



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

LANCOM 1722 VoIP
LANCOM 1723 VoIP
LANCOM 1724 VoIP
LANCOM 1823 VoIP

- Handbuch
- Manual

LANCOM
Systems

LANCOM 1722 VoIP
LANCOM 1723 VoIP
LANCOM 1724 VoIP
LANCOM 1823 VoIP

© 2010 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 7, Windows Vista™, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Apple, das Apple-Logo, Macintosh, PowerMac, iMac, MacBook, iPhone, Mac OS, Leopard, Snow Leopard, Mac und das Mac-Logo sind Marken von Apple Computer, Inc., eingetragen in den USA und anderen Ländern.

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 (eyay@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, August 2010

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

LANCOM VoIP Router bieten umfangreiche Funktionen als Access Router, professionelle Firewall, hochwertiges VPN-Gateway und WLAN Access Point in einem kompakten Gerät und verbinden so Investitionsschutz und Kostensparnis durch Voice over IP in einer zuverlässigen Lösung für kleine und mittelständische Unternehmen, Home-Offices und Filialen.

Nur LANCOM 1823
VoIP



LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points mit eigener Konfiguration betrieben werden (WLAN-Module in der Betriebsart „Access Point-Modus“) oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller gesteuert wird (Betriebsart „Managed-Modus“). Bitte beachten Sie die entsprechenden Hinweise dazu in dieser Dokumentation.

Die verschiedenen Modelle verfügen serienmäßig über integrierte ADSL- sowie ISDN-Schnittstellen als auch über einen LAN-Switch. LANCOM 1723 VoIP bietet zusätzlich Schnittstellen für analoge Telefonsysteme. LANCOM 1823 VoIP bietet neben den Analog-Schnittstellen außerdem professionelle WLAN-Technologie.

Die VoIP-Unterstützung erweitert diese LANCOM Router über die Funktionen der Datenübertragung hinaus zu vollwertigen, integrierten VoIP-Kommunikationslösungen. Die LANCOM VoIP Router bieten damit zusätzlich zu den für VoIP optimierten Quality-of-Service-Funktionen alle Möglichkeiten für die Sprachtelefonie über Datennetzwerke und erlauben mit der schrittweisen Migration der bestehenden TK-Struktur einen preiswerten und einfachen Einstieg in das Thema „Voice over IP“ für Unternehmen. Zu den besonderen Merkmalen der LANCOM VoIP Router zählen u.a.:

- Telefonanlagenfunktionen für analoge, ISDN- und SIP-Teilnehmer
- Vernetzung von Standorten für Sprache und Daten per VPN
- SIP-Proxy und -Registrar zur Anmeldung bei Providern und übergeordneten VoIP-TK-Anlagen
- SIP-Trunking zur Nutzung vieler paralleler Leitungen mit Durchwahlnummern über einen Account mit Stammnummer
- SIP-Gateway mit transparenter Wandlung zwischen SIP und ISDN- bzw. Analog-Telefonie

■ *Ein Wort vorab*

- SIP-Remote-Gateway zur Bereitstellung lokaler SIP-, ISDN- oder Analog-Leitungen für entfernte IP-TK-Anlagen
- Intelligentes Call-Routing und Rufnummernumsetzung
- Unterstützung von Mehrgeräte- und Anlagenanschlüssen zum ISDN-Netz
- Mehrere konfigurierbare ISDN-Schnittstellen (NT/TE), teilweise mit Life-Line-Support und Spannungsweiterleitung zum internen ISDN-Bus
- WLAN nach den Standards IEEE 802.11a/h oder IEEE 802.11b/g

Bitte informieren Sie sich ggf. in der Tabelle 'Was kann Ihr LANCOM VoIP Router?' über den genauen Funktionsumfang Ihres Modells.



LANCOM-Produkte werden ständig weiterentwickelt. Eine genaue Beschreibung des Leistungsumfangs sowie die aktuellen Versionen des LCOS-Betriebssystems finden Sie auf der LANCOM-Webseite.

Modellvarianten

Das vorliegende Benutzerhandbuch gilt für die folgenden Modelle:

- LANCOM 1722 VoIP
- LANCOM 1723 VoIP
- LANCOM 1724 VoIP
- LANCOM 1823 VoIP

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 VoIP 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.

Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

- Installation Guide
- Benutzerhandbuch
- Handbuch TK-Anlagenfunktionen
- Menü-Referenz

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.

Im Handbuch TK-Anlagenfunktionen finden Sie eine ausführliche Schritt-für-Schritt-Anleitung, um einen LANCOM VoIP Router als Telefonanlage für einen Einzelstandort in Betrieb zu nehmen. Ferner werden dort die wichtigsten Bedienungshinweise für Teilnehmer und den Anschluss von Endgeräten beschrieben.

Das Referenzhandbuch befindet sich als Acrobat-Dokument (PDF-Datei) unter www.lancom.eu/download oder auf dem beiliegenden Datenträger (CD/DVD). 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)
- Funknetzwerke (WLAN)
- Sprachkommunikation in Computernetzwerken mit Voice-over-IP (VoIP)
- Backup-Lösungen
- LANCAPI
- weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

■ Kapitel :

Die Menü-Referenz (ebenfalls unter www.lancom.eu/download oder auf der beiliegenden Datenträger (CD/DVD)) beschreibt alle Parameter von LCOS, dem Betriebssystem der LANCOM-Geräte. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte mit WEBconfig bzw. über die Konsole (Telnet).

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.eu



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

Hinweis-Symbole



Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.



Wichtiger Hinweis, der beachtet werden sollte.



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

Inhalt

1 Einleitung	11
1.1 Wie funktionieren ADSL und ADSL 2+?	11
1.2 Welchen Nutzen bietet VPN?	13
1.3 Firewall	15
1.4 Voice-over-IP	16
1.4.1 Anwendungsbeispiele	16
1.4.2 Die zentrale Position der LANCOM VoIP Router	22
1.4.3 VoIP-Eigenschaften der LANCOM VoIP Router	25
1.5 Was kann Ihr LANCOM?	27
2 Installation	34
2.1 Lieferumfang	34
2.2 Systemvoraussetzungen	35
2.2.1 Konfiguration der LANCOM-Geräte	35
2.2.2 Betrieb der Access Points im Managed-Modus	35
2.3 Der LANCOM Router stellt sich vor	35
2.3.1 Statusanzeigen	35
2.3.2 Die Anschlüsse des Geräts	42
2.4 Installation der Hardware	45
2.5 Konfiguration der ISDN- und Analog-Schnittstellen	48
2.6 Installation der Software	49
2.6.1 Software-Setup starten	49
2.6.2 Welche Software installieren?	51
3 Grundkonfiguration	52
3.1 Welche Angaben sind notwendig?	52
3.1.1 TCP/IP-Einstellungen	52
3.1.2 Konfigurationsschutz	54
3.1.3 Einstellungen für das Funk-LAN	55
3.1.4 Gebührenschatz	56
3.2 Anleitung für LANconfig	56
3.3 Anleitung für WEBconfig	57
3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs	61

4 Den Internet-Zugang einrichten	63
4.1 Der Internet-Assistent	65
4.1.1 Anleitung für LANconfig	65
4.1.2 Anleitung für WEBconfig	66
5 Konfiguration der VoIP-Funktionen	67
6 Zwei Netzwerke verbinden	68
6.1 Welche Angaben sind notwendig?	69
6.1.1 Allgemeine Angaben	69
6.1.2 Einstellungen für den TCP/IP-Router	71
6.1.3 Einstellungen für NetBIOS-Routing	73
6.2 Anleitung für LANconfig	73
6.3 1-Click-VPN für Netzwerke (Site-to-Site)	74
6.4 Anleitung für WEBconfig	76
7 Einwahl-Zugang bereitstellen	77
7.1 Welche Angaben sind notwendig?	78
7.1.1 Allgemeine Angaben	78
7.1.2 Einstellungen für TCP/IP	79
7.1.3 Einstellungen für NetBIOS-Routing	80
7.2 Einstellungen am Einwahl-Rechner	80
7.2.1 Einwahl über VPN	80
7.2.2 Einwahl über ISDN	80
7.3 Anleitung für LANconfig	81
7.4 1-Click-VPN für LANCOM Advanced VPN Client	81
7.5 Anleitung für WEBconfig	83

8	Erweiterte WLAN-Konfiguration	84
8.1	WLAN-Konfiguration mit dem Assistenten von LANconfig	84
8.2	Konfiguration der Punkt-zu-Punkt-Verbindungen	86
8.2.1	Geometrische Auslegung von Outdoor-Funknetz-Strecken	87
8.2.2	Ausrichten der Antennen für den P2P-Betrieb	91
8.2.3	Vermessung von Funkstrecken	93
8.2.4	Punkt-zu-Punkt-Betriebsart aktivieren	94
8.2.5	Konfiguration der P2P-Verbindungen	95
8.2.6	Sicherheit von Punkt-zu-Punkt-Verbindungen	98
8.3	Konfiguration des Client-Modus	100
8.3.1	Client-Einstellungen	100
8.3.2	SSID des verfügbaren Netzwerks einstellen	101
8.3.3	Verschlüsselungseinstellungen	102
8.3.4	Roaming	103
9	Faxe versenden mit der LANCAPI	105
9.1	Installation des LANCOM CAPI Faxmodem	106
9.2	Installation des MS Windows Faxdienstes	107
9.3	Versenden eines Faxes	108
9.3.1	Faxe versenden mit beliebigen Büroanwendungen	108
9.3.2	Faxe versenden mit dem Windows Faxdienst	109
10	Optionen und Zubehör	110
10.1	Optionale AirLancer Extender Antennen	110
10.1.1	Antenna Diversity	111
10.1.2	Polarisations-Diversity	111
10.1.3	Installation der AirLancer Extender Antennen	111
10.2	LANCOM Public Spot Option	112

11 Sicherheits-Einstellungen	114
11.1 Sicherheit im Funk-LAN	114
11.1.1 Verschlüsselung des Datentransfers	114
11.1.2 802.1x / EAP	117
11.1.3 LANCOM Enhanced Passphrase Security	117
11.1.4 Zugangskontrolle über MAC-Adresse	118
11.1.5 IPSec-over-WLAN	118
11.2 Der Sicherheits-Assistent	118
11.2.1 Assistent für LANconfig	119
11.2.2 Assistent für WEBconfig	120
11.3 Die Sicherheits-Checkliste	120
12 Konfiguration der ISDN- und Analog-Schnittstellen im Detail	125
12.1 ISDN-Schnittstelle im NT- oder TE-Modus	125
12.2 Buserminierung, Life-Line-Support und Spannungsversorgung	126
12.3 Protokoll-Einstellung	129
12.4 Taktung der ISDN-Anschlüsse	130
13 Rat & Hilfe	132
13.1 Es wird keine DSL-Verbindung aufgebaut	132
13.2 DSL-Übertragung langsam	132
13.3 Unerwünschte Verbindungen mit Windows XP	133
14 Anhang	134
14.1 Leistungs- und Kenndaten	134
14.2 Anschlussbelegung	138
14.2.1 ADSL-Schnittstelle	138
14.2.2 ISDN-Schnittstelle ☒	138
14.2.3 ISDN-Schnittstelle ☎	139
14.2.4 ISDN/Analog-Schnittstelle ☒	139
14.2.5 Analog-Schnittstelle ☎	140
14.2.6 Ethernet-Schnittstellen 10/100Base-T	140
14.2.7 Konfigurationsschnittstelle (Outband)	141
14.3 CE-Konformitätserklärungen	141

1 Einleitung

Die LANCOM VoIP Router sind vollwertige Router und ermöglichen mit der integrierten Firewall einen sicheren Internetzugang für das lokale Netzwerk.

Mit der enthaltenen VPN-Option arbeiten die Geräte als leistungsfähige Dynamic VPN Gateways für Außenstellen oder mobile Nutzer.

Neben dem ADSL-Anschluss verfügen die Geräte auch über ISDN- und teilweise über analoge Telefon-Anschlüsse. Eine ISDN-Leitung kann als Backup für die WAN-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 sowie die ISDN- und Analog-Anschlüsse auch zum Übertragen von Sprache nutzen.

Nur LANCOM 1823
VoIP



LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points mit eigener Konfiguration betrieben werden (WLAN-Module in der Betriebsart „Access Point-Modus“) oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller gesteuert wird (Betriebsart „Managed-Modus“). Bitte beachten Sie die entsprechenden Hinweise dazu in dieser Dokumentation.

LANCOM VoIP Router können durch die LANCOM Content Filter-Option für eine flexible Steuerung des Internet-Zugriffs aufgerüstet werden. Die intelligente Highend-Lösung nutzt eine datenbankgestützte Web-Filtertechnologie, die profilbasierte Berechtigungen sowie praktische Funktionen wie Overrides ermöglicht. Die Nutzung des Content Filters erfordert die Betriebssystemversion LCOS 8.0.

1.1 Wie funktionieren ADSL und ADSL 2+?

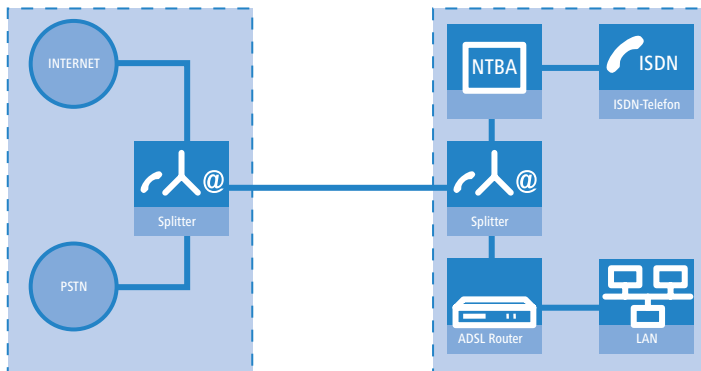
ADSL (Asymmetric Digital Subscriber Line) ist die zur Zeit häufigste Anschluss-technik für digitale Breitbandanschlüsse ins Internet. Bei den DSL-Technologien werden die normalen und ohnehin meist vorhandenen Telefonleitungen (analog oder ISDN) zur Datenübertragung bis zur nächsten Vermittlungsstelle 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.

In die LANCOM VoIP Router ist ein Modem für ADSL/ADSL 2+ integriert. Sie können mit dem mitgelieferten Kabel direkt an den Splitter angeschlossen werden.



Der Betrieb von ADSL ist sowohl über ISDN- als auch über analoge Telefonschlüsse (POTS – **P**lain **O**ld **T**elephone **S**ervice) möglich. Geräte mit integriertem ADSL-Modem werden jeweils in zwei Versionen angeboten. Die Angabe des unterstützten Telefonsystems finden Sie auf der Typenbezeichnung auf der

Unterseite des Geräts. Der Gerätename ist auf dem Etikett mit einem Zusatz versehen, der für das unterstützte Telefonsystem steht:

Zusatz	Unterstütztes Telefonsystem
'Annex A'	ADSL-over-POTS
'Annex B'	ADSL-over-ISDN

Ein Gerät vom Typ 'Annex A' kann ausschließlich an ADSL-over-POTS-Anschlüssen betrieben werden. Ein Gerät vom Typ 'Annex B' kann ausschließlich an einem ADSL-over-ISDN-Anschluss betrieben werden. Welche Variante Sie benötigen, erfahren Sie von Ihrem Netzbetreiber. Die nachträgliche Umrüstung eines Gerätes auf das jeweils andere Telefonsystem ist nicht möglich.

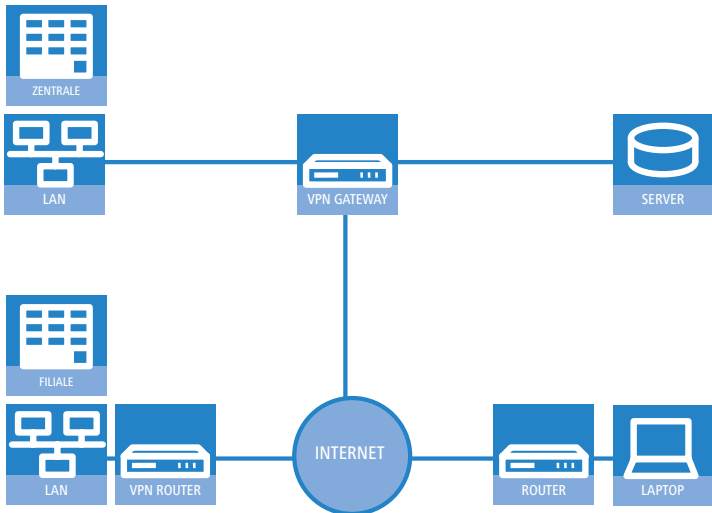
Es existieren auch ADSL-over-ISDN-Anschlüsse, die nicht in Kombination mit einem ISDN-Anschluss, sondern mit einem herkömmlichen analogen Telefonsanschluss betrieben werden. In Deutschland sind beispielsweise alle von der Deutschen Telekom AG bereitgestellten T-DSL-Anschlüsse als ADSL-over-ISDN-Anschlüsse ausgeführt.

1.2 Welchen Nutzen bietet VPN?

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

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

■ Kapitel 1: Einleitung



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.

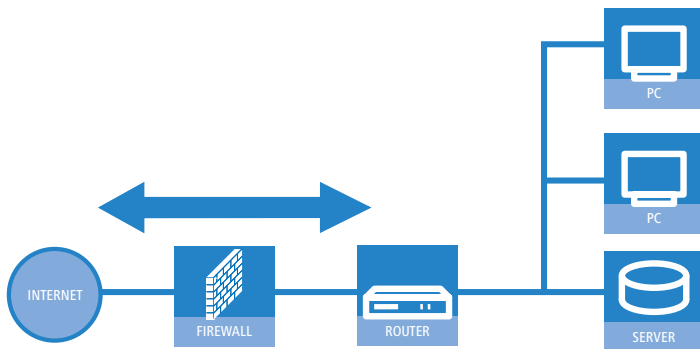
Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über

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 Firewall

Die integrierte Stateful-Inspection-Firewall verhindert wirksam ein Eindringen von ungewolltem Datenverkehr in das eigene Netzwerk, indem eingehender Datenverkehr nur als Reaktion auf ausgehenden Datenverkehr zugelassen wird. Die IP-Masquerading-Funktion im Router versteckt beim Zugang ins Internet alle Arbeitsstationen im LAN hinter einer einzigen öffentlichen IP-Adresse. Die tatsächlichen Identitäten (IP-Adressen) der einzelnen Stationen bleiben verborgen. Firewall-Filter im Router erlauben die gezielte Sperrung von IP-Adressen, Protokollen und Ports. Mit MAC-Adressfiltern kann auch der Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion des Gerätes gezielt kontrolliert werden.



Weitere wichtige Features der Firewall sind:

■ Intrusion Detection

Einbruchsversuche in das lokale Netzwerk oder auf die zentrale Firewall werden über das Intrusion-Detection-System (IDS) des LANCOM erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYS-LOG-Alarmen gewählt werden.

■ Denial-of-Service-Protection

Angriffe aus dem Internet können neben Einbruchsversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Daher ist der LANCOM mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit der Router garantieren.

■ Quality-of-Service/Traffic management

Unter dem Oberbegriff Quality-of-Service (kurz: QoS) sind die Funktionen des LANCOM zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstegütern befassen. Die QoS-Funktionen berücksichtigen das Ergebnis der mächtigen Klassifizierungsmethoden der Firewall (z.B. Einschränkung auf Subnetze, einzelne Arbeitsstationen oder bestimmte Dienste). Dadurch ist eine sehr präzise Steuerung der Dienstegütern möglich.

Mit garantierten Mindestbandbreiten geben Sie Vorfahrt für unternehmenskritische Applikationen, VoIP-Telefonie oder bestimmte Benutzergruppen.



Details zur Funktion der Stateful-Inspection-Firewall entnehmen Sie bitte dem Referenzhandbuch.

1.4 Voice-over-IP



Voice-over-IP (VoIP) steht für Sprachkommunikation in Computernetzwerken auf Basis des Internet Protokolls (IP). Die Kernidee ist, Funktionen der klassischen Telefonie über kostengünstige und weit verbreitete Netzwerkstrukturen wie z.B. das LAN oder das Internet bereit zu stellen. VoIP selbst ist dabei kein Standard, sondern nur ein Sammelbegriff für verschiedene Technologien (Endgeräte, Protokolle, Sprachkodierung usw.) mit denen die Sprachkommunikation in IP-Netzwerken ermöglicht wird.

1.4.1 Anwendungsbeispiele

Voice-over-IP-Lösungen bringen Ihre Vorteile in einem sehr breiten Anwendungsspektrum ein, angefangen von kleinen Unternehmen bis hin zu großen Konzernen mit ausgedehntem Filialbetrieb. In diesem Abschnitt stellen wir einige Beispiele vor.



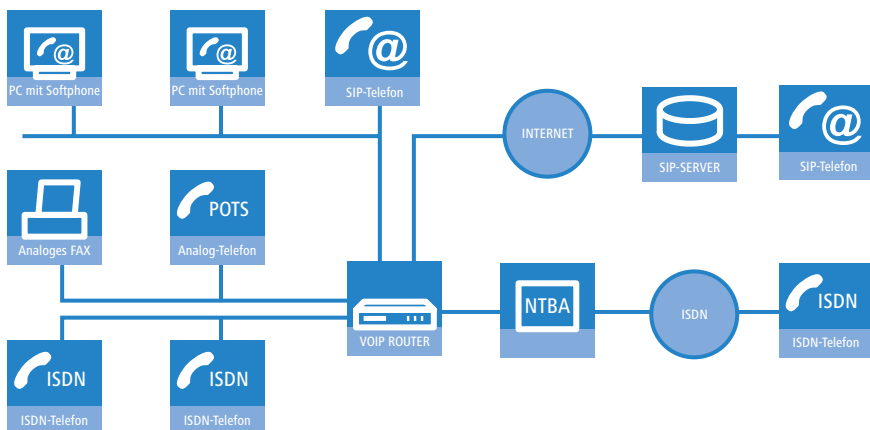
Konkrete Hinweise zur Konfiguration finden Sie im Handbuch TK-Anlagenfunktionen oder im LCOS-Referenzhandbuch.

Verwendung als Telefonanlage

LANCOM VoIP Router können in vielen Fällen eine lokale Telefonanlage vollständig ersetzen. Mit bis zu acht Sprachkanälen (z.B. LANCOM 1724 VoIP) zum Festnetz und der Möglichkeit, SIP-Accounts oder SIP-Trunking einzusetzen sowie Standorte für Sprache und Daten zu vernetzen stellen sie leistungsstarke und zukunftsorientierte Alternativen zu herkömmlichen Telefonanlagen dar.

Eine systematische Anleitung zur Einrichtung der LANCOM VoIP Router für diesen Zweck finden Sie im Handbuch TK-Anlagenfunktionen. Informieren Sie sich zuvor in den folgenden Kapiteln über die grundsätzliche Geräte- und Software-Einrichtung und führen Sie eine Grundkonfiguration durch. Einen Internetanschluss sollten Sie ebenfalls konfigurieren, bevor Sie mit den Einstellungen für die TK-Anlagenfunktionen fortfahren.

Beispiel: LANCOM VoIP Router als TK-Anlage

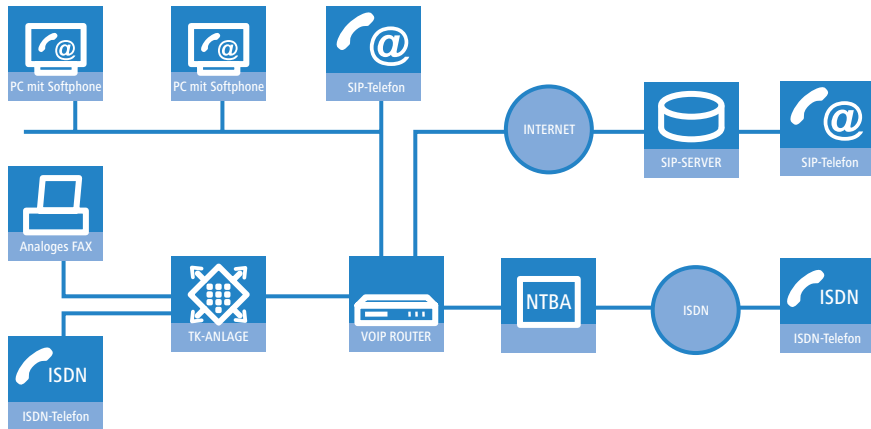


Ergänzung bestehender TK-Anlagen

Bestehende Telefonstrukturen können durch den Einsatz eines LANCOM VoIP Router sehr komfortabel um VoIP-Funktionen erweitert werden. Der LANCOM VoIP Router wird dabei einfach zwischen den öffentlichen Telefonanschluss (z.B. ISDN-NTBA oder Analog-Anschluss) und die TK-Anlage geschaltet.

■ Kapitel 1: Einleitung

Beispiel: ISDN-TK-Anlage



Über die TK-Anlage und die angeschlossenen Telefone sind weiterhin alle Gespräche wie zuvor möglich, auch die Erreichbarkeit unter den bekannten Telefonnummern bleibt erhalten. Zusätzlich bietet diese Anwendung folgende Möglichkeiten:

- Zu den bisher verwendeten ISDN- und Analog-Telefonen können auch SIP-Telefone oder SIP-Softphones in die Telefonstruktur aufgenommen werden.
 - Die SIP-Teilnehmer im eigenen LAN können auch die externen Teilnehmer im öffentlichen Telefonnetz erreichen.
 - Die ISDN- und Analog-Telefone lassen sich weiterhin verwenden, können aber zusätzlich die internen SIP-Telefone sowie SIP-Softphones im LAN erreichen.
- Gespräche mit externen SIP-Teilnehmern im Netz des eigenen Internetproviders können bei vielen Anbietern kostenlos geführt werden.
- Mit der Verbindung zu einem öffentlichen SIP-Provider können auch andere SIP-Teilnehmer erreicht werden. Alternativ zur direkten Telefon-Verbindung lassen sich Teilnehmer in öffentlichen Telefonnetzen auch über den Umweg eines SIP-Providers erreichen. Die Gebühren richten sich nach den Tarifen der jeweiligen Anbieter. Für Fern- und Auslandsgespräche ist in vielen Fällen die Nutzung des SIP-Providers deutlich günstiger als die klassische Telefonverbindung.

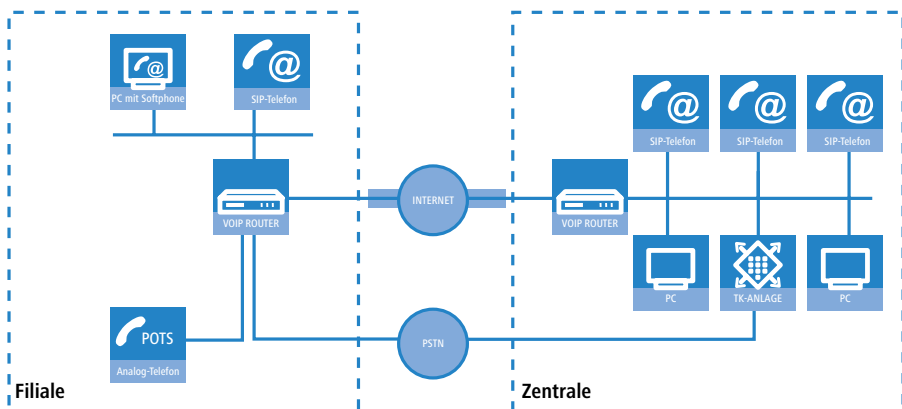
Der LANCOM VoIP Router übernimmt in diesem Aufbau die Vermittlung der Gespräche. Aufgrund der individuellen Konfiguration des Gerätes kann z.B. anhand bestimmter Vorwahlbereiche entschieden werden, ob ein Telefonanruf über die ISDN-Schnittstelle oder als VoIP-Gespräch über das Internet erfolgen soll.

Anbindung von Filialen oder Heimarbeitsplätzen an die Zentrale

Viele Filialen oder Heimarbeitsplätze sind schon über VPN an das Netz der Zentrale angebunden. Allerdings beschränkt sich die Anbindung in vielen Fällen nur auf die Datenübertragung. Mit dem Einsatz von VoIP können die firmeninternen Gespräche über die ohnehin vorhandene VPN-Verbindung kostenlos und – dank der VPN-Verschlüsselung – abhörsicher geführt werden.

Mit dem Einsatz eines LANCOM VoIP Router in der Filiale bzw. am Heimarbeitsplatz erschließen sich die klassische Telefonwelt über ISDN- bzw. Analog-Anschlüsse und VoIP-Telefonie mit nur einem einzigen Telefon: als Endgerät kann ein vorhandenes Analog- bzw. ISDN-Telefon oder ein SIP-Telefon verwendet werden, um eine gebührenfreie Telefon-Verbindung per VPN zur Zentrale oder auch eine Verbindung über das klassische Telefonnetz aufzunehmen.

Beispiel: Filiale mit analogem Telefonanschluss, Zentrale mit SIP-fähiger ISDN-TK-Anlage



Die Vorteile der Telefon-Anbindung an die Zentrale:

- Die Konfiguration der Telefonfunktionen kann an einer Stelle in der VoIP-TK-Anlage der Zentrale vorgenommen werden.

■ Kapitel 1: Einleitung

- Die Teilnehmer aus den Heimbüros oder den Filialen melden sich an der zentralen TK-Anlage an.
- Gespräche innerhalb des Firmennetzwerks werden kostenlos geführt.
- Bei den ausgehenden Gesprächen kann je nach Verbindungs- oder Kostensituation automatisch entschieden werden, welche Leitung genutzt werden soll.

VoIP für Unternehmen mit SIP-Trunking

Eine der größten Hürden für einen vollständigen Umstieg von Unternehmen auf VoIP-Lösungen stellt die Beibehaltung der verwendeten Rufnummern dar. Die üblichen SIP-Accounts bei den entsprechenden Providern bieten zwar teilweise Rufnummern für den Übergang in das Telefon-Festnetz an, dabei handelt es sich in der Regel aber um einzelne Rufnummern aus einen „Pool“ des Providers. Für Unternehmen mit einer größeren Anzahl an Telefonteilnehmern und Rufnummern ist aber die Übernahme der bisherigen Rufnummern und die „Durchwahlfähigkeit“ ein entscheidendes Kriterium bei der Migration zu VoIP. Mit der Funktion SIP-Trunking können LANCOM VoIP Router komplette Rufnummernbereiche aus Stammnummern und zugehörigen Durchwahlen auf eine einzige Verbindung zu einem SIP-Provider abbilden, wenn dieser ebenfalls das Direct Dialing In (DDI) unterstützt und mehrere gleichzeitige Verbindungen anbietet. Die SIP-Provider bieten mit dem SIP-Trunking üblicherweise auch die Übernahme der verwendeten Rufnummern vom bisherigen Telefonanbieter an.

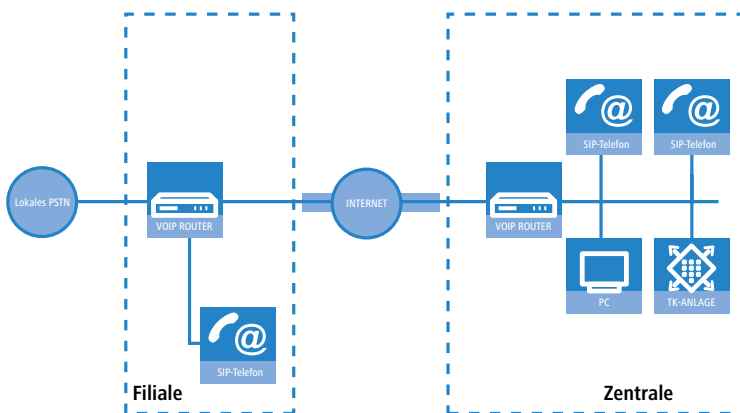
Einbindung lokaler Amts-Anschlüsse mit SIP-Remote-Gateway

Die Netzwerke an national oder international verteilten Unternehmens-Standorten sind oft schon über VPN verbunden. Mit einem LANCOM VoIP Router können nicht nur die SIP- sowie ISDN- oder Analog-Telefone einer Filiale an die SIP-TK-Anlage der Zentrale angebunden werden, auch die lokalen Amtsleitungen der Filiale können mit der Funktion „SIP-Remote-Gateway“ in die Unternehmenskommunikation eingebunden werden.

Das SIP-Remote-Gateway ist für abgehende und ankommende Rufe aktiv:

- Eine Zentrale in Hamburg kann z.B. einen LANCOM VoIP Router mit SIP-Gateway in der Filiale im München nutzen, um Gespräche mit den Kunden und Lieferanten im Ortsbereich München zu den Gebühren für Ortsgespräche zu führen („local break out“).

- Um für die Kunden in einem anderen Land besser erreichbar zu sein, kann die Zentrale in Hamburg z.B. einen LANCOM VoIP Router mit SIP-Remote-Gateway am Vertriebsstandort in Italien nutzen. Die Kunden können den Support oder Service dann über eine entsprechende nationale Service-Rufnummer erreichen. Die Rufe werden auf dem lokalen Amts-Anschluss angenommen und im Netz des Unternehmens an einen freien oder zuständigen Mitarbeiter zugestellt. Über das Call-Routing können dabei z.B. anhand der Rufnummer des Kunden bestimmte Anschlüsse für die Weiterleitung ausgewählt werden.



Die Vorteile des SIP-Remote-Gateways:

- Der lokale Amts-Anschluss an einem bestimmten Standort steht allen Standorten im gesamten Unternehmen zur Verfügung.
- Nationale und internationale Ferngespräche können auf Ortsgespräche oder regionale Gespräche abgebildet werden und so Kosten einsparen.
- Automatisches Routing von eingehenden Rufen zu zuständigen Mitarbeitern.

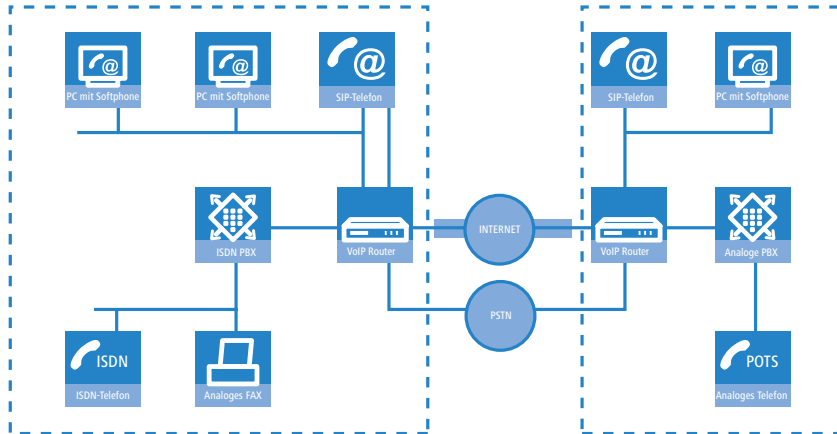
Verbindung von Standorten ohne SIP-TK-Anlage

Auch verteilte Unternehmen ohne eigene SIP-TK-Anlage können die Vorteile der VoIP-Standortverbindung nutzen. In diesem „Peer-to-Peer“-Szenario werden an beiden Standorten LANCOM VoIP Router eingesetzt.

Neben der Datenübertragung über VPN können auch die VoIP-Funktionen zwischen den beiden Standorten genutzt werden.

■ Kapitel 1: Einleitung

Beispiel: Standorte mit ISDN- bzw. Analog-Anschlüssen



Die Vorteile der Peer-to-Peer-Standortverbindung

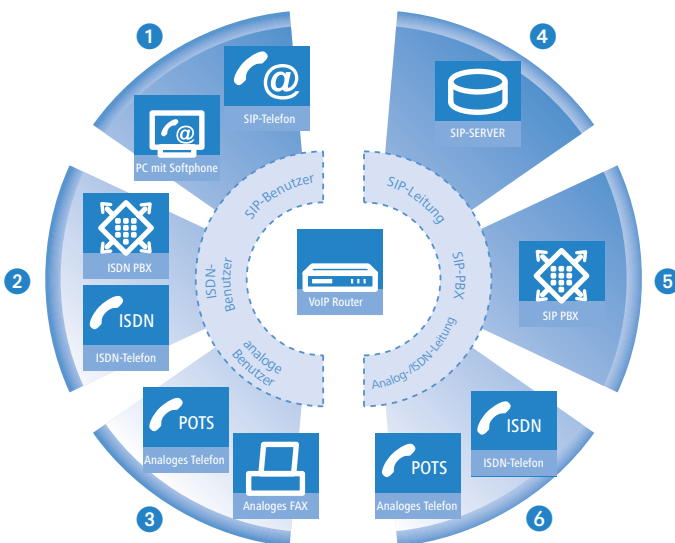
- ISDN- und Analog-TK-Anlagen an verschiedenen Standorten lassen sich zu einem gemeinsamen internen Telefonnetz zusammenschalten.
- Keine SIP-TK-Anlage erforderlich.
- Gespräche innerhalb des Firmennetzwerks werden gebührenfrei geführt.
- Bei den ausgehenden Gesprächen kann je nach Verbindungs- oder Kostensituation entschieden werden, welche Leitung genutzt werden soll.
- Eingehende Gespräche können direkt an die entsprechenden Mitarbeiter eines anderen Standorts vermittelt werden.

1.4.2 Die zentrale Position der LANCOM VoIP Router

LANCOM VoIP Router nehmen eine zentrale Position bei der Vermittlung von Telefongesprächen zwischen internen und externen Gesprächsteilnehmern über verschiedene Kommunikationswege ein. Je nach Modell und Ausstattung verbinden die Geräte die folgenden Kommunikationsteilnehmer und -wege zu einer gemeinsamen Telefonstruktur:

- 1 die intern an LAN, WLAN und DMZ angeschlossenen VoIP-Endgeräte wie SIP-Telefone und SIP-Softphones
- 2 die interne Telefon-Infrastruktur mit ISDN- oder Analog-TK-Anlage sowie ISDN- und Analog-Telefonen

- 3 die analogen Endgeräte, intern eingebunden in das ISDN-Netz entweder über eine TK-Anlage mit a/b-Ports oder alternativ über einen ATA (Analog-Telefon-Adapter) in das VoIP-Netz
- 4 externe SIP-Provider mit allen über den jeweiligen Provider erreichbaren, externen Gesprächsteilnehmern
- 5 übergeordnete SIP-TK-Anlagen mit allen über diese Anlage erreichbaren, internen und externen Gesprächsteilnehmern
- 6 die externe Telefon-Welt über einen Amts-Anschluss oder eine übergeordnete TK-Anlage mit allen über das Festnetz erreichbaren, externen Gesprächsteilnehmern



Benutzer und Leitungen

Telefonie-Teilnehmer in internen Bereichen können in der Sprachkommunikation aktiv werden und werden in der LANCOM VoIP-Umgebung als „Benutzer“ bezeichnet. Das LANCOM unterscheidet dabei:

■ ISDN-Benutzer

Maximal 40 über das ISDN-Netz angeschlossene Endgeräte, inkl. der an einer übergeordneten ISDN-TK-Anlage angeschlossenen ISDN- und Analog-Endgeräte.

■ Kapitel 1: Einleitung

Bei der Anbindung von untergeordneten TK-Anlagen an Anlagenanschlüsse wird die Anzahl der möglichen ISDN-Teilnehmer durch die Länge der Durchwahl (DDI) festgelegt. In diesem Fall können alle an der TK-Anlage angeschlossenen Endgeräte mit einem einzigen ISDN-Benutzer-Eintrag abgebildet werden.

■ Analog-Benutzer

Zwei an den analogen Schnittstellen angeschlossene Endgeräte.

■ SIP-Benutzer

Maximal 32 über LAN, WLAN und DMZ angeschlossene SIP-Endgeräte sowie die über ATA angeschlossenen analogen Endgeräte.

Die externen Kommunikationswege für die Benutzer werden als „Leitungen“ bezeichnet. Das LANCOM kennt die folgenden Leitungen:

■ ISDN

Ein Anschluss an einen ISDN-NTBA über die TE-Schnittstelle. Zusätzlich können an die NT-Schnittstelle ISDN-Endgeräte direkt oder über eine untergeordnete ISDN-TK-Anlage angeschlossen werden.

■ Analog

Ein Anschluss an einen analogen Amts-Anschluss oder an einen Nebenstellenanschluss einer übergeordneten Analog-TK-Anlage.

■ SIP-Leitungen

Maximal 16 SIP-Leitungen. Für die SIP-Leitungen werden drei Varianten unterschieden:

- Als „Einzel-Account“-Leitung verhält sich die Leitung wie ein üblicher SIP-Account mit einer einzigen Rufnummer. Die internen Benutzer können diesen Account gemeinsam für SIP-Telefonate nutzen, dabei ist immer nur ein Gespräch zur gegebenen Zeit möglich.

Je nach Angebot des Providers können über diese Leitungen die Teilnehmer im Netz des Providers, die Teilnehmer in anderen SIP-Netzen (Partner-Netze) oder auch die Teilnehmer im Festnetz erreicht werden. Auch die eigene Erreichbarkeit über eine Rufnummer aus dem Festnetz oder nur über SIP-Namen aus dem Internet ist je nach Anbieter verschieden.

- Als „Trunk“-Leitung verhält sich die Leitung wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die internen Benutzer nutzen diesen Account parallel, es sind mehrere

Gespäche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite).

- Als „SIP-Gateway“-Leitung stellt der LANCOM VoIP Router für eine entfernte SIP-TK-Anlage einen Übergang in ein lokales ISDN-Netz her. Das SIP-Gateway wird mit einer einzigen Nummer bei der SIP-TK-Anlage registriert, es sind allerdings mehrere Gespräche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite). Die Verbindung zwischen der SIP-TK-Anlage und dem LANCOM VoIP Router wird üblicherweise über eine VPN-Verbindung hergestellt.
- Eine „Link“-Leitung verhält sich wie eine Trunk-Leitung jedoch ohne die Beschränkung auf eine Stammnummer mit Durchwahlnummern. Die internen Benutzer nutzen diesen Account parallel, es sind mehrere Gespräche gleichzeitig möglich (bis zur maximalen Ausnutzung der verfügbaren Bandbreite).

■ SIP-PBX-Leitungen

Maximal 4 Verbindungen zu übergeordneten SIP-TK-Anlagen. Bei diesen Leitungen handelt es sich in der Regel um Verbindungen zu großen TK-Anlagen, die im Netzwerk der Zentrale stehen und die über einen VPN-Verbindung erreicht werden können.



Die genaue Anzahl der möglichen Benutzer und Leitungen kann je nach Modell bzw. Software-Option variieren.

1.4.3 VoIP-Eigenschaften der LANCOM VoIP Router

Mehrere ISDN/Analog-Schnittstellen

Die ISDN/Analog-Schnittstellen der LANCOM VoIP Router, die sich als interne oder externe Anschlüsse schalten lassen, bieten je nach Modell bis zu acht parallele Sprachkanäle. Damit lässt sich z.B. eine bestehende TK-Anlage um SIP erweitern und zusätzlich an eine übergeordnete VoIP-TK-Anlage anbinden. Teilnehmer können gleichzeitig lokal mit ISDN- und Analog-Telefonen, SIP-Geräten und Softphones Gespräche mit anderen Telefon-Teilnehmern intern wie extern führen. Die Wandlung zwischen SIP und ISDN bzw. Analog erfolgt automatisch und für den Benutzer transparent.

Telefonieren auch bei Stromausfall

Mit Life-Line-Support und Spannungsweiterleitung zum internen ISDN-Port bleibt Telefonieren über das klassische Telefonnetz sogar bei Stromausfall

möglich. ISDN-Backup, Loadbalancing und VRRP in Kombination mit der Nutzung von Ethernetports als WAN-Interfaces bieten auch für SIP-Verbindungen Redundanz und hohe Zuverlässigkeit. Bei Ausfall einer SIP-Gegenstelle wird automatisch über das klassische Telefonnetz vermittelt. Damit bleibt Telefonieren auch mit VoIP so sicher wie gewohnt.

Punkt-zu-Mehrpunkt und Punkt-zu-Punkt-Anschlüsse bei ISDN

LANCOM VoIP Router unterstützen im ISDN-Bereich Punkt-zu-Mehrpunkt- und Punkt-zu-Punkt-Anschlüsse:

- Punkt-zu-Mehrpunkt-Anschluss (Point-to-Multipoint): An einen solchen Anschluss können bis zu acht ISDN-Endgeräte direkt angeschlossen werden. Bei den Endgeräten handelt es sich z.B. um ISDN-Telefone, aber auch um ISDN-TK-Anlagen, an die weitere Endgeräte angeschlossen werden. Alternativ kann auch ein LANCOM VoIP Router an einen Punkt-zu-Mehrpunkt-Anschluss angeschlossen werden.
- Punkt-zu-Punkt-Anschluss (Point-to-Point): An einen solchen Anschluss kann nur ein ISDN-Endgerät (meistens eine ISDN-TK-Anlage) angeschlossen werden. Alternativ kann auch ein LANCOM VoIP Router an einen Punkt-zu-Punkt-Anschluss angeschlossen werden.

Zum Anschluss eines LANCOM VoIP Router wird das verwendete Interface auf den jeweiligen Anschlussstyp eingestellt.

Die Endgeräte an einem ISDN-Anschluss können auf zwei Arten adressiert werden:

- Die Endgeräte werden über eine Multiple Subscriber Number (MSN) angesprochen, die fest mit dem ISDN-Anschluss verbunden ist und nicht beeinflusst werden kann.
- Die Endgeräte werden über eine Direct Dialing In-Nummer (DDI) angesprochen. Dabei ist nur die „Stammnummer“ mit dem Anschluss verbunden, die Durchwahlnummern zur Adressierung bestimmter Endgeräte werden frei gewählt und an die Stammnummer angehängt. Dabei darf die Stammnummer mit Durchwahl zusammen mit der Ortsnetzvorwahl (ohne führende Null) maximal 11 Zeichen lang sein.



Die Bezeichnungen „Mehreräte-Anschluss“ und „Anlagen-Anschluss“ werden u.a. in Deutschland zur Bezeichnung der technischen Ausführungen Point-to-Multipoint mit MSN bzw. Point-to-Point mit DDI verwendet. In anderen Ländern können die

Anschlussarten durchaus andere Kombinationen aus Protokoll und Rufnummertyp sowie abweichende Namen verwenden. Bitte informieren Sie sich bei Ihrem Netzanbieter über die technischen Spezifikationen Ihres ISDN-Anschlusses.

Bandbreitenreservierung mit Ausfallsicherung

Leistungsstarke VPN-Funktionen ermöglichen die sichere Übertragung von Sprache und Daten zwischen Unternehmensstandorten. Damit lassen sich Telefongebühren für die interne Kommunikation einsparen. Eine professionelle Firewall, vielseitige Routingfunktionen und hochwertige Quality-of-Service-Mechanismen machen den LANCOM VoIP Router zur umfassenden Lösung für sichere Sprach- und Datenkommunikation in einem kompakten Gerät. Alle Funktionalitäten sind in das zentrale Management integriert.

1.5 Was kann Ihr LANCOM?

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

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Anwendungen				
Internet-Zugang	✓	✓	✓	✓
LAN-LAN-Kopplung über VPN	✓	✓	✓	✓
LAN-LAN-Kopplung über ISDN	✓	✓	✓	✓
RAS-Server (über VPN)	✓	✓	✓	✓
RAS-Server (über ISDN)	✓	✓	✓	✓
IP-Router	✓	✓	✓	✓
NetBIOS-Proxy zur Kopplung von Microsoft-Peer-to-Peer-Netzwerken über ISDN	✓	✓	✓	✓
DHCP- und DNS-Server (für LAN und DMZ)	✓	✓	✓	✓
Advanced Routing and Forwarding (ARF-Netze)	16	16	16	16
N:N-Mapping zum Routen von Netzwerken mit den gleichen IP-Adresskreisen über VPN	✓	✓	✓	✓

■ Kapitel 1: Einleitung

DE

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Configuration von LAN-Ports als zusätzliche WAN-Ports		✓	✓	✓	✓
Policy-based Routing zur regelbasierten Auswahl der Zielroute		✓	✓	✓	✓
Load-Balancing zur Bündelung von mehreren DSL-Kanälen		4 Kanäle	2 Kanäle	2 Kanäle	2 Kanäle
Backup-Lösungen und Load-Balancing mit VRRP		✓	✓	✓	✓
PPPoE-Server		✓	✓	✓	✓
WAN-RIP		✓	✓	✓	✓
Rapid-Spanning-Tree-Protokoll					✓
Layer-2-QoS-Tagging		✓	✓	✓	✓
802.1p		✓	✓	✓	✓
NAT Traversal (NAT-T)		✓	✓	✓	✓
DMZ mit konfigurierbarer IDS-Prüfung		✓	✓	✓	✓
ISDN-Festverbindungen		✓	✓	✓	✓
LANCAPI-Server für den Einsatz von Office-Anwendungen wie Fax oder Anrufbeantworter über die ISDN-Schnittstelle.		✓	✓	✓	✓
VoIP-Funktionen 					
SIP-Proxy und -Registrar	Verwaltung lokaler SIP-Benutzer (Anmeldung/Authentifizierung)	✓	✓	✓	✓
	Abbildung von Konten bei SIP-Providern als Leitungen	✓	✓	✓	✓
	SIP-Trunking zur Abbildung von SIP-Accounts mit Stamm- und Durchwahlnummern	✓	✓	✓	✓
	Anmeldung bei und Vermittlung zu übergeordneten SIP-TK-Anlagen	✓	✓	✓	✓
	Individuelles/gemeinsames Passwort zur Authentifizierung	✓	✓	✓	✓
	Automatische Anmeldung und Weiterleitung von SIP-Benutzern	✓	✓	✓	✓

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
	✓	✓	✓	✓
	8	8	8	8
SIP-Gateway	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	✓
	40	40	40	40
	–	2	–	2
	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	✓
Call-Router	✓	✓	✓	✓
	✓	✓	✓	✓
	✓	✓	✓	✓

■ Kapitel 1: Einleitung

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
	Mehrfache Durchläufe, auch nach Nummernersetzung erzwungen	✓	✓	✓	✓
	Bis zu drei alternative Ziele pro Routingregel (zweifaches Backup)	✓	✓	✓	✓
	Regel-basierte Ablehnung von Rufen	✓	✓	✓	✓
	Ergänzen von Rufnummern-Präfixen pro Leitung	✓	✓	✓	✓
	Ergänzen/Entfernen von Stammnummern pro Leitung	✓	✓	✓	✓
Sprachverarbeitung	Echo-Unterdrückung und De-Jitter-Buffer gegenüber SIP-Verbindungen	✓	✓	✓	✓
	Transparente Durchleitung ausgehandelter Codecs	✓	✓	✓	✓
	Beeinflussung (Filter, Qualität, Bandbreite) der Aushandlung von Codecs	✓	✓	✓	✓
WAN-Anschlüsse					
	Anschluss für DSL- oder Kabelmodem	✓	✓	✓	✓
	integriertes ADSL-Modem (mit ADSL2+)	✓	✓	✓	✓
	ISDN-S ₀ -Anschluss im NT-Modus zum Anschluss von untergeordneten ISDN-Geräten (ISDN-Telefone, ISDN-TK-Anlagen) an LANCOM VoIP Router. Umschaltbar in TE-Modus. * Nicht zum Anschluss an externe Vermittlungsstellen (z.B. Telefonnetz) geeignet.	1 ✓	1 ✓*	2 ✓	1 ✓*
	ISDN-S ₀ -Anschluss im TE-Modus zum Anschluss der LANCOM VoIP Router an einen externen ISDN-Anschluss, z.B. an einen NTBA oder an eine übergeordnete ISDN-TK-Anlage. Umschaltbar in NT-Modus.	1 ✓	1 ✓	2 ✓	1 ✓
	Spannungsweiterleitung einer extern anliegenden ISDN-Spannung zum internen ISDN-Port zur Stromversorgung der angeschlossenen Endgeräte.	ISDN1 zu ISDN2		ISDN1 zu ISDN3	
	Geräteinterne Spannungsversorgung des ISDN-NT-Anschlusses zur Stromversorgung von maximal zwei angeschlossenen Telefonen.		✓		✓
	Analog-Anschluss zum Anschluss je eines analogen Endgerätes oder einer analogen TK-Anlage (Mehrfrequenzwahlverfahren).		2		2

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Analog-Anschluss zum Anschluss der LANCOM VoIP Router an einen analogen Amts-Anschluss oder an eine übergeordnete, analoge TK-Anlage (Mehrfrequenzwahlverfahren), kombiniert mit ISDN1.		1		1
Signal- und Spannungsweiterleitung vom analogen Amtsanschluss zu Analog1 bei ausgeschaltetem Router (Life-Line)		✓		✓
Geräteinterne Spannungsversorgung der Analog-Anschlüsse zur Stromversorgung je eines angeschlossenen Endgeräts.		✓		✓
Life-Line-Support zur Sicherung der Telefonfunktion bei ausgeschaltetem Gerät oder nicht konfiguriertem VoIP-Call-Manager	✓	✓		✓
Anschluss für externes Analog- oder GPRS-Modem am COM-Port (benötigt LANCOM Modem Adapter Kit)	✓	✓	✓	✓
WLAN				
Funkübertragung nach IEEE 802.11g und IEEE 802.11b				✓
Funkübertragung nach IEEE 802.11a und IEEE 802.11h				✓
Point-to-Point-Funktion (pro WLAN-Schnittstelle sechs P2P-Strecken definierbar)				✓
Relais-Funktion zur Verbindung zweier P2P-Strecken untereinander				✓
Access-Point-Modus				✓
Client-Modus				✓
Managed-Modus zur zentralen Konfiguration der WLAN-Module durch einem WLAN-Controller				✓
Turbo Modus: Bandbreitenverdopplung im 2,4 GHz- und 5 GHz-Bereich				✓
Super AG inkl. Hardware-Compression und Bursting				✓
Multi SSID				✓
Roaming-Funktion				✓
802.11i / WPA mit Hardware-AES-Verschlüsselung				✓
WEP-Verschlüsselung (bis 128 Bit Schlüssellänge, WEP152)				✓
IEEE 802.1x/EAP				✓

■ Kapitel 1: Einleitung

DE

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
MAC-Adressfilter (ACL)				✓
Individuelle Passphrases pro MAC-Adresse (LEPS)				✓
Closed-Network-Funktion				✓
Integrierter RADIUS-Server				✓
VLAN				✓
Intra-Cell-Blocking				✓
QoS für WLAN (IEEE 802.11e, WMM/WME)				✓
LAN-Anschluss				
Individuelle Fast Ethernet LAN Ports, einzeln schaltbar, z.B. als LAN-Switch oder separate DMZ-Ports, Auto-Crossover. Alternativ schaltbar als WAN-Interface zum Anschluss eines SDSL-Modems.	4	2	2	2
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“.	✓	✓	✓	✓

	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Konfiguration				
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminalmodus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion	✓	✓	✓	✓
1-Click-VPN-Assistenten zur besonders komfortablen Einrichtung von RAS-Zugängen und LAN-Kopplungen über VPN	✓	✓	✓	✓
Fernkonfiguration über ISDN (mit ISDN-PPP-Verbindungen z. B. über das DFÜ-Netzwerk von Windows).	✓	✓	✓	✓
Serielle Konfigurations-Schnittstelle	✓	✓	✓	✓
Rückruffunktion mit PPP-Authentifizierung-Mechanismen zur Beschränkung auf festgelegte ISDN-Rufnummern	✓	✓	✓	✓
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko	✓	✓	✓	✓
Optionale Software-Erweiterungen				
LANCOM VoIP-32 Option zur Erweiterung auf 32 lokale SIP-Benutzer	✓	✓	✓	✓
LANCOM VPN Option mit 25 aktiven Tunneln zur Absicherung von Netzwerkkopplungen inkl. Aktivierung des Hardware-Beschleunigers	✓	✓	✓	✓
LANCOM Next Business Day Service Extension CPE, Art.-Nr. 61411	✓	✓	✓	✓
LANCOM 2-Year Warranty Extension CPE, Art.-Nr. 61414	✓	✓	✓	✓
LANCOM Content Filter für 10 oder 25 Benutzer mit einem oder drei Jahren Laufzeit	✓	✓	✓	✓
LANCOM Fax Gateway Option zur Aktivierung von "Hardfax" im Router, Art.-Nr. 61425	✓	✓	✓	
Optionale Hardware-Erweiterungen				
LANCOM Modem Adapter Kit zum Anschluss eines Analog- oder GSM-Modems an die serielle Schnittstelle	✓	✓	✓	✓
19" Rackmount-Adapter	✓	✓	✓	✓
LANCOM ES-1108P PoE-Switch zur Ethernet-Verkabelung; gleichzeitig zur Spannungsversorgung über Ethernet z.B. für SIP-Telefon LANCOM VP-100	✓	✓	✓	✓
Blitzschutzadapter SA-5 und SA-LAN				✓

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 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Netzteil	✓	✓	✓	✓
LAN-Anschlusskabel (grüne Stecker)	1	1	1	1
ADSL-Anschlusskabel (transparente Stecker)	1	1	1	1
ISDN-Anschlusskabel (hellblaue Stecker)	1	1	2	1
Adapter zum Kreuzen der Kontakte bei umkonfigurierten ISDN-Schnittstellen	1	1	2	1
Analog-Kabel RJ11-Stecker auf TAE-NF-Buchse zum Anschluss von analogen Endgeräten oder TK-Anlagen		2		2
Analog-Kabel RJ45-Stecker (gelbe Markierung) auf RJ11-Stecker zum Anschluss an analogen Amtsanschluss		1		1
Adapter RJ11-Buchse auf TAE-F-Stecker für Deutschland		1		1
Anschlusskabel für die Konfigurationsschnittstelle	✓	✓	✓	✓
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

2.2.1 Konfiguration der LANCOM-Geräte

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

- Betriebssystem mit TCP/IP-Unterstützung, z. B. Windows, Linux, BSD Unix, Apple Mac OS, OS/2.
- Zugang zum LAN über das TCP/IP-Protokoll.



LANconfig und LANmonitor benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser unter einem beliebigen Betriebssystem erforderlich.

2.2.2 Betrieb der Access Points im Managed-Modus

LANCOM Wireless Router und LANCOM Access Points können entweder als autarke Access Points mit eigener Konfiguration betrieben werden („Access Point-Modus“) oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller gesteuert wird („Managed-Modus“).



Für den Betrieb im Managed-Modus benötigen die Access Points eine Firmware der Version 7.22 oder höher und einen aktuellen Loader (Version 1.86 oder höher).

Mit Hilfe des Split-Managements kann die WLAN-Konfiguration von der restlichen Router-Konfiguration getrennt werden. Auf diese Weise können z. B. in Filialen oder Home-Offices die Router- und VPN-Einstellungen lokal erfolgen, die WLAN-Konfiguration kann über einen LANCOM WLAN Controller in der Zentrale erfolgen.

2.3 Der LANCOM Router stellt sich vor

In diesem Abschnitt stellen wir Ihnen Ihr Gerät vor. Sie erhalten einen Überblick über alle Statusanzeigen, Anschlüsse und Schalter.

2.3.1 Statusanzeigen

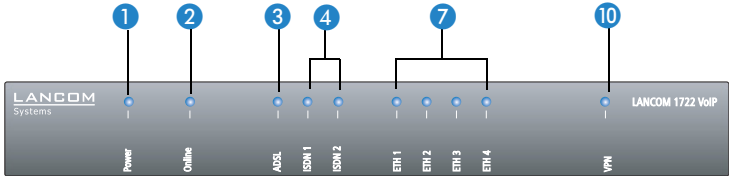
Die verschiedenen LANCOM Router-Modelle verfügen je nach Funktionsumfang über eine unterschiedliche Anzahl von Statusanzeigen auf der Vorderseite.

■ Kapitel 2: Installation

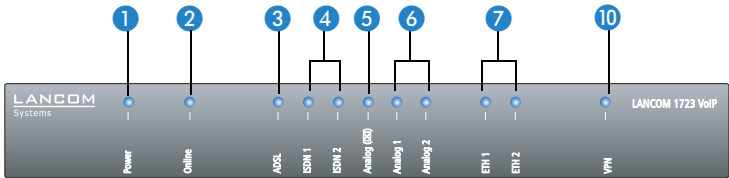
Vorderseite

Die Statusanzeigen auf der Vorderseite des Gerätes geben Aufschluss über den Betriebs- und Verbindungszustand des Gerätes:

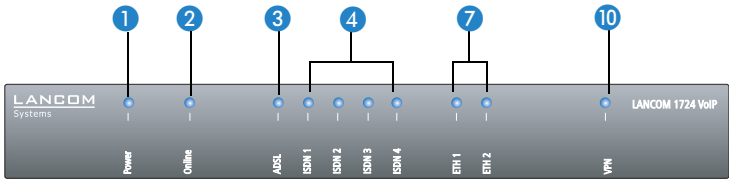
LANCOM 1722 VoIP



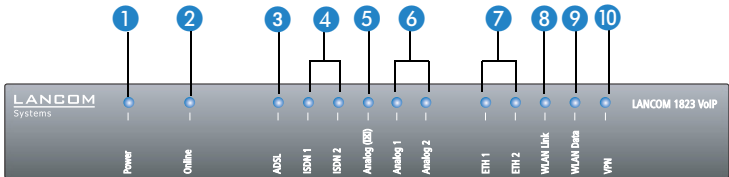
LANCOM 1723 VoIP



LANCOM 1724 VoIP



LANCOM 1823 VoIP



Oberseite

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



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.

1 Power

Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts.

aus		Gerät abgeschaltet
grün	blinkend	Selbsttest nach dem Einschalten
grün	dauerhaft an	Gerät betriebsbereit
rot/grün	abwechselnd blinkend	Gerät unsicher: Kein Konfigurationskennwort gesetzt

■ Kapitel 2: Installation

orange/grün	Im Gehäusedeckel blinkend im Wechsel mit der Online-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat noch keinen WLAN Controller gefunden. Das bzw. die entsprechenden WLAN-Module sind ausgeschaltet, bis sie einen WLAN-Controller gefunden haben, von dem sie eine Konfiguration beziehen können bzw. bis sie manuell auf eine andere Betriebsart umgestellt werden.
orange/rot	Im Gehäusedeckel blinkend im Wechsel mit der Online-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat einen WLAN Controller gefunden. Der WLAN Controller kann dem WLAN-Modul jedoch keine Konfiguration zuweisen, da Firmware- und/oder Loader-Version des Geräts nicht mit dem WLAN Controller kompatibel sind.
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 Normalfall 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.

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 Gebühren-Limits 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 **LCOS-Menübaum** ▶ **Setup** ▶ **Gebuehren** ▶ **Budgets-Zuruecksetzen**.



Signal für ein erreichtes Zeit- oder Gebührenlimit

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
orange/ grün	Im Gehäuse- deckel blinkend im Wechsel mit der Power-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat noch keinen WLAN-Controller gefunden. Das bzw. die entsprechenden WLAN-Module sind ausgeschaltet, bis sie einen WLAN-Controller gefunden haben, von dem sie eine Konfiguration beziehen können bzw. bis sie manuell auf eine andere Betriebsart umgestellt werden.
orange/ rot	Im Gehäuse- deckel blinkend im Wechsel mit der Power-LED	Mindestens ein WLAN-Modul befindet sich im Managed-Modus und hat einen WLAN Controller gefunden. Der WLAN Controller kann dem WLAN-Modul jedoch keine Konfiguration zuweisen, da Firmware- und/oder Loader-Version des Geräts nicht mit dem WLAN Controller kompatibel sind.

1 ADSL

Verbindungszustand am ADSL-Anschluss:

aus		Interface abgeschaltet
orange	blinkend	Initialisierung (Kontaktaufnahme mit Verbindungsstelle)
orange	blitzend	Aufbau der ersten Verbindung
orange	invers blitzend	Aufbau einer weiteren Verbindung
orange	dauerhaft an	mindestens eine logische Verbindung aufgebaut
orange	flackernd	Datenverkehr (Versand oder Empfang)
orange	blitzend	Fehler (CRC-Fehler, Framing-Fehler etc.)
rot	dauerhaft an	Keine Synchronisation bzw. Suchen der Gegenstelle
grün	dauerhaft	Synchronisation erfolgreich
grün	blinkend/blitzend	Handshake/Trainingsphase
rot/ orange	blinkend	Hardware-Fehler

2 ISDN

Statusanzeige für die ISDN-Schnittstellen:

		TE-Modus (externer ISDN- Anschluss)	NT-Modus (interner ISDN- Anschluss)
aus		Interface abgeschaltet oder Layer 1 deaktiviert oder keine Layer 2 TEI	Interface abgeschaltet. Im abgeschalteten Zustand ist der Anschluss ggf. über ein Life-Line-Relais mit einer anderen ISDN-Schnittstelle verbunden.
grün	blinkend	D-Kanal Layer 1 im Aufbau/Layer 2 TEI im Aufbau	
grün	dauerhaft an	D-Kanal aktiviert (Layer 1 aktiv und Layer 2 TEI vorhanden)	D-Kanal aktiviert
orange	blinkend	Aufbau der ersten ISDN-Verbindung	
orange	blitzend	Aufbau einer weiteren ISDN-Verbindung	
orange	invers flackernd	Datenverkehr in Senderichtung	
rot	blinkend	Fehler auf dem B-Kanal	
rot	dauerhaft an	Aufbau D-Kanal Layer 1 oder Layer 2 fehlerhaft beendet	Aufbau D-Kanal Layer 1 fehlerhaft beendet
rot/ orange	blinkend	ISDN-Hardwarefehler	



Wenn die LED einer ISDN-Schnittstelle im TE-Modus 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.

3 Analog
(1 und 2)

Verbindungszustand am analogen Endgeräte-Anschluss:

aus		Interface abgeschaltet.
grün	dauerhaft an	Analoger Anschluss ist eingeschaltet. Hörer am Gerät aufgelegt oder Endgerät ist nicht angeschlossen.
orange	blinkend	Rufaufbau vom LANCOM in Richtung Endgerät (Klingeln)

orange	dauerhaft an	Hörer am Endgerät abgehoben.
orange/ rot	blinkend	Hardware-Fehler
rot	dauerhaft an	Kalibrierung wurde unterbrochen bzw. temporärer Fehler (z.B. bei Temperaturabschaltung)

4 Analog (☒)

Verbindungszustand am analogen Amts-Anschluss:

aus		Interface abgeschaltet.
grün	dauerhaft an	Analoger Amtsanschluss ist eingeschaltet.
orange	blinkend	Rufaufbau von Amt in Richtung LANCOM. Das Amt „klingelt“ am LANCOM.
orange	dauerhaft an	Das LANCOM hat analoge Verbindung – Hörer an einem analogen Endgerät abhoben.
orange/ rot	blinkend	Hardware-Fehler
rot	dauerhaft an	keine Line-Spannung vorhanden (ggf. Kabel unterbrochen)

5 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

6 WLAN Link

Gibt Informationen über die WLAN-Verbindungen der internen WLAN-Module aus. Die WLAN-Link-Anzeige kann folgende Zustände annehmen:

aus		Kein WLAN-Netz definiert oder WLAN-Modul deaktiviert. Es werden keine Beacons vom WLAN-Modul gesendet.
grün		Mindestens ein WLAN-Netz definiert und WLAN-Modul aktiviert. Es werden Beacons vom WLAN-Modul gesendet.
grün	invers blitzend	Anzahl der Blitzer = Anzahl der verbundenen WLAN-Stationen und P2P-Funkstrecken, danach folgt eine Pause (Default). Alternativ kann die Frequenz der Blitzer die Eingangsempfindlichkeit anzeigen.

Kapitel 2: Installation

DE

7 WLAN Data

Gibt Informationen über den Datenverkehr der internen WLAN-Module aus. Die WLAN-Data-Anzeige kann folgende Zustände annehmen:

grün	flackernd	TX-Datenverkehr.
rot	flackern	Fehler im Funk-LAN (TX-Fehler, z.B. Sendefehler aufgrund schlechter Verbindung)
rot	blinkend	Hardwarefehler im WLAN-Modul

8 VPN

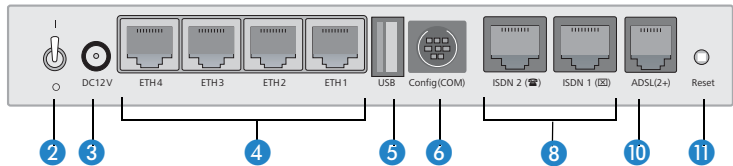
Status einer VPN-Verbindung.

aus		kein VPN-Tunnel aufgebaut
grün	blinkend	Verbindungsaufbau
grün	blitzend	Erste Verbindung
grün	invers blitzend	Weitere Verbindungen
grün	dauerhaft an	VPN-Tunnel sind aufgebaut

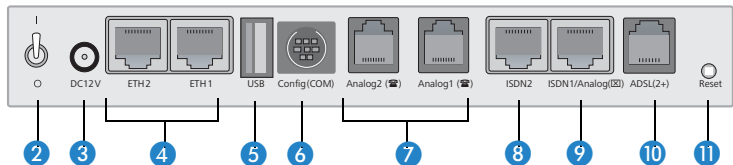
2.3.2 Die Anschlüsse des Geräts

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

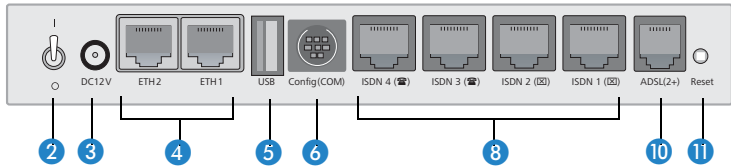
LANCOM 1722 VoIP



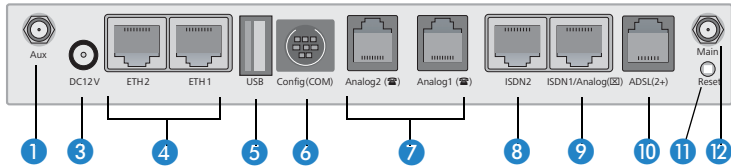
LANCOM 1723 VoIP



LANCOM 1724 VoIP



LANCOM 1823 VoIP



Nur LANCOM 1823
VoIP

1 Aux-Anschluss für das WLAN-Modul. An den Aux-Anschlüssen werden die Diversity-Antennen angeschlossen.

Nicht bei LANCOM
1823 VoIP

2 Netzschalter

3 Anschluss für das mitgelieferte Netzteil

4 Switch mit 10/100Base-Tx-Anschlüssen

5 USB-Anschluss (USB Host)

6 Serielle Konfigurationsschnittstelle (RS 232/V.24)

Nur LANCOM 1723
VoIP und LANCOM
1823 VoIP

7 Anschlüsse für analoge Endgeräte

8 ISDN-Anschlüsse

□ Default LANCOM 1722 VoIP

ISDN 1: TE-Modus, entspricht externem ISDN-Anschluss, alternativ schaltbar in NT-Modus

ISDN 2: NT-Modus, entspricht intern S_0 , alternativ schaltbar in TE-Modus

□ Default LANCOM 1724 VoIP

ISDN 1 und ISDN 2: TE-Modus, alternativ schaltbar in NT-Modus

ISDN 3 und ISDN 4: NT-Modus, alternativ schaltbar in TE-Modus

□ Default LANCOM 1723 VoIP und LANCOM 1823 VoIP

ISDN 2: NT-Modus, alternativ schaltbar in TE-Modus



Die Schnittstelle ISDN 2 darf bei den Modellen LANCOM 1723 VoIP und LANCOM 1823 VoIP aus Sicherheitsgründen weder direkt noch indirekt an eine externe Vermittlungsstelle (z.B. das Telefonnetz) angeschlossen werden!

9 Kombinierte ISDN-Analog-Schnittstelle

- Default LANCOM 1723 VoIP und LANCOM 1823 VoIP

ISDN 1: TE-Modus, alternativ schaltbar in NT-Modus oder als Schnittstelle zum analogen Amts-Anschluss

10 ADSL-Anschluss (ADSL, ADSL 2, ADSL 2+)

11 ResetTaster

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkeinstellung) 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!

Nur LANCOM 1823
VoIP

- 12 Main-Anschluss für das WLAN-Modul.

2.4 Installation der Hardware

Die Installation des LANCOM Router erfolgt in folgenden Schritten:

Nur LANCOM 1823
VoIP

- ① **Antennen** – Schrauben Sie die beiden mitgelieferten Antennen auf der Rückseite des LANCOM VoIP Routers an.



Antennen dürfen nur bei ausgeschaltetem Gerät montiert oder gewechselt werden. Die Montage oder Demontage bei eingeschaltetem Gerät kann zur Zerstörung der WLAN-Module führen!




Beachten Sie bei der Montage von separat erworbenen Antennen, dass die im jeweiligen Land maximal zulässige Sendeleistung des WLAN-Systems nach EIRP nicht überschritten werden darf. Für die

Einhaltung der Grenzwerte ist der Betreiber des Systems verantwortlich.


- ② **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 ④ 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 neben der Übertragungsrate (10/100 Mbit) 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.

- ③ **ADSL** – verbinden Sie die ADSL-Schnittstelle ⑩ über das mitgelieferte ADSL-Anschlusskabel (transparente Stecker) mit dem Splitter.

- ④ **Anschluss an das ISDN-Netz** – für den Anschluss des LANCOM VoIP Router an das ISDN stecken Sie das eine Ende eines mitgelieferten ISDN-Anschlusskabels (hellblaue Stecker) in eine ISDN-Schnittstelle im TE-Modus. Im Auslieferungszustand sind die mit gekennzeichneten ISDN-Schnittstellen auf den TE-Modus „extern“ eingestellt. Stecken Sie das andere Ende des ISDN-Kabels in einen ISDN/S₀-Anlagenanschluss oder -Mehrgeräteanschluss.

-  Die Schnittstelle ISDN 2 darf bei den Modellen LANCOM 1723 VoIP und LANCOM 1823 VoIP auch nach dem Umstellen auf den TE-Modus nicht zum Anschluss an das ISDN-Netz verwendet werden!

-  Bitte beachten Sie auch die Hinweise auf die Konfiguration der ISDN-Schnittstellen.


- ⑤ **ISDN-Endgeräte anschliessen** – für den Anschluss von ISDN-Endgeräten (ISDN-Telefonen oder ISDN-TK-Anlagen) an den LANCOM VoIP Router

verbinden Sie diese mit einer ISDN-Schnittstelle im NT-Modus. Im Auslieferungszustand sind die mit  gekennzeichneten ISDN-Schnittstellen auf den NT-Modus eingestellt („interner ISDN-Anschluss“).




Bei den Modellen LANCOM 1723 VoIP und LANCOM 1823 VoIP können über die ISDN2-Schnittstelle **8** maximal zwei Telefone über die ISDN-Speisung mit Strom versorgt werden. Bitte beachten Sie dazu auch die Hinweise auf die Konfiguration der ISDN-Schnittstellen.

6 **Anschluss an das analoge Telefonnetz** – für den Anschluss des LANCOM VoIP Router an das analoge Telefonnetz stecken Sie das gelb markierte Ende des mitgelieferten Analog-Anschlusskabels (RJ45) in die kombinierte ISDN-Analog-Schnittstelle **9**. Stecken Sie das andere Ende des Analog-Anschlusskabels (RJ11) in einen analogen Amts-Anschluss (z.B. einen Splitter). Falls der Amts-Anschluss über eine TAE-N/F-Buchse verfügt, verwenden Sie den beiliegenden Adapter RJ11-Stecker auf TAE-F-Stecker.

7 **Analoge Endgeräte anschließen** – für den Anschluss von analogen Endgeräten (Telefonen oder TK-Anlagen) an den LANCOM VoIP Router verbinden Sie diese mit einer Analog-Schnittstelle (RJ11-Buchse, mit  gekennzeichnet). Falls Ihre Endgeräte über einen TAE-F- oder TAE-N-Stecker verfügen, verwenden Sie bitte die beiliegenden Adapterkabel RJ11-Stecker auf die TAE-N/F-Buchse.



Die angeschlossenen analogen Endgeräte werden vom LANCOM VoIP Router mit Spannung versorgt. Im Life-Line-Betrieb wird die an einem analogen Amtsanschluss anliegende Spannung an das Endgerät an der Schnittstelle Analog1 () weitergeleitet. Bitte beachten Sie dazu auch die Hinweise auf Life-Line-Support.

8 **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 **6****5** mit einer freien seriellen Schnittstelle des PC.

9 **Externes Modem anschließen** – 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 über eine analoge Leitung realisieren wollen.

- ⑩ **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.

- ⑪ **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 Konfiguration der ISDN- und Analog-Schnittstellen

LANCOM VoIP Router verfügen über mehrere Schnittstellen, die zum Anschluss an ISDN- oder Analog-Amtsleitungen oder zum Anschluss von ISDN- oder Analog-Endgeräten genutzt werden können.

Grundsätzlich sollten Sie entscheiden, ob intern eine Telefonanlage angeschlossen und mit Hilfe des LANCOM VoIP Routers VoIP-fähig gemacht werden soll (z.B. am Einzelstandort oder zur Filial-Vernetzung) oder ob der LANCOM VoIP Router eine lokale Telefonanlage ersetzen soll.

- Wenn Sie eine Telefonanlage VoIP-fähig machen möchten, belassen Sie die ISDN-Schnittstellen im Auslieferungszustand. Prüfen Sie auf der Geräteunterseite, ob sich alle DIP-Schalter in der auf dem Aukleber beschriebenen „Standard-Position“ befinden. Für diesen Anschlusstyp wird kein ISDN-Kreuzadapter benötigt.
- Falls Sie den LANCOM VoIP Router anstelle einer Telefonanlage verwenden möchten, können Sie alle geeigneten ISDN-Schnittstellen zum Anschluss an das öffentliche Telefonnetz verwenden. Dazu müssen Sie die DIP-Schalter auf der Geräteunterseite entsprechend einstellen und ein bis zwei ISDN-Kreuzadapter (nur LANCOM 1724 VoIP) verwenden. Die genaue Einstellung und Einrichtung dieser Konfiguration sind im Handbuch TK-Anlagenfunktionen ausführlich beschrieben.



Detailliertere Informationen zur Bedeutung der DIP-Schalter und individuellen Einrichtung von ISDN- und Analog-Schnittstellen finden Sie im Kapitel 'Konfiguration der ISDN- und Analog-Schnittstellen im Detail' →Seite 125. Für andere Einsatz-Szenarien als zuvor beschrieben oder abweichende Konfiguration der Schnittstellen wird das Durcharbeiten der entsprechenden Kapitel mit Konfigurationsbeispielen im Referenzhandbuch (auf dem mitgelieferten Datenträger (CD/DVD) bzw. im Internet) dringend empfohlen.

2.6 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten Systemsoftware LANconfig und LANmonitor, die unter Windows läuft.



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

2.6.1 Software-Setup starten

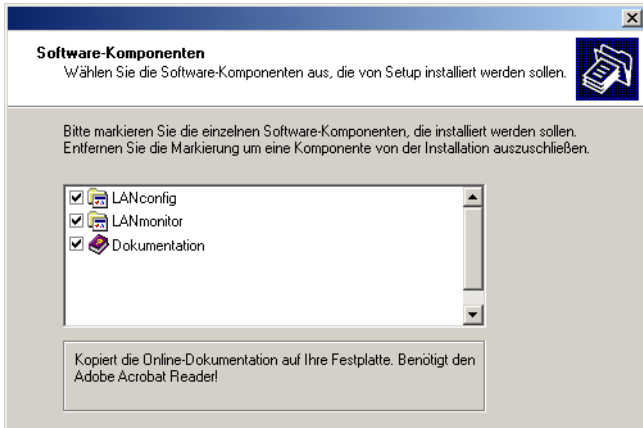
Legen Sie den beiliegenden Datenträger (CD/DVD) in Ihr Laufwerk ein. Daraufhin startet das Setup-Programm automatisch.



Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis des beiliegenden Datenträgers (CD/DVD) auf.

■ Kapitel 2: Installation

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



2.6.2 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.
- Der **WLANmonitor** erlaubt die Beobachtung und Überwachung der WLAN-Netze. Die mit den Access Points verbundenen Clients werden angezeigt, auch nicht authentifizierte Access Points und Clients können angezeigt werden (Rogue AP Detection und Rogue Client Detection).
- Die **LANCAPI** ist eine spezielle Form der CAPI-2.0-Schnittstelle, über die alle Arbeitsstationen im LAN Zugriff auf Bürokommunikations-Funktionen wie Fax und EuroFileTransfer erhalten. Mit der **LANCAPI DFÜ Netzwerkunterstützung** können einzelne Rechner über die LANCAPI Einwahlverbindungen zu einem Internetprovider herstellen. Das **CAPI Faxmodem** stellt Ihnen einen Faxtreiber der Klasse 1 zur Verfügung.
- Der **LANCOM Advanced VPN Client** ermöglicht den Aufbau von VPN-Verbindungen von einem entfernten Rechner über das Internet zu einem Router mit VPN-Funktion.
- 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 VoIP 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 Funk-LAN
- 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 VoIP Router angeschlossen
- Neuaufbau eines Netzwerks

Wenn Sie den LANCOM VoIP 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 VoIP 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 VoIP 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 Sie die IP-Adresse für den Router selbst festlegen möchten (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).

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

■ IP-Adresse und Netzwerkmaske

Teilen Sie dem LANCOM VoIP Router eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaske 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 VoIP 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 VoIP Router können bis zu 16 verschiedene Administratoren eingerichtet werden. Weitere Informationen finden Sie im LCOS-Referenzhandbuch unter „Rechteverwaltung für verschiedene Administratoren“.



Im Managed-Modus erhalten LANCOM Wireless Router und LANCOM Access Points automatisch das gleiche Root-Kennwort wie der WLAN-Controller, wenn auf dem Gerät selbst noch kein Root-Kennwort gesetzt ist.

3.1.3 Einstellungen für das Funk-LAN

Der Netzwerkname (SSID)

Der Grundkonfigurations-Assistent fragt nach dem Netzwerknamen des Access Points (häufig als SSID – **S**ervice **S**et **I**dentifier bezeichnet). Der Name kann frei gewählt werden. Mehrere Access Points mit demselben Netzwerknamen bilden ein gemeinsames Funk-LAN.

Offenes oder geschlossenes Funk-LAN?

Mobilfunkstationen wählen das gewünschte Funk-LAN durch Angabe des Netzwerknamens an. Erleichtert wird die Angabe des Netzwerknamens durch zwei Techniken:

- Mobilfunkstationen können die Umgebung nach Funk-LANs absuchen („scannen“) und die gefundenen Funk-LANs in einer Liste zur Auswahl anbieten.
- Durch Verwendung des Netzwerknamens 'ANY' meldet sich die Mobilfunkstation im nächsten verfügbaren Funk-LAN an.

Um diese Vorgehensweise zu unterbinden kann das Funk-LAN „geschlossen“ werden. In diesem Fall akzeptiert es keine Anmeldungen mit dem Netzwerknamen 'ANY'.

Auswahl eines Funkkanals

Der Access Point arbeitet in einem bestimmten Funkkanal. Der Funkkanal wird aus einer Liste von bis zu 13 Kanälen im 2,4 GHz Frequenzbereich, oder bis zu 19 Kanälen im 5 GHz Frequenzbereich ausgewählt (in verschiedenen Ländern sind einzelne Funkkanäle gesperrt, siehe Anhang).

Der verwendete Kanal und Frequenzbereich legt den Betrieb des gemeinsamen Funkstandards fest, wobei der 5 GHz Frequenzbereich dem IEEE 802.11a/h Standard entspricht und der 2,4 GHz Frequenzbereich den Betrieb im IEEE 802.11g und IEEE 802.11b Standard festlegt.

Wenn in Reichweite des Access Points keine weiteren Access Points arbeiten, so kann ein beliebiger Funkkanal eingestellt werden. Andernfalls müssen im 2,4 GHz-Band die Kanäle so gewählt werden, dass sie sich möglichst nicht überdecken beziehungsweise möglichst weit auseinander liegen. Im 5 GHz-Band reicht normalerweise die automatische Einstellung, in der der LANCOM Access Point über TPC und DFS selbst den besten Kanal einstellt.



Weitere Informationen zu TPC und DFS finden sie im LCOS-Referenzhandbuch.

3.1.4 Gebührenschutz

Der Gebührenschutz 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.

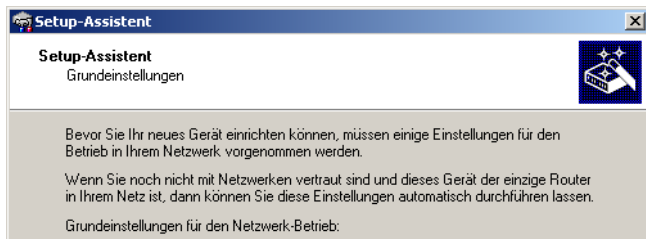
Das Budget kann durch Eingabe des Wertes '0' komplett deaktiviert werden.



In der Grundeinstellung ist der Gebührenschutz auf maximal 600 Minuten innerhalb von sieben Tagen eingestellt. Passen Sie diese Einstellung an Ihre persönlichen Bedürfnisse an oder deaktivieren Sie den Gebührenschutz, 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 Zugriff auf einen unkonfigurierten LANCOM VoIP 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.



Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

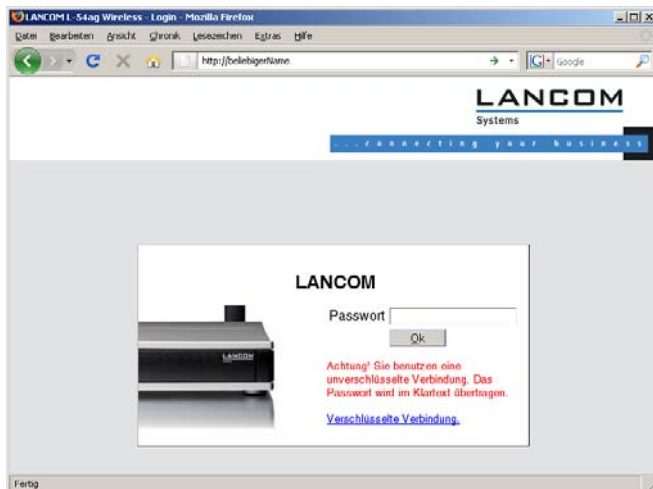
Netz ohne DHCP-Server

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.

Nicht für zentral verwaltete LANCOM Wireless Router oder LANCOM Access Points



Im werkseitigen 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 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).

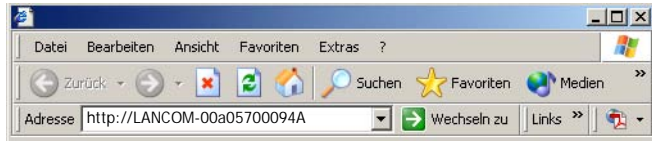
Netz mit DHCP-Server


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

■ Kapitel 3: Grundkonfiguration

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.

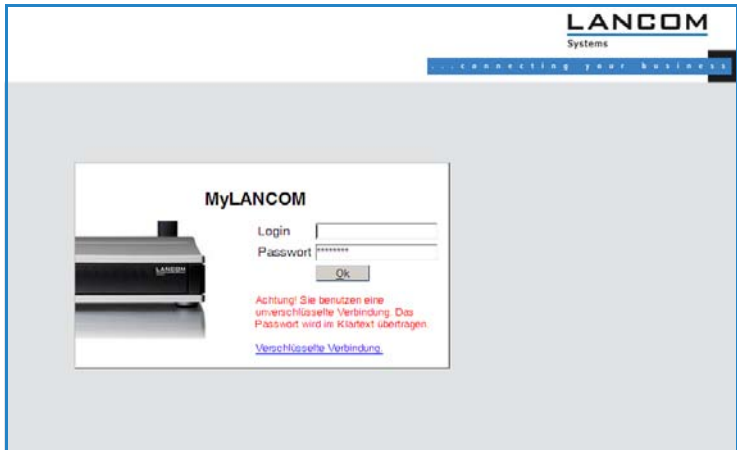
- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
 - Sie nutzen die Funktion "Geräte suchen" in LANconfig oder die Gerätesuche unter WEBconfig von einem anderen erreichbaren 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.

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.

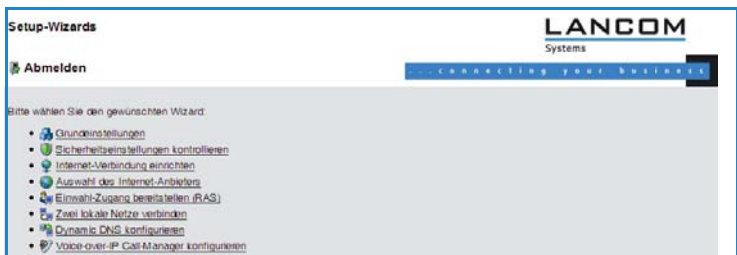
Falls Sie den allgemeinen Konfigurationszugang verwenden, tragen Sie nur das entsprechende Kennwort ein. Das Feld Benutzername bleibt in diesem Fall leer.

 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 VoIP 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**

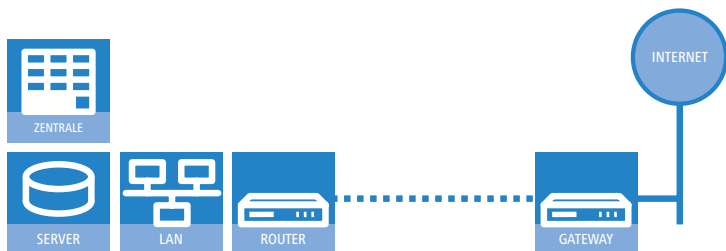
Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des LANCOMs als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.



Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres LANCOM VoIP 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.



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:

■ Kapitel 4: Den Internet-Zugang einrichten

- 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.

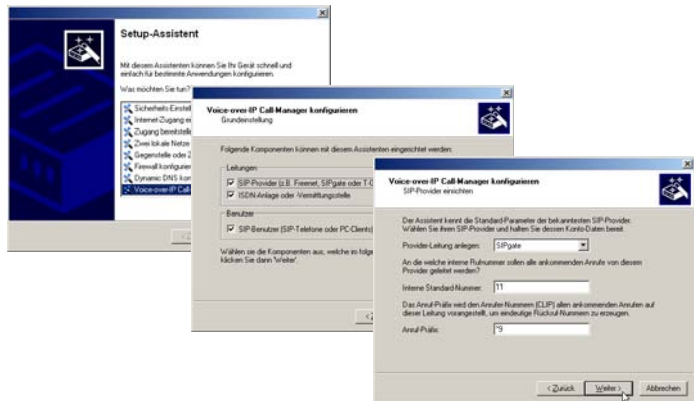
5 Konfiguration der VoIP-Funktionen

Wenn Sie den LANCOM VoIP Router als Telefonanlage einsetzen wollen, lesen Sie bitte nach der Konfiguration der Grundeinstellungen im Handbuch VoIP-TK-Anlagenfunktionen weiter. Dort werden Sie auf kürzestem Weg durch die Einrichtung als Telefonanlage mit Anbindung zum Festnetz (ISDN oder analog) geführt.

Wenn Sie eine ISDN-Telefonanlage hinter dem LANCOM VoIP Router betreiben möchten und deshalb die Telefonie-Schnittstellen in der Default-Konfiguration belassen haben, fahren Sie bitte mit der hier beschriebenen Konfiguration über den Assistenten für den VoIP-Call-Manager fort.

 Für speziellere Anwendungsfälle schlagen Sie bitte in den entsprechenden Kapiteln im LCOS-Referenzhandbuch nach.

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



- 2 Wählen Sie im Auswahlménú den Setup-Assistenten **Voice-over-IP Call Manager konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 In den folgenden Fenstern wählen Sie aus, welche Leitungen und Teilnehmer Sie anlegen möchten. Tragen Sie dazu die erforderlichen Daten ein.
- 4 Der Assistent informiert Sie, sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

6 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 direkte Verbindung zwischen den beiden LANs über eine ISDN-Verbindung hergestellt. In beiden LANs wird dazu ein 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 über WEBconfig eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

6.1 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.

6.1.1 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

■ Kapitel 6: Zwei Netzwerke verbinden

Kopplung	Angabe	Gateway 1		Gateway 2
VPN	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 + ISDN	IP-Netzadresse des entfernten Netzes	'10.0.2.0'		'10.0.1.0'
VPN + ISDN	Netzmaske des entfernten Netzwerks	'255.255.255.0'		'255.255.255.0'
VPN + ISDN	Domänenbezeichnung im entfernten Netzwerk	'filiale.firma'		'zentrale.firma'
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
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.

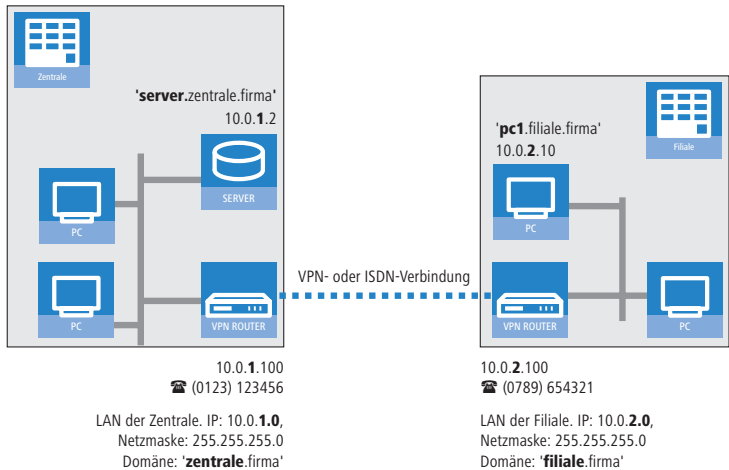
- Wenn Sie Ihr LANCOM noch nicht benannt haben, so fragt Sie der Assistent nach einem neuen **eigenen Gerätenamen**. Mit der Eingabe benennen Sie Ihr LANCOM neu. Achten Sie darauf, dass Sie beide Gegenstellen unterschiedlich benennen.
- Der **Name der Gegenstelle** wird für deren Identifikation benötigt.

- 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-**PPP**): Hier wird zwar die Bandbreite verdoppelt, in aller Regel fallen dafür aber auch doppelte Verbindungsgebühren an.

6.1.2 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 6: 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 manuellen Konfiguration 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'.

6.1.3 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.



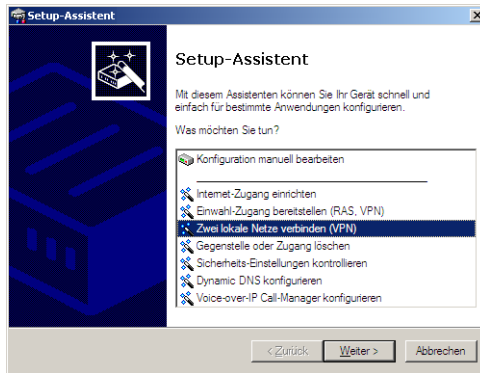
Entfernte Windows-Arbeitsgruppen erscheinen nicht in der Windows-Netzwerkumgebung, sondern können nur direkt (z.B. über die Computer-Suche) angesprochen werden.

6.2 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 die notwendigen Daten ein.

■ Kapitel 6: Zwei Netzwerke verbinden



- 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

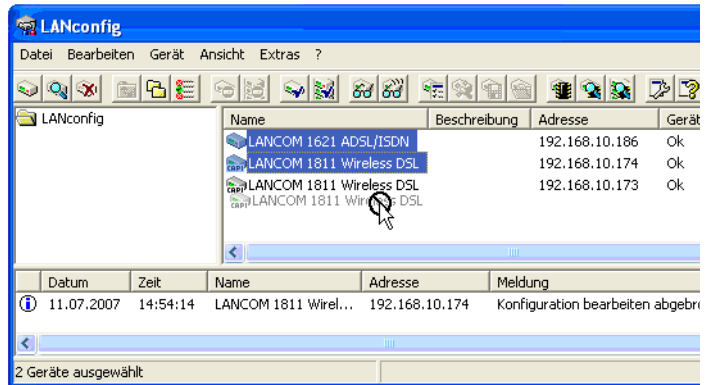
Ping-Statistik für 10.0.1.2:
    Pakete: Gesendet = 4, Empfangen = 4,
    Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 20ms, Mitte
  
```

6.3 1-Click-VPN für Netzwerke (Site-to-Site)

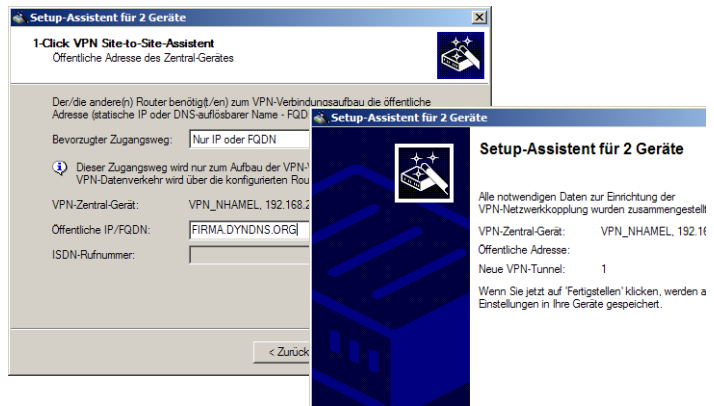
Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können

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.

6.4 Anleitung für WEBconfig



Die Kopplung von Netzwerken über VPN kann unter WEBconfig nicht mit Hilfe des Assistenten, sondern nur in der manuellen Konfiguration 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.

7 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 direkte 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 manuellen Konfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

7.1 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.

7.1.1 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?
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'.

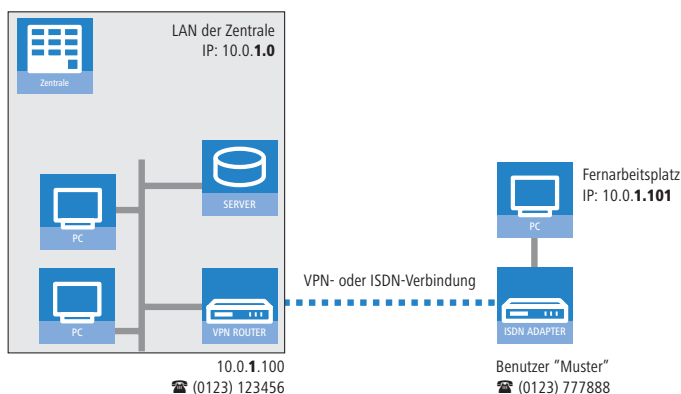
Die ISDN-Anruferkennung (CLI)

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).

7.1.2 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.

7.1.3 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).

7.2 Einstellungen am Einwahl-Rechner

7.2.1 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 dem beiliegenden Datenträger (CD/DVD) eine 30-Tage-Testversion des LANCOM Advanced VPN Client an. Eine genaue Beschreibung des VPN-Client und Hinweise zur Einrichtung finden Sie ebenfalls auf dem beiliegenden Datenträger (CD/DVD).

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

7.2.2 Einwahl über ISDN

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

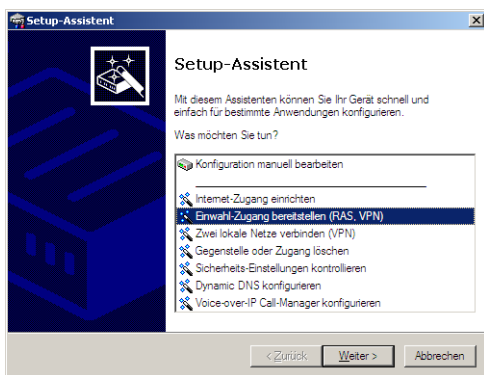
- DFÜ-Netzwerk (bzw. anderer PPP-Client) korrekt eingerichtet
- Netzwerkprotokoll (TCP/IP) installiert und auf den DFÜ-Adapter gebunden
- neue Verbindung im DFÜ-Netzwerk mit Rufnummer des Routers
- Terminal-Adapter oder ISDN-Karte auf PPPHDLC eingestellt
- PPP als DFÜ-Servertyp ausgewählt, 'Software-Komprimierung aktivieren' und 'Verschlüsseltes Kennwort fordern' ausgeschaltet

- Auswahl der gewünschten Netzwerkprotokolle (TCP/IP)
- 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.

7.3 Anleitung für LANconfig

- ① Rufen Sie den Assistenten 'Zugang bereitstellen (RAS, VPN, IPsec over 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').

7.4 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

■ Kapitel 7: Einwahl-Zugang bereitstellen

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'.
- 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, einer 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.

7.5 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').

8 Erweiterte WLAN-Konfiguration

Zur WLAN-Konfiguration der LANCOM Access Points stehen Ihnen komfortable Installations-Assistenten zur Verfügung.

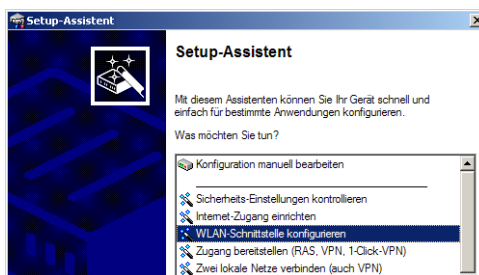
Die Einstellungen betreffen sowohl allgemeine, übergreifende Parameter als auch die jeweiligen Einstellungen einer oder mehrerer logischer WLAN-Netzwerke (WLAN-Funkzellen oder SSIDs).

8.1 WLAN-Konfiguration mit dem Assistenten von LANconfig

Zur WLAN-Konfiguration der LANCOM Access Points stehen Ihnen komfortable Installations-Assistenten zur Verfügung.

Die Einstellungen betreffen sowohl allgemeine, übergreifende Parameter als auch die jeweiligen Einstellungen einer oder mehrerer logischer WLAN-Netzwerke (WLAN-Funkzellen oder SSIDs).

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



- 2 Wählen Sie im Auswahlménü den Setup-Assistenten **WLAN-Schnittstelle konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.
- 3 Nehmen Sie mit Hilfe des Assistenten die gewünschten Einstellungen vor wie in den folgenden Abschnitten beschrieben.

Ländereinstellungen

Der Betrieb von WLAN-Karten ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z. B. in manchen Ländern nicht erlaubt. Um den Betrieb der LANCOM Access Points auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen

WLAN-Interfaces gemeinsam das Land eingestellt, in dem der Access Point betrieben wird.

Betriebsart der WLAN- Module

Die WLAN-Module können in verschiedenen Betriebsarten genutzt werden:

- Als Basisstation (Access Point-Modus) stellt das Gerät für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her. Parallel dazu sind Punkt-zu-Punkt-Verbindungen möglich.
- Auch im Managed-Modus binden die Access Points WLAN-Clients in das Netzwerk ein – in dieser Betriebsart sind die Geräte allerdings Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller konfiguriert wird. In dieser Betriebsart ist keine weitere WLAN-Konfiguration erforderlich, alle WLAN-Parameter werden vom WLAN-Controller übermittelt.
- Als Client sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also z. B. dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden. In dieser Betriebsart sind parallele Punkt-zu-Punkt-Verbindungen **nicht** möglich.

Weitere Informationen finden Sie im Abschnitt →Client-Modus.



Bei Geräten mit zwei WLAN-Modulen kann die Betriebsart für jedes Modul separat festgelegt werden, d.h. das eine WLAN-Modul kann im Managed-Modus, ein anderes z. B. als autarker Access Point betrieben werden.

Physikalische WLAN-Einstellungen

Neben dem verwendeten Funkkanal können Sie bei den physikalischen WLAN-Einstellungen Optionen wie die Bündelung von WLAN-Paketen (TX-Burst), die Hardwarekompression oder die Nutzung von QoS nach 802.11e aktivieren. Außerdem nehmen Sie hier die Einstellungen für das Diversity-Verhalten vor.

Logische WLAN-Netzwerke

Jedes WLAN-Modul kann bis zu acht logische WLAN-Netzwerke aufspannen, in dem sich mobile WLAN-Clients anmelden können. Zur Konfiguration eines logischen WLAN-Netzwerks werden die folgenden Parameter abgefragt:

- Der Netzwerkname (SSID)

- Offenes oder geschlossenes Funk-LAN
- Verschlüsselungseinstellungen
- MAC-Filter
- Client-Bridge-Betrieb
- Filtereinstellungen

Punkt-zu-Punkt-Einstellungen

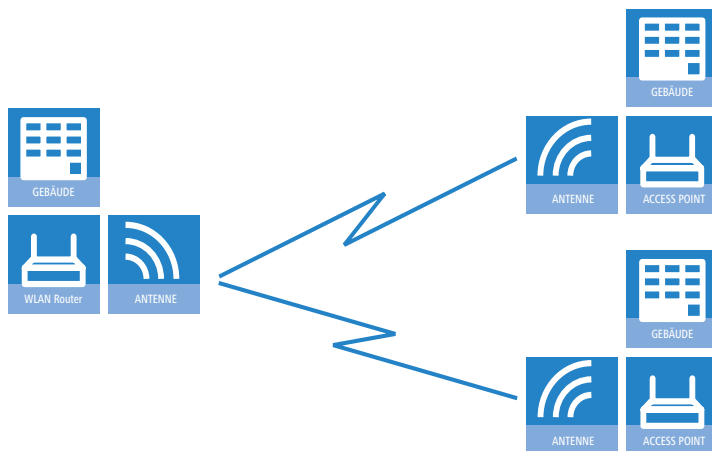
Bei der Konfiguration der P2P-Verbindungen wird neben der Betriebsart auch der Stationsname eingestellt, über den die Access Points eine Verbindung aufbauen können. Außerdem wird hier die Position als „Master“ oder „Slave“ festgelegt.

Neben den Einstellungen für den Access Point selbst wird auch definiert, zu welcher Gegenstelle der Access Point über die P2P-Verbindung Kontakt aufnehmen kann.

Weitere Informationen finden Sie im Abschnitt →Punkt-zu-Punkt-Verbindungen.

8.2 Konfiguration der Punkt-zu-Punkt-Verbindungen

LANCOM Access Points können nicht nur als zentrale Station in einem Funknetzwerk arbeiten, sie können im Punkt-zu-Punkt-Betrieb auch Funkstrecken über größere Distanzen bilden. So können z. B. zwei Netzwerke über mehrere Kilometer hinweg sicher verbunden werden – ohne direkte Verkabelungen oder teure Standleitungen.



Dieses Kapitel stellt die Grundlagen zur Auslegung von Point-to-Point-Strecken vor und gibt Hinweise zur Ausrichtung der Antennen.

8.2.1 Geometrische Auslegung von Outdoor-Funknetz-Strecken

Bei der Auslegung der Funkstrecken sind im Wesentlichen folgende Fragen zu beantworten:

- Welche Antennen müssen für die gewünschte Anwendung eingesetzt werden?
- Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?
- Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

Auswahl der Antennen mit dem LANCOM Antennen-Kalkulator

Zur Berechnung der Ausgangsleistungen in den Access Points und für eine erste Abschätzung der erreichbaren Distanzen und Datenraten können Sie den LANCOM Antennen-Kalkulator verwenden, den Sie zum Download auf unserer Webseite unter www.lancom.de finden.

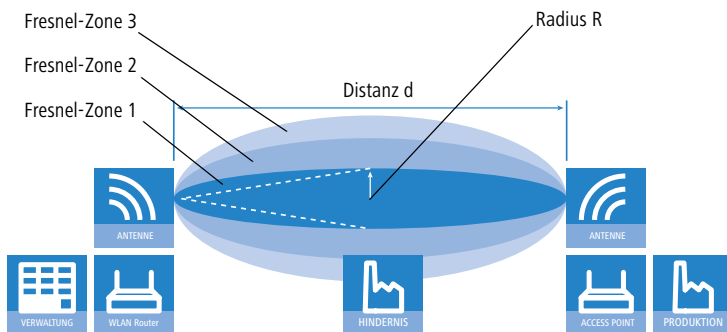
Nach Auswahl der verwendeten Komponenten (Access Points, Antennen, Blitzschutz und Kabel) berechnet der Kalkulator neben Datenraten und Distanzen auch den Antennen-Gewinn, der in den Access Points eingestellt werden muss.

tung. Die Bereiche, in denen sich die Wellen verstärken oder auslöschen, werden als Fresnel-Zonen bezeichnet.



Der Schutz der verwendeten Komponenten vor den Folgen von Blitzeinschlag oder anderen elektrostatischen Vorgängen ist einer der wichtigsten Aspekte bei der Auslegung und Installation von WLAN-Systemen im Outdoor-Einsatz. Bitte beachten Sie die entsprechenden Hinweise zum →'Blitz- und Überspannungsschutz', da LANCOM Systems ansonsten keine Garantie für Schäden an den LANCOM- und AirLancer-Komponenten übernehmen kann!

Informationen zur Installation von WLAN-Systemen im Outdoor-Einsatz finden Sie im 'LANCOM Outdoor Wireless Guide'.



Um die von der Antenne abgestrahlte Leistung möglichst vollständig auf die empfangende Antenne abzubilden, muss die Fresnel-Zone 1 frei bleiben. Jedes störende Element, das in diese Zone hineinragt, beeinträchtigt die effektiv übertragene Leistung deutlich. Dabei schirmt das Objekt nicht nur einen Teil der Fresnel-Zone ab, sondern führt durch Reflexionen zusätzlich zu einer deutlichen Reduzierung der empfangenen Strahlung.

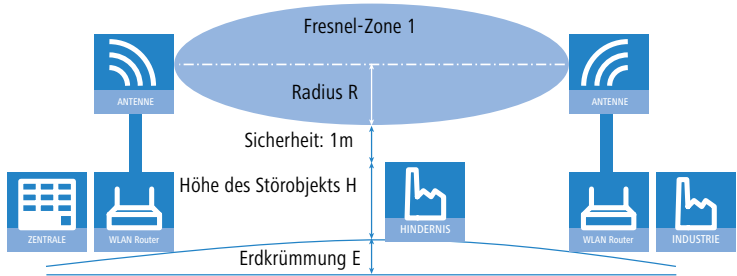
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung (λ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

$$R = 0,5 * \sqrt{\lambda * d}$$

Die Wellenlänge beträgt im 2,4 GHz-Band ca. 0,125 m, im 5 GHz-Band ca. 0,05 m.

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 4 km ergibt sich im 2,4 GHz-Band der Radius der Fresnel-Zone 1 zu **11 m**, im 5 GHz-Band nur zu **7 m**.

Damit die Fresnel-Zone 1 frei und ungestört ist, müssen die Antennen das höchste Störobjekt um diesen Radius überragen. Die gesamte erforderliche Masthöhe (M) der Antennen ergibt sich nach folgendem Bild zu:



$$M = R + 1\text{m} + H + E \text{ (Erdkrümmung)}$$

Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu $E = d^2 \cdot 0,0147$ – bei einer Distanz von 8 km also immerhin schon fast 1m!

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 8 km ergibt sich im 2,4 GHz-Band die Masthöhe über dem höchsten Störobjekt von ca. **13 m**, im 5 GHz-Band zu **9 m**.

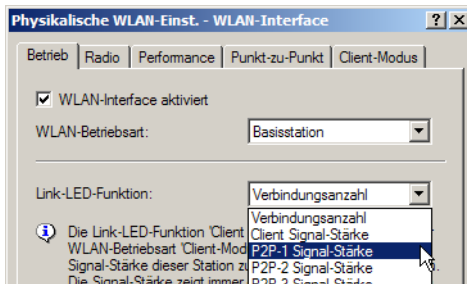
Antennen-Leistungen

Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

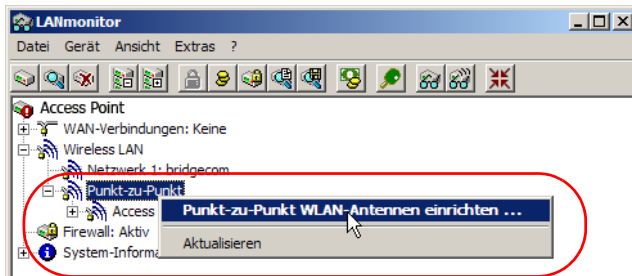
Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden Access Point bis zum Funkmodul im empfangenden Access Point. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft und verstärkende Elemente wie die externen Antennen.

■ Kapitel 8: Erweiterte WLAN- Konfiguration

Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden (LANconfig: **Wireless LAN ► Allgemein ► Physikalische WLAN-Einstellungen ► Betrieb**). Je schneller die LED blinkt, umso besser ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).



Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'



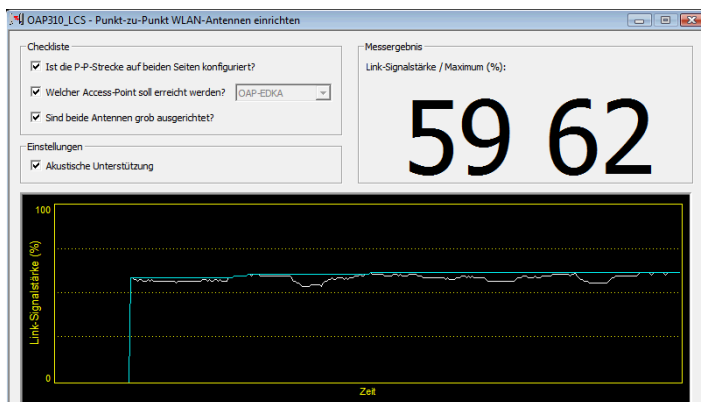
i Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN ► Allgemein ► Physikalische WLAN-Einstellungen ► Punkt-zu-Punkt**).

Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2P-Verbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert (gegenüberliegende Basisstation mit MAC-Adresse oder Stations-Namen definiert)?

- Ist die Punkt-zu-Punkt-Betriebsart aktiviert?
- Welcher Access Point soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitors gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis Sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

8.2.3 Vermessung von Funkstrecken

Nach der Planung und Einrichtung kann die Funkstrecke vermessen werden, um den tatsächlichen Datendurchsatz zu bestimmen. Weitere Informationen zu den verwendeten Tools und zum Mess-Aufbau finden Sie im LANCOM Techpaper „Performance von P2P-Verbindungen im Outdoor-Bereich“ als Download auf www.lancom.de.

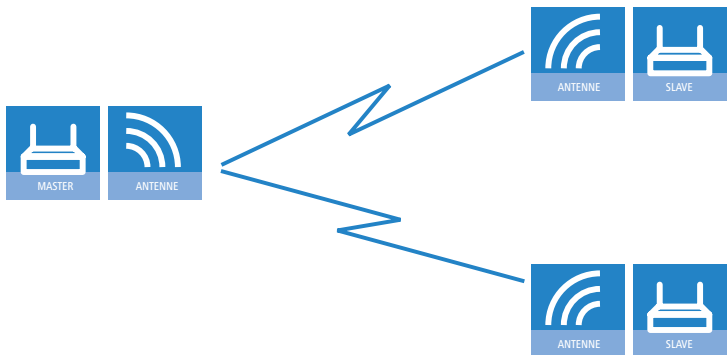
8.2.4 Punkt-zu-Punkt-Betriebsart aktivieren

Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart“ festgelegt:

- **Aus:** Der Access Point kann nur mit mobilen Clients kommunizieren
- **An:** Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- **Exklusiv:** Der Access Point kann nur mit anderen Basis-Stationen kommunizieren

Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituation kann mit dem geeigneten „Kanalwahlverfahren“ verhindert werden:

- **Master:** Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- **Slave:** Alle anderen Access Points suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.



Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4 GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.




Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i/WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich (ein Master als Authentication Server und ein Slave als Client).

8.2.5 Konfiguration der P2P-Verbindungen


Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen werden neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren die MAC-Adressen oder die Stationsnamen der Gegenstellen eingetragen.

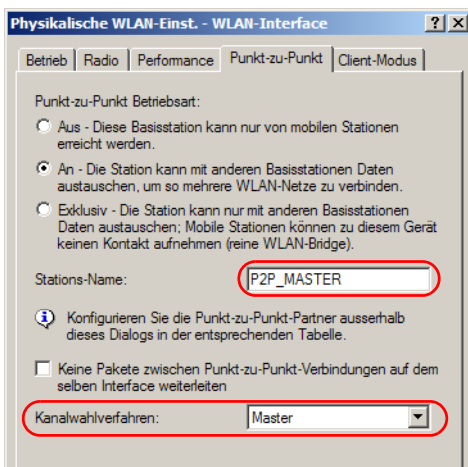
Bei der Konfiguration mit LANconfig finden Sie die Einstellungen für die P2P-Verbindungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'Wireless LAN'.

 Die Konfiguration der P2P-Verbindungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

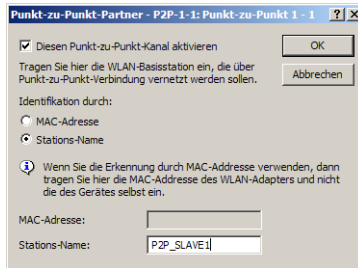
① Öffnen Sie mit der Schaltfläche **Physikalische WLAN-Einst.** die Optionen für das entsprechende WLAN-Interface und wechseln Sie dort auf die Registerkarte 'Punkt-zu-Punkt'.

② Aktivieren Sie hier die geeignete Punkt-zu-Punkt-Betriebsart und stellen Sie als Kanalwahlverfahren entweder 'Master' oder 'Slave' ein. Wenn die Gegenstellen der P2P-Verbindungen über den Stationsnamen identifiziert werden sollen, tragen Sie einen eindeutigen Namen für diese WLAN-Station ein.

 Bei Modellen mit mehreren WLAN-Modulen kann der Stationsname für jede physikalische WLAN-Schnittstelle separat eingetragen werden.



- ③ Schließen Sie die physikalischen WLAN-Einstellungen und öffnen Sie die Liste der **Punkt-zu-Punkt-Partner**. Tragen Sie zu jeder der maximal sechs P2P-Verbindungen entweder die jeweiligen MAC-Adressen der WLAN-Karte auf der Gegenseite ein oder den Namen der entsprechenden WLAN-Station (je nach Wahl der Identifizierung).



Bitte beachten Sie, hier nur die MAC-Adressen der WLAN-Karten auf der anderen Seite der Verbindung einzutragen! Nicht die eigenen MAC-Adressen und nicht die MAC-Adressen von anderen Interfaces, die möglicherweise in den Basisstationen vorhanden sind.

Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweiligen Antennenanschlusses angebracht ist. Verwenden Sie nur die als „WLAN-MAC“ oder „MAC-ID“ gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!

Point-to-Point-Gegenstellen über Stationsnamen anbinden

Bei der Konfiguration der Punkt-zu-Punkt-Verbindungen kann alternativ zu den MAC-Adressen auch der Stationsname der Gegenstellen verwendet werden.

Der Stationsname wird zunächst in den Punkt-zu-Punkt-Einstellungen der Wireless Router oder Access Points definiert.

- LANconfig: **Wireless LAN** ▶ **Allgemein** ▶ **Physikalische WLAN-Einst.** ▶ **Punkt-zu-Punkt**
- WEBconfig: **Setup** ▶ **Schnittstellen** ▶ **WLAN Interpoint-Einstellungen**



Bei Modellen mit mehreren WLAN-Modulen kann der Stationsname für jede physikalische WLAN-Schnittstelle separat eingetragen werden.

Bei der Konfiguration der Punkt-zu-Punkt-Verbindung wird dann die Identifikation durch Stationsnamen gewählt, dazu wird der Name der entsprechenden Station eingetragen.

- LANconfig: **Wireless LAN** ▶ **Allgemein** ▶ **Punkt-zu-Punkt-Partner**
- WEBconfig: **Setup** ▶ **Schnittstellen** ▶ **WLAN Interpoint-Gegenstellen**

8.2.6 Sicherheit von Punkt-zu-Punkt-Verbindungen

Mit IEEE 802.11i kann auch die Sicherheit auf Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessert werden. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security (LEPS).

Verschlüsselung mit 802.11i/WPA

Zum Aktivieren der 802.11i-Verschlüsselung auf einer korrekt konfigurierten P2P-Verbindung passen Sie die Einstellungen für das erste logische WLAN-Netzwerk im verwendeten WLAN-Interface an (also WLAN-1, wenn Sie das erste WLAN-Modul für die P2P-Verbindung nutzen, WLAN-2 wenn Sie das zweite WLAN-Modul z. B. bei einem Access Point mit zwei WLAN-Modulen nutzen).

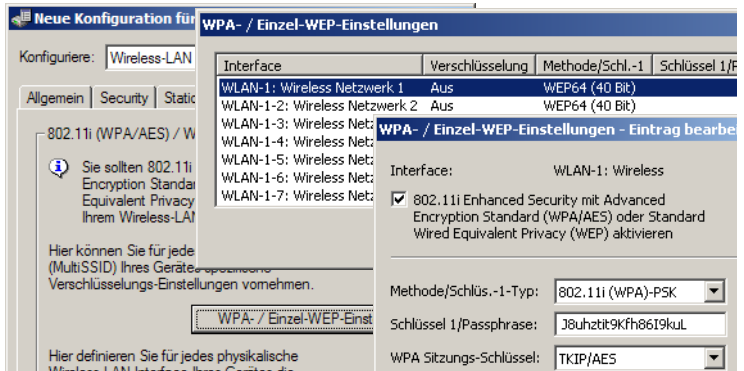
- Aktivieren Sie die 802.11i-Verschlüsselung.
- Wählen Sie als Methode '802.11i (WPA)-PSK' aus.
- Geben Sie die verwendete Passphrase ein.



Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.

Bei der Konfiguration mit LANconfig finden Sie die Verschlüsselungs-Einstellungen im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte '802.11i/WEP'.

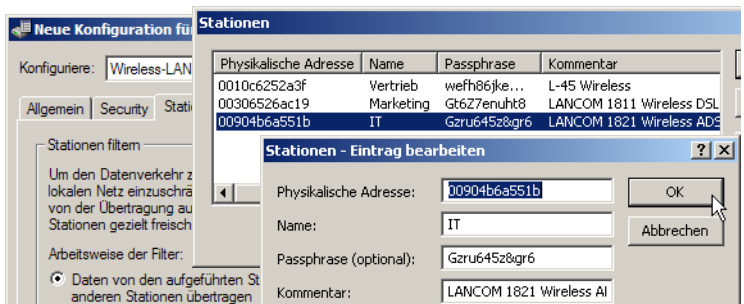


LEPS für P2P-Verbindungen

Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security (LEPS), also der Verknüpfung der MAC-Adresse mit der Passphrase.

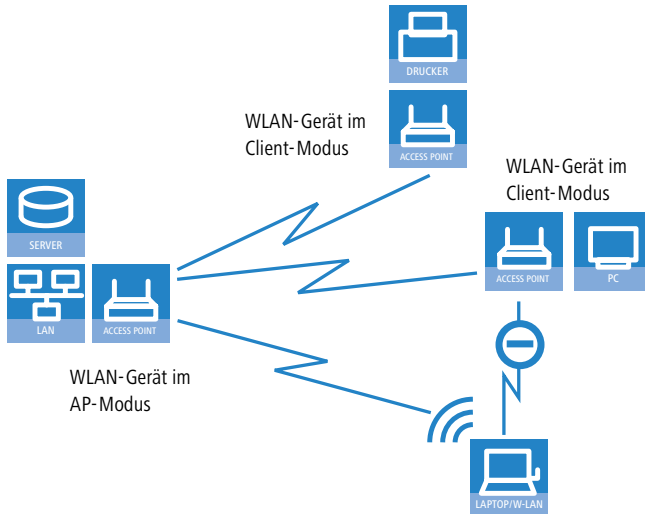
Mit LEPS können einzelne Punkt-zu-Punkt-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein Access Point verwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher.

Bei der Konfiguration mit LANconfig geben Sie die Passphrases der im WLAN zugelassenen Stationen (MAC-Adressen) im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen** ein.



8.3 Konfiguration des Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein Funk-LAN können LANCOM-Geräte mit WLAN-Modul in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher Funk-LAN-Adapter verhalten und nicht wie ein Access Point (AP). Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein Funk-LAN einzubinden.



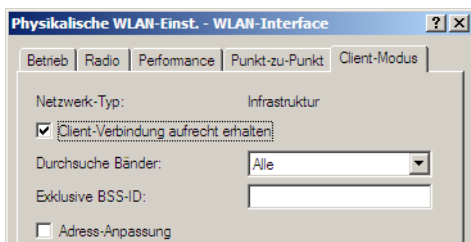
Bei einem WLAN-Gerät im AP-Modus können sich weitere WLAN-Clients anmelden, bei einem WLAN-Gerät im Client-Modus jedoch nicht.

8.3.1 Client-Einstellungen

Für LANCOM Access Points und LANCOM Wireless Router im Client-Modus können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.



Die Konfiguration der Client-Einstellungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

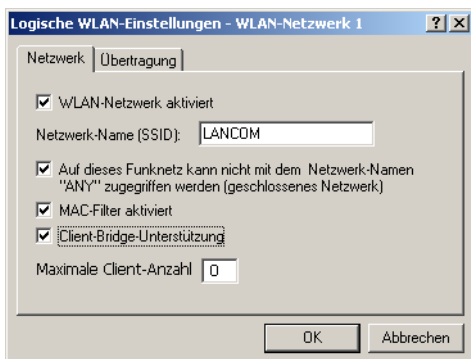


- ① Zum Bearbeiten der Einstellungen für den Client-Modus wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Client-Modus'.
- ② Stellen Sie unter 'Durchsuchte Bänder' ein, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

8.3.2 SSID des verfügbaren Netzwerks einstellen

In den WLAN-Clients muss die SSID des Netzwerks eingetragen werden, zu dem sich die Clientstationen verbinden soll.

- ① Zum Eintragen der SSID wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte 'Allgemein'. Im Abschnitt 'Interfaces' wählen Sie aus der Liste der logischen WLAN-Einstellungen das **erste** WLAN-Interface aus.

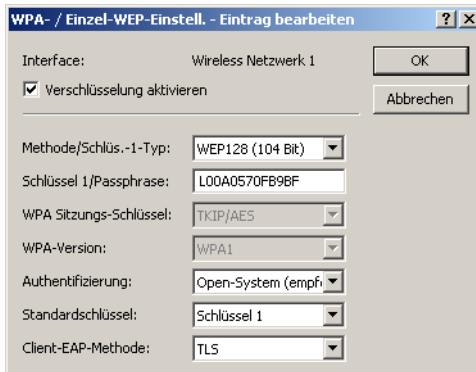


- ② Aktivieren Sie das WLAN-Netzwerk und tragen Sie die SSID des Netzwerks ein, bei dem sich die Clientstation einbuchten soll.

8.3.3 Verschlüsselungseinstellungen

Für den Zugriff auf ein WLAN müssen in der Clientstation die entsprechenden Verschlüsselungsmethoden und Schlüssel eingestellt werden.

- ① Zum Eintragen der Schlüssel wechseln Sie unter LANconfig im Konfigurationsbereich 'Wireless LAN' auf die Registerkarte '802.11i/WEP'. Im Abschnitt 'WPA- / Einzel-WEP-Einstellungen' wählen Sie aus der Liste der logischen WLAN-Einstellungen das **erste** WLAN-Interface aus



- ② Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des Access Points an.
- ③ LANCOM Access Point und LANCOM Wireless Router in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point authentifizieren. Wählen Sie dazu hier die gewünschte Client-EAP-Methode aus. Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des Access Points passen muss, bei dem sich das Gerät einbuchen will.



Je nach gewählter EAP-Methode müssen im Gerät die entsprechenden Zertifikate hinterlegt werden:

- Für TTLS und PEAP nur das EAP/TLS-Root-Zertifikat, als Schlüssel wird dabei die Kombination Benutzername:Kennwort eingetragen.
- Für TLS zusätzlich das EAP/TLS-Gerätezertifikat samt privatem Schlüssel.



Bei der Verwendung von WPA bzw. 802.1X sind evtl. weitere Einstellungen im RADIUS-Server notwendig.

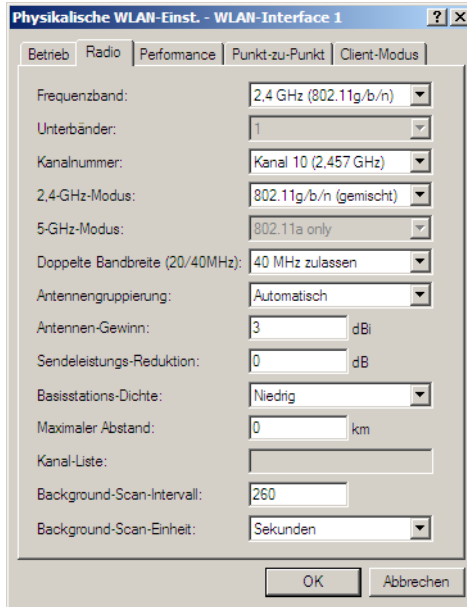
8.3.4 Roaming

Mit Roaming bezeichnet man den Übergang eines WLAN-Clients zu einem anderen Access Point, wenn er keine Verbindung zum bisherigen Access Point mehr aufrecht erhalten kann. Um das Roaming zu ermöglichen, muss sich mindestens ein weiterer Access Point in der Reichweite des Clients befinden, der ein Netzwerk mit der gleichen SSID und den passenden Radio- und Verschlüsselungs-Einstellungen anbietet.

Normalerweise würde der WLAN-Client sich nur dann bei einem anderen Access Point einbuchten, wenn er die Verbindung zu dem bisherigen Access Point vollständig verloren hat (Hard-Roaming). Das Soft-Roaming ermöglicht dem Client hingegen, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen. Mit der Funktion des Background-Scanning kann der LANCOM Wireless Router im Client-Modus schon vor Verbindungsverlust Informationen über andere verfügbare Access Points sammeln. Die Umschaltung auf einen anderen Access Point erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer Access Point in Reichweite über ein stärkeres Signal verfügt.

- ① Zum Aktivieren des Soft-Roaming wechseln Sie unter WEBconfig oder Telnet in den Bereich Setup > Schnittstellen > WLAN > Roaming und wählen dort das physikalische WLAN-Interface.
- ② Schalten Sie das Soft-Roaming ein und stellen Sie ggf. die weiteren Parameter wie die Schwellwerte und Signalpegel ein.
- ③ Zur Konfiguration des Background-Scanning wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.

■ Kapitel 8: Erweiterte WLAN- Konfiguration

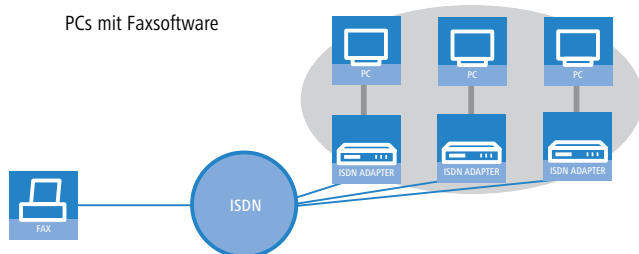


- ④ Tragen Sie als Background-Scan-Intervall die Zeit ein, in welcher der LANCOM Wireless Router zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points absucht. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit auf z. B. 260 Sekunden (2,4 GHz) bzw. 720 Sekunden (5 GHz) eingestellt.

9 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-Adaptern 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-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.



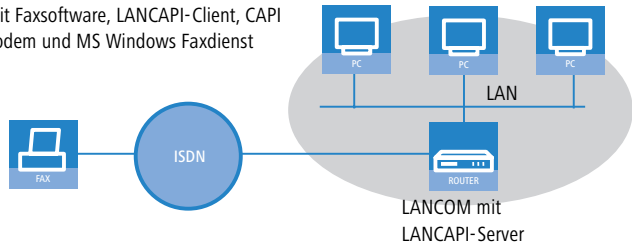
Mit der LANCAPI von LANCOM können Sie von Ihrem Arbeitsplatzrechner aus bequem Faxe versenden, ohne dass ein Faxgerät angeschlossen ist. Hierzu müssen auf Ihrem Rechner jedoch verschiedene Komponenten installiert sein:

- 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.

■ Kapitel 9: Faxe versenden mit der LANCAPi

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

PCs mit Faxsoftware, LANCAPi-Client, CAPI Faxmodem und MS Windows Faxdienst



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.

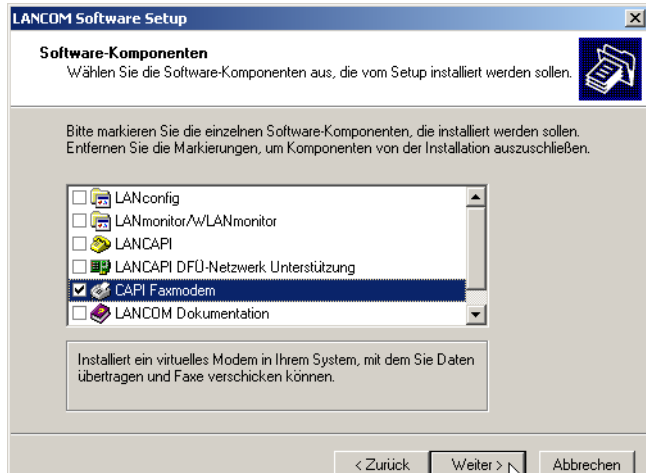


Während der CAPI Faxmodem Treiber ein "virtuelles" Faxmodem wie an einer analogen Leitung simuliert, bietet die Fax Gateway Option den direkten Versand von Faxmitteilungen über LANCAPi (Unterstützung von "Fax Gruppe 3" im CAPI-Profil und Übertragung per T.30). Dies ist für Faxserver-Lösungen interessant, welche einen LANCOM VoIP Router wie eine lokal installierte ISDN-Faxkarte per CAPI 2.0 Schnittstelle nutzen können. Somit sind gleichzeitig - je nach Routermodell - 2, 4 oder 8 parallele Faxübertragungen über ISDN möglich. Zudem bietet der direkte Zugriff auf die Faxfunktion via LANCAPi und Fax Gateway Option mehr Möglichkeiten für den Faxserver, z. B. eine Faxrufnummer pro Mitarbeiter. Die Installation spezieller Hardware in Form von Faxkarten entfällt auf dem Server, was weitere Vorteile für Serverwechsel, Skalierung und Virtualisierung bringt. Für den Faxdienst von Microsoft Windows eignet sich die Fax Gateway Option nicht.

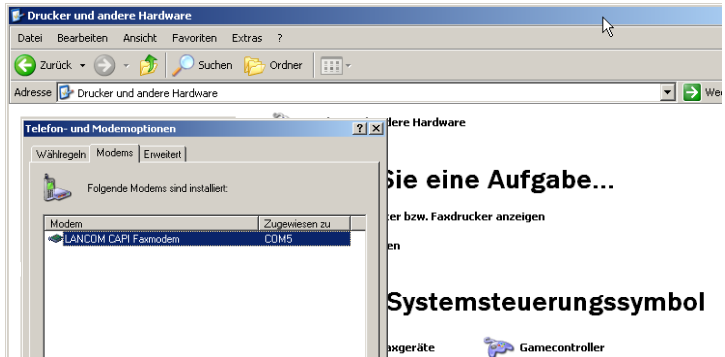
9.1 Installation des LANCOM CAPI Faxmodem

- ① Wählen Sie im Setup-Programm des beiliegenden Datenträgers (CD/DVD) 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.

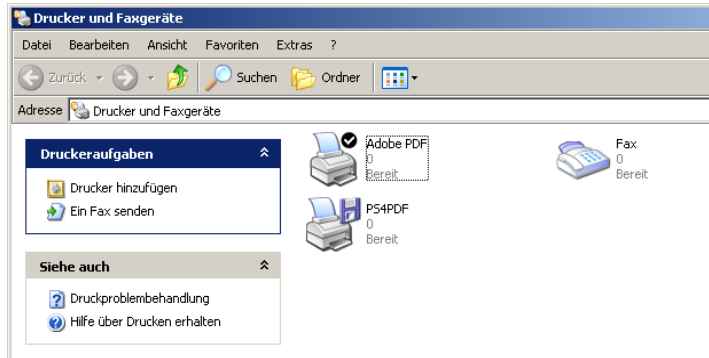


9.2 Installation des MS Windows Faxdienstes

- 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-

■ Kapitel 9: Faxe versenden mit der LANCAPI

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.

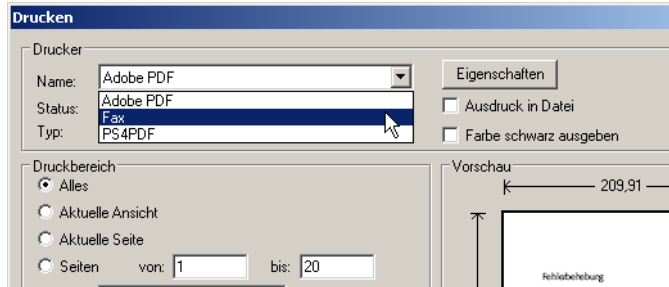
9.3 Versenden eines Faxes

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.

9.3.1 Faxe versenden mit beliebigen Büroanwendungen

- ① Öffnen Sie wie gewohnt ein Dokument in Ihrer Büroanwendung und wählen Sie den Menüpunkt **Datei/Drucken**.

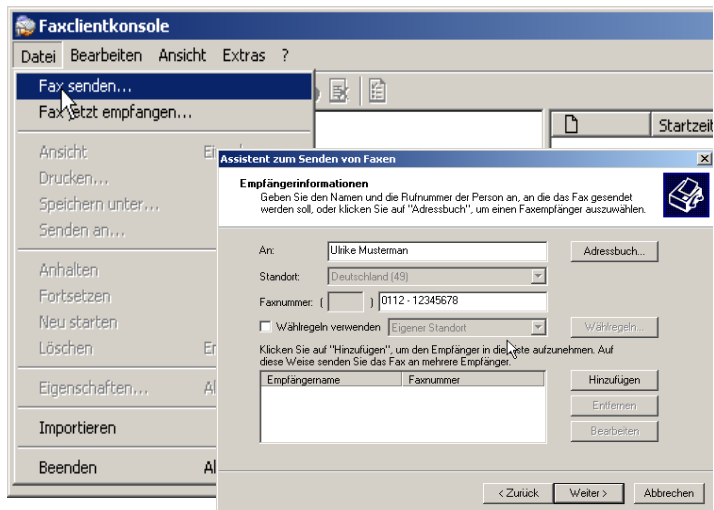
- ② Stellen Sie als Drucker das Faxgerät ein.



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

9.3.2 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.



10 Optionen und Zubehör

Ihr Gerät verfügt über zahlreiche Erweiterungsmöglichkeiten und die Möglichkeit das umfangreiche LANCOM Zubehör zu nutzen. In diesem Kapitel finden Sie Informationen darüber, welches Zubehör erhältlich ist und wie Sie es zusammen mit Ihrem Access Point verwenden können.

- Durch optionale Antennen der AirLancer-Serie lässt sich die Reichweite des Access Points erhöhen und an besondere Umgebungsbedingungen anpassen.
- Mit der LANCOM Public Spot Option lässt sich das Gerät um zusätzliche Abrechnungsfunktionen erweitern und zu einem Wireless Public Spot aufzurüsten.

10.1 Optionale AirLancer Extender Antennen

Um die Reichweite der Geräte zu erhöhen oder den Access Point an besondere Umgebungsbedingungen anzupassen, können Sie AirLancer Extender Antennen an das Gerät anschließen. Eine Übersicht, welche Antennen unterstützt werden und anschließbar sind, finden Sie jederzeit auf der LANCOM Webseite unter www.lancom.eu.



Zur Berechnung der Konfiguration von AirLancer Extender Antennen und auch von Fremdanennen, die Sie an das LANCOM anschließen wollen, können Sie den Antennen-Distanz-Kalkulator nutzen (als Download verfügbar unter www.lancom.eu).



Beachten Sie bei der Montage von separat erworbenen Antennen, dass die im jeweiligen Land maximal zulässige Sendeleistung des WLAN-Systems nach EIRP nicht überschritten werden darf. Für die Einhaltung der Grenzwerte ist der Betreiber des Systems verantwortlich.



Bei Antennen im Außenbereich ist für den inneren Blitzschutz der Überspannungsadapter AirLancer Extender SA-5L **immer erforderlich** – der AirLancer Extender SA-5L wird dabei zwischen dem Access Point und der Antenne montiert, dabei möglichst nah am Access Point.



Antennen dürfen nur bei ausgeschaltetem Gerät montiert oder gewechselt werden. Die Montage oder Demontage bei eingeschaltetem Gerät kann zur Zerstörung der WLAN-Module führen!

10.1.1 Antenna Diversity

Bei der Übertragung von Funksignalen kommt es z. B. durch Reflektion und Streuung des Signals zu starken Qualitätsverlusten. An manchen Stellen überlagern sich die Schwingungen der reflektierten Signale so ungünstig, dass die Signalstärke zurückgeht bzw. vollständig ausgelöscht wird. Zur Verbesserung der Übertragungsqualität kommen sogenannte „Diversity“-Verfahren zum Einsatz. Das Prinzip eines „Diversity“-Verfahrens beruht darauf, dass am Empfangsort das Nachrichtensignal mehrfach (meistens zwei Mal) empfangen wird.

Jedes WLAN-Modul verfügt über zwei Sende/Empfangseinheiten, an die jeweils eine Antenne angeschlossen werden kann. Bei Antenna Diversity prüft das WLAN-Modul, auf welcher Sende/Empfangseinheit (Antenne) von einem bestimmten Client das stärkere Signal empfangen wird und verwendet nur dieses eine (stärkere) Signal. Der Access Point speichert die Information, über welche Sende/Empfangseinheit er zuletzt Daten von den jeweiligen Clients empfangen hat und verwendet diese Einheit (Antenne) dann auch für den Sendevorgang zu diesem Client. Die unterschiedlichen auf dem Access Point eingebuchten Clients nutzen mit Antenne Diversity also immer die beste Sende/Empfangseinheit.

10.1.2 Polarisations-Diversity

Bei anderen Diversity-Verfahren werden die beiden Nachrichtensignale durch eine geeignete Weiterverarbeitung zu einem einzigen Signal zusammengeführt. Am bekanntesten sind Space- (Raum) und Polarisations-Diversity. LANCOM Systems bietet als Erweiterung der LANCOM-Geräte verschiedene Polarisations-Diversity-Antennen an. Bei diesen Modellen werden in einer Sende/Empfangseinheit zwei senkrecht zueinander polarisierte Signale empfangen und dann zu einem Signal kombiniert, das stärker ist als die beiden Einzelsignale – es entsteht der so genannte Polarisations-Gewinn.

10.1.3 Installation der AirLancer Extender Antennen

Für die LANCOM VoIP Router sind folgende Diversityantennen als Zubehör erhältlich:

- AirLancer Extender O-D80g (2,4 GHz), Art.Nr. 61221
- AirLancer Extender O-D60a (5 GHz), Art.Nr. 61222
- AirLancer Extender O-D9a (5 GHz), Art.Nr. 61224



Bitte beachten Sie bei der Montage von externen Antennen die Hinweise zum Blitzschutz im LANCOM Outdoor Wireless Guide (mitgeliefert oder als Download auf www.lancom.eu). Die Montage von Antennen ohne ausreichenden Blitzschutz kann zu ernsthaften Schäden in den Access Points bzw. in der über das Netzwerk angeschlossenen Infrastruktur führen!

Zur Installation einer optionalen AirLancer Antenne schalten Sie das Gerät aus, indem Sie das Kabel der Spannungsversorgung aus dem Gerät herausziehen. Entfernen Sie nun vorsichtig die beiden Diversity-Antennen auf der Rückseite, indem Sie diese abschrauben. Schließen Sie die AirLancer Antenne an den mit 'Antenna Main' beschrifteten Antennenanschluss an.

'Antenna Main'-Anschluss für AirLancer-Antenne



10.2 LANCOM Public Spot Option

Wireless Public Spots sind öffentlich zugängliche Punkte, an denen sich Benutzer mit ihrem eigenen mobilen Rechner per Funk in ein Netzwerk (z. B. ein Firmen-LAN oder das Internet) einwählen können.



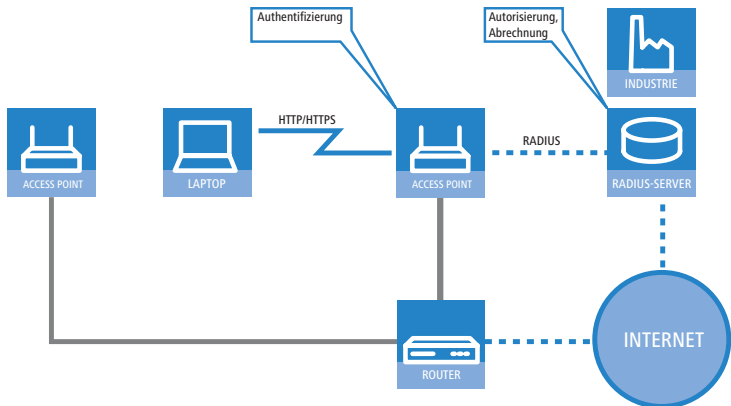
Bitte beachten Sie, dass der Betrieb eines LANCOM VoIP Routers mit LANCOM Public Spot Option (manchmal auch als HotSpot bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines LANCOM VoIP Routers über die jeweils geltenden Vorschriften.

Die Wireless LAN Technologie ist ideal dafür geeignet, um an Plätzen wie Flughäfen, Hotels, Bahnhöfen, Restaurants oder Cafés (sogenannten Public Hot Spots) drahtlose Internet-Dienstleistungen für die Öffentlichkeit anzubieten. Die LANCOM Public Spot Option wendet sich dabei an alle Betreiber von öffentlichen Funknetzen und stellt für die LANCOM Access Points und LANCOM Router Zusatzfunktionen zur Authentifizierung und Abrechnung von öffentlichen Internet-Dienstleistungen zur Verfügung und ermöglicht damit den einfachen Aufbau und die Wartung von Public Hot Spots.

Die Authentifizierung und Abrechnung einzelner Benutzer wird anwenderfreundlich über Web-Seiten realisiert, so dass Client-PCs mit einer Wi-Fi-zer-

tifizierten Funkkarte (z. B. AirLancer) und einem Standard-Internet-Browser direkt online gehen können.

Die LANCOM Public Spot Option ist die optimale Lösung für öffentliche Funk-LANs. Denn Wireless LANs eignen sich sehr gut für Firmennetzwerke und zur Funkvernetzung zu Hause. Für öffentliche Access-Dienste fehlt es im Standard jedoch an Mechanismen zur Authentifizierung und Abrechnung von einzelnen Benutzern (AAA - Authentication / Authorisation / Accounting). Diesen Mangel behebt die LANCOM Systems Open User Authentication (OUA), der Kernbestandteil der LANCOM Public Spot Option. Das OUA-Verfahren realisiert die Authentifizierung aller Funk-Clients per User-Name und Passwort und prüft die Autorisierung einzelner Benutzer per RADIUS. Accounting-Daten (Online-Zeit und Datenvolumen) können pro Benutzer und pro Sitzung an den zentralen RADIUS-Server weitergegeben werden. Client-PCs benötigen lediglich eine Funkkarte (z. B. AirLancer), TCP/IP und einen Internet-Browser. Weitere Software wird nicht benötigt. Die Public Spot Option eignet sich daher optimal zur Einrichtung von drahtlosen Internet-Access-Dienstleistungen in Hotels, Restaurants, Cafés, Flughäfen, Bahnhöfen, Messegeländen oder Universitäten.



Mit der LANCOM Public Spot Option erweitern Sie einen Access Point nachträglich um diese Funktion und rüsten ihn zum Wireless Public Spot auf.

11 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.

11.1 Sicherheit im Funk-LAN

Bei der Betrachtung von Funk-LANs entstehen oft erhebliche Sicherheitsbedenken. Vielfach wird angenommen, ein Datenmissbrauch der über Funk übertragenen Daten sei verhältnismäßig einfach.

Funk-LAN-Geräte von LANCOM Systems erlauben den Einsatz moderner Sicherungstechnologien:

- Verschlüsselung des Datentransfers mit WPA2 mit AES-Verschlüsselung
- 802.1x / EAP
- LANCOM Enhanced Passphrase Security (LEPS)
- Zugangskontrolle über MAC-Adresse
- Optionales IPSec-over-WLAN VPN

11.1.1 Verschlüsselung des Datentransfers

Der Verschlüsselung des Datentransfers kommt bei Funk-LANs eine besondere Rolle zu. Für den Funktransfer nach IEEE 802.11 gibt es die ergänzenden Verschlüsselungsstandards 802.11i/WPA und WEP. Ziel dieser Verschlüsselungsverfahren ist, das Sicherheitsniveau kabelgebundener LANs auch im Funk-LAN zu gewährleisten.



LANCOM Systems empfiehlt für den Passphrase-Betrieb den Einsatz von 802.11i (WPA2) in Verbindung mit AES als sicherste Passphrase-Variante. Der Schlüssel sollte zufällig aus einem großen Zeichenbereich gewählt und möglichst lang (32 bis 63 Zeichen) sein. Hiermit können Wörterbuchattacken vermieden werden.

- Verschlüsseln Sie die im WLAN übertragenen Daten. Aktivieren Sie dazu die maximal mögliche Verschlüsselung (802.11i mit AES, TKIP oder WEP)

und tragen Sie entsprechenden Schlüssel bzw. Passphrases im Access Point und in den WLAN-Clients ein.

- Die Passphrases für 802.11i oder WPA müssen nicht so häufig gewechselt werden, da bereits regelmäßig im Betrieb neue Schlüssel pro Verbindung verwendet werden. Nicht nur deswegen ist die Verschlüsselung per 802.11i/AES oder WPA/TKIP wesentlich sicherer als das veraltete WEP-Verfahren. Falls Sie aus Gründen der Kompatibilität zu älteren WLAN-Clients WEP verwenden, ändern Sie regelmäßig die WEP-Schlüssel in Ihrem Access Point.
- Falls es sich bei den übertragenen Daten um extrem sicherheitsrelevante Informationen handelt, können Sie zusätzlich zur besseren Authentifizierung der Clients das 802.1x-Verfahren aktivieren ('802.1x / EAP' →Seite 117) oder aber eine zusätzliche Verschlüsselung der WLAN-Verbindung einrichten, wie sie auch für VPN-Tunnel verwendet wird ('IPSec-over-WLAN' →Seite 118). In Sonderfällen ist auch eine Kombination dieser beiden Mechanismen möglich.



Detaillierte Informationen zur WLAN-Sicherheit und zu den verwendeten Verschlüsselungsmethoden finden Sie im LCOS Referenzhandbuch.



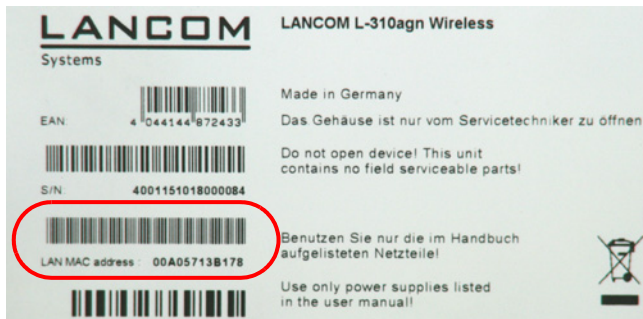
Bitte beachten Sie auch die Informationen im Kasten „Standard-Verschlüsselung mit WPA-PSK“.

Standard-Verschlüsselung mit WPA-PSK

Im werksseitigen Auslieferungszustand bzw. nach einem Reset unterscheiden sich LANCOM Access Points und LANCOM Wireless Router.

- Unkonfigurierte Access Points können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden. Die WLAN-Module sind ausgeschaltet, die Geräte suchen selbständig im LAN einen LANCOM WLAN Controller, von dem sie automatisch eine Konfiguration beziehen können.
- Unkonfigurierte Wireless Router können auch im Auslieferungszustand über die WLAN-Schnittstelle in Betrieb genommen werden. Dazu wird standardmäßig die hier beschriebene Standard-Verschlüsselung mit WPA-PSK verwendet.

Der Preshared Key (PSK) für die Standard-WPA-Verschlüsselung setzt sich aus dem Anfangsbuchstaben „L“ gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise zusammen. Die LAN-MAC-Adressen der LANCOM-Geräte beginnen immer mit der Zeichenfolge „00A057“. Sie finden die LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie **nur** die als „MAC-Address“ gekennzeichnete Nummer, die mit „00A057“ beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!



Für ein Gerät mit der LAN-MAC-Adresse „00A05713B178“ lautet der Preshared Key also „L00A05713B178“. Dieser Schlüssel ist in den 'WPA-/Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1/Passphrase' eingetragen.

Um mit einer WLAN-Karte eine Verbindung zu einem LANCOM Wireless Router im Auslieferungszustand herzustellen, muss in der WLAN-Karte die WPA-Verschlüsselung aktiviert und der 13-stellige Preshared Key eingetragen werden.



Ändern Sie den Preshared Key für WPA nach der ersten Anmeldung, um eine sichere Verbindung zu gewährleisten.

11.1.2 802.1x / EAP

Der internationale Industrie-Standard IEEE 802.1x und das **Extensible Authentication Protocol (EAP)** ermöglichen Access Points die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können zentral auf einem RADIUS-Server (integrierter RADIUS/EAP-Server im LANCOM VoIP Router oder externer RADIUS/EAP-Server) verwaltet und von dem Access Point bei Bedarf von dort abgerufen werden. Das dynamisch erzeugte und kryptografisch sichere Schlüsselmaterial für 802.11i (WPA1/2) ersetzt dabei die manuelle Schlüsselverwaltung.

Seit Windows XP ist die IEEE-802.1x-Technologie bereits fest integriert. Für andere Betriebssysteme existiert Client-Software. Die Treiber der LANCOM AirLancer-Funkkarten verfügen über einen integrierten 802.1x Client.

11.1.3 LANCOM Enhanced Passphrase Security

Mit LEPS (**LANCOM Enhanced Passphrase Security**) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Fehlerquellen beim Verteilen der Passphrase vermeidet. Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zugeordnet – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

LEPS kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden und funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptoren, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im Access Point konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installationen ein Access Point entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin geschützt, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.



Gastzugang mit LEPS: LEPS kann auch zur Einrichtung eines Gast-Zugangs verwendet werden. Dabei werden alle Benutzer des internen WLAN-Netzes mit individuellen Passphrases ausgestattet. Für Gäste steht eine eigene SSID mit einer globalen Passphrase zur Verfügung.

Um Mißbrauch zu verhindern, kann die globale Passphrase regelmäßig – z. B. alle paar Tage – geändert werden.

11.1.4 Zugangskontrolle über MAC-Adresse

Jedes Netzwerkgerät verfügt über eine unverwechselbare Identifizierungsnummer. Diese Identifizierungsnummer wird als MAC-Adresse (**Media Access Control**) bezeichnet und ist weltweit einmalig.

Die MAC-Adresse ist fest in die Hardware einprogrammiert. Auf einem Funk-LAN-Gerät von LANCOM Systems finden Sie die MAC-Adresse auf dem Gehäuse.

Der Zugriff auf ein Infrastruktur-Netzwerk kann unter Angabe von MAC-Adressen auf bestimmte Funk-LAN-Geräte beschränkt werden. Dazu gibt es in den Access Points Filter-Listen (ACL = Access Control List), in denen die zugriffsberechtigten MAC-Adressen hinterlegt werden können.

11.1.5 IPSec-over-WLAN

Mittels IPSec-over-WLAN kann zusätzlich zu den bereits vorgestellten Sicherheitsmechanismen ein Funknetzwerk optimal abgesichert werden. Hierzu sind eine Basisstation mit VPN-Unterstützung und der LANCOM Advanced VPN Client erforderlich, welcher unter aktuellen Windows- oder MAC-Betriebssystemen arbeitet. Für andere Betriebssysteme existiert Clientsoftware von Fremdherstellern.

11.2 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.

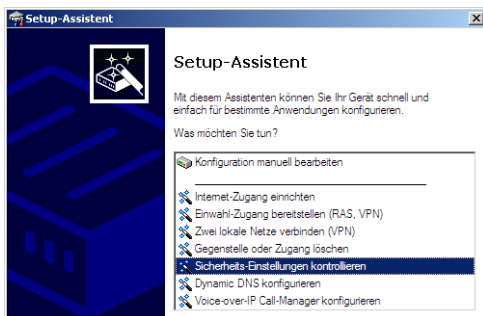
Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

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.

11.2.1 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 Bei Geräten mit WLAN-Schnittstelle haben Sie nun die Möglichkeit, die Sicherheitsparameter für das Funknetzwerk einzustellen. Dazu gehören der Name des Funknetzwerks, die Closed-Network-Funktion und die Verschlüsselung mit 802.11i/WPA oder WEP. Bei einem Gerät mit der Option für eine zweite WLAN-Schnittstelle können Sie diese Parameter für beide Funknetzwerke separat eingeben.
- 6 Für die WLAN-Schnittstelle können Sie anschließend die Filterlisten für Stationen (ACL) und Protokolle definieren. Damit schränken Sie den Datenaustausch zwischen dem drahtlosen Netzwerk und dem lokalen Netzwerk ein.
- 7 Im Bereich der Firewall aktivieren Sie die Stateful-Inspection, das Ping-Blocking und den Stealth-Mode.

- ⑧ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.


11.2.2 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)
- Sicherheitsparameter wie WLAN-Name, Closed-Network-Funktion, WPA-Passphrase, WEP-Schlüssel, ACL-Liste und Protokoll-Filter


11.3 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 das Funknetzwerk durch Verschlüsselung und Zugangskontrolllisten abgesichert?

Mit Hilfe von 802.11i, WPA oder WEP verschlüsseln Sie die Daten im Funknetzwerk mit verschiedenen Verschlüsselungsmethoden wie AES, TKIP oder WEP. LANCOM Systems empfiehlt die stärkste mögliche Verschlüsselung mit 802.11i und AES. Wenn der eingesetzte WLAN Client Adapter diese nicht unterstützt, nutzen Sie TKIP oder zumindest WEP. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter Verschlüsselungs-Funktion mindestens eine Passphrase oder ein WEP-Schlüssel eingetragen und zur Verwendung ausgewählt ist.

 LANCOM Systems rät aus Sicherheitsgründen von der Verwendung von WEP ab! Setzen Sie WEP nur in begründeten Ausnahmefällen ein

und ergänzen Sie die WEP-Verschlüsselung nach Möglichkeit mit anderen Schutzmechanismen!



Ab Werk wird für jedes unkonfigurierte Gerät standardmäßig eine WPA-Verschlüsselung aktiviert. Für WLAN-Interfaces, die von einem LANCOM WLAN Controller verwaltet werden, wird die WPA-Verschlüsselung durch die zentralen Verschlüsselungseinstellungen in den Profilen des WLAN-Controllers überschrieben.

Zur Kontrolle der Einstellungen wählen Sie in LANconfig im Konfigurationsbereich 'Wireless LAN' auf der Registerkarte '802.11i/WEP' die Verschlüsselungseinstellungen für die logischen WLAN-Interfaces aus.

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

Mit der LANCOM Enhanced Passphrase Security (LEPS) ordnen Sie jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zu – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

■ 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 ein-

zelne 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.

12 Konfiguration der ISDN- und Analog-Schnittstellen im Detail

12.1 ISDN-Schnittstelle im NT- oder TE-Modus

Die ISDN-Schnittstellen können je nach Modell wahlweise zum Anschluss an ISDN-Amtsleitungen oder zum Anschluss von ISDN-Endgeräten verwendet werden. Dazu werden die Schnittstellen in den NT- bzw. TE-Modus geschaltet:

- ISDN-TE-Schnittstelle („externer ISDN-Anschluss“): Eine ISDN-Schnittstelle im TE-Modus zum Anschluss an einen ISDN-Bus einer übergeordneten ISDN-TK-Anlage oder einen ISDN-NTBA. Diese ISDN-Schnittstelle kann für Backup-Verbindungen über ISDN oder als Einwahl-Schnittstelle für entfernte Gegenstellen genutzt werden.



Bei den Modellen LANCOM 1723 VoIP und LANCOM 1823 VoIP kann die ISDN2-Schnittstelle in den TE-Modus geschaltet werden, darf aber nicht direkt mit dem Telefonnetz (NTBA) oder indirekt über eine Telefonanlage (mit Durchschleifung/Notschaltung) mit dem Telefonnetz verbunden werden!

- ISDN-NT-Schnittstelle („interner ISDN-Anschluss“): Mit der ISDN-Schnittstelle im NT-Modus stellt der LANCOM VoIP Router selbst einen internen ISDN-Bus zur Verfügung. An diese ISDN-Schnittstelle können ISDN-TK-Anlagen oder ISDN-Telefone angeschlossen werden.

Im Auslieferungszustand sind die mit ☒ gekennzeichneten ISDN-Schnittstellen auf den TE-Modus, die mit ☎ gekennzeichneten ISDN-Schnittstellen auf den NT-Modus eingestellt. Je nach Bedarf können die ISDN-Schnittstellen entsprechend umgestellt werden:

- Mit mehreren TE-Schnittstellen können z.B. alle verfügbaren B-Kanäle für Backup- oder Einwahlzwecke genutzt werden.
- Mit mehreren NT-Schnittstellen können z.B. einer untergeordneten ISDN-TK-Anlage alle verfügbaren B-Kanäle bereitgestellt werden.

Je nach Kombination von ISDN-Schnittstellen im TE- und NT-Modus müssen hardwareseitig ggf. die Funktionen Buserminierung, Life-Line-Support und Spannungsweiterleitung sowie softwareseitig das passende Protokoll eingestellt werden. Die Protokoll-Einstellung berücksichtigt dabei auch den verwendeten ISDN-Anschlussyp (Punkt-zu-Mehrpunkt oder Punkt-zu-Punkt).



Beim Anschluss an eine ISDN-Schnittstelle, die von der Defaulteinstellung abweicht, muss zwingend der beiliegende Adapter verwendet werden. Mit diesem Adapter werden die Kontakte der ISDN-Schnittstelle gekreuzt. Ohne Verwendung des Adapters können sowohl der LANCOM VoIP Router als auch die verbundenen Geräte Schaden nehmen!

12.2 Buserminierung, Life-Line-Support und Spannungsversorgung

Mit den DIP-Schaltern an der Unterseite des Gerätes werden die Hardware-Funktionen der ISDN-Schnittstellen eingestellt.

- Die **Buserminierung** ist in der Regel erforderlich bei einer ISDN-Schnittstelle im NT-Modus.

Für ISDN-Schnittstellen im TE-Modus wird die Buserminierung üblicherweise ausgeschaltet. Falls der LANCOM VoIP Router das letzte Gerät an einem längeren ISDN-Bus ist und dieser nicht selbst terminiert ist, kann ggf. die Aktivierung der Buserminierung für eine ISDN-Schnittstelle im TE-Modus sinnvoll sein.

Nicht bei LANCOM
1724 VoIP

- Bei aktiviertem **Life-Line-Support** werden die Schnittstellen ISDN 1 und ISDN 2 gebrückt, wenn das Gerät durch Stromausfall nicht zur Verfügung steht oder die ISDN-2-Schnittstelle ausgeschaltet ist (Default: ein). Der Life-Line-Support wird eingesetzt beim Anschluss des LANCOM 1722 VoIP über eine TE-Schnittstelle an eine externe ISDN-Leitung bei gleichzeitigem Betrieb von ISDN-Endgeräten am internen ISDN-Anschluss einer NT-Schnittstelle. Im gebrückten Zustand können die ISDN-Endgeräte direkt den externen ISDN-Bus nutzen.

Zum Aktivieren des Life-Line-Supports müssen sich alle vier DIP-Schalter (3 bis 6) in der oberen Position befinden, zum Deaktivieren müssen alle vier DIP-Schalter in die untere Position gebracht werden.



Deaktivieren Sie den Life-Line-Support, wenn beide ISDN-Schnittstellen im gleichen Modus betrieben werden, also z.B. zweimal TE- oder zweimal NT. In diesen Anwendungsfällen dürfen die Schnittstellen bei Stromausfall nicht gebrückt werden!

Nur LANCOM 1722
VoIP und LANCOM
1724 VoIP

- Mit der **ISDN-Spannungsweiterleitung** wird die Busspannung eines externen ISDN-Busses an ISDN 1 an die an ISDN 2 (LANCOM 1722 VoIP) bzw. ISDN 3 (LANCOM 1724 VoIP) angeschlossenen Endgeräte weiterge-

schaltet. Damit können am internen ISDN-Bus des LANCOM VoIP Router auch ISDN-Endgeräte ohne eigene Spannungsversorgung betrieben werden.



Deaktivieren Sie unbedingt die ISDN-Spannungsweiterleitung, wenn beide ISDN-Schnittstellen im TE-Modus betrieben werden, also z.B. beide ISDN-Schnittstellen mit einem ISDN-NTBA verbunden sind. Durch die Spannungsweiterleitung würde in diesem Fall ein Kurzschluss entstehen, der das Gerät und die ISDN-NTBAs beschädigen kann!

Zum Aktivieren der Spannungsweiterleitung müssen sich die entsprechenden DIP-Schalter (7 und 8 beim LANCOM 1722 VoIP, 5 und 6 beim LANCOM 1724 VoIP) in der oberen Position befinden, zum Deaktivieren müssen die DIP-Schalter in die untere Position gebracht werden.

Nur LANCOM 1723
VoIP und LANCOM
1823 VoIP

- Mit der **internen Spannungsversorgung** können bei den Modellen LANCOM 1723 VoIP und LANCOM 1823 VoIP an der ISDN2-Schnittstelle **8** maximal zwei Telefone ohne eigene Spannungsversorgung mit Speisung über ISDN betrieben werden.

Zum Aktivieren der internen Spannungsversorgung müssen sich die entsprechenden DIP-Schalter (1 und 2) in der oberen Position befinden, zum Deaktivieren müssen die DIP-Schalter in die untere Position gebracht werden.



Bei Überlast schaltet sich die Spannungsversorgung automatisch aus, beim Abfallen der Last automatisch wieder ein.

- ① Ziehen Sie vor der Einstellung der DIP-Schalter alle Kabel aus den entsprechenden Buchsen.
- ② Entfernen Sie die transparente Abdeckung der DIP-Schalter.

- ③ Stellen Sie die DIP-Schalter z.B. mit einem schmalen Schraubendreher in die gewünschte Position:

LANCOM 1722 VoIP			LANCOM 1723 VoIP	
DIP	Bedeutung	Default	Bedeutung	Default
1 + 2	ISDN 2 Rx/Tx (100 Ω Buserminierung)	oben (an)	Spannungsversorgung ISDN 2	oben (an)
3 + 4	Life-Line-Support	oben (an)	Life-Line-Support	
5 + 6		oben (an)		oben (an)
7 + 8	ISDN-Spannungsweiterleitung ISDN 1 > ISDN 2	oben (an)		oben (an)
9 + 10	ISDN 1 Rx/Tx (100 Ω Buserminierung)	unten (aus)	ISDN 1 Rx/Tx (100 Ω Buserminierung)	unten (aus)

LANCOM 1724 VoIP			LANCOM 1823 VoIP	
DIP	Bedeutung	Default	Bedeutung	Default
1 + 2	ISDN 4 Rx/Tx (100 Ω Buserminierung)	oben (an)	Spannungsversorgung ISDN 2	oben (an)
3 + 4	ISDN 3 Rx/Tx (100 Ω Buserminierung)	oben (an)	Life-Line-Support	
5 + 6	ISDN-Spannungsweiterleitung ISDN 1 > ISDN 3	unten (aus)		oben (an)
7 + 8	ISDN 2 Rx/Tx (100 Ω Buserminierung)	unten (aus)		oben (an)
9 + 10	ISDN 1 Rx/Tx (100 Ω Buserminierung)	unten (aus)	ISDN 1 Rx/Tx (100 Ω Buserminierung)	unten (aus)

- ④ Stecken Sie die Kabel wieder ein und starten Sie das Gerät.



Zur Einstellung der ISDN-Schnittstellen auf einen anderen Modus ist ausserdem eine entsprechende Software-Konfiguration erforderlich. Beim Anschluss von Geräten an eine ISDN-Schnittstelle, die von der Defaulteinstellung abweicht, muss zwingend der beiliegende Adapter verwendet werden. Mit diesem Adapter werden die Kontakte der ISDN-Schnittstelle gekreuzt.

12.3 Protokoll-Einstellung

Die Parameter der ISDN-Schnittstellen werden im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' eingetragen. Unter WEBconfig, Telnet oder SSH-Client finden Sie die Einstellung der ISDN-Schnittstellen unter `Setup/Interfaces/WAN`.

Wählen Sie das Protokoll für jedes ISDN-Interface je nach Anwendung und Typ des ISDN-Anschlusses. Punkt-zu-Mehrpunkt- sowie Punkt-zu-Punkt-Anschlüsse können an einem LANCOM VoIP Router auch gemischt verwendet werden. Folgende Optionen stehen zur Auswahl:

- **Automatisch** für automatische Auswahl des Betriebsmodus (nur im TE-Modus)
- **DSS1 TE (Euro ISDN)** zum Anschluss an einen ISDN-Bus in Punkt-zu-Mehrpunkt-Ausführung („Mehrgeräte-Anschluss“)
- **DSS1 TE Punkt zu Punkt** zum Anschluss an einen ISDN-Bus in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss“)
- **1TR6 TE (nationales ISDN)** zum Anschluss an einen ISDN-Bus nach dem nationalen ISDN-Protokoll in Deutschland
- **DSS1 NT (Euro ISDN)** zur Bereitstellung von Schnittstellen in Punkt-zu-Mehrpunkt-Ausführung („Mehrgeräte-Anschluss“)
- **DSS1 NT reverse** zur Bereitstellung von Schnittstellen in Punkt-zu-Mehrpunkt-Ausführung bei gleichzeitiger Übernahme des ISDN-Taktes der angeschlossenen ISDN-Leitung, siehe 'Taktung der ISDN-Anschlüsse'
- **DSS1 NT Punkt zu Punkt** zur Bereitstellung von Schnittstellen in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss“)
- **DSS1 NT Punkt zu Punkt reverse** zur Bereitstellung von Schnittstellen in Punkt-zu-Punkt-Ausführung („Anlagen-Anschluss“) bei gleichzeitiger Übernahme des ISDN-Taktes der angeschlossenen ISDN-Leitung, siehe 'Taktung der ISDN-Anschlüsse'
- **DSS1 Takt** zur Übernahme des ISDN-Taktes einer angeschlossenen ISDN-Leitung (siehe 'Taktung der ISDN-Anschlüsse'), ohne Signalisierung und weitere Funktion
- **Festverbindung GRPO** für Gruppe-0-Festverbindungen über ISDN
- **Aus**

Nur LANCOM 1724
VoIP



Der Betrieb im NT-Modus muss immer von Hand eingestellt werden. Wird für den Anschluss ISDN 2 beim LANCOM 1722 VoIP die Einstel-

lung 'Aus' gewählt, so ist dieser ggf. mit ISDN 1 verbunden, wenn das Gerät über die DIP-Schalter für den Life-Line-Support eingerichtet ist.



Wenn ein ISDN-Endgerät an einer ISDN-Schnittstelle im Automatik-Modus nicht richtig erkannt wird, stellen Sie das verwendete Protokoll direkt ein.

12.4 Taktung der ISDN-Anschlüsse

Zur störungsfreien Übertragung müssen alle Komponenten des ISDN-Systems (LANCOM VoIP Router, über- bzw. untergeordnete ISDN-TK-Anlagen, ISDN-Endgeräte und externe ISDN-Telefonnetze) den gleichen ISDN-Takt verwenden. Im LANCOM VoIP Router kann eine ISDN-Schnittstelle im TE-Modus den Takt von der verbundenen ISDN-Leitung übernehmen, da sich das Gerät mit der TE-Schnittstelle selbst wie ein Endgerät verhält. Der LANCOM VoIP Router kann selbst über die ISDN-Schnittstellen im NT-Modus den Takt an angeschlossene Endgeräte oder untergeordnete ISDN-TK-Anlagen weitergeben, da sich das Gerät mit der NT-Schnittstelle wie eine Vermittlungsstelle verhält.

Zur Definition der ISDN-Schnittstellen, über die ein LANCOM VoIP Router den ISDN-Takt empfängt (der dann an alle Geräte an NT-Schnittstellen weitergegeben wird), stehen verschiedene Einstellungen zur Verfügung:

- **PCM Synchronisations-Bus:** Wählt aus allen als TE oder NT reverse konfigurierten Schnittstellen eine, die gegenwärtig einen Takt liefert, automatisch aus. Sollte die gewählte Schnittstelle keinen Takt mehr liefern (z.B. aufgrund von Inaktivität auf dem Bus), so wählt der LANCOM VoIP Router die nächste verfügbare Schnittstelle, die einen Takt liefert.
- **ISDN/S0-Bus:** Mit dieser Einstellung wird gezielt der ISDN-Takt an diesem Anschluss für den LANCOM VoIP Router und die über NT-Schnittstellen verbundenen Geräte übernommen. So kann z.B. der Takt parallel zu einer vorhandenen ISDN-TK-Anlage an einem Anlagenanschluss geschaltet werden.



Die ausgewählte ISDN-Schnittstelle muss dazu als TE-Modus konfiguriert sein.

In den Einstellungen zu den ISDN-Interfaces gibt es noch zwei Modi, die in diesem Zusammenhang eine besondere Rolle spielen:

- **DSS1 NT reverse** oder **DSS1 NT Punkt zu Punkt reverse:** Wenn alle ISDN-Schnittstellen im NT-Modus betrieben werden, läuft das Taktsystem „frei“, da kein ISDN-Takt von einer TE-Schnittstelle übernommen werden

kann. Sind die ISDN-Anschlüsse in diesem Fall z.B. mit einer ISDN-TK-Anlage verbunden, die von einer anderen Quelle mit einem ISDN-Takt versorgt wird, kann es zu Übertragungsstörungen kommen, da der Takt des LANCOM VoIP Router nicht mit dem Takt der TK-Anlage synchron ist. In diesem Fall kann mit der Reverse-Einstellung gezielt der ISDN-Takt von einer Schnittstelle im NT-Modus übernommen werden, um den Takt des LANCOM VoIP Router auf das Gesamtsystem zu synchronisieren.



Die Telefonanlage bzw. die Gegenstelle mit Schnittstelle im TE-Modus muss dazu einen Takt senden können und entsprechend konfiguriert sein.

13 Rat & Hilfe

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

13.1 Es wird keine DSL-Verbindung aufgebaut

Nach dem Start versucht der Router automatisch, Kontakt zum DSL-Anbieter aufzunehmen. Während dieser Phase blinkt die WAN-LED grün. Im Erfolgsfall wechselt diese LED dann auf dauerhaftes Grün. Schlägt die Kontaktaufnahme hingegen fehl, so leuchtet die LAN-LED nicht. In der Regel ist eine der folgenden Ursachen:

Probleme an der Verkabelung?

Verwenden Sie für den DSL-Anschluss ausschließlich das mitgelieferte Anschlusskabel. Dieses Kabel muss mit dem Ethernet-Ausgang des DSL-Modems verbunden sein. Die WAN-LED 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

13.2 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).

13.3 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.

14 Anhang

14.1 Leistungs- und Kenndaten

DE

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Anschlüsse	Ethernet LAN	4 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection		2 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection	
	WAN bzw. ADSL	'Annex A'-Geräte: ADSL over POTS nach ITU G.992.1 Annex A, ANSI T1.413, ITU G.992.2 (G.Lite), G.994.1 (G.hs), ADSL over POTS nach ITU G.992.5 Annex A, ADSL 2+; 'Annex B'-Geräte: ADSL over ISDN nach ITU G.992.1 Annex B, sowie ADSL over ISDN proprietär (Texas Instruments, ADI, Alcatel), ETSI TS 101 388, ADSL over ISDN nach ITU G.992.5 Annex B, ADSL 2+			
	ISDN	2 ISDN-Schnittstellen. Default: 1x NT (S ₀), 1x TE.	2 ISDN-Schnittstellen. Default: 1x NT (S ₀), 1x TE.	4 ISDN-Schnittstellen. Default: 2x NT (S ₀), 2x TE.	2 ISDN-Schnittstellen. Default: 1x NT (S ₀), 1x TE.
		ISDN-Schnittstellen sind schaltbar über Kreuzadapter zu NT oder TE. Buserminierung pro Schnittstelle schaltbar über DIP-Schalter.			
	Analog		2 Analog-Schnittstellen zum Anschluss von Endgeräten. 1 Analog-Schnittstelle zum Anschluss an Amtsanschluss.		2 Analog-Schnittstellen zum Anschluss von Endgeräten. 1 Analog-Schnittstelle zum Anschluss an Amtsanschluss.
	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 über externes Netzteil			

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
WLAN	Frequenzband				2400 - 2483,5 MHz (ISM) oder 5150 - 5750 MHz Nur GB: zusätzlich 5750 - 5850 MHz
	Antennen				2 dualband Dipol-Antennen
VoIP	Funktionen	SIP-Proxy und -Registrar, SIP-Gateway/- Remote-Gateway, Telefonanlagenfunktionen für Analog- (nur 1723/1823 VoIP), ISDN- und SIP-Teilnehmer			
	Sprachverarbeitung	<ul style="list-style-type: none"> ■ Echo-Unterdrückung (G.168) ■ automatischer adaptiver De-Jitter-Buffer ■ transparente Durchleitung ausgehandelter Codecs ■ Beeinflussung der Aushandlung von Codecs (Filter, Qualität/Bandbreite) ■ Sprachkodierung nach G.711 μ-Law/A-Law (64 kBit/s), G.722 High Quality Codec (für UDI-Rufe), G.729 Annex A Low Bandwidth Codec ■ Fax-over-IP (FoIP) mittels SIP- und T.38-Protokoll 			
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)			EU (CE-Zertifizierung: EN 55022, EN 55024, EN 60950), ETS 300 328, EN 55022, EN 301 489-1, EN 301 489-17, EN 60950
Umgebung / Temperatur		5 °C bis +35 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend)			

■ Kapitel 14: Anhang

		LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Optionen		<ul style="list-style-type: none"> ■ LANCOM VoIP-32 Option zur Aufrüstung auf insgesamt 32 lokale SIP-Benutzer (Art.-Nr. 61617) ■ VPN-Option (25 Kanäle, 50 konfigurierbar) inkl. Aktivierung des Hardware-Beschleunigers (Art.-Nr. 60083) ■ LANCOM Public Spot Option (Authentifizierungs- und Accounting-Software für Hotspots) (Art.-Nr. 60642) ■ LANCOM Next Business Day Service Extension CPE, Art.-Nr. 61411 ■ LANCOM 2-Year Warranty Extension CPE, Art.-Nr. 61414 			
Zubehör		<ul style="list-style-type: none"> ■ LANCOM Modem Adapter Kit zum Anschluß von Modems (analog oder GSM) an die serielle Konfigurationsschnittstelle (Art.-Nr. 61500) ■ LANCOM Rack Mount Option (Art.-Nr. 61501) ■ LANCOM LCOS Referenzhandbuch (DE) (Art.-Nr. 61700) 			

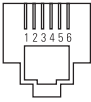
	LANCOM 1722 VoIP	LANCOM 1723 VoIP	LANCOM 1724 VoIP	LANCOM 1823 VoIP
Optionale Antennen und Zubehör	<p>Für alle LANCOM Router</p> <ul style="list-style-type: none"> ■ LANCOM Advanced VPN Client für Windows XP, Windows Vista, Windows 7, 1er Lizenz, Art.-Nr. 61600 ■ LANCOM Advanced VPN Client für Windows XP, Windows Vista, Windows 7, 10er Lizenz, Art.-Nr. 61601 ■ LANCOM Advanced VPN Client für Windows XP, Windows Vista, Windows 7, 25er Lizenz, Art.-Nr. 61602 ■ LANCOM Advanced VPN Client für Mac OS X (10.5 nur Intel, 10.6 oder höher), 1er Lizenz, Art.-Nr. 61606 ■ LANCOM Advanced VPN Client für Mac OS X (10.5 nur Intel, 10.6 oder höher), 10er Lizenz, Art.-Nr. 61607 ■ LANCOM ES-1108P Kompakter, robuster 8-Port-Ethernetswitch mit 4 PoE-Schnittstellen, Art.-Nr. 61450 ■ LANCOM Content Filter +10 Benutzer, 1 Jahr Laufzeit, Art.-Nr. 61590 ■ LANCOM Content Filter +25 Benutzer, 1 Jahr Laufzeit, Art.-Nr. 61591 ■ LANCOM Content Filter +10 Benutzer, 3 Jahre Laufzeit, Art.-Nr. 61593 ■ LANCOM Content Filter +25 Benutzer, 3 Jahre Laufzeit, Art.-Nr. 61594 <p>Nur für LANCOM 1722 VoIP, LANCOM 1723 VoIP und LANCOM 1724 VoIP:</p> <ul style="list-style-type: none"> ■ LANCOM Fax Gateway Option zur Aktivierung von "Hardfax" im Router, sodass 4-8 parallele Faxkanäle (je nach Modell) direkt über LANCAPI ("Fax Gruppe 3" ohne Verwendung von CAPI Faxmodem) genutzt werden können, Art.-Nr. 61425 <p>Nur für LANCOM 1823 VoIP:</p> <ul style="list-style-type: none"> ■ AirLancer Extender I-180 2,4 GHz Indoorantenne Art.-Nr. 60914 ■ AirLancer Extender I-60ag Dualband Indoorantenne Art.-Nr. 61214 ■ AirLancer Extender O-30 2,4 GHz Outdoorantenne Art.-Nr. 60478 ■ AirLancer Extender O-70 2,4 GHz Outdoorantenne Art.-Nr. 60469 ■ AirLancer Extender O-D80g 2,4GHz Polarisationsdiversity Outdoorantenne Art.-Nr. 61221 ■ AirLancer Extender O-360ag Dualband Rundstrahl-Outdoorantenne Art.-Nr. 61223 ■ AirLancer Cable NJ-NP 3m Antennenkabel-Verlängerung Art.-Nr. 61230 ■ AirLancer Cable NJ-NP 6m Antennenkabel-Verlängerung Art.-Nr. 61231 ■ AirLancer Cable NJ-NP 9m Antennenkabel-Verlängerung Art.-Nr. 61232 ■ AirLancer Extender SA-5 Blitzschutz für Antennenkabel Art.-Nr. 61212 ■ AirLancer Extender SA-LAN Blitzschutz für LAN-Kabel Art.-Nr. 61213 ■ AirLancer Extender O-18a 5 GHz Outdoorantenne Art.-Nr. 61210 ■ AirLancer Extender O-D60a 5GHz PolarisationsDiversity Outdoorantenne Art.-Nr. 61222 ■ AirLancer Extender O-9a 5GHz Richtfunk Outdoorantenne Art.-Nr. 6122 			

14.2 Anschlussbelegung

14.2.1 ADSL-Schnittstelle

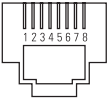
6-polige RJ11-Buchse

DE

Steckverbindung	Pin	IAE
	1	–
	2	–
	3	a
	4	b
	5	–
	6	–

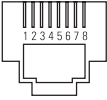
14.2.2 ISDN-Schnittstelle ☒

8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7, belegt als ISDN-TE zum direkten Anschluss an eine ISDN-(Amts)Leitung (NTBA)

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

14.2.3 ISDN-Schnittstelle

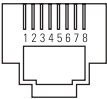
8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7, belegt als ISDN-NT zum direkten Anschluss von ISDN-Endgeräten

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

14.2.4 ISDN/Analog-Schnittstelle


8-polige RJ45-Buchse, parallel belegt:

- als ISDN-TE zum direkten Anschluss an eine ISDN-(Amts)Leitung (NTBA)
- zum Anschluss an einen analogen Amts-Anschluss

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

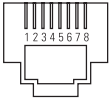
14.2.5 Analog-Schnittstelle

6-polige RJ11-Buchse

Steckverbindung	Pin	IAE
	1	–
	2	–
	3	a
	4	b
	5	–
	6	–


14.2.6 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	–

14.2.7 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

DE

14.3 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 befindet.

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

Index

Numerics

10/100Base-TX	43
3-DES	68, 77
802.11i	31, 114, 117, 119, 120
802.11i/	115
802.1x	31, 114, 115, 117

A

Access Control List	118
Access Point-Modus	3, 11, 35
ACL	117, 118
ADSL	
Anschluss	44
Übertragungsraten	12
ADSL over ISDN	134
ADSL over POTS	134
AES	68, 77, 114
Anlagen-Anschluss	26, 29
Annex A	13
Annex B	13
Anrufbeantworter	12
Anschlussbelegung	138
ADSL-Schnittstelle	138
Ethernet-Schnittstelle	140
Konfigurationsschnittstelle	141
LAN-Schnittstelle	140
Outband	141
WAN-Schnittstelle	140
Antennen-Kalkulator	87
Antennen-Leistungen	90
autark	3, 11, 35
Autosensing	46

B

Background-Scanning	103
Blowfish	68, 77

C

Calling Line Identity (CLI)	79
-----------------------------	----

CAPI-Schnittstelle	105
Client-Modus	100
Common ISDN Application Programming Interface (CAPI)	105

D

Datenfrequenzen	12
DDI	26
Default-Gateway	122
Denial-of-Service-Protection	16
DFS	88
DFÜ-Adapter	80
DHCP	62
DHCP-Server	27, 53, 62
Direct Dialing In	26
DNS	
DNS-Server	27, 62
Zugriffe ins entfernte LAN	72
Dokumentation	34
Domäne	72
Download	6
Downstream	12
DSL-Übertragung zu langsam	132
DSL-Verbindung	
Probleme beim Aufbau	132
Dynamic Frequency Selection	88
dynamische Frequenzwahl	88

E

EAP	31, 114, 117
Einwahl-Zugang	77

F

Fax	12
Fernkonfiguration	57
Fernkonfiguration über ISDN	33
Firewall	15, 32, 122
Stationen sperren	123
FirmSafe	33

Firmware	6	ISDN-Festverbindungsoption	28
Flatrate	64	ISDN-Life-Line	126
Fresnel-Zone	89	ISDN-Modem	77
G		ISDN-Rufnummer	71
Gebührenschatz	56, 57	ISDN-S ₀ -Anschluss	30
Gebührenschatz zurücksetzen	38	ISDN-Spannungsweiterleitung	126
Gebührensperre	38	K	
H		Kennwort	54, 57, 68, 77
Hard-Roaming	103	Kennwort für die ISDN-Verbindung	71
Hardware-Installation	45	Konfigurationsdatei	123
Hinweis-Symbole	6	Konfigurationskennwort	121
HTTPS	58	Konfigurations-Schnittstelle	33
I		Anschlusskabel	34
ICMP	123	Konfigurationsschnittstelle	43
Installation	34	Konfigurationsschutz	32, 54
ADSL	46	Konfigurationszugriff	57
Antennen	45	Konformitätserklärungen	141
ISDN	46	L	
Konfigurations-Schnittstelle	47	LAN	
LAN	46	Anschlusskabel	34
Netzteil	48	LANCAPI	28
Internet-Anbieter	63	LANCOM Enhanced Passphrase Security	114
Internet-Zugang	27, 63	LANCOM Public Spot Option	112
Authentifizierungsdaten	63	LANconfig	51, 56
Flatrate	64	Assistenten aufrufen	66
Intrusion Detection	15	LAN-LAN-Kopplung	27, 68
IP		erforderliche Angaben	69
Filter	122	LANmonitor	51
Ports sperren	123	LEPS	32, 117
IP-Adresse	46, 53, 54, 123	Lieferumfang	34
IP-Masquerading	15, 32, 122	Life-Line	25, 126
IP-Router	27	Life-Line-Support	31, 126
IPSec	68, 77	Loadbalancing	26
IPSec-over-WLAN	114	Loader	35
ISDN		local break out	20
Anschlusskabel	34	M	
D-Kanal	79	MAC-Adresse	116
ISDN-Anruferkennung	71, 78, 79		

■ Index

MAC-Adressfilter	15, 32	R	
Managed-Modus	3, 11, 35	RADIUS	117
Mehrgeräte-Anschluss	26, 29	RAS	14
Mindestbandbreite	16	Remote-Access-Service (RAS)	
MSN	26, 79	Benutzername	78
Multi SSID	31	einrichten	77
Multiple Subscriber Number	26	Einwahl-Rechner konfigurieren	80
N		NetBIOS	80
NAT – siehe IP-Masquerading		Server	27
Nebenstellenanlage	12	Software-Komprimierung aktivieren	80
NetBIOS	73	TCP/IP	79
NetBIOS-Proxy	27	Windows-Arbeitsgruppe suchen	80
Netzmaske	53, 54, 123	Roaming	103
Netzschalter	43	Routerfunktion	11
Netzteil	34, 43	Routing-Tabelle	122
Netzwerkkopplung	68	Rückruffunktion	33, 68, 77
Sicherheitsaspekte	68, 77	S	
Netzwerksegment	46	SDSL-Modem	32
O		Sicherheit	
Optionale Antennen	110	Schutz der Konfiguration	114
Optionen und Zubehör	110	Sicherheits-Checkliste	120
P		Sicherheits-Einstellungen	132
P2P	117	SIP-Gateway	20
PAT – siehe IP-Masquerading		SIP-Provider	18
Ping	74	SIP-Softphone	18
Point-to-Multipoint	26	SIP-TK-Anlage	21
Point-to-Point	26, 117	SNMP	
POTS	12	Konfiguration schützen	122
PPP	77	Soft-Roaming	103
PPP-Client	80	Software-Installation	49
Punkt-zu-Mehrpunkt	125	Spannungsweiterleitung	25, 30, 126
Punkt-zu-Mehrpunkt-Anschluss	29	Sprachfrequenzen	12
Punkt-zu-Punkt	86, 125	Sprachkommunikation	16
Punkt-zu-Punkt-Anschluss	29	SSID	55, 101
Q		Standard-Gateway	61
Quality-of-Service	16	Stateful-Inspection-Firewall	15
		Statusanzeigen	35
		Power	37, 38
		Wireless Link	42

Super AG	31	Verschlüsselungsmethode	102
Support	6	Virtual Private Network	13
Switch	43	Virtual Private Network (VPN)	27
Systemvoraussetzungen	35	Voice-over-IP	16
T		VoIP	16
TCP	123	Anbindung von Filialen oder Heimar-	
TCP/IP	35, 80	beitsplätzen	19
Einstellungen	52	Peer-to-Peer	21
Verbindung testen	74	VoIP-Benutzer	23
TCP/IP-Filter	15, 32, 122	VoIP-Leitungen	24
TCP/IP-Konfiguration		VoIP-TK-Anlage	19
manuell	52, 53	VPN	13
vollautomatisch	52, 53	VPN-Client	80
TCP/IP-Router		VRRP	26
Einstellungen	71	W	
TCP/IP-Windows-Size	133	WEBconfig	57
T-DSL	13	HTTPS	58
Telefon	12	Systemvoraussetzungen	35
Telnet	123	WEP	31, 114, 119, 120
TFTP	123	Windows-Arbeitsgruppen suchen	73
Turbo Modus	31	WLAN	
U		Client-Modus	100
Übertragungsprotokoll	132	Durchsuchte Bänder	101
UDP	123	WPA	31, 114, 117, 119, 120
Upstream	12	Z	
V		Zugang zum Internet einrichten	63
Verschlüsselung	68, 77		