



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

Kurzvorstellung LANCOM Software Version 7.6

März 2009

© 2009, LANCOM Systems GmbH

www.lancom.de

LC.OS 7.6
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Highlights (1/2)



Das LANCOM Betriebssystem LCOS und die entsprechenden Management-Tools (LCMS) stellen regelmäßig **kostenfrei** neue Funktionen für alle aktuellen LANCOM Router, Access Points und Gateways bereit.

Hier die wichtigsten neuen Funktionen und Verbesserungen:

- **Firewall** – Firewall-Redesign mit neuer grafischer Oberfläche zur objektorientierten Konfiguration in LANconfig, Trigger für Backup, neue QoS-Einstellungen (Session-Limits, relative Bandbreiten-Angaben)
- **WEBconfig** – Völlig neu überarbeitetes Web-Interface zur Konfiguration von LANCOM Routern und Access-Points in Anlehnung an LANconfig
- **COM-Port-Server und -Forwarding** – Seriell angeschlossene Geräte können über beliebige IP-Verbindungen hinweg ferngesteuert werden (RFC2217)



Highlights (2/2)



- **LANconfig** – Austausch von Konfigurations-Dateien zwischen ähnlichen Geräten, z.B. zur Migration von Konfigurationen auf zu ersetzende Geräten
- **LL2M – LANCOM Layer 2 Management:** Rescue-Mechanismus zum sicheren Ausführen von Befehlen mit verschlüsselten Layer-2-Paketen
- **iPhone-VPN-Access** – XAUTH Client und Server, der z.B. den VPN-Zugriff via UMTS vom iPhone ab Software Version 2.0 auf das lokale Netz ermöglicht



Weitere Verbesserungen

- **LANmonitor** – Export von Support-Dateien mit Sysinfo, Bootlog & Konfiguration
- **HTTPS-Client** – Zum Download von Firmware- und Konfigurations-Dateien
- **IPSec VPN Backup** – Backup von VPN-Verbindungen über verschiedene Hierarchie-Stufen hinweg, z.B. bei Wegfall eines zentralen VPN-Konzentrators
- **Zertifikate** – Neue OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen
- **WLAN Controller** – Zusammengefasste Monitoring-Sicht auf WLAN-Controller-Cluster, interner Speicher für bis zu drei Skript-Dateien (max. 64K)
- **Public Spot** – Unterstützung von öffentlichen Zertifikaten und Zertifikats-Ketten
- **SIP-Proxy** – Konfigurierbare Registrierung, Überwachung und Privacy-Methode ("CLIR" in SIP) pro Leitung, "CLIR" für SIP-Benutzer
- **Routing** – Lernen von Routing-Tags für ARF aus der Routing-Tabelle und Unterstützung von RIP-Quellen mit Platzhaltern (Wildcards) im Namen
- **PPP** – Freie Einstellung der Protokolle zur Authentifizierung

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Firewall – Neue Benutzeroberfläche

LCS-DEMO-D2008-12-18.lcf - Firewall-Regeln (Filter/QoS)

Prio	Name	Quelle	Quell-Dienst	Ziel	Ziel-Dienst	Aktionen/QoS	Kommentar
1	ALLOW_VPN_CLIENT	LOCALNET	Alle	LCS_ETH_OUT, LCS_ETH_OUT_2	IPSEC	übertragen	
1	ALLOW_BASIC_INTERNET	LOCALNET	Alle	Beliebig	FTP, TELNET, MAIL, WEB, NTP...	übertragen	
0	ALLOW_VPN_LCS_NETBIOS	ARF_LAN1_LCS_VPN	NETBIOS	LANCOM_VPN	Alle	übertragen	
0	ALLOW_VPN_LCS	ARF_LAN1_LCS_VPN	Alle	LANCOM_VPN	RDP, TFTP, IPSEC, SYSLOG, S...	übertragen	
0	ALLOW_PING	LOCALNET	Alle	Beliebig	ICMP	übertragen	
0	BLACKLIST_OF_SPAMBOTS	64.62.243.30	Alle	Beliebig	Alle	Zurückweisen	
0	PRIVATE_LAN_ACCESS_FROM_BUSINESS	ARF_LAN1_LCS_VPN	Alle	ARF_LAN2_PRIVAT	Alle	übertragen	
0	LAN_ACCESS_FROM_PRIVATE_CONTEXT	ARF_LAN2_PRIVAT	Alle	ARF_LAN1_LCS_VPN	Alle	übertragen	
0	DENY_ALL	Beliebig	Alle	Beliebig	Alle	übertragen	

LCS-DEMO-D2008-12-18.lcf - Firewall-Stations-Objekte

Name	Stationen
LOCALNET	Alle Stationen in allen lokalen Netzen
LCS_ETH_OUT_2	213.217.69.75 - 213.217.69.78
LCS_INTRANET	10.0.0.0 / 255.0.0.0
LCS_ETH_OUT	217.6.21.90
ARF_LAN2_PRIVAT	192.168.200.0 / 255.255.248.0
ARF_LAN1_LCS_VPN	192.168.100.0 / 255.255.252.0
LANCOM_VPN	LCS
VPN_CSCHALLE	10.98.100.9

Hinzufügen ... Bearbeiten ... Kopieren ... Entfernen

- **Symbole** für Objekte in Abhängigkeit von Typ (Aktion, QoS, Station, Dienst) und Art (z.B. einzelne Station, Subnetz, Sammlung von MAC-Adressen...)
- **Zeilendarstellung** mit Gitternetzlinien, alternierendem Hintergrund oder der Kombination aus beidem
- **Tipp:** Vorlagen für objekt-orientierte Firewall-Regeln stehen in der Support KnowledgeBase der LANCOM Webseite zum Download bereit

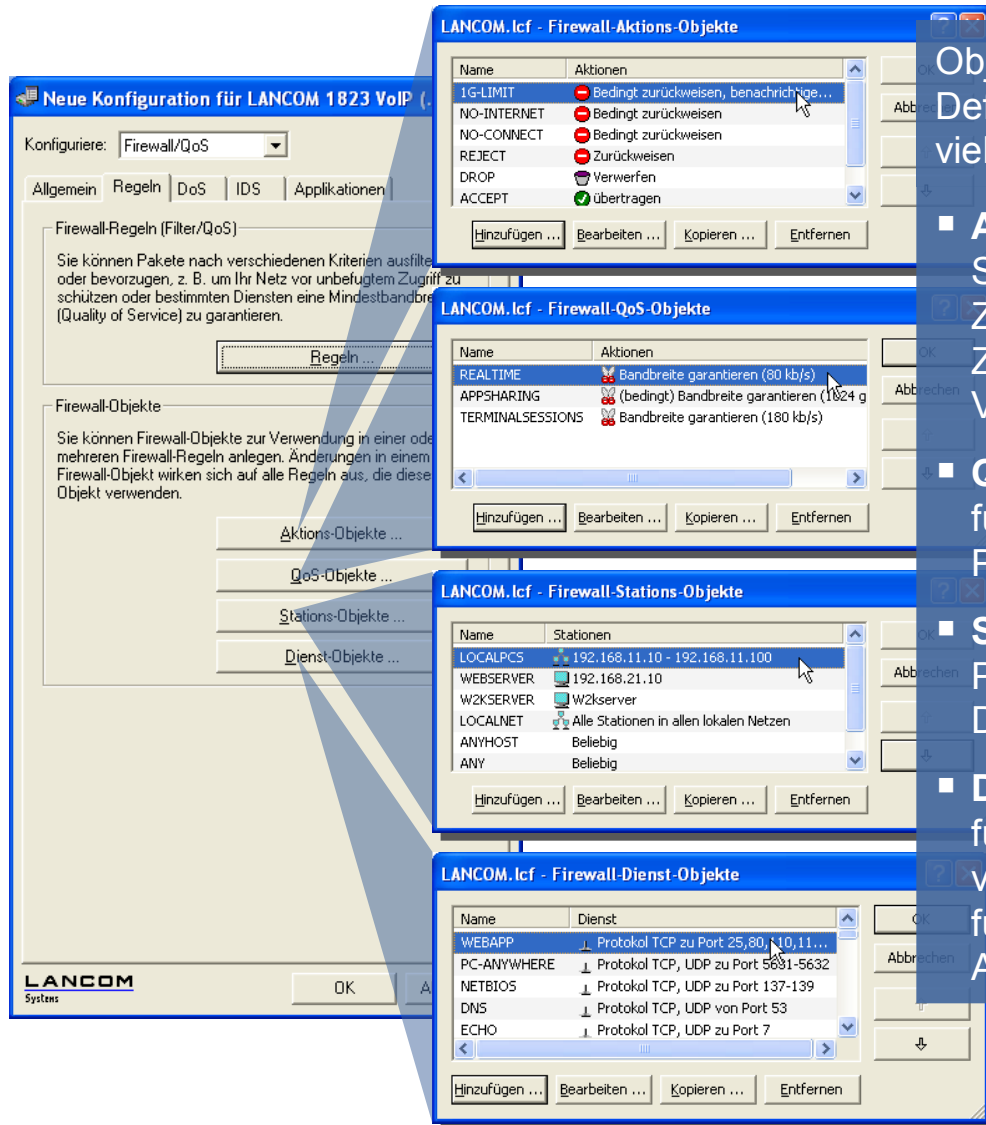
LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 5

LANCOM
Systems

Firewall – Objektorientierte Konfiguration



Objekte vereinfachen die Definition von Regeln zur vielfachen Anwendung:

- **Aktions-Objekte** für ganze Sätze von Limits, Zurückweisungen und Zulassungen von Verbindungen
- **QoS-Objekte** fassen Regeln für Bandbreiten und Priorisierung zusammen
- **Stations-Objekte** als Platzhalter für Quell-/Ziel-Definitionen
- **Dienst-Objekte** mit Regeln für Protokolle und Ports, inkl. vordefinierter Dienst-Objekte für viele typische Netzwerk-Anwendungen

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 6

LANCOM
Systems

Firewall – Neue Funktionen für Backup & QoS

- Firewallregeln in Abhängigkeit vom **Backup-Status** (neue Bedingung)
 - ➔ Somit ist ein anderes Regelwerk möglich, wenn die Backup-Leitung genutzt wird, z.B. um die Bandbreite gering zu halten
- Zuweisen relativer **Bandbreiten in Prozent**
 - ➔ Hilfreich, wenn die tatsächliche Bandbreite einer Leitung zum Konfigurations-Zeitpunkt nicht bekannt ist
- **Begrenzung der Bandbreite** für Verbindungen **pro Station**
 - ➔ Z.B. zum „Ausbremsen“ von File-Sharing oder Begrenzen von Server-Diensten

The screenshot displays the 'Trigger/Aktionen-Set' configuration window in LCOS 7.6. It contains four trigger rule sections, each with a 'Bedingung' (Condition) and 'Aktion' (Action) area. Blue arrows point from the text on the left to specific settings in these sections.

- Section 1:** 'Bedingung' includes 'für Backup-Verbindungen' (checked). 'Aktion' includes '% Bandbreite' (selected) and 'absolut' (selected).
- Section 2:** 'Bedingung' includes 'bei DiffServ-CP: BE' (selected). 'Aktion' includes 'Pro Station' (selected) and 'absolut' (selected).
- Section 3:** 'Bedingung' includes 'für gesendete Pakete' (checked). 'Aktion' includes 'Sessions' (selected) and 'absolut' (selected).

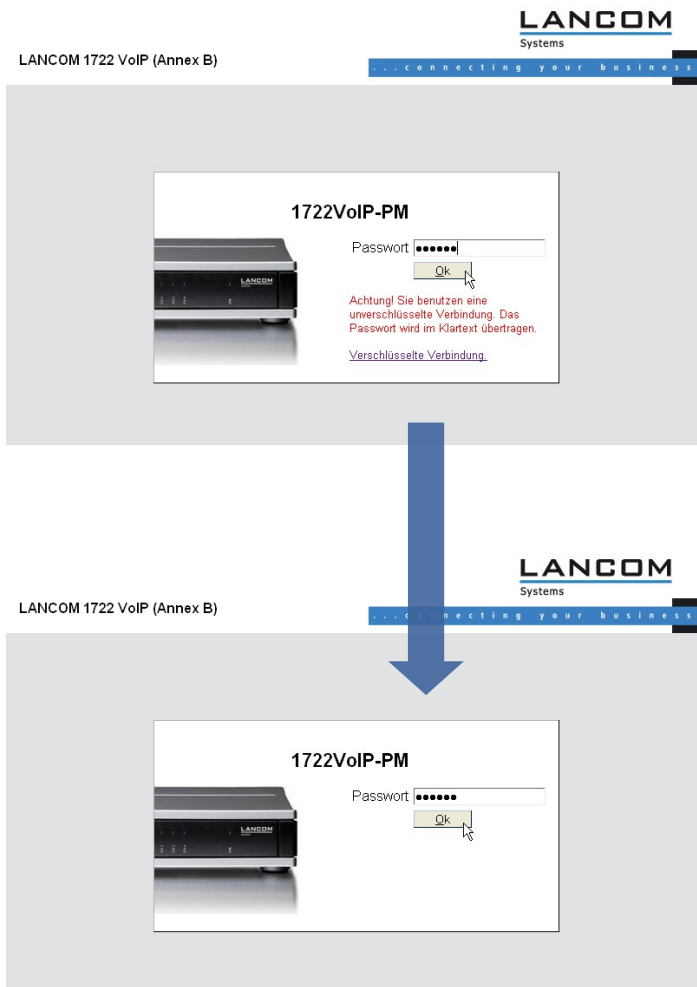
LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 7

LANCOM
Systems

WEBconfig – Login-Seite mit Sicherheitshinweis



- **Login-Seite** in neuem Design mit Geräteabbildung und –Name in abgesetztem Login-Bereich zur leichteren Orientierung
- **Gerätetyp** im Seitenkopf
- **Sicherheitshinweis** bei ungesichertem Zugriff mit Link zur verschlüsselten Seite

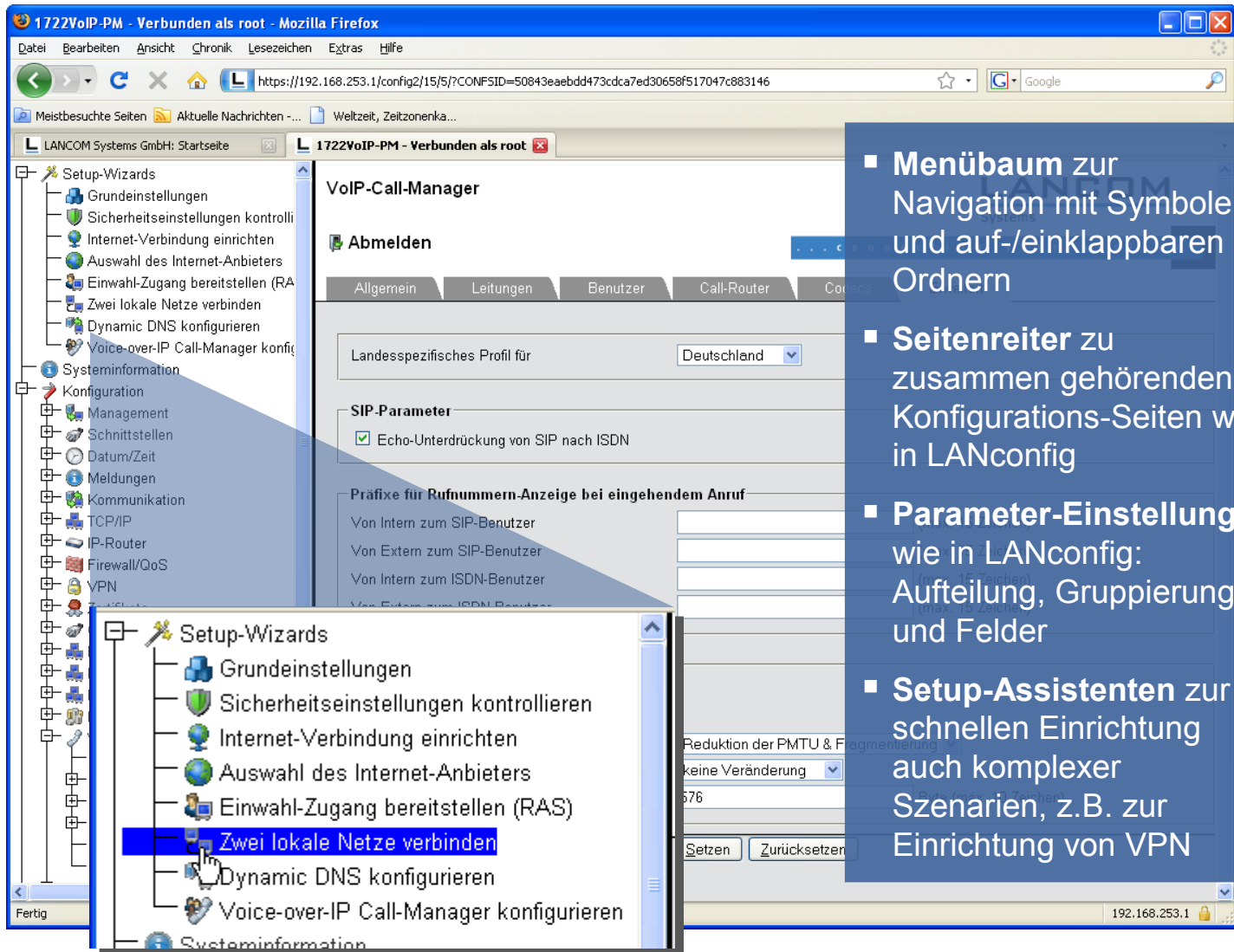
LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 8

LANCOM
Systems

WEBconfig – Neue Benutzeroberfläche



- **Menübaum** zur Navigation mit Symbolen und auf-/einklappbaren Ordnern
- **Seitenreiter** zu zusammen gehörenden Konfigurations-Seiten wie in LANconfig
- **Parameter-Einstellung** wie in LANconfig: Aufteilung, Gruppierung und Felder
- **Setup-Assistenten** zur schnellen Einrichtung auch komplexer Szenarien, z.B. zur Einrichtung von VPN

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 9

LANCOM
Systems

WEBconfig – Neuer Bereich „Systeminformation“

Systeminformation

Abmelden

Systemdaten Gerätestatus Syslog

Schnittstelle/Port	Status/Modus
CPU-Last	Aktuell: 0.65%
Speicher	Gesamt: 26.8 MBytes Frei: 14.5 MBytes
ETH-1	

LANCOM Systems

...connecting your business

Systemdaten Gerätestatus Syslog

Idx.	Zeit	Quelle	Level	Meldung
1	05.11.2008 09:04:23	LOCAL2	Hinweis	Interface INTRANET added, with IP address 192.168.253.1 and netmask 255.255.255.0
2	05.11.2008 09:04:23	LOCAL2	Hinweis	Interface DMZ added, with IP address 0.0.0.0 and netmask 255.255.255.0
3	05.11.2008 09:04:23	LOCAL2	Hinweis	IP router enabled
4	05.11.2008 09:04:23	LOCAL2	Hinweis	IP router enabled
5	05.11.2008 09:08:27	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.253.180
6	05.11.2008 09:09:30	AUTHPRIV	Hinweis	Webconfig: user logout from 192.168.253.180
7	05.11.2008 09:34:25	LOCAL1	Hinweis	Accounting list start
8	05.11.2008 09:34:25	LOCAL1	Hinweis	User: rurlaga-nb Rx(kB): 1473 Tx(kB): 284
9	05.11.2008 09:34:25	LOCAL1	Hinweis	User: vp-100-00a05712783d Rx(kB): 9 Tx(kB): 7
10	05.11.2008 09:34:25	LOCAL1	Hinweis	Accounting list end
11	05.11.2008 10:04:25	LOCAL1	Hinweis	Accounting list start
12	05.11.2008 10:04:25	LOCAL1	Hinweis	User: rurlaga-nb Rx(kB): 49 Tx(kB): 111
13	05.11.2008 10:04:25	LOCAL1	Hinweis	User: vp-100-00a05712783d Rx(kB): 9 Tx(kB): 7
14	05.11.2008 10:04:25	LOCAL1	Hinweis	Accounting list end

■ **Neu: Gerätestatus** mit Darstellung der Interfaces sorgt für schnellen Überblick

■ **Neu: Syslog** zur Anzeige der letzten im Hauptspeicher des Geräts abgelegten Ereignisse

■ **Neu: Ab LCOS 7.6** hat jedes unkonfigurierte LANCOM Gerät zur Diagnose werkseitige Vor-einstellungen für Syslog

■ **Tipp:** Bestehende Geräte können per Script dieselben Einstellungen für Syslog erhalten (Download in der KnowledgeBase)

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 10

LANCOM
Systems

WEBconfig – Online-Hilfe im LCOS-Menübaum

The screenshot shows the LANCOM Webconfig interface in a Mozilla Firefox browser window. The browser title is "1722VoIP-PM - Verbunden als root". The address bar shows the URL "https://192.168.253.1/config/2/19?CONFSID=0564d48660d179beb11f04590d85d15715ce4". The browser tabs show "LANCOM Systems GmbH: Startseite" and "1722VoIP-PM - Verbunden als root".

The main content area displays the "LCOS-Menübaum" (LCOS Menu Tree) on the left and a list of configuration options on the right. The "Online-Hilfe" (Online Help) option is highlighted in the menu tree. The "Online-Hilfe" window is open, showing the "VPN: NAT-T-Aktiv" (VPN: NAT-T-Active) configuration page. The page contains the following text:

VPN: NAT-T-Aktiv

Aktiviert die Verwendung von NAT-T, um die Probleme beim VPN-Verbinden zu überwinden, die durch die Verwendung von NAT-T verursacht werden.

Erlaubte Werte:

- ☐ Ein
- ☐ Aus

Default: Aus

Bitte beachten: NAT-T kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert.

Wichtiger Hinweis: Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das LANCOM als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

LCOS 7.6
[LANCOM OPERATING SYSTEM]

■ **Online-Hilfe** für die Einträge im LCOS-Menübaum über das Fragezeichen-Symbol, wenn eine Verbindung zum Internet besteht

■ **Tipp:** Der **Quellpfad** für die Hilfe kann unter „Setup/HTTP/Dokumentwurzel“ auch auf einen lokalen HTTP-Server eingestellt werden

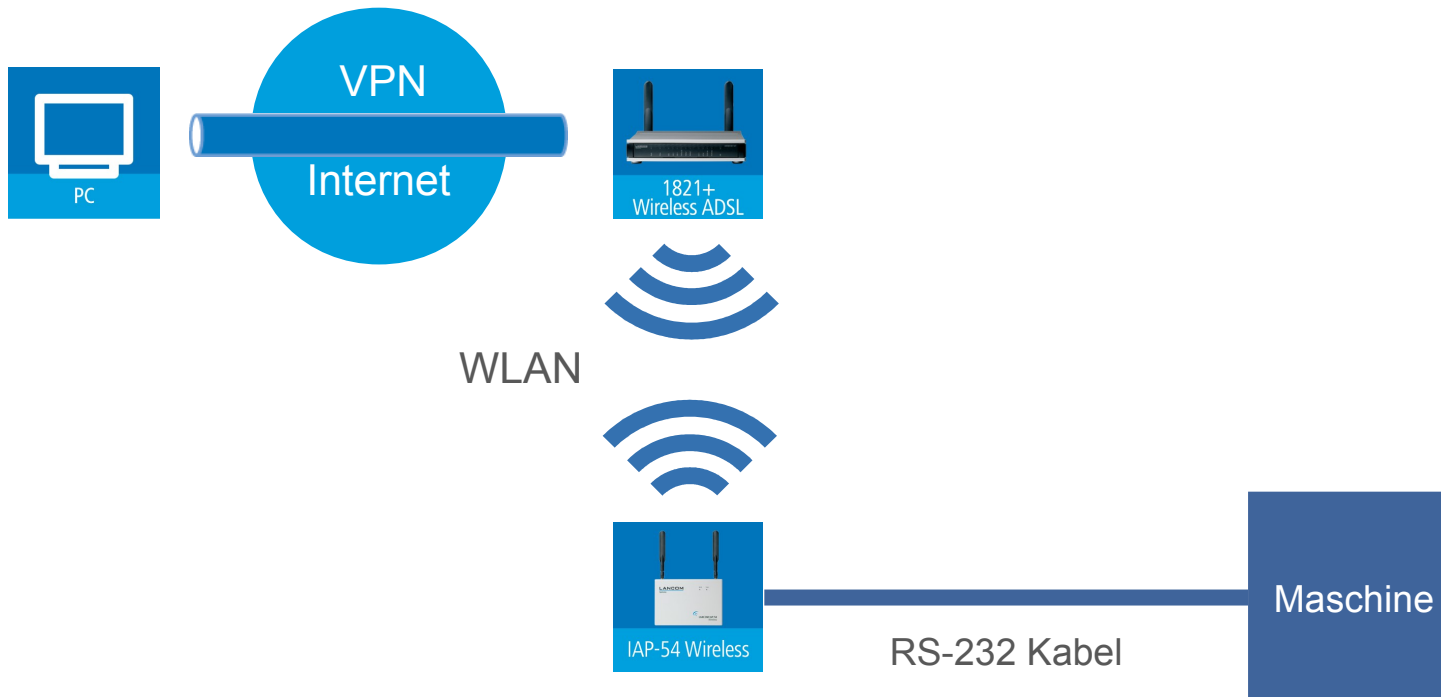
Feature Notes LCOS 7.6

Seite 11

LANCOM
Systems

COM-Port-Forwarding

- **Serielle Kommunikation** über eine IP-Strecke, z.B. **per WLAN oder VPN**
- Angeschlossen an den COM-Port (oder USB-Port) eines LANCOM wird der serielle **Anschluss virtuell** bis zu einem Ziel-PC **verlängert**
- Ein virtueller **COM-Port-Treiber** (für Windows frei verfügbar) emuliert den seriellen Anschluss auf dem PC
- Konform zu **RFC2217** (Telnet Com Port Control Option)
- Einsatzgebiete: Gebäudeautomation, Maschinensteuerung, **Fernwartung alter TK-Anlagen mit seriellem Port**



LCOS 7.6
[LANCOM OPERATING SYSTEM]

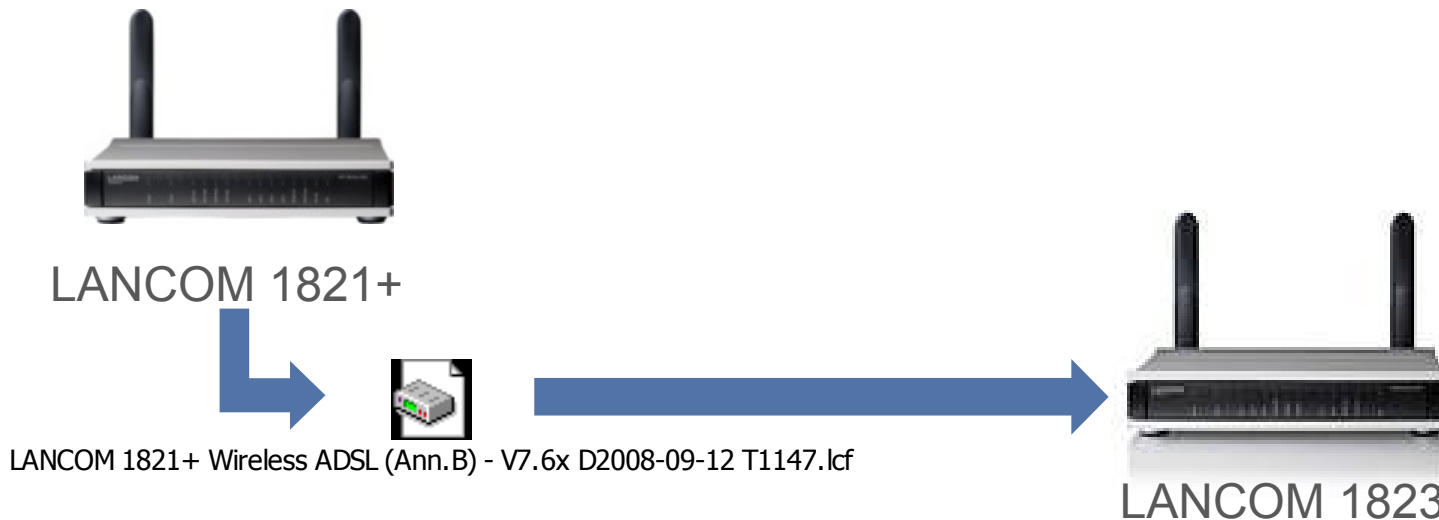
Feature Notes LCOS 7.6

Seite 12

LANCOM
Systems

LANconfig – Austausch von Konfigurationen

- Austausch der Konfiguration **über Gerätetypen und Software-Versionen hinweg**, z.B. LANCOM 1821+ Wireless ADSL mit LANCOM 1823 VoIP
- Zum Austausch genügt die **normale Konfigurations-Datei** („.lcf“), z.B. eine Sicherungskopie
- Damit **können bestehende Konfigurationen**, z.B. im Fall von Ersatzbeschaffungen für nicht mehr erhältliche LANCOM Geräte, leicht auf neue Geräte **migriert werden**
- Bei standort-übergreifend einheitlicher Konfiguration, aber verschiedenen Gerätetypen, z.B. aufgrund der Schnittstellen, **kann eine Master-Konfiguration** auf die verschiedenen Systeme **verteilt werden**



LCOS 7.6
[LANCOM OPERATING SYSTEM]

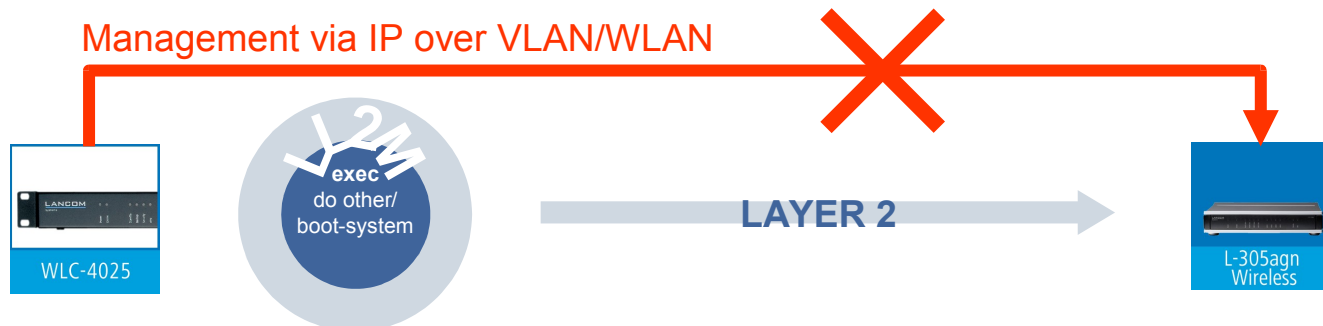
Feature Notes LCOS 7.6

Seite 13

LANCOM
Systems

LL2M – LANCOM Layer-2 Management

- **LANCOM-Layer-2-Management-Protokoll:** verschlüsseltes Layer-2-Paket, das als Payload ausführbare Scriptbefehle an ein LANCOM Gerät übermitteln kann
- Mit LL2M sind **Rescue & Recovery** fehlkonfigurierter Geräte, z.B. bei VLAN-Fehlern, möglich, wenn durch den Fehler kein administrativer Zugriff mehr besteht
- **Geräte** lassen sich per ll2mdetect im lokalen Segment (LAN, WLAN) mittels Multicast oder Broadcast **auffinden**
- ll2mexec ermöglicht **das gezielte Ausführen von Kommandos** auf spezifizierten Geräten
- Die **Sicherheit** entspricht TLS-PSK mit Geräte-Passwörtern, sodass keine Man-in-the-Middle-Attacke möglich ist; um einen Brute-Force-Angriff (mittels Wörterbuch) auf die Passwörter zu unterbinden, werden sichere Geräte-Passwörter empfohlen
- Zusätzlich greift auch der **IPS-Mechanismus** mit vorübergehender Sperre bei falscher Verschlüsselung aufgrund eines falschen Passworts, sodass DoS-Attacken scheitern



LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 14

LANCOM
Systems

iPhone VPN-Unterstützung

Extended IKE Authentication (XAUTH)

- XAUTH ist ein erweitertes Authentifizierungsprotokoll („Extended Authentication“), das bei IPSec-Verbindungen für eine zusätzliche Username/Passwort-Prüfung genutzt werden kann

Was ist neu im LANCOM?

- XAUTH-Client und -Server im LANCOM
- Pro VPN-Verbindung kann nun zusätzlich XAUTH verwendet werden.

Wie sicher ist XAUTH?

- Nicht unterstützt werden im LANCOM mehrere VPN-Verbindungen mit gleichen Schlüsseln (PSK bzw. Zertifikat), die sich nur im XAUTH Usernamen/Passwort unterscheiden (bekanntes Sicherheitsproblem bei XAUTH)
- Pro XAUTH-Verbindung ist ein entsprechender VPN-Eintrag notwendig

Welche neuen VPN-Interoperabilitäten ergeben sich?

- VPN-Anbindung mit Apple iPhone
- LANCOM als XAUTH-Client gegen Fremd-Router
- LANCOM als XAUTH-Server gegen Fremd-Clients (z.B. Cisco Anyconnect)

LCOS 7.6
[LANCOM OPERATING SYSTEM]



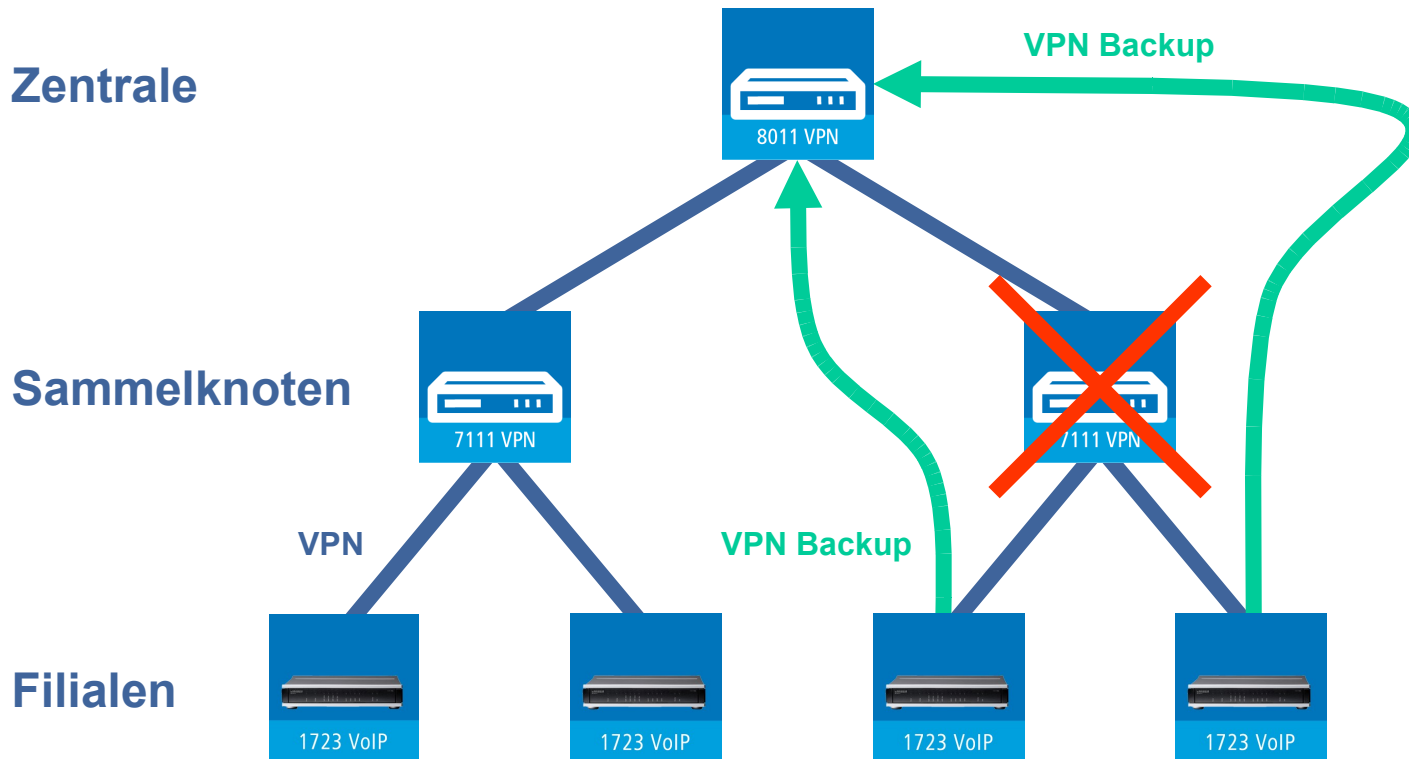
Feature Notes LCOS 7.6

Seite 15

LANCOM
Systems

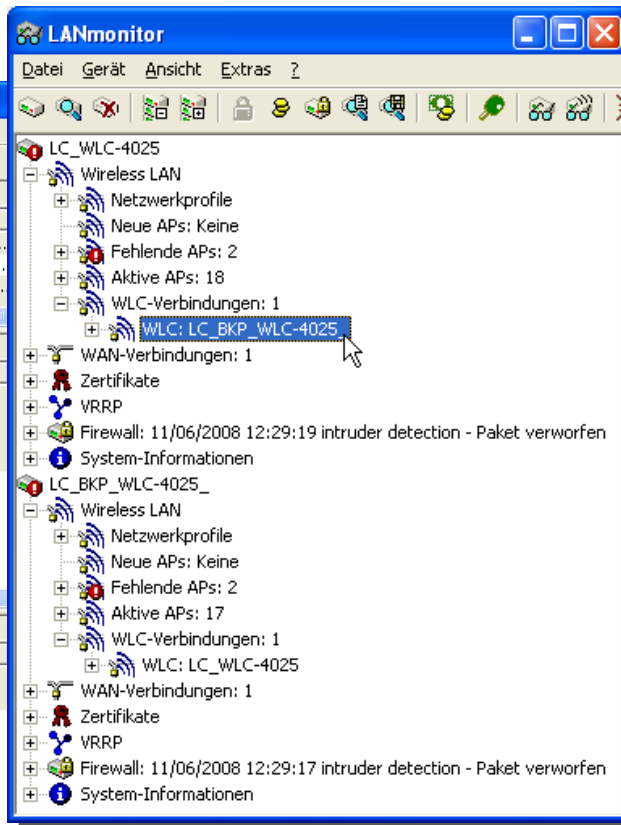
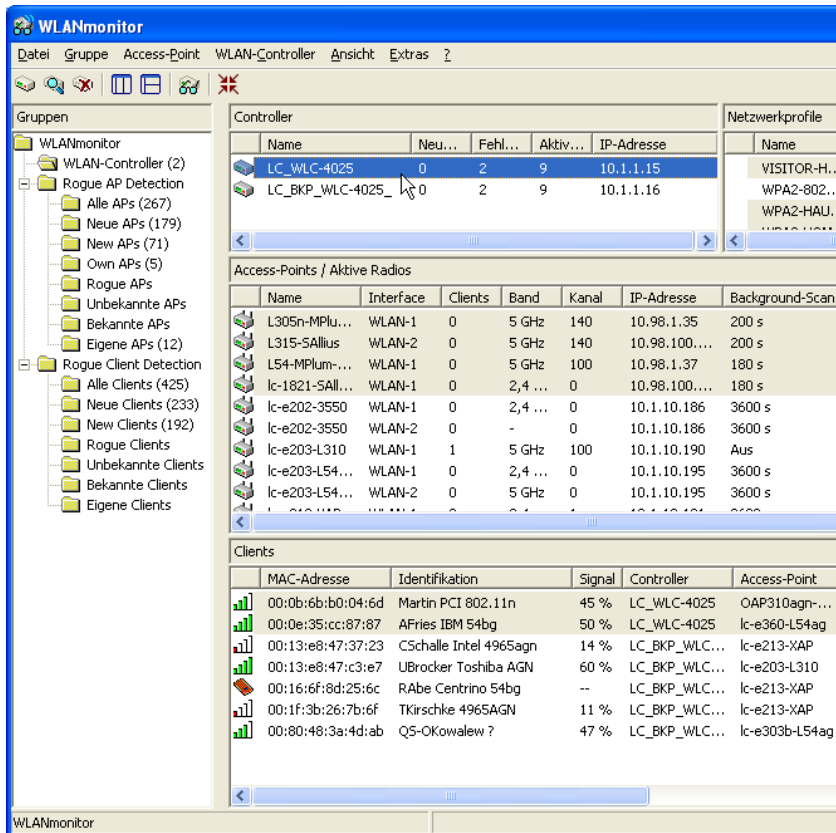
VPN-Backup über mehrere Hierarchie-Stufen

- Im Fall eines **Backups** soll die Verbindung statt zwischen Filiale und Sammelknoten direkt mit der Zentrale aufgebaut werden
- **Die SAs werden** beim Neuaufbau entsprechend **aktualisiert**
- **Rückkehr zur Hauptverbindung**, wenn diese wieder verfügbar ist



WLAN-Controller – Cluster-Monitoring

- Das **Status des Controller-Clusters** wird im LANmonitor dargestellt
- Die **gesammelten Status-Informationen** des Clusters stehen in einem WLANmonitor Fenster zur Verfügung
- Die **Daten aller** zum Cluster gehörenden **Geräte** werden in LANmonitor automatisch zusammengefasst und **konsolidiert** dargestellt



LCOS 7.6
[LANCOM OPERATING SYSTEM]

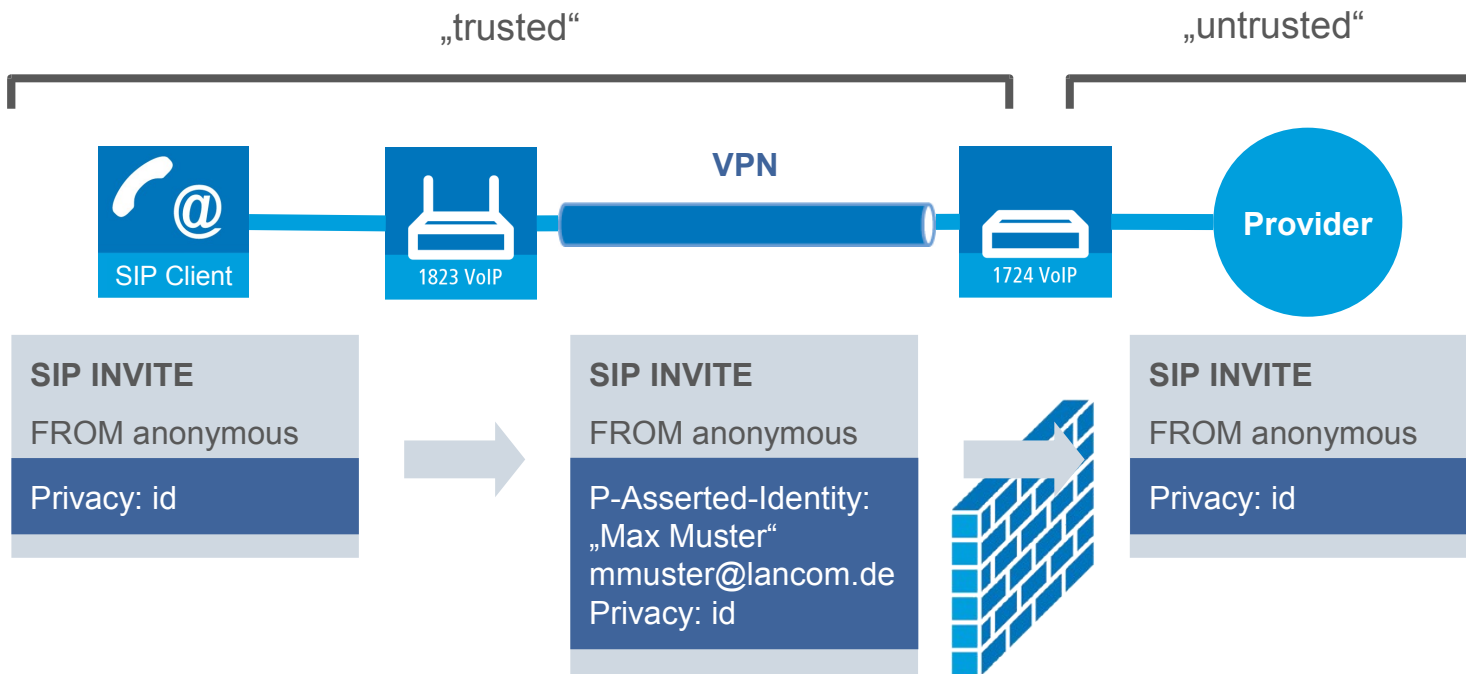
Feature Notes LCOS 7.6

Seite 17

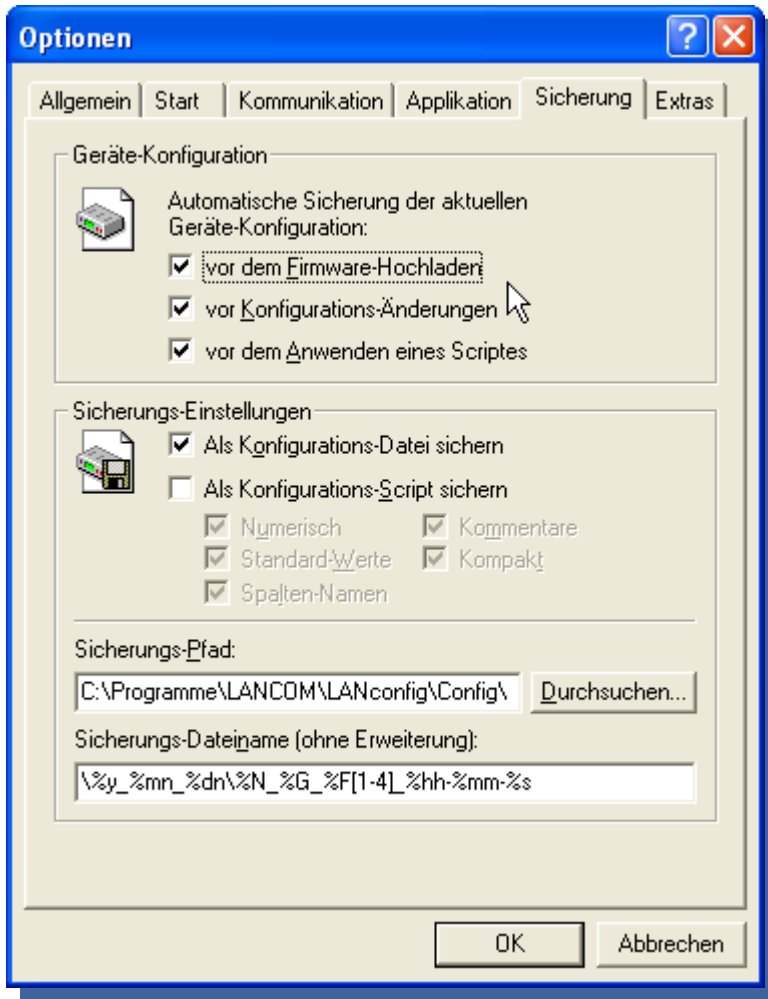
LANCOM
Systems

SIP-Proxy – “CLIR” in SIP

- SIP privacy/screening zur **Rufnummern-Unterdrückung/Anzeige** (“CLIR”)
- **Ausfiltern** beim Übergang in nicht-vertraute Netze (“untrusted”)
- Unterstützung verschiedener Verfahren (**RFC3325, IETF-Draft-SIP-Privacy-04**)
- **CLIR** setzen an analogen, ISDN- oder SIP-Teilnehmern



LANconfig – Automatische Sicherung



- **Automatische Sicherung** der Geräte-Konfiguration bei Hochladen einer Firmware, Änderung der Konfiguration oder Anwenden eines Scripts (alle per Default aktiv)
- Sicherung als **Konfigurations-Datei oder Script**
- **Generische Dateinamen** (konfigurierbar) mit Platzhaltern (z.B. für Datum, Zeit, Gerätename, Typ und Firmware) und einheitlichem Sicherungs-Pfad

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 19

LANCOM
Systems

LANconfig – Mehrfach-Sicherung

- **Sichern mehrerer Konfigurations-Dateien** verschiedener Geräte in einem Schritt
- Ideal zur **Sicherung von Projekt-Installationen**, die verschiedene Geräte umfassen
- **Generische Dateinamen** (konfigurierbar) und einheitlicher Sicherungs-Pfad

LCOS 7.6
[LANCOM OPERATING SYSTEM]

The screenshot shows the LANconfig interface with a list of devices. A context menu is open for the selected device, showing options like 'Konfigurieren', 'Setup Assistent', 'Prüfen', and 'Konfigurations-Verwaltung'. The 'Konfigurations-Verwaltung' option is selected, and a sub-menu is open showing 'Als Datei sichern...' (Strg+S) and 'Als Skript-Datei sichern...'. A dialog box titled 'Merkmal Geräte-Konfigurations-Sicherung' is also visible, showing the backup path and filename format.

Name	Adresse	Gerätestatus	Verlauf	Gerätetyp
ADLERSHOF	10.1.204.99	Ok		LANCOM DSL/
ANGERMUENDE	10.1.204.101	Ok		LANCOM DSL/
CHEMNITZ	10.1.204.102	Ok		LANCOM DSL/
COBURG	10.1.204.97	Ok		LANCOM DSL/
DRESDEN				LANCOM DSL/
ERFURT				LANCOM DSL/
GERA				LANCOM DSL/
GOETTINGEN				LANCOM DSL/
HALLE				LANCOM DSL/
KOETHEN				LANCOM DSL/
LANCOM ES-2126				LANCOM ES-2
LANCOM ES-2126				LANCOM ES-2

Merkmal Geräte-Konfigurations-Sicherung

Sicherungs-Einstellung

Sicherungs-Pfad:

Sicherungs-Dateiname (ohne Erweiterung):

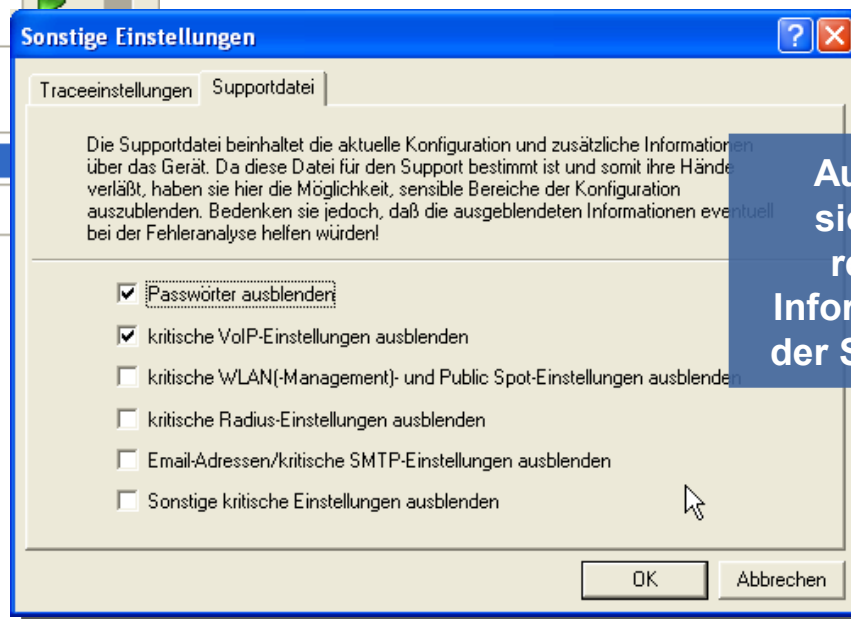
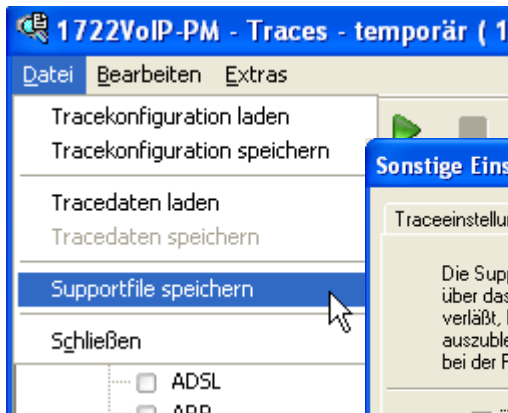
Feature Notes LCOS 7.6

Seite 20

LANCOM
Systems

LANmonitor – Neues in Traces/Supportdatei

- **SSL-verschlüsselter Zugriff** zur Ausführung von Traces auf Geräten
- **Kontinuierliches Backup** mit einstellbarer maximaler Dateigröße
- **Setzen der Zeit** bei Geräten ohne gültige Systemzeit
- **Export einer Supportdatei**, die Sysinfo, Bootlog und Konfiguration enthält
➔ damit werden Antwortzeiten und Qualität des Supports deutlich verbessert



**Ausblenden
sicherheits-
relevanter
Informationen in
der Supportdatei**

LCOS 7.6
[LANCOM OPERATING SYSTEM]

Feature Notes LCOS 7.6

Seite 21

LANCOM
Systems

Service und Support

Wir wünschen Ihnen viel Erfolg mit Ihrem neuen LANCOM Produkt!

Über **Lob und Kritik, Anregungen oder Fragen** freuen wir uns unter
info@lancom.de.

Aktuelle Informationen zu Service und Support entnehmen Sie bitte unserem
Support-Beileger, unseren Internetseiten oder unserer Wissensdatenbank
(**Knowledge Base**) unter www.lancom.de/support.

Sollten Sie trotz Handbuch und unseren aktuellen Support-Themen im Internet
einmal nicht weiter wissen, so steht Ihnen in Deutschland Montags bis Freitags
von 9.00-17.00h unsere **Support-Hotline** unter

0900-1-LANCOM (= 0900-1-526266)

zur Verfügung (1,24€ / Min., aus dem deutschen Festnetz).

Ihr LANCOM Systems Team

LCOS 7.6
[LANCOM OPERATING SYSTEM]

LANCOM

Systems