

Referenzhandbuch

© 2004 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.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit <http://www.openssl.org/>.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, März 2004

Inhalt

1 Einleitung	9
2 System-Design	12
3 Konfiguration	15
3.1 Mittel und Wege für die Konfiguration	15
3.2 Software zur Konfiguration	16
3.3 Die Konfiguration mit verschiedenen Tools	17
3.3.1 LANconfig	17
3.3.2 WEBconfig	19
3.3.3 Telnet	20
3.3.4 TFTP	23
3.3.5 SNMP	23
3.3.6 Fernkonfiguration über das DFÜ-Netzwerk	24
3.4 Abspeichern, Wiederherstellen und Erzeugen von Konfigurationsdateien	28
3.5 Neue Firmware mit LANCOM FirmSafe	29
3.5.1 So funktioniert LANCOM FirmSafe	29
3.5.2 So spielen Sie eine neue Software ein	31
4 Netzwerk-Management mit den LANtools	34
4.1 Projektmanagement mit LANconfig	34
4.1.1 Verzeichnisstruktur	36
4.1.2 Multithreading	37
4.2 Anzeige-Funktionen im LANmonitor	39
4.3 Scheduled Events	42
4.3.1 Zeitautomatik für LCOS-Befehle	42
4.3.2 Die Cron-Tabelle	44
4.3.3 Konfiguration der Zeitautomatik	45
5 Diagnose	47
5.1 LANmonitor – wissen, was läuft	47
5.1.1 Erweiterte Anzeige-Optionen	47
5.1.2 Internet-Verbindung kontrollieren	48
5.2 Trace-Ausgaben – Infos für Profis	50

► *Inhalt*

5.2.1	So starten Sie einen Trace	50
5.2.2	Übersicht der Schlüssel	51
5.2.3	Übersicht der Parameter	51
5.2.4	Kombinationsbefehle	52
5.2.5	Beispiele	53
6	Sicherheit	54
6.1	Schutz für die Konfiguration	54
6.1.1	Passwortschutz	54
6.1.2	Die Login-Sperre	57
6.1.3	Einschränkung der Zugriffsrechte auf die Konfiguration	57
6.2	Den ISDN-Einwahlzugang absichern	62
6.2.1	Die Identifikationskontrolle	62
6.2.2	Der Rückruf	64
6.3	Die Sicherheits-Checkliste	65
7	Routing und WAN-Verbindungen	69
7.1	Allgemeines über WAN-Verbindungen	69
7.1.1	Brücken für Standard-Protokolle	69
7.1.2	Was passiert bei einer Anfrage aus dem LAN?	70
7.2	IP-Routing	71
7.2.1	Die IP-Routing-Tabelle	71
7.2.2	Lokales Routing	74
7.2.3	Dynamisches Routing mit IP-RIP	74
7.2.4	SYN/ACK-Speedup	78
7.3	IP-Masquerading	79
7.3.1	Einfaches Masquerading	79
7.3.2	Inverses Masquerading	83
7.3.3	Unmaskierter Internet-Zugang für Server in der DMZ	86
7.4	N:N-Mapping	87
7.4.1	Anwendungsbeispiele	88
7.4.2	Konfiguration	92
7.5	Die Konfiguration von Gegenstellen	96
7.5.1	Namenliste	96
7.5.2	Layer-Liste	99
7.6	Verbindungsaufbau mit PPP	100
7.6.1	Das Protokoll	101

7.6.2	Alles o.k.? Leitungsüberprüfung mit LCP	103
7.6.3	Zuweisung von IP-Adressen über PPP	104
7.6.4	Einstellungen in der PPP-Liste	105
7.7	DSL-Verbindungsaufbau mit PPTP	107
7.8	Dauerverbindung für Flatrates – Keep-alive	107
7.9	Rückruf-Funktionen	108
7.9.1	Rückruf nach Microsoft CBCP	108
7.9.2	Schneller Rückruf mit dem LANCOM-Verfahren	110
7.9.3	Rückruf nach RFC 1570 (PPP LCP Extensions)	110
7.9.4	Konfiguration der Rückruf-Funktion im Überblick	111
7.10	Kanalbündelung mit MLPPP	112
8	Firewall	116
8.1	Gefährdungsanalyse	116
8.1.1	Die Gefahren	116
8.1.2	Die Wege der Täter	117
8.1.3	Die Methoden	117
8.1.4	Die Opfer	118
8.2	Was ist eine Firewall?	119
8.2.1	Die Aufgaben einer Firewall	120
8.2.2	Unterschiedliche Typen von Firewalls	121
8.3	Die Firewall im LANCOM	127
8.3.1	So prüft die Firewall im LANCOM die Datenpakete	127
8.3.2	Besondere Protokolle	131
8.3.3	Allgemeine Einstellungen der Firewall	134
8.3.4	Die Parameter der Firewall-Regeln	138
8.3.5	Die Alarmierungsfunktionen der Firewall	145
8.3.6	Strategien für die Einstellung der Firewall	149
8.3.7	Tipps zur Einstellung der Firewall	151
8.3.8	Konfiguration der Firewall-Regeln	155
8.3.9	Firewall-Diagnose	165
8.3.10	Grenzen der Firewall	173
8.4	Abwehr von Einbruchsversuchen: Intrusion Detection	174
8.4.1	Beispiele für Einbruchsversuche	174
8.4.2	Konfiguration des IDS	175
8.5	Schutz vor "Denial-of-Service"-Angriffen	176
8.5.1	Beispiele für Denial-of-Service-Angriffe	176
8.5.2	Konfiguration der DoS-Abwehr	180

8.5.3 Konfiguration von ping-Blocking und Stealth-Modus 182

9 Quality-of-Service	183
9.1 Wozu QoS?	183
9.2 Welche Datenpakete bevorzugen?	184
9.2.1 Garantierte Mindestbandbreiten	186
9.2.2 Limitierte Maximalbandbreiten	187
9.3 Das Warteschlangenkonzept	187
9.3.1 Sendeseitige Warteschlangen	187
9.3.2 Empfangsseitige Warteschlangen	190
9.4 Reduzierung der Paketlänge	191
9.5 QoS-Parameter für Voice-over-IP-Anwendungen	193
9.6 QoS in Sende- oder Empfangsrichtung	197
9.7 QoS-Konfiguration	198
9.7.1 ToS- und DiffServ-Felder auswerten	198
9.7.2 Minimal- und Maximalbandbreiten definieren	200
9.7.3 Übertragungsraten für Interfaces festlegen	202
9.7.4 Sende- und Empfangsrichtung	204
9.7.5 Reduzierung der Paketlänge	204
10 Virtuelle LANs (VLANs)	207
10.1 Was ist ein Virtuelles LAN?	207
10.2 So funktioniert ein VLAN	208
10.2.1 Frame-Tagging	208
10.2.2 Umsetzung in den Schnittstellen des LANs	210
10.2.3 Anwendungsbeispiele	211
10.3 Konfiguration von VLANs	213
10.3.1 Die Netzwerktabelle	213
10.3.2 Die Porttabelle	214
10.3.3 Konfiguration mit LANconfig	215
10.3.4 Konfiguration mit WEBconfig oder Telnet	216
11 Bürokommunikation mit LANCAPI	218
11.1 Welche Vorteile bietet die LANCAPI ?	218
11.2 Das Client-Server-Prinzip	218
11.2.1 Konfiguration des LANCAPI-Servers	219
11.2.2 Installation des LANCAPI-Clients	221

11.2.3	Konfiguration des LANCAPI-Clients	222
11.3	So setzen Sie die LANCAPI ein	223
11.4	Das LANCOM CAPI Faxmodem	223
11.5	LANCOM Faxmodem-Option	224
11.6	Unterstützte B-Kanal-Protokolle	225
12	Weitere Server-Dienste	226
12.1	Automatische IP-Adressverwaltung mit DHCP	226
12.1.1	Der DHCP-Server	226
12.1.2	DHCP – 'Ein', 'Aus' oder 'Auto'?	227
12.1.3	So werden die Adressen zugewiesen	228
12.2	DNS	232
12.2.1	Was macht ein DNS-Server?	232
12.2.2	DNS-Forwarding	234
12.2.3	So stellen Sie den DNS-Server ein	235
12.2.4	URL-Blocking	238
12.2.5	Dynamic DNS	240
12.3	Gebührenmanagement	242
12.3.1	Verbindungs-Begrenzung für DSL und Kabelmodem	242
12.3.2	Gebührenabhängige ISDN-Verbindungsbegrenzung	244
12.3.3	Zeitabhängige ISDN-Verbindungsbegrenzung	245
12.3.4	Einstellungen im Gebührenmodul	246
12.4	Das SYSLOG-Modul	246
12.4.1	Einrichten des SYSLOG-Moduls	247
12.4.2	Beispielkonfiguration mit LANconfig	247
12.5	Zeit-Server für das lokale Netz	249
12.5.1	Konfiguration des Zeit-Servers unter LANconfig	249
12.5.2	Konfiguration des Zeit-Servers mit WEBconfig oder Telnet	251
12.5.3	Konfiguration der NTP-Clients	251

▶ *Inhalt*

13 VPN	253
14 Glossar	254
15 Anhang	260
15.1 SNMP-Traps	260
15.2 Unterstützte RFCs	262
15.3 Übersicht über die Funktionen nach LANCOM-Modellen und LCOS-Versionen	264
16 Index	265

1 Einleitung

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)
- ▷ Backuplösungen
- ▷ 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 Sicher-

► Kapitel 1: Einleitung

heit. 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 aus Würselen

Gültigkeit

Das vorliegende Referenzhandbuch gilt für alle LANCOM-Router und LANCOM Wireless Access Points mit einem Firmwarestand Version 3.32 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 LANCOM-Modellen und LCOS-Versionen' → Seite 264).

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 54.

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

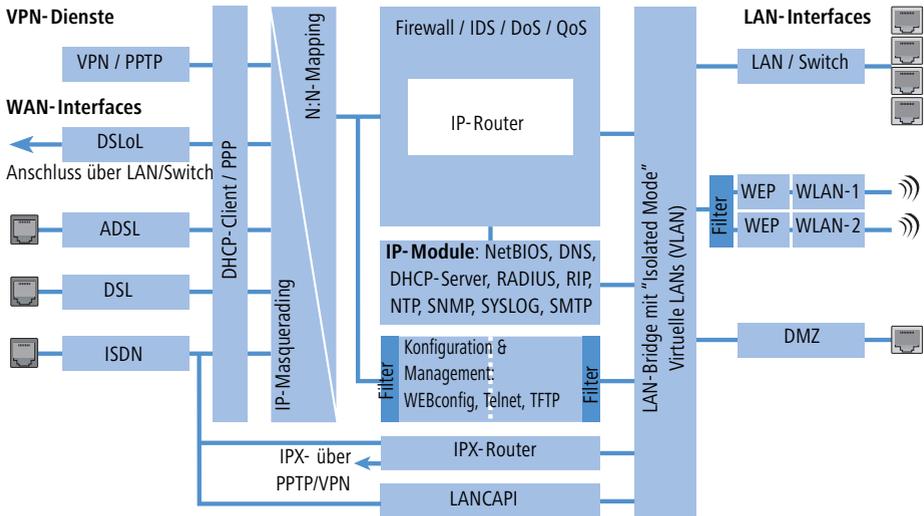
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

2 System-Design

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.
- 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.
- ▶ 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 ist hier jedoch **kein** Durchlauf durch die Firewall notwendig. 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.

▶ *Kapitel 2: System- Design*

- ▶ 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 Kommunikationszugängen) 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

Nicht bei allen
Geräte verfügbar

Nicht bei allen
Geräte verfügbar

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 Fernkonfiguration ist abhängig von einer ISDN-Verbindung.

Zum anderen die Anforderungen an zusätzliche Hard- und Software: Die Inband-Konfiguration benötigt einen der ohnehin vorhandenen Rechner im LAN, WAN oder WLAN und 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.
- **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 begrenzt 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
LANconfig	Ja	Ja	Ja
WEBconfig	Ja	Nein	Ja
SNMP	Ja	Nein	Ja
Terminalprogramm	Nein	Ja	Nein
Telnet	Ja	Nein	Nein
TFTP	Ja	Nein	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 Die Konfiguration mit verschiedenen Tools

3.3.1 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.

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.

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.



LANconfig					
Datei Bearbeiten Gerät Ansicht Extras ?					
	Name	Besch...	Adresse	Gerätestatus	Verlauf
LANconfig					
Intern	lc-e214-L54g		10.1.110.187	Ok	
Kunde_01	lc-e308-L54g		10.1.110.188	Ok	
Kunde_02	lc-e310-L54g		10.1.110.189	Ok	
	LC1621.Internet		10.1.80.125	Ok	
	Calvin		10.1.80.149	Ok	
	Hobbes		10.1.80.150	Ok	
	WLANsrv		10.1.80.245	Ok	
	Yueksel		10.1.82.100	Ok	
	1621AnnexB		10.1.140.159	Geöffneter Konfigurations Dialog	
	1621AnnexA		10.1.140.160	Ok	
	MUENCHEN		10.1.202.214	Ok	

Datum	Zeit	Name	Adresse	Meldung
16.01.2004	10:38:00	1621AnnexB	10.1.140.159	Konfiguration Bearbeiten gestartet
16.01.2004	10:38:00	1621AnnexB	10.1.140.159	Konfiguration Lesen gestartet
16.01.2004	10:38:01	1621AnnexB	10.1.140.159	Konfiguration Lesen erfolgreich
16.01.2004	10:38:06	1621AnnexB	10.1.140.159	Konfiguration Hochladen gestartet
16.01.2004	10:38:09	1621AnnexB	10.1.140.159	Konfiguration Hochladen erfolgreich

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.

▶ Kapitel 3: Konfiguration

- ▶ 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.

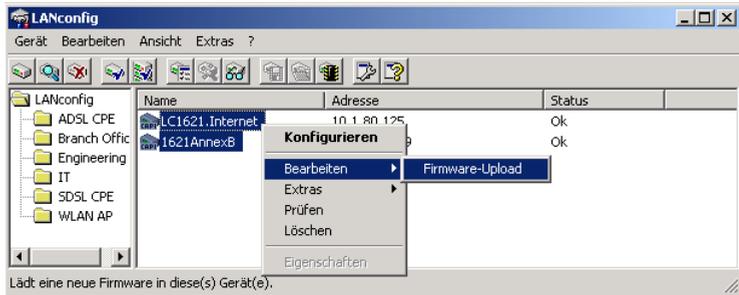
Verwaltung mehrerer Geräte gleichzeitig

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. Einzige Bedingung ist, dass es sich um Geräte gleichen Typs handelt.

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.



3.3.2 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.

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.

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

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.

3.3.3 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.

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 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:

Befehl	Beschreibung
cd <Verzeichnis>	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd .." etc.
del <Name> rm <Name>	Löscht den Tabelleneintrag mit dem Index <Name>
dir [<Verzeichnis>] list [<Verzeichnis>] ls [<Verzeichnis>] ll [<Verzeichnis>]	Zeigt den Inhalt des aktuellen Verzeichnisses an
do <Name> [<Parameter>]	Führt die Aktion <Name> im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
passwd	Ändern des Passworts
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
repeat <INTERVAL> <Kommando>	Wiederholt das Kommando alle INTERVAL Sekunden, bis der Vorgang durch neue Eingaben beendet wird
stop	Beendet den PING-Befehl

► Kapitel 3: Konfiguration

Befehl	Beschreibung
set <Name> <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.
set [<Name>] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
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.)
trace [...]	Konfiguration der Diagnose-Ausgaben. Siehe 'So starten Sie einen Trace' → Seite 50
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 (via TFTP)

- 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.

3.3.4 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 Datei-transfer 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'.

3.3.5 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

3.3.6 Fernkonfiguration über das DFÜ-Netzwerk



Der komplette Abschnitt zur Fernkonfiguration gilt nur für LANCOM mit ISDN-Schnittstelle.

Besonders einfach wird die Einstellung 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 WAN-Anschluss ohne eine einzige Einstellung sofort vom Administrator zu erreichen. Damit sparen Sie beim Anschluss von anderen Netzwerken an Ihr eigenes LAN viel Zeit und Geld für die Reise zum anderen Netzwerk oder für die Einweisung der Mitarbeiter vor Ort in die Konfiguration der Router.

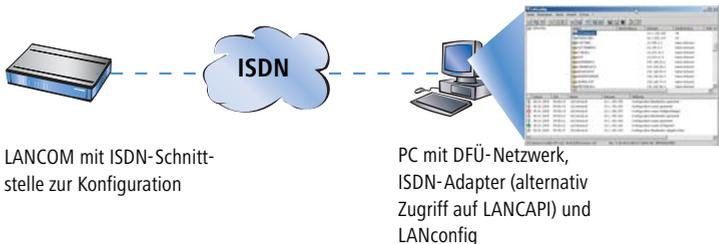
Außerdem können Sie eine spezielle Rufnummer für die Fernkonfiguration reservieren. Damit kann ein Service-Techniker immer auf den Router zugreifen, auch wenn das Gerät durch fehlerhafte Einstellungen eigentlich nicht mehr ansprechbar ist.

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 Anschlussstyp und geben Sie die Rufnummer des

WAN-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.

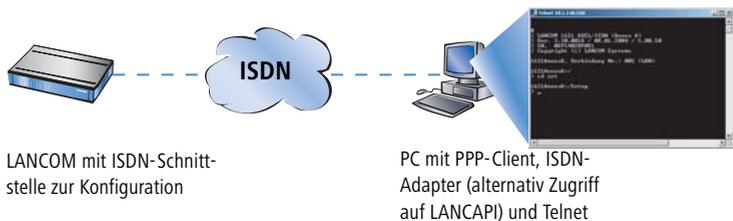
- ② LANconfig legt nun automatisch einen neuen Eintrag im DFÜ-Netzwerk an. Wählen Sie ein PPP-fähiges Gerät (z.B. den NDIS-WAN-Treiber aus dem Lieferumfang der LANCAPI) für die Verbindung aus, und bestätigen Sie mit **OK**.
- ③ Anschließend zeigt LANconfig in der Geräteliste ein neues Gerät mit dem Namen '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:



- ① Stellen Sie mit Ihrem PPP-Client eine Verbindung zum LANCOM her, verwenden Sie dabei folgende Angaben:

► Benutzername 'ADMIN'

► Kapitel 3: Konfiguration

- ▷ Passwort wie beim LANCOS eingestellt
 - ▷ eine IP-Adresse für die Verbindung, nur wenn erforderlich
- ② Starten Sie eine Telnet-Verbindung zum LANCOS. 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 LANCOS 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 LANCOS 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 LANCOS 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 Fernbetriebnahme

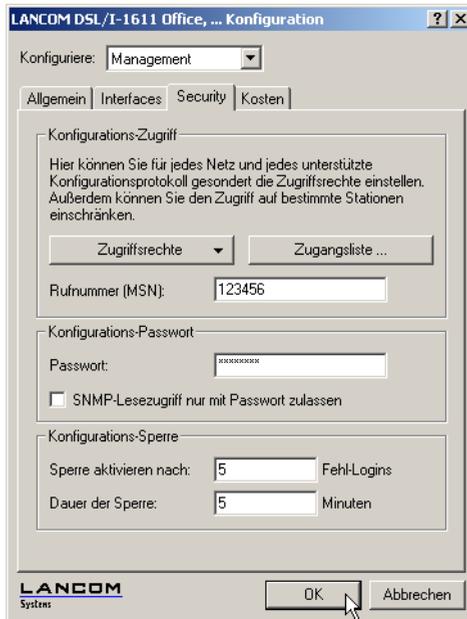
Die PPP-Verbindung von einer beliebigen ISDN-Gegenstelle zum Router gelingt natürlich nur dann, wenn das Gerät jeden Ruf mit den entsprechenden Einstellungen für den PPP-Betrieb annimmt. Im Auslieferungszustand geht das auch, da das Standard-Protokoll (Default-Layer) auf PPP eingestellt ist.

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 'Security'.



- ② Geben Sie als Rufnummer im Bereich 'Konfigurationszugriff' eine Rufnummer 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.

3.4 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. Sollte Ihr LANCOM (z. B. durch einen Defekt) seine Konfigurationsdaten verlieren, spielen Sie einfach die Sicherungskopie ein.

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	Bearbeiten ► Konfiguration als Datei sichern Bearbeiten ► Konfiguration aus Datei wiederherstellen Bearbeiten ► Neue Konfigurations-Datei Bearbeiten ► Konfigurations-Datei bearbeiten Bearbeiten ► Konfigurations-Datei drucken
WEBconfig	Konfiguration speichern ► Konfiguration laden (im Hauptmenü)
TFTP	<pre>tftp 10.0.0.1 get readconfig file1 tftp 10.0.0.1 put file1 writeconfig</pre>

3.5 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!

3.5.1 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.

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,

▶ Kapitel 3: Konfiguration

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 fünf Minuten lang auf einen erfolgreichen Login. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
 - ▷ Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.
- ▶ 'Manuell': Bei der dritten Möglichkeit können Sie vorher 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.



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.

3.5.2 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 **Bearbeiten ▶ Konfiguration 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

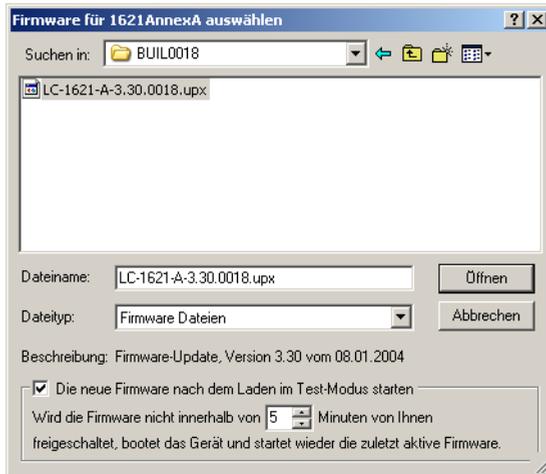


Beim LANconfig markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Gerät ▶ Firmware-Verwaltung ▶ Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende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

► Kapitel 3: Konfiguration

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** ► **Firmware im Test 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.

Mit dem Befehl '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) **writeflash** 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 writeflash
```

4 Netzwerk- Management mit den LANtools

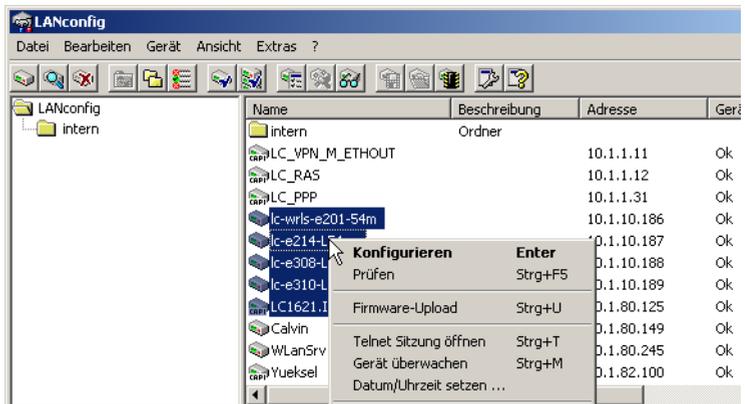
Die LANtools (bestehend aus LANconfig und LANmonitor) eignen sich hervorragend zum Konfigurieren und Überwachen von LANCOM-Geräten in komplexen Anwendungsszenarien. Mehrere Router und/oder Wireless Access Points können in einem Netzwerk können dabei genauso von einer zentralen Stelle aus administriert 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:



► Kapitel 4: Netzwerk- Management mit den LANtools

- 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

The screenshot shows the LANconfig software interface. The main window displays a list of devices with columns for Name, Adresse, Gerätestatus, and Verlauf. The 'Verlauf' column shows progress bars and upload statistics for each device. Below the main list, there is a log table with columns for Datum, Zeit, Name, Adresse, and Meldung.

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)
HOYERSWERDA	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



Der Firmware-Upload auf mehrere Geräte funktioniert nur, wenn es sich um gleiche Gerätetypen handelt!

- 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 249).

- ▶ 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:

- ▶ 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.

Datum	Zeit	Name	Adresse	Meldung
16.01.2004	10:38:00	1621AnnexB		startet
16.01.2004	10:38:00	1621AnnexB		st
16.01.2004	10:38:01	1621AnnexB		st
16.01.2004	10:38:06	1621AnnexB		startet
16.01.2004	10:38:09	1621AnnexB		erfolgreich



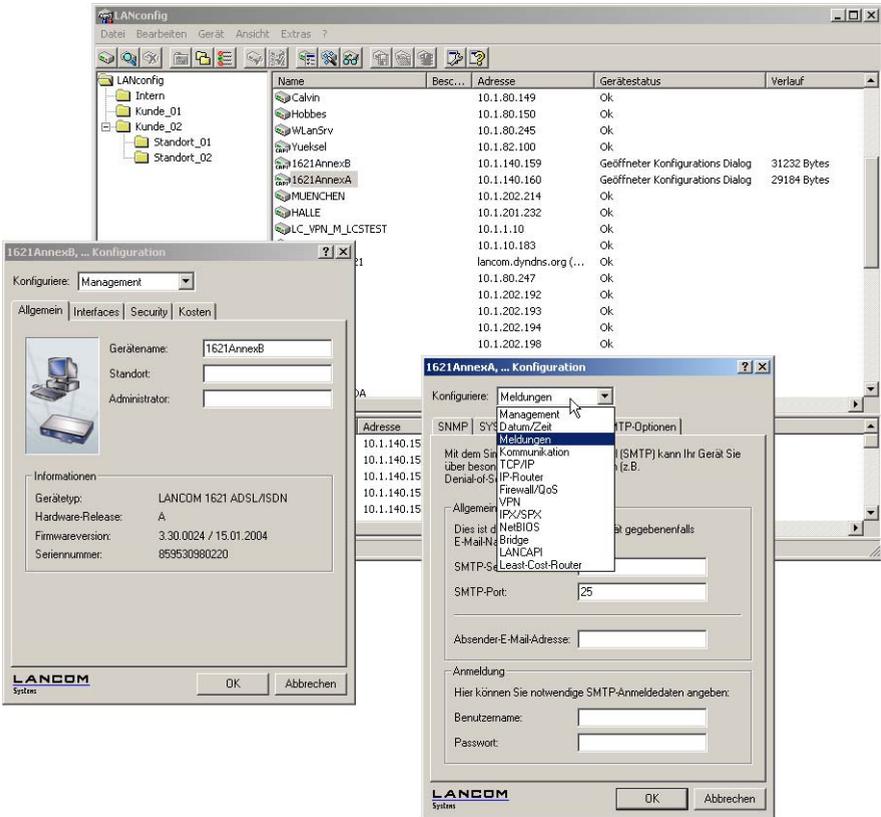
Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann mit der Funktionstaste **F6** oder über das Menü **Ansicht ► Verzeichnisbaum** ein- und ausgeschaltet werden.

4.1.2 Multithreading

Bei der Verwaltung von Projekten ist es oft hilfreich, die Konfigurationen von mehreren Geräten 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

► Kapitel 4: Netzwerk- Management mit den LANtools

Konfigurationen geöffnet werden. Alle Konfigurationen können parallel bearbeitet werden.

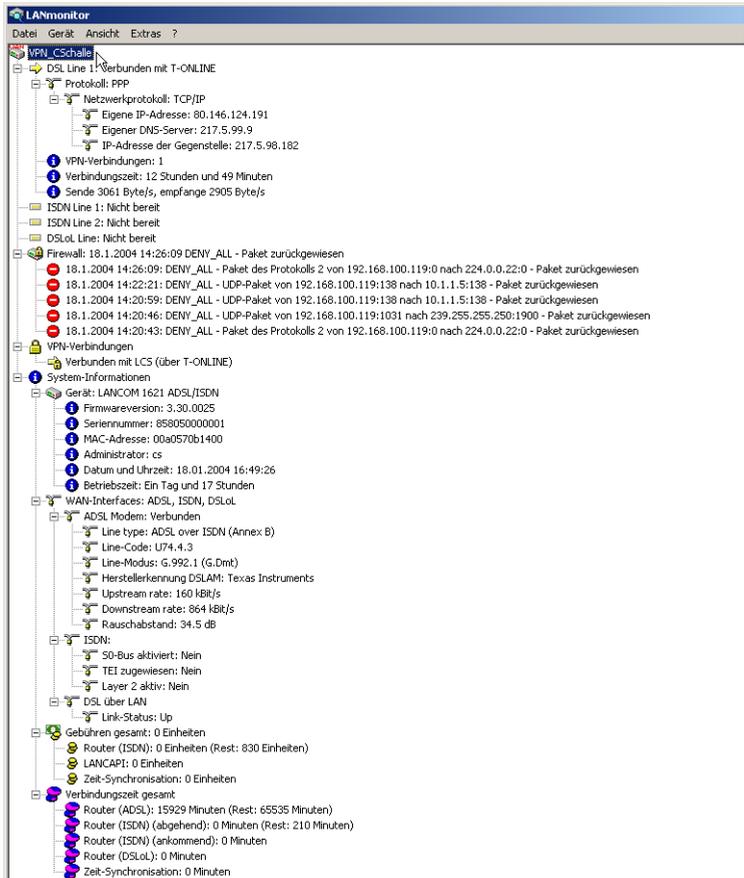


Zwischen den geöffneten Konfigurationen können Inhalte mit "Cut and Paste" über die Zwischenablage übertragen werden.

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.

4.2 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.

► Kapitel 4: Netzwerk- Management mit den LANtools

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

LC_VPN_M_LCSTEST - VPN-Verbindungen						
Verbindungen Ansicht						
Name	Status	Letzter Fehler	Haltezeit	Verbindung	Gateway	Verschlüsselun
VPN_AMAY	Nicht Verbunden	Leistungsüberwa...	0 Sekunden	INTERNET	217.228.41.56	BLOWFISH (12
VPN_CBUERSCH	Verbunden		0 Sekunden	INTERNET	80.142.186.239	BLOWFISH (12
VPN_CSCHALLE	Verbunden		0 Sekunden	INTERNET	80.146.98.22	AES (128 Bit)
VPN_DEICH	Verbunden		0 Sekunden	INTERNET	80.142.139.67	BLOWFISH (12
VPN_ETRABER	Verbunden		0 Sekunden	INTERNET	212.202.73.28	BLOWFISH (12
VPN_FJANSSEN	Verbunden		0 Sekunden	INTERNET	82.82.232.129	BLOWFISH (12
VPN_FTHEINEN	Verbunden		0 Sekunden	INTERNET	80.146.66.20	BLOWFISH (12
VPN_HBATTI	Verbunden		0 Sekunden	INTERNET	80.146.114.101	BLOWFISH (12
VPN_MBAGSIK	Verbunden		0 Sekunden	INTERNET	213.23.254.236	AES (128 Bit)
VPN_MBRIX	Verbunden		0 Sekunden	INTERNET	213.54.77.150	AES (128 Bit)
VPN_MPLUM	Verbunden		0 Sekunden	INTERNET	80.146.89.25	BLOWFISH (12
VPN_OSCHILPE	Verbunden		0 Sekunden	INTERNET	82.72.51.100	AES (128 Bit)
VPN_TNJO	Verbunden		0 Sekunden	INTERNET	217.82.205.102	BLOWFISH (12
VPN_WOHN	Verbunden		0 Sekunden	INTERNET	217.136.170.119	BLOWFISH (12
VPN_WTIW	Verbunden		0 Sekunden	INTERNET	217.80.153.52	BLOWFISH (12

- ▷ 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:

LC_VPN_M_LCSTEST - Accounting-Informationen						
Accounting Ansicht						
Benutzer	Gegenstelle	Typ	Verbindungen	Empfangen	Gesendet	Verbindungszeit: gesa
dual-p3	VPN_MPLUM	VPN-Verbindung	2	2.411 MB	32.090 MB	89 Tage und 8 Stund
wzk-prodtest-sv	VPN_HBATTI	VPN-Verbindung	0	3.989 MB	1.977 MB	88 Tage und 21 Stund
lc_vpn_m_ethout	VPN_WOHN	VPN-Verbindung	0	739.406 KB	2.541 MB	88 Tage und 18 Stund
ics-mail	VPN_WTIW	VPN-Verbindung	0	917.816 KB	799.849 KB	76 Tage und 21 Stund
ftheinen2	VPN_FTHEINEN	VPN-Verbindung	0	108.579 KB	159.375 KB	72 Tage und 23 Stund
lc_vpn_m_ethout	VPN_CSCHALLE	VPN-Verbindung	0	187.790 KB	448.049 KB	53 Tage und 18 Stund
10.1.1.1	VPN_WTIW	VPN-Verbindung	0	1.783 KB	1.553 KB	36 Tage und 5 Stund
ics-mail	VPN_FJANSSEN	VPN-Verbindung	0	464.767 KB	1.968 MB	36 Tage und 0 Stund
lc_vpn_m_ethout	VPN_WOHN	VPN-Verbindung	0	7.015 KB	231.069 KB	35 Tage und 19 Stund
10.1.80.172	VPN_FTHEINEN	VPN-Verbindung	0	11.010 KB	21.643 KB	34 Tage und 15 Stund
ics-data	VPN_MPLUM	VPN-Verbindung	0	7.768 KB	50.828 KB	33 Tage und 19 Stund
10.1.1.1	VPN_CSCHALLE	VPN-Verbindung	0	25.226 KB	21.042 KB	33 Tage und 14 Stund
cbuersch-g5	VPN_CBUERSCH	VPN-Verbindung	0	519.200 KB	49.536 KB	32 Tage und 21 Stund
10.1.80.173	VPN_HBATTI	VPN-Verbindung	0	959.701 KB	177.880 KB	32 Tage und 18 Stund
lc_vpn_m_ethout	VPN_WTIW	VPN-Verbindung	0	1.092 KB	45.516 KB	30 Tage und 20 Stund
deichel3	VPN_DEICH	VPN-Verbindung	0	771.258 KB	826.401 KB	30 Tage und 14 Stund
lc_vpn_m_ethout	VPN_CBUERSCH	VPN-Verbindung	2	4.946 KB	363.813 KB	27 Tage und 11 Stund
10.1.80.172	VPN_FTHEINEN	VPN-Verbindung	0	188 KB	30.061 KB	26 Tage und 9 Stund
lc_vpn_m_ethout	VPN_HBATTI	VPN-Verbindung	0	14.907 KB	546.058 KB	25 Tage und 4 Stund
Atul-n3	VPN_MPLUM	VPN-Verbindung	0	794.443 KB	799.600 KB	19 Tage und 2 Stund

► Kapitel 4: Netzwerk- Management mit den LANtools

- ▷ 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

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_FJANISSEN (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_FTHEIMEN (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_MBAGSIX (über INTERNET)
16.01.2004 10:44:16	VPN	Verbunden mit VPN_MBRUX (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_WCWN (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	Akt
1	1/16/2004 10:44:02	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Sofort	Pak
2	1/16/2004 10:41:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
3	1/16/2004 10:39:53	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
4	1/16/2004 10:38:49	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
5	1/16/2004 10:37:38	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
6	1/16/2004 10:33:52	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
7	1/16/2004 10:32:43	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
8	1/16/2004 10:28:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
9	1/16/2004 10:27:23	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
10	1/16/2004 10:25:11	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
11	1/16/2004 10:23:48	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
12	1/16/2004 10:16:25	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak
13	1/16/2004 10:14:50	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Sofort	Pak
14	1/16/2004 10:11:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Sofort	Pak

▶ Kapitel 4: Netzwerk- Management mit den LANtools

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

4.3 Scheduled Events

4.3.1 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 Einstellung in diesem Bereich Sinn machen. Außerhalb der Bürozeiten

▶ Kapitel 4: Netzwerk- Management mit den LANtools

oder 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.

► Kapitel 4: Netzwerk- Management mit den LANtools

4.3.2 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 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 249). 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 Monatstage 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

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.

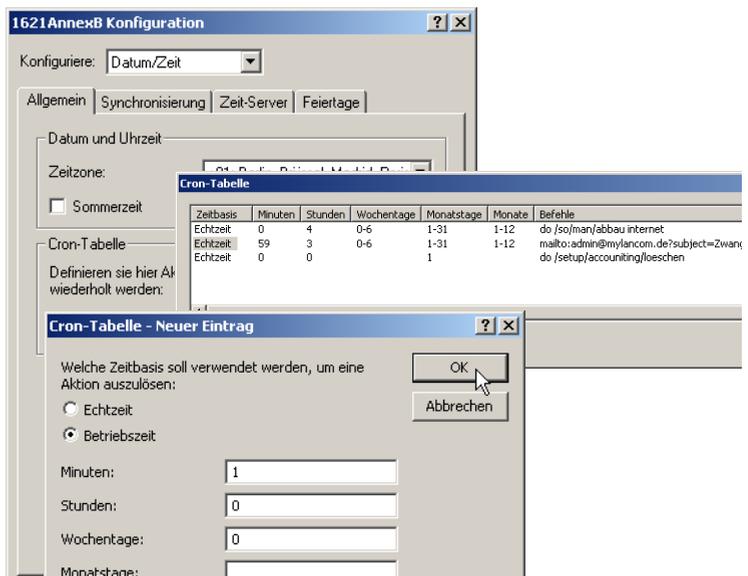
 Zeitgesteuerte Regeln werden mit einer Genauigkeit von einer Minute ausgeführt.

 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 20).

4.3.3 Konfiguration der Zeitautomatik

LANconfig

Unter LANconfig finden Sie die Cron-Tabelle im Konfigurationsbereich 'Datum/Zeit' auf der Registerkarte 'Allgemein':



The screenshot shows the LANconfig interface with the following details:

- 1621AnnexB Konfiguration** (Main Window):
 - Konfigurieren: Datum/Zeit
 - Registerkarte: Allgemein
 - Zeitzone: [Dropdown]
 - Sommerzeit
 - Cron-Tabelle: Definieren sie hier die Aktion, die wiederholt werden soll.
- Cron-Tabelle** (Table):

Zeitbasis	Minuten	Stunden	Wochentage	Monatstage	Monate	Befehle
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=Zwan
Echtzeit	0	0		1		do /setup/accounting/loeschen
- Cron-Tabelle - Neuer Eintrag** (Dialog):
 - Welche Zeitbasis soll verwendet werden, um eine Aktion auszulösen:
 - Echtzeit
 - Betriebszeit
 - Minuten:
 - Stunden:
 - Wochentage:
 - Monatstage:
 - Buttons: OK, Abbrechen

▶ Kapitel 4: Netzwerk- Management mit den LANtools

WEBconfig oder
Telnet

Unter WEBconfig oder Telnet finden Sie die Cron-Tabelle in folgenden Menüs:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Config-Modul ▶ Cron-Tabelle
Terminal/Telnet	/Setup/Config-Modul/Cron-Tabelle

5 Diagnose

5.1 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.

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

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.

5.1.1 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.

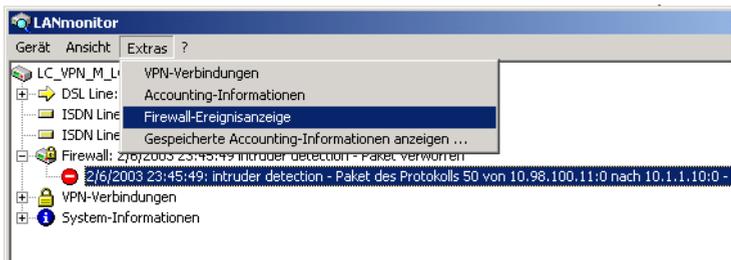
5.1.2 Internet-Verbindung kontrollieren

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.

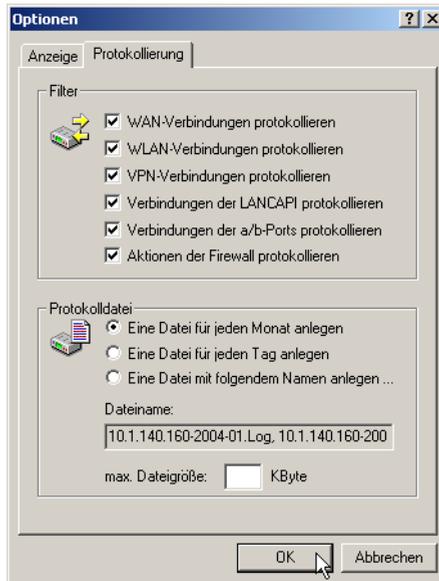
- ② LANmonitor legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle. Starten Sie Ihren Web-Browser, und geben Sie eine beliebige Webseite ein. LANmonitor zeigt nun an, wie auf einem Kanal eine Verbindung aufgebaut wird und welche Gegenstelle 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 einen entsprechenden Eintrag öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen 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 Konfigurationspasswort.
- 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
- ▷ LANCAP1-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.

5.2 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.

5.2.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie z.B. in einer Telnet-Sitzung. Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt. Und was steckt hinter Schlüssel und Parameter?

5.2.2 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 verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

5.2.3 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

Dieser Parameter ruft beim Trace die folgende Anzeige hervor:
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS-Verwaltung
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)
Connact	Meldungen aus dem Aktivitätsprotokoll ('Aktivitätsprotokoll' → Seite 41)

5.2.4 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.

5.2.5 Beispiele

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 ÖFF)
trace + all	schaltet alle Trace-Ausgaben ein
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

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 116
- ▷ 'IP-Masquerading' → Seite 79
- ▷ 'Virtuelle LANs (VLANs)' → Seite 207

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 für lokale Netz 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 '8"?'#-*+_.;:;!° 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

► Kapitel 6: Sicherheit

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.

Eingabe des Passwortes

Das Feld zur Eingabe des Passwortes finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. 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 ► Security ► 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 ► Security ► SNMP-Lesezugriff nur mit Passwort zulassen
WEBconfig	Experten-Konfiguration ► Setup ► SNMP-Modul ► Passw.Zwang-fuer-SNMP-Lesezugriff
Terminal/Telnet	Setup/SNMP-Modul/Passw.Zwang

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 ► Security
WEBconfig	Experten-Konfiguration ► Setup ► Config-Modul
Terminal/Telnet	Setup/Config-Modul

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-Aministrationszugang
- 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)

► Kapitel 6: Sicherheit

- 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

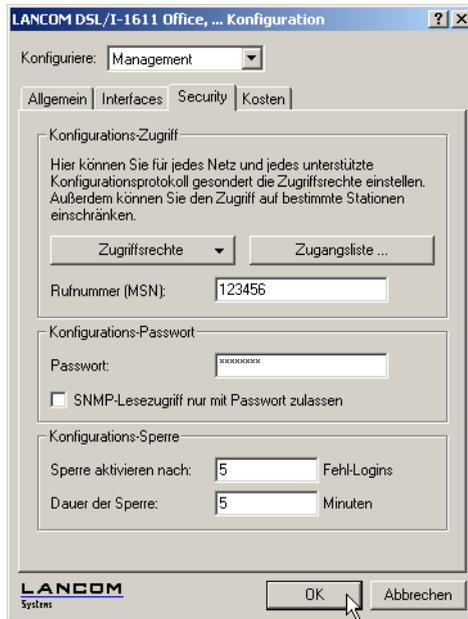
Nur für Modelle mit ISDN-Schnittstelle.

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 'Security'.



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

Geben Sie alternativ unter Telnet den folgenden Befehl ein:

```
set /setup/config-modul/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.

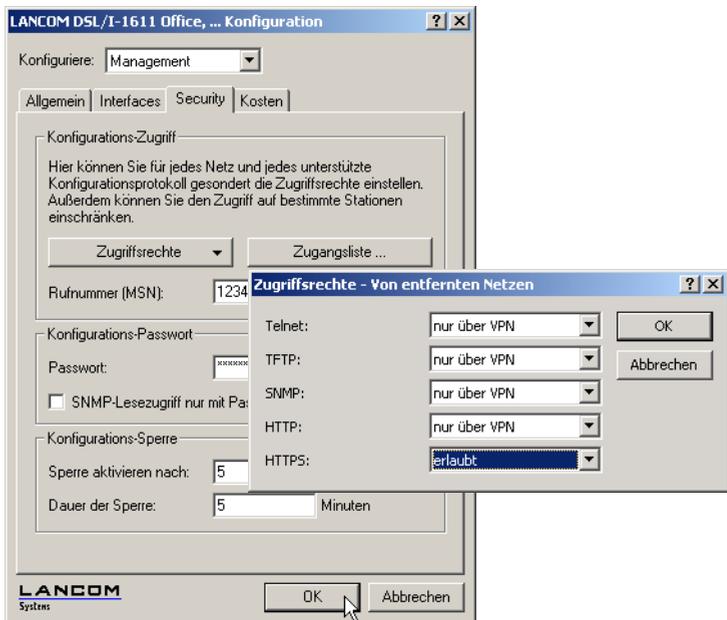
Den Netzwerk-Konfigurationszugriff einschränken

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

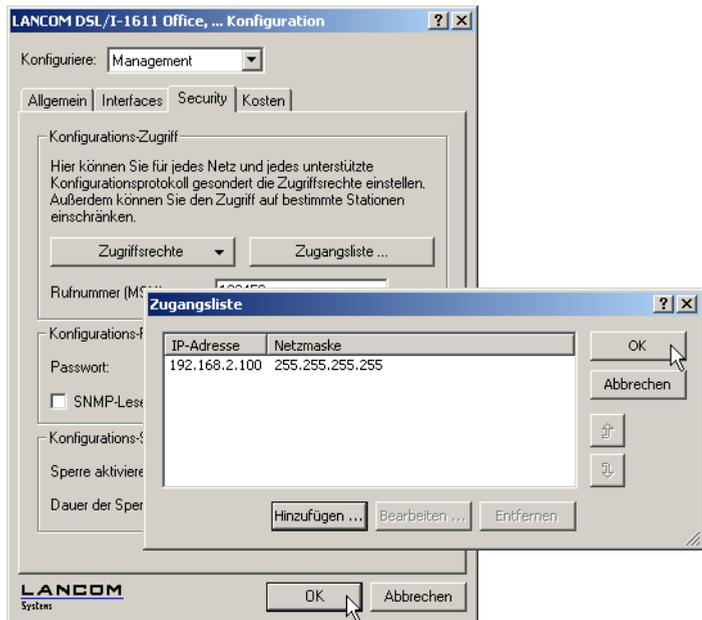
Unter WEBconfig oder Telnet erreichen Sie die Konfiguration der Zugangsliste über folgende Menüs:

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

DE

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 **Zugangsliste** geöffnet:



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

▶ Kapitel 6: Sicherheit

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 Telnet erreichen Sie die Konfiguration der Zugangsliste über folgende Menüs:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration ▶ Setup ▶ TCP-IP-Modul ▶ Zugangs-Liste
Terminal/Telnet	/Setup/TCP-IP-Modul/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
 - ▷ 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 "Identifier" zur Erkennung des Anrufers verwendet werden soll, wird im folgender Liste eingestellt:

Konfigurationstool	Aufruf
LANconfig	Kommunikation ▶ Rufannahme
WEBconfig	Experten-Konfiguration ▶ Setup ▶ WAN-Modul ▶ Schutz
Terminal/Telnet	/Setup/WAN-Modul/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-Modul ► PPP-Liste
Terminal/Telnet	/Setup/WAN-Modul/PPP-Liste

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 – 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. 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 Namenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

Konfigurationstool	Aufruf
LANconfig	Kommunikation ► Gegenstellen ► Namenliste
WEBconfig	Experten-Konfiguration ► Setup ► WAN-Modul ► Namenliste
Terminal/Telnet	/Setup/WAN-Modul/Namenliste

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 Namenliste 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).

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 108.

6.3 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 'Security'. 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 Konfigurationsbereich

▶ Kapitel 6: Sicherheit

'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 fin-

det sich unter 'Aufbau einer expliziten "Deny-All"-Strategie' → Seite 152.

► **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 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 mit WEP-Schlüsseln und einer ACL abgesichert?**

Mit Hilfe von WEP verschlüsseln Sie die Daten im Funknetzwerk mit Schlüsseln von bis zu 128 Bit Länge. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter WEP-Funktion mindestens 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.

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 neben IP auch IPX.

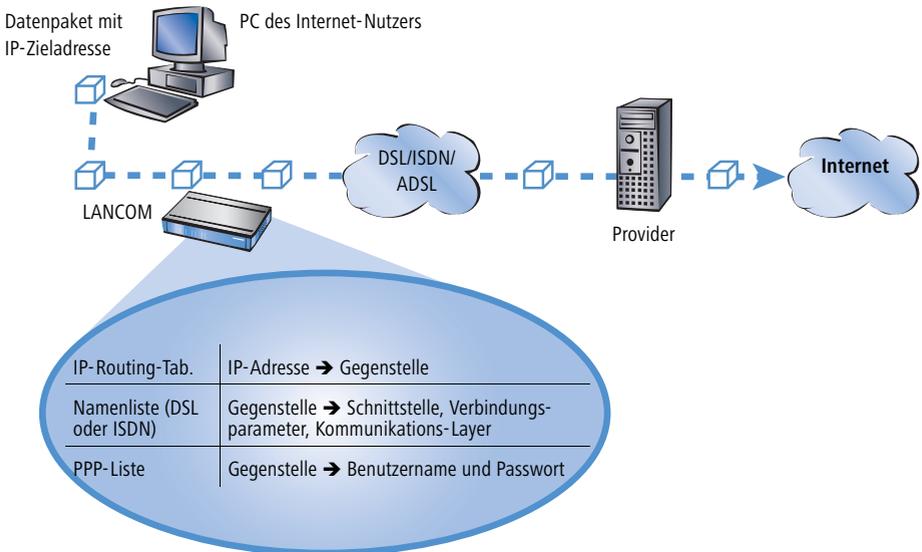
Die enge Zusammenarbeit mit den Router-Modulen

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 Namenliste und findet die notwendigen Verbindungsdaten für den Provider. Zu diesen Verbindungsdaten gehören z. B. die WAN-Schnittstelle (DSL, ISDN) über die der Provi-

der ausgewählt 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-Tabelle in einem Router von LANCOM 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

► Kapitel 7: Routing und WAN-Verbindungen

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-Modul ► IP-Routing-Tab.
Terminal/Telnet	cd /Setup/IP-Router/IP-Routing-Tab.

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	IP-Netzmaske	Gegenstellen-Name	Distanz	Maskierung
192.168.120.0	255.255.255.0	MAIN	2	Aus
192.168.125.0	255.255.255.0	NODE1	3	Aus
192.168.130.0	255.255.255.0	191.168.140.123	0	Aus

Was bedeuten die einzelnen Einträge in der Liste?

► IP-Adresse und IP-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.

► Router-Name

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.

► Kapitel 7: Routing und WAN-Verbindungen

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

Routen mit dem Gegenstellen-Namen '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 Gegenstellen-Name 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.

► 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 79.

7.2.2 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 Ziel-Netz 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-Modul ► Lok.-Routing
Terminal/Telnet	set /Setup/IP-Router/Lok.-Routing Ein

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.

7.2.3 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von LANCOM 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 LANCAPI).
 - ▷ 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.

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-Modul ► RIP-Einstellung
Terminal/Telnet	cd /Setup/IP-Router-Modul/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.

▶ Kapitel 7: Routing und WAN-Verbindungen

- ▶ 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.

7.2.4 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 Verbindungen 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 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-Modul ► Routing-Methode ► SYN/ACK-Speedup
Terminal/Telnet	<pre>cd /Setup/IP-Router-Modul/Routing-Methode set SYN/ACK-Speedup AUS</pre>

7.3 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.

7.3.1 Einfaches Masquerading

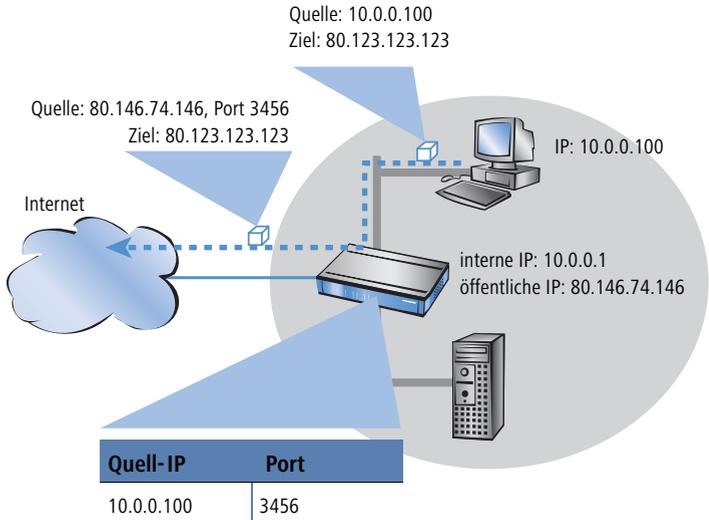
Damit nicht jeder Arbeitsplatzrechner im gesamten Internet bekannt sein muss: IP-Masquerading heißt das Versteck für alle Rechner im Intranet. Dabei wird nur das Routermodul des LANCOM mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt dabei Internet und Intranet.

Wie funktioniert IP-Masquerading?

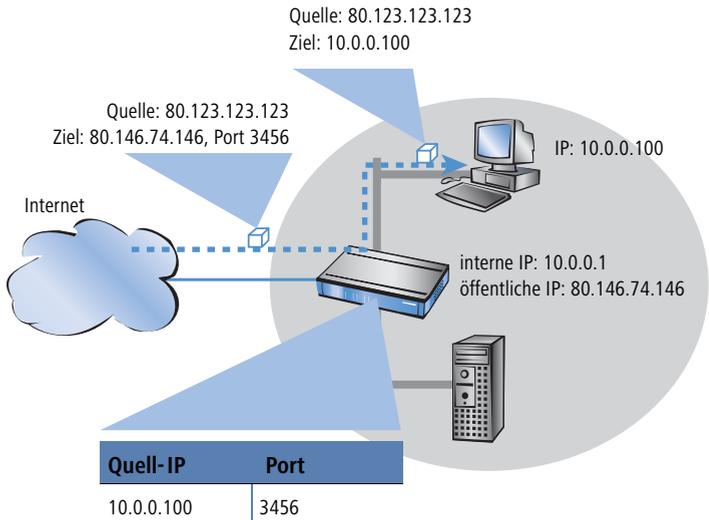
Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle.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

► Kapitel 7: Routing und WAN-Verbindungen

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

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-Modul ► IP-Routing-Tab
Terminal/Telnet	/Setup/IP-Router-Modul/IP-Routing-Tab

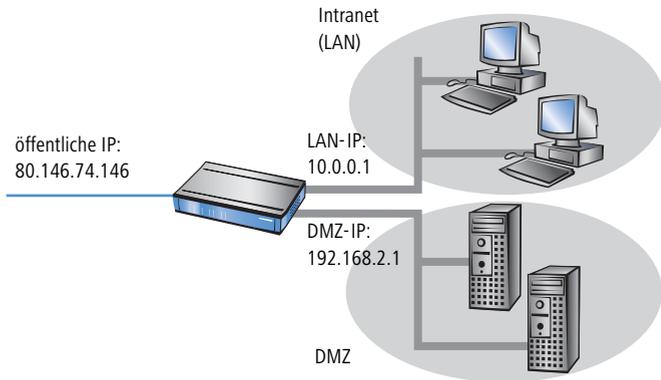
Mehrere Adressen für den Router

Bei 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 Adresse haben. Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her. Dazu wird die Internet-IP-Adresse bei den meisten Standard-Internetzugängen dem Router im Zuge der PPP-Verhandlung dynamisch zugewiesen.

Auf der lokalen Seite kann der Router zwei unterschiedliche IP-Adresskreise verwalten: Das Intranet (LAN) und die DMZ ('De-Militarized Zone'). Die DMZ

► Kapitel 7: Routing und WAN-Verbindungen

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--Modul
Terminal/Telnet	/Setup/TCP-IP-Modul

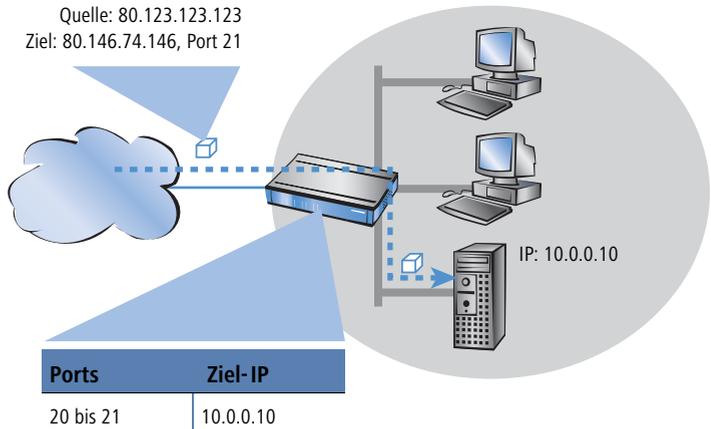
7.3.2 Inverses Masquerading

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

► Kapitel 7: Routing und WAN-Verbindungen

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.



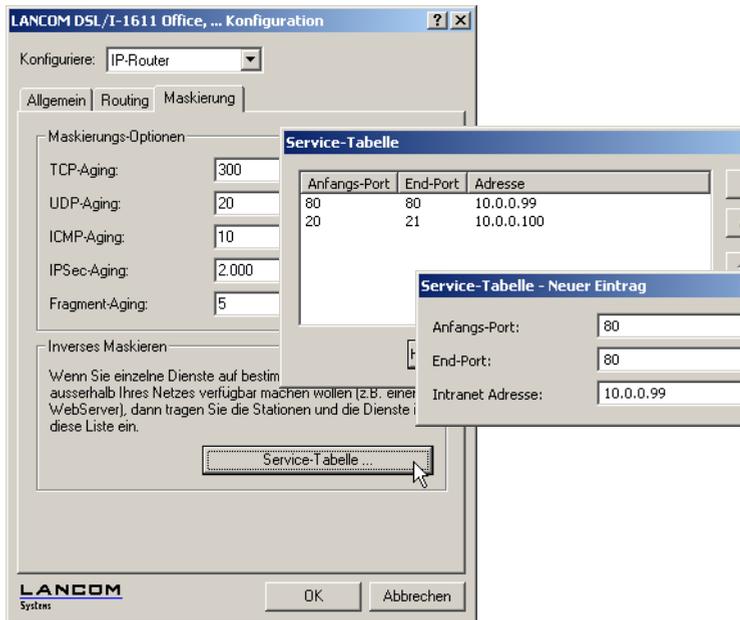
Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

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':



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-Modul ► Masquerading ► Service-Tabelle
Terminal/Telnet	/Setup/IP-Router-Modul/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 Fire-

wall, der den Zugriff aller Rechner auf den jeweiligen Server ermöglicht.

7.3.3 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-standardisierte, 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), oder können die LAN-Ports per Hardware auf Ethernet-Ebene voneinander trennen (LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN beim Betrieb des Switches im 'Private Mode').

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.

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

öffentliche DMZ IP-Adresse	Bedeutung/Verwendung
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 152): Zugriff von "Alle Stationen im lokalen Netz" auf "123.45.67.2" erlauben

7.4 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 79) 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

► Kapitel 7: Routing und WAN-Verbindungen

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 83).

Zur Kopplung von Netzwerken mit gleichen Adressräumen wird ein N:N-Mapping verwendet. Dieses setzt mehrere Adressen ("N") des lokalen Netzes eindeutig 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 werden 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.

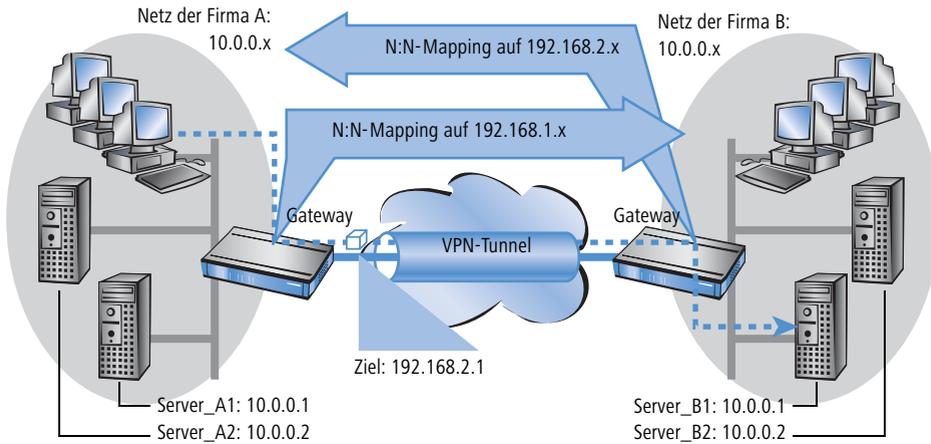
7.4.1 Anwendungsbeispiele

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:

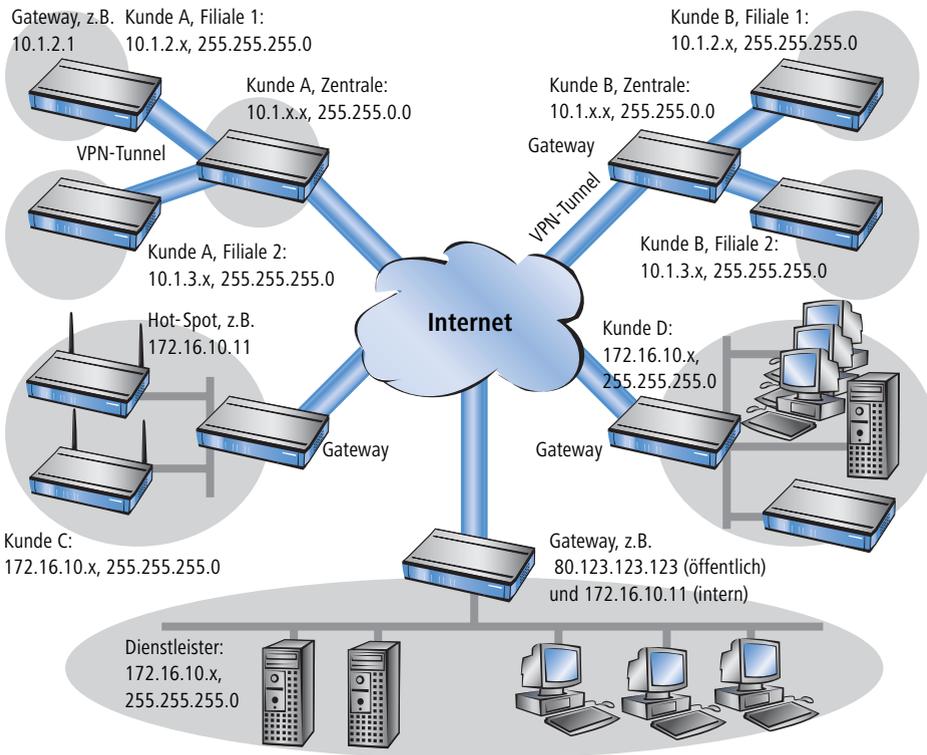


In diesem Beispiel stehen in den Netzen der Firmen A und B Server, die über einen VPN-Tunnel auf das jeweils andere Netz zugreifen wollen. Allen Stationen im LAN soll dabei der Zugang zu den Servern im remoten Netz erlaubt werden. Da beide Netze den gleichen Adresskreis nutzen, ist in dieser Konfiguration 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 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 260).

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:

- 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.

Loopback:
dezentrales
1:1-Mapping



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.

7.4.2 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, dass 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 134)!

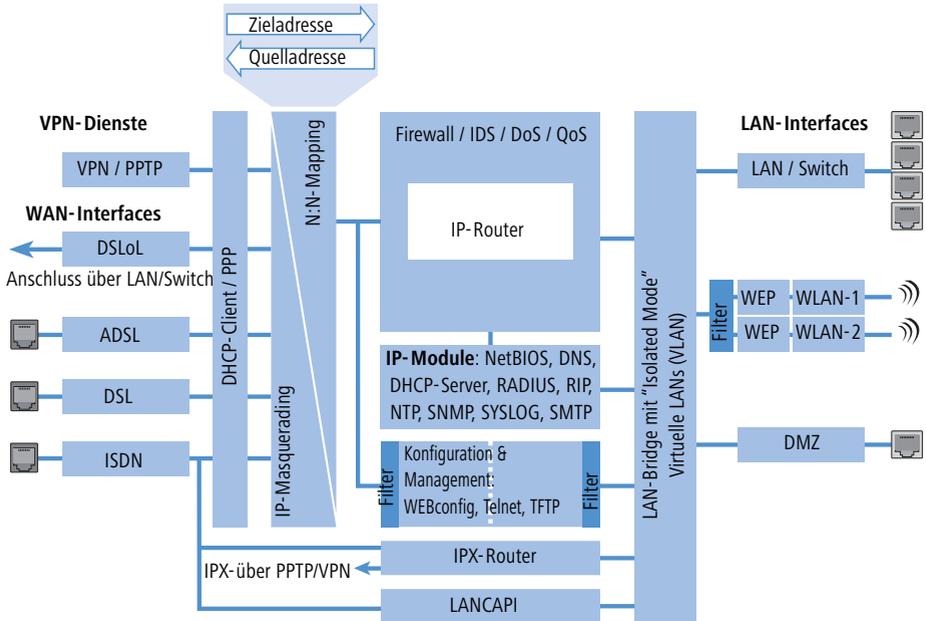
Zusätzliche Konfigurationshinweise

Mit dem Einrichten der Adressumleitung in der NAT-Tabelle werden die Netze und Rechner zunächst nur unter einer anderen Adresse im übergeordneten Netzwerk 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.
- ▶ 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 234).
- ▶ 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.



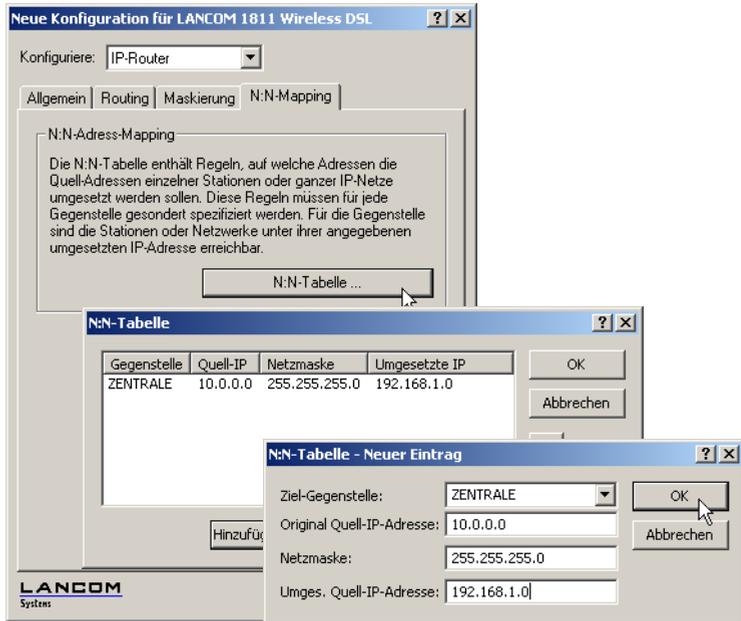
Die Umsetzung der IP-Adressen findet im LANCOM zwischen Firewall und IP-Router auf der einen Seite und dem VPN-Modul auf der anderen Seite statt. Alle Regeln, die sich auf das eigene lokale Netz beziehen, verwenden daher die "ungemappten", originalen Adressen. Die Einträge für das entfernte Netz nutzen 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:

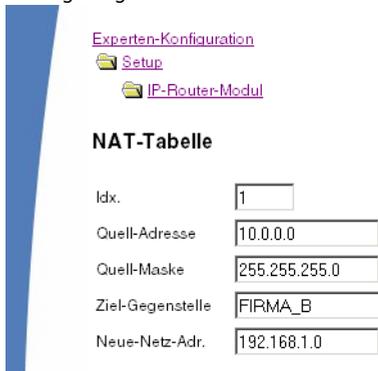


WEBconfig, Telnet

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-Modul / NAT-Tabelle

Die NAT-Tabelle präsentiert sich unter WEBconfig beim Anlegen eines neuen Eintrags folgendermaßen:



Experten-Konfiguration
 Setup
 IP-Router-Modul

NAT-Tabelle

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="FIR:MA_B"/>
Neue-Netz-Adr.	<input type="text" value="192.168.1.0"/>

7.5 Die Konfiguration von Gegenstellen

Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Namenliste (bzw. den Namenlisten) 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 100.

7.5.1 Namenliste

Die verfügbaren Gegenstellen werden in der Namenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt. Für jedes WAN-Interface

gibt es eine separate Namenliste. Die Namenlisten können auf folgenden Wegen aufgerufen werden:

Konfigurationstool	Menü/Tabelle
LANconfig	Kommunikation ► Gegenstellen ► Namenliste (DSL, ADSL bzw. ISDN)
WEBconfig	Experten-Konfiguration ► Setup ► WAN-Modul ► DSL-Namenliste bzw. ISDN-Namenliste oder ADSL-Namenliste
Terminal/Telnet	<pre>cd /Setup/WAN-Modul set DSL-Namenliste [...] set ISDN-Namenliste [...] set ADSL-Namenliste [...]</pre>

Für eine Gegenstelle sind folgende Parameter erforderlich:

Namenliste	Parameter	Bedeutung
DSL	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 Namenliste 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 107).
	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.

► Kapitel 7: Routing und WAN-Verbindungen

Namenliste	Parameter	Bedeutung
ADSL	Name	Wie in der DSL-Namenliste.
	Haltezeit	Wie in der DSL-Namenliste.
	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.
	Access Concentrator	Wie in der DSL-Namenliste.
	Service	Wie in der DSL-Namenliste.
	Layername	Wie in der DSL-Namenliste.
ISDN	Name	Wie in der DSL-Namenliste.
	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 Round-Robin-Liste eingetragen werden.
	Haltezeit	Wie in der DSL-Namenliste.
	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 DSL-Namenliste.
	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 108.



Bitte beachten Sie bei der Bearbeitung der Namenlisten folgende Hinweise:

- ▷ Werden in zwei Namenslisten (z.B. DSL-Namenliste und ISDN-Namenliste) 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 DSL-Namenliste 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 je nach Modell in einer gemischten ADSL/DSLoL-Namenliste oder in einer separaten Namenliste vorgenommen.

7.5.2 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-Modul ► Layer-Liste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set Layer-Liste [...]</code>

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 Namenlisten 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 'Kanalbündelung mit MLPPP' → Seite 112.	
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)	

7.6 Verbindungsaufbau mit PPP

Router von LANCOM 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.

7.6.1 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.
- ▶ Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- ▶ Bündelung von mehreren ISDN-Kanälen (Multilink PPP)

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)

▶ Kapitel 7: Routing und WAN-Verbindungen

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 Passworte 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

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.

7.6.2 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 High-speed-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.

7.6.3 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.

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.

7.6.4 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-Modul ► PPP-Liste
Terminal/Telnet	cd /Setup/WAN-Modul set PPP-Liste [...]

► Kapitel 7: Routing und WAN-Verbindungen

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 Gerätename 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!

7.7 DSL-Verbindungsaufbau mit PPTP

Einige DSL-Anbieter ermöglichen die Einwahl nicht über PPPoE, sondern über PPTP (**P**oint-**t**o-**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-Modul ► PPTP-Liste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set PPTP-Liste [...]</code>

Die PPTP-Konfiguration besteht aus drei Parametern:

- 'Gegenstelle' – Die Bezeichnung aus der DSL-Namensliste.
- '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.

7.8 Dauerverbindung für Flatrates – Keep-alive

Als Flatrates bezeichnet man pauschale Verbindungstarife, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue

► Kapitel 7: Routing und WAN-Verbindungen

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.

Konfiguration des Keep-alive-Verfahrens

Das Keep-alive-Verfahren wird in der Namensliste 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').

7.9 Rückruf-Funktionen

LANCOM mit ISDN-Schnittstelle unterstützen einen automatischen Rückruf.

Neben dem Rückruf über den D-Kanal wird auch das von Microsoft spezifizierte CBCP (Callback Control Protocol) sowie der Rückruf über PPP nach RFC 1570 (PPP LCP Extensions) angeboten. Zusätzlich besteht die Möglichkeit eines besonders schnellen Rückrufs über ein von LANCOM entwickeltes Verfahren. PCs mit Windows-Betriebssystem können nur über das CBCP zurückgerufen werden.

7.9.1 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 Namenliste ausgewählt.

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 Namenliste 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 Namenliste muss **eine** Rufnummer angegeben sein.

► Kapitel 7: Routing und WAN-Verbindungen

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-Version informieren den Benutzer nur darüber, dass der PC auf den Rückruf vom LANCOM wartet.



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.

7.9.2 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 Namenliste 'Den Rückruf der Gegenstelle erwarten' ein ('Looser' bei Konfiguration über WEBconfig, Terminalprogramm oder Telnet).
- Der Rückrufer wählt 'Die Gegenstelle zurückrufen (schnelles Verfahren)' in der Namenliste 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.

7.9.3 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.

7.9.4 Konfiguration der Rückruf-Funktion im Überblick

In der Namenliste 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.

► Kapitel 7: Routing und WAN-Verbindungen

Mit diesem Eintrag stellen Sie den Rückruf so ein:
'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' 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-Routern.



Bei Windows-Gegenstellen **muss** die Einstellung 'Name' gewählt werden.

7.10 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.

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 Pro-

vider, die bei Ihren Einwahlknoten ebenfalls MLPPP-fähige Gegenstellen betreiben.

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-Adapttern unter Windows-Betriebssystemen unterstützt.

► Kapitel 7: Routing und WAN-Verbindungen

- ▷ **buendeln** verwendet zwei B-Kanäle für eine Verbindung.
- ▷ **bnd+cmpr** nutzt beides (Komprimierung und Kanalbündelung) und stellt damit die maximal mögliche Übertragungsleistung zur Verfügung.

② Erstellen Sie nun einen neuen Eintrag in der Namenliste. Achten Sie dabei auf die Haltezeiten für die Verbindung. Beachten Sie folgende Regeln:

- ▷ 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-Modul ► Router-Interface-Liste
Terminal/Telnet	<code>cd /Setup/WAN-Modul</code> <code>set Router-Interface-Liste [...]</code>

- ▷ 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 LANCAP1 möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

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 Referenz-Handbuchs 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.

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.
- 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 Einbruchsversuchen: Intrusion Detection' → Seite 174 und 'Schutz vor "Denial-of-Service"-Angriffen' → Seite 176.

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.

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:

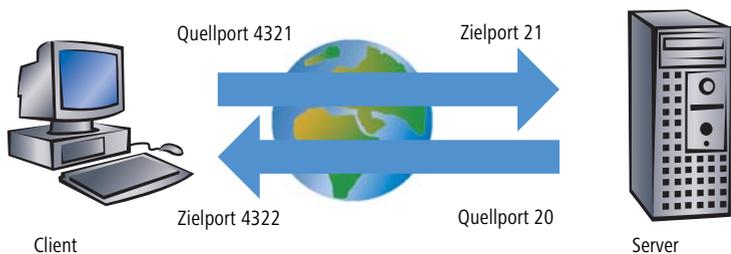
- IP-Adresse von Quelle und Ziel
- Übertragungsprotokoll (TCP, UDP oder ICMP)
- Portnummern von Quelle und Ziel
- MAC-Adresse

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 entgegenspricht.

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 (SPF) 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.

DE

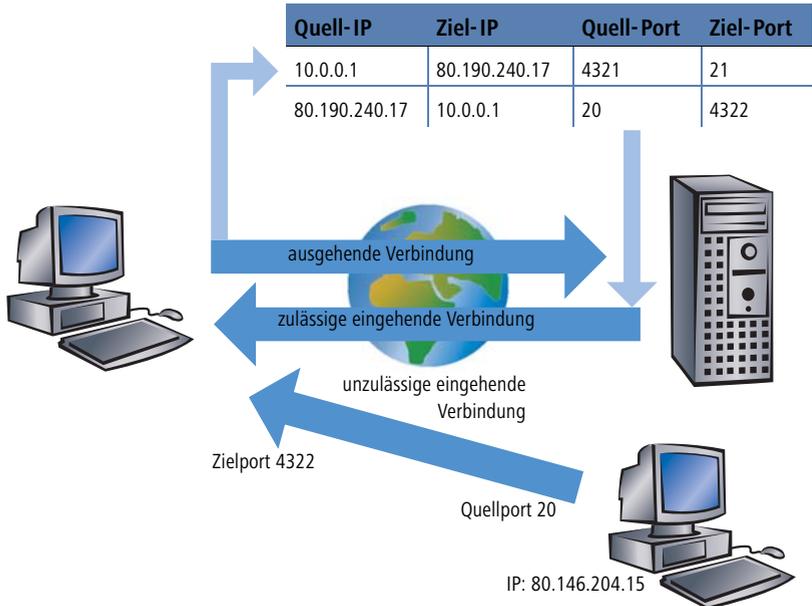
Stateful Inspection: richtungsabhängige Prüfung

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 Gegenstelle 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 Zieladresse sowie die jeweiligen Ports ein. Gleichzeitig kann die Stateful Inspec-

tion 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.

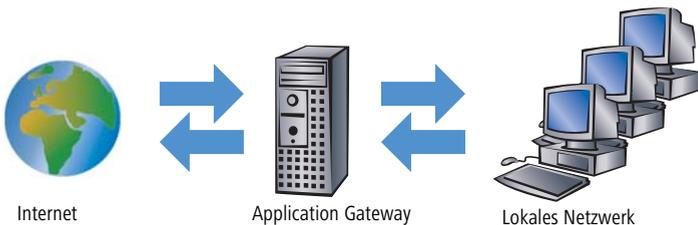
Eine Firewall mit Stateful-Inspection ist zudem meistens in der Lage, die empfangenen Datenpakete zu re-assemblieren, also einzelne Bestandteile zwischenzuspeichern und wieder zu einem gesamten Paket zusammenzubauen.

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 er 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.

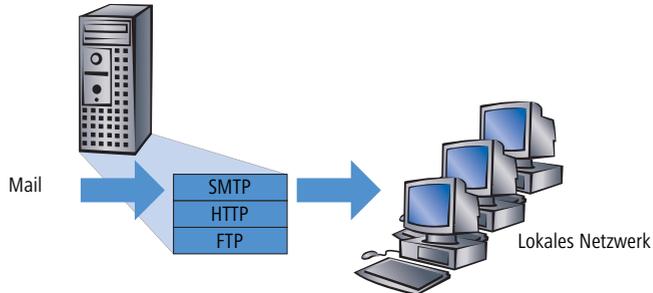
Application Gateway

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.



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.

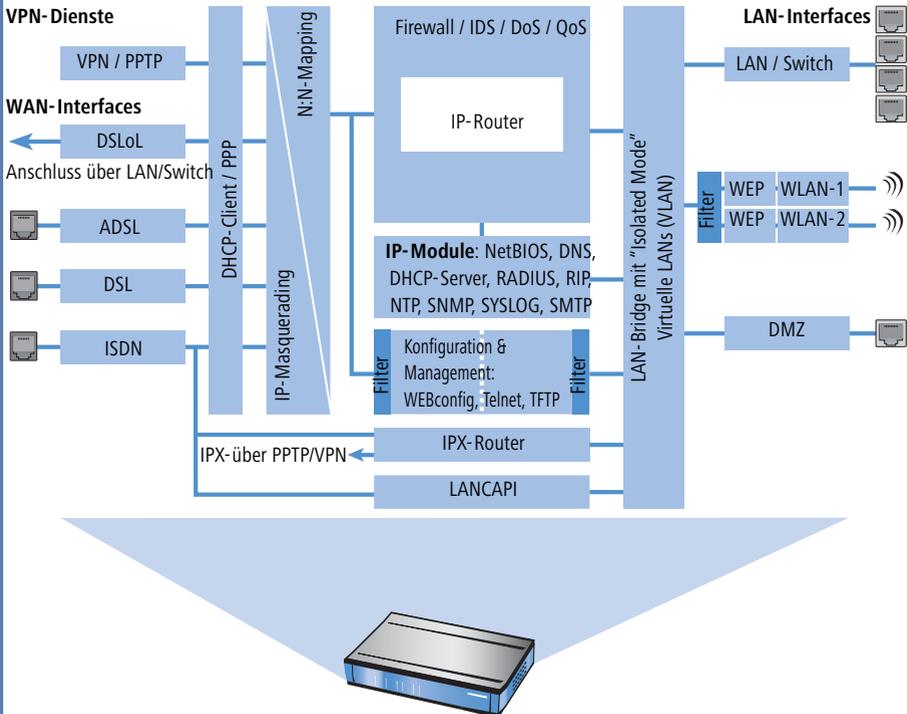
8.3 Die Firewall im LANCOM

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 prüft nur geroutete Datenpakete!



Die Firewall prüft nur die Datenpakete, die vom IP-Router im LANCOM geroutet werden. In der Regel sind das die Datenpakete, die zwischen den internen Netzwerken (LAN, WLAN, DMZ) und der "Außenwelt" über eines der WAN-Interfaces ausgetauscht werden.

Die Kommunikation z.B. zwischen LAN und WLAN untereinander wird normalerweise nicht über den Router abgewickelt, sofern die LAN-Bridge den direkten Austausch erlaubt. Hier wirken also auch nicht die Regeln der Firewall. Gleiches gilt für die so genannten "internen Dienste" des LANCOM wie Telnet, TFTP, SNMP und den Webserver für die Konfiguration über WEBconfig. Die Datenpakete dieser Dienste laufen nicht über den Router und werden daher auch nicht durch die Firewall beeinflusst.



Durch die Positionierung hinter dem Masquerading-Modul (aus Sicht des WANs) arbeitet die Firewall dabei mit den "echten" internen IP-Adressen der LAN-Stationen, nicht mit der nach außen bekannten Internetadresse des LANCOM.

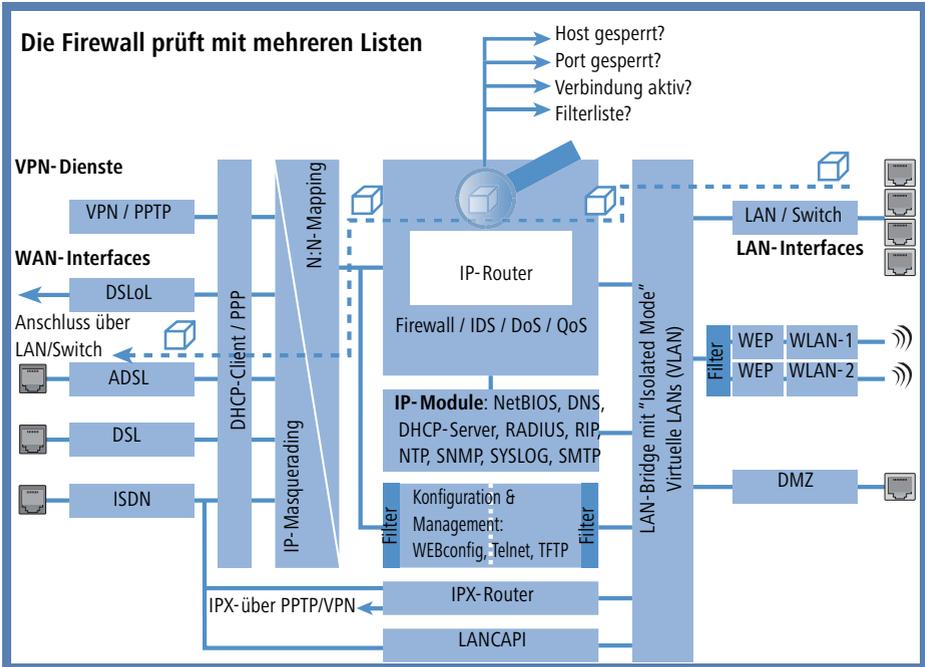
Die Firewall im LANCOM verwendet für die Prüfung der Datenpakete mehrere Listen, die aus den Firewall-Regeln, den daraus ausgelösten Firewall-Aktionen oder den aktiven Datenverbindungen automatisch erzeugt werden:

- ▶ 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 152.

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.

- ▶ 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 138).

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 121).

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:

Port Client	Verbindung	Port Server
12345	Request →	53
12345	Response ←	53

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.

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
- ▶ Default-VPN-Regeln (→ Seite 134)
- ▶ Administrator-E-Mail (→ Seite 135)
- ▶ Fragmente (→ Seite 135)
- ▶ Sitzungswiederherstellung (→ Seite 135)
- ▶ Ping-Block (→ Seite 136)
- ▶ Stealth-Modus (→ Seite 137)
- ▶ Authentifizierungs-Port tarnen (→ Seite 137)

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 87) nur wirksam sind, wenn die Firewall eingeschaltet ist!

Default-VPN-Regeln

Eine VPN-Regel besteht - neben einigen VPN-spezifischen Informationen - u.a. aus der Definition von Quell- und Ziel-Netzwerken. Die Informationen über Quelle und Ziel können prinzipiell aus der IP-Routingtabelle, den TCP/IP-Einstellungen (Intranetadressen und DMZ-Adressen) oder den Firewall-Regeln kommen.

Wie bei den Regeln für gesicherte Dienstgütern (Quality-of-Service) werden auch für die VPN-Verbindungen die vorhandenen Funktionen der Firewall genutzt, um die Datenpakete z.B. nach Subnetzen zu klassifizieren. Die Firewall ist damit eine zentrale Quelle für die VPN-Regeln. Ob weitere Quellen für die VPN-Regeln verwendet werden, kann in der Firewall eingestellt werden. Die entsprechende Option kann folgende Werte annehmen:

- ▶ **Default-VPN-Regeln automatisch erzeugen:** Mit dieser Einstellung werden alle verfügbaren Quellen für die Erzeugung der VPN-Regeln her-

angezogen, also IP-Routingtabelle, TCP/IP-Einstellungen und Firewall-Regeln.

- ▶ **Default-VPN-Regeln von Hand definieren:** Mit dieser Einstellung werden nur die manuell angelegten Firewall-Regeln als Basis für die VPN-Regeln verwendet.



Detaillierte Informationen über VPN-Regeln entnehmen Sie bitte der entsprechenden VPN-Dokumentation.

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) automa-

tisch 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:

- **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 137).

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. Dar-

auffin 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 155.

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 139)
- **Verknüpfung:** Sollen weitere Firewall-Regeln beachtet werden, wenn diese Regel für ein Datenpaket zutrifft? (→ Seite 139)
- **VPN-Regel:** Wird die Firewall-Regel auch zur Erzeugung von VPN-Regeln verwendet? (→ Seite 140)

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 165 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 das 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 134 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.



Detaillierte Informationen über VPN-Regeln entnehmen Sie bitte der entsprechenden VPN-Dokumentation.

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 142)
- **Bedingung:** Ist die Wirksamkeit der Regel durch Bedingungen eingeschränkt? (→ Seite 143)
- **Limit (Trigger):** Beim Erreichen welcher Schwellwerte soll die Regel anspringen? (→ Seite 144)

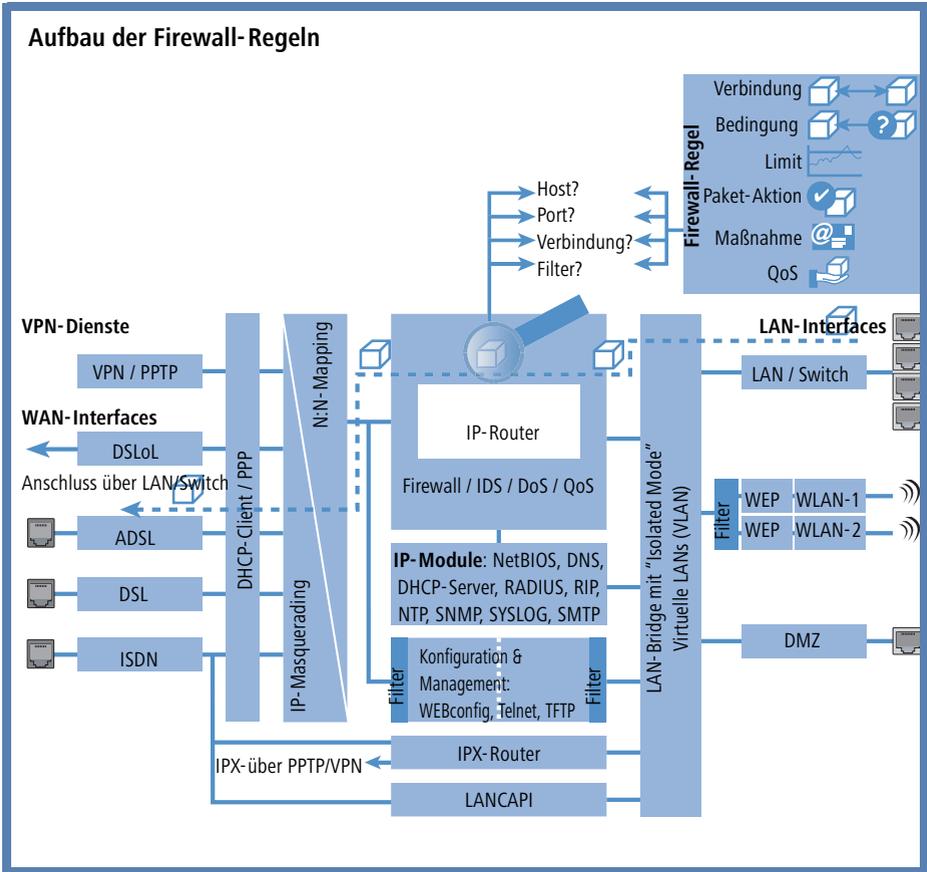
- ▶ **Paket-Aktion:** Was soll mit den Datenpaketen passieren, wenn die Bedingung erfüllt und das Limit erreicht sind? (→ Seite 144)
- ▶ **Sonstige Maßnahmen:** Sollen neben der Paket-Aktion noch weitere Maßnahmen eingeleitet werden? (→ Seite 144)
- ▶ **Quality of Service (QoS):** Werden Datenpakete bestimmter Anwendungen oder mit entsprechenden Markierungen durch die Zusicherung von speziellen Dienstgütern besonders bevorzugt? (→ Seite 145)



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 127 wurde bereits dargestellt, dass die Listen zur Prüfung der Datenpakete letzt-

lich aus den Firewall-Regeln gebildet werden. Die Erweiterung der Grafik stellt sich damit wie folgt dar:



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 Namensliste)
- ▶ 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

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 eingespeichert. 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.



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 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-Ereignisstabelle.

- ▶ **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 183.

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

▶ Kapitel 8: Firewall

- ▶ 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 SNMP SYSLOG
WEBconfig	Experten-Konfiguration Setup SMTP SNMP-Modul SYSLOG-Modul
Terminal/Telnet	/Setup/SMTP bzw. SNMP-Modul oder SYSLOG-Modul

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 247) 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.

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:

```

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

```

Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde (siehe auch 'SNMP' → Seite 23), 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.

► Kapitel 8: Firewall

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.

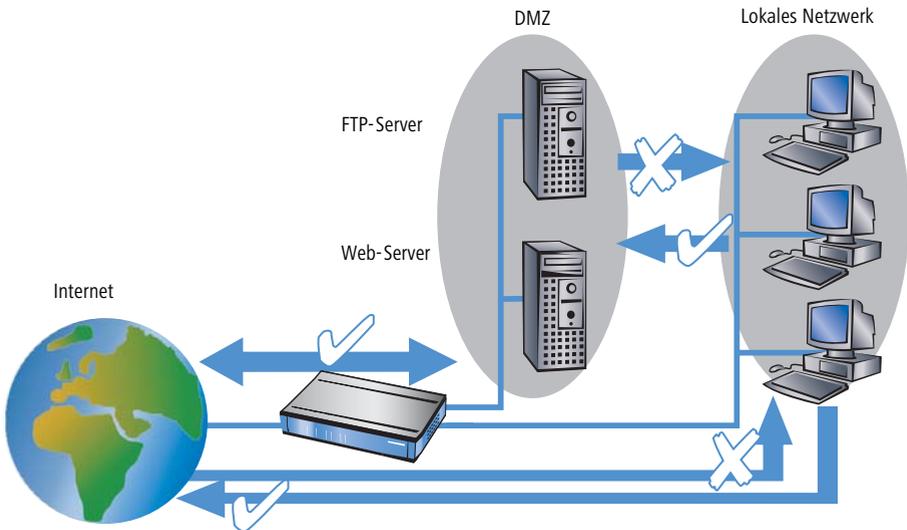
Dieser Ansatz ist für die Sicherheit des LANs besser als die Allow-All-Strategie, führt aber in der Anfangsphase oft zu Schwierigkeiten mit den Benutzern. Einige Dinge laufen eben nach Einschalten der Deny-All-Firewall vielleicht nicht mehr so wie vorher, bestimmte Rechner können ggf. nicht mehr erreicht 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 Rechner positioniert, auf die aus dem unsicheren Netz (Internet) direkt zugegriffen werden soll. Dazu gehören z.B. die eigenen FTP- und Web-Server.

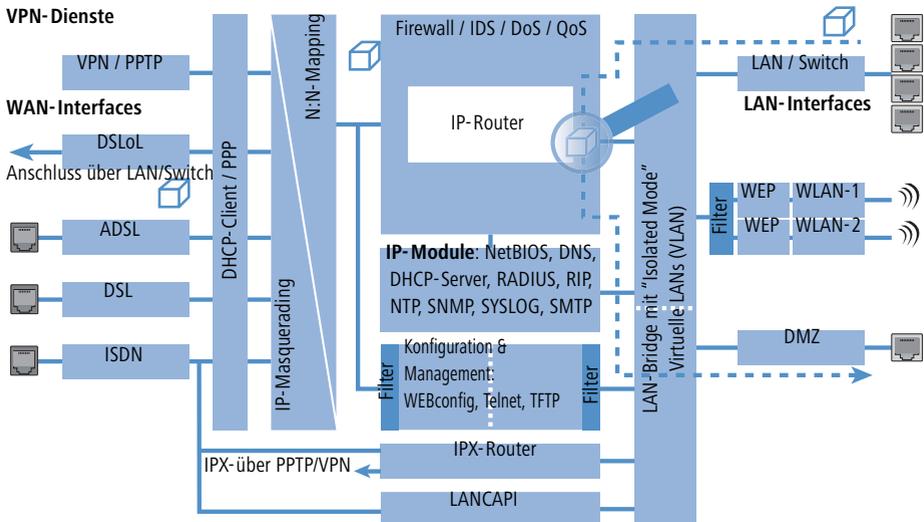
Die Firewall schützt dabei zunächst die DMZ gegen Angriffe aus dem Internet. Zusätzlich schützt die Firewall aber auch das LAN gegen die DMZ. Die Firewall wird dazu so konfiguriert, dass nur folgende Zugriffe möglich sind:

- ▶ 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 "gehackter" 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 herauszufinden, 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.



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 79), 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

▶ Kapitel 8: Firewall

- ▶ 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 96):

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.

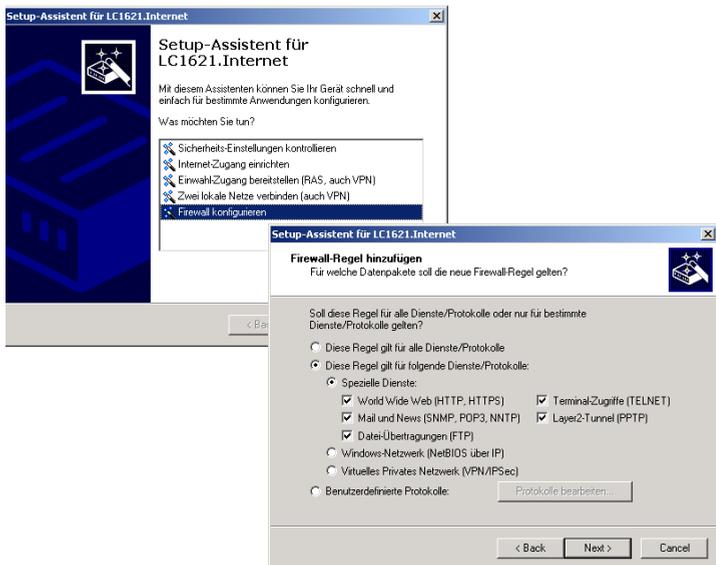


Das LANCOM nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemein (z.B. Deny-All). 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:

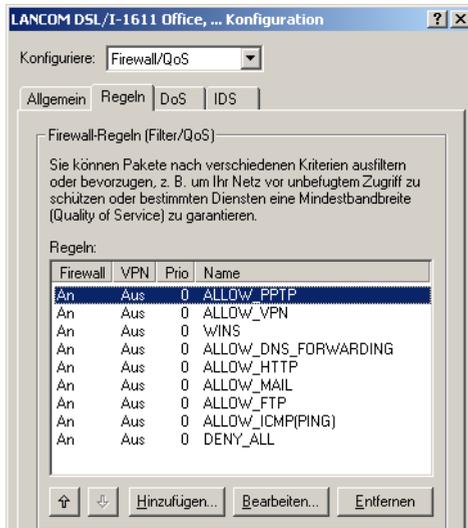


LANconfig

Die Einrichtung der Filter mit Hilfe von LANconfig ist besonders komfortabel. Im Konfigurationsbereich 'Firewall/QoS' befinden sich auf der Registerkarte

► Kapitel 8: Firewall

'Regeln' die Möglichkeiten zum Bearbeiten und Hinzufügen der Firewall-Regeln.



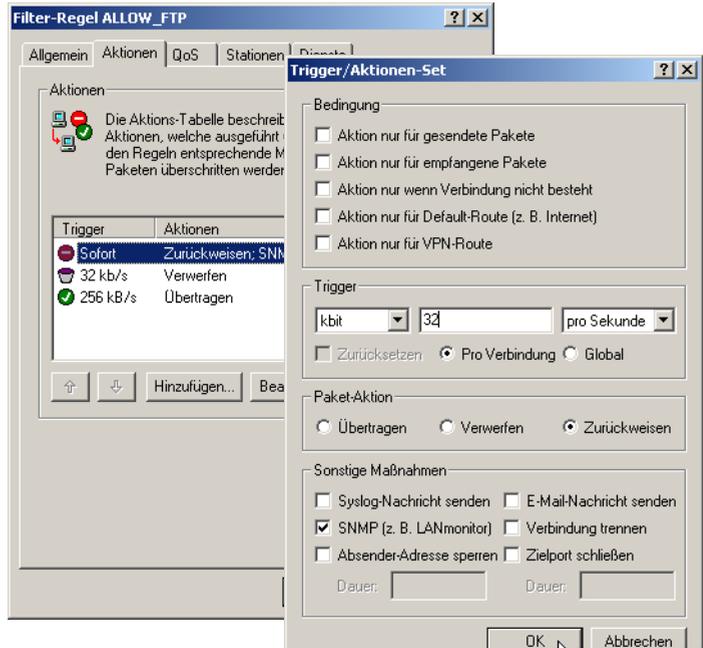
Im Dialog zur Definition der Filterregeln findet man auf den verschiedenen Registerkarten folgende Optionen:

- **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 139)

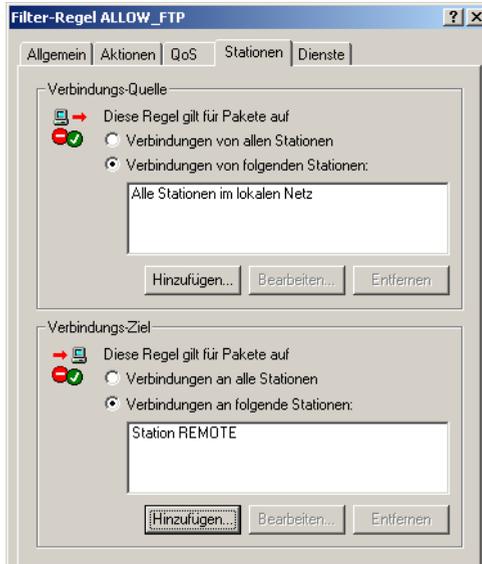
- ▷ Mit der Option 'Diese Regel für die Erzeugung von VPN-Regeln heranziehen' können die Informationen über Quell- und Zielnetzwerke dieser Regel auch für die Bildung von VPN-Netzwerken verwendet werden ('Default-VPN-Regeln' → Seite 134).
- **Aktionen:** Hier legen Sie die Firewall-Aktion fest, bestehend 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 200).



- **Stationen:** Hier werden die Stationen – als Absender oder Adressat der Pakete – festgelegt, für die die Filterregel gelten soll.



- **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-Modul / Firewall: Regel-Tabelle, Objekt-Tabelle, Aktions-Tabelle
Terminal/Telnet	/Setup/IP-Router-Modul/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 Datenpaketen 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 Objekttable 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-/Ausshalter, 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 138.

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekt-Tabelle für Protokolle, Dienste, Stationen (→ Seite 160) und der Aktions-Tabelle für die Firewall-Aktionen (→ Seite 161) bestehen als auch direkte

Beschreibungen in der entsprechenden LCOS-Syntax enthalten (z.B. %P6 für TCP).

[Experten-Konfiguration](#)
 [Setup](#)
 [IP-Router-Modul](#)
 [Firewall](#)

Regel-Tabelle

Name	ALLOW_HTTP
Prot.	<input type="text" value="TCP"/>
Quelle	<input type="text" value="LOCALNET"/>
Ziel	<input type="text" value="ANYHOST %S80,443,591,8008,8080"/>
Aktion	<input type="text" value="%Lcnds0 %A"/>
verknuepft	<input type="text" value="nein"/>
Prio	<input type="text" value="0"/>
Activ	<input type="text" value="ja"/>
VPN-Regel	<input type="text" value="nein"/>



Bei der direkten Eingabe der Regel-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 Objekttablelle 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-Namenliste stehen
Hostname	%D	Hinweis zu Hostnamen beachten (→ Seite 143)
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.



Experten-Konfiguration
 Setup
 IP-Router-Modul
 Firewall

Objekt-Tabelle

Name:

Beschreibung:

 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:

► Kapitel 8: Firewall

► 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 198)	@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

Limit	Beschreibung	Objekt-ID
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
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

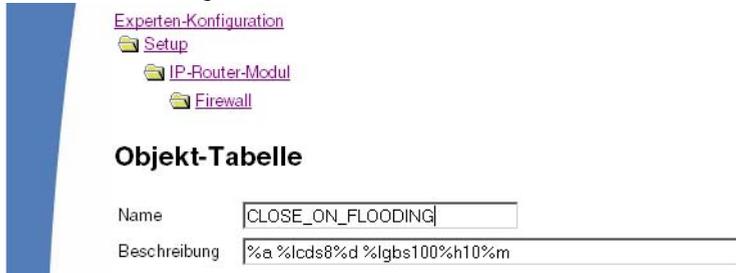
Maßnahmen	Beschreibung	Objekt-ID
Syslog	Gibt eine detaillierte Meldung über Syslog aus	%s
Mail	Schickt eine E-Mail an den Administrator	%m
SNMP	Sendet einen SNMP-Trap	%n
Close-Port	Schließt den Zielport des Pakets für eine einstellbare Zeit	%p
Deny-Host	Sperrt die Absender-Adresse des Pakets für eine 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

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:



Experten-Konfiguration
 Setup
 IP-Router-Modul
 Firewall

Objekt-Tabelle

Name	CLOSE_ON_FLOODING
Beschreibung	%a %lcds8%d %lgbst100%h10%m

- 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 (%lgbst100), 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.

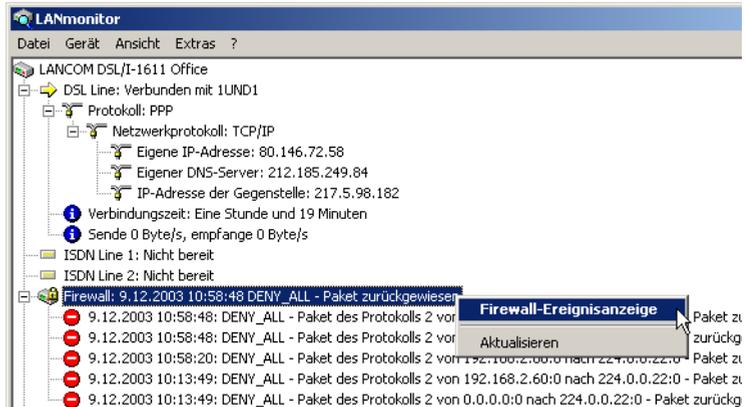
Beim Aufbau der eigentlichen Filter-Tabelle werden die Aktionsobjekte dann genau so wie Protokoll-, Adress- und Dienstobjekte auf die kleinste notwendige Anzahl reduziert, d.h. Mehrfachdefinitionen einer Aktion werden eliminiert und bei widersprüchlichen Aktionen wird die "sicherste" ausgewählt. So wird 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.

► Kapitel 8: Firewall

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 166).

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:

LANCOM DSL/I-1611 Office - Firewall-Ereignisanzeige									
Ereignisanzeige Ansicht									
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 zurückgewie:
2	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
3	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
4	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
5	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
6	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
7	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
8	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
9	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
10	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:
11	8.12.2003 20:16:55	192.168.2.60	224.0.0.22	2 (IGMP)	0	0	DENY_ALL	Sofort	Paket zurückgewie:

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
0001	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022
0002	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022
0003	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022
0004	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022
0005	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022
0006	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022
0007	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022
0008	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022

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

Element	Bedeutung
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)
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 auflistet. Es sind zur Zeit folgende Werte definiert: 0x00000001 Accept 0x00000100 Reject 0x00000200 Aufbaufilter 0x00000400 Internet- (Defaultrouter-) 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 50). 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:

```

Telnet 192.168.2.100
#
! LANGCOM DSL/I-1611 Office
! Ver. 3.30.0003 / 12.11.2003
! SN. 000590300080
! Copyright (c)

Verbindung Nr.: 002 (LAN)
Passwort:
:/
> show filter

Filter 0001 from Rule ALLOW_PPTP:
  Protocol: 107
  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 s
  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 s
  actions after exceeding the limit:
  accept

```

Unter WEBconfig hat die Filterliste den folgenden Aufbau:

[Experten-Konfiguration](#)

 [Status](#)

 [IP-Router-Statistik](#)

Filter-Liste

Idx.	Prot.	Quelle-MAC	Quelle-Adresse	Quelle-Netz-Maske	Q-von	Q-bis	Ziel-MAC	Ziel-Adresse	Ziel-Netz-M
0001	187	000000000000	0.0.0.0	0.0.0.0	0	0	000000000000	0.0.0.0	0.0.0.0
0002	108	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0003	51	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0004	50	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0005	17	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0
0006	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0
0007	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	192.168.2.100	255.255.25
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

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
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</code> anzeigen
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-R
 192.168.2.60	212.227.15.133	6	3584	110	8	00020038	ALLOW_MAIL	1	UND
 192.168.2.60	212.227.15.133	6	3586	110	9	00020038	ALLOW_MAIL	1	UND
 192.168.2.60	212.227.15.133	6	3588	110	300	00020008	ALLOW_MAIL	1	UND
 192.168.2.60	217.72.195.42	6	3577	80	25	00020001	ALLOW_HTTP	1	UND

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 172). 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
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 halbdyna-

mische 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.

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, Entwick-

lungsinformationen 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 176): Es werden auch hier die "halboffenen" Verbindungen gezählt, wobei ein TCP-

Reset, das vom gescannten Rechner gesendet wird, die "halboffene" Verbindung weiterhin offen lässt.

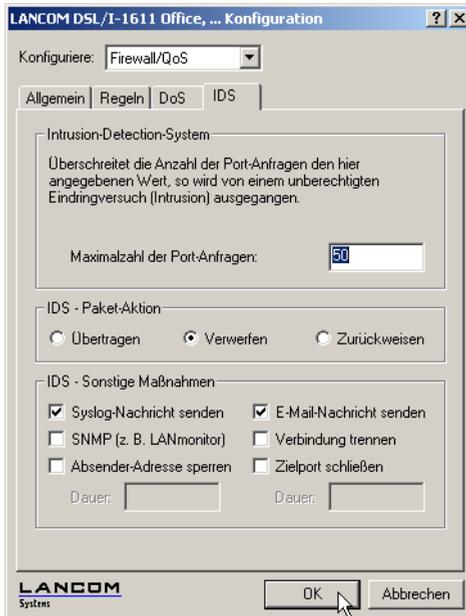
Wenn eine bestimmte Anzahl von halboffenen Verbindungen zwischen dem gescannten und dem scannenden Rechner existiert, so wird dies als Portscan gemeldet.

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

► Kapitel 8: Firewall

WEBconfig, Telnet

Die Verhaltensweise des Intrusion Detection Systems wird unter WEBconfig oder Telnet hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router-Modul/Firewall
Terminal/Telnet	Setup/IP-Router-Modul/Firewall

DE

8.5 Schutz vor "Denial-of-Service"-Angriffen

Angriffe aus dem Internet können neben Einbruchsversuchen 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 Implementationen von TCP/IP-Protokollstacks aus. Zu den Angriffen, die prinzipiellen Schwächen ausnutzen, gehören z.B. SYN-Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementationen 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 ersten 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. 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 Absender-Adresse 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 reassembliert 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.

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.

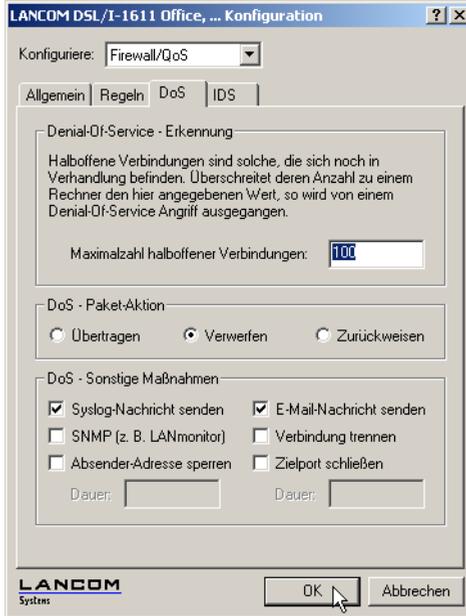


In der Default-Einstellung sind alle Einstellungen auf "sicher" konfiguriert, d.h. maximal 100 zulässige halboffene Verbindungen von verschiedenen Rechnern (vgl. SYN-Flooding), maximal 50 halboffene Verbindungen von einem Rechner (vgl. Portscan) fragmentierte Pakete werden re-assembliert.

8.5.2 Konfiguration der DoS-Abwehr

LANconfig

Die Parameter gegen die DoS-Attacks werden im LANconfig im Konfigurationsbereich 'Firewall/QoS' auf der Registerkarte 'DoS' festgelegt:



Um die Anfälligkeit des Netzes vor DoS-Attacks 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

WEBconfig, Telnet

Die Verhaltensweise der DoS-Erkennung und -Abwehr wird unter WEBconfig oder Telnet hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router-Modul/Firewall
Terminal/Telnet	Setup/IP-Router-Modul/Firewall

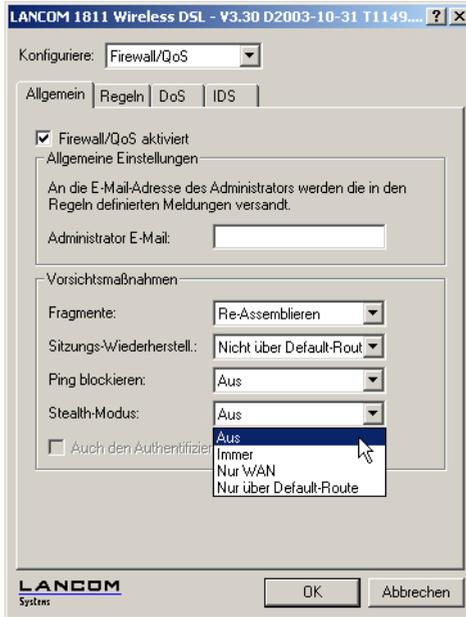
Immer aktiv hingegen sind folgende Schutzmechanismen:

- ▶ 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 'Firewall/QoS' auf der Registerkarte 'Allgemein' festgelegt:



WEBconfig, Telnet

Unter WEBconfig oder Telnet wird das Unterdrücken der Antworten hier konfiguriert:

Konfigurationstool	Aufruf
WEBconfig	Experten-Konfiguration: Setup/IP-Router-Modul/Firewall
Terminal/Telnet	Setup/IP-Router-Modul/Firewall

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 Senderate 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 verschiedenen 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

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.
CS0 (BE)	000000	0
CS1	001000	8
CS2	010000	16
CS3	011000	24
CS4	100000	32
CS5	101000	40
CS6	110000	48
CS7	111000	56

Code-point	DSCP Bits	Dez.
AF11	001010	10
AF12	001100	12
AF13	001110	14
AF21	010010	18
AF22	010100	20
AF23	010110	22
AF31	011010	26
AF32	011100	28

Code-point	DSCP Bits	Dez.
AF33	011110	30
AF41	100010	34
AF42	100100	36
AF43	100110	38
EF	101110	46

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 sicherzustellen, 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 78)

► Urgent Queue II

▶ Kapitel 9: Quality-of-Service

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 zuge teilten 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:

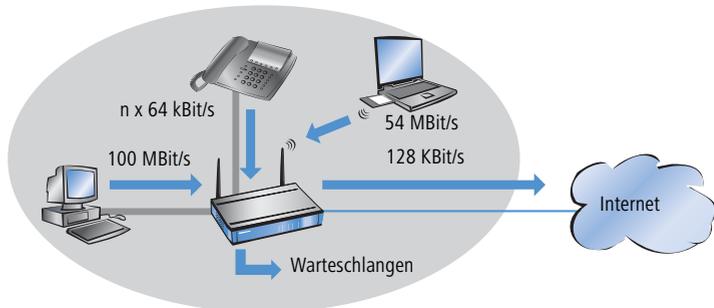
- ▷ Pakete mit ToS "High Reliability"
- ▷ Pakete mit DiffServ "Assured Forwarding"

▶ 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.

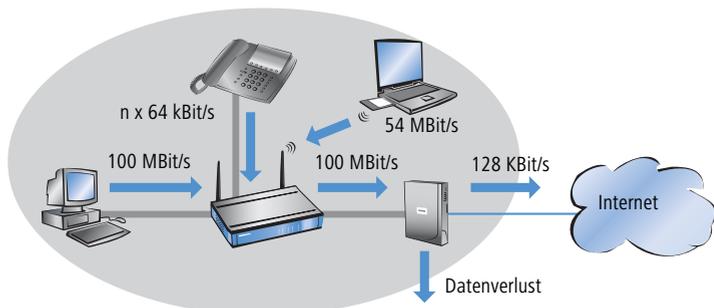
Das Konzept der Warteschlangen funktioniert natürlich nur, wenn sich an der Schnittstelle vom LAN zum WAN ein "Stau" von Datenpaketen bildet. Dieser Stau bildet sich dann, wenn das Interface im LANCOM weniger Daten an das WAN abgeben kann, als aus dem LAN in den Spitzenzeiten angeliefert werden. Das 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.



DE

Anders sieht das aus, wenn ein Ethernet-Interface die Verbindung ins WAN darstellt. Aus Sicht des LANCOM sieht die Verbindung ins Internet über das externe 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!



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

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

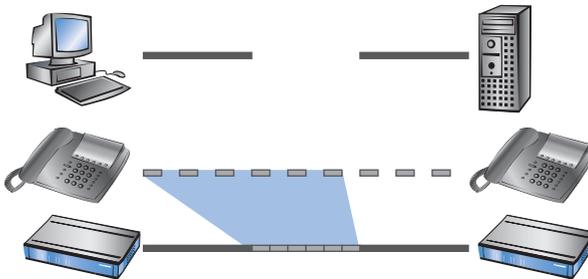
Hier landen alle Pakete, die nicht aufgrund einer empfangsseitig aktiven QoS-Regel gesondert behandelt werden müssen. Pakete in dieser Queue werden direkt weitergeleitet bzw. bestätigt, ohne Maximalbandbreiten zu berücksichtigen.

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.



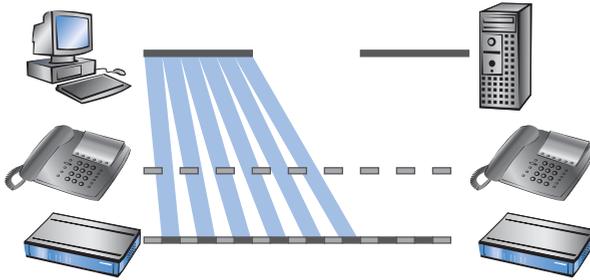
Der FTP-Transfer setzt recht große Datenpakete von 1500 Byte ein, während die Voice-over-IP-Verbindung Pakete von z.B. netto 24 Byte in relativ kurzen Takten verschickt. Wenn sich in dem Moment, in dem ein VoIP-Paket übertragen werden soll, z.B. schon FTP-Pakete in der Sendequeue des LANCOM befinden, kann das VoIP-Paket erst dann verschickt werden, wenn die Leitung wieder frei ist. Je nach Übertragungsrate 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

► Kapitel 9: Quality-of-Service

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 zeitliche 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.

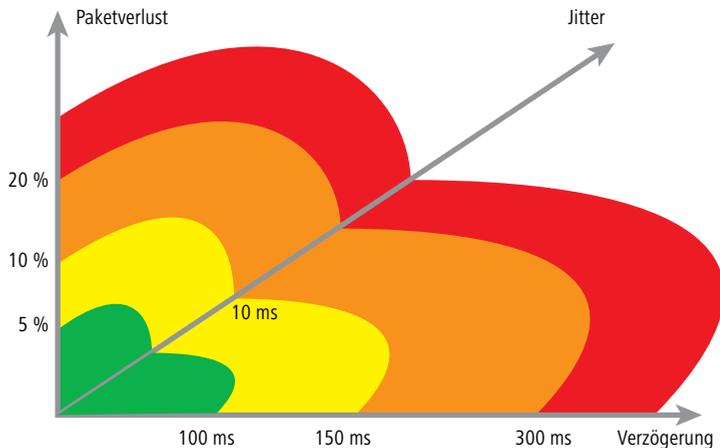
- Das LANCOM kann die zu sendenden Pakete oberhalb einer einstellbaren Maximalgröße (z.B. 256 Byte) selbst in kleinere Einheiten aufteilen. Dieses als "Fragmentieren" bezeichnete Verfahren wird jedoch nicht von allen

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

► Kapitel 9: Quality-of-Service

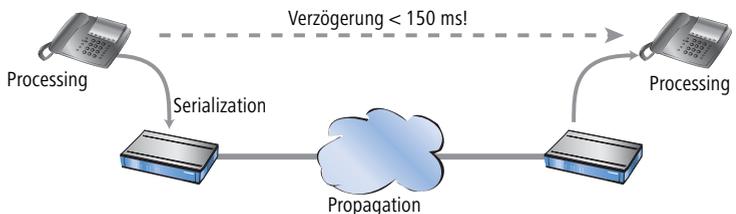
Qualität noch als brauchbar, darüber hinaus gilt die Verbindung als nicht mehr brauchbar für die Sprachübertragung.

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 Pakete ausgeglichen werden.
- Die Verzögerung wird von mehreren Komponenten beeinflusst:
 - ▷ 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.

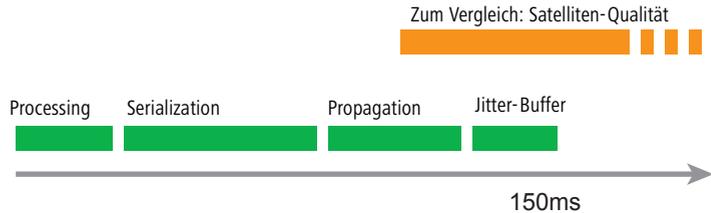
Diese beiden Anteile ergeben zusammen die Verzögerung, die idealerweise nicht mehr als 150 ms betragen sollte.



- 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 Ver-

zögerung, 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.
- 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

► Kapitel 9: Quality-of-Service

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.
- 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	Proces- sing	Serializa- tion	Propga- tion	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 eine 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.
- ▶ **DiffServ:** Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

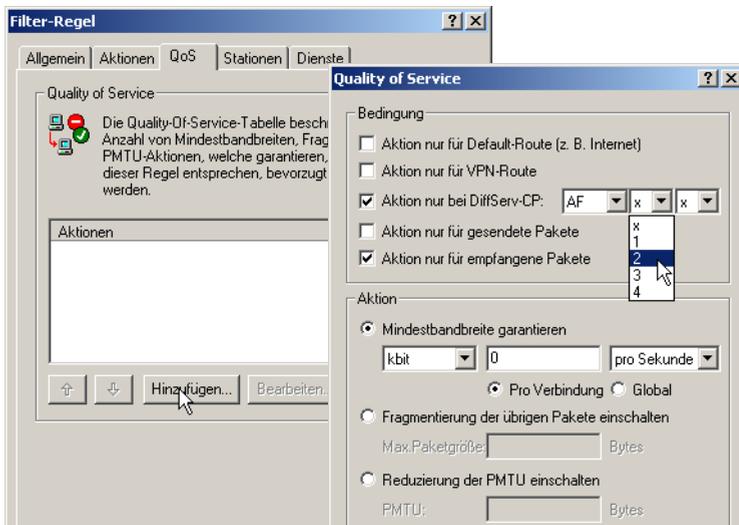
DSCP Codepoints	Übertragungsweise
CSx (inklusive CS0 = BE)	normal übertragen
AFxx	gesichert übertragen
EF	bevorzugt übertragen

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 185.

► Kapitel 9: Quality-of-Service

WEBconfig, Telnnet

Bei der Konfiguration mit WEBconfig oder Telnnet werden diese Parameter an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	Aufruf
WEBconfig	Setup/IP-Router-Modul/Firewall/Regelliste
Telnnet	Setup/IP-Router-Modul/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:

- **%Lcnds0 @dAFxx %A**: Akzeptieren (gesichert Übertragen) bei DiffServ “AF”, Limit “0”
- **%Qcnds32 @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 “%Lcnds0 @dAFxx %A” akzeptiert die mit dem DSCP “AFxx” markierten Pakete zur Signalisierung eines Anrufs. Die mit “EF” gekennzeichneten Sprachdaten werden durch den Eintrag “%Qcnds32 @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 116.

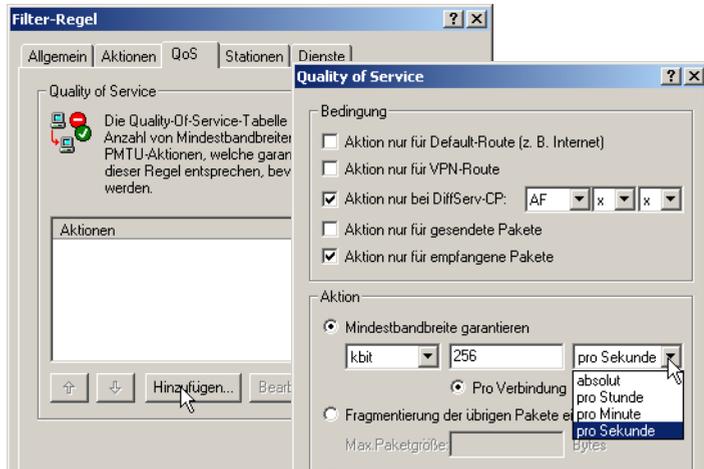
9.7.2 Minimal- und Maximalbandbreiten definieren

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.



- 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-Modul/Firewall/Regelliste
Telnet	Setup/IP-Router-Modul/Firewall/Regel-Liste

▶ Kapitel 9: Quality-of-Service

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:

- ▶ **%Qc32**: Mindestbandbreite von 32 kBit/s für jede Verbindung
- ▶ **%Lg256 %d**: Maximalbandbreite von 256 kBit/s für alle Verbindungen (global)



Weitere Informationen zum Definieren der Firewall-Regeln finden Sie im Kapitel 'Firewall' → Seite 116.

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 Datenübertragungsraten für Ethernet-, DSL und DSLoL-Interfaces werden im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Interfaces' bei den Einstellungen für die verschiedenen WAN-Interfaces festgelegt:

- ▶ Ein DSL und DSLoL-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 187).

- 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

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



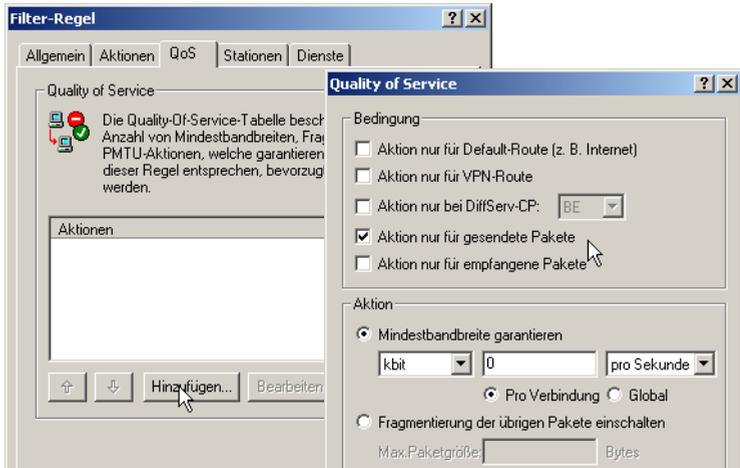
Die Werte für die Upstream-Rate und die Downstream-Rate werden in KBit/s angegeben, die Werte für den externen Overhead in Bytes/Paket.

► Kapitel 9: Quality-of-Service

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-Modul/Firewall/Regelliste
Telnet	Setup/IP-Router-Modul/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

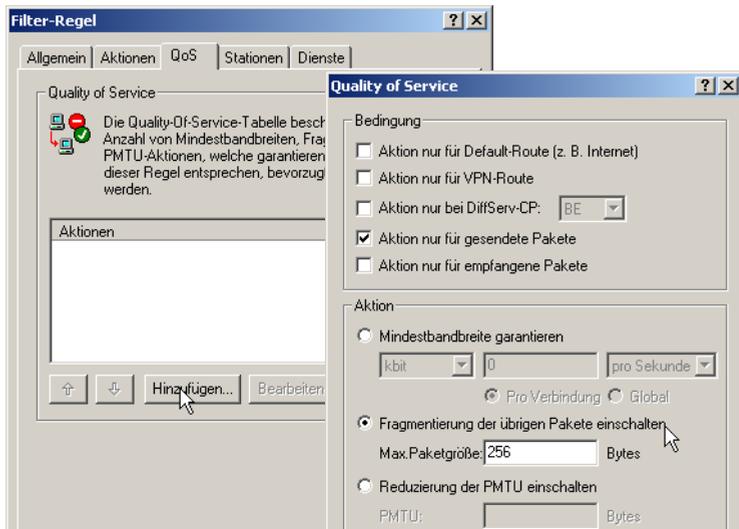
Die Längenreduzierung der Datenpakete wird definiert über eine Regel in der Firewall nach den folgenden Randbedingungen:

► 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, Telnnet

Bei der Konfiguration mit WEBconfig oder Telnnet 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-Modul/Firewall/Regelliste
Telnnet	Setup/IP-Router-Modul/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.

► Kapitel 9: Quality-of-Service

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	%Qc ds32 %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 Virtuelle LANs (VLANs)

10.1 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.

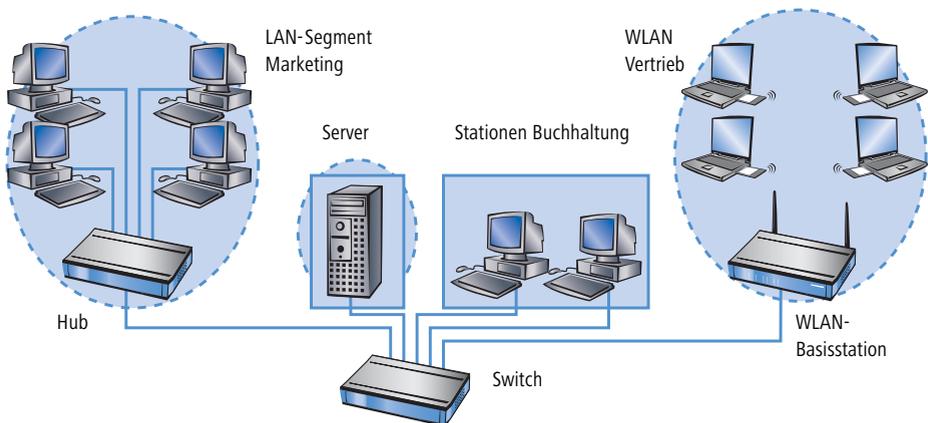
Eine Möglichkeit, diese Probleme zu überwinden, stellen die virtuellen LANs (VLAN) dar, wie sie in IEEE 802.1p/q beschrieben sind. Bei diesem Konzept werden auf einem physikalischen LAN mehrere virtuelle LANs definiert, die sich gegenseitig nicht behindern und die auch den Datenverkehr der jeweils anderen VLANs auf dem physikalischen Ethernetstrang nicht empfangen oder abhören können.

10.2 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.



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.

10.2.1 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 214).

- **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.



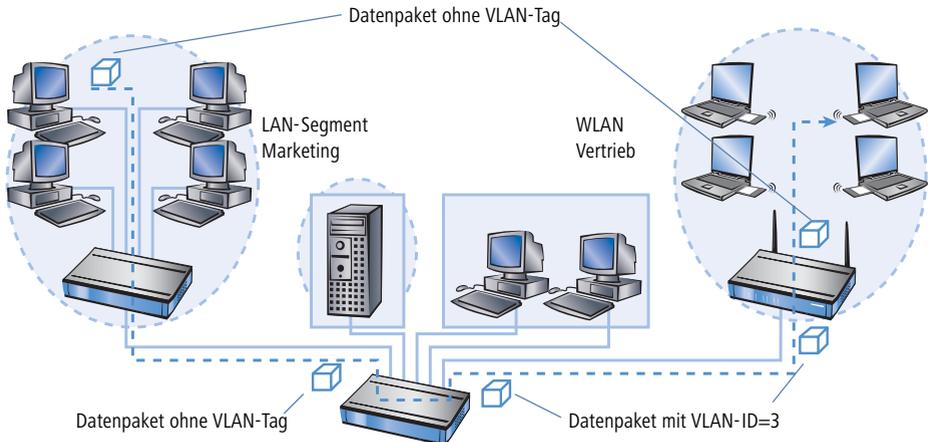
Ältere Switches in LAN können überlange Frames möglicherweise nicht richtig zwischen den einzelnen Ports weiterleiten und verwerfen die getaggten Pakete.

10.2.2 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.

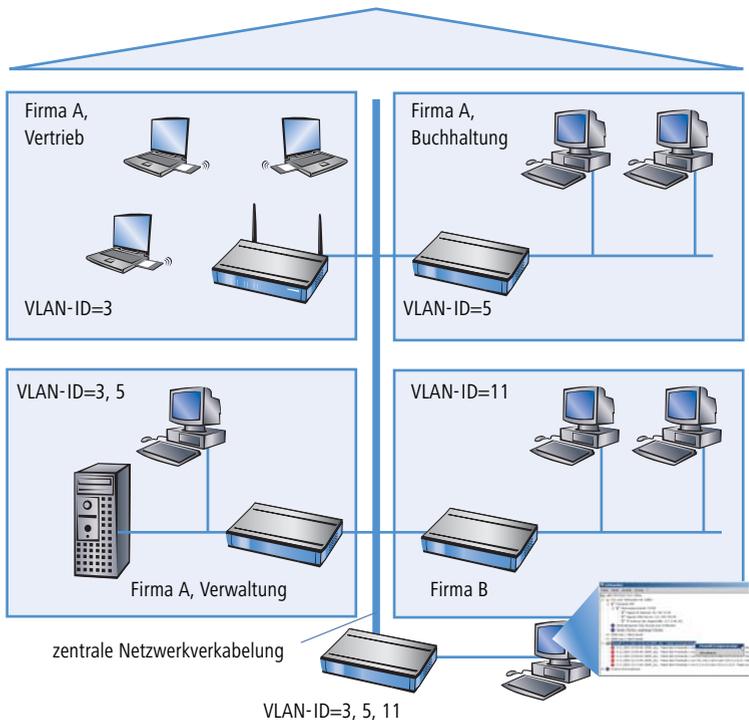
Greifen wir dazu das erste Beispiel wieder auf:



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

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.

10.3 Konfiguration von VLANs

DE



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

10.3.1 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 214) 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

10.3.2 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:

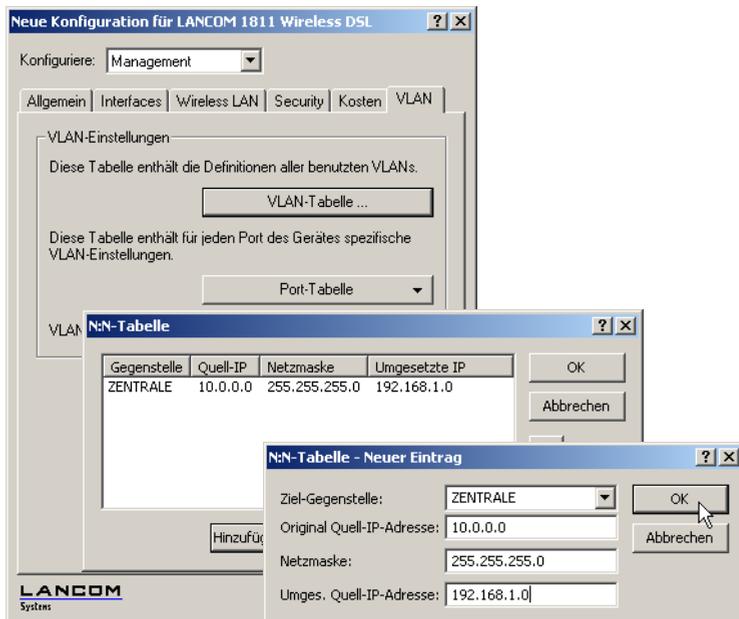
- **Port:** Der Name des Ports, nicht editierbar
- **Tagging verwenden:** Diese Option gibt an, ob Datenpakete auf diesem Port getaggt werden sollen. Das Tagging bezieht sich nur auf solche Datenpakete, die über diesen Port **versendet** werden.
- **Ungetaggte Frames zulassen:** Diese Option gibt an, 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

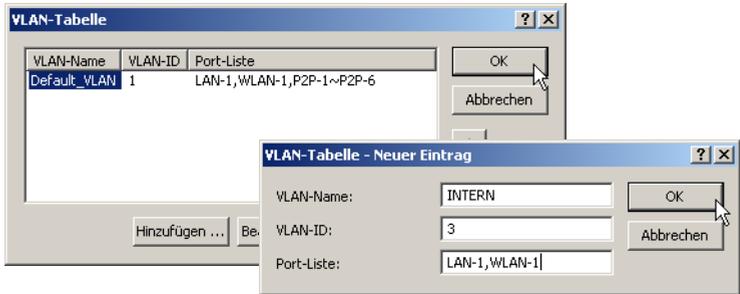
10.3.3 Konfiguration mit LANconfig

Unter LANconfig stellen Sie die Parameter für die virtuellen Netze im Konfigurationsbereich 'Management' auf der Registerkarte 'VLAN' ein:

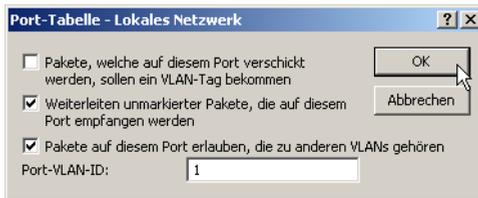


► Kapitel 10: Virtuelle LANs (VLANs)

Über die Schaltfläche **VLAN-Tabelle** erreichen Sie die Definition der verwendeten virtuellen Netze:



Über die Schaltfläche **Port-Tabelle** öffnen Sie eine Drop-Down-Liste, in der Sie jeweils einen VLAN-Port zur Bearbeitung auswählen können:

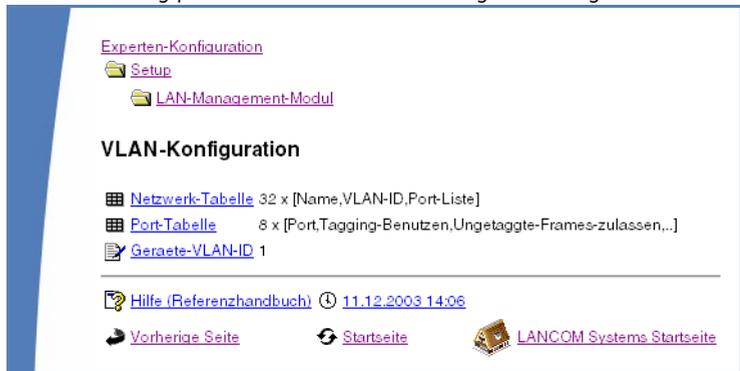


10.3.4 Konfiguration mit WEBconfig oder Telnet

Unter WEBconfig oder Telnet finden Sie die Tabellen zur Konfiguration der VLANs auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ► Setup ► LAN-Management-Modul ► VLAN-Konfiguration
Terminal/Telnet	cd /Setup/LAN-Management-Modul/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,...]

 [Geräte-VLAN-ID](#) 1

 [Hilfe \(Referenzhandbuch\)](#)  11.12.2003 14:06

 [Vorherige Seite](#)  [Startseite](#)  [LANCOM Systems Startseite](#)

11 Bürokommunikation mit LANCAP



Die Ausführungen dieses Abschnittes beziehen sich nur auf Geräte mit ISDN-Schnittstelle.

Die LANCAP von LANCOM ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

11.1 Welche Vorteile bietet die LANCAP ?

Der Einsatz der LANCAP bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die LANCAP 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-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.

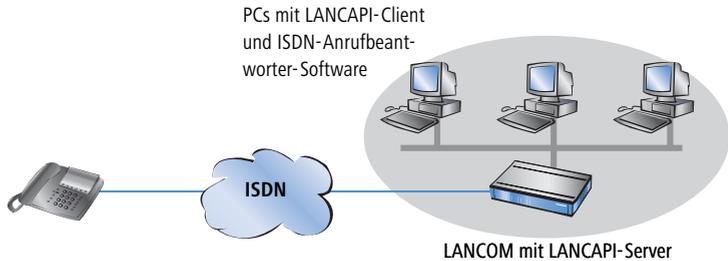
Beim Versenden von Faxen wird z.B. am Arbeitsplatz ein Faxgerät simuliert. Mit der LANCAP leitet der PC das Fax über das Netzwerk an einen Router weiter, welcher die Verbindung zum Empfänger herstellt.



Alle Anwendungen, die Sie über die LANCAP betreiben, verwenden direkte ISDN-Verbindungen und laufen nicht über die Router-Funktion des Geräts. Daher funktionieren die Firewall- und Gebührenüberwachungsfunktionen in diesem Zusammenhang nicht. Die LANCAP ist ebenso unabhängig von allen Routing oder VPN-Funktionen ('System-Design' → Seite 12).

11.2 Das Client-Server-Prinzip

Die LANCAP besteht aus zwei Komponenten, einem Server (im LANCOM) und einem Client (auf den PCs). Der LANCAP-Client wird nur auf den Rechnern im lokalen Netz installiert, die die Funktionen der LANCAP nutzen möchten.



11.2.1 Konfiguration des LANCAPI-Servers

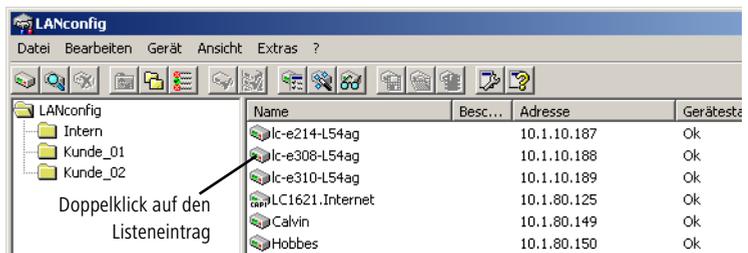
Bei der Konfiguration des LANCAPI-Servers im LANCOM werden im Prinzip zwei Fragen behandelt:

- 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.



► Kapitel 11: Bürokommunikation mit LANCAPI

- 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-Modul** ► **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').



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**.

11.2.2 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 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.

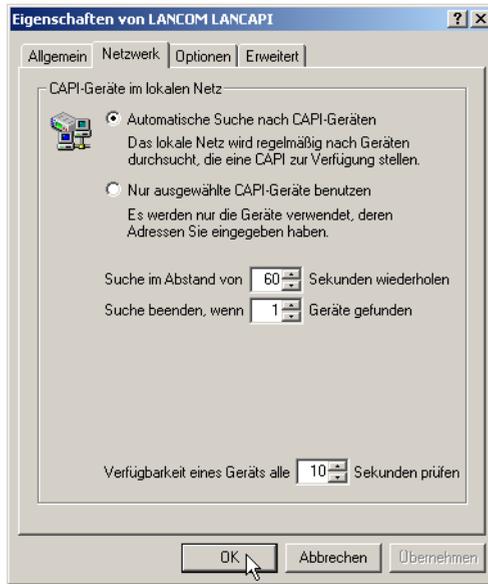
Der LANCAPI-Client startet von nun an automatisch. Seinen Status zeigt das zusätzliche Icon in der Windows-Taskleiste (neben der Uhr) an.



11.2.3 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'. 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 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.



11.3 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'.

11.4 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.

► Kapitel 11: Bürokommunikation mit LANCAPI

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 "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.

11.5 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.

11.6 Unterstützte B-Kanal-Protokolle

Folgende CAPI-Protokolle werden unterstützt:

Wert	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

12 Weitere Server-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

12.1 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.

12.1.1 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

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.

12.1.2 DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server kann drei 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'.

► 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.

► 'Auto': In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz automatisch 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. 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.

Ob der DHCP-Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

Die Default-Einstellung für den Zustand ist 'Auto'.

12.1.3 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.

The screenshot shows the 'LANCOM DSL/T-1611 Office, ... Konfiguration' window with the 'DHCP' tab selected. The 'Konfiguriere:' dropdown is set to 'TCP/IP'. The 'DHCP-Server aktiviert:' dropdown is set to 'Ja'. Under 'Adressen für DHCP-Clients', the following fields are filled: 'Erste Adresse: 192.168.2.50', 'Letzte Adresse: 192.168.2.70', 'Netzmaske: 255.255.255.0', 'Broadcast: 0.0.0.0', and 'Standard-Gateway: 192.168.2.100'. Under 'Weiterleiten von DHCP-Anfragen', the 'Adresse des Servers:' field is filled with '0.0.0.0'. There are two unchecked checkboxes: 'Antworten des Servers an das lokale Netz anpassen' and 'Antworten des Servers zwischenspeichern'. The LANCOM Systems logo is at the bottom left, and 'OK' and 'Abbrechen' buttons are at the bottom right.

- 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.
 - ▷ 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.

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 Netzwerkkumgebung 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.

Auf der Registerkarte 'WINS-Konfiguration' muss zusätzlich die Option 'DHCP für WINS-Auflösung verwenden' eingeschaltet werden, wenn man Windows-Netze über IP mit Namensauflösung über NBNS-Server verwenden will. Der DHCP-Server muss dann außerdem einen NBNS-Eintrag haben.

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 Netzwerkkumgebung.

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-Modul / Tabelle-DHCP
Terminal/Telnet	Setup/DHCP-Modul/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 Gültig-

▶ Kapitel 12: Weitere Server- Dienste

keitsdauer, 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.

12.2 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.

12.2.1 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.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannt 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.

▶ Kapitel 12: Weitere Server- Dienste

- ▶ 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.

12.2.2 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 fündig, holt er die gewünschte Infor-

mation 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-Modul ► DNS-Default ► DNS-Backup
Terminal/Telnet	/Setup/TCP-IP-Modul/DNS-Default /Setup/TCP-IP-Modul/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.

12.2.3 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-Modul
Terminal/Telnet	cd /Setup/DNS-Modul

Gehen Sie zur Einstellung des DNS-Servers wie folgt vor:

► Kapitel 12: Weitere Server- Dienste

- ① Schalten Sie den DNS-Server ein.

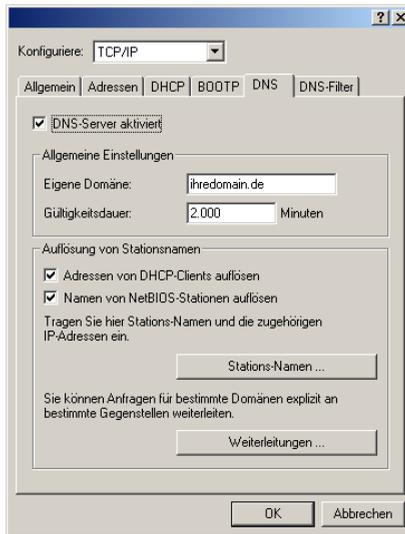
WEBconfig	... ► Zustand
Terminal/Telnet	set Zustand ein

- 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	<code>cd Setup/DNS-Modul/DNS-Tabelle</code> <code>set mail.ihredomain.de 10.0.0.99</code>

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:

The image shows a dialog box titled "Stations-Namen - Neuer Eintrag". It has two input fields: "Stations-Name:" with the text "mail.ihredomain.de" and "IP-Adresse:" with the text "10.0.0.99". There are two buttons: "OK" and "Abbrechen".

Die Angabe der Domain ist dabei optional, aber zu empfehlen.

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 Namenliste etc. wird dann automatisch die Verbindung zum Netz in der Zentrale hergestellt, wo der Mailserver schließlich gefunden wird.

► Kapitel 12: Weitere Server- Dienste

- 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-Modul/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

12.2.4 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-Modul/Filter-Liste set 001 www.gesperrt.de 0.0.0.0 0.0.0.0

DNS-Filter - Neuer Eintrag

Domäne:

IP-Adresse:

Netzmaske:

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:

DNS-Filter - Neuer Eintrag

Domäne:

IP-Adresse:

Netzmaske:

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.

12.2.5 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).

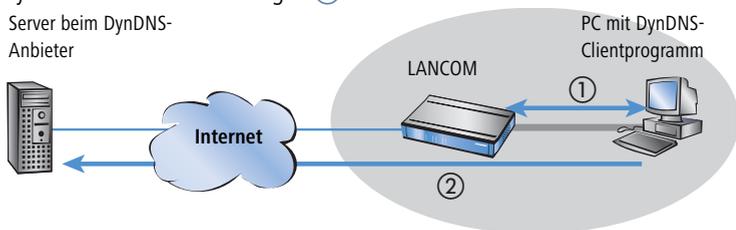
Damit wird ein LANCOM immer unter einem bestimmten Namen (FQDN - 'fully qualified domain name') erreichbar (z.B. "http://MyLANCOM.dynDNS.org").

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.

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.

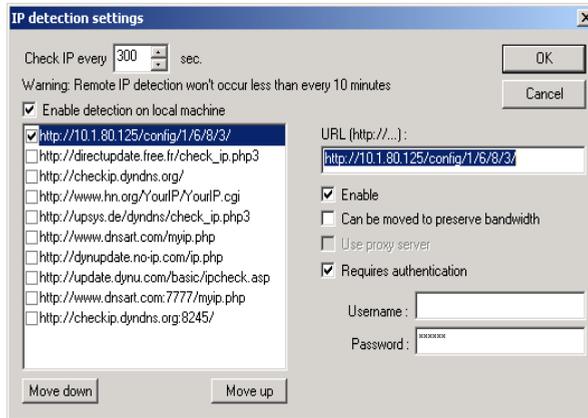
Server beim DynDNS-Anbieter



Die aktuelle WAN-seitige IP-Adresse eines LANCOM kann unter folgender Adresse ausgelesen werden:

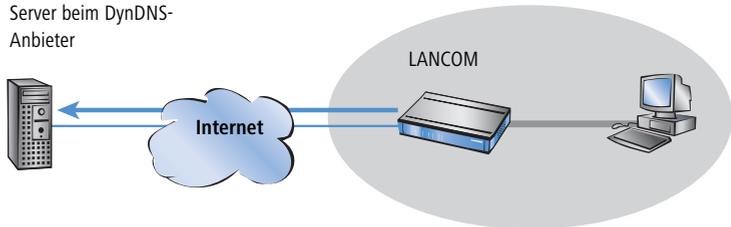
Abbildung: Auslesen der aktuellen IP-Adresse aus einem LANCOM

`http://<Adresse des LANCOM>/config/1/6/8/3/`



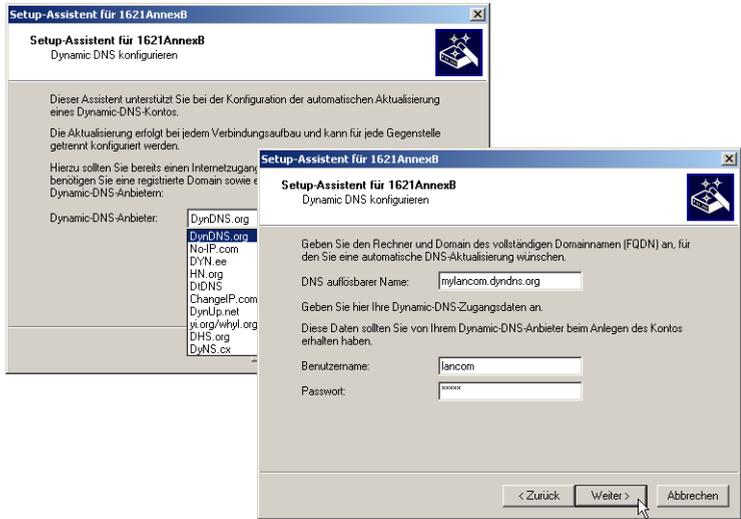
Alternativ kann das LANCOM die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter

Server beim DynDNS-Anbieter



► Kapitel 12: Weitere Server- Dienste

Die dazu notwendigen Einstellungen können komfortabel mit dem Setup-Assistenten von LANconfig vorgenommen werden:



12.3 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.

12.3.1 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.

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!

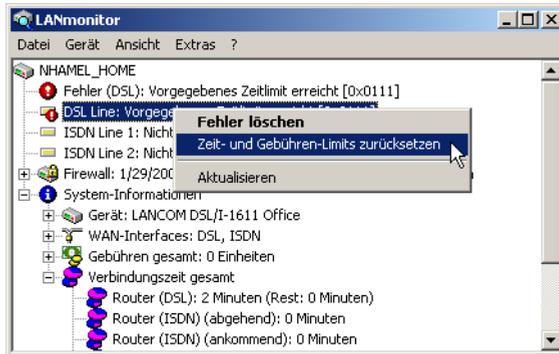


Wenn für die Verbindung, die mit dem Gebührenbudget begrenzt werden soll, in der Namenliste eine Haltezeit von '0' oder '9999' Sekunden eingestellt ist, wird die Gebührenüberwachung ausgeschaltet, die Verbindung trotz Erreichen des Limits nicht unterbrochen

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.

► Kapitel 12: Weitere Server- Dienste

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-Modul ► Aktivieren-Reserve
Terminal/Telnet	cd /Setup/Gebuehren-Modul 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.

12.3.2 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!

12.3.3 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!

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.

12.3.4 Einstellungen im Gebührenmodul

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management ► Kosten
WEBconfig	Experten-Konfiguration ► Setup ► Gebuehren-Modul
Terminal/Telnet	cd /Setup/Gebuehren-Modul

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.

12.4 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.

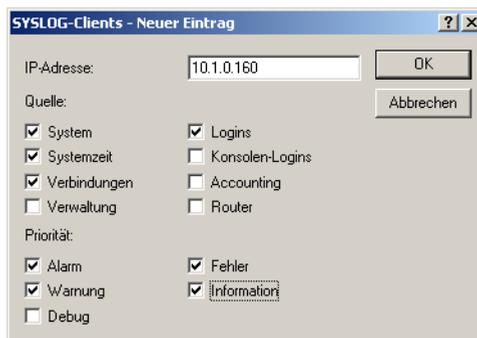
12.4.1 Einrichten des SYSLOG-Moduls

Konfigurationstool	Aufruf/Tabelle
LANconfig	Management ► Meldungen
WEBconfig	Experten-Konfiguration ► Setup ► SYSLOG-Modul
Terminal/Telnet	cd /Setup/SYSLOG-Modul

12.4.2 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.

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im LANCOM einstellen können. Zusätzlich gibt

► Kapitel 12: Weitere Server- Dienste

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

Priorität	Bedeutung	SYSLOG-Priorität
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.

12.5 Zeit-Server für das lokale Netz

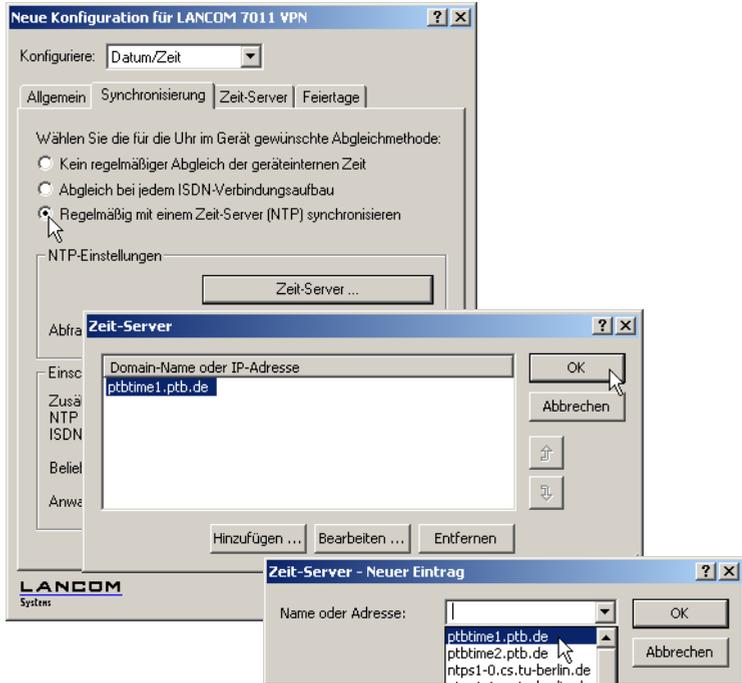
LANCOM Router können hochgenaue Zeitinformationen entweder über ISDN beziehen, oder aber über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit 'Open Access'-Policy, z.B. von der Physikalisch-Technischen Bundesanstalt). Die so ermittelte Zeit kann das LANCOM allen Stationen im lokalen Netz zur Verfügung stellen.

12.5.1 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-Ein-

► Kapitel 12: Weitere Server- Dienste

stellungen' wird dann mit der Schaltfläche **Zeit-Server** die Liste der Zeitserver geöffnet. Mit der Schaltfläche **Hinzufügen** können weitere Server in die Liste aufgenommen werden.



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.



12.5.2 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-Modul
Terminal/Telnet	cd /Setup/NTP-Modul

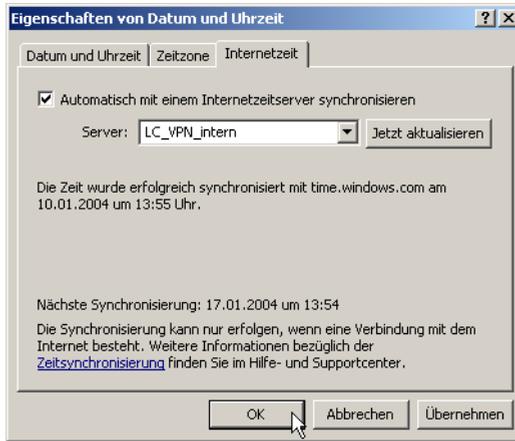
12.5.3 Konfiguration der NTP-Clients

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

► Kapitel 12: Weitere Server- Dienste

Registerkarte 'Internetzeit' kann dort der Server zur Synchronisation der Zeit ausgewählt werden.



13 VPN

Mit einem Virtual Private Network (VPN) können sichere Datenverbindungen über kostengünstige, öffentliche IP-Netzwerke wie z.B. das Internet aufgebaut werden.

Die Beschreibung der VPN-Funktionalität und der entsprechenden Einstellungen finden Sie in den separaten VPN-Dokumentationen:

- ▶ Benutzerhandbuch zu Ihrem VPN-fähigen LANCOM-Gerät
- ▶ Benutzerhandbuch zur LANCOM VPN Option
- ▶ Benutzerhandbuch zum LANCOM VPN Client

14 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 Frequenz-management; für den Einsatz in Europa; OFDM
802.11i	Zukünftige 802.11 Erweiterung mit zusätzlichen Sicherheitsmerkmalen
802.11x	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 Telefonverbindungen. 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
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 übersetzen 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 breitbandigen 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 Oisotropic Radiated Power, mittlere äquivalente isotrope Strahlungsleistung

► Kapitel 14: Glossar

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 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
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 Netzwerkzugang
RC4	Stromchiffrierverfahren von Ron Rivest, "Rens Code"
RFC2284	Request for Comments 2284, "Extensible Authentication Protocol"
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
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	Aneinanderhängen 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"
QoS	Quality-of-Service (siehe hierzu IP Quality-of-Service)

15 Anhang

15.1 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
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

15.2 Unterstützte RFCs

RFC	Titel
1334	PPP Authentication Protocols
2104	HMAC: Keyed-Hashing for Message Authentication
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
2506	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
2131	Dynamic Host Configuration Protocol
2132	DHCP Options and BOOTP Vendor Extensions
2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
2364	PPP Over AAL5
2225	Classical IP and ARP over ATM
1577	Classical IP and ARP over ATM
2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
2364	PPP Over AAL5
1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
1974	PPP Stac LZS Compression Protocol
1877	PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
1058	Routing Information Protocol
1389	RIP Version 2 MIB Extensions

RFC	Titel
1552	The PPP Internetworking Packet Exchange Control Protocol (IPXCP)
1542	Clarifications and Extensions for the Bootstrap Protocol
1631	The IP Network Address Translator (NAT)

15.3 Übersicht über die Funktionen nach LANCOM-Modellen und LCOS-Versionen

	800 1000 1100	I-10	821	1511	1521	1611	1621	1811	1821	3050 3550	4000 4100	6000 6001 6021	7011	L-2	IL-2	L-11	IL-11	L-54g	L-54ag		
Stateful Inspection	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	
DoS	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80
IDS	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80	2.80
QoS	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30	3.30
N:N-Mapping						3.30		3.30	3.30	3.30	3.30	3.30	3.30								
VLAN				3.30	3.30			3.30	3.30	3.30							3.30	3.30	3.30	3.30	
DMZ-Port			1)	1)	1)		1)	1)	1)				✓								
DES, 3-DES, Blowfish						✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓ ²⁾	✓	✓								
AES						3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20 ²⁾	3.20	3.20								
VPN-5 Option						integriert ab 3.32	integriert ab 3.32	integriert ab 3.32	integriert ab 3.32	✓	✓										
VPN Hardware- beschleunigung								in Verbindung mit VPN-25	in Verbindung mit VPN-25												
VPN-25 Option						✓	✓	✓	✓	✓	✓										
VPN-100												✓									
VPN-200													✓								
ADSL-Modem			✓		✓		✓		✓												
4-Port Switch			✓	✓	✓		✓	✓	✓												
ISDN Festverbindungs- Option	✓	✓	✓	✓	✓	✓	✓	✓	✓		integriert	integriert	integriert		✓		✓				
Faxmodem Option	✓	–	–	–	–	–	–	–	–	–	integriert	✓	–	–	✓		✓	–	–		
Dynamic DNS	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10				3.10	3.10	3.10	3.10	3.10
DSLolL			3.10				3.10										3.10	3.10	3.10	3.10	3.10
CRON	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10	3.10

¹⁾ Port-Separierung (Private Mode)

²⁾ nur wenn bei den Geräten die entsprechenden VPN-Optionen freigeschaltet sind

16 Index

Numerics

1-1-Mapping	91
3-DES	264
4-Port Switch	264
802.11	254
802.11a	254
802.11b	254
802.11g	254
802.11h	254
802.11i	254
802.11x	254

A

AAL-5	100
Access Point	254
Access-Router	254
Adress-Pool	228
Adressverwaltung	226
ADSL	13, 52, 254
ADSL-Modem	264
AES	254, 264
Allow-All	130, 149
Anruferkennung	62
AOCD	245
Application Gateway	125
ATM	52
ATM-Anpassungsschicht	100
Ausschluss-Routen	73
Authentifizierung	109
auto reconnect	108

B

Bandbreite	254
Benutzername	27, 63, 106
B-Kanal	
Protokoll	64
B-Kanal-Protokolle	225
Bonk	178
Breitband	254

Bridge	254
Broadcast	254
Brute-Force	57
Bruttodatenrate	190
BSS	254

C

Calling Line Identifier Protocol	65
CAPI	255
CAPI Faxmodem	223
CAPI-Protokolle	225
CAPI-Schnittstelle	218
CCK	255
CHAP	63
Client	255
CLIP	64, 65
Collision Domain	207
Common ISDN Application Programming Interface (CAPI)	218
Conf	106
CRC	255
CRON	264
Cron-Dienst	42
Cron-Tabelle	44
CSMA/CA	255

D

Datendurchsatz	255
Datenkompressionsverfahren	
LZS	113
Datenübertragung	113
Datum/Zeit	249
Default-Gateway	67
Denial of Service	12
Denial-of-Service	176
Bonk	178
Fragrouter	178
Konfiguration	180
LAND	177

► Index

- Ping of Death 177
- Smurf 177
- SYN Flooding 176
- Teardrop 178
- Denial-of-Service-Angriffe 176
 - LAND 177
 - Smurf 177
 - SYN Flooding 176
- Deny-All 149
- DFÜ-Netzwerk 24, 63
- DHCP 52, 100, 226, 255
 - Automodus für den DHCP-Server 227
 - DHCP-Server 226, 233
 - für WINS-Auflösung 231
 - Gültigkeitsdauer 230
 - Zuweisung der Broadcast-Adresse 229
 - Zuweisung der Netzmaske 229
 - Zuweisung des Standard-Gateways 230
 - Zuweisung von DNS- und NBNS-Server 230
- Dienst 232
- Dienstgüte –
 - siehe Quality-of-Service
- Differentiated Services –
 - siehe DiffServ
- Differentiated Services Code Point –
 - siehe DSCP
- DiffServ 184, 185
 - Assured Forwarding 184, 185
 - Best Effort 185
 - Class Selector 185
 - Expedited Forwarding 184, 185, 187
 - IPSec 184
- Distanz einer Route 73
- D-Kanal 52, 64
- DMZ
 - Zuweisung von IP-Adressen 228
- DMZ-Port 264
- DMZ-Schnittstelle 13
- DNS 52, 232, 255
 - DNS-Forwarding 234
 - DNS-Server 226, 230, 232
 - DNS-Tabelle 237, 238
 - Dynamic DNS 240
 - Filterliste im DNS-Server 238
 - Filtermechanismus des DNS-Servers 233
 - URL-Blocking 238
 - verfügbare Informationen im DNS-Server 234
- Domain 232, 238
 - sperren 239
- Domain Name Service (DNS) 232
- Domäne 255
- DoS 264
 - Konfiguration 180
- Download 11, 255
- Downstream 255
- Downstreamrate 190
- DS 255
- DSCP 185
- DSL 13, 255
- DSLolL 14, 264
- DSSS 255
- Durchsatz 113
- Dynamic DNS 240, 255, 264
- Dynamic Host Configuration Protocol (DHCP) 226
- Dynamische Kanalbündelung 113
- Dynamisches Routing 71
- dynDNS 240
- E**
- EAP 255
- EAP-MD5 255
- EAP-TLS 255
- EAP-TTLS 255
- EIRP 255
- E-Mail-Viren 152

Encapsulation	99	Beispielkonfiguration ISDN-Einwahl	
End-Adresse	228	154	
Enterprise specific Traps	260	Beispielkonfiguration Netzwerkopp-	
ESS	256	lung	154
ESSID	256	Beispielkonfiguration V.110-Einwahl	
ETH-10	100	154	
Ethernet	256	Beispielkonfiguration VPN-Einwahl	
exposed host	83	153	
F		Benachrichtigung per E-Mail	147
Fail	106	Benachrichtigung per SNMP-Trap	147
Fast Call Back	65	Besondere Protokolle	131
Fax	223	Default-Einstellung	152
Fax Class 1	223	Default-VPN-Regeln	134
Faxmodem Option	264	Deny-All	149, 152, 153
Faxmodem-Option	225	Diagnose	165
Faxtreiber	223	DMZ	150
Faxübertragung	224	DMZ (Schaubild)	151
Fehlende Gebühreninformationen	245	dualhomed Gateway	125
Fehlersuche	47	Einstellungen	134
Fernkonfiguration	15	Ereignisanzeige	166
Fernüberwachung	88	Filterliste	129, 168
Fernverbindung	24	Firewall-Tabelle	166
Fernwartung		Fragmente	135
mit N-N-Mapping	90	Hostsperrliste	129, 173
Fernzugang	24	ICMP	136
FHSS	256	ICMP-Verbindungen	133
Filterliste	129, 131	Komponenten	119
Firewall	67, 116, 218, 256	Logging-Tabelle	167
Alarmierungsfunktionen	145	NAT	152
Allow-All	130, 149	paketfilterbasiert	121
Anwendungsfälle	153	Parameter der Firewall-Regeln	138
Application Gateway	125	Ping-Blocking	136
Assistent	155	Portsperrliste	129, 172
Aufgaben	120	Prüfen mit mehreren Listen	130
Authentifizierungs-Port	137	Quell- und Zielobjekte	161
Beispielkonfiguration Basic Internet		Schaubild	128
153		Sitzungswiederherstellung	135
Beispielkonfiguration IPSec/PPTP-Frei-		Stafeful Inspection	123
schaltung	154	Stateful-Inspection	152
		Stationen sperren	67

► Index

Strategien für die Einstellung	149	mit TFTP	33
SYSLOG	146	Flash-ROM-Speicher	29
TCP-Stealth-Modus	137	Flatrate	107
TCP-Verbindungen	133	FQDN	240
Tipps zur Einstellung	151	Fragrouter	178
Typen	121	Frame-Tagging	209
UDP-Verbindungen	131	Frequenz	256
Verbindungsliste	129, 170	Frequenzband	256
Firewall/QoS-Aktivierung	134	FTP	256
Firewall-Regel		aktives FTP	197
Absender-Adresse sperren	145	passives FTP	197
Aktionstabelle	161	TCP-gesicherte Übertragung	192
Aufbau	142	FTP-Datentransfer	191
Bedingung	140, 143	FTP-Download	184
E-Mail-Nachricht senden	145	Funkfrequenz	256
Konfiguration	155	G	
Konfiguration mit LANconfig	155	Gateway	226, 256
Konfiguration mit WEBconfig oder Tel- net	159	Gebühren	
Limit	140, 144	Begrenzung	242
Objekttabelle	160	Einheiten	113, 244
Paket-Aktion	141, 144	Information	113, 245
Priorität	139	Management	242
Quality of Service	141, 145	Zeit-Limit	243
Regel-Tabelle	159	Gebührenüberwachung	218
Schaubild	142	Gegenstelle	106
SNMP senden	145	Gerätename	106
Sonstige Maßnahmen	141, 144	Gültigkeitsdauer	227, 230
Syslog-Nachricht senden	145	H	
Trigger	140, 144	Haltezeit	113, 114
Verbindung	140, 142	HDLC	100
Verbindung trennen	145	Hinweis-Symbole	11
Verknüpfung	139	Hohe Telefonkosten	242
VPN-Regel	139, 140	Host	232
Ziel-Port sperren	145	Hostsperrliste	129, 130
Firewall-Tabelle	166	HotSpot	256
FirmSafe	29	HSCSD	100
Firmware	11	HTTPS	19
Firmware-Upload	31	Hub	256
mit Terminalprogramm	32		

I			
IAPP-Roaming	256	IP-Spoofing	174
IBSS	256	IP-Telefonie	191
ICMP	67, 154	IPv4-Adresse	87
ICMP-Verbindungen	133	IPX-Router	13
Identifikationskontrolle	62	ISDN	13, 257
Identifizierung des Anrufers	63	D-Kanal	65
IDS	256, 264	ISDN Festverbindungs-Option	264
Konfiguration	175	ISDN-Administrationszugang	58
IEEE	256	ISM-Frequenzband	257
IEEE 802.1p/q	207	ISP	257
IEEE 802.3	100	K	
Inband	15	Kanalbündelung	112
Konfiguration über Inband	15	Dynamisch	113
mit Telnet	20	Statisch	113
Internet-Zugang	105	Keep-alive	107
Intranet		Konfiguration	
Zuweisung von IP-Adressen	228	Verfahren	15
Intrusion Detection	12, 174	Konfigurationsdatei	68
Konfiguration	175	Konfigurationskennwort	65
Intrusion-Detection		Konfigurations-Schnittstelle	15
IP-Spoofing	174	Kosten begrenzen	242
Portscan	174	L	
Inverses Masquerading	83, 88	LAN	257
IP	256	logisch	209
Filter	67	physikalisch	209
Ports sperren	67	LAN-Bridge	13
IP Quality-of-Service	257	LANCAPI	13
IP-Adresse	48, 67, 104	LANcapi	257
IP-Adressverwaltung	226	LANCOM-Betriebssystem	12
IP-Broadcast	77	LANconfig	17, 24, 34, 257
IP-Header	184	Verwaltung mehrerer Geräte	18
IP-Masquerading	13, 51, 67, 87, 256	LAND	177
IP-Module	13	LANmonitor	39
IP-Multicast	77	Accounting-Informationen	40
IP-Router	12	Aktivitätsprotokoll	41
IP-Routing		Anzeige-Optionen	47
Standard-Router	74	Firewall-Ereignisanzeige	41
IP-Routing-Tabelle	71	Internet-Verbindung kontrollieren	48
IPSec	256	System-Informationen	47

► Index

VPN-Verbindungen	40	NAT	87
LANtools	257	NBNS-Server	226, 231
Layer-2	100	NetBIOS	52, 233
Layer-2-Switch	207	NetBios	257
Layer-3	100	NetBIOS-Netze	233
Layername	99	NetBIOS-Proxy	152
LCOS	9, 12, 257, 264	Nettodatenrate	190
LCP-Echo-Reply	103	Network Address Translation	87
LCP-Echo-Request	103	Netzkopplung	88
LCR	245	Netzmaske	67
Least-Cost-Routing	245	Netzwerk-Management	34
LLC-MUX	99	Netzwerknamen	232
Logging-Tabelle	166	N-N-Mapping	88
Login	30	dezentrales Mapping	91
Login-Sperre	57	DNS-Forwarding	93
Login-Versuche	57	Firewall	93
logische Senderichtung	197	Konfiguration	92
logisches LAN	209	Loopback-Adresse	93
Loopback-Adresse	91	NAT-Tabelle	92
LZS-Datenkompression	113	Netzerkennung über VPN	89
		Routing-Tabelle	93
M		VPN-Regel	93
MAC	257	zentrales Mapping	92
MAC-Adresse	257	NTBA	257
MAC-Frame	209	NTP-Clients	251
Mailserver	237	NTP-Server	249
Maximalbandbreite	185, 187	O	
Mbit	257	OFDM	257
MIB2	260	Online-Minuten	242
MIC	257	Outband	15
Mindestbandbreite	185, 186, 187	Konfiguration über Outband	15
beim Empfang	186	Overhead	183
beim Senden	186	P	
Modem	100	Paket-Dump	52
MS-CHAP	101, 102	Paketfilter	121
Multilink PPP (MLPPP)	101, 112	PAP	63
Multithreading	37	passwd	56
N		Passwort	25, 26, 48, 54, 62, 63, 106
N		PEAP	257
N-Mapping	13, 264		

Periode	242	R	
physikalische Senderichtung	197	RADIUS	258
physikalisches LAN	209	RC4	258
ping	154	Rechner-Namen	232
Ping of Death	177	Remote Access	104
Ping-Blocking	136	RFC2284	258
ping-Blocking Konfiguration	182	RFCs	262
PKI	257	RIP	51
PMTU-Reduzierung	192	Router	258
Point-to-Multipoint (WLAN)	258	Router-Interface-Liste	114
Point-to-Point (WLAN)	258	Router-Name	72
Point-to-Point Tunneling		Routing-Tabelle	67
Protocol (PPTP)	107	Rückruf	62, 64
Port Address Translation	88	Fast Call Back	65, 110
Portscan	174	nach Microsoft CBCP	108
Port-Separierung	264	nach RFC 1570	110
Portsperrliste	129, 130	schnelles LANCOM-Verfahren	110
PPP	48, 63, 100, 112, 258	S	
LCP Extensions	110	Scheduled Events	42
Leitungsüberprüfung mit LCP	103	Schutz	
Rückruf-Funktionen	108	für die Konfiguration	54
Verhandlungsphase	27	SDSL	258
Zuweisung von IP-Adressen	104	Serielle Schnittstelle	15
PPP-Client	24	Server	258
PPPoE	100	Sicherheit	54, 116
PPP-Verbindung	26	Sicherheits-Checkliste	65
PPTP	13, 107, 258	Sicherheitseinstellungen	10, 56
Precedence	185	Sicherung	106
Private Mode	264	Sicherungsverfahren	63
Projektmanagement	34	SINA	258
Q		SMTP	258
QoS	191, 258, 259, 264	Smurf	177
Richtung der Datenübertragung	197	SNMP	23
QoS –		Konfiguration schützen	66
siehe Quality-of-Service		SNMP-Trap	90, 147
Quality of Service	12	SNMP-Traps	260
Quality-of-Service	183	SNMPv3	258
Queue	187	Software einspielen	29
		Splitter	258

► Index

SSID	258	TPC	259
SSL	258	Trace	
Stac- Datenkompression	113	Ausgaben	50
Standard- Faxprogramme	223	Beispiele	53
Start- Adresse	228	Schlüssel und Parameter	50
Stateful Inspection	264	starten	50
Stateful- Paket- Inspection	123	Trojaner	152
Stations- Namen- Tabelle	237	Type-of- Service –	
Statische Kanalbündelung	113	siehe ToS	
Statisches Routing	71	U	
Stealth- Modus		Übertragungsraten	48
Konfiguration	182	Überwachung	47
Support	11	UDP	67, 183
Switch	258	UDP- Verbindungen	131
SYN Flooding	176	Upload	29, 259
SYN/ACK- Speedup	78	Upstream	259
SYSLOG	146, 246	Upstreamrate	190
T		URL- Blocking	238
TAE	258	Username	106
TCP	67, 183	V	
TCP/IP	71, 259	V.110	100
TCP/IP- Filter	67	VC- MUX	99
TCP/IP- Netze	232	Verbindungsbegrenzung	244, 245
TCP- Stealth- Modus	137	Verbindungsliste	129, 131
TCP- Steuerungspakete	187	Verkettung	259
TCP- Verbindungen	133	Virtual Private Network	253
Teardrop	178	virtuelles LAN	207
Telnet	13, 24, 67	VLAN	207, 264
Term	106	Abschirmung des SNMP- Traffics	211
Terminalprogramm	31	Alle VLANs zulassen	214
TFTP	13, 23, 67	Anschluss von WLAN- Stationen	211
Timeout	113	Default- ID	214
TKIP	259	Default- VLAN- ID	209
TLS	259	ID	209
ToS	184, 185	Konfiguration	213
High Reliability	184	Management des LAN- Traffics	211
IPSec	184	Netzwerktafel	213
Low Delay	184, 187	Nutzung einer zentralen Verkabelung	
Priorität	185	212	

Port	214	WLAN	259
Portliste	213	WPA	259
Porttabelle	214	X	
Priorität	209	X.75	100
Tagging verwenden	214	xDSL	259
Umsetzung in den Schnittstellen	210	XOR	259
Ungetaggte Frames zulassen	214	Y	
Verschiedene Organisationen auf einem LAN	212	Y-Verbindung	114
VLAN-ID	213	Z	
VLAN-ID	209	Zeit	106
Voice-over-IP	183, 186	Zeitabhängige Verbindungsbegrenzung	245
VoIP – siehe Voice-over-IP		Zeitautomatik	42
VPN	13, 253, 259, 264	Zeitbudget	245
Client	154	Zeit-Server	249
Fernwartung über N-N-Mapping	90	Zugangsschutz	62
Firewall-Regeln	134	für die Konfiguration	62
Gateway	153	Zugangsschutz für die Konfiguration	
Netzwerkkopplung mit N-N-Mapping	89	nach geprüfter Nummer	63
		nach Nummer	63
W			
WAN	259		
Warteschlangen	187		
gesicherte Queue	188		
Standard-Queue	188		
Urgent Queue II	187		
Urgent-Queue I	187		
WEBconfig	13, 19, 259		
HTTPS	19		
WECA	259		
WEP	259		
Wiederholungen	106		
WiFi	259		
WiFi-Alliance	259		
Wildcards	239		
Windows-Netz	231		
WINS-Konfiguration	231		
WISP	259		