



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

LANCOM WLC-4100

Zentrales "zero touch" Management für 100 LANCOM Access Points und WLAN Router, über Option erweiterbar auf 1000

- "Smart Controller" für anwendungs- oder benutzerbezogene WLAN-Netzwerke
- Zentrale Firmwareverteilung und Management der Access Points
- Automatische Erkennung, Konfiguration und Kanaluweisung von Access Points
- Überwachen und Sicherstellen der Sicherheits- und QoS-Richtlinien
- Skalierbarkeit und Erweiterbarkeit bei mehreren Controllern, inkl. Redundanz
- Einzigartige Betriebssicherheit verhindert den "Single-Point-of-Failure"
- Umfangreiche VLAN-, RADIUS- und 802.1x/EAP-Funktionen
- Maximale Performance mit 802.11n Access Points

Der LANCOM WLC-4100 WLAN Controller eignet sich durch seine Erweiterbarkeit und Kaskadierbarkeit für mittlere und große WLAN-Installationen von hundert bis zu tausend WLAN Access Points, wie sie bei vielen Unternehmen und öffentlichen Einrichtungen, z. B. Universitäten oder Krankenhäusern, in großen Filialketten und Firmenzentralen anzutreffen sind. Der Controller sorgt für eine einfache Installation, einen sicheren Betrieb und ermöglicht dabei die Mehrfachnutzung einer einzigen WLAN-Infrastruktur für unterschiedliche Anwendungen und Benutzergruppen.

Maximale Einfachheit.

Der Controller-Betrieb bietet ein Optimum an einfacher Bedienung – einfach einen neuen Access Point "dazustecken", und der Controller übernimmt die Einrichtung, Kanalzuweisung sowie die Umsetzung und Überwachung der passenden WLAN-Sicherheitsrichtlinie. LANCOM WLAN Controller eignen sich ideal für eine mehrfache Nutzung der WLAN-Infrastruktur – zum Beispiel für Daten, Voice-over-WLAN und Gastzugänge. Als "Smart Controller" können sie die Daten je nach Anwendung oder sogar pro Benutzer unterschiedlich weiterleiten – ob direkt in das LAN gebridged für höchste Performance, oder getrennt vom LAN in ein eigenes VLAN für WLAN-Gastzugänge. Durch die flexiblen Auskopplungsmöglichkeiten ist der Controller "11n Ready", da das kostenspielige LAN-Infrastruktur-Upgrade vermieden wird und der WLAN Controller nicht zum zentralen Flaschenhals wird. Auch entfernte Standorte lassen sich einfach und bequem in das zentrale Management einbinden, eine beliebige IP-Anbindung reicht aus.

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 oder Voice-over-IP, 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.

Die automatischen Kanaleinstellungen verbinden optimale Performance mit einfachster Bedienung. Innovative Anwendungen wie Voice-over-WLAN werden durch schnelle Roaming-Zeiten und Ende-zu-Ende-Übertragung von Quality-of-Service-Informationen unterstützt.

Eine weitere Besonderheit der LANCOM WLAN Controller sind die umfangreichen Redundanzkonzepte. Nicht nur lassen sich mehrere Controller beliebig zu redundanten Clustern mit automtischer Lastverteilung zusammenfassen, sondern bereits bei nur einem Controller wird – anders als bei vielen zentralistischen Systemen – 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 wird ein standortübergreifendes WLAN-Management möglich, bei dem ein jederzeit verfügbarer Produktivbetrieb ohne Kompromittierung der Sicherheit garantiert ist - selbst bei Ausfall der Controller-Verbindung.

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 2 Kanalwahl verbunden)
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support, IEEE 802.11d Support
VLAN	VLAN-ID einstellbar pro Schnittstelle, WLAN SSID, Punkt-zu-Punkt-Verbindung und Routing-Kontext (4.094 IDs)
Multi-SSID	Nutzung von bis zu 8 unabhängigen WLAN-Netzen gleichzeitig pro WLAN-Interface
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
WLAN-Betriebsarten	WLAN Access Point im Infrastruktur-Modus
*) Hinweis	Je nach verwendeten Access Points
WLAN Controller	
Anzahl gemanagter Geräte	Bis zu 100 LANCOM Access Points und WLAN Router können - auch in beliebiger Kombination - durch den LANCOM WLAN Controller zentral gemanaged werden. Über Erweiterungsoptionen können bis zu 1000 LANCOM WLAN Access Points und WLAN Router gemanaged werden. Weitere Kapazitätserweiterungen sind über das Clustering mehrerer Controller möglich.
Smart Controller Technologie	Der LANCOM WLAN Controller unterstützt pro Funkzelle / SSID die unterschiedliche Auskopplung der Nutzdaten: <ul style="list-style-type: none"> ■ 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) *Feature in Vorbereitung
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 Authentisierung 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.
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 Webservers 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 Kanalzuteilung 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)

WLAN Controller	
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).
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 16 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-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: <ul style="list-style-type: none"> ■ LANCOM LANconfig ■ LANCOM LANmonitor ■ LANCOM WLANmonitor
Unterstützte Access Points und WLAN-Router	
Indoor	<ul style="list-style-type: none"> ■ 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
Outdoor	<ul style="list-style-type: none"> ■ LANCOM OAP-54 Wireless ■ LANCOM OAP-54-1 Wireless ■ LANCOM OAP-310 Wireless

Unterstützte Access Points und WLAN-Router	
Industrial	<ul style="list-style-type: none"> ■ LANCOM IAP-54 Wireless ■ LANCOM XAP-40-2 Wireless
UMTS/HSPDA	<ul style="list-style-type: none"> ■ LANCOM 3850 Wireless
WLAN-Router und IADS	<ul style="list-style-type: none"> ■ LANCOM 1811n Wireless ■ LANCOM 1821n Wireless ■ LANCOM 1821+ Wireless ADSL ■ LANCOM 1823 VoIP
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
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-Queueing 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 (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
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
VPN-Redundanz	Ansteuerung von bis zu 16 redundanten VPN-Gateways für Hochverfügbarkeit oder Lastverteilung
Leitungsüberwachung	Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling

VPN	
Anzahl der VPN-Tunnel	5 IPsec-Verbindungen gleichzeitig aktiv, unbegrenzte Anzahl konfigurierbarer Gegenstellen. 5 Tunnel insgesamt gleichzeitig aktiv bei Kombination von IPsec- mit PPTP-Tunneln
Hardware-Beschleuniger	Integrierter Hardwarebeschleuniger für die 3-DES/AES Ver- und Entschlüsselung
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
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. 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)
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP
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
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
VPN-Backup	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)
Algorithmen	3-DES (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 für höhere IPsec-Durchsatzraten mittels LZS- oder Deflate-Komprimierung
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)	
1416 Byte Framegröße UDP	330 Mbit/s
256 Byte Framegröße UDP	63 Mbit/s
IMIX	103 Mbit/s
Firewall-Durchsatz (max.)	
1518 Byte Framegröße UDP	560 Mbit/s
256 Byte Framegröße UDP	97 Mbit/s
Routingfunktionen	
Router	IP- und NetBIOS/IP-Multiprotokoll-Router
Advanced Routing and Forwarding	Separates Verarbeiten von 64 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
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 (Wildcard) im Namen
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)
LAN-Protokolle	
IP	ARP, Proxy ARP, BOOTP, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (Server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP, VLAN

WAN-Protokolle	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC oder PNS) und Plain Ethernet (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IP
Schnittstellen	
Ethernet Ports	4 individuelle Ports, 10/100/1000 Mbit/s Ethernet
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, WAN, Monitor-Port, Aus). LAN Ports können als Switch oder isoliert betrieben werden. Am WAN-Port können externe DSL-Modems oder Netzabschlussrouter inkl. 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) oder seriellen Geräten (COM-Port-Server); bidirektionaler Datenaustausch möglich (max. 480 Mbit/s)
Management	
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 oder globale Voreinstellungen des Konfigurationsprogramms. 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 der LANCOM managed Switches
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 entsprechenden 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 Switches
WLANmonitor	Monitoring-Applikation für Microsoft Windows zur Visualisierung und Überwachung von LANCOM Wireless LAN Installationen, inkl. Rogue AP und Rogue Client-Visualisierung
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)
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 Seiten-Reiter. Assistenten für Grundkonfiguration, Sicherheit, Internetzugang, LAN-LAN-Kopplung. Online Hilfe zu Parametern im LCOS-Menübaum
Geräte-Syslog	Syslog-Speicher im RAM (Größe abhängig von Speicherausstattung), in dem Ereignisse zur Diagnose festgehalten werden. Werkseitig 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
Fernwartung	Fernkonfiguration über Telnet/SSL, 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. 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)
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
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
SNMP	SNMP-Management via SNMP V2, 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 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, Netzwerkanschlüsse auf der Frontseite
Anzahl Lüfter	1
Konformitätserklärungen	
CE	EN 55022, EN 55024, EN 60950
Lieferumfang	
Handbuch	Gedrucktes Benutzerhandbuch (DE, EN)
CD	CD mit Firmware, Management-Software (LANconfig, LANmonitor, WLANmonitor) und Dokumentation
Kabel	Seriell Konfigurationskabel, 1,5 m
Kabel	1 Ethernet-Kabel, 3m
Kabel	Kaltgeräte-Netzkabel
Support	
Garantie	3 Jahre Support über Hotline und Internet KnowledgeBase
Software-Updates	Regelmäßige kostenfreie Updates (LCOS Betriebssystem und Management-Tools) via Internet
Konfigurations-Service	1 LANCOM Config Service Ticket im Lieferumfang enthalten
Optionen	
Service	LANCOM Service Option (24h-Vorabaustausch innerhalb Deutschlands, 4 Jahre Garantie, nicht für PoE Power Injector), Art.-Nr. 61401
Public Spot	LANCOM WLC-PSPOT Option, Art.-Nr. 61624
Geeignetes Zubehör	
Dokumentation	LANCOM LCOS Referenzhandbuch (DE), Art.-Nr. 61702
Artikelnummern	
LANCOM WLC-4100	61369
LANCOM WLC-4100 (UK)	61377

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. 10/09