



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

LANCOM OAP-322

Dual Radio Outdoor Access Point nach 802.11n für professionelle WLAN-Anwendungen im Freien

- Vier externe Antennen für den parallelen Funkbetrieb in 2,4 und 5 GHz
- Optimierung der Netzlast im 2,4 GHz Frequenzband durch Band Steering
- Anschlüsse für Gigabit Ethernet mit Power over Ethernet nach IEEE 802.3af und Fast Ethernet
- Optional mit externer Spannungsversorgung für 10 - 28V
- Robustes IP66-Schutzgehäuse zuverlässig auch bei extremen Temperaturen (-30°C bis +70°C)
- Komfortable Einbindung externer Nutzer durch Public Spot Option

Der Dual Radio Outdoor Access Point LANCOM OAP-322 ist ideal für professionelle WLAN-Anwendungen im Freien, zum Beispiel zur Einrichtung von Hotspot-Szenarien. Dank zwei WLAN-Funkmodulen nach IEEE 802.11n für den parallelen Betrieb der 2,4 GHz- und 5 GHz-Frequenzbänder sowie dem robusten IP66-Schutzgehäuse für extreme Einsatzbedingungen sind flexible Einsatzmöglichkeiten abbildbar. Zudem lässt sich der LANCOM OAP-322 durch die Unterstützung von Power over Ethernet nach IEEE 802.3af auch abseits der Stromversorgung komfortabel und zuverlässig betreiben.

Mehr Flexibilität.

Der LANCOM OAP-322 bietet flexible Einsatzmöglichkeiten im Freien: Ob die komfortable Einrichtung moderner Outdoor-Hotspots mit der LANCOM Public Spot Option, die professionelle WLAN-Ausleuchtung von Freiflächen oder die WLAN-Anbindung an das Firmennetzwerk über Punkt-zu-Punkt-Strecken. Dabei lässt sich das Gerät sowohl autark als standalone Access Point oder gemanagt über einen WLAN Controller betreiben. Auch für die Wahl der Stromversorgung bietet das Gerät flexible Optionen: Je nach örtlichen Gegebenheiten kann der LANCOM OAP-322 per Power over Ethernet nach IEEE 802.3af auch abseits der Stromversorgung oder alternativ mit externer Spannungsversorgung für 10 – 28 V versorgt werden. Dank des robusten IP66-Schutzgehäuses ist das Gerät für den Einsatz in extremen Umgebungen mit Temperaturen zwischen -30 und +70°C geeignet.

Mehr Sicherheit.

LANCOM gewährleistet den Einsatz höchster Sicherheitsstandards durch die Unterstützung umfangreicher Verschlüsselungs- und Authentifizierungsmechanismen wie 802.11i, 802.1x oder WPA2. Mithilfe von Multi-SSID und Protokollfiltern können bis zu 16 Benutzergruppen separate Funknetze zugewiesen werden. Auch Hotspots im Freien lassen sich mit dem LANCOM OAP-322 und der optional erhältlichen LANCOM Public Spot Option sicher realisieren: eine flexibel konfigurierbare Benutzerauthentifizierung stellt sicher, dass sich nur autorisierte Gäste am Hotspot anmelden können. Ausgereifte Quality-of-Service-Funktionen und die Bandbreitenlimitierung sorgen dafür, dass unternehmenskritische Anwendungen stets priorisiert werden und leisten somit einen wichtigen Beitrag zur Ausfallsicherheit.

Mehr Management.

Gerade im Outdoor-Bereich, wenn ein Blick auf die LEDs nicht so einfach möglich ist, weil der Access Point z. B. an einem hohen Mast hängt, ist ein Management System wichtig. Mit dem kostenfreien LANconfig können alle Gerätefunktionen zentral verwaltet werden. Zudem ist insbesondere für Hotspot-Szenarien mit einer Vielzahl verschiedener Clients, eine Optimierung des Funkfelds und der Netzlast von hoher Wichtigkeit. Mit Band Steering lenken Sie Dual Band Clients automatisch vom 2,4 GHz- auf das leistungsfähigere 5 GHz-Frequenzband. Mit Spectral Scan erhalten Sie außerdem ein kostenloses Tool zur Identifikation von WLAN-Störquellen für ein effizientes Netzwerk-Troubleshooting.

Besonders zukunftssicher.

LANCOM Produkte sind grundsätzlich auf eine langjährige Nutzung ausgelegt und verfügen daher über eine zukunftssichere Hardware-Dimensionierung. Selbst über Produktgenerationen hinweg sind Updates des LANCOM Operating Systems – LCOS – mehrmals pro Jahr kostenfrei erhältlich, inklusive "Major Features". LANCOM bietet so einen unvergleichlichen Investitionsschutz.

WLAN	
Frequenzband 2.4 GHz und 5 GHz	2400-2483,5 MHz (ISM) und 5150-5825 MHz (landesspezifische Einschränkungen möglich)
Übertragungsraten 802.11b/g	54 Mbit/s (Fallback auf 48, 36, 24, 18, 12, 9, 6 Mbit/s, Automatic Rate Selection) kompatibel zu IEEE 802.11b (11, 5,5, 2, 1 Mbit/s, Automatic Rate Selection), 802.11 b/g Kompatibilitätsmodus oder reiner g- oder reiner b-Betrieb einstellbar
Übertragungsraten 802.11a/h	54 Mbit/s nach IEEE 802.11a/h (Fallback auf 48, 36, 24, 18, 12, 9, 6 Mbit/s, Automatic Rate Selection), volle Kompatibilität mit TPC (Leistungseinstellung) und DFS (automatische Kanalwahl, Radarerkenkung) nach EN 300 328 und EN 302 502
Ausgangsleistung am Radiomodul, 2.4 GHz	802.11b: +19 dBm @ 1 und 2 Mbit/s, +19 dBm @ 5.5 und 11 Mbit/s 802.11g: +18 dBm @ 6 bis 36 Mbit/s, +17 dBm @ 48 Mbit/s, +16 dBm @ 54 Mbit/s; 802.11n: +19 dBm @ 6,5/13 Mbit/s (MCS0/8, 20 MHz), +10 dBm @ 65/130 Mbit/s (MCS7/15, 20 MHz), +17 dBm @ 15/30 Mbit/s (MCS0/8, 40 MHz), +10 dBm @ 150/300 Mbit/s (MCS7/15, 40 MHz)
Ausgangsleistung am Radiomodul, 5 GHz	802.11a/h: +18 dBm @ 6 bis 24 Mbit/s, +17 dBm @ 36 Mbit/s, +16 dBm @ 48 Mbit/s, +15 dBm @ 54 Mbit/s; 802.11n: +18 dBm @ 6,5/13 Mbit/s (MCS0/8, 20 MHz), +10 dBm @ 65/130 Mbit/s (MCS7/15, 20 MHz), +17 dBm @ 15/30 Mbit/s (MCS0/8, 40 MHz), +10 dBm @ 150/300 Mbit/s (MCS7/15, 40 MHz)
Ausgangsleistung am Radiomodul, 2.4 GHz (WLAN-2)	802.11b: 18 dBm @ 1 und 2 Mbit/s 18 dBm @ 5.5 und 11 Mbit/s 802.11g: 16 dBm @ 54 Mbit/s 802.11n: 15 dBm @ 65/130 Mbit/s (MCS7, 20 MHz) 15 dBm @ 150/300 Mbit/s (MCS7, 40 MHz)
Ausgangsleistung am Radiomodul, 5 GHz (WLAN-2)	802.11a/h: +12 dBm @ 54 Mbit/s 802.11n: +12 dBm @ 65/130 Mbit/s (MCS7, 20 MHz) +12 dBm @ 150/300 Mbit/s (MCS7, 40 MHz)
Max. abgestrahlte Leistung, 2.4 GHz Band	802.11b/g: Bis zu 20 dBm / 100 mW EIRP; Leistungsregulierung entsprechend TPC
Max. abgestrahlte Leistung, 5 GHz Band	802.11a/h: Bis zu 30 dBm / 1000 mW oder bis zu 36 dBm / 4000 mW EIRP mit entsprechend sendeseitig verstärkenden Antennen (je nach nationaler Regulierung zu Kanälen und Anwendungen sowie Vorgaben wie TPC und DFS)
Sendeleistung minimal	Sendeleistungsreduktion per Software in 1 dB-Schritten auf minimal 0,5 dBm
Empfangsempfindlichkeit 2.4 GHz	802.11b: -91 dBm @ 11 Mbit/s, -96 dBm @ 1 Mbit/s; 802.11g: -96 dBm @ 6 Mbit/s, -83 dBm @ 54 Mbit/s; 802.11n: -96 dBm @ 6,5 Mbit/s (MCS0, 20 MHz), -79 dBm @ 65 Mbit/s (MCS7, 20 MHz); -95 dBm @ 13 Mbit/s (MCS8, 20 MHz), -77 dBm @ 130 Mbit/s (MCS15, 20 MHz); -90 dBm @ 15 Mbit/s (MCS0, 40 MHz), -75 dBm @ 150 Mbit/s (MCS7, 40 MHz); -90 dBm @ 30 Mbit/s (MCS8, 40 MHz), -73 dBm @ 300 Mbit/s (MCS15, 40 MHz)
Empfangsempfindlichkeit 5 GHz	802.11a/h: -95 dBm @ 6 Mbit/s, -82 dBm @ 54 Mbit/s; 802.11n: -95 dBm @ 6,5 Mbit/s (MCS0, 20 MHz), -77 dBm @ 65 Mbit/s (MCS7, 20 MHz); -93 dBm @ 13 Mbit/s (MCS8, 20 MHz), -74 dBm @ 130 Mbit/s (MCS15, 20 MHz); -91 dBm @ 15 Mbit/s (MCS0, 40 MHz), -75 dBm @ 150 Mbit/s (MCS7, 40 MHz); -90 dBm @ 30 Mbit/s (MCS8, 40 MHz), -71 dBm @ 300 Mbit/s (MCS15, 40 MHz)
Empfangsempfindlichkeit 2.4 GHz (WLAN-2)	802.11b: -90 dBm @ 11 Mbit/s 802.11g: -76 dBm @ 54 Mbit/s 802.11n: -70 dBm @ 65 Mbit/s (MCS7, 20 MHz) -70 dBm @ 150 Mbit/s (MCS7, 40 MHz)
Empfangsempfindlichkeit 5 GHz (WLAN-2)	802.11a/h: -76 dBm @ 54 Mbit/s 802.11n: -69 dBm @ 65 Mbit/s (MCS7, 20 MHz) -68 dBm @ 150 Mbit/s (MCS7, 40 MHz)
Funkkanäle 2.4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (landesspezifische Einschränkungen möglich)
Funkkanäle 5 GHz	Bis zu 26 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS Kanalwahl verbunden)
Band Steering	Steuerung von WLAN Clients auf das 5 GHz-Frequenzband durch Unterbindung des Zugriffs auf das 2.4 GHz-Band.
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support mit optionaler Zuordnung eines ARF-Kontextes, IEEE 802.11d Support
WPA2 Fast Roaming	Pre-Authentication und PMK-Caching zur schnellen 802.1X-Authentifizierung
Fast Client Roaming	Durch das Background Scanning kann ein mobiler Access Point im Client-Betrieb bereits auf einen anderen Access Point mit stärkerem Signal wechseln, bevor die Verbindung zum aktuellen Access Point zusammenbricht.
VLAN	VLAN-ID einstellbar pro Schnittstelle, WLAN SSID, Punkt-zu-Punkt-Verbindung und Routing-Kontext (4.094 IDs) IEEE 802.1q
Dynamische VLAN-Zuweisung	Dynamische VLAN-Zuweisung für bestimmte Benutzergruppen anhand von MAC-Adressen, BSSID oder SSID mittels externem RADIUS-Server
Q-in-Q Tagging	Unterstützung von geschichtelten 802.1Q VLANs (double tagging)
Multi-SSID	Nutzung von bis zu 8 unabhängigen WLAN-Netzen gleichzeitig pro WLAN-Interface
IGMP-Snooping	Unterstützung des Internet Group Management Protocol (IGMP) in der WLAN-Bridge für WLAN SSIDs und LAN-Schnittstellen zur gezielten Weiterleitung von Multicast-Paketen. Behandlung von Multicast-Paketen ohne Registrierung einstellbar. Konfiguration statischer Mitglieder von Multicast-Gruppen pro VLAN-ID. Konfiguration simulierter Anfrager für Multicast-Mitgliedschaften pro VLAN-ID
Sicherheit	IEEE 802.11i / WPA2 mit Passphrase oder 802.1X und hardwarebeschleunigtem AES, Closed Network, WEP64, WEP128, WEP152, User Authentication, 802.1X /EAP, LEPS, WPA1/TKIP
RADIUS-Server	Integrierter RADIUS-Server zur Verwaltung von MAC-Adress-Listen
EAP-Server	Integrierter EAP-Server zur Authentisierung von 802.1X Clients mittels EAP-TLS, EAP-TTLS, PEAP, MS-CHAP oder MS-CHAP v2
Quality of Service	Priorisierung entsprechend der Wireless Multimedia Extensions (WME, Bestandteil von IEEE 802.11e)
U-APSD/WMM Power Save	Erweiterung des Power Savings nach IEEE 802.11e um Unscheduled Automatic Power Save Delivery (entsprechend WMM Power Save) zum Umschalten von WLAN Clients in einen Stromsparmodus. Erhöhung der Akkulebensdauer bei VoWLAN-Gesprächen (Voice over WLAN)
Bandbreitenlimitierung	Pro WLAN Client (MAC-Adresse) kann eine maximale Sende- und Empfangsrate sowie eine eigenständige VLAN-ID vorgegeben werden

WLAN	
Broken-Link-Detection	Das Fehlen eines Ethernet-Links an einem wählbaren LAN-Interface kann zum automatischen Deaktivieren eines WLAN-Moduls genutzt werden, damit Clients sich an alternativen Basisstationen anmelden können
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
802.1X Supplicant	Authentifizierung eines Access Points im WLAN Client-Modus über 802.1X (EAP-TLS, EAP-TTLS und PEAP) bei einem anderen Access Point
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.
LANCOM Spectral Scan	
Funkfeld-Scan (nur WLAN-2)	Bis zu 13 Kanäle (2.4 GHz) oder bis zu 26 Kanäle (5 GHz) (je nach länderspezifischen Regulierung und manueller Konfiguration)
Signalstärke in den WLAN-Kanäle (nur WLAN-2)	Anzeige der Signalstärke einzelner WLAN-Kanäle zu einem bestimmten Zeitpunkt
IEEE 802.11n Features	
MIMO	Die MIMO-Technologie (Multiple Input, Multiple Output) nutzt mehrere Funksender um räumlich getrennte Datenströme simultan zu übertragen. Je nach Signalstärke kann der Datendurchsatz mit der MIMO-Technologie sogar verdoppelt werden
40 MHz Kanäle	Zwei benachbarte 20 MHz Kanäle können kombiniert und zu einem gemeinsamen 40 MHz Kanal gebündelt werden. Je nach Signalstärke kann hierdurch der Datendurchsatz verdoppelt werden
20/40 MHz Koexistenz-Mechanismus im 2.4GHz Band	Unterstützt die Koexistenz von Access Points mit 20 und 40MHz Kanälen im 2.4GHz Band
MAC Aggregation und Block Acknowledgement	Das Feature MAC Aggregation steigert die Effizienz des 802.11-Standards durch die Kombination mehrerer MAC-Datenpakete mit einem gemeinsamen Header. Der Empfänger quittiert den Empfang der Datensequenz mit einem Block Acknowledgement. Je nach Signalstärke kann diese Technik den Datendurchsatz um bis zu 20% verbessern
Space Time Block Coding (STBC) (nur WLAN-2)	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) (nur WLAN-2)	Low Density Parity Check (LDPC) ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standard Methode zur Fehlerkorrektur Convolution Coding (CC) und optional die effektivere Methode Low Density Parity Check (LDPC).
Maximal Ratio Combining (MRC)	Maximal Ratio Combining (MRC) ermöglicht dem Empfänger (Access Point), im Zusammenspiel mit mehreren Antennen, MIMO Signale optimal zu kombinieren und dadurch den Empfang von Clients zu verbessern.
Kurzes Guard Interval	Das Guard Interval ist die Zeitspanne zwischen einzelnen OFDM-Symbolen. IEEE 802.11n ermöglicht ein kurzes 400 nsec Guard Interval anstelle des klassischen 800 nsec Guard Intervals
WLAN-Betriebsarten	
WLAN Access Point	Infrastruktur-Modus (autonomer Betrieb oder gemanagt durch LANCOM WLAN Controller)
WLAN Router	Verwendung des LAN-Anschlusses für gleichzeitiges DSL-over-LAN, IP-Router, NAT/Reverse NAT (IP-Masquerading) DHCP-Server, DHCP-Client, DHCP-Relay-Server, DNS-Server, PPPoE-Client (inkl. Multi-PPPoE), PPTP-Client und -Server, NetBIOS-Proxy, DynDNS-Client, NTP, Port-Mapping, Policy-based Routing auf Basis von Routing-Tags, Tagging anhand von Firewall-Regeln, dynamisches Routing mit RIPv2, VRRP
WLAN Client	Transparenter WLAN Client-Modus für die drahtlose Verlängerung eines Ethernets (z.B. Anbindung von PCs oder Druckern mit Ethernet-Anschluss, bis zu 64 MAC-Adressen). Automatische Auswahl eines WLAN-Profiles (max. 8) mit individuellen Zugangsparametern in Abhängigkeit von Signalstärke oder Priorität
Spectral Scan (nur WLAN-2)	Durch einen Scan des Funkspektrums werden automatisch nicht-WLAN-Störquellen identifiziert und grafisch dargestellt.
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

Firewall	
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
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
WLAN Protokollfilter	Beschränkung auf die im WLAN erlaubten Übertragungsprotolle sowie Eingrenzung der Quell- und Zieladressen
IP-Redirect	Feste Umleitung aller auf dem WLAN empfangenen Pakete an eine bestimmte Zieladresse
Hochverfügbarkeit / Redundanz	
VRRP	VRRP (Virtual Router Redundancy Protocol) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall. Ermöglicht passive Standby-Gruppen oder wechselseitige Ausfallabsicherung 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
Leitungsüberwachung	Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling
Routingfunktionen	
Router	IP- und NetBIOS/IP-Multiprotokoll-Router, IPv6-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 (Wildcard) im Namen
DHCPv6	DHCPv6-Client, DHCPv6-Server, DHCPv6-Relay, Stateless- und Stateful-Modus, IPv6-Adresse (IA_NA), Präfix-Delegierung (IA_PD)
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

Layer-2-Funktionen	
LLDP	LLDP-Unterstützung zur automatischen Erkennung der im Netzwerk eingebundenen Geräte auf Layer-2.
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
Rapid Spanning Tree	Unterstützung von IEEE 802.1d Spanning Tree und IEEE 802.1w Rapid Spanning Tree zur dynamischen Pfadwahl bei redundanten Layer-2-Anbindungen
IPv6	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, TCP, UDP
Dual Stack	IPv4/IPv6 Dual Stack
IPv6-kompatible LCOS-Anwendungen	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, Firewall
WAN-Protokolle	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC oder PNS) und IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IP
IPv6	IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IPoE (Autokonfiguration, DHCPv6 oder Statisch)
Tunnelprotokolle (IPv4/IPv6)	6to4, 6in4, 6rd (statisch und über DHCP)
xDSL (ext. Modem)	ADSL1, ADSL2 oder ADSL2+ mit externem ADSL2+-Modem
Schnittstellen	
ETH1	10/100/1000 Mbit/s, Autosensing
ETH2	10/100 Mbit/s, Autosensing
Externe Antennenanschlüsse	Vier N-Anschlüsse für externe LANCOM AirLancer-Extender-Antennen oder Antennen anderer Hersteller. Bitte berücksichtigen Sie die gesetzlichen Bestimmungen Ihres Landes für den Betrieb von Antennensystemen. Zur Berechnung einer konformen Antennen-Konfiguration finden Sie Informationen unter www.lancom.de
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 & Monitoring	
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
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+

Management & Monitoring	
Benutzerverwaltung	RADIUS-Benutzerverwaltung für Einwahlzugänge (PPP/PPTP). Unterstützung von RADSEC (Secure RADIUS) zur sicheren Anbindung an RADIUS-Server
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. Schaltbare Umgehung von TACACS+ für CRON, Aktionstabelle und Script-Abearbeitung 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
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
HTTPS Server	Auswahl, ob ein hochgeladenes oder das Default-Zertifikat für den HTTPS Server verwendet werden soll
Large Scale Monitor (LSM)	Der LANCOM Large Scale Monitor (LSM) ist ein professionelles Werkzeug zum Überwachen von mittleren und großen Netzwerken mit 25 bis zu 1.000 Netzwerkkomponenten. Optimal auf alle LANCOM Komponenten wie WLAN Access Points, Controller, Switches und Router abgestimmt, bietet das offene System und die Verwendung von Open-Source Komponenten darüber hinaus die Möglichkeit, auch Fremdprodukte wie z. B. Server und Drucker mit in die Überwachung zu übernehmen. Netzwerkprobleme werden übersichtlich in Tabellen oder auf Karten und Floorplans grafisch dargestellt und führen zu Benachrichtigungen per E-Mail beim Über- oder Unterschreiten von Grenzwerten.
Sicherheit	Zugriff über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbar (Telnet/SSL, SSH, SNMP, HTTPS/HTTP), Access Control List
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
LANCOM WLAN Controller	Unterstützt durch alle LANCOM WLAN Controller (separate optionale Hardware-Komponente zur Installation, Optimierung, Betrieb und Überwachung von WLAN-Funknetzen, außer P2P-Verbindungen)
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	
Größe	255 mm x 250 mm x 80 mm (Länge/Breite/Tiefe)
Gewicht	Gewicht eines OAPs ca. 3 kg inkl. kompletter Mastbefestigungsvorrichtung
LED Anzeigen	5 LEDs für Power, Ethernet 1, Ethernet 2, WLAN1 und WLAN2
Spannungsversorgung	10-28 V Eingangsspannung, optional erhältlich: 24 V Spannungsversorgungsnetzteil LANCOM OAP-320 PSU
Spannungsversorgung	Über Power-over-Ethernet, max. Entfernung zw. Access Point, Power over Ethernet Injektor und Switch darf 100 m nicht überschreiten, 1 x PoE Injektor im Lieferumfang enthalten*

Hardware	
Reset Taster	Konfigurierbarer Reset Taster für Reset und Booten des Gerätes
Umgebung	bei 10 V Eingangsspannung: -33° C bis 55° C, bei 24 V Eingangsspannung: -33° C bis 70° C
Gehäuse	Robustes Metallgehäuse, Schutzklasse IP 66, für Wand- und Mastmontage vorbereitet, Hinweis: bei Aufstellung in Salzwasserumgebungen ist ein geeignetes Umgehäuse zu verwenden
Konformitätserklärungen	
CE	EN 60950-1, EN 301 489-1, EN 301 489-17
2.4 GHz WLAN	EN 300 328
5 GHz WLAN	EN 301 893 Version 1.6.1
Notifizierungen	Notifiziert in den Ländern Deutschland, Belgien, Niederlande, Luxemburg, Österreich, Schweiz, Großbritannien, Italien, Spanien, Frankreich, Portugal, Tschechien, Dänemark
IPv6	IPv6 Ready Gold
Lieferumfang	
Handbuch	Hardware-Schnellübersicht (DE/EN), Installation Guide (DE/EN/FR/ES/IT/PT/NL)
CD/DVD	Datenträger mit Management Software (LANconfig, LANmonitor, LANCAP) und LCOS Dokumentation
Kabel	Wasserdichtes, UV-beständiges Ethernet-PoE-Kabel, einseitig mit Schraubverbindung, 15m
Antennen	Vier 3 dBi Dipol-Dualband-Antennen
Support	
Garantie	3 Jahre, Support über Hotline und Internet KnowledgeBase
Software-Updates	Regelmäßige kostenfreie Updates (LCOS Betriebssystem und LANCOM Management System) via Internet
Optionen	
Vorabaustausch	LANCOM Next Business Day Service Extension IAP & OAP, Art.-Nr. 61412
Garantie-Erweiterung	LANCOM 2-Year Warranty Extension IAP & OAP, Art.-Nr. 61415
Public Spot	LANCOM Public Spot Option (Authentifizierungs- und Accounting-Software für Hotspots, inkl. Voucher-Druck über Standard-PC-Drucker), Art.-Nr. 60642
Geeignetes Zubehör	
LANCOM Large Scale Monitor	Leistungsstarkes Monitoring- und Überwachungssystem für mittlere und große Netzwerke, erweiterbar bis 1000 überwachte Geräte, für proaktives Fehlermanagement, browserbasiertes Remote-Monitoring, intuitive Benutzeroberfläche, grafische Floorplans, einstellbare Trigger für Alarime + Benachrichtigungen, Benutzer-, Rollen- und Rechteverwaltung, Art.-Nr. 62910
LANCOM WLC-4006+ (EU/UK/US)	LANCOM WLAN Controller zum zentralen Management für 6 (optional bis 30) LANCOM Access Points und WLAN Router, Art.-Nr. 62035 (EU), Art.-Nr. 62036 (UK) und Art.-Nr. 62037 (US)
LANCOM WLC-4025+ (EU/UK/US)	LANCOM WLAN Controller zum zentralen Management für 25 (optional bis 100) LANCOM Access Points und WLAN Router, Art.-Nr. 61378 (EU), Art.-Nr. 61379 und Art.-Nr. 61384 (US)
LANCOM WLC-4100 (EU/UK)	LANCOM WLAN Controller zum zentralen Management für 100 (optional bis 1000) LANCOM Access Points und WLAN Router, Art.-Nr. 61369 (EU) und Art.-Nr. 61377 (UK)
Externe Antenne	AirLancer Extender O-30 2.4 GHz Outdoorantenne, Art.-Nr. 60478
Externe Antenne	AirLancer Extender O-70 2.4 GHz Outdoorantenne, Art.-Nr. 60469
Externe Antenne	AirLancer Extender O-9a 5 GHz Outdoorantenne, Art.-Nr. 61220
Externe Antenne	AirLancer Extender O-18a 5 GHz Outdoorantenne, Art.-Nr. 61210
Externe Antenne*	AirLancer Extender O-D80g 2.4 GHz "Dual Linear" Polarisationsdiversity Outdoor-Sektorantenne, Art.-Nr. 61221
Externe Antenne*	AirLancer Extender O-D60a 5 GHz "Dual Linear" Polarisationsdiversity Outdoor-Sektorantenne, Art.-Nr. 61222
Externe Antenne	AirLancer Extender O-360ag Dualband Rundstrahl-Outdoorantenne, Art.-Nr. 61223
Externe Antenne*	AirLancer Extender O-D9a 5 GHz "Dual Linear" Polarisationsdiversity Outdoorantenne, Art.-Nr. 61224
Antennenkabel	AirLancer Cable NJ-NP 3m Antennenkabel-Verlängerung zum Anschluss von LANCOM Outdoor-Antennen, Art.-Nr. 61230
Antennenkabel	AirLancer Cable NJ-NP 6m Antennenkabel-Verlängerung zum Anschluss von LANCOM Outdoor-Antennen, Art.-Nr. 61231
Antennenkabel	AirLancer Cable NJ-NP 9m Antennenkabel-Verlängerung zum Anschluss von LANCOM Outdoor-Antennen, Art.-Nr. 61232
Überspannungsschutz (Antennenkabel)	AirLancer Extender SA-5L Überspannungsschutz, wird zwischen Antenne und Access Point geschaltet, 2.4 und 5 GHz, Art.-Nr. 61553

Geeignetes Zubehör	
Überspannungsschutz (LAN-Kabel)	AirLancer Extender SA-LAN Überspannungsschutz für LAN-Kabel, Art.-Nr. 61213
LAN-Kabel (Outdoor)	LANCOM OAP-320 Ethernet Cable (30 m), Art.-Nr. 61347
*) Hinweis	Für Polarisations-Diversity-Antennen werden je zwei Kabel und Überspannungsschutzadapter benötigt!
Artikelnummern	
LANCOM OAP-322	61552
LANCOM OAP-320 PSU	61690 (EU), Spannungsversorgungsnetzteil für LANCOM OAP-321-3G, LANCOM OAP-3G und OAP-322