



## LANCOM WLC-4025+

Leistungsstarker WLAN-Controller für das zentrale Management von 25 bis zu 100 Access Points und WLAN-Routern

Der LANCOM WLC-4025+ ist ein leistungsfähiger WLAN-Controller mit zentralem WLAN-Management für Installationen mit bis zu 100 Access Points. Dadurch erfolgt die Verteilung von Firmware-Updates und Konfigurationen über nur ein Gerät - eine massive Arbeitserleichterung & Zeitersparnis für jeden Administrator.

- › Zentraler Firmware Rollout, Monitoring & Management von 25 bis zu 100 Access Points und WLAN-Routern
- › Zero-Touch Deployment von angeschlossenen WLAN-Geräten
- › Optimierter Roaming-Verhalten von WLAN-Clients durch IEEE 802.11r und OKC
- › Umfangreiche VLAN-, RADIUS- und IEEE 802.1X/EAP-Funktionen
- › Höchste Betriebssicherheit ohne Single Point auf Failure
- › Dynamische WLAN-Optimierung dank Unterstützung von LANCOM Active Radio Control (ARC)
- › Hochverfügbarkeit von WLAN-Infrastrukturen durch High Availability Clustering Option

# LANCOM WLC-4025+

## Zentraler Firmware Rollout, Monitoring & Management

Mit dem LANCOM WLC-4025+ können bis zu 100 Access Points und WLAN-Router lokal und zentral vollautomatisch konfiguriert und gesteuert werden - eine massive Zeitersparnis und Arbeitserleichterung für den Netzwerkadministrator. Damit bietet der WLAN-Controller eine einheitliche Netzwerk-Kontrolle, Sicherheit und Zuverlässigkeit.

## Zero-Touch Deployment

Schnelle und einfache Netzwerkintegration neuer Access Points sowie automatische Konfigurationsvergabe - ohne manuelle Konfiguration. Nach Netzwerkauthentifizierung vergibt der LANCOM WLC-4025+ an das WLAN-Gerät unmittelbar die geeignete Konfiguration.

## Optimiertes Roaming-Verhalten von WLAN-Clients

LANCOM WLAN-Controller stellen die Kommunikation unter den verwalteten Access Points und WLAN-Routern sicher. Somit werden Clients beim Wechsel zwischen zwei Funkfeldern effizient von einem an das andere WLAN-Gerät übergeben - ohne Verbindungsabbrüche.

## VLAN-, RADIUS- und IEEE 802.1X/EAP-Funktionen

Dank umfangreicher Virtualisierungs- und Sicherheitsfunktionen lassen sich WLAN-Netze sehr effizient und gemäß der firmeneigenen Security Policies gestalten. Die integrierte VLAN-Funktion ermöglicht die Trennung mehrerer sicher getrennter WLAN-Netze in nur einer Infrastruktur. Professionelle Sicherheitsfunktionen erlauben dem Administrator darüber hinaus, den Netzwerkzugriff nur für autorisierte Clients zu erlauben.

## Höchste Betriebssicherheit

Das LANCOM Smart Controller-Prinzip erlaubt höchste Betriebssicherheit: während die Verwaltungsdaten über den Controller laufen, werden Verkehrsdaten vom Client direkt zum Access Point und von dort aus direkt zum Router geschickt. Fällt ein Controller nun aus, schaltet der Access

Point auf „Stand-alone-Betrieb“ um die Kommunikation zwischen Client und Access Point bleibt weiterhin erhalten. Somit entstehen im Arbeitsalltag keine unproduktiven Zeiten, weil Mitarbeiter nicht ins Netz gelangen oder weil WLAN-gesteuerte Produktionsanlagen ausfallen.

## Dynamische Funkfeld-Optimierung dank Active Radio Control

Der LANCOM WLC-4025+ unterstützt das WLAN-Optimierungskonzept LANCOM Active Radio Control. Durch die intelligente Kombination aus innovativen, im Betriebssystem LCOS enthaltenen Features wie Band Steering, Adaptive Noise Immunity, RF Optimization und Client Steering wird die Leistungsfähigkeit des WLANs nachhaltig gesteigert und der Administrator beim professionellen WLAN-Management unterstützt.

## Hochverfügbarkeit

In Kombination mit der LANCOM High Availability Clustering Option werden mehrere WLAN-Controller zu einer hochverfügbaren Gerätegruppe gruppiert. Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem WLC vorgenommen werden, automatisch auf die anderen WLCs des Clusters übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss - für den Administrator eine enorme Zeitersparnis.

## Upgrade der managebaren WLAN-Geräte

Mit der LANCOM WLC Upgrade Option wird die Anzahl der vom Controller verwalteten Access Points oder WLAN-Router erhöht. So bleibt Ihr Netzwerk optimal skalierbar – ohne zusätzliche Hardwarekomponenten.

## Einfach aufrüsten

Die LANCOM Software-Optionen machen aus einem einfachen Netzwerk eine auf individuelle Bedürfnisse abgestimmte und kostengünstige Lösung. Einmal auf die vorhandene Hardware aufgespielt, erweitern sie das Netzwerk um die gewünschte Funktion. Der Vorteil: Es sind

# LANCOM WLC-4025+

keine weiteren Hardware-Komponenten erforderlich. Das reduziert die Anschaffungskosten und den Administrationsaufwand des gesamten Netzwerks. Ein echter Mehrwert im Hinblick auf die Zukunftsfähigkeit, denn dank der Optionen wird das Netzwerk zu einer einzigartigen, skalierbaren Netzwerklösung.

## LANCOM WLC-4025+

LCOS 10.12

WLAN Profileinstellungen*	
Funkkanäle 5 GHz	Bis zu 26 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS-Kanalwahl verbunden)
Funkkanäle 2,4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (landesspezifische Einschränkungen möglich)
Gleichzeitige WLAN Clients	Je nach verwendeten Access Points
IEEE 802.11u	Gemanageten LANCOM Access Points ermöglicht der WLAN-Standard IEEE 802.11u (Hotspot 2.0) einen vom mobilen Benutzer unbemerkten Übergang vom Mobilfunknetz zu WLAN Hotspots. Authentifizierungsmethoden mit SIM-Kartendaten, Zertifikaten oder Benutzername und Passwort ermöglichen eine automatische, verschlüsselte Anmeldung an Hotspots von Roaming-Partnern - ganz ohne aufwändige Eingabe von Login-Daten.
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support mit optionaler Zuordnung eines ARF-Kontextes, IEEE 802.11d Support
Opportunistic Key Caching	Opportunistic Key Caching ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Bei Controller-basierten WLAN-Installationen mit IEEE 802.1X-Authentifizierung werden die Zugangsschlüssel der Clients zwischengespeichert und vom WLAN-Controller automatisch an alle verwalteten Access Points weitergegeben
Fast Roaming	Basierend auf WLAN-Standard IEEE 802.11r, ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Dies wird in Controller-basierten WLAN-Installationen mit IEEE 802.1X-Authentifizierung oder Pre-Shared Key realisiert, indem die Zugangsschlüssel der Clients zwischengespeichert und automatisch an die verwalteten Access Points weitergegeben werden.
Sicherheit	IEEE 802.11i / WPA2 mit Passphrase (WPA2-Personal) oder IEEE 802.1X (WPA2-Enterprise) mit hardwarebeschleunigtem AES, Closed Network, WEP64, WEP128, WEP152, User Authentication, IEEE 802.1X /EAP, LEPS, WPA1/TKIP
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
Auto-WDS*	Auto-WDS ermöglicht die kabellose Integration von Access Points in die vorhandene WLAN-Infrastruktur, inklusive Verwaltung durch WLAN-Controller.
Space Time Block Coding (STBC)*	Codierverfahren nach IEEE 802.11n. Bei der STBC-Codierung wird ein Datenstrom zur Übertragung in Datenblöcke codiert, so dass in einem MIMO-System Verbesserungen der Empfangsbedingungen entstehen.
Low Density Parity Check (LDPC)*	Low Density Parity Check (LDPC) ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standardmethode zur Fehlerkorrektur Convolution Coding (CC) und optional die effektivere Methode Low Density Parity Check (LDPC).
*) Hinweis	Je nach verwendeten Access Points
WLAN-Sicherheit	
Sicherheitsverfahren	IEEE 802.1X (WPA2-Enterprise), IEEE 802.11i (WPA2-Personal), Wi-Fi Certified™ WPA2™, WPA, WEP, IEEE 802.11w (Protected Management Frames), LEPS (LANCOM Enhanced Passphrase Security)
Verschlüsselungsalgorithmen	AES:CCMP (Advanced Encryption Standard mit Counter Mode mit Cipher Block Chaining Message Authentication Code Protocol), TKIP (Temporal Key Integrity Protocol), RC4 (nur bei WEP)
EAP-Typen (Authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST
Radius/EAP-Server	Benutzerverwaltung von MAC-Adressen, Bandbreitenbegrenzung, Passphrase, VLAN je Benutzer, Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP oder MS-CHAPv2
Sonstiges	WLAN-Protokollfilter (ACL), IP-Redirect von empfangenen Paketen aus dem WLAN, IEEE 802.11X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)
Sonstiges	IEEE 802.11X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)
LANCOM Active Radio Control	
Client Steering*	Steuerung von WLAN Clients auf den sinnvollsten Access Point
Band Steering	Steuerung von 5 GHz Clients auf dieses leistungsstarke Frequenzband
Managed RF Optimization*	Auswahl optimaler WLAN-Kanäle durch den Administrator

## LANCOM WLC-4025+

LCOS 10.12

LANCOM Active Radio Control	
Adaptive Noise Immunity	Immunität vor Störsignalen im WLAN
Spectral Scan	Überprüfen des WLAN-Funkspektrum auf Störquellen
Adaptive RF Optimization	Dynamische Auswahl des besten WLAN-Kanals
Airtime Fairness	Verbesserte Ausnutzung der WLAN-Bandbreite
*) Hinweis	Je nach verwendeten Access Points. Band-/Client-Steering ist in der US-Variante nicht verfügbar.
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 IEEE 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, E-Mail-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.
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 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, E-Mail, 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).

## LANCOM WLC-4025+

LCOS 10.12

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 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 IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP oder MS-CHAP v2
RADIUS/EAP Proxy pro SSID	Proxy-Betriebsart für externe RADIUS/EAP-Server (Forwarding und Realm Handling) pro SSID konfigurierbar
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.
LED Steuerung	LEDs der verwalteter WLAN-Geräte lassen sich über Profile abschalten
CA-Hierarchie	Die Certificate Authority (CA) kann bei WLAN-Controllern hierarchisch strukturiert werden. Somit können Access Points zwischen den verschiedenen WLAN-Controllern wechseln, ohne dass es zu Zertifikatskonflikten kommt. Certificate Revocation Lists (CRLs) können untereinander ausgetauscht werden
Load Balancing	Bei der Nutzung von mehreren WLAN-Controllern werden die Access Points gleichmässig auf die verschiedenen WLAN-Controller verteilt um eine optimale Lastverteilung zu gewährleisten. Bei Ausfall eines WLAN-Controllers verteilen sich die Access Points automatisch neu, ist er wieder verfügbar wird auch die Rückverteilung automatisch durchgeführt
Backup	WLAN-Controllern kann eine Priorität zugewiesen werden, was einen Betrieb im Hot-Standby ermöglicht. Access Points wechseln automatisch zu dem WLAN-Controller mit der höchsten Priorität
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	IEEE 802.11e / WME: Automatisches VLAN-Tagging (IEEE 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 unterstützen WLAN Clients vorgegeben werden. Darüber hinausgehende Assoziierungsanfragen werden abgelehnt.
Automatischer Konfigurationsabgleich (Config Sync)*	Durch die Zusammenfassung mehrerer Einzelgeräte zu einer Gerätegruppe (Cluster) können Konfigurationsänderungen, die an einem Gerät vorgenommen werden, automatisch auf die anderen Cluster-Geräte übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss (Config Sync).

## LANCOM WLC-4025+

LCOS 10.12

WLAN-Controller	
Management Software	Im Lieferumfang enthalten: - LANCOM LANconfig - LANCOM LANmonitor - LANCOM WLANmonitor
*)	Nur mit WLC Clustering XL Option
Unterstützte Access Points und WLAN-Router	
Indoor	<ul style="list-style-type: none"> <li>■ LANCOM L-151gn Wireless, LANCOM L-151E Wireless, LANCOM L-54g Wireless, LANCOM L-54ag Wireless, LANCOM L-54 dual Wireless</li> <li>■ LANCOM L-305agn Wireless, LANCOM L-310agn Wireless, LANCOM L-315agn dual Wireless</li> <li>■ LANCOM L-320agn Wireless, LANCOM L-320agn Wireless (white), LANCOM L-321agn Wireless, LANCOM L-322agn dual Wireless, LANCOM L-322E Wireless, LANCOM L-330agn dual Wireless</li> <li>■ LANCOM L-451agn Wireless, LANCOM L-452agn dual Wireless, LANCOM L-460agn dual Wireless</li> <li>■ LANCOM LN-830acn dual Wireless, LANCOM LN-830E Wireless, LANCOM L-822acn dual Wireless, LANCOM L-1302acn dual Wireless, LANCOM L-1310acn dual Wireless, LANCOM LN-860, LANCOM LN-862</li> <li>■ LANCOM LN-1700, LANCOM LN-1702</li> </ul>
Outdoor	<ul style="list-style-type: none"> <li>■ LANCOM OAP-54 Wireless, LANCOM OAP-54-1 Wireless</li> <li>■ LANCOM OAP-310 Wireless</li> <li>■ LANCOM OAP-321, LANCOM OAP-321-3G</li> <li>■ LANCOM OAP-382, LANCOM OAP-322</li> <li>■ LANCOM OAP-821, LANCOM OAP-822, LANCOM OAP-830</li> </ul>
Industrial	<ul style="list-style-type: none"> <li>■ LANCOM IAP-54 Wireless</li> <li>■ LANCOM XAP-40-2 Wireless</li> <li>■ LANCOM IAP-321, LANCOM IAP-321-3G, LANCOM IAP-322</li> <li>■ LANCOM IAP-821, LANCOM IAP-822</li> </ul>
UMTS/HSPDA	<ul style="list-style-type: none"> <li>■ LANCOM 1780EW-4G, LANCOM 1780EW-3G, LANCOM 1780EW-4G+</li> <li>■ LANCOM 3850 Wireless</li> </ul>
WLAN-Router und IADs	<ul style="list-style-type: none"> <li>■ LANCOM 1781VAW, LANCOM 1781AW, LANCOM 1781EW(+)</li> <li>■ LANCOM 1811n Wireless, LANCOM 1821n Wireless, LANCOM 1823 VoIP, LANCOM 1821+ Wireless ADSL</li> <li>■ LANCOM 1783VAW, LANCOM 883 VoIP</li> </ul>
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.
Layer 2-Funktionen	
VLAN	4.096 IDs nach IEEE 802.1q, dynamische Zuweisung, Q-in-Q Tagging
Quality of Service	WME nach IEEE 802.11e, Wi-Fi Certified™ WMM®
Bandbreitenlimitierungen	pro SSID, pro WLAN-Client
Multicast	IGMP-Snooping
Protokolle	Ethernet über GRE-Tunnel (EoGRE), ARP-Lookup, LLDP, DHCP Option 82, IPv6-Router-Advertisement-Snooping, DHCPv6-Snooping, LDRA (Lightweight DHCPv6 Relay Agent), Spanning Tree, Rapid Spanning Tree, ARP, Proxy ARP, BOOTP, DHCP, LACP
Layer 3-Funktionen	
Firewall	Stateful Inspection Firewall mit Paketfilterung, erweitertem Port-Forwarding, N:N IP-Adressumsetzung, Paket-Tagging, unterschiedlichen Aktionen und unterschiedlichen Benachrichtigungen
Quality of Service	Traffic Shaping, Bandbreitenreservierung, DiffServ/TOS, Paketgrößensteuerung, Layer 2-in-Layer 3-Tagging

## LANCOM WLC-4025+

LCOS 10.12

Layer 3-Funktionen	
Sicherheit	Intrusion Prevention, IP-Spoofing, Access-Control-Listen, Denial-of-Service Protection, detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung, URL-Blocker, Passwortschutz, programmierbarer Reset-Taster
PPP-Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAPv2
Hochverfügbarkeit/Redundanz	VRRP (Virtual Router Redundancy Protocol), Analog/GSM-Modem-Backup
Router	IPv4-, IPv6-, NetBIOS/IP-Multiprotokoll-Router, IPv4/IPv6 Dual Stack
Router-Virtualisierung	ARF (Advanced Routing und Forwarding) mit bis zu 16 Kontexten
IPv4-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy, Dynamic DNS-Client, DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection, NetBIOS/IP-Proxy, NTP-Client, SNTP-Server, Policy-based Routing, Bonjour-Proxy, RADIUS
IPv6-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DHCPv6-Client, DHCPv6-Server, DHCPv6-Relay, DNS-Client, DNS-Server, Dynamic DNS-Client, NTP-Client, SNTP-Server, Bonjour-Proxy, RADIUS
IPv6-kompatible LCOS-Anwendungen	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, Firewall, RAS-Einwahl
Dynamische Routing-Protokolle	RIPv2, BGPv4, OSPFv2
IPv4-Protokolle	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, NetBIOS, PPPoE (Server), RADIUS, RADSEC (Secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+
IPv6-Protokolle	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, Syslog, SNMPv1,v2c,v3
WAN-Betriebsarten	VDSL, ADSL1, ADSL2 oder ADSL2+ jeweils auch mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)
WAN-Protokolle	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC oder PNS), L2TPv2 (LAC oder LNS) und IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IP(v6)oE (Autokonfiguration, DHCPv6 oder Statisch)
Tunnelprotokolle (IPv4/IPv6)	6to4, 6in4, 6rd (statisch und über DHCP), Dual Stack Lite (IPv4-in-IPv6-Tunnel)
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 und Site-to-Site-Verbindungen. 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-(MPPE) und L2TPv2-Tunneln, 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, IKEv2	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate (RSA-Signature, Digital-Signature)
Smart Certificate	Komfortable Erstellung von digitalen X.509 Zertifikaten mittels einer eigenen Zertifizierungsstelle (SCEP-CA) via Weboberfläche oder SCEP.
Zertifikate	Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL. 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 Zertifikathierarchie
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP pro Zertifikathierarchie
OCSP Client	Prüfen von X.509-Zertifikaten anhand von OCSP (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



## LANCOM WLC-4025+

LCOS 10.12

VPN	
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), RSA (1024-4096 Bit) und CAST (128 Bit). OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. MD-5, SHA-1 oder SHA-256 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 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
IPv4 VPN	Kopplung von IPv4 Netzwerken
IPv4 VPN über IPv6 WAN	Nutzung von IPv4 VPN über IPv6 WAN-Verbindungen
IPv6 VPN	Kopplung von IPv6 Netzwerken
IPv6 VPN über IPv4 WAN	Nutzung von IPv6 VPN über IPv4 WAN-Verbindungen
RADIUS	RADIUS Authorization und Accounting, Auslagerung von VPN-Konfigurationen in externem RADIUS-Server bei IKEv2, RADIUS CoA (Change of Authorization)
VPN-Durchsatz (max., AES)	
1418 Byte Framegröße UDP	337 MBit/s
Firewall-Durchsatz (max.)	
1518 Byte Framegröße UDP	643 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/Ratingsserver*	Weltweit redundante Ratingsserver 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
URL-Prüfung*	Datenbankbasierte Online-Prüfung von Webseiten (HTTP/HTTPS). HTTPS-Webseiten werden durch die Entnahme von angesteuerten DNS-Namen aus HTTPS-Serverzertifikaten oder durch "Reverse DNS lookup" der IP-Adresse geprüft und ggfs. blockiert.
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. Werkseitig 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

## LANCOM WLC-4025+

LCOS 10.12

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(S)-Verkehrs für maximal 400 unterschiedliche IP-Adressen im LAN
*) Hinweis	Die Kategorisierung erfolgt durch IBM. Die jederzeitige Richtigkeit der Kategorisierungen können weder IBM noch LANCOM garantieren.
***) Hinweis	Die Override-Funktionalität steht nur für HTTP-Seiten zur Verfügung.
VoIP	
SIP ALG	SIP ALG (Application Layer Gateway) agiert als Proxy für SIP. Automatische Öffnung der notwendigen Ports für Sprachdaten. Automatische Adressumsetzung (STUN unnötig).
LAN-Protokolle	
IPv4	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
Schnittstellen	
Ethernet Ports	4 individuelle Ports, 10/100/1000 MBit/s Ethernet. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden
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); 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
Hardware Management und Monitoring	
Management	LANCOM Management Cloud, LANconfig, WEBconfig, WLAN-Controller, LANCOM Layer 2 Management (Notfall-Management)
Management-Funktionen	Alternative Boot-Konfiguration, automatisches Software-Update über LANconfig, individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren, RADIUS- und RADSEC-Benutzerverwaltung, Fernwartung (über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbar über) SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, alternative Steuerung der Zugriffsrechte durch TACACS+, Scripting, zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst
FirmSafe	Zwei speicherbare Firmware-Versionen im Gerät, inkl. Testmodus bei Firmware-Updates
Monitoring	LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring-Funktionen	Geräte-SYSLOG, SNMPv1,v2c,v3 inkl. SNMP-TRAPS, sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, interne Loggingbuffer für SYSLOG und Firewall-Events
Monitoring-Statistiken	Umfangreiche Ethernet-, IP- und DNS-Statistiken, SYSLOG-Fehlerzähler, Accounting inkl. Export von Accounting-Informationen über LANmonitor und SYSLOG, Layer-7-Anwendungserkennung inkl. anwendungsbezogenes Erfassen des verursachten Traffics
iPerf	iPerf ermöglicht es den Datendurchsatz von IP-Netzwerken zu testen (integrierter Client und Server)

## LANCOM WLC-4025+

LCOS 10.12

Management und Monitoring	
SLA-Monitor (ICMP)	Performance-Überwachung von Verbindungen
SD-WLAN	SD-WLAN - Automatische WLAN-Konfiguration über die LANCOM Management Cloud
SD-LAN	SD-LAN - Automatische LAN-Konfiguration über die LANCOM Management Cloud
SD-WAN	SD-WAN - Automatische WAN-Konfiguration über die LANCOM Management Cloud
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
Leistungsaufnahme (max.)	30 Watt
Konformitätserklärungen*	
CE	EN 60950-1, EN 55022, EN 55024
FCC	FCC Part 15, Class B mit FTP-Verkabelung
Draeger-Validierung	Bestätigte Kompatibilität zu Dräger Infinity OneNet Installationen mit Dräger Patientenmonitoren im medizinischen Umfeld per Multicast im WLAN
IPv6	IPv6 Ready Gold
Herkunftsland	Made in Germany
*) Hinweis	Auf unserer Website <a href="http://www.lancom-systems.de">www.lancom-systems.de</a> finden Sie die vollständigen Erklärungen zur Konformität auf der jeweiligen Produktseite
Lieferumfang	
CD/DVD	Datenträger mit Management Software (LANconfig, LANmonitor, LANCAPI) und LCOS-Dokumentation
Kabel	Serielltes Konfigurationskabel, 1,5 m
Kabel	Ethernet-Kabel, 3 m
Kabel	Kaltgeräte-Netzkabel
Support	
Garantie	3 Jahre Support
Software-Updates	Regelmäßige kostenfreie Updates (LCOS Betriebssystem und LANtools) via Internet
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
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
LANCOM Warranty Basic Option L	Option zur Verlängerung der Herstellergarantie von 3 auf 5 Jahre, Art.-Nr. 10712
LANCOM Warranty Advanced Option L	Option zur Verlängerung der Herstellergarantie von 3 auf 5 Jahre und einen Vorabaustausch bei Hardware-Defekt, Art.-Nr. 10717
LANCOM Public Spot XL	Hotspot-Option für LANCOM WLC-4100, WLC-4025(+) sowie LANCOM 9100(+) VPN und LANCOM 7100(+) VPN zur User-Authentifizierung (empfohlen bis zu 2.500), flexible Zugangsmöglichkeiten (Voucher, E-Mail, SMS), inkl. komfortablem Einrichtungs-Assistent, Art.-Nr. 61624
LANCOM Public Spot PMS Accounting Plus	Erweiterung der LANCOM Public Spot (XL) Option für die Anbindung an Hotelabrechnungssysteme mit FIAS-Schnittstelle (wie Micros Fidelio) zur Authentifizierung und Abrechnung von Gastzugängen, für 178x-/19xx-Router, WLCs und aktuelle Central Site Gateways, Art.-Nr. 61638

## LANCOM WLC-4025+

LCOS 10.12

Optionen	
LANCOM WLC AP Upgrade +10	LANCOM WLC AP Upgrade +10 Option, ermöglicht die Verwaltung von 10 weiteren Access Points/WLAN-Router über den WLC, Art.-Nr. 61630
LANCOM WLC AP Upgrade +25	LANCOM WLC AP Upgrade +25 Option, ermöglicht die Verwaltung von 25 weiteren Access Points/WLAN-Router über den WLC, Art.-Nr. 61631
LANCOM Management Cloud	
LANCOM Management Cloud	LANCOM LMC-D-1Y Lizenz (1 Jahr), ermöglicht für ein Jahr die Verwaltung eines Gerätes der Kategorie D mit der LANCOM Management Cloud, Art.-Nr. 50109
LANCOM Management Cloud	LANCOM LMC-D-3Y Lizenz (3 Jahre), ermöglicht für drei Jahre die Verwaltung eines Gerätes der Kategorie D mit der LANCOM Management Cloud, Art.-Nr. 50110
LANCOM Management Cloud	LANCOM LMC-D-5Y Lizenz (5 Jahre), ermöglicht für fünf Jahre die Verwaltung eines Gerätes der Kategorie D mit der LANCOM Management Cloud, Art.-Nr. 50111
Artikelnummer(n)	
LANCOM WLC-4025+ (EU)	61378
LANCOM WLC-4025+ (UK)	61379
LANCOM WLC-4025+ (US)	61384
LANCOM WLC High Availability Clustering XL Option	61636

