



. . . c o n n e c t i n g y o u r b u s i n e s s

LANCOM 821+

LANCOM 1711+ VPN

LANCOM 1721 VPN

- Handbuch
- Manual

LANCOM 821+
LANCOM 1711+ VPN
LANCOM 1721 VPN

© 2008 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 Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM Systems-Logo, LCOS und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

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

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

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Januar 2009

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem LANCOM Router haben Sie sich für einen leistungsfähigen Router entschieden, der serienmäßig sowohl über integrierte DSL- bzw. ADSL- sowie ISDN-Schnittstellen als auch über einen 4-Port-Switch verfügt. Mit diesem Router schließen Sie einen einzelnen Arbeitsplatzrechner oder ein ganzes lokales Netzwerk einfach und komfortabel ans Highspeed-Internet an.

Modellvarianten

Das vorliegende Benutzerhandbuch gilt für die folgenden Modelle der LANCOM Router-Serie:

- LANCOM 821+
- LANCOM 1711+ VPN
- LANCOM 1721 VPN

Modell-
Einschränkungen

Die Teile der Dokumentation, die nur für ein bestimmtes Modell gelten, sind entweder im Text selbst oder durch entsprechende seitliche Hinweise gekennzeichnet.

In den anderen Teilen der Dokumentation werden alle beschriebenen Modelle unter dem Sammelbegriff LANCOM Router zusammengefasst.

Sicherheitseinstellungen

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

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.

Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Referenzhandbuch

■ Ein Wort vorab

Sie lesen derzeit das Benutzerhandbuch. Es enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Das Referenzhandbuch befindet sich als Acrobat-Dokument (PDF-Datei) unter www.lancom.de/download oder auf der beiliegenden Produkt-CD. 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)
- Backup-Lösungen
- LANCAPI
- weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

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. Telefon-

nummern 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.

Inhalt

| | |
|--|-----------|
| 1 Einleitung | 9 |
| 1.1 Wie funktionieren ADSL und ADSL 2+? | 9 |
| 1.2 Welchen Nutzen bietet VPN? | 10 |
| 1.3 Was kann Ihr LANCOM? | 11 |
| 2 Installation | 15 |
| 2.1 Lieferumfang | 15 |
| 2.2 Systemvoraussetzungen | 16 |
| 2.3 Statusanzeigen und Schnittstellen | 16 |
| 2.3.1 Statusanzeigen | 16 |
| 2.3.2 Die Anschlüsse des Geräts | 20 |
| 2.4 Installation der Hardware | 23 |
| 2.5 Installation der Software | 24 |
| 2.5.1 Software-Setup starten | 25 |
| 2.5.2 Welche Software installieren? | 25 |
| 3 Grundkonfiguration | 26 |
| 3.1 Welche Angaben sind notwendig? | 26 |
| 3.1.1 TCP/IP-Einstellungen | 26 |
| 3.1.2 Konfigurationsschutz | 28 |
| 3.1.3 Einstellungen für den DSL-Anschluss | 29 |
| 3.1.4 Einstellungen für den ISDN-Anschluss | 29 |
| 3.1.5 Gebührenschatz | 29 |
| 3.2 Anleitung für LANconfig | 30 |
| 3.3 Anleitung für WEBconfig | 31 |
| 3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs | 35 |
| 4 Den Internet-Zugang einrichten | 37 |
| 4.1 Der Internet-Assistent | 39 |
| 4.1.1 Anleitung für LANconfig | 39 |
| 4.1.2 Anleitung für WEBconfig | 40 |
| 4.2 Der Firewall-Assistent | 40 |
| 4.2.1 Assistent für LANconfig | 41 |
| 4.2.2 Konfiguration unter WEBconfig | 41 |

| | |
|---|-----------|
| 5 Zwei Netzwerke verbinden | 42 |
| 5.1 Welche Angaben sind notwendig? | 43 |
| 5.1.1 Allgemeine Angaben | 43 |
| 5.1.2 Einstellungen für den TCP/IP-Router | 45 |
| 5.1.3 Einstellungen für den IPX-Router | 47 |
| 5.1.4 Einstellungen für NetBIOS-Routing | 48 |
| 5.2 Anleitung für LANconfig | 48 |
| 5.3 1-Click-VPN für Netzwerke (Site-to-Site) | 49 |
| 5.4 Anleitung für WEBconfig | 51 |
| 6 Einwahl-Zugang bereitstellen | 52 |
| 6.1 Welche Angaben sind notwendig? | 53 |
| 6.1.1 Allgemeine Angaben | 53 |
| 6.1.2 Einstellungen für TCP/IP | 54 |
| 6.1.3 Einstellungen für IPX | 55 |
| 6.1.4 Einstellungen für NetBIOS-Routing | 56 |
| 6.2 Einstellungen am Einwahl-Rechner | 56 |
| 6.2.1 Einwahl über VPN | 56 |
| 6.2.2 Einwahl über ISDN | 56 |
| 6.3 Anleitung für LANconfig | 57 |
| 6.4 1-Click-VPN für LANCOM Advanced VPN Client | 57 |
| 6.5 Anleitung für WEBconfig | 59 |
| 7 Faxe versenden mit der LANCAPI | 60 |
| 7.1 Installation des LANCOM CAPI Faxmodem | 61 |
| 7.2 Installation des MS Windows Faxdienstes | 62 |
| 7.3 Versenden eines Faxes | 63 |
| 7.3.1 Faxe versenden mit beliebigen Büroanwendungen | 63 |
| 7.3.2 Faxe versenden mit dem Windows Faxdienst | 63 |
| 8 Sicherheits-Einstellungen | 65 |
| 8.1 Der Sicherheits-Assistent | 65 |
| 8.1.1 Assistent für LANconfig | 66 |
| 8.1.2 Assistent für WEBconfig | 66 |
| 8.2 Die Sicherheits-Checkliste | 67 |

| | |
|--|-----------|
| 9 Rat & Hilfe | 71 |
| 9.1 Es wird keine WAN-Verbindung aufgebaut | 71 |
| 9.2 DSL-Übertragung langsam | 71 |
| 9.3 Unerwünschte Verbindungen mit Windows XP | 72 |
| 9.4 Kabel testen | 72 |
| 10 Anhang | 74 |
| 10.1 Leistungs- und Kenndaten | 74 |
| 10.2 Anschlussbelegung | 75 |
| 10.2.1 WAN-Schnittstelle | 75 |
| 10.2.2 ADSL-Schnittstelle | 76 |
| 10.2.3 ISDN-S ₀ -Schnittstelle | 76 |
| 10.2.4 Ethernet-Schnittstellen 10/100Base-T | 77 |
| 10.2.5 Konfigurationsschnittstelle (Outband) | 77 |
| 10.3 CE-Konformitätserklärungen | 77 |
| 11 Index | 79 |

1 Einleitung

Die LANCOM Router-Modelle LANCOM 821+, LANCOM 1721 VPN und LANCOM 1711+ VPN sind vollwertige Router und ermöglichen mit der integrierte Firewall einen sicheren Internetzugang für das lokale Netzwerk.

Mit der integrierten oder nachträglich aktivierten VPN-Option arbeiten die Geräte LANCOM 1721 VPN und LANCOM 1711+ VPN als leistungsfähige Dynamic VPN Gateways für Außenstellen oder mobile Nutzer.

Neben dem DSL- oder ADSL-Anschluss verfügen die Geräte auch über einen ISDN-Anschluss. Die ISDN-Leitung kann als Backup für die DSL-Verbindung genutzt werden, zum Remote Management des Routers, als Basis für die Office-Kommunikation über die LANCAPI und zum Aufbau von Dynamic VPN Verbindungen zu Außenstellen mit dynamischen IP-Adressen.

In Verbindung mit den Voice-over-IP-Funktionen können die Geräte die breitbandigen Internetverbindungen auch zur Übertragen von Sprache nutzen.

1.1 Wie funktionieren ADSL und ADSL 2+?

ADSL (Asymmetric Digital Subscriber Line) ist die zur Zeit häufigste Anschlusstechnik für digitale Breitbandanschlüsse ins Internet. Bei den DSL-Technologien werden die normalen und ohnehin meist vorhandenen Telefonleitungen (analog oder ISDN) zur Datenübertragung bis zur nächsten Vermittlungsstelle verwendet. Ab der Vermittlungsstelle werden die Daten über Hochgeschwindigkeitsverbindungen im Internet weitergeleitet.

Die asymmetrische DSL-Variante ADSL wurde für Anwendungen entwickelt, bei denen der Teilnehmer große Datenmengen empfängt, selbst jedoch nur verhältnismäßig wenig Daten sendet, z.B. beim Surfen im WWW. Über eine ADSL-Verbindung kann der Teilnehmer bis zu 8 Mbit/Sekunde empfangen („downstream“) und 800 Kbit/Sekunde senden („upstream“). Diese Maximalraten können vom ADSL-Anbieter beliebig reduziert werden.

Um den stark steigenden Anforderungen nach höheren Bandbreiten gerecht zu werden, bieten die weiterentwickelten Standards ADSL 2 und ADSL 2+ höhere Datenraten an, die auch Anwendungen wie Videostreaming oder hochauflösendes Fernsehen (HDTV) über das Internet erlauben. Geräte mit ADSL 2-Unterstützung können je nach Angebot des Providers eine Downstreamrate von bis zu 12 Mbit/s erreichen, Geräte nach dem Standard ADSL 2+ bis zu 24 Mbit/s. Durch eine entsprechende Aushandlung beim Verbindungsaufbau sind die Standards ADSL, ADSL 2 und ADSL 2+ untereinander kompatibel.

Bei ADSL können parallel zur Datenübertragung auch alle klassischen Telefonie-Anwendungen (Telefon, Fax, Anrufbeantworter, Nebenstellenanlage) ohne Einschränkung weiter genutzt werden. Zu diesem Zweck kommen sogenannte „Splitter“ zum Einsatz, welche die „Sprachfrequenzen“ von den „Datenfrequenzen“ trennen.

1.2 Welchen Nutzen bietet VPN?

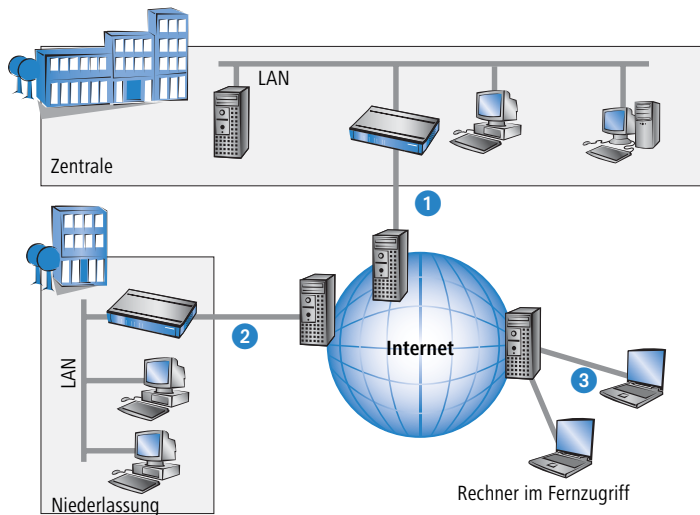
Nur für LANCOM
1711+ VPN und
LANCOM 1721 VPN

Mit einem VPN (**V**irtual **P**riate **N**etwork) können sichere Datenverkehrsverbindungen über das Internet aufgebaut werden.



Die Modelle LANCOM 1721 VPN und LANCOM 1711+ VPN sind standardmäßig mit VPN-Unterstützung für 5 aktive Tunnel ausgestattet. Mit der zusätzlichen LANCOM VPN Option kann die VPN-Unterstützung auf 25 aktive Tunnel erweitert werden (inkl. VPN-Hardware-Beschleunigung).

Bei Nutzung des Internets anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teuren, dedizierten Leitungen zwischen den Teilnehmern mehr.

- 1 Nur noch die Internet-Verbindung des LAN der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.
- 2 Die Niederlassung ist ebenfalls mit einer eigenen Verbindung an das Internet angeschlossen.
- 3 Die RAS-Rechner wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber herkömmlichen Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selbst nur einen Internetzugang. Die Zugangstechnologie spielt dabei keine Rolle: Idealerweise kommen Breitbandtechnologien wie DSL (Digital Subscriber Line) zum Einsatz. Aber auch herkömmliche ISDN-Verbindungen können verwendet werden.

Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

Niedrige Verbindungskosten und hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Übertragungsmedium für ein Unternehmensnetzwerk.

1.3 Was kann Ihr LANCOM?

Die folgende Tabelle zeigt Ihnen die Eigenschaften und Funktionen Ihres Gerätes im unmittelbaren Modellvergleich.

| | LANCOM 821+ | LANCOM 1711+ VPN | LANCOM 1721 VPN |
|----------------------------|----------------|---------------------|--------------------|
| Anwendungen | | | |
| Internet-Zugang | ✓ | ✓ | ✓ |
| LAN-LAN-Kopplung über VPN | | ✓ | ✓ |
| LAN-LAN-Kopplung über ISDN | ✓ | ✓ | ✓ |

■ Kapitel 1: Einleitung

DE

| | LANCOM 821+ | LANCOM 1711+ VPN | LANCOM 1721 VPN |
|--|----------------|---------------------|--------------------|
| RAS-Server (über VPN) | | ✓ | ✓ |
| RAS-Server (über ISDN) | ✓ | ✓ | ✓ |
| IP-Router mit Stateful Inspection Firewall | ✓ | ✓ | ✓ |
| IPX-Router (über ISDN), z.B. zur Kopplung von Novell-Netzwerken oder zur Einwahl in Novell-Netzwerke | ✓ | | ✓ |
| NetBIOS-Proxy zur Kopplung von Microsoft-Peer-to-Peer-Netzwerken über ISDN | ✓ | ✓ | ✓ |
| DHCP- und DNS-Server (für LAN und WAN) | ✓ | ✓ | ✓ |
| N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN | ✓ | ✓ | ✓ |
| Bridge-Funktion zur Verbindung von Netzwerken über ISDN | ✓ | ✓ | ✓ |
| Port-Mapping zur Definition von LAN-Ports als zusätzliche WAN-Ports | ✓ | ✓ | ✓ |
| Policy-based Routing zur regelbasierten Auswahl der Zielroute | ✓ | ✓ | ✓ |
| Load-Balancing zur Bündelung von mehreren DSL-Kanälen | 2 Kanäle | 4 Kanäle | 4 Kanäle |
| Backup-Lösungen und Load-Balancing mit VRRP | ✓ | ✓ | ✓ |
| NAT Traversal (NAT-T) | ✓ | ✓ | ✓ |
| DMZ mit konfigurierbarer IDS-Prüfung | ✓ | ✓ | ✓ |
| PPPoE-Server | ✓ | ✓ | ✓ |
| WAN-RIP | ✓ | ✓ | ✓ |
| Spanning-Tree-Protokoll | ✓ | ✓ | ✓ |
| Layer-2-QoS-Tagging | ✓ | ✓ | ✓ |
| ISDN-Festverbindungen | ✓ | ✓ | ✓ |
| LANCAPI-Server für den Einsatz von Office-Anwendungen wie Fax oder Anrufbeantworter über die ISDN-Schnittstelle. | ✓ | ✓ | ✓ |
| WAN-Anschlüsse | | | |
| Anschluss für DSL- oder Kabelmodem | ✓ | ✓ | ✓ |
| integriertes ADSL-Modem (ADSL2+ ready) | ✓ | | ✓ |

| | LANCOM 821+ | LANCOM 1711+ VPN | LANCOM 1721 VPN |
|--|----------------|---------------------|--------------------|
| ISDN-S ₀ -Anschluss in Punkt-zu-Mehrpunkt-Konfiguration (Mehrgeräteanschluss) oder in Punkt-zu-Punkt-Konfiguration (Anlagenanschluss) mit automatischer D-Kanal-Protokoll-Erkennung. Unterstützt statische und dynamische Kanalbündelung per MLPPP und BACP sowie Stac-Datenkompression (Hi/fn). Auch zum Aufbau von Dynamic VPN-Verbindungen zu Gegenstellen mit dynamischen IP-Adressen (LANCOM 1711+ VPN und LANCOM 1721 VPN). | ✓ | ✓ | ✓ |
| Anschluss für externes Analog- oder GPRS-Modem am COM-Port (benötigt LANCOM Modem Adapter Kit) | ✓ | ✓ | ✓ |
| LAN-Anschluss | | | |
| 4 individuelle Fast Ethernet LAN Ports, einzeln schaltbar, z.B. als LAN-Switch oder separate DMZ-Ports, Auto-Crossover. | ✓ | ✓ | ✓ |
| USB-Anschluss | | | |
| USB 2.0 Host Port (Fullspeed: 12 Mbit/s) zum Anschluss eines USB-Druckers und für zukünftige Erweiterungen | | ✓ | ✓ |
| Sicherheitsfunktionen | | | |
| IPSec-Verschlüsselung über externe Software (VPN-Client) | | ✓ | ✓ |
| 5 integrierte VPN-Tunnel zur Absicherung von Netzwerkverbindungen | | ✓ | ✓ |
| IPSec-Verschlüsselung über Hardware (optional, Aktivierung über VPN-25-Option) | | ✓ | ✓ |
| IP-Masquerading (NAT, PAT) zum Verstecken aller Arbeitsstationen im LAN hinter einer einheitlichen öffentlichen IP-Adresse. | ✓ | ✓ | ✓ |
| Stateful-Inspection Firewall | ✓ | ✓ | ✓ |
| Firewall-Filter zur gezielten Sperrung von IP-Adressen, Protokollen und Ports | ✓ | ✓ | ✓ |
| MAC-Adressfilter kontrolliert u.a. den Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion | ✓ | ✓ | ✓ |
| Konfigurationsschutz zur Abwehr von „Brute-Force-Angriffen“. | ✓ | ✓ | ✓ |
| Konfiguration | | | |
| Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion | ✓ | ✓ | ✓ |
| Fernkonfiguration über ISDN (mit ISDN-PPP-Verbindungen z. B. über das DFÜ-Netzwerk von Windows). | ✓ | ✓ | ✓ |
| Serielle Konfigurations-Schnittstelle | ✓ | ✓ | ✓ |
| Rückruf-Funktion mit PPP-Authentifizierung-Mechanismen zur Beschränkung auf festgelegte ISDN-Rufnummern | ✓ | ✓ | ✓ |

■ Kapitel 1: Einleitung

| | LANCOM 821+ | LANCOM 1711+ VPN | LANCOM 1721 VPN |
|--|----------------|---------------------|--------------------|
| FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko | ✓ | ✓ | ✓ |
| Optionale Software-Erweiterungen | | | |
| LANCOM VPN Option mit 25 aktiven Tunneln zur Absicherung von Netzwerkkopplungen | | ✓ | ✓ |
| LANCOM Service-Option | ✓ | ✓ | ✓ |
| Optionale Hardware-Erweiterungen | | | |
| LANCOM Modem Adapter Kit zum Anschluss eines Analog- oder GSM-Modems an die serielle Schnittstelle | ✓ | ✓ | ✓ |

2 Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben dem eigentlichen Gerät sollte der Karton folgendes Zubehör für Sie bereithalten:

| | LANCOM 821+ | LANCOM 1721 VPN | LANCOM 1711+ VPN |
|--|-------------|-----------------|------------------|
| Netzteil | ✓ | ✓ | ✓ |
| LAN-Anschlusskabel (grüne Stecker) | ✓ | ✓ | ✓ |
| WAN-Anschlusskabel (dunkelblaue Stecker) | | ✓ | |
| ADSL-Anschlusskabel (transparente Stecker) | ✓ | | ✓ |
| ISDN-Anschlusskabel (hellblaue Stecker) | ✓ | ✓ | ✓ |
| Anschlusskabel für die Konfigurationsschnittstelle | ✓ | ✓ | ✓ |
| LANCOM-CD | ✓ | ✓ | ✓ |
| Gedruckte Dokumentation | ✓ | ✓ | ✓ |

Falls etwas fehlen sollte, wenden Sie sich bitte umgehend an Ihren Händler oder an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

2.2 Systemvoraussetzungen

Rechner, die mit einem LANCOM in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Betriebssystem mit TCP/IP-Unterstützung, z.B. Windows Vista™, Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Linux, BSD Unix, Apple Mac OS, OS/2.
- Zugang zum LAN über das TCP/IP-Protokoll.



Die LANtools benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser unter einem beliebigen Betriebssystem erforderlich.

2.3 Statusanzeigen und Schnittstellen

2.3.1 Statusanzeigen

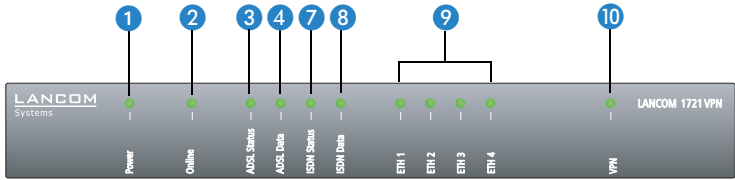
Bedeutung der LEDs

In den folgenden Abschnitten verwenden wir verschiedene Begriffe, um das Verhalten der LEDs zu beschreiben:

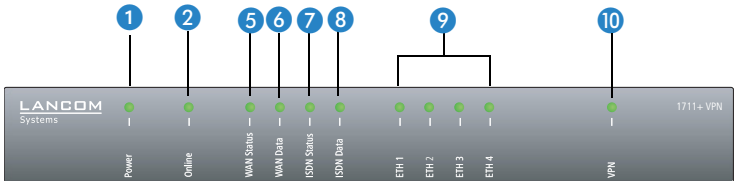
- **Blinken** bedeutet, dass die LED in gleichmäßigen Abständen in der jeweils angegebenen Farbe ein- bzw. ausgeschaltet wird.
- **Blitzen** bedeutet, dass die LED in der jeweiligen Farbe sehr kurz aufleuchtet und dann deutlich länger (etwa 10x so lange) ausgeschaltet bleibt.
- **Invers Blitzen** bedeutet das Gegenteil. Hier leuchtet die LED in der jeweiligen Farbe dauerhaft und wird nur sehr kurz unterbrochen.
- **Flackern** bedeutet, dass die LED in unregelmäßigen Abständen ein- und ausgeschaltet wird.

Vorderseite

Die verschiedenen LANCOM Router-Modelle verfügen je nach Funktionsumfang über eine unterschiedliche Anzahl von Statusanzeigen auf der Vorderseite:

LANCOM 821+und
LANCOM 1721 VPN

LANCOM 1711+ VPN



DE

Oberseite

Die beiden LEDs auf der Oberseite ermöglichen ein bequemes Ablesen der wichtigsten Statusanzeigen auch bei vertikaler Befestigung des Gerätes.



1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Gerätes.

| | | |
|----------|----------------------|---|
| aus | | Gerät abgeschaltet |
| grün | blinkend | Selbsttest nach dem Einschalten |
| grün | dauerhaft an | Gerät betriebsbereit |
| rot/grün | abwechselnd blinkend | Gerät unsicher: Kein Konfigurationskennwort gesetzt |
| rot | blinkend | Zeit- oder Gebührenlimit für Online-Verbindungen erreicht |



Die Power-LED blinkt abwechselnd rot/grün, solange noch kein Konfigurationskennwort gesetzt wurde. Ohne Konfigurationskennwort sind die Konfigurationsdaten des LANCOM ungeschützt. Im Normal-

fall setzen Sie ein Konfigurationskennwort während der Grundkonfiguration (Anleitung im folgenden Kapitel). Informationen zur nachträglichen Vergabe eines Konfigurationskennworts finden Sie im Abschnitt 'Der Sicherheits-Assistent'.

Blinkende Power-LED und keine Verbindung möglich?

Blinkt die Power-LED rot und können keine WAN-Verbindungen mehr aufgebaut werden, so ist das kein Grund zur Besorgnis. Vielmehr wurde ein vorher eingestelltes Zeit- oder Gebührenlimit erreicht.



Signal für ein erreichtes Zeit- oder Gebührenlimit

Es gibt drei Möglichkeiten die Sperre zu lösen:

- Gebührenschatz zurücksetzen.
- Das erreichte Limit erhöhen.
- Die erreichte Sperre ganz deaktivieren (Limit auf '0' setzen).

Im LANmonitor wird Ihnen das Erreichen eines Zeit- oder Gebührenlimits angezeigt. Zum Reset des Gebührenschatzes wählen Sie im Kontextmenü (rechter Mausklick) **Zeit- und Gebührenlimits zurücksetzen**. Die Gebühreneinstellungen legen Sie in LANconfig unter **Management ► Kosten** fest (Sie können nur dann auf diese Einstellungen zugreifen, wenn unter **Extras ► Optionen** die 'Vollständige Darstellung der Konfiguration' aktiviert ist).

Mit WEBconfig finden Sie den Gebührenschatz-Reset und alle Parameter unter **Experten-Konfiguration ► Setup ► Gebühren-Modul**.

2 Online

Die Online-LED zeigt allgemein den Status aller WAN-Schnittstellen an:

| | | |
|------|-----------------|---|
| aus | | keine aktive Verbindung |
| grün | blitzend | Aufbau der ersten Verbindung |
| grün | invers blitzend | Aufbau einer weiteren Verbindung |
| grün | dauerhaft an | mindestens eine Verbindung aufgebaut |
| rot | dauerhaft an | Fehler beim Aufbau der letzten Verbindung |

3 ADSL Status (nur LANCOM 821+ und LANCOM 1721 VPN)

Informationen über den Verbindungszustand am ADSL-Anschluss:

| | | |
|------|-------------------|-----------------------------|
| aus | | Interface abgeschaltet |
| grün | blinkend/blitzend | Handshake/Trainingsphase |
| grün | dauerhaft | Synchronisation erfolgreich |

| | | |
|----------------|--------------|---|
| rot | flackernd | Fehler (CRC-Fehler, Framing-Fehler etc.) |
| rot | dauerhaft an | Keine Synchronisation bzw. Suchen der Gegenstelle |
| rot/ orange | blinkend | Hardware-Fehler |

- 4 ADSL Data
(nur LANCOM
821+ und
LANCOM
1721 VPN)

Informationen über den Datenverkehr am ADSL-Anschluss:

| | | |
|------|------------------|---|
| aus | | keine logische Verbindung |
| grün | blitzend | Aufbau der ersten Verbindung |
| grün | invers blitzend | Aufbau der zweiten Verbindung |
| grün | dauerhaft an | Verbindung über einen B-Kanal aufgebaut |
| grün | invers flackernd | Datenverkehr (Versand oder Empfang) |

- 5 WAN Status
(nur LANCOM
1711+ VPN)

Verbindungszustand am WAN-Anschluss:

| | | |
|------|-----------------|---|
| aus | | keine logische Verbindung |
| grün | blitzend | Aufbau der ersten Verbindung |
| grün | invers blitzend | Aufbau einer weiteren Verbindung |
| grün | dauerhaft an | mindestens eine logische Verbindung aufgebaut |
| rot | dauerhaft an | Fehler im Verbindungsaufbau |

- 6 WAN Data
(nur LANCOM
1711+ VPN)

Anzeige von Datenverkehr am WAN-Anschluss:

| | | |
|------|--------------|-------------------------------------|
| aus | | keine physikalische Verbindung |
| grün | dauerhaft an | physikalische Verbindung aufgebaut |
| grün | flackernd | Datenverkehr (Versand oder Empfang) |

- 7 ISDN Status

Informationen über den Verbindungsstatus am ISDN-S₀-Anschluss:

| | | |
|------|--------------|---|
| aus | | nicht angeschlossen oder keine S ₀ -Spannung (keine Fehlermeldung) |
| grün | blinkend | Initialisierung D-Kanal (Kontaktaufnahme mit Verbindungsstelle) |
| grün | dauerhaft an | D-Kanal betriebsbereit |
| rot | flackernd | Fehler auf dem D-Kanal |
| rot | dauerhaft an | D-Kanal-Aktivierung fehlgeschlagen |



Wenn die ISDN-Status-LED automatisch erlischt, so ist dies kein Zeichen für einen Fehler am S_0 -Bus. Vielmehr schalten zahlreiche ISDN-Anschlüsse und Telefonanlagen den S_0 -Bus nach einer bestimmten inaktiven Zeit in einen Stromsparmodus. Bei Bedarf wird der S_0 -Bus automatisch reaktiviert und die ISDN-Status-LED leuchtet grün.

8 ISDN Data

Gemeinsame Information über den Datenverkehr auf beiden ISDN-B-Kanälen:

| | | |
|------|------------------|---|
| aus | | keine Verbindung aufgebaut |
| grün | blinkend | Anwahl läuft |
| grün | blitzend | Aufbau der ersten Verbindung |
| grün | invers blitzend | Aufbau der zweiten Verbindung |
| grün | dauerhaft an | Verbindung über einen B-Kanal aufgebaut |
| grün | invers flackernd | Datenverkehr (Versand oder Empfang) |

9 ETH

Zustand der LAN-Anschlüsse im integrierten Switch:

| | | |
|------|--------------|---|
| aus | | kein Netzwerkgerät angeschlossen |
| grün | dauerhaft an | Verbindung zu Netzwerkgerät betriebsbereit, kein Datenverkehr |
| grün | flackernd | Datenverkehr |
| rot | flackernd | Kollision von Datenpaketen |

10 VPN
(nur LANCOM
1721 VPN und
LANCOM
1711+ VPN)

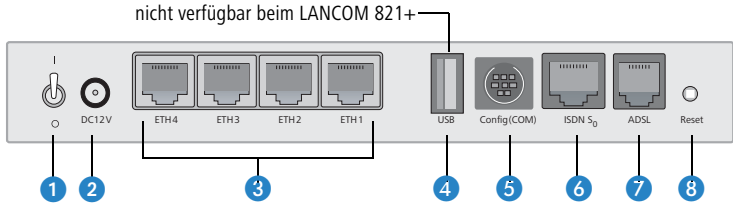
Status einer VPN-Verbindung.

| | | |
|------|-----------------|---------------------------|
| aus | | kein VPN-Tunnel aufgebaut |
| grün | blinkend | Verbindungsaufbau |
| grün | blitzend | erste Verbindung |
| grün | invers blitzend | weitere Verbindungen |
| grün | dauerhaft an | VPN-Tunnel sind aufgebaut |

2.3.2 Die Anschlüsse des Geräts

Auf der Rückseite befinden sich die Anschlüsse und Schalter des Routers:

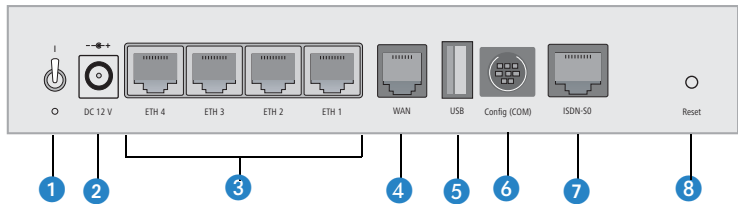
LANCOM 821+ und
LANCOM 1721 VPN



- 1 Netzschalter
- 2 Anschluss für das mitgelieferte Netzteil
- 3 Switch mit vier 10/100Base-Tx-Anschlüssen
- 4 USB-Anschluss
- 5 Serielle Konfigurationsschnittstelle
- 6 ISDN/S₀-Anschluss
- 7 ADSL-Anschluss
- 8 Reset-Schalter

Nur LANCOM 1721
VPN

LANCOM 1711+
VPN



- 1 Netzschalter
- 2 Anschluss für das mitgelieferte Netzteil
- 3 Switch mit vier 10/100Base-Tx-Anschlüssen
- 4 WAN-Anschluss
- 5 USB-Anschluss
- 6 Serielle Konfigurationsschnittstelle
- 7 ISDN/S₀-Anschluss
- 8 Reset-Schalter

Der Reset-Schalter hat zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:

- **Neustart des Geräts** (weicher Reset) – der Schalter wird kürzer als 5 Sekunden gedrückt. Das Gerät startet neu.
- **Zurücksetzen der Konfiguration** (harter Reset) – der Schalter wird länger als 5 Sekunden gedrückt. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Reset-Schalter freigegeben wird startet das Gerät mit Werkseinstellungen neu.

Die Funktion des Reset-Tasters

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Tasters gesteuert werden:

| Konfigurationstool | Aufruf |
|--------------------|---|
| WEBconfig, Telnet | Experten-Konfiguration > Setup > Config |

■ Reset-Taster

Mit dieser Option wird das Verhalten des Reset-Tasters gesteuert:

- Ignorieren: Der Taster wird ignoriert.
- Nur-Booten: Beim Druck auf den Taster wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.



Bitte beachten Sie folgenden Hinweis: Mit der Einstellung 'Ignorieren' oder 'Nur-Booten' wird das Zurücksetzen der Konfiguration auf den Auslieferungszustand durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort nicht mehr vorliegt, gibt es keine Möglichkeit mehr, auf das Gerät zuzugreifen! In diesem Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden – dabei wird das Gerät in den Auslieferungszustand zurückgesetzt, und die bisherige Konfiguration wird gelöscht. Hinweise zum Firmware-Upload über die serielle Konfigurationsschnittstelle finden Sie im LCOS-Referenzhandbuch.

- **Reset-oder-Booten (Standardeinstellung):** Ein kurzer Druck auf den Taster führt zum Neustart, ein Druck von 5 Sekunden oder länger führt zum Neustart mit dem Zurücksetzen der Konfiguration auf den Auslieferungszustand. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Taster freigegeben wird, startet das Gerät mit Werkseinstellungen neu.



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

2.4 Installation der Hardware

Die Installation des LANCOM Router erfolgt in folgenden Schritten:

- ① **LAN** – schließen Sie Ihren LANCOM Router zunächst ans LAN oder einen einzelnen PC an. Stecken Sie das mitgelieferte Netzwerkkabel (grüne Stecker) einerseits in einen LAN-Anschluss des Geräts ③ und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes, eine freie Buchse eines Switches/Hubs oder den Netzwerkeingang eines einzelnen PC.

Die LAN-Anschlüsse erkennen sowohl die Übertragungsrate (10/100 Mbit) als auch den Typ (Node/Hub) angeschlossener Netzwerkgeräte automatisch (Autosensing). Der parallele Anschluss von Geräten unterschiedlicher Geschwindigkeit und Typen ist möglich.



In einem Netzwerksegment sollten sich niemals mehrere unkonfigurierte LANCOM gleichzeitig befinden. Alle unkonfigurierten LANCOM melden sich unter derselben IP-Adresse (mit den Endziffern '254'), es kommt daher zu Adresskonflikten. Zur Vermeidung von Problemen sollten mehrere LANCOM immer nacheinander konfiguriert und jeweils sofort mit einer eindeutigen IP-Adresse (die nicht auf '254' endet) versehen werden.

nur LANCOM 821+/
LANCOM 1721 VPN

- ② **ADSL** – verbinden Sie die ADSL-Schnittstelle ⑦ über das mitgelieferte ADSL-Anschlusskabel (transparente Stecker) mit dem Splitter.

nur LANCOM
1711+ VPN

- ③ **DSL** – verbinden Sie die WAN-Schnittstelle ④ über das mitgelieferte DSL-Anschlusskabel (dunkelblaue Stecker) mit dem ADSL-Modem.

- ④ **ISDN** – für den Anschluss des LANCOM Router an das ISDN stecken Sie das eine Ende des mitgelieferten ISDN-Anschlusskabels (hellblaue Ste-

cker) in die ISDN/S₀-Schnittstelle ⑥ (LANCOM 821+ und LANCOM 1721 VPN) bzw. ⑦ (LANCOM 1711+ VPN) des Routers und das andere Ende in einen ISDN/S₀-Anlagenanschluss oder -Mehrgeräteanschluss.

- ⑤ **Konfigurations-Schnittstelle** – optional können Sie den Router direkt an die serielle Schnittstelle (RS-232, V.24) eines PC anschließen. Verwenden Sie dazu das mitgelieferte Anschlusskabel. Verbinden Sie die Konfigurations-Schnittstelle des LANCOM ⑤ (LANCOM 821+ und LANCOM 1721 VPN) bzw. ⑥ (LANCOM 1711+ VPN) mit einer freien seriellen Schnittstelle des PC.
- ⑥ Schließen Sie optional ein externes Analog- oder GRPS-Modem über das LANCOM Modem Adapter Kit an die serielle Schnittstelle des Geräts an, wenn Sie über einen zusätzlichen WAN-Zugang Aufgaben wie Fernwartung, Backup-Verbindungen oder Dynamic VPN realisieren wollen.
- ⑦ **Mit Spannung versorgen** – versorgen Sie das Gerät an Buchse ② über das mitgelieferte Netzteil mit Spannung.



Verwenden Sie ausschließlich das mitgelieferte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

- ⑧ **Betriebsbereit?** – Nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent. Grün leuchtende LAN-LEDs zeigen an, an welchen LAN-Anschlüssen funktionierende Verbindungen hergestellt sind.



Die Geräte mit integriertem ADSL-Modem können im Betrieb recht warm werden. Bei diesen Modellen ist insbesondere der Umgebungstemperaturbereich von max. 35°C zu beachten. Für eine ausreichende Belüftung ist zu sorgen. Geräte nicht stapeln und keiner direkten Sonneneinstrahlung aussetzen!

2.5 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten Systemsoftware LANtools, die unter Windows läuft.



Sollten Sie Ihren LANCOM VPN Router ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen.

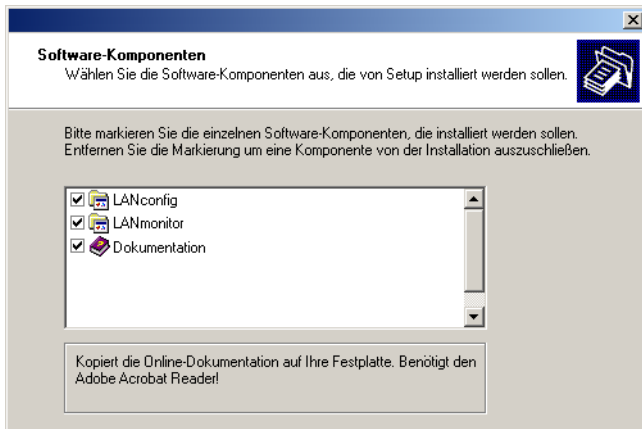
2.5.1 Software-Setup starten

Legen Sie die Produkt-CD in Ihr Laufwerk ein. Daraufhin startet das Setup-Programm automatisch.



Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis der LANCOM-CD auf.

Klicken Sie im Setup auf **Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:



2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM Router und LANCOM Access Points. Alternativ (oder ergänzend) kann über einen Web-Browser WEBconfig verwendet werden.
- Mit **LANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM Router und LANCOM Access Points.
- Mit **Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

3 Grundkonfiguration

Die Grundkonfiguration erfolgt mit Hilfe eines komfortablen Setup-Assistenten, der Sie Schritt für Schritt durch die Konfiguration führt und dabei die notwendigen Informationen abfragt.

Dieses Kapitel zeigt Ihnen zunächst, welche Angaben für die Grundkonfiguration erforderlich sind. Mit Hilfe dieses ersten Abschnitts stellen Sie sich schon vor Aufruf des Assistenten alle notwendigen Daten zusammen.

Anschließend erfolgt die Eingabe der Daten im Setup-Assistenten. Aufruf und Ablauf werden Schritt für Schritt beschrieben – in jeweils einem eigenen Abschnitt für LANconfig und WEBconfig. Dank der vorherigen Zusammenstellung aller notwendigen Angaben gelingt die Grundkonfiguration jetzt schnell und ohne Mühe.

Zum Abschluss dieses Kapitels zeigen wir Ihnen, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind, damit der Zugriff auf das Gerät einwandfrei funktioniert.

3.1 Welche Angaben sind notwendig?

Der Grundkonfigurations-Assistent nimmt die TCP/IP-Grundeinstellung des LANCOM VPN Routers vor und schützt das Gerät mit einem Konfigurationskennwort. Die folgende Beschreibung der vom Assistenten geforderten Angaben gliedert sich in die folgenden Konfigurationsabschnitte:

- TCP/IP-Einstellungen
- Schutz der Konfiguration
- Angaben zum ISDN-Anschluss
- Einstellung des Gebührenschatzes
- Sicherheitseinstellungen

3.1.1 TCP/IP-Einstellungen

Die TCP/IP-Konfiguration kann auf zweierlei Art erfolgen: Entweder vollautomatisch oder manuell. Bei der vollautomatischen TCP/IP-Konfiguration ist keine Benutzereingabe erforderlich. Alle Parameter werden selbstständig vom Setup-Assistenten gesetzt. Bei der manuellen TCP/IP-Konfiguration fragt der Assistent die üblichen TCP/IP-Parameter ab: IP-Adresse, Netzmaske etc. (dazu später mehr).

Die vollautomatische TCP/IP-Konfiguration ist nur in bestimmten Netzwerkumgebungen möglich. Deshalb analysiert der Setup-Assistent das ange-

geschlossene LAN daraufhin, ob die vollautomatische Konfiguration möglich ist oder nicht.

Neues LAN – vollautomatische Konfiguration möglich

Sind alle angeschlossenen Netzwerkgeräte noch unkonfiguriert, dann bietet der Setup-Assistent die vollautomatische TCP/IP-Konfiguration an. Dazu kommt es normalerweise in folgenden Situationen:

- Nur ein Einzelplatz-PC wird an den LANCOM VPN Router angeschlossen
- Neuaufbau eines Netzwerks

Wenn Sie den LANCOM VPN Router in ein bestehendes TCP/IP-LAN integrieren, wird die vollautomatische TCP/IP-Konfiguration nicht angeboten. In diesem Fall können Sie mit dem Abschnitt 'Notwendige Angaben für die manuelle TCP/IP-Konfiguration' fortfahren.

Das Ergebnis der vollautomatischen TCP/IP-Konfiguration: Der LANCOM VPN Router erhält die IP-Adresse '172.23.56.254' (Netzmaske '255.255.255.0'). Außerdem wird der integrierte DHCP-Server aktiviert, so dass der LANCOM VPN Router den Geräten im LAN automatisch IP-Adressen zuweist.

Trotzdem manuell konfigurieren?

Die vollautomatische TCP/IP-Konfiguration ist optional. Sie können stattdessen auch die manuelle Konfiguration wählen. Treffen Sie diese Wahl nach folgenden Überlegungen:

- Wählen Sie die automatische Konfiguration wenn Sie mit Netzwerken und IP-Adressen **nicht** vertraut sind.
- Wählen Sie die manuelle TCP/IP-Konfiguration, wenn Sie mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:
 - Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den Router selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adressbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adressbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server aktiviert wird).
 - Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet.

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

Bei der manuellen TCP/IP-Konfiguration fragt Sie der Setup-Assistent nach folgenden Daten:

■ DHCP-Betriebsart

- Aus: Die erforderlichen IP-Adressen müssen manuell eingetragen werden.
- Server: Der LANCOM VPN Router arbeitet als DHCP-Server im Netzwerk, zumindest die eigene IP-Adresse und die Netzmaske müssen angegeben werden.
- Client: Der LANCOM VPN Router bezieht als DHCP-Client die Adress-Informationen von einem anderen DHCP-Server, es müssen keine Adress-Informationen angegeben werden.

■ IP-Adresse und Netzwerkmaste für den LANCOM VPN Router

Teilen Sie dem LANCOM VPN Router eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaste an.

■ Gateway-Adresse

Geben Sie die IP-Adresse des Gateways an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des Gateways übernimmt.

■ DNS-Server

Geben Sie die IP-Adresse eines DNS-Servers zur Auflösung der Domain-Namen an, wenn Sie die DHCP-Betriebsart 'Aus' gewählt haben oder in der DHCP-Betriebsart 'Server' ein anderes Netzwerkgerät die Aufgabe des DNS-Servers übernimmt.

3.1.2 Konfigurationsschutz

Mit dem Kennwort schützen Sie den Konfigurationszugang zum LANCOM VPN Router und verhindern so, dass Unbefugte diese modifizieren. Die Konfiguration des Gerätes enthält zahlreiche sensible Daten, wie beispielsweise die Daten für den Internet-Zugang, und sollte auf jeden Fall durch ein Kennwort geschützt sein.



In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für einen LANCOM VPN Router können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im

LCOS-Referenzhandbuch unter „Rechteverwaltung für verschiedene Administratoren“.

3.1.3 Einstellungen für den DSL-Anschluss

Für den DSL-Anschluss kann die Angabe des verwendeten Übertragungsprotokolls erforderlich sein. Der Assistent nimmt die korrekte Einstellung für die wichtigsten DSL-Anbieter selbstständig vor. Nur wenn der Assistent Ihren Anbieter nicht aufführt, müssen Sie das von Ihrem DSL-Anbieter verwendete Übertragungsprotokoll angeben.

Der Assistent bietet Ihnen auch ein Universalprotokoll 'Multimode' an, das mit allen gängigen DSL-Anschlüssen funktioniert.

3.1.4 Einstellungen für den ISDN-Anschluss

Wenn Sie den ISDN-Anschluss verwenden möchten, können Sie folgende Einstellungen vornehmen:

- Eine oder mehrere ISDN-MSNs, an der der Router Anrufe entgegennehmen soll. MSNs sind ISDN-Rufnummern, die Ihnen vom Telefonanbieter zugewiesen werden. Sie werden normalerweise ohne Vorwahl angegeben. Die angegebenen Nummern haben nur für Router-Funktionen (LAN-LAN-Kopplung, RAS) Bedeutung, nicht jedoch für die Fernkonfiguration und LANCOM VPN Option.
- Eine Amtsvorwahl für den Zugang zum öffentlichen Netz. Sie ist normalerweise nur beim Anschluss an einer ISDN-Telefonanlage erforderlich. Üblich ist die '0'. Diese Amtsvorwahl wird für alle ausgehenden Rufe verwendet.
- Schließlich sollten Sie wissen, ob die Telefongesellschaft den ISDN-Gebührenimpuls übermittelt. Dieser kann vom LANCOM Router für Gebührenbudgets und die Accounting-Funktion ausgewertet werden.

3.1.5 Gebührenschatz

Der Gebührenschatz verhindert den Verbindungsaufbau von DSL-Verbindungen über ein vorher eingestelltes Maß hinaus und schützt Sie so vor unerwartet hohen Verbindungskosten.

Wenn Sie den LANCOM Router an einem DSL-Anschluss betreiben, der zeitbasiert abgerechnet wird, können Sie die maximale Verbindungszeit in Minuten festsetzen.

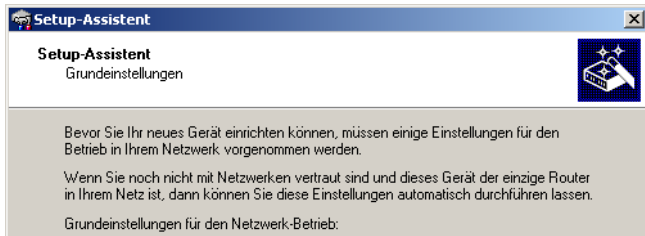
Das Budget kann durch Eingabe des Wertes '0' komplett deaktiviert werden.



In der Grundeinstellung ist der Gebährenschtutz auf maximal 600 Minuten innerhalb von sieben Tagen eingestellt. Passen Sie diese Einstellung an Ihre persönlichen Bedürfnisse an oder deaktivieren Sie den Gebährenschtutz, wenn Sie mit Ihrem Provider einen Pauschal-Tarif (Flatrate) vereinbart haben.

3.2 Anleitung für LANconfig

- ① Starten Sie LANconfig mit **Start ▶ Programme ▶ LANCOM ▶ LANconfig**. LANconfig erkennt neue LANCOM-Geräte im TCP/IP-Netz selbstständig.
- ② Wird bei der Suche ein unkonfiguriertes Gerät gefunden, startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen (die passende Netzwerkumgebung vorausgesetzt) sogar die gesamte Arbeit abnimmt.



Sollte der Setup-Assistent nicht automatisch starten, so suchen Sie manuell nach neuen Geräten an allen Schnittstellen (falls der LANCOM VPN Router über die serielle Konfigurationsschnittstelle angeschlossen ist) oder im Netzwerk (**Gerät ▶ Suchen**).




Sollte der Zugriff auf einen unkonfigurierten LANCOM VPN Router scheitern, so kann dieser Fehler auf die Netzmaske des LAN zurückzuführen sein: Bei weniger als 254 möglichen Hosts (Netzmaske > '255.255.255.0') muss sichergestellt sein, dass die IP-Adresse 'x.x.x.254' im eigenen Subnetz vorhanden ist.

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ⑤ fort.

- ③ Geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.


- ④ Im folgenden Fenster legen Sie zunächst das Kennwort für den Konfigurationszugriff fest. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

Ferner legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

-  Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff durch ein Kennwort abgesichert ist.

- ⑤ Der Gebührenschatz beschränkt auf Wunsch die Kosten von WAN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.

- ⑥ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

-  Im Abschnitt 'TCP/IP-Einstellungen an den Arbeitsplatz-PCs' erfahren Sie, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind.


3.3 Anleitung für WEBconfig

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. 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 Webbrowser gibt.

Sicher mit HTTPS

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

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

-  Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden. Unter Windows empfiehlt LANCOM Systems GmbH den aktuellen Internet Explorer.

Zugang zum Gerät mit WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich das Gerät ansprechen lässt. Das Verhalten der Geräte sowie ihre Erreichbarkeit zur Konfiguration über einen Webbrowser hängen davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen. Der Zugriff mit WEBconfig erfolgt 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.

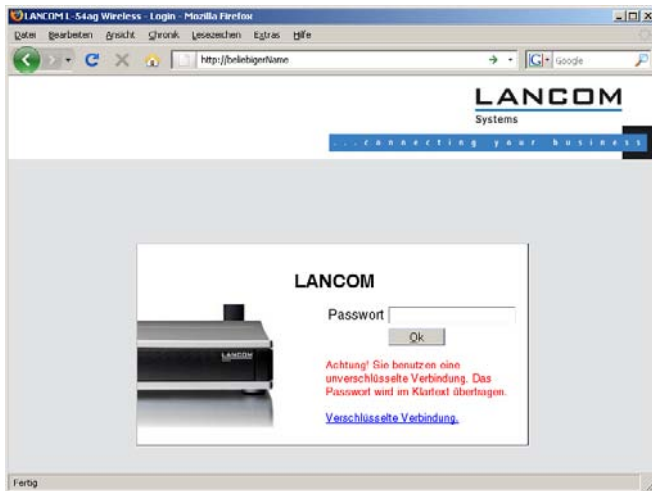
Nach dem Einschalten prüfen unkonfigurierte LANCOM-Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse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

Netz ohne DHCP-Server

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



Im werksseitigen Auslieferungszustand mit aktiviertem DHCP-Server leitet das Gerät alle eingehenden DNS-Anfragen an den internen Webserver weiter. Dadurch können unkonfigurierte LANCOMs einfach durch Eingabe eines beliebigen Names mittels eines Webbrowsers angesprochen und in Betrieb genommen werden.



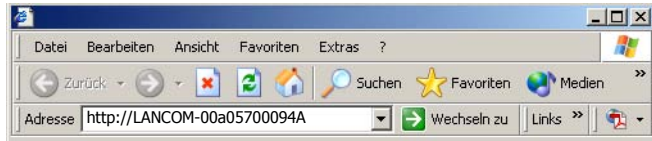
Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start ▶ Ausführen ▶ cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000, Windows XP oder Windows Vista, mit **Start ▶ Ausführen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

Netz mit DHCP-Server

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

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem

DHCP-Server aus, kann das Gerät unter dem Namen "LANCOM-<MAC-Adresse>" (z.B. "LANCOM-00a057xxxxx") erreicht werden.



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

- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
 - Sie nutzen die Funktion "Geräte suchen" in LANconfig oder die Gerätesuche unter WEBconfig von einem anderen erreichbaren LANCOM.
 - Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
 - Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschließen.

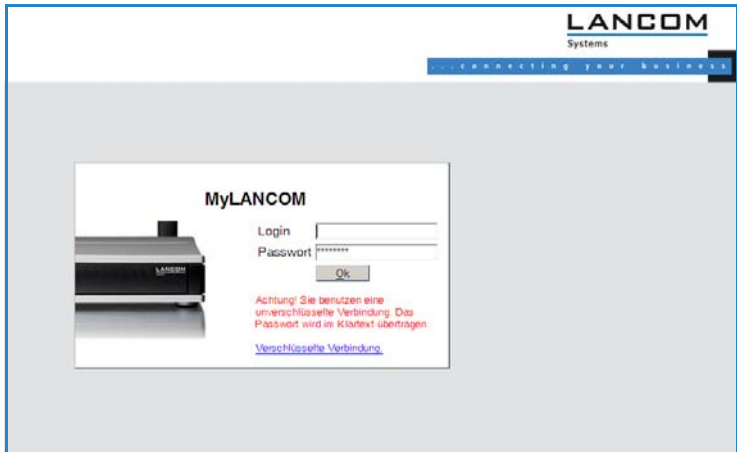
Login

Wenn Sie beim Zugriff auf das Gerät zur Eingabe von Benutzername und Kennwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

Falls Sie den allgemeinen Konfigurationszugang verwenden, tragen Sie nur das entsprechende Kennwort ein. Das Feld Benutzername bleibt in diesem Fall leer.

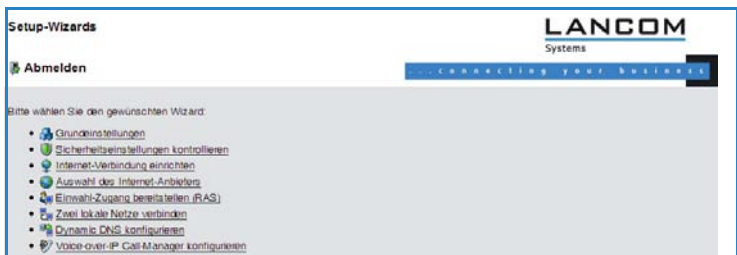


Der Login-Dialog bietet alternativ einen Link für eine verschlüsselte Verbindung über HTTPS. Nutzen Sie nach Möglichkeit immer die HTTPS-Verbindung mit erhöhter Sicherheit.



Setup Wizards

Mit den Setup-Wizards können Sie schnell und komfortabel die häufigsten Einstellungen für ein Gerät vornehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein.



Die Einstellungen werden erst dann in das Gerät gespeichert, wenn Sie die Eingaben auf der letzten Seite des Assistenten bestätigen.

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs

Bei TCP/IP-Netzwerken ist die korrekte Adressierung aller Geräte im LAN außerordentlich wichtig. Ferner sollten alle Rechner die IP-Adressen von zwei zentralen Stellen im LAN kennen:

- Standard-Gateway – erhält alle Pakete, die nicht an Rechner im lokalen Netz adressiert sind

- DNS-Server – übersetzt einen Netzwerk- oder Rechnernamen in eine konkrete IP-Adresse.

Der LANCOM VPN Router kann sowohl die Funktionen eines Standard-Gateways als auch die eines DNS-Servers übernehmen. Außerdem kann er als DHCP-Server allen Rechnern im LAN automatisch eine korrekte IP-Adresse zuweisen.

Die korrekte TCP/IP-Konfiguration der PC im LAN hängt entscheidend davon ab, nach welcher Methode im LAN die IP-Adressen vergeben werden:

- **IP-Adressvergabe über ein LANCOM**

In dieser Betriebsart weist ein LANCOM den PCs im LAN und WLAN (bei Geräten mit Funkmodul) nicht nur eine IP-Adresse zu, sondern übermittelt per DHCP auch seine eigene IP-Adresse als Standard-Gateway und DNS-Server. Die PCs sind deshalb so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen.

- **IP-Adressvergabe über einen separaten DHCP-Server**

Die Arbeitsplatz-PCs sind so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen. Auf dem DHCP-Server ist die IP-Adresse des LANCOMs so zu hinterlegen, dass der DHCP-Server sie an die PCs im LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den LANCOM als DNS-Server angeben.

- **Manuelle Zuweisung der IP-Adressen**

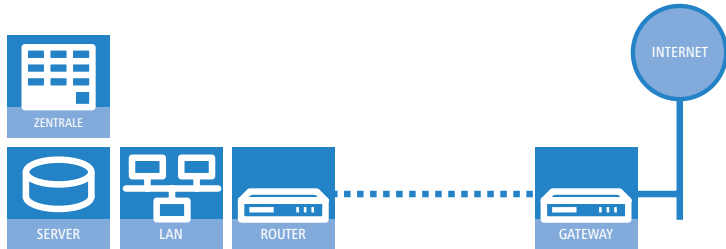
Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des LANCOMs als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.



Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres LANCOM VPN Routers finden Sie im Referenzhandbuch. Bei der Netzwerkkonfiguration der Arbeitsplatzrechner hilft Ihnen die Dokumentation des installierten Betriebssystems weiter.

4 Den Internet-Zugang einrichten

Über den zentralen Internet-Zugang des LANCOM erhalten alle Rechner im LAN Zugriff auf das Internet. Die Verbindung zum Internetanbieter kann über jeden WAN-Anschluss aufgebaut werden, also neben DSL auch über ISDN (sofern vorhanden). Ein Internet-Zugang über ISDN kann beispielsweise als Backup für DSL eingesetzt werden.



Welches WAN-Interface?

Die Einrichtung des Internet-Zugangs erfolgt über einen komfortablen Assistenten. Im ersten Schritt wählen Sie aus, über welches WAN-Interface die Internetverbindung aufgebaut werden soll.

Um eine Internetverbindung über das DSL-Interface aufzubauen, müssen Sie an einem der ETH-Ports des Gerätes ein externes ADSL-Modem anschließen. Bei der Konfiguration des Internetzugangs geben Sie an, an welchem ETH-Port das ADSL-Modem angeschlossen wird.

Kennt der Setup-Assistent Ihren Internet-Anbieter?

Der Assistent kennt die Zugangsdaten der wichtigsten Internetanbieter in ihrem Land und bietet Ihnen eine Liste zur Auswahl an. Wenn Sie Ihren Internetanbieter in dieser Liste finden, so müssen Sie für die Einrichtung des Internet-Zugangs normalerweise keine weiteren Übertragungs-Parameter eingeben. Lediglich die Authentifizierungsdaten, die Ihnen Ihr Internetanbieter zur Verfügung stellt, sind noch erforderlich.

Zusätzlich Angaben bei unbekanntem Internet-Anbieter

Kennt der Setup-Assistent Ihren Internet-Anbieter nicht, so fragt er Sie Schritt für Schritt alle notwendigen Zugangsdaten ab. Diese Zugangsdaten stellt Ihnen Ihr Internet-Anbieter zur Verfügung.

Weitere Verbindungsoptionen

Zusätzlich können Sie (sofern von Ihrem Internetanbieter unterstützt) zusätzliche Optionen im Assistenten ein- oder ausschalten:

- Zeitliche Abrechnung oder Flatrate – wählen Sie aus, nach welchem Modell Ihr Internetanbieter die Nutzung abrechnet.

- Bei der zeitlichen Abrechnung können Sie am LANCOM einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn für eine bestimmte Dauer (die sogenannte Haltezeit) keine Daten mehr übertragen wurden.

Zusätzlich können Sie eine Leitungsüberwachung aktivieren, die inaktive Gegenstellen schneller erkennt und in diesem Fall die Verbindung schon vor Ablauf der Haltezeit abbaut.

- Bei Flatrate-Abrechnung haben Sie ebenfalls die Möglichkeit der aktiven Leitungsüberwachung, und können so die Funktion der Gegenstelle ständig überprüfen.

Außerdem können Sie bei Flatrates Verbindungen dauerhaft aufrecht erhalten („Keep-alive“). Im Fall eines Verbindungsabbruchs wird diese automatisch wieder aufgebaut.

Backup-Verbindung zum Internet anlegen

Die Absicherung der Internetverbindung gehört zu den häufigsten Aufgaben der Backup-Lösungen. Bei der Einrichtung eines Internetzugangs haben Sie zusätzlich die Möglichkeit, eine zweite Verbindung zum Internet über ein alternatives WAN-Interface anzulegen. Haben Sie den Haupt-Internetzugang z. B. über das ADSL-Interface angelegt, können Sie die Backup-Verbindung über UMTS oder ISDN einrichten.

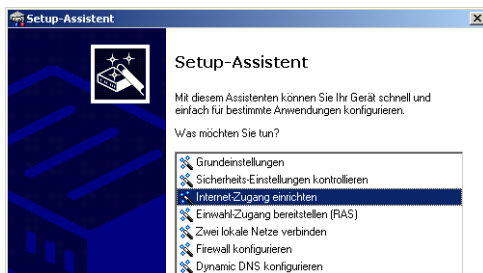


Bei der Konfiguration der Backup-Verbindung können Sie je nach Verfügbarkeit auch einen anderen Provider wählen. Damit überbrücken Sie nicht nur die physikalische Leitung, sondern auch generelle Störungen im Netz des Providers.

4.1 Der Internet-Assistent

4.1.1 Anleitung für LANconfig

- 1 Markieren Sie Ihr Gerät im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



- 2 Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- 4 Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.
- 5 Nach der Eingabe aller erforderlichen Daten bietet Ihnen der Assistent die Einrichtung einer Backup-Verbindung an. Wählen Sie dazu das WAN-Interface, über welches die Backup-Verbindung aufgebaut werden soll, und geben Sie die erforderlichen Zugangsdaten für den Internetzugang über dieses Interface ein.

Der Assistent richtet mit diesen Angaben den alternativen Internetzugang ein und erstellt gleichzeitig die erforderlichen Einträge in der Backup-Tabelle und in der PPP-Tabelle zur Überprüfung der Internetverbindung vor.

- !** Bitte beachten Sie, dass bei einem Backup über UMTS möglicherweise nicht alle Dienste wie auf der Haupt-Internetverbindung verfügbar sind. Manche UMTS-Dienstanbieter ermöglichen die Nutzung von VPN-Tunneln oder VoIP-Anwendungen über Mobilfunkverbindungen nur gegen zusätzliche Gebühren oder sperren diese ganz, andere Anbieter vergeben IP-Adressen aus einem privaten Adresskreis und behindern somit Anwendungen, die an eine öffentliche IP-Adresse

■ Kapitel 4: Den Internet-Zugang einrichten

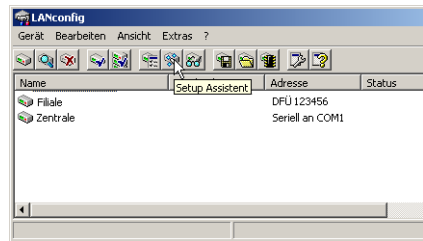
geknüpft sind. Bitte erkundigen Sie sich bei Ihrem UMTS-Anbieter über evtl. vorhandene Einschränkungen.

- ⑥ Der Assistent informiert Sie, sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

DE

LANconfig: Schneller Aufruf der Setup-Assistenten

Die Setup-Assistenten rufen Sie unter LANconfig am schnellsten über den Befehlsknopf in der Button-Leiste auf.



4.1.2 Anleitung für WEBconfig

- ① Wählen Sie im Hauptmenü **Internet-Zugang einrichten**.
- ② In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.
- ③ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.
- ④ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Weiter** ab.

4.2 Der Firewall-Assistent

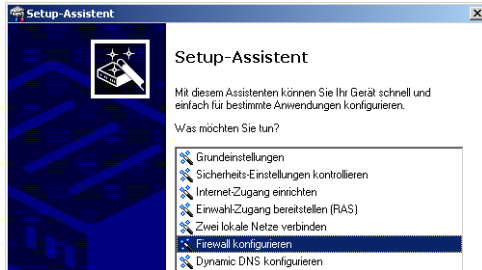
Ihr LANCOM verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres LAN gegenüber dem Internet. Kernidee der Stateful-Inspection-Firewall ist, dass nur selbstinitiiertes Datentransfer als zulässig betrachtet wird. Alle Zugriffe, die unaufgefordert nicht aus dem lokalen Netz heraus erfolgen, sind unzulässig.

Der Firewall-Assistent hilft Ihnen, schnell und komfortabel neue Regeln für die Firewall zu erstellen.

Nähere Informationen zur Firewall Ihres LANCOM und zu deren Konfiguration finden Sie im Referenzmanual.

4.2.1 Assistent für LANconfig

- 1 Markieren Sie Ihr LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



- 2 Wählen Sie im Auswahlménú den Setup-Assistenten **Firewall konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 In den folgenden Fenstern wählen Sie aus, auf welche Dienste/Protokolle sich die Regel bezieht. Im nächsten Schritt legen Sie fest, für welche Quell- und Zielstationen die Regel gilt und welche Aktionen ausgeführt werden sollen, wenn die Regel auf ein Datenpaket zutrifft.
- 4 Zum Abschluss geben Sie der neuen Regel einen Namen, aktivieren sie und legen fest, ob weitere Regeln beachtet werden sollen, wenn die Regel auf ein Datenpaket zutrifft.
- 5 Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

4.2.2 Konfiguration unter WEBconfig

Unter WEBconfig besteht die Möglichkeit, die Parameter zur Absicherung des Internet-Zugriffs unter **Konfiguration ▶ Firewall / QoS ▶ Regeln ▶ Regeltabelle** aufzurufen, die Einstellungen zu kontrollieren und zu ändern.

5 Zwei Netzwerke verbinden

Mit der Netzwerkkopplung (auch LAN-LAN-Kopplung) des LANCOM Router werden zwei lokale Netzwerke miteinander verbunden. Die LAN-LAN-Kopplung kann grundsätzlich auf zwei verschiedenen Wegen realisiert werden:

- **VPN:** Bei der Kopplung über VPN wird die Verbindung zwischen den beiden LANs über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. In beiden LANs wird dazu ein Router mit VPN-Unterstützung benötigt.
- **ISDN:** Bei der Kopplung über ISDN wird eine direkt Verbindung zwischen den beiden LANs über eine ISDN-Verbindung hergestellt. In beiden LANs wird ein dazu Router mit ISDN-Schnittstelle benötigt.

Die Einrichtung einer LAN-LAN-Kopplung erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Immer beide Seiten konfigurieren

Beide an der Netzwerkkopplung beteiligten Router müssen konfiguriert werden. Dabei ist darauf zu achten, dass die Konfigurationsangaben auf beiden Seiten zueinander passen.



Die folgende Anleitung geht davon aus, dass auf beiden Seiten LANCOM Router verwendet werden. Die Netzwerkkopplung ist zwar auch mit Routern anderer Hersteller möglich. Eine gemischte Konfiguration erfordert aber in aller Regel tiefer gehende Eingriffe an beiden Geräten. Ziehen Sie in einem solchen Fall das Referenzhandbuch zu Rate.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein. Ein LANCOM bietet daher eine ganze Reihe von Sicherheitsmechanismen an, bei deren Einsatz ein hervorragender Schutz gewährleistet ist:

- **VPN:** Bei Kopplungen über VPN werden die Daten mittels IPSec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt
- **ISDN:** Bei Kopplungen über ISDN sorgen das Kennwort für die Verbindung, die Überprüfung der ISDN-Nummer und die Rückruffunktion für die Sicherheit der Verbindung.



Die ISDN-Rückruffunktion kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

5.1 Welche Angaben sind notwendig?

Der Assistent fragt alle notwendigen Daten Schritt für Schritt ab. Nach Möglichkeit sollten Ihnen die erforderlichen Angaben schon vor Aufruf des Assistenten vorliegen.

Die Bedeutung aller Angaben, nach denen Sie der Assistent fragt, erklären wir Ihnen an Hand eines typischen Beispiels: der Kopplung einer Filiale an ihre Zentrale. Die beiden beteiligten Router tragen die Namen 'ZENTRALE' und 'FILIALE'.

Den folgenden Tabellen entnehmen Sie, welche Einträge an welchem der beiden Router vorzunehmen sind. Pfeile kennzeichnen die Abhängigkeiten zwischen den Einträgen.

5.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung einer LAN-LAN-Kopplung benötigt. Die erste Spalte zeigt jeweils an, ob die Information für eine Netzwerkkopplung über VPN (einfaches Verfahren mit „Preshared Keys“) und/oder über ISDN erforderlich ist.



Weitere Informationen zur Netzwerkkopplung über VPN-Verbindungen mit anderen Verfahren entnehmen Sie bitte dem LANCOM Referenzhandbuch.

| Kopplung | Angabe | Gateway 1 | | Gateway 2 |
|------------|--|--------------------|--|--------------------|
| VPN | Verfügt die Gegenstelle über einen ISDN-Anschluss? | Ja/Nein | | Ja/Nein |
| VPN | Typ der eigenen IP-Adresse | statisch/dynamisch | | statisch/dynamisch |
| VPN | Typ IP-Adresse der Gegenstelle | statisch/dynamisch | | statisch/dynamisch |
| VPN + ISDN | Name des eigenen Gerätes | 'ZENTRALE' | | 'FILIALE' |
| VPN + ISDN | Name der Gegenstelle | 'FILIALE' | | 'ZENTRALE' |
| VPN + ISDN | ISDN-Rufnummer Gegenstelle | (0123) 123456 | | (0789) 654321 |
| VPN + ISDN | ISDN-Anruferkennung Gegenstelle | (0789) 654321 | | (0123) 123456 |

DE
 Kapitel 5: Zwei Netzwerke verbinden

| Kopplung | Angabe | Gateway 1 | | Gateway 2 |
|------------|---|---------------|---|---------------|
| VPN + ISDN | Kennwort zur sicheren Übertragung der IP-Adresse | 'Geheim' | ↔ | 'Geheim' |
| VPN | Shared Secret für Verschlüsselung | 'Secret' | ↔ | 'Secret' |
| VPN | IP-Adresse der Gegenstelle | '10.0.2.100' | | '10.0.1.100' |
| VPN | IP-Netzadresse des entfernten Netzes | '10.0.2.0' | | '10.0.1.0' |
| VPN | Netzmaske des entfernten Netzwerks | 255.255.255.0 | | 255.255.255.0 |
| VPN | Dömnänenbezeichnung im entfernten Netzwerk | 'zentrale' | | 'filiale' |
| VPN | Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)? | Ja/Nein | | Ja/Nein |
| ISDN | TCP/IP-Routing für Zugriff auf entferntes Netz? | Ja/Nein | | Ja/Nein |
| ISDN | IPX-Routing für Zugriff auf entferntes Netz? | Ja/Nein | | Ja/Nein |
| VPN + ISDN | NetBIOS-Routing für Zugriff auf entferntes Netz? | Ja/Nein | | Ja/Nein |
| VPN + ISDN | Name einer lokalen Arbeitsgruppe (nur bei NetBIOS) | 'workgroup1' | | 'workgroup2' |
| ISDN | Datenkomprimierung | ein/aus | ↔ | ein/aus |
| ISDN | Kanalbündelung | ein/aus | ↔ | ein/aus |

Hinweise zu den einzelnen Werten:

- Verfügt Ihr eigenes Gerät über einen **ISDN-Anschluss**, so fragt der Assistent nach, ob auch die Gegenstelle über einen solchen verfügt.
- Für VPN-Verbindungen über das Internet muss der Typ der IP-Adressen auf beiden Seiten angegeben werden. Es gibt zwei **Typen von IP-Adressen**: statische und dynamische. Eine Erklärung zum Unterschied der beiden IP-Adresstypen finden Sie im Referenzhandbuch.

Die Dynamic-VPN-Funktionalität erlaubt VPN-Verbindungen nicht nur zwischen Gateways mit statischen (festen) IP-Adressen, sondern auch bei Verwendung dynamischer IP-Adressen. Der aktive Aufbau von VPN-Verbindungen zu Gegenstellen mit dynamischer IP-Adresse erfordert eine ISDN-Verbindung.

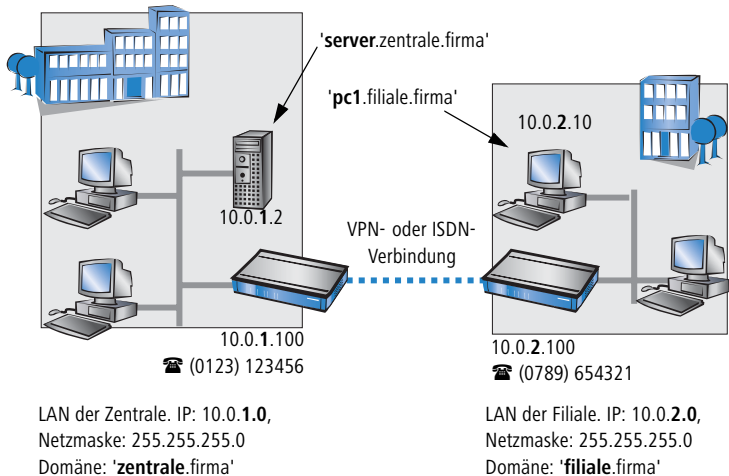
- Wenn Sie Ihr LANCOM noch nicht benannt haben, so fragt Sie der Assistent nach einem neuen **eigenen Gerätenamen**. Mit der Eingabe benennen Sie Ihr LANCOM neu. Achten Sie darauf, dass Sie beide Gegenstellen unterschiedlich benennen.

- Der **Name der Gegenstelle** wird für deren Identifikation benötigt.
- Im Feld **ISDN-Rufnummer** wird die Rufnummer der ISDN-Gegenstelle angegeben. Erforderlich ist die Angabe der kompletten Rufnummer der Gegenstelle einschließlich aller notwendigen Vorwahlen.
- Mit der angegebenen **ISDN-Anruferkennung** wird der Anrufer identifiziert und authentifiziert. Wird ein LANCOM Router angerufen, vergleicht er die für die Gegenstelle eingetragene ISDN-Anruferkennung mit der Kennung, die der Anrufer tatsächlich über den D-Kanal übermittelt. Eine ISDN-Kennung setzt sich üblicherweise aus der nationalen Vorwahl und einer MSN zusammen.
- Das **Kennwort für die ISDN-Verbindung** ist eine Alternative zur ISDN-Anruferkennung. Es wird immer dann zur Authentifizierung des Anrufers herangezogen, wenn keine ISDN-Anruferkennung übermittelt wird. Das Kennwort muss auf beiden Seiten identisch eingegeben werden. Es wird für Anrufe in beide Richtungen verwendet.
- Das **Shared Secret** ist das zentrale Kennwort für die Sicherheit der VPN-Verbindung. Es muss auf beiden Seiten identisch eingegeben werden.
- Die Datenkomprimierung erhöht die Übertragungsgeschwindigkeit ohne zusätzliche Kosten. Ganz im Gegensatz zur Bündelung von zwei ISDN-Kanälen mit MLPPP (**M**ulti**L**ink-**P**PP): Hier wird zwar die Bandbreite verdoppelt, in aller Regel fallen dafür aber auch doppelte Verbindungsgebühren an.

5.1.2 Einstellungen für den TCP/IP-Router

Im TCP/IP-Netzwerk kommt der korrekten Adressierung eine besondere Bedeutung zu. Bei einer Netzwerkkopplung ist zu beachten, dass beide Netzwerke logisch voneinander getrennt sind. Sie müssen daher jeweils über eine eigene Netzwerknummer verfügen (im Beispielfall '10.0.1.x' und '10.0.2.x'). Die beiden Netzwerknummern müssen unterschiedlich sein.

■ Kapitel 5: Zwei Netzwerke verbinden



Im Gegensatz zum Internet-Zugang werden bei der Kopplung von Netzen alle IP-Adressen aus den beteiligten Netzen auch im entfernten LAN sichtbar, nicht nur die der Router. Der Rechner mit der IP-Adresse 10.0.2.10 im LAN der Filiale sieht den Server 10.0.1.2 in der Zentrale und kann (entsprechende Rechte vorausgesetzt) auch auf ihn zugreifen. Gleiches gilt umgekehrt.

DNS-Zugriffe ins entfernte LAN

Der Zugriff auf entfernte Rechner kann in einem TCP/IP-Netzwerk nicht nur über die Angabe der IP-Adresse erfolgen, sondern dank DNS auch über frei definierbare Namen.

Beispielsweise kann der Rechner mit dem Namen 'pc1.filiale.firma' (IP 10.0.2.10) auf den Server in der Zentrale nicht nur über dessen IP-Adresse zugreifen, sondern auch über dessen Namen 'server.zentrale.firma'. Einzige Voraussetzung: Die Domäne des entfernten Netzwerks muss im Assistenten angegeben werden.



Die Angabe der Domäne ist nur im LANconfig-Assistenten möglich. Bei WEBconfig nehmen Sie die entsprechenden Einstellungen später in der Expertenkonfiguration vor. Nähere Informationen finden Sie im LANCOM Router-Referenzhandbuch.

VPN-Extranet

Bei einer LAN-LAN-Kopplung über VPN können Sie die eigenen Stationen hinter einer anderen IP-Adresse maskieren. Bei dieser als 'Extranet-VPN'

bezeichneten Betriebsart erscheinen die eigenen Rechner gegenüber dem entfernten LAN nicht mit ihrer eigenen IP-Adresse, sondern mit einer anderen frei wählbaren (z. B. der des VPN-Gateways).

Den Stationen im entfernten LAN wird dadurch der direkte Zugriff auf die Rechner im eigenen LAN verwehrt. Wurde beispielsweise im LAN der Filiale für den Zugriff auf die Zentrale der Extranet-VPN-Modus hinter der IP-Adresse '10.10.2.100' eingestellt, und greift der Rechner '10.10.2.10' auf den Server '10.10.1.2' zu, so erscheint bei diesem eine Anfrage von der IP '10.10.2.100'. Die tatsächliche IP-Adresse des Rechners bleibt verborgen.

Wenn ein LAN im Extranet-Modus gekoppelt wird, so wird auf der Gegenseite nicht dessen tatsächliche (verborgene) LAN-Adresse angegeben, sondern die IP-Adresse, mit der das LAN nach außen hin auftritt (im Beispiel '10.10.2.100'). Die Netzmaske lautet in diesem Fall '255.255.255.255'.

5.1.3 Einstellungen für den IPX-Router



Die Kopplung von IPX-Netzwerken über VPN kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

Für die Kopplung von zwei typischen IPX-Netzwerken zu einem WAN sind drei IPX-Netzwerknnummern notwendig:

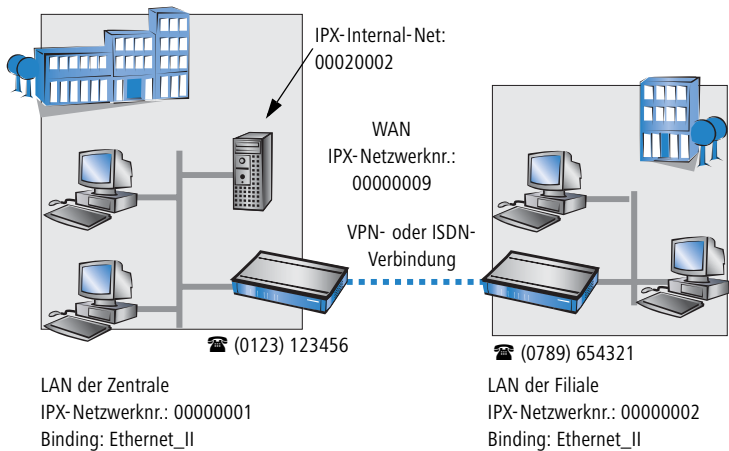
- für das LAN der Zentrale
- für das LAN der Filiale
- für das übergeordnete WAN

Die IPX-Netzwerknnummern in Zentrale und Filiale werden jeweils auf der entfernten Seite angegeben.

Die drei geforderten Netzwerknnummern werden in den IPX-Konventionen als „External Network Numbers“ bezeichnet. Sie gelten (ähnlich IP-Netzwerk-Adressen) für ein ganzes LAN-Segment. Im Gegensatz dazu dienen die IPX-Internal-Network-Nummern zur Adressierung eines bestimmten Novell-Servers im LAN. Alle drei angegebenen Netzwerknnummern müssen sich voneinander und von allen verwendeten IPX-Internal-Network-Nummern unterscheiden.

Ferner kann die Angabe des im entfernten LAN verwendeten Frame-Typs („Binding“) erforderlich sein.

Wenn im entfernten Netz ein Novell-Server arbeitet, ist die Angabe der entfernten IPX-Netzwerknnummer und des verwendeten Bindings nicht erforder-



lich. In diesem Fall muss lediglich eine Netzwerknummer für das WAN manuell angegeben werden.

5.1.4 Einstellungen für NetBIOS-Routing

Das NetBIOS-Routing ist schnell eingerichtet: Zusätzlich zu den Angaben für das verwendete TCP/IP-Protokoll muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.

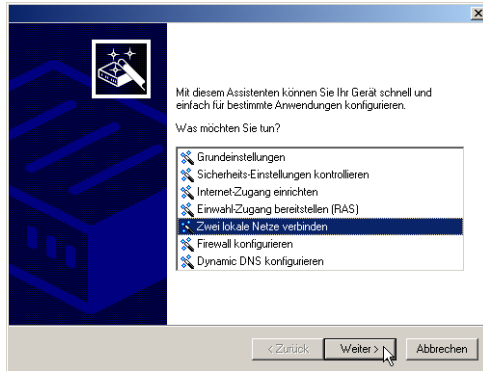


Entfernte Windows-Arbeitsgruppen erscheinen nicht in der Windows-Netzwerkumgebung, sondern können nur direkt (z. B. über die Computer-Suche) angesprochen werden.

5.2 Anleitung für LANconfig

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

- ① Rufen Sie den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie notwendigen Daten ein.



- ② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
- ③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit ping) anzusprechen. Der LANCOM Router sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

Ping – schneller Verbindungstest einer TCP/IP-Verbindung

Für den Test einer TCP/IP-Verbindung schicken Sie einfach ein ping von Ihrem Rechner an einen Rechner im entfernten Netz. Details zum Ping-Befehl finden Sie in der Dokumentation Ihres Betriebssystems.

IPX- und NetBIOS-Verbindungen testen Sie, indem Sie von Ihrem Rechner aus einen entfernten Novell-Server bzw. einen Rechner in der entfernten Windows-Arbeitsgruppe suchen.

```

C:\>ping 10.0.1.2

Ping wird ausgeführt für 10.0.1.2 mit 32

Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit=20ms
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms
Antwort von 10.0.1.2: Bytes=32 Zeit<10ms

Ping-Statistik für 10.0.1.2:
    Pakete: Gesendet = 4, Empfangen = 4,
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 20ms, Mitte
  
```

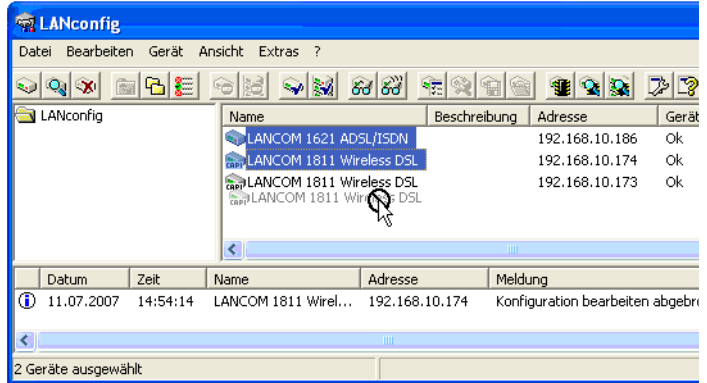
5.3 1-Click-VPN für Netzwerke (Site-to-Site)

Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können

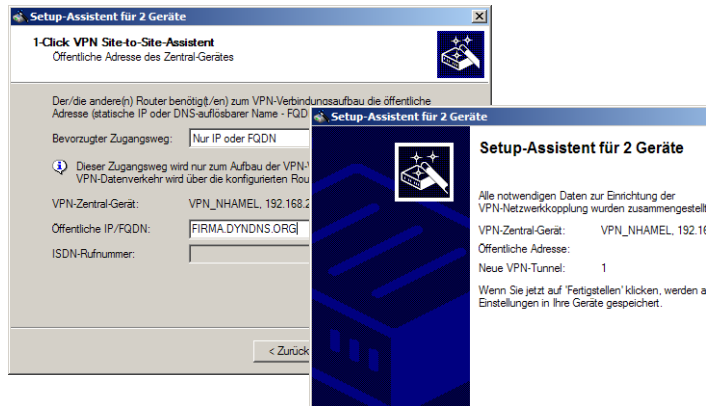
Kapitel 5: Zwei Netzwerke verbinden

sogar mehrere Router gleichzeitig an einen zentrales Netzwerk gekoppelt werden.

- ① Markieren Sie in LANconfig die Router der Filialen, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.
- ② Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.



- ③ Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.



- ④ Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers oder über eine ISDN-Verbindung erfolgen

soll. Geben Sie dazu die Adresse bzw. den Namens des zentralen Routers bzw. seine ISDN-Nummer an.

- ⑤ Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
 - Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht werden.
 - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.



Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

5.4 Anleitung für WEBconfig



Die Kopplung von Netzwerken über VPN kann unter WEBconfig nicht mit Hilfe des Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

- ① Rufen Sie im Hauptmenü den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
- ② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Weiter** ab.
- ③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit ping) anzusprechen. Der LANCOM Router sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

6 Einwahl-Zugang bereitstellen

An Ihrem LANCOM können Sie Einwahl-Zugänge einrichten, über die sich einzelne Rechner in Ihr LAN einwählen können und für die Dauer der Verbindung vollwertiger Teilnehmer des Netzwerks werden. Dieser Dienst wird auch als RAS (**R**emote **A**ccess **S**ervice) bezeichnet. Der RAS-Zugang kann grundsätzlich auf zwei verschiedenen Wegen realisiert werden:

- **VPN:** Bei einem RAS-Zugang über VPN wird die Verbindung zwischen dem LAN und dem Einwahlrechner über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. Der Router im LAN benötigt eine VPN-Unterstützung, der Einwahlrechner einen beliebigen Zugang zum Internet und einen VPN Client.
- **ISDN:** Bei einem RAS-Zugang über ISDN wird eine direkt Verbindung zwischen dem LAN und dem Einwahlrechner über eine ISDN-Verbindung hergestellt. Der Router im LAN benötigt eine ISDN-Schnittstelle, der Einwahlrechner einen ISDN-Adapter oder ein ISDN-Modem. Als Protokoll für die Datenübertragung dient PPP. Damit ist die Unterstützung aller üblichen Geräte und Betriebssysteme gesichert.

Die Einrichtung eines Einwahl-Zugangs erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein.

Ein LANCOM bietet daher eine ganze Reihe von Sicherheitsmechanismen an, bei deren Einsatz ein hervorragender Schutz gewährleistet ist:

- **VPN:** Bei Kopplungen über VPN werden die Daten mittels IPsec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt
- **ISDN:** Bei Kopplungen über ISDN sorgen das Kennwort für die Verbindung, die Überprüfung der ISDN-Nummer und die Rückruffunktion für die Sicherheit der Verbindung.



Die ISDN-Rückruffunktion kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

6.1 Welche Angaben sind notwendig?

Der Assistent richtet den Einwahl-Zugang nur für einen Benutzer ein. Für jeden zusätzlichen Benutzer führen Sie den Assistenten ein weiteres Mal aus.

6.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung eines RAS-Zugangs benötigt. Die erste Spalte zeigt jeweils an, ob die Information für einen RAS-Zugang über VPN (einfaches Verfahren mit „Preshared Keys“) und/oder über ISDN erforderlich ist.



Weitere Informationen zu RAS-Zugängen über VPN-Verbindungen mit anderen Verfahren entnehmen Sie bitte dem LANCOM Referenzhandbuch.

| Kopplung | Angabe |
|------------|---|
| VPN + ISDN | Benutzername |
| VPN + ISDN | Passwort |
| VPN | Shared Secret für Verschlüsselung |
| VPN | Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)? |
| ISDN | Ankommende Rufnummer des Einwahlrechners |
| ISDN | TCP/IP-Routing für Zugriff auf entferntes Netz? |
| ISDN | IPX-Routing für Zugriff auf entferntes Netz? |
| VPN + ISDN | IP-Adresse(n) für den oder die Einwahlrechner: fest oder dynamisch aus einem Adressbereich (IP-Adress-Pool) |
| VPN + ISDN | NetBIOS-Routing für Zugriff auf entferntes Netz? |
| VPN + ISDN | Name einer lokalen Arbeitsgruppe (nur bei NetBIOS) |

Hinweise zu den einzelnen Werten:

- **Benutzername und Passwort:** Mit diesen Zugangsdaten weist sich der Benutzer bei der Einwahl aus.
- **Ankommende Nummer:** Die optionale ISDN-Anruferkennung verwendet der LANCOM Router zusätzlich zur Benutzer-Authentifikation. Auf die Verwendung dieser Sicherheitsfunktion sollte immer dann verzichtet werden, wenn sich der Benutzer von verschiedenen ISDN-Anschlüssen einwählt.



Hinweise zu den anderen Werten, die bei der Einrichtung des RAS-Zugangs benötigt werden, finden Sie im Kapitel 'Zwei Netzwerke verbinden'.

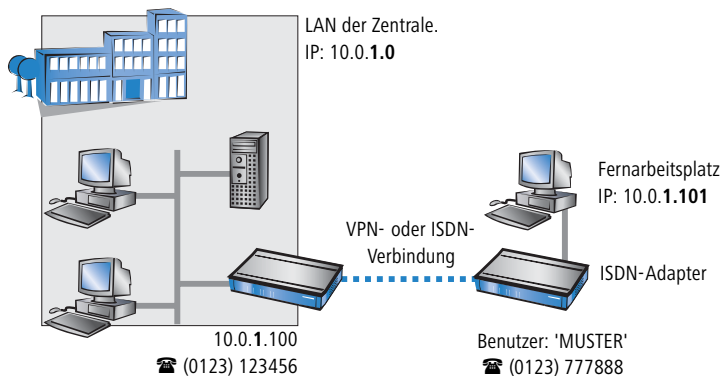
Die ISDN-Anruferkennung (CLI)

Bei der ISDN-Anruferkennung – auch als CLI (**C**alling **L**ine **I**dentify) bezeichnet – handelt sich um die Telefonnummer des Anrufers, die an den angerufenen Teilnehmer übermittelt wird. Sie setzt sich in aller Regel aus der nationalen Vorwahl und einer MSN zusammen.

Die CLI eignet sich aus zwei Gründen besonders gut für die Authentifizierung: Zum einen lässt sie sich nur schwer manipulieren. Zum anderen erfolgt ihre Übertragung kostenlos über den ISDN-Steuerkanal (D-Kanal).

6.1.2 Einstellungen für TCP/IP

Beim Protokoll TCP/IP muss jedem aktiven RAS-Benutzer eine eigene IP-Adresse zugewiesen werden.



Diese IP-Adresse können Sie entweder bei der Anlage eines Benutzers manuell festlegen. Einfacher ist es, den LANCOM Router einem Benutzer automatisch bei der Einwahl eine freie IP-Adresse zuteilen zu lassen. In diesem Fall legen Sie bei der Konfiguration nur den IP-Adressbereich fest, aus dem der LANCOM Router die Adresse für den RAS-Benutzer nehmen soll.

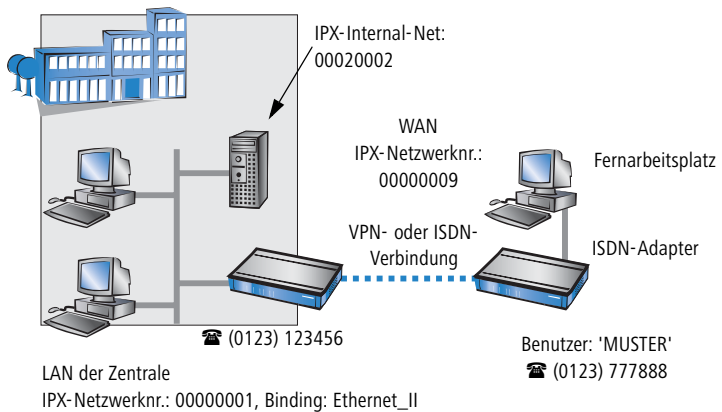
Achten Sie sowohl bei der manuellen als auch bei der automatischen IP-Adresszuteilung darauf, dass es sich um freie Adresse(n) aus dem Adressbereich Ihres lokalen Netzwerks handelt. Im Beispiel wird dem PC bei der Einwahl die IP-Adresse '10.0.1.101' zugewiesen.

Mit dieser IP-Adresse ist der Rechner ein vollwertiger Teilnehmer im LAN: Er kann (bei entsprechender Berechtigung) auf alle anderen Geräte im LAN zugreifen. Umgekehrt gilt dieses Verhältnis auch: auf den entfernten Rechner kann auch aus dem LAN zugegriffen werden.

6.1.3 Einstellungen für IPX

Für die RAS-Einwahl in ein IPX-Netzwerk ist die Angabe von zwei IPX-Netzwerknummern notwendig:

- die IPX-Netzwerknummer der Zentrale
- eine zusätzliche IPX-Netzwerknummer für das übergeordnete WAN



Die geforderten Netzwerknummern werden in den IPX-Konventionen als „External Network Numbers“ bezeichnet. Sie gelten (analog zu IP-Netzwerk-Adressen) für ein komplettes LAN-Segment. Im Gegensatz dazu dienen die IPX-Internal-Network-Nummern zur Adressierung von bestimmten Novell-Servern im LAN. Alle drei angegebenen Netzwerknummern müssen sich voneinander und von allen verwendeten IPX-Internal-Network-Nummern unterscheiden.

Ferner kann die Angabe des im entfernten LAN verwendeten Frame-Typs („Binding“) erforderlich sein.

Wenn im entfernten Netz ein Novell-Server arbeitet, ist die Angabe der entfernten IPX-Netzwerknummer und des verwendeten Bindings nicht erforderlich. Eine Netzwerknummer für das WAN muss allerdings auch in diesem Fall manuell angegeben werden.

6.1.4 Einstellungen für NetBIOS-Routing

Für die Verwendung von NetBIOS muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.



Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muss bei Bedarf zunächst manuell eine Verbindung über das DFÜ-Netzwerk zum LANCOM Router herstellen. Bei bestehender Verbindung kann die Rechner im anderen Netz suchen und auf sie zugreifen (über **Suchen** ► **Computer**, nicht über die Netzwerkumgebung).

6.2 Einstellungen am Einwahl-Rechner

6.2.1 Einwahl über VPN

Für die Einwahl in ein Netzwerk über VPN benötigt ein Rechner:

- Einen Zugang zum Internet
- Einen VPN-Client

LANCOM Systems bietet auf der beiliegenden CD eine 30-Tage-Testversion des LANCOM Advanced VPN Client an. Eine genaue Beschreibung des VPN-Client und Hinweise zur Einrichtung finden Sie ebenfalls auf der CD.

Der Assistent fragt im folgenden die Werte ab, die beim Anlegen des RAS-Zugangs im LANCOM Router festgelegt wurden.

6.2.2 Einwahl über ISDN

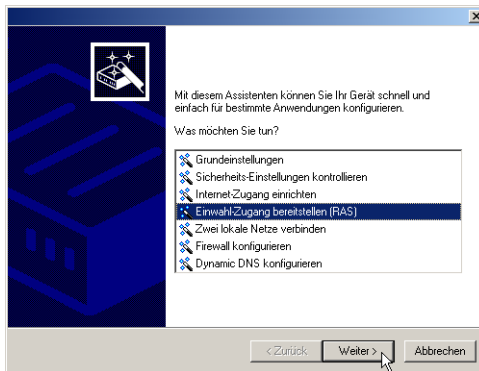
Beim Einwahl-Rechner sind einige Einstellungen nötig, die hier nur kurz am Beispiel eines Windows-Rechners aufgeführt sind:

- DFÜ-Netzwerk (bzw. anderer PPP-Client) korrekt eingerichtet
- Netzwerkprotokoll (TCP/IP, IPX) installiert und auf den DFÜ-Adapter gebunden
- neue Verbindung im DFÜ-Netzwerk mit Rufnummer des Routers
- Terminal-Adapter oder ISDN-Karte auf PPPHDLC eingestellt
- PPP als DFÜ-Servertyp ausgewählt, 'Software-Komprimierung aktivieren' und 'Verschlüsseltes Kennwort fordern' ausgeschaltet
- Auswahl der gewünschten Netzwerkprotokolle (TCP/IP, IPX)
- Zusätzliche TCP/IP-Einstellungen:
 - Zuweisung von IP-Adresse und Namensserveradresse aktiviert
 - 'IP-Headerkomprimierung' deaktiviert

Mit diesen Einstellungen kann sich ein PC über ISDN in das entfernte LAN einwählen und in üblicher Weise auf dessen Ressourcen zugreifen.

6.3 Anleitung für LANconfig

- 1 Rufen Sie den Assistenten 'Zugang bereitstellen (RAS, VPN, IPSec oder WLAN)' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.



- 2 Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
- 3 Konfigurieren Sie wie beschrieben den Zugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung').

6.4 1-Click-VPN für LANCOM Advanced VPN Client

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Client in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des LANCOM VPN Router entnommen und mit zufällig ermittelten Werten ergänzt (z.B. für den Preshared Key).

- 1 Starten Sie über LANconfig den Setup-Assistenten 'Zugang bereitstellen' und wählen Sie die 'VPN-Verbindung'.

■ Kapitel 6: Einwahl-Zugang bereitstellen

- ② Aktivieren Sie die Optionen 'LANCOM Advanced VPN Client' und 'Beschleunigen Sie das Konfigurieren mit 1-Click-VPN'.
- ③ Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
- ④ Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:
 - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
 - Profil per E-Mail versenden
 - Profil ausdrucken



Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte!

Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z.B.:

- Gateway: Sofern im LANCOM VPN Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
- FQDN: Kombination aus dem Namen der Verbindung, eine fortlaufenden Nummer und der internen Domäne im LANCOM VPN Router
- Domäne: Sofern im LANCOM VPN Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wird der 'Aggressive Mode' verwendet.

- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom LANCOM VPN Router zugewiesen.

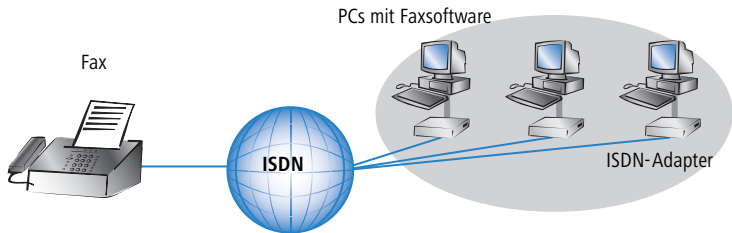
6.5 Anleitung für WEBconfig

- ① Rufen Sie im Hauptmenü den Assistenten 'Einwahl-Zugang bereitstellen (RAS)' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
- ② Konfigurieren Sie wie beschrieben den Zugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung').

7 Faxe versenden mit der LANCAPI

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

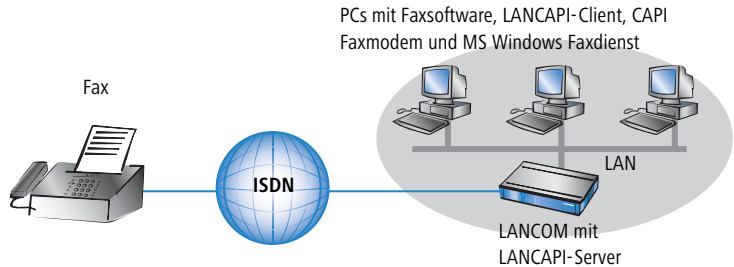
Der Einsatz der LANCAPI bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die LANCAPI uneingeschränkten Zugriff auf ISDN-Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofiletransfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle ISDN-Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptoren oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.



Mit der LANCAPI von LANCOM können Sie von Ihrem Arbeitsplatzrechner aus bequem Faxe versenden, ohne dass ein Faxgerät angeschlossen ist. Hierzu müssen auf Ihrem Rechner jedoch verschiedene Komponenten installiert sein:

- der **LANCAPI-Client**. Dieser stellt die Verbindung zwischen Ihrem Arbeitsplatzrechner und dem LANCAPI-Server her.
- das **LANCOM CAPI Faxmodem**. Dieses Tool simuliert ein Faxgerät auf Ihrem Arbeitsplatzrechner.

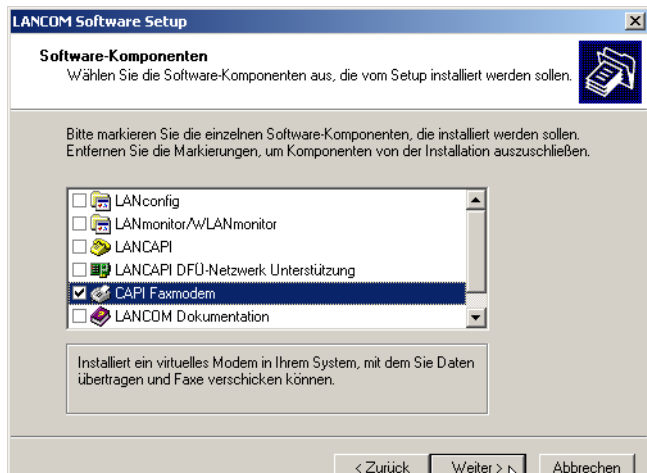
- der **MS-Windows Faxdienst**. Er ist die Schnittstelle zwischen Faxanwendungen und dem virtuellen Fax.



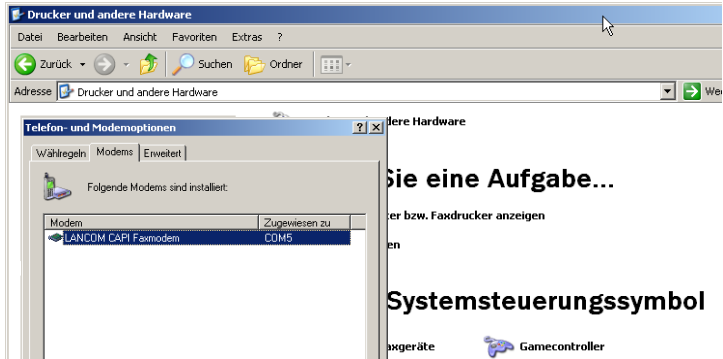
Die Installation des LANCAPI-Clients wird im Referenzhandbuch beschrieben. Dieses Kapitel beschäftigt sich mit der Installation und Konfiguration von LANCOM CAPI Faxmodem und MS-Windows Faxdienst.

7.1 Installation des LANCOM CAPI Faxmodem

- ① Wählen Sie im Setup-Programm Ihrer LANCOM-CD den Eintrag **LANCOM Software installieren**.
- ② Markieren Sie die Option **CAPI Faxmodem**, klicken Sie **Weiter** und folgen Sie den Hinweisen der Installationsroutine.

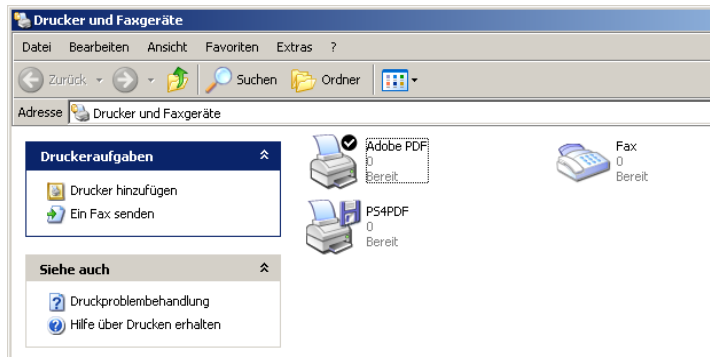


Ist die Installation erfolgreich verlaufen, ist das LANCOM CAPI Faxmodem in den **Telefon- und Modemoptionen** der Systemsteuerung eingetragen.



7.2 Installation des MS Windows Faxdienstes

- ① Wählen Sie in der Systemsteuerung die Option **Drucker und Faxgeräte**.
- ② Wählen Sie im Fenster Drucker und Faxgeräte die Option **lokalen Faxdrucker installieren**. Folgen Sie ggf. den Anweisungen des Installations-tools. In dem aktuellen Fenster erscheint ein Icon für den neu angelegten Faxdrucker.



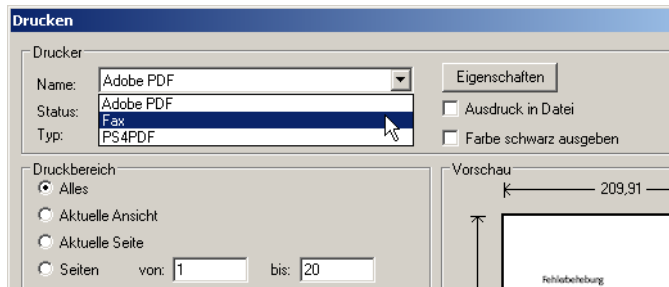
Zum Überprüfen der Installation klicken sie mit der rechten Maustaste auf das Fax-Icon und wählen **Eigenschaften**. Im Register 'Geräte' sollte das LANCOM CAPI Faxmodem eingetragen sein.

7.3 Versenden eines Faxes

Nachdem alle erforderlichen Komponenten installiert wurden, gibt es mehrere Möglichkeiten, ein Fax von Ihrem Arbeitsplatzrechner aus zu versenden. Haben Sie bereits eine fertige Datei, können Sie diese direkt aus Ihrer jeweiligen Anwendung heraus verschicken. Wollen Sie dagegen nur eine kurze Notiz versenden, wählen sie den MS-Windows Faxdienst. Alternativ können Sie natürlich auch eine beliebige Fax-Software verwenden.

7.3.1 Faxe versenden mit beliebigen Büroanwendungen

- ① Öffnen Sie wie gewohnt ein Dokument in Ihrer Büroanwendung und wählen Sie den Menüpunkt **Datei/Drucken**.
- ② Stellen Sie als Drucker das Faxgerät ein.

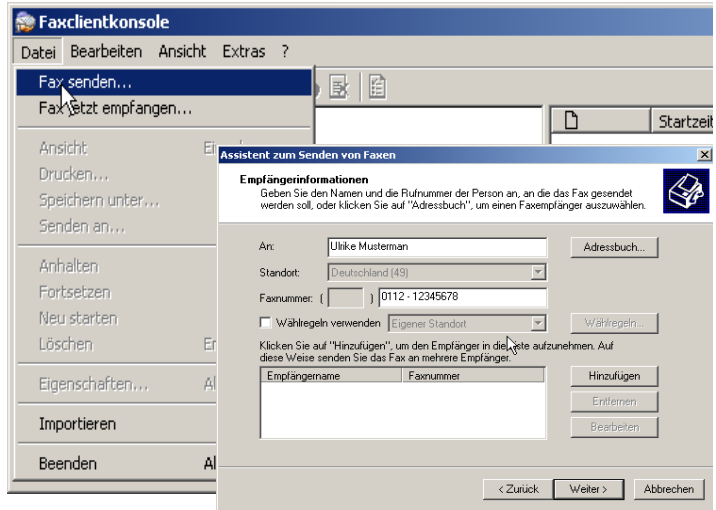


- ③ Klicken Sie auf OK. Es erscheint ein Assistent, der Sie durch den weiteren Sendevorgang leitet.

7.3.2 Faxe versenden mit dem Windows Faxdienst

- ① Öffnen Sie in der Systemsteuerung das Fenster **Drucker und Faxgeräte**.
- ② Doppelklicken Sie mit der linken Maustaste das Icon des Faxgerätes.

- ③ Es öffnet sich die Faxclientkonsole. Wählen Sie den Menüpunkt **Datei/Fax senden**. Ein Assistent führt sie durch den weiteren Sendevorgang.



8 Sicherheits- Einstellungen

Ihr LANCOM verfügt über zahlreiche Sicherheitsfunktionen. In diesem Kapitel finden Sie alle Informationen, die Sie für eine optimale Absicherung des Gerätes benötigen.



Die Konfiguration der Sicherheitseinstellungen können Sie sehr schnell und komfortabel mit dem Sicherheits-Assistenten von LANconfig oder WEBconfig vornehmen.

DE

8.1 Der Sicherheits-Assistent

Der Zugriff auf die Konfiguration des Geräts erlaubt nicht nur das Auslesen kritischer Informationen (z. B. Internet-Kennwort). Vielmehr können auch die Einstellungen der Sicherheitsfunktionen (z. B. Firewall) nach Belieben geändert werden. Dadurch bringt der unbefugte Konfigurationszugriff nicht nur das einzelne Gerät, sondern das gesamte Netzwerk in große Gefahr.

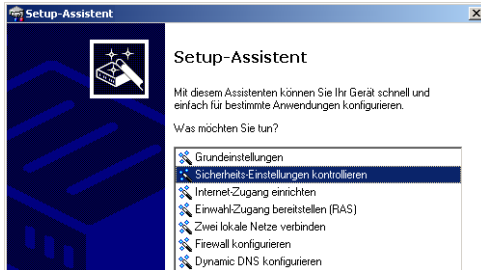
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

Das Gerät sperrt den Konfigurationszugang automatisch für eine festgelegte Dauer, wenn eine bestimmte Anzahl von Anmelde-Fehlversuchen festgestellt wird. Sowohl die kritische Anzahl Fehlversuche als auch die Dauer der Sperre lassen sich modifizieren. Standardmäßig sperrt das Gerät nach dem fünften Fehlerversuch für eine Dauer von fünf Minuten.

Neben diesen grundlegenden Einstellungen prüfen Sie mit dem Sicherheitsassistenten auch die Sicherheitseinstellungen für das Funknetzwerk, sofern Ihr Gerät über eine WLAN-Schnittstelle verfügt.

8.1.1 Assistent für LANconfig

- 1 Markieren Sie Ihren LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



- 2 Wählen Sie im Auswahlfenster den Setup-Assistenten **Sicherheitseinstellungen kontrollieren** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 In den folgenden Fenstern stellen Sie das Passwort ein und wählen die zulässigen Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken aus.
- 4 In einem weiteren Schritt werden die Parameter der Konfigurationssperre wie Anzahl der Fehllogins und Dauer der Sperre eingestellt.
- 5 Im Bereich der Firewall aktivieren Sie die Stateful-Inspection, das Ping-Blocking und den Stealth-Mode.
- 6 Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen ab**.

8.1.2 Assistent für WEBconfig

Unter WEBconfig besteht die Möglichkeit, den Assistenten **Sicherheitseinstellungen** aufzurufen und die Einstellungen zu kontrollieren und zu ändern. Dabei werden die folgenden Werte bearbeitet:

- Passwort für das Gerät
- zulässige Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken
- Parameter der Konfigurationssperre (Anzahl der Fehllogins und Dauer der Sperre)

8.2 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Profis alle wichtigen Sicherheitseinstellungen im Überblick. Die meisten Punkte dieser Checkliste sind in einfachen Konfigurationen unbedenklich. In solchen Fällen reichen die Sicherheitseinstellungen aus, die während der Grundkonfiguration oder mit dem Sicherheits-Assistenten gesetzt werden.



Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

■ 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 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 die Firewall aktiviert?

Die Stateful-Inspection Firewall der LANCOM-Geräte 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.



Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

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

Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter 'Firewall/QoS' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich im Referenzhandbuch.

■ **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 'IP-Router' auf der Registerkarte 'Routing'.

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

Die Firewall-Filter des LANCOMs 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 das Gerät 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 das Gerät 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 die Möglichkeiten zum Schutz der WAN-Zugänge bei einem Diebstahl des Gerätes aktiviert?

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

Durch die Funktion der ISDN-Standort-Verifikation kann das Gerät nur an einem bestimmten ISDN-Anschluß betrieben werden. Nach dem Einschalten prüft das Gerät über einen Selbstanruf zu einer festgelegten Rufnummer, ob es sich noch am „richtigen“ ISDN-Anschluß befindet (weitere Informationen finden Sie im Referenzhandbuch).

Mit den Funktionen des Scripting kann die gesamte Konfiguration des Gerätes nur im RAM gespeichert werden, der beim Booten des Gerätes gelöscht wird. Die Konfiguration wird dabei gezielt nicht in den bootresistenten Flash-Speicher geschrieben. Mit dem Trennen von der Stromversorgung und dem Aufstellen an einem anderen Ort wird damit die

gesamte Konfiguration des Gerätes gelöscht (weitere Informationen finden Sie im Referenzhandbuch).

■ **Haben Sie den Reset-Taster gegen das unbeabsichtigte Zurücksetzen der Konfiguration gesichert?**

Manche Geräte können nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Buttons gesteuert werden, der Reset-Taster wird dann entweder ignoriert oder es wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.

9 Rat & Hilfe

In diesem Kapitel finden Sie Ratschläge und Hilfestellungen für die erste Hilfe bei einigen typischen Problemen.

9.1 Es wird keine WAN-Verbindung aufgebaut

Nach dem Start versucht der Router automatisch, Kontakt zum Internet-Anbieter aufzunehmen. Während dieser Phase blinkt die LED für den Status der Internetverbindung grün. Im Erfolgsfall wechselt diese LED dann auf dauerhaftes Grün. Schlägt die Kontaktaufnahme hingegen fehl, so leuchtet die Online-LED rot. In der Regel ist eine der folgenden Ursachen verantwortlich:

Probleme an der Verkabelung?

Verwenden Sie für den DSL-Anschluss ausschließlich das mitgelieferte Anschlusskabel. Dieses Kabel muss mit dem Ethernet-Ausgang des DSL-Modems bzw. dem Netzanschluss verbunden sein. Die LED des WAN-Anschlusses muss zum Zeichen der physikalischen Verbindung grün leuchten.

Stimmt das gewählte Übertragungsprotokoll?

Das Übertragungsprotokoll wird bei der Grundeinstellung gesetzt. Dabei setzt der Grundeinstellungs-Assistent für zahlreiche DSL-Anbieter selbstständig das korrekte Übertragungsprotokoll. Nur wenn Ihr DSL-Anbieter dem Assistenten unbekannt ist, müssen Sie das verwendete Protokoll selber angeben. In jedem Fall sollte das Protokoll funktionieren, das Ihnen Ihr DSL-Anbieter angibt.

Die Protokoll-Einstellung kontrollieren und korrigieren Sie unter:

| Konfigurationstool | Aufruf |
|--------------------|---|
| LANconfig | Kommunikation ► allgemein ► Kommunikations-Layer |
| WEBconfig | Expertenkonfiguration ► Setup ► WAN-Modul ► Layer-Liste |

9.2 DSL-Übertragung langsam

Die Übertragungsgeschwindigkeit einer (Internet-) DSL-Verbindung hängt von zahlreichen Faktoren ab, von denen die meisten außerhalb des eigenen Einflussbereiches liegen: Entscheidend sind neben der Bandbreite der eigenen Internet-Anbindung beispielsweise auch die Internet-Anbindung und Auslas-

tung des angesprochenen Ziels. Außerdem können zahlreiche Faktoren im Internet die Übertragungsleistung beeinflussen.

Vergrößerung der TCP/IP-Windows-Size unter Windows

Wenn die tatsächliche Übertragungsleistung einer DSL-Verbindung deutlich unter den vom DSL-Anbieter angegebenen Maximalwerten liegt, gibt es außer diesen externen Einflussfaktoren nur wenige mögliche Fehlerquellen an den eigenen Geräten.

Ein übliches Problem tritt auf, wenn an einem Windows-PC über eine asynchrone Verbindung gleichzeitig große Datenmengen geladen und gesendet werden. In diesem Fall kann es zu einer starken Beeinträchtigung der Download-Geschwindigkeit kommen. Verantwortlich ist die sogenannte TCP/IP-Receive-Windows-Size im Windows-Betriebssystem, die standardmäßig auf einen für asynchrone Verbindungen zu kleinen Wert gesetzt ist.

Eine Anleitung zur Vergrößerung der Windows-Size finden Sie in der Wissensdatenbank im Support-Bereich der LANCOM Systems-Website (www.lancom.de).

9.3 Unerwünschte Verbindungen mit Windows XP

Windows-XP-Rechner versuchen beim Start, die eigene Uhrzeit mit einem Zeitserver im Internet abzugleichen. Deshalb kommt es beim Start eines Windows-XP-Rechners im WLAN zum Verbindungsaufbau des LANCOM mit dem Internet.

Zur Abhilfe schaltet man an den Windows-XP-Rechnern die automatische Zeitsynchronisation unter **Rechter Mausklick auf die Uhrzeit ► Datum ► Uhrzeit ändern ► Internetzeit** aus.

9.4 Kabel testen

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

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

Klick auf die Schaltfläche **Ausführen** starten Sie den Test für das eingetragene Interface.

[Experten-Konfiguration](#)

 [Status](#)

 [LAN-Statistik](#)

Kabel-Test

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

Parameter

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

[Experten-Konfiguration](#)

 [Status](#)

 [LAN-Statistik](#)

Kabel-Test-Ergebnisse

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

Als Ergebnisse können folgende Werte erscheinen:

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

10 Anhang

10.1 Leistungs- und Kenndaten

| | | LANCOM 821+ | LANCOM 1721 VPN | LANCOM 1711+ VPN |
|-----------------------|---|--|---|----------------------------|
| Anschlüsse | Ethernet LAN | 4 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection | | |
| | WAN bzw. ADSL | ADSL over ISDN nach ITU G.992.1 Annex B (kompatibel zum U-R2-Anschluss der Deutschen Telekom) oder ADSL over POTS nach ITU G.992.1 Annex A ADSL over ISDN nach ITU 992.3, ITU G.992.5 Annex B (ADSL2+) oder ADSL over POTS nach ITU G.992.3 und ITU G.992.5 Annex A | | 10/100Base-TX, Autosensing |
| | ISDN | ISDN S ₀ | | |
| | Serielle Schnittstelle / COM Port | serieller V.24/V.28-Port (8-pol. Mini-DIN), in Verbindung mit LANCOM Modem Adapter Kit zum Anschluss eines externen Analog- oder GPRS-Modems geeignet. | | |
| | Stromversorgung | 12V DC über externes Netzteil. Zulässiges Netzteil: ■ NEST 12V/1A DC/S Hohlstkr 2.1/5.5mm (RoHS) LANCOM Art.-Nr. 110524 Typenbezeichnung auf dem Netzteil „Type: 15.2230S“ | | |
| Gehäuse | 210 x 143 x 45 mm (B x H x T), robustes Kunststoffgehäuse, Anschlüsse auf der Rückseite, stapelbar, für Wandmontage vorbereitet | | | |
| Normen | EU (CE-Zertifizierung: EN 55022, EN 55024, EN 60950) | | | |
| Umgebung / Temperatur | 5 °C bis +40 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend) | | 5 °C bis +55 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend) | |
| Optionen | LANCOM Service-Option (4 Jahre Garantie, Vorabaustausch) (Art.-Nr. 61401) | | | |

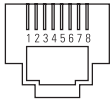
| | LANCOM 821+ | LANCOM 1721 VPN | LANCOM 1711+ VPN |
|---------|-------------|---|---|
| | | | LANCOM VPN Option 25 Kanäle (hardwarebeschleunigt, maximal 25 gleichzeitige Verbindungen, 50 Verbindungen konfigurierbar) für VPN im WAN (Art.-Nr. 60083) |
| Zubehör | | LANCOM Modem Adapter Kit zum Anschluß von Modems (analog oder GSM) an die serielle Konfigurationsschnittstelle (Art.-Nr. 110288) LANCOM Rack Mount Option (Art.-Nr. 61501) LANCOM LCOS Referenzhandbuch (DE) (Art.-Nr. 61700) | |
| | | | LANCOM Advanced VPN Client (Art.-Nr. 61600) LANCOM Advanced VPN Client (10er Bulk) (Art.-Nr. 61601) LANCOM Advanced VPN Client (25er Bulk) (Art.-Nr. 61602) |

10.2 Anschlussbelegung

10.2.1 WAN-Schnittstelle

Nur LANCOM
1711+ VPN

8-polige RJ45-Buchse

| Steckverbindung | Pin | IAE |
|--|-----|-----|
|  | 1 | T+ |
| | 2 | T- |
| | 3 | R+ |
| | 4 | – |
| | 5 | – |
| | 6 | R- |
| | 7 | – |
| | 8 | – |

10.2.2 ADSL-Schnittstelle

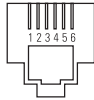
Nur LANCOM 821+
und LANCOM 1721
VPN

6-polige RJ11-Buchse

Steckverbindung

Pin

IAE



| | |
|---|---|
| 1 | – |
| 2 | – |
| 3 | a |
| 4 | b |
| 5 | – |
| 6 | – |

10.2.3 ISDN-S₀-Schnittstelle

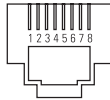
8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung

Pin

Leitung

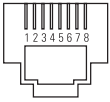
IAE



| | | |
|---|----|----|
| 1 | – | – |
| 2 | – | – |
| 3 | T+ | 2a |
| 4 | R+ | 1a |
| 5 | R- | 1b |
| 6 | T- | 2b |
| 7 | – | – |
| 8 | – | – |


10.2.4 Ethernet-Schnittstellen 10/100Base-T

8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

| Steckverbindung | Pin | Leitung |
|---|-----|---------|
|  | 1 | T+ |
| | 2 | T- |
| | 3 | R+ |
| | 4 | – |
| | 5 | – |
| | 6 | R- |
| | 7 | – |
| | 8 | – |

10.2.5 Konfigurationsschnittstelle (Outband)

8-polige Mini-DIN-Buchse

| Steckverbindung | Pin | Leitung |
|---|-----|---------|
|  | 1 | CTS |
| | 2 | RTS |
| | 3 | RxD |
| | 4 | RI |
| | 5 | TxD |
| | 6 | DSR |
| | 7 | DCD |
| | 8 | DTR |
| | U | GND |

10.3 CE-Konformitätserklärungen



Hiermit erklärt LANCOM Systems, dass sich die in dieser Dokumentation beschriebenen Geräte in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befinden.

■ *Kapitel 10: Anhang*

Die CE-Konformitätserklärungen für Ihr Gerät finden Sie im jeweiligen Produktbereich der LANCOM-Website (www.lancom.de).

Index

Numerics

| | |
|---------------|--------|
| 10/100Base-TX | 21 |
| 3-DES | 42, 52 |

A

| | |
|------------------------------------|--------|
| Accounting | 29 |
| ADSL | 19 |
| Anschluss | 21 |
| Übertragungsraten | 9 |
| ADSL-Anschlusskabel | 15 |
| AES | 42, 52 |
| Amtsvorwahl | 29 |
| Anrufbeantworter | 10 |
| Anschlussbelegung | 75 |
| ADSL-Schnittstelle | 76 |
| DSL-Schnittstelle | 75 |
| Ethernet-Schnittstelle | 77 |
| ISDN-S ₀ -Schnittstelle | 76 |
| Konfigurationsschnittstelle | 77 |
| LAN-Schnittstelle | 77 |
| Outband | 77 |
| WAN-Schnittstelle | 77 |
| Autosensing | 23 |

B

| | |
|----------|--------|
| Blowfish | 42, 52 |
|----------|--------|

C

| | |
|--|----|
| Calling Line Identity (CLI) | 54 |
| CAPI-Schnittstelle | 60 |
| Common ISDN Application Programming Interface (CAPI) | 60 |

D

| | |
|-----------------|------------|
| Datenfrequenzen | 10 |
| Default-Gateway | 68 |
| DFÜ-Adapter | 56 |
| DHCP | 36 |
| DHCP-Server | 12, 27, 36 |
| DNS | |

| | |
|------------|--------|
| DNS-Server | 12, 36 |
|------------|--------|

| | |
|----------------------------|----|
| Zugriffe ins entfernte LAN | 46 |
|----------------------------|----|

| | |
|---------------|----|
| Dokumentation | 15 |
|---------------|----|

| | |
|--------|----|
| Domäne | 46 |
|--------|----|

| | |
|----------|---|
| Download | 4 |
|----------|---|

| | |
|------------|---|
| Downstream | 9 |
|------------|---|

| | |
|----------------------------|----|
| DSL-Übertragung zu langsam | 71 |
|----------------------------|----|

E

| | |
|----------------|----|
| Einwahl-Zugang | 52 |
|----------------|----|

F

| | |
|-----|----|
| Fax | 10 |
|-----|----|

| | |
|-------------------|----|
| Fernkonfiguration | 31 |
|-------------------|----|

| | |
|-----------------------------|----|
| Fernkonfiguration über ISDN | 13 |
|-----------------------------|----|

| | |
|----------|----------------|
| Firewall | 11, 12, 13, 68 |
|----------|----------------|

| | |
|-------------------|----|
| Stationen sperren | 68 |
|-------------------|----|

| | |
|-----------------|----|
| Firewall-Filter | 40 |
|-----------------|----|

| | |
|----------|----|
| FirmSafe | 14 |
|----------|----|

| | |
|----------|---|
| Firmware | 4 |
|----------|---|

| | |
|----------|----|
| Flatrate | 38 |
|----------|----|

G

| | |
|----------------|----|
| Gebührenbudget | 29 |
|----------------|----|

| | |
|----------------|----|
| Gebührenimpuls | 29 |
|----------------|----|

| | |
|----------------|--------|
| Gebührenschatz | 29, 31 |
|----------------|--------|

| | |
|-----------------------------|----|
| Gebührenschatz zurücksetzen | 18 |
|-----------------------------|----|

| | |
|----------------|----|
| Gebührensperre | 18 |
|----------------|----|

H

| | |
|-----------------------|----|
| Hardware-Installation | 22 |
|-----------------------|----|

| | |
|-----------------|---|
| Hinweis-Symbole | 5 |
|-----------------|---|

| | |
|-------|----|
| HTTPS | 31 |
|-------|----|

I

| | |
|------|----|
| ICMP | 68 |
|------|----|

| | |
|--------------|----|
| Installation | 15 |
|--------------|----|

| | |
|------|----|
| ADSL | 23 |
|------|----|

| | |
|-----|----|
| DSL | 23 |
|-----|----|

| | |
|------|----|
| ISDN | 23 |
|------|----|

■ Index

| | | | |
|----------------------------------|--------------------|------------------------------|------------|
| Konfigurations-Schnittstelle | 24 | Konfigurationsdatei | 69 |
| LAN | 23 | Konfigurationskennwort | 67 |
| LANtools | 24 | Konfigurations-Schnittstelle | 13 |
| Netzteil | 24 | Anschlusskabel | 15 |
| Internet-Anbieter | 37 | Konfigurationsschnittstelle | 21 |
| Internet-Zugang | 11, 37 | Konfigurationsschutz | 13, 28 |
| Authentifizierungsdaten | 37 | Konfigurationszugriff | 31 |
| Flatrate | 38 | Konformitätserklärungen | 77 |
| IP | | L | |
| Filter | 68 | LAN | |
| Ports sperren | 68 | Anschlusskabel | 15 |
| IP-Adresse | 23, 27, 28, 47, 69 | LANCAPI | 12, 29 |
| IP-Masquerading | 13, 68 | LANconfig | 25, 30 |
| IP-Router | 12 | Assistenten aufrufen | 40 |
| IPSec | 42, 52 | LAN-LAN-Kopplung | 11, 29, 42 |
| IPX | 56 | erforderliche Angaben | 43 |
| Binding | 48, 55 | LANmonitor | 25 |
| External Network Number | 47, 55 | LANtools | |
| Frame-Typs | 47 | Systemvoraussetzungen | 16 |
| Internal-Net-Number | 55 | Lieferumfang | 15 |
| IPX-Konventionen | 47 | M | |
| IPX-Router | 12 | MAC-Adressfilter | 13 |
| Einstellungen | 47 | MSN | 54 |
| ISDN | | N | |
| Anschlusskabel | 15 | NAT – siehe IP-Masquerading | |
| D-Kanal | 54 | Nebenstellenanlage | 10 |
| MSN | 29 | NetBIOS | 48 |
| S ₀ -Anschluss | 21 | NetBIOS-Proxy | 12 |
| ISDN-Anruferkennung | 45, 53, 54 | Netzmaske | 27, 28, 69 |
| ISDN-Anschluss | | Netzschalter | 21 |
| Grundeinstellungen | 29 | Netzteil | 15, 21 |
| ISDN-Festverbindungsoption | 12 | Netzwerkkopplung | 42 |
| ISDN-Modem | 52 | Sicherheitsaspekte | 42, 52 |
| ISDN-Rufnummer | 45 | Netzwerksegment | 23, 47 |
| ISDN-S ₀ -Anschluss | 13 | Neustart des Geräts | 22 |
| ISDN-Telefonanlage | 29 | P | |
| K | | PAT – siehe IP-Masquerading | |
| Kennwort | 28, 31, 42, 52 | Ping | 49 |
| Kennwort für die ISDN-Verbindung | 45 | | |

| | | | |
|-----------------------------------|--------|--------------------------------|------------|
| PPP | 52 | T | |
| PPP-Client | 56 | TCP | 68 |
| R | | TCP/IP | 16, 56 |
| RAS | 11 | Einstellungen | 26 |
| Remote Access Service (RAS) | | Verbindung testen | 49 |
| MSN angeben | 29 | TCP/IP-Filter | 11, 13, 68 |
| Remote-Access-Service (RAS) | | TCP/IP-Konfiguration | |
| Benutzername | 53 | manuell | 26, 28 |
| einrichten | 52 | vollautomatisch | 26, 27 |
| Einwahl-Rechner konfigurieren | 56 | TCP/IP-Router | |
| IPX | 55 | Einstellungen | 45 |
| NetBIOS | 56 | TCP/IP-Windows-Size | 72 |
| Server | 12 | Telefon | 10 |
| Software-Komprimierung aktivieren | 56 | Telnet | 69 |
| TCP/IP | 54 | TFTP | 69 |
| Windows-Arbeitsgruppe suchen | 56 | U | |
| Reset-Schalter | 21 | Übertragungsprotokoll | 71 |
| Routerfunktion | 9 | UDP | 68 |
| Routing-Tabelle | 68 | Upstream | 9 |
| Rückruf-Funktion | 13 | V | |
| Rückruffunktion | 42, 52 | Verschlüsselung | 42, 52 |
| S | | Virtual Private Network | 10 |
| Sicherheits-Checkliste | 67 | Virtual Private Network (VPN) | 11 |
| Sicherheits-Einstellungen | 71 | VPN | 10 |
| SNMP | | VPN-Client | 56 |
| Konfiguration schützen | 67 | W | |
| Software-Installation | 24 | WAN | |
| Sprachfrequenzen | 10 | Anschlusskabel | 15 |
| Standard-Gateway | 35 | WAN-Anschluss | 21 |
| Stateful Inspection Firewall | 12 | WEBconfig | 31 |
| Stateful-Inspection-Firewall | 40 | HTTPS | 31 |
| Statusanzeigen | 16 | Systemvoraussetzungen | 16 |
| Online | 18 | Windows-Arbeitsgruppen suchen | 48 |
| Power | 17, 18 | Z | |
| Support | 4 | Zugang zum Internet einrichten | 37 |
| Switch | 21 | Zurücksetzen der Konfiguration | 22 |
| Systemvoraussetzungen | 16 | | |

