



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

## LANCOM WLC-4025+

Zentrales Management für 25 (optional 100) LANCOM Access Points und WLAN Router

- Zentrale Firmwareverteilung und Management der Access Points
- Automatische Erkennung, Konfiguration und Kanalzuweisung von Access Points
- Überwachen und Sicherstellen der Verschlüsselungs- und QoS-Richtlinien
- Einzigartige Betriebssicherheit ohne "Single-Point-of-Failure"
- Umfangreichste VLAN-, RADIUS- und 802.1X/EAP-Funktionen
- Maximale Performance mit 802.11n Access Points

Der LANCOM WLC-4025+ WLAN Controller eignet sich durch seine Erweiterbarkeit und Kaskadierbarkeit für WLAN-Installationen von 25 bis zu 100 WLAN Access Points, wie sie bei vielen Unternehmen und öffentlichen Einrichtungen wie z.B. Universitäten oder Krankenhäusern anzutreffen sind. Der Controller sorgt für eine einfache Installation und einen sicheren Betrieb und ermöglicht dabei die Mehrfachnutzung einer einzigen WLAN-Infrastruktur für unterschiedliche Anwendungen und Benutzergruppen.

#### **Mehr Management.**

Mit LCMS, dem LANCOM Management System, steht zu LANCOM Routern, Central Site Gateways, Accesspoints, WLAN Controllern und Managed Switches ein kostenfreies Softwarepaket zur Konfiguration, Fernwartung und zur Echtzeitüberwachung unter Microsoft Windows Betriebssystemen bereit. LANconfig, die Anwendung zur Konfiguration auch aus der Ferne mittels HTTP, HTTPS, TFTP oder ISDN-Einwahl, bietet einfache Assistenten von der Grundkonfiguration bis zur Einrichtung von VPN-Verbindungen, aber auch die detaillierte Einstellung der Parameter von Geräten. Dieselbe Installation von LCMS kann dabei verschiedenste LANCOM Geräte anzeigen und warten. Mit LANmonitor stehen die detaillierte Echtzeitüberwachung von Parametern, der Abruf von Protokollen und Statistiken sowie das detaillierte Anfertigen und Analysieren von Trace-Protokollen offen. Neben Komfortfunktionen wie der Firewall-GUI zur objektorientierten Einrichtung der Firewall bieten die automatische Sicherung von Konfigurationen, das Sichern und Einspielen von Skripten sowie die Organisation in Ordnern und ein dynamischer Suchfilter professionelle Funktionen zur Verwaltung von Projekten. Darüber hinaus stehen für Service-Provider umfangreiche Scripting-Methoden sowie professionelle Managementzugänge mit individuellen Zugriffsrechten über SSH, HTTPS, TFTP, Telnet und ISDN-Einwahl zur Verfügung. Für Rollout und Betrieb bieten automatisches Laden von Konfigurationen und Firmware vom USB-Datenträger und die Möglichkeit projekt-spezifische Bootkonfigurationen statt der Standard-Werkseinstellung zu hinterlegen, Potenzial zur Einsparung teurer manueller Wartungsvorgänge.

#### **Mehr Virtualisierung.**

Mit Advanced Routing and Forwarding (ARF) bietet LANCOM eine einzigartige Technologie zur Netzvirtualisierung. Verschiedene logische Netze mit eigenen Eigenschaften für DHCP, DNS, Routing und Firewall lassen sich damit in einem Gerät und auf derselben physischen Infrastruktur betreiben. Die Netze werden zum Beispiel im LAN verschiedenen VLANs zugeordnet im WAN getagged oder verschiedenen Einwahlen zugeordnet. Durch die innovative Tunnel-in-Tunnel-Technik für VPN können die separierten Netze zwischen LANCOM Routern sogar über dieselbe IPsec-VPN-Verbindung isoliert übertragen werden - auch bei Überschneiden der IP-Adresskreise. ARF eignet sich zur standort-übergreifenden Trennung logischer Netze zum Beispiel für verschiedene Anwendungen oder Dienstleister auf derselben Infrastruktur, sodass diese an keiner Stelle in Konflikt geraten können. Der Übergriff - bewusster Angriff oder versehentliche Fehleingaben - von einem logischen Netz auf das andere wird mit ARF wirksam unterbunden. ARF ermöglicht speziell Unternehmen mit vielen Standorten den Wechsel auf eine rein IP-basierte Infrastruktur und bietet damit enorme Einsparpotenziale im Betrieb.

#### **Umfangreichste Sicherheitsfunktionen.**

Auch in Punkto Sicherheit bietet der Controller-Betrieb eine neue Dimension: Alle eigenen Access Points werden eindeutig anhand digitaler Zertifikate identifiziert und laufend überwacht. Das Background-Scanning bietet eine permanente Übersicht über das gesamte Frequenzband. Die darauf basierende Rogue AP Detection und Rogue Client Detection des im Lieferumfang enthaltenen WLANmonitors bietet eine komplette Übersicht über alle in Funkreichweite befindlichen WLAN-Netzwerke und -Clients. Benutzerauthentifizierungen und Zugangskontrolle können mittels RADIUS/EAP realisiert werden – entweder über den im LANCOM WLAN Controller integrierten RADIUS/EAP-Server oder über beliebige externe RADIUS/EAP-Server, denen gegenüber der LANCOM WLAN Controller als Proxy auftritt. Zur Trennung von Benutzergruppen bietet der WLAN Controller umfangreichste VLAN-Unterstützung, angefangen von einem statischen Mapping von SSIDs auf VLANs z.B. für WLAN-Gastzugänge, über die "Advanced Routing and Forwarding"-Funktionen für mehrere IP- bzw. VLAN-Kontexte, bis hin zu einer benutzer- oder standortbezogenen dynamischen VLAN-Zuweisung.

#### **Höchste Performance - jederzeit.**

Anders als bei vielen zentralistischen Systemen wird effektiv die Entstehung eines "Single Point of Failure" vermieden. Das wird zum einen durch die "Smart Controller"-Systemarchitektur erreicht (Daten können flexibel, je nach Anwendung entweder zentral oder dezentral ausgekoppelt werden), zum anderen durch die Möglichkeit eines optionalen, pro SSID definierbaren autarken Weiterbetriebs. Dadurch erst wird ein standortübergreifendes WLAN-Management möglich, bei dem ein jederzeit verfügbarer Produktivbetrieb selbst bei Ausfall der Controller-Verbindung ohne Kompromittierung der Sicherheit garantiert ist.

### **Besonders Zukunftssicher.**

Durch die Smart Controller Technologie und Details wie den integrierten Hardware-Krypto-Beschleuniger ist der LANCOM WLAN Controller besonders zukunftssicher. Es können alle aktuellen LANCOM 2.4 und 5 GHz WLAN Access Points und WLAN Router per kostenfreiem LCOS-Update in das WLAN-Management integriert werden. Besonders die Access Points der LANCOM L-300er Serie, die auf dem 802.11n Standard basieren, können problemlos integriert werden, ohne dass der Controller bei höheren Datenraten zum zentralen Flaschenhals wird. Die "Split-Management"-Integration der LANCOM WLAN Router und Integrated Access Devices ermöglicht erstmals auch die Einbindung von Home Offices in eine firmenweite WLAN-Sicherheitsrichtlinie. Für die WLAN Controller Firmware und die enthaltenen Management-Programme LANconfig, LANmonitor und WLANmonitor sichert LANCOM Systems eine beständige Weiterentwicklung zu, wobei Software-Updates bereits im Gerätepreis enthalten sind.

WLAN Profileinstellungen*	
Funkkanäle 2.4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (2.4 GHz Band)
Funkkanäle 5 GHz	Bis zu 26 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS Kanalwahl verbunden)
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support mit optionaler Zuordnung eines ARF-Kontextes, IEEE 802.11d Support
VLAN	VLAN-ID einstellbar pro Schnittstelle, WLAN SSID, Punkt-zu-Punkt-Verbindung und Routing-Kontext (4.094 IDs) IEEE 802.1q
Sicherheit	IEEE 802.11i / WPA2 mit Passphrase oder 802.1X und hardwarebeschleunigtem AES, Closed Network, WEP64, WEP128, WEP152, 802.1X /EAP
Quality of Service	Priorisierung entsprechend der Wireless Multimedia Extensions (WME, Bestandteil von IEEE 802.11e)
Background Scanning	Erkennung von fremden Access Points ("Rogue Access Points") und der Kanaleigenschaften auf allen WLAN-Kanälen während des normalen Access-Point-Betriebes. Das Background-Scan-Intervall gibt an, in welchen zeitlichen Abständen ein Wireless Router oder Access Point nach fremden WLAN-Netzen in Reichweite sucht. Mit der Zeiteinheit kann ausgewählt werden, ob die eingetragenen Werte für Millisekunden, Sekunden, Minuten, Stunden oder Tage gelten
Client Detection	Erkennung von fremden WLAN Clients ("Rogue Clients") anhand von Probe-Requests
*) Hinweis	Je nach verwendeten Access Points
WLAN Controller	
Anzahl gemanagter Geräte	Bis zu 25 LANCOM Access Points und WLAN Router können - auch in beliebiger Kombination - durch den LANCOM WLAN Controller zentral gemanagt werden. Mit den optionalen WLC Erweiterungsoptionen können bis zu 100 LANCOM WLAN Access Points und WLAN Router gemanagt werden. Weitere Kapazitätserweiterungen sind über mehrere Controller beliebig durch Kaskadierung möglich.
Smart Controller Technologie	Der LANCOM WLAN Controller unterstützt pro Funkzelle / SSID die unterschiedliche Auskopplung der Nutzdaten: – direkt in das LAN gebridged (maximale Performance z.B. für 802.11n-basierte Access Points) – per VLAN strikt vom LAN separiert (z.B. für WLAN-Gastzugänge) – zentral zum Controller getunnelt* (Layer-3-Tunneling über IP-Netze hinweg) *ab LCOS 8.5x
Auto Discovery	Automatisches Finden der WLAN Controller durch die LANCOM Access Points oder WLAN Router anhand von IP-Broadcasts, einstellbaren DNS-Namen oder IP-Adressen. Auch Geräte in entfernten Außenstellen oder Home Offices, die nicht direkt einen zentralen Controller erreichen, können in das zentrale Management eingebunden werden.
Authentifizierung und Autorisierung	Access Points können manuell oder automatisch authentifiziert werden. Signalisierung neuer Access Points durch LED-Anzeige, Email-Benachrichtigung, SYSLOG und SNMP-Traps. Manuelle Authentifizierung über grafisches Benutzerinterface in LANmonitor oder WEBconfig. Halbautomatische Authentifizierung anhand von Access Point Listen im Controller ("Bulk-Modus"). Vollautomatischer Modus mit einstellbarer Default-Konfiguration (separat an- und abschaltbar, z.B. während der Rollout-Phase). Eindeutige Identifikation autorisierter Access Points anhand digitaler Zertifikate, Zertifikatserstellung durch integrierte CA (Certificate Authority), Zertifikatsverteilung mittels SCEP (Simple Certificate Enrollment Protocol). Sperrung von Access Points mittels CRL (Certificate Revocation List)
Management-Kommunikationsprotokoll	CAPWAP (Control and Provisioning Protocol for Wireless Access Points). Zur Kommunikation zwischen Controller und Access Points genügt eine beliebige IP-Verbindung, so dass auch ein netzwerksegment- und standortübergreifendes WLAN-Management möglich ist.
Layer-3-Tunneling	Layer-3-Tunnel gemäß CAPWAP-Standard, um WLANs pro SSID zu einem IP-Subnetz zu verschalten (Bridge). Die Layer-3-Tunnel transportieren Layer-2-Pakete gekapselt durch Layer-3-Netze zu einem LANCOM WLAN Controller, so dass der Datenverkehr gemanagter Access Points unabhängig von der bestehenden Netzinfrastruktur aggregiert werden kann. Dies ermöglicht Roaming ohne einen Wechsel der IP-Adresse und das logische Zusammenfassen von SSID, ohne den Einsatz von VLANs
Verschlüsselung	DTLS-Verschlüsselung des Kontrollkanals zwischen WLAN Controller und Access Point (256 bit AES Verschlüsselung mit digitalen Zertifikaten, inkl. Hardware-Krypto-Beschleuniger, Verschlüsselung zu Diagnosezwecken abschaltbar)
Firmware Management	Konfiguration von mehreren LANCOM Wireless Routern und LANCOM Access Points wird vom Controller aus vorgenommen. Einrichten eines Webserver erforderlich. Eine Automatisierung der Firmware Updates ist möglich. Der WLAN-Controller prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion die aktuell verfügbaren Dateien und vergleicht sie mit den Versionen in den Geräten. Dieser Vorgang kann auch z. B. nachts durch einen Cron-Job ausgelöst werden. Wenn auf dem Access Point nicht die gewünschte Version läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points ein.
Skriptverteilung	Ermöglicht die vollständige Konfiguration von nicht WLAN-spezifischen Funktionen wie Redirects, Protokollfilter, ARF etc. Interner Speicher für bis zu drei Skript-Dateien (max. 64 kByte) zur Provisionierung von Access-Points ohne separaten HTTP-Server
RF Management und automatische Funkfeld-Optimierung	Die Kanalzuweisung erfolgt wahlweise statisch oder automatisch. Bei Aktivierung der Funkfeld-Optimierungs-Funktion suchen sich die APs im 2.4 GHz-Band automatisch die optimalen Kanäle. Diese Kanalwahl wird an den Controller übermittelt und der Controller speichert sie für die jeweiligen APs. Funkfeld-Optimierung kann auch für einzelne APs (wiederholt) durchgeführt werden. Sendeleistungseinstellung statisch 0 bis -20 dB. Alarmierung bei Ausfall eines Access Points über LED, Email, SYSLOG und SNMP-Traps
Konfigurationsmanagement	Definition und Gruppierung aller logischen und physikalischen WLAN-Parameter mittels WLAN-Konfigurationsprofilen. Vollautomatische oder manuelle Zuweisung von Profilen zu WLAN Access Points, automatische Konfigurationsübermittlung und -prüfung (Policy Enforcement)
Vererbung von Konfigurationsprofilen	Unterstützung hierarchischer WLAN-Profilgruppen inklusive konfigurierbarer Parameter-Vererbung zur Ableitung abweichender standortspezifischer WLAN-Konfigurationen
Management-Betriebsmodi	Einstellbarer Betriebsmodus "managed" oder "unmanaged" pro Radio-Modul. Bei LANCOM WLAN Routern wird ausschließlich der WLAN-Teil vom Controller aktiv verwaltet (Split-Management).

WLAN Controller	
Autarker Weiterbetrieb	Im "managed"-Modus kann festgelegt werden, ob der Access Point seine WLAN-Konfiguration nicht persistent erhält (keine Speicherung von Konfigurationsdaten, Normalfall im Betrieb mit Controller) und bei Verlust der Verbindung zum Controller sofort den Betrieb einstellt oder ob für eine einstellbare Zeit ein autarker Weiterbetrieb im Rahmen der technischen Möglichkeiten gestattet ist (z.B. Weiterbetrieb von Funkzellen mit WPA2 / PSK bei Ausfall der Controller-Verbindung oder nach Stromausfall). Nach Ablauf der optionalen Weiterbetriebszeit wird die WLAN-Konfiguration im WLAN AP gelöscht. Der autarke Weiterbetrieb ist pro SSID einstellbar.
VLAN und IP-Kontexte	Pro SSID kann ein festes VLAN vorgegeben werden. Der WLAN Controller kann eigenständig bis zu 64 separate IP-Netze zur Verfügung stellen, die jeweils individuell auf VLANs und damit auch auf SSIDs abgebildet werden können (Advanced Routing and Forwarding, ARF). Der Controller kann unter anderem individuelle DHCP-, DNS-, Routing-, Firewall- und VPN-Funktionen für diese Netze übernehmen.
Dynamische VLAN-Zuweisung	Dynamische VLAN-Zuweisung für bestimmte Benutzergruppen anhand von MAC-Adressen, BSSID oder SSID mittels externem RADIUS-Server
RADIUS-Accounting pro SSID	Verteilung pro SSID individueller Einstellungen zu 802.1X
RADIUS-Server	Integrierter RADIUS-Server zur Verwaltung von MAC-Adress-Listen. Unterstützung von RADSEC (Secure RADIUS) zur sicheren Anbindung an RADIUS-Server
EAP-Server	Integrierter EAP-Server zur Authentisierung von 802.1X Clients mittels EAP-TLS, EAP-TTLS, PEAP, MS-CHAP oder MS-CHAP v2
RADIUS/EAP Proxy	Proxy-Betriebsart für externe RADIUS/EAP-Server (Forwarding und Realm Handling)
Redundanz, Controller-Backup und Lastverteilung	Jedem gemanagten LANCOM Access Point können mehrere alternative WLAN Controller zugewiesen werden. Innerhalb dieser Gruppen wird auslastungsabhängig ein passender Controller ausgewählt, so dass sich bei größeren Installationen auch im Backup-Fall automatisch eine Gleichverteilung auf alle Controller ergibt.
Fast Roaming	Die Access Points unterstützen PMK-Caching und Pre-Authentication für schnelles Roaming. Im WPA2- und WPA2-PSK-Modus beträgt die Roaming-Zeit unter 85 ms (Voraussetzungen: Ausreichende Signalqualität, hinreichende Überlappung von Funkzellen sowie Clients mit geeignet eingestelltem, niedrigen Roaming-Threshold).
QoS	802.11e / WME: Automatisches VLAN-Tagging (802.1p) in den Access Points. Umsetzung auf DiffServ-Attribute im WLAN Controller, sofern dieser als Layer-3-Router zum Einsatz kommt
Background Scanning, Rogue AP und Rogue Client Detection	Während des normalen Betriebs kann ohne Unterbrechung des Funkbetriebes im Hintergrund ein Background-Scan gefahren werden, so dass auf allen Kanälen Informationen über alle Funkkanalauslastungen sowie über alle sichtbaren Access Points und Clients gesammelt werden können (Hintergrundbetrieb als "Probe" bzw. "Sensor"). Fremde Access Points und Clients werden zentral an die Rogue AP Detection des LANCOM WLANmonitor gemeldet.
WLAN Visualisierung	Das im Lieferumfang enthaltene Management-Programm LANCOM WLANmonitor dient als zentrales Monitoring-Programm für den WLAN Controller und visualisiert die Zuordnung und Performance von allen WLAN Controllern, Access Points, SSIDs und Clients.
WLAN-Gastzugänge	Statisches Mapping von Gast-SSIDs in VLANs, Zugriffsbeschränkungen und VLAN-Routing mittels ARF (Advanced Routing and Forwarding)
Public-Spot-Funktion	Funktion optional (siehe Optionen). Einfaches Einrichten von Zugangsdaten mit nur 2 Maus-Klicks über den Voucher-Druck-Assistent möglich. Die Voucher lassen sich über PC-Standard-Drucker ausdrucken. Anpassung des Voucher-Druck-Assistenten an das Unternehmen durch Einbindung des individuellen Firmenlogos. Funktioniert auch ohne externen RADIUS- oder Accounting-Server. Einstellung von Zeit- und/oder Volumenbudgets sowie Kriterium für Start der Abrechnung. Unterstützung von öffentlichen Zertifikaten und Zertifikats-Ketten von Trust Centern für Public Spot. Somit sind für gängige Internet-Browser vertrauenswürdige Login-Seiten mit gesichertem Zugriff (HTTPS) ohne Warnungen möglich
WLAN Client Limiting	Zur gleichmäßigen Auslastung mehrerer Access Points kann pro Access Point und pro SSID die maximale Anzahl der unterstützten WLAN Clients vorgegeben werden. Darüber hinausgehende Assoziierungsanfragen werden abgelehnt.
Management Software	Im Lieferumfang enthalten: – LANCOM LANconfig – LANCOM LANmonitor – LANCOM WLANmonitor
Unterstützte Access Points und WLAN-Router	
Indoor	– LANCOM L-54g Wireless – LANCOM L-54ag Wireless – LANCOM L-54 dual Wireless – LANCOM L-305agn Wireless – LANCOM L-310agn Wireless – LANCOM L-315agn dual Wireless – LANCOM L-320agn dual Wireless – LANCOM L-321agn dual Wireless – LANCOM L-322agn dual Wireless
Outdoor	– LANCOM OAP-54 Wireless – LANCOM OAP-54-1 Wireless – LANCOM OAP-310 Wireless – LANCOM OAP-321 – LANCOM OAP-321-3G
Industrial	– LANCOM IAP-54 Wireless – LANCOM XAP-40-2 Wireless – LANCOM IAP-321 – LANCOM IAP-321-3G
UMTS/HSPDA	– LANCOM 1780EW-3G – LANCOM 3850 Wireless
WLAN-Router und IADs	– LANCOM 1781AW – LANCOM 1781EW – LANCOM 1811n Wireless – LANCOM 1821n Wireless – LANCOM 1823 VoIP – LANCOM 1821+ Wireless ADSL
Funktionen im Layer-3-Routing-Betrieb	
Hinweis	Die folgenden Funktionen sind teilweise für das Gerät nur dann aktiv, wenn es als Router, Firewall oder VPN-Gateway betrieben wird.
Firewall	
Stateful Inspection Firewall	Richtungsabhängige Prüfung anhand von Verbindungsinformationen. Trigger für Firewall-Regeln in Abhängigkeit vom Backup-Status, z.B. für vereinfachte Regelsätze bei schmalbandigen Backup-Leitungen. Limitierung der Session-Anzahl pro Gegenstelle (ID)
Paketfilter	Prüfung anhand der Header-Informationen eines Pakets (IP oder MAC Quell-/Zieladressen; Quell-/Zielports, DiffServ-Attribut); gegenstellenabhängig, richtungsabhängig, bandbreitenabhängig
Erweitertes Port-Forwarding	Network Address Translation (NAT), optional auch abhängig von Protokolltyp und WAN-Adresse, um z.B. Webserver im LAN von außen verfügbar zu machen

Firewall	
N:N IP-Adressumsetzung	N:N-Mapping zum Umsetzen oder Verstecken von IP-Adressen oder ganzen Netzwerken
Tagging	Markierung von Paketen in der Firewall mit Routing-Tags, z.B. für Policy-based Routing
Aktionen	Weiterleiten, Verwerfen, Zurückweisen, Absenderadresse sperren, Zielport schließen, Verbindung trennen
Benachrichtigungen	Via Email, SYSLOG oder SNMP-Trap
Quality of Service	
Traffic Shaping	Dynamisches Bandbreitenmanagement mit IP Traffic-Shaping
Bandbreitenreservierung	Dynamische Reservierung von Mindest- und Maximalbandbreiten, absolut oder verbindungsbezogen, für Sende- und Empfangsrichtung getrennt einstellbar. Setzen von relativen Bandbreiten-Limits für QoS in Prozent
DiffServ/TOS	Priority-Queuing der Pakete anhand des DiffServ/TOS-Felds
Paketgrößensteuerung	Automatische Steuerung der Paketgrößen über Fragmentierung oder Anpassung der Path Maximum Transmission Unit (PMTU)
Layer 2/Layer 3-Tagging	Automatisches oder festes Umsetzen von Layer-2-Prioritätsinformationen (nach IEEE 802.1p markierte Ethernet-Frames) auf Layer-3-DiffServ-Attribute im Routing-Betrieb. Umsetzen von Layer 3 auf Layer 2 mit automatischer Erkennung der 802.1p-Unterstützung des Zielgerätes
Sicherheit	
Intrusion Prevention	Überwachung und Sperrung von Login-Versuchen und Portscans
IP-Spoofing	Überprüfung der Quell-IP-Adressen auf allen Interfaces: nur die IP-Adressen des zuvor definierten IP-Netzes werden akzeptiert
Access-Control-Listen	Filterung anhand von IP- oder MAC-Adresse sowie zuvor definierten Protokollen für den Konfigurationszugang
Denial-of-Service Protection	Schutz vor Fragmentierungsfehlern und SYN-Flooding
Allgemein	Detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung
URL-Blocker	Filtern von unerwünschten URLs anhand von DNS-Hitlisten sowie Wildcard-Filtern. Weiterreichende Möglichkeiten durch Nutzung der Content Filter Option
Passwortschutz	Passwortgeschützter Konfigurationszugang für jedes Interface einstellbar
Alarmierung	Alarmierung durch Email, SNMP-Traps und SYSLOG
Authentifizierungsmechanismen	EAP-TLS, EAP-TTLS, PEAP, MS-CHAP und MS-CHAP v2 als EAP-Authentifizierungsmechanismen, PAP, CHAP, MS-CHAP und MS-CHAP v2 als PPP-Authentifizierungsmechanismen
Programmierbarer Reset-Taster	Einstellbarer Reset-Taster für "ignore", "boot-only" und "reset-or-boot"
Hochverfügbarkeit / Redundanz	
VRRP	VRRP (Virtual Router Redundancy Protocol) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall. Ermöglicht passive Standby-Gruppen oder wechselseitige Ausfallsicherung mehrerer aktiver Geräte inkl. Lastverteilung sowie frei einstellbare Backup-Prioritäten
FirmSafe	Für absolut sichere Software-Upgrades durch zwei speicherbare Firmware-Versionen, inkl. Testmodus bei Firmware-Updates
Load-Balancing	Statische und dynamische Lastverteilung auf bis zu 4 WAN-Strecken. Kanalbündlung durch Multilink-PPP (sofern vom Netzbetreiber unterstützt)
VPN-Redundanz	Backup von VPN-Verbindungen über verschiedene Hierarchie-Stufen hinweg, z.B. bei Wegfall eines zentralen VPN-Konzentrators und Ausweichen auf mehrere verteilte Gegenstellen. Beliebige Anzahl an Definitionen für VPN-Gegenstellen in der Konfiguration (Tunnel-Limit gilt nur für aktive Verbindungen). Bis zu 32 alternative Gegenstellen mit jeweils eigenem Routing-Tag als Backup oder zur Lastverteilung pro VPN-Gegenstelle. Die automatische Auswahl kann der Reihe nach, aufgrund der letzten erfolgreichen Verbindung oder zufällig (VPN-Load-Balancing) erfolgen
Leitungsüberwachung	Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling
VPN	
IPSec over HTTPS	Ermöglicht IPSec VPN durch Firewalls in Netzen, für die z. B. Port 500 für IKE gesperrt ist, auf Basis von TCP über Port 443. Geeignet für Client-to-Site (mit LANCOM Advanced VPN Client 2.22 für Windows oder 1.00 für Mac OS X oder höher) und Site-to-Site-Verbindungen (LANCOM VPN Gateways oder Router mit LCOS 8.0 oder höher). IPSec over HTTPS basiert auf der NCP VPN Path Finder Technology
Anzahl der VPN-Tunnel	5 Tunnel gleichzeitig aktiv bei Kombination von IPSec- mit PPTP-Tunneln (MPPE), unbegrenzte Anzahl konfigurierbarer Gegenstellen.
Hardware-Beschleuniger	Integrierter Hardwarebeschleuniger für die 3DES/AES-Ver- und -Entschlüsselung
Echtzeituhr	Integrierte, gepufferte Echtzeituhr zur Speicherung der Uhrzeit bei Stromausfällen, sodass die zeitliche Validierung der Gültigkeit von Zertifikaten immer möglich ist
Zufallszahlen-Generator	Erzeugung echter Zufallszahlen in Hardware, z. B. zur Verbesserung der Generierung von Schlüsseln für Zertifikate direkt nach dem Einschalten
1-Click-VPN Site-to-Site	Erzeugen von VPN-Verbindungen zwischen LANCOM-Routern per "Drag and Drop" mit einem Klick in LANconfig
IKE	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate

VPN	
Zertifikate	Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL, Upload von PKCS#12-Dateien über HTTPS-Interface und LANconfig. Gleichzeitige Unterstützung mehrerer Certification Authorities durch Verwaltung von bis zu neun parallelen Zertifikatshierarchien in Containern (VPN-1 bis VPN-9). Vereinfachte Adressierung der einzelnen Zertifikate durch Angabe des Containers (VPN-1 bis VPN-9) der Zertifikatshierarchie. Platzhalter zur Prüfung von Zertifikaten auf Teile der Identität im Subject. Secure Key Storage zur Sicherung eines privaten Schlüssels (PKCS#12) gegen Diebstahl
Zertifikatsrollout	Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) pro Zertifikatshierarchie
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP pro Zertifikatshierarchie
OCSF Client	Prüfen von X.509-Zertifikaten anhand von OCSF (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs
XAUTH	XAUTH-Client zur Anmeldung von LANCOM Routern und Access Points an XAUTH-Servern inkl. IKE-Config-Mode. XAUTH-Server, der die Anmeldung von Clients per XAUTH an LANCOM Routern ermöglicht. Anbindung des XAUTH-Servers an RADIUS-Server zur Authentisierung von VPN-Zugängen pro Verbindung über eine zentrale Benutzerverwaltung. Authentisierung für VPN-Client-Zugänge via XAUTH mit RADIUS-Anbindung auch mit OTP-Tokens
Proadaptive VPN	Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen. Propagieren der dynamisch gelernten Routen kann auf Wunsch per RIPv2 erfolgen
Algorithmen	3DES (168 Bit), AES (128, 192 und 256 Bit), DES, Blowfish (128-448 Bit) und CAST (128 Bit). OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. MD-5 oder SHA-1 Hashes
NAT-Traversal	Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen
IPCOMP	VPN-Datenkompression zur Optimierung des Durchsatzes auf schmalbandigen Strecken mittels LZS- oder Deflate-Komprimierung (muss von Gegenseite unterstützt werden)
Dynamic DNS	Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic-DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird
Spezifisches DNS-Forwarding	DNS-Forwarding einstellbar pro DNS-Domäne, z.B. zur Auflösung interner Namen durch eigenen DNS-Server im VPN und Auflösung externer Namen durch Internet-DNS-Server. Eintrag für Backup-DNS pro DNS-Weiterleitung
VPN-Durchsatz (max., AES)	
1418 Byte Framegröße UDP	337 Mbit/s
256 Byte Framegröße UDP	67 Mbit/s
Firewall-Durchsatz (max.)	
1518 Byte Framegröße UDP	643 Mbit/s
256 Byte Framegröße UDP	112 Mbit/s
Content Filter (optional)	
Demo-Version	Aktivierung der 30-Tage Testversion nach kostenloser Produktregistrierung unter <a href="http://www.lancom.de/routeroptions">http://www.lancom.de/routeroptions</a>
URL-Filter-Datenbank/Ratingserver	Weltweit redundante Ratingserver der IBM Security Solutions zur Abfrage von URL-Klassifizierungen. Datenbank mit über 100 Millionen Einträgen, die etwa 10 Milliarden Webinhalte abdeckt. Täglich fast 150.000 Aktualisierungen durch Webcrawler, welche automatisiert Webseiten untersuchen und kategorisieren: durch Textklassifizierung mit optischer Zeichenerkennung, Schlüsselwortsuche, Bewertung von Häufigkeit und Wort-Kombinationen, durch Webseitenvergleich hinsichtlich Text, Bildern und Seitenelementen, durch Objekterkennung von speziellen Zeichen, Symbolen, Warenzeichen, verbotenen Bildern, durch Erkennung von Erotik und Nacktheit anhand der Konzentration von Hauttönen in Bildern, durch Struktur- und Linkanalyse, durch Malware-Erkennung in Binärdateien und Installationspaketen
HTTPS-Filter	Über Firewall zusätzlich aktivierbare Möglichkeit zur Filterung von HTTPS-Anfragen
Kategorien/Kategorie-Profile	Definition von Filterregeln pro Profil durch Zusammenstellen von Kategorie-Profilen aus 58 Kategorien, z.B. zur Einschränkung der Internetnutzung auf geschäftliche Anwendungen (Unterbinden privater Nutzung) oder Schutz vor jugendgefährdenden oder gefährlichen Inhalten wie z.B. Malware-Seiten. Übersichtliche Auswahl durch Zusammenstellung thematisch ähnlicher Kategorien zu Gruppen. Inhalte pro Kategorie erlauben, blockieren oder für Override freigeben
Override	Für Kategorien kann ein Override vergeben werden, der es Anwendern fallweise erlaubt, eigentlich gesperrte Seiten durch manuelle Bestätigung zu laden. Der Override kann zeitlich beschränkt für die Kategorie, die Domäne oder eine Kombination aus beidem ausgesprochen werden. Möglichkeit zur Benachrichtigung eines Administrators im Fall von Overrides
Black-/Whitelist	Manuell konfigurierbare Listen zum expliziten Erlauben (Whitelist) oder Verbieten (Blacklist) von Webseiten pro Profil, unabhängig von der Bewertung durch den Ratingserver. Platzhalter (Wildcards) zur Definition von Gruppen von Seiten oder Filtern von Unterseiten
Profile	Zusammenfassen von Zeitrahmen, Black-/Whitelists und Kategorie-Profilen zu getrennt aktivierbaren Profilen für Content Filter Aktionen. Werksseitig aktiviertes Default-Profil mit Standard-Einstellungen zum Blocken von rassistischen, pornografischen, kriminellen, extremistischen Inhalten sowie anonymen Proxies, Waffen/Militär, Drogen, SPAM und Malware
Zeitrahmen	Flexible Definition von Zeitrahmen, um Profile zur Filterung in Abhängigkeit von Tageszeiten oder Wochentagen zu definieren, z. B. für Lockerung während Pausenzeiten für privates Surfen
Flexibel anwendbare Firewall-Aktion	Anwendung des Content Filters durch Content Filter Aktionen mit Auswahl des gewünschten Profils in der Firewall. Firewall-Regeln ermöglichen die flexible Anwendung eigener Profile für verschiedene Clients, Netze oder Verbindungen zu bestimmten Servern

Content Filter (optional)	
Individuelle Rückmeldungen (bei blockiert, Fehler, Override)	Antwortseiten des Content Filters für blockierte Seiten, Fehler und Override können individuell gestaltet und durch Variablen mit aktuellen Informationen zu Kategorie, URL und Kategorisierung des Ratingservers versehen werden. Sprachabhängige Definition von Antwortseiten, je nach vom Anwender ausgewählter Anzeigesprache des Webbrowsers
Umleitung zu externen Webseiten	Alternativ zur Anzeige der geräteinternen Antwortseiten für blockierte Seiten, Fehler oder Override können auch Seiten von externen Webservern aufgerufen werden (Redirect)
Lizenzmanagement	Automatische Benachrichtigung vor Ablauf der Lizenz per E-Mail, LANmonitor, SYSLOG und SNMP-Trap. Aktivierung der nächsten Lizenz-Verlängerung zu beliebigem Zeitpunkt vor dem Ablauf der aktuellen Lizenz (Start des neuen Lizenzzeitraumes passend zum Ablauf der aktuellen Lizenz)
Statistiken	Anzeige der Anzahl der geprüften und gesperrten Webseiten je Kategorie in LANmonitor. Logging aller Content-Filter-Events in LANmonitor; tägliches, wöchentliches oder monatliches Anlegen einer Protokolldatei. Hitliste der meist aufgerufenen Seiten und Ratingergebnisse. Auswertung der Verbindungseigenschaften, minimalen, maximalen und durchschnittlichen Antwortzeiten des Ratingservers
Alarmierungen	Benachrichtigung bei Content-Filterung einstellbar via E-Mail, SNMP, SYSLOG sowie LANmonitor
Assistent für Standard-Konfigurationen	Assistent zur Einrichtung des Content Filters für typische Anwendungsszenarien in wenigen Schritten, inklusive Erzeugung der nötigen Firewall-Regeln mit entsprechender Aktion
Maximale Benutzeranzahl	Gleichzeitige Prüfung des HTTP-Verkehrs für maximal 400 unterschiedliche IP-Adressen im LAN
VoIP	
SIP ALG	Das SIP ALG (Application Layer Gateway) agiert als Proxy für SIP-Kommunikation. Bei SIP-Telefonaten werden vom ALG automatisch die notwendigen Ports für die entsprechenden Medienpakete geöffnet. Durch automatische Adressumsetzung für Geräte im LAN entfällt der Einsatz von STUN.
Routingfunktionen	
Router	IP- und NetBIOS/IP-Multiprotokoll-Router
Advanced Routing and Forwarding	Separates Verarbeiten von 16 Kontexten durch Virtualisierung des Routers. Abbildung in VLANs und vollkommen unabhängige Verwaltung und Konfiguration von IP-Netzen im Gerät möglich, d.h. individuelle Einstellung von DHCP, DNS, Firewalling, QoS, VLAN, Routing usw. Automatisches Lernen von Routing-Tags für ARF-Kontexte aus der Routing-Tabelle
HTTP	HTTP- und HTTPS-Server für die Konfiguration per Webinterface
DNS	DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy und Dynamic DNS-Client
DHCP	DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection. Cluster-Betrieb mehrerer LANCOM DHCP-Server pro Kontext (ARF-Netz) mit Caching aller DNS-Zuordnungen aller DHCP-Server. DHCP-Weiterleitung zu mehreren (redundanten) DHCP-Servern
NetBIOS	NetBIOS/IP-Proxy
NTP	NTP-Client und SNTP-Server, automatische Sommerzeit-Anpassung
Policy-based Routing	Policy-based Routing auf Basis von Routing Tags. Anhand von Firewall-Regeln können bestimmte Daten so markiert werden, dass diese dann anhand ihrer Markierung gezielt vom Router z. B. nur auf bestimmte Gegenstellen oder Leitungen geroutet werden
Dynamisches Routing	Dynamisches Routing mit RIPv2. Lernen und Propagieren von Routen, getrennt einstellbar für LAN und WAN. Extended RIPv2 mit HopCount, Poisoned Reverse, Triggered Update für LAN (nach RFC 2453) und WAN (nach RFC 2091) sowie Filtereinstellungen zum Propagieren von Routen. Definition von RIP-Quellen mit Platzhaltern (Wildcards) im Namen
Layer-2-Funktionen	
ARP-Lookup	Von Diensten im LCOS (Telnet, SSH, SNMP, SMTP, HTTP(S), SNMP etc.) über Ethernet versandte Antwortpakete auf Anfragen von Stationen können direkt zur anfragenden Station (Default) geleitet werden oder an ein durch ARP-Lookup ermitteltes Ziel
COM-Port-Server	
COM-Port-Forwarding	COM-Port-Server für die DIN-Schnittstellen, der ein seriell angeschlossenes Gerät mit virtuellem COM-Port via Telnet (RFC 2217) zur Fernsteuerung verwaltet (nutzbar mit gängigen virtuellen COM-Port-Treibern gemäß RFC 2217). Schaltbare Newline-Konvertierung und alternativer Binärmodus. TCP-Keepalive nach RFC 1122, mit konfigurierbarem Keepalive-Intervall, Wiederholungs-Timeout und -Anzahl
LAN-Protokolle	
IP	ARP, Proxy ARP, BOOTP, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (Server), RADIUS, RIP-1, RIP-2, RTP, SNMP, TCP, TFTP, UDP, VRRP, VLAN
WAN-Protokolle	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC oder PNS) und IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IP
xDSL (ext. Modem)	ADSL1, ADSL2 oder ADSL2+ mit externem ADSL2+-Modem
ISDN	ISDN-Daten- oder Sprachnutzung über die integrierte ISDN-Schnittstelle
Schnittstellen	
Ethernet Ports	4 individuelle Ports, 10/100/1000 Mbit/s Ethernet. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden

Schnittstellen	
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). Als WAN-Port können zusätzliche, externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden.
USB 2.0 Host-Port	USB 2.0 Hi-Speed Host-Port zum Anschluss von USB-Druckern (USB-Druck-Server), seriellen Geräten (COM-Port-Server), USB-Datenträgern (FAT Dateisystem) oder unterstützte UMTS-USB-Modems; bidirektionaler Datenaustausch möglich*
Serielle Schnittstelle	Serielle Konfigurationsschnittstelle / COM-Port (8-pol. Mini-DIN): 9.600-115.000 Bit/s, optional zum Anschluss eines Analog-/GPRS-Modems geeignet. Unterstützt internen COM-Port-Server und ermöglicht die transparente asynchrone Übertragung serieller Daten via TCP
LCMS (LANCOM Management System)	
LANconfig	Konfigurationsprogramm für Microsoft Windows, inkl. komfortabler Setup-Assistenten. Möglichkeit zur Gruppenkonfiguration, gleichzeitige Fernkonfiguration und Management mehrerer Geräte via IP-Verbindung (HTTPS, HTTP, TFTP). Projekt- oder benutzerbezogene Einstellung des Konfigurationsprogramms. Baumansicht mit gleicher Struktur wie in WEBconfig zum schnellen Springen zwischen Einstellungsseiten im Konfigurationsfenster. Passwortfelder mit optional einblendbarem Klartextpasswort sowie Erzeugung komplexer Passwörter. Automatisches Speichern der aktuellen Konfiguration vor jedem Firmware-Update. Austausch von Konfigurations-Dateien zwischen ähnlichen Geräten, z.B. zur Migration alter Konfigurationen auf neue LANCOM Produkte. Erkennen und Anzeige von LANCOM Managed Switches. Umfangreiche Anwendungshilfe zu LANconfig und Hilfe zu den Konfigurationsparametern von Geräten. LANCOM QuickFinder als Suchfilter innerhalb von LANconfig und Gerätekonfigurationen, der die Ansicht sofort bei Eingabe auf die Trefferliste reduziert.
LANmonitor	Monitoring-Applikation für Microsoft Windows zur (Fern-)Überwachung und Protokollierung von Geräte- und Verbindungsstatus von LANCOM Geräten, inkl. PING-Diagnose und TRACE mit Filtern und Speichern der Ergebnisse in einer Datei. Suchfunktion innerhalb und Vergleich von TRACE-Ausgaben. Assistenten für Standard-Diagnosen. Export von Diagnose-Dateien für Supportzwecke (enthalten Bootlog, Sysinfo und die Gerätekonfiguration ohne Passwörter). Grafische Darstellung von Kenngrößen (in der Ansicht von LANmonitor mit entsprechendem Symbol gekennzeichnet) mit zeitlichem Verlauf sowie tabellarischer Gegenüberstellung von Minimum, Maximum und Mittelwert in separatem Fenster, z. B. für Sende- und Empfangsraten, CPU-Last, freien Speicher. Monitoring der LANCOM managed/web smart Switches. LANCOM QuickFinder ermöglicht Blättern zwischen den einzelnen Suchergebnissen, die optisch hervorgehoben werden
WLANmonitor	Monitoring-Applikation für Microsoft Windows zur Visualisierung und Überwachung von LANCOM Wireless LAN Installationen, inkl. Rogue AP und Rogue Client-Visualisierung. LANCOM QuickFinder als Suchfilter, der die Ansicht sofort bei Eingabe auf die Trefferliste reduziert
Firewall GUI	Grafische Oberfläche zur Konfiguration der objekt-orientierten Firewall in LANconfig: Tabellenansicht mit Symbolen zum schnellen Erfassen von Objekten, Objekte für Aktionen/Quality-of-Service/Gegenstellen/Dienste, Default-Objekte für typische Anwendungsfälle, Definition individueller Objekte (z.B. für Anwendergruppen)
Automatisches Softwareupdate	Automatische Aktualisierung von LCMS nach Bestätigung. Suche von Updates, inklusive LCOS Versionen für verwaltete Geräte auf dem Downloadserver von myLANCOM (erfordert myLANCOM-Account). Wahlweise Aktualisierung ausgewählter Geräte bei heruntergeladenen Updates
Management	
WEBconfig	Integrierter Webserver zur Konfiguration der LANCOM-Geräte über Internetbrowser mittels HTTPS oder HTTP. Konfiguration von LANCOM Routern und Access Points in Anlehnung an LANconfig mit Systemübersicht, Syslog- und Ereignis-Anzeige, Symbolen im Menübaum, Schnellzugriff über Seitenreiter. Assistenten für Grundkonfiguration, Sicherheit, Internetzugang, LAN-LAN-Kopplung. Online-Hilfe zu Parametern im LCOS-Menübaum
Alternative Boot-Konfiguration	Zur Vorgabe von projekt-/kunden-spezifischen Werten beim Rollout von Geräten können auf bis zu zwei boot- und reset-persistenten Speicherplätzen individuelle Konfigurationen für kundenspezifische Standardeinstellungen (Speicherplatz '1') oder als Rollout-Konfiguration (Speicherplatz '2') abgelegt werden. Zusätzlich ist die Ablage eines persistenten Standard-Zertifikats zur Authentifizierung für Verbindungen beim Rollout möglich
Automatisches Update von USB	Automatisches Laden von geeigneten Firmware- und Konfigurationsdateien nach dem Einstecken von USB-Datenspeichern (FAT-Dateisystem) in LANCOM Router mit USB-Schnittstelle und Werkseinstellungen. Die Funktionalität kann auch für den laufenden Betrieb aktiviert werden. Prüfung des Routers, ob die auf dem USB-Speichermedium vorliegenden Dateien zum Gerät passen und aktueller sind als bereits installierte
Geräte-Syslog	Syslog-Speicher im RAM (Größe abhängig von Speicherausstattung), in dem Ereignisse zur Diagnose festgehalten werden. Werksseitig vorgegebener Regelsatz zur Protokollierung von Ereignissen im Syslog, der vom Anwender angepasst werden kann. Darstellung und Speichern des internen Syslog-Speichers (Ereignisanzeige) von LANCOM Geräten über LANmonitor, Ansicht auch über WEBconfig
Zugriffsrechte	Individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren. Alternative Steuerung der Zugriffsrechte pro Parameter durch TACACS+
Fernwartung	Fernkonfiguration über Telnet/SSH (mit Passwort oder öffentlichem Schlüssel), Browser (HTTP/HTTPS), TFTP oder SNMP; Firmware-Upload über HTTP/HTTPS oder TFTP
TACACS+	Unterstützung des Protokolls TACACS+ für Authentifizierung, Autorisierung und Accounting (AAA) mit verbindungsorientierter und verschlüsselter Übertragung der Inhalte. Authentifizierung und Autorisierung sind vollständig separiert. LANCOM Zugriffsrechte werden auf TACACS+-Berechtigungsstufen umgesetzt. Über TACACS+ können Zugriffsberechtigungen pro Parameter, Pfad, Kommando oder Funktionalität für LANconfig, WEBconfig oder Telnet/SSH gesetzt sowie alle Zugriffe und Änderungen der Konfiguration protokolliert werden. Berechtigungsprüfung und Protokollierung für SNMP Get- und Set-Anfragen. Das Berechtigungssystem wird auch in WEBconfig mit Auswahl eines TACACS+-Servers bei der Anmeldung unterstützt. LANconfig unterstützt die Anmeldung über das gewählte Gerät am TACACS+-Server. Prüfung der Ausführung und jeden Kommandos innerhalb von Skripten gegen die Datenbank des TACACS+-Servers. Schaltbare Umgehung von TACACS+ für CRON, Aktionstabelle und Script-Abarbeitung zur Entlastung zentraler TACACS+-Server. Redundanz durch Konfiguration mehrerer TACACS+-Server. Konfigurierbare Möglichkeit zum Rückfall auf lokale Benutzerkonten bei Verbindungsfehlern zu den TACACS+-Servern. Kompatibilitätsmodus zur Unterstützung vieler freier TACACS+-Implementierungen
Fernwartung von Drittgeräten	Zum Fernzugriff auf Komponenten hinter dem LANCOM können nach Authentifizierung beliebige TCP-basierte Protokolle getunnelt werden (z. B. für einen HTTP(S)-Zugriff auf VoIP-Telefone oder Drucker im LAN). Zudem ermöglichen SSH- und Telnet-Client den Zugriff auf diese Geräte von einem LANCOM Gerät mit Interface zum Zielnetz aus, wenn die Kommandozeile des LANCOM Geräts erreicht werden kann

Management	
TFTP- & HTTP(S)-Client	Zum Download von Firmware- und Konfigurations-Dateien von einem TFTP-, HTTP- oder HTTPS-Server mit variablen Dateinamen (Platzhalter für Name, MAC-/IP-Adresse, Seriennummer), z.B. für Roll-Out-Management. Kommandos für den Zugriff per Telnet-Sitzung, Script oder CRON-Job. Die HTTPS-Client Authentisierung kann sowohl über Benutzername und Passwort, als auch über ein Zertifikat erfolgen
SSH- & Telnet-Client	SSH-Client-Funktionalität kompatibel zu OpenSSH unter Linux und Unix-Betriebssystemen zum Zugriff auf Drittkomponenten von einem LANCOM Router aus. Nutzung auch bei Verwendung von SSH zum Login auf dem LANCOM Gerät. Unterstützung von zertifikats- und passwort-basierter Authentifizierung. Erzeugung eigener Schlüssel mittels sshkeygen. Beschränkung der SSH-Client-Funktionalität auf Administratoren mit entsprechender Berechtigung. Telnet-Client-Funktion zum Zugriff/zur Administration von Drittgeräten oder anderen LANCOM Geräten von der Kommandozeile aus
Einfacher HTTP(S)-Fileserver	Ablegen von HTML-Seiten, Grafiken und Vorlagen für Public Spot Seiten, Voucher, Hinweisseiten des Content Filters auf einem USB-Datenträger (FAT Dateisystem) in vorgegebenem Ordner als Alternative zum begrenzten internen Speicher
HTTPS Server	Auswahl, ob ein hochgeladenes oder das Default-Zertifikat für den HTTPS Server verwendet werden soll
Scripting	Scripting-Funktion zur Batch-Programmierung von allen Kommandozeilenparametern und zur Übertragung von (Teil-) Konfigurationen über unterschiedliche Softwarestände und Gerätetypen, inkl. Testmodus für Parameteränderungen. Nutzung der Zeitsteuerung (CRON) oder des Verbindungsauf- und -abbaus zum Ausführen von Scripts zur Automatisierung. Versenden von E-Mails per Script mit beliebigen Ausgaben als Anhang
Load-Befehle	Die Befehle LoadFirmware, LoadConfig und LoadScript können konditional ausgeführt werden, um so automatische Ladevorgänge zu steuern. Zum Beispiel kann bei einer täglichen Ausführung von LoadFirmware geprüft werden, ob die aktuelle Firmware älter oder neuer ist als die angefragte Firmware. Anhand dieser Information wird dann entschieden, ob das Update durchgeführt werden soll. Der Befehl LoadFile erlaubt das Laden von Dateien auf ein Gerät, inklusive von Zertifikaten und gesicherten PKCS#12-Containern
SNMP	SNMP-Management via SNMPv2, private MIB per WEBconfig exportierbar, MIB II
Zeitsteuerung	Zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst. Aktionen können "unscharf", d.h. mit zufälliger Zeitvarianz ausgeführt werden
Diagnose	Sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, LANmonitor für Zustandsanzeige, interne Loggingbuffer für SYSLOG und Firewall-Events, Monitor-Modus für Ethernet-Ports
Statistiken	
Statistiken	Umfangreiche Ethernet-, IP- und DNS-Statistiken; SYSLOG-Fehlerzähler
Accounting	Verbindungs- und Onlinezeit sowie Übertragungsvolumen pro Station. Snapshot-Funktion zum regelmäßigen Auslesen der Werte am Ende einer Abrechnungsperiode. Zeitlich steuerbares (CRON) Kommando zum Zurücksetzen der Zähler aller Konten
Export	Accounting-Information exportierbar via LANmonitor und SYSLOG
Hardware	
Spannungsversorgung	Internes Netzteil (110–230 V, 50-60 Hz)
Umgebung	Temperaturbereich 5–40° C; Luftfeuchtigkeit 0–95%; nicht kondensierend
Gehäuse	Robustes Metallgehäuse, 19" 1 HE mit abschraubbaren Montagewinkeln, Netzwerkanlüsse auf der Frontseite
Anzahl Lüfter	1
Leistungsaufnahme (max.)	30 Watt
Konformitätserklärungen	
CE	EN 55024, EN 60950
Draeger-Validierung	Eignung von LANCOM Geräten mit WLAN und IGMP Snooping zur Übermittlung von Patientendaten im medizinischen Umfeld per Multicast im WLAN
Lieferumfang	
CD/DVD	Datenträger mit Firmware, Management-Software (LANconfig, LANmonitor, WLANmonitor) und Dokumentation
Kabel	Seriell-Konfigurationskabel, 1,5 m
Kabel	Ethernet-Kabel, 3 m
Kabel	Kaltgeräte-Netzkabel
Support	
Garantie	3 Jahre, Support über Hotline und Internet KnowledgeBase
Software-Updates	Regelmäßige kostenfreie Updates (LCOS Betriebssystem und LANCOM Management System) via Internet
Konfigurations-Service	1 LANCOM Config Service Ticket im Lieferumfang enthalten
Optionen	
LANCOM Content Filter	LANCOM Content Filter +10 Benutzer, 1 Jahr Laufzeit, Art.-Nr. 61590
LANCOM Content Filter	LANCOM Content Filter +25 Benutzer, 1 Jahr Laufzeit, Art.-Nr. 61591

Optionen	
LANCOM Content Filter	LANCOM Content Filter +100 Benutzer, 1 Jahr Laufzeit, Art.-Nr. 61592
LANCOM Content Filter	LANCOM Content Filter +10 Benutzer, 3 Jahre Laufzeit, Art.-Nr. 61593
LANCOM Content Filter	LANCOM Content Filter +25 Benutzer, 3 Jahre Laufzeit, Art.-Nr. 61594
LANCOM Content Filter	LANCOM Content Filter +100 Benutzer, 3 Jahre Laufzeit, Art.-Nr. 61595
Vorabaustausch	LANCOM Next Business Day Service Extension Central Site, Art.-Nr. 61413
Garantie-Erweiterung	LANCOM 2-Year Warranty Extension Central Site, Art.-Nr. 61416
Public Spot Unlimited Option	LANCOM Public Spot Unlimited Option, unbegrenzte User-Anzahl, Art.-Nr. 61624
Management	LANCOM WLC AP Upgrade +10 Option, ermöglicht die Verwaltung von 10 weiteren Access Points/WLAN-Router über den WLC, Art.-Nr. 61630
Management	LANCOM WLC AP Upgrade +25 Option, ermöglicht die Verwaltung von 25 weiteren Access Points/WLAN-Router über den WLC, Art.-Nr. 61631
Geeignetes Zubehör	
Dokumentation	LANCOM LCOS Referenzhandbuch (DE) Online auf <a href="http://www.lancom-systems.de/publikationen/">http://www.lancom-systems.de/publikationen/</a>
Artikelnummern	
LANCOM WLC-4025+	61378
LANCOM WLC-4025+ (UK)	61379

LANCOM, LANCOM Systems und LCOS sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Änderungen vorbehalten. Keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen. 3/2012