch die Roaming-Funktion

Der Funkbereich, in der eine Basis-Station von Mobil-Stationen erreicht werden kann, wird als Funkzelle bezeichnet. Wenn die Reichweite einer Funkzelle nicht mehr ausreicht, um alle mobilen Stationen zu einem Funk-Netzwerk zusammenschließen, können auch mehrere Basis-Stationen eingesetzt werden. Damit wird es möglich, von einer Funkzelle in die andere zu wechseln, ohne dass die Verbindung zum Netzwerk unterbrochen wird. Die Übermittlung von Roaming-Informationen und Daten zwischen den Basis-Stationen erfolgt über ein kabelbasiertes LAN.



Im Beispiel ermöglicht die Roaming-Funktion der Mobilstation den Zugriff auf den Rechner in Funkzelle A auch nach ihrem Wechsel in Funkzelle B. Nach dem Funkzellenwechsel leitet die Basis-Station in Funkzelle B die Daten der Mobilstation über LAN an die Basis-Station in Funkzelle A weiter. Von dort gelangen sie über Funk an den Rechner in Funkzelle A. Die Verbindung zwischen beiden Geräten bleibt auf diese Weise jederzeit bestehen.

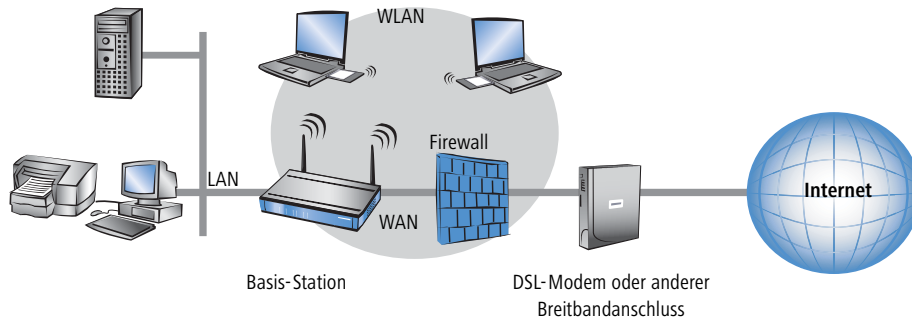
Ein Funk-LAN kann aus beliebig vielen Funkzellen bestehen. Dem Wachstum eines Funk-LANs sind somit keine Grenzen gesetzt.

▷ Was ist ein WLAN?

Basis-Station als Router

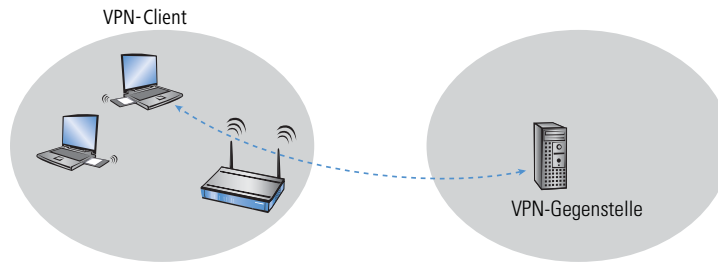
Die LANCOM Wireless Basis-Stationen besitzen einen WAN-Anschluss für alle gängigen Breitband-Modems mit Ethernet-Anschluss (DSL- oder Kabelmodems). Außerdem verfügt die Basis-Station über alle Funktionen eines vollwertigen IP- und IPX-Routers. So ausgestattet dient sie den Stationen in Funk-LAN und LAN z.B. als Gateway ins Internet. Der Router überprüft empfangene Datenpakete daraufhin, ob sie in ein anderes Netz oder zu einem anderen Rechner übertragen werden müssen. Erforderliche Verbindungen baut der Router selbstständig auf.

Die integrierte Stateful-Inspection Firewall verhindert wirksam ein Eindringen von ungewolltem Datenverkehr in das eigene Netzwerk indem eingehender Datenverkehr nur als Reaktion auf ausgehenden Datenverkehr zugelassen wird. Die IP-Masquerading-Funktion im Router versteckt beim Zugang ins Internet alle Arbeitsstationen im LAN hinter einer einzigen öffentlichen IP-Adresse. Die tatsächlichen Identitäten (IP-Adressen) der einzelnen Stationen bleiben verborgen. Firewall-Filter im Router erlauben die gezielte Sperrung von IP-Adressen, Protokollen und Ports. Mit MAC-Adressfiltern kann auch der Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion des Gerätes gezielt kontrolliert werden.

**VPN Pass-Through**

Zur Abschirmung von sensiblen Daten wird immer häufiger die VPN-Technologie eingesetzt (VPN = Virtual Private Network). Die LANCOM Wireless Basisstation kann die verschlüsselten Daten zwischen einem VPN-Client im WLAN und einem anderen Rechner im kabelgebundenen LAN routen und dabei gleichzeitig maskieren. Dieses „Durchreichen“ der VPN-kodierten Daten nennt sich in der Fachsprache „VPN-Pass-Through“. Unterstützt werden:

- ▶ PPTP-Pass-Through
- ▶ IPsec-Pass-Through

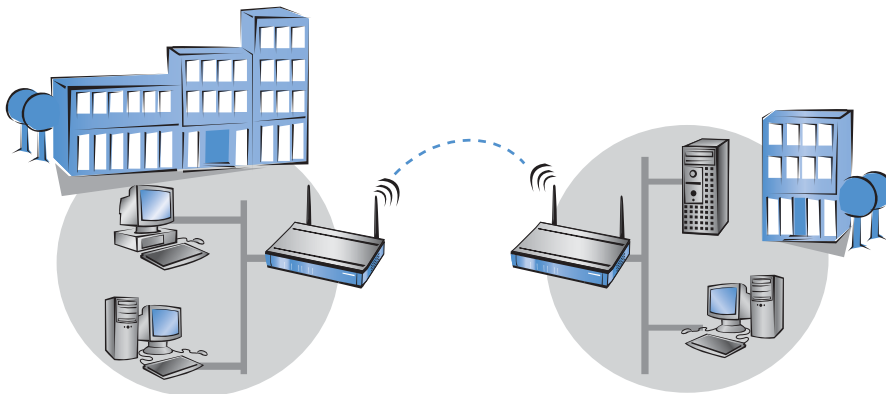


Die LANCOM Wireless Basis-Station unterstützt die VPN-Pass-Through-Funktion für beliebig viele Stationen im Funknetzwerk.

Funk-Brücke zwischen zwei Ethernet-Segmenten

Mit zwei Basis-Stationen können zwei LANs über Funk verbunden werden (Point-to-Point Modus). In diesem sogenannten Bridge-Modus werden automatisch alle Daten in das entfernte Netzwerk übertragen.

Durch den Einsatz von Richtfunkantennen (z. B. AirLancer Extender) lassen sich auch größere Distanzen sicher überbrücken. Eine zusätzliche Erhöhung der Reichweite kann durch den Einsatz weiterer Basis-Stationen erreicht werden, die im Relay-Modus zwischen den beiden LAN-Segmenten betrieben werden.



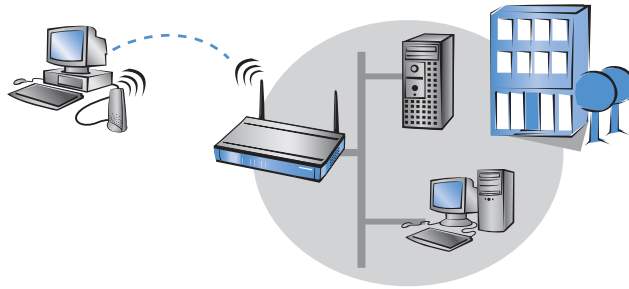
Point-to-Multipoint-Betrieb

Problemlos lassen sich bis zu sieben entfernte Netzwerk-Segmente durch Funkbrücken im sogenannten P2MP-Betrieb (Point-to-Multipoint) zu einem einheitlichen Netzwerk koppeln.

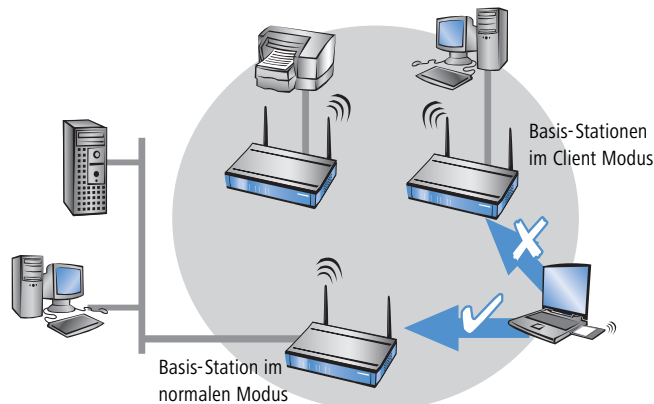
Point-to-Station-Betrieb

Im sogenannten P2Station-Betrieb (Point-to-Station) wird eine einzelne Station an ein entferntes LAN gekoppelt.

▷ Was ist ein WLAN?

**Basis-Station im Client-Modus**

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein Funk-LAN können LANCOM Basis-Stationen in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher Funk-LAN-Adapter verhalten und nicht wie eine Basis Station. Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein Funk-LAN einzubinden.



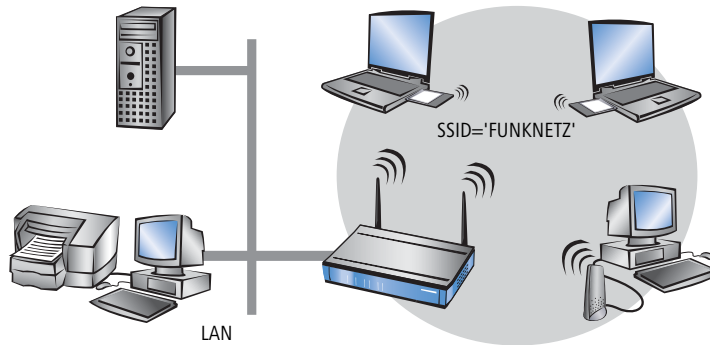
Bei einem Access Point im normalen Modus können sich weitere WLAN-Clients anmelden, bei einem Access Point im Client-Modus jedoch nicht.

Mehrere Funkzellen mit Multi-SSID

Normalerweise spannt eine Funknetzwerkkarte genau eine Funkzelle auf. Diese Funkzellen werden durch einen Netzwerknamen repräsentiert, der in der Konfiguration der Access Points und Netzwerkkarten als 'SSID' (**S**ervice **S**et **I**dentifier) eingetragen wird. Für diese Funkzelle gelten bestimmte Einstellungen, die in der Konfiguration des Access Points unter dieser SSID festgelegt werden. Zu diesen Einstellungen gehören z.B. die Übertragungsgeschwindigkeit und der erste WEP-Schlüssel, der auch als Passphrase für die 802.11i oder WPA-Verschlüsselung verwendet wird.

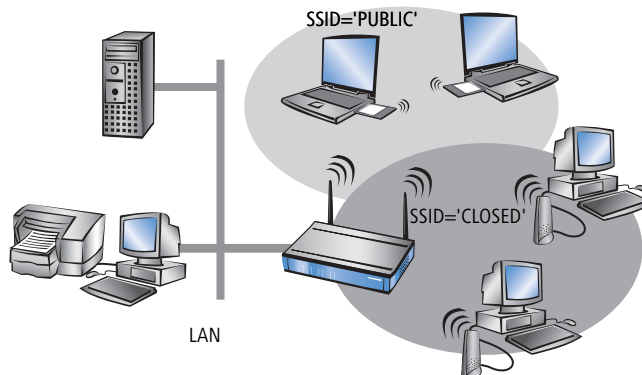
▷ Was ist ein WLAN?

Nur diejenigen Clients im Funknetzwerk, die über die passende SSID verfügen, können sich als Teilnehmer mit dieser Funkzelle verbinden und arbeiten dann mit den eingestellten Parametern. Der Access Point verhält sich also allen Clients gegenüber gleich.



In manchen Anwendungen ist es jedoch erwünscht, die Clients im Funknetzwerk in bestimmte Gruppen zu unterteilen, die auch mit speziellen Einstellungen vom Access Point behandelt werden. So kann es z.B. erforderlich sein, ein öffentlich zugängliches Funknetz ohne jegliche Verschlüsselung zu betreiben, gleichzeitig aber auch ein geschütztes, 802.11i-, WPA- oder WEP-verschlüsseltes Funknetz im geschlossenen Modus zu betreiben.

Für solche Anwendungen eignet sich die Multi-SSID-Funktion der LANCOM Access Points. Mit Hilfe dieser Funktion kann einer physikalischen WLAN-Schnittstelle eines Access Points mehr als eine SSID zugewiesen werden. Bis zu acht verschiedene, logische Funkzellen – jede mit einer eigenen SSID – können so von einer WLAN-Schnittstelle aufgespannt werden.



12.2 Entwicklung der WLAN-Sicherheit

Die WLAN-Standards WPA und 802.11i sind dabei, den in der Vergangenheit angegriffenen Ruf von WLANs bezüglich der Sicherheit wieder herzustellen. Die im originalen Standard vorgesehenen Verfahren haben sich in der Praxis als unzureichend erwiesen. Dieser Mangel führte zu einer Reihe von proprietären Erweiterungen des Standards wie 'CKIP' von Cisco oder 'KeyGuard' von Symbol Technologies, zum anderen zu Lösungen, die auf höheren Protokollschichten mit Mitteln wie PPTP oder IPSec die benötigte Sicherheit bieten. All diese Verfahren funktionieren zwar prinzipiell, bringen auf der anderen Seite jedoch Einschränkungen, z.B. bezüglich der Interoperabilität oder des Datendurchsatzes.

Mit dem im Sommer 2004 verabschiedeten Standard 802.11i hat das IEEE-Komitee das Thema 'WLAN und Sicherheit' von Grund auf neu definiert. Das Resultat sind standardisierte Methoden, die den Aufbau von sicheren und herstellerübergreifenden WLANs nach aktuellen Maßstäben ermöglichen.

Auf dem Weg vom ursprünglichen WEP des 802.11-Standards bis zu 802.11i sind dabei eine ganze Reihe von Begriffen entstanden, die teilweise eher zu einer Verwirrung und Verunsicherung der Anwender geführt haben. Dieses Kapitel soll helfen, die Begriffe zu erklären und die verwendeten Verfahren in der chronologischen Reihenfolge ihrer Entwicklung zu erläutern.

12.2.1 Einige Grundbegriffe

Auch wenn immer wieder in Zusammenhang mit Computernetzen pauschal von 'Sicherheit' gesprochen wird, so ist es doch für die folgenden Ausführungen wichtig, die dabei gestellten Forderungen etwas näher zu differenzieren.

Authentifizierung

Als ersten Punkt der Sicherheit betrachten wir den Zugangsschutz:

- ▶ Dabei handelt es sich zum einen um einen Schutzmechanismus, der nur autorisierten Nutzern den Zugang zum Netzwerk gewährt.
- ▶ Zum anderen soll aber auch sicherstellt werden, dass der Client sich mit genau dem gewünschten Access Point verbindet, und nicht mit einem von unbefugten Dritten eingeschmuggelten Access Point mit dem gleichen Netzwerk-Namen. So eine Authentifizierung kann z.B. durch Zertifikate oder Passwörter gewährleistet werden.

Authentizität

Authentizität: Nachweis der Urheberschaft von Daten und der Echtheit des Datenmaterials; die Durchführung eines solchen Nachweises bezeichnet man als Authentifizierung

Integrität

Ist der Zugang einmal gewährt, so möchte man sicherstellen, dass Datenpakete den Empfänger unverfälscht erreichen, d.h. dass niemand die Pakete verändert oder andere Daten in den Kommunikationsweg einschleusen kann. Die Manipulation der Datenpakete selbst kann man nicht verhindern; aber man kann durch geeignete Prüfsummenverfahren veränderte Pakete identifizieren und verwerfen.

Vertraulichkeit

Vom Zugangsschutz getrennt zu sehen ist die Vertraulichkeit, d.h. unbefugte Dritte dürfen nicht in der Lage sein, den Datenverkehr mitzulesen. Dazu werden die Daten verschlüsselt. Solche Verschlüsselungsverfahren sind z.B. DES, AES, RC4 oder Blowfish. Zur Verschlüsselung gehört natürlich auf der Empfängerseite eine entsprechende Entschlüsselung, üblicherweise mit dem gleichen Schlüssel (so genannte symmetrische Verschlüsselungsverfahren). Dabei ergibt sich natürlich das Problem, wie der Sender dem Empfänger den verwendeten Schlüssel erstmalig mitteilt – eine einfache Übertragung könnte von einem Dritten sehr einfach mitgelesen werden, der damit den Datenverkehr leicht entschlüsseln könnte.

Im einfachsten Fall überlässt man dieses Problem dem Anwender, d.h. man setzt die Möglichkeit voraus, dass er die Schlüssel auf beiden Seiten der Verbindung bekannt machen kann. In diesem Fall spricht man von Pre-Shared-Keys oder kurz 'PSK'.

Ausgefeiltere Verfahren kommen dann zum Einsatz, wenn der Einsatz von Pre-Shared-Keys nicht praktikabel ist, z.B. in einer über SSL aufgebauten HTTP-Verbindung – hierbei kann der Anwender nicht so einfach an den Schlüssel von einem entfernten Web-Server gelangen. In diesem Falle werden so genannte asymmetrische Verschlüsselungsverfahren wie z.B. RSA eingesetzt, d.h. zum **Entschlüsseln** der Daten wird ein anderer Schlüssel als zum **Verschlüsseln** benutzt, es kommen also Schlüsselpaare zum Einsatz. Solche Verfahren sind jedoch viel langsamer als symmetrische Verschlüsselungsverfahren, was zu einer zweistufigen Lösung führt:

- ▶ Der Sender verfügt über ein asymmetrisches Schlüsselpaar. Den öffentlichen Teil dieses Schlüsselpaares, also den Schlüssel zum **Verschlüsseln**, überträgt er an den Empfänger, z.B. in Form eines Zertifikats. Da dieser Teil des Schlüsselpaares nicht zum **Entschlüsseln** genutzt werden kann, gibt es hier keine Bedenken bzgl. der Sicherheit.
- ▶ Der Empfänger wählt einen beliebigen symmetrischen Schlüssel aus. Dieser symmetrischen Schlüssel, der sowohl zum **Ver-** als auch zum **Entschlüsseln** dient, muss nun gesichert zum Sender übertragen werden. Dazu wird er mit dem öffentlichen Schlüssel des Senders verschlüsselt und an den Sender zurückgeschickt. Der symmetrische Schlüssel kann nun ausschließlich mit dem privaten Schlüssel des Senders wieder entschlüsselt werden. Ein potenzieller Mithörer das Schlüsselaustauschs kann dieses Information aber nicht entschlüsseln, die Übertragung des symmetrischen Schlüssels ist also gesichert.

Auf diese Weise können symmetrische Schlüssel sicher über das Internet übertragen werden. In den folgenden Abschnitten werden uns solche Verfahren wieder begegnen, zum Teil auch in etwas modifizierter Form.

12.2.2 WEP

WEP ist eine Abkürzung für **Wired Equivalent Privacy**. Die primäre Zielsetzung von WEP ist die Vertraulichkeit von Daten. Im Gegensatz zu Signalen, die über Kabel übertragen werden, breiten sich Funkwellen beliebig in alle Richtungen aus – auch auf die Straße vor dem Haus und an andere Orte, wo sie gar nicht erwünscht sind. Das Problem des unerwünschten Mithörens tritt bei der drahtlosen Datenübertragung besonders augenscheinlich auf, auch wenn es prinzipiell auch bei größeren Installationen kabelgebundener Netze vorhanden ist – allerdings kann man den Zugang zu Kabeln durch entsprechende Organisation eher begrenzen als bei Funkwellen.

Das IEEE-Komitee hat bei der Entwicklung der WLAN-Sicherheitsstandards nicht geplant, ein 'perfektes' Verschlüsselungsverfahren zu entwerfen. Solche hochsicheren Verschlüsselungsverfahren werden z.B. für Electronic-Banking

▷ *Entwicklung der WLAN-Sicherheit*

verlangt und auch einsetzt – in diesen Fällen bringen allerdings die Anwendungen selber entsprechend hochwertige Verschlüsselungsverfahren mit, und es wäre unnötig, diesen Aufwand nochmals auf der Ebene der Funkübertragung zu treiben. Mit den neuen Sicherheitsstandards sollte lediglich solchen Anwendungen, die in kabelgebundenen LANs üblicherweise ohne Verschlüsselung arbeiten, eine ausreichende Sicherheit gegen das Mitlesen durch unbefugte Dritte ermöglicht werden.

WEP ist ein symmetrisches Verschlüsselungsverfahren und benutzt als Basistechnologie zur Verschlüsselung den RC4-Algorithmus, ein in anderen Bereichen bereits bekanntes und durchaus als sicher eingestuftes Verfahren. RC4 benutzt einen zwischen 8 und 2048 Bit langen Schlüssel, aus dem nach einem festgelegten Verfahren eine pseudozufällige Folge von Bytes erzeugt wird. Das zu verschlüsselnde Datenpaket wird dann sukzessive Byte für Byte mit diesem Byte-Strom verschlüsselt. Der Empfänger wiederholt einfach diesen Vorgang mit dem gleichen Schlüssel und damit der gleichen Folge, um wieder das ursprüngliche Datenpaket zu erhalten.

RC4 hat aber einen gravierenden Nachteil: man darf einen bestimmten RC4-Schlüssel nur einmal für ein einziges Paket verwenden, da aus zwei verschiedenen Paketen, die mit dem gleichen RC4-Schlüssel kodiert wurden, möglicherweise die ursprünglichen Daten wiederhergestellt werden könnten. Da der Schlüssel für die Kodierung nicht vom Anwender für jedes Datenpaket neu eingetragen werden kann, kombiniert WEP diesen Schlüssel mit einem weiteren, internen Schlüssel (Initial Vector=IV). Dieser wird automatisch von Paket zu Paket gewechselt.

Der IEEE-Standard sah ursprünglich eine relativ kurze Schlüssellänge von 40 Bit vor, die sich wahrscheinlich an den damals existierenden US-Exportbeschränkungen für starke Kryptographie orientierte – diese Variante wird unter Einbezug der 24 Bit des IV meist als WEP64 bezeichnet. Die meisten WLAN-Karten unterstützen heutzutage eine Variante, bei der Anwender einen 104 Bit langen Schlüssel konfigurieren kann, was einen 128 Bit langen RC4-Schlüssel ergibt – folgerichtig wird dies oft als WEP128 bezeichnet. Seltener finden sich Schlüssellängen von 128 Bit (WEP152) oder 232 Bit (WEP256). RC4 kann zwar prinzipiell mit Schlüssellängen bis zu 2048 Bit arbeiten (WEP-Schlüssel bis zu 2024 Bit), in der Praxis stoßen die Schlüssellängen an die einfache Grenze, bis zu der ein Anwender die Zahlenkolonnen noch fehlerfrei eingeben kann.

Der IEEE-Standard sieht vor, dass in einem WLAN bis zu vier verschiedene WEP-Schlüssel existieren können. Der Sender kodiert in das verschlüsselte Paket neben dem Initial Vector die Nummer des verwendeten WEP-Schlüssels, so dass der Empfänger den passenden Schlüssel verwenden kann. Die Idee dahinter war, dass sich so alte Schlüssel in einem WLAN graduell gegen neue Schlüssel austauschen lassen, indem Stationen, die den neuen Schlüssel noch nicht erhalten haben, für eine Übergangszeit noch einen alten Schlüssel weiter verwenden können.

Eine der Hauptschwächen von WEP ist der viel zu kurze Initial Vector. Wie bereits erwähnt, ist die Wiederverwendung eines Schlüssels bei RC4 eine große Sicherheitslücke, was bei einer Länge von nur 24 Bit je nach Datenrate schon nach wenigen Stunden der Fall ist. Da zudem aus bestimmten Stellen der verschlüsselten Datenpakete sehr schnell Rückschlüsse auf die verwendeten Schlüssel gezogen werden können, muss ein Mithörer nur einen sehr kleinen Teil des Datenverkehrs mit spezialisierte Sniffer-Tools auswerten, um die Schlüssel knacken zu können. Diese Schwachstellen degradierten WEP leider zu einem Verschlüsselungsverfahren, das bestenfalls zum Schutz eines Heimnetzwerkes gegen 'zufällige Lauscher' taugt.

12.2.3 WEPplus

Wie im vorangegangenen Abschnitt ausgeführt, ist die Verwendung 'schwacher' IV-Werte das Problem gewesen, welches das WEP-Verfahren am stärksten schwächt. Ein erster 'Schnellschuss', um WLANs gegen solche Programme zu sichern, war die einfache Überlegung, dass die schwachen IV-Werte bekannt sind und man sie beim Verschlüsseln einfach überspringen kann – da der verwendete IV ja im Paket mit übertragen wird, ist so eine Vorgehensweise voll kompatibel gegenüber WLAN-Karten, die diese WEPplus getaufte Erweiterung nicht kennen. Eine echte Verbesserung der Sicherheit erhält man natürlich erst dann, wenn alle Partner in einem WLAN diese Methode benutzen.

Ein potentieller Angreifer ist in einem mit WEPplus ausgestatteten Netzwerk wieder darauf angewiesen, den ganzen Datenverkehr mitzuschneiden und auf IV-Wiederholungen zu warten – es reicht nicht mehr aus, nur auf die wenigen Pakete mit schwachen IVs zu warten. Das legt die Latte für einen Angreifer schon wieder höher. WEPplus ist daher bei sachlicher Betrachtung eine leichte Verbesserung – für den Heimgebrauch geeignet, solange man häufig genug neue Schlüssel konfiguriert. Für den Einsatz im professionellen Umfeld reicht das allerdings noch nicht.

12.2.4 EAP und 802.1x

Es liegt auf der Hand, dass ein 'Zusatz' wie WEPplus das grundsätzliche Problem des zu kurzen IVs nicht aus der Welt schaffen kann, ohne das Format der Pakete auf dem WLAN zu ändern und damit inkompatibel zu allen bisher existierenden WLAN-Karten zu werden. Es gibt aber eine Möglichkeit, mehrere der aufgetauchten Probleme mit einer zentralen Änderung zu lösen: man verwendet nicht mehr wie bisher die fest konfigurierten WEP-Schlüssel und handelt sie stattdessen dynamisch aus. Als dabei anzuwendendes Verfahren hat sich dabei das Extensible Authentication Protocol durchgesetzt. Wie der Name schon nahelegt, ist der ursprüngliche Zweck von EAP die Authentifizierung, d.h. der geregelte Zugang zu einem WLAN – die Möglichkeit, einen für die folgende Sitzung gültigen WEP-Schlüssel zu installieren, fällt dabei sozusagen als Zusatznutzen ab. Abbildung 2 zeigt den grundsätzlichen Ablauf einer mittels EAP geschützten Sitzung.

▷ Entwicklung der WLAN-Sicherheit

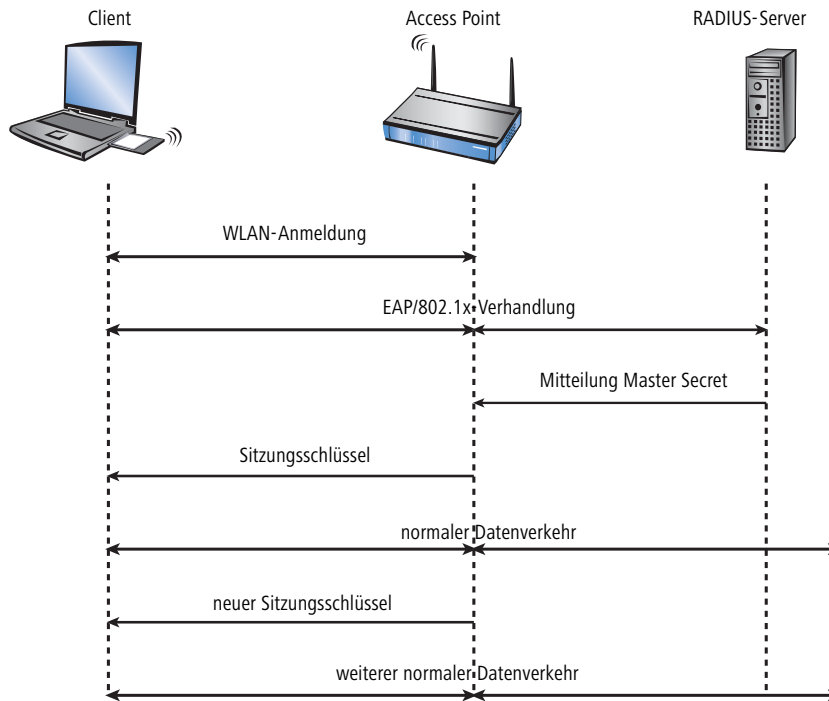


Abbildung 2: Schematischer Ablauf einer WLAN-Sitzung mit EAP/802.1x

In der ersten Phase meldet sich der Client wie gewohnt beim Access Point an und erreicht einen Zustand, in dem er bei normalem WEP oder WEPplus jetzt über den Access Point Daten senden und empfangen könnte – nicht so jedoch bei EAP, denn in diesem Zustand verfügt der Client ja noch über keinerlei Schlüssel, mit denen man den Datenverkehr vor Abhören schützen könnte. Stattdessen steht der Client aus Sicht des Access Points in einem 'Zwischenzustand', in dem er nur bestimmte Pakete vom Client weiter leitet, und diese auch nur gerichtet an einen Authentifizierungs-Server. Bei diesen Paketen handelt es sich um das bereits erwähnte EAP/802.1x. Der Access Point packt diese Pakete in RADIUS-Anfragen um und reicht sie an den Authentifizierungs-Server weiter. Umgekehrt wandelt der Access Point darauf vom RADIUS-Server kommende Antworten wieder in EAP-Pakete um und reicht sie an den Client weiter.

Der Access Point dient dabei sozusagen als 'Mittelsmann' zwischen Client und Server: er muss den Inhalt dieser Pakete nicht prüfen, er stellt lediglich sicher, dass kein anderer Datenverkehr von oder zu dem Client erfolgen kann. Über den so gebildeten „Tunnel“ durch den Access Point versichern sich Client und Server nun ihrer gegenseitigen Authentizität, d.h. der Server überprüft die Zugangsberechtigung des Clients zum Netz, und der Client überprüft, ob er wirklich mit dem richtigen Netz verbunden ist. Von Hackern aufgestellte „wilde“ Access Points lassen sich so erkennen.

Es gibt eine ganze Reihe von Authentifizierungsverfahren, die in diesem Tunnel angewendet werden können. Ein gängiges (und von Windows XP unterstütztes) Verfahren ist z.B. TLS, bei dem Server und Client Zertifikate austau-

schen, ein anderes ist TTLS, bei dem nur der Server ein Zertifikat liefert – der Client authentifiziert sich über einen Benutzernamen und ein Passwort.

Nachdem die Authentifizierungsphase abgeschlossen ist, ist gleichzeitig ein auch ohne WEP-Verschlüsselung gesicherter Tunnel entstanden, in den im nächsten Schritt der Access Point eingebunden wird. Dazu schickt der RADIUS-Server das sogenannte 'Master Secret', einen während der Verhandlung berechneten Sitzungsschlüssel, zum Access Point. Das LAN hinter dem Access Point wird in diesem Szenario als sicher betrachtet, von daher kann diese Übertragung im Klartext erfolgen.

Mit diesem Sitzungsschlüssel übernimmt der Access Point jetzt den gebildeten Tunnel und kann ihn nutzen, um dem Client die eigentlichen WEP-Schlüssel mitzuteilen. Je nach Fähigkeiten der Access-Point-Hardware kann das ein echter Sitzungsschlüssel sein (d.h. ein WEP-Schlüssel, der nur für Datenpakete zwischen dem Access Point und genau diesem Client benutzt wird) oder ein sogenannter Gruppenschlüssel, den der Access Point für die Kommunikation mit mehreren Clients benutzt. Klassische WEP-Hardware kennt meistens nur Gruppenschlüssel, nämlich die im Kapitel über WEP erwähnten vier.

Der besondere Vorteil dieses Verfahrens ist es, dass der Access Point über den EAP-Tunnel die WEP-Schlüssel regelmäßig wechseln kann, d.h. ein sogenanntes Rekeying durchführen kann. Auf diese Weise lassen sich WEP-Schlüssel gegen andere ersetzen, lange bevor sie durch IV-Kollisionen Gefahr laufen, geknackt zu werden. Eine gängige 'Nutzungszeit' für so einen WEP-Schlüssel sind z.B. 5 Minuten.

Nachteilig ist bei diesem Verfahren seine Komplexität: Die Pflege des zentralen RADIUS-Servers und der dort gespeicherten Zertifikate ist im allgemeinen nur in größeren Einrichtungen mit separater IT-Abteilung möglich – für den Heimgebrauch oder kleinere Unternehmen ist es weniger geeignet. Diese praktischen Hürden haben den Einsatz von EAP/802.1x daher bisher auf professionellen Bereich beschränkt – der Heimanwender musste sich weiterhin mit bestenfalls WEPplus begnügen, oder sich selber auf Anwendungsebene um das Sicherheitsproblem kümmern.

12.2.5 TKIP und WPA

Wie in den letzten Abschnitten klar geworden ist, ist der WEP-Algorithmus prinzipiell fehlerhaft und unsicher; die bisherigen Maßnahmen waren im wesentlichen entweder 'Schnellschüsse' mit nur geringen Verbesserungen oder so kompliziert, dass sie für den Heimbutzer oder kleine Installationen schlicht unpraktikabel sind.

Die IEEE hatte nach Bekanntwerden der Probleme mit WEP mit der Entwicklung des Standards IEEE 802.11i begonnen. Als Zwischenlösung wurde von der WiFi-Alliance der 'Standard' Wifi Protected Access (WPA) definiert. WPA setzt auf die folgenden Änderungen:

- ▶ TKIP und Michael als Ersatz für WEP
- ▶ Ein standardisiertes Handshake-Verfahren zwischen Client und Access Point zur Ermittlung/Übertragung der Sitzungsschlüssel.
- ▶ Ein vereinfachtes Verfahren zur Ermittlung des im letzten Abschnitt erwähnten Master Secret, das ohne einen RADIUS-Server auskommt.
- ▶ Aushandlung des Verschlüsselungsverfahrens zwischen Access Point und Client.

▷ *Entwicklung der WLAN-Sicherheit***TKIP**

TKIP steht für **T**emporal **K**ey **I**ntegrity **P**rotocol. Wie der Name nahelegt, handelt es sich dabei um eine Zwischenlösung, die nur übergangsweise bis zur Einführung eines wirklich starken Verschlüsselungsverfahrens genutzt werden soll, aber trotzdem mit dem Problemen von WEP aufräumt. Eine Anforderung an dieses Verfahren war die Kompatibilität mit existierender WEP/RC4-Hardware.

Bei der Verschlüsselung werden bekannte Bestandteile des WEP-Verfahrens weiter verwendet, aber an den entscheidenden Stellen um den „Michael-Hash“ zur besseren Verschlüsselung und das TKIP-Verfahren zur Berechnung der RC4-Schlüssel erweitert. Desweiteren ist der intern hochgezählte und im Paket im Klartext übertragene IV statt 24 jetzt 48 Bit lang – damit ist das Problem der sich wiederholenden IV-Werte praktisch ausgeschlossen.

Als weiteres Detail mischt TKIP in Berechnung der Schlüssel auch noch die MAC-Adresse des Senders ein. Auf diese Weise ist sichergestellt, dass eine Verwendung gleicher IVs von verschiedenen Sendern nicht zu identischen RC4-Schlüsseln und damit wieder zu Angriffsmöglichkeiten führt.

Der Michael-Hash stellt jedoch keine besonders hohe kryptographische Hürde dar: kann der Angreifer den TKIP-Schlüssel brechen oder verschlüsselte Pakete durch Modifikationen ähnlich wie bei WEP an der CRC-Prüfung vorbeischieben, bleiben nicht mehr allzu viele Hürden zu überwinden. WPA definiert aus diesem Grund Gegenmaßnahmen, wenn eine WLAN-Karte mehr als zwei Michael-Fehler pro Minute erkennt: sowohl Client als auch Access Point brechen dann für eine Minute den Datentransfer ab und handeln danach TKIP- und Michael-Schlüssel neu aus.

Der Key-Handshake

Bereits bei der Besprechung von 802.1x wurde dargestellt, dass EAP/802.1x die Möglichkeit bietet, dem Client beim Beginn einer Sitzung die dafür gültigen Schlüssel mitzuteilen. WPA stellt dies jetzt auf eine standardisierte Grundlage, und berücksichtigt dabei auch die von modernen Access Points gegebene Möglichkeit, neben den vier 'globalen' Schlüsseln auch noch für jeden eingebuchten Client einen Session-Key auszuhandeln, der exklusiv für Datenpakete von oder zu diesem Client benutzt wird. Beim Key-Handshake werden unter WPA zunächst die Pairwise Keys und dann die Group Keys ausgetauscht.

Nach erfolgreichem Group-Key-Handshake kann der Access Point den Client für den normalen Datentransfer freischalten. Es steht dem Access Point dabei frei, auch weiterhin während der Sitzung über solche Pakete ein Rekeying durchzuführen. Prinzipiell könnte sogar der Client das Rekeying vom Access Point anfordern.

WPA berücksichtigt auch den Fall älterer WLAN-Hardware, in dem der Access Point keine Pairwise-Keys unterstützt, sondern nur Group-Keys. Die erste Phase des Handshakes läuft in diesem Fall genauso ab wie vorher, nur führt dies nicht zu der Installation eines Pairwise-Keys – der Group-Key-Handshake läuft weiterhin im Klartext ab, eine Verschlüsselung in den EAP-Paketen selber verhindert aber, dass ein Angreifer die Schlüssel einfach mitlesen kann.

WPA mit Passphrase

Der im vorigen Abschnitt beschriebene Handshake läuft bei WPA grundsätzlich ab, d.h. der Anwender wird niemals selber irgendeine TKIP- oder Michael-Schlüssel definieren müssen. In Umgebungen, in denen kein RADIUS-Server zur Erteilung des Master-Secrets vorhanden ist (z.B. bei kleinere Firmen oder Heimanwendern) sieht WPA deshalb neben der Authentifizierung über einen RADIUS-Server noch das PSK-Verfahren vor; dabei muss der Anwender sowohl auf dem Access Point als auch auf allen Stationen eine zwischen 8 und 32 Zeichen lange Passphrase einge-

ben, aus der zusammen mit der verwendeten SSID das Master-Secret über ein Hash-Verfahren berechnet wird. Das Master Secret ist in so einem PSK-Netz also konstant, trotzdem ergeben sich immer unterschiedliche TKIP-Schlüssel. In einem PSK-Netz hängen – ähnlich wie bei klassischem WEP – sowohl Zugangsschutz als auch Vertraulichkeit davon ab, dass die Passphrase nicht in unbefugte Hände gerät. Solange dies aber gegeben ist, bietet WPA-PSK eine deutlich höhere Sicherheit gegen Einbrüche und Abhören als jede WEP-Variante. Für größere Installationen, in denen eine solche Passphrase einem zu großen Nutzerkreis bekannt gemacht werden müsste, als dass sie geheimzuhalten wäre, wird EAP/802.1x in Zusammenhang mit dem hier beschriebenen Key-Handshake genutzt.

Verhandlung des Verschlüsselungsverfahrens

Da die ursprüngliche WEP-Definition feste Schlüssellänge von 40 Bit vorschrieb, musste bei der Anmeldung eines Clients an einem Access Point lediglich angezeigt werden, ob eine Verschlüsselung genutzt wird oder nicht. Bereits bei Schlüssellängen von mehr als 40 Bit muss aber auch die Länge des verwendeten Schlüssels bekannt gegeben werden. WPA stellt einen Mechanismus bereit, mit dem sich Client und Access Point über das zu verwendende Verschlüsselungs- und Authentifizierungsverfahren verständigen können. Dabei werden folgenden Informationen bereitgestellt:

- ▶ Das in diesem Netz zu verwendende Verschlüsselungsverfahren für Broadcasts (also die Art des Group Keys). Jeder Client, der sich in ein WPA-WLAN einbuchen will, muss dieses Verfahren unterstützen. Hier ist neben TKIP auch noch WEP zugelassen, um gemischte WEP/WPA-Netze zu unterstützen – in einem reinen WPA-Netz wird man aber TKIP wählen.
- ▶ Eine Liste von Verschlüsselungsverfahren, die der Access Point für den Pairwise Key anbietet – hier ist WEP explizit nicht mehr erlaubt.
- ▶ Eine Liste von Authentifizierungsverfahren, über die sich ein Client gegenüber dem WLAN als zugangsberechtigt zeigen kann – mögliche Verfahren sind im Moment EAP/802.1x oder PSK.

Wie erwähnt, sieht der ursprüngliche WPA-Standard einzig TKIP/Michael als verbessertes Verschlüsselungsverfahren vor. Mit der Weiterentwicklung des 802.11i-Standards wurde das weiter unten beschriebene AES/CCM-Verfahren hinzugenommen. So ist es heutzutage in einem WPA-Netz möglich, dass einige Clients über TKIP mit dem Access Point kommunizieren, andere Clients jedoch über AES.

12.2.6 AES und 802.11i

Mitte 2004 wurde der lang erwartete Standard 802.11i vom IEEE verabschiedet, der das ganze Sicherheitskonzept von WLAN auf eine neue Basis stellt. Wie im vorigen Abschnitt erwähnt, hat WPA bereits eine ganze Reihe von Konzepten in 802.11i vorweggenommen – deshalb sollen in diesem Abschnitt nur die Komponenten beschrieben werden, die gegenüber WPA neu sind.

AES

Die augenfälligste Erweiterung betrifft die Einführung eines neuen Verschlüsselungsverfahrens, nämlich AES-CCM. Wie der Name schon andeutet, basiert dieses Verschlüsselungsverfahren auf dem DES-Nachfolger AES, im Gegensatz zu WEP und TKIP, die beide auf RC4 basieren. Da nur die neueste Generation von WLAN-Chips AES-Hardware

▷ *Entwicklung der WLAN-Sicherheit*

enthält, definiert 802.11i auch weiterhin TKIP, allerdings mit umgekehrtem Vorzeichen: eine 802.11i-standardkonforme Hardware muss AES unterstützen, während TKIP optional ist – bei WPA war es genau umgekehrt.

Der Zusatz CCM bezieht sich auf die Art und Weise, wie AES auf WLAN-Pakete angewendet wird. Das Verfahren ist insgesamt recht kompliziert, weshalb CCM sinnvoll eigentlich nur in Hardware implementiert werden wird – software-basierte Implementierungen sind zwar möglich, führen aber auf den üblicherweise in Access Points eingesetzten Prozessoren zu erheblichen Geschwindigkeitseinbußen.

Im Gegensatz zu TKIP benötigt AES nur noch einen 128 Bit langen Schlüssel, mit dem sowohl die Verschlüsselung als auch der Schutz gegen unerkanntes Verändern von Paketen erreicht wird. Des Weiteren ist CCM voll symmetrisch, d.h. es wird der gleiche Schlüssel in beide Kommunikationsrichtungen angewendet – eine standardkonforme TKIP-Implementierung hingegen verlangt die Verwendung unterschiedlicher Michael-Schlüssel in Sende- und Empfangsrichtung, so dass CCM in seiner Anwendung deutlich unkomplizierter ist als TKIP.

Ähnlich wie TKIP verwendet CCM einen 48 Bit langen Initial Vector in jedem Paket – eine IV-Wiederholung ist damit in der Praxis ausgeschlossen. Wie bei TKIP merkt der Empfänger sich den zuletzt benutzten IV und verwirft Pakete mit einem IV, der gleich oder niedriger als der Vergleichswert ist.

Prä-Authentifizierung und PMK-Caching

802.11i soll den Einsatz von WLAN auch für Sprachverbindungen (VoIP) in Unternehmensnetzen erlauben. Vor allem in Zusammenhang mit WLAN-basierten schnurlosen Telefonen kommt einem schnellen Roaming, d.h. dem Wechsel zwischen Access Points ohne längere Unterbrechungen, eine besondere Bedeutung zu. Bei Telefongesprächen sind bereits Unterbrechungen von wenigen 100 Millisekunden störend, allerdings kann eine vollständige Authentifizierung über 802.1x inklusive der folgenden Schlüsselverhandlung mit dem Access Point deutlich länger dauern.

Als erste Maßnahme wurde deshalb das sogenannte PMK-Caching eingeführt. Das PMK dient nach einer 802.1x-Authentifizierung zwischen Client und Access Point als Basis für die Schlüsselverhandlung. In VoIP-Umgebungen ist es denkbar, dass ein Anwender sich zwischen einer relativ kleinen Zahl von Access Points hin- und herbewegt. Dabei wird es vorkommen, dass ein Client wieder zu einem Access Point wechselt, an dem er bereits früher einmal angemeldet war. In so einem Fall wäre es unsinnig, die ganze 802.1x-Authentifizierung noch einmal zu wiederholen. Aus diesem Grund kann der Access Point das PMK mit einer Kennung, der sogenannten PMKID, versehen, die er an den Client übermittelt. Bei einer Wiederanmeldung fragt der Client mittels der PMKID, ob er dieses PMK noch vorrätig hat. Falls ja, kann die 802.1x-Phase übersprungen werden und die Verbindung ist schnell wieder verfügbar. Diese Optimierung greift naturgemäß nicht, wenn das PMK in einem WLAN aufgrund einer Passphrase berechnet wird, denn dann ist es ja ohnehin überall gleich und bekannt.

Eine weitere Maßnahme erlaubt auch für den Fall der erstmaligen Anmeldung eine Beschleunigung, sie erfordert aber etwas Vorausschau vom Client: dieser muss bereits im Betrieb eine schlechter werdende Verbindung zum Access Point erkennen und einen neuen Access Point selektieren, während er noch Verbindung zum alten Access Point hat. In diesem Fall hat er die Möglichkeit, die 802.1x-Verhandlung über den alten Access Point mit dem neuen Access Point zu führen, was wiederum die 'Totzeit' um die Zeit der 802.1x-Verhandlung verkürzt.

12.2.7 Fazit

Nach dem Bekanntwerden der Sicherheitslücken in der WEP-Verschlüsselung, den kurzfristigen Lösungsversuchen wie WEPplus und Zwischenschritten wie WPA hat das IEEE-Komitee den neuen WLAN-Sicherheitsstandard 802.11i vorgelegt. Das bei WPA verwendete TKIP-Verfahren basiert auf dem schon älteren RC4-Algorithmus, auf dem schon WEP aufbaute. Erst mit AES wird der wichtige und endgültige Schritt zu einem wirklich sicheren Verschlüsselungsverfahren vollzogen. Die bekannten praktischen und theoretischen Sicherheitslücken der Vorgängerverfahren gehören mit 802.11i/AES der Vergangenheit an.

Das AES-Verfahren bietet genügend Sicherheit, um die notwendigen Spezifikationen des Federal Information Standards (FIPS) 140-2 einzuhalten, die von vielen staatlichen Stellen gefordert werden.

LANCOM Systems verwendet in seinen 54MBit/s-Produkten den Atheros Chipsatz mit einem Hardware-AES-Beschleuniger. Dadurch ist die höchstmögliche Verschlüsselung ohne Performanceverluste gewährleistet.

Mit dem benutzerfreundlichen Pre-Shared-Key-Verfahren (Eingabe einer Passphrase von 8-63 Zeichen Länge) ist 802.11i für jedermann schnell und einfach einzurichten. In professionellen Infrastrukturen mit einer großen Anzahl von Nutzern kann mit 802.1x und RADIUS-Servern gearbeitet werden.

Im Zusammenspiel mit weiteren Einstellungsmöglichkeiten wie Multi-SSID und VLAN-Tagging ist es möglich, rundum sichere und gleichzeitig für mehrere Benutzergruppen angepasste Netze mit verschiedenen Sicherheitsstufen anzubieten.

- ▶ VLAN-Tagging ist ab LCOS Version 3.32 verfügbar.
- ▶ Multi-SSID ist ab LCOS 3.42 verfügbar.
- ▶ LANCOM Systems bietet ab der LCOS Version 3.50 das PSK-Verfahren an.
- ▶ 802.1x wird ab der LCOS-Version 3.52 unterstützt.

12.3 Absicherung des Funknetzwerks

Ein drahtloses LAN verwendet – anders als ein herkömmliches LAN – kein Kabel, sondern die Luft als Übertragungsmedium. Da dieses Medium für jeden „Lauscher“ leicht zugänglich ist, nimmt die Abschirmung der Daten in einem WLAN einen großen Stellenwert ein.

Je nachdem, wie kritisch die Sicherheit der auf dem WLAN übertragenen Daten eingestuft wird, können Sie die folgenden Schritte zur Absicherung Ihres Funknetzwerks unternehmen:

- ① Aktivieren Sie die „Closed-Network-Funktion“. Damit werden alle WLAN-Clients ausgeschlossen, die mit der allgemeinen SSID „Any“ einen Verbindungsaufbau versuchen und die nicht die eingestellten SSIDs kennen. (‘Netzwerkeinstellungen’ →Seite 377)
- ② Verwenden Sie nicht die Standard-SSID Ihres Access Points. Wählen Sie als SSID nur solche Namen, die nicht direkt erraten werden können. Der Name Ihrer Firma ist z.B. kein besonders sichere SSID. (‘Netzwerkeinstellungen’ →Seite 377)
- ③ Wenn Sie genau wissen, welche Funknetzwerkarten auf Ihr WLAN zugreifen dürfen, dann tragen Sie die MAC-Adressen dieser Karten in die Access-Control-List ein und schließen Sie alle anderen Karten von der Kommuni-

▷ Absicherung des Funknetzwerks

kation mit dem Access Point aus. Damit wird der Zugriff auf das WLAN auf die Clients mit den eingetragenen MAC-Adressen beschränkt. ('Access Control List' →Seite 359)

- ④ Verschlüsseln Sie die im WLAN übertragenen Daten. Aktivieren Sie dazu die maximal mögliche Verschlüsselung (802.11i mit AES, WPA oder WEP) und tragen Sie entsprechenden Schlüssel bzw. Passphrases im Access Point und in den WLAN-Clients ein ('Verschlüsselungs-Einstellungen' →Seite 361 und 'WEP-Gruppen-Schlüssel' →Seite 364).
- ⑤ Ändern Sie regelmäßig die WEP-Schlüssel. Wechseln Sie dazu den Standardschlüssel ('Verschlüsselungs-Einstellungen' →Seite 361) in der Konfiguration. Alternativ können Sie über einen Cron-Job die Schlüssel automatisch z.B. jeden Tag ändern lassen ('Zeitautomatik für LCOS-Befehle' →Seite 433). Die Passphrases für 802.11i oder WPA müssen nicht regelmäßig gewechselt werden, da bereits regelmäßig im Betrieb neue Schlüssel pro Verbindung verwendet werden. Nicht nur deswegen ist die Verschlüsselung per 802.11i/AES oder WPA/TKIP wesentlich sicherer als das WEP-Verfahren.
- ⑥ Falls es sich bei den übertragenen Daten um extrem sicherheitsrelevante Informationen handelt, können Sie bei der Verwendung der WEP-Verschlüsselung zusätzlich zur besseren Authentifizierung der Clients das 802.1x-Verfahren aktivieren ('IEEE 802.1x/EAP' →Seite 381) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' →Seite 382). In Sonderfällen ist auch eine Kombination dieser beiden Mechanismen möglich.



Bitte lesen Sie bei Interesse auch die Schrift „Sicherheit im Funk-LAN“ vom Bundesministerium für Sicherheit in der Informationstechnik. Sie finden es als PDF-Dokument auf unserer Webseite www.lancom.de unter **Support ▶ FAQ**.

12.3.1 LEPS – LANCOM Enhanced Passphrase Security

LEPS behebt die Unsicherheit von globalen Passphrases

Mit den modernen Verschlüsselungsverfahren WPA und IEEE 802.11i kann der Datenverkehr im WLAN deutlich besser als mit WEP gegen unerwünschte „Lauschangriffe“ geschützt werden. Die Verwendung einer Passphrase als zentraler Schlüssel ist sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1x-Installationen wird nicht benötigt. Dennoch birgt die Verwendung der abhörsicheren Verfahren WPA und IEEE 802.11i einige Schwachstellen:

- ▶ Eine Passphrase gilt **global** für **alle** WLAN-Clients
- ▶ Die Passphrase kann durch Unachtsamkeit ggf. an Unbefugte weitergegeben werden
- ▶ Mit der „durchgesickerten“ Passphrase kann jeder Angreifer in das Funknetzwerk eindringen

In der Praxis bedeutet das: Falls die Passphrase „verloren geht“ oder ein Mitarbeiter mit Kenntnis der Passphrase das Unternehmen verlässt, müsste aus Sicherheitsaspekten die Passphrase im Access Point geändert werden – und damit auch in allen WLAN-Clients. Da das nicht immer sichergestellt werden kann, würde sich also ein Verfahren anbieten, bei dem nicht eine globale Passphrase für alle WLAN-Clients gemeinsam gilt, sondern für jeden Benutzer im WLAN eine eigene Passphrase konfiguriert werden kann. In diesem Fall muss z.B. beim Ausscheiden eines Mitarbeiters aus

dem Unternehmen nur seine „persönliche“ Passphrase gelöscht werden, alle anderen behalten ihre Gültigkeit und Vertraulichkeit.

Mit LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeidet.

Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL (Access Control List) eine **individuelle** Passphrase zugeordnet – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA oder 802.11i verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. LEPS funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adapttern, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.



Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

Konfiguration

Bei der Konfiguration von LEPS wird lediglich jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dazu wird der MAC-Filter positiv eingestellt, d.h. die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

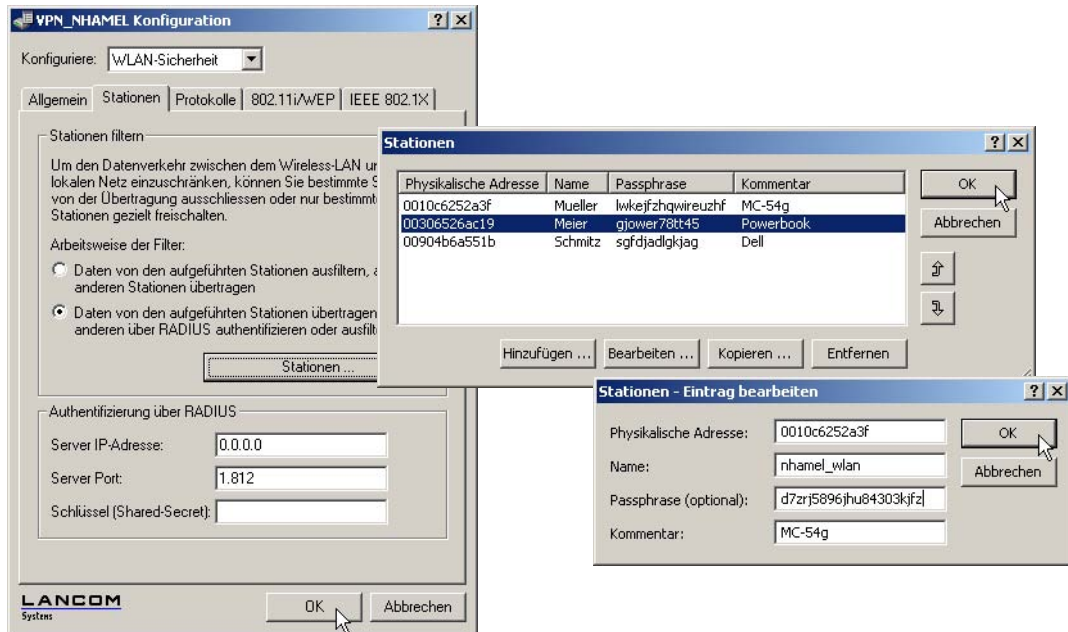


Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Liste der im WLAN zugelassenen Stationen im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen**.

▷ Absicherung des Funknetzwerks



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Zugangs-Liste für das Funknetzwerk auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WLAN ► Zugangs-Liste
Terminal/Telnet	Setup/WLAN/Zugangs-Liste

12.3.2 Standard-WEP-Verschlüsselung

Ab LCOS Version 4.0 ist für jedes unkonfigurierte Gerät standardmäßig eine WEP128-Verschlüsselung aktiviert.

Wenn Ihr Gerät über eine oder mehrere WLAN-Schnittstellen verfügt, können Sie es von einem Rechner mit WLAN-Karte aus auch „drahtlos“ konfigurieren. Um mit einem WLAN-Client eine Verbindung zu einem neuen LANCOM Access Point zur drahtlosen Konfiguration herzustellen, muss im WLAN-Client der 13-stellige Standard-WEP-Schlüssel eingetragen werden.

Der Standard-WEP-Schlüssel setzt sich aus dem Anfangsbuchstaben „L“ gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057“. Sie finden Sie LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie nur die als „MAC-Adresse“ gekennzeichnete Zeichenkette, die mit „00A057“ beginnt. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die LAN-MAC-Adresse!



Für ein Gerät mit der LAN-MAC-Adresse „00A0570FB9BF“ lautet der Standard-WEP-Schlüssel also „L00A0570FB9BF“. Dieser Schlüssel ist in den 'Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1' eingetragen.



Um mit einem WLAN-Client eine Verbindung zu einem neuen (unkonfigurierten) LANCOM Access Point herzustellen, muss im WLAN Client die WEP128-Verschlüsselung aktiviert und der 13-stellige Standard-WEP-Schlüssel eingetragen werden wie oben beschrieben.

12.4 Konfiguration der WLAN-Parameter

Die Einstellungen für die Funknetzwerke können an verschiedenen Stellen in der Konfiguration vorgenommen werden:

- ▶ Manche Parameter betreffen die physikalische WLAN-Schnittstelle. Einige LANCOM-Modelle verfügen über eine WLAN-Schnittstelle, andere Modelle haben die Möglichkeit, auch eine zweite WLAN-Karte zu verwenden. Die Einstellungen für die physikalischen WLAN-Schnittstellen gelten für alle logischen Funknetzwerke, die mit dieser Karte aufgespannt werden. Zu diesen Parametern gehören z.B. die Sendeleistung der Antenne und die Betriebsart der WLAN-Karte (Access Point oder Client).
- ▶ Andere Parameter beziehen sich nur auf die jeweiligen logischen Funknetze, die mit einem physikalischen Interface aufgespannt werden. Dazu gehört z.B. die SSID oder die Aktivierung der Verschlüsselung, entweder 802.11i mit AES oder WPA mit TKIP oder WEP.
- ▶ Eine dritte Gruppe von Parametern hat zwar Auswirkungen auf den Betrieb des Funknetzwerks, ist aber nicht **nur** für WLANs von Bedeutung. Dazu gehören z.B. die Protokollfilter in der LAN-Bridge.

12.4.1 WLAN-Sicherheit

In diesem Konfigurationsbereich schränken Sie die Kommunikation der Teilnehmer im Funknetzwerk ein. Dazu wird die Datenübertragung zwischen bestimmten Teilnehmer-Gruppen, nach einzelnen Stationen oder nach verwendetem Protokoll begrenzt. Außerdem werden hier die Schlüssel für die jeweilige Verschlüsselung im WLAN eingestellt.

Allgemeine Einstellungen

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Die zugelassene Kommunikation können Sie für alle physikalischen und logischen Netzwerke gemeinsam zentral einstellen und dabei die drei folgenden Fälle unterscheiden:

Kommunikation der WLAN-Clients untereinander

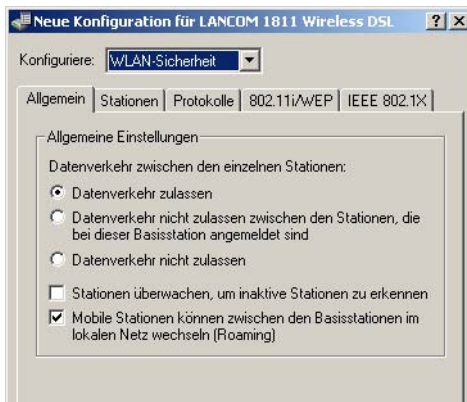
▷ Konfiguration der WLAN- Parameter

- ▶ Datenverkehr zulassen: Bei dieser Einstellung können alle WLAN-Clients auch mit den anderen Stationen im eigenen und in den anderen erreichbaren Funknetzwerken kommunizieren.
- ▶ Datenverkehr nicht zulassen zwischen Stationen, die bei diesem Access Point angemeldet sind: In diesem Fall können die WLAN-Clients nur mit den mobilen Stationen in anderen erreichbaren Funknetzwerken kommunizieren, nicht jedoch mit den Stationen im eigenen WLAN.
- ▶ Datenverkehr nicht zulassen: Mit der letzten Variante schließen Sie die Kommunikation der WLAN-Clients untereinander völlig aus.

Roaming Neben der Kommunikation der Clients untereinander kann hier auch eingestellt werden, ob die mobilen Stationen in die Funkzellen eines benachbarten Access Points wechseln (roamen) können.

Überwachung der Stationen Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der Access Point zur Überwachung in regelmäßigen Abständen Pakete an die eingebuchten Stationen schicken. Kommen von einer Station keine Antworten mehr auf diese Pakete, wird sie als nicht mehr aktiv an das Abrechnungssystem gemeldet.

Konfiguration mit LANconfig Bei der Konfiguration mit LANconfig finden Sie die allgemeinen WLAN-Zugriffseinstellungen im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Allgemein'.



Konfiguration mit WEBconfig oder Telnet Unter WEBconfig oder Telnet finden Sie die allgemeinen WLAN-Zugriffseinstellungen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WLAN ► Inter-Stationen-Verkehr, Überwachen-Stationen bzw. IAAP-Protokoll (für Roaming)
Terminal/Telnet	cd /Setup/WLAN/Inter-Stationen-Verkehr, Überwachen-Stationen bzw. IAAP-Protokoll (für Roaming)

Access Control List

Mit der **Access Control List (ACL)** gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-LAN-Adapter.

Konfiguration
mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Access Control List im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Stationen'.

Kontrollieren Sie, ob die Einstellung 'Daten von den aufgeführten Stationen übertragen, alle anderen Stationen ausfiltern' aktiviert ist. Fügen Sie neue Stationen die an Ihren Funk-Netzwerk teilnehmen sollen ggf. über den Schalter 'Stationen' hinzu.



Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die Access Control List auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WLAN ▶ Zugriffsliste
Terminal/Telnet	cd /Setup/WLAN/Zugriffsliste

Protokoll-Filter

Mit dem Protokoll-Filter können Sie die Behandlung von bestimmten Protokollen bei der Übertragung aus dem WLAN ins LAN beeinflussen.

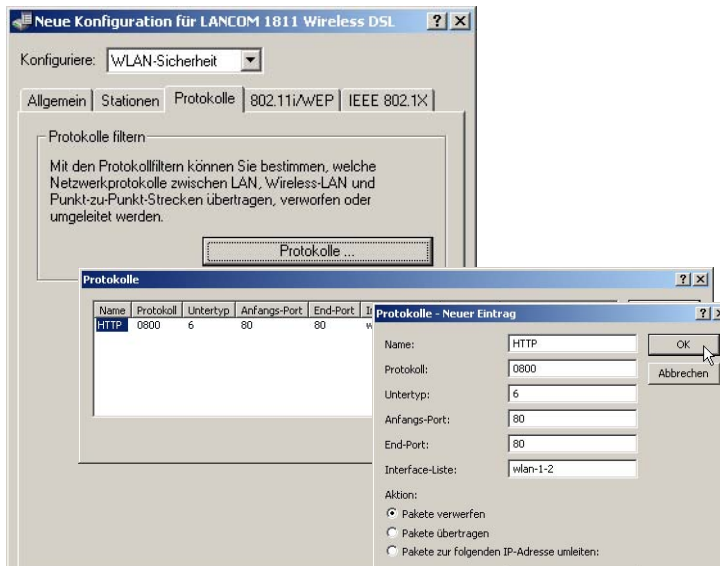


Pakete aus dem WLAN für bestimmte Protokolle/Ports können mit dem Protokoll-Filter auf spezielle IP-Adressen im LAN umgeleitet werden. Diese als „Redirect“ bezeichnete Funktion ist im Abschnitt 'Redirect-Funktion' →Seite 380 näher beschrieben.

Konfiguration
mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Protokoll-Filter im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Protokolle'.

▷ Konfiguration der WLAN- Parameter



Legen Sie für jedes Protokoll, das einer besonderen Behandlung bedarf, einen Eintrag in der Protokoll-Liste an. Geben Sie dabei folgende Werte ein:

- ▶ frei wählbarer Name für den Filtereintrag
- ▶ Protokoll-Nummer, z.B. '0800' für IP. Wird kein Protokoll eingetragen, so gilt dieser Filter für **alle** Pakete.
- ▶ Unterprotokoll, z.B. '6' für TCP. Wird kein Unterprotokoll eingetragen, so gilt dieser Filter für **alle** Pakete des eingetragenen Protokolls.
- ▶ Port-Start und Port-Ende, z.B. je '80' für HTTP. Werden keine Ports eingetragen, so gilt dieser Filter für alle Ports des entsprechenden Protokolls/Unterprotokolls.



Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter www.iana.org.

- ▶ Aktion für die Datenpakete:
 - ▷ Durchlassen
 - ▷ Verwerfen
 - ▷ Umleiten (mit Angabe der Zieladresse)
- ▶ Interface-Liste mit den Schnittstellen, für die der Filter gilt
- ▶ Umleiteadresse, wenn als Aktion 'Umleiten' gewählt ist

Beispiel:

Name	Protokoll	Unter- typ	Anfangs- -Port	End- -Port	Interface-Liste	Aktion	Umleite-IP- Adresse
ARP	0806	0	0	0	WLAN-1-2	Durchlassen	0.0.0.0
DHCP	0800	17	67	68	WLAN-1-2	Durchlassen	0.0.0.0
TELNET	0800	6	23	23	WLAN-1-2	Umleiten	192.168.11.5
ICMP	0800	1	0	0	WLAN-1-2	Durchlassen	0.0.0.0
HTTP	0800	6	80	80	WLAN-1-2	Umleiten	192.168.11.5

ARP, DHCP, ICMP werden durchgelassen, Telnet und HTTP werden umgelenkt auf 192.168.11.5, alle anderen Pakete werden verworfen.



Sobald ein Eintrag im Protokoll-Filter vorgenommen wird, werden alle Pakete, auf die dieser Filter nicht passt, automatisch verworfen!

Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die Protokoll-Filter auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► LAN-Bridge ► Protokoll-Tabelle
Terminal/Telnet	cd /Setup/LAN-Bridge/Protokoll-Tabelle

Verschlüsselungs-Einstellungen

Die Access Points der LANCOM-Familie unterstützen die aktuellsten Verfahren zur Verschlüsselung und Absicherung der Daten, die über eine WLAN-Verbindung übertragen werden.

- Der IEEE-Standard 802.11i/WPA steht für die höchste Sicherheit, die derzeit für WLAN-Verbindungen erreicht werden kann. Dieser Standard setzt u.a auf ein neues Verschlüsselungsverfahren (AES-CCM) und erreicht im Zusammenspiel mit einigen anderen Methoden eine Sicherheit, die bisher nur von VPN-Verbindungen erzielt werden konnte. Beim Einsatz von AES-fähiger Hardware (wie den 54-MBit-AirLancer-Clients und den 54-MBit-LANCOM-Access-Points) ist die Übertragung jedoch deutlich schneller als bei einer entsprechenden VPN-Absicherung.
- Aus Gründen der Kompatibilität zu älterer Hardware wird auch weiterhin das WEP-Verfahren unterstützt. WEP (**W**ired **E**quivalent **P**rivacy) war das ursprünglich im 802.11-Standard vorgesehene Verfahren zur Verschlüsselung der Daten bei Funkübertragungen. Dabei kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Im Laufe der Zeit sind bei WEP jedoch einige Sicherheitslücken bekannt geworden, weshalb nach Möglichkeit nur noch die aktuellen 802.11i/WPA-Methoden eingesetzt werden sollten.

▷ Konfiguration der WLAN- Parameter



Weitere Informationen zum 802.11i- und WPA-Standard finden Sie unter 'Entwicklung der WLAN-Sicherheit' →Seite 344.

Auf der Registerkarte '802.11i/WEP' im Konfigurationsbereich 'WLAN-Sicherheit' werden die Verschlüsselungsparameter für die einzelnen logischen WLANs eingestellt. Öffnen Sie die Liste über die Schaltfläche **WPA/Einzel-WEP-Einstellungen**.

Verschlüsselungsart

Für die einzelnen logischen WLAN-Interfaces wählen Sie zunächst die Verschlüsselungsart aus:

- ▶ Ja – Zugriff nur für Stationen mit Verschlüsselung (empfohlen): In diesem Modus können sich nur solche WLAN-Clients bei der Basisstation anmelden, bei denen WEP aktiviert ist und die über die entsprechenden Schlüssel verfügen.
- ▶ Ja – Zugriff auch für Stationen ohne Verschlüsselung erlauben: In diesem Modus können sich WLAN-Clients mit aktiviertem WEP und AirLancer MC 11-Clients (ohne WEP) bei dieser Basisstation anmelden.
- ▶ Nein – keine Verschlüsselung

Methode/
Schlüssel-1-
Typ

Stellen Sie hier das zu verwendende Verschlüsselungsverfahren ein.

- ▶ 802.11i (WPA)-PSK – Die Verschlüsselung nach dem 802.11i-Standard bietet die höchste Sicherheit. Die dabei eingesetzte 128-Bit-AES-Verschlüsselung entspricht der Sicherheit einer VPN-Verbindung. Wählen Sie diese Einstellung, wenn kein RADIUS-Server zur Verfügung steht und die Authentifizierung mit Hilfe eines Preshared Keys erfolgt.
- ▶ 802.11i (WPA)-802.1x – Wenn die die Authentifizierung über einen RADIUS-Server erfolgt, wählen Sie die Option '802.11i (WPA)-802.1x'. Achten Sie bei dieser Einstellung darauf, auch den RADIUS-Server bei den 802.1x-Einstellungen zu konfigurieren.
- ▶ WEP 152, WEP 128, WEP 64 – Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit. Diese Einstellung ist nur zu empfehlen, wenn die verwendete Hardware der WLAN-Clients die modernen Verfahren nicht unterstützt.
- ▶ WEP 152-802.1x, WEP 128-802.1x, WEP 64-802.1x – Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit und zusätzlicher Authentifizierung über 802.1x/EAP. Auch diese Einstellung kommt i.d.R. dann zum Einsatz, wenn die verwendete Hardware der WLAN-Clients den 802.11i-Standard nicht unterstützt. Durch die 802.1x/EAP-Authentifizierung bietet diese Einstellung zwar eine höhere Sicherheit als eine reine WEP-Verschlüsselung, die Notwendigkeit eines RADIUS-Servers stellt allerdings sehr hohe Anforderungen an die IT-Struktur.

Schlüssel-1/
Passphrase

Je nach eingestelltem Verschlüsselungsverfahren können Sie hier einen speziellen WEP-Schlüssel für das jeweilige logische WLAN-Interface bzw. eine Passphrase bei der Verwendung von WPA-PSK eintragen:

- ▶ Die Passphrase – also das 'Passwort' für das WPA-PSK-Verfahren – wird als Kette aus mindestens 8 und maximal 63 ASCII-Zeichen eingetragen.



Bitte beachten Sie, dass die Sicherheit des Verschlüsselungssystems bei der Verwendung einer Passphrase von der vertraulichen Behandlung dieses Kennworts abhängt. Die Passphrase sollte nicht einem größeren Anwenderkreis bekannt gemacht werden.

- ▶ Der WEP-Schlüssel-1, der nur speziell für das jeweilige logische WLAN-Interface gilt, kann je nach Schlüssel-länge unterschiedlich eingetragen werden. Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel 'Regeln für die Eingabe von WEP-Schlüsseln' →Seite 366.

WPA Sitzungs-
Schlüssel

Wenn als Verschlüsselungsmethode '802.11i (WPA)-PSK' eingestellt wurde, kann hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels ausgewählt werden:

- ▶ AES – Es wird das AES-Verfahren verwendet.
- ▶ TKIP – Es wird das TKIP-Verfahren verwendet.
- ▶ AES/TKIP – Es wird das AES-Verfahren verwendet. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wird TKIP eingesetzt.

Authentifizie-
rung

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, stehen zwei verschiedene Verfahren für die Authentifizierung der WLAN-Clients zur Verfügung:

- ▶ Beim 'OpenSystem'-Verfahren wird komplett auf eine Authentifizierung verzichtet. Die Datenpakete müssen von Beginn an richtig verschlüsselt übertragen werden, um von der Basisstation akzeptiert zu werden.
- ▶ Beim 'SharedKey'-Verfahren wird das erste Datenpakete unverschlüsselt übertragen um muss vom Client richtig verschlüsselt zurückgesendet werden. Bei diesem Verfahren steht einem potenziellen Angreifer mindestens ein Datenpaket unverschlüsselt zur Verfügung.

Standard-
schlüssel

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, kann der Access Point für jedes logische WLAN-Interface aus vier verschiedenen WEP-Schlüsseln wählen:

- ▶ Drei WEP-Schlüssel für das physikalische Interface
- ▶ Ein zusätzlicher WEP-Schlüssel speziell für jedes logische WLAN-Interface

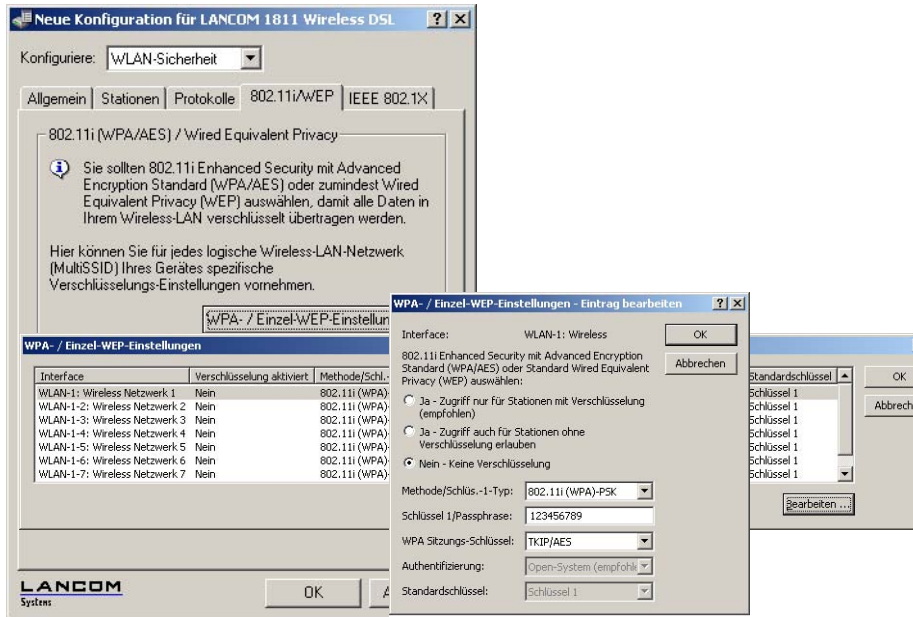
Bei den Einzel-WEP-Einstellungen wird der zusätzliche Schlüssel für jedes logische WLAN-Interface eingestellt (siehe 'Schlüssel-1/Passphrase'). Wählen Sie außerdem aus, welcher der vier eingestellten Schlüssel aktuell für die Verschlüsselung der Daten verwendet werden soll (Standardschlüssel). Mit dieser Einstellung können Sie den Schlüssel häufiger wechseln, um die Abhörsicherheit zusätzlich zu steigern.

Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel 'Regeln für die Eingabe von WEP-Schlüsseln' →Seite 366.

Konfiguration
mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Einzel-WEP-Einstellungen im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte '802.11i/WEP'.

► Konfiguration der WLAN- Parameter



Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die einzelnen Verschlüsselungs-Einstellungen der logischen WLAN-Netzwerke auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► WLAN-Schnittstellen ► Verschlüsselungs-Einstellungen
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Verschlüsselungs-Einstellungen

WEP- Gruppen- Schlüssel

Mit **Wired Equivalent Privacy (WEP)** steht ein Verfahren zur effektiven Verschlüsselung der Daten für die Funkübertragung zur Verfügung. Bei WEP kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Für jedes WLAN-Interface stehen vier WEP-Schlüssel zur Verfügung: ein spezieller Schlüssel für jedes logische WLAN-Interface und drei gemeinsame Gruppen-WEP-Schlüssel für jedes physikalische WLAN-Interface.

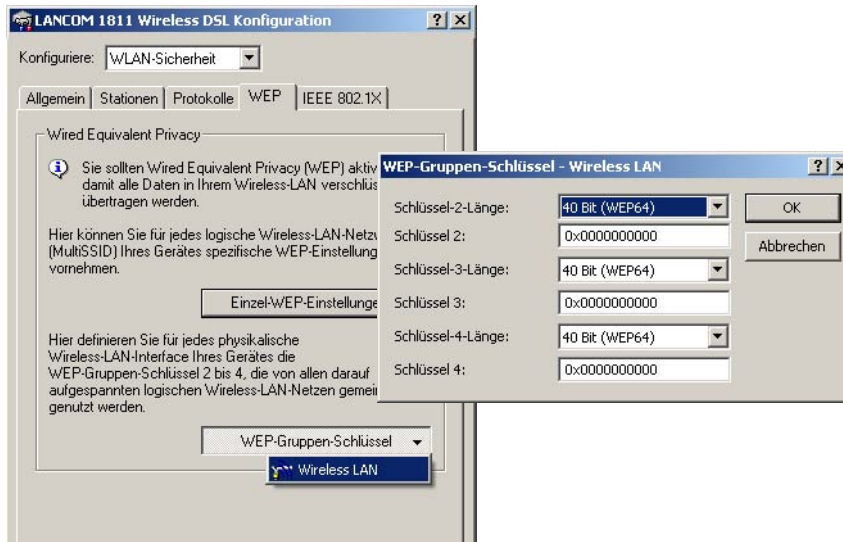


Wenn bei der Verwendung von 802.1x/EAP die 'dynamische Schlüssel-Erzeugung und -Übertragung' aktiviert ist, werden die Gruppen-Schlüssel von 802.1x/EAP verwendet und stehen damit für die WEP-Verschlüsselung nicht mehr zur Verfügung.

Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel 'Regeln für die Eingabe von WEP-Schlüsseln' →Seite 366.

Konfiguration
mit LANconfig

Auf der Registerkarte '802.11i/WEP' im Konfigurationsbereich 'WLAN-Sicherheit' werden die drei WEP-Schlüssel 2 bis 4 eingestellt. Öffnen Sie die Liste über die Schaltfläche **WEP-Gruppen-Schlüssel**. Diese WEP-Schlüssel gelten für das physikalische WLAN-Interface und damit global für alle zugehörigen logischen WLAN-Interfaces.



Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die Gruppenschlüssel der physikalischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Gruppen-Schlüssel
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Gruppen-Schluesssel

▷ Konfiguration der WLAN- Parameter

Regeln für die Eingabe von WEP-Schlüsseln

Die WEP-Schlüssel können als ASCII-Zeichen oder in Hexadezimaler Darstellung eingetragen werden. Die hexadezimale Darstellung beginnt jeweils mit den Zeichen '0x'. Die Schlüssel haben je nach WEP-Verfahren folgende Länge:

Verfahren	ASCII	HEX
WEP 64	5 Zeichen Beispiel: 'aR45Z'	10 Zeichen Beispiel: '0x0A5C1B6D8E'
WEP 128	13 Zeichen	26 Zeichen
WEP 152	16 Zeichen	32 Zeichen

Der ASCII-Zeichensatz umfasst die Zeichen '0' bis '9', 'a' bis 'z', 'A' bis 'Z' sowie die folgenden Sonderzeichen:

! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ' { | } ~

In der HEX-Darstellung wird jedes Zeichen durch ein Zeichenpaar aus den Ziffern '0' bis '9' und den Buchstaben 'A' bis 'F' dargestellt, daher benötigen die HEX-Schlüssel die doppelte Anzahl an Zeichen zur Darstellung.

Wählen Sie die Länge und das Format (ASCII oder HEX) der Schlüssel immer nach den Möglichkeiten der Funknetzwerkarten aus, die sich in Ihrem WLAN anmelden sollen. Wenn Sie im Access Point eine Verschlüsselung nach WEP 152 eingestellt haben, können manche Clients sich nicht mehr in diesem WLAN anmelden, weil sie die entsprechende Schlüssellänge nicht unterstützen.

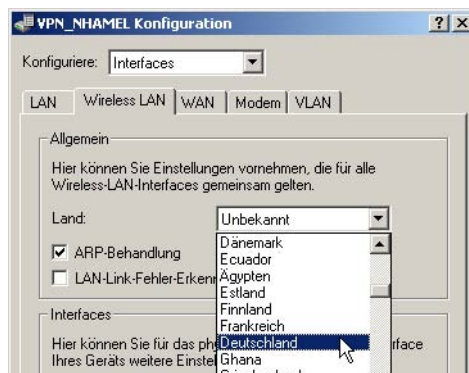
12.4.2 Allgemeine WLAN- Einstellungen

Ländereinstellung

Der Betrieb von WLAN-Karten ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z.B. in manchen Ländern nicht erlaubt. Um den Betrieb der LANCOM Access Points auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der Access Point betrieben wird.

Konfiguration mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Ländereinstellung im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN' in der Gruppe 'Allgemein':



▷ Konfiguration der WLAN- Parameter

Neben der Ländereinstellung finden sich in dieser Gruppe zwei weitere Parameter:

ARP-Behandlung

- ▶ Mobile Stationen im Funknetz, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der 'ARP-Behandlung' übernimmt der Access Point diese Aufgabe und beantwortet die ARP Anfragen an Stelle der Stationen im Stromsparmodus.

Link-Fehler-Erkennung

- ▶ Die 'Link-Fehler-Erkennung' schaltet die WLAN-Karte ab, wenn der Access Point keine Verbindung zum LAN mehr hat.

Konfiguration mit WEBconfig oder Telnnet

Unter WEBconfig oder Telnnet finden Sie die allgemeinen WLAN-Parameter auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WLAN
Terminal/Telnnet	cd /Setup/WLAN

12.4.3 WLAN-Routing (Isolierter Modus)

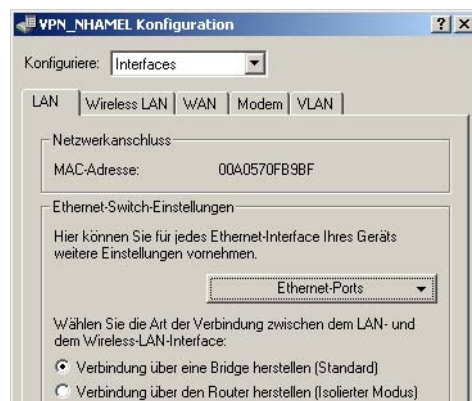
In der Standardeinstellung wird der Datenverkehr zwischen LAN und WLAN „gebrückt“, also transparent übertragen. Dabei verläuft der Datenverkehr zwischen dem drahtgebundenen und den drahtlosen Netzwerk **nicht** über den IP-Router. Damit stehen auch die im IP-Router integrierten Funktionen Firewall und Quality-of-Service nicht für den Datenverkehr zwischen WLAN und LAN zur Verfügung. Um diese Möglichkeiten dennoch zu nutzen, werden die WLAN-Schnittstellen in den „isolierten Modus“ versetzt, der Datenverkehr wird gezielt über den IP-Router geleitet.



Damit der IP-Router Daten zwischen LAN und WLAN richtig übertragen kann, müssen die beiden Bereiche über unterschiedliche IP-Adresskreise verfügen und das lokale Routing muss in den IP-Router-Einstellungen aktiviert werden.

Konfiguration mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie das WLAN-Routing im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'LAN' in der Gruppe 'Ethernet-Switch-Einstellungen':



▷ Konfiguration der WLAN- Parameter

Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie das WLAN- Routing auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten- Konfiguration ► Setup ► LAN- Bridge ► Isolierter Modus
Terminal/Telnet	cd /Setup/LAN-Bridge/Isolierter-Modus

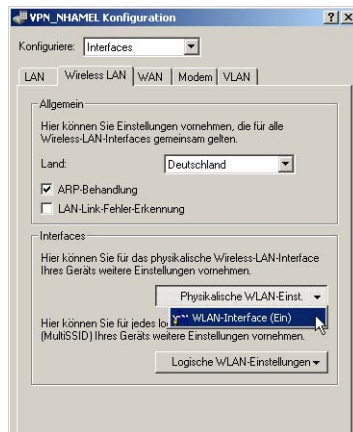
12.4.4 Die physikalischen WLAN- Schnittstellen

Einstellung der WLAN- Karte

Neben den Parametern für alle WLAN- Karten gemeinsam gelten eine Reihe von Einstellungen für jede WLAN- Karte des Access Points speziell.

Konfiguration mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Einstellung der WLAN- Karte im Konfigurationsbereich 'Management' auf der Registerkarte 'Wireless LAN'. Öffnen Sie die Liste der physikalischen WLAN- Schnittstellen mit einem Klick auf die Schaltfläche **Physikalische WLAN- Einst.**



Betriebsart der WLAN- Karte

Betriebsart

LANCOM Wireless- Geräte können grundsätzlich in zwei verschiedenen Betriebsarten arbeiten:

- Als Basisstation (Access Point) stellt es für die WLAN- Clients die Verbindung zu einem kabelgebundenen LAN her.
- Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.

Wählen Sie die Betriebsart auf der Registerkarte 'Betrieb'. Wenn das WLAN- Interface nicht benötigt wird, kann es vollständig deaktiviert werden.



Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die Einstellung der Betriebsart der physikalischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Betriebs-Einstellungen
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Betriebs-Einstellungen

Radio-Einstellungen

Frequenz-
band, Unter-
band

Mit der Auswahl des Frequenzbandes auf der Registerkarte 'Radio' bei den Einstellungen für die physikalischen Interfaces legen Sie fest, ob die WLAN-Karte im 2,4 GHz- oder im 5 GHz-Band arbeitet (siehe auch 'Standardisierte Funkübertragung nach IEEE' →Seite 334), und damit gleichzeitig die möglichen Funkkanäle.

Im 5 GHz-Band kann außerdem ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.



In einigen Ländern ist das DFS-Verfahren zur automatischen Kanalsuche vorgeschrieben. Mit der Wahl des Unterbands wird damit auch der Bereich der Funkkanäle festgelegt, die für die automatische Kanalauswahl verwendet werden kann.

▶ Automatische Auswahl der 5GHz-WLAN-Kanäle über DFS mit Black- und White-List

Beim DFS-Verfahren (Dynamic Frequency Selection) wird automatisch eine freie Frequenz gewählt, z. B. um das Stören von Radaranlagen zu verhindern und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Nach dem Einschalten oder Booten wählt das Gerät aus den (z.B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus und prüft, ob auf diesem Kanal ein Radarsignal gefunden wird und ob auf diesem Kanal schon ein anderes Wireless LAN arbeitet. Dieser Scan-Vorgang wird solange wiederholt, bis ein radarfreier Kanal mit möglichst wenig anderen Netzwerken gefunden wurde. Anschließend wird der gewählte Kanal erneut für 60 Sekunden beobachtet, um evtl. auftretende Radarsignale sicher auszuschließen. Die Datenübertragung kann daher durch diesen Scan-Vorgang und die erneute Suche eines freien Kanals für 60 Sekunden unterbrochen werden.

Um diese Pausen in der Datenübertragung bei jedem Kanalwechsel zu verhindern, verlegt ein LANCOM ab der LCOS-Version 5.00 den Scanvorgang **vor** die Auswahl eines konkreten Kanals. Die Informationen über die gescannten Kanäle werden in einer internen Datenbank gespeichert:

▷ Konfiguration der WLAN-Parameter

- ▷ Wurde auf dem Kanal ein Radarsignal gefunden?
- ▷ Wieviele andere Netzwerke wurden auf dem Kanal gefunden?

Mit Hilfe dieser Datenbank kann das WLAN-Gerät einen Kanal aus einer Liste der radarfreien Kanäle mit der geringsten Anzahl an anderen Netzwerken auswählen. Nach der Auswahl eines Kanals kann die Datenübertragung dann sofort ohne weitere Wartezeit beginnen.

- ▷ Die „Blacklist“ dieser Datenbank speichert die Kanäle, die aufgrund der gefundenen Radarsignale geblockt werden. Diese Einträge verschwinden nach jeweils 30 Minuten aus der Liste, um die Informationen ständig auf dem aktuellen Stand zu halten.
- ▷ Die „Whitelist“ der Datenbank speichert die Kanäle, auf denen kein Radarsignal gefunden wurde. Diese Einträge bleiben für die nächsten 24 Stunden gültig, können aber zwischenzeitlich beim Auftreten eines Radarsignals durch einen Eintrag in der Blacklist überschrieben werden.

Der 60-Sekunden-Scanvorgang wird nur unter den folgenden Voraussetzungen wieder notwendig:

- ▷ Das Gerät wird eingeschaltet oder kalt gestartet. In diesem Fall ist die Datenbank leer, das Gerät kann nicht aus der Whitelist die bevorzugten Kanäle auswählen.
- ▷ Das Gerät ist seit 24 Stunden in Betrieb, die Markierungen der Whitelist sind aus der Datenbank „herausgealtert“. In diesem Fall muss die Datenbank neu gefüllt werden.



Damit der 60-Sekunden-Scanvorgang nicht zur unpassenden Zeit ausgelöst wird, können Sie unter Telnet im Menü /Setup/WLAN mit dem Befehl `set DFS-Rescan-Stunden [Stunde] Zeitpunkt` einstellen, zu der das Löschen der Datenbank erzwungen wird. Für die Definition der Stunde können die Möglichkeiten der cron-Befehle genutzt werden, z.B. '1,6,13' für einen DFS-Scan immer um 1 Uhr, um 6 und um 13 Uhr oder '0-23/4' für einen DFS-Scan in der Zeit von 0 bis 23 Uhr alle vier Stunden. Voraussetzung für das Erzwingen des DFS-Scans ist eine korrekte Systemzeit im Gerät.

Kanalnummer

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.



Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

Kompatibilität
smodus

Im 2,4 GHz-Band gibt es zwei verschiedene Funk-Standards: den IEEE 802.11b-Standard mit einer Übertragungsgeschwindigkeit von bis zu 11 MBit/s und den IEEE 802.11g-Standard mit bis zu 54 MBit/s. Wenn als Frequenzband das 2,4 GHz-Band ausgewählt ist, kann zusätzlich die Übertragungsgeschwindigkeit eingestellt werden.



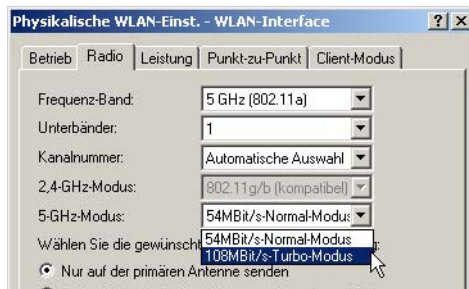
Bitte beachten Sie, dass sich Clients, die nur einen langsameren Standard unterstützen, sich ggf. nicht mehr in Ihrem WLAN anmelden können, wenn Sie die Übertragungsgeschwindigkeit auf einen hohen Wert einstellen.

▷ Konfiguration der WLAN-Parameter

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere Clients nicht auszuschließen, bietet sich der 802.11g/b-Kompatibilitätsmodus an. In diesem Modus arbeitet die WLAN-Karte im Access Point grundsätzlich nach dem schnelleren Standard, fällt aber auf den langsameren Modus zurück, wenn sich entsprechende Clients im WLAN anmelden. Im '2-MBit-Kompatibilitätsmodus' unterstützt der Access Point auch die älteren 802.11b-Karten mit einer maximalen Übertragungsgeschwindigkeit von 2 MBit/s.

Turbomodus

Wenn Sie gleichzeitig zwei benachbarte, freie Kanäle für die Funkübertragung nutzen, können Sie die Übertragungsgeschwindigkeit auf bis zu 108 MBit/s steigern. Stellen Sie diese Option im 2,4 GHz-Band in der Drop-Down-Liste '2,4 GHz-Modus' ein, im 5 GHz-Band in der entsprechenden Liste '5 GHz-Modus' darunter.



Diversity-Einstellungen

Die Diversity-Einstellungen legen fest, welche Antennen zum Senden bzw. zum Empfangen verwendet werden:

- ▶ 'Nur auf der primären Antenne senden' (Rx-Diversity): In dieser Standardeinstellung wird über die am Main-Anschluss des Access Points angeschlossene Antenne gesendet. Zum Empfangen (RX) wird die Antennen ausgewählt, die den bestem Empfang hat (an Main oder AUX).
- ▶ 'Automatisch die beste Antenne zum Senden selektieren' (Tx- und Rx-Diversity): Wird die Diversity-Funktion auch auf das Senden angewendet (TX), wird auch zum Senden die Antennen mit dem stärksten Signal ausgewählt.
- ▶ 'Auf der primären Antennen Senden und auf der sekundären empfangen' (kein Diversity): Hierbei wird nur die Main-Antenne zum Senden verwendet, zum Empfangen bevorzugt die Antenne am AUX-Anschluss. Mit dieser Variante können Antennen mit sehr hohen Leistungen zum Empfangen eingesetzt werden, die aus rechtlichen Gründen nicht zum Senden verwendet werden dürfen.

Antennen-Gewinn
Sendeleistungs-Reduktion

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist ein Dämpfung der Leistung auf den zulässigen Wert erforderlich.

- ▶ In das Feld 'Antennen-Gewinn' wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Bei einer AirLancer Extender O-18a-Antenne mit einem Gewinn von 18dBi wird bei einer Kabellänge von 4m Länge mit einer Dämpfung 1dB/m ein 'Antennen-Gewinn' von $18 - 4 = 14$ eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.
- ▶ Im Gegensatz dazu reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter. Siehe dazu auch 'Aufbau von Outdoor-Funknetz-Strecken' →Seite 385.

▷ Konfiguration der WLAN- Parameter



Durch die Sendeleistungsreduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z.B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

Basisstations-Dichte

Mit zunehmender Dichte von Access Points überlagern sich die Empfangsbereich der Antennen. Mit der Einstellung der 'Basisstations-Dichte' kann die Empfangs-Empfindlichkeit der Antennen reduziert werden.



Maximaler Abstand

Bei sehr großen Entfernungen zwischen Sender und Empfänger im Funknetz steigt die Laufzeit der Datenpakete. Ab einer bestimmten Grenze erreichen die Antworten auf die ausgesandten Pakete den Sender nicht mehr innerhalb der erlaubten Zeit. Mit der Angabe des maximalen Abstands kann die Wartezeit auf die Antworten erhöht werden. Diese Distanz wird umgerechnet in eine Laufzeit, die den Datenpakete bei der drahtlosen Kommunikation zugestanden werden soll.

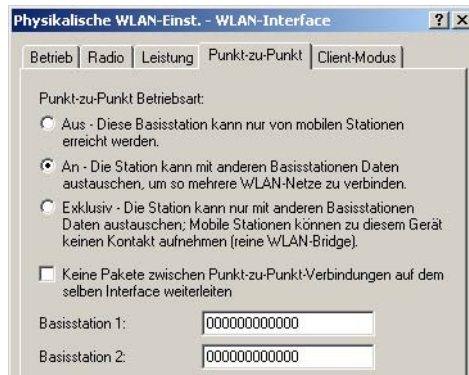
Konfiguration mit WEBconfig oder Telnnet

Unter WEBconfig oder Telnnet finden Sie die Radio-Parameter auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► WLAN-Schnittstellen ► Radio-Einstellungen
Terminal/Telnnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Radio-Einstellungen

Punkt-zu-Punkt-Verbindungen

Access Points können nicht nur mit mobilen Clients kommunizieren, sie können auch Daten von einer Basisstation zur anderen übertragen. Auf der Registerkarte 'Punkt-zu-Punkt' bei den Einstellungen für die physikalischen Interfaces legen Sie fest, ob auch der Datenaustausch mit anderen Access Points erlaubt sein soll. Zur Auswahl stehen:



- ▶ Punkt-zu-Punkt 'Aus': Die Basisstation kann nur mit mobilen Clients kommunizieren
- ▶ Punkt-zu-Punkt 'An': Die Basisstation kann mit anderen Basisstationen und mit mobilen Clients kommunizieren
- ▶ Punkt-zu-Punkt 'Exklusiv': Die Basisstation kann nur mit anderen Basisstationen kommunizieren

In den Eingabefeldern werden die MAC-Adressen der WLAN-Karten eingetragen, zu denen eine Punkt-zu-Punkt-Verbindung aufgebaut wird (maximal 7).



Bitte beachten Sie, hier nur die MAC-Adressen der WLAN-Karten auf der anderen Seite der Verbindung einzutragen! Nicht die eigenen MAC-Adressen und nicht die MAC-Adressen von anderen Interfaces, die möglicherweise in den Basisstationen vorhanden sind.

Konfiguration
mit WEBconfig
oder Telnet

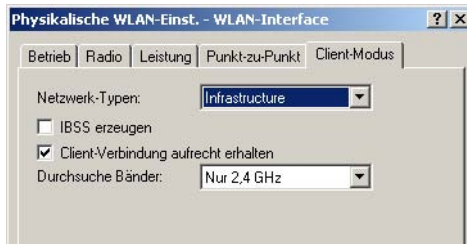
Unter WEBconfig oder Telnet finden Sie die Einstellungen für die Punkt-zu-Punkt-Verbindungen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Interpoint-Einstellungen
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Interpoint-Einstellungen

Client-Modus

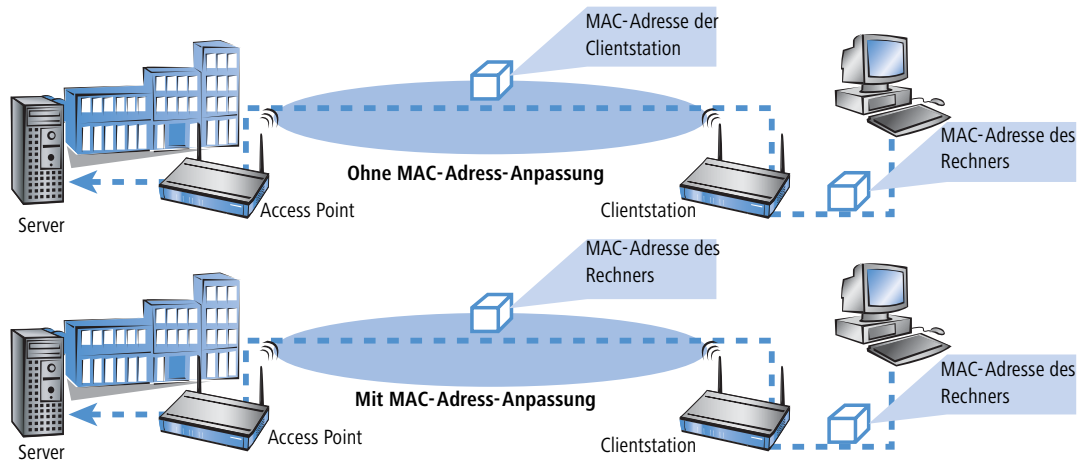
Wenn das LANCOM Wireless-Gerät als Client betrieben wird, können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces noch weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.

▷ Konfiguration der WLAN- Parameter



- | | |
|-------------------------------------|--|
| Netzwerktypen | Mit der Auswahl der 'Netzwerktypen' wird festgelegt, ob sich die Station nur an Infrastruktur- oder auch in Adhoc-Netzwerken anmelden darf. Weitere Informationen zu diesen Netzwerktypen finden Sie unter 'Der Ad-hoc-Modus' →Seite 337 und 'Das Infrastruktur-Netzwerk' →Seite 338. |
| IBBS erzeugen | Wenn die Station selbst ein IBBS (Independent Basic Service Set), also ein Adhoc-Netzwerk aufbauen kann, verbindet sich die Station auch mit anderen WLAN-Clients. Bei der Anbindung von Geräten mit einer Clientstation ist das aber meistens nicht erwünscht bzw. nicht erforderlich. |
| Client-Verbindung aufrecht erhalten | Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen. |
| Durchsuchte Bänder | Legen Sie hier fest, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden. |
| Bevorzugte BSS-ID | Wenn sich die Clientstation nur bei einem bestimmten Access Point einbuchten soll, können Sie hier die MAC-Adresse der WLAN-Karte aus diesem Access Point eintragen. |
| Adress-Anpassung | Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der Access-Point auf der anderen Seite der Verbindung „sieht“ also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners. |

▷ Konfiguration der WLAN- Parameter



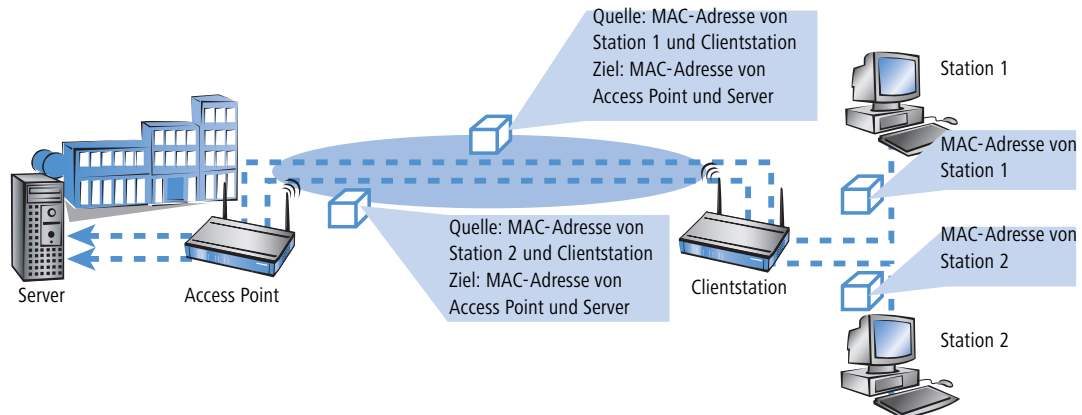
In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den Access Point übertragen wird. Mit der Option 'Adress-Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen.



Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur **ein** Rechner angeschlossen ist!

Client-Bridge-
Unterstützung

Während mit der Adress-Anpassung ('Adress-Anpassung' → Seite 374) nur die MAC-Adresse eines **einzigen** angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.



▷ Konfiguration der WLAN- Parameter

Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestossen werden.

Der Client-Bridge-Modus hat folgende Vorteile gegenüber den anderen Verfahren:

- ▶ Gegenüber dem „normalen“ Client-Modus entfällt die Adress-Übersetzung (Maskierung) in der Clientstation.
- ▶ Gegenüber den Punkt-zu-Punkt-Verbindungen entfällt die manchmal unerwünschte feste Eintragung der MAC-Adressen. Darüber hinaus können mit dem Client-Bridge-Modus mehr als sechs Verbindungen (Einschränkung bei P2P) eingerichtet werden.



Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden. Die Verwendung des Client-Bridge-Modus muss in den Einstellungen für das logische Netzwerk des Access Points ebenfalls aktiviert werden.

Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Einstellungen für den Client-Modus auf folgenden Pfaden:

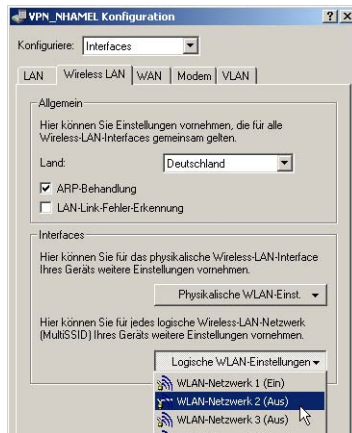
Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► WLAN-Schnittstellen ► Client-Einstellungen
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Client-Einstellungen

12.4.5 Die logischen WLAN-Schnittstellen

Jede physikalische WLAN-Schnittstelle kann bis zu acht verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche Access Points benötigt werden.

Konfiguration mit LANconfig

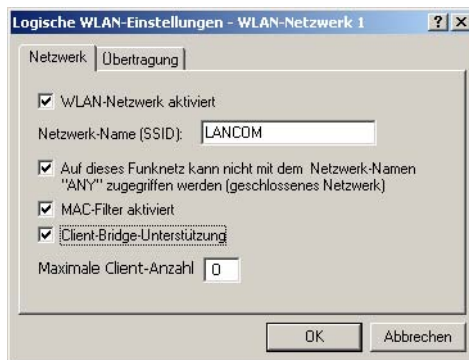
Bei der Konfiguration mit LANconfig finden Sie die Einstellung der logischen WLAN-Interfaces im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN'. Öffnen Sie die Liste der logischen WLAN-Schnittstellen mit einem Klick auf die Schaltfläche **Logische WLAN-Einstellungen** und wählen Sie das gewünschte logische Interface aus.



Netzwerkeinstellungen

Aktivieren Mit dem Schalter 'WLAN-Netzwerk aktiviert' kann das logische WLAN separat ein- oder ausgeschaltet werden.

SSID einstellen Stellen Sie für jedes benötigte logische Funknetzwerk auf der Registerkarte 'Netzwerk' bei den Einstellungen für die logischen Interfaces eine eindeutige SSID (den Netzwerknamen) ein. Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.



**Closed-Net-
work-Modus**

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den 'Closed-Network-Modus' ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID 'Any' in Ihrem Funknetzwerk anmelden.

▷ Konfiguration der WLAN- Parameter

MAC-Filter
aktiviert

In der MAC-Filterliste (**WLAN-Sicherheit ► Stationen ► Stationen**) werden die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.



Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

Maximale Client-Anzahl

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

Client-Bridge-Unterstützung

Aktivieren Sie diese Option für einen Access Point, wenn Sie im WLAN-Client-Modus für eine Clientstation die Client-Bridge-Unterstützung aktiviert haben ('Client-Bridge-Unterstützung' →Seite 375).



Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

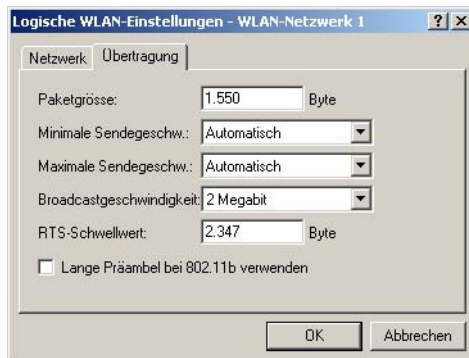
Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Netzwerk-Einstellungen für die logischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► Schnittstellen ► WLAN-Schnittstellen ► Netzwerk-Einstellungen
Terminal/Telnet	cd /Setup/Schnittstellen/WLAN-Schnittstellen/ Netzwerk-Einstellungen

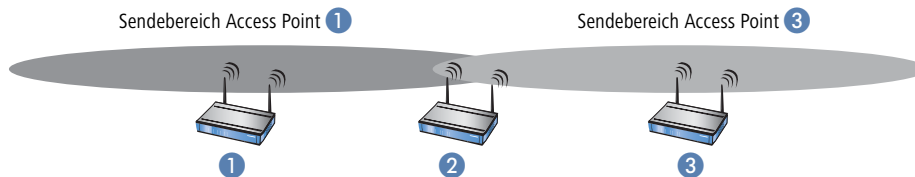
Einstellungen für die Übertragung

Die Details für die Datenübertragung auf dem logischen Interface stellen Sie auf der Registerkarte 'Übertragung' ein.

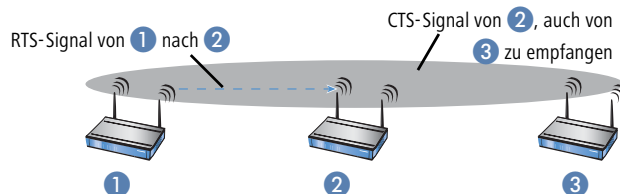


▷ Konfiguration der WLAN-Parameter

Paketgröße	Bei kleinen Datenpaket ist die Gefahr für Übertragungsfehler geringer als bei großen Paketen, allerdings steigt auch der Anteil der Header-Informationen am Datenverkehr, die effektive Nutzlast sinkt also. Erhöhen Sie den voreingestellten Wert nur, wenn das Funknetzwerk überwiegend frei von Störungen ist und nur wenig Übertragungsfehler auftreten. Reduzieren Sie den Wert entsprechend, um die Übertragungsfehler zu vermeiden.
Minimale und maximale Geschwindigkeit	Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die minimalen und maximalen Übertragungsgeschwindigkeiten fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.
Broadcastgeschwindigkeit	Die eingestellte Broadcastgeschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch „schneller“ zu erreichen sind.
RTS-Schwellwert	Mit dem RTS-Schwellwert wird das Phänomen der „Hidden-Station“ vermieden.



Dabei sind drei Access Points 1, 2, und 3 so positioniert, dass zwischen den beiden äußeren Geräten keine direkte Funkverbindung mehr möglich ist. Wenn nun 1 ein Paket an 2 sendet, bemerkt 3 diesen Vorgang nicht, da er außerhalb des Sendebereichs von 1 steht. 3 sendet also möglicherweise während der laufenden Übertragung von 1 ebenfalls ein Paket an 2, denn 3 hält das Medium (in diesem Falle die Funkverbindung) für frei. Es kommt zur Kollision, keine der beiden Übertragungen von 1 oder 3 nach 2 ist erfolgreich. Um diese Kollisionen zu vermeiden, wird das RTS/CTS-Protokoll eingesetzt.



Dazu schickt 1 vor der eigentlichen Übertragung ein RTS-Paket an 2, das 2 mit einem CTS beantwortet. Das von 2 ausgestrahlte CTS ist jetzt aber in „Hörweite“ von 3, so dass 3 mit seinem Paket an 2 warten kann. Die RTS- und CTS-Signale beinhalten jeweils eine Zeitangabe, wie lange die folgende Übertragung dauern wird.

Eine Kollision bei den recht kurzen RTS-Pakete ist sehr unwahrscheinlich, die Verwendung von RTS/CTS erhöht aber dennoch den Overhead. Der Einsatz dieses Verfahrens lohnt sich daher nur für längere Datenpakete, bei denen Kol-

▷ Konfiguration der WLAN- Parameter

lisionen wahrscheinlich sind. Mit dem RTS-Schwellwert wird eingestellt, ab welcher Paketlänge das RTS/CTS eingesetzt werden soll. Der passende Werte ist in der jeweiligen Umgebung im Versuch zu ermitteln.

Lange Präambel bei 802.11b

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die „lange Präambel“ nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

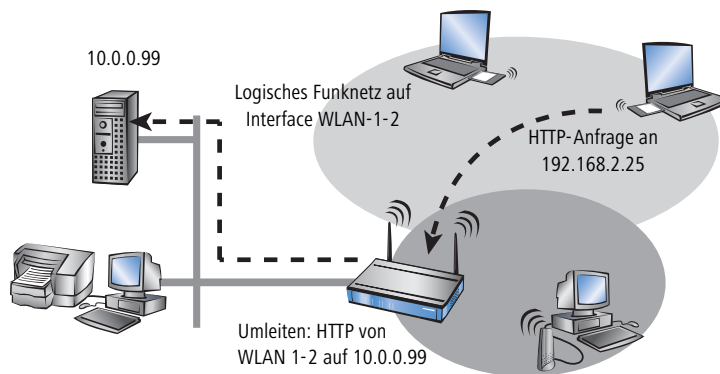
12.4.6 Zusätzliche WLAN-Funktionen

Neben der den verschiedenen Verschlüsselungs-Möglichkeiten 802.11i/AES, WPA/TKIP oder WEP und dem Closed-Network gibt es noch eine Reihe weiterer Funktionen, mit denen der Betrieb eines Funknetzwerks abgesichert werden kann. Mit der Redirect-Funktion kann die Anbindung von WLAN-Clients in wechselnden Umgebungen komfortabel gesteuert werden. Da diese Funktionen teilweise auch für andere Module des LANCOM LCOS von Bedeutung sind, finden sich die Konfigurationsparameter in Bereichen außerhalb der WLAN-Einstellung.

Redirect-Funktion

Die Teilnehmer (Clients) in Funknetzwerken haben vor allem eine Eigenschaft oft gemeinsam: eine hohe Mobilität. Die Clients verbinden sich also nicht unbedingt immer mit dem gleichen Access Point, sondern wechseln den Access Point und das zugehörige LAN relativ häufig.

Die Redirect-Funktion hilft dabei, die Anwendungen von WLAN-Clients bei der Übertragung in das LAN automatisch immer auf den richtigen Zielrechner einzustellen. Wenn die Anfragen von WLAN-Clients über HTTP aus einem bestimmten logischen Funknetzwerk immer auf einen bestimmten Server im LAN umgeleitet werden sollen, wird für das entsprechende Protokoll ein Filtereintrag mit der Aktion 'Umleiten' für das gewünschte logische WLAN-Interface aufgestellt.



Alle Anfragen mit diesem Protokoll aus diesem logischen Funknetz werden dann automatisch umgeleitet auf den Zielservers im LAN. Bei der Rückübertragung der Datenpakete werden die entsprechenden Absenderadressen und Ports aufgrund der Einträge in der Verbindungsstatistik wieder eingesetzt, so dass ein störungsfreier Betrieb in bei-

den Richtungen möglich ist. Weitere Informationen zum Einstellen der Protokoll-Filter finden Sie unter 'Protokoll-Filter' →Seite 359.

IEEE 802.1x/EAP

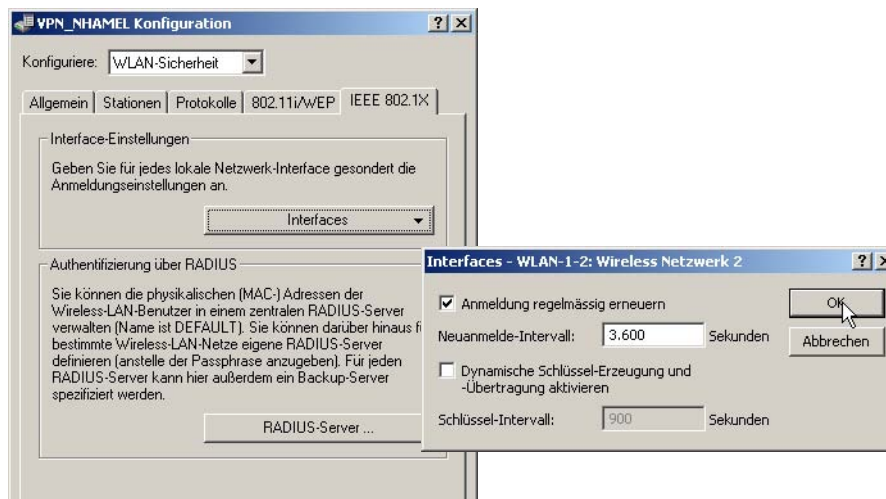
Der internationale Industrie-Standard IEEE 802.1x und das **Extensible Authentication Protocol (EAP)** ermöglichen Basis-Stationen die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können zentral auf einem RADIUS-Server verwaltet und von der Basis-Station bei Bedarf von dort abgerufen werden.

Diese Technologie ermöglicht außerdem den gesicherten Versand und den regelmäßigen automatischen Wechsel von WEP Schlüsseln. Auf diese Weise verbessert IEEE 802.1x die Sicherungswirkung von WEP.

In Windows XP ist die IEEE-802.1x-Technologie bereits fest integriert. Für andere Betriebssysteme existiert Client-Software.

Konfiguration
mit LANconfig

Bei der Konfiguration mit LANconfig finden Sie die IEEE-802.1x-Einstellungen im Konfigurationsbereich 'Benutzer-Anmeldung'. Entscheiden Sie hier ob Sie IEEE-802.1x aktivieren möchten. Bei aktiviertem IEEE-802.1x ist es zwingend erforderlich, einen RADIUS-Server für die IEEE-802.1x Authentifizierung anzugeben.



Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die IEEE-802.1x-Einstellungen auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► IEEE802.1x ► Ports
Terminal/Telnet	cd /Setup/IEEE802.1x/Ports

▷ IEEE 802.11i für Punkt- zu- Punkt-Verbindungen im WLAN

Nur mit LANCOM VPN Option. Nicht mit allen LANCOM-Geräten möglich.

IPSec-over-WLAN

Mit Hilfe der IPSec-over-WLAN-Technologie kann zusätzlich zu den bereits vorgestellten Sicherheitsmechanismen ein Funknetzwerk für besonders sensiblen Datenaustausch optimal abgesichert werden. Dazu wird die LANCOM Wireless Basisstation mit der LANCOM VPN Option zum VPN Gateway aufgerüstet. Zusätzlich zur Verschlüsselung per 802.11i, WPA oder WEP bietet das LANCOM Wireless somit die Möglichkeit, die Funkstrecke über ein IPSec-basiertes VPN zu verschlüsseln.

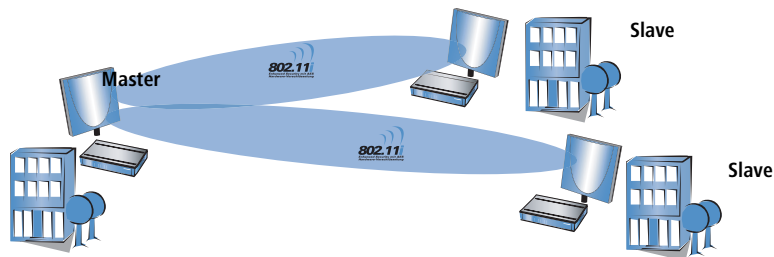
12.5 IEEE 802.11i für Punkt-zu-Punkt-Verbindungen im WLAN

12.5.1 Mehr Sicherheit im P2P-Betrieb

Mit IEEE 802.11i kann auch die Sicherheit auf Point-to-Point-Verbindungen im WLAN deutlich verbessert werden. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security (LEPS).

12.5.2 Konfiguration

Um die Vorteile der 802.11i-Verschlüsselung auf P2P-Strecken nutzen zu können, muss zunächst der Punkt-zu-Punkt-Betrieb in den beteiligten Geräten aktiviert sein. Zusätzlich muss auf jeder Verbindung ein Gerät als 'Master' und ein Gerät als 'Slave' konfiguriert sein. Auf beiden Seiten der Verbindung muss schließlich die MAC-Adresse des jeweils gegenüberliegenden WLAN-Clients eingetragen sein.



MAC-Adresse finden über WEBconfig, Telnnet oder Terminalprogramm

Unter WEBconfig oder Telnnet bzw. Terminalprogramm finden Sie die MAC-Adressen der WLAN-Karten in den Geräten auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Status ▶ WLAN-Statistik ▶ Interface-Statistiken
Terminal/Telnnet	Status/WLAN-Statistik/Interface-Statistiken

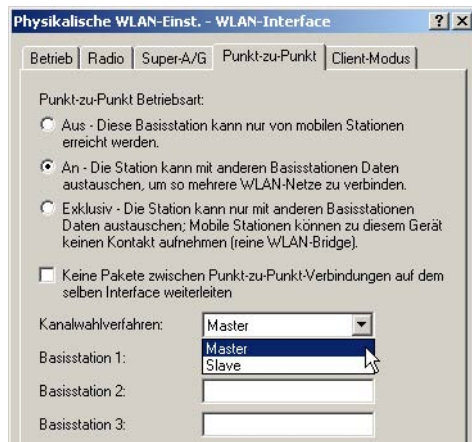
▷ IEEE 802.11i für Punkt- zu- Punkt- Verbindungen im WLAN

Sie finden die WLAN-MAC-Adresse alternativ auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie nur die als „WLAN-MAC“ oder „MAC-ID“ gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!



LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Einstellungen für die P2P-Verbindungen im Konfigurationsbereich 'Management' auf der Registerkarte 'Wireless LAN'. Öffnen Sie mit der Schaltfläche **Physikalische WLAN-Einst.** die Optionen für das entsprechende WLAN-Interface und wechseln Sie dort auf die Registerkarte 'Punkt-zu-Punkt'. Aktivieren Sie hier den Punkt-zu-Punkt-Modus und stellen Sie als 'Kanalwahlverfahren' entweder 'Master' oder 'Slave' ein. Tragen Sie dazu die jeweiligen MAC-Adressen der WLAN-Karte auf der Gegenseite ein.



Zum Aktivieren der 802.11i-Verschlüsselung auf der P2P-Verbindung passen Sie die Einstellungen für das erste logische WLAN-Netzwerk im verwendeten WLAN-Interface an (also WLAN-1, wenn Sie die erste WLAN-Karte für die P2P-Verbindung nutzen, WLAN-2 wenn Sie die zweite Karte z.B. bei einem LANCOM 3550 Wireless nutzen).

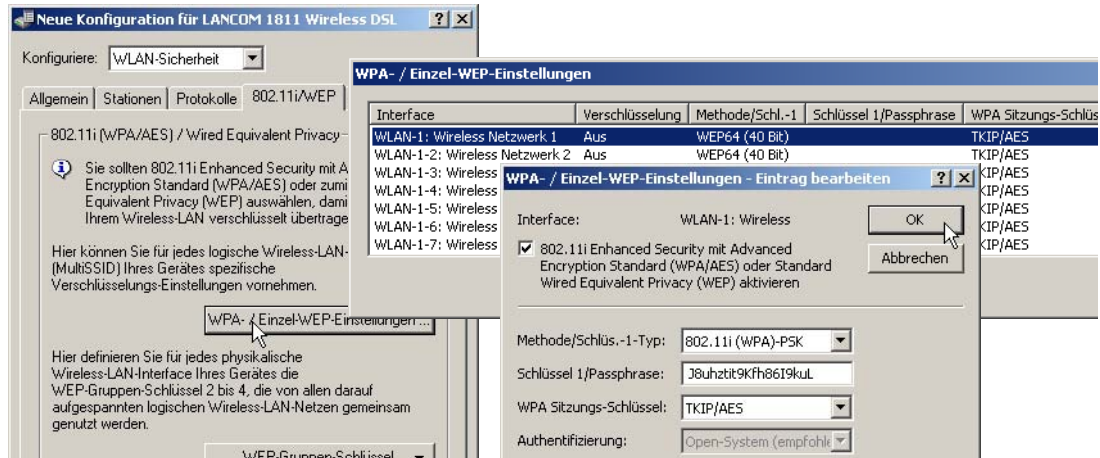
- ▶ Aktivieren Sie die 802.11i-Verschlüsselung.
- ▶ Wählen Sie als Methode '802.11i (WPA)-PSK' aus.
- ▶ Geben Sie die verwendete Passphrase ein.



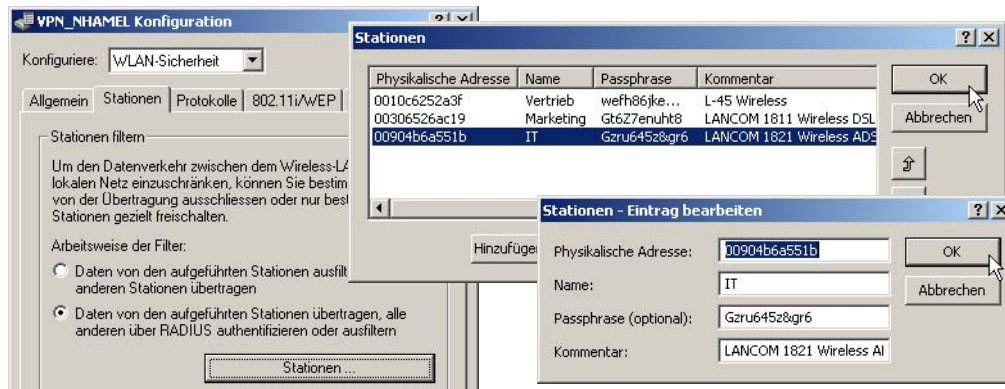
Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

▷ IEEE 802.11i für Punkt- zu- Punkt- Verbindungen im WLAN

In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.



Eine noch höhere Sicherheit erzielen Sie durch die zusätzliche Verwendung von LEPS, also der Verknüpfung der MAC-Adresse mit der Passphrase. Bei der Konfiguration mit LANconfig geben Sie die Passphrases der im WLAN zugelassenen Stationen (MAC-Adressen) im Konfigurationsbereich 'WLAN-Sicherheit' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen** ein.



Konfiguration
mit WEBconfig
oder Telnet

Unter WEBconfig oder Telnet finden Sie die Einstellungen für den Punkt-zu-Punkt-Betrieb der physikalischen WLAN-Interfaces auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Interpoint-Einstellungen
Terminal/Telnet	/Setup/Schnittstellen/WLAN-Schnittstellen/Interpoint-Einstellungen

Die Verschlüsselungs-Einstellungen für die einzelnen logischen WLAN-Netzwerke finden Sie unter:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Schnittstellen ▶ WLAN-Schnittstellen ▶ Verschlüsselungs-Einstellungen
Terminal/Telnet	/Setup/Schnittstellen/WLAN-Schnittstellen/Verschlüsselungs-Einstellungen

Die Zugangs-Liste für die Zuordnung der MAC-Adressen zu den Passphrases (LEPS) finden Sie unter:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WLAN ▶ Zugangs-Liste
Terminal/Telnet	Setup/WLAN/Zugangs-Liste

12.6 Aufbau von Outdoor-Funknetz- Strecken

LANCOM Access Points eignen sich in Verbindung mit den entsprechenden externen Antennen hervorragend zum Aufbau von Funkstrecken (Point-to-Point) zu einem zweiten Access Point.

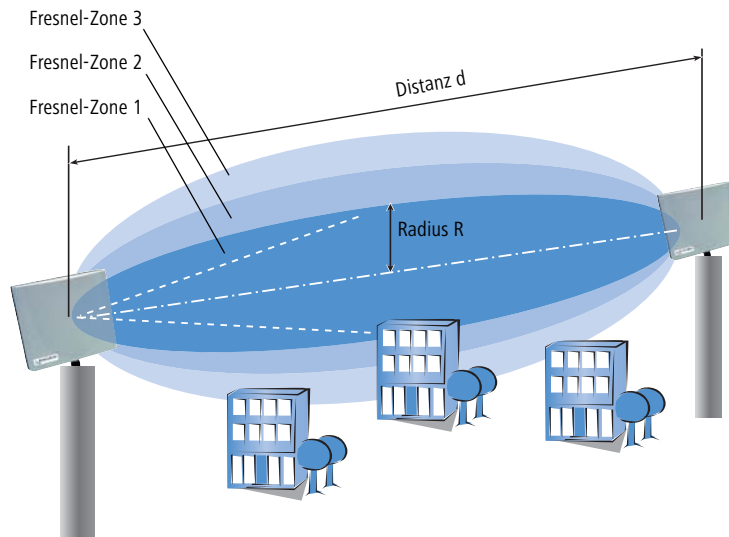
Bei der Auslegung der Funkstrecken sind im wesentlichen zwei Fragen zu beantworten:

- ▶ Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?
- ▶ Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

12.6.1 Geometrische Auslegung der Funkstrecke

Die Antennen strahlen Ihre Leistung nicht linear, sondern in einem modellabhängigen Winkel ab. Durch die kugelförmige Ausbreitung der Wellen kommt es in bestimmten Abständen von der direkten Verbindung zwischen Sender und Empfänger zur Verstärkungen oder zu Auslöschungen der effektiven Leistung. Die Bereiche, in denen sich die Wellen verstärken oder Auslöschen, werden als Fresnel-Zonen bezeichnet.

▷ Aufbau von Outdoor- Funknetz- Strecken



Um die von der Antenne abgestrahlte Leistung möglichst vollständig auf die empfangende Antenne abzubilden, muss die Fresnel-Zone 1 frei bleiben. Jedes störende Element, das in diese Zone hineinragt, beeinträchtigt die effektiv übertragene Leistung deutlich. Dabei schirmt das Objekt nicht nur seine eigene Fläche einen Teil der Fresnel-Zone ab, sondern führt durch Reflexionen zusätzlich zu einer deutlichen Reduzierung der empfangenen Strahlung.

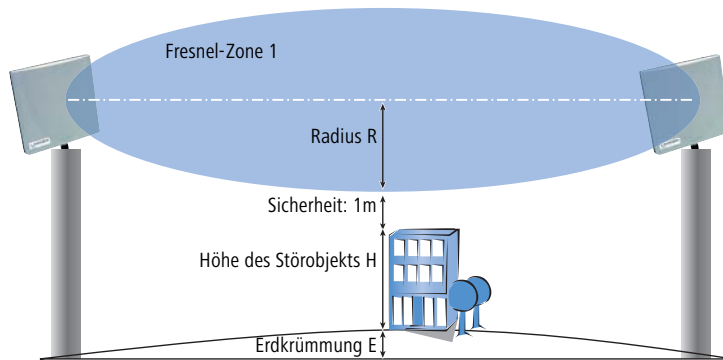
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung (λ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

$$R = 0,5 * \sqrt{\lambda * d}$$

Die Wellenlänge beträgt im 2,4 GHz-Band ca. 0,125m, im 5 GHz-Band ca. 0,06 m.

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 4 km ergibt sich im 2,4 GHz-Band der Radius der Fresnel-Zone 1 zu **11 m**, im 5 GHz-Band nur zu **7 m**.

Damit die Fresnel-Zone 1 frei und ungestört ist, müssen die Antennen das höchste Störobjekt um diesen Radius überragen. Die gesamte erforderliche Masthöhe (M) der Antennen ergibt sich nach folgendem Bild zu:



$$M = R + 1\text{m} + H + E \text{ (Erkrümmung)}$$

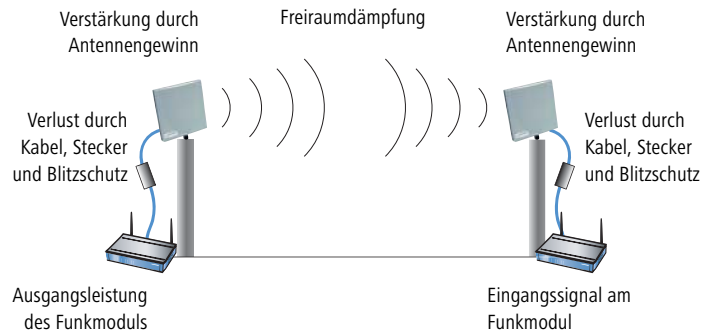
Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu $E = d^2 \cdot 0,0147$ – bei einer Distanz von 8 km also immerhin schon fast 1m!

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 8 km ergibt sich im 2,4 GHz-Band die Masthöhe über dem höchsten Störobjekt von ca. **13 m**, im 5 GHz-Band zu **9 m**.

12.6.2 Antennen-Leistungen

Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden Access Point bis zum Funkmodul im empfangenden Access Point. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft, und verstärkende Elemente wie die externen Antennen.




▷ Aufbau von Outdoor- Funknetz- Strecken

- ① Die Berechnung der Leistungsstrecke beginnt am Funkmodul des Senders. Das Funkmodul in den LANCOM Access Points gibt im 802.11a-Modus die folgenden Leistungen in Abhängigkeit vom verwendeten Kanal und der Datenübertragungsrate ab:

MBit/s	5,150 - 5,250 GHz	5,250 - 5,350 GHz	5,470 - 5,725 GHz	5,725 - 5,850 GHz
6	17	17	17	17
9	17	17	17	17
12	17	17	17	17
18	17	17	17	17
24	17	17	17	17
36	14	14	14	14
48	13	13	13	13
54	12	12	12	12
72 (Turbo)	14	14	14	14
96 (Turbo)	13	13	13	13
108 (Turbo)	12	12	12	12

Bei einer angestrebten Datenübertragungsrate von 24 MBit/s gibt das Funkmodul eine Leistung von 17 dBm ab.

-  Die Datenübertragungsrate wird aufgrund der empfangenen Leistung eingestellt. Ein WLAN-Modul hat eine bestimmte Eingangsempfindlichkeit, die einem Leistungspegel von z.B. -80dBm entspricht. Wird diese unterschritten, ist also die empfangene Leistung zu gering, kann auf eine geringere Datenrate herabgeschaltet werden, die einer besseren Empfindlichkeit mit einem niedrigeren Leistungslevel entspricht.
- ② Bei den Outdoor-Funkstrecken wird üblicherweise eine externe Antenne über ein Verlängerungskabel angeschlossen, zur Sicherheit wird ein Blitzschutz eingesetzt. Das Kabel dämpft die Leistung um ca. 1 dB pro Meter. Bei einem Kabel von z.B. 4 m Länge reduziert sich die Leistung um 4 dB, der Blitzschutz und die Steckverbindungen senken die Leistung zusätzlich um 1 dB. Die Leistung vor der externen Antenne beträgt also:
 $17 \text{ dBm} - 4 \text{ dB} - 1 \text{ dB} = 12 \text{ dBm}$.
- ③ Die an der Antenne aufgenommen Leistung wird dort wieder verstärkt. Eine AirLancer Extender O-18a (mit einem Abstrahlwinkel von 18°) bringt einen „Antennengewinn“ von 18 dBm mit. Die von der Antenne abgestrahlte Gesamtleistung beträgt also:
 $12 \text{ dBm} + 18 \text{ dBm} = 30 \text{ dBm}$.



Diese hier abgestrahlte Leistung muss auf jeden Fall innerhalb der gesetzlichen Grenzen für das Land liegen, in dem Sie die Antenne betreiben!

- ④ Bei der Funkübertragung durch die Luft reduziert sich die Leistung um die so genannte „Freiraum-Dämpfung“ x , die sich aus der Distanz d (in km) zwischen Sender und Empfänger logarithmisch berechnet zu:

$$x = 100 + 20 * \log (d) \text{ [dB] im 2,4 GHz-Band}$$

$$x = 105 + 20 * \log (d) \text{ [dB] im 5GHz-Band}$$

Für eine 802.11a-Übertragung über eine Distanz von 4 km ergibt sich die Freiraumdämpfung x zu:

$$x = 105 \text{ dB} + 20 * \log (4) \text{ dB} = 105 \text{ dB} + 12 \text{ dB} = 117 \text{ dB.}$$

- ⑤ Zu dieser Dämpfung wird noch ein „Sicherheitszuschlag“ von 10 dB addiert, so dass die gesamte Dämpfung für das Beispiel mit 127 dB angenommen werden kann.

- ⑥ Diese Dämpfung zwischen der sendenden und der empfangenden Antenne wird von der Ausgangsleistung der Sendeantenne abgezogen:

$$30 \text{ dBm} - 127 \text{ dBm} = -97 \text{ dBm.}$$

Damit ist die Leistung bestimmt, die bei der empfangenden Antenne aufgenommen wird.

- ⑦ Auch auf der Empfangsseite gibt es wieder verstärkende und dämpfende Elemente. Bei einer gleichen Antenne wie auf der Sendeseite ergibt sich auch hier wieder ein Antennengewinn von 18 dB und ein Verlust durch Kabel (wider 4m), Blitzschutz und Stecker zu 5 dB. Das Funksignal kommt also mit folgender Leistung am Modul des Empfängers an:

$$-97 \text{ dBm} + 18 \text{ dBi} - 5 \text{ dB} = -84 \text{ dBm.}$$

- ⑧ Aus der Tabelle für die Empfangsempfindlichkeit des Funkmoduls ergibt sich daraus die erreichbare Datenrate, in diesem Fall 24 MBit/s:

Empfangsempfindlichkeit 802.11a [dBm]		
MBit/s	5,150 - 5,725 GHz	5,725 - 5,850 GHz
6	-90	-85
9	-89	-84
12	-88	-83
18	-87	-82
24	-85	-80
36	-81	-76
48	-76	-71

▷ *Aufbau von Outdoor- Funknetz- Strecken*

MBit/s	Empfangsempfindlichkeit 802.11a [dBm]	
	5,150 - 5,725 GHz	5,725 - 5,850 GHz
54	-73	-68
72 (Turbo)	-78	-73
96 (Turbo)	-73	-68
108 (Turbo)	-70	-65



Diese Werte sind das Ergebnis einer Berechnung, bei der eine 'Sicherheit' von 10dB eingerechnet worden ist. Da jeder Funkstreckenaufbau individuell andere Bedingungen hat, können diese Werte nur als Orientierung dienen.

12.6.3 Abstrahlleistung und maximale Distanz

Für eine vereinfachte Berechnung der erreichbaren Distanzen bzw. der realisierbaren Datenübertragungsraten können Sie die Werte für AirLancer Extender Antennen den nachfolgenden Tabellen entnehmen. Alle Tabellen berücksichtigen eine Reserve von 10 dB, können also als recht realitätsnah betrachtet werden.

Für jede Antenne zeigt die Tabelle ein Spalte für den Point-to-Point-Betrieb (P2, Verbindung zwischen zwei Access Points) und den Point-2-Multipoint-Betrieb (P2mP, Verbindung von einem Access Point zu den angeschlossenen Clients, z.B. Notebooks).

Die letzte Spalte der Tabellen zeigt jeweils die einzustellende Sendeleistungsreduktion, damit die Obergrenzen von 30 dBm (802.11a) bzw. 20 dBm (802.11b/g) nicht überschritten werden.



Die Angaben bzgl. 802.11a gelten nur für die Länder Deutschland, Niederlande, Luxemburg und Großbritannien. In Belgien, Österreich und der Schweiz ist nur der 802.11b/g-Standard für den Outdoor-Betrieb zugelassen.

AirLancer Extender O-18a (802.11a)

- Antennengewinn: 18 dBi
- angenommener Kabelverlust: 4 dB

MBit/s	maximale Distanz [km]	
	P2P	P2mP
6	7,94	1,78
9	7,08	1,58
12	6,31	1,41

▷ Aufbau von Outdoor- Funknetz- Strecken

MBit/s	maximale Distanz [km]	
	P2P	P2mP
18	5,62	1,26
24	4,47	1,00
36	2,00	0,45
48	1,00	0,22
54	0,63	0,14
72 (Turbo)	1,41	0,32
96 (Turbo)	0,71	0,16
108 (Turbo)	0,45	0,10

AirLancer Extender O-30 (802.11b/g)

- ▶ Antennengewinn: 15 dBi
- ▶ angenommener Kabelverlust: 9 dB

MBit/s	maximale Distanz [km]	
	P2P	P2mP
1,0	2,82	1,58
2,0	2,51	1,41
5,5	2,24	1,26
6,0	2,24	1,26
9,0	2,24	1,26
11,0	2,00	1,12
12,0	1,78	1,00
18,0	1,41	0,79
24,0	1,00	0,56
36,0	0,71	0,40
48,0	0,35	0,20
54,0	0,18	0,10

AirLancer Extender O-70 (802.11b/g)

- ▶ Antennengewinn: 8,5 dBi

▷ *Aufbau von Outdoor- Funknetz- Strecken*

- ▶ angenommener Kabelverlust: 6 dB

MBit/s	maximale Distanz [km]	
	P2P	P2mP
1,0	1,26	1,06
2,0	1,12	0,94
5,5	1,00	0,84
6,0	1,00	0,84
9,0	1,00	0,84
11,0	0,89	0,75
12,0	0,79	0,67
18,0	0,63	0,53
24,0	0,45	0,38
36,0	0,32	0,27
48,0	0,16	0,13
54,0	0,08	0,07

12.6.4 Reduzieren der Sendeleistung

In jedem Land gibt es spezielle Vorschriften über die zulässige Leistung von WLAN-Antennen, oft unterschiedlich je nach verwendetem WLAN-Standard und getrennt nach Indoor- und Outdoor-Einsatz. Die von der externen Antenne abgestrahlte Leistung darf diese maximale Leistung nicht überschreiten. Die relevante Leistung ergibt sich aus der Summe der Funkmodul-Leistung und dem Antennengewinn, abzüglich der Dämpfung durch Kabel, Stecker und Blitzschutz. Die Einstellung der Sendeleistungs-Reduktion ist im Abschnitt 'Radio-Einstellungen' →Seite 369 beschrieben.

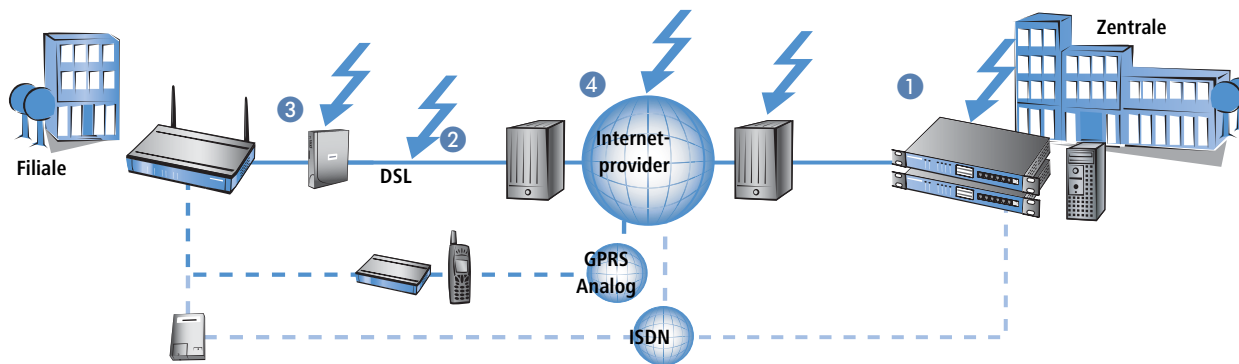
13 Backup- Lösungen

13.1 Hochverfügbarkeit von Netzwerken

Die vernetzte Zusammenarbeit über mehrere Standorte oder sogar über Kontinente hinweg ist aus dem modernen Wirtschaftsleben nicht mehr wegzudenken. Die Kommunikationswege zwischen Zentralen, Filialen oder Außendienstmitarbeitern setzen dabei immer mehr auf öffentliche Infrastrukturen auf. VPN hat sich als defacto-Standard für die kostengünstige und sichere Unternehmenskommunikation über das Internet etabliert.

Allerdings können bei diesen Netzwerkstrukturen eine Reihe von notwendigen Elementen von Störungen betroffen sein, die empfindliche Auswirkungen auf den Geschäftsbetrieb haben:

- ▶ Das entfernte Internet- Gateway ① kann ausfallen.
- ▶ Die physikalischen Leitungen, über die Verbindungen ins Internet oder zu einem entfernten Netzwerk aufgebaut werden, können betroffen sein:
 - ▷ Die Internetzugangsleitung zwischen dem Standort und dem Provider ② kann ausfallen, z.B. durch Beschädigung des Kabels bei Bauarbeiten.
 - ▷ Der DSL-Anschluss an einem Standort ③ kann ausfallen, während die ISDN-Leitungen noch ihren Dienst versehen.
- ▶ Das Netzwerk des Providers ④ kann gestört sein oder ausfallen.



Internet Router und Access Points von LANCOM bieten eine Reihe von Sicherheits- und Backup-Funktionen, mit denen Sie Ihr Netz vor den Folgen dieser Störungen schützen können.

13.1.1 Wie wird die Störung einer Netzwerkverbindung erkannt?

Um eine Netzwerkverbindung vor den Folgen einer Störung schützen zu können, muss zunächst einmal die Störung selbst als solche erkannt werden. Folgende Verfahren bieten sich an, um die Verbindungen zu überprüfen:

▷ *Hochverfügbarkeit von Netzwerken*

- ▶ Überprüfen der PPP-Verbindung bis zum Provider mittels PPP LCP Echo Monitoring.
- ▶ Überprüfen der Erreichbarkeit beliebiger Gegenstellen über Name oder IP-Adresse mit ICMP Polling (Ping von Ende zu Ende).
- ▶ Überprüfen von Tunnelendpunkten mit „Dead-Peer-Detection“ (DPD).

PPP LCP Echo Monitoring

Bei diesem Verfahren wird eine PPP-Verbindung zu einer bestimmten Gegenstelle durch regelmäßige LCP-Anfragen überprüft. Üblicherweise wird mit diesem Verfahren z.B. die Verbindung zum Internet-Provider geprüft. Die LCP-Anfragen werden dabei direkt an den Einwahlknoten gerichtet.

In der PPP-Liste wird dabei für diese Verbindung ein zeitlicher Abstand definiert, in dem die LCP-Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der LCP-Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt die Leitung als gestört.

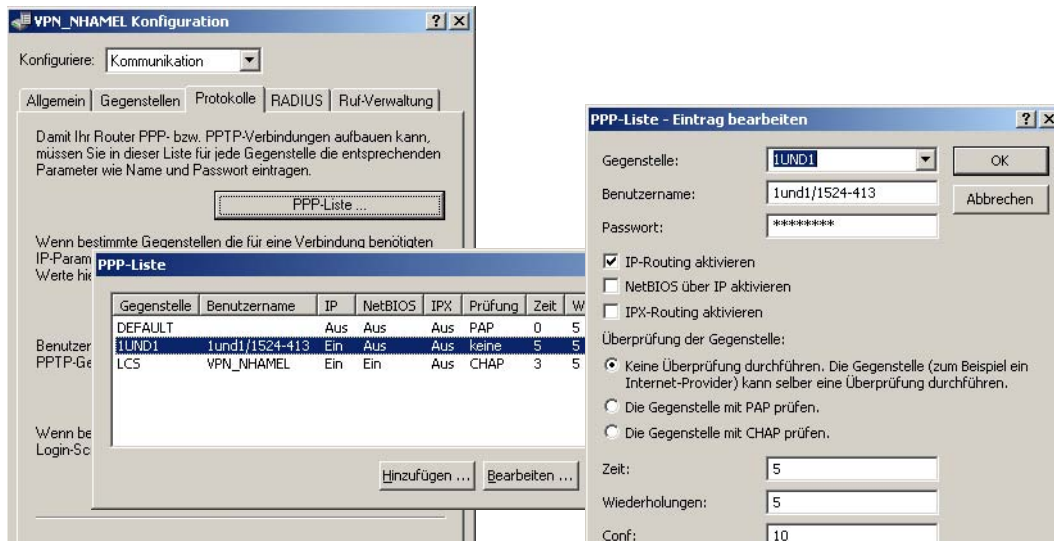
- ▶ **Zeit:** Die in der PPP-Liste eingetragene Zeit muss mit dem Faktor 10 multipliziert werden, um das tatsächliche Intervall zwischen zwei LCP-Anfragen zu erhalten. Ein Eintrag der Zeit von „5“ bedeutet also, dass alle 50 Sekunden eine LCP-Anfrage gestartet wird.
- ▶ **Wiederholungen:** Bleibt die Antwort auf eine LCP-Anfrage aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Ein Eintrag der Wiederholung von „5“ bedeutet also, dass die LCP-Anfrage 5 mal wiederholt wird, bevor die Leitung als gestört betrachtet wird.



Mit dem PPP LCP Monitoring wird nur die PPP-Strecke bis zum Internet-Provider geprüft.

Konfiguration
mit LANconfig

Die Einstellungen für das LCP-Monitoring finden Sie in LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Protokolle' in der 'PPP-Liste'.



Konfiguration
mit
WEBconfig,
Telnet oder
SSH

Unter WEBconfig, Telnet oder SSH-Client finden Sie die Einstellungen für das LCP-Monitoring auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► PPP
Terminal/Telnet	Setup/WAN/PPP

ICMP Polling

Auch beim ICMP-Polling werden ähnlich dem LCP-Monitoring regelmäßig Anfragen an eine Gegenstelle geschickt. Hier werden ping-Befehle abgesetzt, deren Beantwortung überwacht wird. Anders als beim LCP-Monitoring kann für die ICMP-Pings jedoch die Ziel-Gegenstelle frei definiert werden. Mit einem Ping auf einen Router in einem entfernten Netz kann man so die gesamte Verbindung überwachen, nicht nur bis zum Internet-Provider.

In der Polling-Tabelle wird für die Gegenstelle ein Ping-Interval definiert, in dem die Anfragen an die Gegenstelle verschickt werden. Außerdem wird die Anzahl der Wiederholungen definiert, mit der bei Ausbleiben der Antworten erneut eine Anfrage gesendet wird. Erhält der Absender auch auf alle Wiederholungen keine Antwort, gilt das Ziel der Ping-Anfragen als nicht erreichbar.

Zu jeder Gegenstelle können dabei bis zu vier verschiedene IP-Adressen eingetragen werden, die parallel im entfernten Netz geprüft werden. Nur wenn alle eingetragenen IP-Adressen nicht erreichbar sind, gilt die Leitung als gestört.



Mit dem ICMP-Polling kann eine komplette Verbindung von Ende zu Ende überwacht werden.

► Name der Gegenstelle

▷ *Hochverfügbarkeit von Netzwerken*

- **IP-Adresse 1-4:** IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

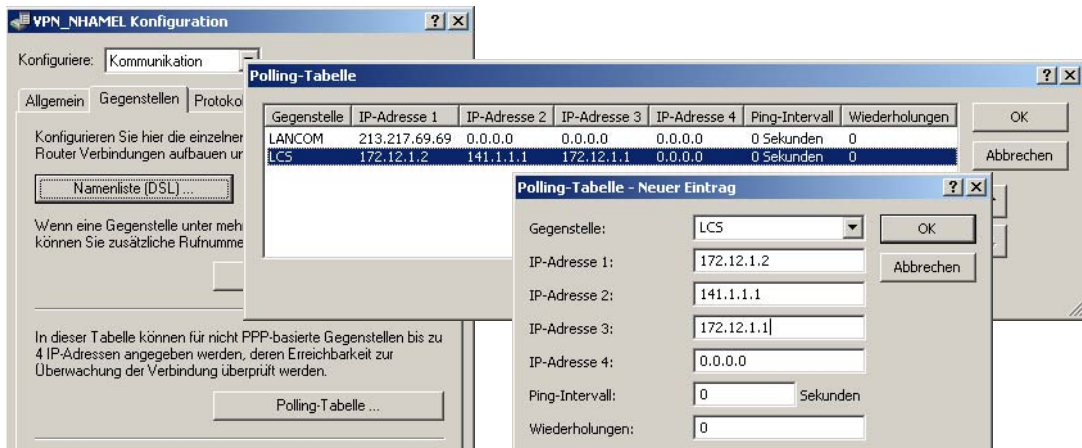


Wird für eine Gegenstelle keine IP-Adresse eingetragen, die mit einem Ping geprüft werden kann, so wird die IP-Adresse des DNS-Servers geprüft, der bei der PPP-Verhandlung übermittelt wurde.

- **Ping-Intervall:** Die in der Polling-Tabelle eingetragene Zeit gibt das Intervall zwischen zwei Ping-Anfragen an. Wird hier eine „0“ eingetragen, gilt der Standardwert von 30 Sekunden.
- **Wiederholungen:** Bleibt die Antwort auf einen Ping aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird. Wird hier eine „0“ eingetragen, gilt der Standardwert von 5 Wiederholungen.

Konfiguration mit LANconfig

Die Einstellungen für das ICMP-Polling finden Sie in LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Gegenstellen' in der 'Polling-Tabelle'.



Konfiguration mit WEBconfig, Telnet oder SSH

Unter WEBconfig, Telnet oder SSH-Client finden Sie die Einstellungen für das LCP-Monitoring auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► WAN ► Polling-Tabelle
Terminal/Telnet	Setup/WAN/Polling-Tabelle

Dead-Peer-Detection (DPD)

Diese Verbindungsüberwachung wird bei der Einwahl von VPN-Clients in ein VPN-Gateway eingesetzt. Damit soll sichergestellt werden, dass ein Client ausgebucht wird, wenn die VPN-Verbindung z.B. durch kurzzeitigen Ausfall der Internetverbindung gestört wurde. Ohne eine entsprechende Leitungsüberwachung würde das VPN-Gateway den

▷ Hochverfügbarkeit von Netzwerken

Client weiter in der Liste der eingebuchten Gegenstelle führen. Eine erneute Einwahl des Clients würde damit verhindert, weil z.B. beim WLANmonitor eine erneute Einwahl mit der gleichen Seriennummer nicht möglich ist.



Aus dem gleichen Grunde würde ohne Leitungsüberwachung die Einwahl eines Benutzers mit gleicher „Identity“ – also gleichem Usernamen – verhindert, da der entsprechende Benutzer weiterhin in der Liste der eingebuchten Clients geführt würde.

Bei der Dead-Peer-Detection tauschen Gateway und Client während der Verbindung regelmäßig „Keep-Alive“-Pakete aus. Bleiben die Antworten aus, bucht das Gateway den Client aus und ermöglicht so nach Wiederherstellen der VPN-Verbindung eine erneute Anmeldung mit der gleichen Identity. Für VPN-Clients wird die DPD-Zeit üblicherweise auf 60 Sekunden eingestellt.

Konfiguration mit LANconfig

Die Einstellungen für die Dead-Peer-Detection finden Sie in LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' in der 'Verbindungs-Liste'.

Name	Haltezeit	DPD	Extranet-Adresse
LCS	30 Sekunden	0 Sekunden	10.99.
CHOFMJDSTER	0 Sekunden	0 Sekunden	0.0.0.
JWRIGHT	0 Sekunden	60 Sekunden	0.0.0.
CHOFMJDSTER2	0 Sekunden	60 Sekunden	0.0.0.
KMUSTERMANN	0 Sekunden	60 Sekunden	0.0.0.
NHAMEL_MOBIL	0 Sekunden	60 Sekunden	0.0.0.
TEST	0 Sekunden	3.000 Sekunden	0.0.0.

Konfiguration mit WEBconfig, Telnnet oder SSH

Unter WEBconfig, Telnnet oder SSH-Client finden Sie die Einstellungen für die Dead-Peer-Detection auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ VPN ▶ Namen-Liste
Terminal/Telnnet	Setup/VPN/Namen-Liste

▷ Hochverfügbarkeit von Netzwerken

13.1.2 Hochverfügbarkeit der Leitungen – die Backup-Verbindung

Wenn eine Verbindung zum Internet-Provider oder zu einem entfernten Netzwerk gestört ist, kann eine Backup-Verbindung temporär die Aufgaben der eigentlichen Datenleitung übernehmen. Voraussetzung dafür ist eine zweite physikalische Leitung, über die die entsprechende Gegenstelle erreicht werden kann. Als typische Backup-Leitungen kommen z.B. in Frage:

- ▶ ISDN-Leitung als Backup für einen DSL-Internetzugang
- ▶ ISDN-Leitung als Backup für eine VPN-Netzwerkkopplung
- ▶ Modem-Verbindung (GSM oder analog) als Backup für DSL- oder ISDN-Leitungen und VPN-Verbindungen

Konfiguration der Backup-Verbindung

Zur Definition einer Backup-Verbindung sind im Prinzip die folgenden Konfigurationsschritte notwendig:

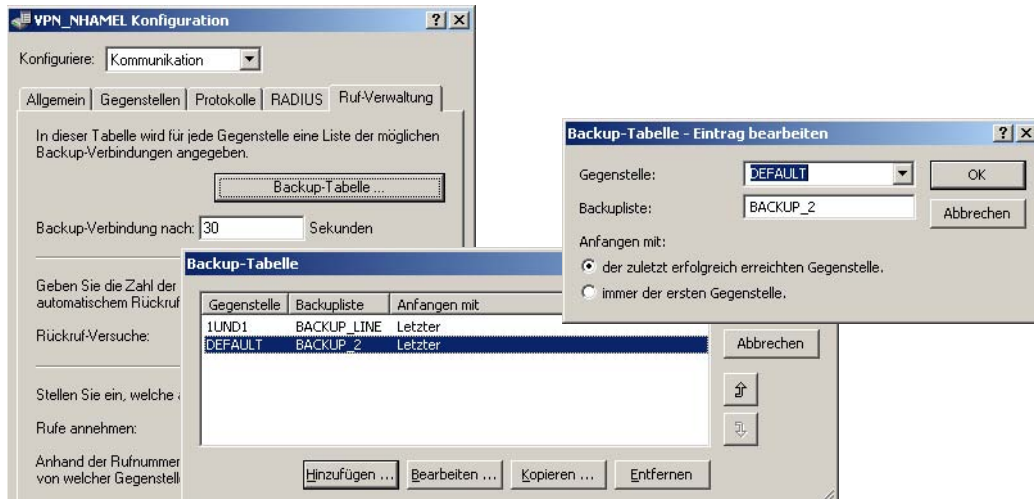
- ① Für die Backup-Verbindung wird auf der entsprechenden WAN-Schnittstelle die Gegenstelle so eingerichtet, dass sie über diesen alternativen Weg erreichbar ist. Soll z.B. die ISDN-Leitung als Backup-Verbindung dienen, wird die Gegenstelle als ISDN-Gegenstelle angelegt (mit den zugehörigen Einträgen bei den Kommunikations-Layern und in der PPP-Liste).
- ② Ggf. müssen Sie zur Überwachung der Verbindung noch einen Eintrag in der Polling-Tabelle anlegen, wenn die Gegenstelle nicht über LCP-Anfragen geprüft werden kann.
- ③ Zuordnung der neuen Backup-Verbindung zu der Gegenstelle, die über das Backup abgesichert werden soll. Diesen Eintrag nehmen Sie in der Backup-Tabelle vor. Für die Backup-Verbindung werden keine eigenen Einträge in der Routing-Tabelle benötigt. Die Backup-Verbindung übernimmt die Quell- und Ziel-Netze automatisch von der Gegenstelle, die im störungsfreien Betrieb die Daten routet.

In der Backup-Tabelle können einer Gegenstelle auch mehrere Backup-Leitungen zugeordnet werden. Dabei wird dann festgelegt, welche der Backup-Leitungen im Bedarfsfalle zuerst aufgebaut werden soll:

- ▷ Die zuletzt erfolgreich erreichte Gegenstelle
- ▷ Immer die erste Gegenstelle in der Liste

Konfiguration
mit LANconfig

Die Backup-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Ruf-Verwaltung' in der 'Backup-Tabelle'.



Konfiguration
mit
WEBconfig,
Telnet oder
SSH

Unter WEBconfig, Telnet oder SSH-Client finden Sie die Einstellungen Backup-Tabelle auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WAN ▶ Backup-Tabelle
Terminal/Telnet	Setup/WAN/Backup-Tabelle

Auslösen der Backup-Verbindung

Der Backup-Fall wird ausgelöst, wenn der für die Verbindung definierte Überwachungsmechanismus (LCP- oder ICMP-Polling) keine Rückmeldung von den überwachten Gegenstellen erhält.

Die Backup-Verbindung wird dann aufgebaut, wenn:

- ▶ Die Backup-Verzögerungszeit abgelaufen ist und
- ▶ entweder
 - ▷ ein Datenpaket übertragen werden soll oder
 - ▷ für die Backup-Verbindung eine Haltezeit von 9999 Sekunden definiert wurde.

Die Backup-Verzögerungszeit wird unter LANconfig im Konfigurationsbereich 'Kommunikation' auf der Registerkarte 'Ruf-Verwaltung' eingetragen oder alternativ unter telnet unter /Setup/WAN/Backup-St. -Sekunden.

▷ Hochverfügbarkeit von Netzwerken

**Rückkehr zur Standard-Verbindung**

Während die Backup-Verbindung die Datenübertragung übernimmt, versucht der Router permanent die Standard-Verbindung wieder aufzubauen. Sobald die Standard-Leitung wieder steht, wird die Backup-Verbindung beendet und die Leitungsüberwachung über LCP- oder ICMP-Polling setzt wieder ein.

Nur Keep-Alive-Verbindungen kommen automatisch zurück!

Die über eine Backup-Verbindung abgesicherte Standard-Verbindung wird nach dem Backup-Fall nur dann automatisch wieder aufgebaut, wenn die Haltezeit der Verbindung richtig konfiguriert ist:

- ▶ Eine Haltezeit mit dem Wert „0“ bedeutet, dass die Verbindung nicht aktiv getrennt wird. Wird die Verbindung jedoch durch eine Störung abgebaut oder abgebrochen, wird sie nicht automatisch neu aufgebaut. Erst wenn eine Kommunikation über die Verbindung angefordert wird, wird diese wieder aufgebaut.
- ▶ Eine Haltezeit mit dem Wert „9999“ bedeutet, dass die Verbindung permanent offen gehalten wird. Bei einer Trennung wird sie sofort wieder aktiv aufgebaut. Dieses Verhalten wird auch als **Keep-Alive** bezeichnet.

Stellen Sie sowohl für die Verbindung zum Internet-Provider (in der entsprechenden Namen-Liste) als auch für backup-gesicherte VPN-Verbindungen (in der VPN-Verbindungsliste) die Haltezeit auf „9999“, damit die Verbindung nach Beenden der Störung automatisch wieder aufgebaut wird und die Datenübertragung übernimmt.

13.1.3 Hochverfügbarkeit der Gateways – redundante Gateways mit VPN Load Balancing

Neben den Leitungen zum Provider oder in eine anderes Netzwerk kann auch das eigene Gateway ausfallen. Besonders nachhaltige Folgen hat das z.B. dann, wenn ein zentrales VPN-Gateway ausfällt, über das sich viele Netzwerke von Außenstellen mit dem Netzwerk der Zentrale verbinden.

Um auch in diesem Fall die Erreichbarkeit der Zentrale zu gewährleisten, können mehrere VPN-Endpunkte (i.d.R. gleich konfigurierte, parallel betriebene zentrale VPN-Gateways) installiert werden. Sobald die Leitungsüberwachung (über Dead-Peer-Detection oder ICMP-Polling) fehlschlägt, kann nach verschiedenen Strategien (z.B. per zufälliger Auswahl aus den verfügbaren Gateways) ein neuer VPN-Endpunkt angesprochen werden. Innerhalb der Zentrale werden die in diesem Fall veränderte Routen das lokale Default-Gateway über dynamisches Routing (RIP V2) propagiert.

▷ Hochverfügbarkeit von Netzwerken

Damit die zusätzlichen VPN-Gateways in einer solchen Installation nicht als „tote Leitungen“ auf ihren Einsatz warten, können sich alle verfügbaren Geräte auch im Normalbetrieb die Last der ein- und ausgehenden Verbindungen teilen und so einen intelligenten „Lastenausgleich“ realisieren.

Weitere Informationen zu redundanten Gateways und zum „Load Balancing“ finden Sie unter 'VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“' →Seite 313.

M.1.4 Hochverfügbarkeit des Internetzugangs – Multi-PPPoE

Als dritte grundsätzlich verschiedene Störungsmöglichkeit betrachten wir den Fall, in dem sowohl die eigenen Gateways als auch die Verbindungsleitungen in Ordnung sind, es aber zu zeitweiligen Störungen im Netzwerk des Providers kommt. Für diesen Fall können in einem Gerät mehrere PPPoE-Verbindungen auf einem physikalischen Interface eingerichtet werden (Multi-PPPoE).

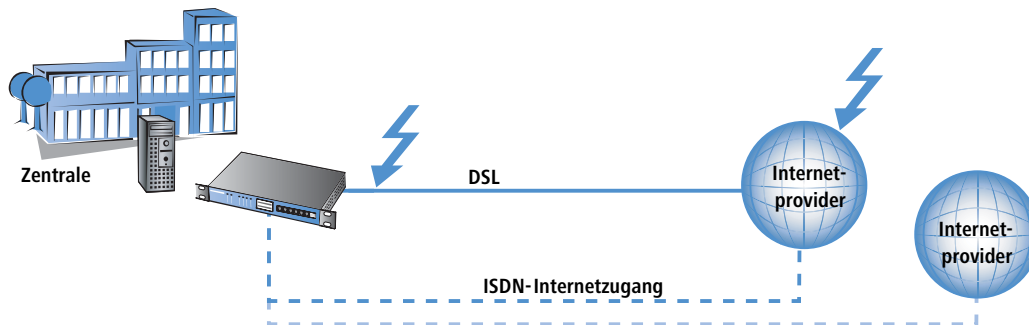
Zur Definition dieser Backup-Lösungen als alternative Internetzugänge richten Sie in Ihrem Gerät z.B. über die Setup-Assistenten nacheinander zwei Internet-Zugänge ein. Der Internet-Zugang, der im Normalfall verwendet werden soll, wird dabei als letzter konfiguriert. Dadurch werden die Einträge in der Routing-Tabelle mit der richtigen Gegenstelle verbunden.

Zusätzlich wird dann in der Backup-Tabelle ein Eintrag gemacht, mit dem die Gegenstelle des Standard-Providers mit dem alternativen Internetzugang abgesichert wird.

Weitere Informationen zur Definition mehrerer PPPoE-Verbindungen finden Sie unter 'Multi-PPPoE' →Seite 128.

13.1.5 Anwendungsbeispiele

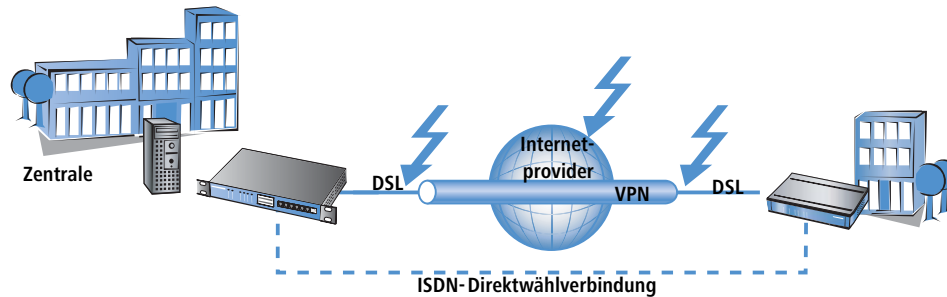
DSL-Internetzugang mit ISDN-Internetzugang absichern



In diesem recht einfachen Backup-Szenario wird der Internetzugang über einen DSL-Zugang realisiert. Für den Fall einer Störung des Internetzugangs über DSL wird eine ISDN-Verbindung als Backup-Leitung definiert.

Diese Backup-Lösung kann z.B. mit Hilfe der Setup-Assistenten von LANconfig sehr komfortabel eingerichtet werden. Als zusätzliche Sicherheit kann für die Backup-Verbindung ein anderer Provider gewählt werden als für den Standard-Zugang: Mit dieser Lösung wird auch der Fall abgedeckt, dass das Netz des Providers gestört ist und der Fehler nicht in der DSL-Leitung zu finden ist.

▷ Hochverfügbarkeit von Netzwerken

Dynamic-VPN-Netzwerkkopplung mit ISDN-Direktwählverbindung absichern

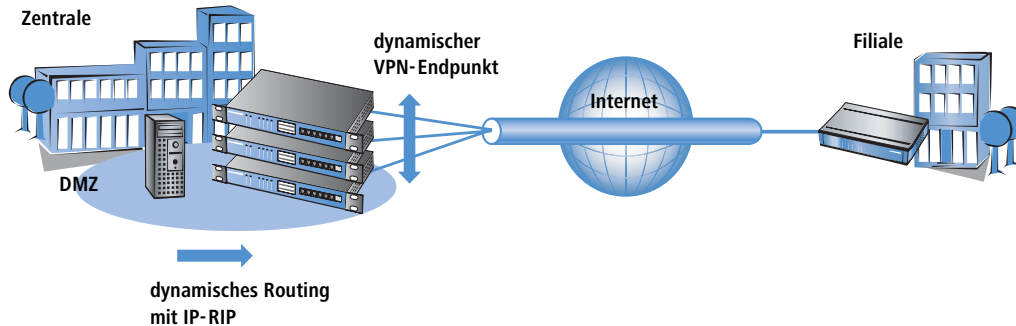
Bei der Anbindung einer Filiale über eine VPN-Verbindung an die Zentrale kann es sinnvoll sein, die internetbasierte VPN-Verbindung durch eine direkte ISDN-Wählverbindung abzusichern. Falls die Internetverbindung bei einem der beiden Router ausfällt, kann die Datenübertragung über die ISDN-Kopplung fortgesetzt werden.

In diesem Szenario gehen wir von einer vollständig konfigurierten VPN-Verbindung zwischen den beiden Netzwerken aus.

- ▶ Zusätzlich wird dann eine LAN-LAN-Kopplung über ISDN zwischen den beiden Netzwerken angelegt. Verwenden Sie für diese Netzwerkkopplung **nicht** die Setup-Assistenten! Die Assistenten würden auch die Einträge in der Routing-Tabelle verändern und damit die funktionierende VPN-Netzwerkverbindung stören. Legen Sie die ISDN-Netzwerkkopplung in den Routern auf beiden Seiten von Hand an – mit den entsprechenden Einträgen für die Gegenstellen in der Gegenstellenliste, der PPP-Liste und mit den benötigten Rufnummern und Zugangskennungen.
- ▶ Legen Sie im Gateway der Zentrale einen Eintrag in der Backup-Tabelle an, der die VPN-Gegenstelle über die direkt anzuwählende ISDN-Gegenstelle absichert.
- ▶ Außerdem legen Sie in der Polling-Tabelle im Router der Zentrale einen Eintrag an, der eine Gegenstelle im Netzwerk der Zentrale überwacht: üblicherweise die LAN-IP-Adresse des entfernten VPN-Gateways. Mit diesem Eintrag wird sichergestellt, dass der Router in der Zentrale umgehend auf eine Störung der VPN-Verbindung reagieren kann.

Wird nun die Verbindung zwischen Zentrale und Filiale irgendwo gestört (auf den Strecken zum Internetprovider oder beim Provider selbst) kann die ISDN-Leitung die Datenübertragung unabhängig vom Internet selbst übernehmen.

Redundante VPN-Gateways



In verteilten Unternehmensstrukturen, die auf Vernetzung der Standorte über VPN setzen, kommt der Verfügbarkeit der zentralen VPN-Gateways eine besondere Bedeutung zu. Nur wenn diese zentralen Einwahlknoten einwandfrei funktionieren, kann die betriebliche Kommunikation reibungslos ablaufen.

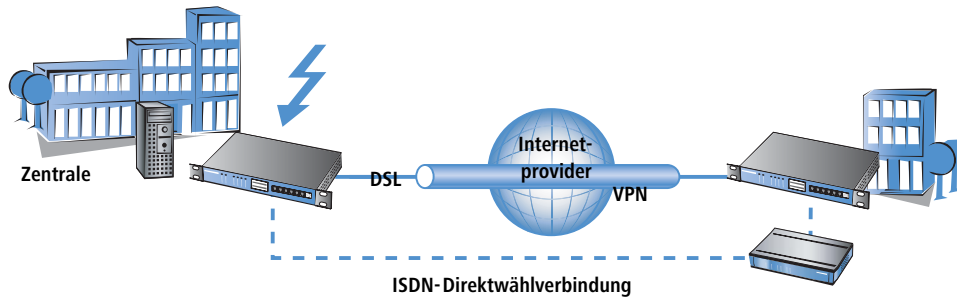
Mit der Möglichkeit, mehrere „Remote-Gateway“-Adressen als „dynamischer VPN-Endpunkt“ für eine VPN-Verbindung zu konfigurieren, bieten LANCOM VPN-Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN-Konfiguration eingesetzt. In den Außenstellen werden alle vorhandenen Gateways als mögliche Gegenstellen für die gewünschte VPN-Verbindung eingetragen. Falls eines der Gateways nicht erreichbar ist, weicht der entfernte Router automatisch auf eine der anderen Gegenstellen aus.

Damit die Rechner im LAN der Zentrale auch wissen, welche Aussenstelle gerade über welches VPN-Gateway erreicht werden kann, werden die jeweils aktuellen Outbound-Routen zu den verbundenen Gegenstellen über RIPv2 im Netzwerk der Zentrale propagiert.

i Wenn die Außenstellen so konfiguriert werden, dass sie beim Aufbau der VPN-Verbindung die Gegenstelle zufällig auswählen, wird mit diesem Mechanismus ein leistungsfähiger Lastenausgleich zwischen den VPN-Gateways in der Zentrale realisiert („VPN Load Balancing“).

Weitere Informationen zu redundanten Gateways und zum „VPN Load Balancing“ finden Sie unter 'VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“' →Seite 313.

▷ Hochverfügbarkeit von Netzwerken

VPN-Gateway mit ISDN-Gateway über RIP absichern

In einem weiteren Schritt können auch die VPN-Gateways selbst gegen Störungen gesichert werden. In diesem Fall betrachten wir eine VPN-Verbindung über zwei entsprechende Gateways. Falls eines der beiden VPN-Geräte gestört ist, soll eine ISDN-Verbindung die Datenübertragung übernehmen, in diesem Fall eine direkte Wahlverbindung.

Zur Konfiguration dieser Lösung gehen wir wieder von einer funktionierenden VPN-Kopplung der beiden Netzwerke aus. Zusätzlich sind noch folgende Schritte erforderlich:

- ▶ Zwischen den beiden ISDN-Routern wird eine normale ISDN-Netzwerkkopplung eingerichtet, die die gleichen Netzbereiche routet wie die VPN-Verbindung. In der Routing-Tabelle wird dabei jedoch eine Distanz eingetragen, die mindestens um 1 höher ist als die entsprechende Route des VPN-Gateways.
- ▶ In allen beteiligten Routern wird das lokale RIP (RIP V2) aktiviert. damit können die VPN- und ISDN-Router jeweils die bekannten Routen zu den gegenüberliegenden Routern austauschen. Mit der höheren Distanz ist die Route im ISDN-Gateway dabei im Normalfall die schlechtere Route.
- ▶ In diesem Fall müssen keine Backup-Verbindungen definiert werden, da im Bedarfsfall ein anderes Gerät die Datenübertragung übernehmen soll.

Wird nun die Verbindung zwischen den beiden VPN-Geräten gestört, ändert sich automatisch der Wert für die Distanz der entsprechenden Routen: eine nicht erreichbare Route wird mit der Distanz 16 markiert. Dadurch wird die im ISDN-Router eingetragene Route automatisch die „bessere“ Lösung, alle Datenpakete werden nun über die ISDN-Stecke geführt. Sobald die VPN-Verbindung wieder hergestellt ist, ändert sich die Distanz wieder auf einen Wert unterhalb der ISDN-Verbindung, der Backup-Fall endet wie gewünscht.

14 Bürokommunikation mit LANCAPI



Die Ausführungen dieses Abschnittes beziehen sich nur auf Geräte mit ISDN-Schnittstelle.

Die LANCAPI von LANCOM Systems ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adapttern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

14.1 Welche Vorteile bietet die LANCAPI ?

Der Einsatz der LANCAPI bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die LANCAPI uneingeschränkten Zugriff auf ISDN-Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofiletransfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle ISDN-Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adapttern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

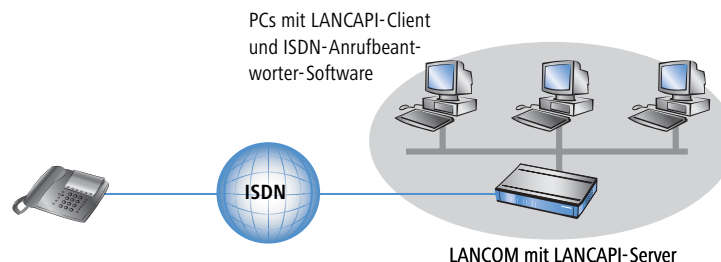
Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein Faxgerät simuliert. Mit der LANCAPI leitet der PC das Fax über das Netzwerk an einen Router weiter, welcher die Verbindung zum Empfänger herstellt.



Alle Anwendungen, die Sie über die LANCAPI betreiben, verwenden direkte ISDN-Verbindungen und laufen nicht über die Router-Funktion des Geräts. Daher werden Firewall- und Gebührenüberwachungsfunktionen in diesem Zusammenhang nicht berücksichtigt. Die LANCAPI ist ebenso unabhängig von allen Routing oder VPN-Funktionen ('System-Design' → Seite 17).

14.2 Das Client-Server-Prinzip

Die LANCAPI besteht aus zwei Komponenten, einem Server (im LANCOM) und einem Client (auf den PCs). Der LANCAPI-Client wird nur auf den Rechnern im lokalen Netz installiert, die die Funktionen der LANCAPI nutzen möchten.



▷ Das Client-Server-Prinzip

14.2.1 Konfiguration des LANCAPI-Servers

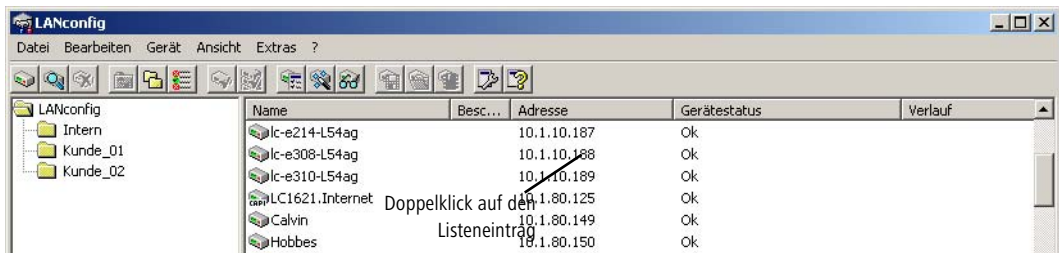
Bei der Konfiguration des LANCAPI-Servers im LANCOM werden im Prinzip zwei Fragen behandelt:

- Auf welche Rufnummer aus dem ISDN-Netz soll die LANCAPI reagieren?
- Welche der Rechner im lokalen Netz sollen über die LANCAPI Zugang zum Telefonnetz erhalten?

Die Konfiguration am Router erfolgt über die Konfigurationstabellen von LANconfig oder WEBconfig. In den folgenden beiden Abschnitten finden Sie Schritt-für-Schritt-Anleitung für jedes dieser Konfigurationsprogramme.

Anleitung für LANconfig

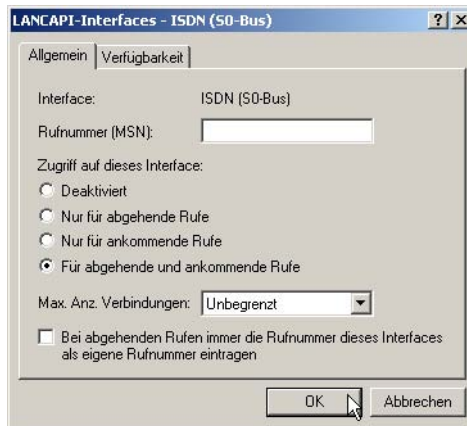
- ① Öffnen Sie die Konfiguration des Routers durch einen Doppelklick auf den Gerätenamen in der Liste und geben Sie auf Nachfrage Ihr Kennwort ein.



- ② Wählen Sie im Konfigurationsbereich 'LANCAPI' auf der Registerkarte 'Allgemein' bei den **LANCAPI-Interfaces** die ISDN-Schnittstelle aus.



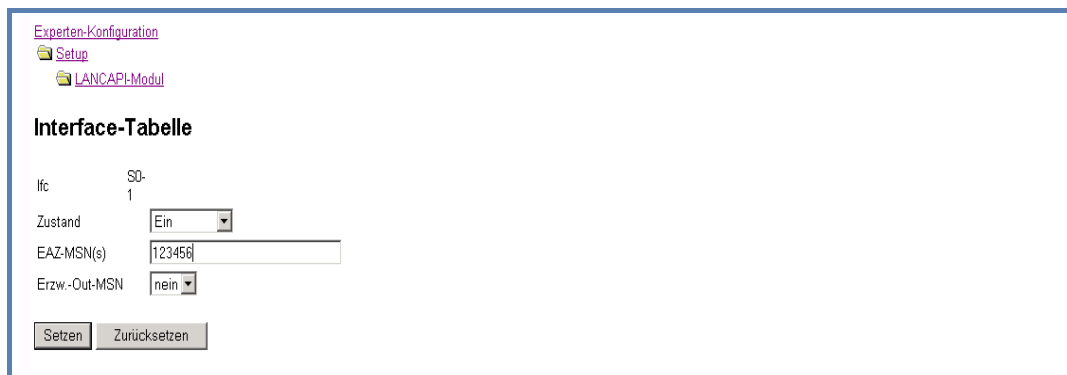
- ③ Aktivieren Sie den LANCAPI-Server für abgehende und ankommende Rufe, oder lassen Sie nur abgehende Anrufe zu.



Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'Rufnummern (MSN/EAZ)' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen.

Anleitung für WEBconfig


- ① Wählen Sie im Hauptmenü die **Experten-Konfiguration**.
- ② Wählen Sie in den folgenden Menüs **Setup** ► **LANCAPI** ► **Interface-Tabelle**.
- ③ Wählen Sie in der **Interface-Tabelle** den (einzigen) Eintrag **S0-1**.
- ④ Aktivieren Sie den LANCAPI-Server für abgehende und ankommende Rufe ('Ein'), oder lassen Sie nur abgehende Anrufe zu ('Abgehend').



▷ *Das Client- Server- Prinzip*

Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'EAZ/MSNs' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen. Bestätigen Sie Ihre Angaben mit **Setzen**.

14.2.2 Installation des LANCAPI-Clients

 Für die Installation des LANCAPI-Clients auf einem System unter Windows XP oder Windows 2000 benötigen Sie Administrator-Rechte.

- ① Legen Sie an einem Client-PC die LANCOM-CD in Ihr CD-ROM-Laufwerk ein. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' im Hauptverzeichnis der LANCOM-CD.
- ② Wählen Sie den Eintrag **LANCOM Systems Software installieren**.
- ③ Markieren Sie die Option **LANCAPI**. Klicken Sie auf **Weiter**, und folgen Sie den Hinweisen der Installationsroutine. Zum Abschluss wird (sofern erforderlich) ein Neustart des Rechners durchgeführt.

Der LANCAPI-Client startet von nun an automatisch. Seinen Status zeigt das zusätzliche Icon in der Windows-Taskleiste (neben der Uhr) an.



= aktiv



= Störung



= inaktiv

14.2.3 Konfiguration des LANCAPI-Clients

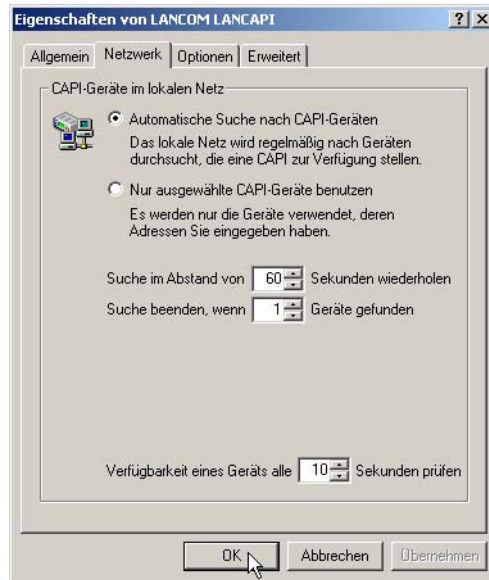
Bei der Einstellung der PC-Clients für die LANCAPI legen Sie fest, welche LANCAPI-Server verwendet werden sollen und wie diese überprüft werden. Wenn Sie nur einen LANCOM in Ihrem LAN als LANCAPI-Server betreiben, können Sie im Prinzip alle Parameter in den Voreinstellungen belassen.

- ① Starten Sie den LANCAPI-Client aus der Programmgruppe 'LANCOM Systems'. Auf der Registerkarte 'Allgemein' finden Sie Informationen zum Treiber zum bereitgestellten Dienst.
- ② Wechseln Sie im LANCAPI-Client auf das Register **Netzwerk**. Hier können Sie zunächst wählen, ob der PC seinen LANCAPI-Server selbst suchen soll oder ob ein bestimmter Server (und damit eine bestimmte ISDN-Leitung) verwendet werden soll.
 - ▷ Im ersten Fall legen Sie fest, in welchem zeitlichen Intervall der Client nach einem Server sucht. Dabei sucht er so lange, bis er die im nächsten Feld eingestellte Anzahl an Servern gefunden hat. Hat er die geforderte Zahl an Servern gefunden, hört er mit der Suche auf.
 - ▷ Wenn der Client nicht automatisch nach Servern suchen soll, geben Sie in der Liste die IP-Adressen der Server an, die der Client verwenden soll. Diese Festlegung ist z.B. dann sinnvoll, wenn Sie mehrere LANCOM in

▷ So setzen Sie die LANCAPI ein

Ihrem LAN als LANCAPI-Server betreiben und eine Gruppe von PCs einen bestimmten Server verwenden sollen.

- ▷ Für beide Optionen können Sie auch einstellen, in welchem Intervall der Client prüft, ob die gefundenen oder per Liste definierten Server noch aktiv sind.



14.3 So setzen Sie die LANCAPI ein

Zur Verwendung der LANCAPI gibt es zwei Möglichkeiten:

- ▶ Sie setzen eine Software ein, die direkt auf einer CAPI-Schnittstelle (in diesem Fall der LANCAPI) aufsetzt. Eine solche Software sucht bei der Installation nach der CAPI und verwendet diese anschließend automatisch.
- ▶ Andere Programme, wie LapLink, können Verbindungen über verschiedene Wege aufbauen, z.B. über das DFÜ-Netzwerk von Windows. Beim Anlegen einer neuen DFÜ-Verbindung können Sie auswählen, welches der installierten Kommunikationsgeräte Sie verwenden möchten. Wählen Sie für die LANCAPI den Eintrag 'ISDN WAN Line 1'.

14.4 Das LANCOM CAPI Faxmodem

Mit dem LANCOM CAPI Faxmodem steht Ihnen unter Windows ein Faxtreiber (Fax Class 1) zur Verfügung, der als Schnittstelle zwischen dem LANCAPI-Client und der Faxanwendung auf dem PC den Betrieb von Standard-Faxprogrammen über ein LANCOM ermöglicht.

▷ LANCOM Faxmodem- Option

Das LANCOM CAPI Faxmodem emuliert die Modem-Funktion sowie die Fax-Protokolle in der Software auf dem PC. Hierzu wird eine ausreichende Rechnerleistung (ab ca. 500 MHz Pentium) benötigt.

Installation

Das LANCOM CAPI Faxmodem wird über das CD-Setup installiert. Installieren Sie das LANCOM CAPI Faxmodem immer zusammen mit der aktuellen LANCAPI. Nach dem Neustart steht Ihnen im System das LANCOM CAPI Faxmodem zur Verfügung, z. B. unter Windows 98 unter **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Modems**.

Faxen über CAPI Faxmodem

Das CAPI Faxmodem wird von den gängigen Faxprogrammen bei der Installation automatisch erkannt und als 'Class 1'-Faxmodem identifiziert. Damit sind Faxübertragungen mit bis zu 14.400 bit/s möglich. Falls Ihr Faxprogramm eine Unterscheidung erlaubt (z. B. WinFax bzw. Talkworks Pro), wählen Sie bei der Einrichtung des Modems die Option 'CLASS 1 (Software Flow Control)' aus

Faxen unter Windows 2000 und XP

Windows XP oder Windows 2000 bieten im Zusammenspiel mit dem CAPI Faxmodem volle Faxfunktionalität. Ein zusätzliches Faxprogramm ist nicht erforderlich.

Dazu starten Sie in der Systemsteuerung unter "Software" "Windows Komponenten hinzufügen / entfernen" und wählen die "Faxdienste" aus.

Nach der Installation befindet sich das Fax unter "Drucker und Faxgeräte", und kann von jedem Windows-Programm anstelle eines Drucker ausgewählt werden.



Das CAPI Faxmodem ist nur dann für die Übertragung von Faxnachrichten bereit, wenn die LANCAPI aktiv ist.

14.5 LANCOM Faxmodem- Option

Neben dem CAPI Faxmodem steht für einige LANCOM-Modelle (LANCOM 800, 4000, 4100) darüber hinaus die Faxmodem-Option zur Verfügung. Bei dieser Lösung sind die Fax- und Modem-Dienste im LANCOM selbst realisiert, die PCs werden von den Belastungen der Modem-Emulation befreit.

14.6 Unterstützte B-Kanal-Protokolle

Folgende CAPI-Protokolle werden unterstützt:

We rt	Bemerkung
B1-Protokoll	
0	64 KBit/s mit HDLC Framing
1	64 KBit/s transparent mit Byte-Framing des Netzwerks
2	V.110 asynchron mit Start-Stop-Byte-Framing
4*	T.30-Modem für Fax Gruppe 3
7*	Modem mit vollständiger Verhandlung (B2 muss 7 sein)
B2-Protokoll	
0	ISO 7776 (X.75 SLP)
1	Transparent
4*	T.30 für Fax Gruppe 3
7*	Modem mit vollständiger Verhandlung (z.B. V.42 bis, MNP 5)
9	V.120 asynchron
B3-Protokoll	
0	Transparent
1	T.90NL, kompatibel zu T.70NL in Übereinstimmung mit T.90, Anhang II
2	ISO 8208 (X.25 DTE-DTE)
4*	T.30 für Fax Gruppe 3
5*	T.30 für Fax Gruppe 3 erweitert
7*	Modem

* = Gilt nur für LANCOM Faxmodem-Option

▷ *Automatische IP-Adressverwaltung mit DHCP*

15 Weitere Dienste

Ein LANCOM bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- ▶ Automatische Adressverwaltung mit DHCP
- ▶ Namenverwaltung von Rechnern und Netzwerken mit DNS
- ▶ Protokollierung von Netzverkehr mit SYSLOG
- ▶ Gebührenerfassung
- ▶ Bürokommunikations-Funktionen mit LANCAPI
- ▶ Zeit-Server

15.1 Automatische IP-Adressverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen.

Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, allen Rechnern im Netz „von Hand“ diese Adressen einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe.

In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

Die LANCOM-Geräte verfügen über einen eingebauten DHCP-Server, der die Zuweisung der IP-Adressen im LAN übernehmen kann. Wenn im lokalen Netz schon ein anderer DHCP-Server vorhanden ist, kann das Gerät alternativ im DHCP-Client-Modus selbst die benötigten Adress-Informationen von dem anderen DHCP-Server beziehen.

15.1.1 Der DHCP-Server

LANCOM kann als DHCP-Server die IP-Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

- ▶ IP-Adresse
- ▶ Netzmaske
- ▶ Broadcast-Adresse
- ▶ Standard-Gateway
- ▶ DNS-Server
- ▶ NBNS-Server
- ▶ Gültigkeitsdauer der zugewiesenen Parameter

▷ Automatische IP- Adressverwaltung mit DHCP

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adress-Pool oder ermittelt die Adressen selbstständig aus der eigenen IP-Adresse (oder Intranet-Adresse).

Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbstständig festlegen.

Im einfachsten Fall müssen Sie daher nur das neue Gerät im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der DHCP-Server regelt im Zusammenspiel mit LANconfig über einen Assistenten dann alle weiteren Adresszuweisungen im lokalen Netz selbst.

15.1.2 DHCP – 'Ein', 'Aus', 'Auto', 'Client' oder 'Weiterleiten'?

Der DHCP-Server kann die folgenden verschiedene Zustände annehmen:

- ▶ 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft.
 - ▷ Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
 - ▷ Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.



Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.

- ▶ 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- ▶ 'Auto': In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED.
 - ▷ Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Damit wird u.a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.
 - ▷ Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem spätern Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wechselt das Gerät automatisch wieder in den DHCP-Client-Modus.
- ▶ 'Client': Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN.



Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

▷ Automatische IP-Adressverwaltung mit DHCP

- ▶ 'Weiterleiten': Der DHCP-Server ist eingeschaltet, das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkbereich weiter.

Ob der DHCP-Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

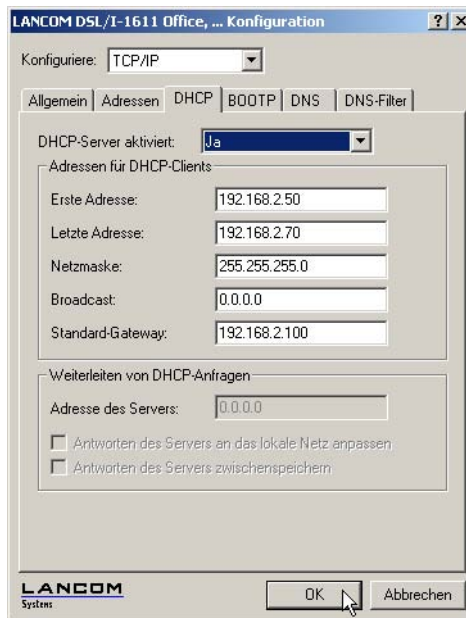
Die Default-Einstellung für den Zustand ist 'Auto'.

15.1.3 So werden die Adressen zugewiesen

Zuweisung von IP-Adressen

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muss er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- ▶ Die IP-Adresse kann aus dem eingestellten Adress-Pool genommen werden (Start-Adress-Pool bis End-Adress-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.



- ▶ Wird stattdessen '0.0.0.0' eingegeben, so ermittelt der DHCP-Server selbstständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für die DMZ-Adresse oder Intranet-Adresse im 'TCP/IP-Modul'. Dabei wird wie folgt vorgegangen:
 - ▷ Ist nur die Intranet-Adresse oder nur die DMZ-Adresse eingegeben, so wird über die zugehörige Netzmaske der Start bzw. das Ende des Pools bestimmt.

▷ Automatische IP- Adressverwaltung mit DHCP

- ▷ Sind beide angegeben, so hat die Intranet-Adresse den Vorrang bei der Bestimmung des Pools.

Aus der verwendeten Adresse (Intranet- oder DMZ-Adresse) und der zugehörigen Netzmaske ermittelt der DHCP-Server die erste und die letzte mögliche IP-Adresse im lokalen Netz als Start- bzw. End-Adresse des Adress-Pools.

- ▶ Wenn der Router weder eine eigene Intranet- noch eine DMZ-Adresse hat, befindet sich das Gerät in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '172.23.56.254' und den Adress-Pool '172.23.56.x' für die Zuweisung der IP-Adressen im Netz.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Server die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adresszuweisung. Wenn im DHCP-Modul eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem TCP/IP-Modul verwendet. Die Reihenfolge ist dabei die gleiche wie bei der Adresszuweisung.

Zuweisung der Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z.B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.



Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

Zuweisung des Standard-Gateways

Das LANCOM weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu. Falls erforderlich, kann diese Zuweisung durch die Einstellungen am Arbeitsplatzrechner überschrieben werden.

Zuweisung von DNS- und NBNS-Server

Hierzu werden die zugehörigen Einträge aus dem 'TCP/IP-Modul' herangezogen.

▷ Automatische IP-Adressverwaltung mit DHCP

Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse als DNS-Adresse weiter. Diese wird bestimmt, wie unter 'Zuweisung einer IP-Adresse' beschrieben. Der Router verwendet dann DNS-Forwarding (siehe auch 'DNS-Forwarding'), um DNS- oder NBNS-Anfragen des Hosts aufzulösen.

Gültigkeitsdauer einer Zuweisung

Die dem Rechner einmal zugewiesenen Adressen haben nur eine begrenzte Gültigkeit. Nach Ablauf dieser Gültigkeitsdauer darf der Rechner sie nicht mehr verwenden. Damit der Rechner die Adressen (vor allem seine IP-Adresse) danach nicht immer wieder verliert, beantragt er rechtzeitig eine Verlängerung, die ihm in der Regel auch immer gewährt wird. Nur wenn die Gültigkeitsdauer abläuft, während der Rechner abgeschaltet ist, verliert er die Adresse.

Bei jeder Anfrage kann ein Host eine bestimmte Gültigkeitsdauer fordern. Ein DHCP-Server kann dem Host aber auch eine davon abweichende Gültigkeitsdauer zuweisen. Das DHCP-Modul bietet zwei Einstellungen, um die Gültigkeitsdauer zu beeinflussen:

▶ Maximale Gültigkeit in Minuten

Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

Fordert ein Host eine Gültigkeit an, die die maximale Dauer überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!

Die Voreinstellung von 6000 Minuten entspricht ca. 4 Tagen.

▶ Default-Gültigkeit in Minuten

Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Die Voreinstellung von 500 Minuten entspricht ca. 8 Stunden.

Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, dass die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Windows-Einstellungen mit einem Klick auf **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk**. Wählen Sie den Eintrag für **TCP/IP** Ihres Netzwerkadapters, und öffnen Sie die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z.B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

Unter Windows geschieht das z.B. über die Eigenschaften der Netzwerkumgebung.

Klicken Sie auf **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

IP-Adressen im LAN überprüfen

Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ DHCP ▶ Tabelle-DHCP
Terminal/Telnet	Setup/DHCP/Tabelle-DHCP

Eine Übersicht über die IP-Adressen im LAN gibt die DHCP-Tabelle. Sie zeigt die zugewiesene bzw. verwendete IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adresszuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- ▶ 'neu'
Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- ▶ 'unbek.'
Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- ▶ 'stat.'
Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.
- ▶ 'dyn.'
Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

15.2 DNS

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet, um z.B. einer Anfrage nach 'www.lancom.de' die entsprechende IP-Adresse zurückliefern zu können. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuzuordnen zu können.

15.2.1 Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: Ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z.B. 'www.domain.com' oder 'ftp.domain.com' heißen.

▷ DNS

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die Default-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, die Funktionen des DNS-Servers direkt im LANCOM anzusiedeln:

- ▶ Ein LANCOM kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.
- ▶ Beim Routing von Windows-Netzen über NetBIOS kennt ein LANCOM außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Namen und Adressen bekannt.
- ▶ Der DNS-Server im LANCOM kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Wie reagiert der DNS-Server auf eine Anfrage?

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- ▶ Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, dass er auf diesen Namen nicht zugreifen darf.
- ▶ Dann sucht er in der eigenen statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- ▶ Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- ▶ Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-Informationen kann bei Bedarf ausgeschaltet werden.
- ▶ Schließlich prüft der DNS-Server, ob die Anfrage über ein WAN-Interface an einen anderen DNS-Server weitergeleitet werden soll (Spezielles DNS-Forwarding über die DNS-Destinationstabelle).

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den generellen DNS-Forwarding-Mechanismus an einen anderen DNS-Server (z. B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

15.2.2 DNS-Forwarding

Wenn eine Anfrage nicht aus den eigenen DNS-Tabellen bedient werden kann, leitet der DNS-Server die Anfrage an andere DNS-Server weiter. Dieser Vorgang heißt DNS-Forwarding (DNS-Weiterleitung).

Dabei unterscheidet man zwischen

- ▶ **speziellem DNS-Forwarding**
Anfragen nach bestimmten Namensbereichen werden an bestimmte DNS-Server weitergeleitet.
- ▶ **generellem DNS-Forwarding**
Alle anderen nicht näher spezifizierten Namen werden an den „übergeordneten“ DNS-Server weitergeleitet.

Spezielles DNS-Forwarding

Beim speziellen DNS-Forwarding können Namensbereiche definiert werden, für deren Auflösung festgelegte DNS-Server angesprochen werden.

Ein typischer Anwendungsfall für spezielles DNS-Forwarding ergibt sich beim Heimarbeitsplatz: Der Benutzer möchte gleichzeitig sowohl auf das firmeneigene Intranet als auch direkt auf das Internet zugreifen können. Die Anfragen ins Intranet müssen an den DNS-Server der Firma, alle anderen Anfragen an den DNS-Server des Internet-Providers geleitet werden.

Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen DNS-Server weitergeleitet. Dieser DNS-Server bestimmt sich nach folgenden Regeln:

- ▶ Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird er dort gefunden, holt er die gewünschte Information von diesem Server. Bis zu zwei übergeordnete DNS-Server können angegeben werden.

LANconfig	TCP/IP ▶ Adressen ▶ Erster DNS-Server / Zweiter DNS-Server
WEBconfig	Experten-Konfiguration ▶ Setup ▶ TCP/IP ▶ DNS-Default ▶ DNS-Backup
Terminal/Telnet	/Setup/TCP-IP/DNS-Default /Setup/TCP-IP/DNS-Backup

- ▶ Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z. B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- ▶ Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der Intranet-Adresse Ihres Routers als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z. B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder sollten Sie zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

▷ DNS

15.2.3 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie im folgenden Menü bzw. in folgender Liste:

Konfigurationstool	Aufruf/Tabelle
LANconfig	TCP/IP ► DNS-Server
WEBconfig	Experten-Konfiguration ► Setup ► DNS
Terminal/Telnet	cd /Setup/DNS

Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

- 1 Schalten Sie den DNS-Server ein.

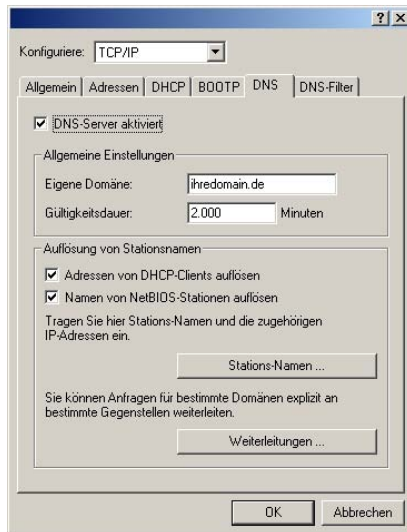
WEBconfig	... ► Zustand
Terminal/Telnet	set Zustand ein

- 2 Geben Sie die Domain ein, in der sich der DNS-Server befindet. Mit Hilfe dieser Domain erkennt der DNS-Server bei Anfrage, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

WEBconfig	... ► Domain
Terminal/Telnet	set Domain ihredomain.com

- 3 Geben Sie an, ob die Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwendet werden sollen.

WEBconfig	... ► DHCP-verwenden ... ► NetBIOS-verwenden
Terminal/Telnet	set DHCP-verwenden ja set NetBIOS-verwenden ja



Aktivierter DNS-Server
in der TCP-IP-Konfiguration

- ④ Der DNS-Server dient hauptsächlich dazu, Anfragen nach Namen im Internet von den Anfragen nach Namen bei anderen Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die Stations-Namen-Tabelle ein,
- ▷ deren Name und IP-Adresse Sie kennen,
 - ▷ die nicht im eigenen LAN liegen,
 - ▷ die nicht im Internet liegen und
 - ▷ die über den Router erreichbar sind.

Mit folgenden Befehlen fügen Sie Stationen zur Stations-Namen-Tabelle hinzu:

LANconfig	TCP/IP ▶ DNS ▶ Stations-Namen ▶ Hinzufügen
WEBconfig	... ▶ DNS-Tabelle ▶ Hinzufügen
Terminal/Telnet	<pre>cd Setup/DNS/DNS-Tabelle set mail.ihredomain.de 10.0.0.99</pre>

Wenn Sie z.B. in einem externen Büro arbeiten und über den Router den Mailserver in der Zentrale (Name: mail.ihredomain.de, IP: 10.0.0.99) erreichen wollen, tragen Sie ein:



Die Angabe der Domain ist dabei optional, aber zu empfehlen.

▷ DNS

Wenn Sie nun das Mailprogramm starten, wird es vermutlich automatisch den Server 'mail.ihredomain.de' suchen. Der DNS-Server gibt daraufhin die IP-Adresse '10.0.0.99' zurück. Das Mailprogramm sucht dann nach dieser IP-Adresse. Mit entsprechenden Einträgen in IP-Routing-Tabelle und Gegenstellenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

- ⑤ Um ganze Namensbereiche von einem anderen DNS-Server auflösen zu lassen, fügen Sie einen Weiterleitungseintrag bestehend aus Namensbereich und Gegenstelle hinzu:

LANconfig	TCP/IP ► DNS ► Weiterleitungen ► Hinzufügen
WEBconfig	... ► DNS-Destinationstabelle ► Hinzufügen
Terminal/Telnet	cd Setup/DNS/Destinationstabelle set *.intern FIRMA

Bei der Angabe der Namensbereiche dürfen die Wildcards '?' für einzelne Zeichen und '*' für mehrere Zeichen verwendet werden.

Um alle Domains mit der Endung '.intern' auf einen DNS-Server im LAN der Gegenstelle 'FIRMA' umzuleiten, erstellen Sie folgenden Eintrag:



- ! Der DNS-Server kann entweder über den Name der Gegenstelle (für automatische Konfiguration über PPP) oder die explizite IP-Adresse des zuständigen Nameservers angegeben werden

15.2.4 URL-Blocking

- ① Mit der Filterliste können Sie schließlich den Zugriff auf bestimmte Namen oder Domains sperren.

Um die Domain (in diesem Fall den Web-Server) 'www.gesperrt.de' für alle Rechner im LAN zu sperren, sind die folgenden Befehle und Eingaben notwendig:

LANconfig	TCP/IP ► DNS-Filter ► DNS-Filter ► Hinzufügen
WEBconfig	... ► Filter-Liste ► Hinzufügen
Terminal/Telnet	cd Setup/DNS/Filter-Liste set 001 www.gesperrt.de 0.0.0.0 0.0.0.0

Der Index '001' kann bei der Konfiguration über Telnet oder WEBconfig frei gewählt werden und dient nur der eindeutigen Bezeichnung des Eintrags.



Bei der Eingabe der Domäne sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt.

Um nur einem bestimmten Rechner (z. B. mit IP 10.0.0.123) den Zugriff auf DE-Domains zu sperren, tragen Sie folgende Werte ein:

Im Konsolenmodus lautet der Befehl:

```
set 002 *.de 10.0.0.123 255.255.255.255
```



Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

15.2.5 Dynamic DNS

Damit auch Systeme mit dynamischen IP-Adressen über das WAN - also beispielsweise über das Internet - erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server Anbietern (z.B. www.dynDNS.org).

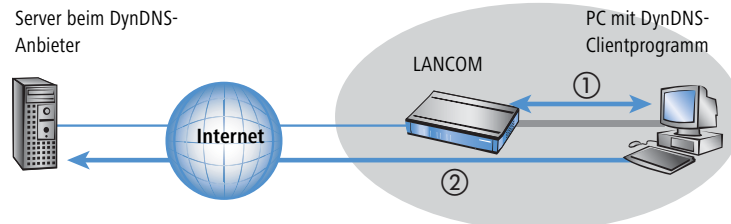
Damit wird ein LANCOM immer unter einem bestimmten Namen (FQDN - 'fully qualified domain name') erreichbar (z.B. "http://MyLANCOM.dynDNS.org").

Der Vorteil liegt auf der Hand: Wenn Sie z.B. eine Fernwartung an einem Anschluss ohne ISDN durchführen wollen (z.B. über WEBconfig / HTTPS), oder über den LANCOM VPN-Client auf eine Außenstelle mit dynamischer IP-Adresse zugreifen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen.

▷ DNS

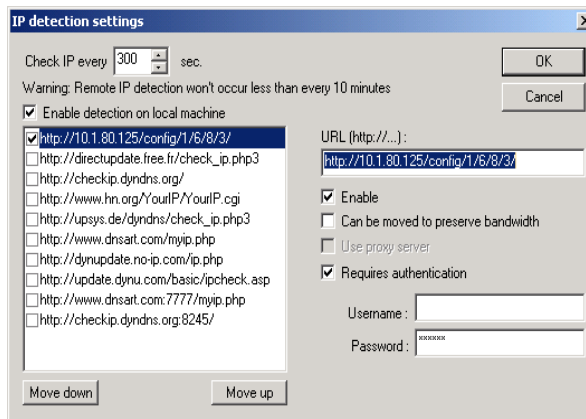
Wie gelangt die aktuelle IP-Adresse zum Dynamic DNS Server?

Dynamic DNS Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines LANCOM ermitteln können ①, und im Falle einer Änderung an den jeweiligen Dynamic DNS Server übertragen ②.

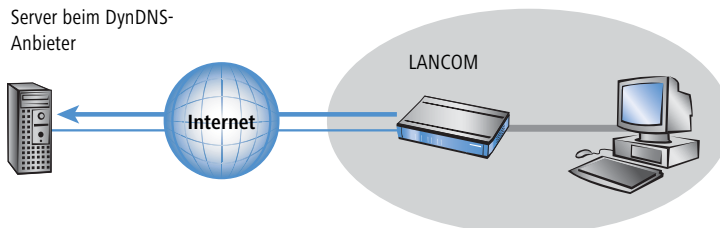


Die aktuelle WAN-seitige IP-Adresse eines LANCOM kann unter folgender Adresse ausgelesen werden:

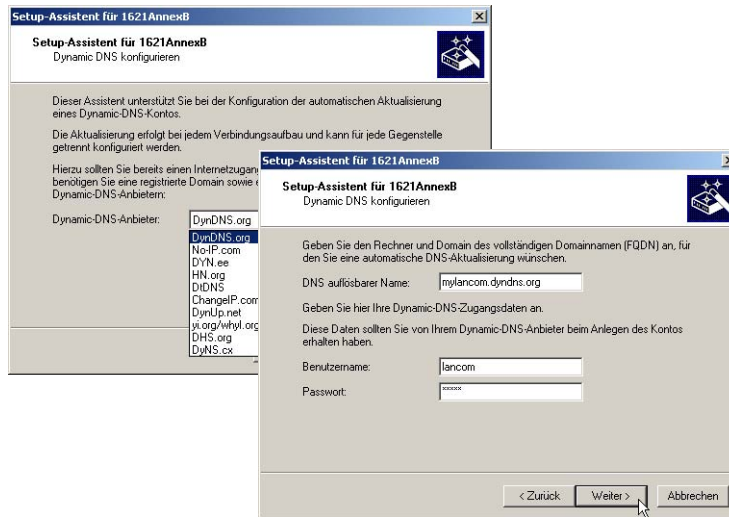
`http://<Adresse des LANCOM>/config/1/6/8/3/`



Alternativ kann das LANCOM die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:



Die dazu notwendigen Einstellungen können komfortabel mit dem Setup-Assistenten von LANconfig vorgenommen werden:



15.3 Gebührenmanagement

Die Eigenschaft des Routers, Verbindungen selbstständig zu allen gewünschten Gegenstellen aufzubauen und sie mit dem Ende der Übertragung automatisch wieder zu beenden, ermöglicht dem Benutzer sehr komfortablen Zugriff z. B. auf das Internet. Bei der Datenübertragung über kostenpflichtige Leitungen können jedoch durch Fehlkonfiguration des Routers (z. B. bei der Filterkonfiguration) oder durch übermäßigen Gebrauch des Angebots (z.B. andauerndes Surfen im Internet) recht hohe Kosten entstehen.

Um diese Kosten zu begrenzen, bietet die LCOS verschiedene Möglichkeiten:

- ▶ Die verfügbaren Online-Minuten können für eine bestimmte Periode eingeschränkt werden.
- ▶ Für ISDN-Verbindungen kann für eine bestimmte Periode ein Gebührenlimit oder ein Zeitlimit festgelegt werden.

15.3.1 Verbindungs-Begrenzung für DSL und Kabelmodem

Auch wenn sich eine DSL- oder eine Kabelmodem-Verbindung wie eine Festverbindung verhält, bei der kein Verbindungsaufbau notwendig ist (und damit auch eigentlich weder Anfang noch Ende der Verbindung erkennbar sind), werden die Kosten je nach Provider zeitabhängig berechnet.



Im weiteren Verlauf dieses Abschnitts wird nur noch von DSL-Verbindungen die Rede sein. Die Ausführungen gelten aber genauso für jede andere Verbindung, die über den Ethernet-WAN-Anschluss des LANCOM erfolgt, beispielsweise für Kabelmodem-Verbindungen.

▷ *Gebührenmanagement*

Um die Kosten begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeit-Limit für DSL-Verbindungen in einer Periode vereinbart. Im Auslieferungszustand dürfen die DSL-Verbindungen z.B. für maximal 600 Minuten in sechs Tagen genutzt werden.



Wird die Grenze eines Budgets erreicht, werden automatisch alle offenen DSL-Verbindungen beendet. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigeben!



Wenn für die Verbindung, die mit dem Gebührenbudget begrenzt werden soll, in der Gegenstellenliste eine Haltezeit von '0' oder '9999' Sekunden eingestellt ist, wird die Gebührenüberwachung ausgeschaltet, die Verbindung trotz Erreichen des Limits nicht unterbrochen

Wenn Sie für einmalige Aktionen das Online-Budget verlängern wollen, z. B. um eine sehr große Datei aus dem Internet zu laden, müssen Sie nicht unbedingt das Zeit-Limit verändern. Sie können für solche Fälle manuell das Limit zurücksetzen.

Klicken Sie dazu mit der rechten Maustaste auf die Fehlermeldung im LANmonitor und wählen Sie im Kontextmenü den Eintrag 'Zeit- und Gebührenlimit zurücksetzen':



Sollten Sie in LANmonitor die System-Informationen nicht sehen, aktivieren Sie die entsprechende Anzeige mit **Ansicht ▶ Anzeigen ▶ System-Informationen**.

In WEBconfig und in der Konsole lauten die Befehle zur Freischaltung des zusätzlichen Zeit-Limits:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Gebuehren ▶ Aktivieren-Reserve
Terminal/Telnet	cd /Setup/Gebuehren do Aktivieren-Reserve

Bei Aktivierung des zusätzlichen Zeit-Limits wird dieses für die aktuelle Periode freigeschaltet. In der nächsten Periode gilt wieder das normale Zeit-Limit.

15.3.2 Gebührenabhängige ISDN-Verbindungsbegrenzung

Werden an einem ISDN-Anschluss Gebühreninformationen übermittelt, können die anfallenden Verbindungsgebühren recht einfach eingeschränkt werden. Im Default-Zustand dürfen z.B. maximal 830 Gebühreneinheiten in sechs Tagen verbraucht werden. Ist diese Grenze erreicht, erlaubt der Router keinen weiteren aktiven Verbindungsaufbau.



Die Gebührenüberwachung des Routers können Sie am besten bei freigeschalteter „Gebühreninformation **während** der Verbindung“ im ISDN-Netz (nach AOCD) nutzen. Beantragen Sie ggf. die Freischaltung dieses Merkmals bei Ihrer Telefongesellschaft. Eine Gebührenüberwachung mit dem Merkmal „Gebühreninformation **nach** der Verbindung“ ist im Prinzip auch möglich, jedoch werden dabei ggf. Dauerverbindungen nicht erkannt!



Wenn Sie das Least-Cost-Routing für die Router-Module eingeschaltet haben, werden ggf. auch Verbindungen über Provider aufgebaut, die keine Gebühreninformationen übertragen!

15.3.3 Zeitabhängige ISDN-Verbindungsbegrenzung

Der Mechanismus der ISDN-Gebührenüberwachung greift nicht, wenn am ISDN-Anschluss keine Gebühreninformationen übertragen werden. Das ist z.B. dann der Fall, wenn die Übermittlung der Gebühreninformationen entweder nicht beantragt wurde oder die Telefongesellschaft diese Informationen grundsätzlich nicht übermittelt.

Um die Kosten für ISDN-Verbindungen auch ohne Gebühreninformationen begrenzen zu können, kann die maximale Verbindungsdauer mit Hilfe der Zeit gesteuert werden. Dazu wird ein Zeitbudget für eine Periode vereinbart. Im Default-Zustand dürfen z.B. für maximal 210 Minuten innerhalb von sechs Tagen Verbindungen aktiv aufgebaut werden.



Wird die Grenze eines Budgets erreicht, werden automatisch alle offenen Router-Verbindungen beendet, die der Router selbst aufgebaut hat. Erst nach dem Ablauf der aktuellen Periode werden die Budgets wieder freigegeben und aktive Verbindungen ermöglicht. Der Administrator kann die Budgets natürlich auch vorzeitig wieder freigeben!

▷ *Das SYSLOG-Modul*

Mit einem Budget von 0 Einheiten bzw. 0 Minuten kann die Gebühren- bzw. Zeitüberwachung der Routerfunktionen ausgeschaltet werden.



Nur die Router-Funktionen sind durch den Gebühren- oder Zeitschutz abgesichert! Verbindungen über die LANCAPI werden davon nicht erfasst.

15.3.4 Einstellungen im Gebührenmodul

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management ▶ Kosten
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Gebuehren
Terminal/Telnet	cd /Setup/Gebuehren

Im Gebührenmodul können Sie die Onlinezeit überwachen und für den Aufbauschutz nutzen.

- ▶ Tage/Periode
 - Dauer einer Überwachungsperiode in Tagen angegeben
- ▶ Budget-Einheiten, Online-Minuten-Budget
 - Maximale ISDN-Einheiten bzw. Online-Minuten in einer Überwachungsperiode



Die Informationen über die Gebühren und Verbindungszeiten werden über einen Bootvorgang hinaus gesichert (z. B. beim Einspielen einer neuen Firmware) und gehen erst verloren, wenn das Gerät ausgeschaltet wird. Alle hier erwähnten Zeitangaben werden in Minuten gemacht.

15.4 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf den LANCOM protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

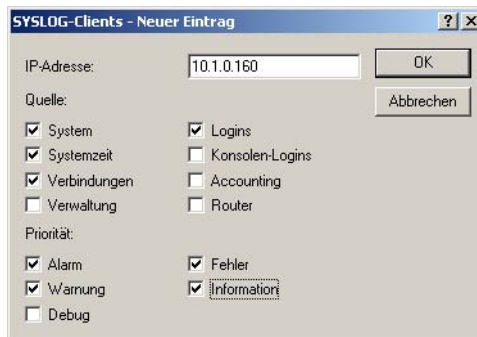
15.4.1 Einrichten des SYSLOG- Moduls

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management ► Meldungen
WEBconfig	Experten-Konfiguration ► Setup ► SYSLOG
Terminal/Telnet	cd /Setup/SYSLOG

15.4.2 Beispielkonfiguration mit LANconfig

SYSLOG- Client anlegen

- ① Starten Sie LANconfig. Unter 'Management' wählen Sie die Karte 'Meldungen'.
- ② Schalten Sie das Modul ein, und klicken Sie auf **SYSLOG- Clients**.
- ③ Im nächsten Fenster klicken Sie auf **Hinzufügen....**
- ④ Geben Sie zunächst die IP-Adresse des SYSLOG-Clients ein, und legen Sie im Weiteren die Quellen und Prioritäten fest.



SYSLOG kommt aus der UNIX-Welt, in der bestimmte Quellen vordefiniert sind. LANCOM ordnet seine eigenen internen Quellen diesen vordefinierten SYSLOG-Quellen, den sogenannten „Facilities“, zu.

▷ *Das SYSLOG-Modul*

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im LANCOM einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des LANCOM und den SYSLOG-Facilities an.

Quelle	Bedeutung	Facility
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im LANCOM auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	Bedeutung	SYSLOG-Priorität
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z.B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z.B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

- ⑤ Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle wird der SYSLOG-Client mit seinen Parametern eingetragen.

Facilities

Über die Schaltfläche **Facility-Zuordnung** können alle Meldungen vom LANCOM einer Facility zugeordnet und dadurch vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Beispiel

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei `/etc/syslog.conf` durch den Eintrag

```
local7.* /var/log/lancom.log
```

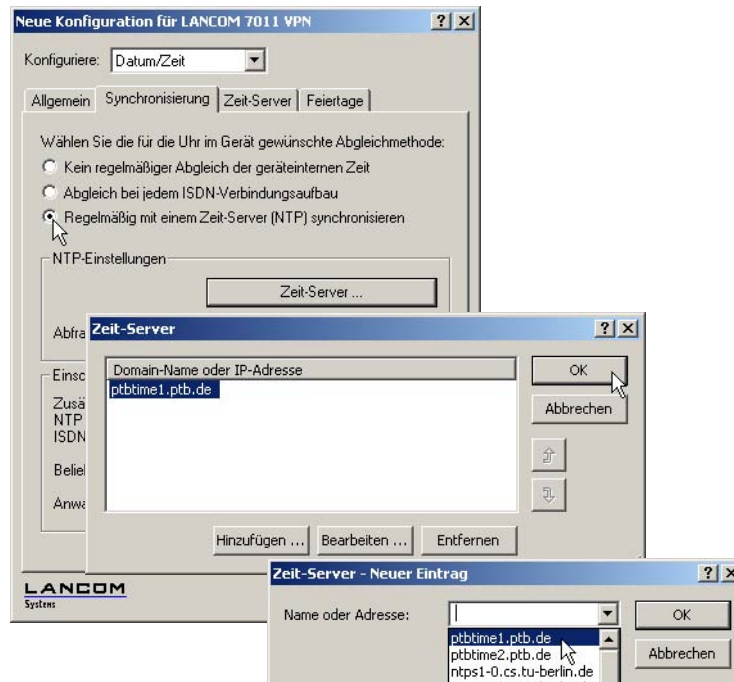
alle Ausgaben des LANCOM in die Datei `/var/log/lancom.log` geschrieben.

15.5 Zeit-Server für das lokale Netz

LANCOM Router können hochgenaue Zeitinformationen entweder über ISDN beziehen, oder aber über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit 'Open Access'-Policy, z.B. von der Physikalisch-Technischen Bundesanstalt). Die so ermittelte Zeit kann das LANCOM allen Stationen im lokalen Netz zur Verfügung stellen.

15.5.1 Konfiguration des Zeit-Servers unter LANconfig

Damit ein LANCOM die aktuelle Zeit im Netzwerk bekannt machen kann, wird im Konfigurationsbereich 'Datum/Zeit' auf der Registerkarte 'Synchronisierung' der regelmäßig Abgleich mit einem Zeitserver aktiviert. In den 'NTP-Einstellungen' wird dann mit der Schaltfläche **Zeit-Server** die Liste der Zeitserver geöffnet. Mit der Schaltfläche **Hinzufügen** können weitere Server in die Liste aufgenommen werden.



▷ Zeit-Server für das lokale Netz

Mit diesen Einstellungen bezieht zunächst nur das LANCOM selbst die Zeit von den öffentlichen Zeitservern. Um die aktuelle Zeit auch im LAN den anderen Geräte bekannt zu machen, wird im auf der Registerkarte 'Zeit-Server' der Zeit-Server aktiviert. Außerdem wird der Sendemodus eingeschaltet, wenn das LANCOM die Zeit in festen Intervallen aktiv in das Netz senden soll.



15.5.2 Konfiguration des Zeit-Servers mit WEBconfig oder Telnet

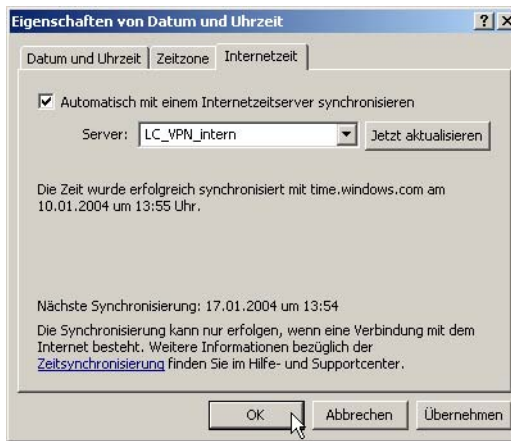
Bei der Konfiguration mit WEBconfig oder Telnet finden sich die benötigten Parameter in folgenden Bereichen:

Konfigurationstool	Aufruf/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ NTP
Terminal/Telnet	cd /Setup/NTP

15.5.3 Konfiguration der NTP-Clients

Die NTP-Clients müssen so konfiguriert sein, dass sie die Zeitinformationen vom LANCOM verwenden. Nicht alle Betriebssysteme verfügen über einen integrierten NTP-Client: Windows XP verfügt über einen solchen, für andere Windows-Betriebssysteme ist ein separater NTP-Client notwendig, bei Linux-Distributionen muss NTP entsprechend mitinstalliert sein.

Die 'Eigenschaften von Datum und Zeit' in einem XP-System werden mit einem Doppelklick auf die Uhrzeit unten rechts im Bildschirm geöffnet. Auf der Registerkarte 'Internetzeit' kann dort der Server zur Synchronisation der Zeit ausgewählt werden.



15.6 Scheduled Events

15.6.1 Zeitautomatik für LCOS-Befehle

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei **jede** beliebige LANCOM Kommandozeilenfunktion. Es können damit also alle LANCOM Features mit einer zeitlichen Steuerung versehen werden.

Anwendungsbeispiele:

- ▶ Verbindungsauf- und -abbauen zu bestimmten Zeiten:

Bei vielen Flatrate-Tarifen für die Internetnutzung wird die Verbindung durch den Provider automatisch nach 24 Stunden "Dauerbetrieb" getrennt. Diese Zwangstrennung kann zu unerwünschten Störungen führen, wenn diese tagsüber zu nicht festgelegten Zeitpunkten stattfindet und dabei VPN-Tunnel abgebaut und die IP-Adresse des LANCOM geändert werden. Um die Zwangstrennung zeitlich zu steuern, kann z.B. jede Nacht um 24 Uhr ein manueller Abbau der Internetverbindung angestoßen werden. Die Zwangstrennung erfolgt dann nicht mehr tagsüber zu ungeeigneten Zeitpunkten.

Als zweites Beispiel können die Geräte in einer verteilten Netzwerkstruktur, die nur über dynamische IP-Adressen verfügen, zu bestimmten Zeitpunkten eine Verbindung zum VPN-Gateway in der Zentrale aufbauen, damit über diese Verbindung Daten sicher aus dem Netzen der Filialen ausgelesen werden können. Auf diese Weise ist ein geschützter Zugriff z.B. auf die Kassendaten der Filialen auch ohne ISDN-Verbindungen möglich.

- ▶ Ein- und Ausschalten von Firewall-Regeln oder QoS-Regeln

Die Regeln für Firewall und QoS sind zunächst einmal zeitlich konstant. Je nach Tageszeit oder Wochentag kann es aber sein, dass unterschiedliche Einstellungen in diesem Bereich Sinn machen. Außerhalb der Bürozeiten oder

▷ *Scheduled Events*

am Wochenende können z.B. andere Prioritäten für die garantierten Bandbreiten gelten als zwischen 9:00 und 17:00 Uhr.

▶ Durchführung regelmäßiger Firmware- oder Konfigurationsupdates

Die Zeitautomatik erlaubt nicht nur das setzen einzelnen Werte in der Konfiguration, auch das komplette Umschalten auf eine andere Konfiguration ist möglich. Mit dieser Möglichkeit können Sie eine ganze Reihe von Befehlen bündeln und mit einem Kommando ändern. Der Wechsel der Gerätekonfiguration mit vollständig anderen Werten für das Wochenende und wieder zurück in der Nacht zum Montag gelingt so mit einer einzigen Zeile in der Zeitautomatik.

Auch das regelmäßige Updates der neuesten Firmware von einer festen Quelle aus ist so über die Zeitsteuerung zu realisieren.

▶ E-Mail-Benachrichtigungen

Mit der Zeitautomatik kann das LANCOM nicht nur bei bestimmten Firewall-Ereignissen E-Mails an den Administrator versenden, sondern auch zu festgelegten Zeitpunkten. Die E-Mail kann so z.B. über den erfolgreichen Aufbau der Internetverbindung nach der Zwangstrennung informieren oder nach dem Booten des Gerätes über den Grund des Neustarts informieren.

▶ Ein- und Ausschalten von Interfaces

Zu den Möglichkeiten für die Zeitautomatik gehört auch das Ein- und Ausschalten von einzelnen Schnittstellen in festen zeitlichen Intervallen. Damit kann z.B. ein WLAN-Interface nur zu bestimmten Zeiten den drahtlosen Zugang zum Netzwerk erlauben.

▶ Löschen von bestimmten Tabellen

Bei manchen Tabellen im LCOS macht es Sinn, die Inhalte regelmäßig zu löschen. Wenn Ihr Internetanschluss z.B. an eine monatliche Volumenbeschränkung gebunden ist, können Sie mit dem monatlichen Löschen der Accounting-Tabelle den Überblick über das tatsächlich jeden Monat verbrauchte Datenvolumen behalten.

15.6.2 Die Cron-Tabelle

Die Parameter für die Zeitautomatik werden in der Cron-Tabelle abgelegt. Die Cron-Tabelle hat folgenden Aufbau:

Eintrag	Beschreibung
Index	Eindeutige Kennzeichnung des Tabelleneintrages
Zeitbasis	Das Feld 'Zeitbasis' bestimmt ob die zeitliche Steuerung auf Grundlage der Echtzeit oder auf Grundlage der Betriebszeit des Gerätes ausgeführt werden soll. Echtzeit-basierte Regeln werten alle Zeit-/Datumsangaben aus, während Betriebszeit-basierte Regeln nur die Minuten- und Stundenangaben seit dem letzten Gerätestart auswerten.
Minuten Stunden Wochentage Montstage Monate	Die Werte 'Minute' bis 'Monate' definieren die Zeitpunkte, an denen ein Kommando ausgeführt werden soll. Wird ein Wert nicht angegeben, so wird er auch nicht in die Steuerung einbezogen. Pro Parameter kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-Maximalwert") eingegeben werden. Die Syntax des 'Wochentage'-Feldes entspricht dabei der üblichen cron- Interpretation: 0 Sonntag 1 Montag 2 Dienstag 3 Mittwoch 4 Donnerstag 5 Freitag 6 Samstag
Befehl	Das auszuführende Kommando oder eine Komma-separierte Kommando-Liste



Echtzeit-basierte Regel können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z.B. via NTP ('Zeit-Server für das lokale Netz' →Seite 431).

Beispiele:

Zeitbasis	Min.	Std.	W.-Tage	M.-Tage	Monate	Befehl
Echtzeit	0	4	0-6	1-31	1-12	do /so/man/abbau internet
Echtzeit	59	3	0-6	1-31	1-12	mailto:admin@mylancom.de?subject=Zwangstrennung?body=Manuelles Trennen der Internetverbindung
Echtzeit	0	0		1		do /setup/accounting/loeschen
Echtzeit	0	18	1,2,3,4,5			do /so/man/aufbau ZENTRALE

- ▶ Der erste Eintrag trennt jeden Morgen um 4:00 Uhr die Verbindung zum Internetprovider (Zwangstrennung).
- ▶ Der dritte Eintrag sendet jeden Morgen um 3:59, also kurz vor der Zwangstrennung, eine Info-Mail an den Admin.
- ▶ Der vierte Eintrag löscht an jedem 1. eines Monats die Accounting-Tabelle.
- ▶ Der fünfte Eintrag baut an jedem Werktag um 18:00 Uhr eine Verbindung zur Zentrale auf.

▷ Scheduled Events

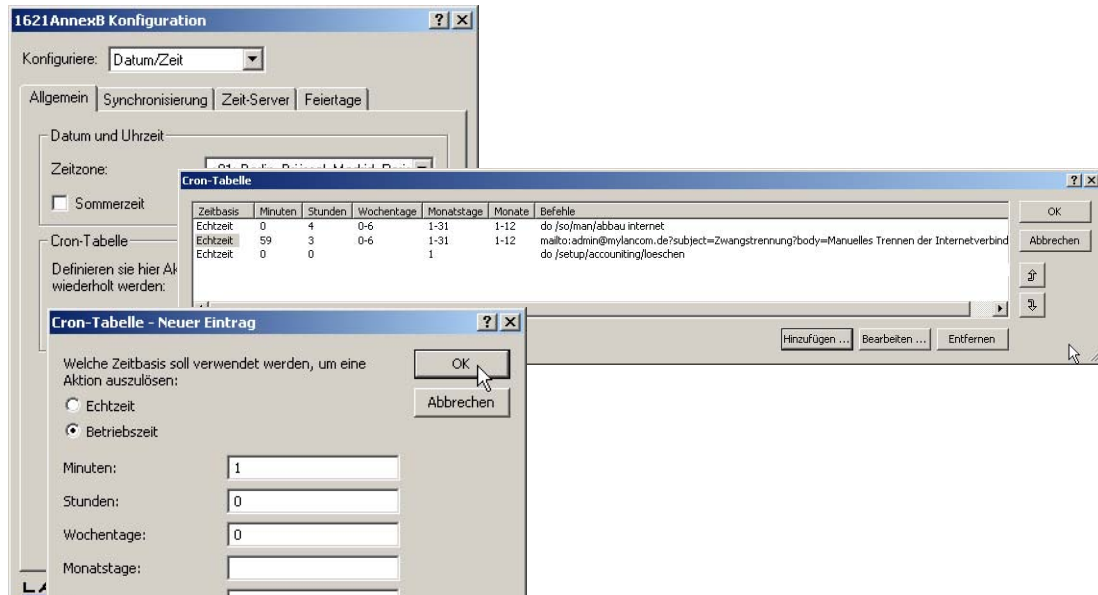


Zeitgesteuerte Regeln werden mit einer Genauigkeit von einer Minute ausgeführt. Bitte beachten Sie, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da ansonsten die Kommandos der Zeitautomatik nicht beachtet werden. Die Defaultsprache Englisch kann dazu bei Bedarf auf Deutsch umgestellt werden ('Die Sprache der Konsole auf Deutsch ändern' →Seite 25).

15.6.3 Konfiguration der Zeitautomatik

LANconfig

Unter LANconfig finden Sie die Cron-Tabelle im Konfigurationsbereich 'Datum/Zeit' auf der Registerkarte 'Allgemein':



WEBconfig
oder Telnnet

Unter WEBconfig oder Telnnet finden Sie die Cron-Tabelle in folgenden Menüs:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ► Setup ► Config ► Cron-Tabelle
Terminal/Telnnet	/Setup/Config/Cron-Tabelle

15.7 Port-Mapping

15.7.1 Freies Umsetzen von TCP/IP-Ports auf maskierten Verbindungen

Wird auf einer Verbindung das IP-Masquerading eingesetzt, werden die IP-Adressen der Rechner im eigenen Netz hinter der IP-Adresse des Routers versteckt. Um einzelne Rechner aus dem LAN dennoch von außen direkt ansprechbar zu machen, wird beim inversen Masquerading einem eingehenden Port-Bereich in der Service-Tabelle eine bestimmte IP-Adresse aus dem LAN zugeordnet.

Manchmal ist es allerdings gewünscht, dass der so eingerichtete „exposed host“ nicht mit dem standardmäßig verwendeten Port angesprochen wird, sondern aus Sicherheitsgründen ein anderer Port verwendet wird. In diesem Fall wird also nicht nur das Umsetzen von Ports auf eine IP-Adresse benötigt, sondern auch das Umsetzen auf andere Ports. Ein weiteres Anwendungsbeispiel für diese Port-Umsetzung ist das Umsetzen von mehreren Ports aus dem WAN auf einen gemeinsamen Port im LAN, die jedoch verschiedenen IP-Adressen zugeordnet werden (N-IP-Mapping).

15.7.2 Konfiguration

Bei der Konfiguration des Port-Mappings wird einem Port oder Portbereich (Anfangs-Port bis End-Port) eine IP-Adresse aus dem LAN als Ziel und der im LAN zu verwendende Port (Map-Port) zugewiesen.



Wird als Map-Port die „0“ eingetragen, werden im LAN die gleichen Ports verwendet wie im WAN. Wird ein Portbereich umgesetzt, gibt der Map-Port den ersten verwendeten Port im LAN an. Beim Umsetzen des Portbereichs '1200' bis '1205' auf den internen Map-Port '1000' werden also die Ports von 1000 bis einschließlich 1005 für den Datenverkehr im LAN verwendet.

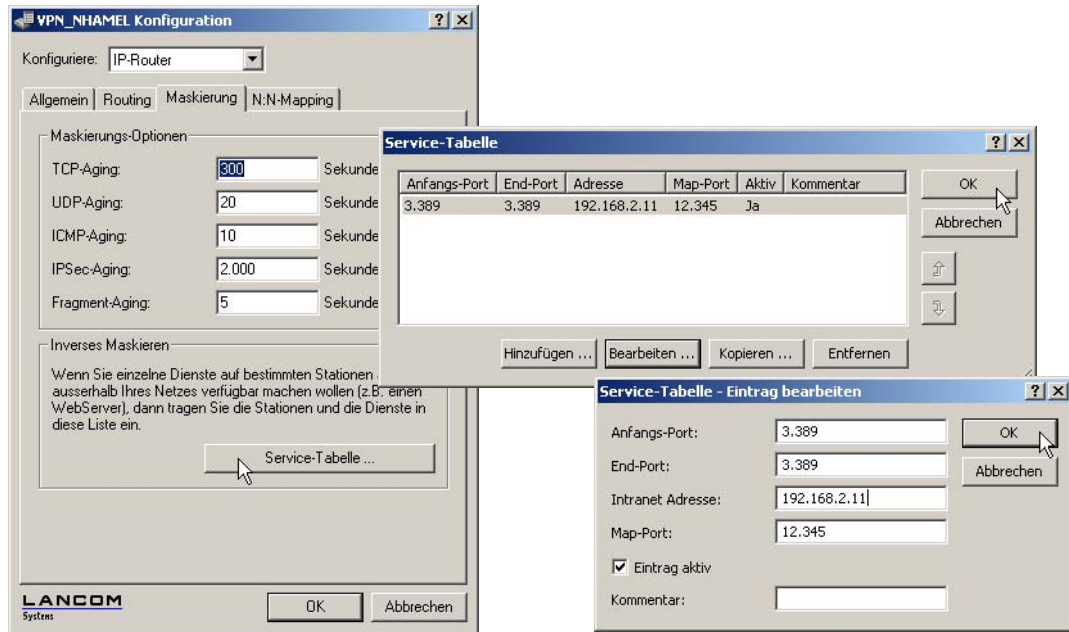


Das Port-Mapping ist statisch, deshalb können zwei Ports oder Portbereiche nicht auf den gleichen Map-Port eines Ziel-Rechners im LAN umgesetzt werden. Für verschiedene Zielrechner können gleiche Port-Mappings verwendet werden.

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Service-Tabelle im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Maskierung' unter der Schaltfläche **Service-Tabelle**.

► Port- Mapping



WEBconfig,
Telnet oder
Terminalpro-
gramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Service-Tabelle für das Funknetzwerk auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► IP-Router ► Maskierung ► Service-Tabelle
Terminal/Telnet	Setup/IP-Router/Maskierung/Service-Tabelle

16 Anhang

16.1 Fehlermeldungen im LANmonitor

Es besteht die Möglichkeit über den LANmonitor VPN - Fehlermeldungen auszulesen. Diese Fehlermeldungen werden in diesem Dokument aufgelistet, interpretiert und ein Workflow vorgeschlagen.

16.1.1 Allgemeine Fehlermeldungen

Verbindungsaufbau abgebrochen	
Verbindungsaufbau fehlgeschlagen (D-Kanal Layer 1)	Bus-Aktivierung fehlgeschlagen
Verbindungsaufbau fehlgeschlagen (D-Kanal Layer 2)	kein UA auf SABME
Verbindungsaufbau fehlgeschlagen (Layer 1)	a/b-Ports
Verbindungsaufbau fehlgeschlagen (Layer 2)	a/b-Ports
ISDN Leitungsfehler (Layer 1)	Kabel nicht gesteckt
Verbindungsabbruch (Layer 2)	X.75 / V.110
Lokaler Fehler	Angeforderte Ressource nicht verfügbar -> ISDN-Problem, TK-Anlage booten
PPP Anmeldung bei Gegenstelle - PAP abgelehnt	Gegenstelle kann nur PAP, es ist aber CHAP gefordert
PPP Anmeldung von Gegenstelle - Timeout (PPP-PAP RX)	Gegenstelle hat PAP-Request nicht gesendet
PPP Anmeldung bei Gegenstelle - Timeout (PPP-PAP TX)	Gegenstelle hat PAP-Requests nicht beantwortet
PPP Anmeldung von Gegenstelle - CHAP abgelehnt	auf ein CHAP-Challenge wird ein CHAP-Reject empfangen
PPP Anmeldung von Gegenstelle - Timeout (PPP-CHAP RX)	Gegenstelle hat CHAP-Response nicht gesendet
PPP Anmeldung bei Gegenstelle - Timeout (PPP-CHAP TX)	Gegenstelle hat CHAP-Response nicht beantwortet
Vorgegebenes Zeitlimit erreicht	genau wie Gebührenlimit...
Verbindungsaufbau fehlgeschlagen (Layer 1)	keine HDLC-Flags gefunden
Verbindungsaufbau fehlgeschlagen (Layer 2)	X.75 / V.110 funktioniert nicht
DSL Leitungsfehler (Layer 1)	Kabel nicht gesteckt

16.1.2 VPN-Fehlermeldungen



Zur korrekten Auswertung der Fehlermeldungen zu VPN-Verbindungen muss auf beiden LANCOM-Geräten mindestens die LCOS-Version 3.22 installiert sein.

▷ Fehlermeldungen im LANmonitor

Bei einer VPN-Verbindung handelt es sich immer um eine ausgehende oder ankommenden Verbindung. Um das Fehlersuche schneller und effizienter zu machen, werden die Meldungen zwischen einem Initiator und einem Responder unterschieden. Der Initiator ist die Gegenstelle, die die Verbindung initiiert. Beim Responder handelt es sich um denjenigen, der die Verbindung annimmt. Nachdem die Fehlermeldung ausgelesen wurde, schauen Sie anschließend in dem entsprechenden Menüpunkt auf der jeweiligen Gegenstelle nach.

Beispiel:

Bei der Fehlermeldung 'Zeitüberschreitung während IKE- oder IPSec-Verhandlung (Initiator)' kann kein direktes Fehlerbild entdeckt werden. Der Responder jedoch hat einen Fehler z.B. 'Kein übereinstimmendes Proposal gefunden (Responder, IPSec)' festgestellt, den er mittels eines SNMP-Trap an einem SNMP-Client (LANmonitor) geschickt hat. Anhand dieser Fehlermeldung kann man in der Konfiguration die entsprechenden Parameter kontrollieren und ggf. ändern. Daher ist es immer erforderlich, die Fehlermeldungen auf beiden Seiten zu verifizieren.

Meldung	Initiator	Responder	
Lizenzüberschreitung - keine VPN-Kanäle mehr verfügbar	x	x	Die Anzahl der maximal möglichen VPN - Kanäle wurde erreicht.
Kein Route zum entfernten Gateway	x	x	Die Router zum entfernten Gateway konnte nicht gefunden werden. Bitte überprüfen Sie die öffentliche IP-Adresse oder den DynDNS Namen der Gegenstelle.
Dynamic VPN - kein passender Eintrag in PPP-Liste vorhanden	x		Beim dynamischen VPN konnte der abgehende Ruf nicht mit den gesendeten PPP - Daten authentifizieren. Bitte gleichen Sie den PPP - Benutzernamen und das PPP - Passwort auf beiden Seiten unter "Konfiguriere --> Kommunikation --> Protokolle -> PPP - Liste --> Gegenstellename" ab.
Dynamic VPN - kein passender Eintrag in PPP-Liste vorhanden		x	Der eingehende Ruf konnte nicht mit den empfangenen PPP - Daten authentifiziert werden. Bitte gleichen Sie den PPP - Benutzernamen und das PPP - Passwort auf beiden Seiten unter "Konfiguriere --> Kommunikation --> Protokolle --> PPP - Liste --> Gegenstellename" ab.
Zeitüberschreitung während IKE- oder IPSec-Verhandlung	x	x	Es wurde eine Zeitüberschreitung erreicht. Der Router auf der gegenstelle reagiert nicht mehr. Bitte überprüfen Sie VPN - Fehlermeldung im LANmonitor auf der Gegenstelle.
Leitungsüberwachung (Line Polling) zum entfernten Gateway fehlgeschlagen			Das LCP Polling ist fehlgeschlagen. Bitte überprüfen Sie auf der gegenseite ob das Ping - Blockieren in dem Firewall menü unter "Konfiguriere --> Firewall --> Allgemein --> "Ping Blockieren"
Kein Eintrag in der Pollingtable und Keep-Alive ist eingestellt			Die Haltezeit des VPN - Tunnels unter "Konfiguriere --> VPN --> Verbindungs-Liste --> VPN Gegenstellennamen" ist auf Keep - Alive (9999 s) eingestellt. Das erforderliche ICMP Polling fehlt jedoch. Bitte fügen Sie unter "Konfiguriere --> Kommunikation --> Gegenstellen --> " Polling - Tabelle " hinzu. Als Gegenstelle tragen Sie die VPN - Gegenstelle, als IP-Adresse tragen Sie eine IP - Adresse aus dem LAN auf der gegenstelle.
Dynamic VPN - vorgegebenes Gebührenlimit erreicht	x		Das Gebührenlimit unter "Konfiguriere --> Kosten --> Gebühren - Limit (ISDN)" wurde erreicht. Bitte das Gerät neu booten.

▷ Fehlermeldungen im LANmonitor

Meldung	Initiator	Responder	
Dynamic VPN - vorgegebenes Zeitlimit erreicht	x		Das Zeitlimit unter "Konfiguriere --> Kosten --> Zeit - Limit (ISDN)" wurde erreicht. Bitte das Gerät neu booten.
Dynamic VPN - keine ISDN Rufnummer für Verhandlungskanal	x		Beim dynamischen VPN zur VPN Gegenstelle fehlt die ISDN - Rufnummer. Bitte tragen Sie die Rufnummer unter "Konfiguriere --> Kommunikation --> Gegenstellen --> Gegenstelle (ISDN/seriell) --> "Gegenstellename" " ein.
Dynamic VPN - Mehrere Verbindungen auf ISDN Interface für Verhandlungskanal nicht erlaubt			Beim Aufbau mehrerer ISDN VVerbindung wurde ein Limit erreicht. Bitte überprüfen Sie unter "Konfiguriere --> Management --> Interfaces --> interface - Einstellungen --> ISDN --> max. abgehende Rufe".
Vorgegebenes Gebührenlimit erreicht	x		Das Gebührenlimit wurde erreicht "Konfiguriere --> Management --> Kosten --> Gebührenlimit (ISDN)". Signalisiert durch ein gleichzeitiges blinken der Power LED.
Vorgegebenes Zeitlimit erreicht	x		Das Zeitlimit wurde erreicht "Konfiguriere --> Management --> Kosten --> Zeitlimit (ISDN)". Signalisiert durch ein gleichzeitiges blinken der Power LED.
Keine IP-Adresse für PPTP Server	x		Die IP - Adresse des einzuwählenden PPTP Servers ist nicht eingetragen. Tragen Sie die IP-Adresse unter "Konfiguriere --> Kommunikation --> Protokolle --> PPTP - Liste". Siehe dazu auch
Exchange type nicht übereinstimmend (Main bzw. Aggressive Mode)		x (IKE)	Der Exchange Type stimmt nicht mit der Gegenstelle überein. Bitte überprüfen Sie den Wert unter "Konfiguriere --> VPN --> Verbindungs - Liste --> VPN-Gegenstelleneintrag editieren --> IKE Exchange"
Kein übereinstimmendes Proposal gefunden	x (IKE)		Die IKE Prposals stimmen nicht überein. --> VPN Regeln überprüfen
Kein übereinstimmendes Proposal gefunden		x (IKE)	Die IKE Prposals stimmen nicht überein. --> VPN Regeln überprüfen
IKE Gruppen stimmen nicht überein		x (IKE)	Bitte überprüfen Sie die IKE - Gruppen auf beiden Gegenstellen unter "Konfiguriere --> VPN --> Verbindungs - Parmater --> "VPN Gegenstellename" --> IKE - Gruppe"
Life type - Angabe wird nicht unterstützt (andere als kByte oder Sekunden?)		x (IKE)	Der Wert für die Gültigkeitsdauer wird nicht unterstützt. Bitte entweder Lifetime in "sec = Sekunden" oder "kb = Kilobyte" verwenden. Überprüfen Sie diese Einstellung unter "Konfiguriere --> VPN --> Parameter --> Gültigkeitsdauer".
Life time - keine übereinstimmenden Angaben		x (IKE)	Die eingestellte Lifetime stimmt nicht mit der Gegenstelle überein. Überprüfen Sie diese Einstellung unter "Konfiguriere --> VPN --> Parameter --> Gültigkeitsdauer".
ID type - Angabe wird nicht unterstützt (andere als IP Netzwerk, Domain oder E-Mail)		x (IKE)	Falsche Eingabe der Identität. Bitte korrigieren Sie Ihre Eingabe "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
ID type - keine übereinstimmende Angaben (z.B. IP Netzwerk, Domain oder E-Mail)		x (IKE)	Beide Gegenstellen verwenden unterschiedliche Identitäten. Gleichen Sie die Identitäten auf beiden Gegenstellen ab "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"

▷ Fehlermeldungen im LANmonitor

Meldung	Initiator	Responder	
Keine Regel für ID gefunden - unbekannte Verbindung oder fehlerhafte ID (z.B. Definition des entfernten Gateways)		x (IKE)	Die eingehende VPN - Verbindung konnte keiner Gegenstelle zugeordnet werden.
IKE Schlüssel stimmen nicht überein	x (IKE)		Überprüfen Sie die Preshared-Keys unter "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
IKE Schlüssel stimmen nicht überein		x (IKE)	Überprüfen Sie die Preshared-Keys unter "Konfiguriere --> VPN --> IKE --> IKE - Schlüssel"
Nicht genügend Speicher	x (IKE)		Die Anzahl der VPN Verbindungen hat den Speicher des Gerätes ausgelastet. Weitere VPN - Verbindungen sollten aus Stabilitätsgründen des Gerätes nicht erstellt werden.
Nicht genügend Speicher		x (IKE)	Die Anzahl der VPN Verbindungen hat den Speicher des Gerätes ausgelastet. Weitere VPN - Verbindungen sollten aus Stabilitätsgründen des Gerätes nicht erstellt werden.
Keine Regel für ID's gefunden - unbekannte Verbindung oder fehlerhafte ID (z.B. IP-Netzwerkdefinition)		x (IKE)	Die eingehende Verbindung konnte keiner Gegenstelle zugewiesen werden. Bitte folgende Parameter überprüfen : ID type stimmt nicht überein (Siehe dieses Dokument) , falsche Netzwerkdefinition, VPN Regeln stimmen nicht (siehe VPN REGEL).
Kein übereinstimmendes Proposal gefunden	x (IPsec)	x (IPsec)	Die Gegenstellen konnten sich auf kein übereinstimmendes Proposal einigen. Bitte überprüfen Sie die Einstellungen unter "Konfiguriere --> VPN --> IKE -- IKE - Prposals" sowie unter "Konfiguriere --> VPN --> IPSec-Parameter --> IPSec - Proposal - Listen".
IPSec PFS Gruppen stimmen nicht überein			Bitte überprüfen Sie die PFS (Perfect Forward Secrecy) unter "Konfiguriere --> VPN --> Verbindungs - Parameter --> "VPN Gegenstellename" --> PFS - Gruppe"

16.2 SNMP-Traps

MIB2-Traps	Erklärung
coldstart	Gerät wurde durch Aus- und Einschalten der Stromzufuhr neu gestartet.
warmstart	LCOS wurde neu gestartet, z.B. durch einen Software-Reboot
authentication failed (= console login failed)	Anmeldung beim Zugriff auf die Konfiguration fehlgeschlagen

Enterprise specific Traps	Erklärung
Firmware upload started	Firmware-Upload gestartet
Configuration upload started	Einspielen der Firmware bzw. der Konfiguration gestartet
Upload succeeded	Einspielen der Firmware bzw. der Konfiguration erfolgreich
Upload failed (timeout)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Überschreitung der Maximalzeit
Upload failed (incomplete)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Unvollständige Konfiguration
Upload failed (bad device)	Einspielen der Firmware bzw. der Konfiguration fehlgeschlagen: Falsches Gerät
Configuration download started	Auslesen der Konfiguration gestartet
Download succeeded	Auslesen der Konfiguration erfolgreich
Console login	Anmeldung zur Konfiguration erfolgt
Console logout	Abmeldung von der Konfiguration erfolgt
Firewall-Trap	Information über ein Firewall-Ereignis
Connection status	WAN-Verbindungsstatus
VPN Connection status	VPN-Verbindungsstatus
WAN-Ethernet UP/DOWN	WAN-Interface verfügbar oder nicht verfügbar

WLAN-Traps	Betriebsmodus	Erklärung
WLAN Scan started	Access-Point oder Client	WLAN-Station hat einen Scan nach freien Funkkanälen gestartet
Started WLAN BSS ID	Access-Point	WLAN-Station hat eine neue Funkzelle aufgebaut
Joined WLAN BSS ID	Client	WLAN-Station hat eine Funkzelle gefunden
Authenticated WLAN station	Access-Point	Authentifizierung einer Client-WLAN-Station erfolgreich
Deauthenticated WLAN station	Access-Point	Client-WLAN-Station hat sich abgemeldet
Associated WLAN station	Access-Point	Client-WLAN-Station verbunden
Reassociated WLAN station	Access-Point	Client-WLAN-Station erneut verbunden, war zuvor bei einem anderen Access Point angemeldet

▷ Funkkanäle

WLAN-Traps	Betriebsmodus	Erklärung
RADIUS access check for WLAN station succeeded	Access-Point	Überprüfung des RADIUS-Zugangs der WLAN-Station erfolgreich
RADIUS access check for WLAN station failed	Access-Point	Überprüfung des RADIUS-Zugangs der WLAN-Station fehlgeschlagen
Disassociated WLAN station due to station request	Access-Point	WLAN-Station abgemeldet aufgrund einer Anforderung der Station
Rejected association from WLAN station	Access-Point	Anmeldung der WLAN-Station zurückgewiesen
WLAN card hung, resetting	Access-Point oder Client	WLAN-Karte angehalten, Reset

16.3 Funkkanäle

16.3.1 Funkkanäle im 2,4 GHz Frequenzband

Im nutzbaren Frequenzraum von 2400 bis 2483 MHz stehen bis zu 13 DSSS-Kanäle zur Verfügung. In der folgenden Übersicht sehen Sie, welche Kanäle von den verschiedenen Regionen (EU/WORLD) unterstützt werden. Die letzte Spalte zeigt, welche Kanäle ohne gegenseitige Überlagerung konfiguriert werden können.

Frequenzbereich	2400–2500 MHz		keine Überlagerung mit
	Kanal-Nr.	EU (ETSI)	
1	2412	2412	6, 11
2	2417	2417	7
3	2422	2422	8
4	2427	2427	9
5	2432	2432	10
6	2437	2437	1, 11
7	2442	2442	2
8	2447	2447	3
9	2452	2452	4
10	2457	2457	5
11	2462	2462	1, 6
12	2467	–	–
13	2472	–	–

Die fett dargestellten Werte sind die Vorgabeeinstellungen, mit denen der Funkadapter in dem Access Point arbeitet.

16.3.2 Funkkanäle im 5 GHz Frequenzband

Im nutzbaren Frequenzraum von 5,13 bis 5,805 GHz stehen bis zu 19 Kanäle in Europa zur Verfügung, unterteilt in drei Frequenzbänder, für die unterschiedliche Nutzungsbedingungen gelten können:

- ▶ Band 1: 5150 - 5350 MHz (Kanäle 36, 40, 44, 48, 52, 56, 60 und 64)
- ▶ Band 2: 5470 - 5725 MHz (Kanäle 100, 104, 108, 112, 116, 120, 124, 128, 132, 136 und 140)
- ▶ Band 3: 5725 - 5875 MHz (Kanäle 147, 151, 155, 167)



Bitte beachten Sie, dass die Frequenzbereiche und Funkkanäle aus Band 3 ausschließlich für die Verwendung in Großbritannien vorgesehen sind!

In der folgenden Übersicht sehen Sie, welche Kanäle in den verschiedenen Regionen verwendet werden dürfen.

	Kanalnummer	Frequenz	ETSI (EU)	FCC (US)
Band 1	36	5,180 GHz	ja	ja
	40	5,200 GHz	ja	ja
	44	5,220 GHz	ja	ja
	48	5,240 GHz	ja	ja
	52	5,260 GHz	ja	ja
	56	5,280 GHz	ja	ja
	60	5,300 GHz	ja	ja
	64	5,320 GHz	ja	ja
Band 2	100	5,500 GHz	ja	nein
	104	5,520 GHz	ja	nein
	108	5,540 GHz	ja	nein
	112	5,560 GHz	ja	nein
	116	5,580 GHz	ja	nein
	120	5,600 GHz	ja	nein
	124	5,620 GHz	ja	nein
	128	5,640 GHz	ja	nein
	132	5,660 GHz	ja	nein
	136	5,680 GHz	ja	nein
	140	5,700 GHz	ja	nein

▷ Funkkanäle

	Kanalnummer	Frequenz	ETSI (EU)	FCC (US)
Band 3 (nur UK)	147	5,735 GHz	nein	ja
	151	5,755 GHz	nein	ja
	155	5,775 GHz	nein	ja
	167	5,835 GHz	nein	ja

16.3.3 Funkkanäle und Frequenzbänder für Indoor- und Outdoor-Verwendung

In einigen Ländern gelten spezielle Vorschriften, welche Frequenzbänder und Kanäle im Indoor- bzw. Outdoorbetrieb verwendet werden dürfen. Die folgende Tabelle gibt Aufschluss über die zulässige Verwendung:

Land	Band (GHz)	Unterband	Frequenz (GHz)	Kanäle	Turbo-Kanäle	Sendeleistung (mW/dBm)	Verwendung Indoor/Outdoor
Deutschland, Österreich, Schweiz, Niederlande, Belgien, Luxemburg, Italien, Malta	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
UK	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
		2	5,470-5,725	100-140	106-130	1000/30	I+O
		3	5,725-5,585	147, 151, 155, 167	–	2000/33,1	Nur für feste Outdoor-WLAN-Installationen!
Tschechien	2,4	1	2,4-2,4835	1-13	6	100/20	I+O
	5	1	5,15-5,35	36-64	42-58	200/23	I
Frankreich	2,4	1	2,4-2,4835	1-13	6 (nur bis 10 dBm max!)	100/20	I
	2,4	1	2,4-2,454	1-9		100/20	O
	2,4	1	2,454-2,4835	10-13	10/10	O	
	5	1	5,15-5,35	36-64	42-58	200/23	I

Weitere Informationen über die Nutzungsbeschränkungen für Funk-LAN-Geräte in den EU-Ländern finden Sie unter folgenden Internetadressen:

Land	Organisation	Link
Belgien	Institut Belge des Postes et Telecommunications (BIPT)	www.bipt.be
Dänemark	National Telecom Agency	www.tst.dk
Deutschland	Regulierungsbehörde für Telekommunikation und Post	www.regtp.de
Finnland	Finnish Communications Regulatory Authority (FICORA)	www.ficora.fi
Frankreich	Autorité de Régulation des Télécommunications (ART)	www.art-telecom.fr

Land	Organisation	Link
Griechenland	National Telecommunications Commission (EET)	www.eett.gr
Großbritannien	Office of Telecommunications (Oftel)	www.oftel.gov.uk
	Postal Services Commission (Postcomm)	www.postcomm.gov.uk/
	Radiocommunications Agency	www.open.gov.uk/radiocom
Irland	Commission for Communications Regulation (ComReg)	www.comreg.ie
Island	Post and Telecom Administration (PTA)	www.pta.is
Italien	L'Autorità per le garanzie nelle comunicazioni (AGC)	www.agcom.it
Lettland	Telecommunication State Inspection	www.vei.lv
Liechtenstein	Amt für Kommunikation (AK)	www.ak.li
Litauen	Radio Administration	www.rtt.lt/
Luxemburg	Institut Luxembourgeois des Télécommunications (ILT)	www.etat.lu/ILT
Niederlande	Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)	www.opta.nl
	Agentschap Telecom	www.agentschap-telecom.nl
	Ministerie Economische Zaken	www.ez.nl
Norwegen	Norwegian Post and Telecommunications Authority (NPT)	www.npt.no
Österreich	Rundfunk und Telekom Regulierungs-GmbH	www.rtr.at
	Bundesministerium für Verkehr, Innovation und Technologie	www.bmvit.gv.at
Polen	Urząd Regulacji Telekomunikacji (URT)	www.urt.gov.pl
Portugal	Autoridade Nacional De Comunicações (ICP-Anacom)	www.anacom.pt
Schweden	National Post and Telecom Agency	www.pst.se
Schweiz	Bundesamt für Kommunikation	www.bakom.ch
Slowenien	Agencija za telekomunikacije, radiodifuzijo in pošto	www.atrp.si
Spanien	Comision del Mercado de las Telecomunicaciones (CMT)	www.cmt.es
Tschechien	Czech Telecommunication Office	www.ctu.cz
Ungarn	Communication Authority (HIF)	www.hif.hu



Bitte informieren Sie sich über die aktuellen Funk-Regelungen des Landes, in dem Sie ein Funk-LAN-Gerät in Betrieb nehmen wollen, und stellen Sie in den WLAN-Einstellungen unbedingt das Land ein, in dem Sie das Gerät betreiben.

▷ *Unterstützte RFCs***16.4 Unterstützte RFCs**

RFC	Titel
1058	Routing Information Protocol
1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
1334	PPP Authentication Protocols
1389	RIP Version 2 MIB Extensions
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
1542	Clarifications and Extensions for the Bootstrap Protocol
1552	The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
1577	Classical IP and ARP over ATM
1631	The IP Network Address Translator (NAT)
1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
1974	PPP Stac LZS Compression Protocol
2284	Extensible Authentication Protocol
2104	HMAC: Keyed-Hashing for Message Authentication
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions
2225	Classical IP and ARP over ATM
2364	PPP Over AAL5
2401	Security Architecture for the Internet Protocol
2402	IP Authentication Header
2403	The Use of HMAC-MD5-96 within ESP and AH
2404	The Use of HMAC-SHA-1-96 within ESP and AH
2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
2406	IP Encapsulating Security Payload (ESP)
2407	The Internet IP Security Domain of Interpretation for ISAKMP
2408	Internet Security Association and Key Management Protocol (ISAKMP)
2409	The Internet Key Exchange (IKE)
2410	The NULL Encryption Algorithm and Its Use With IPsec
2412	The OAKLEY Key Determination Protocol
2451	The ESP CBC-Mode Cipher Algorithms

RFC	Titel
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

16.5 Glossar

802.11	Funk-LAN Spezifikation des IEEE; Datenrate bis 2 Mbit/s; im 2,4 GHz ISM Band; FHSS und DSSS; auch Infrarot Spektrum Kommunikation vorgesehen
802.11a	802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 5 GHz Band; OFDM
802.11b	802.11 Erweiterung; Daten bis 11 Mbit/s; im 2,4 GHz Band; hohe Marktdurchdringung; DSSS/CCK
802.11g	802.11 Erweiterung; Datenrate bis 54 Mbit/s; im 2,4 GHz Band; OFDM und DSSS
802.11h	802.11a Anpassung, Datenrate bis 54 Mbit/s; im 5 GHz Band; im Bereich der Sendeleistung und Frequenzmanagement; für den Einsatz in Europa; OFDM
802.11i	Zukünftige 802.11 Erweiterung mit zusätzlichen Sicherheitsmerkmalen
802.1x	Spezifikation eines portbasierenden Authentisierungsmechanismus durch IEEE
AES	Advanced Encryption Standard
Access Point	Basisstation in einem Wireless LAN; unabhängige LAN-WLAN-Bridge; verbindet Stationen eines LAN (lokales Netz) mit einem WLAN (Funknetz) im Point-to-Multipoint Betrieb; verbindet zwei Netze über ein Funknetz im Point-to-Point Betrieb
Access Router	Aktive Netzwerkkomponente für die Anbindung eines lokalen Netzwerks an das Internet oder ein Firmennetzwerk
ADSL	Asymmetrical Digital Subscriber Line - Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über normale Telefonverkabelungen. Mit ADSL sind Übertragungen (Downstream) bis zu 6 Mbit/s über normale Telefonkabel realisierbar, für die bidirektionale Übertragung steht ein zweites Frequenzband mit Übertragungsgeschwindigkeiten bis zu 640 kbit/s (Upstream) zur Verfügung - daher auch die Bezeichnung asymmetrisch.
Bandbreite	Datensatz mit welcher ein Nutzer im Internet surfen kann; je höher die Bandbreite, desto schneller
Breitband	Dienst, der sich durch hohe Bandbreite auszeichnet; z.B.: DSL oder WLAN
Bridge	Transportprotokoll-unabhängige, transparente Netzwerkkomponente; überträgt alle Pakete, die als "nicht lokal" identifiziert werden und kennt nur den Unterschied zwischen "lokal" und "remote". Arbeitet auf Layer-2 des OSI-Modells
Broadcast	Broadcasts sind Pakete an alle Stationen eines lokalen Netzes; Bridges übertragen Broadcasts; Router übertragen keine Broadcasts
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI ist ein Standard zur Ansteuerung von ISDN-Adaptern
CCK	Code Complementary Keying; Modulationsart bei DSSS
Client	Jeder mit einem Funk-LAN-Adapter (Funk-LAN-Karte) ausgestattete Rechner, der von anderen Teilnehmern des Funk-Netzwerkes Dienste in Anspruch nimmt

▷ Glossar

CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; Zugriffsverfahren auf den Funkkanal bei 802.11
CRC	Cyclic Redundancy Check; Bitfehler Erkennungsverfahren
Datendurchsatz	Geschwindigkeit, mit der im Internet gesurft werden kann; abhängig von der Bandbreite und der Anzahl der Nutzer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service - Rechner kommunizieren mit Rechnern in entfernten Netzen über IP-Adressen; DNS-Server übersetzten Namen in IP-Adressen; ohne DNS-Server müsste man sich alle IP-Adressen merken und könnte nicht mit Namen arbeiten (www.lancom.de)
Domäne	in sich geschlossener Netzwerkbereich; => Intranet
Download / Downstream	Download / Downstream kennzeichnet die Richtung des Datenflusses in einem WAN. Bei Downstream handelt es sich um die Richtung vom Head-End/Internet zu dem am Netz angeschlossenen Teilnehmer.
DS	Distribution System
DSL	Digital Subscriber Line - DSL-Verfahren sind alle Verfahren zur digitalen breibandigen Nutzung von Telefonleitungen im Anschlussbereich, wie ADSL, HDSL, SDSL, VDSL usw., die auch als xDSL bezeichnet werden
DSSS	Direct Sequence Spread Spectrum; Codemultiplex - Bandspreizverfahren
Dynamic DNS	IPSec-VPN-Implementation, welche die transparente Einbindung von lokalen Netzwerken in eine VPN-Lösung erlaubt, selbst wenn deren Router mit dynamischen Adressen (Dial-Up) arbeiten
EAP	Extensible Authentication Protocol
EAP-MD5	EAP-Variante, die Passwörter zur einseitigen Authentisierung benutzt
EAP-TLS	EAP-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EAP-TTLS	EPA-Tunneled-Transport-Layer Security; EAP-Variante, die Zertifikate zur gegenseitigen Authentisierung benutzt
EIRP	Effective Osotropic Radiated Power, mittlere äquivalente isotrope Strahlungsleistung
ESS	Extended Service Set
ESSID	Extended Service Set Identity; "Netzwerkname" des Funk-LAN
Ethernet	Strang- oder sternförmig aufgebautes, physikalisches Transportmedium; alle Stationen können gleichzeitig senden; Kollisionen werden erkannt und durch das Netzwerk-Protokoll behoben
FHSS	Frequency Hopping Spread Spectrum; Frequenzsprung - Bandspreizverfahren
Firewall	Schutzmechanismen für ein Intranet gegen Zugriffe von außen
Frequenz	Anzahl der Schwingungen pro Sekunde (angegeben in Hertz; 1 Hz = 1 Schwingung pro Sekunde; GHz = Gigahertz = 1 Mrd. Hertz Schwingungen pro Sekunde)
FTP	File Transfer Protocol - Filetransfer-Protokoll dient dem Dateitransfer zwischen verschiedenen Systemen und der einfachen Dateihandhabung; FTP basiert auf dem Übertragungsprotokoll TCP
Frequenzband	Zusammenhängender Frequenzbereich, der sich durch gleiche Übertragungseigenschaften auszeichnet
Funkfrequenz	Jede Funkanwendung findet in weltweit streng reglementierten Funkfrequenzen statt
Gateway	Netzwerkkomponente, die auf einem Layer des => OSI-Modells Zugang zu anderen Netzwerkkomponenten bietet. Pakete, die nicht an eine lokale Gegenstelle gehen, werden an das Gateway geschickt. Das Gateway kümmert sich um die Kommunikation mit entfernten Netzen.

Hub	Netzwerkkomponente; Verteiler; Kollektor; auch zur Umsetzung von einem Anschluss-Typ auf einen anderen
HotSpot	Lokal begrenztes Funknetz dessen Basisstation über einen Internetzugang verfügt; öffentlicher drahtloser Internetzugang
IAPP-Roaming	Roaming zwischen den Zellen eines Funknetzwerks über das IAPP (Inter Access Point Protocol)
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System - frühest mögliches Erkennen von Angriffen auf das Netzwerk
IEEE	Institute of Electrical and Electronics Engineers, New York - www.ieee.org
IP	Internet Protocol
IP-Masquerading	Kombination aus PAT (Port Adress Translation) und NAT (Network Adress Translation) von LANCOM Systems verwendetes Verfahren zur Anbindung eines Intranets (mehrere Workstations) ans Internet über eine einzige IP-Adresse; gleichzeitig sind die internen Rechner vor Zugriffen von außen geschützt
IPSec	Internet Protocol Security
IP Quality-of-Service	Diese Funktionen geben Vorfahrt für unternehmenskritische Applikationen, bestimmte Dienste oder Benutzergruppen
ISDN	Integrated Services Digital Network - schneller Verbindungsaufbau; zwei unabhängige Kanäle; höhere Übertragungsraten als analog (bis 128 Kbit/s); nutzt die alten analogen Leitungen; Komfortmerkmale (Rufumleitung, Rückruf bei besetzt etc.); unterstützt sowohl analoge als auch digitale Dienste
ISM-Frequenzband	Industrial-Scientific-Medical, lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können
ISP	Internet Service Provider - Dienstleister, der über eine Verbindung ins Internet verfügt (Backbone) und Einwahlpunkte für Endkunden bereitstellt
LCOS	LANCOM Operating System - einheitliches Betriebssystem für die LANCOM-Produkte
LAN	Local Area Network - lokales Netzwerk; standortbegrenzt
LANcapi	Virtuelle CAPI, die über das Netzwerk angeboten wird; mit der in allen LANCOM-Routern mit ISDN-Schnittstelle implementierten LANcapi kann auch ein im LAN angeschlossener PC ISDN-Telematikdienste nutzen
LANconfig	Software zur Konfiguration von LANCOM-Geräten unter Windows
LANtools	Umfangreiches, benutzfreundliches Set für Management und Überwachung der LANCOM-Produkte und -Lösungen
MAC	Media Access Control; Funkzugriffsprotokoll auf ISO Layer 2 Data Link; es definiert Paket-Format, Paket-Adressierung und Fehlerdetektion
MAC-Adresse	Seriennummer einer Netzkomponente, die durch den Hersteller vergeben wird
Mbit	Megabit: Standardgröße für die Angabe von Datenmengen im Zusammenhang mit Bandbreiten
MIC	Message Integrity Check, kryptographischer Integritätsschutzmechanismus
NetBios	Network Basic Input/Output System. Von IBM entwickeltes und später von Microsoft übernommenes, nicht routbares Netzwerkprotokoll für lokale Netze.
NTBA	Network Termination Basic Adaptor . Der NTBA (Netzabschlussadapter) ist bei einem ISDN-Basisanschluss für die Umsetzung des von der Telefongesellschaft verlegten Anschlusses auf den S0-Bus zuständig.
OFDM	Orthogonal Frequency Division Multiplex

▷ Glossar

PEAP	Protected EAP, EAP-Variante zur gegenseitigen Authentisierung
PKI	Public Key Infrastructure
PPP	Point to Point Protocol: Netzwerkprotokoll für die Verbindung zwischen zwei Rechnern. PPP setzt auf TCP/IP auf.
PPTP	Point to Point Tunneling Protocol: Netzwerkprotokoll zum Aufbau virtueller privater Netze über das Internet.
Point-to-Multipoint (WLAN)	Mehrere WLAN-Stationen buchen sich auf eine Basis-Station ein und bilden mit den fest verkabelten Stationen ein gemeinsames Netzwerk
Point-to-Point (WLAN)	Zwei Basis-Stationen verbinden zwei kabelgebundene Netze über WLAN; der Point-to-Point Betrieb ermöglicht Kopplungen von Netzwerken auch über Straßen hinweg ohne Kabel
QoS	Quality-of-Service (siehe hierzu IP Quality-of-Service)
RADIUS	Remote Authentication Dial-In User Service; Authentisierungs- und Überwachungsprotokoll auf Anwendungsebene für Authentisierung, Integritätsschutz und Accounting im Bereich Netzzugang
RC4	Stromchiffrierverfahren von Ron Rivest, "Rens Code"
RFC	Request for Comments
Router	intelligente Netzwerkkomponente; vergleichbar mit einer Poststelle, die aufgrund von logischer Zieladresse eines Paketes entscheiden kann, an welche nächste Netzwerkkomponente dieses Paket übertragen wird; kennt die gesamte Topologie des Netzes
SDSL	Single Line Digital Subscriber Line - Downstream und Upstream mit 2,048 Mbit/s (zweiadriges Kabel)
Server	Rechner, der im Netzwerk Dienste (z.B. Dateien, NEWS, EMail, WWW-Seiten) zur Verfügung stellt
SINA	Sichere Inter-Netzwerk Architektur
SMTP	Simple Mail Transfer Protocol - SMTP-Protokoll ist der Internet-Standard zur Verteilung von elektronischer Post; das Protokoll setzt auf dem TCP-Protokoll auf
SNMPv3	Simple Network Management Protocol Version 3
SSID	Service Set Identity; "Netzwerkname" des Funk-LANs
SSL	Secure Socket Layer
Splitter	Der Splitter ist vergleichbar mit einer Audio-Frequenzweiche; bei einem ADSL-Anschluss trennt der Splitter die ISDN-Signale von den DSL-Signalen; die ISDN-Signale gehen zum NTBA; die DSL-Signale gehen zum DSL-Modem
Switch	Ein zentraler Verteiler in einem sternförmigen Netz; jede Station hat die volle Bandbreite zur Verfügung; wenn eine Station ausfällt, wird der Rest des Netzes nicht beeinträchtigt; wird zur Kollisionsvermeidung eingesetzt; erhöht den Gesamtdurchsatz des Netzes; Switchs sind kaskadierbar
TAE	Telefon-Anschluss-Einheit. Stecker zum Anschluss von analogen Geräten wie ein Telefon oder Modem an das Telefonnetz.
TCP/IP	Transmission Control Protocol/Internet Protocol; Familie von Protokollen (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) wird hauptsächlich im Internet verwendet, hält aber auch immer mehr Einzug in Intranets
TKIP	Temporal Key Integrity
TLS	Transport-Layer Security
TPC	Transmission Power Control

* Die Zahlen in der Tabelle geben die LCOS-Version an, mit der die Funktion implementiert wurde.

¹⁾ Port-Separierung (Private Mode)

²⁾ nur wenn bei den Geräten die entsprechenden VPN-Optionen freigeschaltet sind

³⁾ nicht bei 11-MBit-WLAN-Karten

⁴⁾ optional VPN-500 und VPN-1000 erhältlich

⁵⁾ Kompatibel zu ADSL und ADSL2

Upload/Upstream	Upload / Upstream kennzeichnet die Richtung des Datenflusses in einem WAN; bei Upstream handelt es sich um die Richtung vom am Netz angeschlossenen Teilnehmer zum Head-End/Internet
Verkettung	Aneinanderhänger von Bitfolgen
VPN	Virtual Private Network - ein VPN ist ein Netzwerk bestehend aus virtuellen Verbindungen, über welche nichtöffentliche bzw. firmeninterne Daten sicher übertragen werden können, auch wenn öffentliche Netzwerkinfrastrukturen genutzt werden
WAN	Wide Area Network - Netzwerk-Verbindung über weite Strecken (z.B. über ISDN mit einem LANCOM-Router)
WECA	Wireless Ethernet Compatibility Alliance; Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11; umbenannt zu WiFi-Alliance
WEBconfig	Webbasierte Konfigurationsoberfläche für LANCOM-Geräte.
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity; Marketing Begriff generiert durch WECA
WiFi-Alliance	Vereinigung von Herstellern von Funk-LAN-Komponenten nach IEEE 802.11;früher WECA
WLAN	Wireless Local Area Network - lokales Funknetz
WPA	WiFi Protected Access; Bezeichnung für über IEEE 802.11 hinaus gehende Sicherheitsmechanismen; generiert durch die WiFi-Alliance
WISP	Wireless Internet Service Provider
xDSL	xDSL steht für die Familie der Digital Subscriber Line Techniken
XOR	Logische Verknüpfung "exklusiv oder"

▷ Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

16.6 Übersicht über die Funktionen nach Modellen und LCOS*-Versionen

	800/1000/1100	I-10	821	1511	1521	1611	1621	1711
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	✓	✓	2.80	2.80	✓
IP-QoS, Traffic Shaping	3.30	3.30	3.30	3.30	✓	3.30	3.30	✓
N:N-Mapping			4.10	✓	4.10	3.30	3.30	✓
VLAN				3.30	✓			
DMZ-Port			1)	1)	1)		1)	1)
AES, 3-DES, DES, Blowfish, CAST						3.32	3.32	✓
VPN-5 Option verfügbar						integriert ab 3.32	integriert ab 3.32	integriert
VPN-25 Option verfügbar						✓	✓	✓
VPN Hardwarebeschleunigung								in Verbindung mit VPN-25
VPN-100								
VPN-200								
ADSL-Modem			✓		✓		✓	
Switch-Ports			4	4	4		4	4
ISDN Festverbindungs-Option	✓	✓	✓	✓	✓	✓	✓	✓
Faxmodem Option	✓	-	-	-	-	-	-	-
Dynamic DNS, CRON	3.10	3.10	3.10	✓	✓	3.10	3.10	✓
DSLolL			3.10		✓		3.10	
WLAN-802.11b				✓	✓			
WLAN-802.11g				✓	✓			
WLAN-802.11a (inkl. Turbo-Modus)								
Multi-SSID, IP-Redirect				3.42	3.42			
Super A/G				3.42	3.42			
DHCP Auto Client Modus	3.42	3.42	3.42	3.42	3.42	3.42	3.42	3.42
802.11i m. HW-AES				3.50	3.50			
SSH-Konfigurations-Zugang			4.00	4.00	4.00	4.00	4.00	4.00
Redundante VPN-Gateways						4.00	4.00	4.00
Rechteverwaltung für Admins			4.00	4.00	4.00	4.00	4.00	4.00
LEPS				4.00	4.00			
Freies Port-Mapping			4.00	4.00	4.00	4.00	4.00	4.00
mehrere Loopback-Adressen			4.00	4.00	4.00	4.00	4.00	4.00
Multi-PPPoE			4.00	4.00	4.00	4.00	4.00	4.00
Standard-WEP-Verschlüsselung				4.00	4.00			
802.11i für P2P im WLAN				4.00	4.00			
IKE-Config-Mode						4.00	4.00	4.00

▷ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	800/1000/1100	I-10	821	1511	1521	1611	1621	1711
Modembetrieb an serieller Schnittstelle			4.10	4.10	4.10	4.10	4.10	4.10
Load Balancing			2 Kanäle 5.00	2 Kanäle 5.00	2 Kanäle 5.00		2 Kanäle 5.00	4 Kanäle 5.00
WLANmonitor				5.00	5.00			
Gruppenkonfiguration				5.00	5.00			
Scripting			5.00	5.00	5.00	5.00	5.00	5.00
digitale Zertifikate (X.509) inkl. PKCS #12						5.00	5.00	5.00
AES 256 / IPCOMP						5.00	5.00	5.00
volltransparenter Client Bridge Mode				5.00	5.00			
Ethernet Port Mapping				5.00	5.00			5.00
Policy based Routing			5.00	5.00	5.00	5.00	5.00	5.00
ISDN basierende Diebstahlsicherung			5.00	5.00	5.00	5.00	5.00	5.00
Port Sniffer				5.00	5.00			5.00

▷ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	1811	1821	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
Stateful Inspection, DoS, IDS	✓	✓	2.80	2.80	2.80	2.80	✓	✓
IP-QoS, Traffic Shaping	✓	✓	3.30	3.30	3.30	3.30	✓	✓
N:N-Mapping	3.30	✓	3.30	3.30	3.30	3.30	✓	✓
VLAN	3.30	✓	3.30					
DMZ-Port	1)	1)				✓	1)	1)
AES, 3-DES, DES, Blowfish, CAST	3.32	✓	✓	✓	✓	✓	✓	✓
VPN-5 Option verfügbar	integriert ab 3.32	integriert	✓	✓				
VPN-25 Option verfügbar	✓	✓	✓	✓				
VPN Hardwarebeschleunigung	in Verbindung mit VPN-25	in Verbindung mit VPN-25					✓	✓
VPN-100					✓		✓	
VPN-200						✓		✓ ⁴⁾
ADSL-Modem		✓						
Switch-Ports	4	4					4	4
ISDN Festverbindungs-Option	✓	✓		integriert	integriert	integriert	integriert	integriert
Faxmodem Option	-	-	-	integriert	✓	-	✓	-
Dynamic DNS, CRON	✓	✓	3.10	3.10	3.10	3.10	✓	✓
DSLolL		✓						
WLAN-802.11b	✓	✓	✓					
WLAN-802.11g	✓	✓	✓ ⁶⁾					
WLAN-802.11a (inkl. Turbo-Modus)	✓	✓	✓ ⁶⁾					
Multi-SSID, IP-Redirect	3.42	3.42	3.42 ³⁾					
Super A/G	3.42	3.42	3.42 ³⁾					
DHCP Auto Client Modus	3.42	3.42	3.42	3.42	3.42	3.42	✓	3.42
802.11i m. HW-AES	3.50	3.50	- / 3.50					
SSH-Konfigurations-Zugang	4.00	4.00	4.00	4.00	4.00	4.00	✓	4.00
Redundante VPN-Gateways	4.00	4.00	4.00 ²⁾	4.00	4.00	4.00	✓	4.00
Rechteverwaltung für Admins	4.00	4.00	4.00	4.00	4.00	4.00	✓	4.00
LEPS	4.00	4.00	4.00					
Freies Port-Mapping	4.00	4.00	4.00	4.00	4.00	4.00	✓	4.00
mehrere Loopback-Adressen	4.00	4.00	4.00	4.00	4.00	4.00	✓	4.00
Multi-PPPoE	4.00	4.00	4.00			4.00	✓	4.00
Standard-WEP-Verschlüsselung	4.00	4.00	4.00					
802.11i für P2P im WLAN	4.00	4.00	4.00					

▷ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	1811	1821	3050 3550	4000 4100	6000 6001 6021	7011	7111	8011
IKE- Config- Mode	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00
Modembetrieb an serieller Schnittstelle	4.10	4.10					4.10	4.10
Load Balancing	4 Kanäle 5.00	4 Kanäle 5.00					4 Kanäle 5.00	4 Kanäle 5.00
WLANmonitor	5.00	5.00	5.00					
Gruppenkonfiguration	5.00	5.00	5.00					
Scripting	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
digitale Zertifikate (X.509) inkl. PKCS #12	5.00	5.00	5.00			5.00	5.00	5.00
AES 256 / IPCOMP	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
volltransparenter Client Bridge Mode	5.00	5.00	5.00					
Ethernet Port Mapping	5.00	5.00					5.00	5.00
Policy based Routing	5.00	5.00	5.00	5.00	5.00	5.00	5.00	5.00
ISDN basierende Diebstahlsicherung	5.00	5.00		5.00	5.00	5.00	5.00	5.00
Port Sniffer	5.00						5.00	5.00

▷ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	OAP	800+	DSL/I-10+
Stateful Inspection, DoS, IDS	2.80	2.80	2.80	2.80	2.80	2.80	✓	✓	✓
IP-QoS, Traffic Shaping	3.30	3.30	3.30	3.30	3.30	3.30	✓	✓	✓
N:N-Mapping					4.10	4.10	✓	4.10	4.10
VLAN			3.30	3.30	3.30	3.30	✓		
DMZ-Port								1)	1)
AES, 3-DES, DES, Blowfish, CAST									
VPN-5 Option verfügbar									
VPN-25 Option verfügbar							✓		
VPN Hardwarebeschleunigung							in Verbindung mit VPN-25		
VPN-100									
VPN-200									
ADSL-Modem									
Switch-Ports								4	3
ISDN Festverbindungs-Option		✓		✓				✓	✓
Faxmodem Option	-	✓		✓	-	-	-	✓	✓
Dynamic DNS, CRON			3.10	3.10	3.10	3.10	✓	✓	✓
DSLolL			3.10	3.10	3.10	3.10			
WLAN-802.11b	✓	✓	✓	✓	✓	✓	✓		
WLAN-802.11g					✓	✓	✓		
WLAN-802.11a (inkl. Turbo-Modus)						✓	✓		
Multi-SSID, IP-Redirect	3.42	3.42	3.42	3.42	3.42	3.42	✓		
Super A/G					3.42	3.42	✓		
DHCP Auto Client Modus	3.42	3.42	3.42	3.42	3.42	3.42	✓	✓	✓
802.11i m. HW-AES					3.50	3.50	✓		
SSH-Konfigurations-Zugang					4.00	4.00	✓	✓	✓
Redundante VPN-Gateways									
Rechteverwaltung für Admins					4.00	4.00	✓	✓	✓
LEPS					4.00	4.00	✓		
Freies Port-Mapping					4.00	4.00	✓	✓	✓
mehrere Loopback-Adressen					4.00	4.00	✓	✓	✓
Multi-PPPoE					4.00	4.00	✓		✓
Standard-WEP-Verschlüsselung					4.00	4.00	✓		
802.11i für P2P im WLAN					4.00	4.00	✓		
IKE-Config-Mode									
Modembetrieb an serieller Schnittstelle					4.10	4.10		4.10	4.10

▷ Übersicht über die Funktionen nach Modellen und LCOS*- Versionen

	L-2	IL-2	L-11	IL-11	L-54g	L-54ag IAP	OAP	800+	DSL/I-10+
Load Balancing									2 Kanäle 5.00
WLANmonitor					5.00	5.00	5.00		
Gruppenkonfiguration					5.00	5.00	5.00		
Scripting					5.00	5.00	5.00	5.00	5.00
digitale Zertifikate (X.509) inkl. PKCS #12							5.00		
AES 256 / IPCOMP							5.00		
volltransparenter Client Bridge Mode					5.00	5.00	5.00		
Ethernet Port Mapping							5.00		5.00
Policy based Routing					5.00	5.00	5.00	5.00	5.00
ISDN basierende Diebstahlsicherung								5.00	5.00
Port Sniffer							5.00	5.00	5.00

17 Index

Numerics

1-1-Mapping	142
2,4 GHz ISM-Frequenzband	335
3-DES	252, 320, 454, 456, 458
5 GHz Frequenzband	334
802.11	334, 449
802.11i	344
PMK-Caching	352
VoIP	352
802.11x	
Rekeying	349

A

AAL-5	121
Access Control List	359
Access Point	449
Access Points	78
Access Router	449
Administratoren	41
Administratorengruppe	41
Adress-Pool	414
Adressverwaltung	412
ADSL	18, 83, 449
ADSL-Modem	454, 456, 458
AES	252, 320, 345, 449, 454, 456, 458
AES-CCM	351
Aggressive Mode	251
AH	252, 319, 321
Allow-All	179, 195
Anruferkennung	99
Antennen-Gewinn	371
AOCD	427
Application Gateway	175
asymmetrischen Verschlüsselung	279
AT-Befehle	163
ATM	83
ATM-Anpassungsschicht	121
Ausschluss-Routen	111
Authentifizierung	153, 344, 347

Authentifizierungsverfahren

TLS	348
TTLS	348
Authentizität	278
auto reconnect	152

B

Backup-Lösungen	393
Backup-Verbindung	165, 398
Bandbreite	449
Benutzername	35, 99, 150
Benutzerrechte	43
B-Kanal	
Protokoll	100
B-Kanal-Protokolle	411
Blacklist	370
Blowfish	252, 320, 345
Bonk	222
Breitband	449
Bridge	449
Broadcast	449
Brute-Force	94
Bruttodatenrate	232
BSS	449

C

CA	282
Calling Line Identifier Protocol	100
CAP1	449
CAP1 Faxmodem	409
CAP1 Protokolle	411
CAP1 Schnittstelle	405
CAST	252, 320
CCK	449
Certification Authority	282
CHAP	99
Client	449
Client-Modus	342, 373
CLIP	100
Collision Domain	325

Common ISDN Application Programming Interface (CAPI)	405	Zuweisung der Broadcast-Adresse	415
Conf	150	Zuweisung der Netzmaske	415
CRC	450	Zuweisung des Standard-Gateways	415
CRON	454, 456, 458	Zuweisung von DNS- und NBNS-Server	415
CRON-Dienst	433	Dienst	417
CRON-Tabelle	435	Dienstgüte –	
CSMA/CA	450	siehe Quality-of-Service	
D		Differentiated Services –	
Datendurchsatz	450	siehe DiffServ	
Datenkompressionsverfahren		Differentiated Services Code Point –	
LZS	156	siehe DSCP	
Datenübertragung	156	Diffie-Hellman-Verfahren	323
Datum/Zeit	431	DiffServ	227, 228
Dead-Peer-Detection	394, 396	Assured Forwarding	227, 228
Default-Gateway	105	Best Effort	228
Deflate	252	Class Selector	228
Denial of Service	18	Expedited Forwarding	227, 228, 230
Denial-of-Service	220	IPSec	227
Bonk	222	Distanz einer Route	111
Fragrouter	222	D-Kanal	83, 100
Konfiguration	222	DMZ	
LAND	221	Zuweisung von IP-Adressen	414
Ping of Death	221	DMZ-Port	454, 456, 458
Smurf	220	DMZ-Schnittstelle	18
SYN Flooding	220	DNS	83, 417, 450
Teardrop	221	DNS-Forwarding	418
Denial-of-Service-Angriffe	220	DNS-Server	412, 415, 417
LAND	221	DNS-Tabelle	421, 422
Smurf	220	Dynamic DNS	423
SYN Flooding	220	Filterliste im DNS-Server	422
Deny-All	195	Filtermechanismus des DNS-Servers	418
DES	252, 320, 345	URL-Blocking	422
DFS	369	verfügbare Informationen im DNS-Server	418
Black- und White-List	369	Domain	417, 422
DFÜ-Netzwerk	32, 99	sperrern	423
DHCP	82, 121, 412, 450	Domain Name Service (DNS)	417
Automodus für den DHCP-Server	413	Domäne	450
DHCP-Server	412, 418	DoS	454, 456, 458
Gültigkeitsdauer	416	Konfiguration	222
		Download	15, 450
		Downstream	450

Downstreamrate	232	End-Adresse	414
DPD	394, 396	Enhanced Passphrase Security	354
DS	450	Enterprise specific Traps	443
DSCP	228	ESP	252, 319
DSL	18, 450	ESS	450
DSLol	18, 454, 456, 458	ESSID	450
DSSS	335, 450	ETH-10	121
Durchsatz	156	Ethernet	450
Dynamic DNS	423, 450, 454, 456, 458	exposed host	124
Dynamic Frequency Selection	369	Extensible Authentication Protocol	347, 381
Dynamic Host Configuration Protocol (DHCP)	412	F	
Dynamic VPN		Fail	150
Beispiele	310	Fast Call Back	101
dynamisch - dynamisch	257, 312	Fax	409
dynamisch - statisch	255, 310	Fax Class 1	409
Einführung	254	Faxmodem Option	454, 456, 458
Funktionsweise	255	Faxmodem-Option	411
ICMP	310	Faxtreiber	409
PPP-Liste	265	Faxübertragung	410
statisch - dynamisch	256, 310	Fehlende Gebühreninformationen	427
UDP	310	Fehlersuche	74
Dynamic-VPN	402	Fernkonfiguration	19
Dynamische Kanalbündelung	156	Fernüberwachung	140
Dynamisches Routing	110	Fernverbindung	33
dynDNS	423	Fernwartung	
E		mit N-N-Mapping	141
EAP	347, 450	FHSS	450
Ablauf einer mittels EAP geschützten Sitzung	347	Filterliste	178, 180
RADIUS-Server	348	Firewall	105, 168, 340, 405, 450
EAP/802.1x	349	Alarmierungsfunktionen	191
Master Secret	349	Allow-All	179, 195
EAP-MD5	450	Anwendungsfälle	199
EAP-TLS	450	Application Gateway	175
EAP-TTLS	450	Assistent	201
Einzel-WEP-Einstellungen	362	Aufgaben	171
EIRP	450	Authentifizierungs-Port	184
E-Mail-Benachrichtigung	191	Beispielkonfiguration Basic Internet	199
E-Mail-Viren	198	Beispielkonfiguration IPSec/PPTP-Freischaltung	200
Encapsulation	120	Beispielkonfiguration ISDN-Einwahl	200
		Beispielkonfiguration Netzwerkkopplung	200

Beispielkonfiguration V.110-Einwahl	200	Firewall/QoS-Aktivierung	182
Beispielkonfiguration VPN-Einwahl	199	Firewall-Regel	
Benachrichtigung per E-Mail	192	Absender-Adresse sperren	190
Benachrichtigung per SNMP-Trap	194	Aktionstabelle	207
Besondere Protokolle	180	Aufbau	188
Default-Einstellung	197	Bedingung	187, 189
Deny-All	195, 198, 199	E-Mail-Nachricht senden	190
Diagnose	211	Konfiguration	201
DMZ	195	Konfiguration mit LANconfig	201
DMZ (Schaubild)	196	Konfiguration mit WEBconfig oder Telnet	205
dualhomed Gateway	175	Limit	187, 189
Einstellungen	182	Objekttabelle	206
Ereignisanzeige	211	Paket-Aktion	187, 190
Filterliste	178, 213	Priorität	185
Firewall-Tabelle	211	Quality of Service	187, 191
Fragmente	182	Regel-Tabelle	205
Hostsperrliste	178, 217	Schaubild	188
ICMP	183	SNMP senden	190
ICMP-Verbindungen	181	Sonstige Maßnahmen	187, 190
Komponenten	170	Syslog-Nachricht senden	190
Logging-Tabelle	211	Trigger	187, 189
NAT	198	Verbindung	186, 188
paketfilterbasiert	172	Verbindung trennen	190
Parameter der Firewall-Regeln	185	Verknüpfung	185, 186
Ping-Blocking	183	VPN-Regel	185, 186
Portsperrliste	178, 217	Ziel-Port sperren	190
Prüfen mit mehreren Listen	179	Firewall-Tabelle	211
Quell- und Zielobjekte	207	FirmSafe	37
Schaubild	177	Firmware	15, 29
Sitzungswiederherstellung	183	Firmware-Updates	51
Stafeful Inspection	173	Firmware-Upload	38
Stateful-Inspection	198	mit Terminalprogramm	39
Stationen sperren	106	mit TFTP	40
Strategien für die Einstellung	195	Firmware-Versionen	53
SYSLOG	191	Flash-No-Modus	57
TCP-Stealth-Modus	184	Flash-ROM-Speicher	37
TCP-Verbindungen	181	Flash-Yes-Modus	56
Tipps zur Einstellung	197	Flatrate	151
Typen	172	FQDN	423
UDP-Verbindungen	180	Fragrouter	222
Verbindungsliste	178, 215	Frame-Tagging	326

Frequenz	450	Hohe Telefonkosten	425
Frequenzband	450	Home-Office	128
FTP	450	Host	417
aktives FTP	238	Hostsperrliste	178, 179
passives FTP	238	HotSpot	451
TCP-gesicherte Übertragung	234	HSCSD	121
FTP-Datentransfer	233	HTTPS	23
FTP-Download	226	Hub	451
Funkfrequenz	450	I	
Funkkanäle	444	IAPP-Roaming	451
Funk-LANs		IBBS	374
Ad-hoc	337	IBSS	451
Betriebsarten	337	ICMP	106, 200, 310
Funk-Brücke	341	ICMP Polling	394, 395
Infrastruktur-Netzwerk	338	ICMP-Verbindungen	181
Funknetzwerk	334	Identifikationskontrolle	98, 99
Funktionsrechte	42	Identifizierung des Anrufers	99
Funkzelle	339, 342	IDS	451, 454, 456, 458
G		Konfiguration	219
Gateway	412, 450	IEEE	451
Gebühren		IEEE 802.11a	334
Begrenzung	425	IEEE 802.11b	334, 335
Einheiten	156, 427	IEEE 802.11g	334, 335
Information	156, 427	IEEE 802.1p/q	325
Management	425	IEEE 802.1x/EAP	381
Zeit-Limit	426	IEEE 802.3	121, 334
Gebührenüberwachung	405	IKE	252, 323
Gegenstelle	150	IKE Config Mode	266
Gegenstellen	164	IKE-Proposals	298
Gerätename	150	Inband	19
GRPS-Backup-Verbindung	161	Konfiguration über Inband	19
Gruppen-Konfiguration	66	mit Telnet	25
Gültigkeitsdauer	412, 416	Integrität	278
H		Internet-Zugang	149
Haltezeit	156, 157	Intranet	
Hash	288	Zuweisung von IP-Adressen	414
Hash-Algorithmen	252	Intrusion Detection	18, 218
HDLC	121	Konfiguration	219
Hidden-Station	379	Intrusion-Detection	
Hinweis-Symbole	16	IP-Spoofing	218

Portscan	218		
Inverses Masquerading	124, 139		
IP	451		
Filter	105		
Ports sperren	105		
IP Quality-of-Service	451		
IP-Adresse	76, 106, 149		
IP-Adressen			
dynamische	254, 255		
statische	254		
IP-Adressverwaltung	412		
IP-Broadcast	117		
IPCOMP	252		
IP-Header	227		
IP-Masquerading	18, 82, 105, 139, 340, 451		
IP-Module	18		
IP-Multicast	117		
IP-Parameter	265		
IP-Redirect	17		
IP-Router	17		
IP-Routing			
Standard-Router	114		
IP-Routing-Tabelle	110		
IPSec	251, 316, 344, 451		
IPSec-over-WLAN	382		
IP-Spoofing	218		
IP-Telefonie	233		
IPv4-Adresse	139		
IPv6	317		
IPX-Router	18		
ISAKMP	252, 323		
ISDN	18, 451		
B-Kanal	258		
D-Kanal	100, 257, 258		
Euro-ISDN (DSS-1)	258		
LLC	258		
ISDN Festverbindungs-Option	454, 456, 458		
ISDN-Administrationszugang	95		
ISDN-Fernzugang	32		
ISM-Frequenzband	335, 451		
ISP	451		
		K	
		Kanalbündelung	155
		Dynamisch	156
		Statisch	156
		Keep-alive	151
		Keep-Alive-Verbindungen	400
		Kompatibilitätsmodus	337
		Konfiguration	
		Verfahren	19
		Konfigurationsdatei	106
		Konfigurationskennwort	104
		Konfigurations-Schnittstelle	19
		Konfigurationsupdates	55
		Kontaktbelegung	166
		Kosten begrenzen	425
		L	
		L2F	317
		L2TP	317
		LAN	451
		logisch	326
		physikalisch	326
		LAN-Bridge	18
		LANCAPI	18
		LANcapi	451
		LANCOM-Betriebssystem	17
		LANconfig	21, 32, 48, 451
		Verwaltung mehrerer Geräte	22
		LAND	221
		LANmonitor	70
		Accounting-Informationen	72
		Aktivitätsprotokoll	73
		Anzeige-Optionen	74
		Firewall-Ereignisanzeige	73
		Internet-Verbindung kontrollieren	75
		System-Informationen	74
		VPN-Verbindungen	71
		LANtools	451
		Lastenausgleich	313
		Layer-2	121
		Layer-2-Switch	325

Layer-3	121	MTU	166
Layername	120	Multilink PPP (MLPPP)	155, 156
LCOS	14, 17, 451, 454	Multilink-PPP (MLPPP)	146
LCP-Echo-Reply	148	Multilink-PPPoE (MLPPPoE)	146
LCP-Echo-Request	148	Multi-PPPoE	128, 130, 401
LCR	427	Multi-SSID	342, 343, 376
Least-Cost-Routing	427	Multithreading	50
LEPS	354	N	
LLC-MUX	120	N	
Logging-Tabelle	211	N-Mapping	18, 454, 456, 458
Login	37	NAT	139
Login-Sperre	94	NBNS-Server	412
Login-Versuche	94	NetBIOS	82, 418
logische Funknetze	357	NBNS	265
logische Senderichtung	238	NetBios	451
logisches LAN	326	NetBIOS/IP	265
Loopback-Adresse	142	NetBIOS-Netze	418
Loopback-Adressen	47	NetBIOS-Proxy	198, 265
LZS-Datenkompression	156	Nettodatenrate	232
M		Nettoübertragungsrate	336
MAC	451	Network Address Translation	139
MAC-Adresse	356, 451	Netzkopplung	140
MAC-Adressfilter	340	Netzmaske	106
MAC-Filter aktiviert	378	Netzwerk-Management	48
MAC-Frame	327	Netzwerknamen	417
Mailserver	422	N-N-Mapping	139
Main Mode	251	dezentrales Mapping	142
maskierten Verbindungen	437	DNS-Forwarding	144
Maximalbandbreite	227, 229	Firewall	144
Mbit	451	Konfiguration	143
MIB2	443	Loopback-Adresse	144
MIC	451	NAT-Tabelle	143
Mindestbandbreite	227, 229, 230	Netzwerkkopplung über VPN	141
beim Empfang	229	Routing-Tabelle	143
beim Senden	229	VPN-Regel	144
MLPPPoE	130	zentrales Mapping	142
Modem	121	NTBA	451
Modem Adapter Kit	159	NTP-Clients	432
Modem-Parameter	160	NTP-Server	431
MS-CHAP	146, 147		

O			
OFDM		335, 451	
Online-Minuten		425	
OpenSSL		294	
Outband		19	
Konfiguration über Outband		19	
Overhead		226	
P			
P2P-Betrieb		382	
P2P-Master		384	
Paket-Dump		83	
Paketfilter		172	
PAP		99	
passwd		94	
Passwort	33, 34, 75, 92, 98, 99,	150	
Passwortschutz		53	
PEAP		452	
Periode		425	
physikalische Senderichtung		238	
physikalische WLAN-Schnittstelle		357	
physikalisches LAN		326	
ping		200	
Ping of Death		221	
Ping-Befehl		88	
Ping-Blocking		183	
ping-Blocking			
Konfiguration		224	
PKCS#12-Datei		291	
PKI		281, 452	
PMTU-Reduzierung		234	
Point-to-Multipoint		337	
Point-to-Multipoint (WLAN)		452	
Point-to-Point (WLAN)		452	
Point-to-Point Tunneling			
Protocol (PPTP)		151	
Policy-based Routing		112	
Port Address Translation		139	
Port-Mapping		437	
Portscan		218	
Port-Separierung		452	
Portsperrliste			178, 179
PPP			76, 99, 121, 156, 452
LCP Extensions			154
Leitungsüberprüfung mit LCP			148
Rückruf-Funktionen			152
Verhandlungsphase			35
Zuweisung von IP-Adressen			149
PPP LCP Echo Monitoring			394
PPP-Client			32
PPPoE			121
PPP-Verbindung			34
PPTP		18, 151, 317, 344,	452
Precedence			228
Preshared Key			252
Pre-Shared-Key			345
Preshared-Key-Verfahren			283
Private			279
Private Key			279
Private Mode			452
Projektmanagement			48
Protokoll-Filter			359
Prüfsumme			288
PSK			345
PSK-Verfahren			283
Public Key			279
Public-Key			324
Public-Key-Infrastructure			281
Public-Key-Verfahren			279
Punkt-zu-Punkt-Verbindungen			382
Q			
QoS		233, 452, 454, 456,	458
Richtung der Datenübertragung			238
QoS –			
siehe Quality-of-Service			
Quality of Service			18
Quality-of-Service			226
Queue			230
R			
Radarsignal			370
RADIUS			348, 452

RADIUS-Server	381	Security Parameter Index	318
RAS	247, 248	Serielle Schnittstelle	19
RC4	345, 452	seriellen Schnittstelle	157
Rechner-Namen	417	Server	452
Rechteverwaltung	41	Service Set Identifier	342
Redirect	359, 380	Sicherheit	92, 168
redundante Gateways	400	Sicherheits-Checkliste	104
RegTP	281	Sicherheitseinstellungen	15, 94
Reichweite	336, 339	Sicherung	150
Remote Access	149	Sicherungsverfahren	100
RFC	452	SINA	452
RFCs	448	SMTP	452
Rijndael	320	Smurf	220
RIP	82	SNMP	31, 42, 75
Roll-Out	56	Konfiguration schützen	105
Router	111, 340, 452	SNMP-ID	27
Router-Interface-Liste	157	SNMP-Lesezugriff	53
Routing-Tabelle	105	SNMP-Trap	142, 191, 194
Routing-Tag	185	SNMP-Traps	443
RSA	252, 345	SNMPv3	452
RTS/CTS-Protokoll	379	Software einspielen	37
RTS-Schwellwert	379	Speicherauslastung	75
Rückruf	99, 100	Splitter	452
Fast Call Back	101, 154	SSH-Zugang	31
nach Microsoft CBCP	152	SSID	78, 342, 452
nach RFC 1570	154	SSL	452
schnelles LANCOM-Verfahren	154	Stac-Datenkompression	156
RX-Rate	79	Stand alone Windows CA	289
S		Standard-Faxprogramme	409
Scheduled Events	433	Start-Adresse	414
Schlüssel		Stateful Inspection	454, 456, 458
Öffentlich	279	Stateful-Inspection	340
privat	279	Stateful-Packet-Inspection	173
Schlüssellängen	252	Stations-Namen-Tabelle	421
Schutz		Statische Kanalbündelung	156
für die Konfiguration	92	Statisches Routing	110
Scripting	55	Statistik	163, 167
Befehle	62	Stealth-Modus	
SDSL	452	Konfiguration	224
Security Association	318	Support	16
		Switch	452

symmetrische Verschlüsselung	278	Trojaner	198
SYN Flooding	220	Tunnelmodus	252, 319
SYN/ACK-Speedup	117	Turbo-Modus	335, 336
SYSLOG	86, 191, 428	TX-Rate	79
SYSLOG-Meldung	191	Type-of-Service – siehe ToS	
T		U	
TAE	452	Übertragungsraten	76, 336
TCP	106, 226	Überwachung	73
TCP/IP	109, 452	UDP	106, 226, 310
TCP/IP-Filter	105	UDP-Verbindungen	180
TCP/IP-Netze	417	Upload	37, 453
TCP-Stealth-Modus	184	Upstream	453
TCP-Steuerungspakete	230	Upstreamrate	232
TCP-Verbindungen	181	URL-Blocking	422
Teardrop	221	Username	150
Teil-Konfiguration	66	V	
Telnet	18, 32, 106	V.110	121
Ausgabe der SNMP-ID	27	VC-MUX	120
Temporal Key Integrity Protocol	350	Verbindungsbegrenzung	427
Term	150	Verbindungsliste	178, 180
Terminalprogramm	38	Verkettung	453
TFTP	18, 29, 42, 106	Verschlüsselte Konfiguration	31
TFTP laden	29	Verschlüsselung	250, 320, 324, 345
Timeout	156	asymmetrisch	279
TKIP	452	asymmetrische	345
TLS	452	Kombination symmetrisch/asymmetrisch	280
ToS	227, 228	symmetrisch	278
High Reliability	227	symmetrische	345
IPSec	227	Verschlüsselungsverfahren	
Low Delay	227, 230	AES-CCM	351
Priorität	228	Vertraulichkeit	278
TPC	452	Virtual Private Network	247
Trace		virtuelles LAN	325
Ausgaben	81	VLAN	325, 454, 456, 458
Beispiele	85	Abschirmung des SNMP-Traffics	328
Schlüssel und Parameter	81	Alle VLANs zulassen	331
starten	81	Anschluss von WLAN-Stationen	328
Trace-Ausgaben	163	Default-ID	331
Transportmodus	252, 319	Default-VLAN-ID	326
Triple-DES	252, 320		

ID	326	W	
Konfiguration	330	WAN	453
Management des LAN-Traffics	328	Warteschlangen	230
Netzwerktafel	330	gesicherte Queue	230
Nutzung einer zentralen Verkabelung	329	Standard-Queue	231
Port	330	Urgent Queue II	230
Portliste	330	Urgent-Queue I	230
Porttafel	330	WEBconfig	18, 23, 453
Priorität	327	HTTPS	23
Tagging verwenden	331	WECA	453
Umsetzung in den Schnittstellen	327	well known groups	252
Ungetaggte Frames zulassen	331	WEP	361, 364, 453
Verschiedene Organisationen auf einem LAN	329	Einzel-WEP-Einstellungen	361
VLAN-ID	330	Erklärung des Verfahrens	345
VLAN-ID	326	RC4	346
Voice-over-IP	226, 229	Sniffer-Tools	346
VoIP –		WEP-Gruppen-Schlüssel	365
siehe Voice-over-IP		WEPplus	347
VPN	18, 247, 453, 454, 456, 458	Grenzen	347
Beispiele	308	WEP-Schlüssel	
Client	200	dynamisch	347
dynamisch - dynamisch	312	WEP-Verschlüsselung	356
dynamisch - statisch	310	Whitelist	370
Fernwartung über N-N-Mapping	141	Wiederholungen	150
Gateway	199	WiFi	453
Konfiguration	262	Wifi Protected Access	349
Konfiguration mit LANconfig	270	WiFi-Alliance	453
Konfiguration mit WEBconfig	274	Wildcards	423
Netzwerkkopplung mit N-N-Mapping	140	Windows Netzwerke	265
statisch - dynamisch	310	WINS-Server	265
statisch - statisch	309	Wired Equivalent Privacy	345
VPN Anwendungsbeispiel	250	Wireless LAN	334
VPN Load Balancing	400	Wireless Local Area Network	334
VPN-Client	253	WISP	453
VPN-Gateway	404	WLAN	334, 453
VPN-Netzbeziehungen	267	ACL	359
VPN-Regeln	264	Ad-hoc-Modus	337
VPN-Verbindungen	313	Adress-Anpassung	374
Diagnose	277	ARP-Behandlung	367
manuelles Einrichten	265	Basisstations-Dichte	372
Setup-Assistent	263	Betriebsart	368

Bevorzugte BSS-ID	374	WEP	345
Bridge-Modus	337	WEPplus	347
Client-Bridge-Unterstützung	375	WPA	349
Client-Modus	337, 373	WPA	344, 349, 453
Client-Verbindung aufrecht erhalten	374	Group Key	350
Closed-Network-Modus	377	Handshake-Verfahren	349
DFS-Verfahren	369	Key-Handshake	350
Durchsuchte Bänder	374	Master Secret,	349
Frequenzband	369	Michael	349
IBBS	374	Pairwise Key	350
Infrastruktur-Modus	337	Passphrase	350
IPSec-over-WLAN	382	Rekeying	350
Kanalnummer	370	TKIP	349, 350
Kompatibilitätsmodus	370	X	
Ländereinstellung	366	X.509	252
Link-Fehler-Erkennung	367	X.75	121
Maximaler Abstand	372	xDSL	453
Multi-SSID	337	XOR	453
Netzwerkeinstellungen	377	Y	
Netzwerktypen	374	Y-Verbindung	157
Point-to-Point-Modus	337	Z	
Protokoll-Filter	359	Zeit	150
Punkt-zu-Punkt-Verbindungen	372	Zeitabhängige Verbindungs-	
Radio-Einstellungen	369	begrenzung	427
Redirect	380	Zeitautomatik	433
Sendeleistungs-Reduktion	371	Zeitbudget	427
SSID	377	Zeit-Server	431
Turbomodus	371	Zertifikate	278
Unterband	369	Aufbau	284
WEP-Gruppen-Schlüssel	364	Dateitypen	286
WLANmonitor	77	Export	292, 293
WLAN-Schnittstelle		Gültigkeit	286
logisch	376	OpenSSL	294
physikalisch	368	PKCS#12-Datei	291
WLAN-Sicherheit	344	Sicherheitsklassen	288
802.11i	351	Vorteile	283
802.1x	347	X.509-Standard	284
AES	351	Zertifizierung	
EAP	347	Anbieter	282
Sniffer-Tools	346		
TKIP	349		

ZLIB	252	Zugangsschutz für die Konfiguration	
Zugangsschutz	99	nach geprüfter Nummer	99
für die Konfiguration	98	nach Nummer	99

